paloalto TECHDOCS

Administration Prisma Access

4.00 and later



docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2022-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

April 23, 2025

Table of Contents

Vue d'ensemble du Prisma Access 13

Sécuriser le trafic Internet en utilisant Prisma Access 17

L'importance de la sécurité Internet 17

Prisma Access Passerelle Web Sécurisée Cloud (SWG) 17

Utiliser Prisma Access pour sécuriser les utilisateurs et les points de terminaison 18

Comment gérer Prisma Access 19

Visibilité et surveillance de Prisma Access avec Strata Cloud Manager 23

Prisma Access emplacements 25

Emplacements de calcul, ville et pays 26

Théâtre et groupe d'emplacements 31

Emplacements par région 35

Emplacements de proxy explicite 40

Emplacement Colo Connect : 41

Régions Strata Logging Service prises en charge 42

Emplacements de type Réseaux distants : hautes performances, Réplication du trafic et Accès entrant sécurisé 43

Emplacements Prisma Access Chine 46

Emplacements FedRAMP modéré et élevé 46

Carte des emplacements en Amérique du Nord 46

Emplacements de zones locales 47

Prisma Access et les emplacements de traitement des services associés 48

Gestion de l'infrastructure Prisma Access 50

API Prisma Access 52

API pour Prisma Access (Managed by Strata Cloud Manager) 52

API pour Prisma Access (Managed by Panorama) 52

Accéder à l'API Prisma Access (Managed by Panorama) à l'aide du navigateur et l'interface web 53

Utiliser les commandes curl pour récupérer des commandes d'API gérée par Panorama 55

Utiliser les commandes CLI avec Prisma Access (Managed by Panorama) 56

API Prisma Access Insights 56

Migrer Prisma Access de Panorama vers Strata Cloud Manager 58

Préparer la migration vers Prisma Access (Managed by Strata Cloud Manager) 58

Migrer le déploiement Prisma Access (Managed by Panorama) vers Strata Cloud Manager 59

Prisma Access Versions et mises à niveau 73

Prisma Access Types de version 74

 ©2025 Palo Alto Networks, Inc.

Mises à niveau urgentes programmées....75
Types de mise à niveau de Prisma Access....76
Cadence des mises à jour logicielles et de contenu pour Prisma Access....79
Mises à niveau du plan de données de Prisma Access....87
Recevoir des alertes de mise à niveau et des mises à jour....93
Afficher les versions logicielles de Prisma Access....99
Prisma Access (Managed by Strata Cloud Manager)....99
Prisma Access (Managed by Panorama)....100
Configuration Prisma Access....105
Configurer Prisma Access....107
Configurer l'infrastructure de service Prisma Access....115
Utilisateurs mobiles : Allocation d'adresses IP....130
Exemple : exemples de mise à l'échelle des adresses IP publiques (utilisateurs mobiles)....131
Allocation d'adresses IP de bouclage (utilisateurs mobiles)....133
Réseaux distants : Nœuds de terminaison IPSec et Adresses IP de service....136
Réseaux distants : Modifications de l'adresse IP liées à l'allocation de la bande passante....137
Réseaux distants : Adresse IP de service et allocation d'adresses IP de sortie....140
Récupérer les adresses IP pour Prisma Access....141
Optimisation IP pour les déploiements de type Utilisateurs mobiles – GlobalProtect....170
Exemples d'API pour la récupération d'adresses IP Prisma Access....172
Recevoir des notifications lorsque les adresses IP Prisma Access changent....175
Utiliser des scripts hérités pour récupérer les adresses IP....177
Récupérer les adresses IP des utilisateurs mobiles....179
Récupérer les adresses IP publiques, de bouclage et de sortie....180
Prisma Access Zones....183
DNS pour Prisma Access....185
High Availability (haute disponibilité - HA) pour Prisma Access....191
Modèles prédéfinis : Intégrer une connexion aux services ou un réseau distant....194
Profils cryptographiques IKE et IPSec pris en charge pour les périphériques SD-WAN courants....199
Prisma Access Connexions aux services....201
Planifier une connexion aux services....203
Rassembler ces informations sur le HQ ou le centre de données....203
Configurer une connexion aux services dans Prisma Access....205
Utiliser une connexion aux services pour permettre l'accès entre les utilisateurs mobiles et les réseaux distants....235
Considérations sur le routage dynamique pour les connexions aux services....237

 ©2025 Palo Alto Networks, Inc.

Fonctionnement — Routage du trafic de connexion aux services 237
Prisma Access Routage par défaut 238
Routage hot potato 241

Connecteur ZTNA Prisma Access 247

Composants du connecteur ZTNA 249
Cas d'utilisation du connecteur ZTNA 250
Cas d'utilisation pris en charge pour les connexions aux services et le connecteur ZTNA 254
Principes du connecteur ZTNA 2.0 255
Exigences et directives du connecteur ZTNA 256
Versions de Prisma Access prises en charge configuration requise 256
Prises en charge des applications 257
Restrictions relatives aux caractéristiques et aux fonctionnalités 258
Considérations relatives à l'échelle et au débit 259
Prise en charge des environnements d'hébergement d'applications 259
Configuration réseau requise 260
Adresses IP et FQDN pour autoriser le connecteur ZTNA 262
Gestion des certificats 265
Activer le connecteur ZTNA 267
Configurer le connecteur ZTNA 274
Mettre à niveau les connecteurs ZTNA 284
Outils de diagnostic de connecteur ZTNA 287
Supprimer des blocs IP de connecteur 295
Configurer la découverte automatique des applications à l'aide de Cloud Identity Engine 300
Découverte de cibles d'applications privées 301
Politique de sécurité pour les applications activées avec le connecteur ZTNA 308
Intégrer la VM du connecteur ZTNA dans votre centre de données 326
Déploiements pris en charge du connecteur ZTNA 326
Déploiements Microsoft Azure pris en charge par le connecteur ZTNA 330
Déploiements de Google Cloud Platform pris en charge par le connecteur ZTNA 347
Déploiements d'Amazon Web Services pris en charge par le connecteur ZTNA 359
Déploiements VMware ESXi pris en charge par le connecteur ZTNA Prisma Access 367
Déploiements de KVM pris en charge par le connecteur ZTNA Prisma Access 378
Déploiements Hyper-V pris en charge par le connecteur ZTNA de Prisma Access 384
Surveiller le connecteur ZTNA 398

 ©2025 Palo Alto Networks, Inc.

Afficher les journaux du connecteur ZTNA..... 401
Préserver le mappage User-ID pour les connexions de connecteurs ZTNA avec le source NAT.....404

Configurer les paramètres d'accès à privilèges dynamique..... 413

Qu'est-ce que l'accès à privilèges dynamique ?..... 414
Activer l'accès à privilèges dynamique pour Prisma Access via Common Services.....416
Autoriser le mappage des groupes d'utilisateurs dans Cloud Identity Engine pour l'accès à privilèges dynamiques.....418
Activer l'agent d'accès.....426
Configurer l'infrastructure de l'agent pour l'accès à privilèges dynamique.....428
- Configurer les paramètres d'infrastructure.....428
- Sélectionner les emplacements Prisma Access.....430
- Activer le support SC-NAT pour l'accès à privilèges dynamique.....434
- Activer le résumé de l'itinéraire pour l'accès à privilèges dynamique.....435

Créer un extrait.....438
Configurer les paramètres Prisma Access Agent spécifiques au projet.....441
- Configurer les profils de transfert pour gérer le trafic des agents pour les agents d'accès à privilège dynamique.....441
- Configurer les paramètres de l'application Prisma Access Agent pour l'accès à privilèges dynamique.....456
- Configurer les paramètres DNS pour l'accès à privilèges dynamique.....461
- Configurer les paramètres de collecte de données HIP pour l'accès à privilèges dynamique.....462

Créer un projet.....467
Redirection du trafic pour l'accès à privilèges dynamique.....471
Configurer le Prisma Access Agent pour l'accès à privilèges dynamique.....473
- Configurer les déploiements par étapes pour le Prisma Access Agent.....473
- Configurez les paramètres globaux généraux pour Prisma Access Agents.....484
- Configurer les notifications HIP pour l'accès à privilèges dynamique Prisma Access Agent.....488

Transmettez les Prisma Access Agent la configuration.....498
Télécharger le package Prisma Access Agent activé par accès à privilèges dynamique.....501
Utiliser le Prisma Access Agent pour accéder à vos projets..... 503
- Installer Prisma Access Agent..... 503
- Se connecter à Prisma Access Agent compatible avec l'accès à privilèges dynamique..... 511
- Modifier les préférences pour l'accès à privilèges dynamiques activé Prisma Access Agent..... 514

 ©2025 Palo Alto Networks, Inc.

Connecter l'accès à privilèges dynamique activé Prisma Access Agent vers un autre emplacement 515
Changer de projet 516
Connecter l'accès à privilèges dynamique activé Prisma Access Agent vers un autre serveur 517
Basculer entre Prisma Access Agent et l'application GlobalProtect 519
Afficher et surveiller les utilisateurs de l'accès à privilèges dynamiques 521
Utilisateurs connectés 521
Afficher et surveiller les projets de l'accès à privilèges dynamiques 527
Projets 527

Prisma Access Colo-Connect 531

Cas d'utilisation de Colo-Connect 533
Accès à large bande passante aux applications privées 533
Connectivité privée pour les applications privées 533
Utilisation d'un fournisseur NaaS tiers 533
En quoi Colo-Connect est-il différent des connexions aux services et du connecteur ZTNA ? 535
Caractéristiques et fonctionnalités non prises en charge par Colo-Connect 536
Exigences et conditions préalables pour Prisma Access Colo-Connect 537
Configurer Prisma Access Colo-Connect 539

Accélération des applications dans Prisma Access 595

Exigences et directives en matière d'accélération des applications 597
Configurer l'accélération des applications 600

Utilisateurs mobiles Prisma Access 625

Utilisateurs mobiles : GlobalProtect 627
Liste de contrôle de planification pour GlobalProtect sur Prisma Access 628
Configurer les utilisateurs mobiles GlobalProtect 631
GlobalProtect – Personnaliser les paramètres de tunnel 667
GlobalProtect – Personnaliser les paramètres de l'application 672
Requête de ticket pour désactiver GlobalProtect 684
Préouverture de session GlobalProtect 689
GlobalProtect — VPN sans client 706
Surveiller les utilisateurs mobiles GlobalProtect 708
Pools d'adresses IP pour un déploiement de type Utilisateurs mobiles – GlobalProtect 714
Comment l'application GlobalProtect sélectionne des emplacements Prisma Access pour les utilisateurs mobiles 720
Liste d'autorisation des utilisateurs mobiles de GlobalProtect 722
Mises à niveau de l'application GlobalProtect 734

 ©2025 Palo Alto Networks, Inc.

Intégrer Prisma Access à des passerelles GlobalProtect sur site 743
Utilisateurs mobiles : Proxy explicite 754
Directives de configuration du proxy explicite 757
GlobalProtect en mode proxy 762
GlobalProtect en mode tunnel et proxy 778
Visibilité et application de l'adresse IP privée pour le trafic de proxy basé sur l'agent 801
Authentification SAML pour le proxy explicite 803
Configurer un proxy explicite 806
Authentification Kerberos pour les déploiements de proxy explicite 830
Authentification Cloud Identity Engine pour les déploiements de proxy explicite 864
Mode proxy sur les réseaux distants 870
Comment le proxy explicite identifie les utilisateurs 881
Profils de transfert de proxy explicite 883
Directives relatives aux fichiers PAC 892
Bonnes pratiques en matière de proxy explicite 899
Surveiller et dépanner le proxy explicite 900
Paramètres de blocage pour le proxy explicite 903
Utiliser des objets spéciaux pour limiter le trafic Internet proxy explicite à des adresses IP spécifiques 906
Accéder au centre de données à l'aide d'un proxy explicite 906
Intégration d'Office 365 basée sur une application avec le proxy explicite 910
Configurer le chaînage de proxy avec le proxy Blue Coat 914
Utiliser un proxy explicite avec GlobalProtect (ou un VPN tiers) 920
Optimisation de l'adresse IP pour les utilisateurs de proxys explicites : déploiements de proxys 934
Résolution DNS pour les utilisateurs mobiles — Déploiements de proxys explicites 935
Afficher des mappages de l'utilisateur à l'adresse IP ou à des groupes 937
Signaler les problèmes d'accès au site pour les utilisateurs mobiles 943
Permettre aux utilisateurs mobiles de s'authentifier auprès de Prisma Access 945
Support et fonctionnalités d'authentification 947
Configurer l'authentification 952
Permettre aux utilisateurs mobiles d'accéder aux ressources de l'entreprise 958

Prisma Access Réseaux distants 963

Liste de contrôle de planification pour les réseaux distants 964
Allouer de la bande passante au réseau distant 969
Planifier votre migration vers le nouveau modèle 984

 ©2025 Palo Alto Networks, Inc.

Allocation de bande passante pour un déploiement de bande passante agrégée migrée....987
Directives relatives à la migration QoS....989
Migrer les paramètres de gestion de la bande passante....994
Intégrer un réseau distant....1002
Connecter un site de réseau distant à Prisma Access....1029
Ajouter des tunnels VPN IPSec principaux et secondaires....1029
Plus d'options IKE....1030
Plus d'options IPSec....1032
Activer le routage pour votre réseau distant....1033
Résoudre les problèmes de connexion au site....1036
Intégrer plusieurs réseaux distants....1038
Champs du tableau des réseaux distants....1040
Vérifier si le réseau distant est connecté à Prisma Access....1051
Vérifier l'état BGP de la connexion à distance....1053
Configurer un réseau distant et une connexion aux services connectés via un lien WAN....1055
QoS pour les réseaux distants....1058
Modifier la bande passante garantie....1077
Réseaux distants : haute performance....1081
Capacités et lignes directrices des réseaux distants hautes performances....1081
Intégration d'une VDI de bureau partagé à Prisma Access à l'aide d'un serveur de terminaux....1103

Surveillance et visibilité de Prisma Access....1113

Journaux Prisma Access....1115
Journaux externes et autres données....1117
Prisma Access Tableaux de bord et rapports Activité....1118
Afficher et surveiller Prisma Access dans Strata Cloud Manager....1120
Premiers pas avec la surveillance de Prisma Access dans Strata Cloud Manager....1122
Afficher et surveiller les applications....1124
Afficher et surveiller l'accélération des applications....1127
Afficher les utilisateurs mobiles....1129
Afficher et surveiller IPv6 pour les utilisateurs mobiles....1129
Afficher et surveiller les sites des succursales....1131
Afficher et surveiller les centres de données....1139
Afficher et surveiller les services réseau....1158
Afficher l'utilisation de l'abonnement....1163
Afficher et surveiller les emplacements Prisma Access....1165
Afficher et surveiller les Device-ID tiers....1167

 ©2025 Palo Alto Networks, Inc.

Afficher et surveiller l'isolation de navigateur à distance....1169
Prisma Access et Autonomous DEM....1171

Prisma Access Politique basée sur l'utilisateur....1173

Configurer la stratégie basée sur l'utilisateur pour Prisma Access....1174
Intégrer le Cloud Identity Engine à Prisma Access....1177
Récupérer les mappages de groupe User-ID pour Prisma Access....1184
Redistribution d'identité....1194
Configurer Third-Party Device-ID dans Prisma Access....1211
API d'identification de périphériques tiers....1218
Mettre à jour les verdicts....1218
Supprimer tous les verdicts....1221
Verdicts de requête....1222
Interroger les verdicts par adresse IP....1224
Statistiques du Verdict de requête....1225

Multilocation Prisma Access....1227

Présentation de la configuration multilocataire....1228
Planifier votre déploiement multilocataire....1233
Créer un tout nouveau déploiement multilocataire....1236
Activer le multilocataire et migrer le premier locataire....1237
Ajouter des locataires à Prisma Access....1244
Supprimer un locataire....1250
Créer un utilisateur administrateur au niveau du locataire....1255
Contrôler l'accès basé sur les rôles pour les utilisateurs administrateur au niveau du locataire....1259
Supprimer l'accès au plug-in pour un utilisateur administrateur de niveau locataire....1260
Trier les journaux par ID de groupe de périphériques dans un déploiement multilocataire....1265

Prisma Access dans un environnement FedRAMP....1267

Exigences FedRAMP de Prisma Access....1268
Conditions préalables à l'installation et à l'activation du produit....1268
Versions requises de Panorama, du plug-in et du plan de données PAN-OS....1269
Emplacements FedRAMP pris en charge par Prisma Access....1271
Fonctionnalités prises en charge et non prises en charge dans un déploiement Prisma Access FedRAMP....1271
Configurer Prisma Access dans un environnement FedRAMP....1273

Déploiements Prisma Access avancés....1279

 ©2025 Palo Alto Networks, Inc.

Ajouter un nouvel emplacement de calcul pour un emplacement Prisma Access déployé....1281
Prise en charge de l'IPv6....1283
Présentation de la prise en charge de l'IPv6 natif....1285
Activer et configurer la mise en réseau IPv6 et les pools d'adresses IP dans votre infrastructure Prisma Access....1289
Activer la mise en réseau IPv6 pour les utilisateurs mobiles – Déploiement de GlobalProtect....1297
Activer la mise en réseau IPv6 pour les connexions aux services....1302
Activer la mise en réseau IPv6 pour les réseaux distants....1309
Résolution DNS pour les utilisateurs mobiles – Déploiements GlobalProtect et de réseaux distants....1319
Résolution DNS pour les déploiements d'utilisateurs mobiles GlobalProtect....1321
Résolution DNS pour les réseaux distants....1323
Comment BGP annonce les pools d'adresses IP des utilisateurs mobiles pour les connexions aux services et les connexions au réseau distant....1325
Prise en charge du proxy pour Prisma Access et Strata Logging Service....1327
Bloquer les connexions entrantes en provenance de pays spécifiques....1328
Sécuriser le trafic Internet depuis AWS WorkSpace....1329
Configurer d'un fichier PAC sur les clients AWS WorkSpace....1329
Configurer un tunnel de site à site entre AWS et Prisma Access....1331
Prisma Access pour les réseaux sans itinéraire par défaut....1332
Qu'est-ce qu'un réseau sans itinéraire par défaut ?....1332
Considérations relatives aux réseaux sans itinéraire par défaut....1332
Recommandations de déploiement pour sécuriser l'accès à Internet pour les réseaux sans itinéraire par défaut....1332
Considérations clés....1333
Prisma Access Déploiements avancés de connexion aux services....1334
Redondance multicloud des connexions aux services....1334
Utiliser la redirection du trafic pour transférer le trafic lié à Internet aux connexions aux services....1345
Routage pour le trafic de connexion aux services....1371
Créer un réseau à large bande passante à l'aide de plusieurs connexions aux services....1384
Préserver le mappage de User-ID et Device-ID pour les connexions aux services avec NAT source....1398
Déploiements Utilisateurs mobiles – GlobalProtect avancés dans Prisma Access....1407
Configurer plusieurs portails dans Prisma Access....1407
Prise en charge de l'enregistrement DNS dynamique pour le dépannage et les mises à jour à distance....1418

 ©2025 Palo Alto Networks, Inc.

Prise en charge de l'enregistrement DNS dynamique pour les utilisateurs mobiles – GlobalProtect....1434
Identification et mise en quarantaine des périphériques compromis dans un déploiement GlobalProtect Prisma Access....1441
Trafic de l'entonnoir IPv6 chez les utilisateurs mobiles : déploiements GlobalProtect....1451
Redistribuer les informations HIP avec Prisma Access....1455
Voir les rapports HIP....1465
Prise en charge de l'encodage Gzip dans un VPN sans client....1467
Réplication du trafic dans Prisma Access....1469
Prisma Access Déploiements avancés de réseau à distance....1482
Passerelle interne Prisma Access....1482
Fournir un accès sécurisé entrant aux emplacements réseau distants....1493
Prisma Access pour Clean Pipe....1521
Vue d'ensemble de Prisma Access pour Clean Pipe....1522
Cas d'utilisation de Clean Pipe....1522
Exemples de configuration Clean Pipe....1523
Exigences relatives à l'interconnexion Clean Pipe et partenaire....1524
Terminer la configuration de Clean Pipe....1526
Activer le multilocataire et créer un locataire....1531

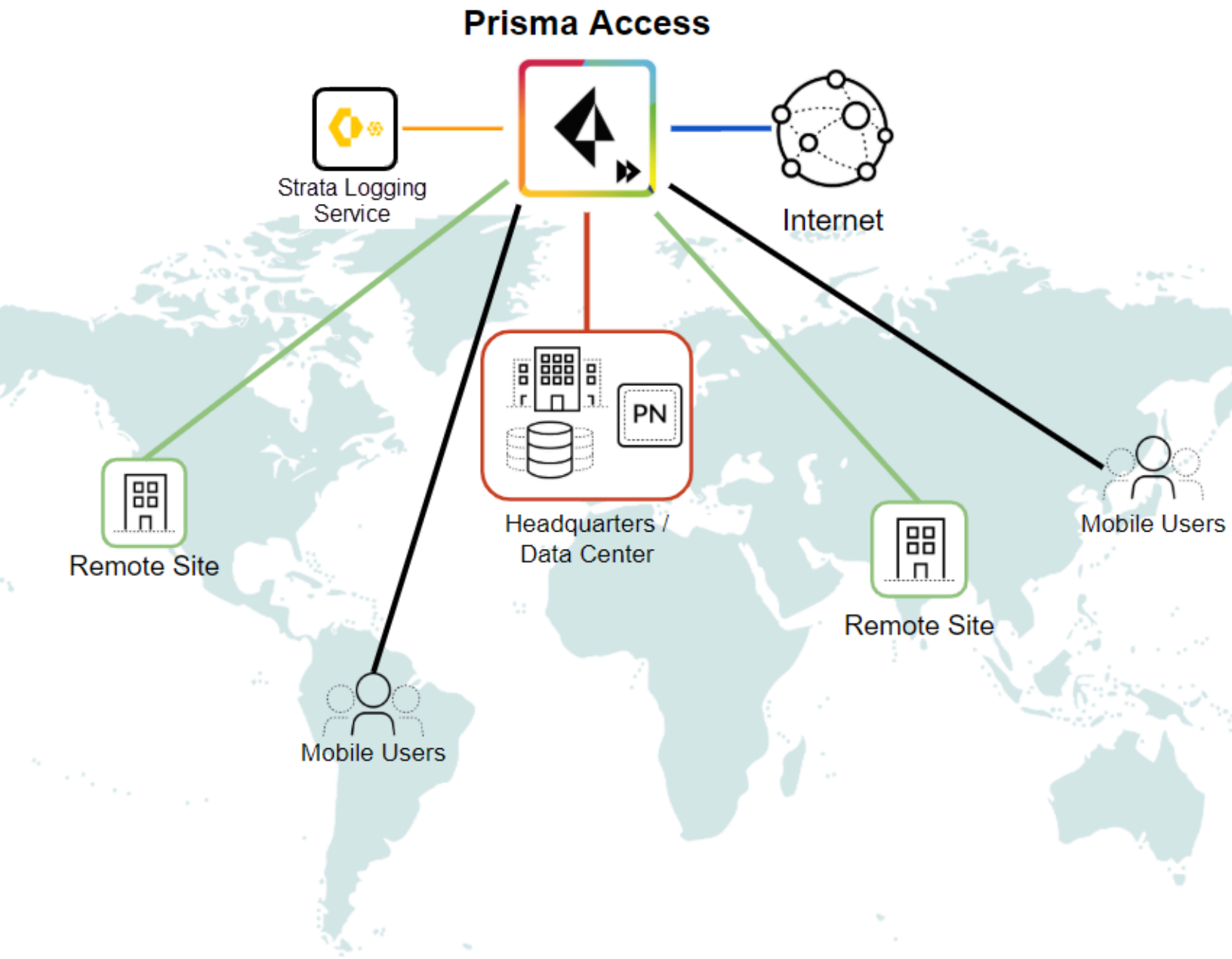
 ©2025 Palo Alto Networks, Inc.

Vue d’ensemble du Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Pour assurer la sécurité de vos applications et de vos données, vous devez sécuriser tous les utilisateurs à tous les emplacements, en tout temps. Mais comment y parvenir alors que votre empreinte s’étend à l’échelle mondiale, que de plus en plus d’utilisateurs sont mobiles et que vos applications et données sortent de votre réseau et sont transférées dans le cloud ? Prisma Access Cette sécurité cohérente permet à vos utilisateurs d’accéder en toute sécurité aux applications du cloud et du datacenter, ainsi qu’à Internet, qu’ils se trouvent à votre siège social, dans vos succursales ou en déplacement. Prisma Access Inspecte en permanence tout le trafic sur tous les ports, permettant un accès sécurisé à Internet, ainsi qu’à vos applications SaaS approuvées, à vos environnements de cloud public, à vos centres de données et à votre siège social. La prévention des menaces, la prévention des logiciels malveillants, le filtrage d’URL, le déchiffrement SSL et les politiques basées sur les applications sont intégrés pour vous fournir le même niveau de sécurité, quel que soit l’endroit où se trouvent vos utilisateurs ou les ressources auxquelles ils accèdent. Tous les journaux Prisma Access sont stockés dans le Strata Logging Service, fournissant des analyses centralisées, des rapports et des analyses sur l’ensemble des utilisateurs, des applications et des sites.

Prisma Access offre une protection à grande échelle avec une couverture mondiale afin que vous ne deviez pas vous soucier de choses comme le dimensionnement et le déploiement de pare-feu matériels dans vos succursales ou la création et la gestion d’appliances dans des installations de colocation. Prisma Access fournit l’infrastructure réseau nécessaire pour connecter toutes vos succursales distantes, vos sites de siège, vos centres de données et vos utilisateurs mobiles sans que vous ne deviez créer votre propre infrastructure de sécurité mondiale et étendre votre capacité opérationnelle.



Avec Prisma Access, Palo Alto Networks déploie et gère l’infrastructure de sécurité à l’échelle mondiale pour sécuriser vos réseaux distants et vos utilisateurs mobiles. Prisma Access chiffre les données de bout en bout entre les nœuds de traitement de la sécurité des utilisateurs mobiles (MU-SPN) et les nœuds de traitement de la sécurité du réseau à distance (RN-SPN), entre les SPN et les nœuds d’accès d’entreprise de connexion de service (SC-CAN) et entre les SC-CAN et le centre de données.

- **Infrastructure de service**—Prisma Access utilise une infrastructure de service interne pour sécuriser le réseau de votre organisation. Vous fournissez un sous-réseau pour l’infrastructure, et Prisma Access utilise les adresses IP de ce sous-réseau pour établir une infrastructure réseau entre vos emplacements réseau distants et les utilisateurs mobiles, ainsi que des connexions de

 ©2025 Palo Alto Networks, Inc.

service à vos ressources réseau internes (le cas échéant). La communication interne au sein du cloud est établie à l'aide d'un routage dynamique.

- **Connexions au service**—si votre licence Prisma Access l'inclut, vous avez la possibilité d'établir des tunnels IPSec pour autoriser la communication entre les ressources internes de votre réseau et les utilisateurs mobiles et les utilisateurs de vos emplacements réseau distants. Vous pouvez, par exemple, créer une connexion de service à un serveur d'authentification au siège social ou au centre de données de votre organisation.

  Même si vous n'avez pas besoin d'une connexion de service pour votre siège social ou votre centre de données, nous vous recommandons d'en créer une pour autoriser la communication réseau entre les utilisateurs mobiles et les emplacements réseau distants, et entre les utilisateurs mobiles situés dans différents emplacements géographiques.
- **Utilisateurs mobiles**—Fournit une sécurité cohérente à vos utilisateurs mobiles, qu'ils accèdent aux applications de votre centre de données, utilisent des applications SaaS ou naviguent sur Internet. Vous pouvez permettre à vos utilisateurs mobiles de se connecter à Prisma Access par :
  - **GlobalProtect**

    Vous pouvez déployer l'application GlobalProtect auprès de vos utilisateurs (disponible pour les smartphones, les tablettes ou les ordinateurs portables exécutant Microsoft Windows, Apple macOS et iOS, Android, Google Chrome OS et Linux) pour leur permettre de tunneliser le trafic vers Prisma Access pour l'application des politiques et la prévention des menaces. L'application GlobalProtect fournit également des rapports sur le profil d'informations d'hôte (HIP) afin que vous puissiez créer des politiques granulaires basées sur l'état du périphérique pour vous assurer que les points de terminaison respectent vos normes de sécurité (par exemple, ils sont équipés des correctifs, du chiffrement et des définitions de virus les plus récents) afin d'accéder à vos applications les plus sensibles. Ou, pour activer l'accès sécurisé aux utilisateurs sur des périphériques non gérés, vous pouvez activer **VPN sans client**. Prisma Access évolue dynamiquement par région en fonction de l'endroit où se trouvent vos utilisateurs à ce moment-là.
  - **Proxy explicite**

    Si le réseau existant de votre organisation utilise déjà des proxys explicites et déploie des fichiers PAC sur vos points de terminaison clients, vous pouvez migrer en douceur vers Prisma Access pour sécuriser le trafic Internet sortant des utilisateurs mobiles.
- **Réseaux distants** : utilisez des réseaux distants pour sécuriser les emplacements réseau distants, tels que les succursales et les utilisateurs de ces succursales avec des pare-feux nouvelle génération basés sur le cloud. Vous pouvez activer l'accès aux sous-réseaux de chaque emplacement réseau distant à l'aide d'itinéraires statiques, de routage dynamique à l'aide de BGP ou d'une combinaison d'itinéraires statiques et dynamiques. Tous les emplacements réseau distants que vous intégrez sont entièrement maillés.
- **Connecteur ZTNA** : le connecteur ZTNA (Zero Trust Network Access) vous permet de vous connecter aux applications privées de votre entreprise de manière simple et sécurisée. Connecteur ZTNA permet aux utilisateurs mobiles et aux utilisateurs des succursales d'accéder à vos applications privées à l'aide d'un tunnel sécurisé automatisé, ce qui élimine la nécessité de configurer des tunnels IPSec et des définitions de routage pour accéder aux applications privées. Le connecteur ZTNA ne nécessite aucun routage de la part de l'infrastructure du client et peut fournir un accès aux applications qui utilisent des adresses IP superposées dans vos réseaux.

 ©2025 Palo Alto Networks, Inc.

- **Strata Logging Service**—Prisma Access transfère tous les journaux à Service de journalisation des strates ; dans le cadre de l’activation Prisma Access, vous allez spécifier l’instance Strata Logging Service à laquelle vous souhaitez transférer des journaux Prisma Access. Le trafic de journaux n’utilise pas la bande passante sous licence pour laquelle vous avez acheté Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Sécuriser le trafic Internet en utilisant Prisma Access

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access	❑ Licence Prisma Access

L'importance de la sécurité Internet

La sécurisation de l'accès à Internet n'a jamais été aussi importante et aussi difficile. Les solutions héritées existantes ont du mal à détecter le phishing évasif et ciblé ainsi que d'autres attaques basées sur le web, tout en négligeant les nouvelles menaces posées par le trafic DNS non sécurisé. Palo Alto Networks Prisma Access dispose de la sécurité Internet avec des services de filtrage d'URL avancé et de sécurité DNS alimentés par l'apprentissage automatique, une première dans l'industrie. En utilisant Prisma Access, vous pouvez prévenir les attaques de phishing évasif et ciblé ainsi que les attaques sans fichier en temps réel, et vous protéger des dernières attaques sophistiquées basées sur le DNS.

Prisma Access Passerelle Web Sécurisée Cloud (SWG)

Une passerelle web sécurisée est un élément crucial dans le paysage numérique actuel en raison de la complexité croissante et de la fréquence des cybermenaces. Les cybercriminels conçoivent continuellement de nouvelles tactiques et techniques pour contourner les défenses de sécurité, l'une d'elles étant de camoufler du code malveillant dans des sites Web apparemment légitimes. Lorsque les utilisateurs accèdent à ces sites Web compromis, ils divulguent involontairement des identifiants ou exposent des organisations à un code nuisible, ce qui peut causer des ravages si cela n'est pas détecté.

Dans un environnement chargé de risques, l'absence d'une passerelle de sécurité robuste amplifie considérablement le risque pour les actifs numériques d'une organisation. Ce risque pourrait entraîner un accès non autorisé, un vol de données et une perturbation des opérations commerciales, en particulier avec la prévalence croissante des attaques de phishing et de ransomware. Sans la barrière de sécurité fournie par SWG, une attaque par ransomware pourrait effectivement prendre une organisation en otage, entraînant des dommages financiers et réputationnels.

L'utilisation du trafic chiffré est désormais courante, HTTPS représentant la majorité du trafic web. Une organisation est exposée à des risques pour la sécurité dissimulés dans des canaux chiffrés si elle ne dispose pas d'un SWG capable de déchiffrer et d'inspecter efficacement ce trafic.

Cependant, l'utilisation de produits à plusieurs points pour SWG, l'accès aux applications privées et CASB ne fait qu'aggraver les choses. Des produits isolés assemblés en une seule offre entraînent des lacunes en matière de parité des fonctionnalités et de mauvais résultats en matière de sécurité, vous rendant vulnérable aux attaques. Avec ces solutions, vous obtenez une sécurité incohérente pour les applications Internet et privées.

Pour relever ces défis, Prisma Access offre un produit unifié, une gestion, une stratégie et des données convergentes pour tous les utilisateurs et des applications sur toutes les capacités, y compris ZTNA, SWG, NG-CASB, FWaaS, DLP, et plus.

 ©2025 Palo Alto Networks, Inc.

Les clients peuvent facilement migrer des solutions proxy héritées sur site et basées sur le cloud Prisma Access pour obtenir une visibilité en ligne et un contrôle du trafic Internet et des applications SaaS avec des protections de sécurité alimentées par l’IA de premier plan dans l’industrie.

Utiliser Prisma Access pour sécuriser les utilisateurs et les points de terminaison

Prisma Access est conçu pour prévenir les cyberattaques réussies, et c’est pourquoi il fait plus que simplement sécuriser le web. Pour arrêter les cyberattaques, il est nécessaire d’inspecter tout le trafic. Tout ce qui est en deçà d’une inspection complète de tout le trafic introduit un écart significatif en matière de sécurité. Prisma Access protège de manière cohérente tout le trafic sur tous les ports et de toutes les applications, permettant à votre organisation de :

- Prévenir les cyberattaques réussies grâce à des philosophies de sécurité éprouvées et à des renseignements sur les menaces pour une visibilité approfondie et un contrôle précis qui s’étend à l’ensemble de votre organisation.
- Inspectez complètement tout le trafic d’application dans les deux sens, y compris le trafic chiffré SSL ou TLS, sur tous les ports, qu’il communique avec Internet, avec le cloud ou entre les succursales.
- Bénéficiez d’une intelligence des menaces complète alimentée par des données de menaces automatisées de Palo Alto Networks et de centaines de flux tiers.

En savoir plus sur Prisma Access et ses solutions.

 ©2025 Palo Alto Networks, Inc.

Comment gérer Prisma Access

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Il y a deux façons de gérer Prisma Access, mais vous ne pouvez pas passer d'une interface de gestion à l'autre après avoir activé votre licence Prisma Access (à l'exception de l'utilisation du flux de travail de migration pour passer d'un Prisma Access (Managed by Panorama) à un déploiement Prisma Access (Managed by Strata Cloud Manager)). Vous devez donc décider comment vous souhaitez gérer Prisma Access avant de commencer :

- **Prisma Access (Managed by Strata Cloud Manager)**

  Pour gérer Prisma Access à partir du cloud, utilisez Strata Cloud Manager. Grâce à la gestion du cloud, vous pouvez rapidement intégrer des branches et des utilisateurs mobiles grâce à des flux de travail axés sur les tâches qui vous permettent de configurer et de tester votre environnement en quelques minutes. La gestion du cloud avec Strata Cloud Manager simplifie le processus d'intégration en fournissant des règles de politiques d'accès à Internet et de décryptage prédéfinies basées sur les bonnes pratiques. Configurez rapidement des tunnels IPSec en utilisant des paramètres par défaut adaptés aux périphériques compatibles IPSec les plus courants et activez le déchiffrement SSL pour les catégories d'URL recommandées.

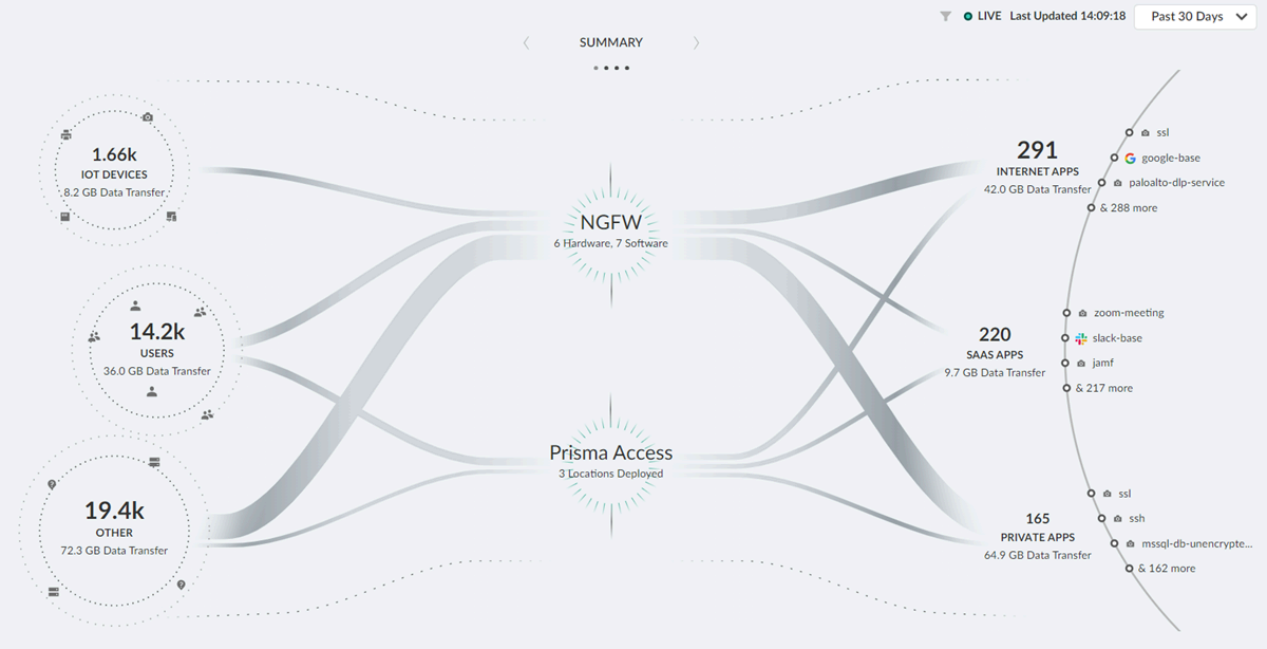
  Centre de commande de Strata Cloud Manager

  Le Centre de commande de Strata Cloud Manager s'affiche lorsque vous lancez votre Strata Cloud Manager. Ce centre de commande vous aide à évaluer l'état de votre réseau, à obtenir une meilleure visibilité et une vue d'ensemble de vos données. Le centre de commande dispose de différents tableaux de bord pour afficher différents types de rapports.

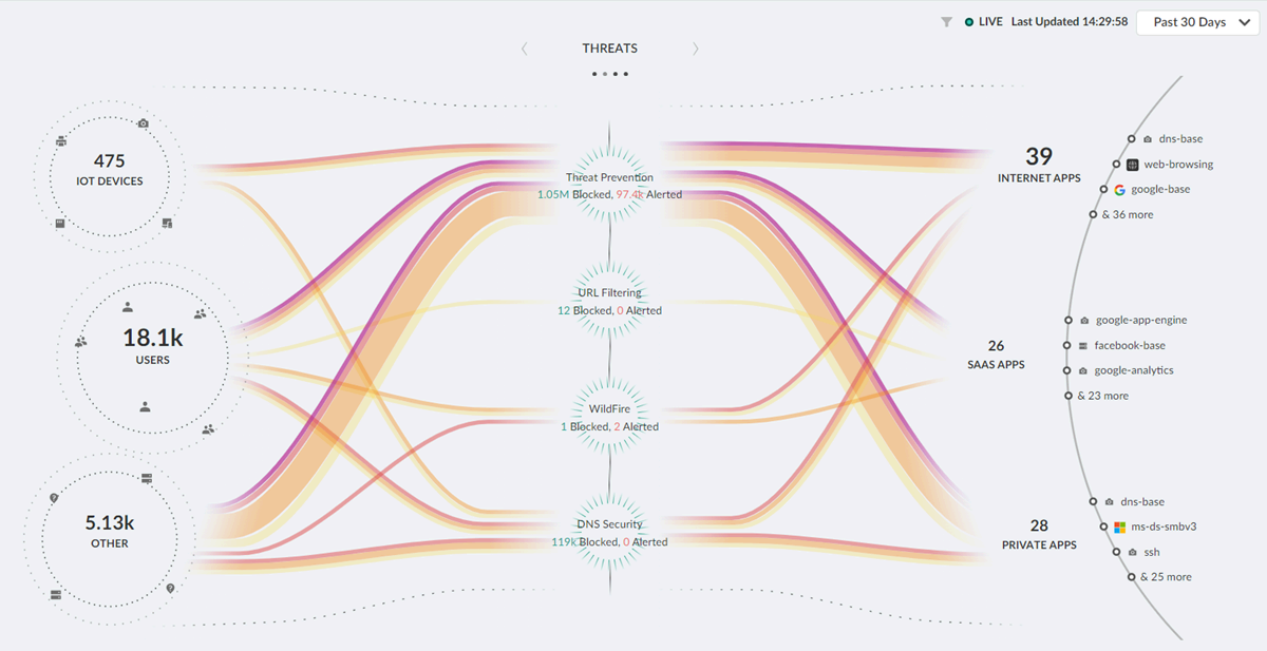
  - **Summary (Résumé)** : Dans le tableau de bord récapitulatif, vous pouvez afficher les différents types de sources de données, l'infrastructure de la plateforme, comme NGFW ou

 ©2025 Palo Alto Networks, Inc.

Prisma Access, à travers laquelle les données circulent de diverses sources de données vers différentes applications de votre réseau.

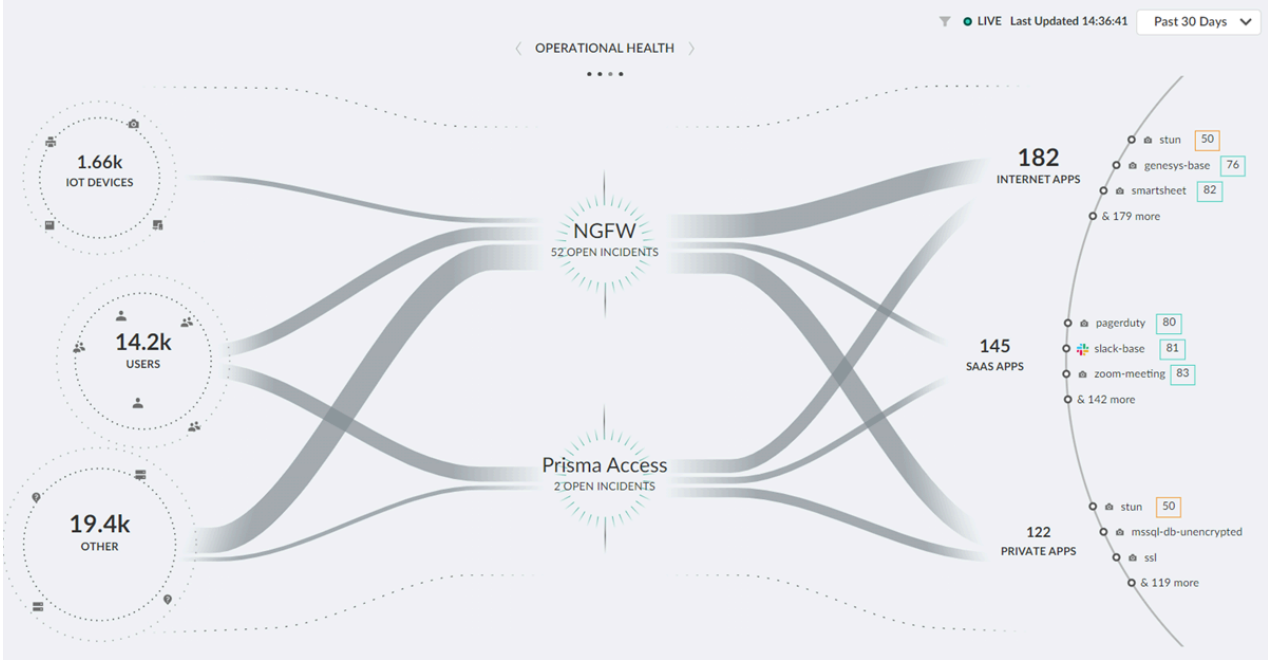


- **Threats (Menaces)** : Dans votre tableau de bord des menaces, vous pouvez afficher les menaces détectées par vos applications de sécurité. Vous pouvez utiliser ce tableau de bord pour surveiller les menaces bloquées et autorisées sur votre réseau ou pour examiner les zones de votre réseau susceptibles d’avoir un faible pourcentage de trafic inspecté.



 ©2025 Palo Alto Networks, Inc.

- **Operational Health (Santé opérationnelle)** : Affiche l’état et l’expérience utilisateur de votre réseau tel qu’il est surveillé par l’ADEM. Vous pouvez utiliser cette vue pour surveiller l’expérience utilisateur sur votre réseau et examiner la gravité des incidents ouverts.



- **Data Security (Sécurité des données)** : Affiche le trafic au sein de votre réseau qui a été signalé comme contenant des données sensibles par les abonnements de sécurité DLP et SaaS. Vous pouvez utiliser cette vue pour surveiller les données qui circulent à travers vos pare-feu et vos applications SaaS connectées, ainsi que la gravité des risques liés aux données sur votre réseau.



Cliquez sur l’une de ces catégories dans vos tableaux de bord pour filtrer les résultats en conséquence.

©2025 Palo Alto Networks, Inc.

- **Prisma Access (Managed by Panorama)**

  Utilisez le plug-in Cloud Services sur Panorama pour configurer et gérer Prisma Access. Il s'agit d'une bonne option si vous utilisez déjà Panorama pour gérer des pare-feu nouvelle génération et que vous disposez d'une politique commune que vous souhaitez utiliser pour accéder à vos applications d'entreprise.

  Même si vous utilisez Panorama pour gérer Prisma Access, vous pouvez toujours utiliser Strata Cloud Manager pour de nombreuses fonctionnalités de visibilité et de surveillance de Prisma Access. En savoir plus.

Une fois que vous avez choisi l'option de gestion que vous souhaitez utiliser, commencez par suivre le flux de travail de mise sous licence et d'activation de l'option que vous avez sélectionnée :

- Pour commencer avec Prisma Access (Managed by Panorama) Access, effectuez l'activation de la licence à partir du portail de support client (CSP) et installez le plug-in Cloud Services sur Panorama.
- Pour commencer avec Cloud Managed Prisma Access, effectuez l'activation de la licence à partir de la plateforme.



Parité des fonctionnalités entre Panorama et Cloud Management

Il y a quelques différences entre ce qui est pris en charge sur Prisma Access (Managed by Panorama) Access et Prisma Access (Managed by Strata Cloud Manager). Pour obtenir la liste des fonctionnalités prises en charge dans Prisma Access (Managed by Panorama) et Prisma Access (Managed by Strata Cloud Manager), reportez-vous à la matrice de compatibilité.

 ©2025 Palo Alto Networks, Inc.

Visibilité et surveillance de Prisma Access avec Strata Cloud Manager

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Panorama géré)	• Licence Prisma Access

Vous avez le choix entre deux méthodes pour gérer Prisma Access :

- Pour Prisma Access (Managed by Strata Cloud Manager), vous pouvez utiliser **Strata Cloud Manager**
- ou **Panorama** pour gérer Prisma Access

Ces deux interfaces de gestion vous permettent de gérer l'intégration, la configuration et l'application des politiques de sécurité pour votre environnement Prisma Access. Cependant, Prisma Access inclut également une visibilité et une surveillance robustes pour votre environnement Prisma Access, ces fonctionnalités étant fournies dans Strata Cloud Manager.

Ce qui est important :

Quelle que soit l'interface de gestion que vous utilisez pour Prisma Access (Strata Cloud Manager ou Panorama), vous pouvez utiliser Strata Cloud Manager pour bon nombre de vos fonctionnalités de visibilité Prisma Access et pour interagir avec des abonnements complémentaires tels que Autonomous DEM alimenté par l'IA.

Fonctionnalités de visibilité et de surveillance Prisma Access sur Strata Cloud Manager	
DEM autonome	Fournit une visibilité et des informations natives de bout en bout sur tout le trafic utilisateur dans votre environnement Secure Access Service Edge (SASE). La fonctionnalité ADEM est nativement intégrée à l'application GlobalProtect et à Prisma Access et ne nécessite donc pas le déploiement d'appareils ou d'agents supplémentaires. Vous pouvez rapidement isoler la source des problèmes d'expérience numérique et simplifier la correction. *Cette fonctionnalité nécessite la licence complémentaire Autonomous DEM pour être utilisée avec Prisma Access (Managed by Panorama) Access.*
Tableaux de bord et création de rapports dans Strata Cloud Manager	Les fonctionnalités de visibilité de Strata Cloud Manager identifient les principales conclusions que vous pouvez utiliser pour éclairer vos mises à jour de politique et combler les lacunes en matière de sécurité d'entreprise et de productivité des utilisateurs.

 ©2025 Palo Alto Networks, Inc.

Fonctionnalités de visibilité et de surveillance Prisma Access sur Strata Cloud Manager	
	• **Tableaux de bord interactifs** Examinez les données des applications, des menaces, des utilisateurs et des abonnements de sécurité à l’œuvre dans votre réseau • **Rapports** De nombreux tableaux de bord prennent en charge les rapports, où vous pouvez partager des données hors ligne et planifier des mises à jour régulières
Centre de commande de Strata Cloud Manager	Le centre de commande est un résumé visuel et interactif des périphériques IoT, des utilisateurs, des hôtes et du trafic sur votre réseau. S’appuyant sur les données de vos abonnements ADEM et de sécurité en mode cloud, le centre de commande révèle d’importantes informations sur les menaces, l’expérience utilisateur et la sécurité des données sur votre réseau. Le centre de commande vous permet d’interagir avec les données et de visualiser les relations entre les événements sur le réseau. Ainsi, vous pouvez identifier les anomalies ou trouver des améliorations à apporter à votre sécurité réseau.

 ©2025 Palo Alto Networks, Inc.

Prisma Access emplacements

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Vous pouvez déployer Prisma Access sur les emplacements de votre choix, en fonction de vos préférences en matière d'emplacement des données et de l'endroit où vous avez le plus d'utilisateurs. Prisma Access fournit plus de 100 sites dans le monde entier afin que vos utilisateurs bénéficient d'une expérience adaptée à leurs paramètres régionaux. Tous les emplacements Prisma Access sont mappés à un emplacement de calcul de sécurité qui optimise les performances et la latence. Cela signifie que le trafic dans certains pays sera dirigé vers cet emplacement de calcul défini.

Si vous devez limiter les emplacements de calcul à des pays spécifiques, consultez le tableau qui indique le pays de traitement pour Prisma Access et les services associés.

Il existe différents types d'emplacements Prisma Access :

- **Emplacements triés par emplacement de calcul** : lorsque vous configurez des réseaux distants, vous allouez la bande passante en fonction de l'emplacement de calcul. Au moins deux emplacements Prisma Access (souvent plus) géographiquement proches l'un de l'autre sont regroupés en *emplacements de calcul*. Vous allouez la bande passante à ce niveau au lieu de l'allouer à des emplacements Prisma Access individuels ou à des sites de réseau distant spécifiques. Ainsi, Prisma Access peut allouer dynamiquement la bande passante aux sites d'un emplacement de calcul en fonction de la charge ou de la demande.
- **Théâtre et groupe d'emplacements** : lorsque vous allouez des pools d'adresses IP dans un déploiement Utilisateurs mobiles – GlobalProtect, vous pouvez spécifier des pools d'adresses IP par groupe d'emplacements (plus petit que le théâtre), par théâtre ou au niveau mondial. Utilisez des pools d'adresses IP propres au groupe d'emplacements si vous disposez de services qui dépendent de l'adresse IP source de l'utilisateur pour identifier les détails de ce dernier (tels que les services basés sur l'emplacement ou les services basés sur un groupe d'utilisateurs ou une fonction) afin de pouvoir appliquer des politiques de contrôle d'accès ou d'effectuer des opérations de routage ou de politique dans différents pays si les pays se trouvent dans des régions de calcul différentes.
- **Emplacements par région** : une région est associée à chaque emplacement Prisma Access.
- **Emplacements de proxy explicite** : le proxy explicite possède son propre ensemble d'emplacements, qui constituent un sous-ensemble des emplacements Prisma Access.
- **Emplacements Colo-Connect** : Colo-Connect possède son propre ensemble d'emplacements, qui constituent un sous-ensemble des emplacements Prisma Access.
- **Régions Strata Logging Service** : Prisma Access prend en charge un sous-ensemble de régions Strata Logging Service.

 ©2025 Palo Alto Networks, Inc.

- **Emplacements de type Réseaux distants : hautes performances, Réplication du trafic et Accès entrant sécurisé** : les déploiements de type Réseaux distants hautes performances, Réplication du trafic et Accès entrant sécurisé utilisent un sous-ensemble d'emplacements Prisma Access.
- **Emplacements de type Prisma Access Chine** : les déploiements de type Prisma Access Chine utilisent des emplacements en Chine continentale.
- **Emplacements FedRAMP modéré et élevé** : les déploiements de type FedRAMP modéré et élevé sur Prisma Access utilisent un sous-ensemble d'emplacements Prisma Access.
- **Carte des emplacements en Amérique du Nord** : pour vous aider à sélectionner des emplacements en Amérique du Nord, consultez cette carte qui montre la couverture géographique des emplacements en Amérique du Nord.
- **Zones locales** : les zones locales placent les services de calcul, de stockage, de base de données et autres à proximité de grands centres urbains et industriels. Ces emplacements disposent de leurs propres emplacements de calcul.

  Pour ajouter une zone locale, contactez votre représentant Palo Alto Networks.

  Gardez à l'esprit les directives suivantes lors du déploiement de zones locales :

  - Les emplacements de zone locale ne prennent pas en charge l'IPv6.
  - Les emplacements de zone locale n'utilisent pas les adresses IP enregistrées de Palo Alto Networks.
  - La vitesse de 1 Gbit/s pour les réseaux distants n'est pas prise en charge.
  - La redondance des nœuds de connexion aux services et aux réseaux distants entre les zones de disponibilité n'est pas disponible si vous les déployez dans la même zone locale, car les deux nœuds sont provisionnés dans une seule zone.
  - Ces zones locales n'utilisent pas les adresses IP enregistrées de Palo Alto Networks. Si vous rencontrez des problèmes lors de l'accès aux URL, signalez le problème du site web à l'adresse https://reportasite.gpcloudservice.com/ ou contactez le support Palo Alto Networks.

Consultez le document Prisma Access Privacy Datasheet (Fiche technique sur la confidentialité de Prisma Access) *pour en savoir plus sur les emplacements Prisma Access et les endroits où Prisma Access traite le trafic.*

Emplacements de calcul, ville et pays

Le premier emplacement répertorié dans chaque emplacement de calcul (en gras) indique la ville et le pays de l'emplacement de calcul.

Les emplacements indiqués par deux astérisques (**) sont des *zones locales*, qui ne prennent pas en charge toutes les fonctionnalités de Prisma Access.

Emplacement de calcul	Prisma Access Emplacement	Ville et pays
Asie Nord-Est	**Japon Centre**	**Tokyo, Japon**

 ©2025 Palo Alto Networks, Inc.

Emplacement de calcul	Prisma Access Emplacement	Ville et pays
Asie Sud	**Inde Ouest**	**Mumbai, Inde**
	Bangladesh	Dacca, Bangladesh
	Inde Sud	Chennai, Inde
	Pakistan Sud	Karachi, Pakistan
	Pakistan Ouest	Lahore, Pakistan
Asie Sud-Est (Indonésie)	**Indonésie**	**Jakarta, Indonésie**
Asie Sud-Est (Singapour)	**Singapour**	**Singapour**
	Cambodge	Phnom Penh, Cambodge
	Malaisie	Kuala Lumpur, Malaisie
	Myanmar	Yangon, Birmanie
	Pakistan Ouest (II)	Islamabad, Pakistan
	Philippines	Quezon City, Philippines
	Sri Lanka	Colombo, Sri Lanka
	Thaïlande	Bangkok, Thaïlande
	Viet Nam	Hô Chi Minh-Ville, Viet Nam
Australie Sud	**Australie Sud**	**Melbourne, Australie**
Australie Sud-Est	**Australie Sud-Est**	**Sydney, Australie**
	Est de l'Australie	Brisbane, Australie
	Nouvelle-Zélande	Auckland, Nouvelle-Zélande
	Papouasie-Nouvelle-Guinée	Port Moresby, Papouasie-Nouvelle-Guinée
Australie Ouest (Perth)**	**Australie Ouest (Perth)****	**Perth, Australie**
Bahreïn	**Bahreïn**	**Manama, Bahreïn**
Belgique	**Belgique**	**Saint-Ghislain, Belgique**
	Lettonie	Riga, Lettonie
	Sénégal	Dakar, Sénégal
Canada Centre (Montréal)	**Est du Canada**	**Québec, Canada**
Canada Centre (Toronto)	**Centre du Canada**	**Toronto, Canada**

©2025 Palo Alto Networks, Inc.

Emplacement de calcul	Prisma Access Emplacement	Ville et pays
Canada Ouest (Calgary)	**Canada Ouest**	**Calgary, Canada**
Europe Centre	**Allemagne Centre**	**Francfort, Allemagne**
	Autriche	Vienne, Autriche
	Bulgarie	Sofia, Bulgarie
	Croatie (Hrvatska)	Zagreb, Croatie
	République tchèque	Prague, République tchèque
	Égypte	Le Caire, Égypte
	Allemagne Nord	Hambourg, Allemagne
	Allemagne Sud	Munich, Allemagne
	Grèce	Athènes, Grèce
	Hongrie	Budapest, Hongrie
	Koweït	Al Ahmadi, Koweït
	Liechtenstein	Schaan, Liechtenstein
	Luxembourg	Ville de Luxembourg, Luxembourg
	Moldavie	Chisinau, Moldavie
	Nigéria	Lagos, Nigéria
	Roumanie	Bucarest, Roumanie
	Slovaquie	Bratislava, Slovaquie
	Slovénie	Ljubljana, Slovénie
	Turquie	Istanbul, Turquie
	Ukraine	Kiev, Ukraine
	Ouzbékistan	Tachkent, Ouzbékistan
Europe Centre (Varsovie)	**Pologne**	**Varsovie, Pologne**
Europe Nord	**Finlande**	**Hamina, Finlande**
	Biélorussie	Minsk, Biélorussie
	Kazakhstan	Astana, Kazakhstan
	Lituanie	Vilnius, Lituanie
	Norvège	Oslo, Norvège
	Russie Centre	Moscou, Russie
	Russie Nord-Ouest	Saint-Pétersbourg, Russie

©2025 Palo Alto Networks, Inc.

Emplacement de calcul	Prisma Access Emplacement	Ville et pays
Europe Nord (Stockholm)	**Suède**	**Stockholm, Suède**
Europe Nord-Ouest	**Royaume-Uni** Ghana	**Londres, Royaume-Uni** Accra, Ghana
Europe Nord-Ouest (Paris)	**France Sud**	**Paris, France**
Europe Sud	**Italie** Jordanie Kenya Monaco	**Milan, Italie** Amman, Jordanie Mombasa, Kenya Monaco
Europe Sud-Ouest	**Espagne Centre** Andorre Portugal Espagne Est	**Madrid, Espagne** Andorre-la-Vieille, Andorre Lisbonne, Portugal Barcelone, Espagne
Europe Ouest	**Pays-Bas Centre** Danemark Pays-Bas Sud	**Port d'Ems, Pays-Bas** Copenhague, Danemark Rotterdam, Pays-Bas
France Nord	**France Nord**	**Paris, France**
Hong Kong	**Hong Kong**	**Hong Kong, Chine**
Inde Nord	**Inde Nord**	**New Delhi, Inde**
Irlande	**Irlande**	**Dublin, Irlande**
Japon Sud	**Japon Sud**	**Osaka, Japon**
Moyen-Orient Centre (Qatar)	**Qatar**	**Doha, Qatar**
Moyen-Orient Centre (Arabie saoudite)	**Arabie Saoudite**	**Riyad, Arabie saoudite**
Moyen-Orient Centre (EAU)	**Émirats arabes unis**	**Dubaï, Émirats arabes unis**
Moyen-Orient Ouest	**Israël**	**Tel-Aviv, Israël**
Nigéria (Lagos)**	**Nigéria (Lagos)****	**Lagos, Nigéria**

©2025 Palo Alto Networks, Inc.

Emplacement de calcul	Prisma Access Emplacement	Ville et pays
Nouvelle-Zélande (Auckland)**	**Nouvelle-Zélande (Auckland)****	**Auckland, Nouvelle-Zélande**
Afrique du Sud Centre	**Afrique du Sud Centre**	**Johannesburg, Afrique du Sud**
Afrique du Sud Ouest	**Afrique du Sud Ouest**	**Cape Town, Afrique du Sud**
Amérique du Sud Est	**Sud du Brésil** Brésil Centre Brésil Est Paraguay Venezuela	**Sao Paulo, Brésil** Brasilia, Brésil Rio de Janeiro, Brésil Assomption, Paraguay Caracas, Venezuela
Amérique du Sud Ouest	**Chili** Argentine Bolivie Pérou Uruguay	**Santiago, Chili** Buenos Aires, Argentine Santa Cruz de la Sierra, Bolivie Lima, Pérou Montevideo, Uruguay
Amérique du Sud Ouest (Lima)**	**Amérique du Sud Ouest (Lima)****	**Lima, Pérou**
Corée du Sud	**Corée du Sud**	**Séoul, Corée du Sud**
Suisse	**Suisse** Ouganda	**Zurich, Suisse** Kampala, Ouganda
Taïwan	**Taïwan**	**Changhua, Taïwan**
États-Unis Centre	**États-Unis Centre**	**Council Bluffs, États-Unis**
États-Unis Centre (Chicago)**	**États-Unis Centre (Chicago)****	**Chicago, États-Unis**
États-Unis Centre Ouest	**États-Unis Centre Ouest**	**Salt Lake City, États-Unis**
États-Unis Est	**États-Unis Est** États-Unis Nord-Est Guatemala	**Ashburn, États-Unis** New York, États-Unis Guatemala, Guatemala
États-Unis Nord-Ouest	**États-Unis Nord-Ouest**	**The Dalles, États-Unis**

 ©2025 Palo Alto Networks, Inc.

Emplacement de calcul	Prisma Access Emplacement	Ville et pays
États-Unis Sud	**États-Unis Sud** Mexique Centre Mexique Ouest	**Dallas, États-Unis** Mexico, Mexique Guadalajara, Mexique
États-Unis Sud-Est	**États-Unis Sud-Est** Colombie Costa Rica Équateur Panama	**Moncks Corner, États-Unis** Bogota, Colombie San José, Costa Rica Guayaquil, Équateur Panama, Panama
États-Unis Sud-Est (Miami)**	**États-Unis Sud-Est (Miami)****	**Miami, États-Unis**
États-Unis Sud-Ouest	**États-Unis Sud-Ouest** États-Unis Ouest	**Los Angeles, États-Unis** San Francisco, États-Unis

Théâtre et groupe d'emplacements

Théâtre / groupe d'emplacements	ID de groupe du pool d'adresses IP
Colombie Costa Rica Équateur Guatemala Mexique Centre Panama États-Unis Est États-Unis Sud-Est États-Unis Centre Costa Rica États-Unis Nord Centre États-Unis Nord-Est États-Unis Sud États-Unis Sud-Est Venezuela	1

©2025 Palo Alto Networks, Inc.

Théâtre / groupe d'emplacements	ID de groupe du pool d'adresses IP
Est du Canada Centre du Canada	2
Irlande	3
France Sud Ghana Royaume-Uni	4
France Nord	5
Asie, Australie et Japon	6
Andorre Autriche Bulgarie Croatie (Hrvatska) République tchèque Égypte Allemagne Centre Allemagne Nord Allemagne Sud Grèce Hongrie Israël Italie Jordanie Kenya Koweït Liechtenstein Luxembourg Moldavie Monaco Nigéria Pologne	7

©2025 Palo Alto Networks, Inc.

Théâtre / groupe d'emplacements	ID de groupe du pool d'adresses IP
Portugal Roumanie Slovaquie Slovénie Arabie Saoudite Afrique du Sud Centre Espagne Centre Espagne Est Turquie Ukraine Émirats arabes unis Ouzbékistan	
Biélorussie Finlande Kazakhstan Lituanie Norvège Russie Centre Russie Nord-Ouest Suède	8
Danemark Pays-Bas Centre Pays-Bas Sud	9
Afrique, Europe et Moyen-Orient	10
Suisse Ouganda	11
Belgique Lettonie Sénégal	12
Brésil Centre	13

©2025 Palo Alto Networks, Inc.

Théâtre / groupe d’emplacements	ID de groupe du pool d’adresses IP
Brésil Est Sud du Brésil Paraguay Venezuela	
Est de l’Australie Australie Sud Australie Sud-Est Nouvelle-Zélande Papouasie-Nouvelle-Guinée	14
Cambodge Indonésie Malaisie Myanmar Philippines Singapour Thaïlande Viet Nam	15
Hong Kong	16
Taïwan	17
Corée du Sud	18
Bangladesh Inde Nord Inde Sud Inde Ouest Pakistan Ouest Pakistan Sud Qatar	19
Afrique du Sud Ouest Suède Afrique du Sud Ouest	20

©2025 Palo Alto Networks, Inc.

Théâtre / groupe d'emplacements	ID de groupe du pool d'adresses IP
Japon Centre Japon Sud	21
Bahreïn	22
Canada Ouest Mexique Centre Mexique Ouest États-Unis Centre Ouest États-Unis Nord-Ouest États-Unis Sud-Ouest États-Unis Ouest	23
Argentine Bolivie Chili Pérou Uruguay	24

Emplacements par région

Emplacements
Région Afrique
Kenya
Nigéria
Sénégal
Afrique du Sud Centre
Afrique du Sud Ouest
Région Asie
Bangladesh
Cambodge

©2025 Palo Alto Networks, Inc.

Emplacements
Hong Kong
Inde Nord
Inde Sud
Inde Ouest
Indonésie
Kazakhstan
Malaisie
Myanmar
Pakistan Sud
Pakistan Ouest
Pakistan Ouest (II)
Papouasie-Nouvelle-Guinée
Philippines
Singapour
Corée du Sud
Sri Lanka
Taïwan
Thaïlande
Viet Nam
Région ANZ
Est de l'Australie
Australie Sud
Australie Sud-Est
Nouvelle-Zélande
Région Europe

 ©2025 Palo Alto Networks, Inc.

Emplacements
Andorre
Autriche
Biélorussie
Belgique
Bulgarie
Croatie (Hrvatska)
République tchèque
Danemark
Finlande
France Nord
France Sud
Allemagne Centre
Allemagne Nord
Allemagne Sud
Ghana
Grèce
Hongrie
Irlande
Italie
Lettonie
Liechtenstein
Lituanie
Luxembourg
Moldavie
Monaco

 ©2025 Palo Alto Networks, Inc.

Emplacements
Pays-Bas Centre
Pays-Bas Sud
Norvège
Pologne
Portugal
Roumanie
Russie Centre
Russie Nord-Ouest
Slovaquie
Slovénie
Espagne Centre
Espagne Est
Suède
Suisse
Ouganda
Royaume-Uni
Ukraine
Ouzbékistan
Région Japon
Japon Centre
Japon Sud
Région Moyen-Orient
Bahreïn
Égypte
Israël

©2025 Palo Alto Networks, Inc.

Emplacements
Jordanie
Koweït
Qatar
Arabie Saoudite
Turquie
Émirats arabes unis
Région Amérique du Nord
Centre du Canada
Est du Canada
Canada Ouest
Costa Rica
Mexique Centre
Mexique Ouest
Panama
États-Unis Centre
États-Unis Centre Ouest
États-Unis Est
États-Unis Nord-Est
États-Unis Nord-Ouest
États-Unis Sud
États-Unis Sud-Est
États-Unis Sud-Ouest
États-Unis Ouest
Région Amérique du Sud
Argentine

©2025 Palo Alto Networks, Inc.

Emplacements
Bolivie
Brésil Centre
Brésil Est
Sud du Brésil
Chili
Colombie
Équateur
Paraguay
Pérou
Uruguay
Venezuela

Emplacements de proxy explicite

Prisma Access prend en charge les emplacements suivants pour le proxy explicite. Le proxy explicite utilise GeoDNS pour résoudre l'utilisateur mobile et le connecter à l'emplacement Prisma Access déployé le plus proche.

- **Afrique, Europe et Moyen-Orient :**
  - Belgique
  - Finlande
  - France Sud
  - Allemagne Centre
  - Israël
  - Italie
  - Pays-Bas Centre
  - Pologne
  - Qatar
  - Arabie Saoudite
  - Afrique du Sud Centre
  - Espagne Centre
  - Suisse
  - Royaume-Uni

 ©2025 Palo Alto Networks, Inc.

- **Asie, Australie et Japon :**
  - Australie Sud
  - Australie Sud-Est
  - Chine
  - Hong Kong
  - Japon Centre
  - Japon Sud
  - Inde Nord
  - Inde Ouest
  - Indonésie
  - Singapour
  - Corée du Sud
  - Taïwan
- **Amérique du Nord et Amérique du Sud :**
  - Sud du Brésil
  - Chili
  - Centre du Canada
  - Est du Canada
  - États-Unis Centre
  - États-Unis Est
  - États-Unis Nord-Ouest
  - États-Unis Sud
  - États-Unis Sud-Est
  - États-Unis Sud-Ouest
  - États-Unis Centre Ouest

Emplacement Colo Connect :

Prisma Access Colo-Connect prend en charge les emplacements Prisma Access suivants. Lorsque vous créez des connexions aux services pour la prise en charge de Colo-Connect, veillez à les créer uniquement dans les emplacements suivants.



Pour les liens d'interconnexion dédiés, utilisez la liste GCP des emplacements dans lesquels vous pouvez créer des liens d'interconnexion dédiés.

- Australie Sud
- Australie Sud-Est
- Belgique
- Sud du Brésil

 ©2025 Palo Alto Networks, Inc.

- Centre du Canada
- Est du Canada
- Chili
- Finlande
- France Sud
- Allemagne Centre
- Hong Kong
- Inde Nord
- Inde Ouest
- Indonésie
- Italie
- Japon Centre
- Japon Sud
- Pays-Bas Centre
- Qatar
- Arabie Saoudite
- Singapour
- Afrique du Sud Centre
- Espagne Centre
- Suisse
- Taïwan
- Royaume-Uni
- États-Unis Centre
- États-Unis Centre Ouest
- États-Unis Est
- États-Unis Nord-Ouest
- États-Unis Sud
- États-Unis Sud-Est
- États-Unis Sud-Ouest

Régions Strata Logging Service prises en charge

Prisma Access prend en charge les régions Strata Logging Service suivantes :

- Australie
- Canada
- France
- Allemagne

 ©2025 Palo Alto Networks, Inc.

- Japon
- Inde
- Indonésie
- Israël
- Pays-Bas – Europe
- Qatar
- Arabie Saoudite
- Singapour
- Suisse
- Taïwan
- Royaume-Uni
- États-Unis – Amériques

Emplacements de type Réseaux distants : hautes performances, Réplication du trafic et Accès entrant sécurisé

Les emplacements de réseaux distants hautes performances suivants sont pris en charge avec Prisma Access :

- Andorre
- Argentine
- Est de l'Australie
- Australie Sud
- Australie Sud-Est
- Autriche
- Bangladesh
- Biélorussie
- Belgique
- Bolivie
- Brésil Centre
- Brésil Est
- Sud du Brésil
- Bulgarie
- Cambodge
- Centre du Canada
- Est du Canada
- Chili
- Colombie

 ©2025 Palo Alto Networks, Inc.

- Costa Rica
- Croatie (Hrvatska)
- République tchèque
- Danemark
- Équateur
- Égypte
- Finlande
- France Nord
- France Sud
- Allemagne Centre
- Allemagne Nord
- Allemagne Sud
- Ghana
- Grèce
- Guatemala
- Hong Kong
- Hongrie
- Inde Nord
- Inde Sud
- Inde Ouest
- Indonésie
- Israël
- Italie
- Japon Centre
- Japon Sud
- Jordanie
- Kazakhstan
- Kenya
- Koweït
- Lettonie
- Liechtenstein
- Lituanie
- Luxembourg
- Malaisie
- Mexique Centre
- Mexique Ouest

 ©2025 Palo Alto Networks, Inc.

- Moldavie
- Monaco
- Myanmar
- Pays-Bas Centre
- Pays-Bas Sud
- Nouvelle-Zélande
- Nigéria
- Norvège
- Pakistan Sud
- Pakistan Ouest
- Pakistan Ouest (II)
- Panama
- Papouasie-Nouvelle-Guinée
- Paraguay
- Pérou
- Philippines
- Pologne
- Portugal
- Qatar
- Roumanie
- Russie Centre
- Russie Nord-Ouest
- Arabie Saoudite
- Sénégal
- Singapour
- Slovaquie
- Slovénie
- Afrique du Sud Centre
- Corée du Sud
- Espagne Centre
- Espagne Est
- Sri Lanka
- Suisse
- Taïwan
- Thaïlande
- Turquie

 ©2025 Palo Alto Networks, Inc.

- Ouganda
- Royaume-Uni
- Ukraine
- Uruguay
- États-Unis Centre
- États-Unis Centre Ouest
- États-Unis Est
- États-Unis Nord-Est
- États-Unis Nord-Ouest
- États-Unis Sud
- États-Unis Sud-Est
- États-Unis Sud-Ouest
- États-Unis Ouest
- Ouzbékistan
- Venezuela
- Viet Nam

Emplacements Prisma Access Chine

Prisma Access Chine prend en charge les emplacements suivants en Chine continentale :

- Chine Nord – Pékin (utilise l'emplacement de calcul Chine Nord)
- Chine Nord-Ouest – Ningxia (utilise l'emplacement de calcul Chine Nord-Ouest)

Emplacements FedRAMP modéré et élevé

Vous retrouverez la liste des emplacements FedRAMP dans la documentation sur Prisma SASE FedRAMP.

Carte des emplacements en Amérique du Nord

Utilisez la carte suivante comme référence pour vous aider à choisir des emplacements Prisma Access en Amérique du Nord.

©2025 Palo Alto Networks, Inc.



Emplacements de zones locales

Les zones locales suivantes sont prises en charge avec l’IPv4 dans Prisma Access :

- *Consultez votre représentant Palo Alto Networks pour lancer une demande de déploiement dans l’une des zones locales suivantes.*
- *L’IPv6 n’est pas pris en charge.*

- Australie Ouest (Perth)
- Nouvelle-Zélande (Auckland)
- Nigéria (Lagos)
- Amérique du Sud Ouest (Lima)
- États-Unis Centre (Chicago)
- États-Unis Sud-Est (Miami)

©2025 Palo Alto Networks, Inc.

Prisma Access et les emplacements de traitement des services associés

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Prisma Access offre une expérience locale dans plus de 100 emplacements dans le monde entier et mappe chaque emplacement à un emplacement de calcul de sécurité basé sur des performances et une latence optimisées.

Si vous avez besoin de limiter les emplacements de calcul à des pays spécifiques, consultez la cartographie des pays pour chaque emplacement Prisma Access et effectuez vos déploiements uniquement dans les emplacements associés à ces pays pendant la configuration de Prisma Access.

Le tableau suivant vous fournit l'emplacement de traitement du pays pour les régions de service de journalisation Strata, le Strata Cloud Manager (pour Prisma Access (Managed by Strata Cloud Manager), Prisma Access Insights, Autonomous DEM et SaaS Security Inline.

Strata Logging Service	Configuration Strata Cloud Manager :	Données Prisma Access Insights :	Autonomous DEM	SaaS Security Inline
Royaume-Uni	Royaume-Uni	Royaume-Uni	Royaume-Uni	Royaume-Uni
Pays-Bas	Allemagne	Pays-Bas	Pays-Bas	Allemagne (UE)
Allemagne	Allemagne	Allemagne	Allemagne	Allemagne (UE)
Suisse	Suisse	Suisse	Suisse	Allemagne (UE)
France	Allemagne	France	France	Allemagne (UE)
Singapour	Singapour	Singapour	Singapour	Singapour
Inde	Inde	Inde	Inde	Inde
Japon	Japon	Japon	Japon	Japon
Canada	Canada	Canada	Canada	États-Unis
États-Unis	États-Unis	États-Unis	États-Unis	États-Unis
Australie	Australie	Australie	Australie	Australie
Israël	Allemagne	Israël	Israël	Allemagne (UE)

©2025 Palo Alto Networks, Inc.

Strata Logging Service	Configuration Strata Cloud Manager :	Données Prisma Access Insights :	Autonomous DEM	SaaS Security Inline
Qatar	Qatar	Qatar	Qatar	Allemagne (UE)
Arabie Saoudite	Allemagne	Arabie Saoudite	Arabie Saoudite	Allemagne (UE)
Taïwan	Singapour	Taïwan	Taïwan	Singapour
Indonésie	Singapour	Indonésie	Indonésie	Singapour

 ©2025 Palo Alto Networks, Inc.

Gestion de l’infrastructure Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Panorama géré)	❑ Licence Prisma Access

Prisma Access utilise un modèle de propriété partagée. Palo Alto Networks gère l’infrastructure de sécurité sous-jacente, pour s’assurer qu'elle est sécurisée, résiliente, à jour et disponible lorsque vous en avez besoin. La responsabilité de votre organisation consiste à intégrer les emplacements et les utilisateurs, de transmettre les politiques, de les mettre à jour, d'interroger les journaux et de générer des rapports.

Palo Alto Networks gère les parties suivantes de l’infrastructure de sécurité. En plus de l’infrastructure de sécurité, Prisma Access gère les versions et les mises à niveau :

- **Prisma Access**
- **Strata Logging Service** : nous gérons le mécanisme de livraison des journaux.
- **Mises à jour du contenu** : nous gérons les versions et les mises à niveau, y compris les mises à jour de PAN-OS. Pour vos utilisateurs mobiles, Prisma Access héberge plusieurs versions de l’application GlobalProtect et vous pouvez sélectionner la version active de l’application GlobalProtect dans cette liste.
- **Tolérance aux pannes** : nous gérons la disponibilité du service.
- **Mise à l’échelle automatique** : nous mettons automatiquement à l’échelle le service lorsque vous ajoutez des connexions aux services ou des réseaux distants, ou lorsque des utilisateurs mobiles supplémentaires se connectent à une ou plusieurs passerelles dans une seule région.
- **Provisionnement** : nous provisionnons l’infrastructure avec tout ce qui est nécessaire.
- **Surveillance du service** : nous surveillons l’état du service et le maintenons en bon état de fonctionnement.
- **Mappage des emplacements de calcul** : chaque emplacement Prisma Access est mappé à l’emplacement de calcul de sécurité en fonction des performances et de la latence optimisées, ce qui signifie que, sauf modification contraire par un administrateur système, le trafic dans certains pays sera dirigé vers un emplacement de calcul défini. Consultez la fiche de données de confidentialité de Prisma Access pour connaître le mappage de l’emplacement vers l’emplacement de calcul.

Votre organisation gère les composants suivants de l’infrastructure de sécurité.

- **Utilisateurs** : vous gérez l’intégration des utilisateurs mobiles.
- **Authentification** : vous gérez l’authentification de ces utilisateurs.
- **Gestion des périphériques mobiles (MDM)** : vous pouvez contrôler les périphériques mobiles de votre organisation qui sont protégés par Prisma Access à l’aide de votre propre logiciel MDM.

 ©2025 Palo Alto Networks, Inc.

- (Prisma Access (Managed by Panorama) uniquement) **Plug-in Panorama et Cloud Services** : assurez-vous que le Panorama sur lequel le plug-in Cloud Services est installé exécute une version de Panorama qui prend en charge le plug-in Cloud Services. En outre, vous devez mettre à niveau le plug-in Cloud Services dans Panorama après que nous vous avons informé qu'un nouveau plugin est disponible.
- **Création et gestion des politiques** : vous planifiez et créez les politiques dans Panorama pour les utiliser avec Prisma Access.
- **Analyse des journaux et forensique** : Prisma Access fournit les journaux, vous fournissez l’analyse et la création de rapport, en utilisant des outils intégrés fournis par nous ou par un autre fournisseur.
- **Sécurité sur site** : vous fournissez la sécurité sur site entre les micro-segmentations de votre réseau sur site. Dans certains déploiements, vous pouvez également diriger tout le trafic pour être sécurisé à l’aide de Prisma Access.
- **Mise en réseau** : vous fournissez la connectivité réseau à Prisma Access.
- **Surveillance** : vous surveillez l’état du réseau sur site.
- **Connectivité du service** : vous fournissez la connectivité à la passerelle Prisma Access pour les utilisateurs mobiles (par exemple, fournir un ISP) et vous fournissez également les périphériques sur site utilisés comme terminaux des tunnels IPSec utilisés par les connexions aux services et les connexions aux réseaux distants.
- **Intégration** : vous intégrez les utilisateurs mobiles, les sites du siège social/centre de données et les sites de succursales.
- (Prisma Access (Managed by Panorama) uniquement)**Sauvegarde** : vous gérez la sauvegarde de la configuration Panorama.

 ©2025 Palo Alto Networks, Inc.

API Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

API pour Prisma Access (Managed by Strata Cloud Manager)

Vous pouvez trouver plus d'informations sur les API pour Prisma Access (Managed by Strata Cloud Manager) sur pan.dev, le site de documentation des développeurs de Palo Alto Networks. Prisma Access (Managed by Strata Cloud Manager) utilise ces API pour l'intégration, la configuration et les opérations des services.

API pour Prisma Access (Managed by Panorama)

En plus des API XML disponibles pour la configuration et la gestion dans Panorama, il existe des API XML pour le plug-in Cloud Services que vous pouvez employer pour effectuer des tâches spécifiques à Prisma Access. Utilisez ces API via un service, une application ou un script tiers afin d'automatiser les tâches de configuration et de création de rapports pour Prisma Access.



 ©2025 Palo Alto Networks, Inc.

Accéder à l’API Prisma Access (Managed by Panorama) à l’aide du navigateur et l’interface web

Pour accéder à l’API à l’aide du navigateur, connectez-vous au Panorama qui gère Prisma Access avec des privilèges d'administrateur, puis saisissez /api à la fin de l’URL. L’URL passe à l’interface du navigateur API XML.

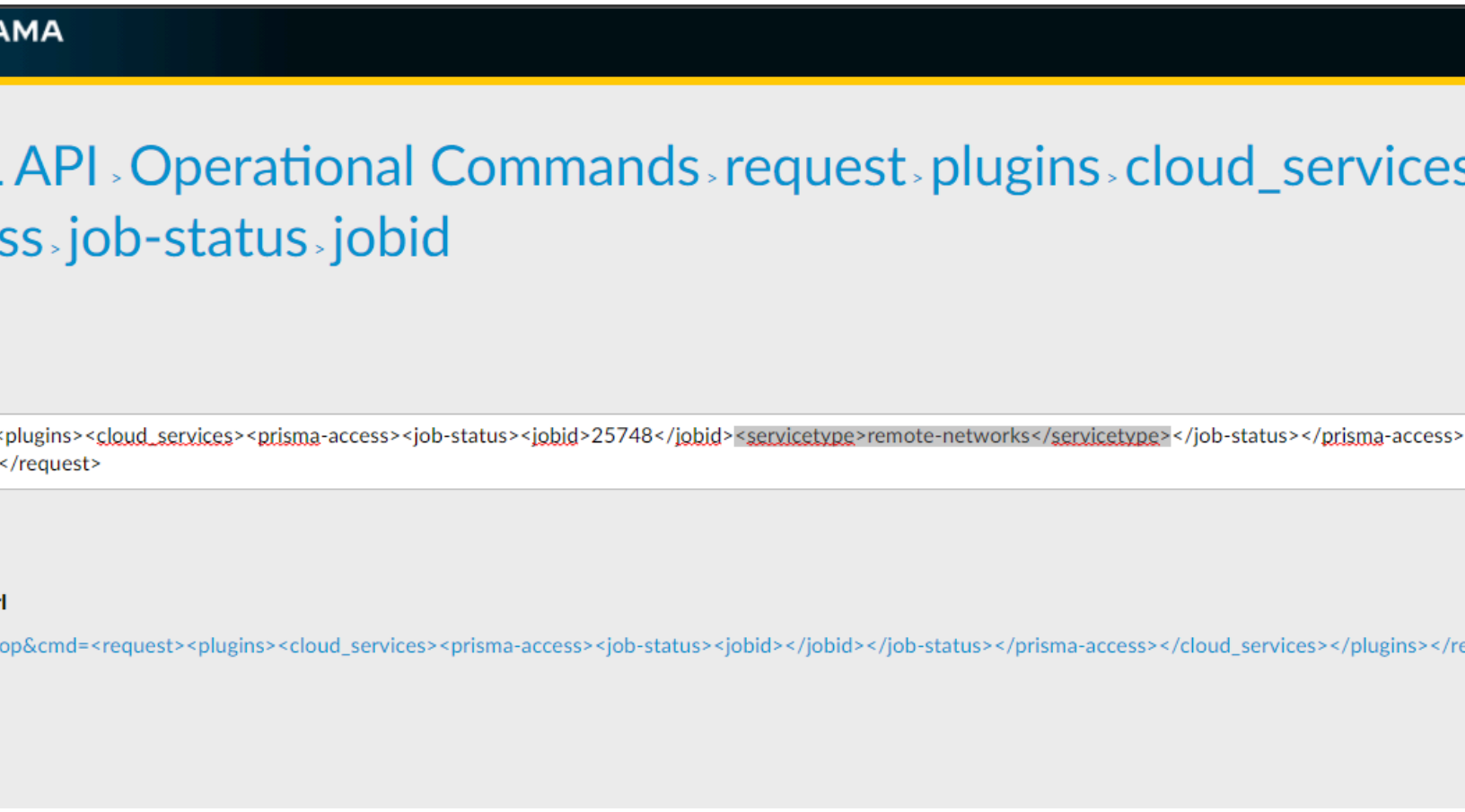
Les API Prisma Access sont situées dans les nœuds XML Path Language (XPath) suivants dans l’arborescence XML :

- Commandes de configuration : **XML API (API XML)** > **Configuration Commands (Commandes de configuration)** > **devices (périphériques)** > **entry[@name='localhost.localdomain']** > **plugins (plug-ins)** > **cloud_services**
- Commandes opérationnelles : **XML API (API XML)** > **Operational Commands (Commandes opérationnelles)** > **request (requête)** > **plugins (plug-ins)** > **cloud_services** > **prisma-access**

Lorsque vous naviguez dans l’arborescence XML, Prisma Access renseigne l’arbre dans la zone **XML** . Vous pouvez saisir les valeurs requises dans la zone **XML** et cliquer sur **Submit (Soumettre)** pour traiter une requête XML. Par exemple, pour demander l’état d'intégration d'un travail, accédez à **XML API (API XML)** > **Operational Commands (Commandes opérationnelles)** > **request (requête)** > **plugins (plug-ins)** > **cloud_services** > **prisma-access** > **job-status** > **jobid**, saisissez l’identifiant du travail dans le champ **jobid**, renseignez la zone de type de service **servicetype** et cliquez sur **Submit (Soumettre)** pour soumettre votre requête.

Ce XML récupère uniquement l’état d'intégration d'un travail. Pour récupérer l’état de toutes les opérations de validation, utilisez l’interface utilisateur Prisma Access.

 ©2025 Palo Alto Networks, Inc.



Prisma Access renvoie la sortie au format XML.

 ©2025 Palo Alto Networks, Inc.

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<response status="success">
  <result>
    <result>
      <status>pass</status>
      <msg>
        <response>
          <status>SUCCESS</status>
          <servicetype>remote-networks</servicetype>
          <workflow>jobStatusResponse</workflow>
          <InstanceSummary>
            <Remote-Network>
              <overview>
                <TotalInstances>0</TotalInstances>
                <ProvisioningInProgress>0</ProvisioningInProgress>
                <ProvisioningFailed>0</ProvisioningFailed>
                <ProvisioningComplete>0</ProvisioningComplete>
              </overview>
            </Remote-Network>
          </InstanceSummary>
          <percentageCompletion>100</percentageCompletion>
          <jobid>25748</jobid>
          <errorCode>0</errorCode>
          <apiVersion>2.0</apiVersion>
        </response>
      </msg>
    </result>
  </result>
</response>
```


Vous pouvez également utiliser l'interface Web pour rechercher des API dans Panorama.

Utiliser les commandes curl pour récupérer des commandes d'API gérée par Panorama

Si vous préférez utiliser la CLI pour récupérer les résultats des commandes API, vous pouvez utiliser les API en conjonction avec l'API que vous utilisez pour récupérer les adresses IP publiques et d'infrastructure de Prisma Access. Pour ce faire, utilisez la commande suivante :

Commandes de configuration :

`curl -k -X GET "https://`*<panorama-ip-address>*`/api/?key=`*<api-key>*`&type=config&cmd=`*<api-parameters></api-parameters>*

Commandes opérationnelles :

`curl -k -X GET "https://`*<panorama-ip-address>*`/api/?key=`*<api-key>*`&type=op&cmd=`*<api-parameters></api-parameters>*

Où :

 ©2025 Palo Alto Networks, Inc.

- *<panorama-ip-address>* est l'adresse IP du Panorama qui gère Prisma Access.
- *<api-key>* est la clé API qui récupère les adresses IP pour Prisma Access (**Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** > **Generate API Key (Générer une clé API)**).
- *<api-parameters>* et *</api-parameters>* sont les paramètres d'API que vous utilisez pour récupérer les informations demandées auprès de l'API.

Si vous disposez d'un déploiement multilocataire, ajoutez le nom du locataire pour lequel vous souhaitez récupérer les informations d'API dans l'API.

Prenons par exemple un déploiement Prisma Access donné qui a les paramètres suivants :

- **Adresse IP Panorama :** 1.2.3.4
- **Clé API :** 12345abcde
- **Nom du locataire :** tenant-1

Si vous souhaitez récupérer le nombre d'utilisateurs mobiles actifs pour ce locataire, vous devez saisir la commande curl suivante :

```
curl -k -X GET "https://1.2.3.4/api/?
key=12345abcde&type=op&cmd=<request><plugins><cloud_services><prisma-
access><multi-tenant><tenant-name><entry%20name='tenant-1'></entry></
tenant-name><remote-active-users-count/></multi-tenant></prisma-
access></cloud_services></plugins></request>"
```

Utiliser les commandes CLI avec Prisma Access (Managed by Panorama)

Prisma Access vous permet d'utiliser des commandes CLI pour récupérer des données Prisma Access. Pour accéder à la CLI, établissez une connexion SSH en utilisant l'adresse IP du Panorama qui gère Prisma Access.

La CLI utilise les mêmes modes et a le même comportement que les commandes PAN-OS, à l'exception de la saisie du nom du locataire pour les déploiements multilocataires ; vous saisissez le nom du locataire à l'aide de la commande `tenant-name` *tenant-name*. Par exemple, pour le nom de locataire *tenant-1*, saisissez la commande suivante pour récupérer le nombre d'utilisateurs actifs dans un déploiement multilocataire :

```
admin-Panorama> request plugins cloud_services prisma-access multi-
tenant remote-active-users-count tenant-name tenant-1 pass Nombre
 actuel d'utilisateurs : 253
```

API Prisma Access Insights

Les API Prisma Access Insights vous permettent d'interroger les locataires Prisma Access Insights pour rechercher des ressources de données. Il existe deux versions des API. Les API Prisma Access Insights 2.0 et 1.0 vous permettent toutes deux d'interroger les locataires Prisma Access pour déterminer l'intégrité du déploiement de réseau Prisma Access. Les appels d'API sont les mêmes pour les deux versions. Toutefois, les jetons d'accès utilisés et le mécanisme par lequel vous obtenez un jeton d'accès diffèrent entre les deux versions.

 ©2025 Palo Alto Networks, Inc.

Pour commencer avec Prisma Access Insights, consultez le guide du développeur : Welcome to Prisma SASE (Bienvenue dans Prisma SASE).

La page Prisma Access Insights API (API Prisma Access Insights) décrit le contenu propre aux API Prisma Access Insights. Vous trouverez également des informations sur l'API version 2.0 et l'API version 1.0, des exemples d'utilisation des API Prisma Access Insights et une FAQ sur PAI.

À propos des API 2.0

Les API 2.0 de Prisma Access Insights sont conçues pour les clients Prisma Access (Managed by Strata Cloud Manager), lorsque les locataires ont été intégrés par Palo Alto Networks à l'aide d'un identifiant de groupe de services aux locataires (TSG). Pour savoir si votre locataire utilise des ID TSG, accédez à la page Prisma Access hub, cliquez sur le nom de l'application **Prisma Access Insights** et consultez la section **Manage Apps (Gérer les applications)**.

Les clients Prisma Access (Managed by Panorama) peuvent également utiliser les API 2.0. Dans ce cas, si le déploiement Prisma Access (Managed by Panorama) est multilocataire, seul le superlocataire dispose de l'ID TSG et les sous-locataires sont inclus dans l'en-tête avec l'ID du locataire Strata Logging Service.

Cas d'utilisation des API 2.0

Après la migration du superlocataire vers l'ID TSG, lors de la recherche d'un sous-locataire :

L'en-tête a besoin des informations suivantes : `Prisma-Tenant:tsg_id:sub_tenant_id`

À propos des API 1.0

Les API 1.0 de Prisma Access Insights sont conçues pour tous les clients Prisma Access (Managed by Strata Cloud Manager) à un seul locataire ainsi que pour les clients Prisma Access (Managed by Panorama) multilocataires et à un seul locataire.

Cas d'utilisation des API 1.0

Avant la migration du superlocataire vers l'ID TSG, lorsque vous recherchez des informations sur un sous-locataire à l'aide des API 1.0, incluez l'ID du superlocataire sur le terminal :

`/api/sase/v1.0/resource/tenant/{super_tenant_id}/`

Incluez l'en-tête suivant dans l'appel : `Prisma-Tenant: {tenant_id}: {sub_tenant_id}`

 ©2025 Palo Alto Networks, Inc.

Migrer Prisma Access de Panorama vers Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access Pour lancer la migration de Prisma Access (Managed by Panorama) vers Prisma Access (Managed by Strata Cloud Manager), contactez l'équipe de compte Palo Alto Networks.

Si vous disposez d'un déploiement Prisma Access dont la configuration est gérée par Panorama et que vous souhaitez migrer vers Strata Cloud Manager pour la gestion de la configuration, Palo Alto Networks propose un flux de travail intégré au produit qui vous permet de migrer la configuration Prisma Access existante vers Strata Cloud Manager.

La gestion de la configuration Prisma Access à l'aide de Strata Cloud Manager au lieu de Panorama offre certains avantages. En voici quelques exemples :

- Évaluations continues des meilleures pratiques
- Configurations par défaut sécurisées
- Optimisation de la configuration basée sur l'apprentissage automatique (ML)
- Flux de travail de sécurité web rationalisés
- Résumé visuel interactif (centre de commande) aidant à évaluer l'intégrité, la sécurité et l'efficacité du réseau
- Flux de travail intuitifs pour les tâches complexes
- API de gestion simples et sécurisés
- Architecture cloud native offrant évolutivité, résilience et portée mondiale
- Aucun matériel à gérer ou logiciel à maintenir

Préparer la migration vers Prisma Access (Managed by Strata Cloud Manager)

Avant de commencer la migration, vous devez connaître la configuration logicielle minimale requise et les types de déploiements Prisma Access (Managed by Panorama) que vous pouvez migrer.

- **Quand migrer** : n'effectuez pas la migration pendant une mise à niveau du plan de données ou de l'infrastructure. Vérifiez vos préférences de mise à niveau pour voir si une mise à niveau du plan de données est prévue.
- **Migration unidirectionnelle de Panorama vers Prisma Access (Managed by Strata Cloud Manager)** : la migration peut uniquement avoir lieu d'un déploiement Prisma Access (Managed by Panorama) vers un déploiement Prisma Access (Managed by Strata Cloud Manager). Après

 ©2025 Palo Alto Networks, Inc.

avoir migré vers Strata Cloud Manager, vous ne pourrez pas rétablir la gestion par Panorama du déploiement Prisma Access.

- **Version minimale de Panorama** : vous avez besoin de Panorama 10.0 ou version ultérieure.
- **Rôle administrateur requis** : vous devez être connecté en tant que super utilisateur dans Strata Cloud Manager pour commencer la migration.
- **Exigences en matière de licences** : vous avez besoin d'une licence Prisma Access.
- **Cloud Identity Engine** : vous devez avoir intégré le composant de synchronisation d'annuaire du Cloud Identity Engine à Prisma Access (Managed by Panorama) avant la migration.
- **Fonctionnalités non prises en charge** : le programme de migration ne prend pas en charge les fonctionnalités Prisma Access suivantes :
  - Déploiements multilocataires
  - Sécurité IoT
  - Filtrage des données (utilisez Enterprise DLP comme solution de rechange)
  - Proxy SSH
  - Authentification distincte pour les portails et les passerelles GlobalProtect
- **Problèmes de différences de configuration** : lorsque vous exécutez config diff pendant la migration, ignorez les différences qui affichent les noms d'objet suivants, car elles n'affectent pas votre configuration :
  - Clientless-vpn crypto-settings
  - Hip-profiles rename
  - Mobile-user-redundancy
  - Exclude-video-traffic

Migrer le déploiement Prisma Access (Managed by Panorama) vers Strata Cloud Manager

Pour migrer le déploiement Prisma Access (Managed by Panorama) vers un déploiement Prisma Access (Managed by Strata Cloud Manager), procédez comme suit.

En résumé, vous devez :

1. Vérifier que vous avez appliqué la dernière configuration sur Prisma Access, enregistré la dernière configuration et exporté un fichier de configuration .xml à partir du Panorama qui gère Prisma Access.
2. Démarrer le programme de migration à partir de Strata Cloud Manager.
3. Vérifier les différences de configuration (diffs) entre la configuration Panorama et la configuration Strata Cloud Manager migrée.
4. Résoudre les différences et terminer la migration.

 ©2025 Palo Alto Networks, Inc.

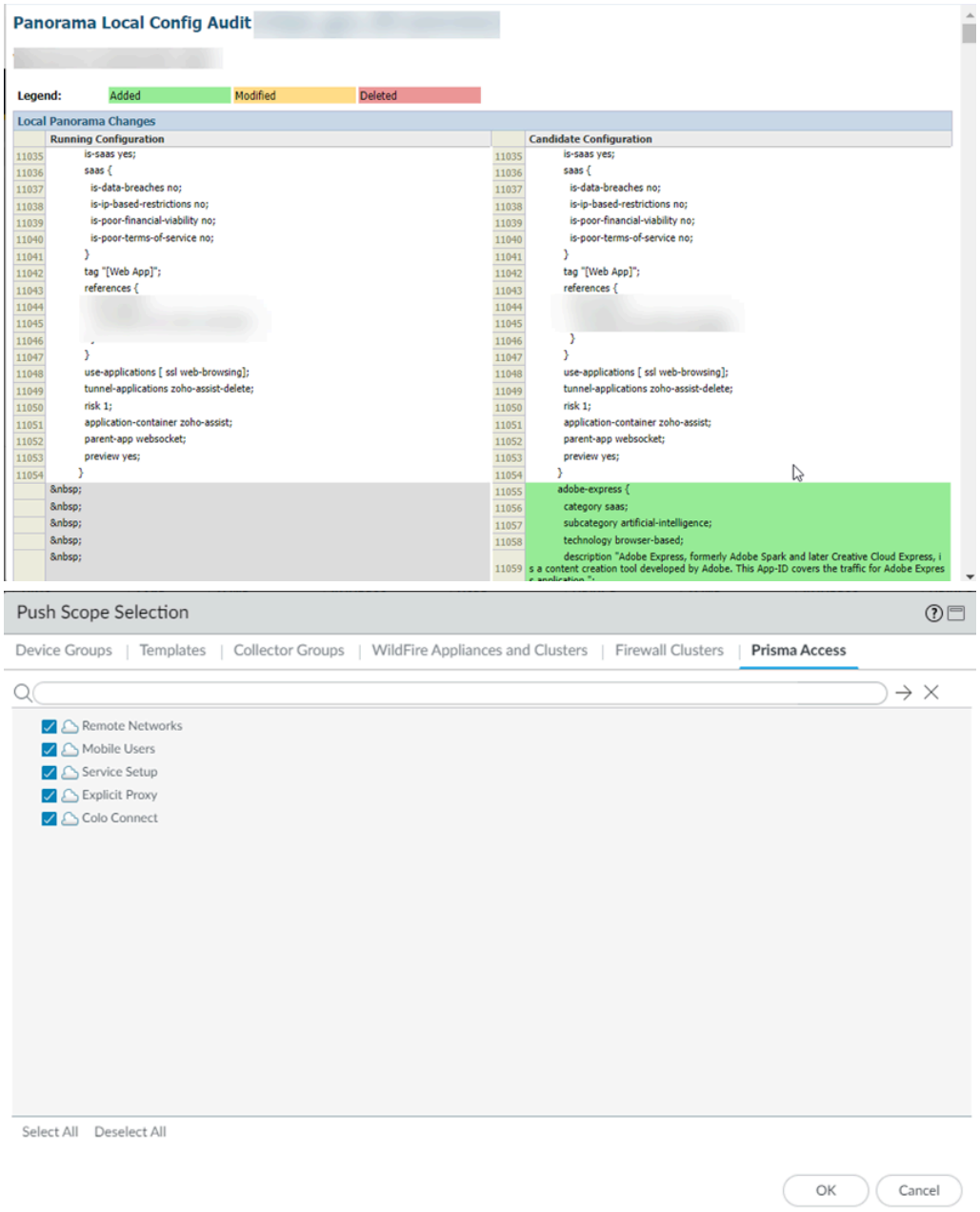
STEP 1 | Préparez votre Panorama pour la migration.

1. Connectez-vous au Panorama qui gère Prisma Access avec un compte d’administration auquel le rôle de super utilisateur est attribué.
2. (Facultatif) Si vous avez configuré une clé principale personnalisée pour votre Panorama et pour Prisma Access, notez-la.

   Si votre déploiement utilise la clé principale par défaut, cette étape n’est pas requise.
3. Assurez-vous que la configuration actuelle de Panorama est à jour, que vous avez validé toutes les modifications à Panorama et que vous avez appliqué ces modifications sur Prisma Access. Pour ce faire, accédez à **Commit (Valider)** > **Commit & Push (Valider et appliquer)** et sélectionnez **Preview Changes (Prévisualiser les modifications)**.
4. (Facultatif) Vérifiez les différences entre la configuration en cours d’exécution et la configuration candidate, puis décidez si vous souhaitez appliquer ces modifications. Si vous souhaitez valider et appliquer les modifications, sélectionnez **Edit Selections**

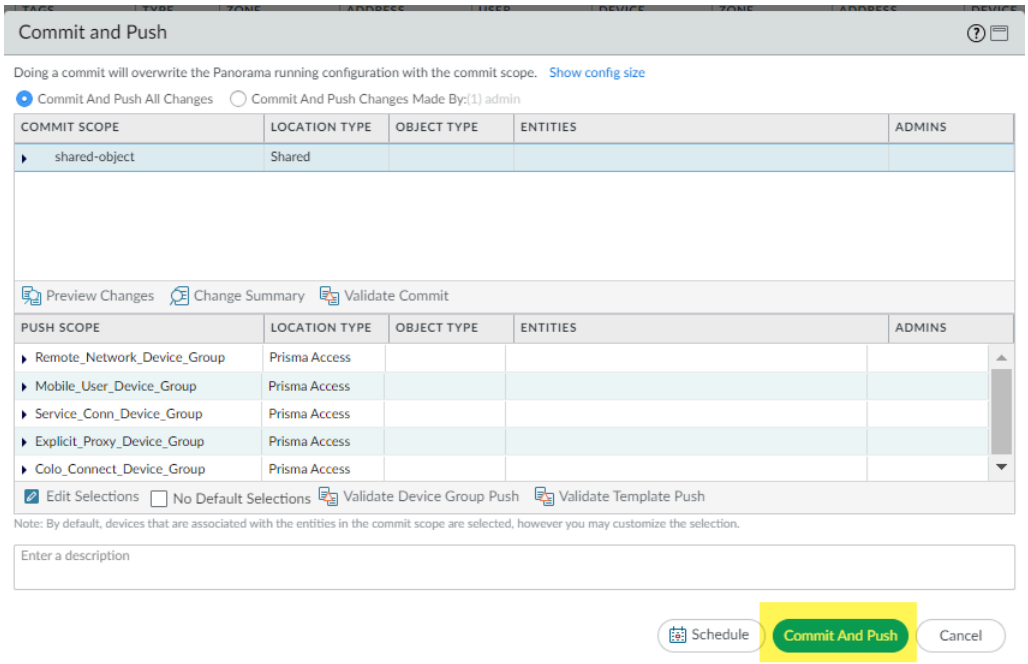
 ©2025 Palo Alto Networks, Inc.

(Modifier les sélections), puis sélectionnez les composants Prisma Access que vous souhaitez appliquer dans **Push Scope (Étendue de la transmission)**.



5. (Facultatif) Sélectionnez **Commit and Push (Valider et appliquer)** pour valider et appliquer les modifications.

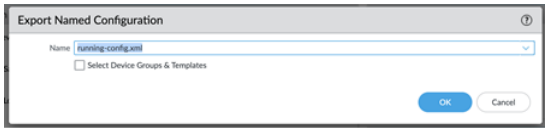
 ©2025 Palo Alto Networks, Inc.



6. Accédez à **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et sélectionnez **Export named Panorama configuration snapshot (Exporter l'instantané de configuration Panorama nommé)**.

   Ce fichier .xml doit être chargé sur Strata Cloud Manager pendant le processus de migration. **Chargez uniquement le fichier de configuration .xml ; ne chargez pas de fichiers de support technique ni aucun autre fichier.**

7. Sélectionnez le fichier de configuration **running-config.xml**, puis appuyez sur **OK**.

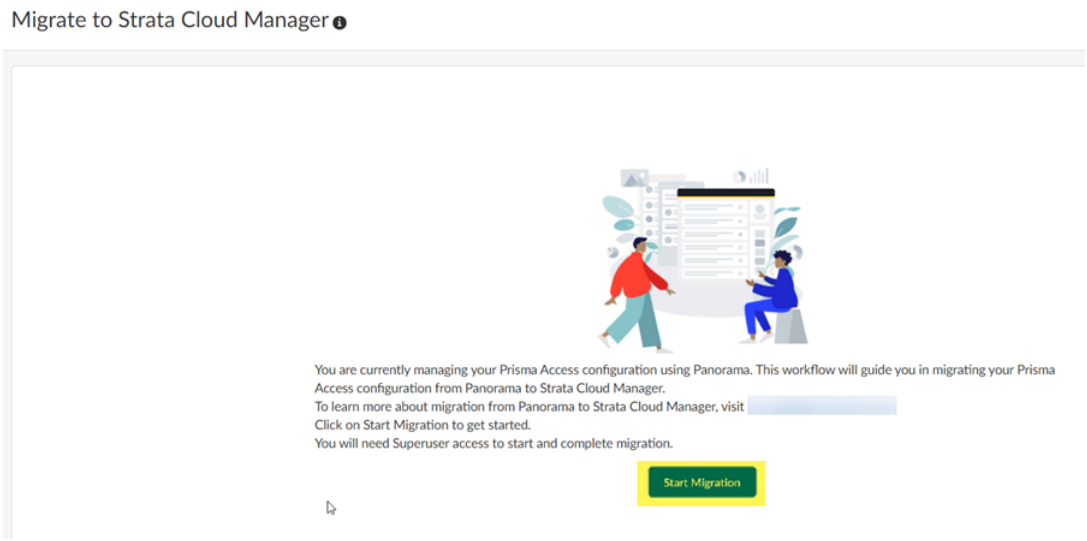


STEP 2 | Connectez-vous à Strata Cloud Manager en tant qu'administrateur avec un rôle de super utilisateur et accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)**.

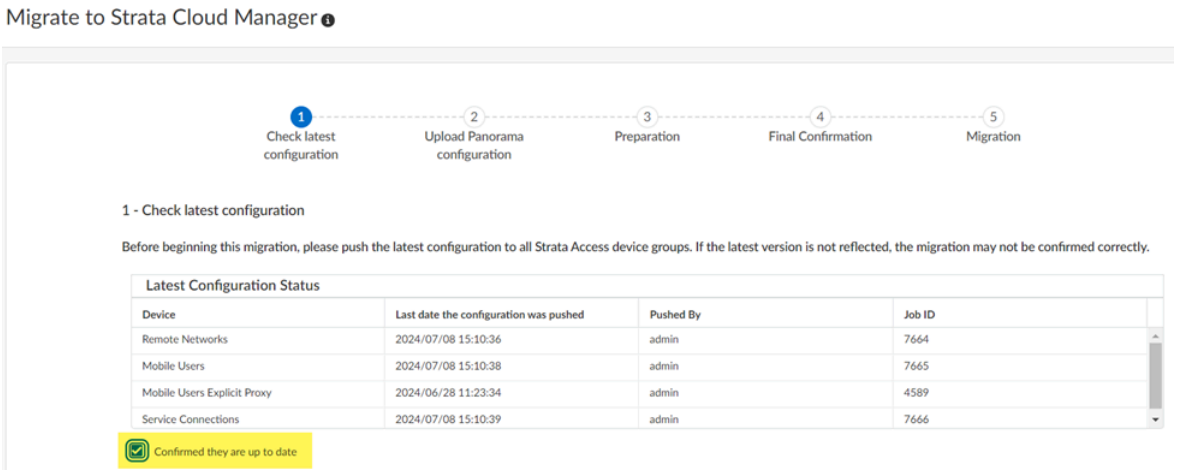
Le programme de migration détecte que vous disposez d'un déploiement géré par Panorama.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Sélectionnez **Start Migration (Démarrer la migration)**.



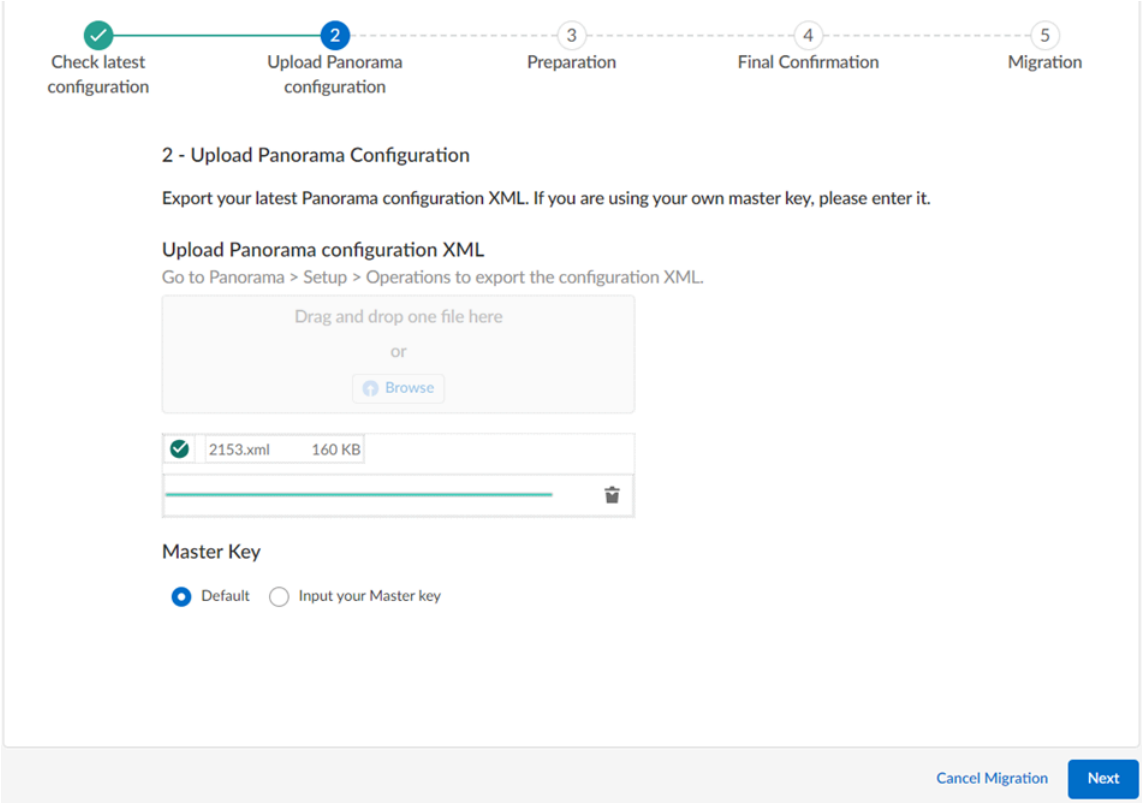
STEP 4 | Le programme de migration vous demande de vérifier si la configuration est à jour et vous indique le dernier utilisateur qui l'a mise à jour. Après avoir vérifié que cette configuration comporte les dernières modifications, sélectionnez **Confirmed they are up to date (Confirmation de leur mise à jour)** et cliquez sur **Next (Suivant)**.



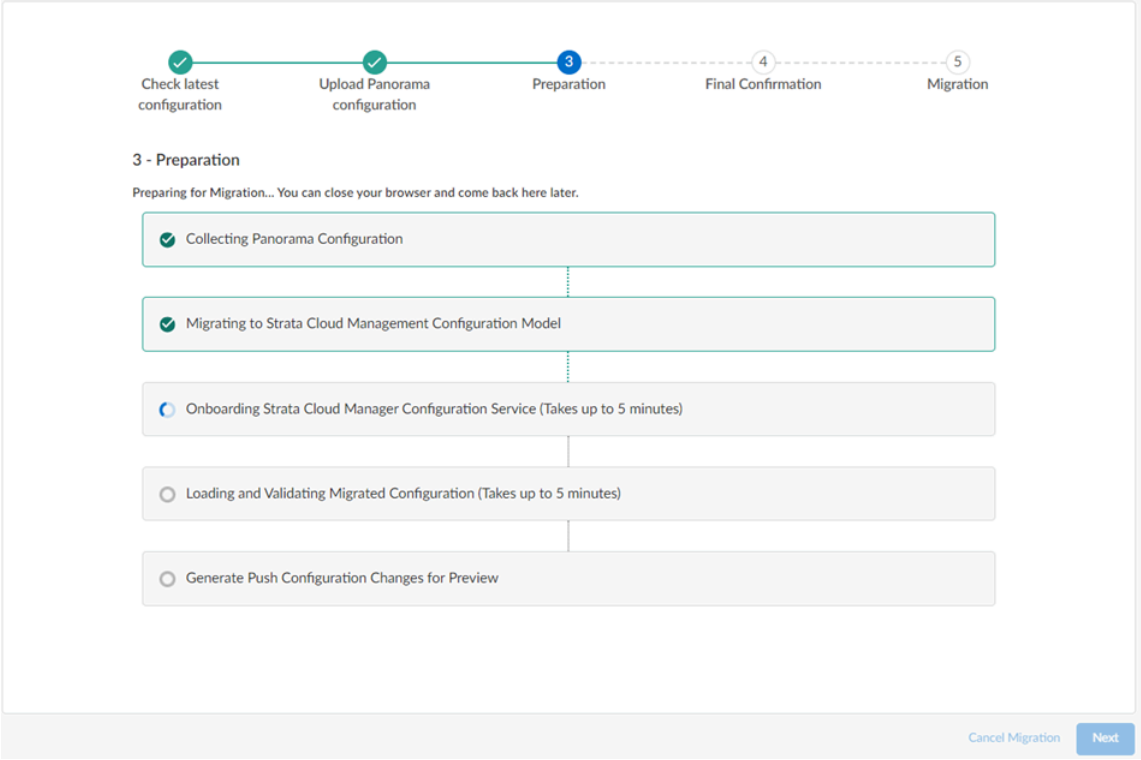
STEP 5 | Sélectionnez le fichier .xml de configuration Panorama que vous avez téléchargé au cours d'une précédente étape en le faisant glisser et en le déposant, ou en utilisant l'option **Choose File (Choisir un fichier)**.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Saisissez votre **Master Key (Clé principale)**, ou si vous n'avez pas créé de clé principale personnalisée, demandez à Strata Cloud Manager d'utiliser la clé principale **Default (Par défaut)**, puis cliquez sur **Next (Suivant)**.



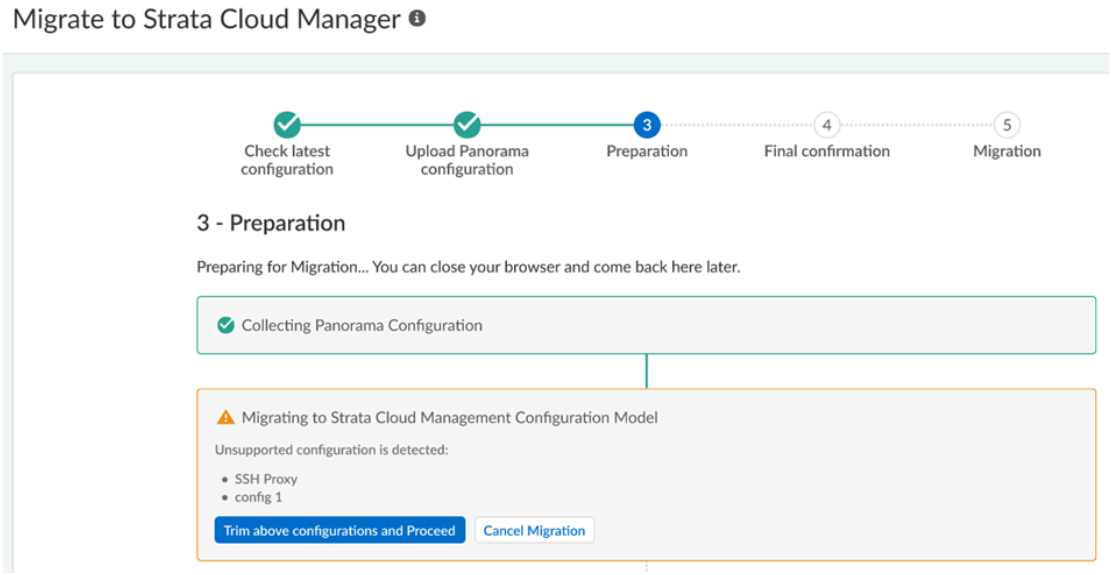
Le programme de migration commence.



 ©2025 Palo Alto Networks, Inc.

Attendez que toutes les étapes soient terminées.

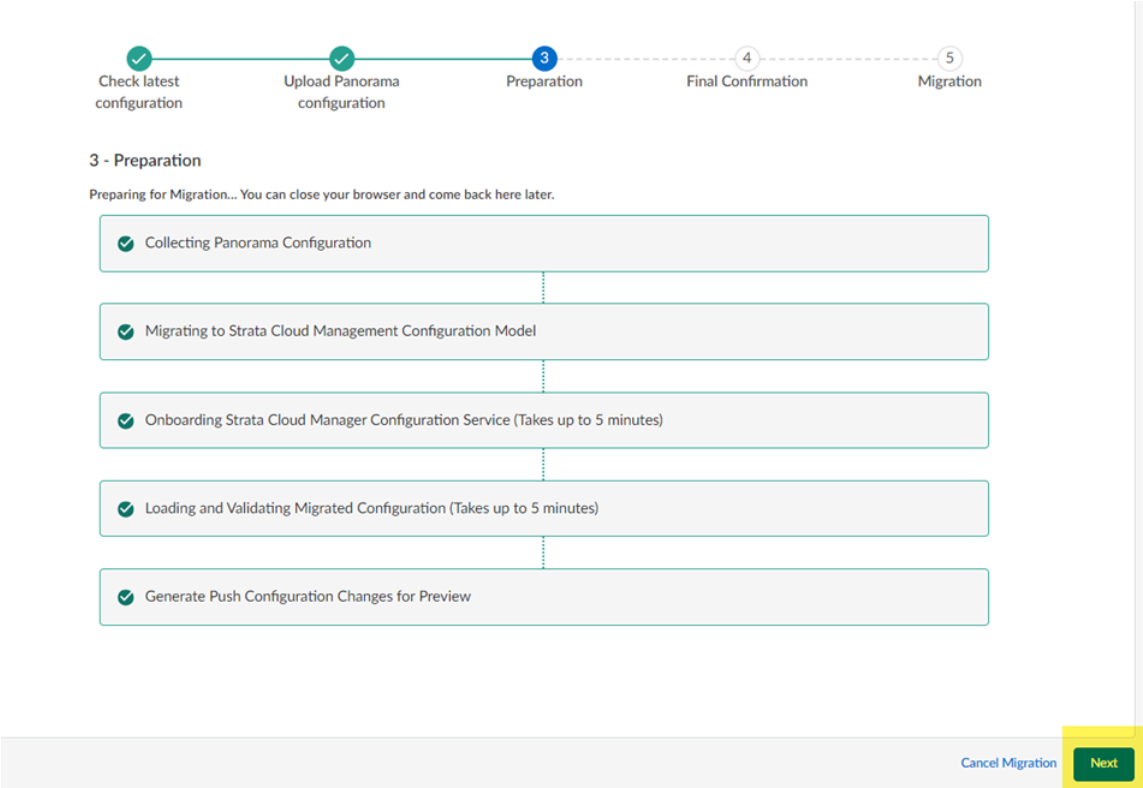
STEP 7 | Si, lors de la migration, le programme indique qu'il a rencontré une configuration non prise en charge, vous pouvez sélectionner **Trim the above configurations and proceed (Couper les configurations ci-dessus et continuer)** ou **Cancel migration (Annuler la migration)**.



Certaines configurations non prises en charge (comme les configurations multilocataires) annulent la migration et le programme de migration ne peut pas résoudre le problème. Le cas échéant, sélectionnez **Cancel Migration (Annuler la migration)**.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Une fois la migration terminée, cliquez sur **Next (Suivant)**.



STEP 9 | Si le programme de migration a apporté des modifications, passez-les en revue sur l'écran de confirmation finale.

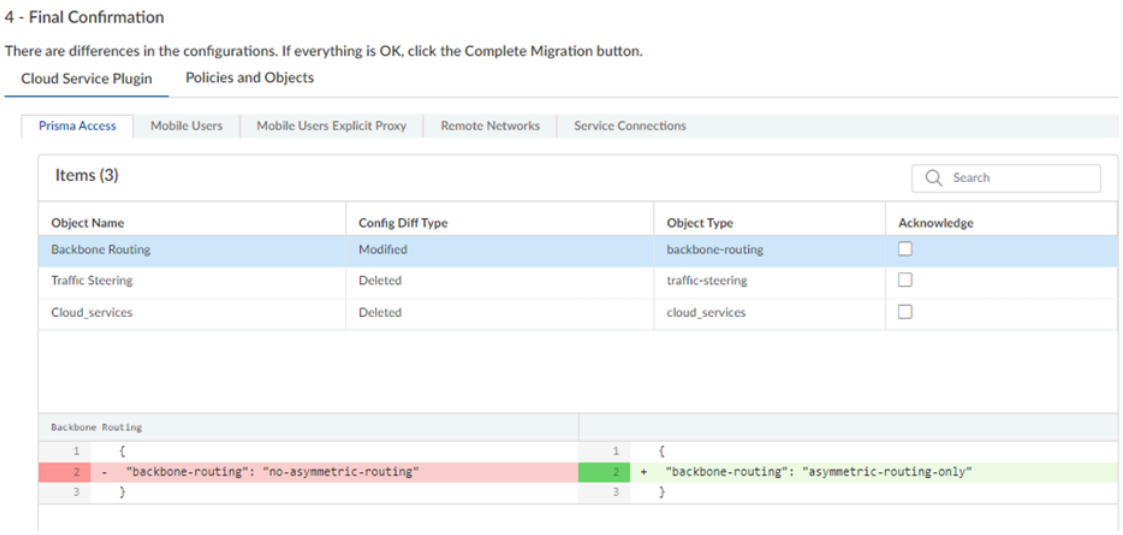
Le programme de migration peut apporter des modifications à la configuration pour tenir compte des différences entre la configuration Panorama et la configuration Strata Cloud Manager, ou pour corriger une fonctionnalité non prise en charge. Si des modifications

 ©2025 Palo Alto Networks, Inc.

sont nécessaires, le programme de migration affiche ces modifications dans une vue des différences, avec les nouvelles lignes en vert et les lignes supprimées en rouge.

Ignorez les différences qui affichent les noms d'objets suivants, car elles n'affectent pas votre configuration :

- *Clientless-vpn crypto-settings*
- *Hip-profiles rename*
- *Mobile-user-redundancy*
- *Exclude-video-traffic*



STEP 10 | (Facultatif) Modifiez les différences de configuration.

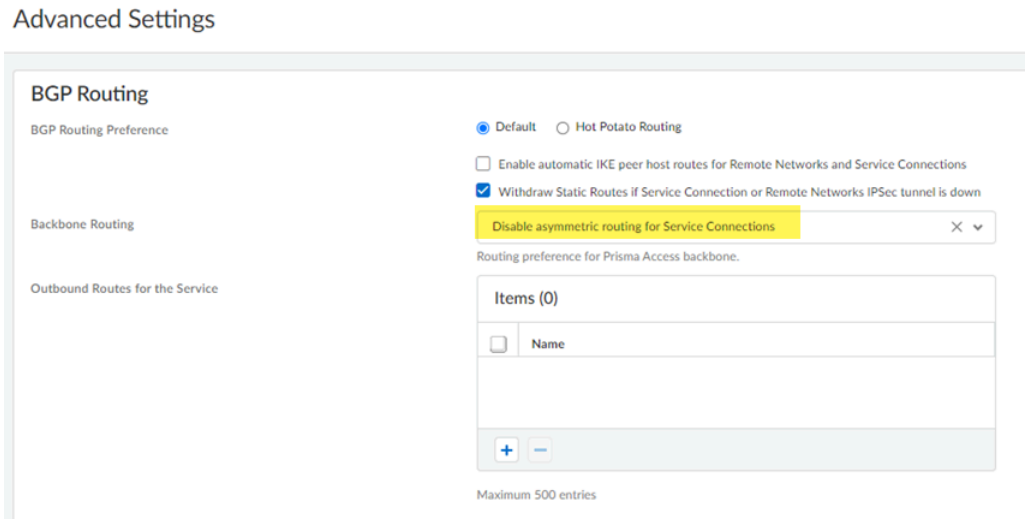
Les modifications que vous apportez ne sont pas validées sur la configuration tant que vous n'avez pas terminé la migration et appliqué les modifications sur Strata Cloud Manager.

1. Accédez à la zone dans la configuration Prisma Access où vous avez trouvé les différences, puis modifiez la configuration.

   Pour l'exemple donné à l'étape précédente, le programme de migration a apporté une modification au routage principal (en remplaçant **no-asymmetric-routing** par **asymmetric-routing-only**). Pour rétablir ce paramètre tel qu'il était défini dans la configuration d'origine, accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration Prisma Access)** > **Service Connections (Connexions aux services)** > **Advanced Settings (Paramètres avancés)** > et définissez le **Backbone Routing (Routage**

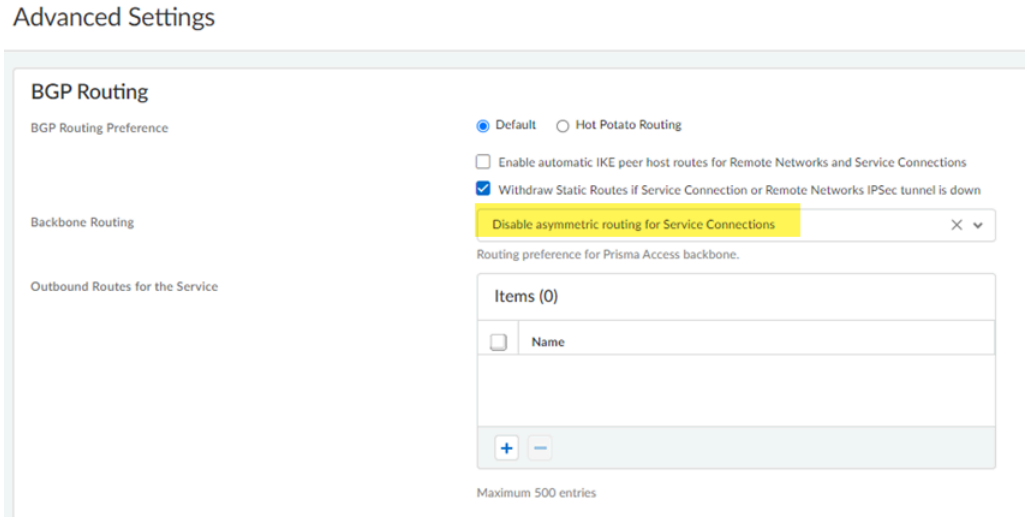
 ©2025 Palo Alto Networks, Inc.

principal) sur **Disable Asymmetric Routing for Service Connections (Désactiver le routage asymétrique pour les connexions aux services)**.



2. (Facultatif) Pour ne pas perdre le fil de vos modifications, sélectionnez **Acknowledge (Accepter)** au fur et à mesure que vous les réalisez.

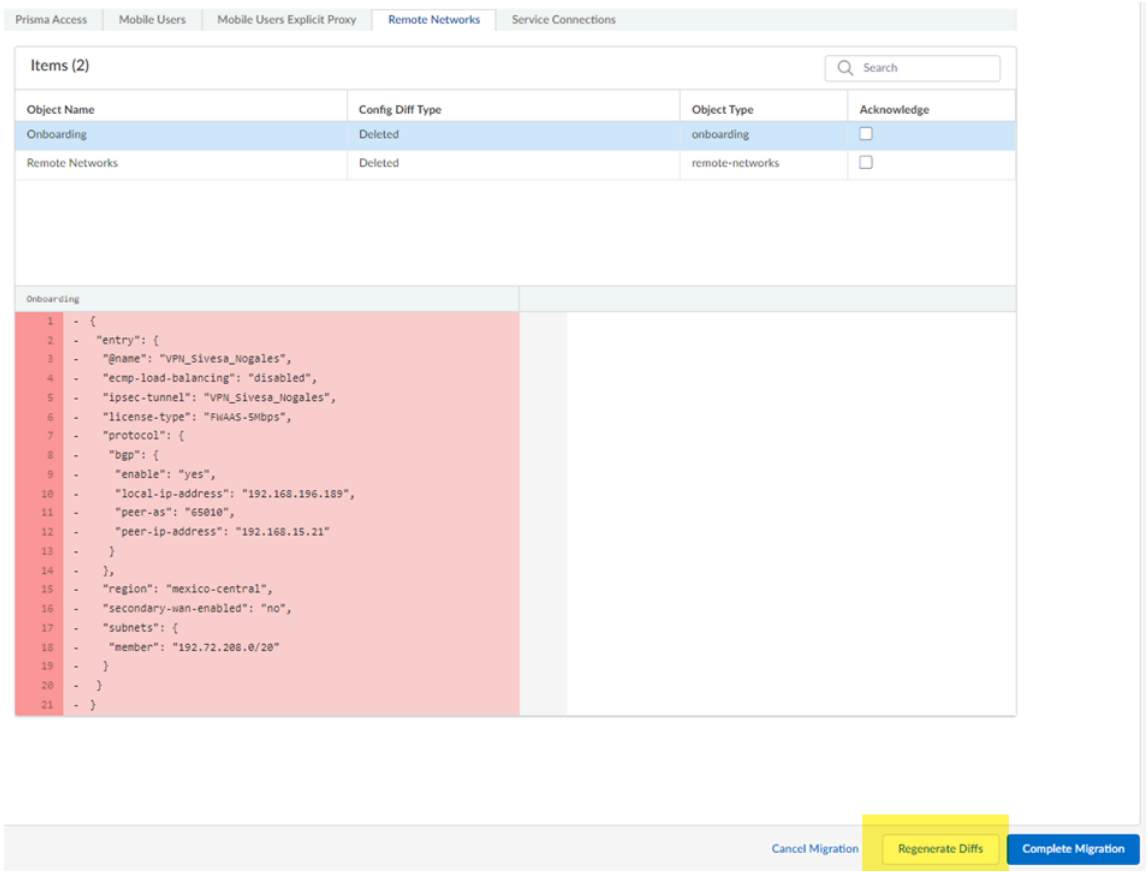
   Bien que cela ne soit pas obligatoire, il peut être utile d'accepter les modifications au fur et à mesure que vous les réalisez afin de savoir où vous en êtes.



3. Continuez de passer en revue les changements, d'y apporter des modifications et de les accepter.

 ©2025 Palo Alto Networks, Inc.

STEP 11 | (Facultatif) Si vous avez apporté des modifications à la configuration, sélectionnez **Regenerate Diffs (Régénérer les différences)** pour voir les différences mises à jour.

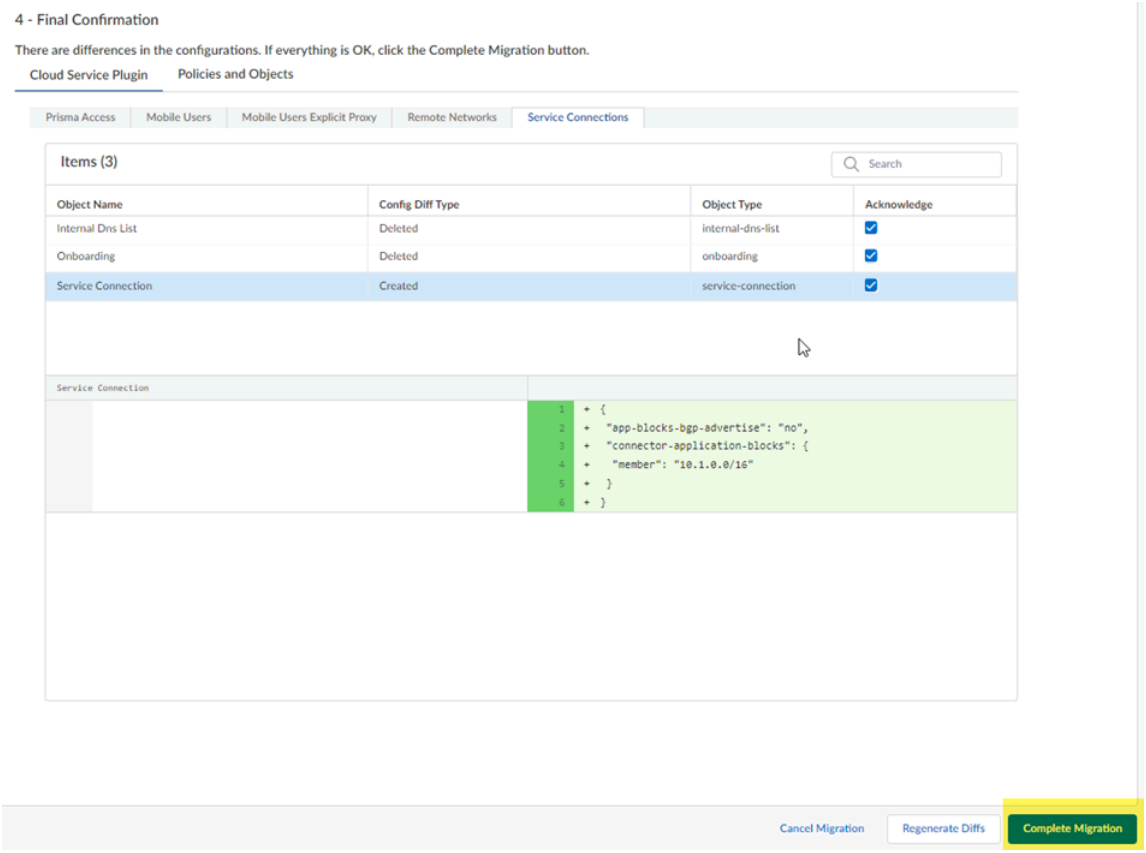


 ©2025 Palo Alto Networks, Inc.

STEP 12 | Sélectionnez **Complete Migration (Terminer la migration)**.

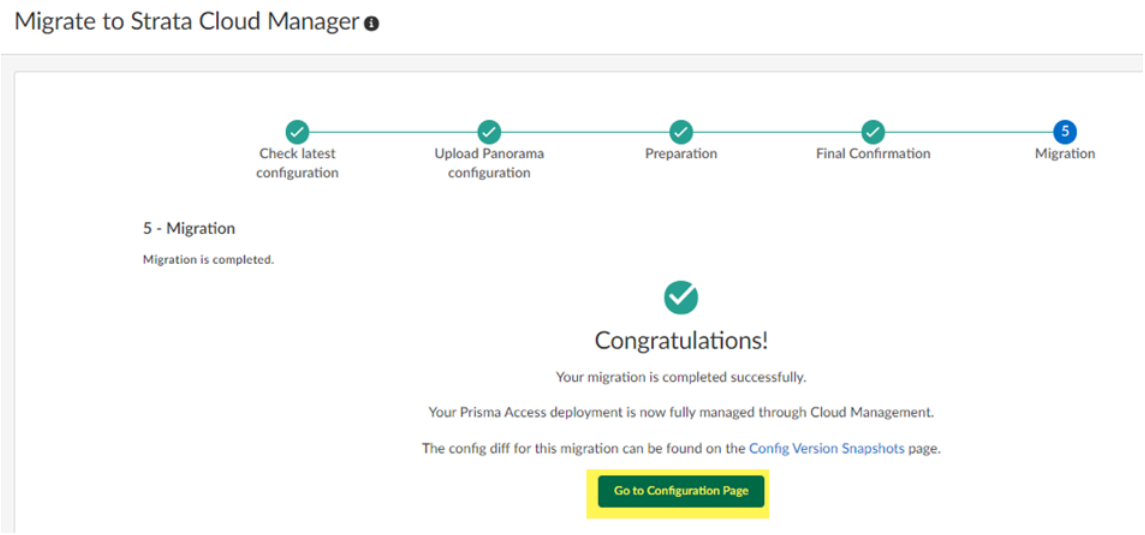
Bien que cela ne soit pas obligatoire, vous pouvez également sélectionner **Acknowledge (Accepter)** pour accepter les modifications.

Après avoir sélectionné Complete Migration (Terminer la migration), vous ne pourrez pas revenir à un déploiement géré par Panorama. Votre déploiement utilisera définitivement Strata Cloud Manager pour sa gestion.

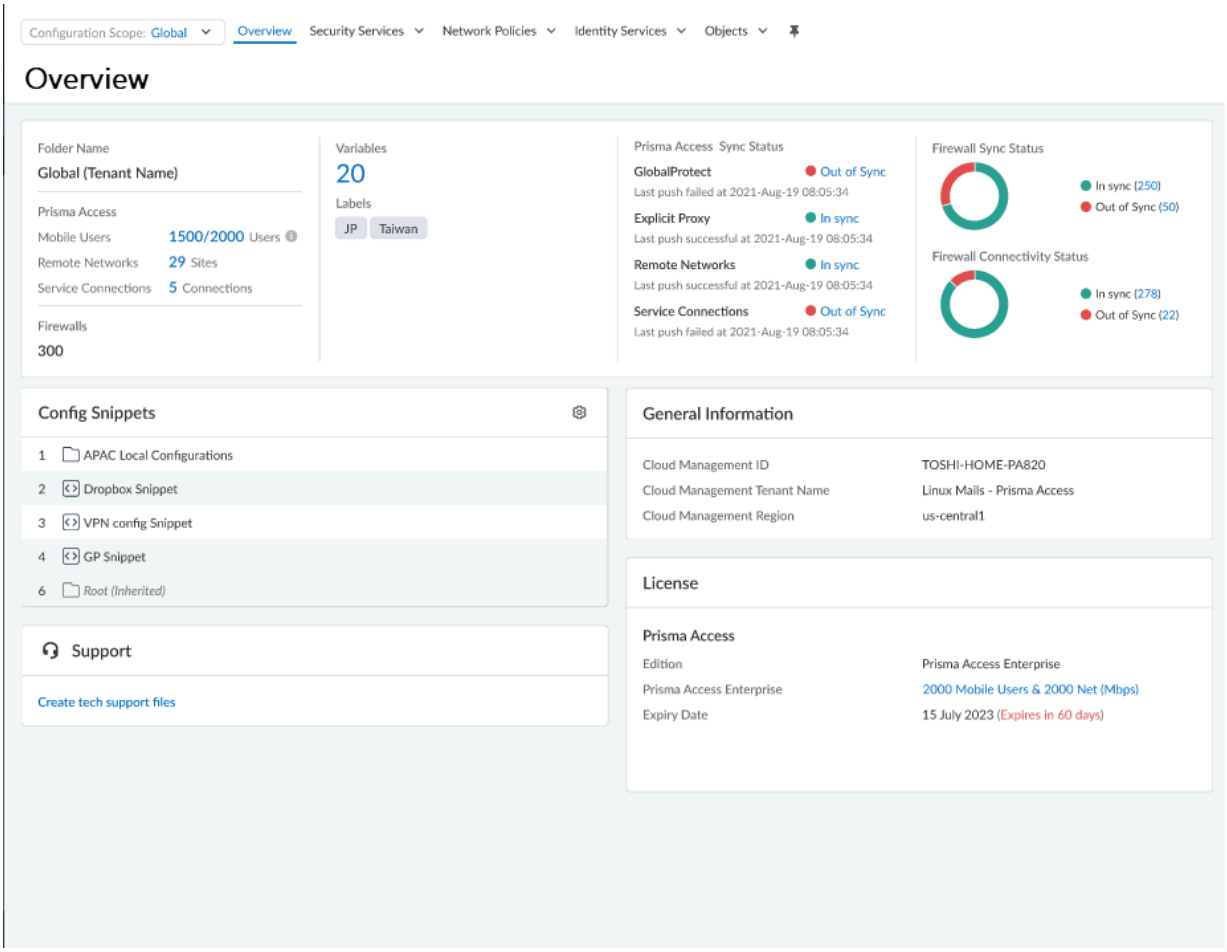


 ©2025 Palo Alto Networks, Inc.

STEP 13 | (Facultatif) Sélectionnez **Go to Configuration Page (Aller à la page de configuration)** pour voir la configuration migrée.



Le déploiement migré s'affiche.



 ©2025 Palo Alto Networks, Inc.

STEP 14 | Sélectionnez **Push Config (Transmettre la configuration)** > **Push (Pousser)** pour appliquer les modifications de la configuration migrée.

Cette opération de transmission permet de s’assurer que la migration s’est terminée correctement et que Prisma Access a appliqué toutes les modifications à la configuration migrée.

STEP 15 | Notez tous les messages que vous avez reçus pendant l’opération de transmission et, si vous rencontrez des problèmes, apportez les modifications nécessaires à la configuration.

 ©2025 Palo Alto Networks, Inc.

Prisma Access Versions et mises à niveau

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Les versions et les mises à jour de Prisma Access vous permettent de rester à jour et de sécuriser vos utilisateurs. Certaines des mises à jour sont gérées par Palo Alto Networks, telles que celles de l'infrastructure Prisma Access se met à jour et vous recevrez une notification préalable pour vous organiser en conséquence. Les autres mises à jour relèvent de votre responsabilité et vous devez planifier la version spécifiée de la mise à jour de contenu, de la mise à jour logicielle et de la version du plug-in (si nécessaire), dès que possible.



Vous pouvez récupérer l'état de tous les services cloud, y compris Prisma Access et Strata Logging Service, ainsi qu'un historique de la disponibilité de chaque service, en accédant au site Internet https://sase.status.paloaltonetworks.com/. *Vous pouvez également vous inscrire pour recevoir des mises à jour par e-mail ou par SMS sur ce site afin d'être averti à l'avance lorsque des mises à jour de l'infrastructure sont prévues et des notifications en temps réel lorsque des mises à jour se produisent, et lorsque Palo Alto Networks crée, met à jour ou résout un incident.*

Prisma Access Types de version

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Prisma Access dispose de mises à niveau, y compris des versions majeures et la maintenance de l'infrastructure, qui incluent de nouvelles fonctionnalités et des optimisations pour offrir une sécurité de pointe à vos réseaux distants et à vos utilisateurs mobiles.

La liste suivante définit les types de versions, ainsi que la notification préalable que nous vous fournissons pour chaque version. Pour vous assurer de recevoir des notifications pour toutes les versions, inscrivez-vous pour recevoir des notifications par e-mail ou par SMS pour Prisma Access sur le site https://sase.status.paloaltonetworks.com/ et inscrivez-vous pour recevoir des alertes Strata Cloud Manager.

- **Sortie majeure**—Une version majeure inclut généralement de nouvelles fonctionnalités et des optimisations importantes, et ces mises à jour sont poussées avec une fenêtre de maintenance planifiée configurée par Palo Alto Networks. Palo Alto Networks informe les clients de ces activités de maintenance planifiées par le biais de notifications par e-mail via sase.status.paloaltonetworks.com.

  Notification—Palo Alto Networks vous fournit les notifications suivantes pour les versions majeures :

Type de déploiement	Période de notification
Déploiements en production	Palo Alto Networks vous envoie une notification 21 jours avant la sortie d'une version majeure.
Déploiements en laboratoire	Palo Alto Networks vous fournit une notification 7 jours avant la sortie d'une version majeure.



En plus d'une mise à niveau majeure programmée, Palo Alto Networks pourrait avoir besoin de réaliser des mises à niveau urgentes programmées, qui suivent un horaire différent.

Les locataires de laboratoire ne sont pas couverts par l'accord de niveau de service (SLA) Prisma Access et il est vivement conseillé aux clients d'utiliser les locataires uniquement à des fins de test de pré-production et de qualification.

©2025 Palo Alto Networks, Inc.

- **Maintenance des infrastructures**—Inclut des fonctionnalités et des optimisations incrémentielles. Dans certains cas, Palo Alto Networks peut combiner un correctif avec la maintenance des infrastructures.

  Notification—Palo Alto Networks vous fournit les notifications suivantes :

Type de déploiement	Période de notification
Déploiements en production	Palo Alto Networks vous envoie une notification 10 jours avant la maintenance des infrastructures.
Déploiements en laboratoire	Palo Alto Networks vous fournit une notification 7 jours avant la maintenance des infrastructures.

  En plus d'une mise à niveau majeure programmée, Palo Alto Networks pourrait avoir besoin de réaliser des mises à niveau urgentes programmées, qui suivent un horaire différent.

- **Version du plug-in Cloud Services (Déploiements gérés par Panorama uniquement)** —Si Prisma Access nécessite un nouveau plug-in, il est disponible en téléchargement via le Palo Alto Networks Portail d'assistance à la clientèle (CSP) et sur Panorama à la date de disponibilité générale (GA) de la version.

  Prisma Access peut forcer tous les locataires à effectuer une mise à niveau vers une version spécifique du plug-in Cloud Services pour maintenir la compatibilité descendante et les versions logicielles prises en charge. Une telle mesure d'application donnera un **préavis de 14 jours** (via sase.status.paloaltonetworks.com) pour planifier la mise à jour du plug-in. Le service vous recommande vivement de passer au dernier plug-in dès qu'il est disponible en téléchargement.

Mises à niveau urgentes programmées

Palo Alto Networks doit parfois effectuer des mises à niveau urgentes du plan de données ou des infrastructures, y compris des correctifs ou des corrections de bogues d'urgence (par exemple, des correctifs pour les menaces zero-day ou des modifications de plug-in). Palo Alto Networks s'efforcera de vous donner un préavis de 48 heures avant une mise à niveau urgente et programmée ; cependant, à l'occasion, vous pouvez recevoir un préavis plus court pour une mise à niveau planifiée urgente.

©2025 Palo Alto Networks, Inc.

Types de mise à niveau de Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Palo Alto Networks met à niveau son infrastructure basée sur le cloud sans aucune intervention de votre part. Certaines mises à niveau nécessitent que vous effectuiez une action, comme installer un nouveau plug-in.

La liste suivante comprend les différents types de mises à niveau de Prisma Access :

- **Mise à niveau de l'infrastructure** : Palo Alto Networks met à niveau l'infrastructure Prisma Access, également connue sous le nom de Prisma Access *Control Plane (Plan de contrôle Prisma Access)*, qui comprend l'infrastructure de backend, d'orchestration et de surveillance des services sous-jacents.

  Vous pouvez vous attendre à recevoir des mises à niveau d'infrastructure 4 à 6 fois par an.
- **Mise à niveau du plan de données** : Palo Alto Networks met à niveau le plan de données Prisma Access qui permet l'inspection du trafic et l'application de la politique de sécurité sur votre réseau et le trafic des utilisateurs.

  Vous utilisez l'application pour vous inscrire aux notifications par e-mail d'alerte de mise à niveau de plan de données et indiquer vos préférences de mise à niveau.
- **Maintenance planifiée de Prisma Access** : Prisma Access réserve une fenêtre toutes les deux semaines pour effectuer des opérations de maintenance liées aux correctifs et aux corrections de bogues d'urgence de l'infrastructure.
- (Déploiements gérés par Panorama uniquement) **Mise à niveau du plug-in Cloud Services** : lorsqu'une nouvelle version du plug-in est disponible, votre administrateur réseau devra mettre à niveau le plug-in Cloud Services sur l'appareil Panorama qui gère Prisma Access.
- (Déploiements gérés par Panorama uniquement) **Mise à niveau de la version du logiciel Panorama** : une mise à niveau de votre logiciel Panorama pourrait être nécessaire pour garantir une compatibilité continue avec Prisma Access.

Le tableau suivant vous montre ce qui est inclus avec chaque version, y compris la fenêtre de maintenance que nous fournissons et tout impact sur votre service Prisma Access.

Type de mise à niveau	Fenêtre de maintenance	Impact
Mise à niveau de l'infrastructure	2-8 heures	Aucun impact sur le trafic réseau ; cependant, vous ne pouvez pas effectuer de validations pendant la fenêtre de maintenance.

©2025 Palo Alto Networks, Inc.

Type de mise à niveau	Fenêtre de maintenance	Impact
		Palo Alto Networks planifie les mises à niveau à une heure locale qui perturbe le moins possible les fonctions professionnelles.
Mise à niveau du plan de données	72 heures	Palo Alto Networks utilise cette fenêtre pour mettre à niveau le plan de données pour tous les clients. Vous pouvez apporter des modifications de configuration et des validations pendant cette période. Notre objectif est de réduire au minimum l'impact sur le trafic réseau, mais dans certains cas, il peut y avoir une brève interruption. Pour plus d'informations, reportez-vous à la section Mises à niveau du plan de données de Prisma Access. Vous utilisez l'application pour vous inscrire aux notifications d'alerte par e-mail concernant la mise à niveau du plan de données et indiquer vos préférences de mise à niveau, y compris la fenêtre temporelle préférée pour votre mise à niveau.
Mise à niveau du plug-in Cloud Services (Déploiements gérés par Panorama uniquement)	Vous installez le plug-in lorsqu'il devient disponible.	Prisma Access pourrait vous obliger à mettre à niveau tous les locataires vers une version spécifique du plug-in afin de maintenir la compatibilité descendante et les versions de logiciels prises en charge. Pendant la mise à niveau du plug-in, vous ne pouvez pas apporter de modifications de configuration et de validations dans Panorama.
Mise à niveau de la version du logiciel Panorama	Vous planifiez et effectuez la mise à niveau sur le	Lorsque Prisma Access met à niveau son infrastructure

 ©2025 Palo Alto Networks, Inc.

Type de mise à niveau	Fenêtre de maintenance	Impact
(Déploiements gérés par Panorama uniquement)	Panorama qui gère Prisma Access.	et son plan de données après une version majeure, les mises à niveau peuvent être incompatibles avec les versions antérieures de Panorama. En raison de la publication rapide de Prisma Access et du plug-in Cloud Services, les dates de compatibilité logicielle (fin de prise en charge) pour Panorama sont plus courtes que les dates de fin de vie logicielle pour les versions de Panorama et s'appliquent uniquement à la compatibilité des versions de Panorama avec Prisma Access. Pour plus d'informations, y compris les dates de fin de prise en charge pour Panorama lorsqu'il est utilisé avec Prisma Access, reportez-vous à la compatibilité des versions de Prisma Access et Panorama dans la matrice de compatibilité de Palo Alto Networks.

 ©2025 Palo Alto Networks, Inc.

Cadence des mises à jour logicielles et de contenu pour Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

- Strata Cloud Manager
- Panorama

Cadence des mises à jour logicielles et de contenu pour Prisma Access (Managed by Strata Cloud Manager)

Le tableau suivant décrit comment Prisma Access met à jour ses composants d'infrastructure, y compris les mises à jour logicielles et de contenu. Ce tableau indique également si Prisma Access met à jour automatiquement le logiciel. Si certaines mises à jour ne sont pas automatiques, vous pouvez apprendre comment appliquer ces mises à jour d'infrastructure.

Vous pouvez également vérifier l'état de tous les services cloud depuis le hub.

Composant	Calendrier de mise à jour	Commentaires
Application GlobalProtect	• **Versions majeures de l'application GlobalProtect (par exemple, *x*.0 ou 4.*x*) :** Prisma Access met à jour l'application avec la dernière version majeure 7 à 10 jours après la disponibilité générale de la version *x*.0.1 de cette version. Par exemple, avec une version d'application 4.0, Prisma Access met à jour l'application 7 à 10 jours après la sortie de la version 4.0.1. • **Versions mineures de l'application GlobalProtect (par exemple, 4.1.*x*) :** Prisma Access met à jour l'application avec la dernière version mineure 7 à 10 jours après la disponibilité générale de cette version.	Le cloud contrôle la version de l'application disponible pour la mise à niveau.
Mises à niveau logicielles	Palo Alto Networks® met à niveau l'infrastructure PAN-OS lorsqu'une nouvelle	Inscrivez-vous pour recevoir les mises à niveau

 ©2025 Palo Alto Networks, Inc.

Composant	Calendrier de mise à jour	Commentaires
PAN-OS dans l'infrastructure Prisma Access — prévues	version de Prisma Access est disponible. Palo Alto Networks® vous prévient trois semaines à l'avance avant une mise à niveau programmée.	de l'infrastructure par e-mail ou par SMS dans le hub.
Mises à jour des applications et des menaces	Tous les jours avec un seuil de 24 heures. Palo Alto Networks® publie de nouveaux App-ID le troisième mardi de chaque mois. Prévoyez de revoir et d'intégrer ces nouveaux App-ID dans les 24 heures. Utilisez le nouveau filtre App-ID pour minimiser cet impact possible sur le trafic. La nouvelle caractéristique App-ID vous permet de voir les nouvelles applications sur votre réseau et vous fournit des informations détaillées sur l'activité des applications nouvellement catégorisées. Ce que vous apprenez peut vous aider à prendre les bonnes décisions concernant la mise à jour de votre politique de sécurité afin de faire appliquer les ID d'application les plus récents.	
Protection antivirus	Toutes les heures, 10 minutes après l'heure	Prisma Access est toujours à jour avec la dernière version d'antivirus.
WildFire	Temps réel	Prisma Access est toujours à jour avec la dernière version de WildFire.
Fichier de données GlobalProtect	Toutes les heures	Prisma Access est toujours à jour avec la dernière version du fichier de données GlobalProtect.
VPN sans client Signatures d'applications	Toutes les heures	Prisma Access est toujours à jour avec la dernière version de signature d'application VPN sans client.

Cadence des mises à jour logicielles et de contenu pour Prisma Access (Managed by Panorama)

Le tableau suivant vous informe des mises à jour logicielles et de contenu pour obtenir les dernières applications et signatures de menaces, et tirer parti des capacités de prévention des

 ©2025 Palo Alto Networks, Inc.

menaces fournies par Palo Alto Networks. Si la colonne **Cloud Controlled? (Contrôlé par le cloud ?)** présente l'attribut **No (Non)**, vous effectuez les actions requises pour mettre à jour le composant.

Composant	Calendrier de mise à jour	Cloud Controlled? (Contrôlé par le cloud ?) (Yes/No) (Oui/Non)	Commentaires

Mises à niveau du logiciel Panorama pour la compatibilité avec Prisma Access	Pour les versionsPrisma Access majeures, vous devrez peut-être mettre à niveau votre version de Panorama pour les cas d'utilisation suivants :
	• **Mise à niveau requise** : Il vous sera parfois demandé de mettre à niveau la version du logiciel sur Panorama pour maintenir la compatibilité avec Prisma Access.
	  • **Fenêtre de maintenance** : votre organisation devra planifier une fenêtre de maintenance pour mettre à niveau la version du logiciel Panorama.
	  • **Impact** : vous ne pouvez pas utiliser la nouvelle version du plug-in tant que vous n'avez pas mis à niveau
		Non	Consultez les dates de fin de prise en charge (End of Support, EoS) pour la compatibilité des versions du logiciel Panorama avec Prisma Access pour savoir quand une version de Panorama devient incompatible avec Prisma Access. Reportez-vous à Prisma Access et compatibilité des versions Panorama pour les versions Panorama actuellement prises en charge à utiliser avec Prisma Access. Pour mettre à niveau votre Panorama vers une nouvelle version, consultez Installer les mises à jour de contenu et logicielles pour Panorama.

©2025 Palo Alto Networks, Inc.

Composant	Calendrier de mise à jour	Cloud Controlled? (Contrôlé par le cloud ?) (Yes/No) (Oui/Non)	Commentaires
	votre version de Panorama. • **Notification** : Palo Alto Networks vous enverra une notification 100 jours avant la mise à niveau majeure prévue. • **Mise à niveau facultative** : dans d'autres cas, vous devrez peut-être mettre à niveau la version du logiciel Panorama pour utiliser les nouvelles fonctionnalités quePrisma Access prend en charge dans la version majeure. • **Fenêtre de maintenance** : votre organisation devra planifier une fenêtre de maintenance pour mettre à niveau la version du logiciel Panorama. • **Impact** : vous ne pouvez pas utiliser les nouvelles fonctionnalités que Prisma Access prend		

©2025 Palo Alto Networks, Inc.

Composant	Calendrier de mise à jour	Cloud Controlled? (Contrôlé par le cloud ?) (Yes/No) (Oui/Non)	Commentaires
	en charge jusqu'à ce que vous mettiez à niveau votre Panorama. • **Notification** : Palo Alto Networks vous informera de toute exigence de Panorama 21 jours avant une mise à niveau de version majeure programmée telle que définie dans Prisma Access Types de version.		
Version du plug-in Cloud Services	Disponible après la sortie du plug-in.	Non	Vous effectuez les tâches pour mettre à niveau le plug-in. Consultez Prisma Access Types de version pour obtenir plus de détails sur quand Prisma Access met à jour sa version de plug-in. Consultez Mettre à niveau le plug-in Cloud Services pour mettre à niveau le plug-in dans l'appareil Panorama.
Application GlobalProtect	• **Versions majeures de l'application GlobalProtect (par exemple, *x*.0 ou 5.*x*) :** Prisma Access met à jour l'agent sur	Oui	Le cloud contrôle les versions de l'application disponibles pour la mise à niveau. Cependant, vous pouvez choisir

©2025 Palo Alto Networks, Inc.

Composant	Calendrier de mise à jour	Cloud Controlled? (Contrôlé par le cloud ?) (Yes/No) (Oui/Non)	Commentaires
	le portail avec la dernière version majeure 7 à 10 jours après la disponibilité générale de la version *x*.0.1 de cette version. Par exemple, avec une version d'agent 5.1, Prisma Access met à jour l'agent sur le portail 7 à 10 jours après la sortie de la version 5.1.1. • **Versions mineures de l'application GlobalProtect (par exemple, 5.1.*x*) :** Prisma Access met à jour l'agent sur le portail avec la dernière maintenance de l'infrastructure 7 à 10 jours après la disponibilité générale de cette version.		entre différentes versions hébergées de l'application, et contrôler comment et quand déployer les mises à jour de l'application GlobalProtect auprès des utilisateurs finaux. Pour plus d'informations, reportez-vous à la sectionMises à niveau de l'application GlobalProtect. Si votre déploiement Prisma Access nécessite un correctif d'urgence de l'application GlobalProtect, ouvrez une demande d'assistance auprès du support technique de Palo Alto Networks pour obtenir de l'aide.
Mises à jour des applications et des menaces	Tous les jours avec un seuil de 24 heures. Palo Alto Networks publie de nouveaux App-ID le troisième mardi de chaque mois. Prévoyez de revoir et d'intégrer ces nouveaux App-ID dans les 24 heures. La nouvelle caractéristique App-	Oui	

 ©2025 Palo Alto Networks, Inc.

Composant	Calendrier de mise à jour	Cloud Controlled? (Contrôlé par le cloud ?) (Yes/No) (Oui/Non)	Commentaires
	ID vous permet de voir les nouvelles applications sur votre réseau et vous fournit des informations détaillées sur l'activité des applications nouvellement catégorisées. Ce que vous apprenez peut vous aider à prendre les bonnes décisions concernant la mise à jour de votre politique de sécurité afin de faire appliquer les ID d'application les plus récents.		
Protection antivirus	Toutes les heures, 10 minutes après l'heure	Oui	Prisma Access est toujours à jour avec la dernière version d'antivirus.
WildFire	Temps réel	Oui	Prisma Access récupère les signatures WildFire pour les logiciels malveillants nouvellement découverts dès que le cloud public WildFire peut les générer.
Fichier de données GlobalProtect	Toutes les heures	Oui	Prisma Access est toujours à jour avec la dernière version du fichier de données GlobalProtect.

©2025 Palo Alto Networks, Inc.

Composant	Calendrier de mise à jour	Cloud Controlled? (Contrôlé par le cloud ?) (Yes/No) (Oui/Non)	Commentaires
Signatures d'application VPN sans client	Toutes les heures	Oui	Prisma Access est toujours à jour avec la dernière version de signature d'application VPN sans client.

©2025 Palo Alto Networks, Inc.

Mises à niveau du plan de données de Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Prisma Access (Managed by Strata Cloud Manager) effectue automatiquement les mises à niveau du plan de données, sans qu'aucune intervention ne soit requise de votre part.

Prisma Access effectue des mises à niveau du plan de données pour fournir de nouvelles fonctionnalités et capacités de sécurité pour aider à protéger les utilisateurs finaux, les actifs et la transformation numérique de votre organisation. Lorsqu'une nouvelle version de Prisma Access nécessite une mise à niveau du plan de données, vous devez comprendre le fonctionnement du processus de mise à niveau et disposer des prérequis avant la mise à niveau.

Vous pouvez vous attendre à ce que votre plan de données soit mis à niveau une à deux fois par an. Certaines versions peuvent proposer une mise à niveau facultative du plan de données en plus des mises à niveau du plan de données requises pour la prise en charge des fonctionnalités Prisma Access qui l'exigent.

- Vue d'ensemble de la mise à niveau du plan de données
- Exemple de mise à niveau du plan de données

Vue d'ensemble de la mise à niveau du plan de données

Prisma Access met à niveau votre plan de données en deux phases à deux dates de week-end et vous tient informé de la mise à niveau à l'aide de Strata Cloud Manager. D'une manière générale, les étapes suivantes sont suivies au cours du processus de mise à niveau.

- Une notification par e-mail de Strata Cloud Manager arrive 21 jours avant la date de début planifiée de la mise à niveau du plan de données. Cette notification par e-mail fournit la date de début de la mise à niveau du plan de données pour la phase 1.

  Il se peut qu'une date soit renseignée dans Strata Cloud Manager avant la notification de 21 jours, mais cette date peut ne pas être définitive tant que vous n'avez pas reçu votre notification de 21 jours.

- Dans l'e-mail, vous êtes invité à sélectionner et à soumettre le ou les emplacements à mettre à niveau en premier et la fenêtre temporelle pour la mise à niveau via Strata Cloud Manager.

  Vous pouvez modifier et soumettre les premiers emplacements à mettre à niveau et la fenêtre temporelle plusieurs fois pour un locataire donné. La dernière soumission qui a eu lieu sept jours avant la date de début planifiée sera choisie par le service pour la mise à niveau. Vous ne

©2025 Palo Alto Networks, Inc.

pourrez pas apporter de modifications dans les sept jours suivant la date de début de la mise à niveau.

Si vous apportez des modifications, l'affichage des modifications que vous avez apportées dans le tableau de bord de mise à niveau sur Insights peut prendre jusqu'à 30 minutes. Vous serez averti par e-mail lorsque Prisma Access a traité et terminé les modifications.

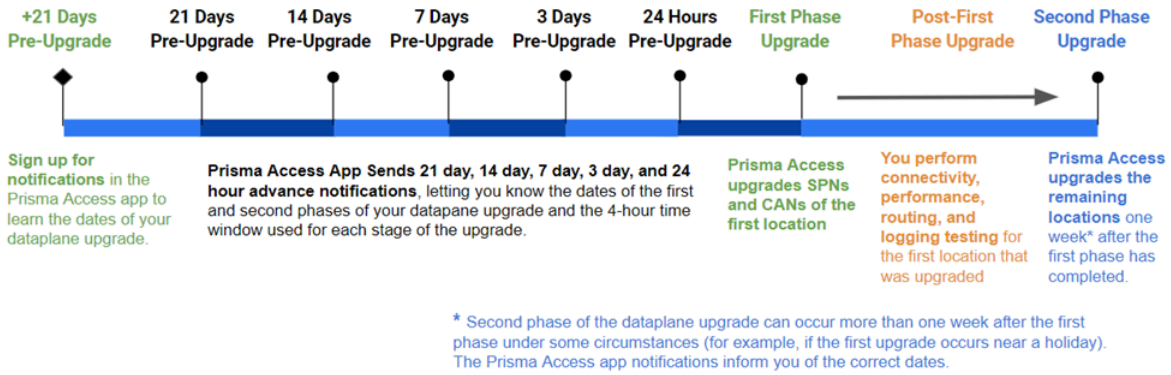
Palo Alto Networks vous suggère vivement de sélectionner des emplacements qui reflètent l'ensemble de votre déploiement. Par exemple, si vous disposez d'un utilisateur mobile, d'une connexion aux services et d'un déploiement réseau distant, sélectionnez un ou plusieurs emplacements qui ont tous les types de déploiement.

- Prisma Access effectuera la phase 1 de la mise à niveau sur le ou les emplacements sélectionnés dans la fenêtre temporelle locale sélectionnée pour ces emplacements.
- Si les emplacements de mise à niveau sélectionnés ont une combinaison d'utilisateurs mobiles (GlobalProtect, utilisateurs mobiles), de proxy explicites, de connexions aux services ou de réseaux distants, le plan de données de chaque déploiement sera mis à niveau vers la version de plan de données requise, comme décrit plus loin dans cette section.
- Une fois la mise à niveau terminée dans le premier emplacement, vous recevrez une notification par e-mail via Strata Cloud Manager. Palo Alto Networks vous recommande de surveiller le service pour détecter tout nouveau problème survenant immédiatement après la mise à niveau du plan de données.
- Dans le cas improbable où vous observeriez un nouveau problème, signalez le problème au support technique de Palo Alto Networks.

  L'équipe de support technique enquêtera sur le problème et prendra des mesures correctives qui peuvent également inclure le retour à la version précédente du plan de données. Cette décision vous sera communiquée via le dossier de support technique.
- S'il n'y a pas de nouveaux problèmes ou si un nouveau problème n'est pas lié à la mise à niveau, Prisma Access procédera à la mise à niveau du plan de données le week-end suivant.
- L'amélioration des emplacements restants aura lieu pendant la même fenêtre temporelle que celle que vous avez sélectionnée pour la première mise à niveau (en heure locale).
- Une fois la mise à niveau du plan de données terminée, vous en serez informé via une alerte par e-mail.
- Si une mise à niveau du plug-in est nécessaire après la mise à niveau du plan de données, Palo Alto Networks vous recommande de mettre à niveau le plug-in une fois la mise à niveau du plan de données terminée.

La figure suivante montre la chronologie utilisée pour la mise à niveau et inclut les tâches que vous devrez effectuer pour la mise à niveau du plan de données (indiquées en vert), ainsi que les étapes que Prisma Access effectue.

 ©2025 Palo Alto Networks, Inc.



La section suivante fournit plus de détails sur le processus de mise à niveau du plan de données.

Une fois que vous vous êtes inscrit pour recevoir des notifications, Prisma Access vous informe des deux dates de week-end qui seront utilisées pour le processus de mise à niveau et envoie ces notifications 21 jours, 14 jours, 7 jours, 3 jours et 24 heures avant que la première phase de la mise à niveau n'ait lieu. Le processus de mise à niveau se déroule en deux phases :

- La phase 1 met à niveau l'emplacement ou les emplacements que vous avez choisis le premier week-end en utilisant la fenêtre temporelle que vous avez fournie et vous informe par e-mail lorsque la mise à niveau est terminée. Si vous n'avez pas choisi les emplacements à mettre à niveau en premier, ou si vous n'avez pas sélectionné de fenêtre temporelle, Prisma Access fait les choix pour vous.

  Palo Alto Networks tente de mettre à niveau les emplacements pendant la fenêtre de quatre heures que vous sélectionnez via Strata Cloud Manager. Palo Alto Networks s'efforcera au mieux d'effectuer les mises à niveau requises pendant cette fenêtre, mais ne peut garantir que les emplacements seront mis à niveau pendant cette période. En cas de problème lors de la mise à niveau, Palo Alto Networks tentera la mise à niveau 24 heures après la fenêtre initiale de quatre heures.

  Pour cette raison, vous devez planifier une fenêtre de requête de modification de 72 heures commençant à 20 heures, heure locale, le vendredi et se terminant à 20 heures, heure locale, le lundi pour chacun des deux week-ends où la mise à niveau du plan de données a lieu. Vous recevrez un e-mail lorsque la mise à niveau sera terminée.

  Prisma Access apporte les modifications suivantes à votre déploiement au cours de la phase 1 de la mise à niveau.

Type de déploiement	Qu'est-ce qui est mis à niveau
Utilisateurs mobiles : déploiements GlobalProtect	Prisma Access met à niveau : • la passerelle GlobalProtect, également connue sous le nom de *Nœud de traitement de sécurité des utilisateurs mobiles (MU-SPN)*, pour le ou les emplacements que vous spécifiez ;

 ©2025 Palo Alto Networks, Inc.

Type de déploiement	Qu'est-ce qui est mis à niveau
	• le portail GlobalProtect associé à cette région.
Utilisateurs mobiles : déploiements de proxy explicites	Prisma Access met à niveau les nœuds de proxy explicite pour l'emplacement ou les emplacements de proxy explicite que vous spécifiez.
Déploiements de réseaux distants	Prisma Access met à niveau le réseau distant de sauvegarde (HA), également appelé *Nœud de traitement de sécurité de réseau distant (RN-SPN)*, fait ensuite du réseau distant de secours le nœud actif pour le ou les emplacements que vous spécifiez. La connexion au réseau distant de secours n'est mise à niveau que le week-end suivant, lorsque les nœuds actifs et de secours sont mis à niveau pour tous les emplacements. S'il existe plusieurs RN-SPN à l'emplacement sélectionné, tous les nœuds principaux sont mis à niveau vers la nouvelle version du plan de données.
Connexions aux services	Prisma Access met à niveau la connexion au service de secours (HA), également appelée nœud d'accès d'entreprise de connexion aux services (SC-CAN), puis fait de la connexion au service de secours le nœud actif pour le ou les emplacements que vous spécifiez. La connexion au service de secours n'est mise à niveau que le week-end suivant, lorsque les nœuds actifs et de secours sont mis à niveau pour tous les emplacements. S'il y a plusieurs SC-CAN à l'emplacement sélectionné, tous les nœuds de secours sont mis à niveau vers la nouvelle version du plan de données.
Connecteurs ZTNA	Les connecteurs ZTNA ne sont pas mis à niveau ; vous pouvez mettre à niveau les connecteurs ZTNA en fonction des besoins.

Entre la première et la deuxième mise à niveau, surveillez les premiers emplacements mis à niveau et effectuez des tests de connectivité, de performances, de routage et de journalisation pour vous assurer que les emplacements ont été mis à niveau avec succès. Si vous rencontrez une défaillance affectant le service après la mise à niveau, ouvrez une demande d'assistance

 ©2025 Palo Alto Networks, Inc.

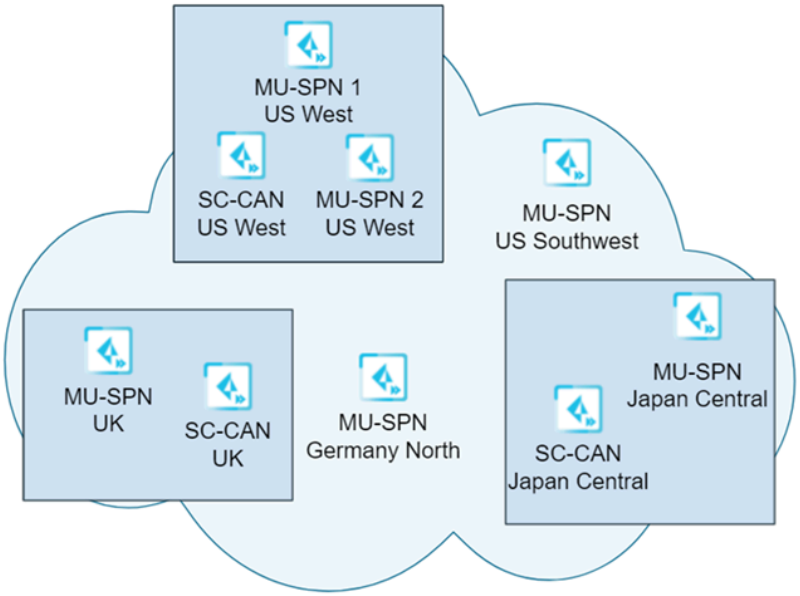
auprès du support technique de Palo Alto Networks pour obtenir de l'aide. Palo Alto Networks tentera de résoudre le problème en restaurant le plan de données à une version précédente du plan de données dans les 24 heures.

- Sept jours après la mise à niveau du premier emplacement par Prisma Access, Prisma Access met à niveau le reste de vos emplacements (mise à niveau de la phase 2), en utilisant la même fenêtre temporelle que celle que vous avez sélectionnée pour la première phase, et vous informe par e-mail lorsque la mise à niveau est terminée.

La fenêtre de mise à niveau peut être plus longue. Par exemple, si la phase 2 se produit pendant un jour férié aux États-Unis d'Amérique, la deuxième phase de la mise à niveau se produit 14 jours après la première phase au lieu de 7. Les notifications que vous recevez dans Strata Cloud Manager vous montrent la chronologie spécifique de la prochaine mise à niveau du plan de données.

Exemple de mise à niveau du plan de données

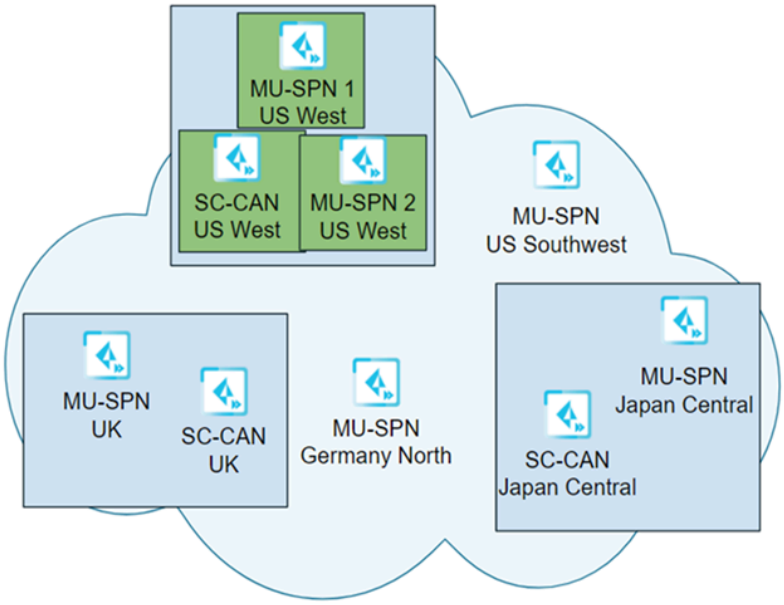
L'exemple suivant illustre un exemple de procédure de mise à niveau du plan de données pour un déploiement d'utilisateurs mobiles avec cinq passerelles (MU-SPN) et trois SC-CAN. L'emplacement USA Ouest comporte deux MU-SPN à la suite d'un événement de mise à l'échelle automatique (un MU-SPN supplémentaire a été ajouté après qu'un grand nombre d'utilisateurs mobiles se sont connectés à cet emplacement).



Dans cet exemple, vous avez sélectionné un seul emplacement (USA Ouest) à mettre à niveau en premier et demandé une fenêtre de mise à niveau de quatre heures de 8 h à 12 h le samedi pour la mise à niveau.

Le premier week-end de mise à niveau (phase 1), la mise à niveau a lieu pour les SC-CAN et les MU-SPN à l'emplacement USA Ouest entre 8 h et 12 h. heure du Pacifique, le samedi.

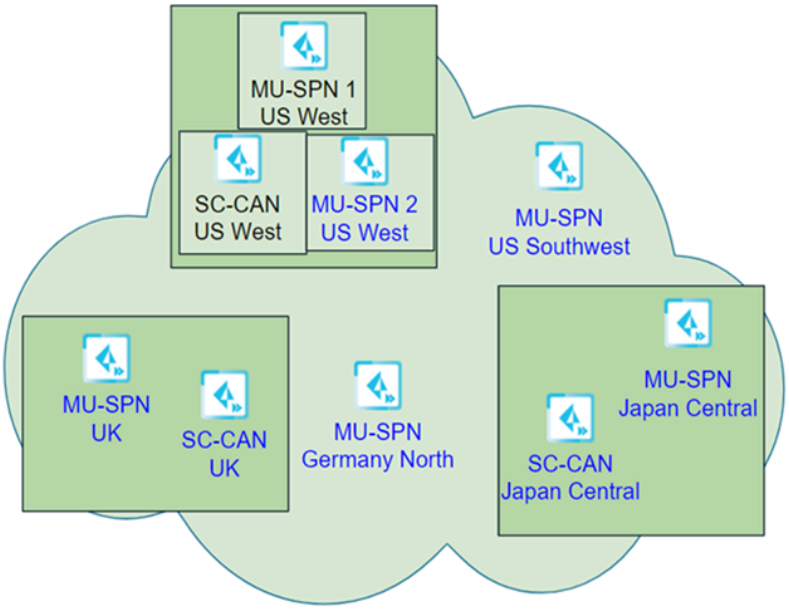
 ©2025 Palo Alto Networks, Inc.



Sept jours après la mise à niveau du premier emplacement, Palo Alto Networks met à niveau les composants restants (phase 2) en utilisant la même fenêtre temporelle de quatre heures que celle utilisée pour la première phase de la mise à niveau (de 8 h à 12 h le samedi).

Dans cet exemple, Prisma Access utilise les informations de fuseau horaire suivantes lors de la mise à niveau du plan de données :

- Les MU-SPN et SC-CAN du Centre du Japon sont mises à niveau en utilisant l'heure locale au Japon.
- Les UK MU-SPN et SC-CAN sont mis à niveau en utilisant l'heure locale au Royaume-Uni.
- Le MU-SPN du Sud-Ouest des États-Unis est mis à niveau en utilisant l'heure du Pacifique.



 ©2025 Palo Alto Networks, Inc.

Recevoir des alertes de mise à niveau et des mises à jour

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Pour rester informé du calendrier de mise à niveau de votre plan de données et pour sélectionner vos préférences de mise à niveau, vous devez utiliser Strata Cloud Manager pour vous abonner aux notifications Prisma Access. Strata Cloud Manager utilise des alertes par e-mail pour vous informer des deux dates de week-end où votre mise à niveau a lieu ; vous sélectionnez le ou les emplacements que vous souhaitez mettre à niveau en premier et la fenêtre temporelle de quatre heures à utiliser pour la mise à niveau.

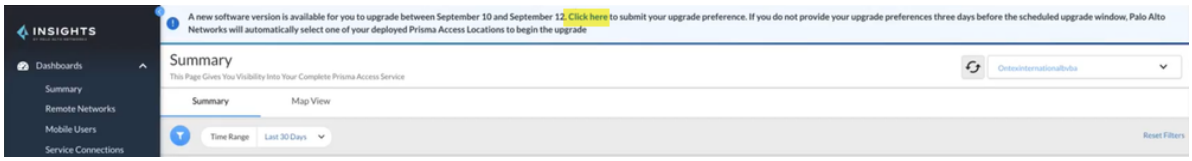
Une fois la mise à niveau démarrée, vous pouvez également surveiller l'état de la mise à niveau à l'aide de Strata Cloud Manager comme illustré dans les étapes suivantes.

STEP 1 | Inscrivez-vous pour recevoir des notifications d'alerte de Strata Cloud Manager.

STEP 2 | Vérifiez vos notifications pour être informé des mises à niveau à venir du plan de données ; ensuite, sélectionnez vos préférences de mise à niveau à l'aide de l'une des méthodes suivantes.

- Sélectionnez **Workflow (Flux de travail)** > **Software Upgrades (Mises à niveau logicielles)** > **Prisma Access** > **Upgrade Preferences (Préférences de mise à niveau)**.

  Le tableau de bord de mise à niveau s'affiche.

- Connectez-vous à Strata Cloud Manager, affichez la bannière en haut de la page pour votre mise à niveau planifiée, puis sélectionnez **Click here (Cliquer ici)**.
- Vérifiez si vous recevez des notifications dans vos e-mails pour votre mise à niveau planifiée et cliquez sur le lien hypertexte dans l'e-mail.
- Sélectionnez **Workflow (Flux de travail)** > **Software Upgrades (Mises à niveau logicielles)** > **Prisma Access** > **Upgrade Preferences (Préférences de mise à niveau)**.

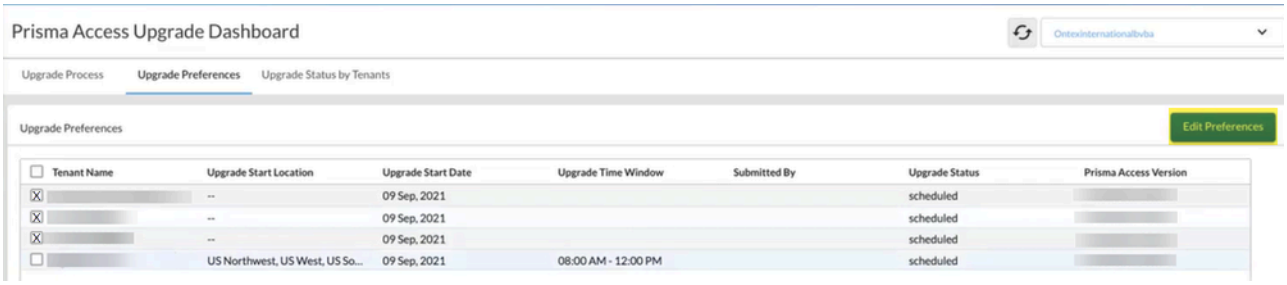
STEP 3 | (Facultatif) Lisez le **Upgrade Process (Processus de mise à niveau)** pour en savoir plus sur le fonctionnement du processus de mise à niveau.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Choisissez vos **Upgrade Preferences (Préférences de mise à niveau)**.

Si vous avez un déploiement multilocataire, tous les locataires s'affichent dans cette zone. Si vous avez déjà sélectionné vos préférences de mise à niveau pour votre déploiement, ces sélections s'affichent ici.

1. Sélectionnez les locataires pour lesquels vous souhaitez définir les préférences de mise à niveau, puis sélectionnez **Edit Preferences (Modifier les préférences)**.



2. Sélectionnez l'icône **Preferred Prisma Access Locations (Emplacements Prisma Access préférés)** que vous souhaitez mettre à niveau en premier.

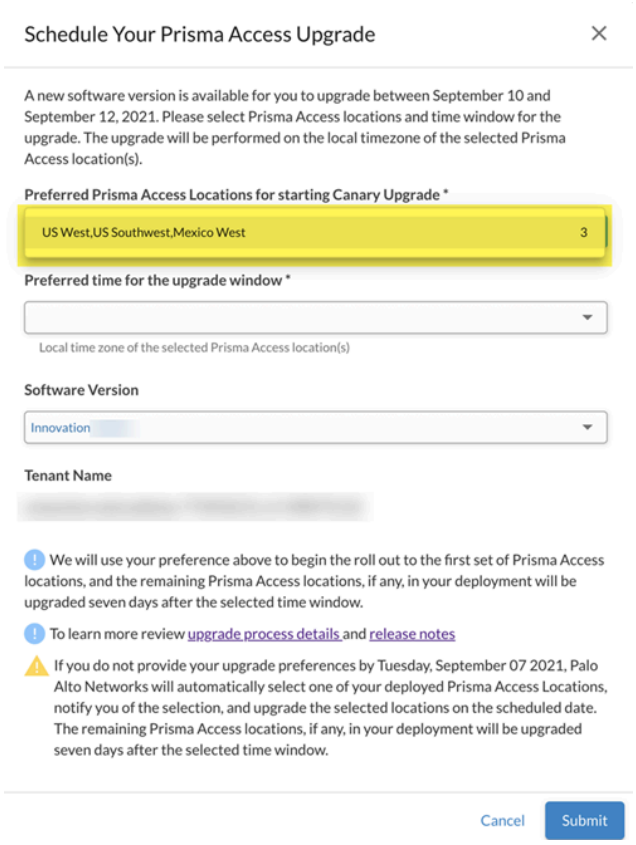
   Palo Alto Networks vous suggère vivement de sélectionner des emplacements qui reflètent l'ensemble de votre déploiement. Par exemple, si vous disposez d'un utilisateur mobile, d'une connexion aux services et d'un déploiement réseau distant, sélectionnez un ou plusieurs emplacements qui ont tous les types de déploiement.

   Sélectionnez l'un des choix dans la liste déroulante.

   - Prisma Access affiche uniquement les emplacements où vous avez déployé des utilisateurs mobiles, des réseaux distants, des connexions aux services ou toute combinaison de ceux-ci.
   - Les groupes de la liste déroulante appartiennent au même emplacement de calcul.

   Prisma Access vous informera par e-mail lorsque les emplacements ont été mis à niveau.

©2025 Palo Alto Networks, Inc.



Après la mise à niveau réussie du premier ensemble d'emplacements Prisma Access, l'équipe Prisma Access surveille ces emplacements pendant sept jours, puis met à niveau tous les autres emplacements Prisma Access. La sélection d'un seul emplacement ou d'un petit nombre d'emplacements vous permet de surveiller ces emplacements avant que le reste de vos emplacements ne soit mis à niveau une semaine plus tard.

Si aucun emplacement ne s'affiche dans la liste déroulante, cela signifie que vous avez sélectionné plusieurs locataires qui n'ont pas d'emplacements communs déployés ou

 ©2025 Palo Alto Networks, Inc.

que vous n'avez pas encore intégré d'emplacements pour les locataires que vous avez sélectionnés.

3. Sélectionnez l'icône **Preferred time for the upgrade window (Heure préférée pour la fenêtre de mise à niveau)** dans la liste des options disponibles.

   Choisissez parmi les fenêtres temporelles de mise à niveau suivantes. Les fenêtres temporelles sont locales à l'emplacement ou aux emplacements en cours de mise à niveau et sont toutes des fenêtres de quatre heures :

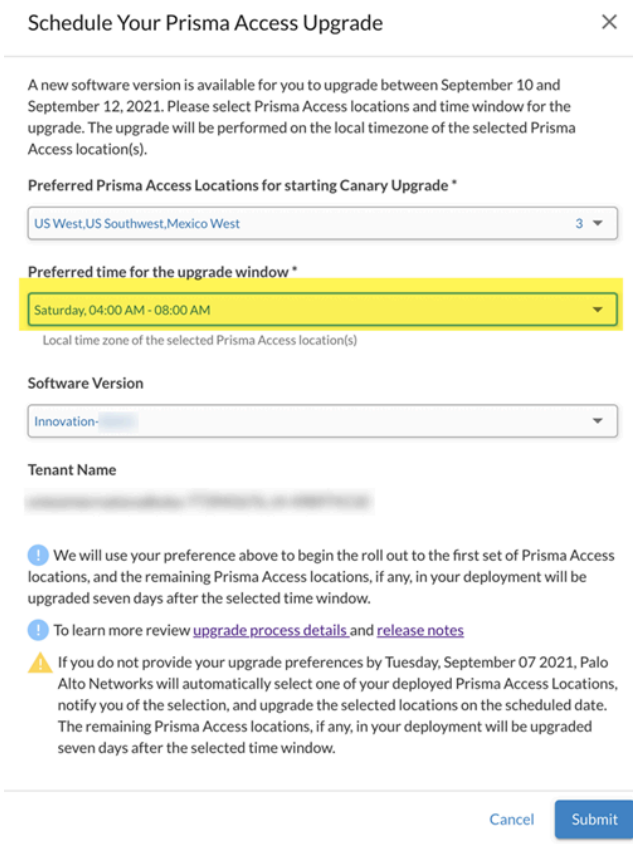
   - Vendredi 20 h à 12 h (minuit)
   - Samedi 0 h (minuit) à 4 h
   - Samedi 4 h à 8 h
   - Samedi 8 h à 12 h (midi)
   - Samedi 12 h (midi) à 16 h
   - Samedi 16 h à 20 h

   Palo Alto Networks utilise votre préférence pour commencer le déploiement à l'emplacement ou aux emplacements Prisma Access que vous avez sélectionnés. La dernière soumission qui a eu lieu sept jours avant la date de début planifiée sera choisie par le service pour la mise à niveau. Si vous apportez des modifications, l'affichage des modifications que vous avez apportées dans le tableau de bord de mise à niveau sur

 ©2025 Palo Alto Networks, Inc.

Insights peut prendre jusqu'à 30 minutes. Vous serez averti par e-mail lorsque Prisma Access a traité et terminé les modifications.

Si vous ne fournissez pas vos préférences de mise à niveau sept jours avant la fenêtre de mise à niveau planifiée, Palo Alto Networks sélectionnera automatiquement le premier ensemble de vos emplacements Prisma Access déployés, vous informera de la sélection et mettra à niveau les emplacements sélectionnés à la date planifiée. Les emplacements restants Prisma Access, le cas échéant, de votre déploiement seront mis à niveau sept jours après la fenêtre temporelle sélectionnée.



4. Sélectionnez l'icône **Software Version (Version du logiciel)** vers laquelle vous souhaitez effectuer la mise à niveau, si plusieurs versions sont disponibles.
5. **Submit (Soumettez)** vos modifications.

STEP 5 | Une fois votre déploiement commencé, sélectionnez **Workflows (Flux de travail)** > **Software Upgrades (Mises à niveau logicielles)** > > **Prisma Access** > **Upgrade Status by Tenants (État**

 ©2025 Palo Alto Networks, Inc.

de la mise à niveau par les locataires) et consultez le **Upgrade Status by Location (État de la mise à niveau par emplacement)**.

Cette page affiche les informations suivantes pour chaque emplacement en cours de mise à niveau :

- Nom du locataire en cours de mise à niveau.
- Dates de début et de fin du processus de mise à niveau.
- Version du plan de données vers laquelle le locataire est mis à niveau.
- Fenêtre temporelle préférée pour la mise à niveau.
- Emplacements initiaux qui sont mis à niveau.
- Date à laquelle les emplacements restants seront mis à niveau.

En outre, un tableau affiche les emplacements en cours de mise à niveau, la date de début et la fenêtre temporelle de la mise à niveau, ainsi que le fuseau horaire utilisé pour la mise à niveau. La colonne **Upgrade Status (État de la mise à niveau)** vous fournit les informations suivantes :

État de mise à niveau	Description
Planifié	La mise à niveau du plan de données a été planifiée.
Commencé	La mise à niveau a commencé.
En cours	La mise à niveau du plan de données est en cours.
Réessayer	La mise à niveau du plan de données n'a pas abouti, mais Prisma Access continue d'être opérationnel avec l'ancienne version du plan de données. Prisma Access réessaiera la mise à niveau avant l'expiration de la fenêtre de maintenance du week-end.
Réussite	La mise à niveau s'est terminée avec succès.

STEP 6 | Une fois que le premier ensemble d'emplacements a terminé la mise à niveau du plan de données, surveillez les emplacements mis à niveau et effectuez des tests de connectivité, de performances, de routage et de journalisation pour vous assurer que les mises à niveau ont réussi.

STEP 7 | Lorsque la mise à niveau du deuxième ensemble d'emplacements est planifiée, surveillez ces emplacements et vérifiez leur état en sélectionnant **Workflows (Flux de travail)** > **Software Upgrades (Mises à niveau logicielles)** > **Prisma Access** > **Upgrade Status by Tenants (État de la mise à niveau par les locataires)**.

Prisma Access vous envoie une notification par e-mail une fois la mise à niveau du plan de données terminée.

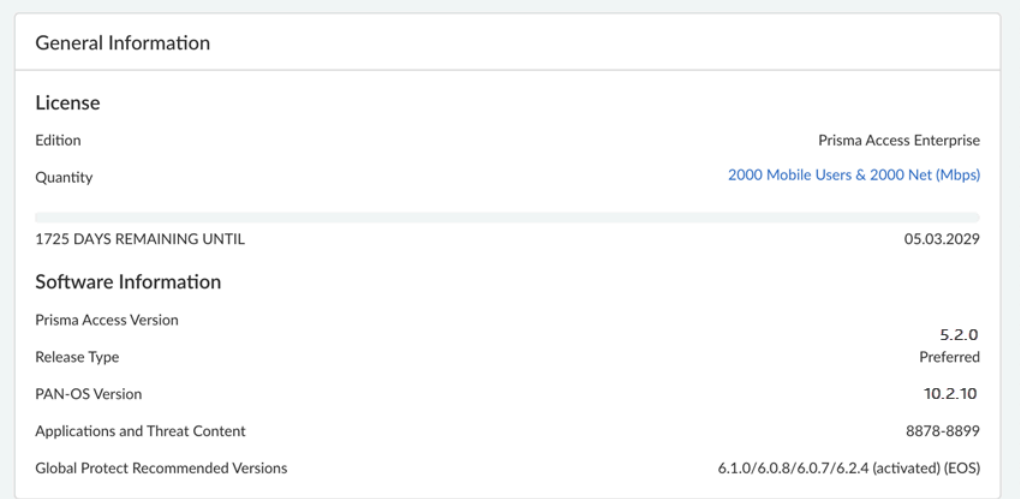
 ©2025 Palo Alto Networks, Inc.

Afficher les versions logicielles de Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Prisma Access (Managed by Strata Cloud Manager)

Vous trouverez des informations sur la version du logiciel et du contenu dans **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Vue d'ensemble)** > **General Information (Informations générales)**. Sélectionnez la portée de la configuration **Prisma Access**.



La page General Information (Informations générales) vous fournit les informations suivantes :

nominale	Description
ID de locataire	Vous permet de partager des coordonnées (nom de l'entreprise, nom du contact, adresse e-mail et numéro de téléphone) afin que vous puissiez être contacté au sujet des mises à niveau du service Palo Alto Networks. ID du locataire.
Nom du locataire	Nom du locataire.
Région	Région du locataire.
Version de Prisma Access	Version actuelle de Prisma Access.

©2025 Palo Alto Networks, Inc.

nominale	Description
Version de PAN-OS	Version de PAN-OS que votre plan de données exécute. Le plan de données est la composante de l'infrastructure Prisma Access qui permet l'inspection du trafic et l'application des politiques sur votre réseau et le trafic utilisateur.
Type de version	Type de version que vous exécutez (Preferred (Préférée) ou Innovation). Une version Innovation nécessite un plan de données PAN-OS supérieur à celui d'une version Preferred (Préférée).
Applications et contenu des menaces	Version des mises à jour des applications et du contenu des menaces que vous exécutez.

Prisma Access (Managed by Panorama)

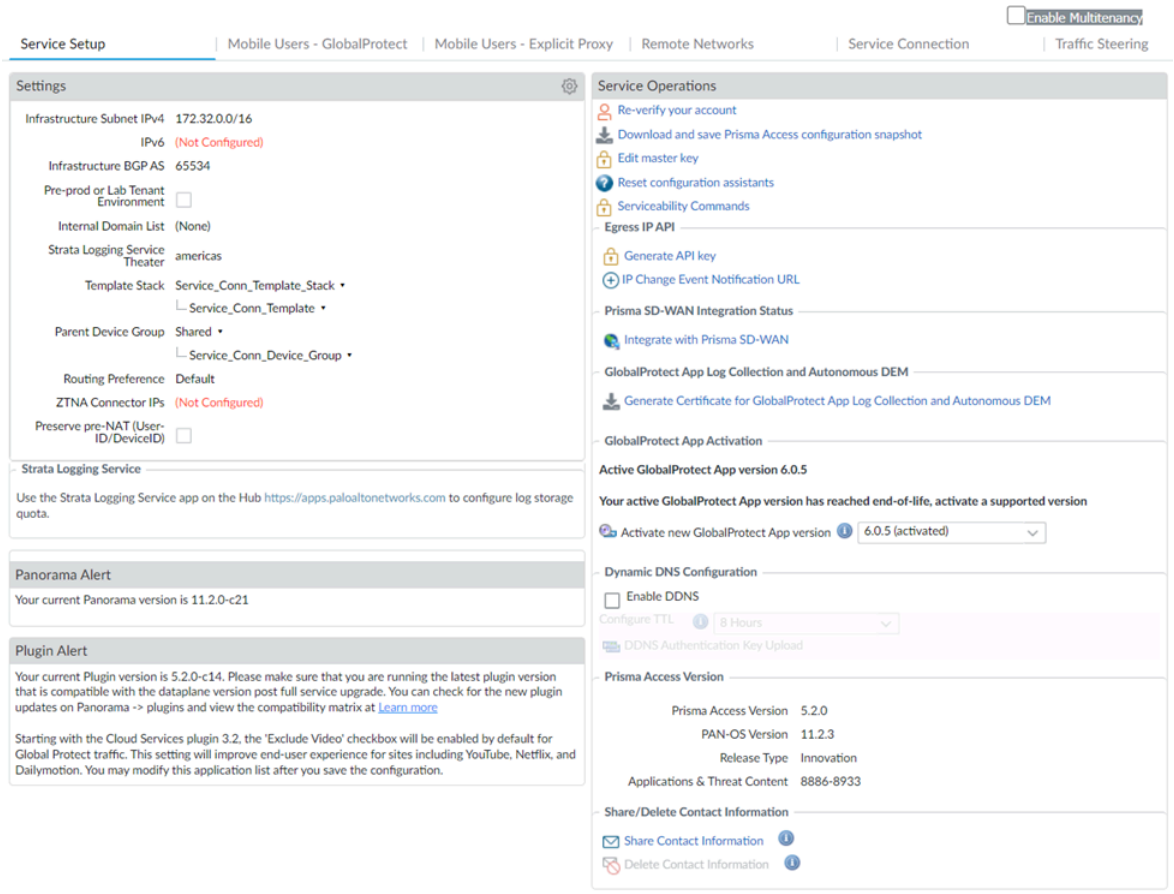
Prisma Access se compose de composants que vous gérez tels que Panorama et le plug-in Cloud Services, des composants que Prisma Access gère, tels que la version du plan de données et des composants que Prisma Access gère, mais dont vous pouvez contrôler la version (la version GlobalProtect hébergée sur le portail Prisma Access). La page Configuration du service (**Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** vous montre l'état de ces composants sur une seule page. Cette page contient également des notifications qui vous indiquent quand la version actuelle de Panorama et les versions du plug-in seront en fin de prise en charge (EoS) pour une utilisation avec Prisma Access. Palo Alto Networks vous informe à l'avance des dates de fin de prise en charge afin de donner à votre organisation suffisamment de temps pour planifier la mise à niveau.



Toutes les dates sont exprimées en temps universel coordonné (UTC).

La page Service Setup (Configuration du service) vous fournit les informations suivantes :

©2025 Palo Alto Networks, Inc.



nominale	Description
Alerte Panorama	Affiche la version actuelle de Panorama que vous utilisez. La zone **Upgrade requirements (Exigences de mise à niveau)** vous fournit des informations sur les versions de Panorama, y compris les dates auxquelles les versions Panorama actuellement compatibles atteignent leur date de fin de prise en charge (EoS) pour la gestion de Prisma Access. Utilisez ces informations pour planifier votre mise à niveau de Panorama avant sa date de fin de prise en charge.
Alerte de plug-in	Affiche le plug-in Cloud Services actuel installé sur le Panorama qui gère Prisma Access. La zone **Upgrade requirements (Exigences de mise à niveau)** vous fournit les dates auxquelles la prochaine version du plug-in sera publiée, la date limite pour la mise à niveau vers le prochain plug-in et la date à laquelle vous ne pourrez pas apporter de modifications et de validations en utilisant

 ©2025 Palo Alto Networks, Inc.

nominale	Description
	la version antérieure du plug-in. Utilisez ces informations pour planifier la prochaine mise à niveau du plug-in Cloud Services.
État de l'intégration Prisma SD-WAN	Sélectionnez **Integrate with Prisma SD-WAN (Intégration avec Prisma SD-WAN)** pour activer le client léger CloudBlade qui permet la fonctionnalité entre Prisma SD-WAN et Prisma Access.
Collecte de journaux de l'application GlobalProtect et DEM autonome	Si vous avez activé la collecte des journaux d'application GlobalProtect pour le résolution des problèmes, ou activé la gestion de l'expérience numérique autonome (Autonomous Digital Experience Management, ADEM) pour vos utilisateurs mobiles, cliquez sur **Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM (Générer un certificat pour la collecte de journaux de l'application GlobalProtect et Autonomous DEM)** pour générer un certificat. Ce certificat permet à l'application GlobalProtect de s'authentifier auprès de Strata Logging Service (pour collecter les journaux) et d'Autonomous DEM. Lorsque vous générez le certificat, Prisma Access télécharge également le certificat sur **Device Certificates (Certificats de périphérique)** dans Panorama **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)** sous le modèle **Mobile_User_Template** dans le **Shared (Partagé)** à transmettre au périphérique mobile.
Activation de l'application GlobalProtect	Affiche la version en cours d'exécution (active) de l'application GlobalProtect que les utilisateurs mobiles peuvent télécharger à partir du portail Prisma Access et vous montre les versions de l'application GlobalProtect disponibles auxquelles vous pouvez vous mettre à niveau.
Configuration DNS du client	Indique si vous avez activé Dynamic DNS (DDNS) pour la résolution des problèmes du réseau distant.

 ©2025 Palo Alto Networks, Inc.

nominale	Description
Version de Prisma Access	Version actuelle de Prisma Access.
Version de PAN-OS	Version de PAN-OS que votre plan de données exécute. Le plan de données est la composante de l'infrastructure Prisma Access qui permet l'inspection du trafic et l'application des politiques sur votre réseau et le trafic utilisateur.
Type de version	Type de version que vous exécutez (Preferred (Préférée) ou Innovation). Une version Innovation nécessite un plan de données PAN-OS supérieur à celui d'une version Preferred (Préférée).
Applications et contenu des menaces	Version des mises à jour des applications et du contenu des menaces que vous exécutez.
Partager/Supprimer les coordonnées	Vous permet de partager des coordonnées (nom de l'entreprise, nom du contact, adresse e-mail et numéro de téléphone) afin que vous puissiez être contacté au sujet des mises à niveau du service Palo Alto Networks. Si vous avez déjà saisi vos coordonnées, vous pouvez supprimer les informations que vous avez saisies dans cette zone. N'utilisez pas les caractères spéciaux suivants dans la zone des informations de contact : • " (guillemets doubles) • ' (apostrophe) • < (signe inférieur à) • > (signe supérieur à) • & (esperluette)

©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Configuration Prisma Access

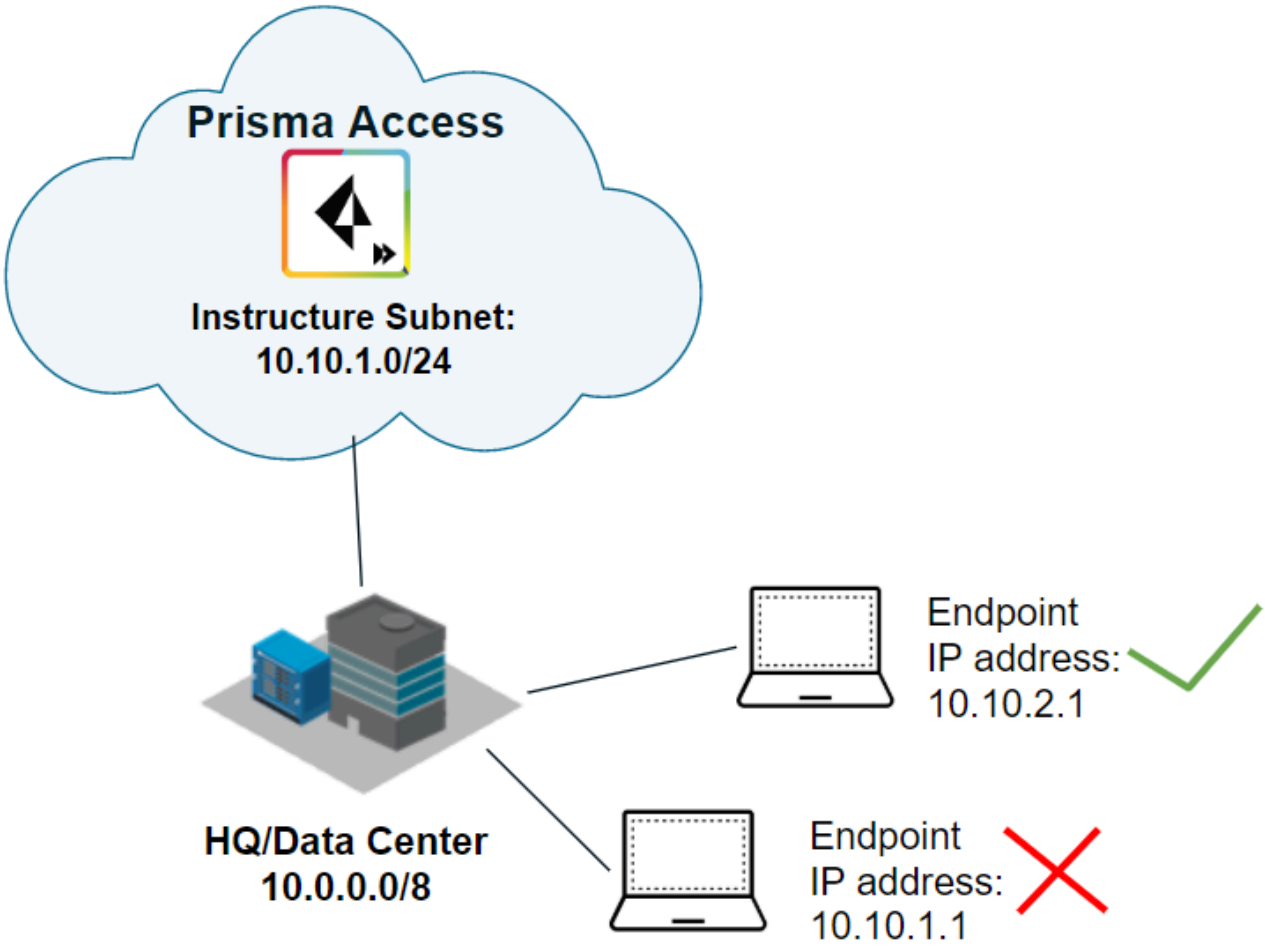
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Utilisez les recommandations et exigences suivantes lorsque vous ajoutez un sous-réseau d'infrastructure pour :

- Vous pouvez attribuer Prisma Access un sous-réseau d'infrastructure d'un super-réseau existant dans le pool d'adresses IP de votre organisation, mais n'attribuez aucune des adresses IP du sous-réseau d'infrastructure à une autre utilisation dans votre réseau existant.

  L'exemple suivant montre un Prisma Access sous-réseau d'infrastructure, 10.10.1.0/24, que vous avez attribué à partir d'un super-réseau existant, 10.0.0.0/8. Une fois que vous avez attribué 10.10.1.0/24 comme sous-réseau d'infrastructure, votre organisation ne peut utiliser aucune adresse IP de ce sous-réseau. Par exemple, vous pouvez attribuer 10.10.2.1 à un point

de terminaison, mais 10.10.1.1 n'est pas autorisé car cette adresse IP fait partie du sous-réseau d'infrastructure.



- Si vous créez un nouveau sous-réseau pour le sous-réseau d'infrastructure, utilisez un sous-réseau qui ne chevauche pas d'autres adresses IP que vous utilisez en interne.
- (Recommandé) Utilisez un sous-réseau conforme au RFC 1918. Bien que l'utilisation d'adresses IP (publiques) non conformes à la norme RFC 1918 soit possible, nous ne la recommandons pas en raison des conflits possibles avec l'espace public d'adresses IP sur Internet.
- Ne spécifiez aucun sous-réseau qui chevauche les adresses IP et sous-réseaux suivants, car Prisma Access réserve ces adresses IP et sous-réseaux à son usage interne :
  - 169.254.0.0/16
  - 100.64.0.0/10
- Le sous-réseau ne peut pas chevaucher les pools d'adresses IP que vous prévoyez d'utiliser pour les pools d'adresses que vous attribuez à votre déploiement d'utilisateurs mobiles.
- Étant donné que l'infrastructure de service peut être très grande, vous devez désigner au minimum un sous-réseau /24.

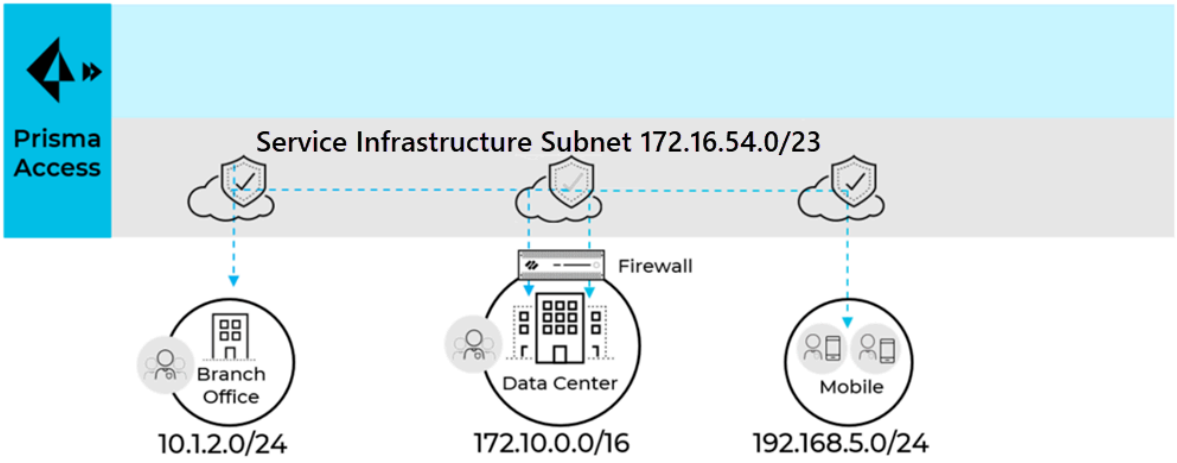
 ©2025 Palo Alto Networks, Inc.

Configurer Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Avant de pouvoir utiliser Prisma Access pour sécuriser vos réseaux distants et vos utilisateurs mobiles, configurez un sous-réseau d'infrastructure. Prisma Access utilise les adresses IP de ce sous-réseau pour établir un réseau entre vos emplacements de réseaux distants, vos utilisateurs mobiles, votre siège social et votre centre de données (le cas échéant). Prisma Access utilise également les connexions aux services pour accéder aux ressources internes à partir de votre siège social ou de votre centre de données.

Ce sous-réseau sera une extension de votre réseau existant. Par conséquent, il ne doit pas chevaucher les sous-réseaux IP existants dans votre réseau. L'exemple suivant montre un sous-réseau 172.16.54.0/23 utilisé pour le sous-réseau d'infrastructure Prisma Access.



Pour les petits réseaux avec moins de 50 sites et 2 500 utilisateurs mobiles, envisagez un sous-réseau /24. Pour les réseaux de taille moyenne avec moins de 100 sites et moins de 5 000 utilisateurs mobiles, envisagez un sous-réseau /23. Dans la plupart des cas, un sous-réseau /23 suffit. S'il y a plus de 100 sites ou 5 000 utilisateurs mobiles ou une croissance future prévue, contactez Palo Alto Networks pour évaluer si vous avez besoin d'une taille de sous-réseau plus grande.

Apprenez comment configurer Prisma Access.

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

Configurer Prisma Access (Strata Cloud Manager)

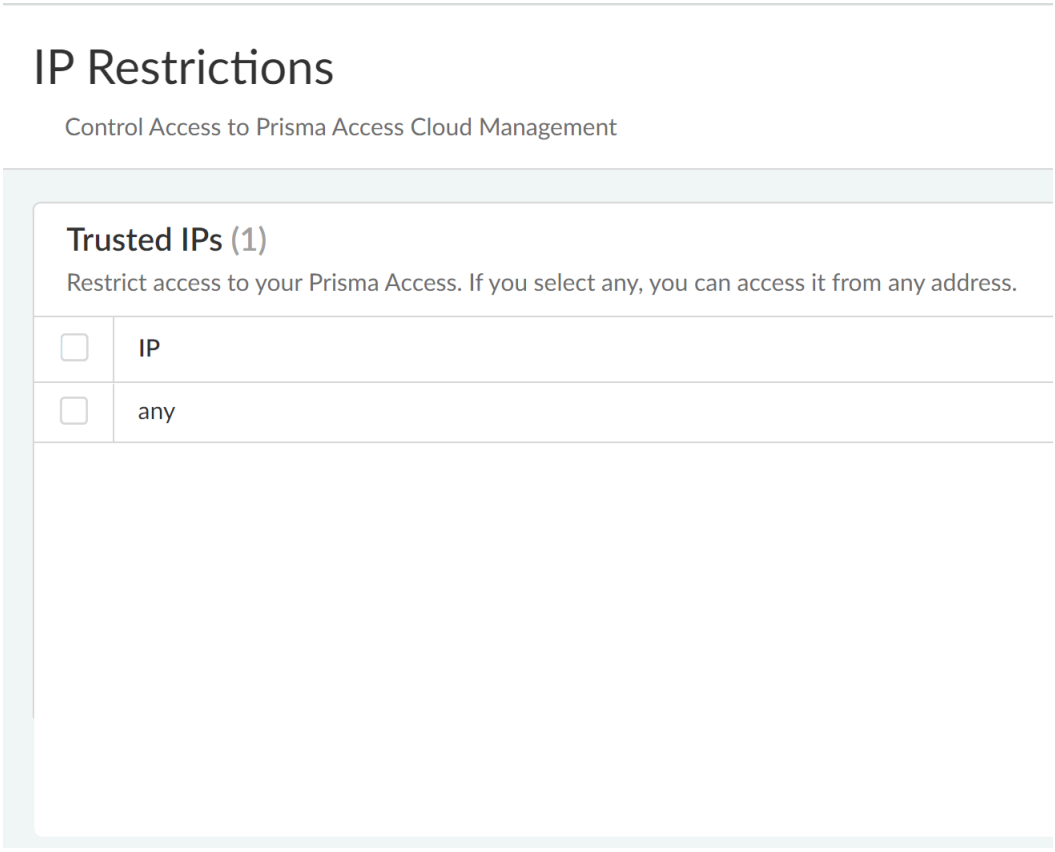
Le flux de travail suivant vous fournit les étapes récapitulatives que vous suivez pour installer et configurer Prisma Access.

STEP 1 | Lancez Strata Cloud Manager via le hub.

1. Lancez un navigateur Internet et **Sign In (Connexion)** au hub.
2. Lancez Strata Cloud Manager

STEP 2 | Spécifiez des adresses IP fiables pour les administrateurs Prisma Access (Managed by Strata Cloud Manager).

Seuls les administrateurs qui se connectent à partir de ces adresses IP sources (et qui s'authentifient avec succès) peuvent accéder à la Prisma Access (Managed by Strata Cloud Manager). Les adresses IP doivent être des adresses publiques. Par défaut, aucune adresse approuvée n'est appliquée (la liste est définie sur aucun). Pour commencer, recherchez le menu **Settings (Paramètres)** dans le panneau de navigation de gauche et cliquez sur **IP Restrictions (Restrictions IP)**.



STEP 3 | Identifiez vos besoins en matière de licence ; alors Activez et installez les composants Prisma Access.

STEP 4 | Activez l'infrastructure de services et les connexions aux services qui permettent la communication entre les éléments de Prisma Access.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Sécurisez les utilisateurs mobiles avec GlobalProtect ou Proxy explicite, selon les besoins de votre déploiement.

STEP 6 | Planifiez, créez et configurez des connexions réseau distantes.

STEP 7 | (Facultatif) Remplacez la méthode d'authentification locale par la méthode d'authentification de votre organisation.

STEP 8 | (Facultatif) Transférez les journaux de Strata Logging Service à un récepteur Syslog externe.

STEP 9 | (Facultatif) Vérifiez l'état de Prisma Access.

Vous pouvez récupérer l'état de tous les services cloud, y compris Prisma Access et Strata Logging Service et un enregistrement historique de la disponibilité du service en accédant à l'instance d'application à partir du hub.

Vous pouvez également vous inscrire pour recevoir des notifications par e-mail ou par SMS afin d'être informé lorsque des mises à jour de l'infrastructure sont prévues. lorsque des mises à jour ont lieu ; et lorsque Palo Alto Networks® crée, met à jour ou résout un incident. Pour vous inscrire aux mises à jour par courriel, rendez-vous dans la section Ressources de la page d'accueil du hub, puis sélectionnez **Service Status (État du service)**. Vous pouvez alors **Subscribe (S'inscrire)** aux mises à jour et incidents spécifiques pour vos services cloud.

Configurer Prisma Access (Panorama)

Le flux de travail suivant vous fournit les étapes récapitulatives que vous suivez pour installer et configurer Prisma Access (Managed by Panorama) Access.

Si vous configurez un déploiement qui inclut plusieurs instances de Prisma Access sur un seul Panorama (multilocataire), reportez-vous à . La plupart des organisations n'ont pas besoin de créer et de gérer plusieurs locataires.

STEP 1 | Ajoutez les URL et les ports suivants à une liste autorisée sur tout appareil de sécurité que vous utilisez avec l'appliance Panorama qui gère Prisma Access.

De plus, si votre appliance Panorama utilise un (**Panorama** > **Setup (Configuration)** > **Service** > **Proxy Server (Serveur proxy)**), ou si vous utilisez un proxy de transfert SSL avec Prisma

 ©2025 Palo Alto Networks, Inc.

Access, veillez à ajouter les URL et les ports suivants à une liste d'autorisation sur le proxy ou le serveur proxy.

- api.gpcloudservice.com (pour Prisma Access)
- api.paloaltonetworks.com (pour Prisma Access)
- apitrusted.paloaltonetworks.com (pour Prisma Access)
- Les FQDN et ports requis pour Strata Logging Service

> *S'il existe un pare-feu nouvelle génération Palo Alto Networks entre l'appliance Panorama et Internet, vous devez ajouter une règle de politique de sécurité sur le pare-feu pour autoriser les App-ID **paloalto-logging-service** et **paloalto-shared-services** de l'appliance Panorama vers Internet. Ces applications autorisent une communication sécurisée SSL vers Prisma Access et Strata Logging Service que l'appliance Panorama utilise pour interroger les journaux. Si l'appliance Panorama se trouve derrière un pare-feu Couche 4 hérité, autorisez les ports 443 et 444 sortants du Panorama pour autoriser ce trafic à partir du Panorama. Notez que l'ouverture de ports de couche 4 au lieu d'utiliser les App-ID Palo Alto Networks est moins sécurisée et non recommandée.*

STEP 2 | Ajoutez les ports utilisés par Panorama dans des listes d'autorisation de votre réseau.

STEP 3 | Identifiez vos exigences de licence ; puis Activez et installez les composants Prisma Access.

STEP 4 | Importez votre configuration Panorama existante dans Prisma Access ou créez de nouveaux modèles et groupes de périphériques pour commencer la configuration de Prisma Access.

Pour appliquer des configurations, telles que la politique de sécurité, la politique d'authentification, les profils de serveur, les profils de sécurité, les objets d'adresse et les groupes d'applications, sur Prisma Access, vous devez créer des modèles et des groupes de périphériques avec les paramètres de configuration que vous souhaitez appliquer sur Prisma Access ou exploiter vos groupes de périphériques et modèles existants en les ajoutant aux

 ©2025 Palo Alto Networks, Inc.

piles de modèles et aux hiérarchies de groupes de périphériques que Prisma Access crée lorsque vous intégrez le service.

Prisma Access crée les modèles et les groupes de périphériques suivants, en fonction de ce que vous avez acheté (par exemple, si vous n'achetez pas de licence de proxy explicite, vous ne verrez pas les modèles et les groupes de périphériques de proxy explicite) :

- Modèles :
  - **Explicit_Proxy_Template**
  - **Explicit_Proxy_Template_Stack**
  - **Mobile_User_Template**
  - **Mobile_User_Template_Stack**
  - **Remote_Network_Template**
  - **Remote_Network_Template_Stack**
  - **Service_Conn_Template**
  - **Service_Conn_Template_Stack**
- Groupes de périphériques :
  - **Explicit_Proxy_Device_Group**
  - **Mobile_User_Device_Group**
  - **Remote_Network_Device_Group**
  - **Service_Conn_Device_Group**

La configuration est simplifiée dans Prisma Access, car vous n'avez pas besoin de configurer les paramètres d'infrastructure, tels que les interfaces et les protocoles de routage. Cette configuration est automatisée et envoyée à partir de Panorama dans les modèles et les groupes de périphériques que le service crée automatiquement. Vous pouvez configurer tous les paramètres d'infrastructure requis par le service, tels que les paramètres requis pour créer des tunnels VPN IPSec vers les périphériques compatibles IPSec à partir de vos emplacements de réseaux distants, directement à partir du plug-in. Si vous le souhaitez, vous pouvez ajouter des modèles et des hiérarchies de groupes de périphériques à la configuration pour simplifier la configuration du service.

Pour simplifier la configuration du service, créez ou importez les modèles et groupes dde périphériques dont vous avez besoin avant de commencer les tâches de configuration pour l'utilisation de Prisma Access.

Lors de la création de modèles et de groupes de périphériques pour Prisma Access, vous n'avez pas besoin d'y attribuer des périphériques gérés. Au lieu de cela, vous allez les ajouter aux piles de modèles et aux hiérarchies de groupes de périphériques que Prisma Access crée. N'ajoutez aucun des modèles ou groupes de périphériques créés par Prisma Access à d'autres piles de modèles ou groupes de périphériques.

STEP 5 | Inscrivez-vous pour recevoir des notifications par e-mail en utilisant Strata Cloud Manager.

Prisma Access vous fournit des notifications sur le service, y compris toute mise à niveau du plan de données, à l'aide des notifications de cette application.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Modifiez la clé principale par défaut pour Panorama et dans le plug-in Cloud Services.

Palo Alto Networks recommande de modifier la clé principale dans Panorama et dans le plug-in Cloud Services comme bonne pratique de sécurité et de modifier la clé principale tous les mois.

Parce que les clés principales de Panorama et de Prisma Access ne se synchronisent pas, Palo Alto Networks vous recommande de ne pas alterner automatiquement la clé principale dans Panorama sans synchroniser également la clé principale dans Prisma Access. Vous pouvez utiliser les commandes de l'interface utilisateur ou de l'API de Panorama pour modifier les clés principales.

Veillez à garder une trace de la clé principale que vous déployez, car les clés principales ne peuvent pas être récupérées. Lorsqu'une clé principale expire, vous devez entrer la clé principale actuelle afin de configurer une nouvelle clé principale. Vous devez rétablir les paramètres d'usine de votre appliance Panorama si vous ne pouvez pas fournir la clé principale actuelle à son expiration.

1. Modifiez la clé principale dans Panorama.
   1. Sélectionnez **Panorama** > **Master Key and Diagnostics (Clé principale et diagnostics)**.

      Ne spécifiez pas de **Current Master Key (Clé principale actuelle)**.
   2. Configurez la **New Master Key (Nouvelle clé principale)** et **Confirm Master Key (Confirmez la clé principale)**.

      Notez la clé principale que vous avez configurée.
   3. Configurez la Lifetime (Durée de vie) de la clé principale et la Time for Reminder (Durée du rappel).
   4. Cliquez sur **OK**.
2. Modifiez la clé principale de Prisma Access en sélectionnant **Panorama** > **Cloud Services** > **Configuration** > **Service Operations (Opérations du service)** > **Edit master key (Modifier la clé principale)**, puis en saisissant la même clé principale que celle que vous avez saisie pour Panorama.

Vous pouvez également modifier la clé principale à l'aide des commandes API. Cela nécessite deux étapes : une pour modifier la clé principale de Panorama et une autre pour modifier la clé principale de Prisma Access. Utilisez les commandes API suivantes pour modifier la clé principale :

- Panorama : **XML API (API XML)** > **Operational Commands (Commandes opérationnelles)** > **request (requête)** > **master-key (clé principale)**
- Prisma Access : **XML API (API XML)** > **Operational Commands (Commandes opérationnelles)** > **request (requête)** > **plugins (plug-ins)** > **cloud_services** > **prisma-access** > **sync (synchronisation)**

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Activez l'infrastructure de services et les connexions aux services qui permettent la communication entre les éléments de Prisma Access.

1. Planifiez l'activation de l'infrastructure de services et des connexions aux services.
2. Activez l'infrastructure de services.
3. Créez une connexion aux services pour permettre l'accès à vos ressources d'entreprise.

   Si vous n'avez pas besoin d'accéder à vos ressources d'entreprise, vous devez tout de même créer une connexion aux services pour permettre l'accès entre les utilisateurs mobiles et les réseaux distants.

STEP 8 | Déploiements d'utilisateurs mobiles Prisma Access et sécurisez les utilisateurs mobiles avec GlobalProtect ou un proxy explicite, selon les besoins de votre déploiement.

Pour configurer GlobalProtect sur Prisma Access (Managed by Panorama) :

1. Configurez des zones pour les utilisateurs mobiles en créant deux zones dans le Mobile_User_Template (modèle Utilisateurs mobiles) (par exemple, Mobile-Users et Internet) et en mappant les zones. Vous devez mapper toute zone qui n'est pas des utilisateurs connectés à Prisma Access, des sièges sociaux ou des branches à Untrust (non approuvée).

   Sous **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users (Utilisateurs mobiles)**, mappez Internet à Untrust (non approuvée) ; Mobile-Users à Trust (approuvée).
2. Configurez l'authentification.

   Nous vous recommandons d'utiliser l'authentification locale comme première étape pour vérifier que le service est configuré et que vos utilisateurs ont accès à Internet. Vous pourrez ensuite passer à l'utilisation de vos méthodes d'authentification d'entreprise.
3. Configurez les politiques de sécurité pour le groupe de périphériques.

   Pour créer une politique de sécurité autorisant le trafic vers Internet, sélectionnez le groupe de périphériques Mobile_User_Device_Group **Policies (Politiques)** > **Security (Sécurité)** > **Prerules (Pré-règles)** > **Add (Ajouter)** une règle. Par exemple : Mobile-Users vers Internet.
4. Validez et appliquez vos modifications pour commencer à utiliser le service.
5. Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Monitor (Surveiller)** > **Mobile Users (Utilisateurs mobiles)** pour afficher le **Status (État)** et vérifier que vous pouvez envoyer une commande ping au FQDN du portail.
6. Validez que Prisma Access sécurise le trafic Internet pour les utilisateurs mobiles en téléchargeant et installant l'application GlobalProtect, en utilisant l'application pour vous connecter au portail en tant qu'utilisateur mobile (utilisateur local), en naviguant sur quelques sites Web sur Internet et en vérifiant les journaux du trafic sur Panorama.

Pour sécuriser les utilisateurs mobiles à l'aide d'un proxy explicite :

1. Lisez les Directives de configuration du proxy explicite.
2. Configurez l'authentification SAML. L'authentification SAML est requise pour le proxy explicite.
3. Configurez le mappage de groupe à l'aide du Cloud Identity Engine.
4. Terminez la configuration du proxy explicite.
5. Validez et appliquez vos modifications.

 ©2025 Palo Alto Networks, Inc.

STEP 9 | Planifiez, créez et configurez des connexions à des réseaux distants.

1. Ajoutez un ou plusieurs réseaux distants à Prisma Access.

   Vous pouvez intégrer un emplacement, puis ajouter des emplacements supplémentaires à l'aide de la fonction d'importation en bloc.
2. Créez une règle de politique de sécurité pour autoriser le trafic des réseaux distants vers le siège social (par exemple : de « approuvé » à « approuvé »).
3. Validez la connectivité entre la connexion aux services, la connexion au réseau distant et les utilisateurs mobiles.

STEP 10 | Exécutez le script API utilisé pour récupérer les adresses IP Prisma Access et Utilisez le script hérité pour récupérer les adresses IP des utilisateurs mobiles.

Vous ajoutez ces adresses à une liste autorisée sur le réseau de votre organisation pour limiter l'accès entrant à votre réseau d'entreprise et à vos applications.

STEP 11 | (Facultatif) Remplacez la méthode d'authentification locale par la méthode d'authentification de votre organisation.

1. Créez un profil d'authentification qui répond aux exigences de votre organisation (SAML, LDAP, RADIUS, etc.).
2. Si votre organisation utilise un serveur d'authentification sur site tel que RADIUS ou Active Directory, ajoutez les adresses IP que Prisma Access utilise comme adresse IP source pour les requêtes internes (Récupérer les adresses IP pour Prisma Access) aux listes d'autorisation dans votre réseau ou autorisez les adresses IP de l'ensemble du sous-réseau d'infrastructure (Prisma Access récupère l'adresse IP de bouclage dans ce sous-réseau).
3. Mettez à jour le profil d'authentification du portail et de la passerelle Prisma Access pour utiliser ce nouveau profil d'authentification.

STEP 12 | (Facultatif) Transférez les journaux de Strata Logging Service à un récepteur Syslog externe.

 ©2025 Palo Alto Networks, Inc.

Configurer l'infrastructure de service Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Version Prisma Access minimale requise pour le **Pre-prod or Lab Tenant (Locataire Pré-prod ou Lab)** : 3.0 Préféré

Prisma Access utilise ce sous-réseau pour créer le réseau principal pour la communication entre vos réseaux de succursales, les utilisateurs mobiles et l'infrastructure de sécurité Prisma Access, ainsi qu'avec les réseaux du siège social (QG) et des centres de données que vous prévoyez de connecter à Prisma Access via des connexions aux services.

Pour permettre la communication entre vos sites réseau distants, les utilisateurs mobiles et le siège ou les centres de données auxquels vous prévoyez de vous connecter à Prisma Access via des connexions aux services, configurez le sous-réseau de l'infrastructure de service. Prisma Access utilise ce sous-réseau pour créer le réseau principal pour la communication entre vos réseaux de succursales, les utilisateurs mobiles et l'infrastructure de sécurité Prisma Access, ainsi qu'avec les réseaux du siège et des centres de données auxquels vous prévoyez de vous connecter à Prisma Access via des connexions aux services.

- Strata Cloud Manager
- Panorama

Configurer Prisma Access l'infrastructure de service (Strata Cloud Manager)

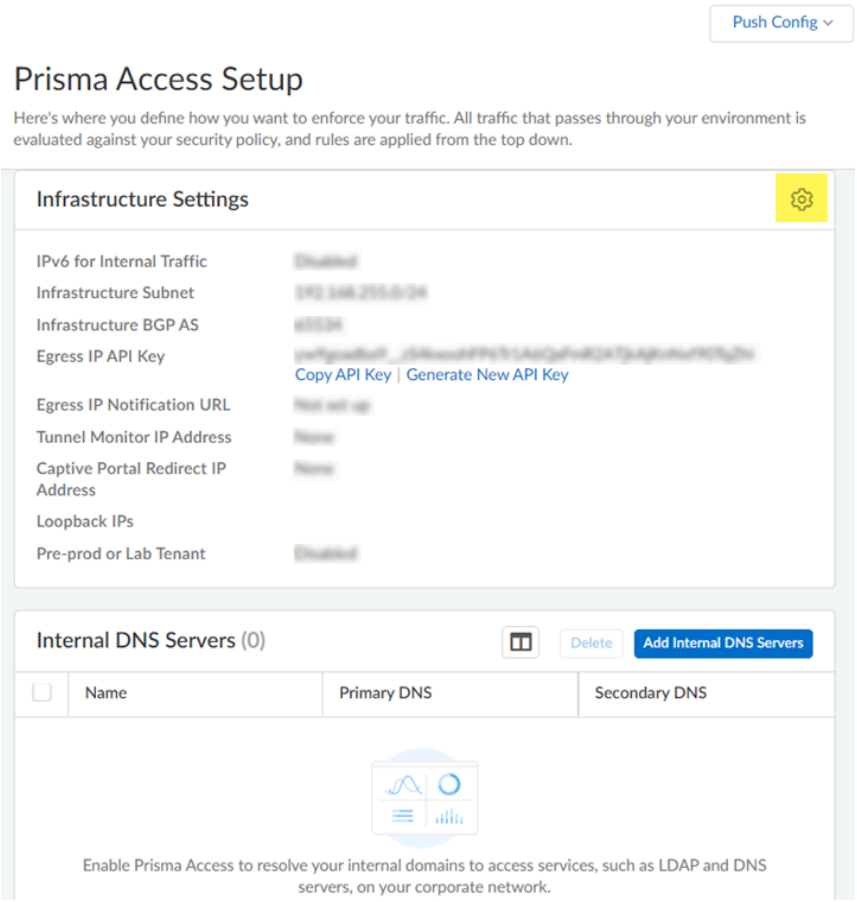
Utilisez les recommandations et exigences suivantes lorsque vous ajoutez un sous-réseau d'infrastructure pour Prisma Access :

- ❑ Utilisez un sous-réseau conforme au RFC 1918. Bien que l'utilisation d'adresses IP (publiques) non conformes à la norme RFC 1918 soit possible, nous ne le recommandons pas en raison des conflits possibles avec l'espace d'adresses IP publiques sur Internet.
- ❑ Ne spécifiez aucun sous-réseau qui chevauche la plage de sous-réseaux 169.254.0.0/16 et 100.64.0.0/10, car Prisma Access réserve ces adresses IP et sous-réseaux à son usage interne.
- ❑ Ce sous-réseau est une extension de votre réseau existant et ne peut donc pas se chevaucher avec les sous-réseaux IP que vous utilisez au sein de votre réseau d'entreprise ou avec les pools d'adresses IP que vous attribuez pour Prisma Access les utilisateurs ou Prisma Access pour les réseaux.
- ❑ Étant donné que l'infrastructure de service nécessite un grand nombre d'adresses IP, vous devez désigner un sous-réseau /24 (par exemple, 172.16.55.0/24).
- ❑ Si vous utilisez le routage dynamique pour vos réseaux distants ou vos connexions aux services, vous devez également configurer un numéro AS privé BGP conforme au RFC 6996.

STEP 1 | Lancez Prisma Access

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Allez dans **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Paramètres d'infrastructure)** et cliquez sur la roue dentée pour modifier les paramètres.



STEP 3 | Entrez un **Infrastructure Subnet (Sous-réseau d'infrastructure)** que Prisma Access peut utiliser pour assurer la communication entre vos emplacements de réseau distant, les utilisateurs mobiles et le siège social ou les centres de données que vous prévoyez de connecter à Prisma Access via des connexions aux services.

Utilisez un sous-réseau conforme au RFC 1918 pour le sous-réseau d'infrastructure. Bien que l'utilisation d'adresses IP (publiques) non conformes à la norme RFC 1918 soit possible, nous ne le recommandons pas en raison des conflits possibles avec l'espace d'adresses IP publiques sur Internet.

STEP 4 | (Facultatif) Si vous configurez IPv6, sélectionnez **IPv6 for Internal Traffic (IPv6 pour le trafic interne)** et sélectionnez un sous-réseau IPv6.

STEP 5 | Entrez l'**Infrastructure BGP AS** que vous souhaitez utiliser dans Prisma Access l'infrastructure.

Si vous souhaitez activer le routage dynamique afin que Prisma Access puisse découvrir dynamiquement des itinéraires vers des ressources dans vos réseaux distants et vos emplacements de siège ou de centre de données, vous devez utiliser le protocole BGP (Border Gateway Protocol). L'**Infrastructure BGP AS** est le numéro du système autonome (AS) qui

 ©2025 Palo Alto Networks, Inc.

identifie les itinéraires par lesquels BGP peut envoyer le trafic. Si vous ne fournissez pas de numéro AS, Prisma Access utilise le numéro AS par défaut (65534).

Si vous souhaitez spécifier votre propre numéro AS, vous devez utiliser un numéro AS privé conforme à la RFC 6996. Les formats acceptés sont la notation AS Plain de 4 octets [64512-65534],[4200000000-4294967294] ou AS Dot [0.64512-0.65534], [64086.59904-65535.65534].

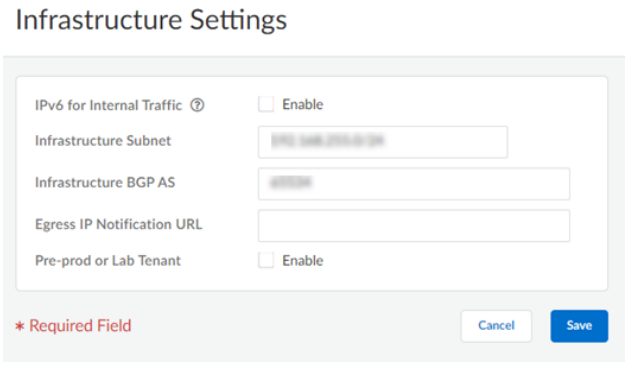
STEP 6 | Si vous permettez à vos utilisateurs d'accéder aux applications en fonction de l'adresse IP source, vous devrez obtenir la liste des adresses IP à partir desquelles le trafic de Prisma Access utilise comme adresse source afin que vous puissiez les autoriser dans vos stratégies d'accès à l'application.

Copy (Copier) la **Egress IP API Key (Clé API IP de sortie)** pour permettre l'utilisation de l'API d'adresse IP de sortie Prisma Access. Aussi, parce que l'adresse IP que Prisma Access utilise change périodiquement, par exemple lorsque vous ajoutez un nouvel emplacement, lorsque Prisma Access doit mettre à l'échelle les ressources dans un emplacement existant ou lorsqu'il y a une mise à niveau de l'infrastructure : vous devez savoir quand les adresses IP changent afin de pouvoir mettre à jour vos règles de politique ou automatiser ces mises à jour en définissant une **Egress IP Notification URL (URL de notification IP de sortie)**. Voir Récupérer les adresses IP pour Prisma Access pour plus de détails.

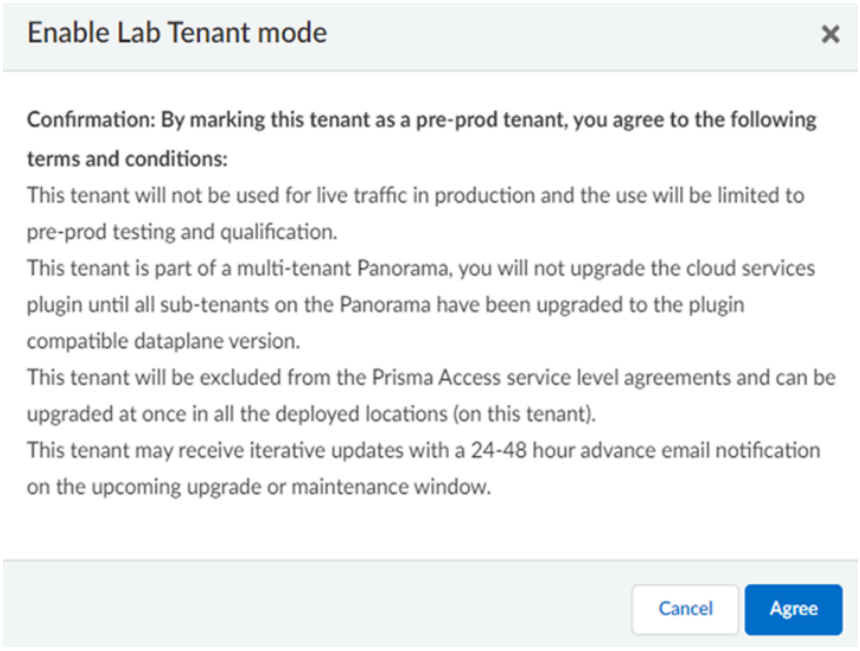
 ©2025 Palo Alto Networks, Inc.

STEP 7 | (Facultatif) Activez le locataire en tant que locataire de pré-production ou de laboratoire.

1. **Enable (Activer)** le locataire en tant que **Pre-prod or Lab Tenant (Locataire de pré-production ou de laboratoire)**.



2. **Agree (Accepter)** pour confirmer.



   Lorsque vous activez un locataire en tant que locataire de pré-production ou de laboratoire, vous pouvez planifier des mises à niveau pour ce locataire uniquement avant de mettre à niveau d'autres locataires de production. Le locataire reçoit des notifications 24 à 48 heures avant une mise à niveau à venir. Lorsque vous désactivez le locataire à partir d'un locataire de pré-production ou d'un locataire de laboratoire, il est considéré comme un locataire de production.

3. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

STEP 8 | Pour activer Prisma Access pour résoudre vos domaines internes, **Add Internal DNS Servers (Ajouter des serveurs DNS internes)**.

Si vous prévoyez de configurer des connexions aux services pour permettre l'accès aux ressources de votre réseau d'entreprise et que vous avez également besoin de Prisma Access pour résoudre vos domaines internes, vous devez définir la liste des domaines internes. Les requêtes DNS pour les domaines de la liste de domaines interne sont envoyées à vos serveurs

 ©2025 Palo Alto Networks, Inc.

DNS locaux pour s'assurer que les ressources sont disponibles pour les utilisateurs du réseau distant Prisma Access et les utilisateurs mobiles.

1. Entrez le serveur **Primary DNS (DNS primaire)** et le serveur **Secondary DNS (DNS secondaire)** qui Prisma Access doit être utilisé pour résoudre les noms de domaine internes.
2. **Add (Ajouter)** les **Domain Names (Noms de domaine)** internes que vous voulez que Prisma Access résolve.

   Utilisez un caractère générique (*) devant les domaines de la liste de domaines, par exemple, *.acme.local ou *.acme.com

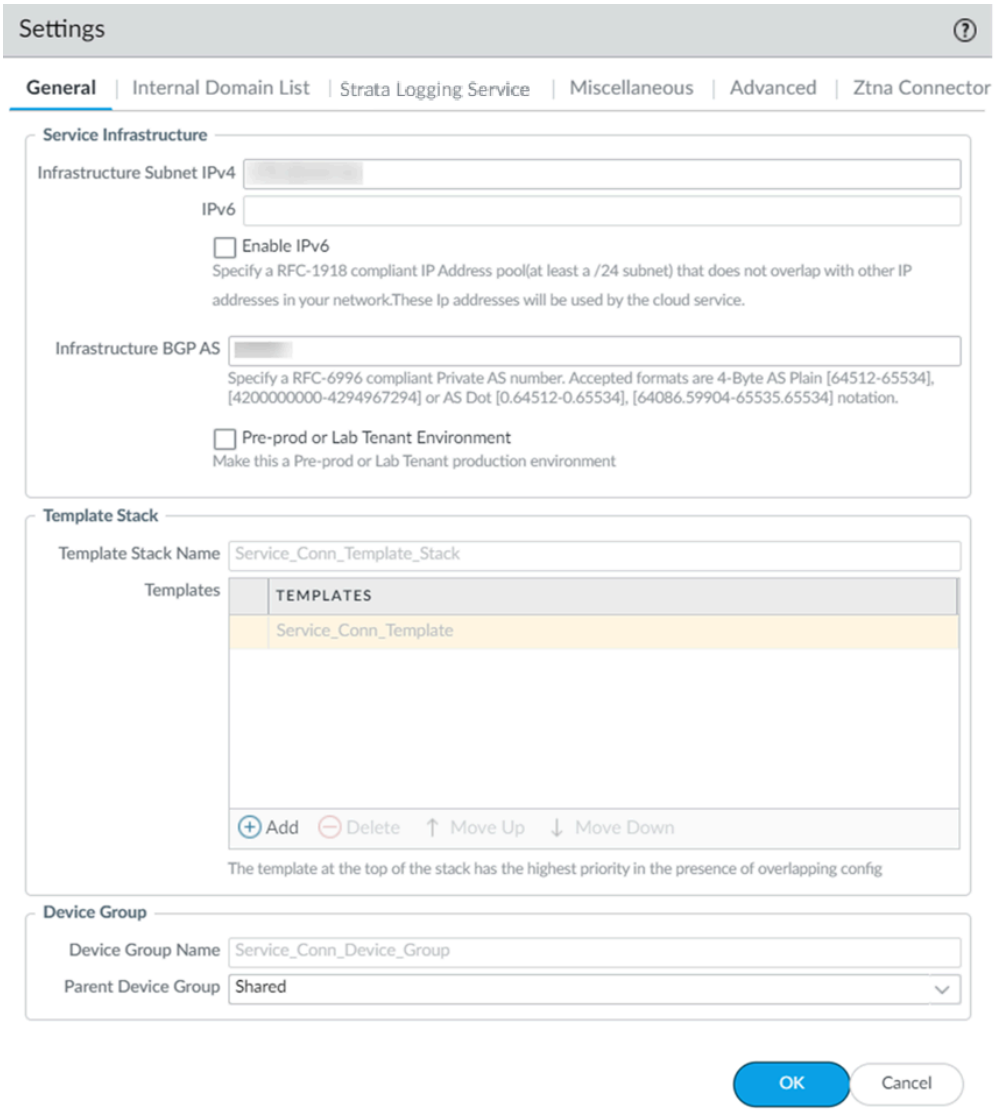
STEP 9 | **Push Config (Transmettre la configuration)** pour enregistrer les paramètres de votre infrastructure de service dans Prisma Access.

Configurer l'infrastructure de service Prisma Access (Panorama)

Avant de pouvoir commencer à configurer des Prisma Access pour sécuriser vos réseaux distants et/ou vos utilisateurs mobiles, vous devez configurer un sous-réseau d'infrastructure, que Prisma Access utilisera pour créer le réseau de base pour la communication entre vos connexions aux services, vos réseaux distants et vos utilisateurs mobiles, ainsi qu'avec les réseaux d'entreprise que vous prévoyez de connecter à Prisma Access via des connexions aux services. Étant donné qu'un grand nombre d'adresses IP seront nécessaires pour mettre en place l'infrastructure, vous devez utiliser un sous-réseau /24 (par exemple, 172.16.55.0/24) au minimum. Assurez-vous de respecter toutes les directives et exigences.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** et cliquez sur l'icône engrenage pour modifier les paramètres.



STEP 2 | Sous l'onglet **General (Général)**, spécifiez un **Infrastructure Subnet (Sous-réseau d'infrastructure)** qui répond aux exigences, par exemple 172.16.55.0/24.

STEP 3 | (Facultatif) Si vous configurez IPv6, sélectionnez **IPv6 for Internal Traffic (IPv6 pour le trafic interne)** et sélectionnez un sous-réseau IPv6.

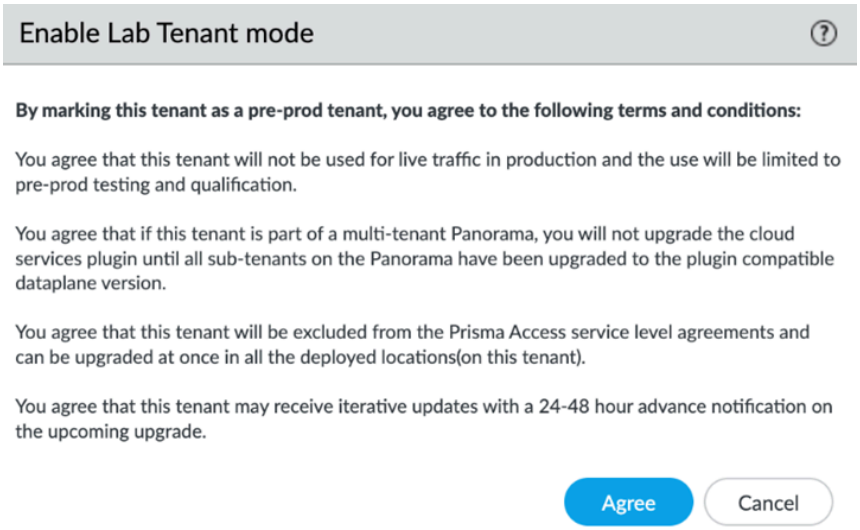
STEP 4 | (Facultatif) Si vous souhaitez permettre à Prisma Access d'utiliser BGP pour découvrir dynamiquement des itinéraires vers des ressources sur vos réseaux distants et les emplacements de votre siège social/centre de données, saisissez l'**Infrastructure BGP AS** que vous souhaitez utiliser dans l'infrastructure Prisma Access.

Si vous ne fournissez pas de numéro AS, le numéro AS par défaut 65534 sera utilisé.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Facultatif) Activer un locataire comme **Pre-prod or Lab Tenant Environment (Environnement locataire de pré-production ou locataire de laboratoire)**.

Lorsque vous activez un locataire en tant que locataire de pré-production ou de laboratoire, vous pouvez planifier des mises à niveau pour ce locataire uniquement avant de mettre à niveau d'autres locataires de production. Le locataire reçoit des notifications 24 à 48 heures avant une prochaine mise à niveau.



Lorsque vous désactivez le locataire à partir d'un locataire de pré-production ou d'un locataire de laboratoire, il est considéré comme un locataire de production.

Prisma Access pour Clean Pipe ne prend pas en charge cette fonctionnalité.

STEP 6 | (Facultatif) Activez Prisma Access pour résoudre vos domaines internes à l'aide de vos serveurs DNS d'entreprise.

Utilisez cette étape si vous avez besoin de Prisma Access pour pouvoir résoudre vos domaines internes afin d'accéder à des services, tels que des serveurs LDAP, sur votre réseau d'entreprise via des connexions aux services. Par exemple, si vous souhaitez qu'une recherche DNS pour votre domaine d'entreprise porte exclusivement sur le serveur DNS d'entreprise, spécifiez ici le domaine d'entreprise et les serveurs DNS d'entreprise.

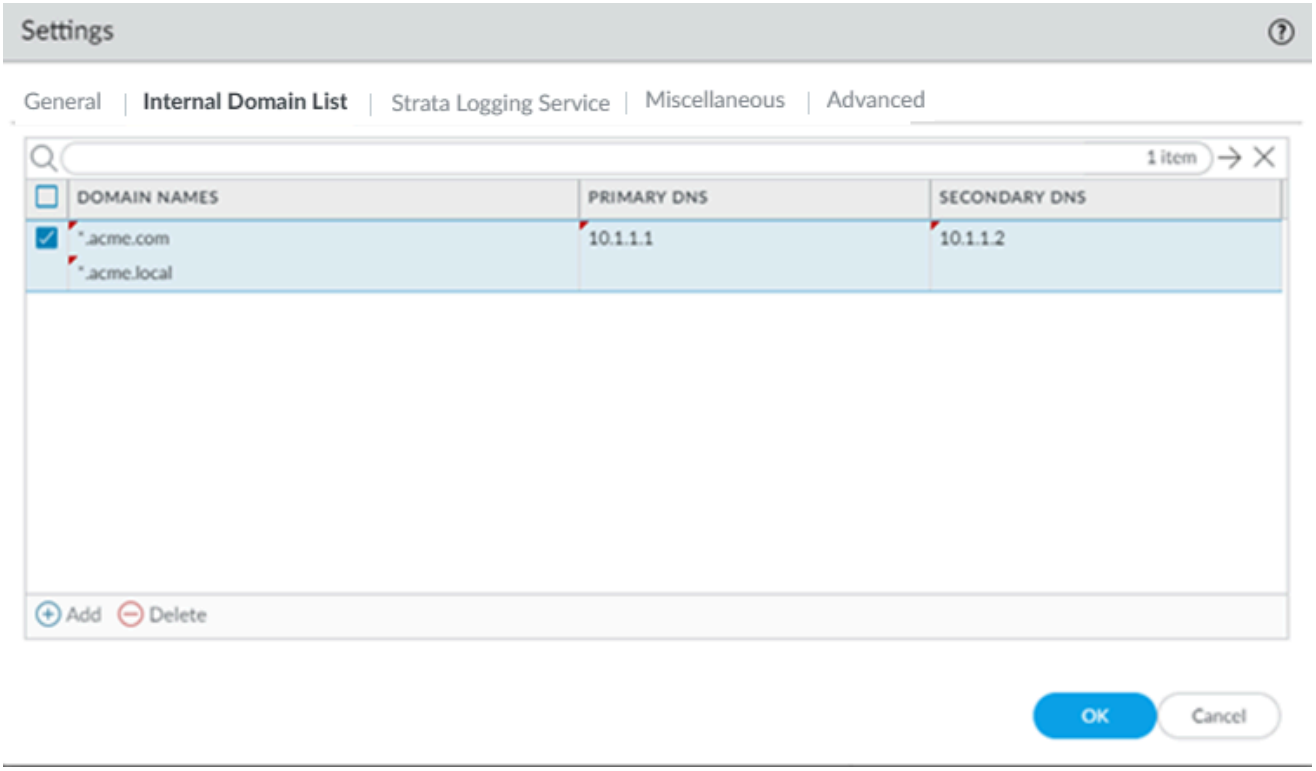
1. Sélectionnez l'onglet **Internal Domain List (Liste des domaines internes)**.

 ©2025 Palo Alto Networks, Inc.

2. **Add (Ajouter)** les serveurs **Domain Names (Noms de domaine)**, **Primary DNS (DNS primaire)** et **Secondary DNS (DNS secondaire)** que vous souhaitez Prisma Access pour résoudre vos noms de domaine internes.

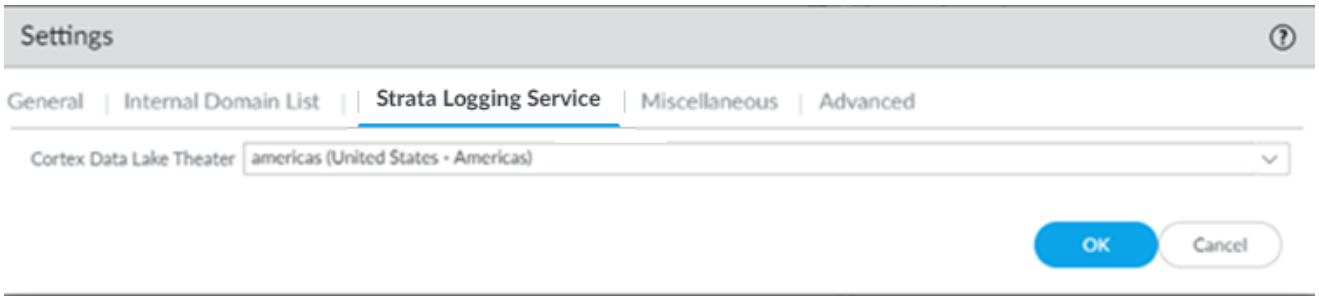
   Utilisez un caractère générique (*) devant les domaines de la liste de domaines, par exemple, *.acme.local ou *.acme.com

   Ne saisissez pas d'adresse 127.0.0.1 car cela peut causer des problèmes de routage interne à Prisma Access.



STEP 7 | Activez Strata Logging Service.

1. Sélectionnez l'onglet **Strata Logging Service (Service de journalisation Strata)**.
2. Sélectionnez un **Strata Logging Service Theater (Théâtre de service de journalisation Strata)** et cliquez sur **OK**.



3. Configurez les groupes de périphériques que vous utilisez pour pousser les paramètres à Prisma Access avec un profil de transfert de journal qui transmet les types de journal

 ©2025 Palo Alto Networks, Inc.

souhaités au **Panorama/Strata Logging Service (Service de journalisation Panorama/Strata)**.

Le plug-in Cloud Services ajoute automatiquement les paramètres de journalisation suivants (**Device (Périphérique)** > **Log Settings (Paramètres des journaux)**) après une nouvelle installation ou lors de la suppression de modèles non Prisma Access d'une pile de modèles Prisma Access :

- Les paramètres des journaux pour les journaux Système (**system-gpcs-default**), User-ID (**userid-gpcs-default**), HIP Match (**hipmatch-gpcs-default**) et GlobalProtect (**gp-prismaaccess-default**) sont ajoutés au modèle Mobile_User_Template.
- Les paramètres des journaux pour les journaux Système (**system-gpcs-default**), User-ID (**userid-gpcs-default**) et GlobalProtect (**gp-prismaaccess-default**) sont ajoutés au Remote_Network_Template.
- Les paramètres des journaux pour les journaux Système (**system-gpcs-default**) et GlobalProtect (**gp-prismaaccess-default**) sont ajoutés au Modèle Service_Conn_Template.

Ces configurations des paramètres des journaux redirigent automatiquement les journaux Système, User-ID, HIP Match et GlobalProtect vers les Strata Logging Service.

Pour appliquer les modifications des paramètres des journaux, exécutez les étapes suivantes, puis validez et poussez vos modifications :

- Pour appliquer le paramètre de journal au modèle d'utilisateur mobile, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users (Utilisateurs mobiles)**, cliquez sur l'icône d'engrenage pour modifier les paramètres et cliquez sur OK.
- Pour appliquer le paramètre de journal au modèle de réseau distant, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**, cliquez sur l'icône d'engrenage pour modifier les paramètres et cliquez sur OK.
- Pour appliquer le paramètre journal au modèle de connexion aux services, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration de service)**, cliquez sur l'icône d'engrenage pour modifier les paramètres et cliquez sur OK.

La façon dont vous activez la redirection de journaux pour les autres types de journaux dépend du type. Pour les journaux générés en fonction d'une correspondance de stratégie, utilisez un profil de transfert de journaux. Consultez le Guide de démarrage du service de journalisation Strata pour plus d'informations.

STEP 8 | (Facultatif) Configurer les paramètres **Miscellaneous (Divers)**.

1. (Facultatif) Ajoutez le jeton de fin pour les URL dans les listes dynamiques externes (EDL) ou les catégories d'URL personnalisées en sélectionnant **Append the ending token to the URLs in the URL filtering configuration (Ajouter le jeton de fin aux URL dans la configuration de filtrage des URL)**.

   Si vous utilisez des URL dans des EDL ou des catégories d'URL personnalisées et que vous n'ajoutez pas de barre oblique directe (**/**) à l'URL, il est possible d'autoriser plus d'URL que prévu. Par exemple, entrer **`example.com`** comme URL correspondante

 ©2025 Palo Alto Networks, Inc.

au lieu de **`example.com/`** correspondrait également à example.com.website.info ou example.com.br.

En sélectionnant **Append the ending token to the URLs in the URL filtering configuration (Ajouter le jeton de fin aux URL dans la configuration de filtrage d'URL)**, Prisma Access définit un jeton de fin aux URL dans les EDL ou les catégories d'URL personnalisées de sorte que, si vous entrez **`example.com`**, Prisma Access le traite comme il traiterait example.com/ et ne correspond qu'à cette URL.

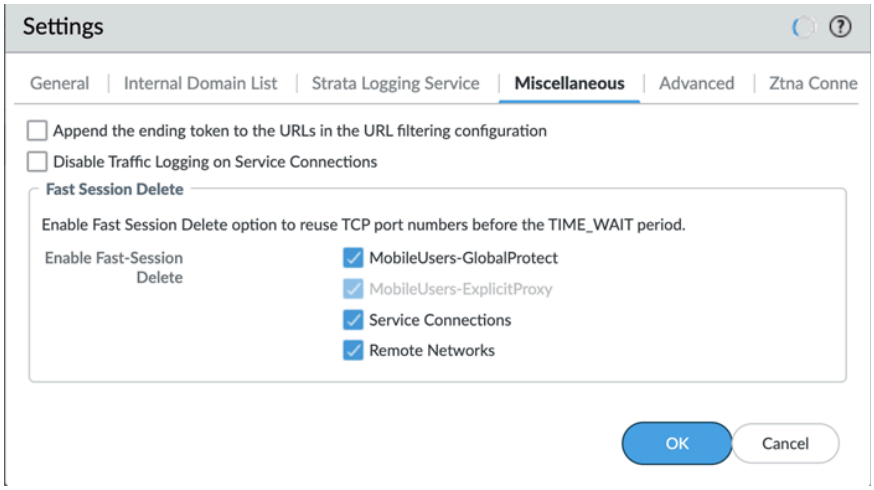
2. (Facultatif) **Disable Traffic Logging on Service Connections (Désactiver la journalisation du trafic sur les connexions aux services)** pour désactiver la journalisation sur les connexions aux services pour votre déploiement Prisma Access.

   Si la majorité des flux de trafic enregistrés par les connexions aux services sont asymétriques, la désactivation de la journalisation des connexions aux services peut être nécessaire pour réduire la consommation de stockage de la journalisation des Strata Logging Service. Si votre déploiement n'a pas de flux asymétriques via les connexions aux services, vous ne devez pas désactiver la journalisation.

3. (Facultatif) Pour activer la suppression Fast-Session pour les réseaux distants, les connexions aux services ou les utilisateurs mobiles — Déploiements GlobalProtect, cochez les cases pour **Mobile Users—GlobalProtect (Utilisateurs mobiles—GlobalProtect)**, **Service Connections (Connexions aux services)** ou **Remote Networks (Réseaux distants)**.

   Supprimer la session rapide permet à Prisma Access de réutiliser les numéros de port TCP avant l'expiration de la période TCP TIME_WAIT, et peut être utile pour les sessions décryptées SSL qui peuvent être de courte durée.

   Pour les utilisateurs mobiles—Déploiements de proxy explicites, supprimer la session rapide est un élément clé de ses fonctionnalités et vous ne pouvez pas le désactiver.



 ©2025 Palo Alto Networks, Inc.

STEP 9 | (Facultatif) Configurer les paramètres **Advanced (Avancés)** (préférences de routage, options symétriques de chemin réseau pour les connexions aux services et redistribution HIP).

1. Spécifiez la **Routing Preference (Préférence de routage)** à utiliser avec les connexions aux services.

   Vous pouvez spécifier les préférences réseau pour utiliser soit le réseau de votre organisation, soit le réseau Prisma Access, pour traiter le trafic de connexion aux services.

   - **Default (Par défaut)** — Prisma Access utilise le routage par défaut dans son réseau interne.
   - **Hot potato routing (Routage hot potato)**–Prisma Access désactive le trafic de connexion aux services vers le WAN de votre organisation le plus rapidement possible.

   Modifier la méthode de routage des connexions aux services Prisma Access nécessite une compréhension approfondie de la topologie et des dispositifs de routage de votre organisation, ainsi qu'une compréhension du fonctionnement du routage Prisma Access. Nous vous recommandons de lire attentivement les Routage pour le trafic de connexion aux services *avant de changer la méthode de routage par défaut.*
2. Configurez le **Backbone Routing (Routage principal)** à utiliser pour les connexions aux services.

   Par défaut, le backbone Prisma Access demande que vous disposiez d'un chemin réseau symétrique pour le trafic qui revient du centre de données ou de l'emplacement du siège par le biais d'une connexion aux services. Si vous souhaitez utiliser ECMP ou un autre mécanisme d'équilibrage de charge pour les connexions aux services à partir de votre CPE, vous pouvez activer des flux asymétriques à travers le backbone Prisma Access.

   - Sélectionnez **no-asymmetric-routing** pour exiger des flux symétriques à travers le backbone de connexion aux services.
   - Sélectionnez **asymmetric-routing-only** pour permettre aux Prisma Access d'utiliser des flux asymétriques à travers le backbone de connexion aux services.
   - Si vous avez plusieurs connexions aux services à un emplacement, vous pouvez profiter de l'équilibrage des charges dans votre déploiement Prisma Access en sélectionnant **asymmetric-routing-with-load-share** (le paramètre par défaut). Cependant, l'équilibrage des charges se fait au meilleur effort, et l'équilibrage des charges échouera si l'une des connexions aux services tombe en panne.
3. Redistribuer les informations HIP avec Prisma Access pour utiliser les connexions aux services pour redistribuer les informations HIP des utilisateurs mobiles et des utilisateurs sur les réseaux distants.
4. Identification et mise en quarantaine des périphériques compromis dans un déploiement GlobalProtect Prisma Access pour que Prisma Access identifie et mette en quarantaine les périphériques compromis qui sont connectés à l'application GlobalProtect.
5. **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down (Retirer les itinéraires statiques si le tunnel IPSec de la connexion aux services ou des**

 ©2025 Palo Alto Networks, Inc.

réseaux distants est en panne) si vous souhaitez que Prisma Access supprime les routes statiques lorsqu'un tunnel tombe sans tunnel de sauvegarde.

Prisma Access supprime l'itinéraire dans les situations suivantes :

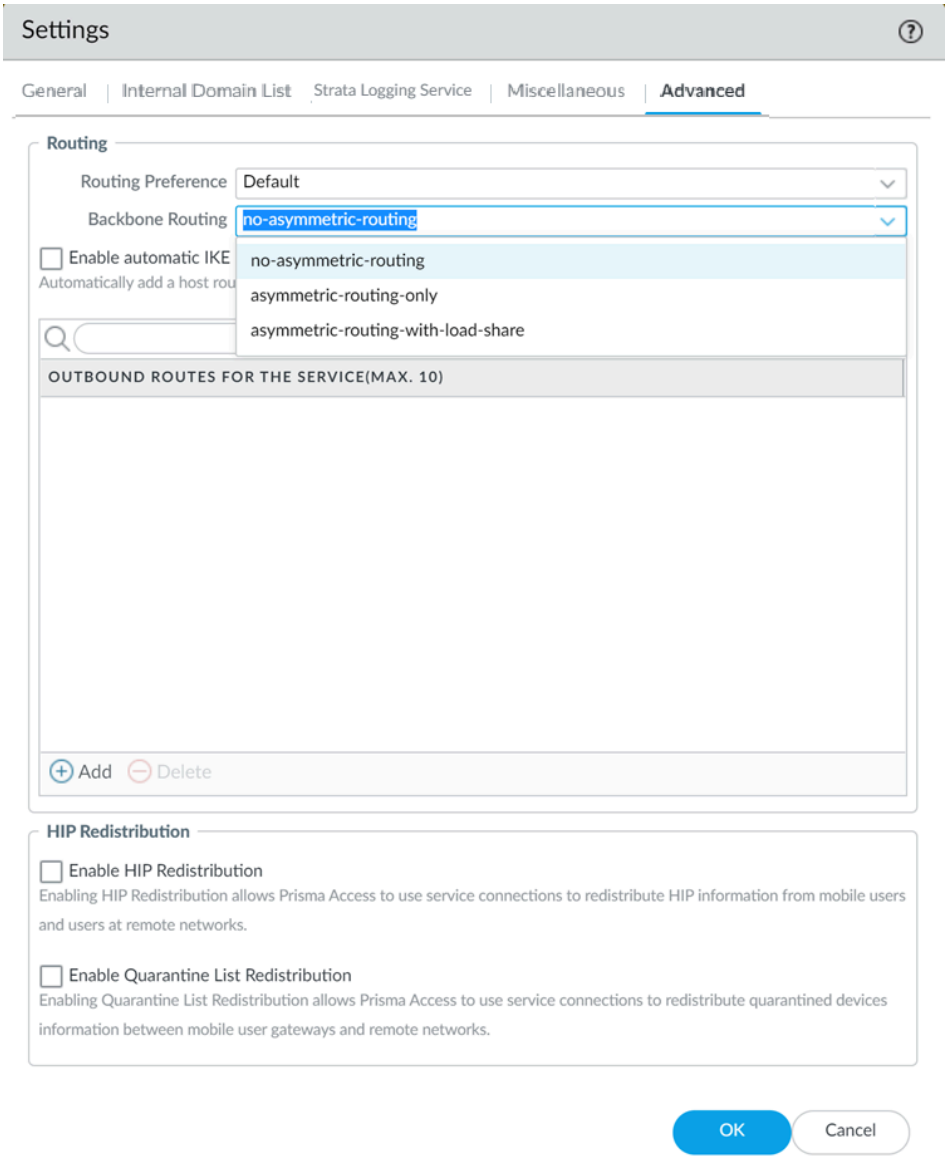
- Le tunnel primaire descend et il n'y a pas de tunnel secondaire.
- Si un tunnel primaire et secondaire est configuré, mais les deux descendent.

Vous ne pouvez pas appliquer cette modification si la surveillance du tunnel n'est pas activée.

6. (Facultatif) Si vous souhaitez acheminer des paquets de tunnel IPSec de connexion réseau et de service distants vers les passerelles IKE statiques sur Internet, **Enable automatic IKE peer host routes for Remote Networks and Service Connections (Activer les itinéraires IKE automatiques d'hôtes homologues pour les réseaux distants et les connexions aux services)**.
7. (Facultatif) **Specify Outbound Routes for the Service (Max 10) (Spécifiez les routes sortantes pour le service (Max 10))** en ajoutant jusqu'à 10 préfixes pour lesquels Prisma Access ajoute des itinéraires statiques sur toutes les connexions aux services et les

 ©2025 Palo Alto Networks, Inc.

connexions réseau distantes. Prisma Access achemine ensuite le trafic vers ces préfixes sur Internet.



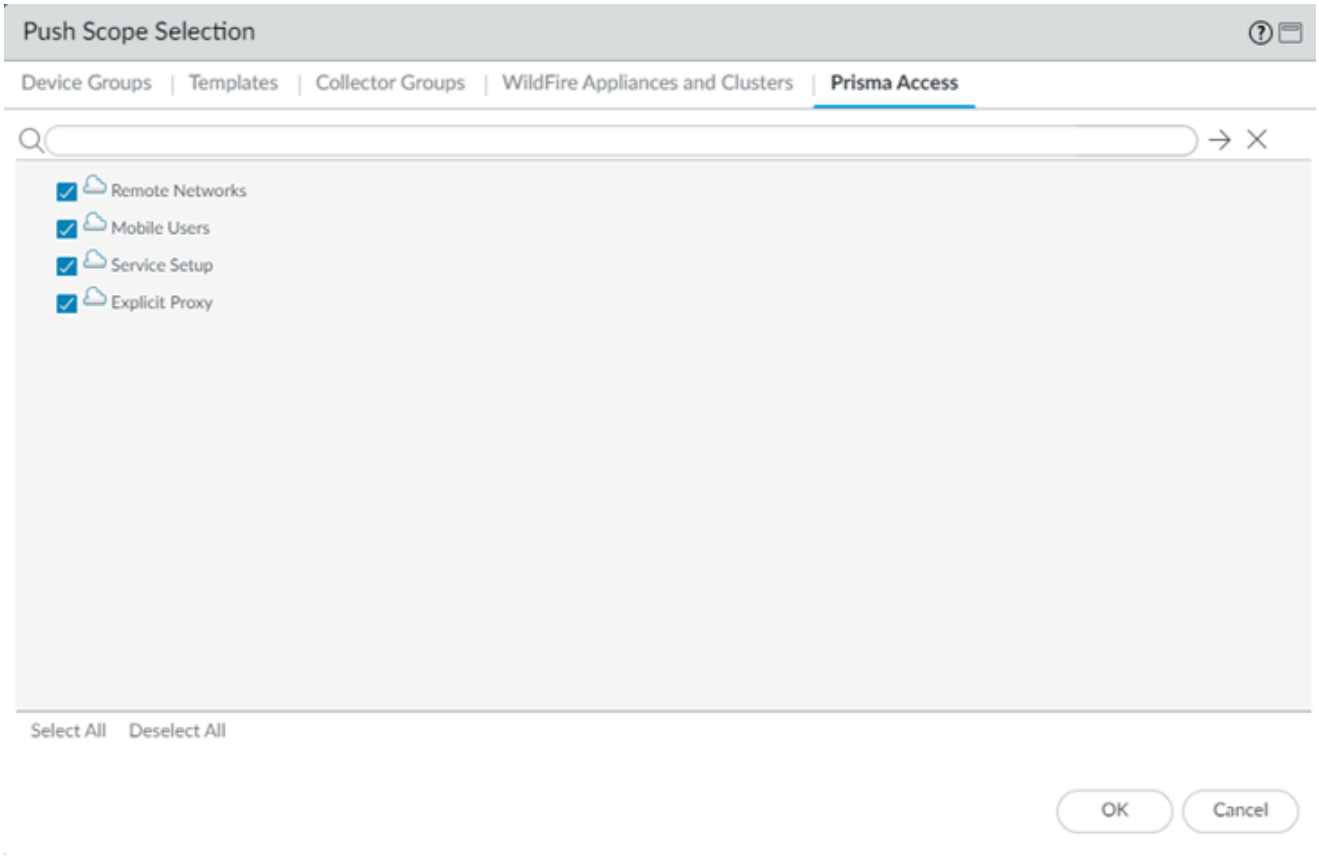
STEP 10 | Cliquez sur **OK** pour enregistrer les paramètres de configuration du service.

©2025 Palo Alto Networks, Inc.

STEP 11 | Validez toutes vos modifications dans Panorama et poussez les modifications de configuration à Prisma Access.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.
2. Cliquez sur **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)**, puis sur **Edit Selections (Modifier les sélections)**.
3. Dans l'onglet **Prisma Access**, assurez-vous que **Service Setup (Configuration du service)** est sélectionné, puis cliquez sur **OK**.

   Prisma Access devrait sélectionner automatiquement les composants qui doivent être validés.

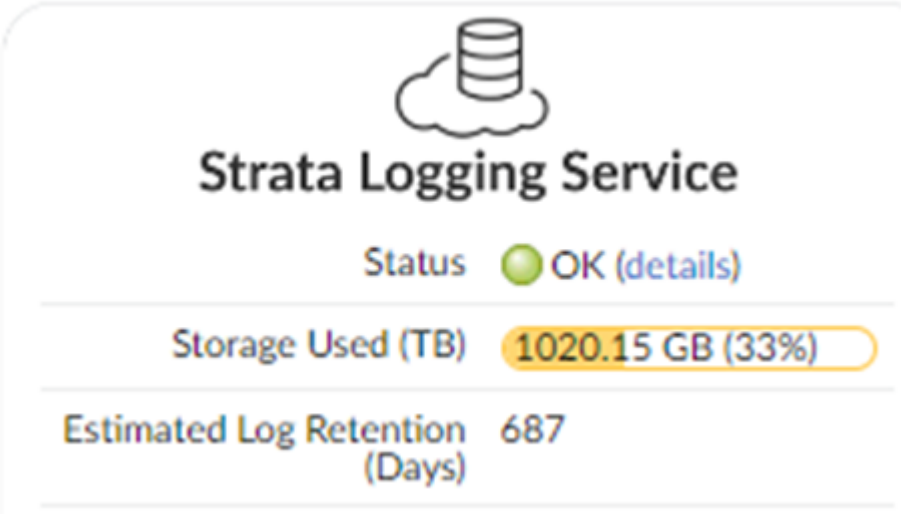


4. Cliquez sur **Push (Pousser)**.

 ©2025 Palo Alto Networks, Inc.

STEP 12 | Vérifiez que Prisma Access est correctement connecté à Strata Logging Service.

1. Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Status (État)** > **Strata Logging Service (Service de journalisation Strata)** et vérifiez que l'état est **OK**.



Si l'état est **Error (Erreur)**, cliquez sur le lien détails pour afficher les erreurs.

STEP 13 | Poursuivre la mise en place des Prisma Access :

- Créer une connexion aux services pour autoriser l'accès aux applications privées
- Configurer Prisma Access pour les réseaux
- Configurer Prisma Access pour les utilisateurs

 ©2025 Palo Alto Networks, Inc.

Utilisateurs mobiles : Allocation d'adresses IP

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Après que vous avez configuré le déploiement Prisma Access, il est utile de savoir à quels moments les adresses IP changent afin de pouvoir proactivement planifier l'infrastructure, récupérer les adresses IP et ajouter les adresses IP requises aux listes d'autorisation en conséquence. Les changements d'adresse IP peuvent être le résultat de modifications que vous effectuez (par exemple, l'ajout d'un autre emplacement d'utilisateur mobile) ou de modifications que Prisma Access effectue automatiquement (par exemple, un grand nombre d'utilisateurs mobiles accède à la même passerelle Prisma Access).

Une fois que vous avez déployé Prisma Access pour les utilisateurs pour la première fois, Prisma Access attribue deux *adresses IP publiques et, le cas échéant, de sortie* pour chaque portail et passerelle. Ces adresses IP sont uniques, non partagées, dédiées au déploiement Prisma Access et restent allouées au locataire jusqu'à l'expiration de l'abonnement Prisma Access et la fin de la période de grâce.

Si vous avez une configuration multilocataire, Prisma Access ajoute des adresses IP dédiées pour chaque locataire.

Étant donné que l'adresse IP publique correspond à l'adresse IP source que Prisma Access utilise pour les requêtes effectuées vers une destination Internet, vous devrez peut-être connaître l'adresse IP publique et l'ajouter à une liste d'autorisation sur votre réseau afin de fournir aux utilisateurs un accès aux ressources telles que les applications SaaS ou les applications partenaires accessibles au public.

De nouvelles adresses IP publiques peuvent être ajoutées au locataire si les événements suivants se produisent :

- Un grand nombre d'utilisateurs mobiles accèdent à un emplacement dans le même emplacement.

  Si le nombre d'utilisateurs nécessite une capacité plus élevée, Prisma Access peut ajouter une ou plusieurs passerelles. Prisma Access ajoute une ou plusieurs passerelles pour répondre à l'augmentation du nombre d'utilisateurs, attribue une ou plusieurs adresses IP publiques existantes à la nouvelle passerelle et ajoute un nouvel ensemble d'adresses IP aux emplacements d'utilisateurs mobiles pour remplacer celles qui ont été utilisées.
- Vous ajoutez un ou plusieurs emplacements à votre déploiement.

  Lorsque vous ajoutez d'autres emplacements, Prisma Access ajoute une autre passerelle et un nouvel ensemble d'adresses IP pour chaque emplacement ajouté.

Étant donné que Prisma Access active davantage d'adresses IP publiques après un événement de mise à l'échelle et lorsque vous ajoutez un emplacement, vous devez ajouter une URL de notification d'événement de changement d'adresse IP ou utiliser l'API pour récupérer les adresses des utilisateurs mobiles afin d'être averti des changements d'adresses IP dans votre infrastructure

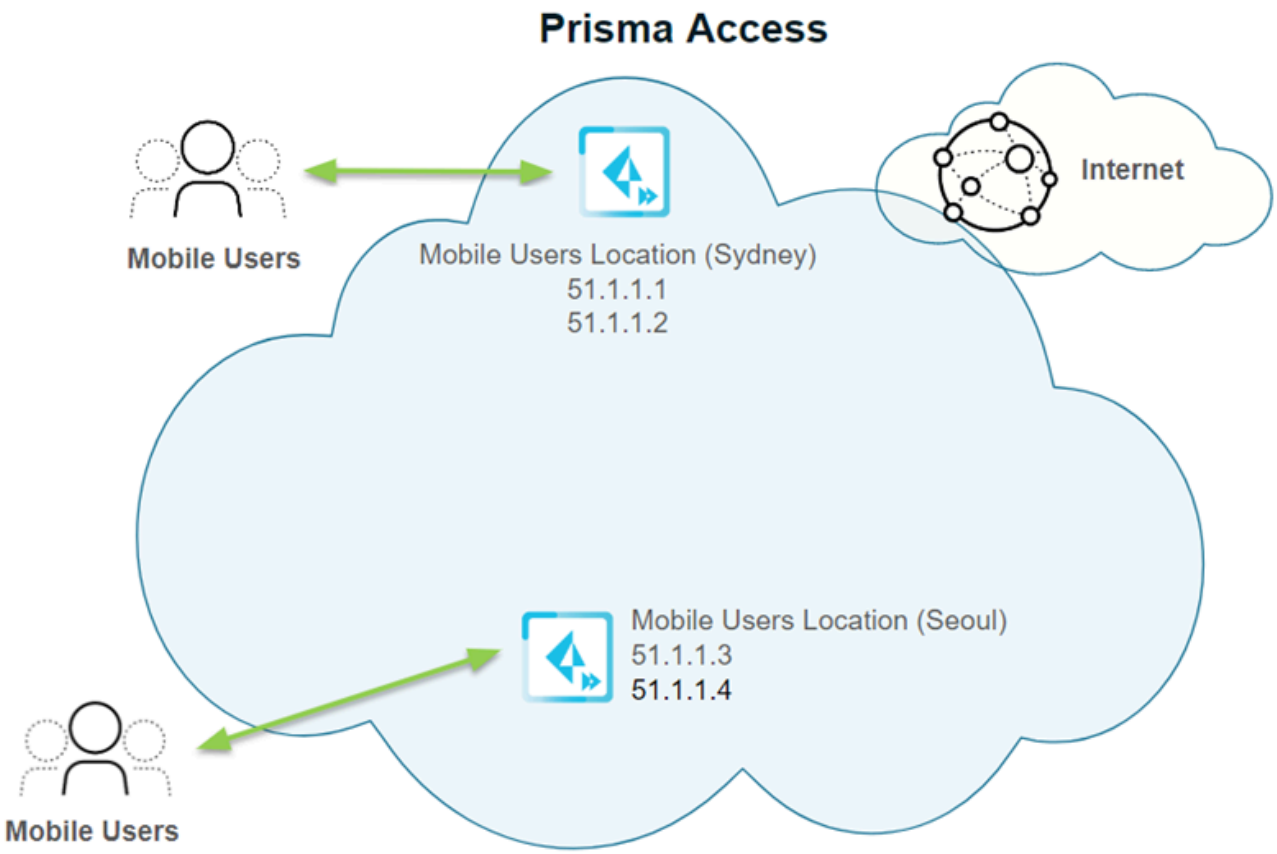
 ©2025 Palo Alto Networks, Inc.

Prisma Access. Vous pouvez ensuite ajouter toute adresse ajoutée ou modifiée à une liste d'autorisation.

Exemple : exemples de mise à l'échelle des adresses IP publiques (utilisateurs mobiles)

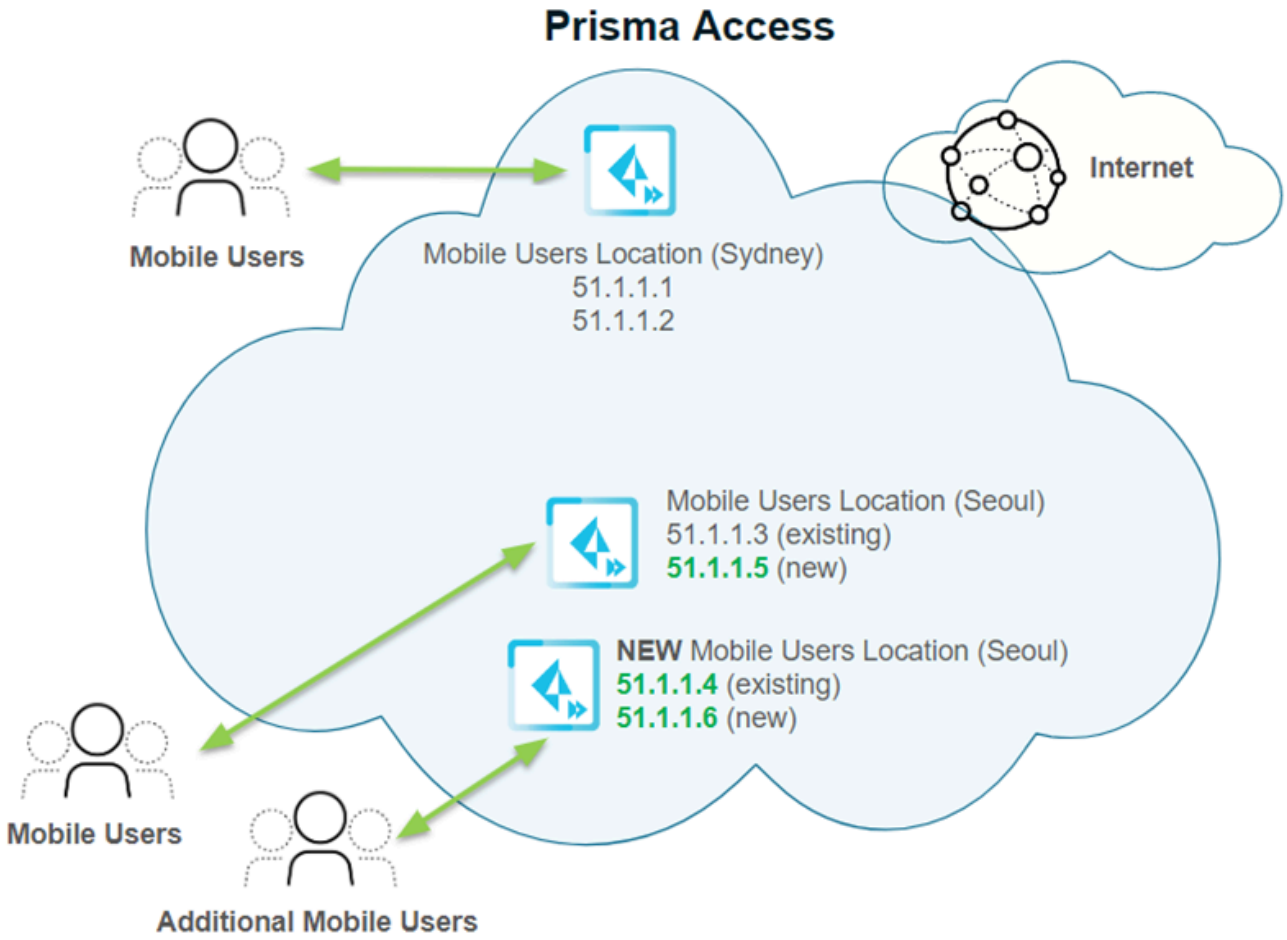
Les exemples suivants illustrent le processus d'allocation d'adresses IP publiques d'un utilisateur mobile que Prisma Access utilise lors d'un événement de mise à l'échelle ou lorsque vous ajoutez un nouvel emplacement.

Dans l'exemple suivant, vous avez spécifié deux emplacements dans la région Asie-Pacifique pour le déploiement d'un nouvel utilisateur mobile : Sydney et Séoul. Chaque emplacement reçoit deux adresses IP de passerelle.



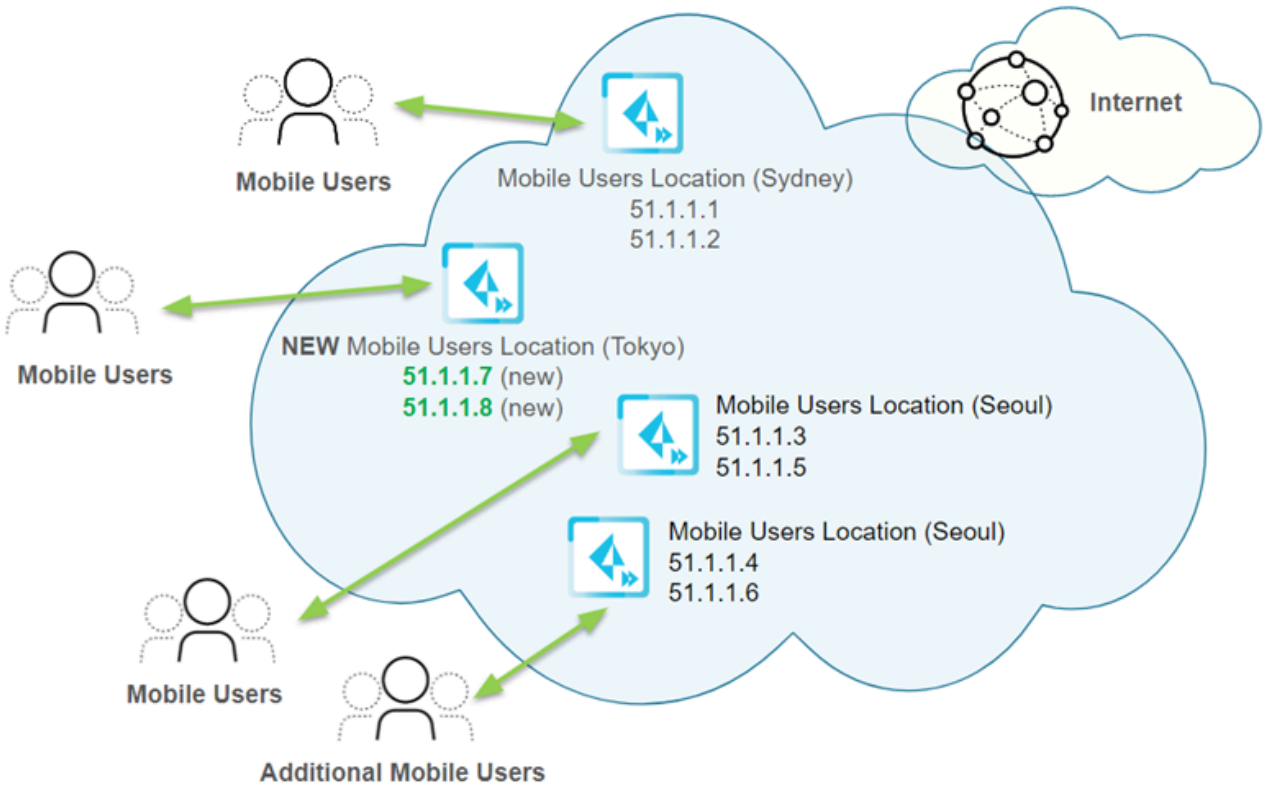
Ensuite, un grand nombre d'utilisateurs se connectent à l'emplacement de Séoul. Pour accommoder ces utilisateurs supplémentaires, Prisma Access ajoute une deuxième passerelle pour l'emplacement de Séoul, prend l'une des adresses de passerelle de la première passerelle de Séoul (51.1.1.4) et l'affecte à la deuxième passerelle de Séoul. Il ajoute ensuite deux adresses IP supplémentaires (51.1.1.5 et 51.1.1.6 dans cet exemple) et les ajoute aux deux passerelles de Séoul.

 ©2025 Palo Alto Networks, Inc.



Ensuite, vous ajoutez un autre emplacement, Tokyo, dans la région Asie-Pacifique. Prisma Access crée deux nouvelles adresses IP pour la nouvelle passerelle (51.1.1.7 et 51.1.1.8).

 ©2025 Palo Alto Networks, Inc.



Chaque fois que vous ajoutez un emplacement ou que vous organisez un événement de mise à l'échelle, vous devez récupérer les nouvelles adresses IP de sortie et de passerelle que Prisma Access a assignées et les ajouter à une liste d'autorisations dans votre réseau. Prisma Access conserve à tout moment deux ensembles d'adresses IP pour toutes les passerelles actives à chaque emplacement.

Allocation d'adresses IP de bouclage (utilisateurs mobiles)

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Les adresses de bouclage sont des adresses IP que Prisma Access utilise pour les requêtes adressées à une source interne et sont attribuées à partir du sous-réseau d'infrastructure. Les adresses IP de bouclage peuvent changer pour les utilisateurs mobiles lors d'une mise à niveau de l'infrastructure ou du plan de données.

Les adresses IP de bouclage ne changent pas pour les connexions aux services ou les connexions aux réseaux distants lors d'une mise à niveau de l'infrastructure ou du plan de données ; seules les adresses IP de bouclage des utilisateurs mobiles peuvent changer.

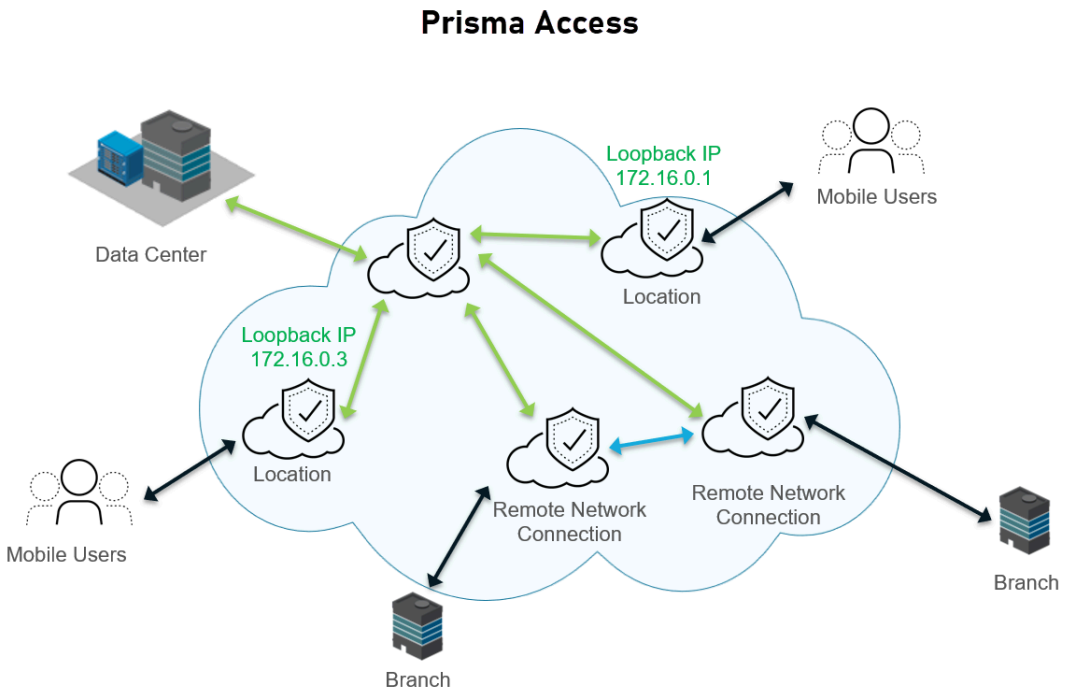
 ©2025 Palo Alto Networks, Inc.

Prisma Access alloue les adresses IP de bouclage à partir du sous-réseau d'infrastructure que vous spécifiez lorsque vous activez l'infrastructure Prisma Access. Vous pouvez ajouter l'intégralité du sous-réseau d'infrastructure à une liste d'autorisation et éviter de devoir prévoir les changements d'adresse IP de bouclage des utilisateurs mobiles lors d'une mise à niveau de l'infrastructure ou du plan de données. Pour trouver le sous-réseau d'infrastructure, sélectionnez :

- Prisma Access (Managed by Strata Cloud Manager) : **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Paramètres d'infrastructure)** et recherchez **Infrastructure Subnet (Sous-réseau d'infrastructure)**
- Prisma Access (Managed by Panorama) : **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Infrastructure (Infrastructure de service)** et recherchez **Infrastructure Subnet (Sous-réseau d'infrastructure)**

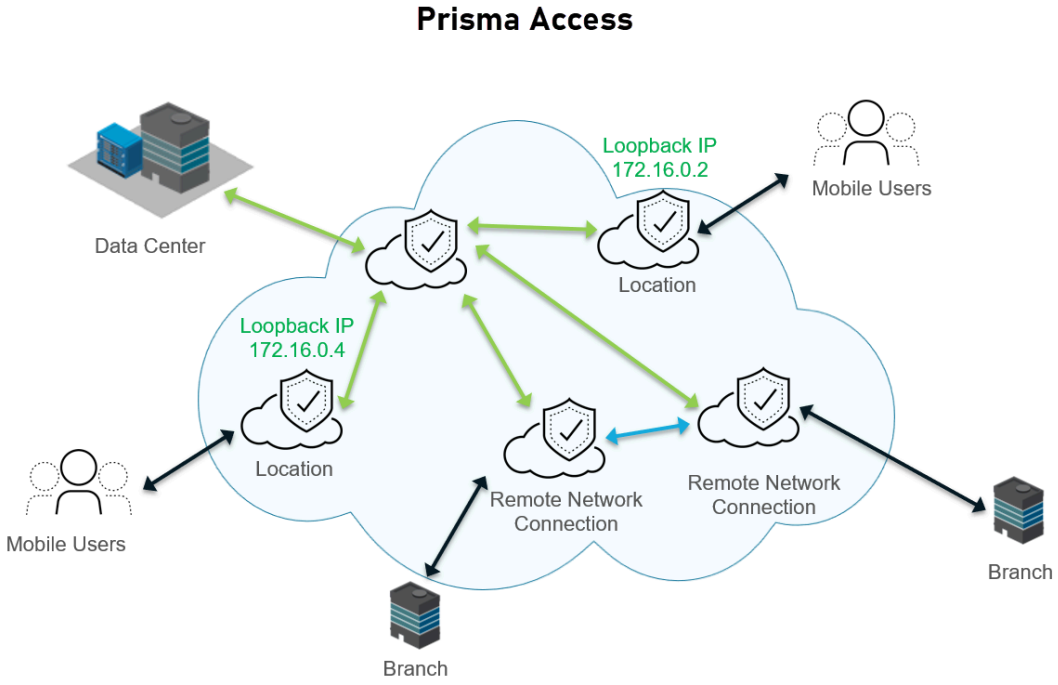
Récupérez ces adresses à l'aide de l'API utilisée pour récupérer les adresses IP publiques et les adresses IP de bouclage.

L'exemple suivant montre un déploiement Prisma Access dont le sous-réseau d'infrastructure utilise l'adresse 172.16.0.0/16. Prisma Access a attribué les adresses IP de bouclage 172.16.0.1 et 172.16.0.3 aux utilisateurs mobiles du sous-réseau d'infrastructure.



Après une mise à niveau de l'infrastructure ou du plan de données (par exemple, dans le cadre de la préparation pour une nouvelle version du plug-in Cloud Services), Prisma Access attribue deux adresses IP différentes aux utilisateurs mobiles du sous-réseau d'infrastructure (l'adresse 172.16.0.1 est remplacée par 172.16.0.2 et l'adresse 172.16.0.3 est remplacée par 172.16.0.4).

 ©2025 Palo Alto Networks, Inc.

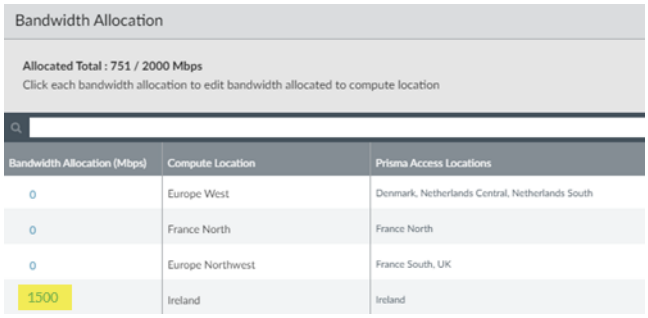


 ©2025 Palo Alto Networks, Inc.

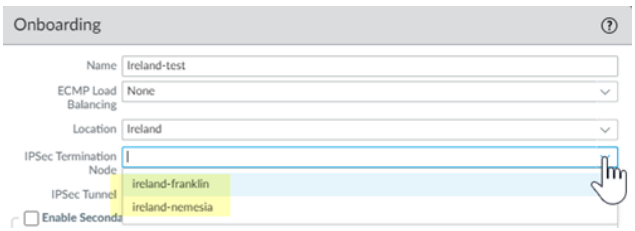
Réseaux distants : Nœuds de terminaison IPSec et Adresses IP de service

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• Licence Prisma Access

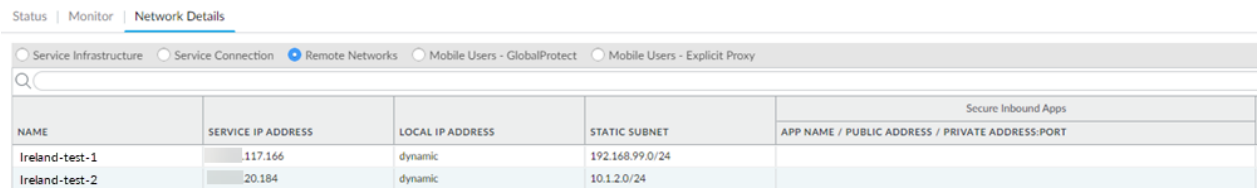
Lorsque vous intégrez un réseau distant, vous l'associez à un *nœud de terminaison IPSec*, et chaque nœud de terminaison IPSec dispose d'une **Service IP Address (Adresse IP de service)** qui lui est associée. Vous utilisez cette adresse comme adresse IP homologue pour votre CPE lorsque vous configurez le tunnel IPSec pour la connexion réseau distante. Chaque nœud de terminaison peut vous fournir jusqu'à 1 000 Mbit/s de bande passante. L'association de plus de 1 000 Mbit/s de bande passante à un emplacement de calcul vous fournit plusieurs **Service IP Address (Adresse IP de service)**.



Lorsque vous intégrez un réseau distant dans un site de calcul en Irlande, vous avez le choix entre deux nœuds de terminaison IPSec, car la bande passante totale est supérieure à 1 000 Mbit/s.



Chaque nœud de terminaison IPSec possède sa propre **Service IP Address (Adresse IP de service)**, comme indiqué dans **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails réseau)** > **Remote Networks (Réseaux distants)**.



 ©2025 Palo Alto Networks, Inc.

Réseaux distants : Modifications de l'adresse IP liées à l'allocation de la bande passante

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Cette section s'applique si vous avez un déploiement hérité Prisma Access qui alloue la bande passante par emplacement. Tous les nouveaux déploiements allouent la bande passante en fonction de l'emplacement de calcul ; pour en savoir plus sur la manière dont Prisma Access attribue ces adresses IP, voir Réseaux distants : Nœuds de terminaison IPSec et Adresses IP de service.

Les adresses IP pour les connexions réseau distantes sont uniques, non partagées et dédiées à votre déploiement Prisma Access. Ces adresses IP ne changent pas lorsque Prisma Access les crée dans le cadre de l'intégration du réseau à distance, et les adresses IP persistent après une mise à niveau. Toutefois, soyez prudent lorsque vous augmentez la bande passante d'une connexion existante, car l'adresse IP d'un réseau distant peut changer si cette augmentation entraîne une augmentation de la bande passante dans un emplacement supérieure à 500 Mbit/s.

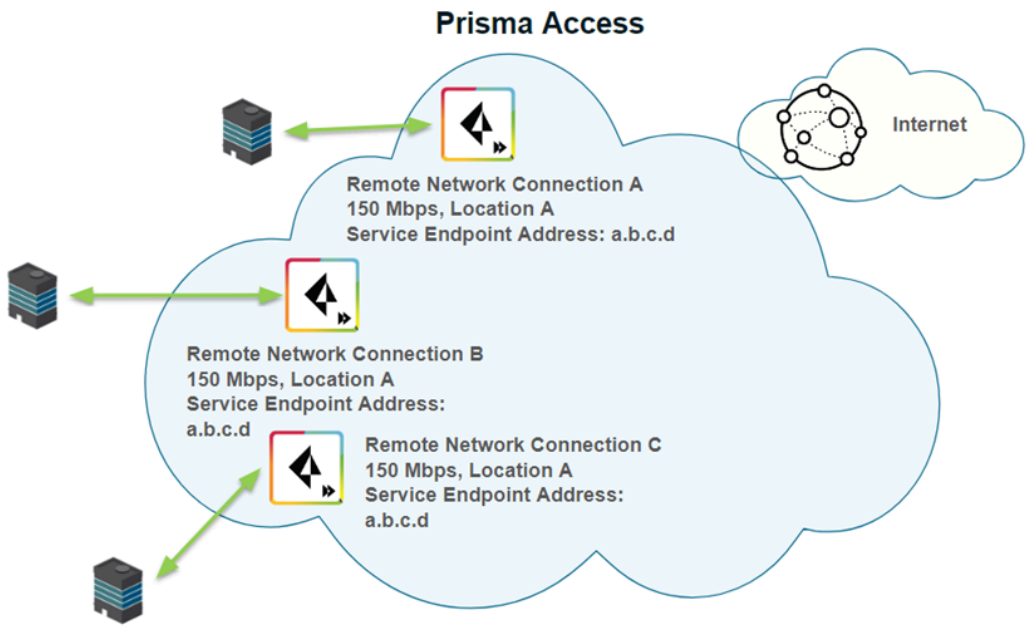
De plus, les adresses IP de sortie peuvent changer si Prisma Access crée un nouvel emplacement Prisma Access de calcul et si vous décidez d'utiliser ce nouvel emplacement de calcul avec les emplacements que vous avez déjà intégrés.

Ces directives de bande passante s'appliquent uniquement lorsque vous mettez à niveau une connexion existante. Une connexion réseau distante unique, même une connexion de 1 000 Mbit/s (Prévisualisation), reçoit toujours une seule **Service IP Address (Adresse IP de service)**, quelle que soit sa taille.

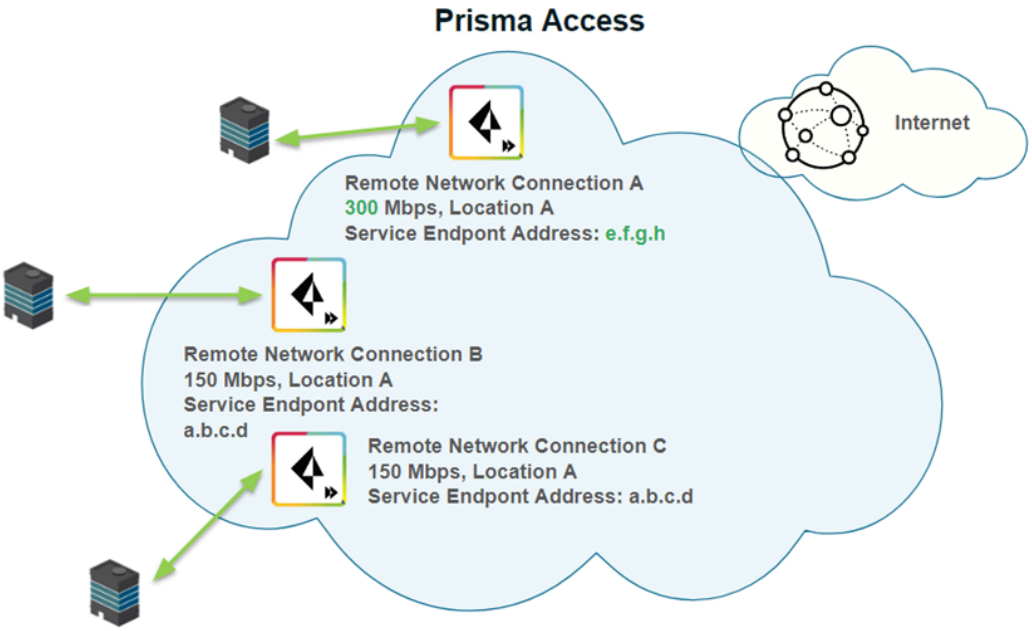
L'option de bande passante de 1 000 Mbit/s est en mode prévisualisation. Le débit pendant la prévisualisation est fourni dans la mesure du possible et les performances réelles varient en fonction de la composition du trafic.

L'exemple suivant montre trois connexions réseau distantes au même emplacement, chacune avec une bande passante de 150 Mbit/s. Étant donné que la bande passante totale est de 500 Mbit/s, Prisma Access attribue une adresse IP unique à toutes les connexions de l'emplacement.

 ©2025 Palo Alto Networks, Inc.



L'exemple suivant montre l'augmentation de la bande passante de la connexion réseau distante A de 150 Mbit/s à 300 Mbit/s. Étant donné que la bande passante totale de toutes les connexions est maintenant supérieure à 500 Mbit/s, Prisma Access attribue une nouvelle adresse IP de service pour la connexion avec la bande passante supplémentaire. Les autres adresses IP de service restent inchangées.



À l'inverse, étant donné quatre réseaux distants avec une bande passante de 100 Mbit/s, si vous augmentez la bande passante de l'un des réseaux distants à 100 Mbit/s, la **Service IP Address (Adresse IP du service)** de ce réseau distant ne change pas, car la bande passante totale est désormais de 500 Mbit/s.

 ©2025 Palo Alto Networks, Inc.

*Si vous réduisez la bande passante d'une connexion réseau distante, la **Service IP Address (Adresse IP du service)** ne change pas.*

Pour trouver les adresses IP de service dans Panorama, sélectionnez l'onglet **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** et cliquez sur le bouton radio **Remote Networks (Réseaux distants)** pour afficher la **Service IP Address (Adresse IP de service)** pour les réseaux distants, ou utilisez le script API.

 ©2025 Palo Alto Networks, Inc.

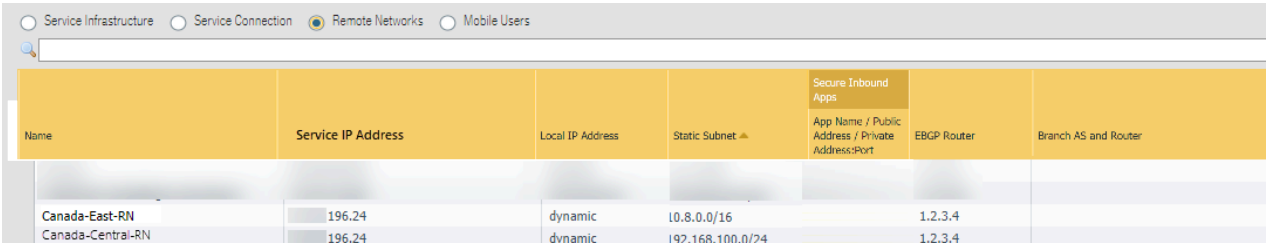
Réseaux distants : Adresse IP de service et allocation d'adresses IP de sortie

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• Licence Prisma Access

Prisma Access dispose de plus de 100 sites disponibles pour accueillir des déploiements dans le monde entier et offrir une expérience localisée. Deux emplacements peuvent être mappés au même , que vous utilisez comme adresse IP homologue lorsque vous configurez le tunnel IPSec pour la connexion réseau distante. Toutefois, les emplacements peuvent utiliser des adresses IP de sortie différentes pour s'assurer que l'utilisateur obtient la langue par défaut correcte pour la région.

Connexions aux services *ne prend pas en charge la localisation linguistique, car la sortie vers Internet n'est pas prise en charge sur les connexions aux services. Prisma Access n'attribue qu'une seule adresse IP de service par connexion aux services, et que cette adresse IP est géographiquement enregistrée dans* l'emplacement de calcul *qui correspond à l'emplacement que vous spécifiez lors de l'intégration.*

L'exemple suivant montre un déploiement client avec deux emplacements de réseau distants déployés au Canada : Centre du Canada et Est du Canada Prisma Access se voient attribué la même **Service IP Address (Adresse IP de service)** vers les deux emplacements. Lorsque vous configurez le tunnel réseau distant, utilisez cette adresse IP en tant qu'adresse IP homologue lorsque vous créez le tunnel IPSec pour la connexion réseau distante.



Cependant, l'Est du Canada utilise une langue par défaut différente (français) que le Centre du Canada (anglais). Pour cette raison, Prisma Access leur attribue différentes adresses IP de sortie. Si vous exécutez le script d'API pour les adresses IP de sortie, vous recevrez deux adresses IP différentes pour ces deux emplacements.

 ©2025 Palo Alto Networks, Inc.

Récupérer les adresses IP pour Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Si vous ajoutez manuellement les adresses IP de votre Prisma Access à une liste d'autorisation dans votre réseau, ou si vous utilisez un script d'automatisation pour appliquer des restrictions basées sur IP afin de limiter l'accès entrant aux applications d'entreprise, vous devez comprendre ce que font ces adresses et pourquoi vous devez les autoriser, ainsi que les tâches que vous effectuez pour les récupérer.

Prisma Access ne provisionne pas ces adresses IP tant que vous n'avez pas terminé votre configuration Prisma Access. Une fois votre déploiement terminé, vous récupérez ces adresses IP à l'aide d'un script API. Le script API utilise une clé API que vous obtenez à partir de Prisma Access UI et un fichier .txt que vous créez qui spécifie les adresses que vous souhaitez récupérer.

Bien que vous n'effectuiez pas ces tâches tant que vous n'avez pas terminé votre configuration Prisma Access, il est utile de comprendre ces concepts à l'avance, afin de comprendre ce qu'il faut faire une fois votre déploiement terminé.

- Strata Cloud Manager
- Panorama

Récupérer les adresses IP de Prisma Access (Strata Cloud Manager)

Prisma Access Adresses IP de l'infrastructure

Le tableau suivant vous fournit une liste des adresses IP que Prisma Access utilise pour chaque type de déploiement, ainsi que le mot-clé que vous utilisez lorsque vous exécutez le script d'API pour récupérer les adresses IP, et si vous devez ou non les ajouter à une liste d'autorisation.

Type de déploiement	Type d'adresse IP	Description
Utilisateur mobile	Prisma Access passerelle (**gp_gateway**)	Récupère les adresses IP de la passerelle. Ajoutez des adresses IP de passerelle et de portail aux listes d'autorisation pour vos déploiements d'utilisateurs mobiles. Les utilisateurs mobiles se connectent à une passerelle Prisma Access pour accéder aux ressources internes ou Internet, telles que les applications SaaS

 ©2025 Palo Alto Networks, Inc.

Type de déploiement	Type d'adresse IP	Description
		ou publiques, auxquelles vous avez donné l'accès.
	Portail Prisma Access (**gp_portal**)	Récupère les adresses IP du portail. Ajoutez des adresses IP de passerelle et de portail aux listes d'autorisation pour vos déploiements d'utilisateurs mobiles. Les utilisateurs mobiles se connectent au portail Prisma Access pour recevoir leur configuration initiale et l'emplacement de la passerelle.
	Adresses IP de bouclage	Cette adresse est l'adresse IP source utilisée par Prisma Access pour les demandes adressées à une source interne, et est attribuée à partir de l'infrastructure. Ajoutez l'adresse IP de bouclage à une liste d'autorisation dans votre réseau pour donner Prisma Access à des ressources internes telles que les serveurs d'authentification RADIUS ou Active Directory. Palo Alto Networks vous recommande d'autoriser toutes les adresses IP de l'ensemble du sous-réseau d'infrastructure de votre réseau, car les adresses de bouclage pour les utilisateurs mobiles peuvent changer.
Utilisateurs mobiles—Proxy explicite	Service de cache d'authentification (ACS)	L'adresse du service Prisma Access qui stocke l'état d'authentification des utilisateurs proxy explicites. Cette adresse n'est utilisée que pour les déploiements d'utilisateurs mobiles (proxy explicite).
	Équilibreur de charge réseau	L'adresse que Prisma Access utilise pour l'équilibreur de charge réseau proxy explicite. Cette adresse n'est utilisée que pour les déploiements d'utilisateurs mobiles (proxy explicite).
Réseau à distance	Adresses IP du réseau distant (**remote_network**)	Comprend les **Service IP Addresses (Adresses IP de service)** que Prisma

 ©2025 Palo Alto Networks, Inc.

Type de déploiement	Type d'adresse IP	Description
		Access assigne pour la connexion réseau à distance Prisma Access et les adresses IP de sortie que Prisma Access utilise pour s'assurer que les utilisateurs du réseau distant obtiennent la langue par défaut correcte pour leur région. Ajoutez ces adresses aux listes d'autorisation de votre réseau pour donner Prisma Access aux ressources Internet.
	Adresses IP de bouclage	Il s'agit de l'adresse IP source utilisée par Prisma Access pour les requêtes adressées à une source interne, et elle est attribuée à partir du sous-réseau d'infrastructure. Ajoutez l'adresse IP de bouclage à une liste d'autorisation pour donner Prisma Access à des ressources internes telles que les serveurs d'authentification RADIUS ou Active Directory.

Exécutez le script API utilisé pour récupérer les adresses IP

Procédez comme suit pour récupérer les adresses IP que Prisma Access utilise dans son infrastructure.

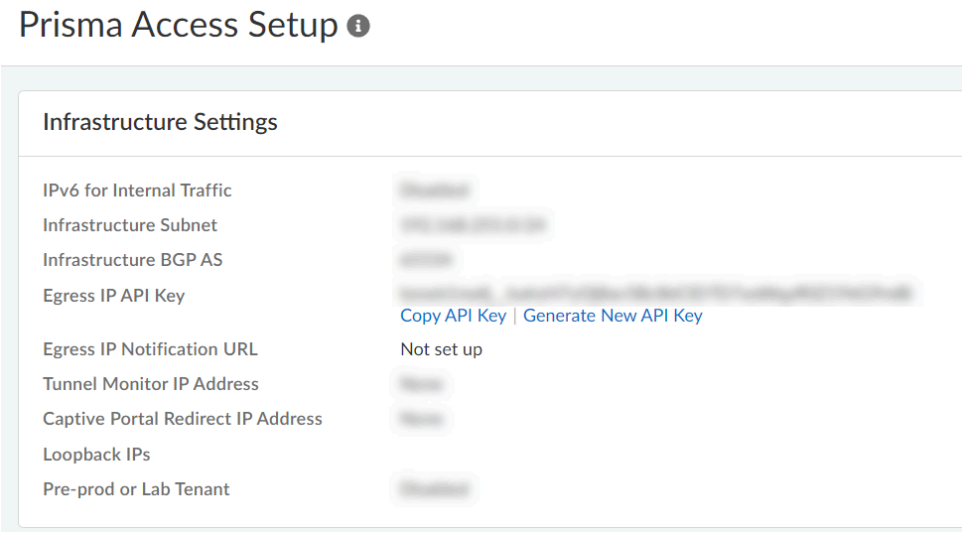
Cette commande ne récupère pas les adresses de bouclage ; pour récupérer les adresses IP de bouclage, utilisez la commande API héritée.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Obtenez la clé API.

Vous avez besoin de cette clé pour vous authentifier pour Prisma Access et récupérer la liste des adresses IP à l'aide de la commande API.

1. Allez à Prisma Access (Managed by Strata Cloud Manager), et sélectionnez **Workflows (Flux de travail)** > **Prisma AccessSetup (Configuration de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Paramètres d'infrastructure)**.
2. Sélectionnez **Generate New API Key (Générer une nouvelle clé API)**.



Si vous avez déjà généré une clé API, la clé actuelle s'affiche. Si vous n'avez pas encore généré de clé ou si vous souhaitez remplacer la clé existante pour répondre à l'audit ou à la vérification de conformité pour la rotation des clés, cliquez sur **Generate New API Key (Générer une nouvelle clé API)** pour une nouvelle clé.

STEP 2 | Créez un fichier .txt et placez les options de commande API dans le fichier.

À l'aide de l'API, la commande à utiliser est un processus en deux étapes. Tout d'abord, vous créez un fichier .txt, en spécifiant les paramètres des adresses IP à récupérer, puis vous enregistrez le fichier dans un dossier accessible à partir de l'emplacement où vous exécutez la commande. Ensuite, vous exécutez l'API et spécifiez le nom et l'emplacement du fichier .txt que vous avez créé dans la commande.

Spécifiez les mots-clés et arguments suivants dans le fichier .txt. Les exemples de cette rubrique utilisent un nom de fichier de **options.txt** mais vous pouvez spécifier n'importe quel nom de fichier, à condition de le référencer dans la commande.

Argument	Choix possibles (Mots clés)	Commentaires
serviceType	**all** **remote_network** **gp_gateway** **gp_portal** **swg_proxy**	**all**—Récupère les adresses IP que vous devez ajouter à une liste d'autorisation pour tous les types de services (réseaux distants, utilisateurs mobiles (passerelles et portails) et Clean Pipe, le cas échéant pour votre déploiement).

 ©2025 Palo Alto Networks, Inc.

Argument	Choix possibles (Mots clés)	Commentaires
	rbi	**remote_network**—Récupère les adresses IP que vous devez ajouter à une liste d'autorisation pour les déploiements de réseau à distance. **gp_gateway**—Récupère les adresses IP de passerelle que vous devez ajouter à une liste d'autorisation pour les déploiements d'utilisateurs mobiles. **gp_portal**—Récupère les adresses IP du portail que vous devez ajouter à une liste d'autorisation pour les déploiements d'utilisateurs mobiles. **swg_proxy**—Récupère les adresses IP de sortie pour chaque emplacement de proxy explicite déployé, le service de cache d'authentification (ACS) et les équilibreurs de charge réseau. **rbi**—Récupère les adresses IP de sortie que vous devez ajouter à une liste d'autorisation pour les déploiements Isolation du navigateur distant (RBI) pour se connecter à des applications SaaS.
addrType	**all** **actif** **service_ip** **auth_cache_service** **network_load_balancer**	**all (tout)** ou **active (actif)**—Récupère toutes les adresses IP que vous devez ajouter à une liste d'autorisation. Cette API ne récupère pas les adresses IP de bouclage. Pour récupérer les adresses IP de bouclage, utilisez la commande API héritée. **service_ip**—Récupère la **Service IP Address (Adresse IP du service)** que vous utilisez comme adresse IP homologue lorsque vous configurez le tunnel IPSec pour la connexion réseau à distance. **auth_cache_service**—Récupère l'adresse IP de l'ACS proxy explicite (applicable aux utilisateurs mobiles—déploiements de proxy explicite uniquement). **network_load_balancer**—Récupère l'adresse IP de l'équilibreur de charge du réseau proxy explicite (applicable aux utilisateurs mobiles—déploiements de proxy explicite uniquement).

 ©2025 Palo Alto Networks, Inc.

Argument	Choix possibles (Mots clés)	Commentaires
actionType	**pre_allocate**	Déploiements d'utilisateurs mobiles uniquement—Un **actionType** de **pre_allocate** vous permet de récupérer des adresses IP ou des sous-réseaux pour les passerelles et portails Prisma Access pour les déploiements d'utilisateurs mobiles. Utilisez ceci avec un **serviceType** de **gp_gateway** pour récupérer les adresses IP de passerelle pré-allouées et un **serviceType** de **gp_portal** pour récupérer les adresses IP de passerelle préallouées. La récupération des adresses IP préallouées vous permet d'ajouter les adresses IP de la passerelle et du portail aux listes d'autorisation de votre organisation avant d'intégrer les emplacements des utilisateurs mobiles, ce qui permet aux utilisateurs mobiles d'accéder aux applications SaaS externes immédiatement après l'intégration des emplacements.
location	**all** **deployed**	**all (tout)**—Récupère les adresses IP de tous les emplacements. Pour les déploiements d'utilisateurs mobiles, ce mot-clé récupère les adresses IP des emplacements que vous avez ajoutés lors de l'intégration et des emplacements que vous n'avez pas ajoutés. **deployed (déployé)**—Récupère les adresses IP dans tous les emplacements que vous avez ajoutés lors de l'intégration des utilisateurs mobiles. Ce mot-clé s'applique uniquement aux déploiements d'utilisateurs mobiles. Prisma Access associe des adresses IP à chaque emplacement d'utilisateur mobile lors de l'approvisionnement, même si vous n'avez pas sélectionné cet emplacement lors de l'intégration d'un utilisateur mobile. Si vous spécifiez **all (tout)**, la commande API récupère les adresses IP de tous les emplacements des utilisateurs mobiles, y compris ceux que vous n'avez pas sélectionnés pour le déploiement. Si vous spécifiez **deployed (déployé)**, la commande API récupère uniquement les adresses IP des

 ©2025 Palo Alto Networks, Inc.

Argument	Choix possibles (Mots clés)	Commentaires
		emplacements que vous avez sélectionnés lors de l'intégration.

Spécifiez les options dans le fichier .txt au format suivant :

```
 { "serviceType": "service-type", "addrType": "address-type",
"location": "location" }
```

STEP 3 | Saisissez la commande suivante pour récupérer les adresses IP :

- Pour utiliser la nouvelle API introduite dans Prisma Access 2.1, entrez la commande suivante :

```
  curl -X POST --data @option.txt -H header-api-key:Current-
API-Key "https://api.prod.datapath.prismaaccess.com/
getPrismaAccessIP/v2"
```

  Depuis mai 2023, certains déploiements gérés dans le Cloud utilisent https://api.prod6.datapath.prismaaccess.com/getPrismaAccessIP/v2 (notez le `prod6` dans l'URL au lieu de `prod`).

- Pour utiliser l'API héritée, entrez la commande suivante. Cette commande utilise un point de terminaison d'API hérité qui sera obsolète en mai 2022 :

```
  curl -X POST --data @option.txt -k -H header-api-key:Current-
API-Key "https://api.gpcloudservice.com/getPrismaAccessIP/v2"
```

Où *option.txt* est le fichier .txt que vous avez créé lors d'une étape précédente et *Current-API-Key* est la Prisma Access Clé API.

Par exemple, étant donné un nom de fichier .txt de **option.txt** et une clé API de **12345abcde**, utilisez la commande API suivante pour récupérer l'adresse IP publique de tous les emplacements :

```
 curl -X POST --data @option.txt -H header-api-key:12345abcde
"https://api.prod.datapath.prismaaccess.com/getPrismaAccessIP/v2"
```

La commande API peut renvoyer une grande quantité d'informations. Pour rendre la sortie plus lisible, si Python est installé, vous pouvez ajouter `| python -m json.tool` à la fin de la commande cURL.

La commande API renvoie les adresses au format suivant :

```
{ "result": [ { "address_details": [ { "address": "1.2.3.4"
"allow_listed": false "addressType": "address-type" "serviceType":
```

 ©2025 Palo Alto Networks, Inc.

```
 "service-type" } ], "addresses": [ "1.2.3.4" ] "zone": "zone-
name", "zone_subnet": [zone-subnet ] }, "status": "success"
```

Où :

- **address_details** affiche les détails de l'adresse de chaque emplacement.
  - **serviceType** affiche le type d'adresse IP (réseau distant (**remote_network**), passerelle d'accès Prisma (**gp_gateway**), Prisma Access portail (**gp_portal**), Clean Pipe (**clean_pipe**), ou Isolation du navigateur distant (**rbi**).
  - **addressType** spécifie le type d'adresse spécifié avec le mot clé `addrType` (soit **active (actif)** soit **pre-allocated (pré-alloué)** si vous pré-allouez des adresses IP pour les emplacements des utilisateurs mobiles).
  - **address (adresse)** affiche l'adresse IP que vous devez ajouter à vos listes d'autorisation.

    Si l'API renvoie plusieurs adresses IP, Prisma Access résume les adresses IP dans le champ **addresses (adresses)**.
- **addresses (adresses)** répertorie toutes les adresses IP de l'emplacement que vous devez ajouter à vos listes d'autorisation.
- **zone** est l'emplacement Prisma Access associé aux adresses IP.
- **zone_subnet** est le sous-réseau des passerelles et des portails pour les utilisateurs mobiles. Prisma Access fournit également ce sous-réseau si vous pré-allouez des adresses IP pour les emplacements des utilisateurs mobiles.

En cas de problème avec les options du fichier .txt, l'API renvoie une erreur similaire à la suivante :

```
 {"status": "error","result": "Invalid json format in the request.
trace_id: xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx "}
```

STEP 4 | Mettez à jour les listes d'autorisation sur vos serveurs locaux ou les règles de stratégie d'application SaaS avec les adresses IP que vous avez récupérées.

Exemples de commandes API

Utilisez les exemples suivants lorsque vous entrez des mots-clés et des arguments dans le fichier .txt pour la commande API. Pour modifier la sortie de la commande, modifiez les options dans le fichier .txt ; la commande elle-même ne change pas.

Récupérer ces adresses IP	Spécifiez ces paramètres dans le fichier .txt	Commentaires
Adresses IP des utilisateurs mobiles		
Toutes les adresses IP des utilisateurs mobiles	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "all" }`	Un *addrType all* signifie que Prisma Access récupère toutes les adresses IP de la passerelle d'utilisateur mobile.

 ©2025 Palo Alto Networks, Inc.

Récupérer ces adresses IP	Spécifiez ces paramètres dans le fichier .txt	Commentaires
		Un *location all* signifie que Prisma Access récupère les adresses IP de tous les emplacements disponibles, y compris ceux que vous n'avez pas intégrés. Prisma Access réserve les adresses IP d'emplacements non intégrés afin que vous puissiez les ajouter à vos listes d'autorisation avant de les intégrer.
Adresses IP pour les emplacements des utilisateurs mobiles intégrés	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "deployed" }`	Un *location deployed* signifie que Prisma Access récupère uniquement les adresses IP des emplacements que vous avez sélectionnés lors de l'intégration des utilisateurs mobiles.
Toutes les adresses IP actives pour les emplacements des utilisateurs mobiles intégrés	`{ "serviceType": "gp_gateway", "addrType": "active", "location": "deployed" }`	Un *addrType active* signifie que Prisma Access récupère uniquement les adresses IP des emplacements que vous avez intégrés.
Adresses IP du réseau distant		
Récupérer toutes les adresses IP du réseau distant	`{ "serviceType": "remote_network", "addrType": "all", "location": "all" }`	Cette commande récupère les adresses IP publiques et de sortie des réseaux distants que vous avez intégrés. N'utilisez pas un *location deployed*. Vous pouvez utiliser un *addrType active*, mais il récupère les mêmes adresses que si vous aviez spécifié un *addrType all*.
Adresses IP de proxy explicite		
Récupérer les adresses IP ACS des emplacements déployés	`{ "serviceType": "swg_proxy", "location": "deployed", "addrType": "auth_cache_service" }`	Cette commande récupère l'adresse IP ACS pour votre déploiement de proxy explicite. La saisie d'un *addrType all* récupère tous les types d'adresses (adresses IP de l'ACS et de l'équilibreur de charge réseau).

©2025 Palo Alto Networks, Inc.

Récupérer ces adresses IP	Spécifiez ces paramètres dans le fichier .txt	Commentaires
Adresses IP d'isolation du navigateur distant		
Récupérer les adresses IP d'isolation du navigateur à distance (Remote Browser Isolation, RBI) des emplacements déployés	`{ "serviceType": "rbi", "location": "all", "addrType": "all" }`	Cette commande récupère les adresses IP de sortie pour chaque emplacement RBI déployé. Vous pouvez ajouter ces adresses IP à une liste d'autorisation pour vous connecter aux applications SaaS.

Scripts hérités utilisés pour récupérer les adresses IP et de bouclage

Le tableau suivant présente les mots-clés et les paramètres disponibles dans les scripts d'API hérités utilisés avec Prisma Accesset fournit des informations et des recommandations sur l'API à utiliser pour le type de déploiement dont vous disposez.

Ces commandes héritées récupèrent deux types d'adresses IP, *public IP* et *egress IP*. Nous vous fournissons deux commandes d'API héritées différentes afin que vous puissiez récupérer toutes les adresses IP que vous devez ajouter à une liste d'autorisation.

- Une *public IP address* est l'adresse IP source que Prisma Access utilise pour les requêtes adressées à une source basée sur Internet. Ajoutez l'adresse IP publique à une liste d'autorisation dans votre réseau pour donner Prisma Access à des ressources Internet telles que des applications SaaS ou des applications partenaires accessibles au public.

  Les déploiements d'utilisateurs mobiles, de réseaux distants et Clean Pipe utilisent des adresses IP publiques.
- Une *egress IP address* est une adresse IP que Prisma Access utilise pour le trafic sortant vers Internet, et vous devez également ajouter ces adresses à une liste d'autorisation pour permettre à Prisma Access d'accéder aux ressources Internet.

  Entre autres fins, Prisma Access utilise les adresses IP de sortie afin que les utilisateurs reçoivent les pages Web dans la langue qu'ils attendent d'un emplacement Prisma Access. Tous

 ©2025 Palo Alto Networks, Inc.

les emplacements ont des adresses IP publiques ; cependant, tous les emplacements n'ont pas d'adresses IP de sortie. Les emplacements suivants n'utilisent pas d'adresses IP de sortie :

- Bahreïn
- Belgique
- Nord de la France
- Sud de la France
- Hong Kong
- Irlande
- Corée du Sud
- Taïwan
- Royaume-Uni

Les déploiements d'utilisateurs mobiles, de réseaux distants et Clean Pipe utilisent des adresses IP de sortie.

Commandes utilisées dans les déploiements d'utilisateurs mobiles	
Nom de la commande	**Commentaires**
Commande **get_egress_ip_all=yes** `curl -k -H header-api-key:`*Current-API-Key*`"https://api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes`	Cette commande récupère toutes les adresses IP que vous ajoutez à une liste d'autorisation pour donner Prisma Access à des ressources Internet telles que des applications SaaS ou des applications partenaires accessibles au public. Cette commande comporte les contraintes suivantes : • Cette commande permet de récupérer un grand nombre d'adresses (plus de 200). Si votre entreprise ne peut pas ajouter ce nombre d'adresses IP à une liste d'autorisation, vous pouvez utiliser les mots-clés *gpcs_gp_gw* et *gpcs_gp_portal* pour récupérer uniquement les adresses IP que vous utilisez actuellement ; cependant, vous devrez réexécuter ces commandes chaque fois que vous ajoutez un emplacement. De plus, si un événement de mise à l'échelle se produit, vous devrez ajouter les nouvelles adresses IP à une liste d'autorisation. • Prisma Access ne répertorie pas les emplacements associés à ces adresses IP ; par conséquent, nous vous recommandons d'ajouter toutes les adresses IP renvoyées avec cette commande à une liste d'autorisation. • Cette commande ne vous donne pas d'adresses de bouclage.
Mots-clés **gpcs_gp_gw** et **gpcs_gp_portal**	Utilisez cette commande si votre déploiement limite le nombre d'adresses IP que vous pouvez ajouter à une liste d'autorisation. Ajoutez toutes les adresses IP renvoyées

 ©2025 Palo Alto Networks, Inc.

Commandes utilisées dans les déploiements d'utilisateurs mobiles	
Nom de la commande	**Commentaires**
`curl -k -H header-api-key:`*Current-API-Key*`"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_gp_gw | gpcs_gp_portal&addrType=public_ip | egress_ip_list | loopback_ip"`	avec cette commande à une liste d'autorisation dans votre réseau. Vous pouvez également récupérer les adresses IP de bouclage à l'aide de cette commande.

Commandes utilisées dans les déploiements de réseaux distants	
Nom de la commande	**Commentaires**
Mot clé **gpcs_remote_network** `curl -k -H header-api-key:`*Current-API-Key*`"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_remote_network&addrType=public_ip | egress_ip_list | loopback_ip"`	Utilisez cette commande pour trouver les adresses IP que vous devez ajouter à une liste d'autorisation pour les déploiements de réseaux distants. Vous pouvez également utiliser cette commande pour trouver les adresses IP de sortie pour les déploiements de réseaux distants ; les adresses de sortie et IP peuvent être différentes dans certaines situations.

Commandes utilisées dans les déploiements Clean Pipe	
Nom de la commande	**Commentaires**
Mot clé **gpcs_clean_pipe** `curl -k -H header-api-key:`*Current-API-Key*`"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_clean_pipe&addrType=public_ip | egress_ip_list | loopback_ip"`	Utilisez cette commande pour rechercher les adresses IP que vous devez ajouter à une liste d'autorisation pour les déploiements Clean Pipe.

Récupérez des adresses IP publiques et de sortie pour les déploiements d'utilisateurs mobiles

Ce script hérité a été remplacé par un par un script API plus récent. Palo Alto Networks vous recommande d'utiliser le script le plus récent pour récupérer toutes les adresses IP, à l'exception des adresses de bouclage.

Si vous ajoutez des adresses IP publiques à des listes d'autorisation pour permettre aux utilisateurs mobiles d'accéder à des applications SaaS ou publiques, Prisma Access fournit deux

 ©2025 Palo Alto Networks, Inc.

adresses IP pour chaque adresse IP de passerelle et de portail afin qu'une adresse IP puisse être utilisée lors d'une mise à l'échelle ou d'un autre événement. Vous pouvez ajouter cet ensemble d'adresses IP à une liste d'autorisations avant qu'elles ne soient utilisées, ce qui permet d'éviter tout problème avec les utilisateurs mobiles pouvant accéder aux applications SaaS ou publiques lors d'un événement de mise à l'échelle.

Récupérez ces nouvelles adresses en effectuant la tâche suivante :

STEP 1 | Obtenez la clé API en sélectionnant **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Paramètres d'infrastructure)** > **Generate New API Key (Générer une nouvelle clé API)**.

Vous avez besoin de cette clé pour vous authentifier Prisma Access et récupérer la liste des adresses IP à l'aide de la commande cURL indiquée ci-dessous. Seul un administrateur ou un super-utilisateur Panorama peut générer cette clé API ou y accéder.

STEP 2 | Entrez la commande suivante pour récupérer les adresses IP publiques de l'utilisateur mobile :

```
  curl -k -H header-api-key:Current-API-Key "https://
api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes"
```

Où *Current-API-Key* est la clé API Prisma Access.

Par exemple, étant donné une clé API de **12345abcde**, utilisez la commande API suivante pour récupérer l'adresse IP publique de tous les emplacements :

```
  curl -k -H header-api-key:12345abcde "https://
api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes"
```

Récupérer les adresses IP publiques, de bouclage et de sortie

Pour récupérer des adresses IP publiques, de bouclage et de sortie, procédez comme suit.

STEP 1 | Récupérez les adresses IP publiques, les adresses IP de bouclage ou les deux pour Prisma Access.

Utilisez la clé API et l'URL du point de terminaison d'API manuellement ou dans un script d'automatisation :

```
 header-api-key :Current API Key "https://api.gpcloudservice.com/
getAddrList/latest?fwType=$fwType&addrType=$addrType"
```

Où vous devez remplacer Current API Key par votre clé API et utiliser un ou les deux mots-clés et arguments suivants :

Mot clé	Description
fwType mot clé	

 ©2025 Palo Alto Networks, Inc.

Mot clé	Description
gpcs_gp_gw	Récupère Prisma Access les adresses IP de passerelle (pour les déploiements d'utilisateurs mobiles).
gpcs_gp_portal	Récupère Prisma Access les adresses IP du portail (pour les déploiements d'utilisateurs mobiles).
gpcs_remote_network	Récupère Prisma Access les adresses IP du réseau distant (pour les déploiements de réseaux distants).
gpcs_clean_pipe	Récupère Prisma Access les adresses IP Clean Pipe.
addrType mot clé	
public_ip	Récupère les adresses IP source que Prisma Access utilise pour les requêtes adressées à une source Internet. Pour les emplacements des utilisateurs mobiles, Prisma Access répertorie les adresses IP par emplacement. Pour les réseaux distants, Prisma Access répertorie les adresses IP par nom de réseau distant.
egress_ip_list	Récupère les adresses IP que Prisma Access utilise avec des adresses IP publiques pour le trafic sortant supplémentaire vers Internet. Pour les emplacements des utilisateurs mobiles, Prisma Access répertorie les adresses IP par emplacement. Pour les réseaux distants, Prisma Access répertorie les adresses IP par nom de réseau distant.
loopback_ip	Récupère les adresses IP sources utilisées par Prisma Access pour les requêtes adressées à une source interne (par exemple, un serveur RADIUS ou Active Directory) et est attribué à partir du sous-réseau d'infrastructure.

Si vous ne spécifiez pas de mot clé, Prisma Access récupère toutes les adresses IP.

Par exemple, vous pouvez essayer la commande cURL suivante pour récupérer manuellement la liste des adresses IP publiques de tous les réseaux distants :

```
curl -k -H clé-api-en-
tête :1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7
 "https://api.gpcloudservice.com/getAddrList/latest?
fwType=gpcs_remote_network&addrType=public_ip"
```

Ou utilisez un simple script python pour récupérer la liste de toutes les adresses IP, par exemple :

```
  #!/usr/bin/python import subprocess import json api_key =
 '1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7' # Replace
 with your key api_end_point = 'https://api.gpcloudservice.com/
```

 ©2025 Palo Alto Networks, Inc.

```
getAddrList/latest' # This call retrieves IP addresses
 for all your Prisma Access firewalls args = ['curl', '-
k', '-H', 'header-api-key:' + api_key, api_end_point] p =
 subprocess.Popen(args, stdout=subprocess.PIPE) output =
 p.communicate() dout = json.loads(output[0]) addrStrList
 = dout['result']['addrList'] addrList = [] for addr_str
 in addrStrList: addrList.append(addr_str.split(":")[1])
 print(addrList)
```

STEP 2 | Mettez à jour les listes d'autorisation sur vos serveurs locaux ou les règles de stratégie d'application SaaS avec les adresses IP que vous avez récupérées.

Pré-allouer des adresses IP pour les emplacements des utilisateurs mobiles

Prisma Access utilise les adresses IP de la passerelle et du portail pour les déploiements d'utilisateurs mobiles—GlobalProtect, ainsi que pour le service de cache d'authentification (ACS) et les adresses IP de l'équilibreur de charge réseau pour les utilisateurs mobiles—Proxy explicite. Les adresses IP des utilisateurs mobiles—GlobalProtect sont appelées *egress IP addresses*. Si vous devez pré-allouer des adresses IP d'utilisateurs mobiles avant d'intégrer l'emplacement (par exemple, si votre organisation doit ajouter les adresses IP pour les déploiements des utilisateurs mobiles–GlobalProtect dans les listes d'autorisation pour permettre aux utilisateurs mobiles d'accéder à des applications SaaS externes), vous pouvez exécuter un script API pour que Prisma Access pré-alloue ces adresses IP à un emplacement à l'avance, avant de l'intégrer. Vous pouvez ensuite ajouter les adresses IP de sortie de l'emplacement aux listes d'autorisation de votre organisation avant d'intégrer l'emplacement.

La réponse de l'API inclut également les sous-réseaux du pool d'adresses IP publiques pour les adresses IP de sortie de l'emplacement demandé. Les adresses IP de sortie de tous les emplacements que vous ajoutez font partie de ce sous-réseau. L'ajout des sous-réseaux à vos listes d'autorisation permet d'ajouter des emplacements futurs sans autre modification de la liste d'autorisation.

Prisma Access ne pré-alloue pas vos adresses IP et sous-réseaux, sauf si vous les demandez à l'aide du script API. Une fois que vous avez exécuté le script de pré-allocation, ils ont une période de validité de 90 jours. Ces adresses IP et sous-réseaux sont uniques, non partagés et dédiés à votre déploiement Prisma Access pendant la période de validité. Vous devez intégrer vos emplacements avant la fin de la période de validité, sinon vous perdez les adresses ; pour trouver la période de validité à tout moment, exécutez le script API.

Palo Alto Networks vous recommande de ne pré-allouer des adresses IP qu'aux emplacements que vous souhaitez intégrer ultérieurement.

Pour pré-allouer des adresses IP, effectuez la tâche suivante.

STEP 1 | Récupérez la Prisma Access clé API.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Préallouez les adresses IP de sortie de l'utilisateur mobile en créant un fichier .txt et en spécifiant les options suivantes dans le fichier .txt que vous créez.

Entrez le texte suivant dans le fichier .txt :

- **Utilisateurs mobiles—Déploiements GlobalProtect :**

```
 { "actionType": "pre_allocate", "serviceType": "gp_gateway",
"location": ["location"] }
```

- **Utilisateurs mobiles—Déploiements de proxy explicite :**

```
{ "actionType": "pre_allocate", "serviceType": "swg_proxy",
 "location": ["location"]}
```

Où *location* est l'emplacement Prisma Access où vous souhaitez pré-allouer les adresses IP.

Entrez un maximum de 12 emplacements. La saisie de plus de 12 emplacements peut entraîner des erreurs de délai d'expiration lorsque Prisma Access récupère les adresses IP pré-allouées.

STEP 3 | Entrez cette commande CURL.

STEP 4 | Récupérez les adresses IP et les sous-réseaux que vous avez demandés, y compris leur période de validité, en rouvrant le fichier .txt, en supprimant les informations existantes et en le modifiant.

- **Utilisateurs mobiles—Déploiements GlobalProtect :**
  - Pour demander à Prisma Access de récupérer toutes les adresses IP pré-allouées, entrez le texte suivant dans le fichier .txt.

```
 { "serviceType": "all", "addrType": "pre_allocated",
"location": "all" }
```

  - Pour demander à Prisma Access de récupérer toutes les adresses IP pré-allouées pour Prisma Access les passerelles pour un emplacement donné, entrez les mêmes informations dans le fichier .txt mais remplacez-les par « `tous` » avec « `gp_gateway` » dans le fichier .txt.
  - Pour demander à Prisma Access de récupérer toutes les adresses IP pré-allouées pour Prisma Access les portails pour un emplacement donné, entrez les mêmes informations

 ©2025 Palo Alto Networks, Inc.

dans le fichier .txt mais remplacez-les par « `tous` » avec « `gp_portal` » dans le fichier .txt.

- **Utilisateurs mobiles—Déploiements de proxy explicite :**

  Pour demander que Prisma Access pré-alloue toutes les adresses IP que vous devez ajouter aux listes d'autorisation pour un déploiement de proxy explicite, entrez le texte suivant dans le fichier .txt.

```
{ "actionType": "pre_allocate", "serviceType": "swg_proxy",
 "location": ["all"] }
```

Palo Alto Networks vous recommande d'entrer `all` afin que vous puissiez récupérer toutes les adresses IP de sortie pré-allouées requises à ajouter à vos listes d'autorisation.

Pour les déploiements Utilisateurs mobiles—GlobalProtect, la commande API peut renvoyer une grande quantité d'informations. Pour rendre la sortie plus lisible, si Python est installé, vous pouvez ajouter `| python -m json.tool` *à la fin de la commande cURL.*

STEP 5 | Entrez à nouveau cette commande CURL pour récupérer les adresses pré-allouées.

Prisma Access renvoie les informations au format suivant :

```
    "result": [ { "zone": "prisma-access-zone1", "addresses":
 [ ["ip-address1","ip-address2"] "zone_subnet" : [subnet-and-
mask1","subnet-and-mask2"] "address_details":[ {"address":"ip-
address1", "service_type":"service-type", "addressType":"pre-
allocated", "expiring_in" : "validity-period" }, {"address":"ip-
address2", "service_type":"gp_gateway", "addressType":"pre-
allocated", "validity_period_remaining" : "90 days" } , },
```

Où les variables représentent la sortie de commande API suivante :

Variable	Explication
prisma-access-zone1	L'emplacement Prisma Access pour lequel des adresses IP pré-allouées ont été récupérées.
ip-address1 et *ip-address2*	Les adresses IP de sortie que Prisma Access a pré-alloué pour l'emplacement spécifié. Prisma Access récupère deux adresses IP pour chaque emplacement ; vous devez ajouter ces deux adresses IP à vos listes d'autorisation.
subnet-and-mask1 et *subnet-and-mask2*	Les sous-réseaux que Prisma Access a pré-alloué et réservé pour les adresses IP de sortie dans votre déploiement.
service-type	Le type de l'adresse IP de sortie pré-allouée (soit `gp_portal` pour un Prisma Access portail

 ©2025 Palo Alto Networks, Inc.

Variable	Explication
	ou `gp_gateway` pour une Prisma Access passerelle).
validity-period	Le temps restant, en jours, pendant lequel l'adresse IP pré-allouée est valide. Intégrez l'emplacement de votre utilisateur mobile avant la fin de la période de validité des adresses IP. Si les adresses IP pré-allouées expirent, vous pouvez réexécuter le script API pour récupérer un autre ensemble d'adresses IP pré-allouées.

Vous pouvez recevoir une erreur si vous tentez de pré-allouer des adresses IP pour des emplacements qui répondent à l'un des critères suivants :

- Vous avez déjà intégré l'emplacement.
- Vous avez intégré, puis supprimé l'emplacement.

  Dans ce cas, entrez le texte suivant dans le fichier .txt pour récupérer les adresses IP Utilisateurs mobiles—GlobalProtect de l'emplacement :

```
 { "serviceType": "gp_gateway", "addrType": "all", "location":
"all" }
```

- Vous avez atteint le nombre maximal d'emplacements d'utilisateurs mobiles autorisé par votre licence et vous ne pouvez plus ajouter d'emplacements.
- Vous avez mal saisi le nom de l'emplacement.
- Vous avez saisi un **serviceType** autre que **gp_gateway**.
- vous avez saisi un **actionType** autre que **pre_allocate**.

Configurer Prisma Access Notifications de changement d'adresse IP

Pour être informé des modifications d'adresse IP publique pour les réseaux distants et des modifications d'adresse IP de bouclage pour les connexions aux services, les connexions réseau distantes et les utilisateurs mobiles, vous pouvez spécifier une URL à laquelle vous pouvez être alerté d'une modification. Prisma Access utilise une requête HTTP POST pour envoyer la notification. Cette requête POST inclut les données de notification suivantes au format JSON :

```
 {"addrType": "public_ip", "addrChangeType": "add", "utc_timestamp":
"2019-01-31 23:08:19.383894", "text": "Address List Change
Notification"}
```

```
 {"addrType": "public_ip", "addrChangeType": "delete",
"utc_timestamp": "2019-01-31 23:13:35.882151", "text": "Address List
Change Notification"}
```

 ©2025 Palo Alto Networks, Inc.

```
 {"addrType": "loopback_ip", "addrChangeType": "update",
"utc_timestamp": "2019-01-31 23:29:27.100329", "text": "2018-05-11
23:29:27.100329"}
```

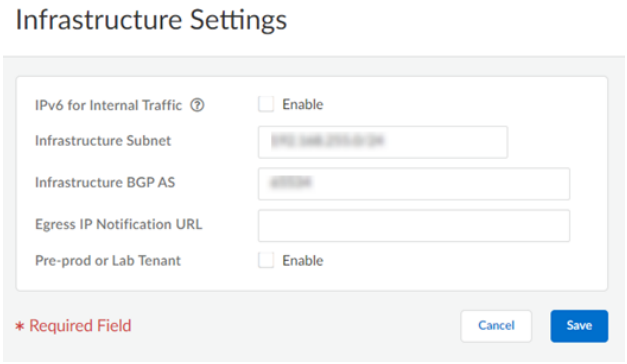
Lorsque vous recevez une notification, vous devez suivre un processus en deux étapes. Tout d'abord, vous devez manuellement ou programmatiquement récupérer les adresses IP ou de bouclage. Ensuite, vous devez mettre à jour les adresses IP dans la liste d'autorisation appropriée de votre organisation pour garantir que les utilisateurs ne subissent aucune interruption de service.

Prisma Access envoie cette notification quelques secondes avant que la nouvelle adresse IP ne devienne active. Nous vous recommandons d'utiliser des scripts d'automatisation pour récupérer et ajouter les nouvelles adresses IP à une liste d'autorisation dans votre réseau.

Pour ajouter une URL de notification d'adresse IP, complétez la tâche suivante.

STEP 1 | Allez à **Workflows (Flux de travail)** > **Prisma AccessSetup (Configuration de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Paramètres d'infrastructure)**.

STEP 2 | Ajoutez une **Egress IP Notification URL (URL de notification IP de sortie)** où vous pouvez être informé des changements d'adresse IP dans votre infrastructure Prisma Access.



Vous pouvez spécifier une adresse IP ou un FQDN vers un service Web HTTP ou HTTPS qui écoute les notifications de changement. Prisma Access envoie ces notifications depuis Internet en utilisant une adresse IP publique.

Vous ne devez pas envoyer votre configuration pour que l'URL de notification prenne effet.

Récupérer les adresses IP pour Prisma Access (Panorama)

Si vous ajoutez manuellement les adresses IP de votre Prisma Access à une liste d'autorisation dans votre réseau, ou si vous utilisez un script d'automatisation pour appliquer des restrictions basées sur IP afin de limiter l'accès entrant aux applications d'entreprise, vous devez comprendre ce que font ces adresses et pourquoi vous devez les autoriser, ainsi que les tâches que vous effectuez pour les récupérer.

Prisma Access ne provisionne pas ces adresses IP tant que vous n'avez pas terminé votre Prisma Access configuration. Une fois votre déploiement terminé, vous récupérez ces adresses IP à l'aide d'un script API. Le script API utilise une clé API que vous obtenez à partir de Prisma Access UI et un fichier .txt que vous créez qui spécifie les adresses que vous souhaitez récupérer.

 ©2025 Palo Alto Networks, Inc.

Si vous disposez d'un déploiement Mobile Users – GlobalProtect, vous pouvez utiliser le Prisma Access UI au lieu de cette API pour gérer l'allocation d'adresses IP publiques et confirmer que les adresses IP ont été ajoutées à vos listes d'autorisation avant que Prisma Access libère les adresses IP. De cette façon, Prisma Access provisionne uniquement les adresses IP que vous avez autorisées dans la liste.

Le tableau suivant vous fournit la liste des adresses IP que Prisma Access utilise pour chaque type de déploiement, ainsi que le mot clé que vous utilisez lorsque vous exécutez le script d'API pour récupérer les adresses IP, et décrit si vous devez ou non les ajouter aux listes d'autorisation de votre organisation.

Type de déploiement	Type d'adresse IP	Description
Utilisateurs mobiles—GlobalProtect	Prisma Access passerelle (**gp_gateway**)	Adresses IP de la passerelle. Vous devez ajouter les adresses IP de la passerelle et du portail aux listes d'autorisation pour vos déploiements d'utilisateurs mobiles. Les utilisateurs mobiles se connectent à une passerelle Prisma Access pour accéder aux ressources internes ou Internet, telles que les applications SaaS ou publiques, auxquelles vous avez donné l'accès. Pour les utilisateurs mobiles, lors du déploiement initial, Prisma Access alloue deux adresses IP pour chaque emplacement que vous déployez.
	Portail Prisma Access (**gp_portal**)	Adresses IP du portail. Vous devez ajouter les adresses IP de la passerelle et du portail aux listes d'autorisation pour vos déploiements d'utilisateurs mobiles. Les utilisateurs mobiles se connectent au portail Prisma Access pour recevoir leur configuration initiale et l'emplacement de la passerelle.

 ©2025 Palo Alto Networks, Inc.

Type de déploiement	Type d'adresse IP	Description
	Adresses IP de bouclage	L'adresse IP source utilisée par Prisma Access pour les demandes adressées à une source interne, et est attribuée à partir de Configurer l'infrastructure de service Prisma Access (Panorama). Ajoutez l'adresse IP de bouclage à une liste d'autorisation dans votre réseau pour donner Prisma Access à des ressources internes telles que les serveurs d'authentification RADIUS ou Active Directory. Palo Alto Networks vous recommande d'autoriser toutes les adresses IP de l'ensemble du sous-réseau d'infrastructure de votre réseau, car les adresses IP de bouclage peuvent changer. Pour trouver le sous-réseau d'infrastructure, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Infrastructure (Infrastructure de service)**. Le sous-réseau s'affiche dans la zone **Infrastructure Subnet (Sous-réseau d'infrastructure)**. Pour récupérer les adresses IP de bouclage, utilisez le script API hérité.
Utilisateurs mobiles—Proxy explicite	Service de cache d'authentification (ACS)	L'adresse du service Prisma Access qui stocke l'état d'authentification des utilisateurs proxy explicites. Cette adresse n'est utilisée que pour le proxy explicite pour les utilisateurs mobiles.

©2025 Palo Alto Networks, Inc.

Type de déploiement	Type d'adresse IP	Description
	Équilibreur de charge réseau	L'adresse que Prisma Access utilise pour l'équilibreur de charge réseau proxy explicite. Cette adresse n'est utilisée que pour le proxy explicite pour les utilisateurs mobiles.
Réseau à distance	Adresses IP du réseau distant (**remote_network**)	Les **Service IP Addresses (Adresses IP de service)** que Prisma Access assigne pour la connexion réseau à distance Prisma Access et Réseaux distants : Adresse IP de service et allocation d'adresses IP de sortie que Prisma Accessutilise pour s'assurer que les utilisateurs du réseau distant obtiennent la langue par défaut correcte pour leur région. Ajoutez ces adresses aux listes d'autorisation de votre réseau pour donner Prisma Access aux ressources Internet.
	Adresses IP de bouclage	L'adresse IP source utilisée par Prisma Access pour les demandes adressées à une source interne, et est attribuée à partir de Configurer l'infrastructure de service Prisma Access (Panorama). Ajoutez l'adresse IP de bouclage à une liste d'autorisation pour donner Prisma Access à des ressources internes telles que les serveurs d'authentification RADIUS ou Active Directory. Pour récupérer les adresses IP de bouclage, utilisez le script API hérité.
Clean Pipe	Adresses IP Clean Pipe (**clean_pipe**)	Ajoutez ces adresses IP à une liste d'autorisation pour permettre au service Clean

 ©2025 Palo Alto Networks, Inc.

Type de déploiement	Type d'adresse IP	Description
		Pipe d'accéder aux ressources Internet.
	Adresses IP de bouclage	L'adresse IP source utilisée par Prisma Access pour les demandes adressées à une source interne, et est attribuée à partir de Configurer l'infrastructure de service Prisma Access (Panorama). Ajoutez l'adresse IP de bouclage à une liste d'autorisation pour donner Prisma Access à des ressources internes telles que les serveurs d'authentification RADIUS ou Active Directory. Pour récupérer les adresses IP de bouclage, utilisez le script API hérité.

Exécutez le script API utilisé pour récupérer les adresses IP Prisma Access

Prisma Access fournit un script d'API que vous pouvez utiliser pour récupérer les adresses IP publiques et privées qu'il utilise dans son infrastructure. Si vous devez ajouter des adresses IP publiques aux listes d'autorisation dans le réseau de votre organisation, procédez comme suit pour récupérer ces adresses IP à l'aide du script API.

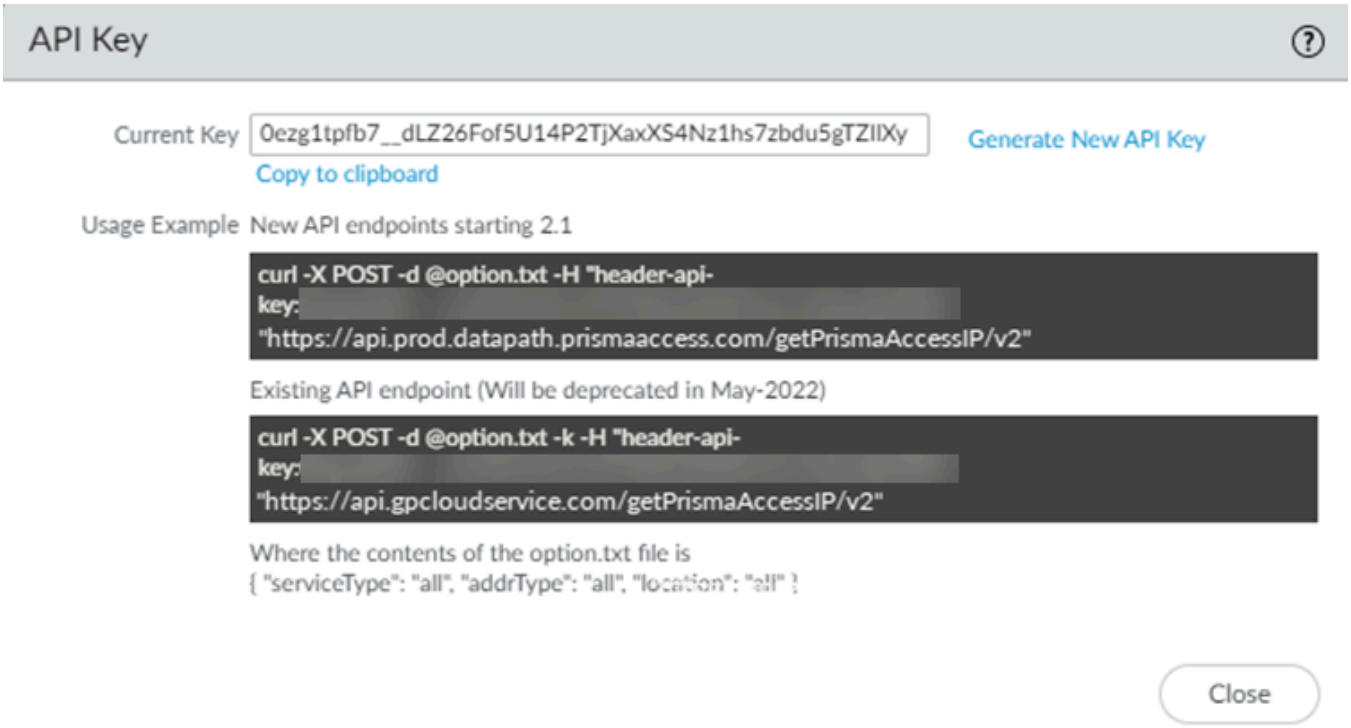
Cette commande ne récupère pas les adresses de bouclage ; pour récupérer les adresses IP de bouclage, utilisez l'API héritée.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Obtenez la clé API.

Vous avez besoin de cette clé pour vous authentifier pour Prisma Access et récupérer la liste des adresses IP à l'aide de la commande API. Seul un administrateur ou un super-utilisateur Panorama peut générer cette clé API ou y accéder.

1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)**.
2. Sélectionnez **Generate API Key (Générer une clé API)**.



Si vous avez déjà généré une clé API, la **Current Key (Clé actuelle)** Affiche. Si vous n'avez pas encore généré de clé ou si vous souhaitez remplacer la clé existante pour répondre à l'audit ou à la vérification de conformité pour la rotation des clés, cliquez sur **Generate New API Key (Générer une nouvelle clé API)** pour une nouvelle clé.

STEP 2 | Créez un fichier .txt et placez les options de commande API dans le fichier.

À l'aide de l'API, la commande à utiliser est un processus en deux étapes. Tout d'abord, vous créez un fichier .txt, en spécifiant les paramètres des adresses IP à récupérer, puis vous enregistrez le fichier dans un dossier accessible à partir de l'emplacement où vous exécutez la commande. Ensuite, vous exécutez l'API et spécifiez le nom et l'emplacement du fichier .txt que vous avez créé dans la commande.

Spécifiez les mots-clés et arguments suivants dans le fichier .txt. Voir Exemples d'API pour la récupération d'adresses IP Prisma Access pour des exemples. Les exemples de ce document

 ©2025 Palo Alto Networks, Inc.

utilisent un nom de fichier **options.txt** mais vous pouvez spécifier n'importe quel nom de fichier, à condition de le référencer dans la commande.

Argument	Choix possibles (mots clés)	Commentaires
serviceType	**all** **remote_network** **gp_gateway** **gp_portal** **clean_pipe** **swg_proxy** **rbi**	**all**—Récupère les adresses IP que vous devez ajouter à une liste d'autorisation pour tous les types de services (réseaux distants, utilisateurs mobiles (passerelles et portails) et Clean Pipe, le cas échéant pour votre déploiement). **remote_network**—Récupère les adresses IP que vous devez ajouter à une liste d'autorisation pour les déploiements de réseau à distance. **gp_gateway**—Récupère les adresses IP de la passerelle Utilisateurs mobiles—GlobalProtect que vous devez ajouter à une liste d'autorisation pour les déploiements d'utilisateurs mobiles. **gp_portal**—Récupère les adresses IP du portail Utilisateurs mobiles—GlobalProtect que vous devez ajouter à une liste d'autorisation pour les déploiements d'utilisateurs mobiles. **clean_pipe**—Récupère les adresses IP que vous devez ajouter à une liste d'autorisation pour les déploiements clean pipe. **swg_proxy**—Récupère les adresses IP de sortie pour chaque emplacement de proxy explicite déployé, le service de cache d'authentification (ACS) et les équilibreurs de charge réseau.

 ©2025 Palo Alto Networks, Inc.

Argument	Choix possibles (mots clés)	Commentaires
		rbi—Récupère les adresses IP de sortie que vous devez ajouter à une liste d'autorisation pour les déploiements Isolation du navigateur distant (RBI) pour se connecter à des applications SaaS.
addrType	**all** **actif** **service_ip** **auth_cache_service** **network_load_balancer**	**all (tout)** ou **active (actif)**—Récupère toutes les adresses IP que vous devez ajouter à une liste d'autorisation. Cette API ne récupère pas les adresses IP de bouclage. Pour récupérer les adresses IP de bouclage, utilisez l'API héritée. **service_ip**—Récupère la **Service IP Address (Adresse IP du service)** que vous utilisez comme adresse IP homologue lorsque vous configurez le tunnel IPSec pour la connexion réseau à distance. **auth_cache_service**—Récupère l'adresse IP de l'ACS proxy explicite (applicable uniquement aux déploiements de proxy explicite). **network_load_balancer**—Récupère l'adresse IP de l'équilibreur de charge du réseau proxy explicite (applicable uniquement aux déploiements de proxy explicite).
actionType	**pre_allocate**	Déploiements d'utilisateurs mobiles uniquement—Un **actionType** de **pre_allocate** vous permet de récupérer des adresses IP ou des sous-réseaux pour les passerelles et portails Prisma Access pour les déploiements d'utilisateurs

 ©2025 Palo Alto Networks, Inc.

Argument	Choix possibles (mots clés)	Commentaires
		mobiles. Utilisez ceci avec un **serviceType gp_gateway** pour récupérer les adresses IP de passerelle pré-allouées et un **serviceType gp_portal** pour récupérer les adresses IP de portail pré-allouées. La récupération des adresses IP pré-allouées vous permet d'ajouter les adresses IP de la passerelle et du portail aux listes d'autorisation de votre organisation avant d'intégrer les emplacements des utilisateurs mobiles, ce qui permet aux utilisateurs mobiles d'accéder aux applications SaaS externes immédiatement après l'intégration des emplacements.
location	**all** **deployed**	**all (tout)**—Récupère les adresses IP de tous les emplacements. Pour les déploiements d'utilisateurs mobiles, ce mot-clé récupère les adresses IP des emplacements que vous avez ajoutés lors de l'intégration et des emplacements que vous n'avez pas ajoutés. **deployed (déployé)**—Récupère les adresses IP dans tous les emplacements que vous avez ajoutés lors de l'intégration des utilisateurs mobiles. Ce mot clé s'applique uniquement aux déploiements d'utilisateurs mobiles. Prisma Access associe des adresses IP à chaque emplacement d'utilisateur mobile lors de l'approvisionnement, même si vous n'avez pas sélectionné cet emplacement lors de l'intégration d'un utilisateur

 ©2025 Palo Alto Networks, Inc.

Argument	Choix possibles (mots clés)	Commentaires
		mobile. Si vous spécifiez **all (tout)**, la commande API récupère les adresses IP de tous les emplacements des utilisateurs mobiles, y compris ceux que vous n'avez pas sélectionnés pour le déploiement. Si vous spécifiez **deployed (déployé)**, la commande API récupère uniquement les adresses IP des emplacements que vous avez sélectionnés lors de l'intégration.

Spécifiez les options dans le fichier .txt au format suivant :

```
 { "serviceType": "service-type", "addrType": "address-type",
"location": "location" }
```

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Saisissez la commande suivante pour récupérer les adresses IP :

- Pour utiliser la nouvelle API introduite dans Prisma Access 2.1, entrez la commande suivante :

```
curl -X POST --data @option.txt -H header-api-key:Current-API-Key "https://api.prod.datapath.prismaaccess.com/getPrismaAccessIP/v2"
```

Depuis mai 2023, certains déploiements gérés dans Panorama utilisent https://api.prod6.datapath.prismaaccess.com/getPrismaAccessIP/v2 (notez le `prod6` dans l'URL au lieu de `prod`).

- Pour utiliser l'API héritée, entrez la commande suivante. Cette commande utilise un point de terminaison d'API hérité qui sera obsolète en mai 2022 :

```
curl -X POST --data @option.txt -k -H header-api-key:Current-API-Key "https://api.gpcloudservice.com/getPrismaAccessIP/v2"
```

Où *option.txt* est le fichier .txt que vous avez créé lors d'une étape précédente et *Current-API-Key* est la Prisma Access Clé API.

Par exemple, étant donné un nom de fichier .txt de **option.txt** et une clé API de **12345abcde**, utilisez la commande API suivante pour récupérer l'adresse IP publique de tous les emplacements :

```
curl -X POST --data @option.txt -H header-api-key:12345abcde "https://api.prod.datapath.prismaaccess.com/getPrismaAccessIP/v2"
```

La commande API peut renvoyer une grande quantité d'informations. Pour rendre la sortie plus lisible, si Python est installé, vous pouvez ajouter `| python -m json.tool` à la fin de la commande cURL.

La commande API renvoie les adresses au format suivant :

```
{ "result": [ { "address_details": [ { "address": "1.2.3.4" "allow_listed": false "addressType": "address-type" "serviceType":
```

 ©2025 Palo Alto Networks, Inc.

```
 "service-type" } ], "addresses": [ "1.2.3.4" ] "zone": "zone-
name", "zone_subnet": [zone-subnet ] }, "status": "success"
```

Où :

- **address_details** affiche les détails de l'adresse de chaque emplacement.
  - **serviceType** affiche le type d'adresse IP (réseau distant (**remote_network**), passerelle d'accès Prisma (**gp_gateway**), portail Prisma Access (**gp_portal**), Clean Pipe (**clean_pipe**), ou Isolation du navigateur distant (**rbi**).
  - **addressType** spécifie le type d'adresse spécifié avec le mot clé `addrType` (soit **active (actif)** soit **pre-allocated (pré-alloué)** si vous pré-allouez des adresses IP pour les emplacements des utilisateurs mobiles).
  - **address (adresse)** affiche l'adresse IP que vous devez ajouter à vos listes d'autorisation.

    Si l'API renvoie plusieurs adresses IP, Prisma Access résume les adresses IP dans le champ **addresses (adresses)**.
- **addresses (adresses)** répertorie toutes les adresses IP de l'emplacement que vous devez ajouter à vos listes d'autorisation.
- **zone** est l'emplacement Prisma Access associé aux adresses IP.
- **zone_subnet** est le sous-réseau des passerelles et des portails pour les utilisateurs mobiles. Prisma Access fournit également ce sous-réseau si vous pré-allouez des adresses IP pour les emplacements des utilisateurs mobiles.

En cas de problème avec les options du fichier .txt, l'API renvoie une erreur similaire à la suivante :

```
 {"status": "error","result": "Invalid json format in the request.
trace_id: xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx "}
```

STEP 4 | Mettez à jour les listes d'autorisation sur vos serveurs locaux ou les règles de stratégie d'application SaaS avec les adresses IP que vous avez récupérées.

Optimisation IP pour les déploiements de type Utilisateurs mobiles – GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Licence Prisma Access • Prisma Access version 5.0 ou ultérieure

L'optimisation IP est un ensemble d'améliorations architecturales qui réduisent le nombre total d'adresses IP dans votre déploiement, simplifiant vos flux de travail de mise en liste d'autorisation tout en améliorant la résilience et en permettant une intégration plus rapide des locataires Prisma Access.

 ©2025 Palo Alto Networks, Inc.

- **Mise en liste d'autorisation des adresses IP publiques simplifiée pour les déploiements de type Utilisateurs mobiles – GlobalProtect** : l'ajout d'un emplacement Prisma Access ou la réalisation d'un événement de mise à l'échelle à un emplacement Prisma Access existant pourrait entraîner l'allocation de nouvelles adresses IP au nœud de traitement de la sécurité des utilisateurs mobiles (MU-SPN). La meilleure pratique consiste à récupérer les nouvelles adresses IP de sortie et de passerelle attribuées par Prisma Access et de les ajouter à une liste d'autorisation dans votre réseau afin d'éviter toute perturbation des applications SaaS ou du pare-feu d'entreprise. Cela peut entraîner une situation dans laquelle vous devez gérer un grand nombre d'adresses IP. L'optimisation IP réduit le nombre d'adresses IP que vous devez gérer.
- **Intégration plus rapide des locataires Prisma Access** : sans l'optimisation IP, vous devriez attribuer des adresses IP privées uniques à chaque périphérique sur Prisma Access et les réseaux privés, ce qui vous obligerait à allouer de gros blocs d'adresses IP à partir de l'espace d'adressage IP routable limité de votre entreprise. L'optimisation IP permet à Prisma Access d'allouer par défaut les adresses d'un espace d'adressage partagé et de réaliser la NAT du trafic des applications privées.



L'optimisation IP est réservée aux nouveaux déploiements GlobalProtect sur Prisma Access. Les déploiements GlobalProtect existants, y compris les nouveaux locataires que vous créez à partir d'un déploiement multilocataire existant, ne peuvent pas profiter de cette fonctionnalité. En outre, si vous faites migrer votre déploiement GlobalProtect depuis des passerelles et portails sur site vers Prisma Access, veillez à ce que tous les utilisateurs exécutent l'application GlobalProtect 6.1.4 et versions ultérieures, 6.2.3 et versions ultérieures, ou 6.3.0 et versions ultérieures avant d'activer cette fonctionnalité.

Prenez note des exigences supplémentaires suivantes pour l'optimisation IP :

- *L'optimisation IP nécessite Prisma Access 5.0 ou version ultérieure pour l'optimisation des utilisateurs mobiles , et peut être activée lorsque vous configurez GlobalProtect pour la première fois.*
- *Lorsque vous configurez GlobalProtect pour la première fois, il vous sera demandé si vous souhaitez ou non activer l'optimisation IP Prisma Access.*
- *Les déploiements de l'optimisation IP ne prennent pas en charge l'IPv6 pour l'accès aux applications publiques (externes) ; l'accès aux applications privées est pris en charge. Pour activer l'IPv6 pour votre nouveau déploiement Prisma Access, contactez l'équipe de compte Palo Alto Networks, qui ouvrira un dossier TAC pour répondre à la demande.*
- *Le fonctionnement de l'API permettant de récupérer les adresses IP Prisma Access reste inchangé, même si l'optimisation IP est activée.*

 ©2025 Palo Alto Networks, Inc.

Exemples d'API pour la récupération d'adresses IP Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• Licence Prisma Access

Utilisez les exemples suivants lorsque vous saisissez des mots-clés et des arguments dans le fichier .txt pour que la commande API récupère les adresses IP de l'infrastructure. Pour modifier le résultat de la commande, modifiez les options dans le fichier .txt ; La commande elle-même ne change pas.

Récupérer ces adresses IP	Spécifier ces paramètres dans le fichier .txt	Commentaires
Adresses IP des utilisateurs mobiles		
Toutes les adresses IP des utilisateurs mobiles	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "all" }`	Un *addrType* (type d'adresse) *all* (tous) signifie que Prisma Access récupère toutes les adresses IP des emplacements que vous avez sélectionnés Configurer les utilisateurs mobiles GlobalProtect (Panorama). Un *location* (emplacement) *all* (tous) signifie que Prisma Access récupère les adresses IP de tous les emplacements disponibles, y compris ceux que vous n'avez pas intégrés. Prisma Access réserve les adresses IP d'emplacements non intégrés afin que vous puissiez les ajouter à vos listes d'autorisation avant de les intégrer.
Adresses IP pour les emplacements des utilisateurs mobiles intégrés	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "deployed" }` Ou	Le type de *location* (emplacement) *deployed* (déployé) signifie que Prisma Access récupère uniquement les adresses IP des emplacements que vous avez intégrés.

 ©2025 Palo Alto Networks, Inc.

Récupérer ces adresses IP	Spécifier ces paramètres dans le fichier .txt	Commentaires
	`{ "serviceType": "gp_gateway", "addrType": "active", "location": "deployed" }`	Utilisez un *addrType* (type d'adresse) *all* (tous) ou *active* (actif) pour récupérer ces adresses IP de passerelle.
Adresses IP du réseau distant		
Récupérer toutes les adresses IP du réseau distant	`{ "serviceType": "remote_network", "addrType": "all", "location": "all" }`	Cette commande récupère les adresses IP publiques et de sortie des réseaux distants que vous avez intégrés. N'utilisez pas le *location* (emplacement) *deployed* (déployé). Vous pouvez utiliser un *addrType* (type d'adresse) *active* (actif), mais il récupère les mêmes adresses que si vous aviez spécifié un *addrType* (type d'adresse) *all* (tous).
Adresses IP Clean Pipe		
Récupérer toutes les adresses IP Clean Pipe	`{ "serviceType": "clean_pipe", "addrType": "all", "location": "all" }`	Cette commande récupère les adresses IP publiques et de sortie Clean Pipe que vous avez intégrées. N'utilisez pas le *location* (emplacement) *deployed* (déployé). Vous pouvez utiliser un *addrType* (type d'adresse) *active* (actif), mais il récupère les mêmes adresses que si vous aviez spécifié un *addrType* (type d'adresse) *all* (tous).
Adresses IP de proxy explicite		
Récupérer les adresses IP ACS des emplacements déployés	`{ "serviceType": "swg_proxy", "location": "all", "addrType": "all" }`	Cette commande récupère les adresses IP de sortie pour chaque emplacement de proxy explicite déployé, le service de cache d'authentification (authentication cache service, ACS) et les équilibreurs de charge réseau (pertinents

 ©2025 Palo Alto Networks, Inc.

Récupérer ces adresses IP	Spécifier ces paramètres dans le fichier .txt	Commentaires
		pour les déploiements de proxy explicite uniquement).
Adresses IP d'isolation du navigateur distant		
Récupérer les adresses IP d'isolation du navigateur à distance (Remote Browser Isolation, RBI) des emplacements déployés	`{ "serviceType": "rbi", "location": "all", "addrType": "all" }`	Cette commande récupère les adresses IP de sortie pour chaque emplacement RBI déployé. Vous pouvez ajouter ces adresses IP à une liste d'autorisation pour vous connecter aux applications SaaS.

 ©2025 Palo Alto Networks, Inc.

Recevoir des notifications lorsque les adresses IP Prisma Access changent

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Pour être informé des changements d'adresse IP publique pour les réseaux distants et des changements d'adresse IP en boucle pour les connexions aux services, les connexions de réseau distant et les utilisateurs mobiles, vous pouvez spécifier une URL à laquelle vous pouvez être alerté d'un changement. Prisma Access utilise une requête HTTP POST pour envoyer la notification. Cette requête POST inclut les données de notification suivantes au format JSON :

```
 {"addrType": "public_ip", "addrChangeType": "add", "utc_timestamp":
"2019-01-31 23:08:19.383894", "text": "Address List Change
Notification"}
```

```
 {"addrType": "public_ip", "addrChangeType": "delete",
"utc_timestamp": "2019-01-31 23:13:35.882151", "text": "Address List
Change Notification"}
```

```
 {"addrType": "loopback_ip", "addrChangeType": "update",
"utc_timestamp": "2019-01-31 23:29:27.100329", "text": "2018-05-11
23:29:27.100329"}
```

Lorsque vous recevez une notification, vous devez suivre un processus en deux étapes. Tout d'abord, vous devez récupérer manuellement ou par programme les adresses IP ou en boucle. Ensuite, vous devez mettre à jour les adresses IP dans la liste d'autorisation appropriée de votre organisation pour garantir que les utilisateurs ne subissent aucune interruption de service.



Prisma Access envoie cette notification quelques secondes avant que la nouvelle adresse IP ne devienne active. Nous vous recommandons d'utiliser des scripts d'automatisation pour récupérer et ajouter les nouvelles adresses IP à une liste d'autorisation dans votre réseau.

Pour ajouter une URL de notification d'adresse IP, complétez la tâche suivante.

- Pour les déploiements Prisma Access (Managed by Strata Cloud Manager), accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Paramètres d'infrastructure)**, cliquez sur l'icône d'engrenage pour modifier les paramètres, ajoutez une **Egress IP Notification URL (URL de**

 ©2025 Palo Alto Networks, Inc.

notification d'IP sortante) où vous pouvez être informé des changements d'adresse IP dans votre infrastructure Prisma Access, et **Save (Enregistrez)** vos modifications.

- Pour les déploiements Prisma Access (Managed by Panorama), accédez à **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** et ajoutez une **IP Change Event Notification URL (URL de notification d'événement de changement d'IP)** où vous pouvez être informé des changements d'adresse IP dans votre infrastructure Prisma Access, puis cliquez sur **OK**.



Vous pouvez spécifier une adresse IP ou un FQDN vers un service Web HTTP ou HTTPS qui écoute les notifications de changement. Prisma Access envoie ces notifications depuis Internet en utilisant une adresse IP publique.

Vous n'avez pas besoin de valider vos modifications pour que l'URL de notification prenne effet.

 ©2025 Palo Alto Networks, Inc.

Utiliser des scripts hérités pour récupérer les adresses IP

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• Licence Prisma Access

Les commandes décrites dans cette section sont remplacées par un script API plus récent à partir de Prisma Access 1.5 ; toutefois, ils sont toujours pris en charge lorsque vous avez besoin d'obtenir l'adresse de bouclage ou pour les déploiements qui les utilisent dans des scripts ou d'autres outils automatisés.

Le tableau suivant présente les mots-clés et les paramètres disponibles dans les scripts d'API hérités utilisés avec Prisma Accesset fournit des informations et des recommandations sur l'API à utiliser pour le type de déploiement dont vous disposez.

Ces commandes héritées récupèrent également les adresses *public IP* et *egress IP* ; cependant, Palo Alto Networks vous recommande d'utiliser le script d'API plus récent pour récupérer ces commandes et d'utiliser uniquement l'API héritée pour récupérer les adresses IP de bouclage.

- Une *public IP address* est l'adresse IP source que Prisma Access utilise pour les requêtes adressées à une source basée sur Internet. Ajoutez l'adresse IP publique à une liste d'autorisation dans votre réseau pour donner Prisma Access à des ressources Internet telles que des applications SaaS ou des applications partenaires accessibles au public.

  Les déploiements d'utilisateurs mobiles, de réseaux distants et Clean Pipe utilisent des adresses IP publiques.
- Une *egress IP address* est une adresse IP que Prisma Access utilise pour le trafic sortant vers Internet, et vous devez également ajouter ces adresses à une liste d'autorisation pour permettre à Prisma Access d'accéder aux ressources Internet.

  Entre autres fins, Prisma Access utilise les adresses IP de sortie afin que les utilisateurs reçoivent des pages Web dans lalangue à laquelle ils s'attendent à partir d'un emplacement Prisma Access. Tous les emplacements ont des adresses IP publiques ; cependant, tous les emplacements n'ont pas d'adresses IP de sortie. Les emplacements suivants n'utilisent pas d'adresses IP de sortie :

  - Tous les lieux que vous avez ajoutés avant la publication de Prisma Access 1.4.
  - Bahreïn
  - Belgique
  - Nord de la France
  - Sud de la France
  - Hong Kong
  - Irlande
  - Corée du Sud
  - Taïwan

 ©2025 Palo Alto Networks, Inc.

- Royaume-Uni

Les déploiements d'utilisateurs mobiles, de réseaux distants et Clean Pipe utilisent des adresses IP de sortie.

Commandes utilisées dans les déploiements d'utilisateurs mobiles	
Nom de la commande	**Commentaires**
Commande **get_egress_ip_all=oui** `curl -H header-api-key :`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?get_egress_ip_all=yes`	Cette commande récupère toutes les adresses IP que vous ajoutez à une liste d'autorisation pour donner Prisma Access à des ressources Internet telles que des applications SaaS ou des applications partenaires accessibles au public. Cette commande comporte les contraintes suivantes : • Cette commande permet de récupérer un grand nombre d'adresses (plus de 200). Si votre entreprise ne peut pas ajouter ce nombre d'adresses IP à une liste d'autorisation, vous pouvez utiliser les mots-clés *gpcs_gp_gw* et *gpcs_gp_portal* pour récupérer uniquement les adresses IP que vous utilisez actuellement ; cependant, vous devrez réexécuter ces commandes chaque fois que vous ajouterez un emplacement. De plus, si un événement de mise à l'échelle se produit, vous devrez ajouter les nouvelles adresses IP à une liste d'autorisation. • Prisma Access ne répertorie pas les emplacements associés à ces adresses IP ; par conséquent, nous vous recommandons d'ajouter toutes les adresses IP renvoyées avec cette commande à une liste d'autorisation. • Cette commande ne vous donne pas d'adresses de bouclage.
Mots-clés **gpcs_gp_gw** et **gpcs_gp_portal** `curl -H header-api-key:`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?fwType=gpcs_gp_gw | gpcs_gp_portal&addrType=public_ip | egress_ip_list | loopback_ip"`	Utilisez cette commande si votre déploiement limite le nombre d'adresses IP que vous pouvez ajouter à une liste d'autorisation. Vous devez ajouter toutes les adresses IP renvoyées avec cette commande à une liste d'autorisation dans votre réseau. Vous pouvez également récupérer les adresses IP de bouclage à l'aide de cette commande.

 ©2025 Palo Alto Networks, Inc.

Commandes utilisées dans les déploiements de réseaux distants	
Nom de la commande	**Commentaires**
Mot-clé **gpcs_remote_network** `curl -H header-api-key:`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?fwType=gpcs_remote_network&addrType=public_ip | egress_ip_list | loopback_ip"`	Utilisez cette commande pour trouver les adresses IP que vous devez ajouter à une liste d'autorisation pour les déploiements de réseaux distants. Vous pouvez également utiliser cette commande pour trouver les adresses IP de sortie pour les déploiements de réseaux distants ; les adresses de sortie et IP peuvent être différentes dans certaines situations.

Commandes utilisées dans les déploiements Clean Pipe	
Nom de la commande	**Commentaires**
Mot-clé **gpcs_clean_pipe** `curl -H header-api-key:`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?fwType=gpcs_clean_pipe&addrType=public_ip | egress_ip_list | loopback_ip"`	Utilisez cette commande pour rechercher les adresses IP que vous devez ajouter à une liste d'autorisation pour les déploiements Clean Pipe.

Récupérer les adresses IP des utilisateurs mobiles

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Ce script hérité a été remplacé par un nouveau script API à partir de Prisma Access 1.5. Palo Alto Networks vous recommande d'utiliser le script le plus récent pour récupérer toutes les adresses IP, à l'exception des adresses de bouclage.

Si vous ajoutez des adresses IP publiques à des listes d'autorisation pour permettre aux utilisateurs mobiles d'accéder à des applications SaaS ou publiques, Prisma Access fournit deux adresses IP pour chaque adresse IP de passerelle et de portail afin qu'une adresse IP puisse être utilisée lors d'une mise à l'échelle ou d'un autre événement. Vous pouvez ajouter cet ensemble d'adresses IP à une liste d'autorisations avant qu'elles ne soient utilisées, ce qui permet d'éviter tout problème avec les utilisateurs mobiles pouvant accéder aux applications SaaS ou publiques lors d'un événement de mise à l'échelle.

Récupérez ces nouvelles adresses en effectuant la tâche suivante :

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Obtenez la clé API en sélectionnant **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** ; puis en sélectionnant **Generate API Key (Générer clé API)**.

Vous avez besoin de cette clé pour vous authentifier Prisma Access et récupérer la liste des adresses IP à l'aide de la commande curl indiquée ci-dessous. Seul un administrateur ou un super-utilisateur Panorama peut générer cette clé API ou y accéder.

STEP 2 | Entrez la commande suivante pour récupérer les adresses IP publiques de l'utilisateur mobile :

```
  curl -H header-api-key:Current-API-Key "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
get_egress_ip_all=yes"
```

Où *Current-API-Key* est la clé API Prisma Access.

Par exemple, étant donné une clé API de **12345abcde**, utilisez la commande API suivante pour récupérer l'adresse IP publique de tous les emplacements :

```
  curl -H header-api-key:12345abcde "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
get_egress_ip_all=yes"
```

Chaque fois que Prisma Access utilise un ensemble d'adresses IP publiques, il alloue un autre ensemble d'adresses IP. Si vous pensez que Prisma Access a utilisé l'ensemble supplémentaire d'adresses IP publiques (par exemple, si un grand nombre d'utilisateurs mobiles ont accédé à un seul emplacement), vous pouvez exécuter à nouveau cette commande API pour trouver le nouvel ensemble d'adresses IP publiques. Toutes les adresses IP persistent après une mise à niveau.

Récupérer les adresses IP publiques, de bouclage et de sortie

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• Licence Prisma Access

Ce script hérité a été remplacé par un script plus récent à partir de Prisma Access 1.5. Palo Alto Networks vous recommande d'utiliser le script le plus récent pour récupérer toutes les adresses IP, à l'exception des adresses de bouclage.

Pour récupérer des adresses IP publiques, de bouclage et de sortie, procédez comme suit.

STEP 1 | Obtenez la clé API et ajoutez une **IP Change Event Notification URL (URL de notification d'événement de changement d'adresse IP)** où vous pouvez être informé des changements d'adresse IP dans votre infrastructure Prisma Access.

Pour plus d'informations, reportez-vous à la sectionRecevoir des notifications lorsque les adresses IP Prisma Access changent.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Récupérez les adresses IP publiques, les adresses IP de bouclage ou les deux pour Prisma Access.

Utilisez la clé API et l'URL du point de terminaison API manuellement ou dans un script d'automatisation :

```
 header-api-key :Current API Key "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
fwType=$fwType&addrType=$addrType"
```

où vous devez remplacer la clé API actuelle par votre clé API et utiliser l'un ou les deux mots clés et arguments suivants :

Description	du mot clé
Mot clé**fwType**	
gpcs_gp_gw	Récupère Prisma Access adresses IP de passerelle (pour les déploiements d'utilisateurs mobiles).
gpcs_gp_portal	Récupère Prisma Access adresses IP du portail (pour les déploiements d'utilisateurs mobiles).
gpcs_remote_network	Récupère Prisma Access adresses IP de réseau distant (pour les déploiements de réseau distant).
gpcs_clean_pipe	Récupère Prisma Access adresses IP de Clean Pipe.
Mot clé**addrType**	
public_ip	Récupère les adresses IP sources que Prisma Access utilise pour les requêtes adressées à une source Internet. Pour les emplacements des utilisateurs mobiles, Prisma Access répertorie les adresses IP par emplacement. Pour les réseaux distants, Prisma Access répertorie les adresses IP par nom de réseau distant.
egress_ip_list	Récupère les adresses IP que Prisma Access utilise avec des adresses IP publiques pour un trafic de sortie supplémentaire vers Internet. Pour les emplacements des utilisateurs mobiles, Prisma Access répertorie les adresses IP par emplacement. Pour les réseaux distants,

 ©2025 Palo Alto Networks, Inc.

Description	du mot clé
	Prisma Access répertorie les adresses IP par nom de réseau distant.
loopback_ip	Récupère les adresses IP sources utilisées par Prisma Access pour les demandes adressées à une source interne (par exemple, un serveur RADIUS ou Active Directory) et est attribuée à partir du sous-réseau d'infrastructure.

Si vous ne spécifiez pas de mot clé, Prisma Access récupère toutes les adresses IP.

Par exemple, vous pouvez essayer la commande Curl suivante pour récupérer manuellement la liste des adresses IP publiques pour tous les réseaux distants :

```
curl -H header-api-
key:1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7
 "https://api.prod.datapath.prismaaccess.com/getAddrList/latest?
fwType=gpcs_remote_network&addrType=public_ip"
```

ou utilisez un simple script python pour récupérer la liste de toutes les adresses IP, par exemple :

```
  #!/usr/bin/python import subprocess import json api_key
 = '1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7'
 # Replace with your key api_end_point = 'https://
api.prod.datapath.prismaaccess.com/getAddrList/latest' # This call
 retrieves IP addresses for all your Prisma Access firewalls args =
 ['curl', '-k', '-H', 'header-api-key:' + api_key, api_end_point]
 p = subprocess.Popen(args, stdout=subprocess.PIPE) output
 = p.communicate() dout = json.loads(output[0]) addrStrList
 = dout['result']['addrList'] addrList = [] for addr_str
 in addrStrList: addrList.append(addr_str.split(":")[1])
 print(addrList)
```

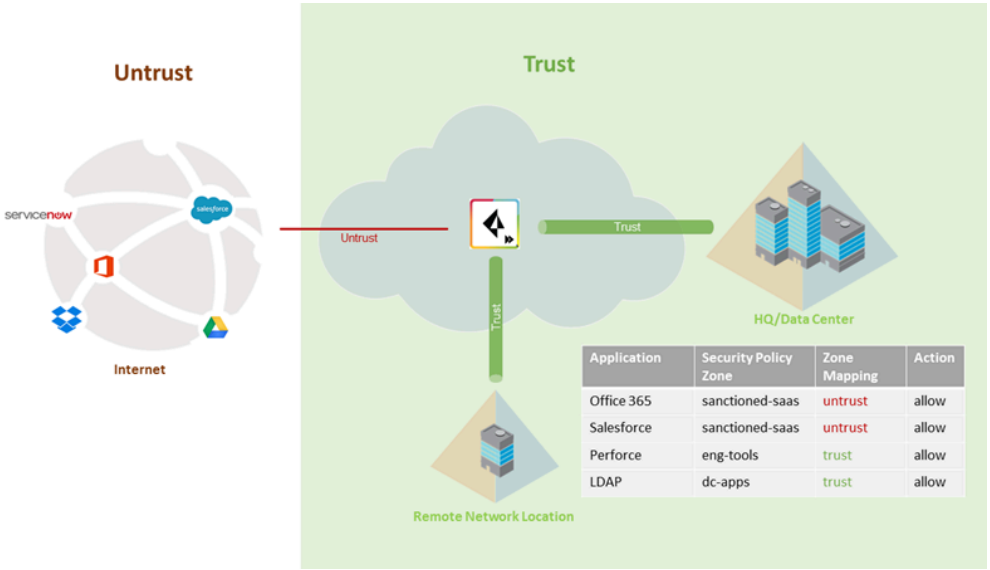
STEP 3 | Mettez à jour les listes d'autorisation sur vos serveurs locaux ou les règles de stratégie d'application SaaS avec les adresses IP que vous avez récupérées.

©2025 Palo Alto Networks, Inc.

Prisma Access Zones

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Sur un pare-feu, les zones sont associées à des interfaces. Mais à l'intérieur Prisma Access, l'infrastructure réseau est automatiquement configurée pour vous. Cela signifie que vous ne devez plus vous soucier de configurer les interfaces et de les associer aux zones que vous créez. Toutefois, pour permettre une application cohérente des stratégies de sécurité, vous devez créer des mappages de zones afin que Prisma Access sache s'il faut associer une zone à une interface interne (de confiance) ou à une interface externe (non fiable). Cela garantira une application correcte des règles de votre politique de sécurité. Par défaut, toutes les zones que vous envoyez à Prisma Access sont définies comme non fiables. Vous devez laisser toutes les zones associées au trafic Internet définies comme non fiables, y compris vos applications SaaS approuvées. Toutefois, pour toutes les zones qui permettent d'accéder aux applications sur votre réseau interne ou dans votre centre de données, vous devez les définir comme fiables. Notez que dans l'exemple ci-dessous, toutes les applications SaaS approuvées (Office 365 et Salesforce dans ce cas) sont segmentées dans la zone SaaS approuvée pour permettre la visibilité et l'application des politiques sur l'utilisation de ces applications. Pour activer Prisma Access pour associer la zone SaaS approuvée à une interface externe, vous devez mapper cette zone comme non fiable. De même, les zones eng-tools et dc-apps permettent d'accéder aux applications du siège social et vous devez donc les désigner comme zones fiables.



Prisma Access prend en charge trois zones (fiables, non fiables et VPN sans client) et simplifie la création de politiques en les configurant pour vous.

©2025 Palo Alto Networks, Inc.

Employé	Description
Approuvée	Zone contenant toutes les adresses IP approuvées et intégrées, les connexions aux services ou les utilisateurs mobiles au sein du réseau de l'entreprise.
Non approuvée	Toutes les adresses IP non approuvées, les connexions aux services ou les utilisateurs mobiles en dehors du réseau de l'entreprise. Par défaut, toute adresse IP ou utilisateur mobile qui n'est pas approuvé n'est pas fiable par nature.
VPN sans client	Sécurisez l'accès à distance aux applications Web d'entreprise courantes qui utilisent les technologies HTML, HTML5 et Javascript. Les utilisateurs ont l'avantage d'un accès sécurisé à partir de navigateurs Web sur lesquels SSL est activé sans installer le logiciel client. Cela est utile lorsque vous devez activer l'accès à ces applications pour des partenaires ou des entrepreneurs et pour activer de manière sécurisée les actifs non gérés, y compris les appareils personnels. *La zone pour le VPN sans client est mappée à la zone de confiance par défaut ; ce paramètre ne peut pas être modifié.*

Les journaux Prisma Access qui affichent une zone de **inter-fw** sont des journaux utilisés pour la communication au sein de l'infrastructure Prisma Access.

Lors de la création de zones, n'utilisez pas les noms suivants pour les zones, car il s'agit de noms utilisés pour les zones internes :

- approuvé
- non approuvé
- inter-FW
- Tout nom que vous utilisez pour les réseaux distants (les noms de réseaux distants sont utilisés comme zone source dans les journaux Strata Logging Service)

Les journaux Prisma Access qui affichent une zone inter-FW sont des journaux utilisés pour la communication au sein de l'infrastructure Prisma Access.

 ©2025 Palo Alto Networks, Inc.

DNS pour Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Prisma Access vous permet de spécifier des serveurs DNS pour résoudre à la fois les domaines internes à votre organisation et les domaines externes. Faites cela pour fournir l'accès à des services sur votre réseau d'entreprise, tels que des serveurs LDAP et DNS, en particulier si vous prévoyez de configurer des connexions aux services pour fournir un accès à ce type de ressources au siège ou dans les centres de données. Prisma Access soutient la résolution DNS pour les utilisateurs mobiles - Global Protect et les déploiements de réseaux distants. Les requêtes DNS pour les domaines de la liste de domaines interne sont envoyées à vos serveurs DNS locaux pour s'assurer que les ressources sont disponibles pour les utilisateurs du réseau distant Prisma Access et les utilisateurs mobiles.

Par exemple, si vous souhaitez qu'une recherche DNS pour votre domaine d'entreprise porte exclusivement sur le serveur DNS d'entreprise, spécifiez ici le domaine d'entreprise et les serveurs DNS d'entreprise. Pour vous assurer que les terminaux utilisent la fonction **DNS Proxy IP Address (Adresse IP du proxy DNS)**, ils doivent être configurés pour résoudre le DNS via l'adresse IP indiquée dans **Workflow (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Prisma Access DNS Proxy IP Address (Adresse IP du proxy DNS Prisma Access)**.

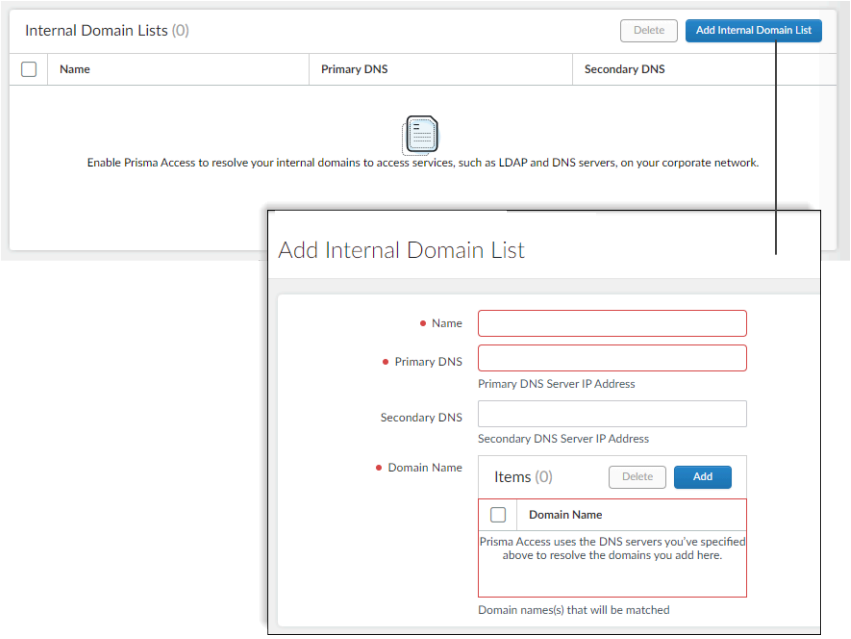
- Strata Cloud Manager
- Panorama

DNS pour Prisma Access (Strata Cloud Manager)

Voici comment procéder à la configuration de Prisma Access pour résoudre les domaines internes et comment personnaliser les paramètres DNS (pour résoudre les domaines internes et publics) pour les déploiements d'utilisateurs mobiles et les sites de réseau distant.

©2025 Palo Alto Networks, Inc.

- Configurez des listes de domaines internes qui s'appliquent à tout le trafic.
  1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** et **Add Internal DNS Servers (Ajouter des serveurs DNS internes)**.



  2. Entrez le serveur DNS principal et le serveur DNS secondaire que Prisma Access doit utiliser pour résoudre les noms de domaine internes.
  3. Ajoutez les noms de domaine internes à envoyer à ces serveurs DNS pour résolution.

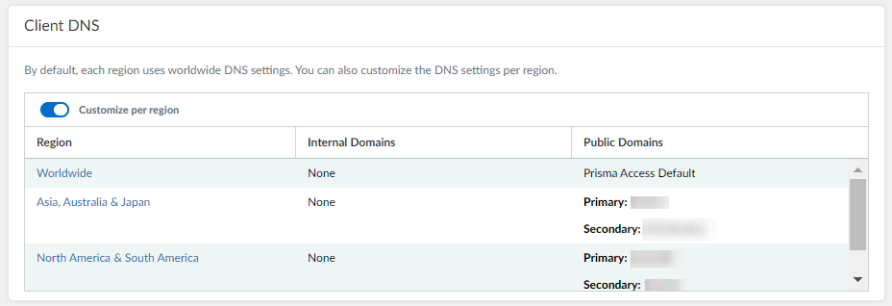
     Utilisez un caractère générique (*) devant les domaines de la liste de domaines, par exemple, *.acme.local ou *.acme.com

 ©2025 Palo Alto Networks, Inc.

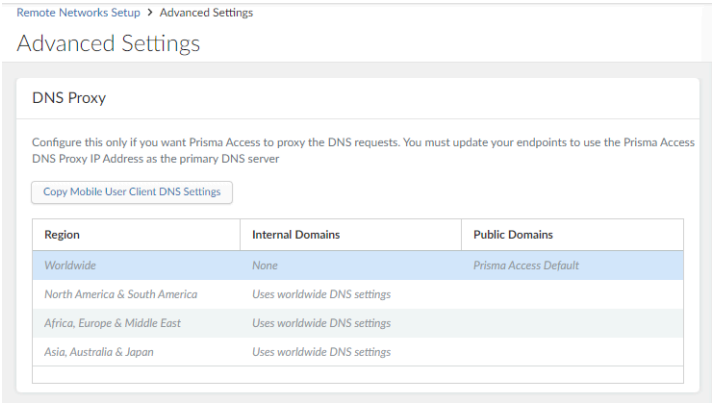
- Ajoutez des listes de domaines internes qui s'appliquent uniquement à des déploiements d'utilisateurs mobiles spécifiques ou à des sites de réseau distant.

  1. Configurez les paramètres DNS :

     - **Utilisateurs mobiles**—Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **Infrastructure Settings (Paramètres d'infrastructure)**, puis à **Client DNS (DNS client)**.



     - **Réseaux distants**—Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Remote Networks (Réseaux distants)** > **Advanced Settings (Paramètres avancés)**, puis à **DNS Proxy (Proxy DNS)**.



  2. Utilisez le paramètre universel par défaut (le serveur DNS par défaut Prisma Access) ou personnalisez les paramètres en fonction de la région. Dans les deux cas, sélectionnez la région à ajuster et personnalisez les paramètres DNS de cette région.
  3. Cochez l'option pour **use these DNS settings to resolve internal domains (utiliser ces paramètres DNS pour résoudre les domaines internes)** et éventuellement pour **Use the internal DNS Server for resolving public domains too (Utiliser également le serveur DNS interne pour résoudre les domaines publics)**. Si vous ne sélectionnez pas cette option, Prisma Access utilise son serveur DNS cloud par défaut pour résoudre les requêtes de domaines publics.
  4. Autorisez le trafic de toutes les adresses de votre pool d'adresses IP d'utilisateurs mobiles vers vos serveurs DNS.

     Le proxy DNS dans Prisma Access envoie les requêtes aux serveurs DNS que vous spécifiez. L'adresse source dans la requête DNS est la première adresse IP du pool d'IP que vous attribuez à la région. Pour garantir que vos requêtes DNS peuvent atteindre les serveurs, vous devez vous assurer que vous autorisez le trafic provenant de toutes les adresses de votre pool d'adresses IP d'utilisateurs mobiles vers vos serveurs DNS.

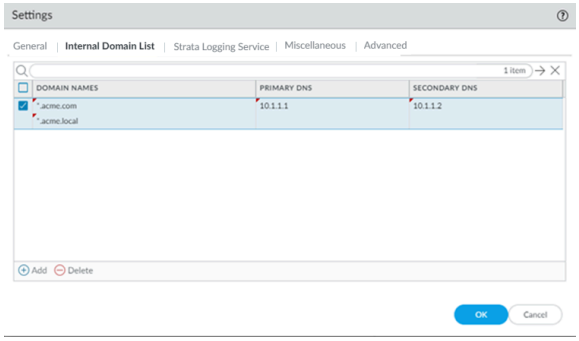
 ©2025 Palo Alto Networks, Inc.

DNS pour Prisma Access (Panorama)

Configurez Prisma Access pour résoudre des domaines internes.

- Configurez des listes de domaines internes qui s'appliquent à tout le trafic.
  1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** et cliquez sur l'icône engrenage pour modifier les paramètres.
  2. Sélectionnez l'onglet **Internal Domain List (Liste des domaines internes)**.
  3. Ajoutez les noms de domaine, les serveurs DNS primaires et secondaires que vous souhaitez que Prisma Access utilise pour résoudre vos noms de domaine internes.

     Utilisez un caractère générique (*) devant les domaines de la liste de domaines, par exemple, *.acme.local ou *.acme.com

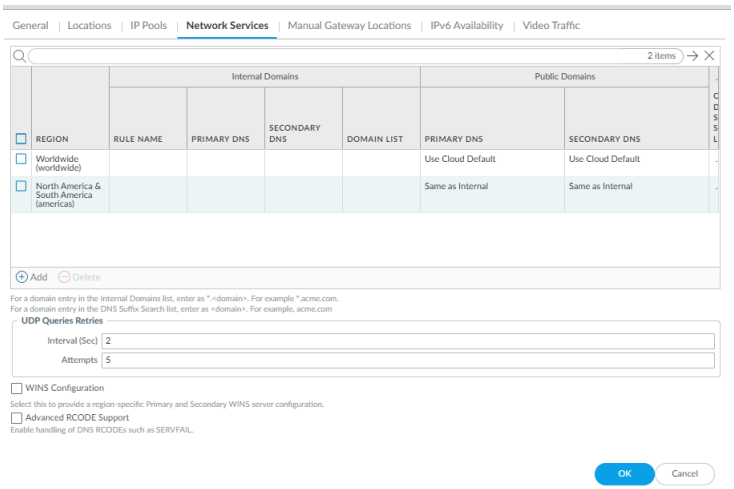


 ©2025 Palo Alto Networks, Inc.

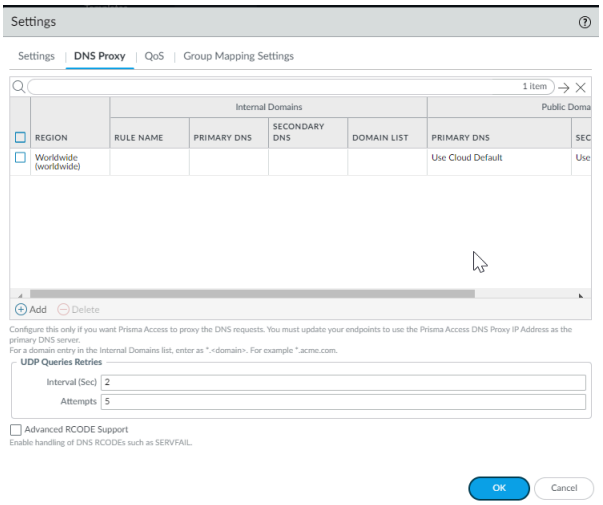
- Ajoutez des listes de domaines internes qui s'appliquent uniquement à des déploiements d'utilisateurs mobiles spécifiques ou à des sites de réseau distant.

  1. Configurez les paramètres DNS :

     - **Utilisateurs mobiles**—Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users - GlobalProtect (Utilisateurs mobiles - GlobalProtect)** et sélectionnez la passerelle externe > et cliquez sur **Network Services (Services du réseau)**.



     - **Réseaux distants**—Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** > **Settings (Paramètres)** > **DNS Proxy (Proxy DNS)**.



  2. Utilisez le paramètre universel par défaut (le serveur DNS par défaut Prisma Access) ou personnalisez les paramètres en fonction de la région. Dans les deux cas, sélectionnez la région à ajuster et personnalisez les paramètres DNS de cette région.
  3. Ajoutez une ou plusieurs règles pour configurer les paramètres DNS de **Internal Domain (Domaine interne)**.

     - Saisissez un nom de règle unique pour la règle.
     - Si vous souhaitez que votre serveur DNS interne résolve uniquement les domaines que vous spécifiez, saisissez les domaines à résoudre dans la liste de domaines. Spécifiez

 ©2025 Palo Alto Networks, Inc.

un astérisque devant le domaine ; par exemple, *.acme.com. Vous pouvez spécifier un maximum de 1 024 entrées de domaine.

Prisma Access dispose d'une règle prédéfinie pour résoudre les domaines *.amazonaws.com à l'aide du serveur cloud par défaut. Si vous souhaitez que vos serveurs DNS internes résolvent un domaine *.amazonaws.com plus spécifique (par exemple, *.s3.amazonaws.com), entrez l'URL dans la liste des domaines. Prisma Access évalue les noms de domaine du plus long au plus court, puis du plus haut au plus bas dans la liste.

- Si vous disposez d'un serveur DNS personnalisé qui peut accéder à vos domaines internes, spécifiez les adresses IP du serveur DNS principal et du serveur DNS secondaire, ou sélectionnez Use Cloud Default (Utiliser la valeur par défaut du cloud) pour utiliser le serveur DNS Prisma Access par défaut.

4. Spécifiez les paramètres DNS pour les **Public Domains (Domaines publics)**.
   - **Use Cloud Default (Utiliser la valeur par défaut du cloud)** : utilisez le serveur DNS Prisma Access par défaut.
   - **Same as Internal Domains (Même valeur que les domaines internes)** : utilisez le même serveur que vous utilisez pour résoudre les domaines internes. Lorsque vous sélectionnez cette option, le serveur DNS utilisé pour résoudre les domaines publics est le même que le serveur configuré pour la première règle dans la section **Internal Domains (Domaines internes)**.
   - **Custom DNS Server (Serveur DNS personnalisé)** : si vous disposez d'un serveur DNS capable d'accéder à vos domaines publics (externes), saisissez l'adresse du serveur DNS principal dans ce champ.
5. (Facultatif) Vous pouvez ajouter un suffixe DNS pour spécifier le suffixe que le client doit utiliser localement lorsqu'un nom d'hôte non qualifié est saisi et qu'il ne peut pas résoudre, par exemple, acme.local. Dans le guide de l'administrateur de Prisma Access (géré par Panorama), ne saisissez pas de caractère générique (*) devant le suffixe du domaine (par exemple, acme.com). Vous pouvez ajouter plusieurs suffixes.
6. Autorisez le trafic de toutes les adresses de votre pool d'adresses IP d'utilisateurs mobiles vers vos serveurs DNS.

   Le proxy DNS dans Prisma Access envoie les requêtes aux serveurs DNS que vous spécifiez. L'adresse source dans la requête DNS est la première adresse IP du pool d'IP que vous attribuez à la région. Pour garantir que vos requêtes DNS peuvent atteindre les serveurs, vous devez vous assurer que vous autorisez le trafic provenant de toutes les adresses de votre pool d'adresses IP d'utilisateurs mobiles vers vos serveurs DNS.

 ©2025 Palo Alto Networks, Inc.

High Availability (haute disponibilité - HA) pour Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• Licence Prisma Access

Le déploiement des appliances Panorama en configuration High Availability (haute disponibilité - HA) assure la redondance en cas de défaillance du système ou du réseau et garantit une connectivité continue à Prisma Access. Dans une configuration HA, un homologue d'appliance Panorama est l'actif-principal et l'autre est le passif-secondaire. En cas de basculement, l'homologue secondaire devient actif et reprend le rôle de gestion de Prisma Access.

Pour simplifier la configuration de l'HA, configurez les appliances Panorama en HA après avoir acheté les codes et composants d'authentification Prisma Access et Strata Logging Service et associez le numéro de série de l'appliance Panorama principale sur laquelle vous prévoyez d'installer le plug-in Cloud Services avec les codes d'authentification, mais avant d'activer et d'installer Panorama Managed Prisma Access. Cependant, vous pouvez également utiliser ce processus pour configurer les appliances Panorama existantes sur lesquelles le plug-in est déjà installé.

Que vous commenciez à utiliser une nouvelle paire d'appliances Panorama, ou que vous ayez déjà configuré votre appliance Panorama autonome et terminé les procédures de mise sous licence et d'installation, assurez-vous de vérifier les conditions préalables avant d'activer HA :

- Vous devez enregistrer les homologues HA de l'appliance Panorama sur le même compte client sur le portail du support client (CSP).
- Les homologues de l'appliance Panorama doivent avoir le même facteur de forme (appliances matérielles du même modèle ou appliances virtuelles identiques) et la même version de système d'exploitation et doivent avoir le même ensemble de licences. La licence de support premium est requise pour Prisma Access et Strata Logging Service.
- Le numéro de série de l'appliance Panorama principal est lié à vos codes d'authentification Prisma Access et Strata Logging Service. Si vous avez installé et configuré le plug-in sur une appliance Panorama autonome, assurez-vous que vous utilisez cette appliance Panorama comme homologue principal. Si vous devez assigner cet homologue autonome en tant qu'appliance Panorama secondaire, contactez le support Palo Alto Networks pour obtenir de l'aide sur le transfert de la licence à l'homologue de l'appliance Panorama principale avant de continuer.

Si vous désactivez HA pour une paire Panorama et revenez à une configuration où un seul Panorama gère les Prisma Access, vous devez revérifier votre compte pour éviter les erreurs lors de la récupération de l'état des composants Prisma Access.

Pour configurer vos appliances Panorama en configuration HA, suivez les étapes suivantes.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Définir la HD (haute disponibilité) sur Panorama.

Définissez l'appliance Panorama principale comme **Primary (Principale)** et l'appliance Panorama secondaire comme **Secondary (Secondaire)** et assurez-vous que le numéro de série de votre appliance Panorama principale est lié à vos codes d'authentification Prisma Access et Strata Logging Service.

STEP 2 | Assurez-vous que les appliances Panorama principale (active) et secondaire (passive) sont synchronisées et que l'état de liaison HA entre elles est haut.

1. Accédez au **Dashboard (Tableau de bord)** sur l'appliance Panorama principale et sélectionnez **Widgets** > **System (Système)** > **High Availability (Haute disponibilité)** pour afficher le widget HA.
2. **Sync to peer (Synchroniser avec l'homologue)**, cliquez sur **Yes (Oui)** et attendez que **Running config (Configuration actuelle)** affiche **Synchronized (Synchronisé)**.
3. Assurez-vous que l'homologue **Local** est **active (actif)**.
4. Accédez au **Dashboard (Tableau de bord)** sur l'appliance Panorama passive et sélectionnez **Widgets** > **System (Système)** > **High Availability (Haute disponibilité)** pour afficher le widget HA.
5. Vérifiez que **Running config (Configuration actuelle)** affiche **Synchronized (Synchronisé)**.
6. Assurez-vous que l'homologue **Local** est **passive (passif)**.

STEP 3 | Installez les composants Prisma Access sur l'appliance Panorama principale.

1. Connectez-vous à l'appliance Panorama principale et sélectionnez **Panorama** > **Licenses (Licences)**.
2. Cliquez sur **Retrieve the license keys from license server (Récupérer les clés de licence auprès du serveur de licences)**.
3. Activez et installez Panorama Managed Prisma Access, notamment en générant un mot de passe à usage unique (OTP) et en vérifiant votre compte.

STEP 4 | Vérifiez que HA est activé.

1. Sur l'appliance Panorama principale, Accédez au CLI et saisissez la commande opérationnelle suivante :

   ```
   tail follow yes mp-log plugin_cloud_services.log
   ```

2. Trouvez le texte suivant dans la sortie journal, où *X* est le numéro de série de l'appliance Panorama principale et *Y* est le numéro de série de l'appliance Panorama secondaire :

   ```
   2017-11-06 15:14:07.790 -0800 INFO: [hainfo] Sending
    update to CSP for HA peer serial information to https://
   updates.paloaltonetworks.com/licensesvc/licenseservice.asmx/
   PanoramaHAInfo (https://updates.paloaltonetworks.com/
   licensesvc/licenseservice.asmx/PanoramaHAInfo)
    2017-11-06 15:14:07.791 -0800 INFO: [hainfo] Data
    string is primarypanoramasn=<varname>X</varname>
    &secondarypanoramasn=<varname>Y</varname> 2017-11-06
    15:14:17.595 -0800 INFO: [hainfo] HTTP_CODE 200, RESPONSE:
    <?xml version="1.0" encoding="utf-8"?> <PanoramaHA
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance (http://
   ```

 ©2025 Palo Alto Networks, Inc.

```
www.w3.org/2001/XMLSchema-instance)" xmlns:xsd="http://
www.w3.org/2001/XMLSchema (http://www.w3.org/2001/
XMLSchema)" xmlns="http://www.paloaltonetworks.com/ (http://
www.paloaltonetworks.com/)"> <success>true</success> </
PanoramaHA> 2017-11-06 15:14:17.596 -0800 INFO: [hainfo]
 Cached HA Peer's serial number <varname>Y</varname>
```

3. Connectez-vous au portail de support client (CSP) et sélectionnez **Assets (Ressources)** > **Cloud Services** pour vérifier que les deux homologues Panorama sont liés à vos licences Prisma Access et Strata Logging Service.
4. Vérifiez les champs correspondant à l'appliance Panorama principale et secondaire.

   Les champs Auth Code (Code d'authentification), Model Name (Nom du modèle), License Description (Description de la licence) et Expiration Date (Date d'expiration) doivent être les mêmes pour l'appliance Panorama principale et secondaire, car Palo Alto Networks a associé automatiquement la licence Prisma Access à l'appliance Panorama secondaire.

STEP 5 | Connectez-vous à l'appliance Panorama secondaire et activez et installez Panorama Managed Prisma Access.

Lorsque vous vous connectez au portail de support client (CSP) pour générer l'OTP, assurez-vous de spécifier le numéro de série de l'appliance Panorama secondaire.

STEP 6 | Validez vos modifications sur l'appliance Panorama principale et secondaire.

1. **Commit (Validez)** > **Commit and Push (Validez et appliquez)** vos modifications.
2. Cliquez sur **OK** et **Push (Appliquer)**.

STEP 7 | Vérifiez que les appliances Panorama principale et secondaire sont toujours dans un état synchronisé.

 ©2025 Palo Alto Networks, Inc.

Modèles prédéfinis : Intégrer une connexion aux services ou un réseau distant

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• Licence Prisma Access

Prisma Access inclut des modèles IPSec prédéfinis pour les périphériques IPSec et SD-WAN tiers courants. Ces profils accélèrent et simplifient l'intégration des connexions aux services et des connexions aux réseaux distants qui utilisent l'un de ces périphériques pour mettre fin à la connexion.

Le partage d'un modèle commun vous permet également d'intégrer plusieurs connexions à distance du même type avec des cryptos couramment partagés, des clés pré-partagées et des identifiants d'homologue.

- Modèles prédéfinis : Intégrer une connexion aux services ou un réseau distant
- Profils cryptographiques IKE et IPSec pris en charge pour les périphériques SD-WAN courants

Prisma Access vous fournit les modèles prédéfinis suivants que vous pouvez utiliser pour configurer des tunnels IPSec entre votre périphérique sur site et Prisma Access :

- Tunnels IPSec (**Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**) sous Remote_Network_Template et Service_Conn_Template.
- Passerelles IKE (**Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)**) sous Remote_Network_Template et Service_Conn_Template.
- Profils crypto IPSec (**Network (Réseau)** > **Network Profiles (Profils réseau)** > **IPSec Crypto (Crypto IPSec)**) sous Remote_Network_Template et Service_Conn_Template.
- Profils crypto IKE (**Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Crypto (Crypto IKE)**) sous Remote_Network_Template et Service_Conn_Template.

À l'heure actuelle, des modèles pour les fournisseurs suivants sont disponibles :

En plus des modèles suivants, nous fournissons un modèle générique que vous pouvez utiliser avec n'importe quel périphérique local non répertorié ici.

- Appareils Cisco :
  - Routeurs à services intégrés (ISR) Cisco
  - Appliances de sécurité adaptative (ASA) Cisco
- Citrix
- Prisma SD-WAN (anciennement CloudGenix)
- Riverbed
- Silver Peak

Pour intégrer une connexion aux services ou une connexion aux réseaux distants à l'aide des modèles fournis par Prisma Access, effectuez la tâche suivante.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Dans Panorama, effectuez la configuration de manière à ce que les modèles s'affichent dans Panorama.

Lors de la mise à niveau du plug-in Cloud Services, les nouveaux modèles ne s'affichent pas automatiquement. Réalisez cette étape une fois après la mise à niveau afin que les modèles s'affichent en permanence. Les nouvelles installations effectuent cette configuration initiale dans le cadre de leur première configuration et cette étape supplémentaire n'est pas requise.

Vous pouvez également terminer cette étape au cas où vous supprimez ces modèles et que vous avez besoin de les récupérer.

- Pour les connexions aux services, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)**, cliquez sur l'icône d'engrenage dans la zone **Settings (Paramètres)** pour ouvrir les **Settings (Paramètres)**, puis cliquez sur **OK**.
- Pour les connexions aux réseaux distants, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**, cliquez sur l'icône d'engrenage dans la zone **Settings (Paramètres)** pour ouvrir les **Settings (Paramètres)**, puis cliquez sur **OK**.

STEP 2 | Sélectionnez **Network (Réseau)**, puis choisissez le bon **Template (Modèle)** (soit **Remote_Network_Template** si vous êtes en train de créer une connexion à un réseau distant ou **Service_Conn_Template** si vous créez une connexion aux services).

STEP 3 | Déterminez le type de périphérique utilisé pour mettre fin à la connexion aux service ou au réseau distant, et recherchez un modèle à utiliser avec ce périphérique.

Si votre périphérique SD-WAN ou IPSec ne figure pas dans la liste, utilisez les profils génériques.

STEP 4 | Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)** et apportez les modifications suivantes au profil de passerelle IKE de votre périphérique :

Vous pouvez utiliser les profils crypto IPSec et IKE sans modification ; mais vous devez apporter des modifications spécifiques au profil de passerelle IKE pour qu'il corresponde aux paramètres du réseau.

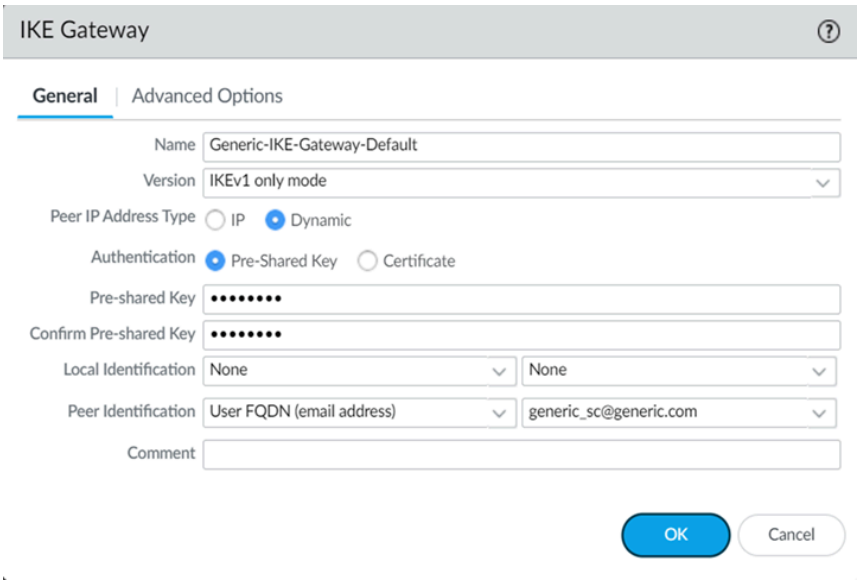
- (Facultatif) Si vous connaissez l'adresse IP publique du périphérique sur site qui sera utilisé pour configurer le tunnel IPSec avec Prisma Access, définissez une adresse IP statique en

 ©2025 Palo Alto Networks, Inc.

spécifiant un **Peer IP Address Type (Type d'adresse IP de l'homologue)** de **IP** et saisissez la **Peer Address (Adresse de l'homologue)** du tunnel IPSec.

- Si vous utilisez une clé pré-partagée pour le tunnel IPSec, spécifiez une **Pre-shared Key (Clé pré-partagée)**.
- Spécifiez une **Peer Identification (Identification de l'homologue)** de **IP Address (Adresse IP)** ou de **User FQDN (FQDN de l'utilisateur)**.

  Assurez-vous de faire correspondre les paramètres que vous spécifiez ici lorsque vous configurez le périphérique utilisé pour mettre fin à l'autre côté du tunnel IPSec.



STEP 5 | Intégrez la connexion aux services ou la connexion au réseau distant, en spécifiant la configuration du **IPSec Tunnel (Tunnel IPSec)** qui correspond au périphérique situé de l'autre côté du tunnel IPSec.

 ©2025 Palo Alto Networks, Inc.

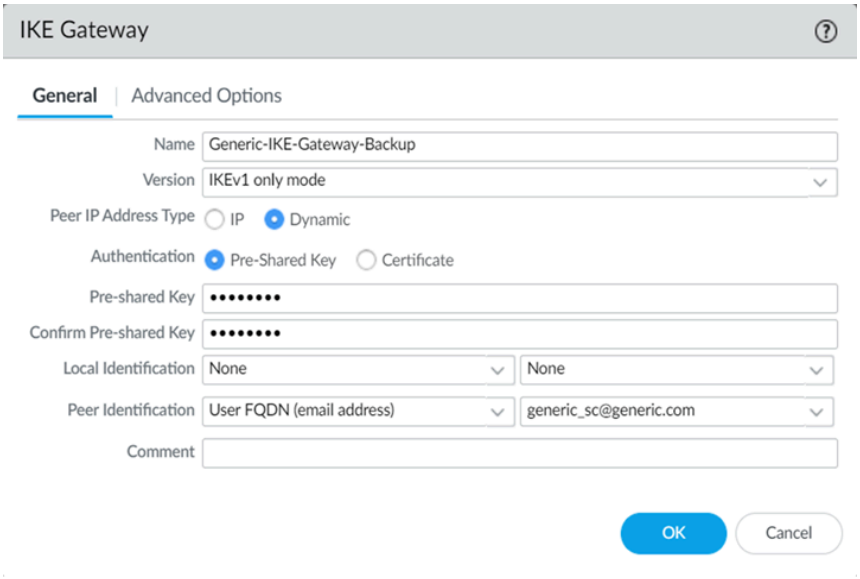
STEP 6 | (Facultatif) Si vous devez ajouter un tunnel de sauvegarde (WAN secondaire) pour une connexion aux services ou une connexion à distance, effectuez les étapes de configuration supplémentaires suivantes.

La configuration d'un WAN secondaire n'est pas prise en charge dans les déploiements suivants :

- Si votre WAN secondaire est configuré en mode actif-actif avec le tunnel IPSec principal.
- Si l'équipement de vos locaux clients (CPE) est configuré dans une configuration ECMP (Equal Cost Multipath) avec le tunnel IPSec principal et secondaire.

1. Créez une nouvelle IKE Gateway (Passerelle IKE) pour le tunnel de sauvegarde, en copiant les paramètres du modèle prédéfini que vous souhaitez dupliquer.

   L'exemple suivant crée une configuration de tunnel de sauvegarde pour les périphériques réseau génériques.

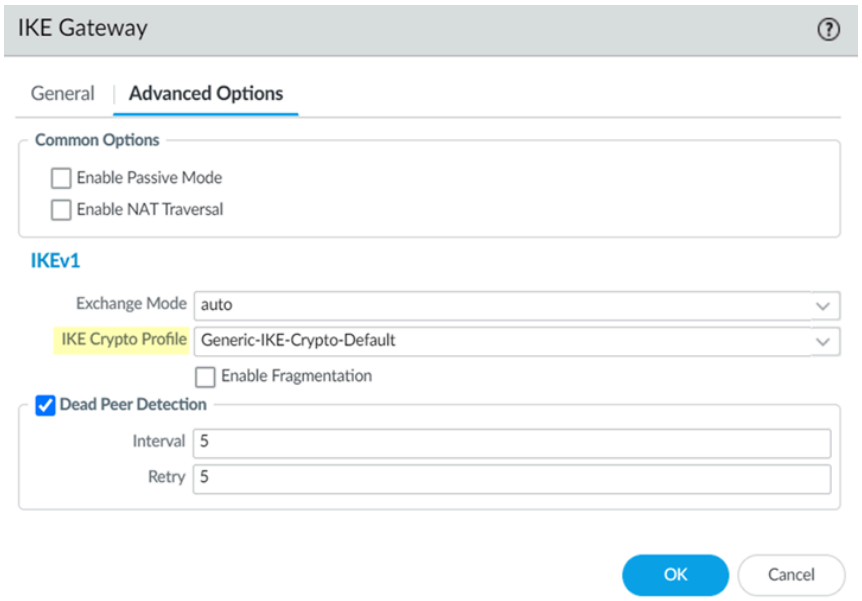


2. Sous **Advanced Options (Options avancées)**, spécifiez le **IKE Crypto Profile (Profil crypto IKE)** pour le modèle prédéfini que vous souhaitez utiliser.

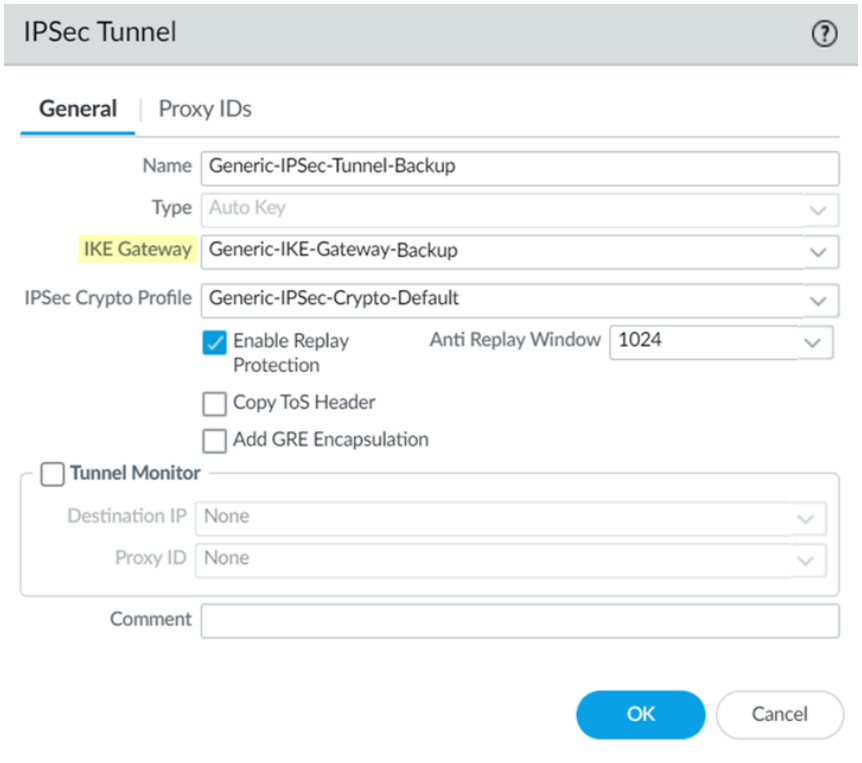
   Palo Alto Networks vous recommande d'utiliser des cryptogrammes GCM au lieu des cryptogrammes CBC pour les tunnels IPSec.

   Si vous intégrez un Prisma SD-WAN, sélectionnez **Enable Passive Mode (Activer le mode passif)**.

 ©2025 Palo Alto Networks, Inc.

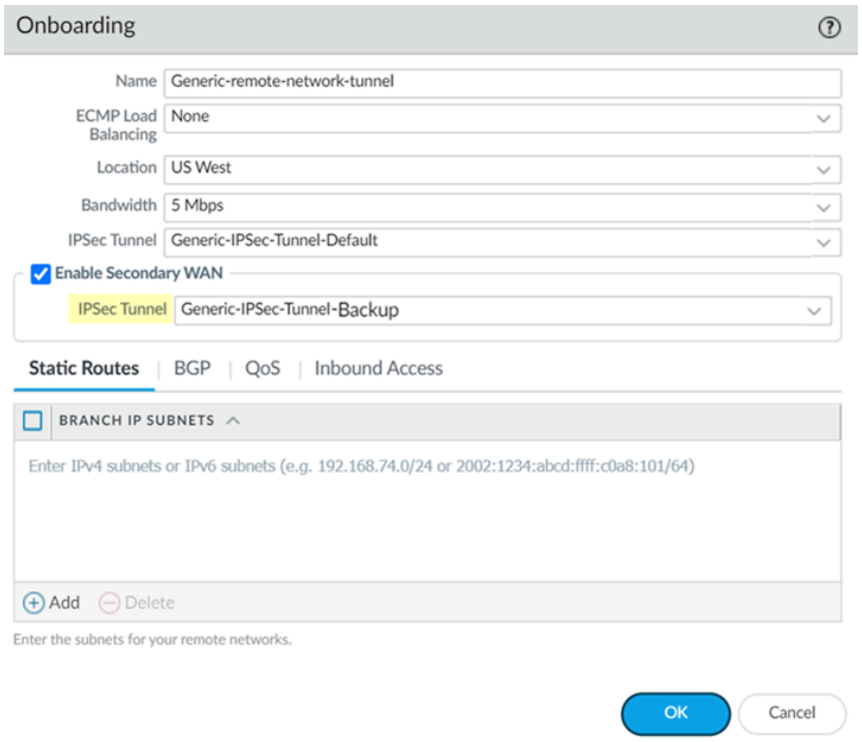


3. Créez un nouveau IPSec Tunnel (Tunnel IPSec), en spécifiant la nouvelle passerelle IKE que vous avez créée, mais en copiant tous les autres paramètres du modèle par défaut.



4. Lorsque vous intégrez la connexion aux services ou la connexion au réseau distant, cliquez sur **Enable Secondary WAN (Activer le WAN secondaire)** et spécifiez le tunnel que vous avez créé pour le WAN de sauvegarde.

 ©2025 Palo Alto Networks, Inc.



STEP 7 | Terminez la configuration de la connexion aux services ou de la connexion au réseau distant en faisant correspondre les cryptos, la clé pré-partagée et les identifiants de l'homologue sur le périphérique utilisé pour mettre fin à l'autre côté du tunnel IPSec.

STEP 8 | (Facultatif) Si vous devez intégrer plusieurs connexions aux réseaux distants qui utilisent les mêmes types de périphériques réseau, vous devez **Export (Exporter)** la configuration du réseau distant, éditer les paramètres, puis **Import (Importer)** cette configuration.

Profils cryptographiques IKE et IPSec pris en charge pour les périphériques SD-WAN courants

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Cette section vous fournit les profils de chiffrement pris en charge pour de nombreux périphériques SD-WAN courants. Si vous configurez un périphérique SD-WAN, utilisez ces profils comme guide pour savoir ce que vous pouvez configurer pour le réseau distant Prisma Access.

- Profils crypto IKE et IPSec pris en charge par Aruba SD-WAN
- Profils crypto IKE et IPSec pris en charge par Aryaka SD-WAN
- Profils crypto IKE et IPSec pris en charge par Citrix SD-WAN

 ©2025 Palo Alto Networks, Inc.

- Profils crypto IKE et IPSec pris en charge par le périphérique SD-WAN Prisma
- Profils crypto IKE et IPSec pris en charge par Nuage Networks SD-WAN
- Profils crypto IKE et IPSec pris en charge par Riverbed SteelConnect SD-WAN
- Profils crypto IKE et IPSec pris en charge par Silver Peak SD-WAN
- Profils crypto IKE et IPSec pris en charge par Viptela SD-WAN

 ©2025 Palo Alto Networks, Inc.

Prisma Access Connexions aux services

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Une connexion de service, également connue sous le nom de nœud d'accès d'entreprise (CAN), permet aux utilisateurs mobiles et aux utilisateurs de réseaux distants d'accéder à des applications et des ressources privées et permet à vos utilisateurs mobiles et à vos réseaux distants de communiquer entre eux.

En plus des connexions aux services, Palo Alto Networks vous fournit d'autres services que vous pouvez utiliser pour accéder à des applications privées :

- Connecteur ZTNA—Le connecteur Zero Trust Network Access (ZTNA) vous permet de vous connecter Prisma Access aux applications privées de votre entreprise de manière simple et sécurisée. Le connecteur ZTNA offre aux utilisateurs mobiles et aux utilisateurs des sites de succursales un accès à vos applications privées via un tunnel sécurisé automatisé. Vous pouvez également découvrir automatiquement les applications privées pour que ZTNA puisse assurer une protection à l'aide du Cloud Identity Engine.
- Prisma Access Colo-Connect—Colo-Connect vous permet d'utiliser Prisma Access pour sécuriser les applications privées à l'aide d'une interconnexion cloud capable de fournir des connexions aux services à large bande passante.

Palo Alto Networks recommande de toujours créer une connexion de service dans votre Prisma Access déploiement. Toutes les connexions aux services présentent les caractéristiques suivantes :

- Une connexion aux services permet d'accéder aux ressources de votre siège social ou de votre centre de données.

  Par exemple, si votre stratégie de sécurité exige l'authentification de l'utilisateur à l'aide d'un service d'authentification local, tel que votre Active Directory, vous devrez activer Prisma Access pour accéder à l'emplacement de l'entreprise où réside le service (et configurer un compte de service que le service peut utiliser pour y accéder). De même, si vous disposez de ressources d'entreprise auxquelles vos réseaux distants et vos utilisateurs mobiles devront accéder, vous devez activer Prisma Access pour accéder au réseau d'entreprise correspondant.

  Si vous créez des connexions aux services pour cette raison, vous devez planifier les connexions aux services avant de les implémenter.

- Une connexion aux services permet aux réseaux distants et aux utilisateurs mobiles de communiquer entre eux.

  Même si vous ne devez pas accéder à votre siège social ou à votre centre de données, vous devrez peut-être autoriser vos utilisateurs mobiles à accéder à vos emplacements réseau distants. Dans ce cas, vous pouvez créer une connexion aux services avec des valeurs d'espace réservé. Cela est nécessaire car, bien que toutes les connexions réseau distantes soient entièrement maillées, les utilisateurs mobiles se connectent à des réseaux distants à l'aide de la connexion aux services dans un réseau en étoile. Pour cette raison, vous pouvez également créer une connexion aux services avec des valeurs d'espace réservé si votre connexion aux services existante ne se trouve pas dans un emplacement géographique idéal.
- Les connexions aux services ne prennent pas en charge la localisation linguistique, car la sortie vers Internet n'est pas prise en charge sur les connexions aux services. Prisma Access n'attribue qu'un seul service adresse IP par connexion aux services, et que cette adresse IP est géographiquement enregistrée dans l'emplacement de calcul qui correspond à l'emplacement que vous spécifiez lors de l'intégration.

Le nombre de connexions aux services que vous recevez dépend de votre licence Prisma Access.

- Si vous disposez d'une licence ZTNA ou Enterprise, le nombre de connexions aux services dépend de l'édition de votre licence. Si vous disposez d'une édition locale, vous pouvez configurer maximum deux connexions aux services ; si vous disposez d'une édition mondiale, vous pouvez configurer maximum cinq connexions aux services.
  - Le connecteur ZTNA vous permet de vous connecter Prisma Access aux applications privées de votre organisation. Le connecteur ZTNA offre aux utilisateurs mobiles et aux utilisateurs des sites de succursales un accès à vos applications privées via un tunnel sécurisé automatisé. Pour plus d'informations, consultez Connecteur ZTNA Prisma Access.
- Si vous gérez plusieurs locataires et que vous disposez d'une licence ZTNA ou Enterprise, le nombre de connexions aux services par locataire dépend du nombre d'unités que vous allouez par locataire et du type de licence dont vous disposez.
  - Si vous disposez d'une licence mondiale et que vous allouez au moins 1 000 unités à un locataire, vous pouvez allouer un maximum de cinq connexions aux services à ce locataire.
  - Si vous disposez d'une licence mondiale et que vous allouez entre 200 et 999 unités à un locataire, vous pouvez allouer un maximum de deux connexions aux services à ce locataire (le même nombre de connexions que pour un déploiement local).
  - Si vous disposez d'une licence locale, vous pouvez allouer maximum deux connexions aux services par locataire, quel que soit le nombre d'unités que vous allouez au-delà du minimum de 200.

  Pour les licences mondiales et locales, vous pouvez acheter des licences supplémentaires pour les connexions aux services si nécessaire. Pour les connexions aux services dans les déploiements avancés, consultez Prisma Access Déploiements avancés de connexion aux services.

Avant de pouvoir commencer à configurer vos connexions aux services, passez en revue les informations que vous devez recueillir en premier.

 ©2025 Palo Alto Networks, Inc.

Planifier une connexion aux services

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Créez des connexions aux services pour autoriser Prisma Access à effectuer les tâches suivantes :

- **Autorisez l'accès aux ressources de votre siège social ou de votre centre de données.**

  Si vous disposez de ressources d'entreprise auxquelles vos réseaux distants et vos utilisateurs mobiles doivent accéder, vous devez activer Prisma Access pour accéder au réseau d'entreprise correspondant.
- **Autorisez les réseaux distants et les utilisateurs mobiles à communiquer entre eux.**

  Même si vous n'avez pas besoin que vos utilisateurs Prisma Access se connectent à votre siège social ou à votre centre de données, vous pourriez devoir autoriser vos utilisateurs mobiles à accéder à vos sites réseau distants. Les connexions aux services sont nécessaires pour ce cas d'utilisation parce que, bien que tous les sites de réseau distant soient entièrement maillés, l'infrastructure des utilisateurs mobiles ne l'est pas. La configuration minimale d'une connexion aux services établit le réseau en étoile dont les utilisateurs mobiles ont besoin pour accéder à un réseau de succursale.

  Pour améliorer l'efficacité du réseau, placez les connexions aux services près du réseau distant ou des réseaux auxquels les utilisateurs mobiles accèdent le plus fréquemment.

Rassembler ces informations sur le HQ ou le centre de données

Avant de commencer à configurer une connexion aux services, rassemblez les informations suivantes pour chacun de vos sièges sociaux ou centres de données auxquels vous souhaitez que Prisma Access puisse se connecter.

Vous n'avez pas besoin de rassembler ces informations si vous créez une connexion aux services uniquement pour autoriser les utilisateurs mobiles à accéder à des emplacements de réseau distant.

Pour les connexions aux services **Prisma Access (Managed by Strata Cloud Manager)** et **Prisma Access (Managed by Panorama)** :

- ❑ Connexion d'un pare-feu, d'un routeur ou d'un périphérique SD-WAN compatible avec IPSec sur le site de votre entreprise.
- ❑ Paramètres IPSec pour terminer le tunnel VPN principal depuis Prisma Access vers le périphérique compatible avec IPSec sur le réseau de votre entreprise.

 ©2025 Palo Alto Networks, Inc.

- Paramètres IPSec pour terminer le tunnel VPN secondaire depuis Prisma Access vers le périphérique compatible avec IPSec de votre réseau d'entreprise.

  Si vous avez un modèle existant contenant des configurations de tunnel IPSec, de surveillance de tunnel et de profil crypto IPSec, vous pouvez ajouter ce modèle à la pile de modèles pour simplifier le processus de création des tunnels IPSec. Sinon, vous pouvez modifier le Service_Conn_Template qui est créé automatiquement et créer les configurations IPSec nécessaires pour établir le tunnel IPSec vers le site de l'entreprise. Prisma Access vous fournit également un ensemble de modèles IPSec prédéfinis pour certains périphériques réseau couramment utilisés, ainsi qu'un modèle générique pour tout périphérique qui n'est pas inclus dans les modèles prédéfinis.
- Liste des sous-réseaux IP sur le site.
- Liste des domaines internes que Prisma Access doit pouvoir résoudre.
- Adresse IP d'un nœud d'accès d'entreprise sur le site de votre réseau auquel Prisma Access peut envoyer des requêtes ping ICMP pour la surveillance du tunnel IPSec.

  Assurez-vous que cette adresse est accessible par ICMP depuis l'ensemble du sous-réseau d'infrastructure Prisma Access.
- Paramètres de connectivité réseau pour le sous-réseau d'infrastructure de service.

  Rendez l'ensemble du sous-réseau d'infrastructure de service accessible depuis le siège social ou le centre de données. Prisma Access utilise des adresses IP pour tout le trafic du plan de contrôle provenant de ce sous-réseau.

Pour les **connexions aux services Prisma Access Panorama uniquement :**

*Cette information n'est requise que lors de la planification des connexions aux services dans **Prisma Access (Managed by Panorama)**.*

- Le compte de service pour votre authentification, si nécessaire pour l'accès.
- Le type de routage (soit statique soit dynamique (BGP)) à utiliser avec les connexions aux services.

  Pour que Prisma Access (Managed by Panorama) achemine les utilisateurs vers les ressources dont ils ont besoin, vous devez fournir les itinéraires vers les ressources. Vous pouvez le faire de l'une des façons suivantes :

  - Définissez un itinéraire statique vers chaque sous-réseau ou ressource spécifique auxquels vous souhaitez que vos utilisateurs puissent accéder.
  - Configurez BGP entre vos emplacements de connexion aux services et Prisma Access.
  - Utilisez une combinaison des deux méthodes

 ©2025 Palo Alto Networks, Inc.

Configurer une connexion aux services dans Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Créez des connexions aux services pour autoriser Prisma Access à effectuer les tâches suivantes :

- **Autorisez l'accès aux ressources de votre siège ou de votre centre de données.**

  Si vous disposez de ressources d'entreprise auxquelles vos réseaux distants et vos utilisateurs mobiles doivent accéder, vous devez activer Prisma Access pour accéder au réseau d'entreprise correspondant. Avant de commencer à configurer une connexion aux services, rassemblez les informations suivantes pour chacun de vos sièges sociaux ou centres de données auxquels vous souhaitez que Prisma Access puisse se connecter.

  - Connexion d'un pare-feu, d'un routeur ou d'un périphérique SD-WAN compatible avec IPSec sur le site de votre entreprise.
  - Paramètres IPSec pour terminer le tunnel VPN principal depuis Prisma Access vers le périphérique compatible IPSec sur le réseau de votre entreprise.
  - Paramètres IPSec pour terminer le tunnel VPN secondaire depuis Prisma Access vers le périphérique compatible IPSec de votre réseau d'entreprise.

    Si vous avez un modèle existant contenant des configurations de tunnel IPSec, de surveillance de tunnel et de profil crypto IPSec, vous pouvez ajouter ce modèle à la pile de modèles pour simplifier le processus de création des tunnels IPSec. Sinon, vous pouvez modifier le Service_Conn_Template qui est créé automatiquement et créer les configurations IPSec nécessaires pour établir le tunnel IPSec vers le site de l'entreprise. Prisma Access vous fournit également un ensemble de modèles IPSec prédéfinis pour certains périphériques réseau couramment utilisés, ainsi qu'un modèle générique pour tout périphérique qui n'est pas inclus dans les modèles prédéfinis.
  - Liste des sous-réseaux IP sur le site.
  - Liste des domaines internes que Prisma Access doit pouvoir résoudre.
  - Adresse IP d'un nœud d'accès d'entreprise sur le site de votre réseau auquel Prisma Access peut envoyer des requêtes ping ICMP pour la surveillance du tunnel IPSec.

    Assurez-vous que cette adresse est accessible par ICMP depuis l'ensemble du sous-réseau d'infrastructure Prisma Access.
  - Paramètres de connectivité réseau pour le sous-réseau d'infrastructure de service.

    Rendez l'ensemble du sous-réseau d'infrastructure de service accessible depuis le siège ou le centre de données. Prisma Access utilise des adresses IP pour tout le trafic du plan de contrôle provenant de ce sous-réseau.

 ©2025 Palo Alto Networks, Inc.

- (Pour Prisma Access (Managed by Panorama) uniquement) Le compte de service pour votre authentification, si nécessaire pour l'accès.
- (Pour Prisma Access (Managed by Panorama) uniquement) Le type de routage (soit statique soit dynamique (BGP)) à utiliser avec les connexions aux services.
- (Pour Prisma Access (Managed by Panorama) uniquement) Pour acheminer les utilisateurs vers les ressources dont ils ont besoin, vous devez fournir les itinéraires vers les ressources. Vous pouvez le faire de l'une des façons suivantes :
  - Définissez un itinéraire statique vers chaque sous-réseau ou ressource spécifique auxquels vous souhaitez que vos utilisateurs puissent accéder.
  - Configurez BGP entre vos emplacements de connexion aux services et Prisma Access.
  - Utilisez une combinaison des deux méthodes.

- **Autorisez les réseaux distants et les utilisateurs mobiles à communiquer entre eux.**

  Même si vous n'avez pas besoin que vos utilisateurs Prisma Access se connectent à votre siège ou à votre centre de données, vous pourriez avoir besoin de permettre à vos utilisateurs mobiles d'accéder à vos sites réseau distants. Les connexions aux services sont nécessaires pour ce cas d'utilisation parce que, bien que tous les sites réseau distants soient entièrement maillés, l'infrastructure des utilisateurs mobiles ne l'est pas. La configuration minimale d'une connexion aux services établit le réseau en étoile dont les utilisateurs mobiles ont besoin pour accéder à un réseau de succursale.

  Pour améliorer l'efficacité du réseau, placez les connexions aux services près du réseau distant ou des réseaux auxquels les utilisateurs mobiles accèdent le plus fréquemment.

- Strata Cloud Manager
- Panorama

Configurer une connexion aux services dans Prisma Access (Strata Cloud Manager)

Pour configurer une connexion aux services pour Prisma Access (Managed by Strata Cloud Manager) pour autoriser l'accès aux applications privées ou aux ressources internes de l'entreprise, procédez comme suit.

STEP 1 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connections (Connexions aux services))** et **Add Service Connection (Ajouter une connexion aux services)**.

STEP 2 | Donnez à la connexion aux services un **Name (Nom)** descriptif.

STEP 3 | Sélectionnez le **Prisma Access Location (Emplacement Prisma Access)** de votre siège ou de votre centre de données.

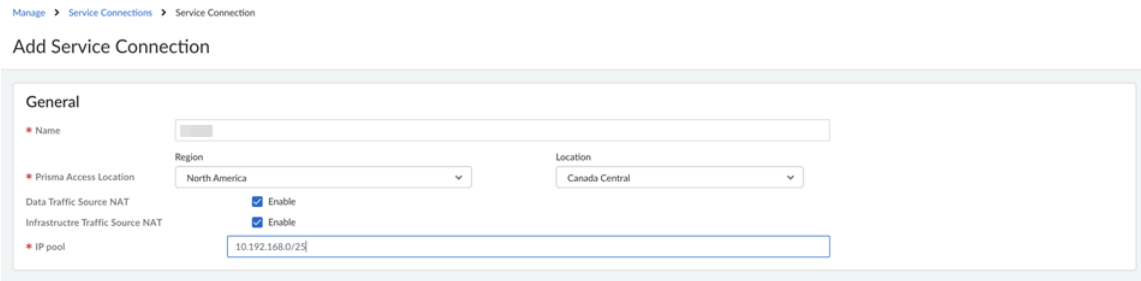
 ©2025 Palo Alto Networks, Inc.

STEP 4 | (Facultatif) Activez le NAT source pour les utilisateurs mobiles : adresses du pool d'adresses IP GlobalProtect, adresses IP dans le sous-réseau Infrastructure, ou les deux.

Vous pouvez spécifier un sous-réseau au niveau d'une ou plusieurs connexions aux services utilisées pour le trafic NAT entre les utilisateurs mobiles Prisma Access GlobalProtect et les applications et ressources privées d'un centre de données.

- **Data Traffic source NAT (NAT source de trafic de données)** : effectue le NAT sur les adresses du pool d'adresses IP des utilisateurs mobiles afin qu'elles ne soient pas annoncées au centre de données et que seuls les sous-réseaux que vous spécifiez aux connexions aux services soient annoncés et acheminés dans le centre de données.
- **Infrastructure Traffic source NAT (NAT source de trafic d'infrastructure)** : effectue le NAT sur les adresses du sous-réseau d'infrastructure afin qu'elles ne soient pas annoncées au centre de données et que seuls les sous-réseaux que vous spécifiez aux connexions aux services soient annoncés et acheminés dans le centre de données.
- **User-ID** : lorsque cette option est sélectionnée, Prisma Access utilise cette connexion aux services pour la redistribution de l'identité.

  ***User-ID Redistribution Management (Gestion de la redistribution de User-ID)** : parfois, des contrôles précis sont nécessaires pour la redistribution des User-ID dans les déploiements Prisma Access à particulièrement grande échelle. La gestion de la redistribution de User-ID vous permet de désactiver manuellement le comportement de redistribution d'identité par défaut pour certaines connexions aux services en retirant la coche dans la colonne **User ID (ID utilisateur)**, puis sélectionnez les connexions aux services spécifiques à utiliser pour la redistribution de l'identité. Il n'est pas nécessaire de le faire pour la plupart des configurations. Contactez le support de Palo Alto Networks pour activer cette fonctionnalité.*
- **Source NAT Pool (Pool de NAT source)** : spécifie le pool d'adresses IP utilisé pour effectuer le NAT sur le pool d'adresses IP des utilisateurs mobiles, le sous-réseau d'infrastructure ou les deux.
  - Utilisez un sous-réseau privé d'adresses IP (RFC 1918) ou un sous-réseau approprié qui peut être acheminé dans votre domaine de routage.
  - Assurez-vous que le sous-réseau ne chevauche pas le pool d'adresses IP des Utilisateurs mobile — GlobalProtect, le sous-réseau d'infrastructure ou toute autre adresse NAT source utilisée pour ce locataire.
  - Entrez un sous-réseau entre /25 et /32.



 ©2025 Palo Alto Networks, Inc.

STEP 5 | Sélectionnez un **IPSec Tunnel (Tunnel IPSec)**. Si vous n'avez pas encore configuré de tunnel IPSec principal ou secondaire, sélectionnez **Set Up (Configurer)** et suivez les étapes ci-dessous.

1. Donnez au tunnel un **nom**descriptif.
2. Sélectionnez le **Branch Device Type (Type de périphérique de branche)** pour le périphérique IPSec et le siège ou le centre de données que vous utilisez pour établir le tunnel avec Prisma Access.
3. Pour l'**adresse IP du périphérique de branche**, choisissez d'utiliser soit une adresse **IP statique** qui identifie le terminal du tunnel, soit une adresse IP **dynamique**.

   Si vous définissez **Branch Device IP Address (Adresse IP du périphérique de branche)** sur **Dynamic (Dynamique)**, vous devez également ajouter l'ID IKE du siège ou du centre de données (**IKE Local Identification (Identification locale IKE)**) ou pour Prisma Access (**IKE Peer Identification (Identification d'homologue IKE)**) pour permettre aux homologues IPSec de s'authentifier.

   Étant donné que vous ne disposez pas des valeurs à utiliser pour l'ID IKE Prisma Access (**IKE Peer Identification (Identification de l'homologue IKE)**) tant que la connexion aux services n'est pas entièrement déployée, vous devez généralement définir l'ID IKE pour le siège ou le centre de données (**IKE Local Identification (Identification locale IKE)**) plutôt que l'ID IKE Prisma Access.

STEP 6 | Activez la **Tunnel Monitoring (Surveillance des tunnels)**.

Entrez une adresse **Destination IP (IP de destination)** de surveillance du tunnel sur le réseau du siège ou du centre de données pour que Prisma Access puisse l'utiliser pour déterminer si le tunnel est actif et, si votre périphérique IPSec de branche utilise un VPN basé sur des politiques, entrez le **Proxy ID (ID de proxy)** associé.

L'adresse IP de surveillance du tunnel que vous saisissez est automatiquement ajoutée à la liste des sous-réseaux de succursale.

STEP 7 | **Enregistrez** les paramètres du tunnel.

STEP 8 | Pour ajouter des paramètres de routage et de qualité de service ou les modifier, accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connections (Connexions aux services)**et **Add Service Connection (Ajouter une connexion aux services)**. Vous pouvez **Set Up (Configurer)** ou **Edit (Modifier)** les paramètres de **Routing (Routage)** ou de **QoS**.

STEP 9 | Configurez des itinéraires statiques.

1. Pour que les itinéraires statiques acheminent le trafic vers et depuis votre siège social ou centre de données, cliquez sur **Add (Ajouter)** pour ajouter les sous-réseaux IP ou les adresses IP que vous voulez sécuriser au niveau de la succursale.

   Si vous apportez des modifications aux sous-réseaux IP de votre réseau de siège social ou de centre de données, vous devez mettre à jour les itinéraires statiques manuellement.

 ©2025 Palo Alto Networks, Inc.

STEP 10 | Configurez le routage dynamique.

1. Pour que le routage dynamique publie les sous-réseaux du siège social ou du centre de données, vous devez **Enable BGP for Dynamic Routing (Activer BGP pour le routage dynamique)**.
2. (Facultatif) Sélectionnez une valeur **MRAI Timer (Minuterie MRAI)**.

   Le routage BGP propose un minuteur que vous pouvez utiliser pour adapter la convergence du routage BGP dans votre réseau, appelé *Intervalle minimum de publication d'itinéraire (MRAI)*. MRAI agit pour limiter le débit des mises à jour par destination, et les routeurs BGP attendent au moins le délai MRAI configuré avant d'envoyer une publication pour le même préfixe. Un nombre plus petit vous donne un temps de convergence plus rapide, mais crée plus de publications sur votre réseau. Un nombre plus élevé diminue le nombre de publications pouvant être envoyées, tout en ralentissant également la convergence de routage. Vous décidez du nombre à mettre dans votre réseau pour obtenir le meilleur équilibre entre une convergence de routage plus rapide et moins de publications.

   Configurez une plage MRAI comprise entre 1 et 600 secondes, avec une valeur par défaut de 30 secondes.
3. Pour réduire le nombre de publications de sous-réseaux IP d'utilisateurs mobiles via BGP vers l'équipement de vos locaux client (Customer Premises Equipment, CPE), spécifiez Prisma Access pour résumer les sous-réseaux avant de les annoncer en sélectionnant **Summarize Mobile User Routes before advertising (Résumer les itinéraires des utilisateurs mobiles avant de les annoncer)**.

   Par défaut, Prisma Access publie les pools d'adresses IP des utilisateurs mobiles par blocs de sous-réseaux /24. Si vous les résumez, Prisma Access publie le pool en fonction du sous-réseau que vous avez spécifié. Par exemple, Prisma Access publie un pool d'adresses IP mobiles d'utilisateurs publics de 10.8.0.0/20 en utilisant le sous-réseau /20, plutôt que de diviser le pool en sous-réseaux de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, et ainsi de suite, avant de les publier. Le résumé de ces publications peut réduire le nombre d'itinéraires stockés dans les tableaux de routage CPE. Par exemple, vous pouvez utiliser le résumé de pool d'adresses IP avec des passerelles VPN cloud (passerelles privées virtuelles [VGW] ou passerelles de transit [TGW]) qui peuvent accepter un nombre limité d'itinéraires.
4. (Facultatif) Pour que Prisma Access génère une publication d'itinéraire par défaut pour le réseau distant à l'aide d'eBGP, sélectionnez **Advertise the Default Route (Publier l'itinéraire par défaut)**. Assurez-vous que votre réseau n'a pas un autre itinéraire par défaut publié par BGP, sinon vous pourriez introduire des problèmes de routage dans votre réseau.
5. (Facultatif) Si vous avez configuré un WAN secondaire et que vous devez modifier l'adresse de l'homologue BGP secondaire (de secours), sélectionnez **Use different BGP Peer for Secondary Tunnel (Utiliser un homologue BGP différent pour le tunnel secondaire)** et saisissez un homologue unique et, éventuellement, une adresse IP locale pour le WAN secondaire.
6. Pour ajouter une communauté des connexions aux services aux préfixes sortants des homologues eBGP de l'équipement des locaux client (Customer Premises Equipment,

 ©2025 Palo Alto Networks, Inc.

CPE), définissez **Add no-export community (Ajouter une communauté de non-export)** sur **Enabled Out (Sortie activée)**. Cette option est **Disabled (Désactivée)** par défaut.

Ne sélectionnez pas **Enabled In (Activé dans)** ou **Enabled Both (Activé les deux)**, car ces choix ne sont pas pris en charge.

7. (Facultatif) Sélectionnez **Do Not Export Routes (Ne pas exporter les itinéraires)** pour empêcher Prisma Access de transférer les itinéraires vers le siège social ou le centre de données.

   Par défaut, Prisma Access publie toutes les informations de routage BGP, y compris les itinéraires locaux et tous les préfixes qu'il reçoit d'autres connexions aux services, réseaux distants et sous-réseaux d'utilisateurs mobiles. Cochez cette case pour empêcher Prisma Access d'envoyer des annonces BGP, mais pour qu'il utilise toujours les informations BGP qu'il reçoit pour apprendre les itinéraires d'autres voisins BGP.

   Parce que Prisma Access n'envoie pas de publications BGP, si vous sélectionnez cette option, vous devez configurer des itinéraires statiques sur votre équipement sur site pour établir des itinéraires de retour vers Prisma Access.

8. Saisissez la **Peer IP Address (Adresse IP de l'homologue)** attribuée comme ID de routeur du routeur eBGP sur le réseau du siège social ou du centre de données.
9. Saisissez le **Peer AS (AS homologue)**, qui est le système autonome (AS) de votre réseau.

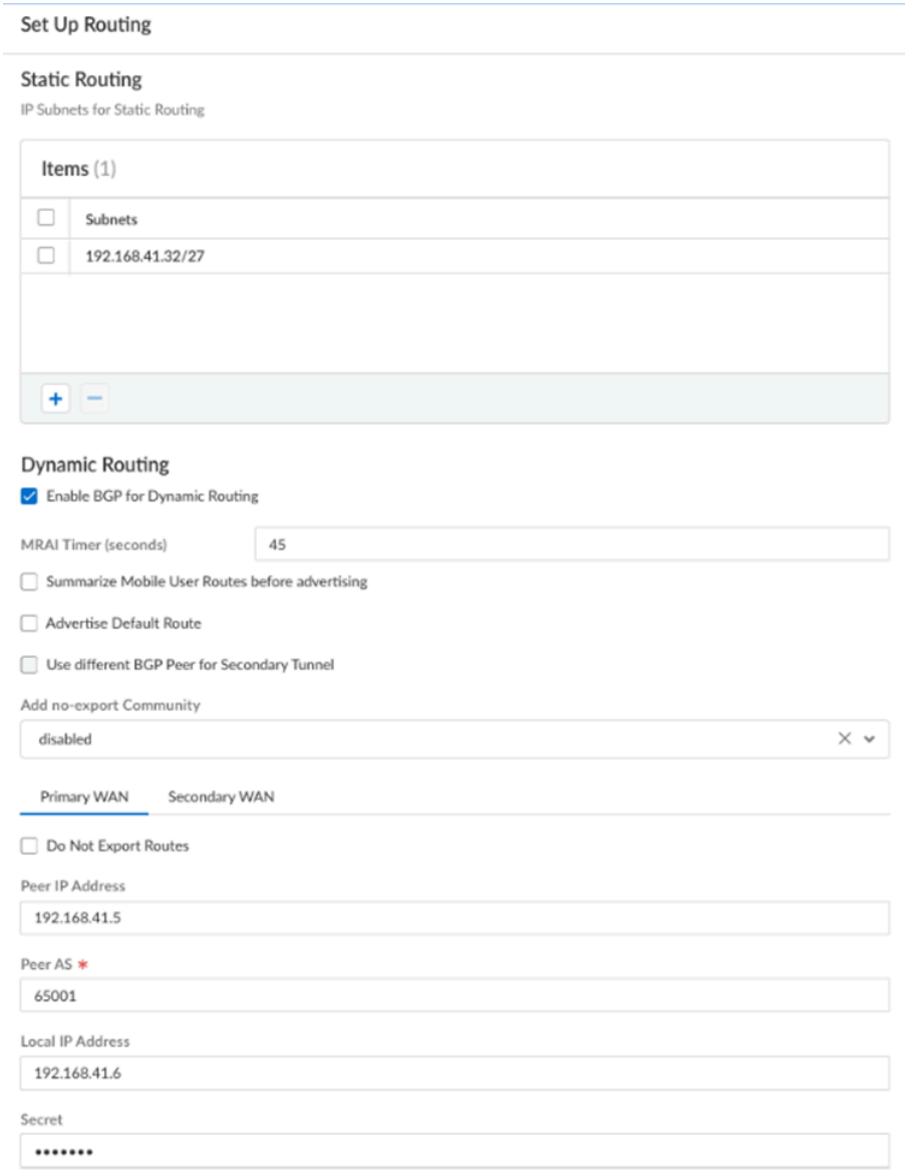
   Utilisez un numéro AS privé BGP conforme à la RFC 6996.

10. Saisissez la **Local IP Address (Adresse IP locale)** qui est utilisée par Prisma Access comme adresse IP locale pour BGP.

    Une adresse locale n'est requise que si votre périphérique de siège social ou de centre de données en a besoin pour que l'appairage BGP réussisse. Assurez-vous que l'adresse que vous spécifiez ne soit pas en conflit ou ne chevauche pas les adresses IP dans le sous-réseau d'infrastructure ou les sous-réseaux du réseau distant.
11. Saisissez un mot de passe **Secret (Phrase secrète)** pour authentifier les communications de l'homologue BGP.

 ©2025 Palo Alto Networks, Inc.

12. Sélectionnez **Confirm Secret (Confirmer la phrase secrète)**.

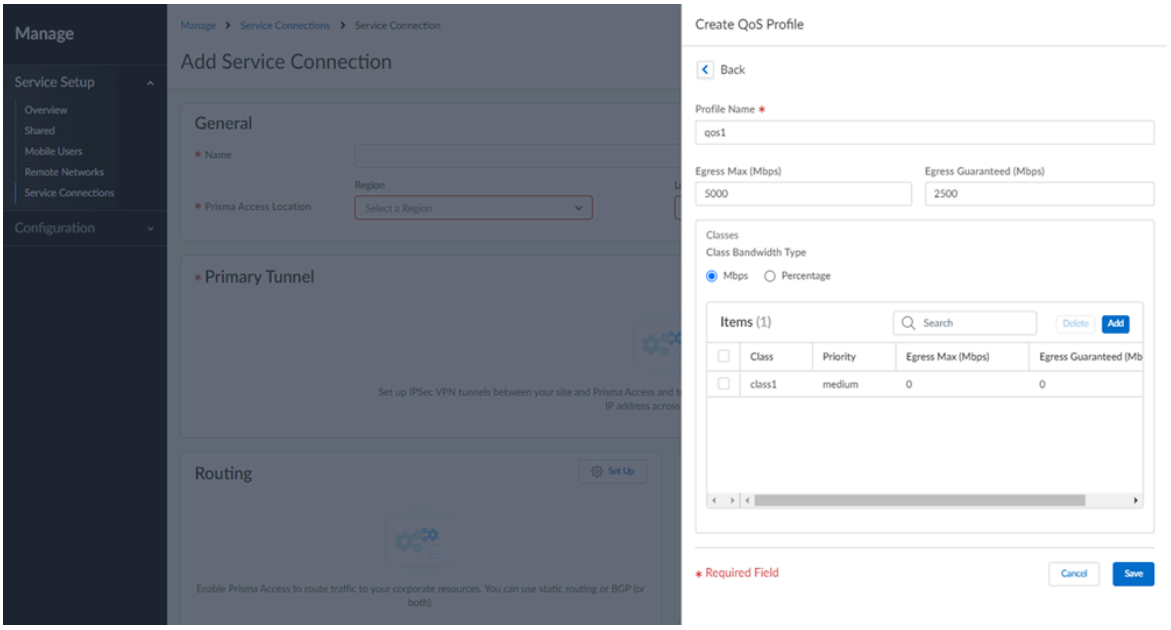


STEP 11 | (Facultatif) Configurez la QoS.

Pour commencer, ajoutez un profil QoS pour définir les classes QoS qui façonneront le trafic entre le siège ou le centre de données et Prisma Access. Vous allez ensuite créer une règle

 ©2025 Palo Alto Networks, Inc.

de politique QoS et ajouter le profil à la règle afin d'appliquer la QoS au trafic du siège ou du centre de données correspondant.



1. Entrez un nom pour votre **QoS Profile (Profil QoS)**.
2. Sélectionnez **Create New (Créer nouveau)**.
3. Définissez le débit maximal (en Mbit/s) pour le trafic quittant la connexion aux services du siège ou du centre de données en tant que **Egress Max (Sortie max.)**.

   Vous pouvez spécifier une valeur allant jusqu'à la bande passante maximale sous licence de votre siège ou de votre centre de données.
4. Définissez la bande passante garantie comme la **Egress Guaranteed (Sortie garantie)** (en Mbit/s).

   L'acheminement du trafic dépassant la valeur Egress Guaranteed (Sortie garantie) se fait dans la mesure du possible, mais il n'est pas garanti. Toute bande passante garantie et inutilisée reste disponible pour l'ensemble du trafic.
5. Définissez chaque **Class (Classe)** QoS et associez-la à une règle de politique.

   Une classe QoS détermine la priorité et la bande passante du trafic correspondant à une règle de politique QoS. Jusqu'à huit classes QoS peuvent être définies dans un même

 ©2025 Palo Alto Networks, Inc.

profil QoS. Sauf configuration contraire, le trafic ne correspondant pas à une classe QoS est affecté à la classe 4.

6. Configurez la **Priority (Priorité)** d'une classe QoS.

   Les différents niveaux de priorité sont : temps réel, élevée, moyenne ou faible.

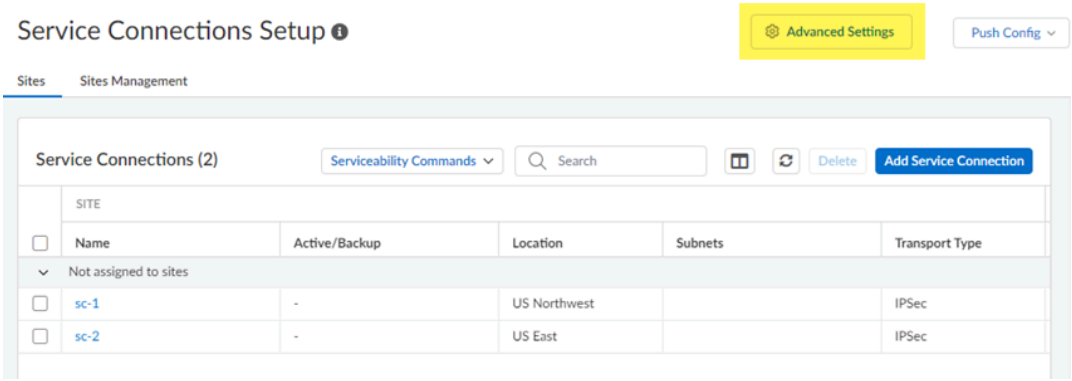
7. Configurez la valeur **Egress Max (Sortie max.)**.

   La valeur maximale de sortie d'une classe QoS ou les valeurs maximales de sortie combinées pour plusieurs classes QoS ne doivent pas dépasser la valeur maximale de sortie du profil QoS.

8. Configurez la valeur **Egress Guaranteed (Sortie garantie)**.

   La bande passante garantie attribuée à la classe QoS n'est pas réservée à cette classe. La bande passante inutilisée reste disponible pour tout le trafic. Lorsque le trafic de la classe dépasse la valeur Egress Guaranteed (Sortie garantie), son acheminement se fait dans la mesure du possible, mais il n'est pas garanti.

STEP 12 | Configurez les **Advanced Settings (Paramètres avancés)** pour votre connexion aux services.



1. Spécifiez les **BGP Routing Preferences (Préférences de routage BGP)** à utiliser avec des connexions aux services.

   Vous pouvez spécifier des préférences réseau pour utiliser le réseau de votre organisation ou bien le réseau Prisma Access pour traiter le trafic de connexion aux services.

   - **Default (Défaut)** : Prisma Access utilise le routage par défaut dans son réseau interne.
   - **Hot potato routing (Routage hot potato)** :Prisma Access désactive le trafic de connexion aux services vers le WAN de votre organisation le plus rapidement possible.

   La modification de la méthode de routage des connexions aux services Prisma Access nécessite une compréhension approfondie de la topologie et des périphériques de routage de votre organisation, ainsi qu'une compréhension du fonctionnement du routage Prisma Access. Nous vous recommandons de lire attentivement les Routage pour le trafic de connexion aux services *avant de changer la méthode de routage par défaut.*

2. **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down (Retirer les itinéraires statiques si le tunnel IPSec de la connexion aux services ou des**

 ©2025 Palo Alto Networks, Inc.

réseaux distants est en panne) si vous souhaitez que Prisma Access supprime les routes statiques lorsqu'un tunnel tombe sans tunnel de secours.

Prisma Access supprime l'itinéraire dans les situations suivantes :

- Le tunnel principal descend et il n'y a pas de tunnel secondaire.
- Un tunnel principal et un tunnel secondaire sont configurés, mais les deux tombent en panne.

Vous ne pouvez pas appliquer cette modification si la surveillance du tunnel n'est pas activée.

3. Configurez le **Backbone Routing (Routage principal)** à utiliser pour les connexions aux services.

   Par défaut, la dorsale Prisma Access nécessite que vous disposiez d'un chemin d'accès réseau symétrique pour le trafic revenant du centre de données ou de l'emplacement du siège par le biais d'une connexion aux services. Si vous souhaitez utiliser ECMP ou un autre mécanisme d'équilibrage de charge pour les connexions aux services à partir de votre CPE, vous pouvez activer des flux asymétriques à travers la dorsale Prisma Access.

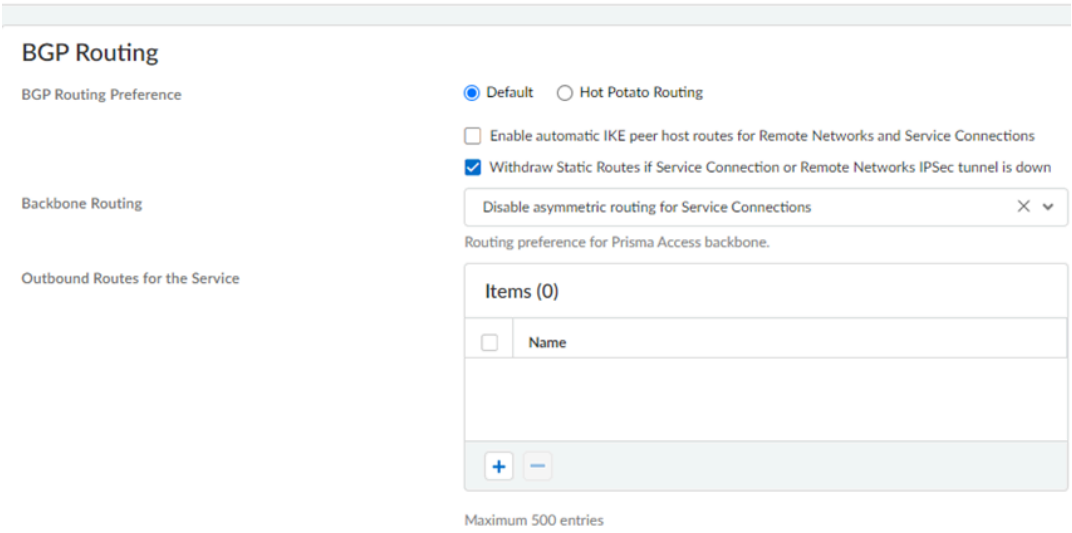
   - Sélectionnez **Disable asymmetric routing for Service Connections (Désactiver le routage asymétrique pour les connexions aux services)** pour exiger des flux symétriques sur la dorsale de connexion aux services.
   - Sélectionnez **Allow asymmetric routing for Service Connections (Autoriser le routage asymétrique pour les connexions aux services)** pour autoriser Prisma Access à utiliser des flux asymétriques sur la dorsale de connexion aux services.
   - Si vous avez plusieurs connexions aux services à un emplacement, vous pouvez tirer parti de l'équilibrage de charge dans votre déploiement Prisma Access en sélectionnant **Allow asymmetric routing and load sharing across Service Connections (Autoriser le routage asymétrique et le partage de charge entre les connexions aux services)** (paramètre par défaut). Cependant, l'équilibrage des charges se fait dans la mesure du possible et il échouera si l'une des connexions aux services tombe en panne.

     Lorsque vous sélectionnez **Allow asymmetric routing and load sharing across Service Connections (Autoriser le routage asymétrique et le partage de charge entre les connexions aux services)**, Prisma Access permet la redondance du réseau entre les portails et les passerelles GlobalProtect, et les connexions aux services. Cette fonctionnalité fournit des chemins réseau redondants entre le plan de données des utilisateurs mobiles et les connexions aux services dans différents emplacements de calcul. L'activation de la redondance offre aux utilisateurs un accès plus résilient aux ressources derrière les connexions aux services dans un centre de données ou des emplacements du siège. Étant donné qu'une connexion aux services est nécessaire pour que les utilisateurs mobiles puissent accéder aux ressources à partir de réseaux distants, les utilisateurs ont également une plus grande résilience pour accéder aux ressources dans des emplacements de réseaux distants.

4. (Facultatif) Spécifiez les **Outbound Routes for the Service (Max 500) (Routes sortantes pour le service (max. 500))** en ajoutant jusqu'à 500 préfixes pour lesquels Prisma Access

 ©2025 Palo Alto Networks, Inc.

ajoute des itinéraires statiques sur toutes les connexions aux services et les connexions réseau distantes. Prisma Access achemine ensuite le trafic vers ces préfixes sur Internet.



Plus d'options IKE

En fonction du type de périphérique IPSec que vous avez sélectionné, Prisma Access fournit un ensemble recommandé de chiffrements et une durée de vie de clé pour le processus d'échange de clés IKE de la phase 1 entre le périphérique à votre siège/centre de données et Prisma Access. Vous pouvez utiliser les paramètres recommandés ou personnaliser les paramètres en fonction de vos besoins.

- Sélectionnez une **IKE Protocol Version (Version du protocole IKE)** pour votre périphérique IPSec et Prisma Access à utiliser pour la négociation IKE.

  Si vous sélectionnez **IKEv1 Only Mode (Mode IKEv1 uniquement)**, Prisma Access ne peut utiliser que le protocole IKEv1 pour la négociation. Si vous sélectionnez **IKEv2 Only Mode (Mode IKEv2 uniquement)**, Prisma Access ne peut utiliser que le protocole IKEv2 pour la négociation. Si vous sélectionnez **IKEv2 Preferred Mode (Mode IKEv2 préféré)**, Prisma Access utilise le protocole IKEv2 uniquement si votre périphérique IPSec prend également en charge IKEv2. Si votre périphérique IPSec ne prend pas en charge IKEv2, Prisma Access revient à l'utilisation du protocole IKEv1.

 ©2025 Palo Alto Networks, Inc.

- Ajoutez un **profil crypto IKEv1** pour personnaliser les paramètres de chiffrement IKE qui définissent les algorithmes de chiffrement et d'authentification utilisés pour le processus d'échange de clés dans la phase 1 du protocole IKE.

  Prisma Access utilise automatiquement un profil crypto IKE par défaut basé sur le **Branch Device Type (Type de périphérique de branche)** utilisé pour établir ce tunnel.

  - **Chiffrement** : spécifiez l'algorithme de chiffrement utilisé dans la négociation IKE SA.

    Prisma Access prend en charge les algorithmes de chiffrement suivants : 3DES (168 bits), AES-128-CBC (128 bits), AES-192-CBC (192 bits), AES-256-CBC (256 bits) et DES (56 bits). Vous pouvez également sélectionner null (aucun chiffrement).
  - **Authentification** : spécifiez l'algorithme d'authentification utilisé dans la négociation IKE SA.

    Prisma Access prend en charge les algorithmes d'authentification suivants : sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits) et md5 (128 bits). Vous pouvez également sélectionner null (pas d'authentification).
  - **Groupe DH** : spécifiez les groupes Diffie-Hellman (DH) utilisés pour générer des clés symétriques pour IKE dans la négociation IKE SA. L'algorithme Diffie-Hellman utilise la clé privée d'une partie et la clé publique de l'autre pour créer un secret partagé, qui est une clé cryptée partagée par les deux homologues du tunnel PN.

    Prisma Access prend en charge les groupes DH suivants : Groupe 1 (768 bits), Groupe 2 (1 024 bits par défaut), Groupe 5 (1 536 bits), Groupe 14 (2 048 bits), Groupe 19 (groupe de courbes elliptiques 256 bits) et Groupe 20 (groupe de courbes elliptiques 384 bits). Pour obtenir la sécurité la plus forte, sélectionnez le groupe avec le nombre le plus élevé.
  - **Durée de vie** : spécifiez l'unité et la durée de validité de la clé de la phase 1 du protocole IKE (8 heures par défaut). Pour IKEv1, l'association de sécurité (Security Association, SA) ne fait pas l'objet d'un changement de clé avant l'expiration de la durée de vie de la clé. Le changement de clef de la phase 1 du protocole IKEv1 se déclenche uniquement lorsque la SA expire. Pour IKEv2, la SA doit être faire l'objet d'un changement de clef avant l'expiration de la durée de vie de la clé. Si la SA ne fait pas l'objet d'un changement de clé à l'expiration, elle doit commencer une nouvelle clé de phase 1.
  - **IKEv2 Authentication Multiple (Multiple d'authentification IKEv2)** : spécifiez la valeur multipliée par la durée de vie de la clé pour déterminer le nombre d'authentifications (plage de 0 à 50 ; valeur par défaut de 0). Le nombre d'authentifications est le nombre de fois où le nœud de traitement de sécurité peut effectuer un changement de clé SA IKE IKEv2 avant de devoir recommencer la réauthentification IKEv2. Une valeur par défaut de 0 désactive la fonctionnalité de réauthentification.

- Activez **IKE Passive Mode (Mode IKE passif)** afin que Prisma Access ne réponde qu'aux connexions IKE et ne les lance pas.

- **IKE NAT Traversal** est activé par défaut.

  Cela signifie que l'encapsulation UDP est utilisée sur les protocoles IKE et UDP, ce qui leur permet de passer par des périphériques de traduction d'adresse réseau (Network Address Translation, NAT) situés entre les terminaux du tunnel VPN IPSec.

 ©2025 Palo Alto Networks, Inc.

Plus d'options IPSec

En fonction du type de périphérique IPSec que vous avez sélectionné, Prisma Access fournit un ensemble recommandé de paramètres de protocole IPSec et de durée de vie de la clé pour sécuriser les données dans le tunnel IPSec entre votre périphérique IPSec et Prisma Access dans la phase 2 du protocole IKE pour l'association de sécurité (Security Association, SA). Vous pouvez utiliser les paramètres recommandés ou personnaliser les paramètres en fonction de vos besoins.

- Personnalisez le **profil crypto IPSec** pour définir comment les données sont sécurisées dans le tunnel lorsque Auto Key IKE génère automatiquement des clés pour les SA IKE pendant la phase 2 du protocole IKE.

  Prisma Access configure automatiquement un profil crypto IPSec par défaut en fonction du fournisseur du **Branch Device Type (Type de périphérique de branche)**. Vous pouvez utiliser le profil par défaut ou créer un profil personnalisé.

  - **Protocole IPSec** : sécurisez les données qui traversent le tunnel VPN. **ESP** : le protocole ESP (Encapsulating Security Payload/Encapsulation sécurisée de la charge utile) crypte les données, authentifie la source et vérifie l'intégrité des données. **AH** : le protocole AH (Authentication Header/En-tête d'authentification) authentifie la source et vérifie l'intégrité des données.

    Si vous utilisez **ESP** comme protocole IPSec, spécifiez également l'algorithme **de chiffrement** utilisé dans la négociation SA IPSec.

    Prisma Access prend en charge les algorithmes de chiffrement suivants : aes-256-gcm (256 bits), aes-256-cbc (256 bits), aes-192-cbc (192 bits), aes-128-gcm (128 bits), aes-128-cbc (128 bits), 3des (168 bits) et des (56 bits). Vous pouvez également sélectionner null (aucun chiffrement).

- **Authentification** : spécifiez l'algorithme d'authentification utilisé dans la négociation SA IPSec.

  Prisma Access prend en charge les algorithmes d'authentification suivants : sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits) et md5 (128 bits). Si le protocole IPSec est ESP, vous pouvez également sélectionner none (aucune authentification).

- **Groupe DH** : spécifiez les groupes Diffie-Hellman (DH) pour IKE dans la négociation de la Security Association (association de sécurité - SA) IPSec.

  Prisma Access prend en charge les groupes DH suivants : Groupe 1 (768 bits), Groupe 2 (1 024 bits par défaut), Groupe 5 (1 536 bits), Groupe 14 (2 048 bits), Groupe 19 (groupe de courbes elliptiques 256 bits) et Groupe 20 (groupe de courbes elliptiques 384 bits). Pour obtenir la sécurité la plus forte, sélectionnez le groupe avec le nombre le plus élevé. Si vous ne souhaitez pas renouveler la clé créée par Prisma Access pendant la phase 1 de l'IKE, sélectionnez **no-pfs (PFS désactivé)** (pas de confidentialité persistante parfaite). Si vous sélectionnez cette option, Prisma Access réutilise la clé actuelle pour la négociation IPSec SA.

- **Lifetime (Durée de vie)** : spécifiez l'unité et la durée de validité de la clé négociée (une heure par défaut).

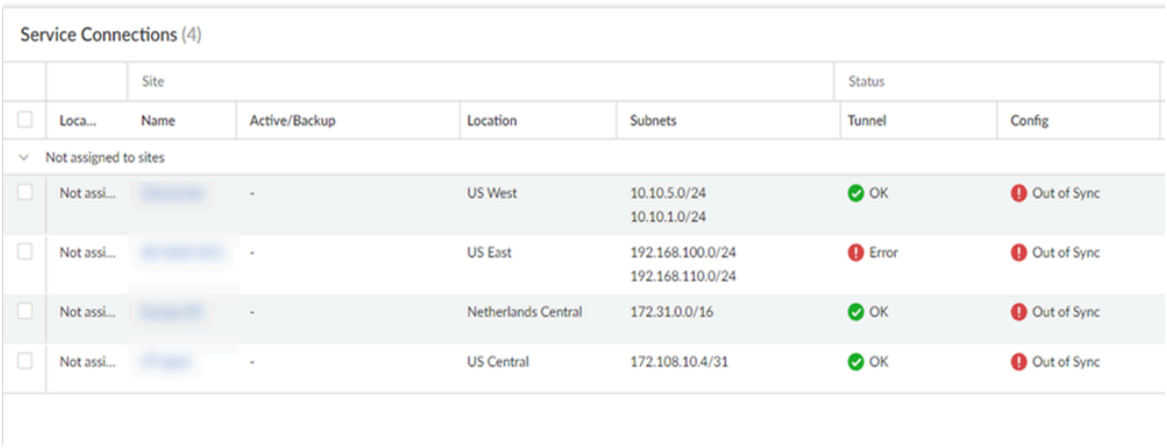
- **Taille réelle** : spécifiez l'unité et la quantité de données que la clé peut utiliser pour le chiffrement.

 ©2025 Palo Alto Networks, Inc.

Vérifiez l'état de la connexion aux services

Pour vérifier que la connexion aux services a été correctement configurée, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connections (Connexions aux services)** et vérifiez que le **Status (État)** est **OK**.

Si l'état n'est pas **OK**, passez la souris sur l'icône d'état pour afficher les erreurs.



La zone **Sites** vous permet d'afficher toutes les connexions aux services intégrées, ainsi que leur état et d'autres détails les concernant.

Site

- **Name (Nom)** : nom de la connexion aux services.
- **Active/Backup (Actif/sauvegarde)** : emplacements actifs et de sauvegarde de la connexion aux services.
- **Subnets (Sous-réseaux)** : les sous-réseaux d'infrastructure attribués à la connexion aux services.

État

- **Tunnel (Tunnel)** : l'état de fonctionnement de la connexion entre Prisma Access et votre connexion aux services.
- **Config (Configuration)** : l'état de votre dernière application de configuration au service. Si la configuration locale et la configuration dans le cloud correspondent, l'état de la configuration est **In sync (En synchronisation)**. Si vous avez effectué une modification localement et que vous n'avez pas encore appliqué la configuration au cloud, l'état peut être affiché comme **Out of sync (Désynchronisé)**. Passez la souris sur l'indicateur d'état pour obtenir des informations plus détaillées. Après avoir validé et appliqué la configuration pour Prisma Access, l'état de configuration passe à **In sync (En synchronisation)**.

Prisma Access

- **Location (Emplacement)** : l'emplacement où la connexion aux services est déployée.
- **Service IP (Adresse IP du service)** : adresse IP de la connexion au service.
- **EBGP Router (Routeur EBGP)** : l'adresse IP du routeur EBGP dans la connexion aux services.

Liens

- **BGP IPv4** : l'état du routage IPv4 BGP dans la connexion aux services.

 ©2025 Palo Alto Networks, Inc.

- **BGP IPv6** : l'état du routage IPv6 BGP dans la connexion aux services.
- **IPSec Tunnel (Tunnel IPSec)** : tunnel IPSec de votre connexion aux services. Le premier tunnel IPSec que vous établissez sera le tunnel **(Primary) ((Principal))**. Si vous avez établi un deuxième tunnel IPSec, il s'agira du tunnel **(Secondary) ((Secondaire))**.
- **Peer IP Address (Adresse IP de l'homologue)** : adresse IP de la passerelle de la connexion aux services.

Configurer une connexion aux services dans Prisma Access (Panorama)

Pour configurer une connexion aux services pour Prisma Access Panorama afin d'autoriser l'accès aux applications privées ou aux ressources internes de l'entreprise, procédez comme suit.

N'utilisez pas CLI pour intégrer et configurer les connexions aux services. Si vous avez besoin d'utiliser CLI pour intégrer des connexions aux services, contactez votre équipe Palo Alto Networks.

STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Connection (Connexion aux services)**.

STEP 2 | Cliquez sur **Add (Ajouter)** pour ajouter une nouvelle connexion aux services à l'un des sites de votre réseau d'entreprise.

STEP 3 | Spécifiez un **Name (Nom)** pour le site d'entreprise.

STEP 4 | Sélectionnez le **Location (Emplacement)** le plus proche de l'emplacement du site.

Reportez-vous à cette section pour obtenir une liste des emplacements Prisma Access.

Les emplacements dotés de deux astérisques sont des **Local Zones (Zones locales)**. Ces emplacements placent les services de calcul, de stockage, de base de données et d'infrastructure à proximité de grands centres de population et d'industrie; cependant, ils présentent également certaines limites. Pour ajouter une zone locale, contactez votre représentant Palo Alto Networks.

STEP 5 | Sélectionnez ou ajoutez une nouvelle configuration de **IPSec Tunnel (Tunnel IPSec)** pour accéder au pare-feu, au routeur ou au périphérique SD-WAN sur le site de l'entreprise :

- Si vous utilisez la configuration d'un **IPSec Tunnel (Tunnel IPSec)** existant, sélectionnez-le dans la liste déroulante. Notez que le tunnel que vous créez pour chaque connexion aux services connecte Prisma Access au périphérique compatible IPSec sur chaque site d'entreprise. Les adresses homologues dans la configuration IKE Gateway doivent être uniques pour chaque tunnel. Vous pouvez toutefois réutiliser certains des autres éléments de configuration courants, tels que les profils crypto.

  Le tunnel IPSec que vous sélectionnez doit utiliser l'échange automatique de clés et IPv4 uniquement. En outre, assurez-vous que le tunnel IPSec, la passerelle IKE et les noms de profil crypto comportent 31 caractères ou moins.

 ©2025 Palo Alto Networks, Inc.

- Pour créer une nouvelle configuration de tunnel IPSec :

  Cliquez sur **New IPSec Tunnel (Nouveau tunnel IPSec)**, donnez-lui un **Name (Nom)** et configurez la passerelle IKE, le profil crypto IPSec et les paramètres de surveillance du tunnel.
- Si le périphérique compatible IPSec de votre siège social ou de votre centre de données utilise un VPN basé sur des politiques :

  dans l'onglet **Proxy IDs (ID de proxy)**, cliquez sur **Add (Ajouter)** pour ajouter un ID de proxy qui correspond aux paramètres configurés sur votre périphérique IPSec local pour garantir que Prisma Access peut établir avec succès un tunnel IPSec avec votre périphérique local.
- Pour détecter et neutraliser les attaques par relecture :

  Laissez **Enable Replay Protection (Activer la protection contre la relecture)**.
- Pour préserver les informations ToS originales :

  Sélectionnez **Copy TOS Header (Copier l'en-tête TOS)** pour copier l'en-tête de type de service (Type of Service, ToS) à partir de l'en-tête IP interne vers l'en-tête IP externe des paquets encapsulés.
- Pour activer la surveillance de tunnel pour la connexion aux services :

  Sélectionnez **Tunnel Monitor (Surveiller le tunnel)**.

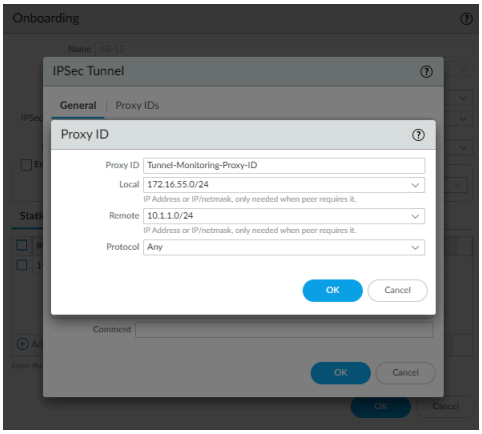
  - Saisissez l'adresse **IP de Destination**.

    Spécifiez une adresse IP sur le site de votre siège social ou de votre centre de données à laquelle Prisma Access peut envoyer des requêtes ping ICMP pour la surveillance du tunnel IPSec. Assurez-vous que cette adresse est accessible par ICMP depuis l'ensemble du sous-réseau de l'infrastructure Prisma Access.
  - Si vous utilisez la surveillance de tunnel avec un périphérique homologue qui utilise plusieurs ID de proxy, spécifiez un **ID de proxy** ou ajoutez un **nouvel ID** de proxy qui autorise l'accès à partir du sous-réseau d'infrastructure à votre siège social ou à votre site de centre de données.

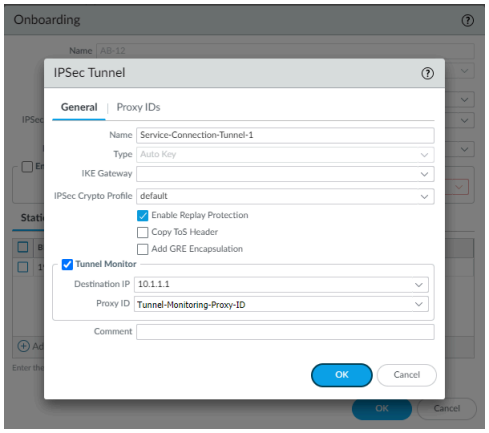
    La figure suivante montre un ID proxy avec le sous-réseau d'infrastructure de service (172.16.55.0/24 dans cet exemple) comme sous-réseau IP **local** et le sous-réseau du

 ©2025 Palo Alto Networks, Inc.

siège ou du centre de données (10.1.1.0/24 dans cet exemple) comme sous-réseau **distant**.



La figure suivante montre l'ID proxy que vous avez créé appliqué à la configuration du moniteur de tunnel en le spécifiant dans le champ **Proxy ID (ID proxy)**.



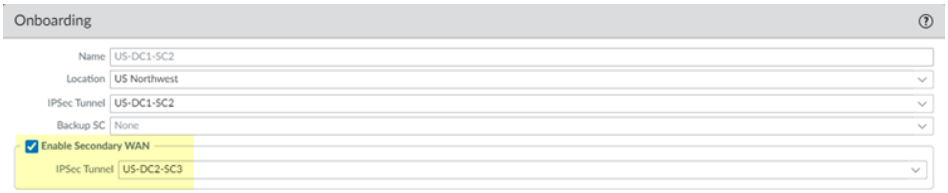
Vous devez configurer un itinéraire statique sur votre CPE vers l'adresse IP du moniteur de tunnel pour que la surveillance du tunnel fonctionne. Pour trouver l'adresse IP de destination à utiliser pour la surveillance du tunnel entre le réseau de votre centre de données ou de votre siège et Prisma Access, sélectionnez ***Panorama*** *>* ***Cloud Services*** *>* ***Status (État)*** *>* ***Network Details (Détails du réseau)****, cliquez sur la case d'option* ***Service Infrastructure (Infrastructure de service)*** *et recherchez la* ***Tunnel Monitor IP Address (Adresse IP de surveillance du tunnel)****.*

STEP 6 | Déploiements BGP et de routage de patates chaudes uniquement : sélectionnez une connexion de service à utiliser comme sauvegarde préférée (**Backup SC**).

Vous pouvez sélectionner n'importe quelle connexion aux services que vous avez déjà ajoutée. Prisma Access utilise le **Backup SC (SC de secours)** que vous sélectionnez comme connexion aux services préférée en cas de défaillance d'une liaison. La sélection d'une connexion aux services de secours peut éviter les problèmes de routage asymétrique si vous avez intégré

 ©2025 Palo Alto Networks, Inc.

plus de deux connexions aux services. Ce choix est disponible en mode de routage hot potato uniquement.



STEP 7 | Si vous avez une liaison WAN secondaire à cet emplacement, sélectionnez **Enable Secondary WAN (Activer le WAN secondaire)**, puis sélectionnez ou configurez un **tunnel IPSec**comme vous l'avez fait pour configurer le tunnel IPSec principal.

Si la liaison WAN principale tombe en panne, Prisma Access détecte la panne et établit un tunnel vers l'emplacement du siège social ou du centre de données via la liaison WAN secondaire. Si la liaison WAN principale devient active, la liaison revient à la liaison principale.

La configuration d'un WAN secondaire n'est pas prise en charge dans les déploiements suivants :

- Si votre WAN secondaire est configuré en mode actif/actif avec le tunnel IPSec principal.
- Si l'équipement de vos locaux clients (Customer Premises Equipment, CPE) est configuré dans une configuration de chemin d'accès multiple à coût égal (Equal Cost Multipath, ECMP) avec le tunnel IPSec principal et secondaire.

Si vous utilisez des itinéraires statiques, le temps de basculement du tunnel est inférieur à 15 secondes à partir du moment de la détection, selon votre fournisseur WAN.

Si vous configurez le routage BGP et que vous avez activé la surveillance des tunnels, le temps d'attente par défaut le plus court pour déterminer qu'un index de paramètres de sécurité (SPI) est défaillant est le moniteur de tunnel, qui supprime toutes les routes vers un homologue lorsqu'il détecte une défaillance de tunnel pendant 15 secondes consécutives. De cette façon, le moniteur de tunnel détermine le comportement des routes BGP. Si vous ne configurez pas la surveillance des tunnels, la minuterie d'attente détermine la durée d'arrêt du tunnel avant la suppression de l'itinéraire. Prisma Access utilise la valeur d'attente BGP par défaut de 90 secondes qui a été définie dans la RFC 4271. Il s'agit du temps d'attente maximal avant que Prisma Access ne supprime un itinéraire pour un SPI inactif. Si le périphérique BGP homologue a un temps d'attente configuré plus court, le minuteur de maintien BGP utilise la valeur inférieure.

Lorsque le tunnel secondaire est installé avec succès, l'itinéraire secondaire a priorité jusqu'à ce que le tunnel primaire refonctionne. Si l'itinéraire principal et l'itinéraire secondaire sont tous deux opérationnels, l'itinéraire principal est prioritaire.

Si vous utilisez un homologue BGP différent pour la connexion secondaire (de secours), Prisma Access ne respecte pas les attributs du discriminateur multi-sortie (Multi-Exit Discriminator, MED) publiés par le CPE. Cette mise en garde s'applique si vous utilisez plusieurs homologues BGP sur des connexions réseau distantes ou des connexions de service.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | (Facultatif) Activez le NAT source pour les utilisateurs mobiles : adresses du pool d'adresses IP GlobalProtect, adresses IP dans le sous-réseau Infrastructure, ou les deux.

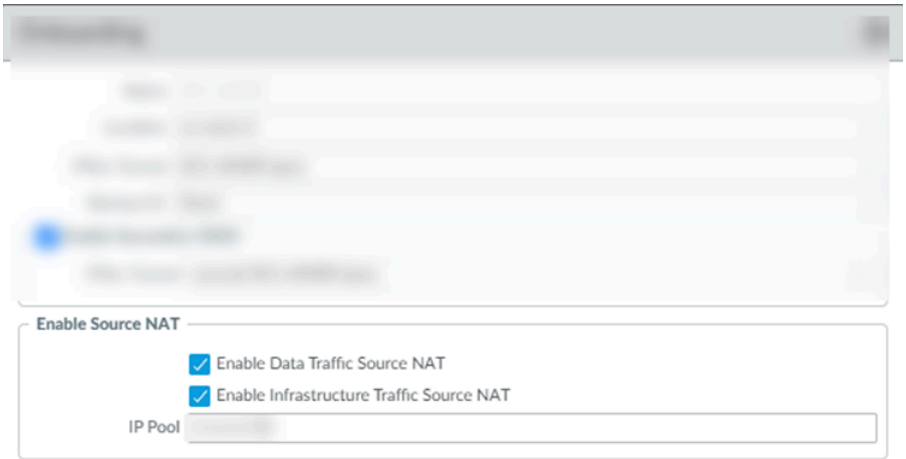
Vous pouvez spécifier un sous-réseau au niveau d'une ou plusieurs connexions aux services utilisées pour le trafic NAT entre les utilisateurs mobiles Prisma Access GlobalProtect et les applications et ressources privées d'un centre de données.

- **Enable Data Traffic source NAT (Activer le NAT source de trafic de données)** : effectue le NAT sur les adresses du pool d'adresses IP des utilisateurs mobiles afin qu'elles ne soient pas annoncées au centre de données et que seuls les sous-réseaux que vous spécifiez aux connexions aux services soient annoncés et acheminés dans le centre de données.
- **Enable Infrastructure Traffic source NAT (Activer le NAT source de trafic d'infrastructure)** : effectue le NAT sur les adresses du sous-réseau d'infrastructure afin qu'elles ne soient pas annoncées au centre de données et que seuls les sous-réseaux que vous spécifiez aux connexions aux services soient annoncés et acheminés dans le centre de données.
- **User-ID** : lorsque cette option est sélectionnée, Prisma Access utilise cette connexion aux services pour la redistribution de l'identité.

  ***User-ID Redistribution Management (Gestion de la redistribution de User-ID)** : parfois, des contrôles précis sont nécessaires pour la redistribution des User-ID dans les déploiements Prisma Access à particulièrement grande échelle. La gestion de la redistribution de User-ID vous permet de désactiver manuellement le comportement de redistribution d'identité par défaut pour certaines connexions aux services en retirant la coche dans la colonne **User ID (ID utilisateur)**, puis sélectionnez les connexions aux services spécifiques à utiliser pour la redistribution de l'identité. Il n'est pas nécessaire de le faire pour la plupart des configurations. Contactez le support de Palo Alto Networks pour activer cette fonctionnalité.*

- **IP Pool (Pool d'adresses IP)** : spécifie le pool d'adresses IP utilisé pour effectuer le NAT sur le pool d'adresses IP des utilisateurs mobiles, le sous-réseau d'infrastructure ou les deux.

  Utilisez un sous-réseau IP privé (RFC 1918) ou un sous-réseau approprié qui est routable dans votre domaine de routage et qui ne chevauche pas le pool d'adresses IP des utilisateurs mobiles – GlobalProtect ou le sous-réseau d'infrastructure. Entrez un sous-réseau entre /25 et /32.



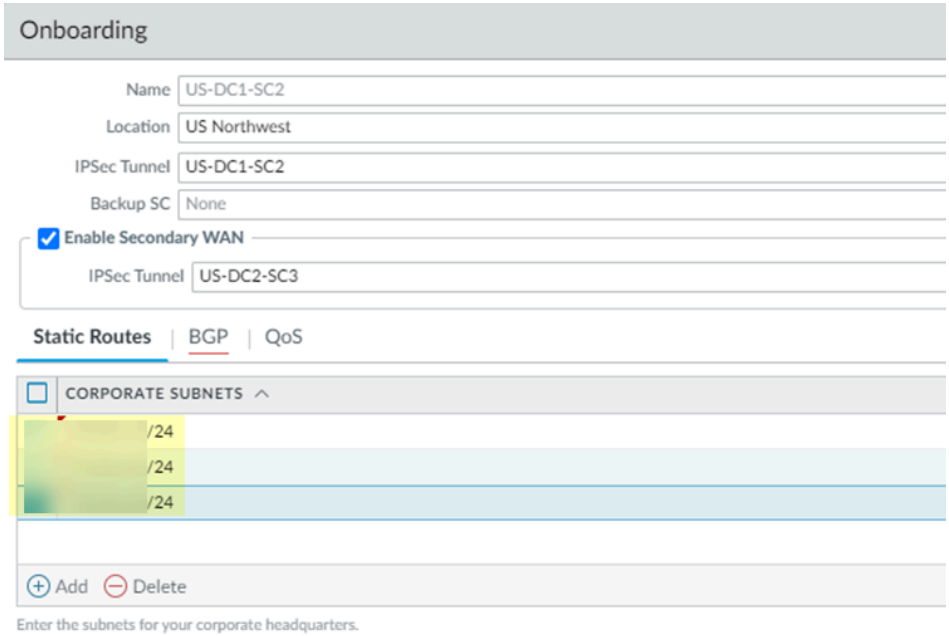
 ©2025 Palo Alto Networks, Inc.

STEP 9 | Activez le routage vers les sous-réseaux ou les adresses IP individuelles sur le site d'entreprise auquel vos utilisateurs auront besoin d'accéder.

Prisma Access utilise ces informations pour acheminer les requêtes vers le site approprié. Les réseaux de chaque site ne peuvent pas se chevaucher les uns avec les autres ni avec les pools d'adresses IP que vous avez désignés pour l'infrastructure de service ou pour le Prisma Access pour les pools d'adresses IP des utilisateurs. Vous pouvez configurer des **Static Routes (Itinéraires statiques)**, **BGP** ou une combinaison des deux.

Pour configurer des **Static Routes (Itinéraires statiques)** :

1. Dans l'onglet **Static Routes (Itinéraires statiques)**, cliquez sur **Add (Ajouter)** et saisissez l'adresse de sous-réseau (par exemple, 172.168.10.0/24) ou l'adresse IP individuelle d'une ressource, comme un serveur DNS (par exemple, 10.32.5.1/32) auquel vos utilisateurs distants auront besoin d'accéder.
2. Répétez l'opération pour tous les sous-réseaux ou adresses IP auxquels Prisma Access aura besoin d'accéder à cet emplacement.



Pour configurer **BGP** :

1. Dans l'onglet **BGP**, sélectionnez **Enable (Activer)**.

   Lorsque vous activez BGP, Prisma Access définit la valeur de durée de vie (Time-To-Live, TTL) pour BGP externe (eBGP) sur 8 pour prendre en compte les sauts supplémentaires

 ©2025 Palo Alto Networks, Inc.

qui peuvent se produire entre l'infrastructure Prisma Access et l'équipement de vos locaux client (Customer Premises Equipment, CPE) qui met fin à la connexion eBGP.

Prisma Access n'accepte pas les annonces d'itinéraire BGP par défaut pour les connexions aux services ou les connexions réseau distantes.

2. (Facultatif) Choisissez parmi les options suivantes :

   - Pour ajouter une communauté de **no-export (non-export)** pour les nœuds d'accès d'entreprise (connexions aux services) aux préfixes sortants des homologues eBGP de l'équipement de vos locaux client (Customer Premises Equipment, CPE), définissez **Add no-export community (Ajouter une communauté de non-export)** sur **Enabled Out (Sortie activée)**. Par défaut, cette capacité est **Disabled (Désactivée)**.

     N'utilisez pas cette fonctionnalité en mode de routage hot potato.

   - Pour empêcher l'homologue BGP Prisma Access de transférer des itinéraires dans le réseau de votre organisation. **Don't Advertise Prisma Access Routes (Ne pas publier les itinéraires Prisma Access)**.

     Par défaut, Prisma Access publie toutes les informations de routage BGP, y compris les itinéraires locaux et tous les préfixes qu'il reçoit d'autres connexions aux services, de réseaux distants et de sous-réseaux d'utilisateurs mobiles. Cochez cette case pour empêcher Prisma Access d'envoyer des publications BGP, mais toujours utiliser les informations BGP qu'il reçoit pour apprendre les itinéraires d'autres voisins BGP.

     Étant donné que Prisma Access n'envoie pas de publications BGP si vous sélectionnez cette option, vous devez configurer des itinéraires statiques sur l'équipement sur site pour établir des itinéraires de retour à Prisma Access.

   - Pour réduire le nombre de publications de sous-réseaux IP d'utilisateurs mobiles via BGP sur l'équipement de vos locaux client (Customer Premises Equipment, CPE), paramétrez Prisma Access de manière à ce qu'il résume les sous-réseaux avant de les publier en sélectionnant **Summarize Mobile User Routes before advertising (Résumer les itinéraires des utilisateurs mobiles avant de publier)**.

     Par défaut, Prisma Access annonce les pools d'adresses IP des utilisateurs mobiles en blocs de sous-réseaux /24. Si vous les résumez, Prisma Access publie le pool en fonction du sous-réseau que vous avez spécifié. Par exemple, Prisma Access publie un pool d'adresses IP mobiles d'utilisateurs publics de 10.8.0.0/20 en utilisant le sous-réseau /20, plutôt que de diviser le pool en sous-réseaux de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24 et ainsi de suite avant de les publier. Le résumé de ces publications peut réduire le nombre d'itinéraires stockés dans les tableaux de routage CPE. Par exemple, vous pouvez utiliser le résumé de pool d'adresses IP avec des passerelles VPN cloud (passerelles privées virtuelles (VGW) ou passerelles de transit (TGW)) qui peuvent accepter un nombre limité d'itinéraires.

     Si le routage hot potato est activé et que vous activez le résumé des itinéraires, Prisma Access ne préfixe plus les chemins AS, ce qui peut entraîner un routage asymétrique. Assurez-vous que votre trafic de retour du centre de données ou de l'emplacement du siège social a garanti un retour symétrique avant d'activer le résumé des itinéraires avec le routage hot potato.

 ©2025 Palo Alto Networks, Inc.

3. (Facultatif) Sélectionnez une valeur de minuterie **MRAI**.

   Le routage BGP propose un minuteur que vous pouvez utiliser pour adapter la convergence du routage BGP dans votre réseau, appelé *Intervalle minimum de publication d'itinéraire (MRAI)*. MRAI agit pour limiter le débit des mises à jour par destination, et les routeurs BGP attendent au moins le délai MRAI configuré avant d'envoyer une publication pour le même préfixe. Un nombre plus petit vous donne un temps de convergence plus rapide, mais crée plus de publications sur votre réseau. Un nombre plus élevé diminue le nombre de publications pouvant être envoyées, tout en ralentissant également la convergence de routage. Vous décidez du nombre à mettre dans votre réseau pour obtenir le meilleur équilibre entre une convergence de routage plus rapide et moins de publications.

   Configurez une plage MRAI comprise entre 1 et 600 secondes, avec une valeur par défaut de 30 secondes.
4. Entrez l'adresse IP assignée comme identifiant de routeur du routeur eBGP sur le réseau du centre de données/siège social pour lequel vous configurez cette connexion aux services en tant que **Peer Address (Adresse de l'homologue)**.
5. Entrez le **Peer AS (Homologue AS)**, qui est le système autonome (Autonomous System, AS) auquel le pare-feu, le routeur virtuel ou le routeur BGP du réseau de votre centre de données/siège social appartiennent.
6. (Facultatif) Entrez une adresse que Prisma Access utilise comme adresse IP locale pour BGP.

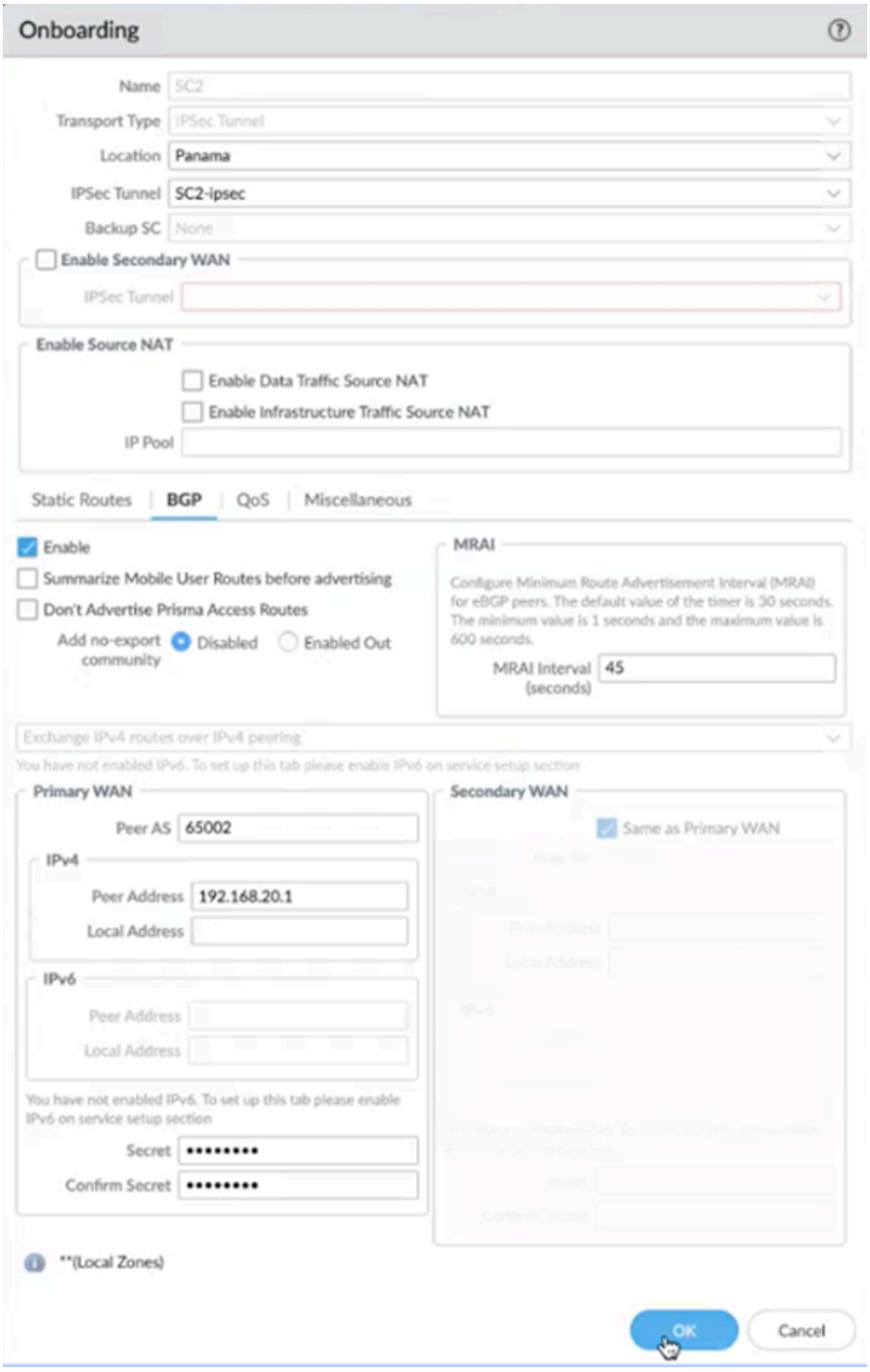
   La spécification d'une **Local Address (Adresse locale)** est utile lorsque le périphérique situé de l'autre côté de la connexion (tel qu'une passerelle virtuelle privée Amazon Web Service (AWS)) nécessite une adresse IP locale spécifique pour que l'appairage BGP réussisse. Assurez-vous que l'adresse que vous spécifiez n'entre pas en conflit ou ne chevauche pas les adresses IP du sous-réseau d'infrastructure ou des sous-réseaux de la connexion aux services.

   *Vous devez configurer un itinéraire statique sur votre CPE vers la **Local Address (Adresse locale)** du BGP.*

   Si vous utilisez la prise en charge IPV6 pour votre connexion aux services, vous pouvez configurer des adresses **IPv6** ainsi que des adresses **IPv4**. Vous devez également activer la mise en réseau IPv6 globalement dans votre infrastructure Prisma Access avant de pouvoir utiliser l'adressage IPv6.

 ©2025 Palo Alto Networks, Inc.

7. (Facultatif) Entrez et confirmez une **Secret (Phrase secrète)** pour authentifier les communications d'un homologue BGP.



STEP 10 | (Facultatif) Si vous avez configuré un **Secondary WAN (WAN secondaire)** et que vous devez changer la **Peer Address (Adresse de l'homologue)** ou la **Local Address (Adresse locale)** pour l'homologue BGP secondaire (de secours), désélectionnez **Same as Primary WAN (Identique**

 ©2025 Palo Alto Networks, Inc.

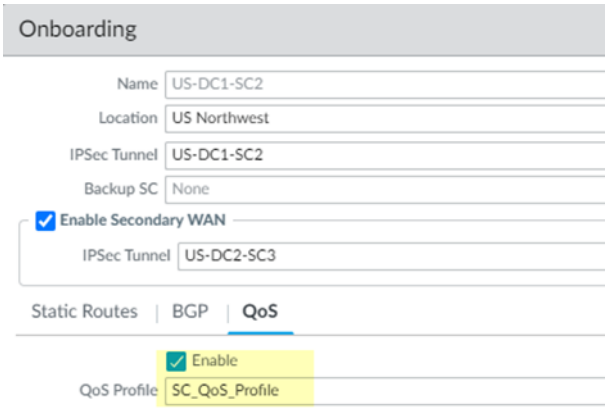
au WAN principal) et entrez une adresse IP d'homologue unique et, éventuellement, une adresse IP locale pour le WAN secondaire.

Dans certains déploiements (par exemple, lors de l'utilisation de BGP pour établir un appairage avec une passerelle VPN AWS), l'homologue BGP pour le WAN principal et secondaire peut être différent. Dans ces scénarios, vous pouvez choisir de définir un homologue BGP différent pour le WAN secondaire.

*Pour les déploiements BGP avec des WAN secondaires, Prisma Access définit les tunnels primaire et secondaire dans un état **UP (Actif)**, mais suit le comportement normal de sauvegarde active BGP pour le trafic réseau. Prisma Access définit le tunnel principal comme actif, et envoie et reçoit du trafic via ce tunnel uniquement. En cas de défaillance du tunnel principal, Prisma Access détecte l'échec à l'aide de règles BGP, définit le tunnel secondaire comme actif, et utilise uniquement le tunnel secondaire pour envoyer et recevoir le trafic.*

STEP 11 | (Facultatif) Activez la **Quality of Service (Qualité de service)** pour la connexion aux services et spécifiez un profil QoS ou ajoutez un **New QoS Profile (Nouveau profil QoS)**.

Vous pouvez créer des profils QoS pour façonner le trafic QoS pour le réseau distant et les connexions aux services, et appliquer ces profils au trafic que vous avez marqué avec des politiques de sécurité PAN-OS, au trafic que vous avez marqué avec un périphérique sur site ou au trafic marqué PAN-OS et sur site. Pour plus d'informations, reportez-vous à la sectionQoS pour les réseaux distants.



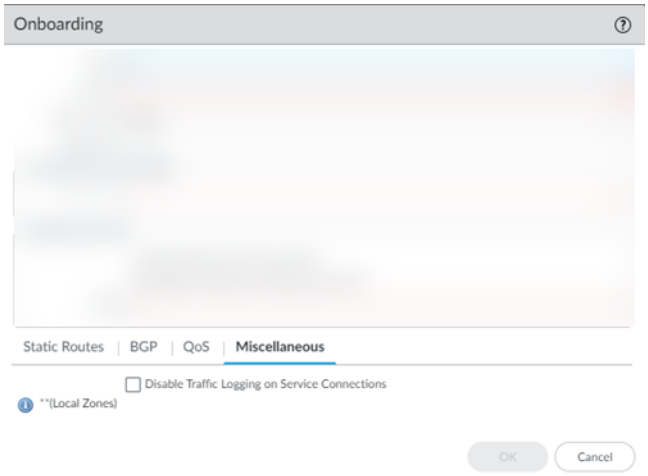
STEP 12 | (Facultatif) Configurez les paramètres **Miscellaneous (Divers)**.

1. (Facultatif) Sélectionnez **Disable Traffic Logging on Service Connections (Désactiver la journalisation du trafic sur les connexions aux services)** pour désactiver la journalisation sur les connexions aux services pour votre déploiement Prisma Access.

   Si la majorité des flux de trafic enregistrés par les connexions aux services sont asymétriques, la désactivation de la journalisation des connexions aux services peut être nécessaire pour réduire la consommation de stockage de la journalisation des Strata

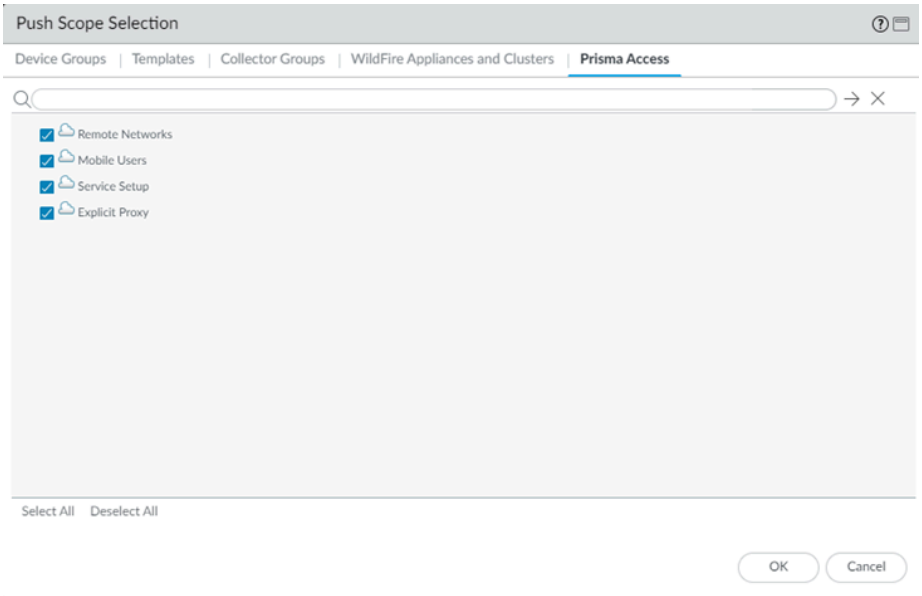
 ©2025 Palo Alto Networks, Inc.

Logging Service. Si votre déploiement n'a pas de flux asymétriques via les connexions aux services, vous ne devez pas désactiver la journalisation.



STEP 13 | Validez vos modifications dans Panorama et transmettez les modifications de configuration à Prisma Access.

1. Cliquez sur **Commit (Valider)** > **Commit and Push (Valider et transmettre)**.
2. Cliquez sur **Edit Selections (Modifier les sélections)** et, dans l'onglet **Prisma Access**, assurez-vous que l'option **Service Setup (Configuration du service)** est sélectionnée dans la **Push Scope (Étendue de la transmission)**, puis cliquez sur **OK**.



3. Cliquez sur **Commit and Push (Valider et appliquer)**.

STEP 14 | Ajoutez d'autres connexions aux services en répétant les étapes 2 à 11.

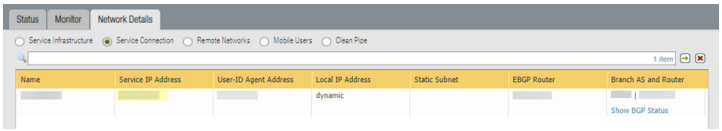
STEP 15 | Configurez le ou les tunnels IPSec à partir de votre périphérique compatible IPSec sur votre réseau d'entreprise de retour Prisma Access.

1. Pour déterminer l'adresse IP du tunnel dans Prisma Access, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)**, cliquez sur le

 ©2025 Palo Alto Networks, Inc.

bouton d'option **Service Connection (Connexion aux services)** et notez la **Service IP Address (Adresse IP du service)** pour le site.

La **Service IP Address (Adresse IP du service)** est l'adresse publique à laquelle vous devez vous connecter lorsque vous créez le tunnel entre votre périphérique compatible IPSec et la connexion aux services.



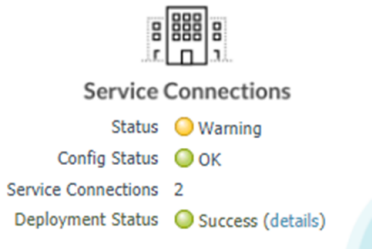
2. Sur votre périphérique compatible IPSec sur le site de l'entreprise, configurez un tunnel IPSec qui se connecte à la **Service IP Address (Adresse IP du service)** dans Prisma Access et validez la modification sur ce périphérique afin que le tunnel puisse être établi.

Vérifier l'état de la connexion aux services

Pour vérifier que la connexion aux services a été correctement configurée, sélectionnez **Panorama > Cloud Services > Status (État) > Status (État)** et vérifiez que l'état est **OK**.

Si vous avez créé une connexion aux services avec des valeurs d'espace réservé pour permettre la communication entre les utilisateurs mobiles et les utilisateurs de réseaux distants, vous n'avez pas besoin de vérifier l'état de la connexion aux services.

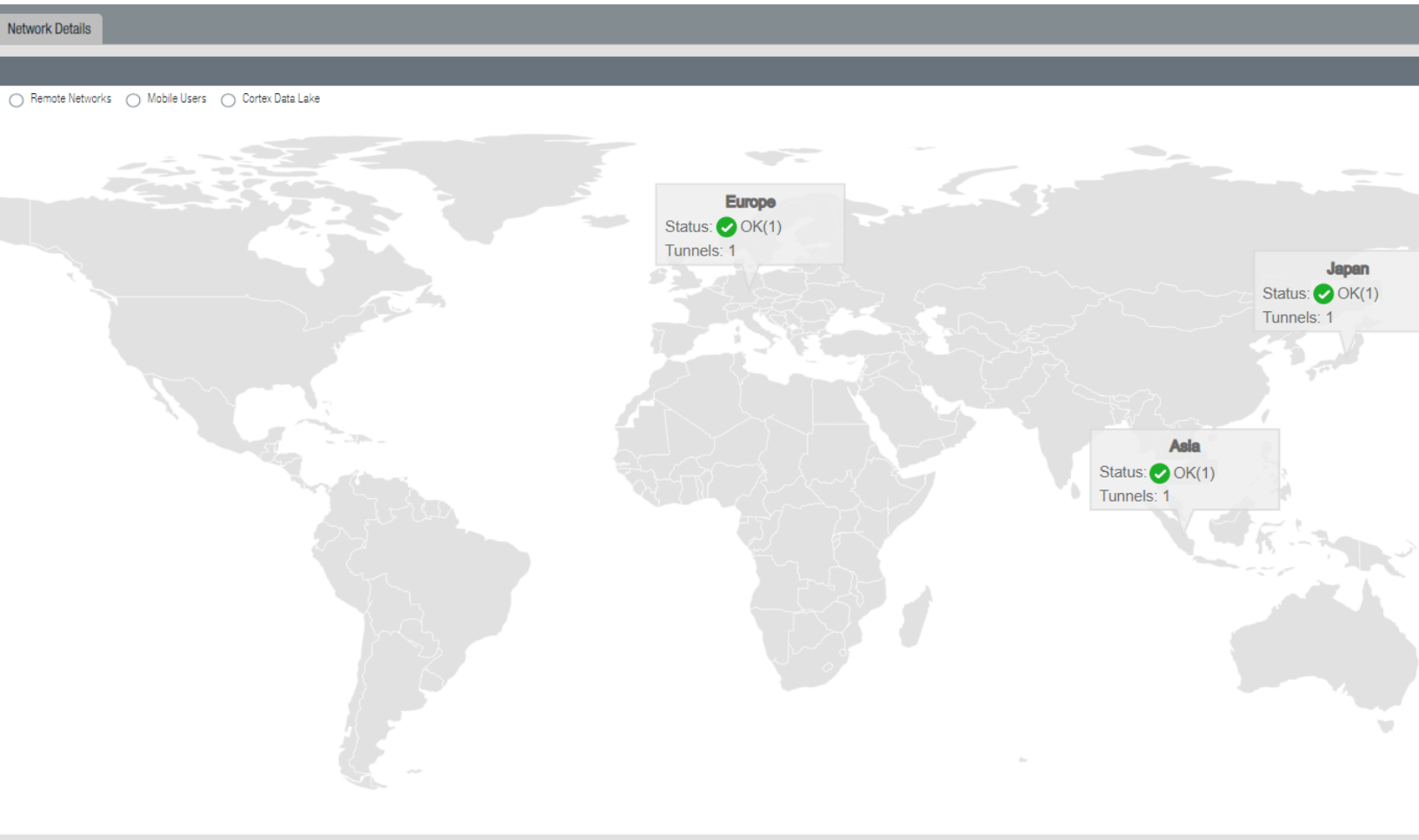
La zone **Deployment Status (État du déploiement)** vous permet d'afficher la progression des tâches d'intégration et de déploiement avant qu'elles ne soient terminées, ainsi que de voir plus d'informations sur l'état des tâches terminées.



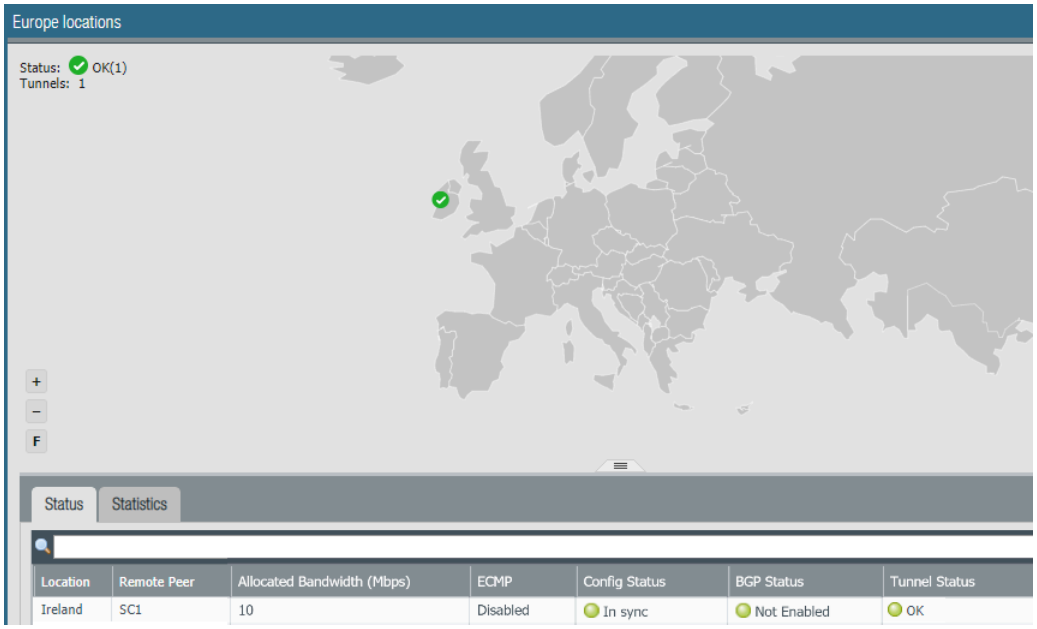
Si l'état n'est pas **OK**, passez la souris sur l'icône d'état pour afficher les erreurs.

Pour afficher une représentation graphique de la connexion aux services avec les détails de l'état, sélectionnez **Service Connection (Connexion aux services)** sur l'onglet **Monitor (Surveiller)**.

 ©2025 Palo Alto Networks, Inc.



Sélectionnez une région pour obtenir plus de détails sur cette région.



Cliquez sur les onglets sous la carte pour afficher des informations supplémentaires sur les connexions aux services.

 ©2025 Palo Alto Networks, Inc.

Onglet **Status (État)** :

- **Location (Emplacement)** : l'emplacement où votre connexion aux services est déployée.
- **Remote Peer (Homologue à distance)** : l'emplacement de l'entreprise vers laquelle cette infrastructure de service configure un tunnel IPSec.
- **Allocated Bandwidth (Bande passante allouée)** : le nombre de connexions aux services que vous avez allouées multiplié par 300 Mbit/s.

  Ce nombre ne reflète pas la bande passante de connexion aux services disponible.

  Bien que chaque connexion aux services fournisse un débit d'environ 1 Gbit/s, le débit réel dépend de plusieurs facteurs, notamment :

  - *Répartition du trafic (par exemple, taille de trame)*
  - *Latence et perte de paquets entre la connexion aux services et l'emplacement du siège social ou du centre de données*
  - *Limites de performance des fournisseurs de services*
  - *Limites de performance du périphérique de résiliation du client*
  - *Autres trafics du centre de données des clients*
- **ECMP** : si vous avez configuré le chemin d'accès multiple à coût égal (Equal Cost Multipath; ECMP) pour cette connexion aux services. Puisque l'ECMP n'est pas utilisé pour les connexions aux services, cet état est **Disabled (Désactivé)**.
- **Config Status (État de la configuration)** : l'état de votre dernière transmission de configuration au service. Si la configuration locale et la configuration dans le cloud correspondent, l'état de la configuration est **In sync (En synchronisation)**. Si vous avez effectué une modification localement et que vous n'avez pas encore appliqué la configuration au cloud, l'état peut être affiché comme **Out of sync (Désynchronisé)**. Passez la souris sur l'indicateur d'état pour obtenir des informations plus détaillées. Après avoir validé et appliqué la configuration pour Prisma Access, l'état de configuration passe à **In sync (En synchronisation)**.
- **BGP Status (État BGP)** : affiche des informations sur l'état BGP entre le pare-feu ou le routeur à l'emplacement de votre entreprise/siège social et Prisma Access où la connexion aux services est établie. Bien que vous puissiez voir temporairement l'état passer par les différents états BGP (**Idle (Inactif)**, **Active (Actif)**, **Open send (Envoi ouvert)**, **Open pend (Attente ouverte)**, **Open confirm (Confirmation ouverte)**, le plus souvent, l'état BGP indique :
  - **Connect (Connecter)** : le routeur de votre centre de données/siège social tente d'établir la relation de l'homologue BGP avec Prisma Access.
  - **Established (Établi)** : la relation de l'homologue BGP a été établie.

  Ce champ indiquera également si la connexion BGP est dans un état d'erreur :
  - **Warning (Avertissement)** : il n'y a pas eu de mise à jour de l'état BGP depuis plus de huit minutes. Cela peut indiquer une panne du pare-feu.
  - **Error (Erreur)** : l'état BGP est inconnu.

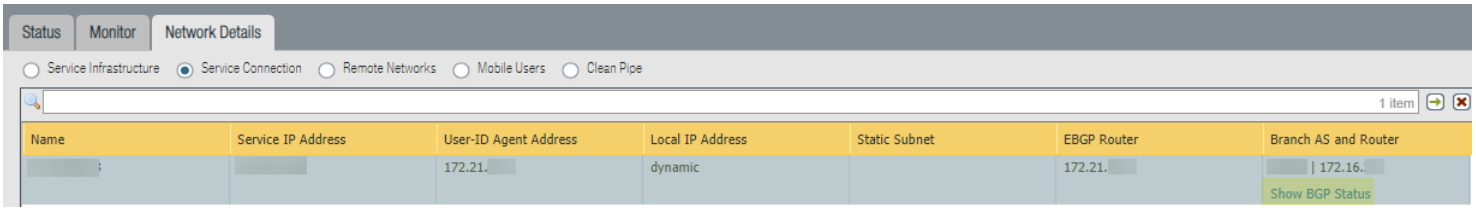
 ©2025 Palo Alto Networks, Inc.

- **Tunnel Status (État du tunnel)** : l'état de fonctionnement de la connexion entre Prisma Access et votre connexion aux services.

Onglet **Statistics (Statistiques)** :

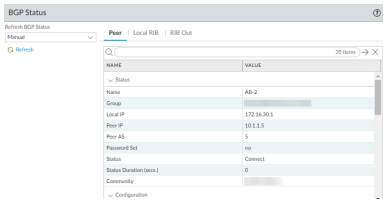
- **Location (Emplacement)** : l'emplacement où votre connexion aux services est déployée.
- **Remote Peer (Homologue à distance)** : emplacement de l'entreprise auquel la connexion aux services configure un tunnel IPSec.
- **Ingress Bandwidth (Mbps) (Bande passante d'entrée (Mbit/s))** : la bande passante entre l'emplacement du siège social/du centre de données et Prisma Access.
- **Ingress Peak Bandwidth (Mbps) (Bande passante maximale d'entrée (Mbit/s))** : la charge maximale depuis l'emplacement du siège/centre de données vers le service cloud.
- **Egress Bandwidth (Mbps) (Bande passante de sortie (Mbit/s))** : la bande passante de Prisma Access dans l'emplacement du siège social/du centre de données.
- **Egress Peak Bandwidth (Mbps) (Bande passante maximale de sortie (Mbit/s))** : la charge de maximale de Prisma Access dans l'emplacement du siège social/du centre de données.
- **QoS** : sélectionnez ce bouton pour afficher un graphique qui affiche des statistiques de QoS en temps réel et historiques, y compris le nombre de paquets abandonnés par classe. Ce graphique s'affiche uniquement pour les connexions aux services ou les connexions au réseau distant pour lesquelles la QoS est activée.

Si vous avez configuré BGP, vous pouvez vérifier son état en sélectionnant **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **Show BGP Status (Afficher l'état BGP)**.



La boîte de dialogue BGP Status (État BGP) s'affiche. Ce tableau fournit les informations suivantes :

- **Peer (Homologue)** : informations de routage pour l'homologue BGP, y compris l'état, le nombre total d'itinéraires, la configuration, les statistiques et les compteurs d'exécution. Le nombre total d'itinéraires s'affiche dans la région **bgpAfiIpv4-unicast Counters (Compteurs bgpAfiIpv4-unicast)**, dans les champs **Incoming Total (Total entrant)** et **Outgoing Total (Total sortant)**.

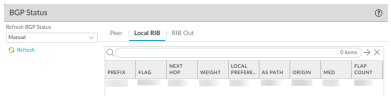


- **Local RIB (RIB locale)** : les itinéraires BGP que Prisma Access utilise localement. Prisma Access sélectionne ces informations dans le tableau BGP RIB-In, qui stocke les informations envoyées par les périphériques réseau voisins, applique les politiques d'importation BGP locales et les

 ©2025 Palo Alto Networks, Inc.

décisions de routage, et stocke les informations RIB locales dans la base d'informations de routage (Routing Information Base, RIB).

Notez que seules les 256 premières entrées sont affichées. Pour afficher des entrées supplémentaires, entrez un sous-réseau ou une adresse IP dans le champ Filter (Filtre), puis cliquez sur Apply Filter (Appliquer le filtre) pour afficher un sous-ensemble des entrées de routage jusqu'à un maximum de 256.



- **RIB Out (Sortie de RIB)** : informations de routage que Prisma Access publie auprès de ses homologues par le biais de messages de mise à jour BGP.

 ©2025 Palo Alto Networks, Inc.

Utiliser une connexion aux services pour permettre l'accès entre les utilisateurs mobiles et les réseaux distants

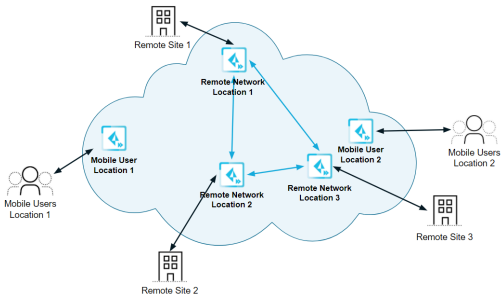
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prima Access qui inclut l'interconnexion réseau pour l'accès de site à site et d'utilisateur à site

Pour configurer une connexion aux services afin de connecter des utilisateurs mobiles et des réseaux distants, procédez comme suit : sélectionnez **Add (Ajouter)** pour ajouter une connexion au serviceà l'aide des valeurs suivantes :

- Spécifiez une **Region (Région)** qui est proche de vos utilisateurs mobiles.
- Ajoutez (**Add**) un **IPSec Tunnel (Tunnel IPSec=** et une **IKE Gateway (Passerelle IKE)**, à l'aide de valeurs d'espace réservé.
- Ajoutez l'espace réservé **Corporate Subnets (Sous-réseaux d'entreprise)**.

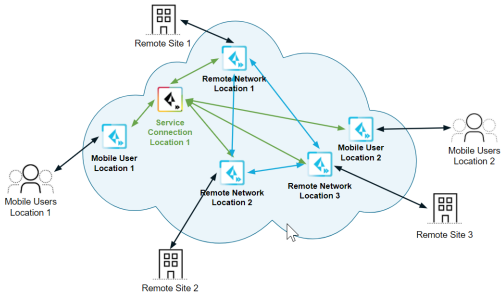
  Puisque Prisma Access n'achemine aucun trafic via ce tunnel, toute valeur qui n'entre pas en conflit avec ou ne chevauche pas d'autres sous-réseaux configurés est valide.

L'exemple suivant montre un déploiement Prisma Access avec des utilisateurs mobiles dans différentes zones géographiques et différents réseaux distants. Les connexions aux réseaux distants sont connectées dans un réseau maillé dans l'infrastructure Prisma Access, mais les utilisateurs mobiles ne peuvent pas se connecter aux réseaux distants. De plus, les utilisateurs mobiles de différentes zones géographiques ne peuvent pas se connecter les uns aux autres sans une connexion aux services.

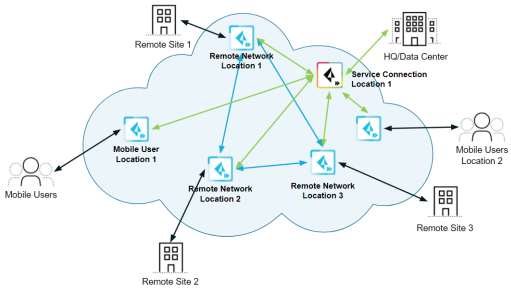


Une fois que vous avez ajouté une connexion aux services, celle-ci connecte les utilisateurs mobiles et les réseaux distants dans un réseau en étoile.

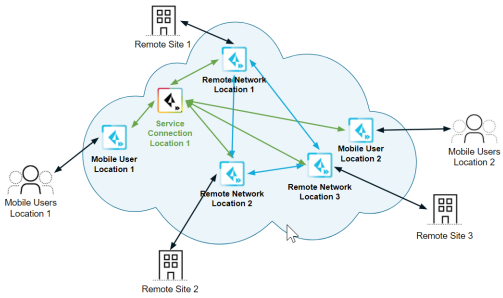
 ©2025 Palo Alto Networks, Inc.



Un autre cas où une connexion aux services de ce type est utile est lorsque la connexion aux services est éloignée des utilisateurs mobiles. La figure suivante montre un exemple de ce déploiement réseau.



L’ajout d’une deuxième connexion aux services plus proche des utilisateurs mobiles crée un réseau plus efficace entre les utilisateurs mobiles et les réseaux distants.



 ©2025 Palo Alto Networks, Inc.

Considérations sur le routage dynamique pour les connexions aux services

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Fonctionnement — Routage du trafic de connexion aux services

Prisma Access utilise BGP pour le routage dynamique et utilise la sélection de chemin BGP pour installer des itinéraires dans la table de routage. Quand Prisma Access achemine le trafic vers votre siège social ou votre centre de données à l'aide de connexions aux services, il utilise des méthodes de routage qui dirigent ce trafic efficacement. Prisma Access utilise un modèle de routage par défaut conçu pour s'adapter à la majorité des déploiements réseau ; cependant, tous les réseaux des organisations ne sont pas identiques. Pour s'adapter à une plus large gamme de déploiements, Prisma Access vous permet de choisir un autre mode pour le routage de la connexion aux services. Les sections suivantes décrivent les méthodes de routage BGP que Prisma Access utilise, ainsi que les facteurs que vous devez prendre en compte dans le réseau de votre organisation avant de changer la méthode de routage de connexion aux services par défaut de Prisma Access.

Changer la méthode de routage de connexion aux services Prisma Access nécessite une compréhension approfondie de la topologie et des périphériques de routage de votre organisation, ainsi qu'une compréhension de la manière dont fonctionne le routage Prisma Access comme décrit dans cette section. Nous vous recommandons de lire attentivement cette section avant de modifier la méthode de routage par défaut.

Prisma Access prend en charge le routage statique et le routage dynamique à l'aide de BGP pour les connexions aux services et les connexions réseau distantes ; cette section suppose que vous utilisez le routage BGP pour vos déploiements Prisma Access. Lorsque vous sélectionnez le routage BGP, le réseau de votre organisation apprend les informations BGP de Prisma Access.

Modes de routage pour les connexions aux services

Vous pouvez choisir parmi les modes de routage suivants avec Prisma Access :

- Routage par défaut—Il s'agit du modèle de routage actuel que Prisma Access utilise.

  Utilisez ce mode de routage si vous souhaitez que Prisma Access utilise les meilleurs mécanismes de sélection de chemin BGP sans ajuster aucun des attributs BGP. Dans ce mode, Prisma Access honorera tout attribut annoncé par l'équipement local du client (CPE).
- Routage Hot Potato—Prisma Access transmet le trafic aussi rapidement que possible au réseau de votre organisation.

  Utilisez cette méthode de routage si vous souhaitez que le réseau de votre organisation effectue la majorité des décisions de routage.

 ©2025 Palo Alto Networks, Inc.

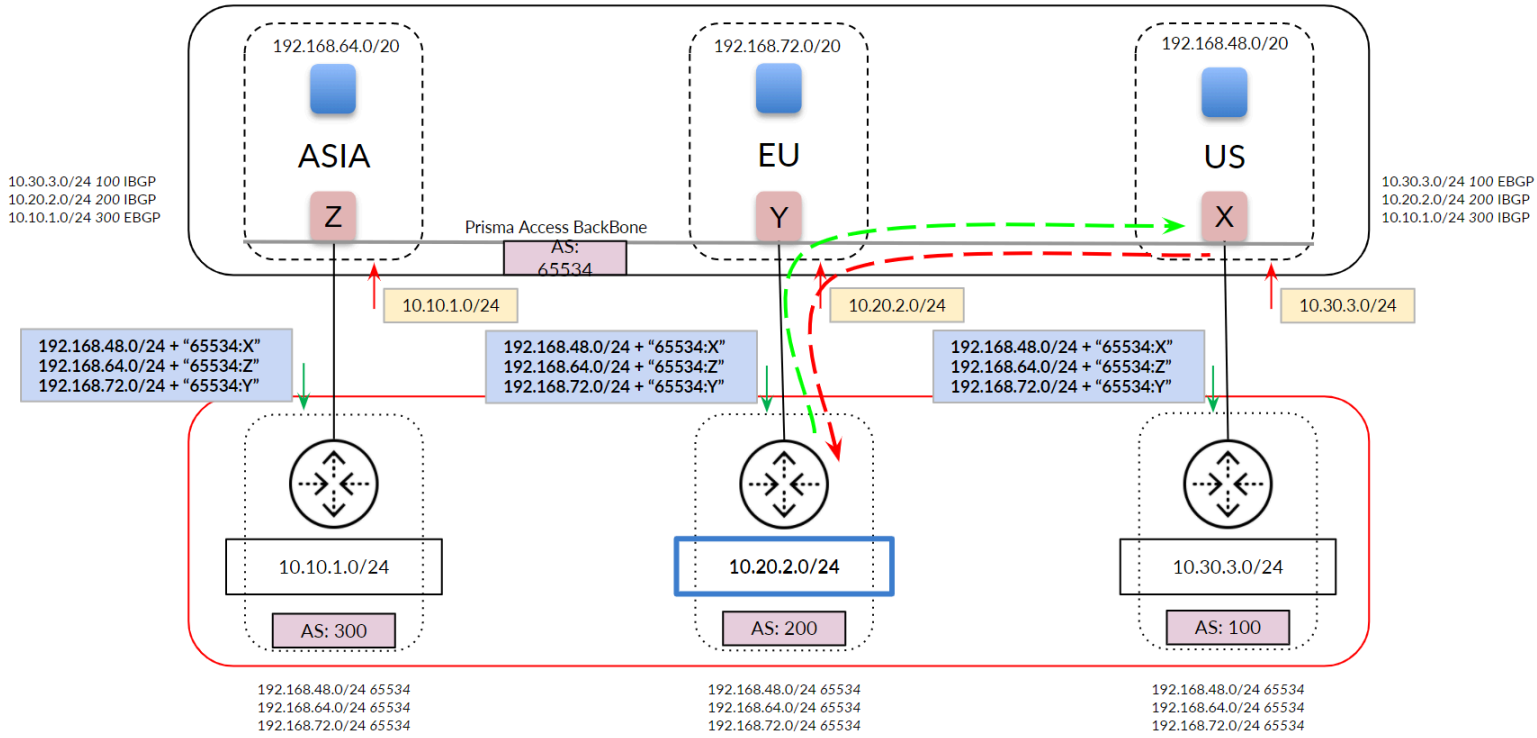
Prisma Access Routage par défaut

La figure suivante montre un exemple de routage Prisma Access du trafic de connexion aux services en mode de routage par défaut. Le réseau de l'organisation dispose de trois réseaux distincts dans trois centres de données et ne dispose pas d'une dorsale reliant les réseaux. En mode de routage par défaut, les pools d'utilisateurs mobiles sont annoncés de manière égale sur les trois réseaux, comme indiqué au bas de la figure.

Notez que, lorsque Prisma Access annonce les itinéraires des utilisateurs mobiles, avant de les annoncer ; ainsi, il annonce les sous-réseaux d'utilisateurs mobiles /20 par morceaux de /24 au fur et à mesure que les préfixes sont consommés par les passerelles.

Prenez note de la façon dont Prisma Access utilise les annonces d'itinéraire BGP :

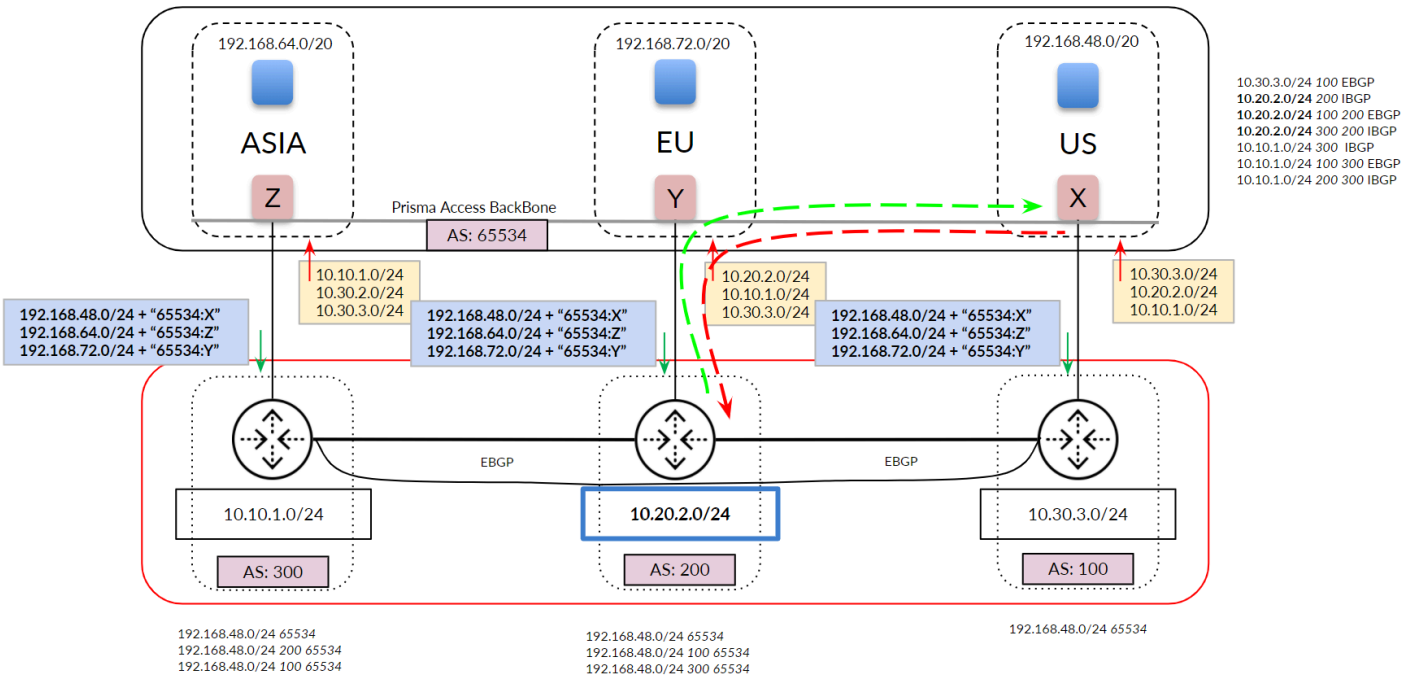
- Prisma Access n'ajuste pas les attributs BGP par défaut pour les itinéraires annoncés par les utilisateurs mobiles (Prisma Access ajoute son numéro AS aux annonces d'itinéraire).
- Prisma Access annonce les itinéraires des utilisateurs mobiles et ajoute des valeurs de communauté BGP dans les itinéraires qu'il annonce via la connexion aux services. La figure suivante montre un déploiement d'utilisateur mobile avec trois connexions aux services et trois blocs d'adresses IP différents spécifiés pour : `192.168.64.0/20` pour la région **Asia, Australia & Japan (Asie, Australie et Japon)**, `192.168.72.0/20` pour la région **Africa, Europe & Middle East (Afrique, Europe et Moyen Orient)** et `192.168.48.0/20` pour la région **North America & South America (Amérique du Nord et Amérique du Sud)**. Prisma Access divise ces itinéraires en blocs de /24 et les annonce avec un numéro AS Prisma Access de **65534**, mais ajoute également les valeurs de la communauté BGP aux annonces (**Z** pour l'Asie, **Y** pour l'UE et **X** pour les États-Unis). Ces itinéraires sont indiqués au milieu de la figure. De cette façon, vous pouvez différencier les connexions aux services dans votre réseau, même si Prisma Access leur attribue le même numéro AS.



 ©2025 Palo Alto Networks, Inc.

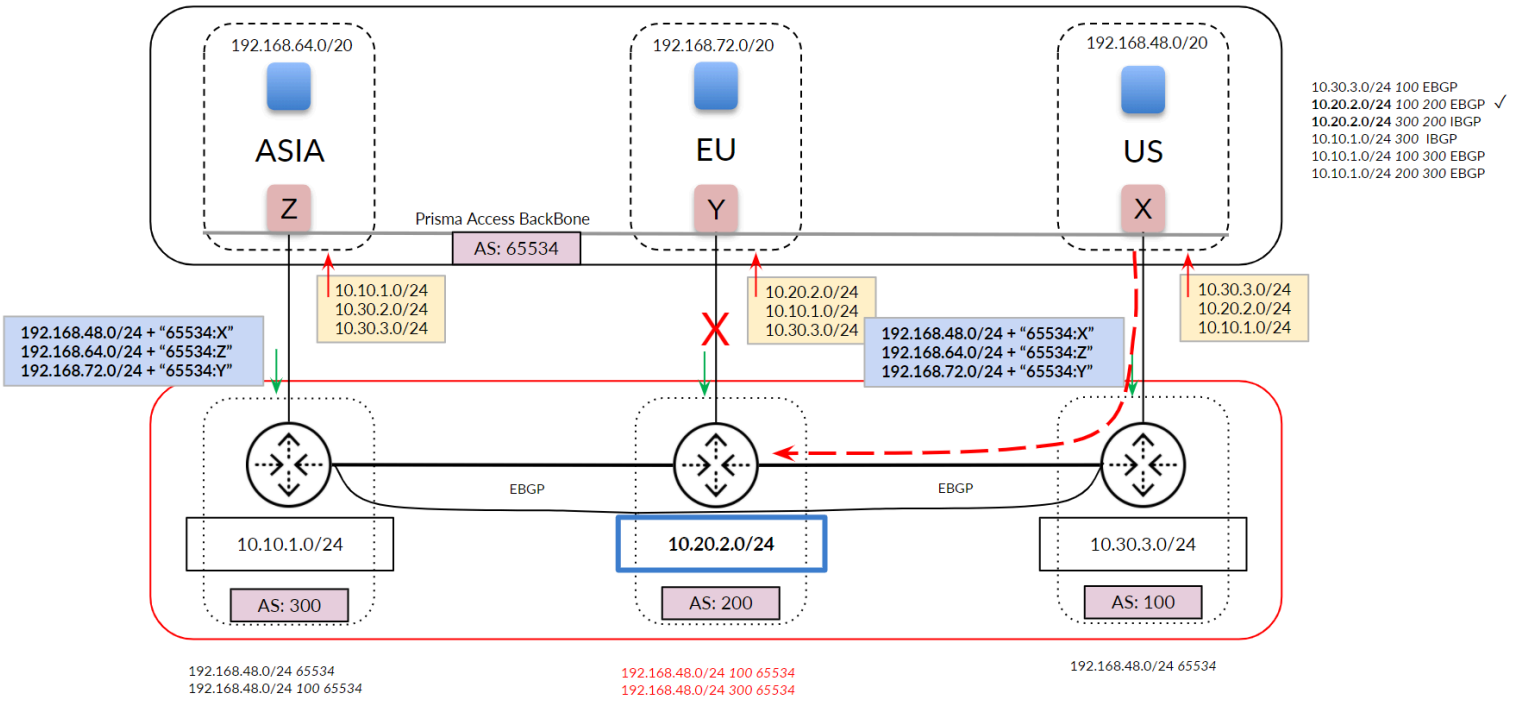
La figure suivante montre un réseau plus courant avec une dorsale eBGP entièrement maillée. La figure montre les itinéraires que Prisma Access a appris du réseau de votre organisation en haut à droite. Notez les itinéraires supplémentaires que Prisma Access a appris via le Prisma Access backbone (iBGP) et le backbone de votre organisation (eBGP).

Pour le trafic entre les utilisateurs mobiles de la région **North America & South America (Amérique du Nord et Amérique du Sud)** (États-Unis dans le diagramme) et le centre de données de la région **Africa, Europe & Middle East (Afrique, Europe et Moyen-Orient)** de votre organisation (UE dans le diagramme), Prisma Access choisit le chemin via la connexion aux services de l'UE car il préfère les itinéraires avec un itinéraire AS-PATH plus court.



Dans les déploiements avec un backbone eBGP entièrement maillé, une asymétrie peut survenir lorsque Prisma Access ne peut pas atteindre un centre de données particulier en raison d'une défaillance ISP/CPE au centre de données du client. La figure suivante montre ce qui pourrait se produire en cas de coupure du lien vers la connexion aux services de l'UE. Votre réseau détecte la défaillance de la liaison et crée une nouvelle table d'itinéraire pour AS 200. Le trafic de la connexion aux services américaine vers AS 200 utilise le chemin via AS 100 car l'itinéraire eBGP pour votre backbone entre AS 200 et AS 100 est préférée à l'itinéraire iBGP entre les connexions aux services UE et États-Unis. Cependant, le trafic de retour n'est pas garanti via le même chemin, car le CPE local peut choisir l'un ou l'autre chemin (affiché en rouge) pour renvoyer le trafic.

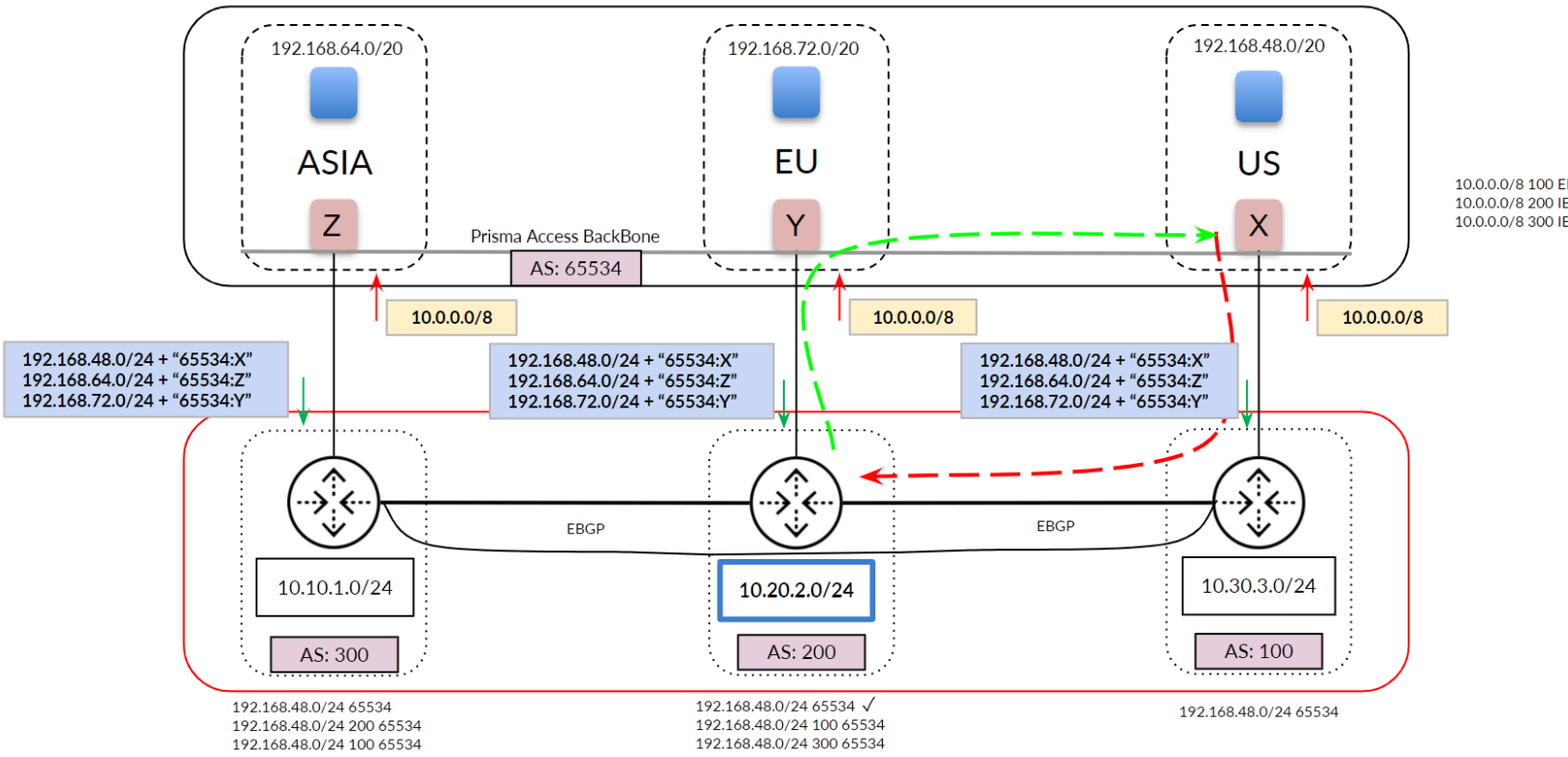
 ©2025 Palo Alto Networks, Inc.



Les exemples précédents montrent un réseau dont les itinéraires n'ont pas été agrégés (c'est-à-dire que vous n'avez pas effectué de résumé de route avant d'envoyer les annonces d'itinéraire BGP à Prisma Access). L'exemple suivant montre un réseau qui résume ses itinéraires vers 10.0.0.0/8 avant de les envoyer à Prisma Access. Si vous sélectionnez le routage par défaut, cette configuration peut entraîner des problèmes de routage asymétrique, car Prisma Access ne peut pas déterminer le chemin de retour correct à partir des itinéraires résumés.

Si votre déploiement Prisma Access possède des réseaux distants, Palo Alto Networks ne recommande pas l'utilisation du résumé d'itinéraire sur les connexions aux services. Le résumé d'itinéraire sur les connexions aux services est destiné uniquement aux déploiements d'utilisateurs mobiles.

 ©2025 Palo Alto Networks, Inc.



Si vous utilisez l'agrégation d'itinéraires pour les utilisateurs mobiles, nous vous recommandons fortement d'activer le routage à chaud au lieu du routage par défaut, où Prisma Access transférez le trafic le plus rapidement possible vers le réseau de votre organisation. De plus, nous vous recommandons de sélectionner un **Backup SC (SC de sauvegarde)** comme décrit dans la section suivante pour chaque connexion de service afin d'avoir un comportement de routage déterministe.

Routage hot potato

Lorsque vous sélectionnez **Hot Potato Routing (Routage Hot Potato)**, Prisma Access fait sortir le trafic lié aux connexions aux services/centres de données de son réseau interne le plus rapidement possible.

Avec un routage hot potato, Prisma Access ajoute le chemin AS (AS-PATH) au préfixe BGP des annonces envoyées depuis les passerelles. Cet ajout est effectué lorsque les préfixes sont annoncés en dehors de la connexion aux services au CPE sur site de votre organisation. Prisma Access ajoute les AS-PATH afin que votre CPE donne la bonne préférence aux tunnels principal et secondaire, de sorte que si le tunnel principal tombe en panne, votre CPE choisit le tunnel secondaire comme tunnel de secours.

Si vous avez spécifié une adresse IP différente pour l'homologue BGP secondaire (de secours), Prisma Access ajoute plus de préfixes en fonction du type de tunnel, comme indiqué dans le tableau suivant.

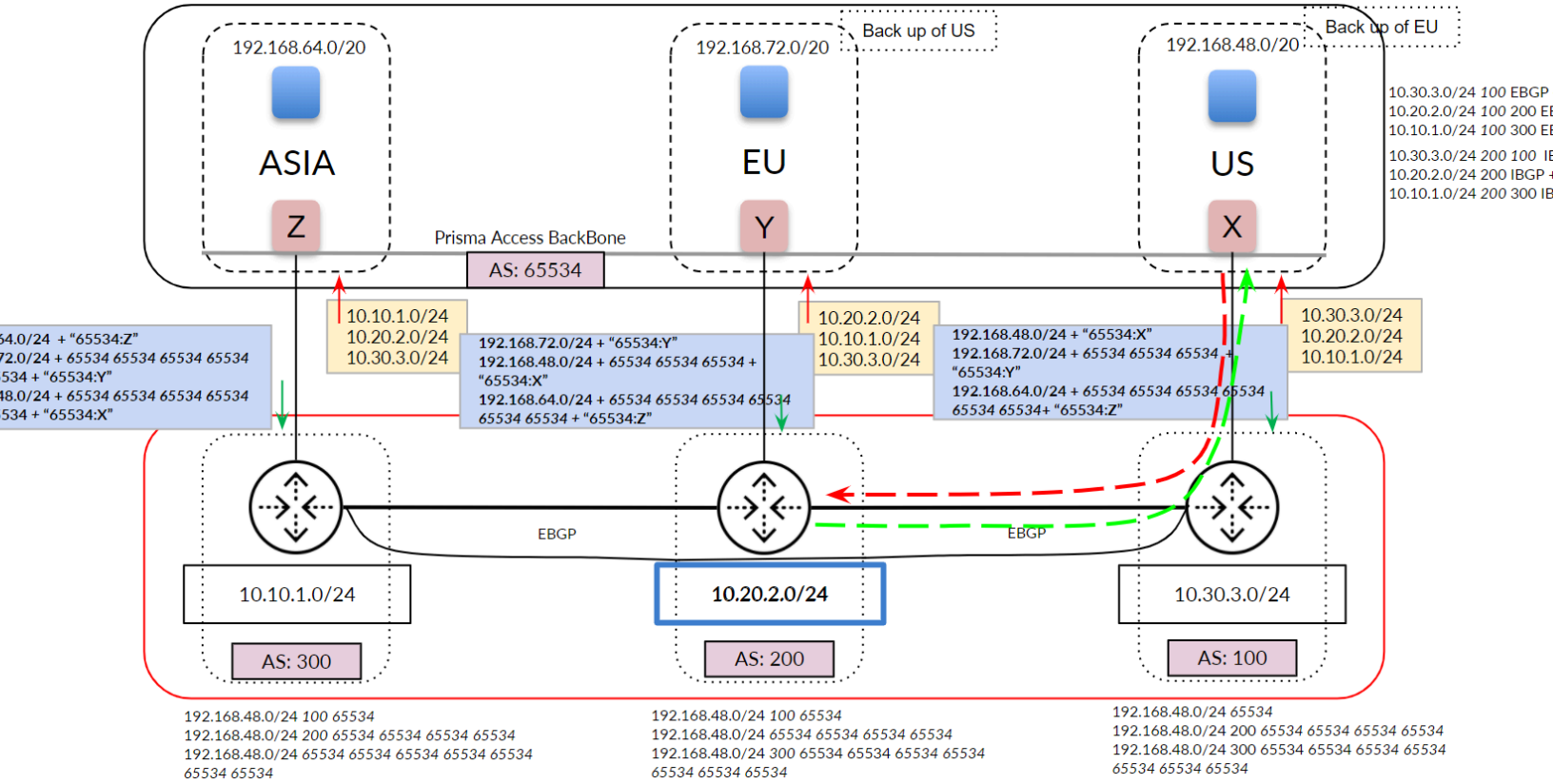
 ©2025 Palo Alto Networks, Inc.

Type de préfixe	Type de tunnel de connexion aux services	Nombre de préfixes As-Path	Nombre total d'AS-PATH observés sur le CPE
Préfixes de passerelle de la connexion aux services principale	Tunnel principal ou secondaire avec la même adresse IP de l'homologue BGP	0	1
Préfixes de passerelle de la connexion aux services de secours	Tunnel principal ou secondaire avec la même adresse IP de l'homologue BGP	3	4
Préfixes de passerelle de toutes les autres connexions aux services	Tunnel principal ou secondaire avec la même adresse IP de l'homologue BGP	6	7
Préfixes de passerelle de la connexion aux services principale	Tunnel secondaire avec une adresse IP de l'homologue BGP différente	1	2
Préfixes de passerelle de la connexion aux services de secours	Tunnel secondaire avec une adresse IP de l'homologue BGP différente	4	5
Préfixes de passerelle de toutes les autres connexions aux services	Tunnel secondaire avec une adresse IP de l'homologue BGP différente	7	8

Spécifiez une **Backup Service Connection (Connexion aux services de sauvegarde)** afin que Prisma Access utilise cette connexion aux services comme sauvegarde lorsqu'une liaison de connexion aux services échoue.

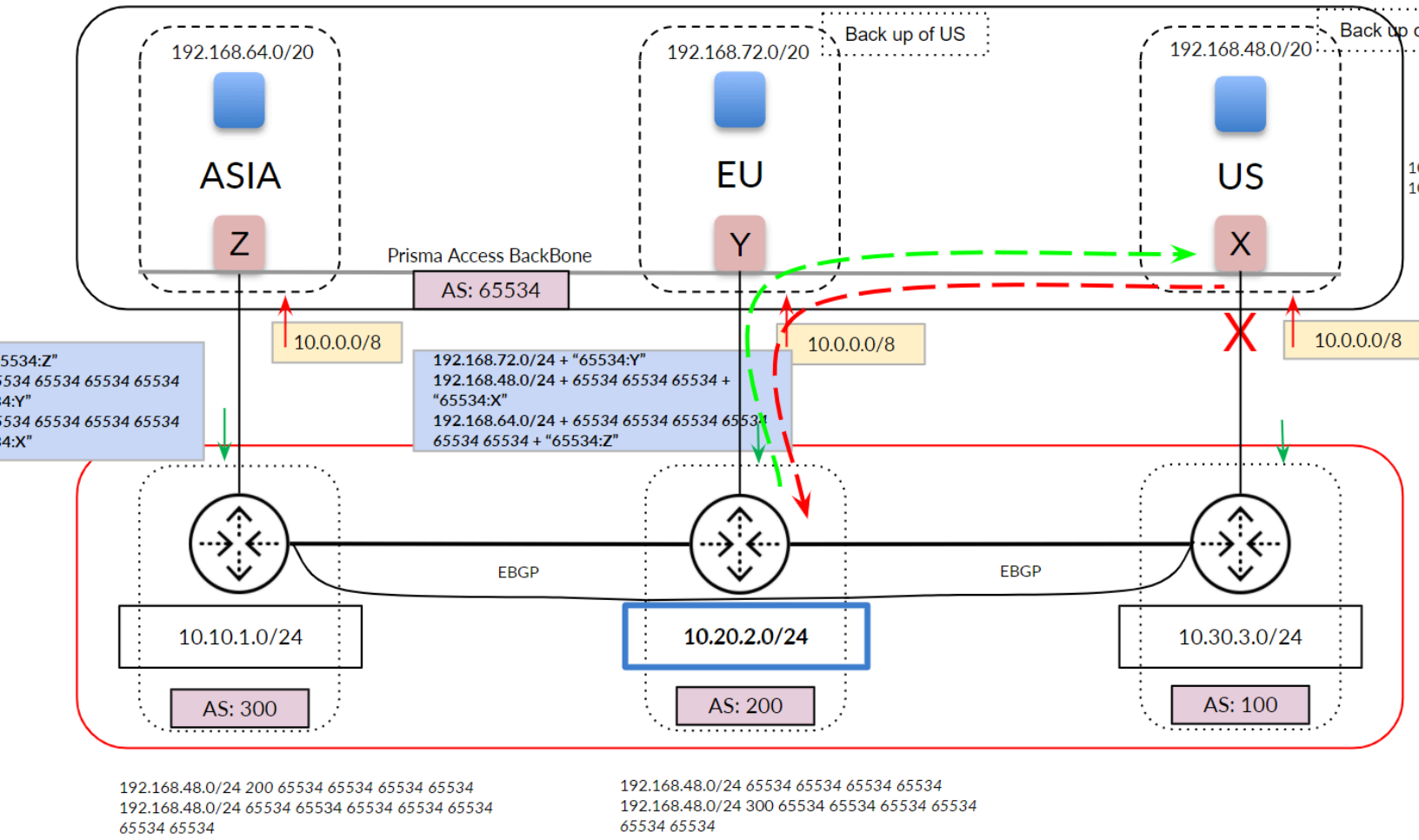
La figure suivante montre une configuration de routage hot potato pour le trafic entre la connexion aux services américaine et AS 200, avec la connexion aux services européenne configurée comme **Backup Service Connection (Connexion aux services de sauvegarde)** de la connexion américaine. En utilisant le routage hot potato, Prisma Access envoie le trafic depuis son chemin de sortie le plus proche via la connexion aux services US. Le trafic de retour emprunte le même chemin via AS100, car ce chemin possède un AS-PATH plus court vers le pool d'utilisateurs mobiles aux États-Unis. Prisma Access ajoute l'AS-PATH à ses annonces de préfixe selon que le tunnel est un tunnel principal, un tunnel de secours ou qu'il n'est pas utilisé pour le tunnel principal ou de secours.

 ©2025 Palo Alto Networks, Inc.



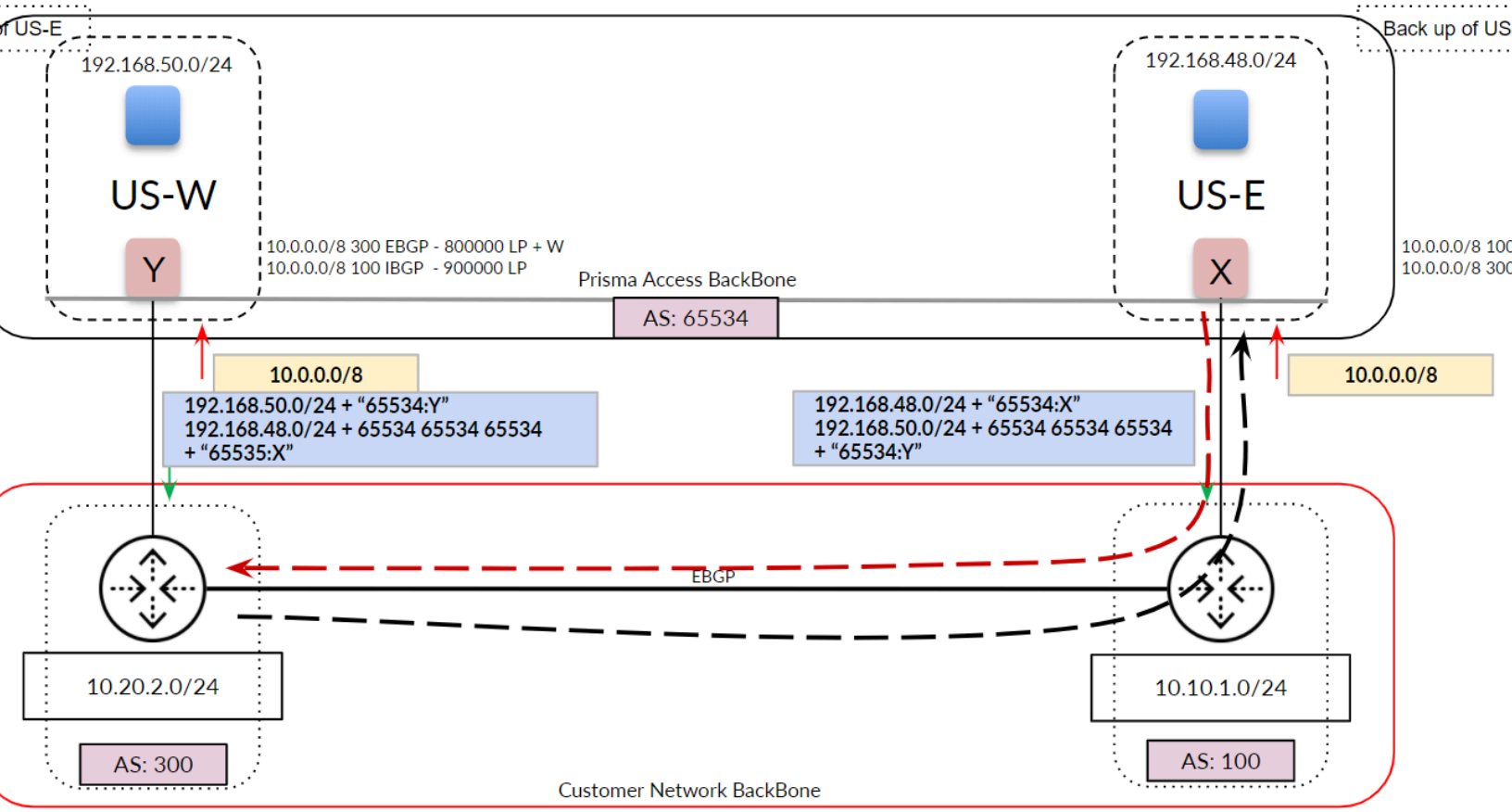
Étant donné que vous avez configuré une connexion aux services de secours, si le lien vers la connexion aux services US tombe en panne, le routage hot potato envoie le trafic en utilisant son itinéraire le plus court via la connexion aux services de l'UE. Ce scénario de routage s'applique également aux réseaux qui utilisent l'agrégation d'itinéraires.

 ©2025 Palo Alto Networks, Inc.



Vous pouvez également utiliser des connexions aux services de secours pour plusieurs connexions aux services dans une seule région. La figure suivante montre un déploiement Prisma Access avec deux connexions aux services dans la région Amérique du Nord. Dans ce cas, vous spécifiez une **Backup Service Connection (Connexion aux services de sauvegarde)** US-E pour la connexion aux services US-W, et vice versa, pour garantir un routage symétrique.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Connecteur ZTNA Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend 200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

Le connecteur Zero Trust Network Access (ZTNA) vous permet de connecter Prisma Access aux applications privées de votre organisation de manière simple et sécurisée. Le connecteur ZTNA permet aux utilisateurs mobiles et aux utilisateurs des succursales d'accéder à vos applications privées à l'aide d'un tunnel sécurisé automatisé. Étant donné que le connecteur ZTNA configure automatiquement les tunnels, vous n'avez donc pas à configurer manuellement les tunnels IPSec et le routage vers les centres de données ou les emplacements du siège, les emplacements de cloud public et les réseaux partenaires où se trouvent vos applications privées.

Les machines virtuelles du connecteur ZTNA que vous déployez se connectent automatiquement à l'emplacement Prisma Access le plus proche, garantissant la meilleure latence possible, en plus de faire évoluer l'accès à la bande passante jusqu'à 2 Gbit/s par connecteur et 8 Gbit/s par groupe de connecteurs.

Prisma Access refuse tout accès par défaut, et un administrateur doit explicitement autoriser l'accès à une ressource à l'aide d'une règle de politique, basée sur nos constructions brevetées User-ID, App-ID et Device-ID, ce qui vous permet de réduire la surface d'attaque et les risques de sécurité. Une fois qu'une connexion est autorisée, nous vérifions en permanence la fiabilité de

cette connexion, nous inspectons en permanence les menaces de sécurité et nous inspectons en permanence les fuites de données. De plus, les adresses IP privées de vos applications ne sont pas exposées lorsque vous utilisez le connecteur ZTNA Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Composants du connecteur ZTNA

- **Connecteurs** : les connecteurs sont les machines virtuelles qui construisent des tunnels pour Prisma Access. Le connecteur ZTNA automatise la gestion du tunnel sans que vous ayez à spécifier les paramètres IPSec et IKE. Vous intégrez des connecteurs dans des machines virtuelles, que vous intégrez dans un service cloud (Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure ou dans un serveur virtuel (VMware ESXi)ou dans une machine virtuelle basée sur le noyau (KVM). Palo Alto Networks vous recommande de déployer la machine virtuelle dans le même sous-réseau que l'application intégrée à Prisma Access. Vous pouvez également fournir un sous-réseau différent, à condition qu'il existe un itinéraire vers les applications à partir du connecteur.

  Après avoir déployé la machine virtuelle du connecteur, Prisma Access gère la machine virtuelle, notamment en vous proposant des options de mise à niveau de la version de la machine virtuelle. Après avoir installé la VM du connecteur ZTNA, il découvre l'emplacement Prisma Access le plus proche et initie un tunnel IPSec sécurisé pour Prisma Access.
- **Groupes de connecteurs** : un groupe de connecteurs est un regroupement logique de connecteurs et d'applications. En ajoutant plusieurs connecteurs dans un groupe de connecteurs, vous fournissez une redondance de tunnel et une bande passante accrue aux applications du groupe. Chaque groupe de connecteurs prend en charge jusqu'à quatre connecteurs.

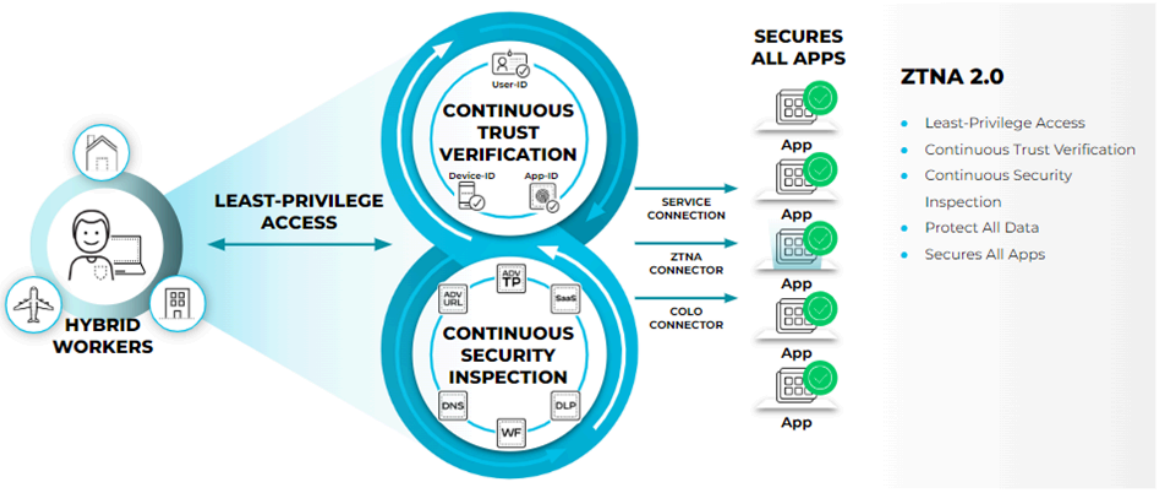
  Si vous souhaitez fournir l'accès à des applications spécifiques à l'aide de différents connecteurs, placez les connecteurs dans des groupes distincts.
- **Cibles** : applications privées que le connecteur ZTNA intègre à Prisma Access. Vous pouvez définir des applications spécifiques auxquelles vous souhaitez fournir un accès à l'aide du FQDN (**FQDN Targets (Cibles FQDN)**), des caractères génériques (**Wildcard Targets (Cibles de caractères génériques)**), ou les adresses IP ou les sous-réseaux où se trouvent les applications. Vous pouvez également faire en sorte que le connecteur ZTNA détecte automatiquement les applications en les extrayant d'un IdP connecté à CIE.

 ©2025 Palo Alto Networks, Inc.

Cas d’utilisation du connecteur ZTNA

Utilisez le connecteur ZTNA dans les scénarios suivants :

- **Se connecter à des applications privées** : utilisez le connecteur ZTNA pour tout le trafic initié par le client qui se connecte à des applications privées.



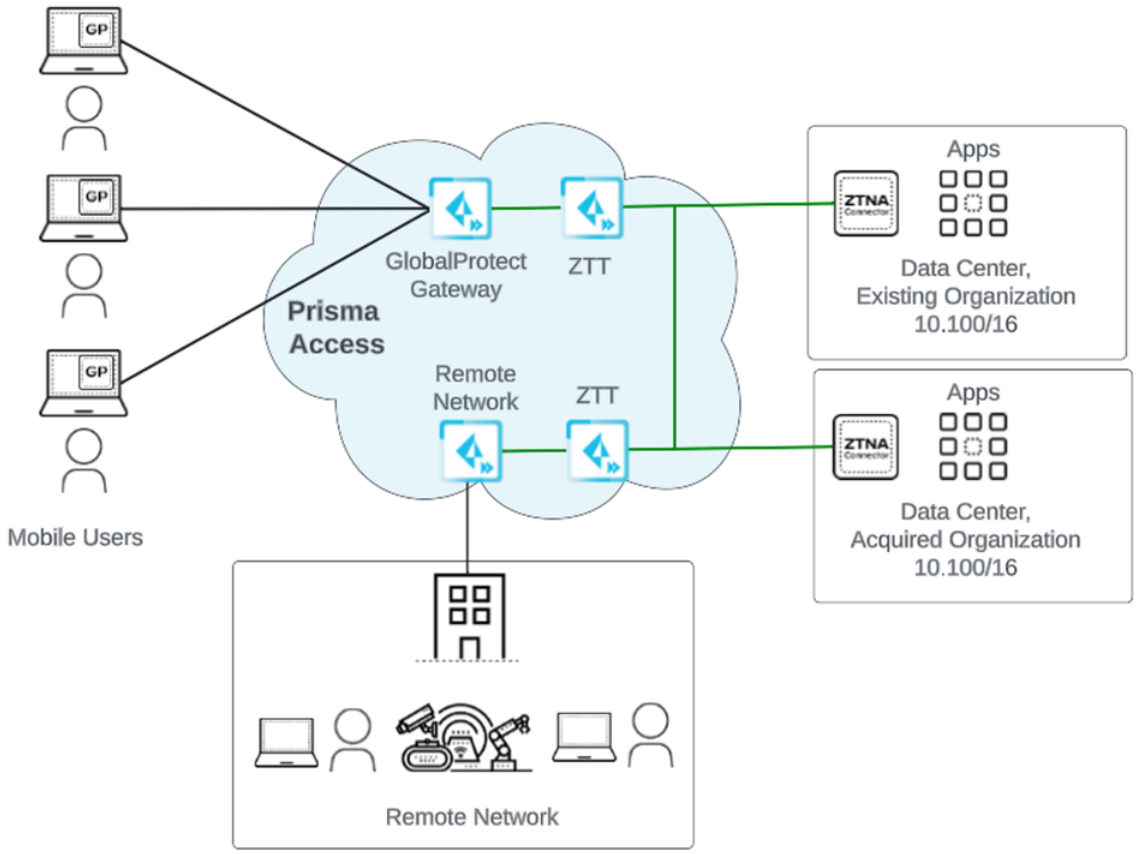
- **Réseaux privés superposés** : si vous êtes administrateur réseau dans une grande entreprise qui a acquis ou fusionné avec une autre organisation, deux réseaux peuvent utiliser des plages d’adresses qui se chevauchent (par exemple, l’espace d’adresse de réseau privé RFC 1918). Pour permettre à vos utilisateurs d’accéder à des applications hébergées dans des réseaux superposés, le routage et la configuration NAT peuvent devenir fastidieux. Le connecteur ZTNA simplifie l’accès aux applications dans les réseaux superposés en vous permettant de vous connecter aux applications à l’aide de FQDN, de caractères génériques FQDN et de sous-réseaux IP, sans que vous ayez à configurer le routage IP.

  Le connecteur ZTNA fournit à vos utilisateurs un accès sécurisé aux applications privées à l’aide des terminateurs de tunnel du connecteur ZTNA (ZTT).

  Lorsque vous activez un connecteur ZTNA dans une région de calcul, les nœuds ZTT sont automatiquement intégrés. Le connecteur ZTNA forme automatiquement des tunnels IPSec avec des ZTT. Les nœuds ZTT d’une région restent actifs pendant 24 heures après la suppression de tous les connecteurs de cette région. Si un nouveau connecteur est déployé dans les 24 heures suivant la suppression de tous les connecteurs dans la même région, il

 ©2025 Palo Alto Networks, Inc.

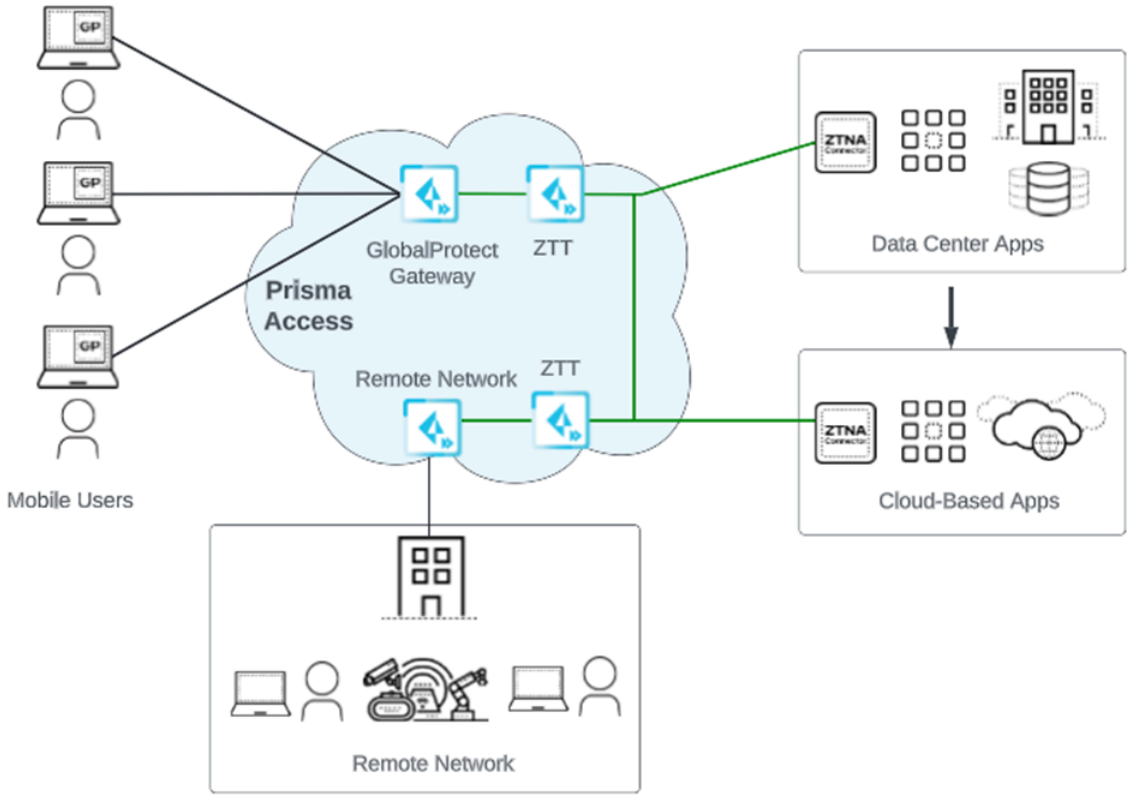
réutilise le ZTT existant. Si un nouveau connecteur ZTNA est activé après 24 heures, un nouveau ZTT est créé.



- **Migration du centre de données vers le cloud** : si votre organisation migre vos applications locales vers le cloud (en migrant vos applications locales existantes à l'aide du « lift and shift » ou en développant des applications cloud natives), vous pouvez héberger des applications dans des VPC cloud dans AWS, GCP, Azure ou d'autres fournisseurs de cloud. Si vous disposez de

 ©2025 Palo Alto Networks, Inc.

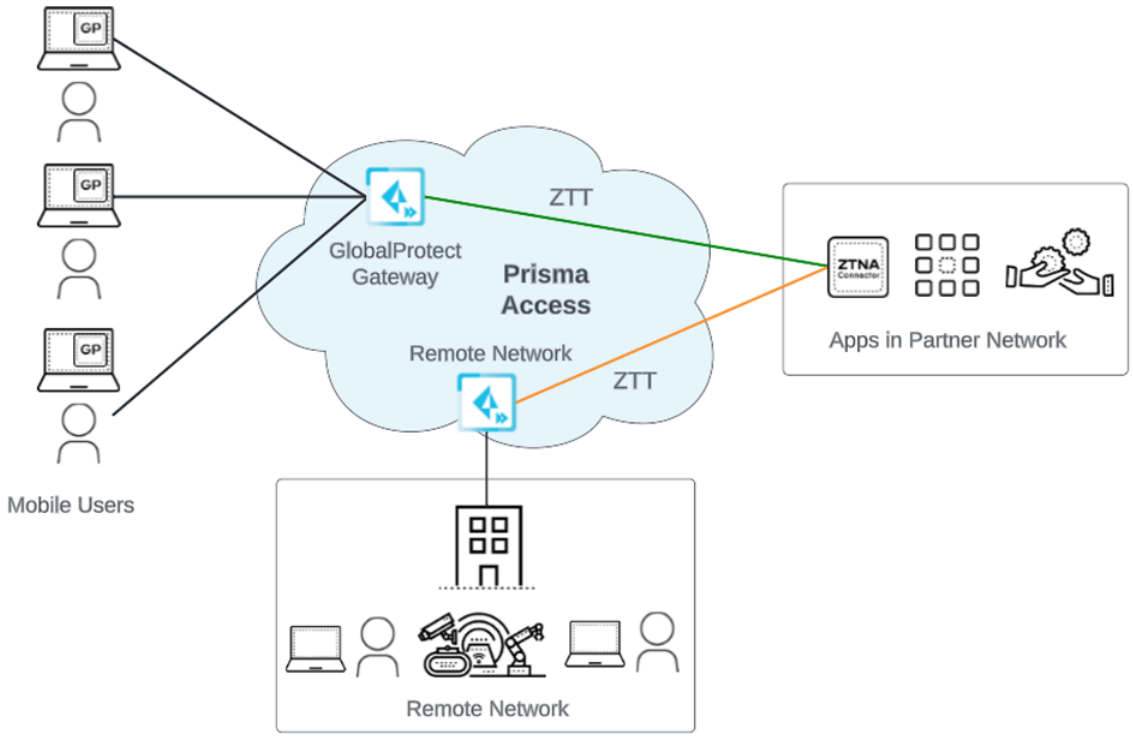
centaines ou de milliers de VPC, le connecteur ZTNA peut accélérer le processus de fourniture d'un accès aux applications fourni par le cloud.



- **Accès aux applications dans les réseaux de partenaires commerciaux** : certaines organisations accèdent à des applications hébergées dans les réseaux de leurs partenaires commerciaux. L'utilisation de connexions aux services pour connecter ces applications nécessite un routage

 ©2025 Palo Alto Networks, Inc.

manuel et une configuration NAT. Le connecteur ZTNA vous permet de vous connecter à ces applications sans effectuer de configuration manuelle du routage IP.



 ©2025 Palo Alto Networks, Inc.

Cas d'utilisation pris en charge pour les connexions aux services et le connecteur ZTNA

Le connecteur ZTNA ne remplace pas les connexions aux services. Il peut compléter ou coexister avec des connexions aux services, ce qui vous permet de sécuriser les applications privées. Si vous avez déjà déployé des connexions aux services, vous pouvez continuer à les utiliser, sauf si vous souhaitez passer à un autre modèle d'accès à l'application. Le tableau suivant présente les cas d'utilisation pris en charge et non pris en charge pour les connexions aux services ou le connecteur ZTNA. Une coche indique que le cas d'utilisation est pris en charge ; un tiret (—) indique qu'il n'est pas pris en charge.

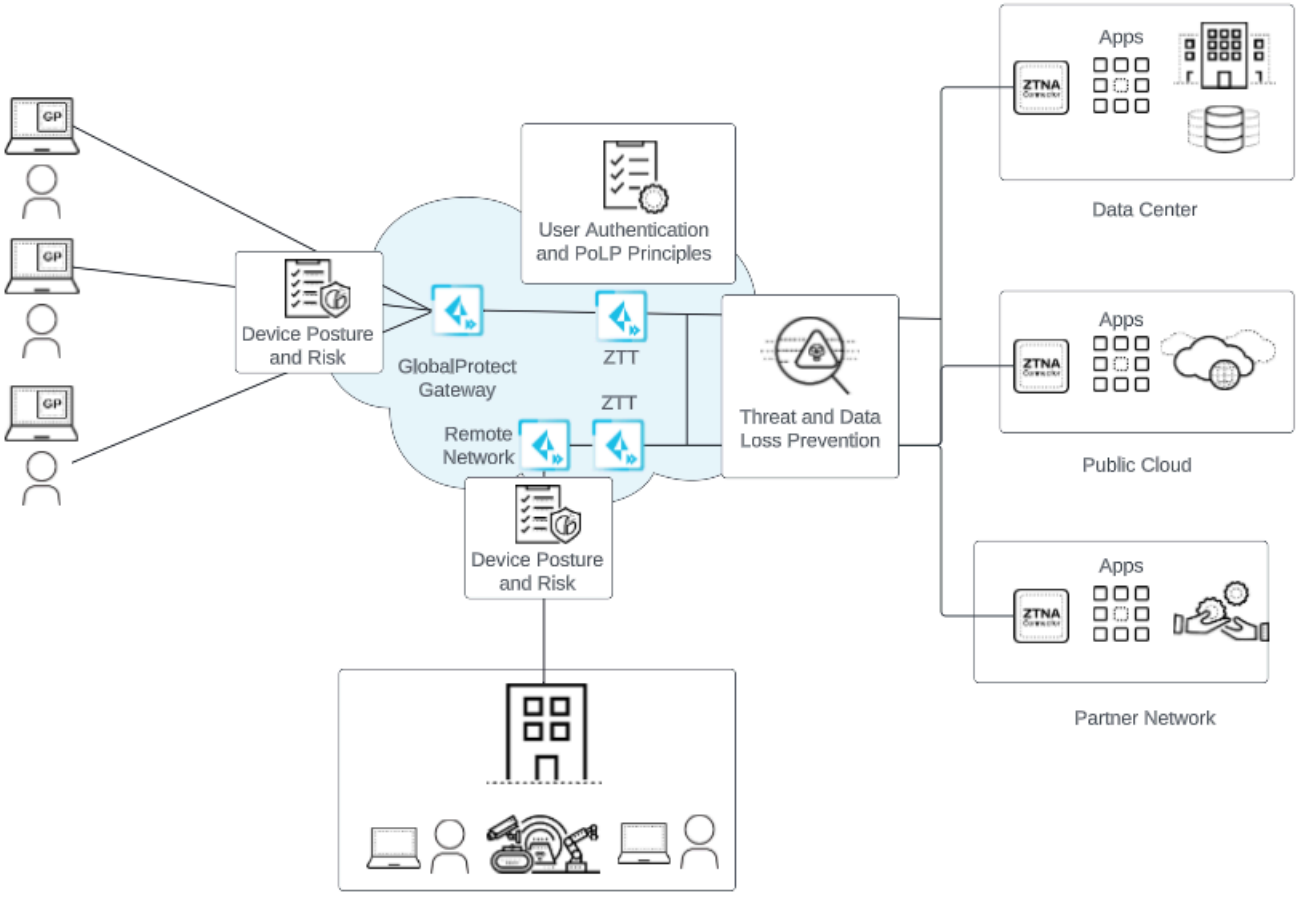
Cas d'utilisation :	Prise en charge du connecteur ZTNA	Prise en charge de la connexion aux services
Accès aux applications dans les réseaux superposés	√	—
Accès à tous les ports et protocoles pour le trafic de l'application initié par le client	√	√
Établissement automatique de tunnels pour Prisma Access	√	—
Découverte de l'emplacement Prisma Access automatique	√	—
Mise à l'échelle automatique des emplacements Prisma Access pour un débit allant jusqu'à 10 Gbit/s	√	—
Accès aux applications privées à l'aide d'adresses IP et de sous-réseaux	√	√
Trafic initié par le serveur (tel qu'un service d'assistance à distance) atteignant un périphérique géré (utilisateur mobile GlobalProtect ou réseau distant).	—	√
Applications ou services qui nécessitent une adresse IP client unique	√	√
Accès aux applications avec des ports dynamiques (tels que le mode FTP actif ou VoIP)	—	√
Déploiements hybrides avec des pare-feu locaux nouvelle génération où des règles de politique basées sur User-ID sont appliquées	√	√

 ©2025 Palo Alto Networks, Inc.

Principes du connecteur ZTNA 2.0

Le connecteur ZTNA vous permet de connecter vos applications privées à Prisma Access en utilisant les principes suivants du connecteur ZTNA 2.0 :

- **Posture et risque du périphérique** : à l'aide de règles de politique basées sur User-ID dans Prisma Access, vous pouvez définir une posture pour les utilisateurs et les périphériques (utilisateurs mobiles et périphériques IoT) afin d'empêcher tout accès non autorisé aux applications privées. Vous pouvez également créer des règles de politique communes entre le connecteur ZTNA et Prisma Access.
- **Authentification de l'utilisateur et accès à moindre privilège** : à l'aide de l'authentification de l'utilisateur et de règles de politiques basées sur l'utilisateur ou le groupe, vous pouvez implémenter le principe du moindre privilège (PoLP) pour permettre aux utilisateurs d'accéder aux applications dont ils ont besoin, tout en bloquant l'accès aux applications dont ils n'ont pas besoin.
- **Prévention des menaces et des pertes de données** : Prisma Access et le connecteur ZTNA utilisent des fonctionnalités de sécurité avancées telles que Advanced Threat Prevention, Advanced URL Filtering, SaaS Security, Advanced WildFire et Enterprise DLP pour s'assurer que vos applications privées et vos données d'application sont sécurisées.



 ©2025 Palo Alto Networks, Inc.

Exigences et directives du connecteur ZTNA

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend 200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

Avant de configurer le connecteur ZTNA, assurez-vous de bien comprendre les exigences et les limites du connecteur, ainsi que les directives à suivre lors de son déploiement.

Versions de Prisma Access prises en charge configuration requise

- Version 4.0 de Prisma Access avec un agent SaaS compatible.

  Mettez à niveau toute version de Prisma Access antérieure à la version 4.0, y compris les versions d'Innovation, vers une version minimale de 4.0.

  Une version 5.0 de Prisma Access au minimum est requise si vous souhaitez utiliser les caractères génériques FQDN ou les sous-réseaux IP pour accéder aux applications. De plus, la version 5.0 de Prisma Access débloque l'utilisation des outils de diagnostic de la vue d'ensemble du vidage, de la capture de paquets et du support technique.
- Vous devez mettre à niveau les versions de vos connecteurs à un minimum de 6-2-2-ztna-connector-B1 pour utiliser la fonctionnalité de la version 5.0.

 ©2025 Palo Alto Networks, Inc.

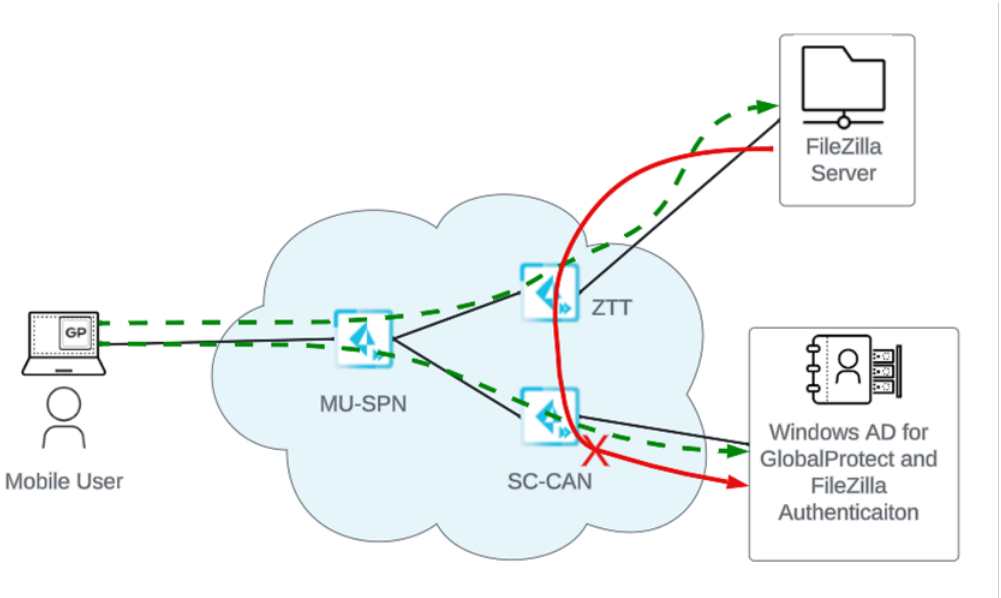
- Pour Prisma Access (Managed by Panorama), mettez à niveau la version du plug-in Cloud Services vers une version minimale de 4.0. Passez au dernier plug-in Cloud Services pour débloquer les dernières fonctionnalités.

Prises en charge des applications

Le connecteur ZTNA permet d'accéder à l'ensemble du trafic de vos applications privées, à l'exception des suivantes :

- Le connecteur ZTNA ne prend pas en charge les éléments suivants :
  - Trafic provenant du centre de données (par exemple, SCCM ou le trafic du service d'assistance à distance).
  - Redistribution de User-ID.
  - Applications qui effectuent le saut de port (telles que VoIP ou FTP en mode actif).
  - Applications de passerelle au niveau de l'application (ALG) telles que FTP et SIP en mode actif.
  - L'authentification intégrée à Windows pour les applications (telles que NTLM ou Kerberos) n'est prise en charge que si vous intégrez les contrôleurs de domaine et les ressources du centre de données en tant que sous-réseaux d'adresses IP. SAML, OAuth et LDAP sont pris en charge.
  - Communication entre les applications derrière une connexion aux services et les applications derrière un connecteur ZTNA.

    Par exemple, vous hébergez un serveur Windows Active Directory (AD) derrière une connexion aux services (puisque les serveurs AD ne sont pas pris en charge derrière un connecteur ZTNA) et hébergez un serveur FTP (Filezilla) derrière un connecteur ZTNA. Si le serveur FTP exige une authentification auprès du serveur Windows AD, l'authentification échoue, car vous ne pouvez pas utiliser Prisma Access en tant que dorsale entre le nœud d'accès d'entreprise de connexion aux services (SC-CAN) et le terminateur de tunnel de connecteur ZTNA (ZTT).



 ©2025 Palo Alto Networks, Inc.

Restrictions relatives aux caractéristiques et aux fonctionnalités

Gardez à l'esprit les restrictions suivantes lors de l'installation et de la configuration d'un déploiement de connecteur ZTNA :

- N'utilisez pas de caractères spéciaux, notamment < > ! @ # $ % ^ & et des caractères chinois, japonais ou coréens, dans les noms d'objets ZTNA.
- Les fonctionnalités suivantes ne sont pas prises en charge avec le déploiement par défaut de Prisma Access : contactez votre équipe Palo Alto Networks pour les activer :
  - Utilisez les adresses RFC 6598 pour vos adresses IP de l'infrastructure Prisma Access avec le connecteur ZTNA
- **Directives relatives aux groupes de connecteurs** : lors de l'ajout de groupes de connecteurs, utilisez les recommandations suivantes :
  - Toutes les applications d'un seul groupe de connecteurs doivent utiliser le même serveur DNS pour la résolution DNS.
  - Si vous accédez à des applications à partir d'un centre de données ou d'un siège social, toutes les applications du groupe de connecteurs doivent provenir du même centre de données ou du même siège social.
  - N'ajoutez pas de connecteurs dans deux régions ou plus au sein d'un seul groupe de connecteurs. Tous les connecteurs d'un groupe de connecteurs doivent se trouver dans la même région.
  - À partir de Prisma Access 5.01, vous pouvez spécifier jusqu'à quatre groupes de connecteurs par cible FQDN ou cible de caractères génériques (les versions 5.0 et antérieures prennent en charge un seul groupe de connecteurs par cible FQDN ou cible de caractères génériques). Assurez-vous que, lorsque vous attribuez des groupes de connecteurs par FQDN ou cible de caractères génériques, vous n'attribuez pas la même application à plus de quatre connecteurs par région.

    Par exemple, vous avez attribué la même application (une cible FQDN ou une cible de caractères génériques) à quatre groupes de connecteurs, chaque groupe a un seul connecteur et tous les connecteurs se trouvent dans la même région. Cette configuration est acceptable, car vous n'attribuez pas plus de quatre connecteurs par application dans une seule région.

    Toutefois, si vous attribuez la même application (soit une cible FQDN, soit une cible de caractères génériques) à trois groupes de connecteurs, chaque groupe a deux connecteurs et tous les connecteurs se trouvent dans la même région, il s'agit d'une configuration non valide, car vous attribuez six connecteurs à la même application dans une seule région.
- Certains connecteurs ZTNA tels que les connecteurs basés sur AWS ou les connecteurs basés sur Azure prennent en charge la mise à l'échelle automatique, où AWS ou Azure surveille l'utilisation de la bande passante réseau sur les connecteurs et ajuste automatiquement la capacité pour maintenir les performances de l'application. Lorsque l'utilisation de la bande passante réseau sur les connecteurs diminue, AWS ou Azure déclenche la montée en charge automatique. Si la mise à l'échelle se produit dans un connecteur ZTNA, les sessions de longue durée existantes gérées par le connecteur ZTNA marqué pour la mise à l'échelle se terminent prématurément. Ce comportement n'a pas d'impact sur les nouvelles sessions de trafic initiées après la mise à l'échelle. Pour les sessions de longue durée, telles que SSH ou RDP, le

 ©2025 Palo Alto Networks, Inc.

connecteur ZTNA met fin à la session pendant la mise à l'échelle et vous devez reconnecter cette session.

Considérations relatives à l'échelle et au débit

Le connecteur ZTNA prend en charge les valeurs maximales suivantes :

- 4 096 applications par locataire dans tous les groupes de connecteurs
- 200 connecteurs par locataire
- 512 applications par groupe de connecteurs
- 4 connecteurs par groupe de connecteurs
- 200 000 sessions simultanées par connecteur

  Chaque connecteur peut prendre en charge 200 000 connexions simultanées. Un groupe de connecteurs peut avoir un maximum de 4 connecteurs pour un maximum de 800 000 connexions simultanées par groupe de connecteurs.
- 26r régions de calcul
- Débit de 1 Gbit/s par connecteur, avec un maximum de 10 Gbit/s par emplacement de calcul Prisma Access

Prise en charge des environnements d'hébergement d'applications

Vous pouvez déployer vos machines virtuelles de connecteur ZTNA dans les environnements de centre de données suivants avec la configuration minimale requise spécifiée :

Fournisseur de cloud	Taille de l'instance	Taille du processeur	Taille de la mémoire	Taille du disque
Amazon AWS	m5.xlarge par région	4 vCPU	16 Go	40 Go
Google Cloud Platform (GCP)	n2-standard-4 par région	4 vCPU	16 Go	40 Go
Microsoft Azure	Standard_D4_v3 par région	4 vCPU	16 Go	40 Go
KVM	Utilise l'image qcow	4 vCPU	16 Go	40 Go
Hyper-V	Utilise l'image vhd	4 vCPU	8 Go de mémoire par VM	40 Go
VMware ESXi	Utilise l'image OVA. Pris en charge sur vSphere et	4 vCPU par VM	8 Go de mémoire par VM	Disque de 40 Go (Thick Provisioned)

 ©2025 Palo Alto Networks, Inc.

Fournisseur de cloud	Taille de l'instance	Taille du processeur	Taille de la mémoire	Taille du disque
	directement sur les hôtes ESXi			

Pour VMware ESXi, vMotion, les instantanés de VM ou les migrations ne sont pas pris en charge pour les VM de connecteur.

Pour KVM, les migrations dynamiques et les instantanés ne sont pas pris en charge sur les VM de connecteur.

Il est de votre responsabilité d'héberger les VM et de vous assurer qu'elles peuvent se connecter à Internet.

AWS, GCP et Azure disposent de connecteurs ZTNA que vous pouvez acquérir sur leurs marketplaces respectifs. Vous pouvez télécharger le fichier OVA (Open Virtualization Application) VMware ESXi et le fichier qcow KVM à partir du portail du support client de Palo Alto.

Configuration réseau requise

Les exigences de mise en réseau suivantes permettent la connectivité entre le connecteur ZTNA et Prisma Access :

- Après avoir activé le connecteur ZTNA, Prisma Access configurez un proxy DNS pour les requêtes DNS utilisant les règles DNS configurées pour les réseaux distants et les utilisateurs mobiles – GlobalProtect.
- La taille de la charge utile UDP, y compris les en-têtes, ne doit pas dépasser une taille MTU de 1 300 octets sur le chemin d'accès au serveur d'applications ZTNA. Palo Alto Networks recommande de maintenir les paquets à cette taille MTU ou en dessous.
- Autorisez les ports UDP 4500 et UDP 500 sortants à partir de l'adresse IP de l'interface WAN (port 1) pour la connectivité IPSec et IKE au terminateur de tunnel ZTNA (ZTT). Si vous souhaitez limiter l'activation d'une connexion UDP sortante 500 et 4500 à une seule adresse IP, activez-la pour l'adresse **PA Service IP (IP de service PA)** (sous **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)**) du connecteur ZTNA.



- Si le connecteur ZTNA utilise une adresse IP publique pour son interface Internet, vous devez autoriser une charge utile de sécurité d'encapsulation IP/50 (Encapsulating Security Payload, ESP).
- Autorisez la connectivité HTTPS du port TCP 443 sortant de l'interface WAN (port 1) et de l'adresse IP aux contrôleurs de connecteur ZTNA.
- Le connecteur ZTNA configure automatiquement le côté ZTT de Prisma Access du tunnel IPSec et le côté du connecteur ZTNA. Les algorithmes configurés pour DH Group/ Encryption/Hash pour IKE et ESP sont les suivants : ecp384/aes256/sha512.

 ©2025 Palo Alto Networks, Inc.

- N'arrêtez pas le tunnel IPSec que le connecteur ZTNA crée et utilise pour accéder aux applications privées.
- (Utilisateurs mobiles – déploiements GlobalProtect uniquement) Lorsque vous intégrez pour la première fois une application dans le connecteur ZTNA, vous devez actualiser l'application GlobalProtect afin que les utilisateurs mobiles reçoivent la configuration de serveur DNS mise à jour. Si vous avez supprimé une application du connecteur ZTNA, vous devez actualiser l'application GlobalProtect afin que les utilisateurs mobiles puissent recevoir la configuration du serveur DNS mise à jour.
- S'il existe un pare-feu entre le connecteur ZTNA et l'application privée, le pare-feu doit autoriser l'accès à l'application à partir du connecteur ZTNA (c'est-à-dire que vous devez autoriser l'accès aux adresses IP, protocoles et ports résolus du serveur d'applications pour l'application privée).

  En outre, vous devez autoriser le protocole (TCP ou ICMP) que vous avez configuré pour les sondes d'état cibles de l'application à l'application. L'application de connecteur sonde le serveur d'applications pour déterminer s'il peut fournir l'accès à l'application, et vous pouvez configurer le type de sondage pour la cible d'application sur **tcp ping**, **icmp ping**ou **none (aucun)** (pas de sondage). Si vous spécifiez **tcp ping**, le pare-feu doit autoriser l'accès TCP à l'application ; si vous spécifiez **icmp ping**, le pare-feu doit autoriser la requête d'écho ICMP et la réponse pour l'application.
- Assurez-vous d'autoriser ICMP dans votre centre de données avant d'utiliser les outils de diagnostic ping et traceroute. Dans certains environnements cloud, ICMP n'est pas autorisé pour des raisons de sécurité. Dans ce cas, ces outils n'affichent aucune activité.

  L'outil de diagnostic traceroute utilise également des ports UDP aléatoires, de sorte que vous devez autoriser toutes les réponses d'erreur UDP et ICMP pour que l'outil traceroute fonctionne.
- Assurez-vous d'avoir configuré les entrées DNS sur les interfaces locales pour permettre au connecteur ZTNA de résoudre les FQDN de l'application, et que vous avez également configuré le connecteur ZTNA, et accédez au serveur DNS sur le port UDP 53 (le port utilisé pour la résolution DNS).
- (Connecteur ZTNA versions 5.0 et ultérieures) Assurez-vous d'avoir configuré des règles de sécurité dans votre réseau pour permettre aux connecteurs ZTNA d'effectuer des sondes d'application dans votre centre de données. Les connecteurs ZTNA utilisent l'adresse IP de leur interface de centre de données comme adresse IP source du sondage de l'application pour les serveurs d'applications. Si le sondage de l'application réussit, l'état de l'application est **Up (Actif)** et les sessions utilisateur vers le connecteur ZTNA ont la même adresse IP d'interface de centre de données que l'adresse IP source. Si le sondage de l'application échoue, l'état de l'application est **Down (Inactif)** ; dans ce cas, vous pouvez utiliser l'option des outils de diagnostic ping et tcp ping pour tester les connexions à l'application.
- Si vous utilisez des adresses partagées RFC 6598 au sein de votre réseau, vous devez spécifier des blocs d'adresses IP que le connecteur ZTNA peut utiliser pour le routage entre Prisma Access et vos connecteurs et entre Prisma Access et vos applications privées.

 ©2025 Palo Alto Networks, Inc.

- Si vous devez restreindre la liste d'adresses IP et de FQDN que vous ajoutez aux listes d'autorisation de votre organisation, ajoutez ceux répertoriés dans Adresses IP et FQDN pour autoriser le connecteur ZTNA.

  Par exemple, si vous configurez un connecteur ZTNA aux États-Unis, ajoutez les URL suivantes aux listes d'autorisation de votre organisation :

  - https://controller.cgnx.net
  - https://locator.cgnx.net
  - https://controller.hood.cgnx.net
  - https://vmfg.hood.cgnx.net
  - https://sdwan-stats-hood-us.cgnx.net
  - time.nist.gov (pour NTP)
  - 0.cloudgenix.pool.ntp.org (pour NTP)
  - 1.cloudgenix.pool.ntp.org (pour NTP)
  - 2.cloudgenix.pool.ntp.org (pour NTP)
  - 3.cloudgenix.pool.ntp.org (pour NTP)

  Limitez la résolution DNS des FQDN précédents à la résolution IPv4. Le connecteur ZTNA ne prend pas en charge l'établissement d'une connexion aux FQDN du contrôleur à l'aide d'IPv6.

- Désactivez le décryptage SSL pour les sessions sur les contrôleurs.

Adresses IP et FQDN pour autoriser le connecteur ZTNA

Pour garantir le bon fonctionnement du connecteur ZTNA, ajoutez les URL et adresses IP suivantes à vos listes d'autorisation.

Nom du service	Port	Direction	Protocole Internet d'interface source	Destination et adresses IP
Accès du connecteur ZTNA à Prisma Access	443	Sortant	Port WAN du connecteur ZTNA	https://controller.cgnx.net Adresse : 52.8.93.87 Adresse : 52.8.25.40 https://locator.cgnx.net Adresse : 13.56.217.238 Adresse : 13.56.201.169 capot: 52.40.98.31 34.218.98.185 Sugarloaf: 18.200.102.82

 ©2025 Palo Alto Networks, Inc.

Nom du service	Port	Direction	Protocole Internet d'interface source	Destination et adresses IP
				18.200.135.33 Faber: 18.139.242.53 54.255.61.109 https://vmfg.cgnx.net Adresse : 52.53.122.104 Adresse : 52.53.102.7 https://controller.elcapitan.cgnx.net Adresse : 52.8.93.87 Adresse : 52.8.25.40 https://vmfg.elcapitan.cgnx.net Adresse : 52.53.122.104 Adresse : 52.53.102.7 https://controller.hood.cgnx.net Adresse : 52.32.167.5 Adresse : 54.70.168.33 https://vmfg.hood.cgnx.net Adresse : 50.112.136.184 Adresse : 34.210.34.87 https://controller.sugarloaf.cgnx.net Adresse : 108.128.176.192 Adresse : 18.200.144.58 https://vmfg.sugarloaf.cgnx.net Adresse : 99.81.179.99 Adresse : 99.80.52.255 https://sdwan-stats-hood-us.cgnx.net https://sdwan-stats-elcapitan-us.cgnx.net https://sdwan-stats-hood-jp.cgnx.net

 ©2025 Palo Alto Networks, Inc.

Nom du service	Port	Direction	Protocole Internet d'interface source	Destination et adresses IP
				https://sdwan-stats-elcapitan-jp.cgnx.net https://sdwan-stats-hood-sg.cgnx.net https://sdwan-stats-elcapitan-sg.cgnx.net https://sdwan-stats-hood-au.cgnx.net https://sdwan-stats-elcapitan-au.cgnx.net https://sdwan-stats-hood-in.cgnx.net https://sdwan-stats-elcapitan-in.cgnx.net https://sdwan-stats-hood-ca.cgnx.net https://sdwan-stats-elcapitan-ca.cgnx.net https://sdwan-stats-sugarloaf-eu.cgnx.net https://sdwan-stats-sugarloaf-de.cgnx.net https://sdwan-stats-sugarloaf-uk.cgnx.net https://controller.bowfell.cgnx.net Adresse : 13.41.243.90 Adresse : 18.171.17.23 https://vmfg.bowfell.cgnx.net Adresse : 52.56.35.36 Adresse : 52.56.224.242 https://controller.faber.cgnx.net Adresse : 52.74.47.220 Adresse : 13.251.109.27 https://vmfg.faber.cgnx.net

 ©2025 Palo Alto Networks, Inc.

Nom du service	Port	Direction	Protocole Internet d'interface source	Destination et adresses IP
				Adresse : 18.142.153.59 Adresse : 52.74.58.219 h ttps:// controller.townsend.cgnx.net Adresse : 13.55.31.41 Adresse : 3.106.168.215 https:// vmfg.townsend.cgnx.net Adresse : 52.64.177.240 Adresse : 13.55.164.51 https://sdwan-stats-faber-sg.cgnx.net https://sdwan-stats-bowfell-uk.cgnx.net https://sdwan-stats-townsend-au.cgnx.net
NTP	123	Sortant	Ports WAN et LAN du connecteur ZTNA	time.nist.gov 0.cloudgenix.pool.ntp.org 1.cloudgenix.pool.ntp.org 2.cloudgenix.pool.ntp.org 3.cloudgenix.pool.ntp.org
DNS	53	Sortant	Ports WAN et LAN du connecteur ZTNA	Serveurs DNS du client ou du fournisseur

Gestion des certificats

Pour garantir la confiance entre les parties lors d'une session de communication sécurisée, Prisma Access utilise des certificats numériques. Chaque certificat contient une clé cryptographique pour crypter un texte brut ou décrypter un texte crypté. Chaque certificat contient également une signature numérique pour authentifier l'identité de l'émetteur. L'émetteur doit figurer dans la liste des Certificate Authorities (autorités de certification ; AC) de confiance de la partie chargée de l'authentification. La partie authentifiante a la possibilité de vérifier que l'émetteur n'a pas révoqué le certificat. Prisma Access utilise des certificats pour sécuriser des fonctionnalités telles que le décryptage et l'authentification, et pour sécuriser la communication entre tous les clients, serveurs, utilisateurs et périphériques se connectant à votre réseau.

 ©2025 Palo Alto Networks, Inc.

Pour les applications intégrées au connecteur ZTNA, configurez vos certificats, ajoutez des autorités de certification et définissez des vérifications de certificats à l'aide de laPrisma Access gestion des certificats.

 ©2025 Palo Alto Networks, Inc.

Activer le connecteur ZTNA

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend 200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

Avant de pouvoir configurer le connecteur ZTNA, vous devez l'activer dans Prisma Access. Avant d'activer le connecteur ZTNA, procédez comme suit :

- Passez en revue les Exigences et directives du connecteur ZTNA.
- Identifiez les blocs d'adresses IP de votre application et de votre connecteur. Vous devez réserver un pool d'adresses distinct à réserver pour une utilisation dans Prisma Access en interne pour acheminer le trafic vers les connecteurs et les applications privées que vous intégrerez. Prisma Access résout les FQDN des applications que vous intégrez au connecteur ZTNA aux adresses IP du bloc d'adresses IP de l'application. De la même manière, Prisma Access utilise le bloc d'adresses IP du connecteur pour acheminer le trafic du réseau distant ou de l'utilisateur mobile vers le connecteur ZTNA approprié.

  Vous devez réserver au moins un sous-réseau /16 pour le pool d'adresses. Utilisez les adresses RFC 1918 ou RFC 6598. Vous pouvez spécifier un pool d'adresses RFC 1918 lors de la configuration du connecteur ZTNA au lieu de RFC 6598. Cependant, vous ne pouvez pas modifier le type de pool d'adresses sur RFC 6598 après avoir spécifié RFC 1918.
- Strata Cloud Manager

 ©2025 Palo Alto Networks, Inc.

- Panorama

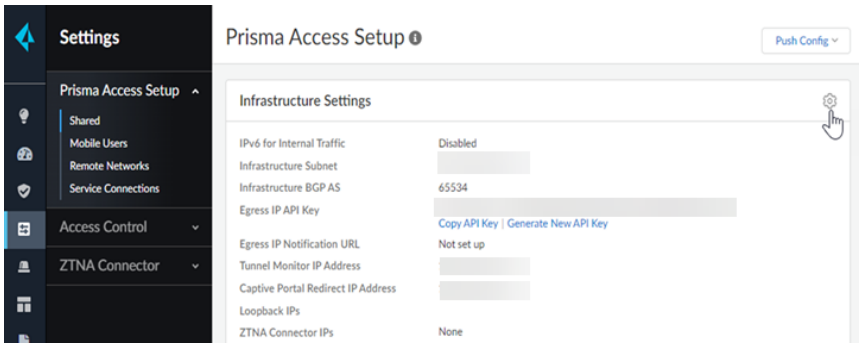
Activer le connecteur ZTNA (Strata Cloud Manager)

Utilisez le flux de travail suivant pour activer le connecteur ZTNA dans Prisma Access géré par le cloud.

STEP 1 | Configurez les blocs d'adresses IP que Prisma Access utilisera en interne pour acheminer le trafic vers le connecteur ZTNA et les applications privées que vous intégrez.

Vous devez définir des blocs d'adresses IP distincts pour vos connecteurs et vos applications et les blocs ne peuvent pas se chevaucher les uns avec les autres, avec le sous-réseau d'infrastructure Prisma Access ou avec votre pool d'adresses IP GlobalProtect.

- Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Paramètres d'infrastructure)**.



- Ajoutez **ZTNA Connectors Application IP Blocks (Blocs d'adresses IP d'applications de connecteurs ZTNA)**.

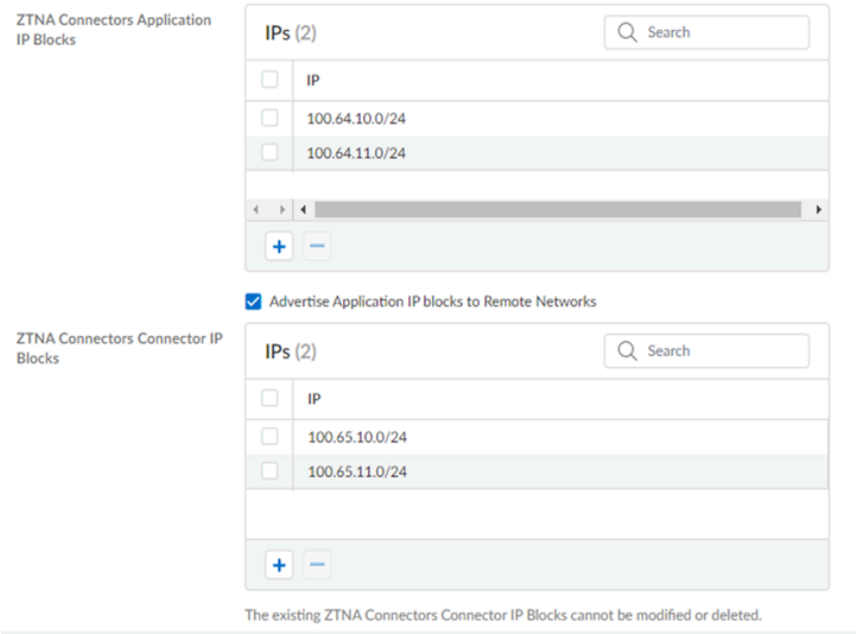
  Vous pouvez ajouter un seul bloc d'adresses IP d'applications ou plusieurs blocs en fonction de votre déploiement. Par exemple, saisissez 100.64.10.0/24 et 100.64.11.0/24. Vous pouvez également **Advertise Application IP blocks to Remote Networks (Publier les blocs d'adresses IP d'application sur les réseaux distants)** pour fournir un accès aux réseaux distants.

- Ajoutez des **ZTNA Connectors Connector IP Blocks (Blocs d'adresses IP de connecteurs ZTNA)** que Prisma Access utilisera en interne pour acheminer le trafic entre les

 ©2025 Palo Alto Networks, Inc.

utilisateurs mobiles, les réseaux distants et les machines virtuelles de connecteur dans vos centres de données.

Vous pouvez ajouter un seul bloc d'adresses IP de connecteur ou plusieurs blocs en fonction de votre déploiement. Par exemple, saisissez 100.65.10.0/24 et 100.65.11.0/24.

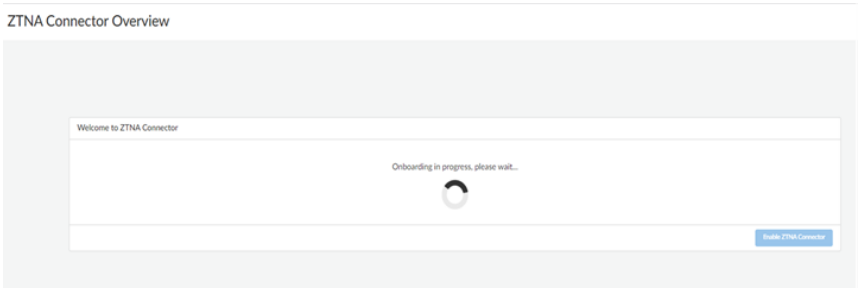


- Cliquez sur **Save (Enregistrer)** pour enregistrer la configuration du bloc d'adresses IP, puis **Commit (Validez)** et transmettez la configuration.

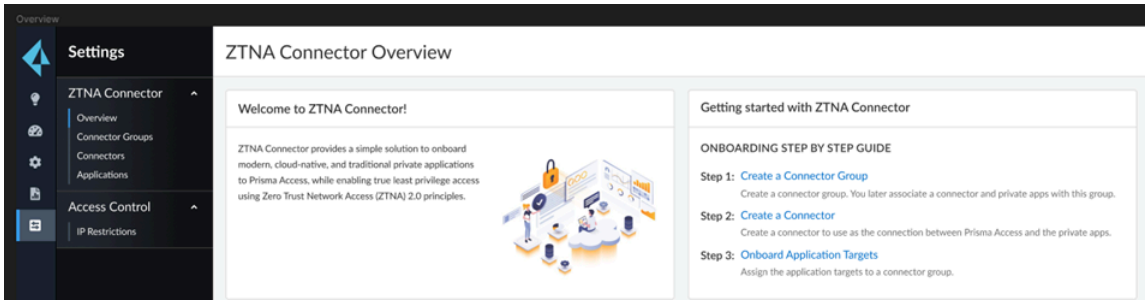
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Lancez le connecteur ZTNA depuis Strata Cloud Manager.

- Sélectionnez **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)**.
- Prisma Access commence à configurer l'infrastructure du connecteur ZTNA. Cela peut prendre quelques minutes.



- Une fois l'intégration terminée, la vue d'ensemble du connecteur ZTNA s'affiche.



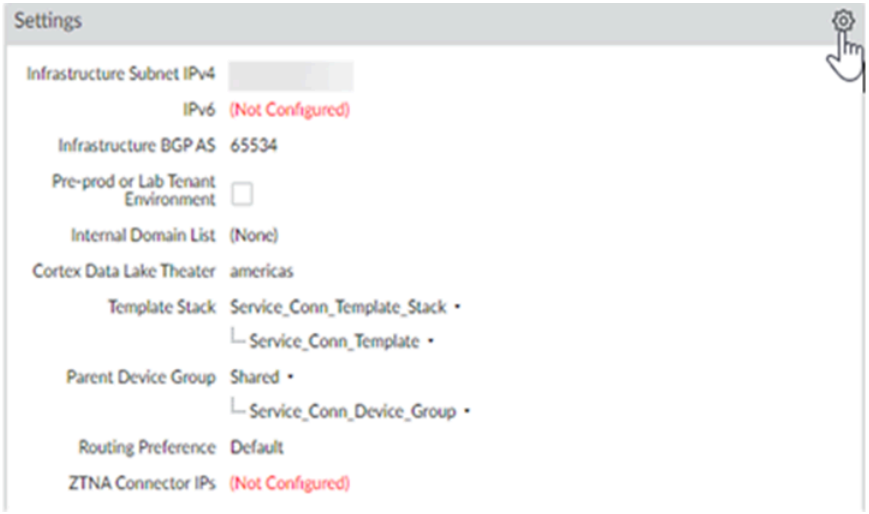
Activer le connecteur ZTNA (Panorama)

Utilisez le flux de travail suivant pour activer le connecteur ZTNA dans Prisma Access (Managed by Panorama).

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Configurez les blocs d'adresses IP que Prisma Access utilisera en interne pour acheminer le trafic vers le connecteur ZTNA et les applications privées que vous intégrez.

- Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** et **Edit (Modifiez)** les **Settings (Paramètres)**.



- Dans l'onglet **ZTNA Connector (Connecteur ZTNA)**, **Add (Ajoutez)** un **Application IP Block (Bloc d'adresses IP d'application)**.

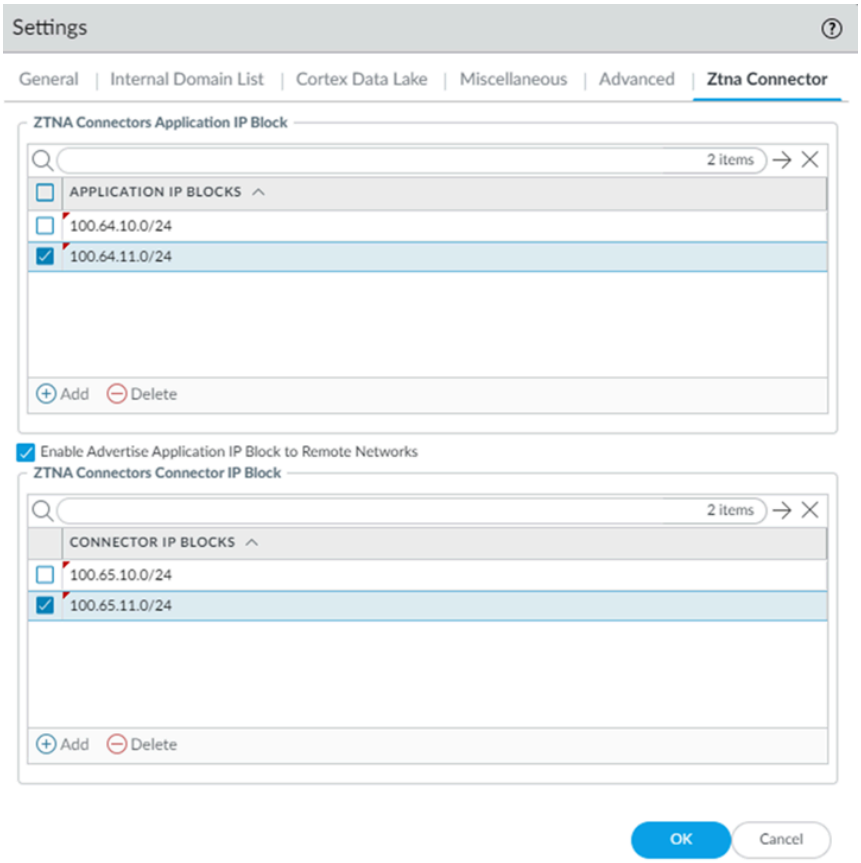
  Vous pouvez ajouter un seul bloc d'adresses IP d'application ou plusieurs blocs en fonction de votre déploiement. Par exemple, saisissiez 100.64.10.0/24 et 100.64.11.0/24. Vous

 ©2025 Palo Alto Networks, Inc.

pouvez également **Enable Advertise Application IP Block to Remote Networks (Activer la publication des blocs d'adresses IP d'application sur les réseaux distants)**.

- Définissez les **Connector IP Blocks (Blocs d'adresses IP du connecteur)** que Prisma Access utilisera en interne pour acheminer le trafic entre les utilisateurs mobiles, les réseaux distants et les machines virtuelles de connecteur dans vos centres de données.

  Vous pouvez ajouter un seul bloc d'adresses IP de connecteur ou plusieurs blocs en fonction de votre déploiement. Par exemple, saisissez 100.65.10.0/24 et 100.65.11.0/24.

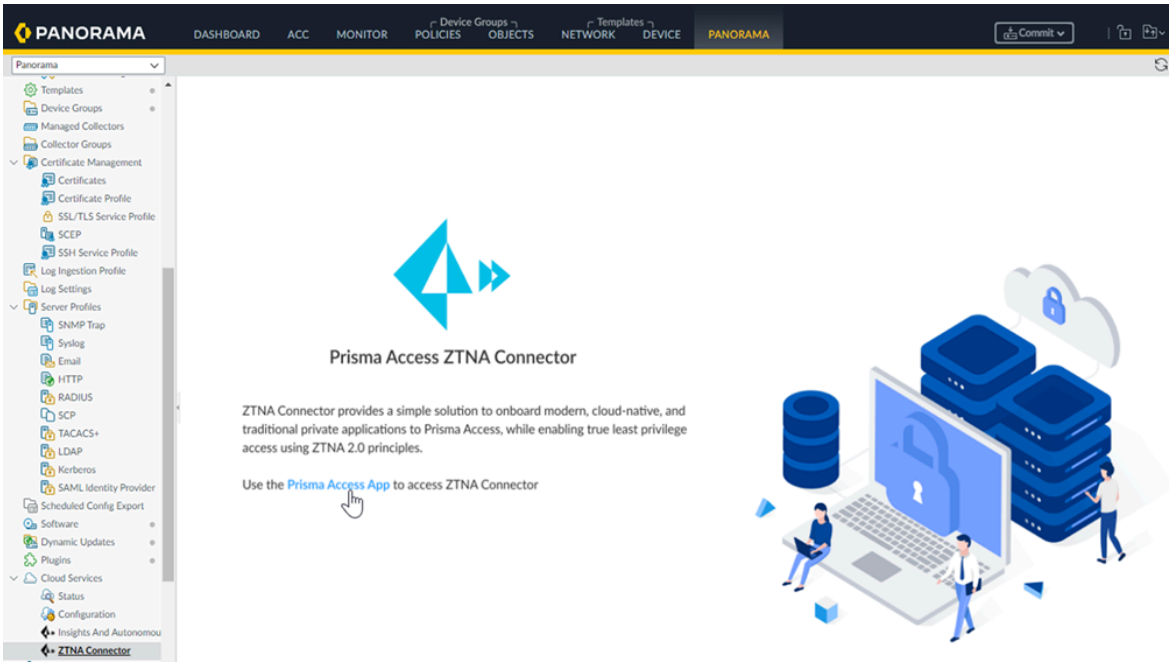


- Cliquez sur **OK** pour enregistrer la configuration du bloc d'adresses IP, puis **Commit (Validez)** et transmettez la configuration.

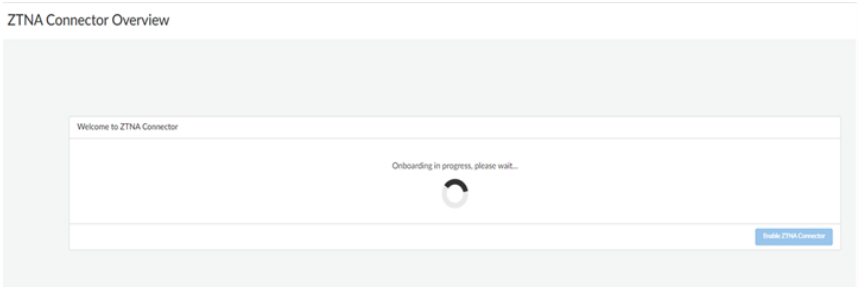
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Lancez le connecteur ZTNA à partir du plug-in Cloud Services sur Panorama.

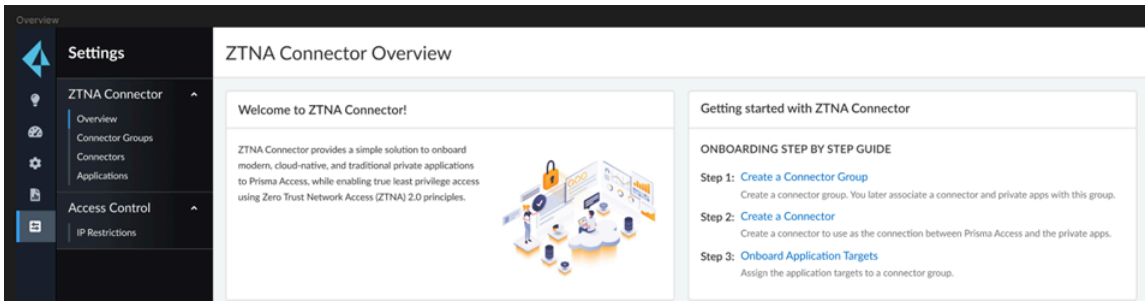
- Sélectionnez **Panorama** > **Cloud Services** > **ZTNA Connector (Connecteur ZTNA)**.
- Cliquez sur Strata Cloud Manager pour lancer le connecteur ZTNA dans Strata Cloud Manager sur la plateforme.



- Depuis Strata Cloud Manager, sélectionnez **Settings (Paramètres)** > **ZTNA Connector (Connecteur ZTNA)**.
- Prisma Access commence à configurer l'infrastructure du connecteur ZTNA. Cela peut prendre quelques minutes.



- Une fois l'intégration terminée, la vue d'ensemble du connecteur ZTNA s'affiche.



 ©2025 Palo Alto Networks, Inc.

Configurer le connecteur ZTNA

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend 200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

Une fois que vous Activer le connecteur ZTNA, vous pouvez commencer à configurer les composants du connecteur ZTNA :

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Identifiez vos blocs d'adresses IP d'application et de connecteur et ajoutez les blocs d'adresses IP dans Prisma Access.

Reportez-vous à la recommandation suivante pour les blocs d'adresses IP :

- *Attribuez une adresse IP distincte à chaque application.*
- *Attribuez à chaque connecteur au moins un bloc d'adresses IP /27 (au moins 32 adresses IP par connecteur).*
- *Attribuez une adresse IP unique à chaque groupe de connecteurs.*

Vous pouvez ajouter davantage de connecteurs ou de blocs d'application selon vos besoins.

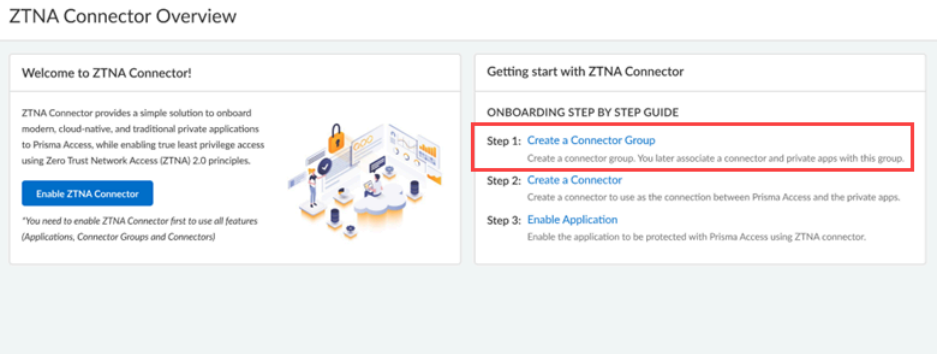
Si vous utilisez des adresses RFC 6598 au sein de votre réseau, vous devez réserver un pool d'adresses IP RFC 6598 distinct pour une utilisation au sein de Prisma Access en interne pour acheminer le trafic vers les connecteurs et les applications privées que vous intégrerez.

STEP 2 | Créez un groupe de connecteurs.

Les groupes de connecteurs sont des regroupements logiques de connecteurs et d'applications. Il existe de nombreuses façons différentes de regrouper des applications et des connecteurs. Vous pouvez regrouper des connecteurs dans différents emplacements géographiques pour plus de redondance. Vous pouvez également créer plusieurs connecteurs dans le même centre de données pour un débit accru. Pour une gestion simplifiée des politiques, il peut être utile de regrouper les applications utilisées par les mêmes groupes d'utilisateurs. Créez d'abord vos groupes de connecteurs, puis ajoutez les connecteurs et les applications aux groupes.

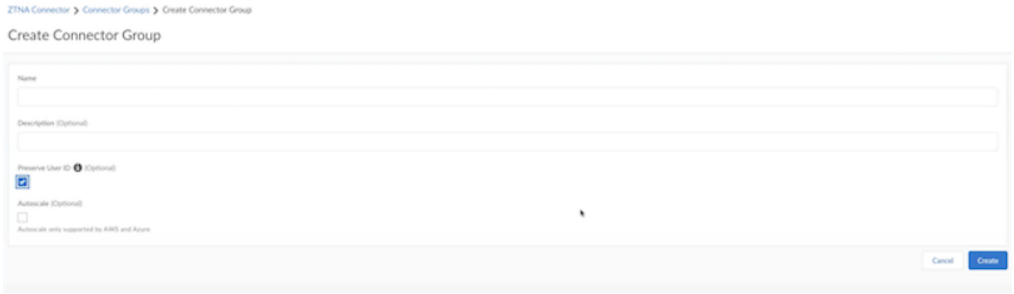
Répétez cette étape autant de fois que nécessaire pour créer tous les groupes de connecteurs dont vous avez besoin pour regrouper vos connecteurs et applications.

1. Sélectionnez**Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)**, sélectionnez **Overview (Aperçu)** ou **Connector Groups (Groupes de connecteurs)**, puis **Create Connector Group (Créer un groupe de connecteurs)**.



 ©2025 Palo Alto Networks, Inc.

2. Donnez un **Name (Nom)** au groupe de connecteurs, activez l'option **Preserve User ID (Préserver User-ID)** et, éventuellement, fournissez-lui une **Description**.



3. (Facultatif) Si votre centre de données se trouve dans Azure ou AWS et que vous souhaitez utiliser la fonctionnalité de mise à l'échelle automatique, sélectionnez **Autoscale (Mise à l'échelle automatique)**. Si vous avez activé cette fonctionnalité, vous n'avez pas besoin de créer de connecteur.
4. Créez un groupe de connecteurs en cliquant sur **Create (Créer)**.

STEP 3 | *Créez un connecteur et ajoutez-le à un groupe de connecteurs uniquement lorsque vous sélectionnez un groupe de connecteurs sans mise à l'échelle automatique.*

Créez des connecteurs et ajoutez-les au groupe de connecteurs.

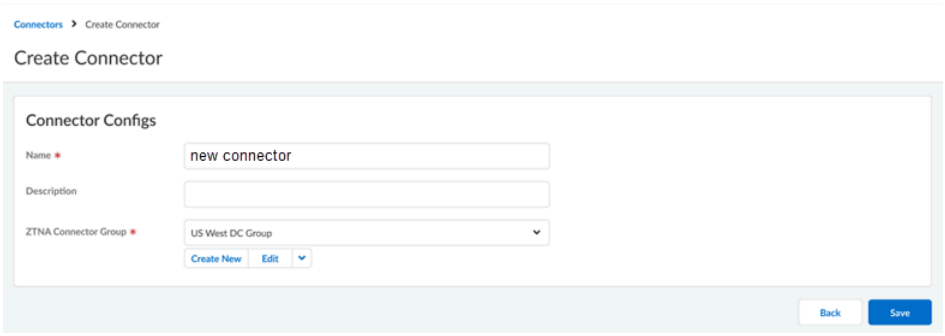
Les connecteurs représentent les VM fonctionnant dans vos centres de données qui se connectent à Prisma Access. Vous devez créer le connecteur dans Prisma Access et utiliser la

 ©2025 Palo Alto Networks, Inc.

phrase secrète/la clé fournie pour intégrer la VM de connecteur correspondante dans votre centre de données.

Répétez cette étape autant de fois que nécessaire pour créer autant de connecteurs que nécessaire pour connecter vos applications de centre de données à Prisma Access.

- Sélectionnez **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)**, sélectionnez **Overview (Aperçu)** ou **Connectors (Connecteurs)**, puis **Create Connector (Créer un connecteur)**.
- Ajoutez un **Name (Nom)** au connecteur.



- (Facultatif) Ajoutez une **Description** au connecteur.
- Sélectionnez le **Connector Group (Groupe de connecteurs)** auquel le connecteur doit être ajouté.

  Pour simplifier le routage et accéder plus rapidement aux serveurs du centre de données, Palo Alto Networks recommande que les connecteurs et les serveurs soient dans le même sous-réseau.
- Créez le connecteur en cliquant sur **Create (Créer)**.

*Pour maintenir les connecteurs ZTNA à jour, vous pouvez mettre à jour leur version logicielle. Les icônes dans les **ZTNA Connector (Connecteur ZTNA)** > **Connector Groups (Groupes de connecteurs)** vous indiquent l'état des connecteurs et si une mise à niveau est disponible.*

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Récupérez la clé et la phrase secrète que vous utiliserez pour configurer le connecteur.

Vous utiliserez les valeurs de la clé et de la phrase secrète lorsque vous configurerez les VM dans une étape ultérieure.

1. Groupe de connecteurs à mise à l'échelle automatique : suivez les étapes ci-dessous :
   1. Accédez à **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connector Groups (Groupes de connecteurs)**.
   2. Sélectionnez **Copy Token (Copier le jeton)** dans la zone **Actions** de votre groupe de connecteurs à mise à l'échelle automatique, puis copiez les valeurs **Key (Clé)** et **Secret (Phrase secrète)**.

      Vous utilisez la clé et la phrase secrète pour associer l'instance cloud ou la VM que vous créez au connecteur.
2. Groupe de connecteurs sans mise à l'échelle automatique : suivez les étapes ci-dessous :
   - Sélectionnez **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)**.
   - Sélectionnez le connecteur que vous souhaitez déployer.
   - Sélectionnez **Copy Token (Copier le jeton)** dans la zone **Actions**, puis copiez les valeurs **Key (Clé)** et **Secret (Phrase secrète)**.

     Vous utilisez la clé et la phrase secrète pour associer l'instance cloud ou la VM que vous créez au connecteur.

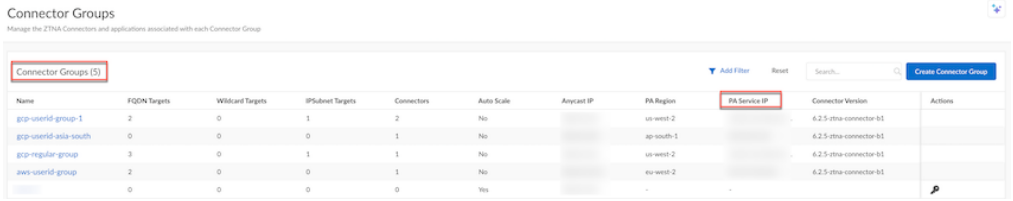


STEP 5 | Déployez vos VM de connecteur ZTNA dans votre centre de données.

STEP 6 | (Facultatif) Sélectionnez **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connector Groups (Groupes de connecteurs)**, notez l'adresse **PA Service IP (IP du service PA)** du groupe de connecteurs et ajoutez cette adresse IP aux listes d'adresses autorisées de votre organisation.

*Vous pouvez voir l'adresse **PA Service IP (IP du service PA)** sous **Connector Groups (Groupes de connecteurs)** uniquement après avoir intégré votre connecteur.*

Si nécessaire, ajoutez cette adresse IP à vos listes d'adresses autorisées afin que votre réseau puisse transmettre et recevoir le trafic du connecteur ZTNA.



 ©2025 Palo Alto Networks, Inc.

STEP 7 | Ajoutez les cibles aux groupes de connecteurs.

Configurez des cibles pour accéder aux applications privées dans les centres de données via vos VM de connecteur ZTNA. Vous pouvez ajouter des cibles basées sur des caractères génériques FQDN, des FQDN ou des sous-réseaux IP. Le connecteur ZTNA effectue le travail de configuration des paramètres réseau et DNS requis pour que vos utilisateurs mobiles et les utilisateurs des succursales puissent accéder aux applications en toute sécurité via Prisma Access.

1. Sélectionnez **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Application Targets (Cibles d'application)**.
2. Sélectionnez le type de cible que vous souhaitez créer.



Grâce à l'amélioration de l'intégration des applications sans validation, l'intégration des applications prend désormais moins d'une minute, permettant un accès rapide aux applications. Cette fonctionnalité vous permet également d'intégrer un plus grand nombre d'applications.

Limitations :

- *Vous ne pouvez pas ajouter le même FQDN dans plusieurs cibles d'application (avec un port/protocole différent).*
- *Lorsque vous ajoutez ou supprimez une cible générique, une validation se produit sur MU ou RN pour ajouter ou supprimer des règles de transfert de proxy DNS. Cependant, la découverte ultérieure d'applications génériques de FQDN correspondants au caractère générique ne nécessite aucune validation supplémentaire, ce qui permet d'intégrer rapidement les applications pour un accès immédiat à celles-ci.*

Pour activer la fonctionnalité d'intégration d'applications sans validation, mettez à jour le plan de données Prisma Access vers la version 11.2.3 et ultérieure.

- **Wildcard Targets (Cibles génériques)** : utilisez un caractère générique (par exemple, *.exemple.com) pour la cible. Lorsque les utilisateurs accèdent à des sites qui correspondent au caractère générique, ces applications sont automatiquement intégrées pour l'accès depuis le connecteur ZTNA pour vos utilisateurs mobiles et vos utilisateurs de réseaux distants. Par exemple, avec un caractère générique *.exemple.com, lorsque les utilisateurs accèdent à l'application sur app1.exemple.com, le connecteur ZTNA crée automatiquement la configuration pour intégrer cette application enfant avec son FQDN, son protocole et son port spécifiques.

  De plus, lorsque les utilisateurs accèdent à une application en fonction d'un caractère générique (par exemple, app1.exemple.com en fonction du caractère générique *.exemple.com), l'application est découverte et automatiquement intégrée en tant que **FQDN Target (Cible FQDN)**.

  1. Accédez aux **Wildcard Targets (Cibles génériques)** et cliquez sur **Create Wildcard Target (Créer une cible générique)**.
  2. Saisissez un **Name (Nom)** unique pour la cible.

 ©2025 Palo Alto Networks, Inc.

3. Saisissez le **Connector Group (Groupe de connecteurs)** à associer à la cible.

   Le groupe doit être de type **FQDN/Wildcard (FQDN/caractère générique)**.

   En commençant par Prisma Access 5.0.1, vous pouvez sélectionner plusieurs groupes de connecteurs pour les cibles génériques et FQDN, jusqu'à un maximum de quatre groupes de connecteurs par cible générique ou FQDN. Suivez les directives lors de la sélection de plusieurs groupes de connecteurs par cible.
4. Saisissez le **Wildcard (Caractère générique)** à utiliser avec la cible.

   Saisissez-le au format .exemple.com ou .mon.exemple.com (l'interface utilisateur ajoute implicitement l'astérisque devant le caractère générique). N'autorisez pas tous les sites en spécifiant un caractère générique *.*, exemple.*.com ou *.com.
5. Sélectionnez le **Protocol (Protocole)** (**TCP**, **UDP** ou les deux).
6. (Facultatif) Pour activer le protocole ICMP d'un utilisateur GlobalProtect vers un centre de données du connecteur ZTNA, sélectionnez **Allow ICMP Protocol (Autoriser le protocole ICMP)**.
7. Sélectionnez le **Port** à utiliser pour l'application.

   Saisissez un port unique, plusieurs ports en utilisant des virgules entre les ports, une plage de ports en utilisant des tirets, ou les deux. N'ajoutez pas d'espaces après les virgules. Sélectionnez **Any (N'importe quel)** port pour faire correspondre tous les ports que vous spécifiez, ou sélectionnez **Match (Faire correspondre)** et entrez le ou les ports à faire correspondre.

   Si vous avez sélectionné **Both (Les deux)** sous **Protocol (Protocole)**, vous devez ajouter des ports au **TCP Port (Port TCP)** et au **UDP Port (Port UDP).**

   Lorsque vous entrez une plage dans le champ **TCP Port (Port TCP)**, sous **Advanced Settings (Paramètres avancés)**, les **Probing Types (Types de sondage) ICMP ping (Ping ICMP)** et **None (Aucun)** sont activés.
8. Entrez le **Probing Type (Type de sondage) TCP ping (Ping TCP)**, **ICMP ping (Ping ICMP)** ou **None (Aucun)** selon le protocole que vous sélectionnez.

   Si vous sélectionnez **TCP ping (Ping TCP)**, sélectionnez un **Probing port (Port de sondage)** et entrez un seul port. Le port ne doit pas nécessairement être compris dans la plage de ports que vous avez saisie dans les zones **Port** et **Protocol (Protocole)**. Le connecteur ZTNA détermine l'accessibilité de l'application en effectuant un ping TCP depuis le port de sondage vers l'adresse IP résolue du FQDN. Si le ping réussit, l'application est considérée **Up (Active)**.

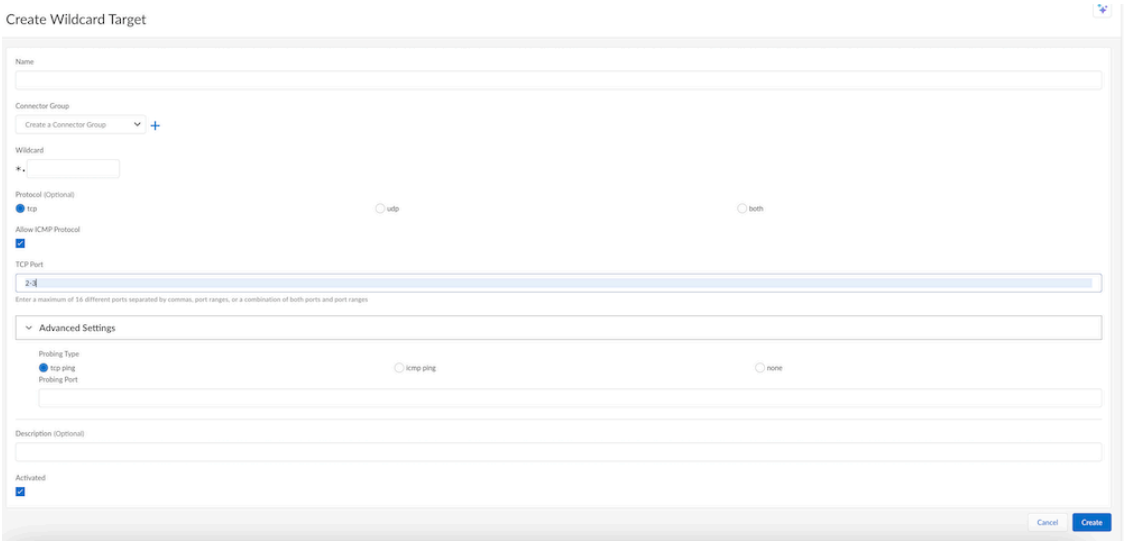
   Vous pouvez également modifier le port de sondage que vous avez ajouté lors de l'intégration de l'application. Lorsque le port de sondage est mis à jour, le connecteur ZTNA démarre l'application de sondage TCP sur le port mis à jour et l'état de l'application est mis à jour en conséquence.

   Si vous sélectionnez **ICMP ping (Ping ICMP)**, le connecteur ZTNA effectue un ping ICMP vers l'adresse IP résolue du FQDN. Si une réponse est reçue au ping ICMP, l'application est considérée **Up (Active)**.

   Si vous sélectionnez **None (aucun)**, aucun sondage n'est effectué et l'application est toujours marquée comme **Up (Active)**.

 ©2025 Palo Alto Networks, Inc.

9. Sélectionnez **Activated (Activé)** et **Create (Créer)** pour créer la cible.



- **Cibles FQDN** : pour créer une cible pour un seul FQDN, créez une cible FQDN.

  En commençant par Prisma Access 5.0, pour les groupes de connecteurs ayant une version de connecteur ZTNA 5.0 ou supérieure, si un FQDN d'application se résout en plusieurs adresses IP privées, le connecteur ZTNA exécute une sonde d'application pour déterminer l'état de toutes les adresses IP résolues et équilibre la charge de l'accès FQDN à plusieurs adresses IP résolues dont l'état de l'application est Up (Active).

  Pour créer une cible FQDN, accédez à **FQDN Targets (Cibles FQDN)** et **Create FQDN Target (Créer une cible FQDN)**. Vous créez une cible FQDN de la même manière que vous créez un caractère générique FQDN, en remplaçant le caractère générique FQDN par un seul FQDN.

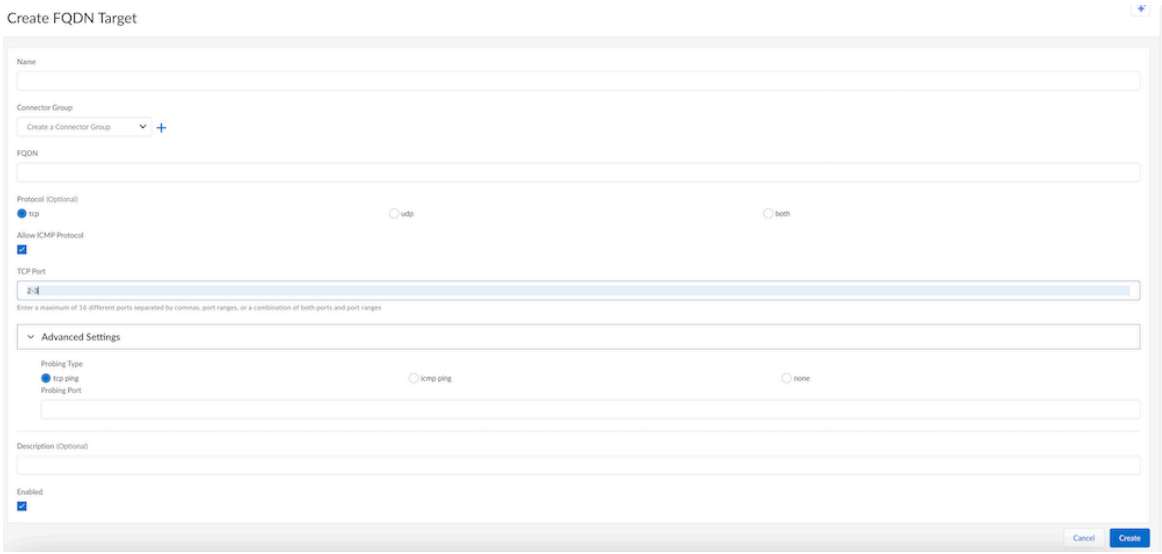
  Commençant par Prisma Access 5.0.1, vous pouvez sélectionner plusieurs groupes de connecteurs par cible FQDN ainsi que des cibles génériques, jusqu'à un maximum de quatre groupes de connecteurs par cible FQDN ou générique. Suivez les directives lors de la configuration de plusieurs groupes de connecteurs par cible.

  Les applications découvertes à la suite d'une cible générique s'affichent également ici. Lorsque les utilisateurs accèdent à des sites qui correspondent au caractère générique, ces applications sont automatiquement intégrées pour l'accès depuis le connecteur ZTNA pour vos utilisateurs mobiles et vos utilisateurs de réseaux distants. Par exemple, avec un caractère générique *.exemple.com, lorsque les utilisateurs accèdent à l'application sur app1.exemple.com, le connecteur ZTNA ajoute automatiquement cette application à la liste des cibles FQDN.

  Une fois qu'une application FQDN est découverte à partir d'une cible générique parent, les modifications apportées à la cible générique ne sont pas mises à jour dans l'application découverte. De plus, le même FQDN découvert n'est pas redécouvert. Si les

 ©2025 Palo Alto Networks, Inc.

caractéristiques de l'application FQDN découverte nécessitent une mise à jour, effectuez une mise à jour manuelle sur l'application découverte en suivant ces étapes.



- **IP Subnet (Sous-réseau IP)** : créez une cible basée sur un sous-réseau IP pour rechercher des applications en fonction des sous-réseaux IP au lieu des FQDN.

  1. Accédez à **IP Subnets (Sous-réseaux IP)** et cliquez sur**Create Subnet Rule (Créer une règle de sous-réseau)** pour créer une règle.
  2. Saisissez un **Name (Nom)** unique pour la règle.
  3. Saisissez le **Connector Group (Groupe de connecteurs)** à associer à la cible.

     Le groupe doit être un type de **IP Subnet (Sous-réseau IP)**.
  4. Spécifiez les **IP Subnets (Sous-réseaux IP)** du centre de données auxquels le connecteur du groupe fournit un accès au routage IP.

     Tous les connecteurs du groupe fournissent un accès de routage aux sous-réseaux IP spécifiés. Vous pouvez sélectionner une seule adresse IP sous la forme 10.1.1.1/32, un seul sous-réseau ou plusieurs sous-réseaux séparés par des virgules. Saisissez un maximum de 16 sous-réseaux.

     Le sous-réseau IP doit être routable dans la structure IP du locataire et les sous-réseaux IP ne peuvent pas chevaucher d'autres sous-réseaux IP du locataire, y compris les éléments suivants :

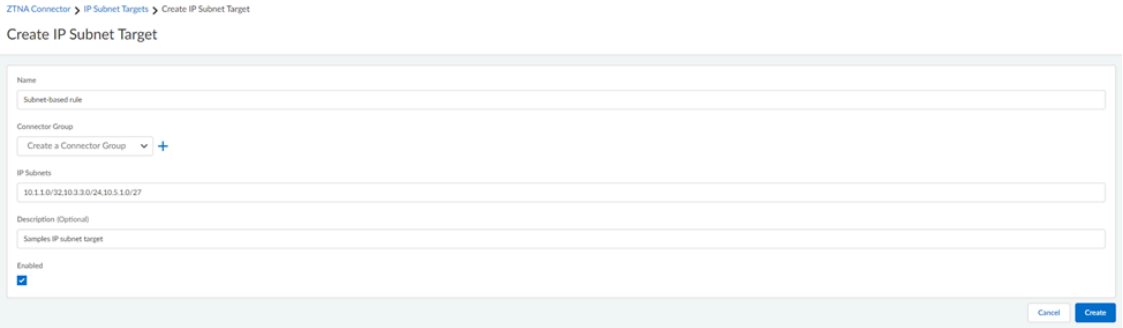
     - Autres sous-réseaux IP routables, y compris les itinéraires statiques configurés par l'utilisateur sur Panorama, les itinéraires publiés depuis la succursale vers le réseau

 ©2025 Palo Alto Networks, Inc.

distant ou les itinéraires publiés depuis le centre de données vers la connexion aux services.

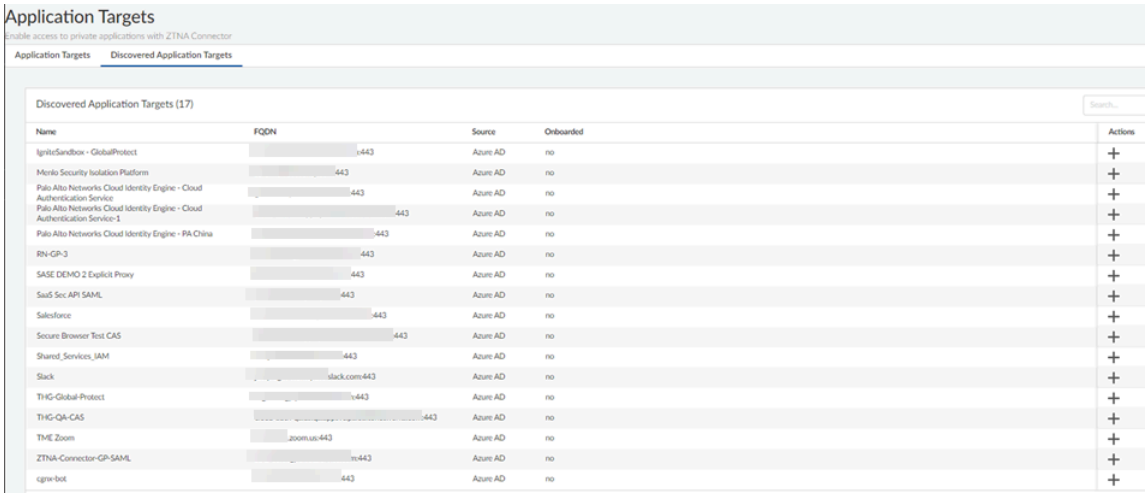
- Sous-réseaux IP de l'application FQDN ZTNA
- Sous-réseaux IP de connecteur ZTNA
- Adresses IP de sous-réseau d'infrastructure
- Utilisateurs mobiles — Pools d'adresses IP GlobalProtect

5. Sélectionnez **Activated (Activé)** et cliquez sur **Create (Créer)** pour créer la cible.



STEP 8 | Ajoutez les applications détectées automatiquement par le connecteur ZTNA au groupe de connecteurs.

1. Configurer la découverte automatique des applications à l'aide de Cloud Identity Engine
2. Sélectionnez **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Application Targets (Cibles d'application)** > **Discovered Application Targets (Cibles d'applications découvertes)**.



3. Cliquez sur + sous **Actions** pour ajouter l'application à un groupe de connecteurs.
4. Donnez à l'application un **Name (Nom)** unique.
5. Sélectionnez le **ZTNA Connector Group (Groupe de connecteurs ZTNA)** à associer à l'application.
6. Entrez le **Probing Type (Type de sondage)** (**TCP ping (Ping TCP)**, **ICMP ping (Ping ICMP)** ou **None (aucun)**).
   - Si vous sélectionnez **TCP Ping (Ping TCP)**, vous sélectionnez également un **Probing Port (Port de sondage)**. Le port ne doit pas nécessairement être compris dans la plage

 ©2025 Palo Alto Networks, Inc.

de ports que vous avez saisie dans les zones **Port** et **Protocol (Protocole)**. Si vous sélectionnez **TCP ping (Ping TCP)** comme type de sondage, Palo Alto Networks vous recommande d'utiliser ce même port pour le **Probing Port (Port de sondage)**.

Le connecteur ZTNA détermine l'accessibilité de l'application en effectuant un ping TCP depuis le port de sondage vers l'adresse IP résolue du FQDN. Si le ping réussit, l'application est considérée **Up (Active)**.

- Vous pouvez également modifier le port de sondage que vous avez ajouté lors de l'intégration de l'application. Lorsque le port de sondage est mis à jour, le connecteur ZTNA démarre l'application de sondage TCP sur le port mis à jour et l'état de l'application est mis à jour en conséquence.
- Si vous sélectionnez **ICMP ping (Ping ICMP)**, le connecteur ZTNA effectue un ping ICMP sur le FQDN. Si une réponse est reçue au ping ICMP, le connecteur ZTNA définit l'état de l'application sur **Up (Active)**.
- Si vous sélectionnez **None (Aucun)**, aucun sondage n'est effectué et l'application est toujours marquée comme **Up (Active)**.

7. Sélectionnez **Enabled (Activé)**.
8. Cliquez sur **Create (Créer)** pour créer une cible d'application.

STEP 9 | Créez des règles de politique de sécurité pour permettre aux utilisateurs d'accéder aux applications dans les connecteurs.

STEP 10 | (Facultatif) Affichez et surveillez les connecteurs ZTNA pour voir les performances de vos connecteurs ZTNA et de vos groupes de connecteurs.

STEP 11 | (Facultatif) Si vous rencontrez des problèmes d'accès aux applications privées à l'aide du connecteur ZTNA, utilisez les outils de diagnostic ping, traceroute et nslookup pour vérifier l'accessibilité des applications.

Mettre à niveau les connecteurs ZTNA

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend

 ©2025 Palo Alto Networks, Inc.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
	200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

Pour maintenir les connecteurs ZTNA à jour, vous pouvez mettre à jour leur version logicielle. Vous devrez peut-être également mettre à niveau vos connecteurs pour prendre en charge une nouvelle fonctionnalité.

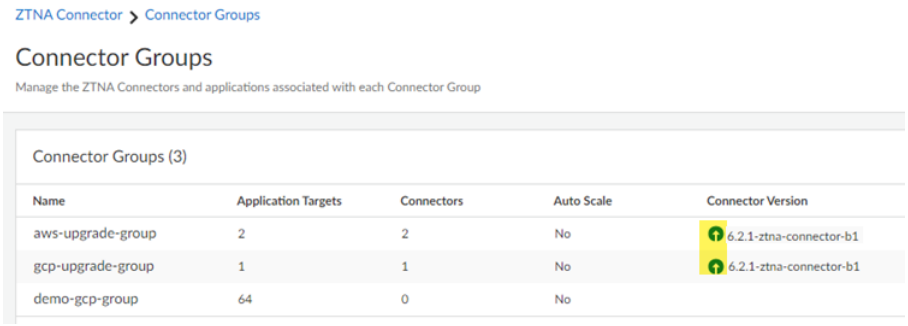
Lorsqu'une nouvelle version du connecteur ZTNA est publiée, les connecteurs de votre déploiement sont vérifiés et, si la version publiée est plus récente que la version existante ou si tous les connecteurs du groupe ne sont pas sur la même version, les icônes de la zone Groupe de connecteurs indiquent qu'une mise à jour est disponible. Si vous choisissez de mettre à jour les connecteurs, vous avez la possibilité de mettre à niveau l'ensemble du groupe. La mise à niveau d'un groupe met automatiquement à niveau tous les connecteurs de ce groupe en parallèle. Vous ne pouvez pas mettre à niveau des connecteurs individuels.

La mise à niveau d'un connecteur ZTNA prend environ 8 à 10 minutes et le connecteur est redémarré au cours de ce processus. Palo Alto Networks vous recommande de planifier une mise à niveau du connecteur pendant une période d'arrêt ou une panne de réseau planifiée.

STEP 1 | Accédez à **ZTNA Connector (Connecteur ZTNA)** > **Connector Groups (Groupes de connecteurs)**. Les flèches vertes indiquent qu'une mise à niveau est disponible.

Vous pouvez uniquement effectuer une mise à niveau vers la dernière version d'image disponible pour le locataire.

STEP 2 | Cliquez sur la flèche verte en regard du groupe de connecteurs.

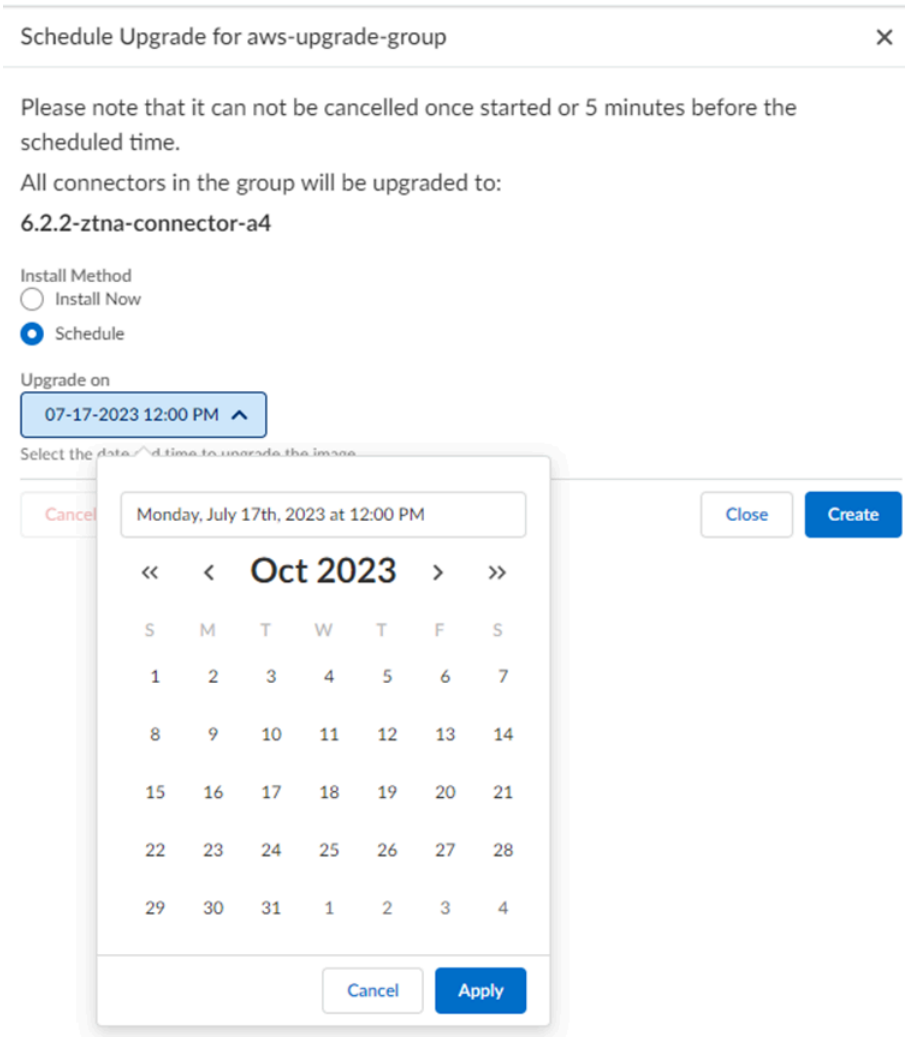


STEP 3 | Sélectionnez **Install Now (Installer maintenant)** pour mettre à niveau le groupe de connecteurs maintenant, ou **Schedule (Planifier)** et indiquez l'heure et la date de la mise à

 ©2025 Palo Alto Networks, Inc.

niveau. L'heure affichée est le fuseau horaire local de l'administrateur utilisant l'interface utilisateur ZTNA.

Vous pouvez **Cancel Scheduled Upgrade (Annuler la mise à niveau planifiée)** jusqu'à cinq minutes avant qu'elle ne commence.



STEP 4 | Vérifiez l'état des connecteurs en affichant l'icône sous **Connector Version (Version du connecteur)**.

Icône	Description
	Une mise à niveau est disponible.
	La mise à niveau est planifiée.

 ©2025 Palo Alto Networks, Inc.

Icône	Description
	La mise à niveau a commencé et est en cours.
Pas d'icône (seule la version du connecteur est affichée) 6.1.1-ztna-connector-a8	La mise à niveau a réussi.
	Tous les connecteurs n'ont pas été mis à niveau.
	La mise à niveau a échoué.

Outils de diagnostic de connecteur ZTNA

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend 200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

 ©2025 Palo Alto Networks, Inc.

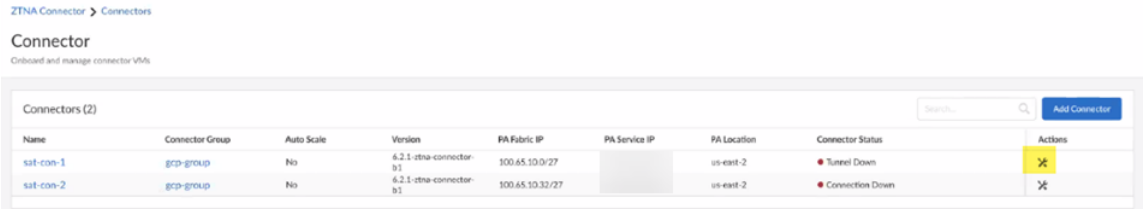
Si vous rencontrez des problèmes avec l'accès aux applications privées à l'aide du connecteur ZTNA, vous pouvez exécuter des tests à partir de l'interface utilisateur du connecteur ZTNA pour vous aider à trouver le problème, à l'aide des outils réseau suivants :

- ping
- TCP Ping
- traceroute
- nslookup
- Vue d'ensemble du vidage
- Vous pouvez également faire des captures de paquets pour aider à déterminer la cause de tout problème avec le connecteur ZTNA.

Assurez-vous que ICMP est autorisé dans votre réseau avant d'utiliser les outils ping et traceroute. ICMP est désactivé dans certains environnements cloud pour des raisons de sécurité et ces outils n'affichent aucune activité.

STEP 1 | Accédez à **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)**.

STEP 2 | Sélectionnez **Actions** > **Diagnostics** pour le connecteur.



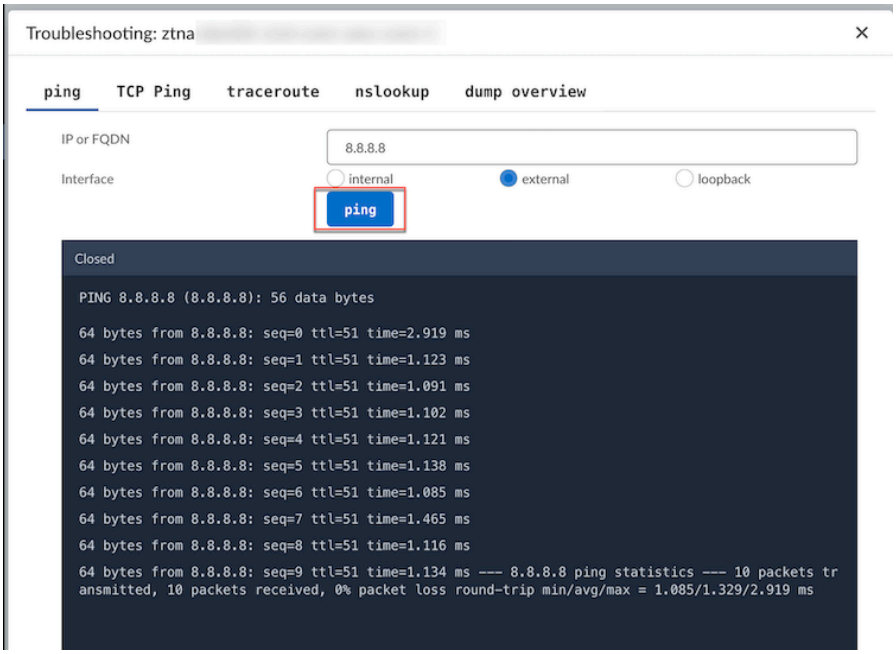
 ©2025 Palo Alto Networks, Inc.

STEP 3 | Exécutez les outils de diagnostic ping, TCP Ping, traceroute ou nslookup.

- **ping** :
  1. Sélectionnez l'**IP or FQDN (IP ou FQDN)** de l'application que vous essayez d'atteindre.
  2. Sélectionnez l'**interface** à partir de laquelle vous testez le ping.

     Si vous avez configuré votre VM avec un déploiement à deux bras, sélectionnez **internal (interne)** pour vérifier le côté LAN (port 2) de la VM et sélectionnez **external (externe)** pour vérifier le côté WAN (port 1).

     Pour un déploiement à un bras, choisissez **internal (interne)** ou **external (externe)**, comme carte latérale WAN et LAN vers le port 1.
  3. Sélectionnez **ping**.



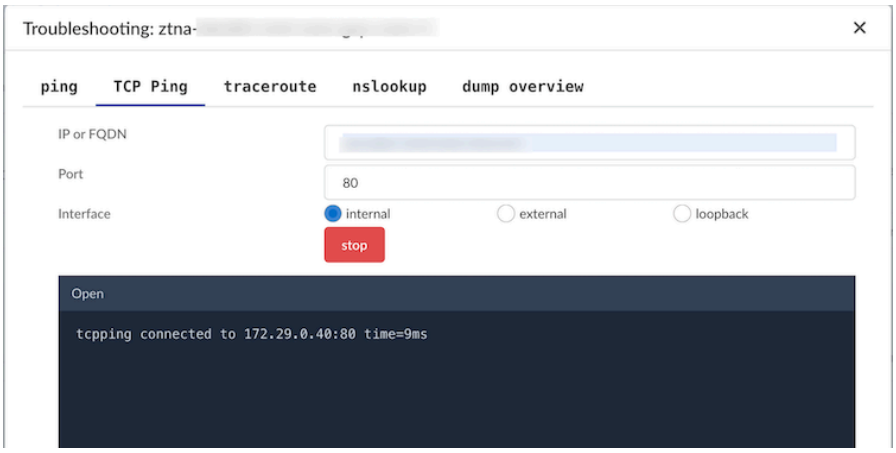
     La sortie ping s'affiche.
  4. Pour finir le test, **Stop (Arrêter)**.
- **TCP Ping (Ping TCP)** :

  *mettez à niveau le connecteur vers la version 6.2.5-b1 du connecteur ZTNA. Si le connecteur n'est pas à jour avec cette version, l'interface utilisateur Strata Cloud Manager ne proposera pas **TCP Ping (Ping TCP)** comme outil de diagnostic.*

  1. Sélectionnez l'**IP or FQDN (IP ou FQDN)** de l'application que vous essayez d'atteindre.
  2. Sélectionnez l'**interface** à partir de laquelle vous testez le ping.

     Si vous avez configuré votre VM avec un déploiement à deux bras, sélectionnez **internal (interne)** pour vérifier le côté LAN (port 2) de la VM et sélectionnez **external (externe)** pour vérifier le côté WAN (port 1).
  3. Sélectionnez **TCP Ping (Ping TCP)**.

 ©2025 Palo Alto Networks, Inc.

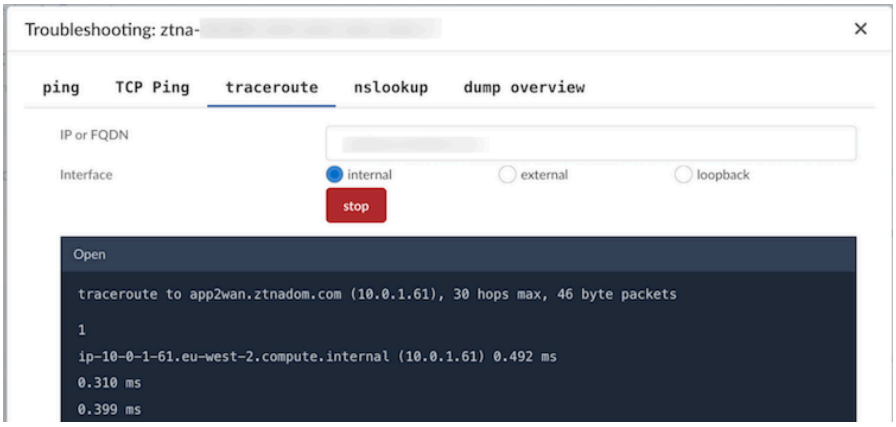


4. Pour finir le test, **Stop (Arrêter)**.

- **traceroute**:

1. Sélectionnez l'**IP or FQDN (IP ou FQDN)** de l'application que vous essayez d'atteindre.
2. Sélectionnez l'**interface** à partir de laquelle vous testez le ping.

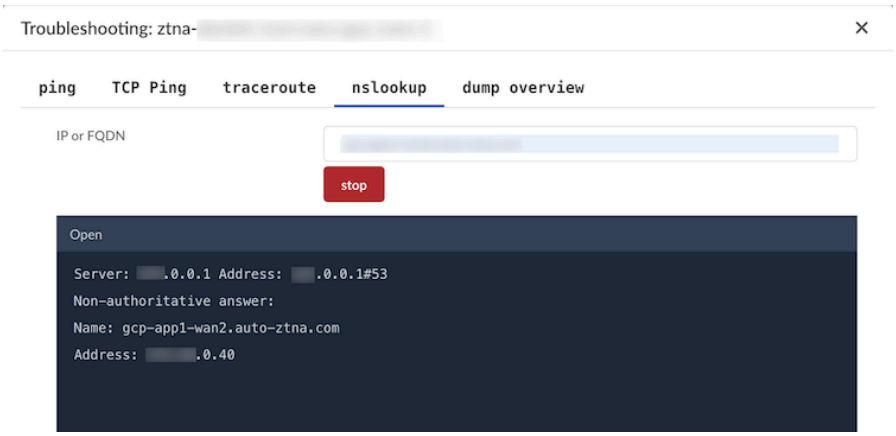
   Si vous avez configuré votre VM avec un déploiement à deux bras, sélectionnez **internal (interne)** pour vérifier le côté LAN (port 2) de la VM et sélectionnez **external (externe)** pour vérifier le côté WAN (port 1).
3. Sélectionnez **traceroute**.
4. Pour terminer le test, **Stop (Arrêter).**



- **nslookup** :

1. Sélectionnez l'**IP or FQDN (IP ou FQDN)** de l'application que vous essayez d'atteindre.
2. Sélectionnez **nslookup**.
3. Pour terminer le test, **Stop (Arrêter).**

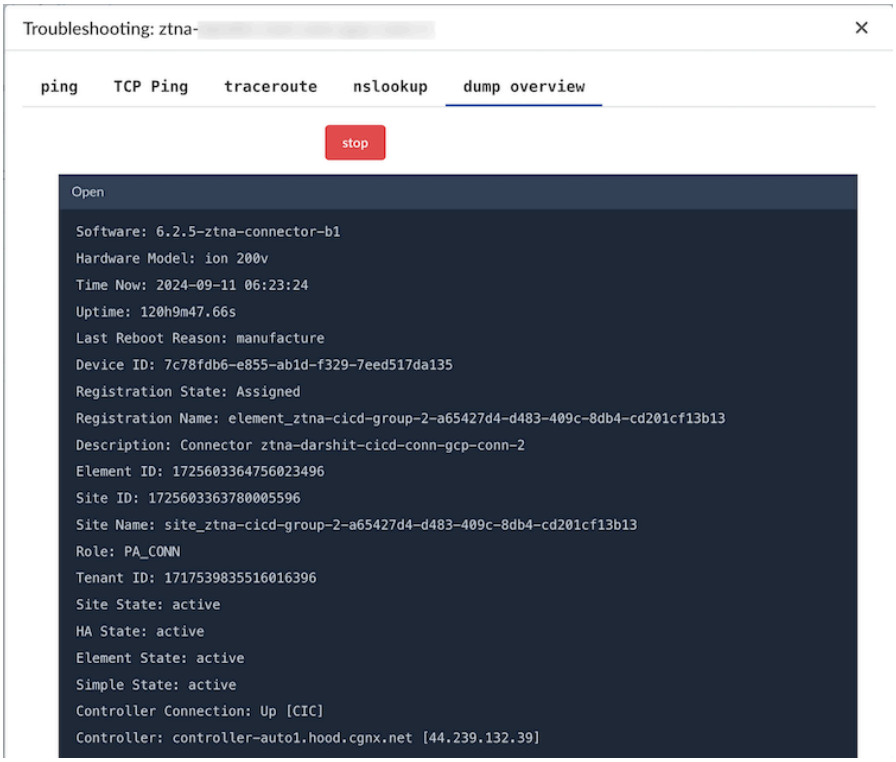
 ©2025 Palo Alto Networks, Inc.



- **Dump overview (Vue d'ensemble du vidage)** :

  1. Cliquez sur **Start (Démarrer)** pour télécharger un vidage système et cliquez sur **Stop (Arrêter)** pour l'arrêter.

     La vue d'ensemble du vidage fournit la version du logiciel, l'interface et l'état de la connexion, ainsi que les informations d'identification du connecteur requises pour la résolution des problèmes PANW.



Captures de paquets

Si vous avez besoin de captures de paquets pour la résolution des problèmes au niveau réseau, vous pouvez effectuer des captures de paquets qui capturent des données réseau à partir de connecteurs spécifiques. Vous pouvez également capturer des paquets basés sur des adresses IP ou des protocoles spécifiques (par exemple, TCP).

Prendre des captures de paquets est utile dans les cas d'utilisation suivants :

 ©2025 Palo Alto Networks, Inc.

- Si votre tunnel n'apparaît pas. Capturer la négociation IKE entre le connecteur et ZTT aiderait à déterminer le problème. Dans ce cas, sélectionnez l'interface **Internet** et utilisez l'adresse IP de la connexion aux services comme interface source ou de destination.
- Si votre application devient inactive, vous pouvez vérifier le sondage des applications en obtenant un tcpdump en utilisant l'adresse IP et le port du serveur, ainsi que le port sur l'interface du centre de données.
- Si le plan de données de bout en bout ne fonctionne pas, mais que le tunnel est actif et que l'application est active. Dans ce cas d'utilisation, obtenir un tcpdump du trafic utilisateur sur le tunnel IPSec destiné à l'adresse IP d'infrastructure de l'application serait bénéfique.

STEP 1 | Accédez à **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)**.

STEP 2 | Sélectionnez la **packet capture (Capture de paquet)** (la loupe) pour le connecteur dont vous souhaitez résoudre les problèmes.



STEP 3 | Sélectionnez l'interface où les paquets seront capturés (**internal (interne)**, **external (externe)** ou **tunnel**).

STEP 4 | (Facultatif) Spécifiez l'adresse **Source or Destination IPv4 (Source ou Destination IPv4)** à partir de laquelle les paquets sont capturés.

Si vous spécifiez cette option, seuls les paquets de cette adresse IP sont capturés.

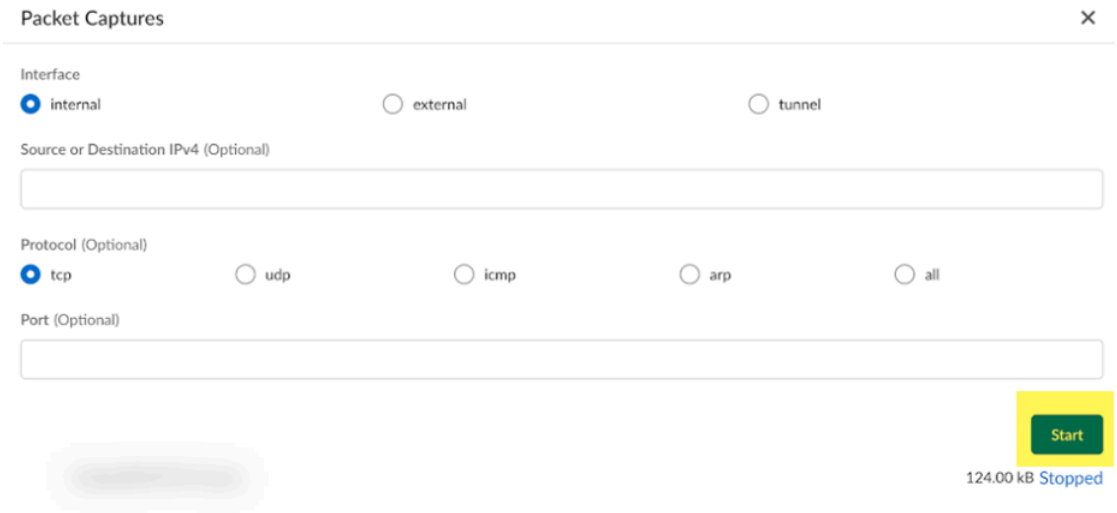
STEP 5 | (Facultatif) Sélectionnez le type de paquets à capturer.

Vous pouvez sélectionner les paquets d'un protocole spécifique à capturer (**tcp**, **udp**, **icmp** ou **arp**), ou **all (tout)** sélectionner pour capturer tous les paquets.

STEP 6 | (Facultatif) Sélectionnez un **Port** à partir duquel les paquets seront capturés.

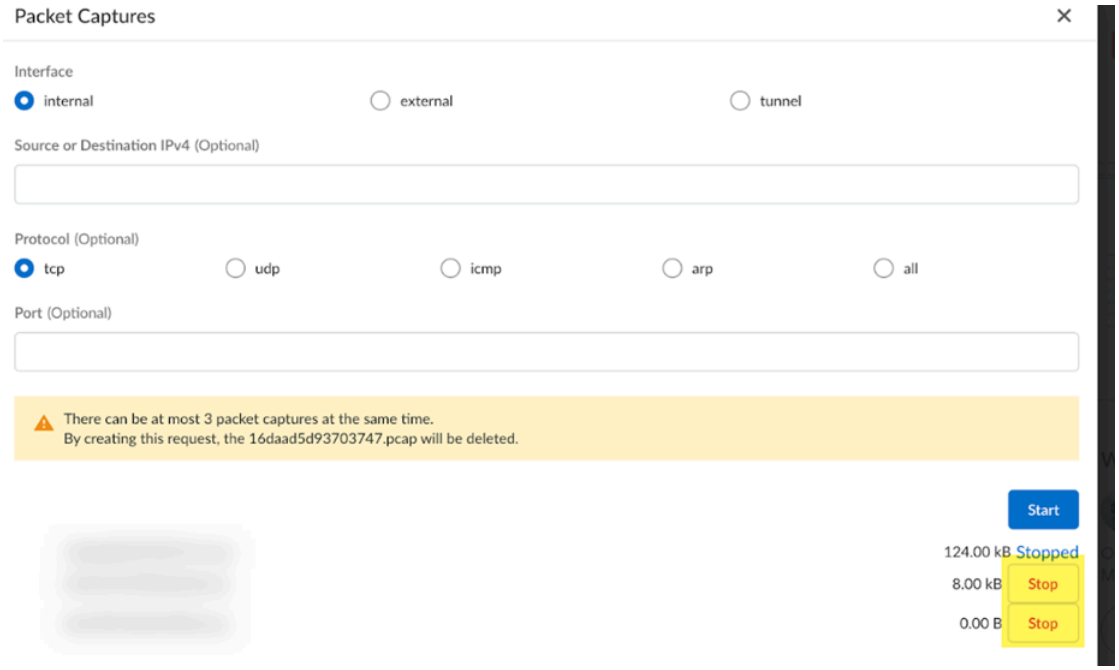
Si vous spécifiez cette option, seuls les paquets de ce port sont capturés.

STEP 7 | **Start (Commencez)** les captures de paquets.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | Pour arrêter les captures de paquets, cliquez sur**Stop (Arrêter)**.



- La taille maximale des fichiers pour les captures de paquets est de 5 Mo. Si vous n'arrêtez pas les captures avant que la taille maximale ne soit atteinte, le fichier est écrasé.
- Un maximum de trois captures de paquets est autorisé sur un connecteur en même temps. Si une quatrième session est initiée, la première session en cours d'exécution est terminée.

Collecter des fichiers de support technique

Le fichier de support technique contient la configuration de votre périphérique, des informations système et quelques journaux (pas le trafic). Palo Alto Networks peut vous demander de télécharger un fichier de support technique pour vous aider à résoudre les problèmes avec le connecteur ZTNA.

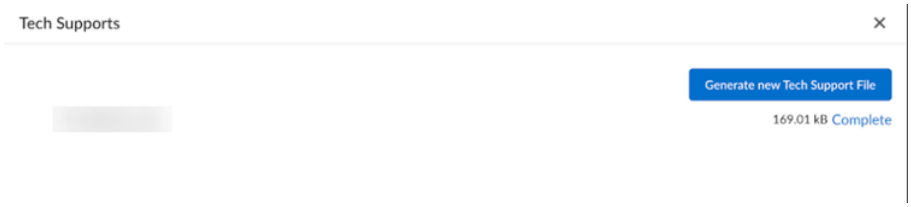
STEP 1 | Accédez à **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)**.

STEP 2 | Sélectionnez le **tech support (support technique)** (la main) pour le connecteur dont vous souhaitez résoudre les problèmes.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | **Generate new Tech Support File (Générer un nouveau fichier de support technique).**



STEP 4 | Sélectionnez **Complete (Terminer)** pour télécharger le fichier de support technique localement.

 ©2025 Palo Alto Networks, Inc.

Supprimer des blocs IP de connecteur

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend 200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

Vous Activer le connecteur ZTNA et ajoutez les blocs IP de connecteur requis que Prisma Access utilisera en interne pour acheminer le trafic entre les utilisateurs mobiles, les réseaux distants et les machines virtuelles de connecteurs de vos centres de données. Avant, vous n'étiez pas en mesure d'apporter des modifications aux blocs IP de connecteur après sa création. Cependant, vous pouvez maintenant supprimer ou mettre à jour les **Connector IP Blocks (Blocs IP de connecteur)**. Suivez la procédure mentionnée pour supprimer ou mettre à jour les blocs.

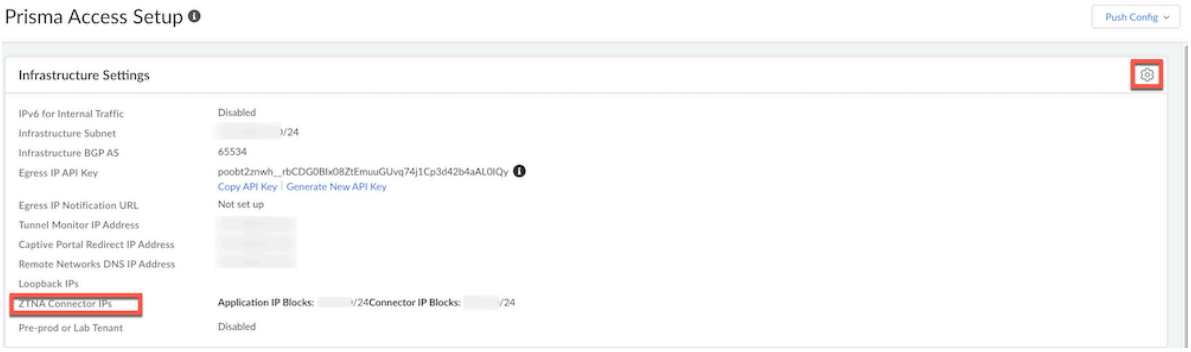
- Panorama
- Strata Cloud Manager

Supprimer les blocs IP de connecteur (Cloud Managed)

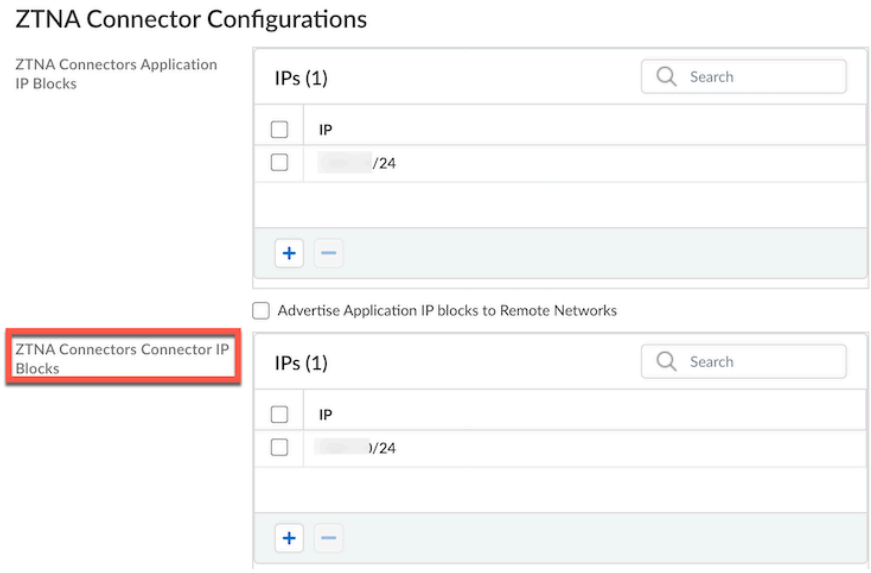
Terminez la procédure suivante pour supprimer les blocs IP de connecteur.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Paramètres d'infrastructure)** et cliquez sur l'engrenage pour modifier les **Settings (Paramètres)**.



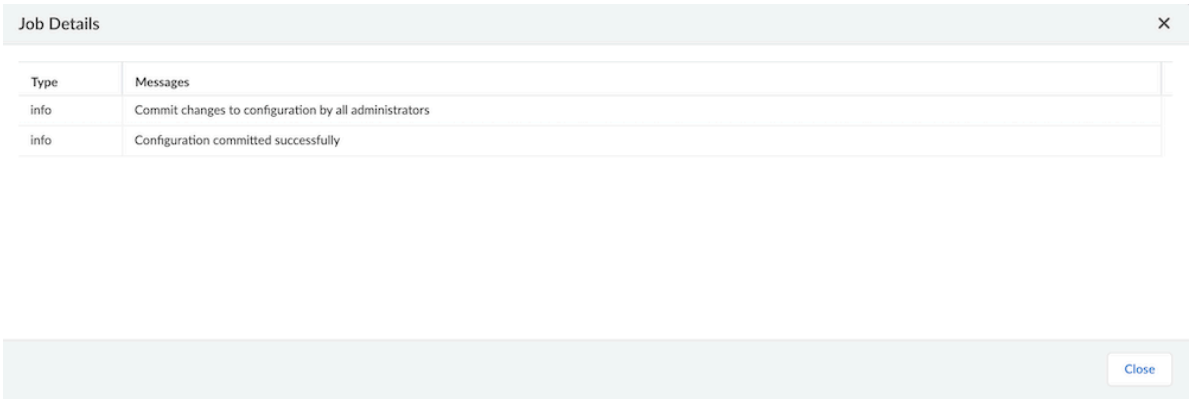
STEP 2 | Dans **ZTNA Connector Configurations (Configurations de connecteur ZTNA)** > **ZTNA Connectors Connector IP Blocks (Blocs IP de connecteurs ZTNA)**, cochez la case située en regard du bloc de connecteur à supprimer et cliquez sur **Save (Enregistrer)**.



 ©2025 Palo Alto Networks, Inc.

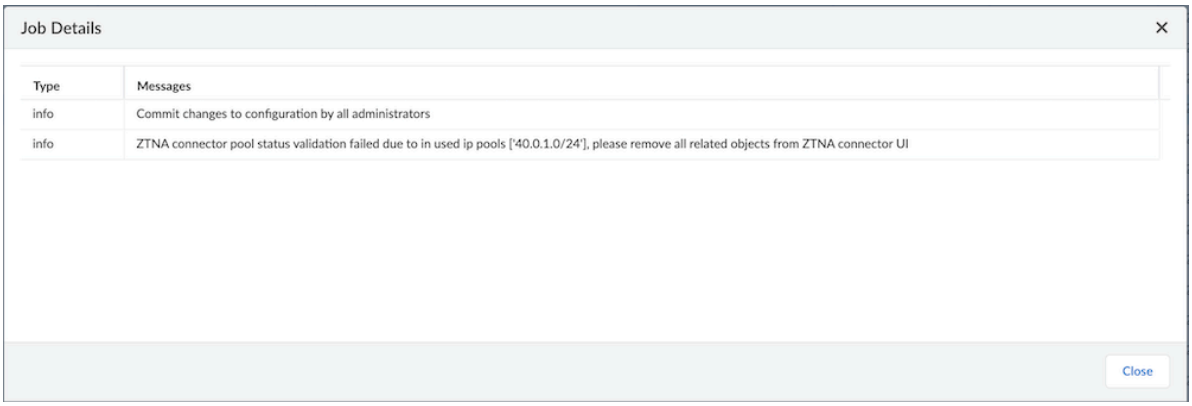
STEP 3 | Cliquez sur **Commit (Valider)** et appliquez les modifications de configuration.

Un message apparaît après la validation.



Si vous avez créé des objets de connecteur ZTNA tels que des connecteurs, des applications, des caractères génériques et des groupes de connecteurs et que vous tentez de supprimer le **Connector IP Block (Bloc IP de connecteur)** sans supprimer au préalable les objets de connecteur ZTNA, la validation et l'application échouent.

Dans ce cas, supprimez les objets de connecteur ZTNA, supprimez le **Connector IP Block (Bloc IP de connecteur)** requis, puis cliquez sur **Commit (Valider)**. La première validation échoue, mais la seconde réussit.

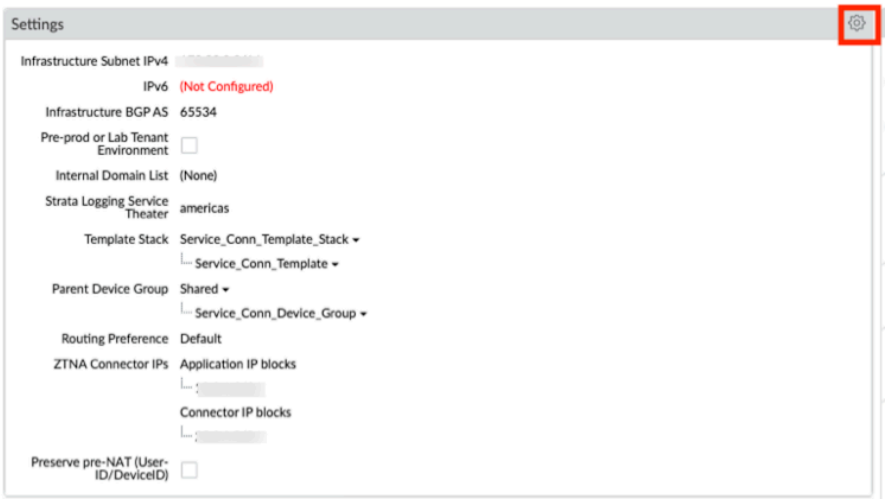


Supprimer des blocs IP de connecteur (Panorama)

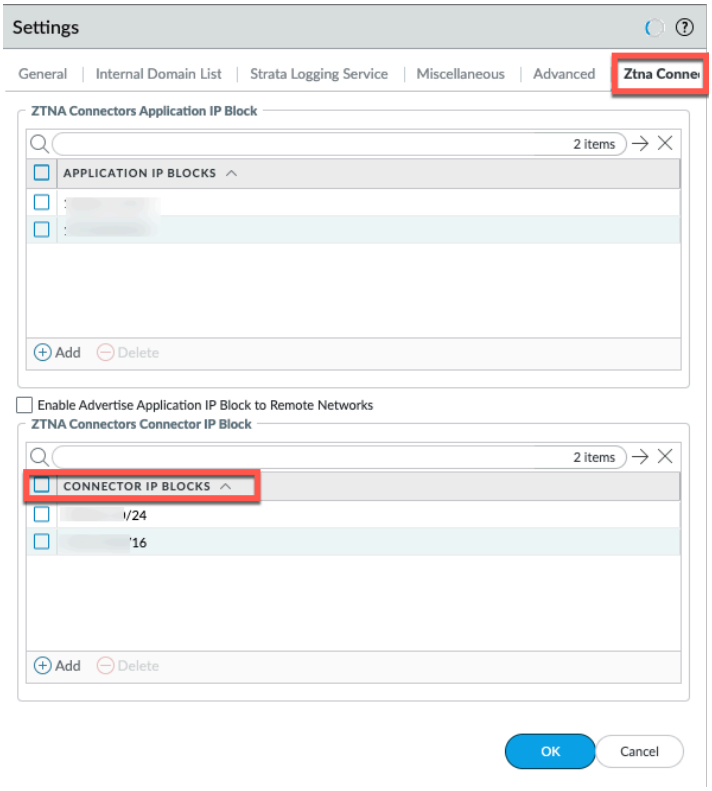
Terminez la procédure suivante pour supprimer les blocs IP de connecteur.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** et cliquez sur l'engrenage pour modifier les **Settings (Paramètres)**.



STEP 2 | Sélectionnez **Ztna Connector (Connecteur ZTNA)**.

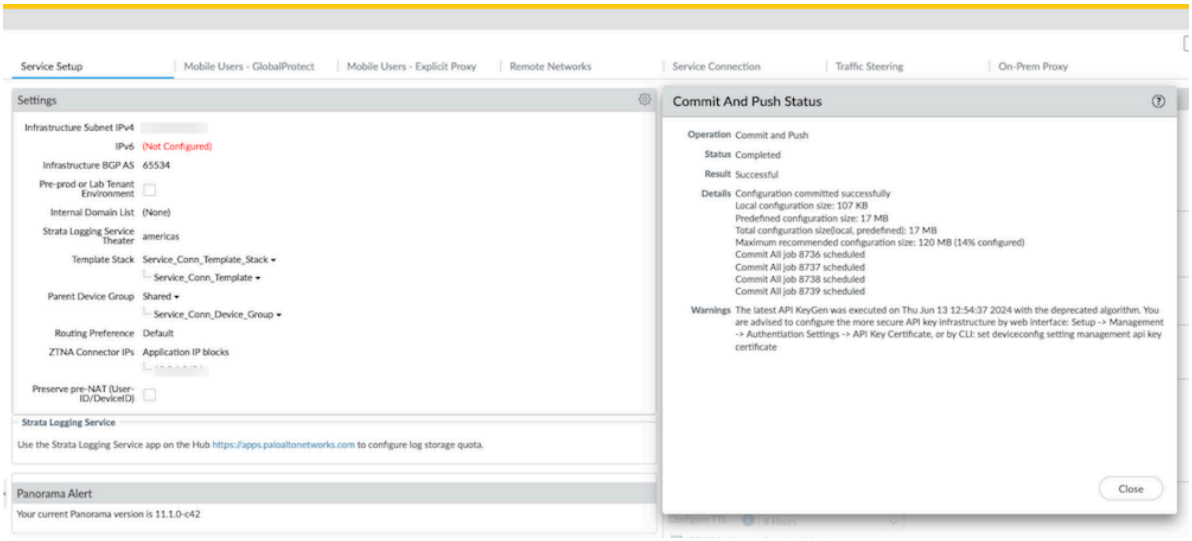


STEP 3 | Cochez la case en regard du bloc de connecteur que vous souhaitez supprimer et cliquez sur **OK** pour enregistrer la configuration.

 ©2025 Palo Alto Networks, Inc.

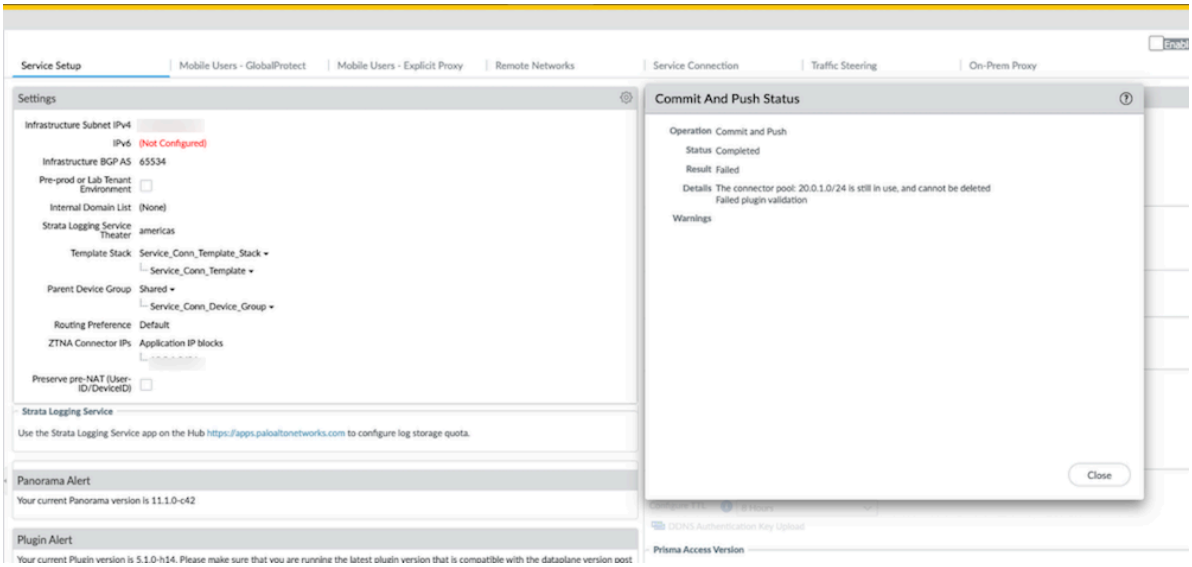
STEP 4 | Sélectionnez **Commit (Valider)** et appliquez les modifications de configuration.

Un message apparaît après la validation.



Si vous avez déjà créé des objets de connecteur ZTNA tels que des connecteurs, des applications, des caractères génériques et des groupes de connecteurs et que vous tentez de supprimer le **Connector IP Block (Bloc IP de connecteur)** sans supprimer les objets de connecteur ZTNA, la validation et l'application échouent.

Dans ce cas, supprimez les objets de connecteur ZTNA, supprimez le **Connector IP Block (Bloc IP de connecteur)** requis, puis cliquez sur **Commit (Valider)** et sur Push (Appliquer) deux fois. La première validation échoue, mais la seconde réussit.



 ©2025 Palo Alto Networks, Inc.

Configurer la découverte automatique des applications à l'aide de Cloud Identity Engine

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend 200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

Pour que le connecteur ZTNA puisse découvrir automatiquement les applications définies dans Azure Active Directory ou Okta Directory, vous devez configurer les éléments suivants :

❑ Activez Cloud Identity Engine dans le hub et créez votre premier locataire.

Vous devez sélectionner **Collect enterprise applications (Collecter les applications d'entreprise)** lorsque vous configurez votre répertoire basé sur le cloud dans Azure ou Okta.

❑ Sélectionnez le type de répertoire auquel vous souhaitez que Cloud Identity Engine accède.

❑ Configurez un répertoire basé sur le cloud, tel que Azure Active Directory (Azure AD) ou Okta Directory pour communiquer avec Cloud Identity Engine.

Les IdP suivants sont pris en charge pour une utilisation avec la découverte d'application :

- Azure AD
- Okta

 ©2025 Palo Alto Networks, Inc.

Découverte de cibles d'applications privées

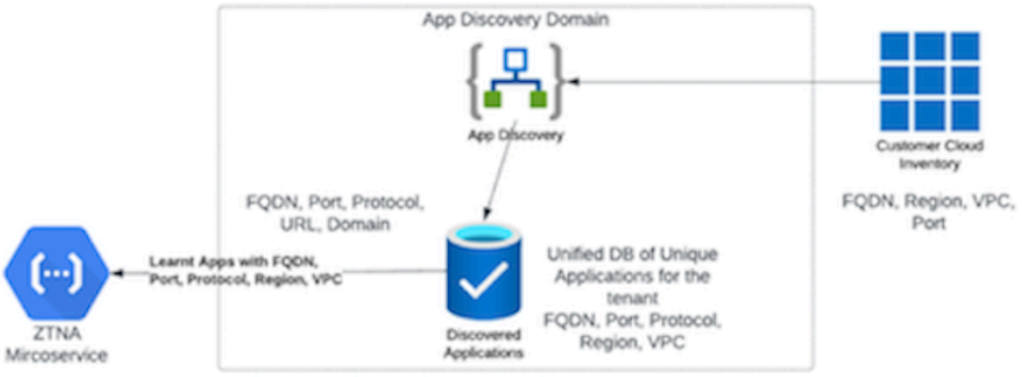
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend 200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

Dans une infrastructure réseau moderne, des milliers d'applications privées sont déployées sur site et dans des centres de données multicloud. Les équipes réseau ne sont pas au courant des applications exécutées dans leur réseau ou dans un sous-réseau particulier du réseau, ce qui entraîne un manque de visibilité des applications.

Pour fournir un accès sécurisé aux applications, vous devez entrer manuellement le FQDN, le port, l'application et être conscient de la dépendance de cette application vis-à-vis des autres applications.

La découverte de cibles d'applications privées permet de découvrir les applications hébergées dans l'environnement cloud et permet d'intégrer ces applications sur la solution de connecteur ZTNA. Le connecteur se connecte également au réseau du fournisseur de cloud, fait la découverte et la stocke dans la base de données. Il fournit également des API aux différents services pour obtenir les applications découvertes. Si l'utilisateur n'a qu'une connexion aux services au lieu d'un connecteur ZTNA, seules les cibles d'application sont découvertes.

 ©2025 Palo Alto Networks, Inc.



La découverte de cibles d'applications privées identifie :

- FQDN
- Port de l'application
- Protocole de l'application

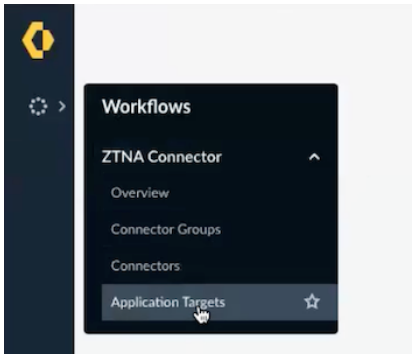
Assurez-vous d'activer le Cloud Identity Engine (CIE) avant d'activer la fonctionnalité de découverte d'applications privées.

Suivez les étapes suivantes pour ajouter un compte cloud, un rôle IAM dans AWS et découvrir les applications cibles.

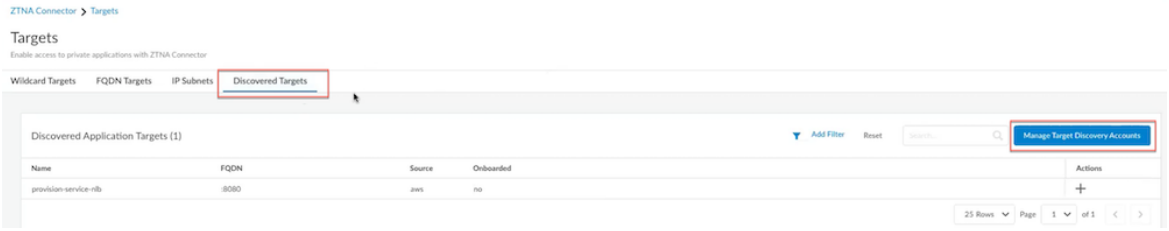
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Obtenez le modèle CloudFormation (CFT) pour ajouter un compte cloud.

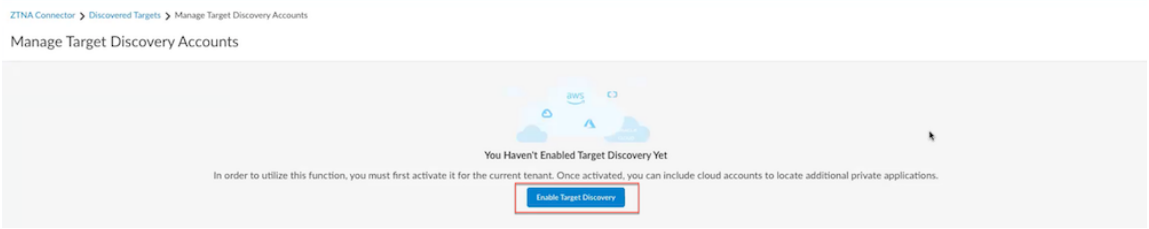
1. Accédez à **Application Targets (Cibles d'applications)(Workflows (Flux de travail) > ZTNA Connector (Connecteur ZTNA) > Application Targets (Cibles d'applications)**).



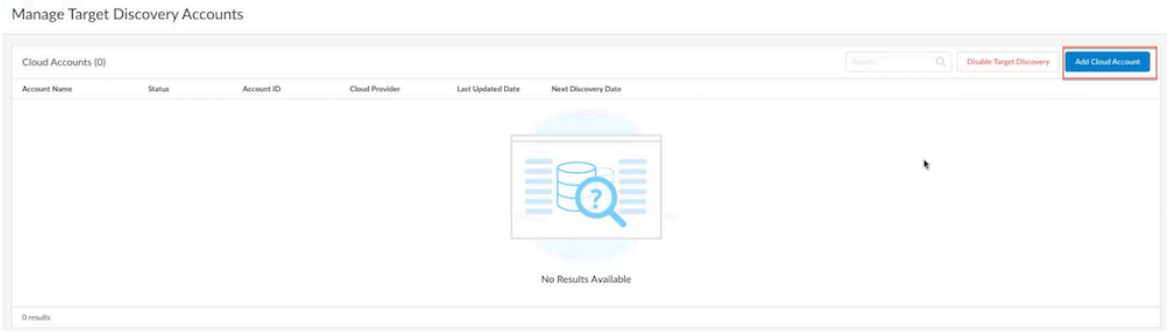
2. Dans la page **Application Targets (Cibles d'applications)**, sélectionnez **Discovered Targets (Cibles découvertes)**, puis **Manage Target Discovery Accounts (Gérer les comptes de découverte de cibles)**.



3. Sélectionnez **Enable Target Discovery (Activer la découverte des cibles)**, puis **Enable (Activer)**.



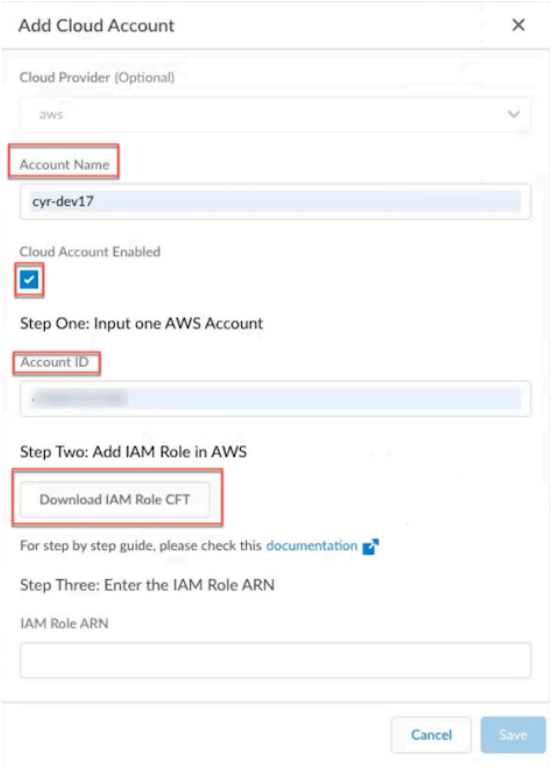
4. Dans la page **Manage Target Discovery Accounts (Gérer les comptes de découverte de cibles)**, sélectionnez **Add Cloud Account (Ajouter un compte cloud)**.



5. Ajoutez un **Account Name (Nom du compte)** et cochez la case sous **Cloud Account Enabled (Compte cloud activé)**. Ajoutez un **Account ID (ID de compte)** AWS et cliquez

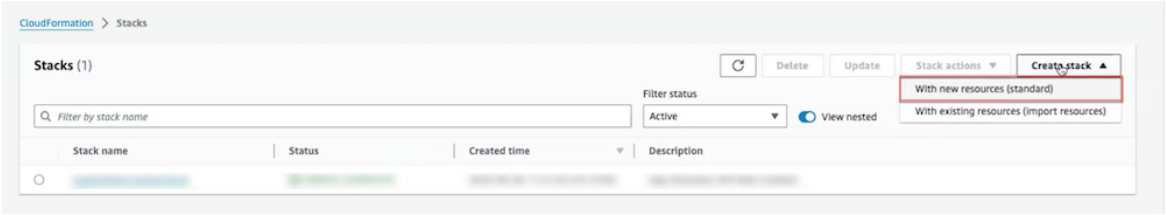
 ©2025 Palo Alto Networks, Inc.

sur **Download IAM Role CFT (Télécharger le CFT de rôle IAM)** pour télécharger le fichier.



STEP 2 | Créez le rôle IAM dans AWS.

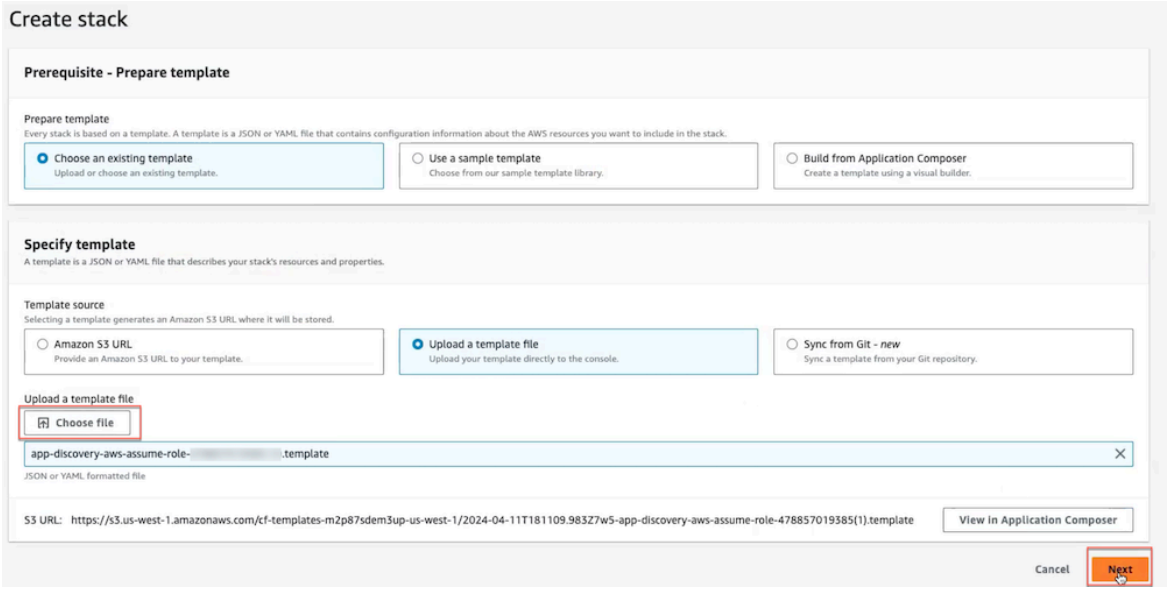
1. Accédez à l'application AWS, sélectionnez votre compte et cliquez sur **Sign in (Se connecter)**.
2. Accédez à **CloudFormation** > **Stacks (Piles)** > **Create stack (Créer une pile)** > **With new resources (standard) (Avec de nouvelles ressources (standard))** pour créer la pile.



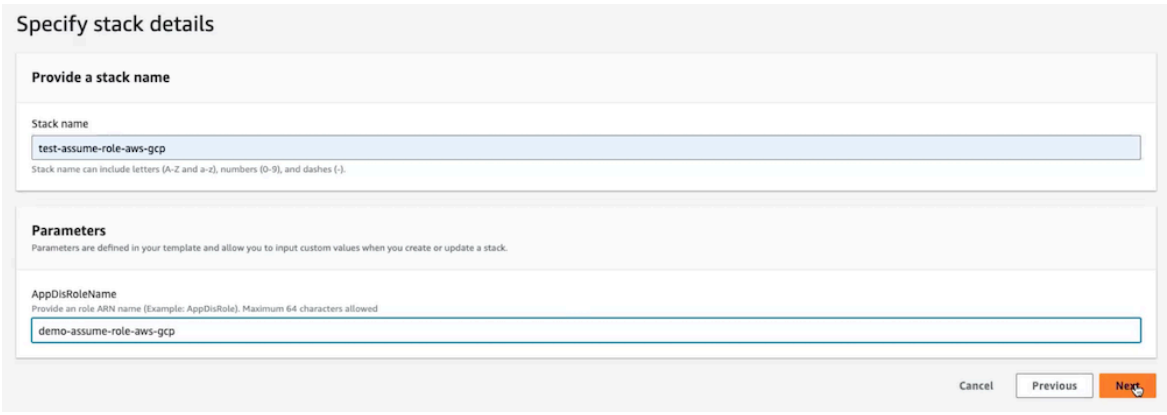
3. Dans la page **Create stack (Créer une pile)**, sous **Prerequisite-Prepare template (Prérequis-Préparer le modèle)**, sélectionnez **Choose an existing template (Choisir un modèle existant)**. Sous **Specify template (Spécifier le modèle)**, sélectionnez **Upload**

 ©2025 Palo Alto Networks, Inc.

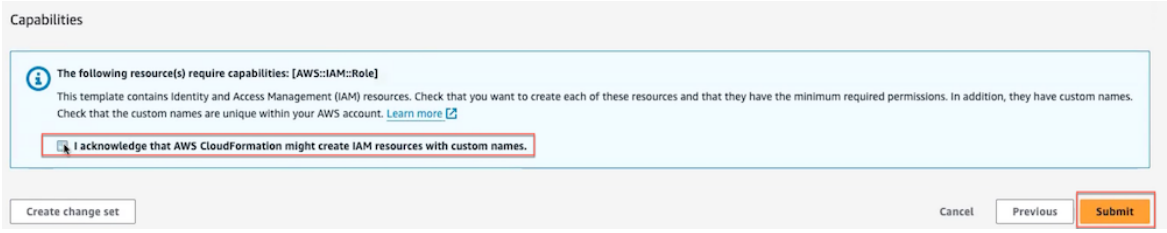
a template file (Télécharger un fichier modèle). Téléchargez le fichier précédemment téléchargé à l'étape 1, puis sélectionnez **Next (Suivant)**.



4. Ajoutez le **Stack name (Nom de pile)**, **AppDisRoleName**, et sélectionnez **Next (Suivant)**.

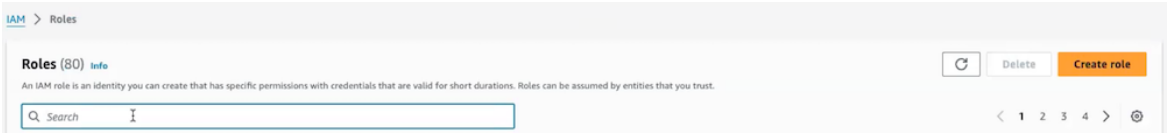


5. Dans la page **Configure stack options (Configurer les options de pile)**, ne faites aucune mise à jour et sélectionnez **Next (Suivant)**.
6. Examinez les modifications. Cochez la case sous **Capabilities (Capacités)** pour accepter la création de ressources IAM avec des noms personnalisés, puis sélectionnez **Submit (Soumettre)**.

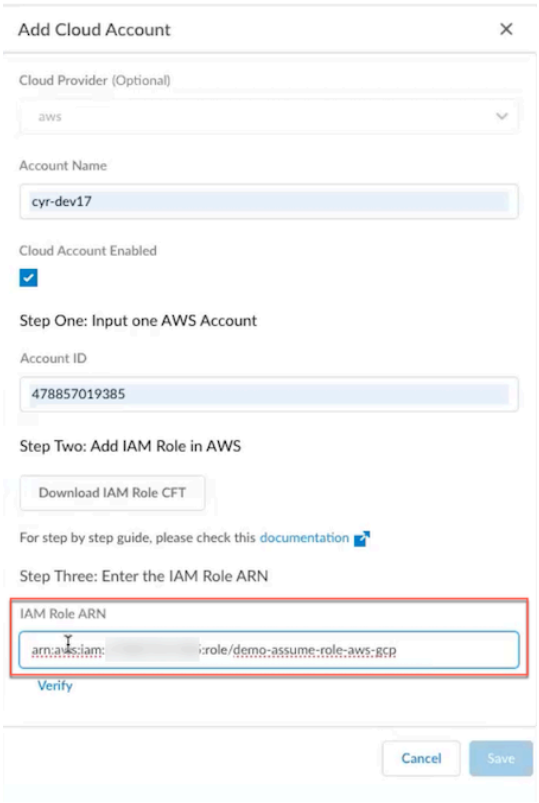


7. Accédez à **IAM** > **Roles (Rôles)** et recherchez le nom du rôle que vous avez défini. Sélectionnez le nom du rôle et copiez l'**ARN** correspondant au rôle.

 ©2025 Palo Alto Networks, Inc.



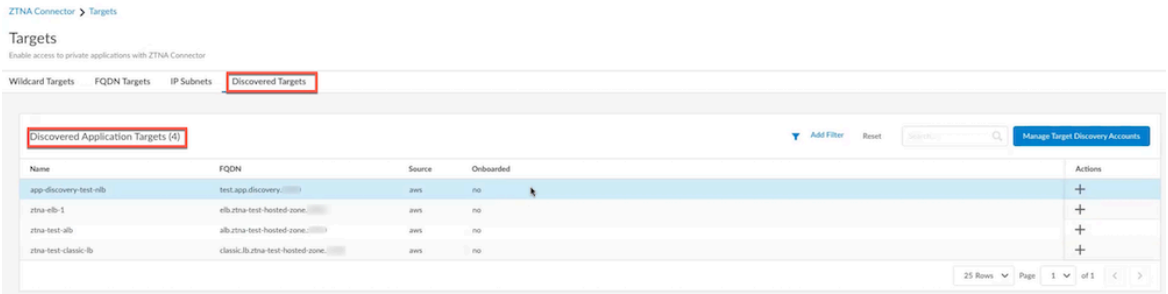
STEP 3 | Collez l'ARN dans le champ de texte **IAM Role ARN (ARN du rôle IAM)**, puis sélectionnez **Verify (Vérifier)**. Lorsque l'ARN est vérifié, sélectionnez **Save (Enregistrer)**.



*Si vous ajoutez un ARN incorrect dans le champ de texte **IAM Role ARN (ARN du rôle IAM)**, la vérification échoue et un message d'erreur s'affiche.*

Après avoir ajouté le compte, vous pouvez voir l'état, l'ID du compte et d'autres détails. La période d'actualisation pour la découverte est de 24 heures. Vous pouvez également ajouter plusieurs comptes au même locataire.

STEP 4 | Pour identifier les applications découvertes, sélectionnez **Discovered Targets (Cibles découvertes)**. Vous trouverez la liste des applications identifiées sous **Discovered Application Targets (Cibles d'applications découvertes)**.

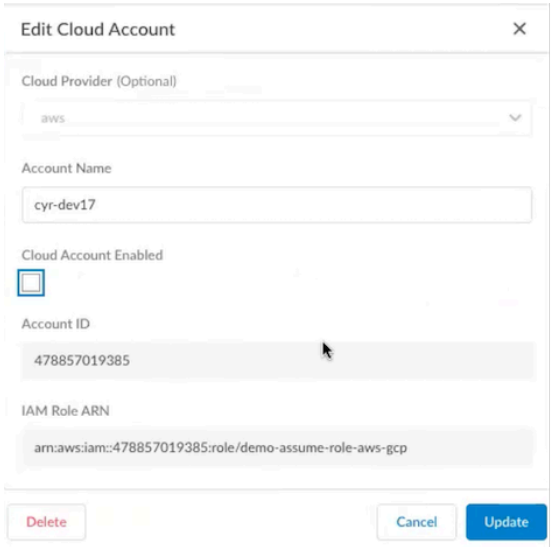


 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Facultatif) Supprimez le compte cloud.

Pour supprimer votre compte cloud et en ajouter un nouveau sans désactiver la découverte de cibles, suivez cette procédure. Toutefois, ces étapes sont obligatoires si vous souhaitez désactiver la fonctionnalité de découverte de cibles.

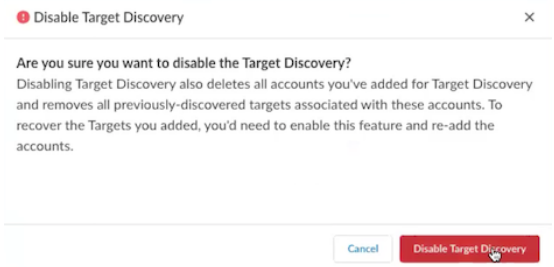
1. Sous **Manage Target Discovery Accounts (Gérer les comptes de découverte de cibles)**, cliquez sur l'**Account Name (Nom du compte)** que vous souhaitez supprimer.
2. Désactivez l'option **Cloud Account Enabled (Compte cloud activé)**, puis sélectionnez **Update (Mettre à jour)**. Lorsque le compte est mis à jour, sélectionnez **Delete (Supprimer)**. Le compte est supprimé.



STEP 6 | (Facultatif) Désactivez la découverte de cibles.

Assurez-vous que tous les comptes cloud sont supprimés avant de désactiver la découverte de cibles.

1. Sélectionnez **Disable Target Discovery (Désactiver la découverte de cibles)**, puis **Disable Target Discovery (Désactiver la découverte de cibles)**.



 ©2025 Palo Alto Networks, Inc.

Politique de sécurité pour les applications activées avec le connecteur ZTNA

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend 200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

Le connecteur ZTNA n'applique pas de politique ; il étend de manière transparente votre politique de sécurité Prisma Access existante aux applications qu'il autorise pour Prisma Access. Cela signifie que vous pouvez utiliser une politique commune à toutes vos applications et à tous vos centres de données, et que vous n'avez pas besoin de rédiger votre politique de sécurité séparément pour les applications intégrées au connecteur ZTNA.

Toutefois, dans le cadre de la configuration du connecteur ZTNA, vous devez vous assurer que votre politique de sécurité :

Permet la circulation entre Prisma Access et le connecteur ZTNA

Pour cela, suivez le Exigences et directives du connecteur ZTNA pour vous assurer que le connecteur ZTNA peut se connecter à Prisma Access.

Les utilisateurs peuvent accéder aux applications derrière le connecteur ZTNA

Pour vous assurer que vos utilisateurs peuvent accéder aux applications du connecteur ZTNA, suivez les étapes ci-dessous pour l'interface que vous utilisez pour gérer Prisma Access.

 ©2025 Palo Alto Networks, Inc.

- Strata Cloud Manager
- Panorama

Politique de sécurité pour les applications activées avec le connecteur ZTNA (Strata Cloud Manager)

Après avoir intégré des applications au connecteur ZTNA, vous devez configurer des règles de politique pour autoriser et contrôler l'accès à ces applications. La procédure de création et d'application de la politique diffère selon que vos applications sont définies par des caractères génériques, des sous-réseaux IP ou des FQDN.

Politique de sécurité pour les applications basées sur des caractères génériques

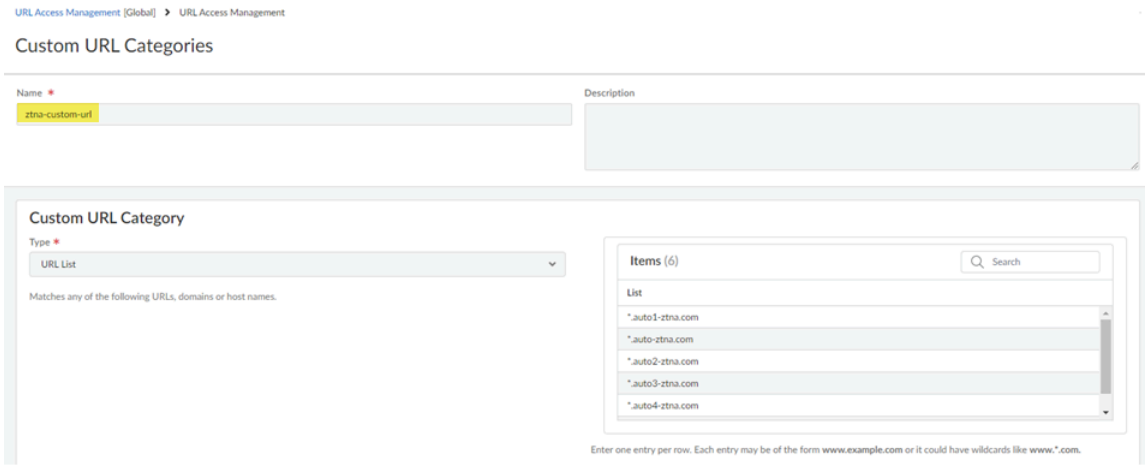
Les applications basées sur Wilcard ((**Settings (Paramètres)** > **ZTNA Connector (Connecteur ZTNA)** > **Application Targets (Cibles d'application)** > **Wildcard Targets (Cibles de caractères génériques)**) nécessitent la création d'une catégorie d'URL personnalisée ; toutefois, ce type de catégorie n'applique la politique que pour le trafic HTTP et HTTPS, et les autres trafics (tels que SSH) ne sont pas autorisés. Pour cette raison, vous devez autoriser temporairement l'accès à toutes les applications en autorisant le trafic vers les blocs IP de l'application du connecteur ZTNA.

Une fois que le connecteur ZTNA a appris les FQDN basés sur les caractères génériques, vous pouvez désactiver la politique qui autorise le blocage de l'adresse IP de l'application et applique l'application de la politique en fonction des FQDN appris.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Créez une catégorie d'URL personnalisée et ajoutez les URL génériques à la catégorie.

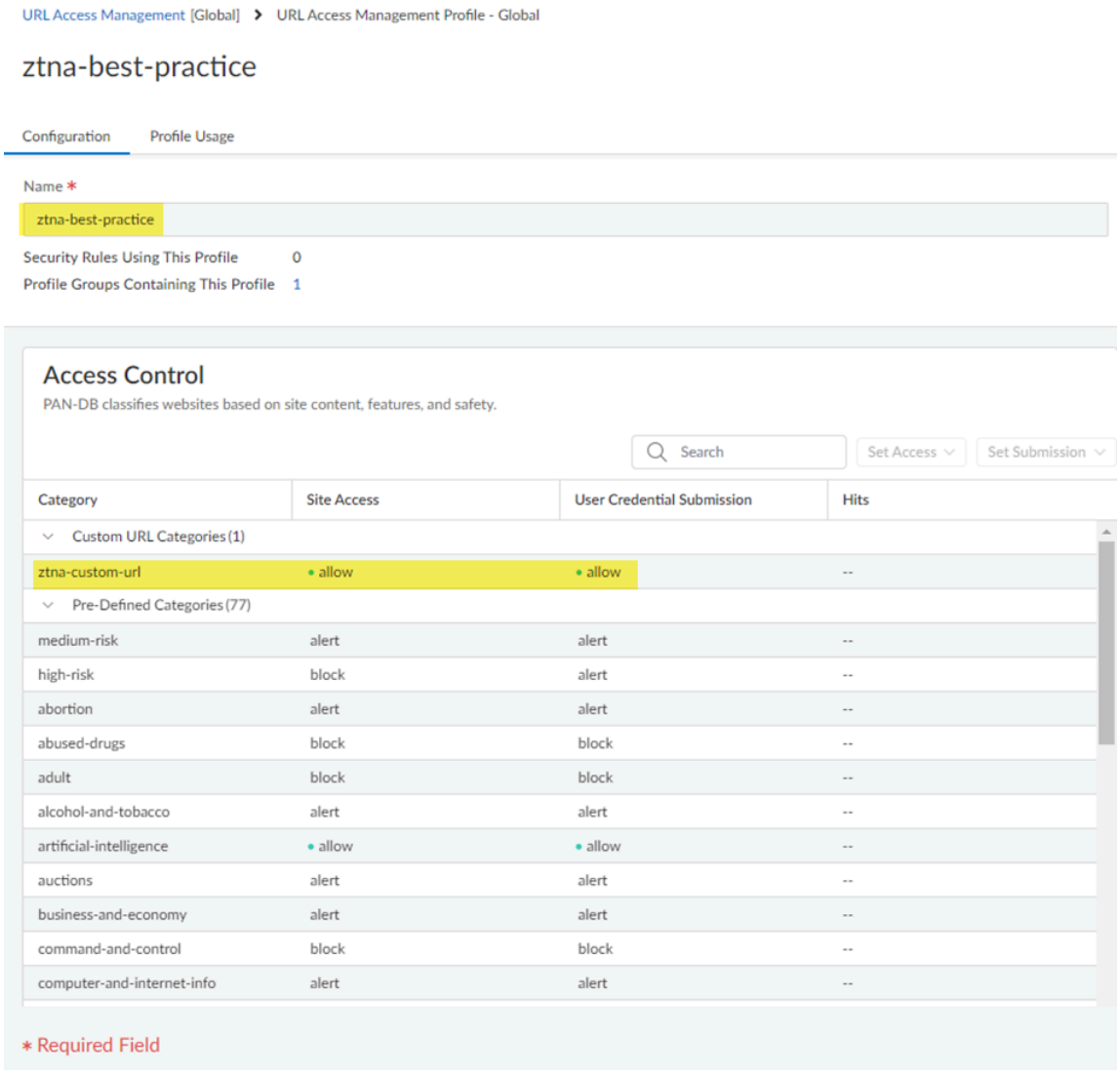
1. Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **URL Access Management (Gestion des accès à l'URL)**.
2. Sous les catégories Custom URL (URL personnalisée), sélectionnez **Add Category (Ajouter une catégorie)**.
3. Donnez un **Name (Nom)** descriptif pour la catégorie d'URL personnalisée et sélectionnez un **Type** de **URL List (Liste d'URL)**.
4. Ajoutez les URL génériques que vous avez créées dans le connecteur ZTNA pour les **Items (Éléments)**.
5. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Créez un profil de gestion de l'accès à l'URL et ajoutez-y la catégorie d'URL personnalisée que vous avez créée.

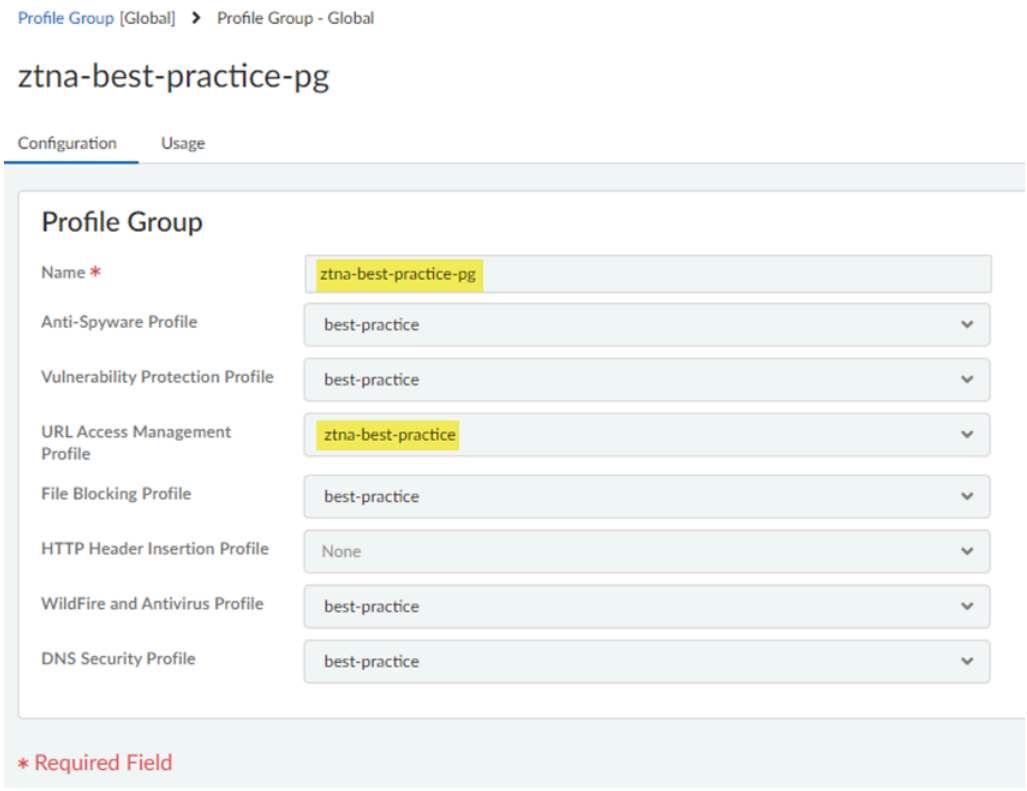
1. Alors que vous êtes encore dans la zone **URL Access Management (Gestion de l'accès à l'URL)**, sélectionnez **URL Access Management Profiles (Profils de gestion de l'accès à l'URL)**.
2. Sélectionnez un profil existant à modifier ou cliquez sur **Add Profile (Ajouter un profil)**.
3. Ajoutez la catégorie d'URL personnalisée que vous avez créée pour le profil.
4. Sélectionnez les paramètres suivants :
   - **Site Access (Accès au site)** : Autoriser
   - **User Credential Submission (Envoi des informations d'identification de l'utilisateur)** : Autoriser
5. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Créez un groupe de profils et associez-y le profil de gestion de l'accès à l'URL.

1. Accédez à **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Profile Groups (Groupes de profils)**.
2. **Add (Ajoutez)** un groupe de profils, en spécifiant le profil de gestion de l'accès à l'URL que vous avez créé.

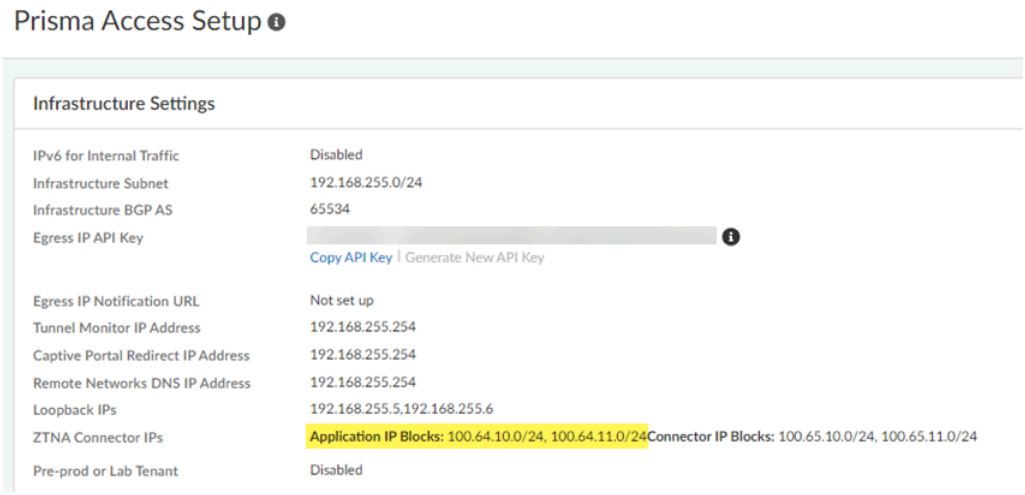


STEP 4 | Créez une politique pour autoriser le groupe de profils et les adresses IP pour les blocs IP de l'application du connecteur ZTNA.

1. Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration Prisma Access)** > **Prisma Access** > **Prisma Access Setup (Configuration Prisma Access)** et notez

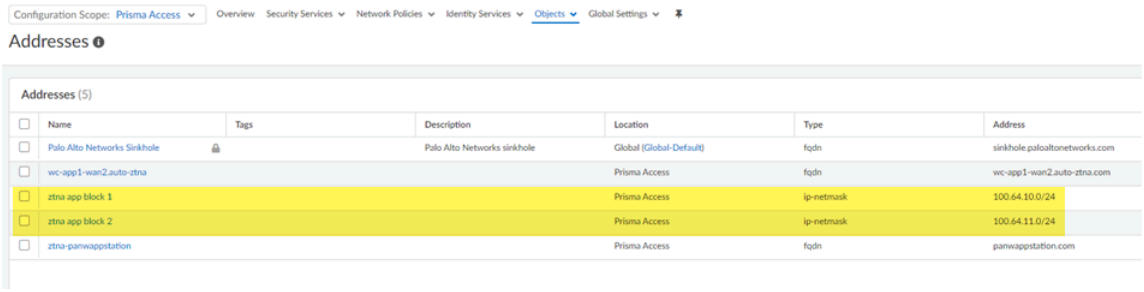
 ©2025 Palo Alto Networks, Inc.

le **Application IP Blocks (Blocs d'adresses IP d'application)** sous les adresses IP du connecteur ZTNA.

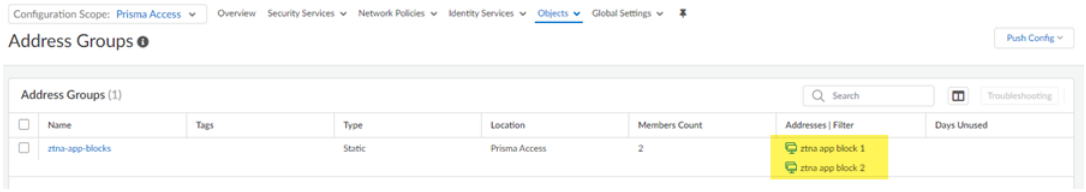


2. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Address (Adresse)** > **Addresses (Adresses)** et **Add (Ajoutez)** des objets d'adresse en fonction des adresses IP que vous avez récupérées.

   Si vous avez des applications basées sur un sous-réseau IP, créez également des objets d'adresse pour ces sous-réseaux.



3. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Address (Adresse)** > **Address Groups (Groupes d'adresses)** et **Add (Ajoutez)** les objets d'adresse que vous avez créés pour un groupe d'adresses.



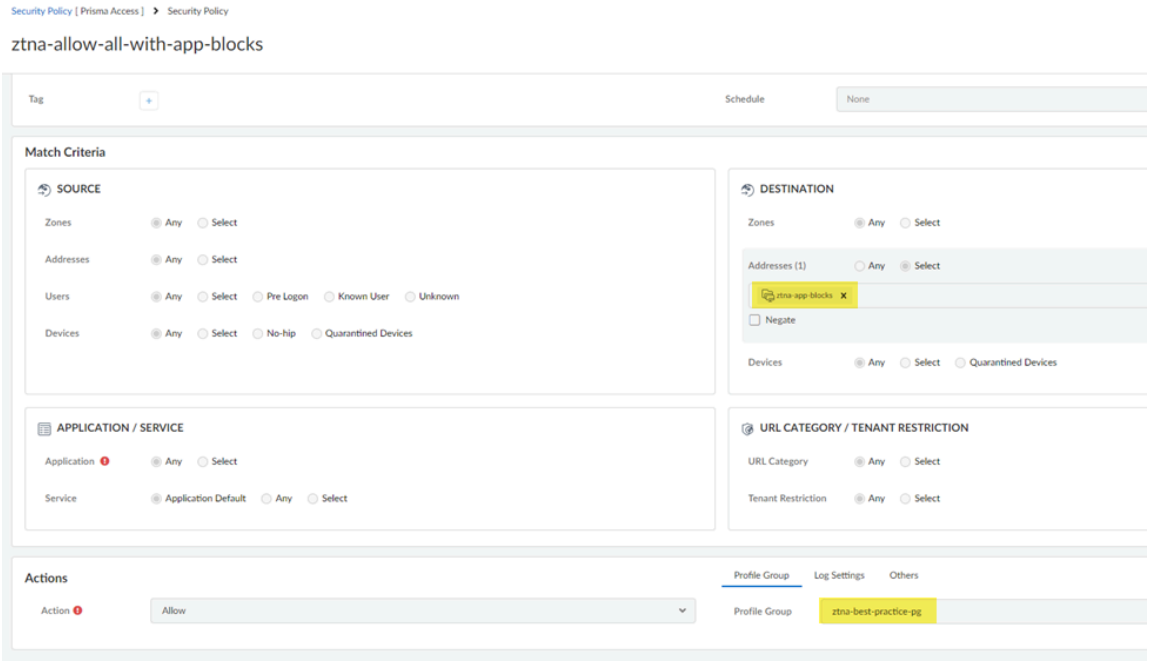
4. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** > **Pre Rules (Pré-règles)** et **Add (Ajoutez)** une politique de sécurité pour autoriser l'accès à tous les blocs d'adresses IP de l'application, en spécifiant le **Address**

 ©2025 Palo Alto Networks, Inc.

Group (Groupe d'adresses) et le **Profil Group (Groupe de profils)** que vous avez créé à une étape précédente.

L'ajout de cette politique de sécurité permet de transmettre tout le trafic des applications basées sur des caractères génériques, tandis que le connecteur ZTNA découvre les applications basées sur des caractères génériques. Sans la règle autorisant les blocs d'adresses IP d'application, les utilisateurs ne peuvent pas accéder aux applications basées sur des caractères génériques.

Vous pouvez laisser cette politique en place jusqu'à ce que le connecteur ZTNA découvre les applications basées sur des caractères génériques. Ensuite, vous pouvez choisir de désactiver cette politique et d'ajouter des règles de politique de sécurité pour chacune des applications découvertes.



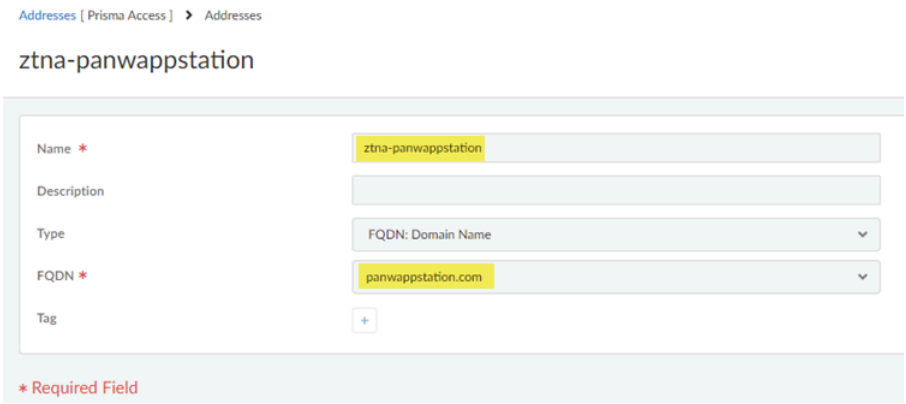
 ©2025 Palo Alto Networks, Inc.

STEP 5 | Une fois que le connecteur ZTNA a découvert les applications basées sur des caractères génériques, configurez une politique de sécurité pour les applications que vous avez ajoutées à l'aide de FQDN.

1. Accédez à **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Application Targets (Cibles d'application)** > **FQDN Targets (Cibles FQDN)** et notez les FQDN utilisés par les applications.
2. Créez un objet d'adresse pour le FQDN (**Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Address (Adresse)** > **Addresses (Adresses)**).

   Sélectionnez la portée de la configuration **Prisma Access**.
3. **Add (Ajoutez)** un objet d'adresse avec l'attribut **Type** de **FQDN: Domain Name (FQDN : nom de domaine)** et saisissez le **FQDN** de l'application découverte.

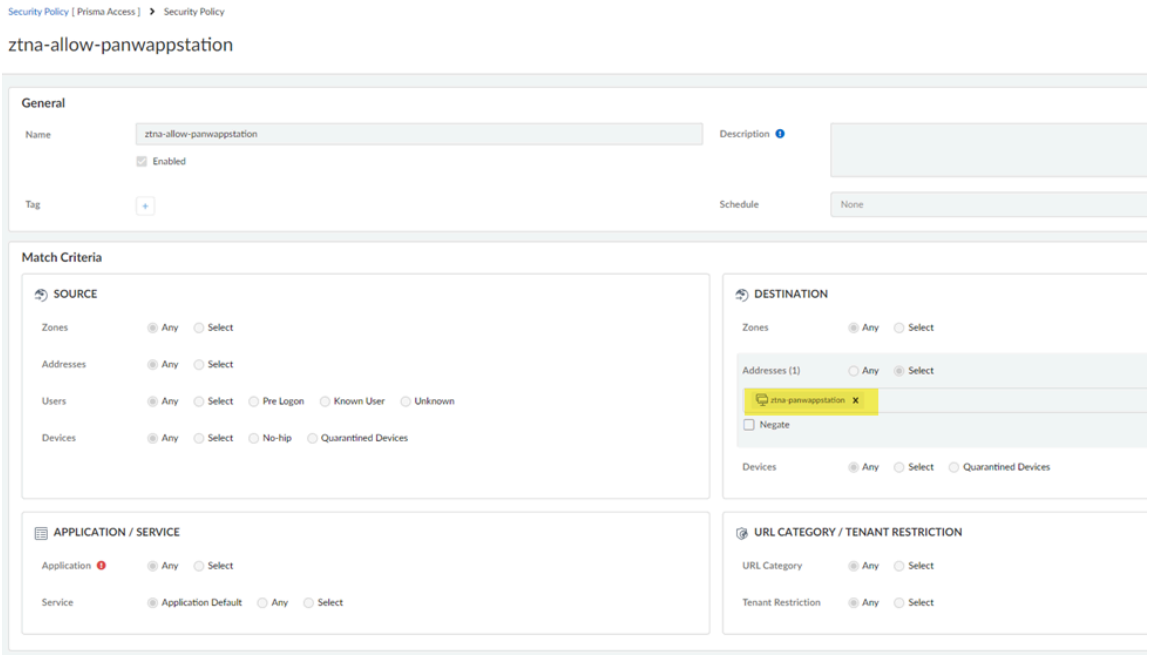
   Saisissez les FQDN pour les cibles FQDN.



4. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique**

 ©2025 Palo Alto Networks, Inc.

de sécurité) > **Pre Rules (Pré-règles)** et **Add (Ajouter)** une politique de sécurité pour autoriser l'accès aux applications découvertes.



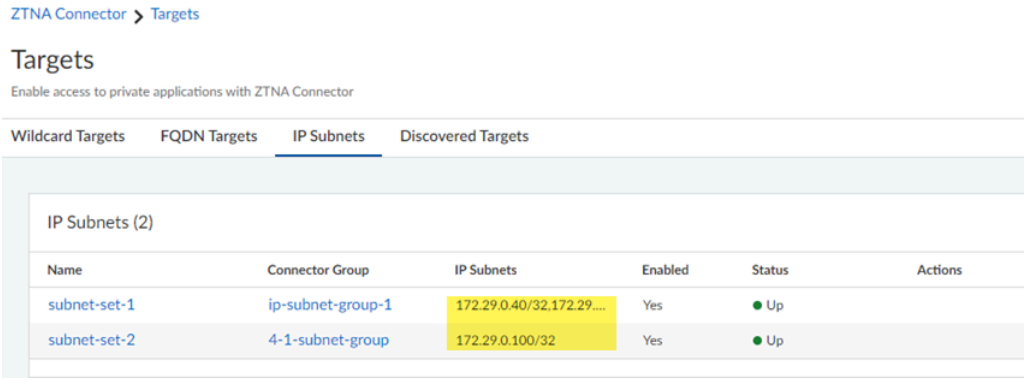
STEP 6 | **Push Config (Transmettez la configuration)** pour enregistrer et transmettre vos modifications de configuration.

STEP 7 | (Facultatif) Une fois que vous avez créé la politique de sécurité basée sur les FQDN, supprimez la politique basée sur les blocs d'applications IP.

Politique de sécurité pour les applications basées sur un sous-réseau IP

Si vous avez créé des cibles d'application de connecteur ZTNA basées sur des sous-réseaux IP (**Settings (Paramètres)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)** > **Application Targets (Cibles d'application)** > **IP Subnets (Sous-réseaux IP)**), procédez comme suit pour autoriser l'accès aux applications.

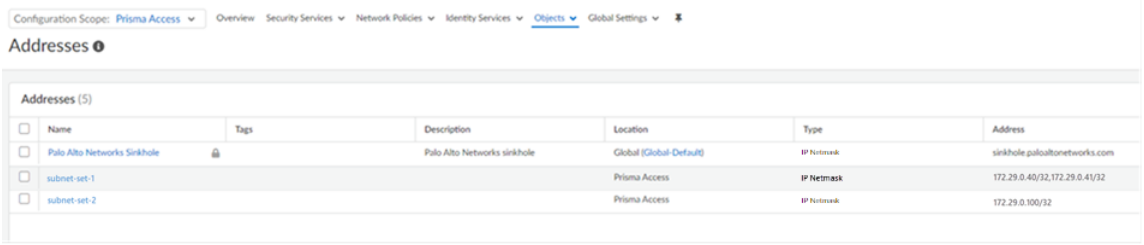
STEP 1 | Accédez à **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Application Targets (Cibles d'application)** > **IP Subnets (Sous-réseaux IP)** et notez les sous-réseaux IP utilisés par les applications.



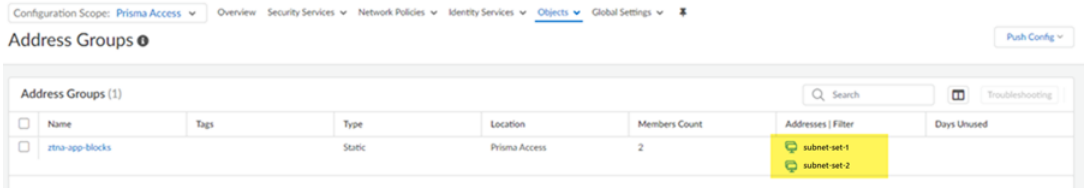
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Créez une politique pour autoriser les adresses IP des sous-réseaux IP utilisés pour les applications.

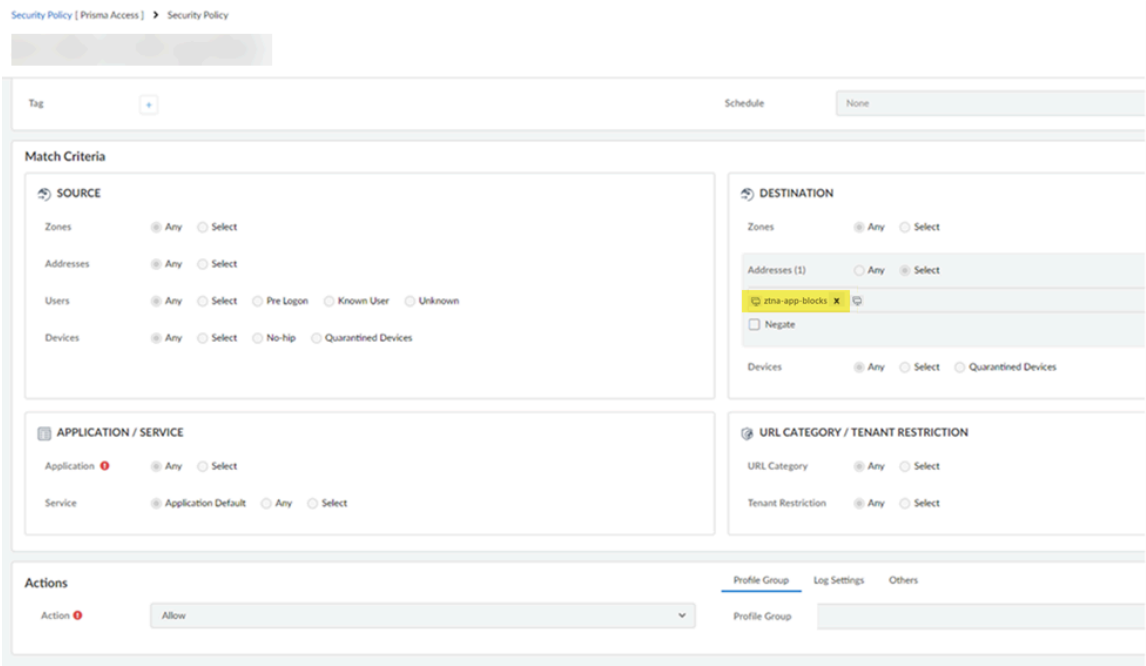
1. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Address (Adresse)** > **Addresses (Adresses)** et **Add (Ajoutez)** des objets d'adresse en fonction des adresses IP que vous avez récupérées.



2. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Address (Adresse)** > **Address Groups (Groupes d'adresses)** et **Add (Ajoutez)** les adresses que vous avez créées dans les groupes d'adresses.



3. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** > **Pre Rules (Pré-règles)** et **Add (Ajoutez)** une politique de sécurité pour autoriser l'accès aux sous-réseaux IP pour les applications, en spécifiant les **Addresses (Adresses)** que vous avez créé à une étape précédente.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | **Push Config (Transmettez la configuration)** pour enregistrer et transmettre vos modifications de configuration.

Politique de sécurité pour les applications basées sur des FQDN

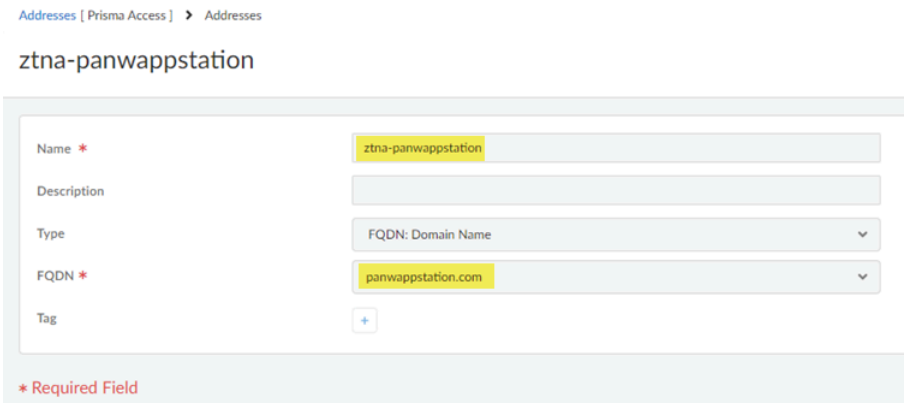
Si vous avez ajouté des cibles basées sur des FQDN (**Settings (Paramètres)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)** > **Application Targets (Cibles d'application)** > **FQDN Targets (Cibles FQDN)**), créez un objet d'adresse et une politique de sécurité pour autoriser l'accès aux applications en procédant comme suit.

STEP 1 | Configurez une politique de sécurité pour les applications que vous avez ajoutées à l'aide de FQDN.

1. Accédez à **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Application Targets (Cibles d'application)** > **FQDN Targets (Cibles FQDN)** et notez les FQDN utilisés par les applications.
2. Créez un objet d'adresse pour le FQDN (**Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Address (Adresse)** > **Addresses (Adresses)**).

   Sélectionnez la portée de la configuration **Prisma Access**.
3. **Add (Ajoutez)** un objet d'adresse avec l'attribut **Type** de **FQDN: Domain Name (FQDN : nom de domaine)** et saisissez le **FQDN** de l'application découverte.

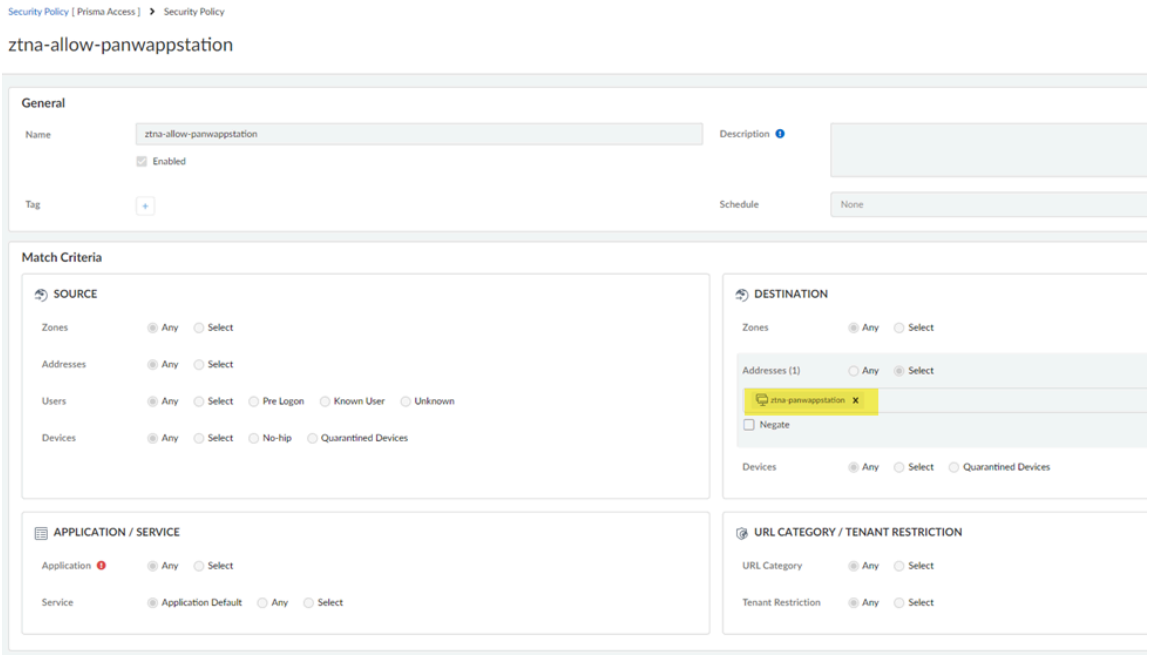
   Saisissez les FQDN de toutes les applications découvertes.



4. Facultatif Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy**

 ©2025 Palo Alto Networks, Inc.

(Politique de sécurité) > **Pre Rules (Pré-règles)** et **Add (Ajoutez)** une politique de sécurité pour autoriser l'accès aux applications découvertes.



STEP 2 | **Push Config (Transmettez la configuration)** pour enregistrer et transmettre vos modifications de configuration.

Politique de sécurité pour les applications activées avec le connecteur ZTNA (Panorama)

Après avoir intégré des applications au connecteur ZTNA, vous devez configurer des règles de politique pour autoriser et contrôler l'accès à ces applications. La procédure de création et d'application de la politique diffère selon que vos applications sont définies par des caractères génériques, des sous-réseaux IP ou des FQDN.

Politique de sécurité pour les applications basées sur des caractères génériques

Les applications basées sur Wilcard ((**Settings (Paramètres)** > **ZTNA Connector (Connecteur ZTNA)** > **Application Targets (Cibles d'application)** > **Wildcard Targets (Cibles de caractères génériques)**) nécessitent la création d'une catégorie d'URL personnalisée ; toutefois, ce type de catégorie n'applique la politique que pour le trafic HTTP et HTTPS, et les autres trafics (tels que SSH) ne sont pas autorisés. Pour cette raison, vous devez autoriser temporairement l'accès à toutes les applications en autorisant le trafic vers les blocs IP de l'application du connecteur ZTNA.

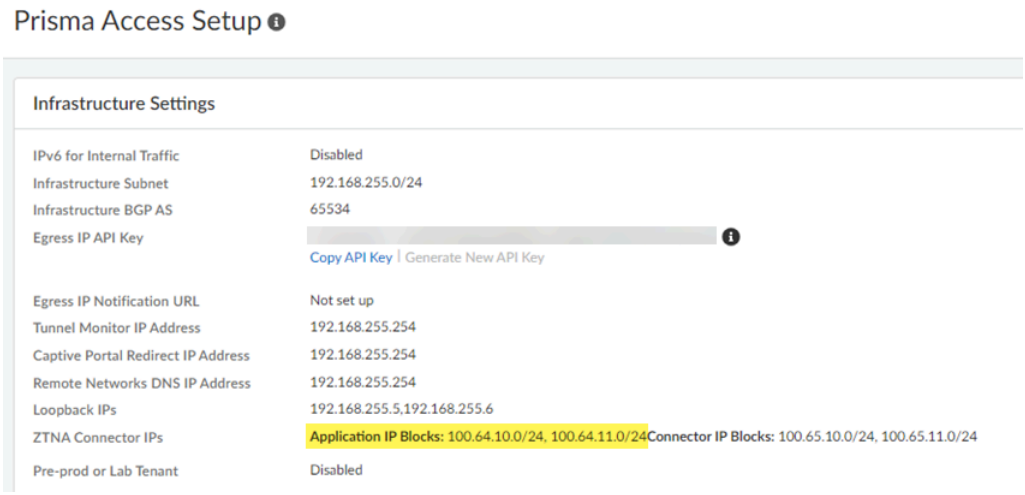
Une fois que le connecteur ZTNA a appris les FQDN basés sur les caractères génériques, vous pouvez désactiver la politique qui autorise le blocage de l'adresse IP de l'application et applique l'application de la politique en fonction des FQDN appris.

STEP 1 | Créez une politique pour autoriser les adresses IP pour les blocs IP de l'application du connecteur ZTNA.

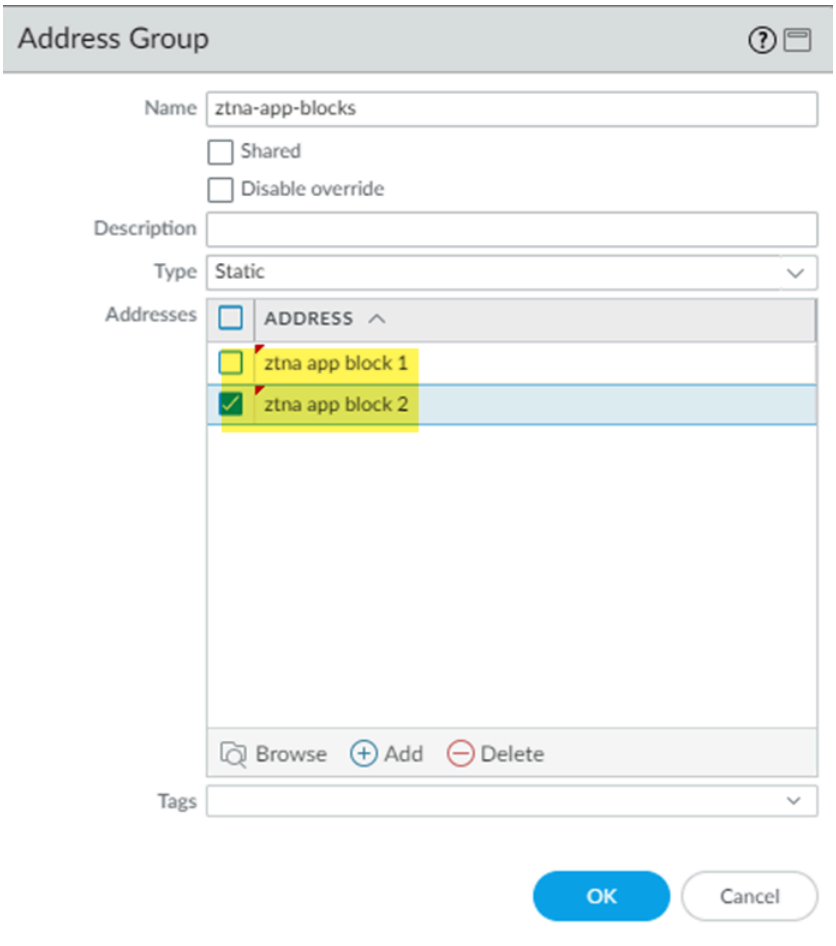
1. Depuis l'interface utilisateur du connecteur ZTNA, accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration Prisma Access)** > **Prisma Access** > **Prisma**

 ©2025 Palo Alto Networks, Inc.

Access Setup (Configuration Prisma Access) et notez le **Application IP Blocks (Blocs d'adresses IP d'application)** sous les adresses IP du connecteur ZTNA.



2. Accédez à **Objects (Objets)** > **Addresses (Adresses)** et **Add (Ajoutez)** des objets d'adresse en fonction des adresses IP que vous avez récupérées.
3. Accédez à **Objects (Objets)** > **Address Groups (Groupes d'adresses)** et **Add (Ajoutez)** les objets d'adresse que vous avez créés à un groupe d'adresses.

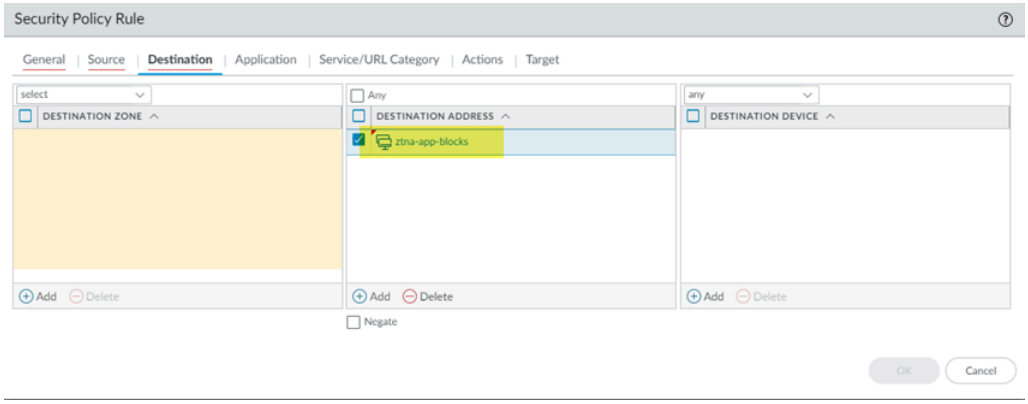


 ©2025 Palo Alto Networks, Inc.

4. Accédez à **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Pré-règles)** et **Add (Ajoutez)** une politique de sécurité pour autoriser l'accès à tous les blocs d'adresses IP d'application, en spécifiant le **Address Group (Groupe d'adresses)** que vous avez créé à une étape précédente.

   L'ajout de cette politique de sécurité permet de transmettre tout le trafic des applications basées sur des caractères génériques, tandis que le connecteur ZTNA découvre les applications basées sur des caractères génériques. Sans la règle autorisant les blocs d'adresses IP d'application, les utilisateurs ne peuvent pas accéder aux applications basées sur des caractères génériques.

   Vous pouvez laisser cette politique en place jusqu'à ce que le connecteur ZTNA découvre les applications basées sur des caractères génériques. Ensuite, vous pouvez choisir de désactiver cette politique et d'ajouter des règles de politique de sécurité pour chacune des applications découvertes.



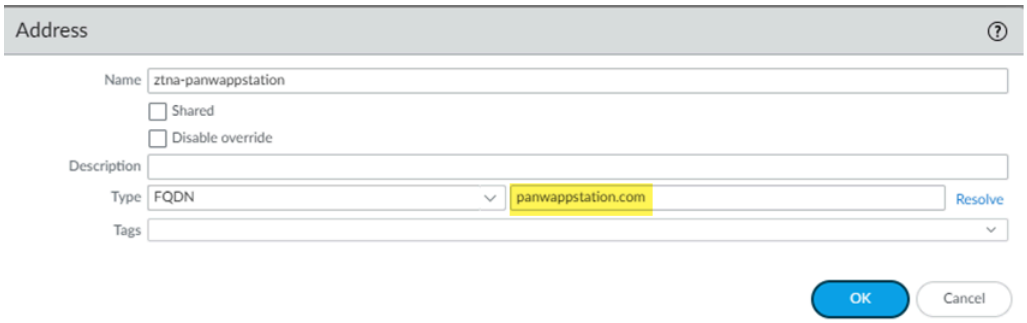
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Une fois que le connecteur ZTNA a découvert les applications basées sur des caractères génériques, configurez une politique de sécurité pour les applications que vous avez ajoutées à l'aide de FQDN.

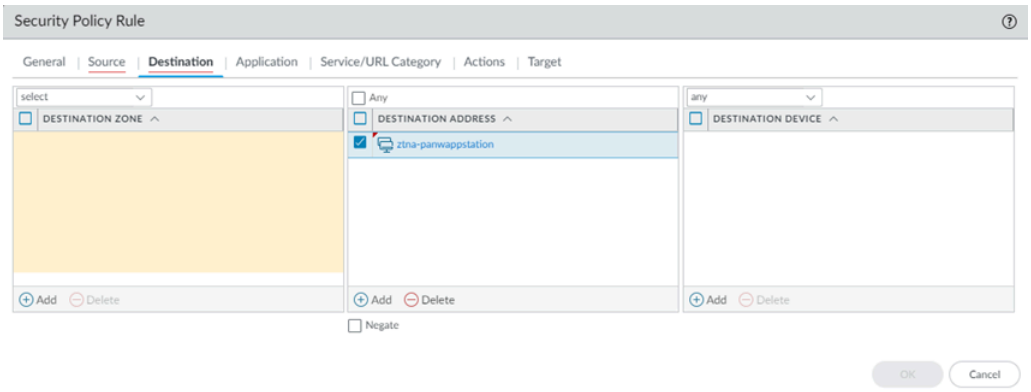
1. Accédez à **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Application Targets (Cibles d'application)** > **FQDN Targets (Cibles FQDN)** et notez les FQDN utilisés par les applications.
2. Créez un objet d'adresse pour le FQDN (**Objects (Objets)** > **Addresses (Adresses)**).

   Sélectionnez soit **Mobile_User_Device_Group**, soit **Remote_Network_Device_Group**, selon que les utilisateurs mobiles ou les utilisateurs des sites de succursales accéderont aux applications privées derrière le connecteur ZTNA.
3. **Add (Ajoutez)** un objet d'adresse avec le **Type** de **FQDN** et saisissez le **FQDN** de l'application découverte.

   Saisissez les FQDN pour les cibles FQDN.



4. Accédez à **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Pré-règles)** et **Add (Ajoutez)** une politique de sécurité pour autoriser l'accès aux applications découvertes.



STEP 3 | **Commit and Push (Validez et appliquez)** vos modifications.

STEP 4 | (Facultatif) Une fois que vous avez créé la politique de sécurité basée sur les FQDN, supprimez la politique basée sur les blocs d'applications IP.

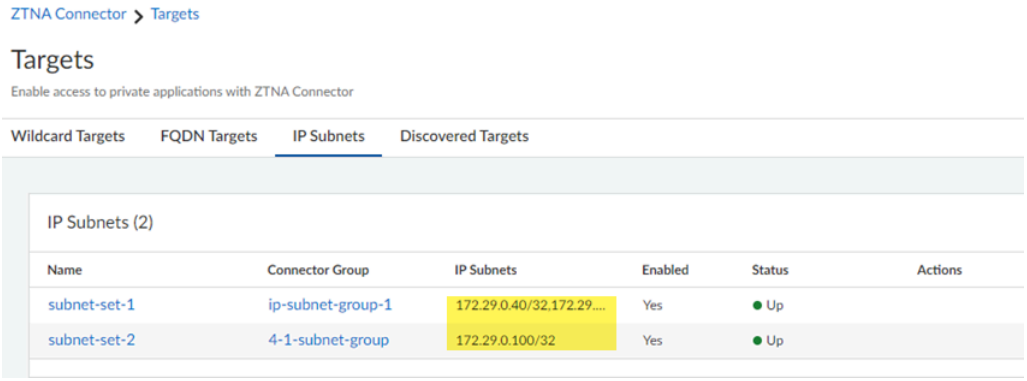
Politique de sécurité pour les applications basées sur un sous-réseau IP

Si vous avez créé des cibles d'application de connecteur ZTNA basées sur des sous-réseaux IP (**Settings (Paramètres)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)** >

 ©2025 Palo Alto Networks, Inc.

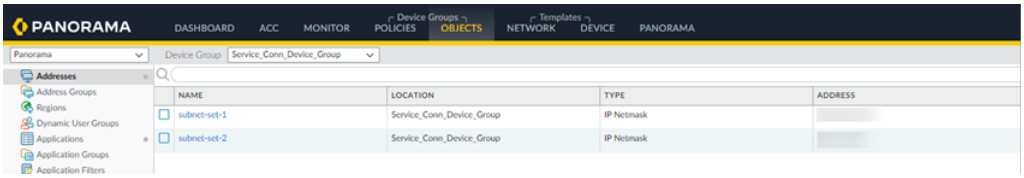
Application Targets (Cibles d'application) > **IP Subnets (Sous-réseaux IP)**), procédez comme suit pour autoriser l'accès aux applications.

STEP 1 | Accédez à **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Application Targets (Cibles d'application)** > **IP Subnets (Sous-réseaux IP)** et notez les sous-réseaux IP utilisés par les applications.

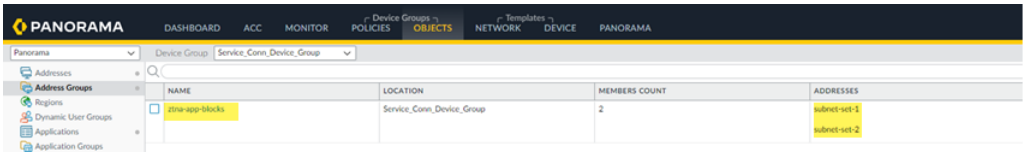


STEP 2 | Créez une politique pour autoriser les adresses IP des sous-réseaux IP utilisés pour les applications.

1. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Address (Adresse)** > **Addresses (Adresses)** et **Add (Ajoutez)** des objets d'adresse en fonction des adresses IP que vous avez récupérées.



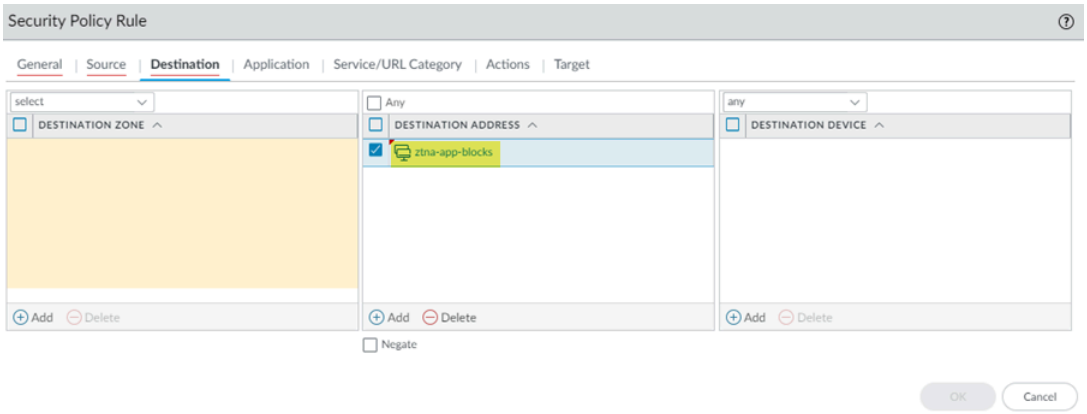
2. Accédez à **Objects (Objets)** > **Address Groups (Groupes d'adresses)** et **Add (Ajoutez)** les adresses que vous avez créées aux groupes d'adresses.



3. Accédez à **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Pré-règles)** et **Add (Ajoutez)** une politique de sécurité pour autoriser l'accès aux sous-réseaux IP pour les

 ©2025 Palo Alto Networks, Inc.

applications, en spécifiant les **Addresses (Adresses)** que vous avez créées à une étape précédente.



STEP 3 | **Push Config (Transmettez la configuration)** pour enregistrer et transmettre vos modifications de configuration.

Politique de sécurité pour les applications basées sur des FQDN

Si vous avez ajouté des cibles basées sur des FQDN (**Settings (Paramètres)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)** > **Application Targets (Cibles d'application)** > **FQDN Targets (Cibles FQDN)**), créez un objet d'adresse et une politique de sécurité pour autoriser l'accès aux applications en procédant comme suit.

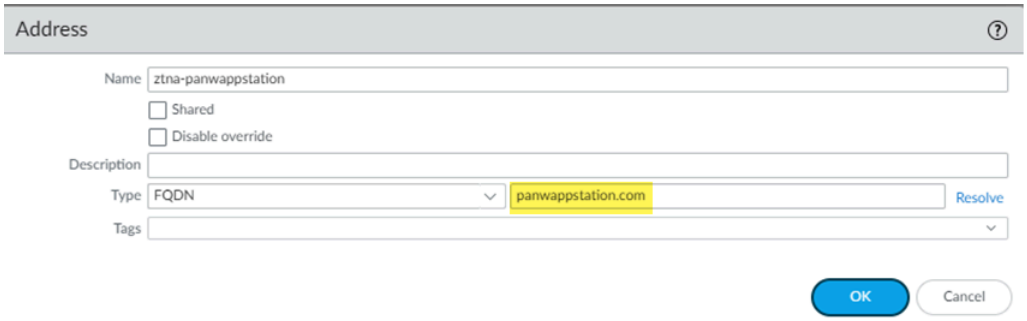
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Configurez une politique de sécurité pour les applications que vous avez ajoutées à l'aide de FQDN.

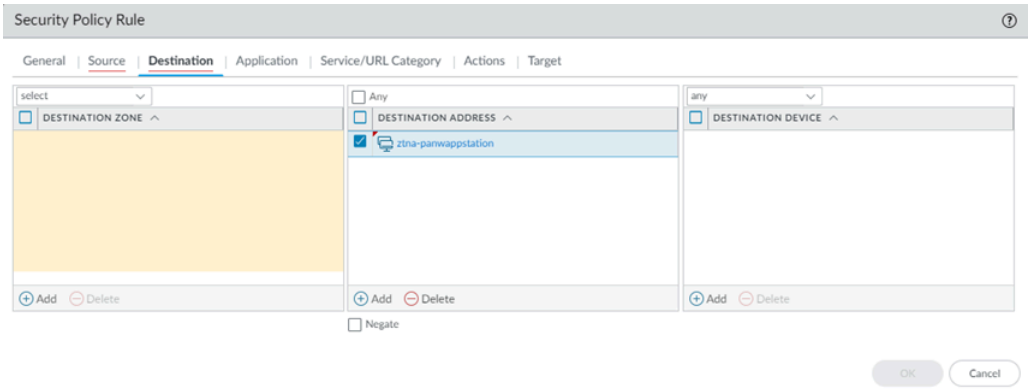
1. Accédez à **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Application Targets (Cibles d'application)** > **FQDN Targets (Cibles FQDN)** et notez les FQDN utilisés par les applications.
2. Créez un objet d'adresse pour le FQDN (**Objects (Objets)** > **Addresses (Adresses)**).

   Sélectionnez soit **Mobile_User_Device_Group**, soit **Remote_Network_Device_Group**, selon que les utilisateurs mobiles ou les utilisateurs des sites de succursales accéderont aux applications privées derrière le connecteur ZTNA.
3. **Add (Ajoutez)** un objet d'adresse avec le **Type** de **FQDN** et saisissez le **FQDN** de l'application découverte.

   Saisissez les FQDN de toutes les applications découvertes.



4. Facultatif Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** > **Pre Rules (Pré-règles)** et **Add (Ajoutez)** une politique de sécurité pour autoriser l'accès aux applications découvertes.



STEP 2 | **Push Config (Transmettez la configuration)** pour enregistrer et transmettre vos modifications de configuration.

 ©2025 Palo Alto Networks, Inc.

Intégrer la VM du connecteur ZTNA dans votre centre de données

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend 200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

Après avoir configuré vos groupes de connecteurs, connecteurs et cibles d'application dans Prisma Access, vous devez déployer la VM de connecteur dans votre centre de données. Pour simplifier l'intégration des connecteurs, des modèles de déploiement pour chaque environnement de centre de données sont disponibles sur le portail de support client de Palo Alto Networks ou sur le marketplace des fournisseurs cloud. Le modèle que vous utilisez dépend de votre utilisation prévue d'un déploiement à un bras ou un déploiement à deux bras.

Déploiements pris en charge du connecteur ZTNA

Le connecteur ZTNA initie la connexion à l'adresse IP publique de Prisma Access dans le cloud. Vous n'avez pas besoin de définir des règles de sécurité de pare-feu d'entrée. Cependant, comme le connecteur ZTNA initie la connexion, vous devrez ajouter des règles de sortie pour permettre l'accès du connecteur ZTNA au contrôleur cloud et à la connexion IPSec vers le plan de données Prisma Access. Le connecteur ZTNA initie la connexion à l'adresse IP publique de Prisma Access

 ©2025 Palo Alto Networks, Inc.

dans le cloud. Pour cette raison, vous avez besoin des règles de sortie suivantes afin que le connecteur ZTNA puisse créer un tunnel IPSec vers Prisma Access :

- **Côté internet** : autoriser la sortie pour HTTPS (TCP 443) et IKE/IPSec (UDP 500 et 4500)
- **Côté centre de données** : autoriser les ports d'application sortants.

  Par exemple, autorisez les ports d'application sortants HTTP (80) et HTTPS (443). Ces exemples sont des ports TCP. Si votre centre de données utilise d'autres ports, autorisez plutôt ces ports.

Vous pouvez déployer la VM du connecteur dans les topologies de déploiement suivantes :

- **Déploiement à un bras**

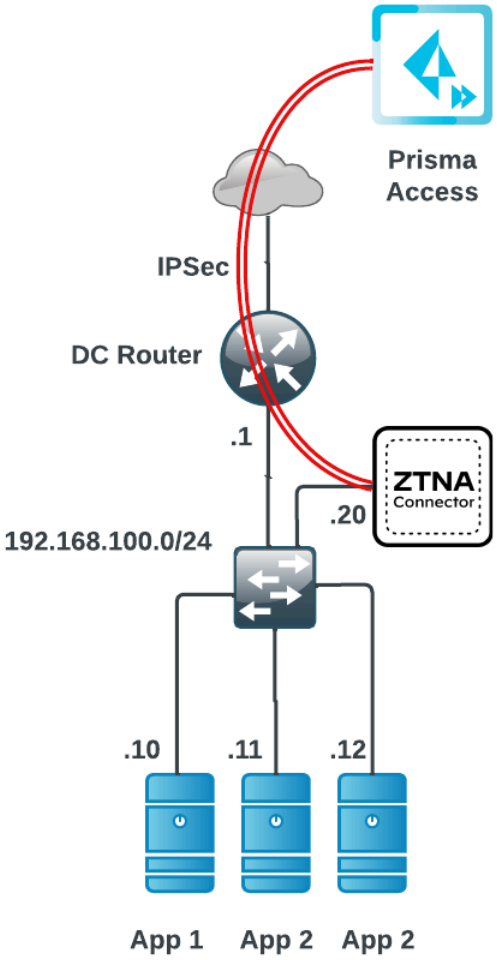
  Les déploiements à un bras sont uniquement pris en charge dans des environnements cloud natifs tels qu'AWS, Azure ou GCP. Pour les déploiements sur site tels que ESXi ou une machine virtuelle basée sur noyau (KVM) ou Microsoft Hyper-V, utilisez le déploiement à deux bras.

  Dans ce déploiement, votre connecteur ZTNA se trouve sur un sous-réseau de centre de données privé, avec accès à Internet via un routeur de centre de données. L'accès aux

 ©2025 Palo Alto Networks, Inc.

applications peut se faire localement sur le même sous-réseau, ou via le routeur du centre de données.

Le diagramme suivant montre l'exemple d'un déploiement réseau du connecteur ZTNA utilisant un déploiement à un bras.



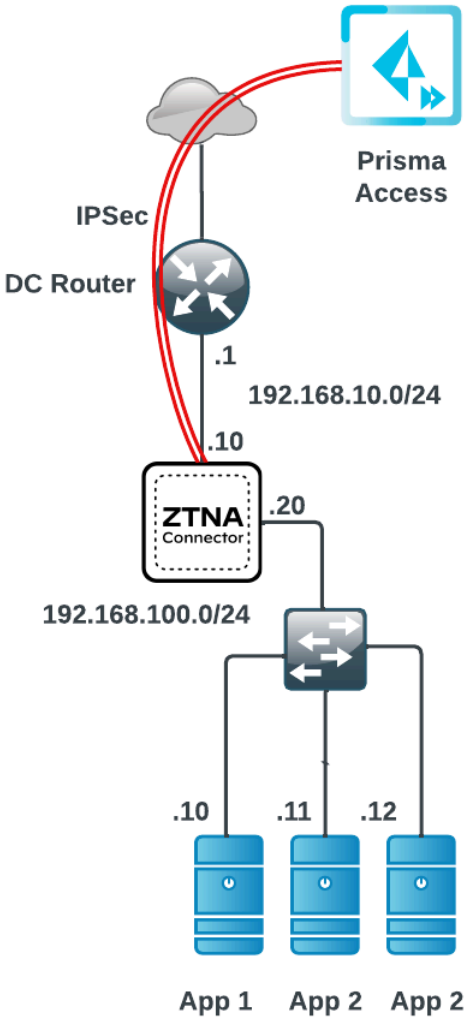
 ©2025 Palo Alto Networks, Inc.

- **Déploiement à deux bras**

  Si vous souhaitez avoir plus de contrôle sur vos règles de sécurité d'entrée et de sortie, ou si vous avez un déploiement de VM sur site, vous pouvez utiliser un déploiement à deux bras, avec une interface sur Internet et l'autre sur le centre de données.

  > *Lors de la configuration des adresses IP sur un connecteur à deux bras, vérifiez que vous avez correctement configuré les attributions d'adresses IP pour le connecteur ZTNA avant de lancer la machine virtuelle. Par exemple, l'exemple de diagramme suivant utilise les adresses IP 192.168.10.10 et 192.168.10.20. En prenant ces exemples d'adresses, configurez les ports du connecteur ZTNA sur 192.168.10.10 et 192.168.100.20, sinon Prisma Access ne pourra pas accéder aux applications du centre de données via le connecteur ZTNA. Les adresses IP 192.168.10.10 et 192.168.100.20 sont des exemples et vous n'êtes pas obligé de les utiliser pour que votre déploiement fonctionne.*

  Le diagramme suivant montre l'exemple d'un déploiement réseau du connecteur ZTNA utilisant un déploiement à deux bras.

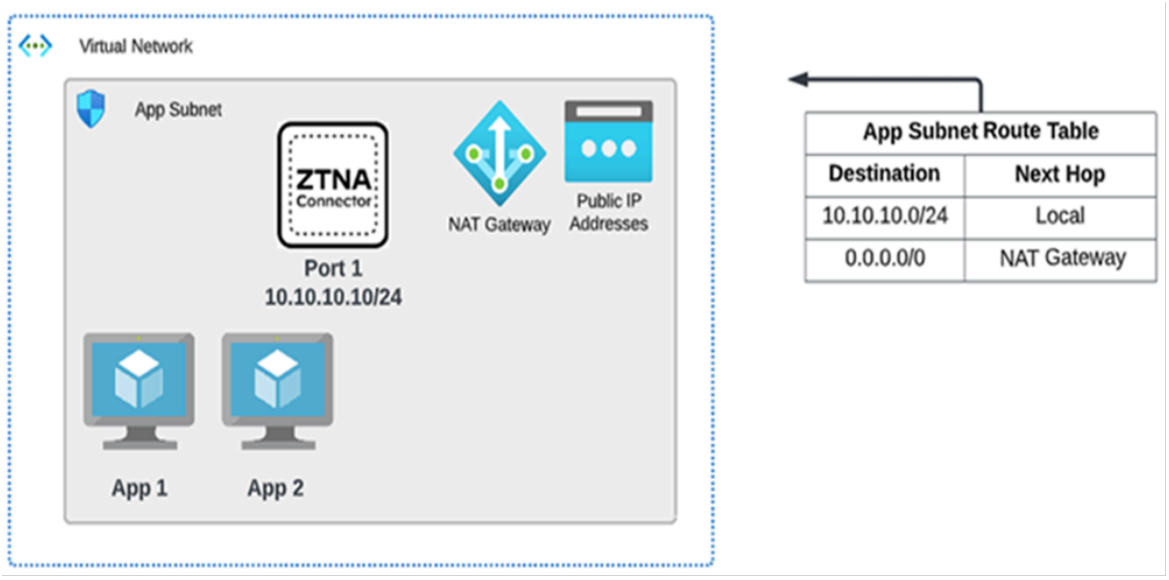


 ©2025 Palo Alto Networks, Inc.

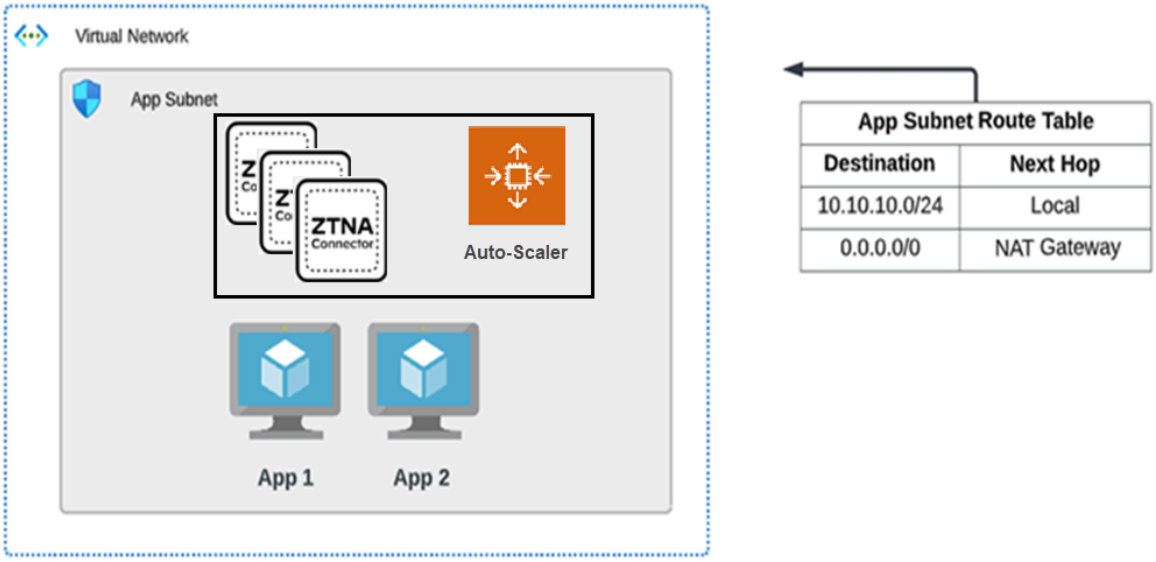
Déploiements Microsoft Azure pris en charge par le connecteur ZTNA

Le déploiement réseau du connecteur ZTNA Prisma Access dans Microsoft Azure prend en charge deux déploiements et un modèle correspondant pour chaque déploiement.

Le diagramme suivant montre un exemple de déploiement du connecteur ZTNA Prisma Access dans Azure à l'aide du mode à un bras avec une passerelle NAT.

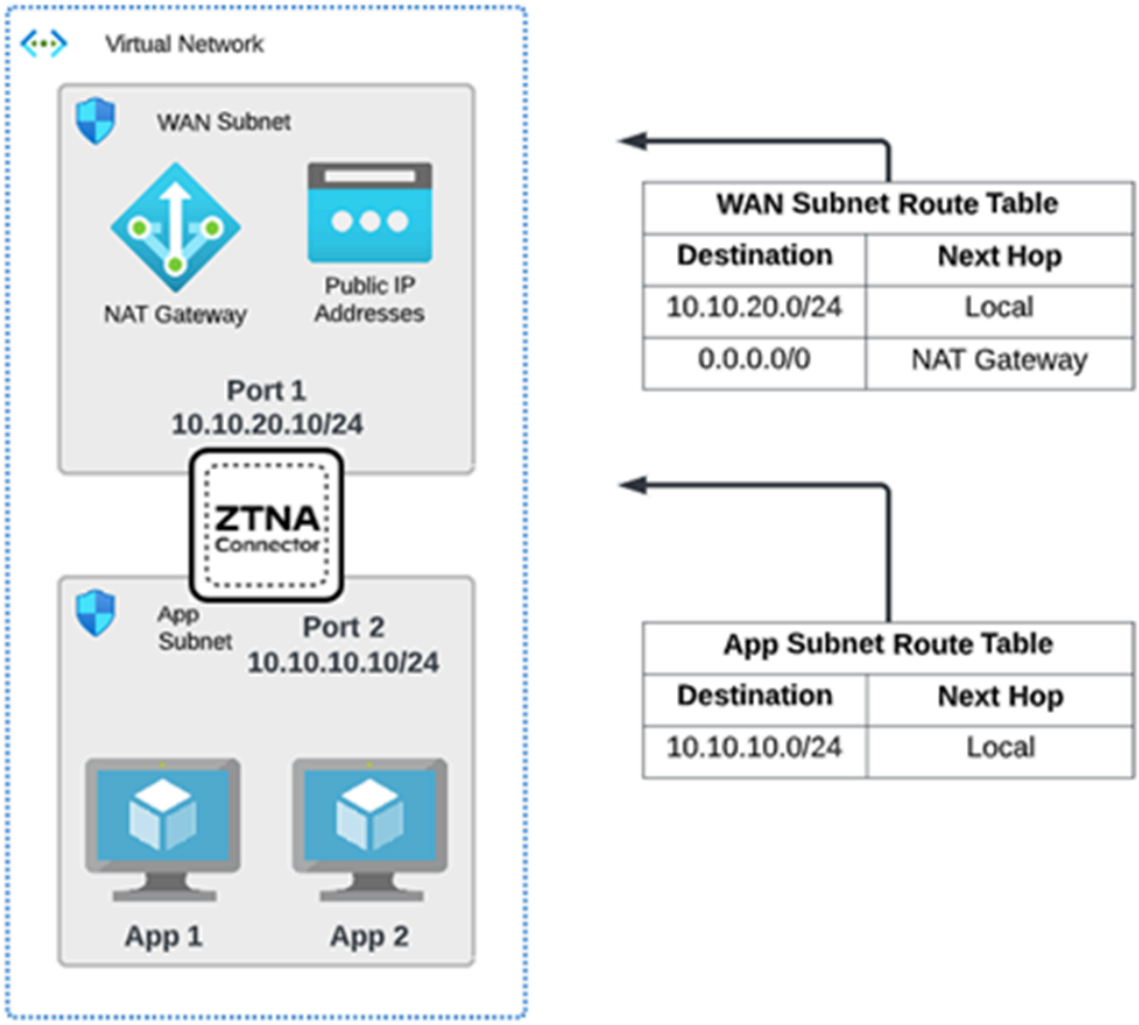


Le diagramme suivant montre un exemple de déploiement du connecteur ZTNA dans AWS à l'aide d'une mise à l'échelle automatique à un bras avec une passerelle NAT.



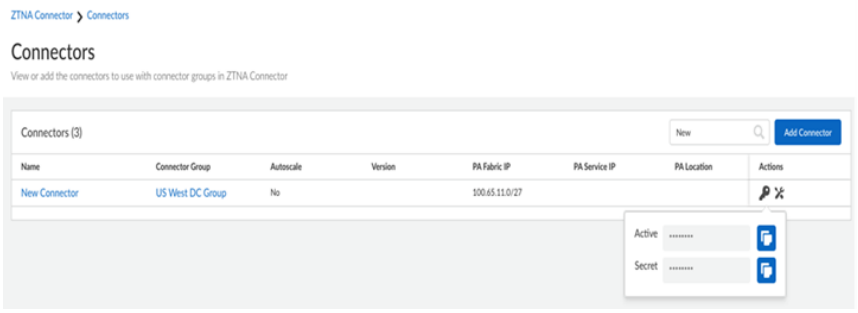
Le diagramme suivant montre un exemple de déploiement du connecteur ZTNA Prisma Access dans Azure à l'aide du mode à deux bras avec une passerelle NAT.

 ©2025 Palo Alto Networks, Inc.



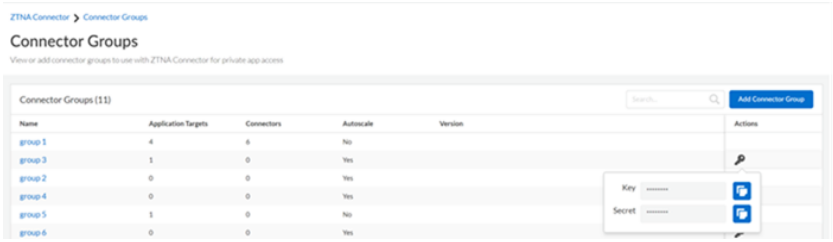
Intégrer un connecteur ZTNA dans Microsoft Azure

- Passez en revue les Exigences et directives et le FQDN et les ports que vous devez configurer pour utiliser le connecteur ZTNA dans Microsoft Azure.
- Sur la plateforme Prisma SASE, récupérez et copiez les valeurs de la clé et du secret du connecteur : **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)**, recherchez l'objet Connecteur que vous avez créé dans Prisma Access pour l'associer à cette VM, puis sélectionnez **Copy Token (Copier le jeton)**. Ensuite, copiez les valeurs **Key (Clé)** et **Secret**.



 ©2025 Palo Alto Networks, Inc.

- Pour le déploiement de **la mise à l'échelle automatique du connecteur ZTNA Prisma Access à un bras**, vous devez récupérer et copier les valeurs de la clé et du secret du groupe de connecteurs : **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connector Groups (Groupes de connecteurs)**, recherchez l'objet Groupe de connecteurs que vous avez créé dans Prisma Access pour l'associer à cette VM, puis sélectionnez **Copy Token (Copier le jeton)**. Ensuite, copiez les valeurs **Clé** et **Secret**.



Une fois que vous avez rempli toutes les conditions préalables, suivez ces étapes pour intégrer un connecteur ZTNA dans Microsoft Azure.

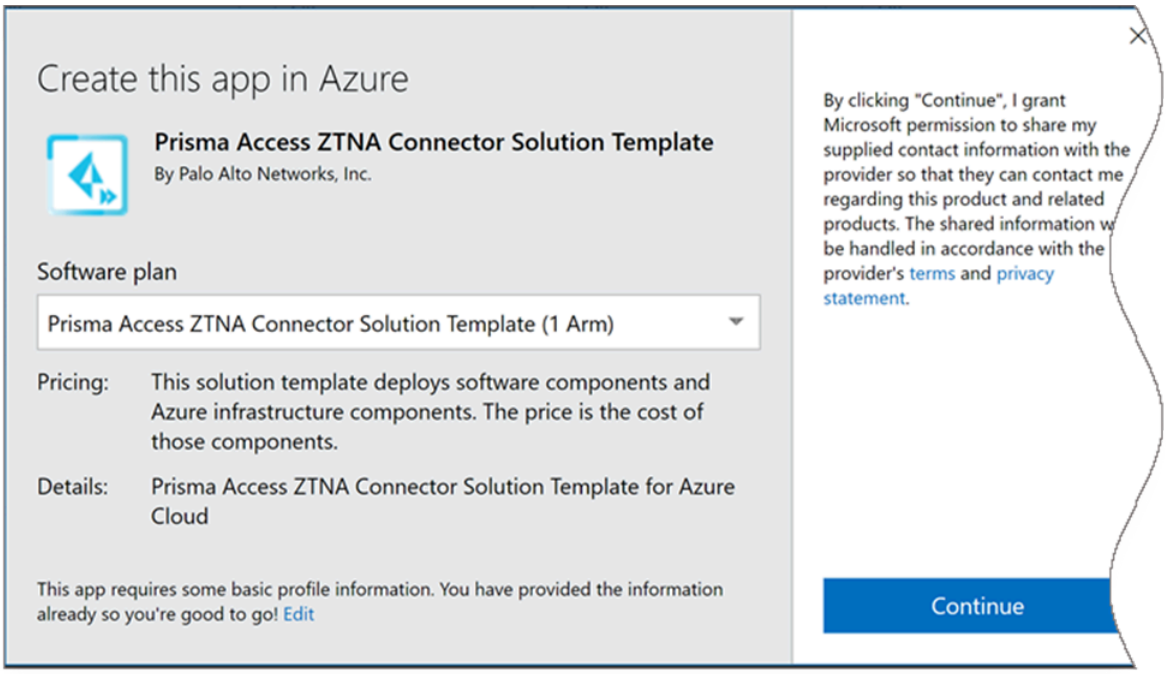
STEP 1 | Connectez-vous à Azure Marketplace et recherchez le **Prisma Access ZTNA Connector (Connecteur ZTNA Prisma Access)**.

STEP 2 | Cliquez sur **Get Now (Obtenir maintenant)**.



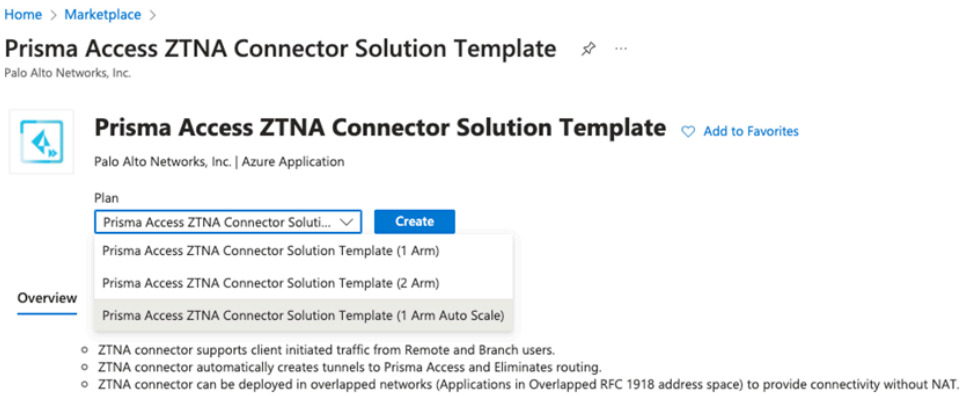
 ©2025 Palo Alto Networks, Inc.

STEP 3 | **Continue (Continuez)** le processus de création.



STEP 4 | Choisissez le plan logiciel et cliquez sur **Create (Créer)** pour créer cette application dans Azure :

- Modèle de solution de connecteur ZTNA Prisma Access (1 bras)
- Déployer le connecteur ZTNA à un bras avec mise à l'échelle automatique dans Microsoft Azure
- Modèle de solution de connecteur ZTNA Prisma Access (2 bras)



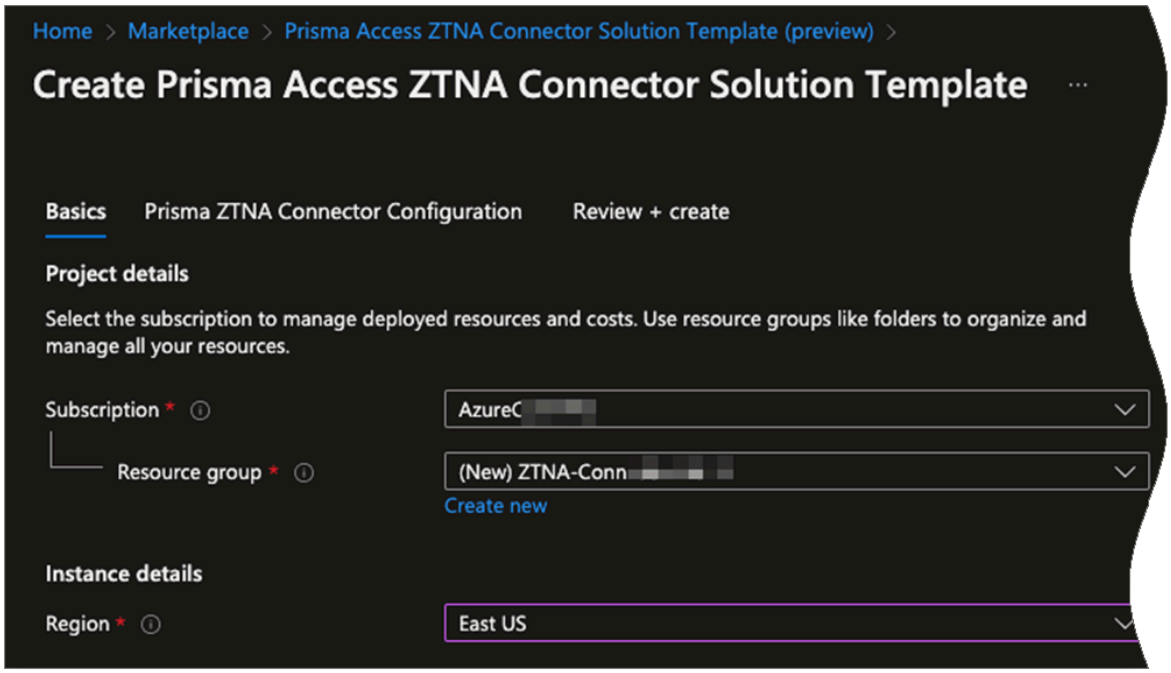
Déployer le connecteur ZTNA à un bras dans Microsoft Azure

Suivez les étapes suivantes pour déployer le connecteur ZTNA à un bras dans Microsoft Azure :

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Configurez les éléments suivants dans l'onglet **Basics (Bases)** :

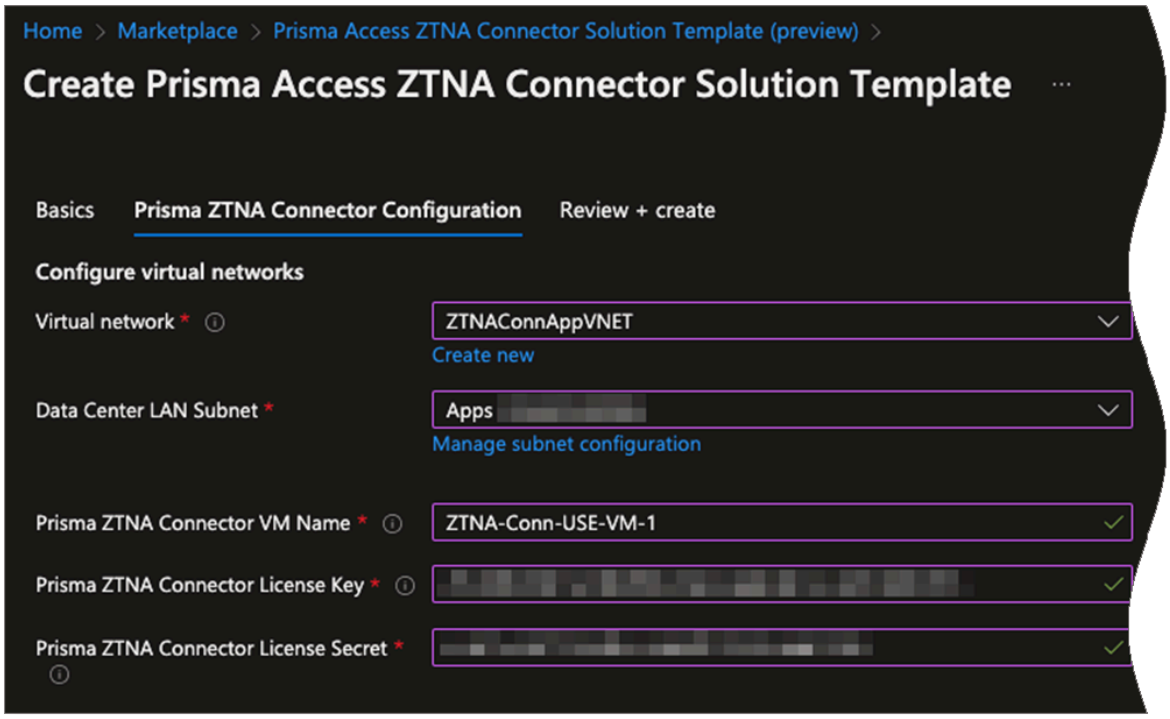
- Sélectionnez votre **Subscription (Abonnement)** Azure pour gérer les ressources déployées.
- Sélectionnez un **Resource Group (Groupe de ressources)** existant ou cliquez sur **Create New (Créer un nouveau)** pour en créer un.
- Sélectionnez une **Region (Région)** Azure adaptée à votre emplacement.
- Cliquez sur **Next: Prisma ZTNA Connector Configuration (Suivant : configuration du connecteur ZTNA Prisma)**.



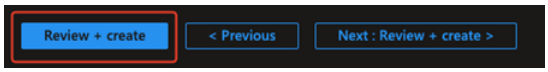
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configurez un réseau virtuel dans l'onglet **Prisma ZTNA Connector Configuration (Configuration du connecteur ZTNA Prisma)** :

- Créez un réseau virtuel ou sélectionnez un **Virtual network (Réseau virtuel)** existant.
- Sélectionnez le **Data Center LAN Subnet (Sous-réseau LAN du centre de données)** dans lequel vous avez provisionné des applications à intégrer à ce connecteur.
- Saisissez le **Prisma ZTNA Connector VM Name (Nom de la VM du connecteur ZTNA Prisma)**.
- Saisissez les valeurs de **Prisma ZTNA Connector License Key (Clé de licence du connecteur ZTNA Prisma)** et de **Prisma ZTNA Connector License Secret (Secret de la licence du connecteur ZTNA Prisma)** que vous avez récupérées à partir du portail Prisma SASE.



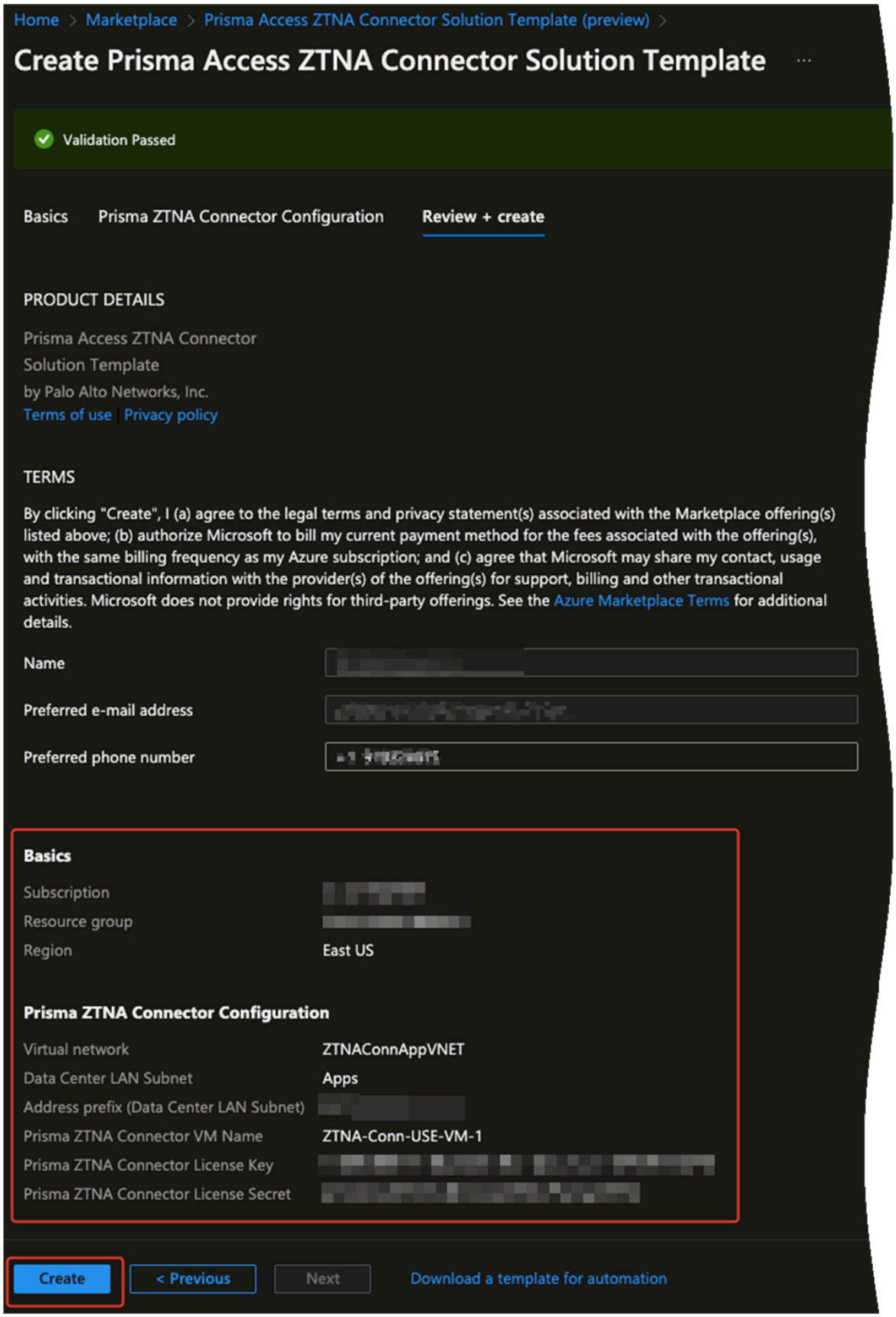
- Cliquez sur **Review + create (Examiner et créer)** pour examiner la configuration de votre connecteur ZTNA Prisma géré.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Confirmez les détails que vous avez fournis et cliquez sur **Create (Créer)** pour démarrer le déploiement de la machine virtuelle.

 ©2025 Palo Alto Networks, Inc.



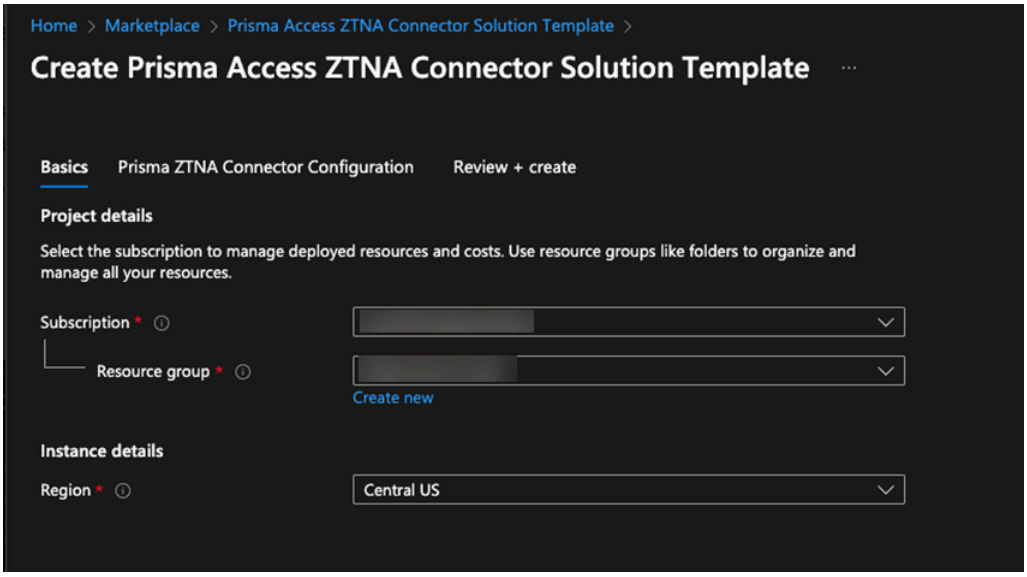
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Une fois le déploiement terminé, sélectionnez **Go to resource (Accéder à la ressource)**.

Déployer le connecteur ZTNA à un bras avec mise à l'échelle automatique dans Microsoft Azure

STEP 1 | Configurez les éléments suivants dans l'onglet **Basics (Bases)** :

- Sélectionnez votre **Subscription (Abonnement)** Azure pour gérer les ressources déployées.
- Sélectionnez un **Resource Group (Groupe de ressources)** existant ou cliquez sur **Create New (Créer un nouveau)** pour en créer un.
- Sélectionnez une **Region (Région)** Azure adaptée à votre emplacement.
- Cliquez sur **Next: Prisma ZTNA Connector Configuration (Suivant : configuration du connecteur ZTNA Prisma)**.



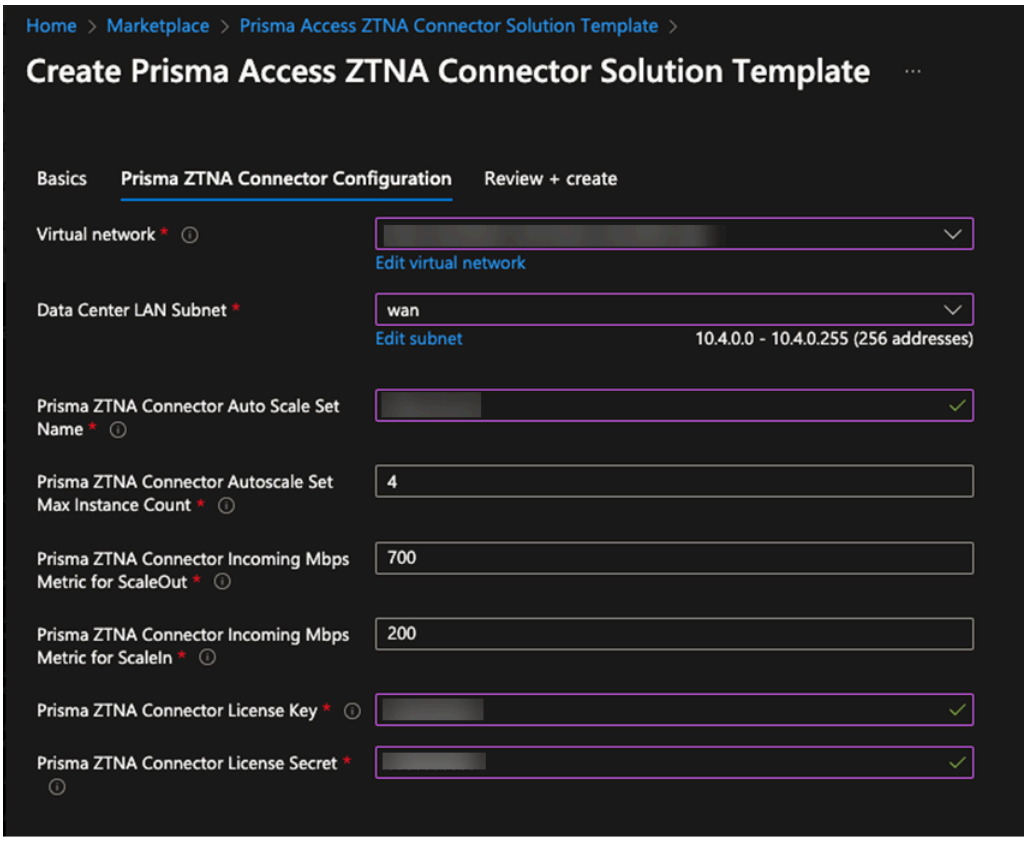
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configurez un réseau virtuel dans l'onglet **Next: Prisma ZTNA Connector Configuration (Suivant : configuration du connecteur ZTNA Prisma)** :

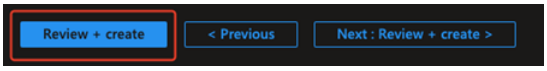
- Créez un **Virtual network (Réseau virtuel)** ou sélectionnez un **Virtual network (Réseau virtuel)** existant.
- Sélectionnez le **Data Center LAN Subnet (Sous-réseau LAN du centre de données)** dans lequel vous avez provisionné des applications à intégrer à ce connecteur.
- Saisissez le **Prisma ZTNA Connector Auto Scale Set Name (Nom défini pour la mise à l'échelle automatique du connecteur ZTNA Prisma)**, en spécifiant le nom de l'ensemble d'échelles créé dans Azure.
- Saisissez le **Prisma ZTNA Connector Autoscale Set Max Instance Count (Nombre maximal d'instances défini pour la mise à l'échelle automatique du connecteur ZTNA)**. Le nombre maximal de connecteurs ZTNA autorisés dans le groupe de connecteurs est de 4.
- Saisissez la **Prisma ZTNA Connector Incoming Mbps Metric for ScaleOut (Métrique des Mbit/s entrants du connecteur ZTNA Prisma pour la mise à l'échelle ascendante)**. Saisissez une valeur comprise entre 100 et 1 000.
- Saisissez la **Prisma ZTNA Connector Incoming Mbps Metric for ScaleIn (Métrique des Mbit/s entrants du connecteur ZTNA Prisma pour la mise à l'échelle descendante)**. Saisissez une valeur comprise entre 1 et 500.
- Saisissez les valeurs de **Prisma ZTNA Connector License Key (Clé de licence du connecteur ZTNA Prisma)** et de **Prisma ZTNA Connector License Secret (Secret de la licence du**

 ©2025 Palo Alto Networks, Inc.

connecteur ZTNA Prisma) que vous avez récupérées à partir du portail Prisma SASE pour le groupe de connecteurs que vous souhaitez intégrer au connecteur.

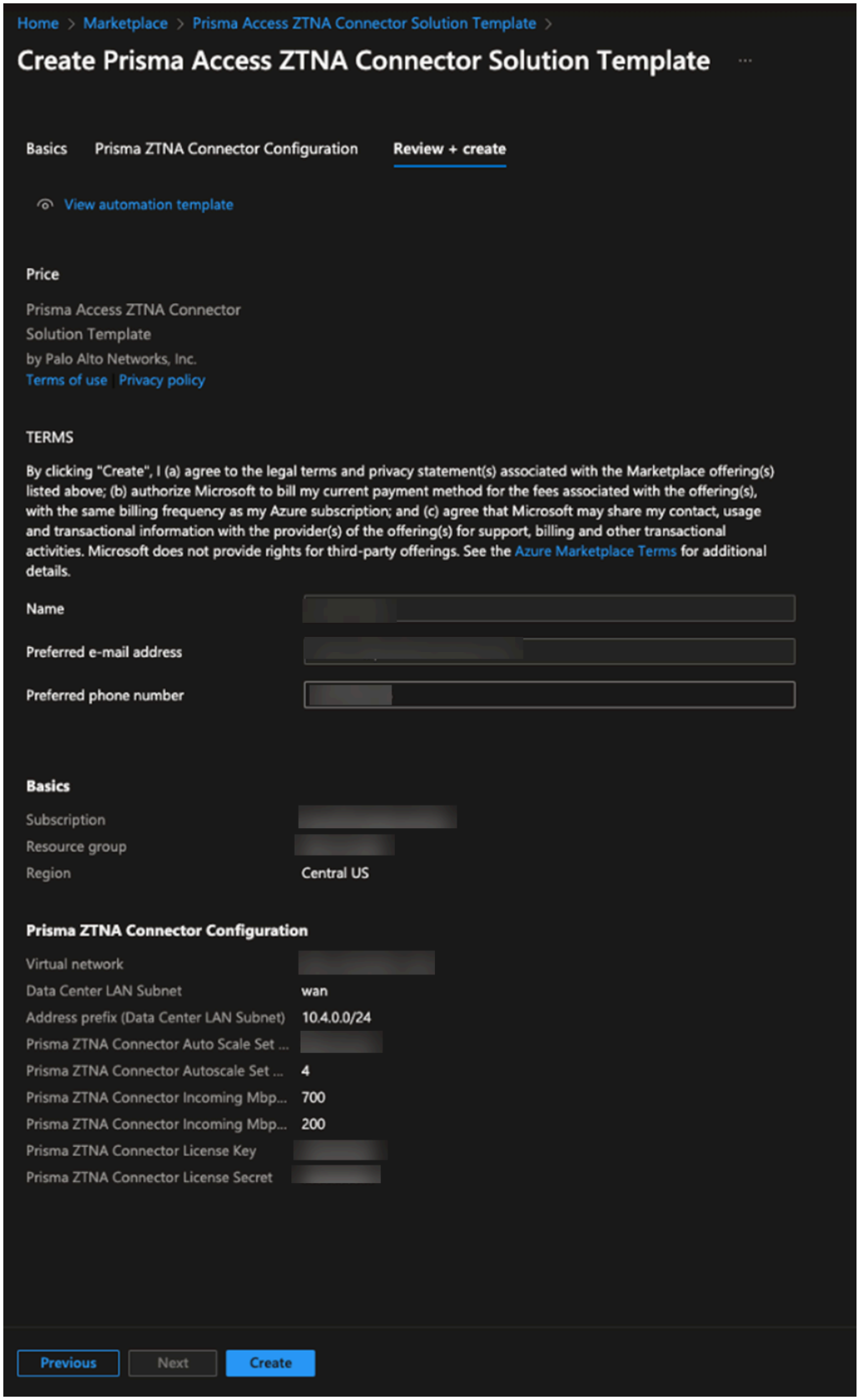


- Cliquez sur **Review + create (Examiner et créer)** pour examiner la configuration de votre connecteur ZTNA Prisma géré.



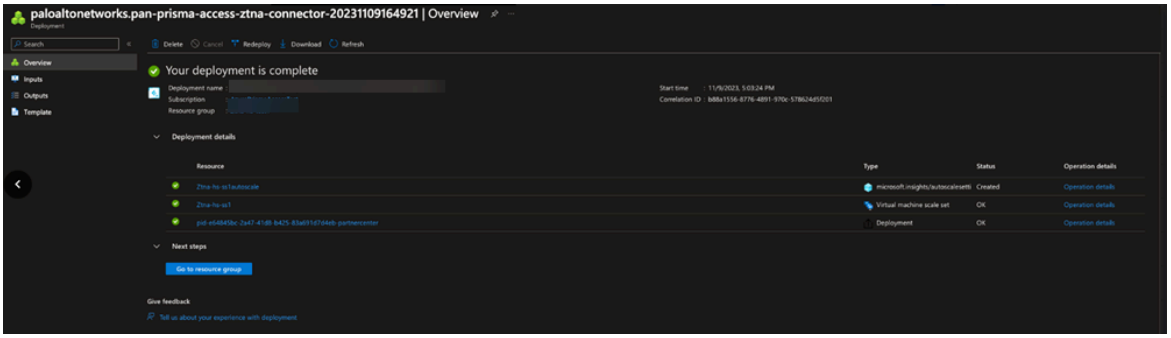
 ©2025 Palo Alto Networks, Inc.

STEP 3 | Confirmez les détails que vous avez fournis et cliquez sur **Create (Créer)** pour démarrer le déploiement de la machine virtuelle.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Une fois le déploiement terminé, sélectionnez **Go to resource group (Accéder au groupe de ressources)**.

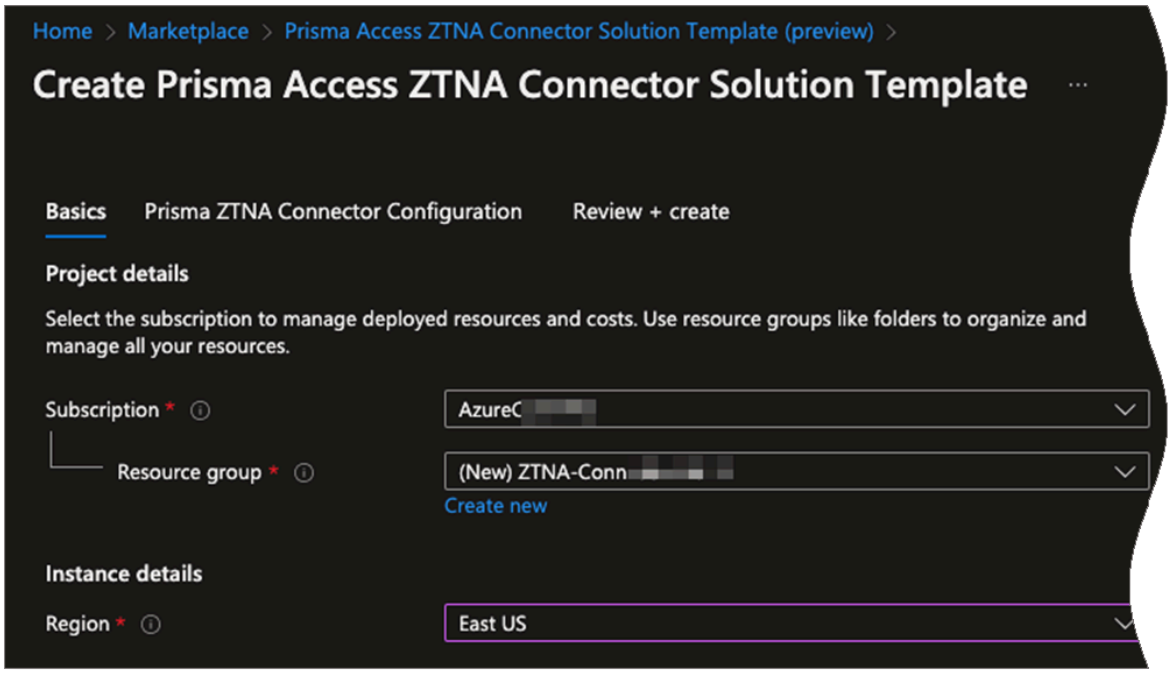


Déployer le connecteur ZTNA à deux bras dans Microsoft Azure

Suivez les étapes suivantes pour déployer le connecteur ZTNA à deux bras dans Microsoft Azure :

STEP 1 | Configurez les éléments suivants dans l'onglet **Basics (Bases)** :

- Sélectionnez votre **Subscription (Abonnement)** Azure pour gérer les ressources déployées.
- Sélectionnez un **Resource Group (Groupe de ressources)** existant ou cliquez sur **Create New (Créer un nouveau)** pour en créer un.
- Sélectionnez une **Region (Région)** Azure adaptée à votre emplacement.
- Cliquez sur **Next: Prisma ZTNA Connector Configuration (Suivant : configuration du connecteur ZTNA Prisma)**.

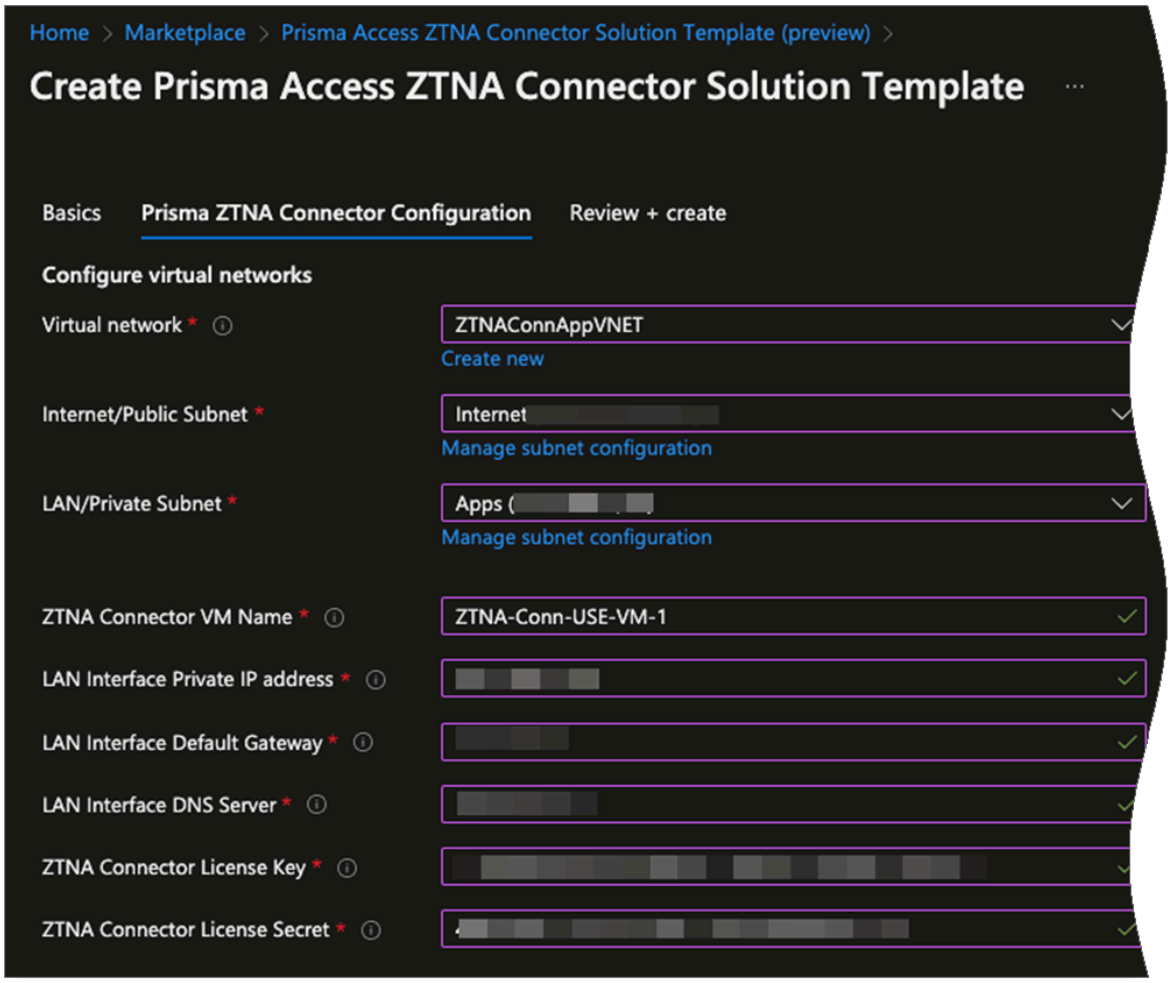


 ©2025 Palo Alto Networks, Inc.

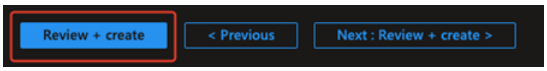
STEP 2 | Configurez un réseau virtuel dans l'onglet **Next: Prisma ZTNA Connector Configuration (Suivant : configuration du connecteur ZTNA Prisma)** :

- Créez un **Virtual network (Réseau virtuel)** ou utilisez un **Virtual network (Réseau virtuel)** existant.
- Sélectionnez le **Internet/Public Subnet (Sous-réseau Internet/public)** pour la connectivité WAN à IPSec. Vous devez associer le sous-réseau à une passerelle NAT pour la connectivité Internet.
- Sélectionnez le **Data Center LAN Subnet (Sous-réseau LAN du centre de données)** dans lequel vous avez provisionné les applications à intégrer à ce connecteur.
- Saisissez le **Prisma ZTNA Connector VM Name (Nom de la VM du connecteur ZTNA Prisma)**.
- Saisissez **LAN Interface Private IP address (Adresse IP privée de l'interface LAN)**.
- Saisissez l'adresse IP de **LAN Interface Default Gateway (Passerelle par défaut de l'interface LAN)**.
- Saisissez l'adresse IP du **LAN Interface DNS Server (Serveur DNS de l'interface LAN)**.
- Saisissez les valeurs de **Prisma ZTNA Connector License Key (Clé de licence du connecteur ZTNA Prisma)** et de **Prisma ZTNA Connector License Secret (Secret de la licence du connecteur ZTNA Prisma)** que vous avez récupérées à partir du portail Prisma SASE.

 ©2025 Palo Alto Networks, Inc.



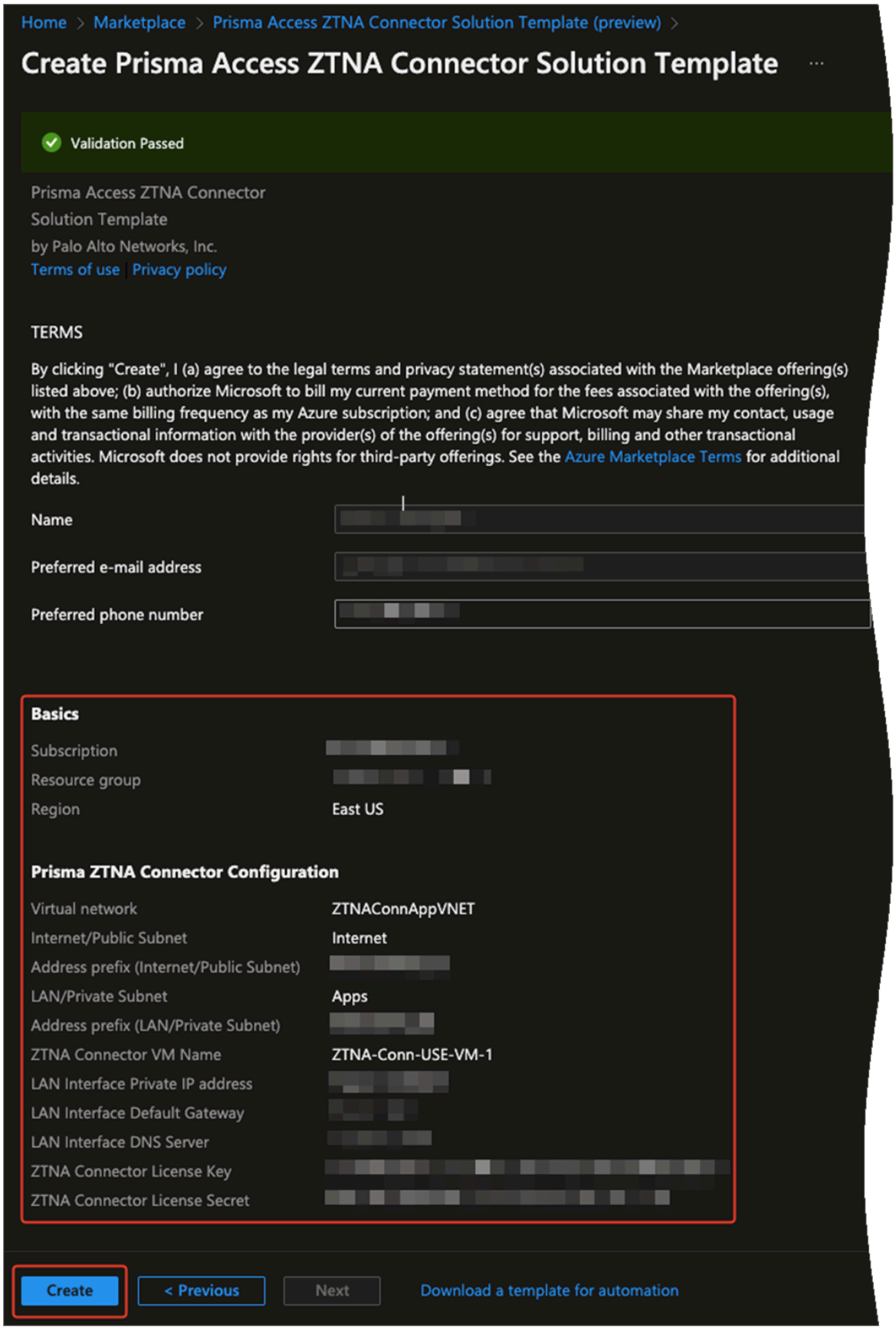
- Cliquez sur **Review + create (Examiner et créer)** pour examiner la configuration de votre connecteur ZTNA Prisma géré.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Confirmez les détails que vous avez fournis et cliquez sur **Create (Créer)** pour démarrer le déploiement de la machine virtuelle.

 ©2025 Palo Alto Networks, Inc.



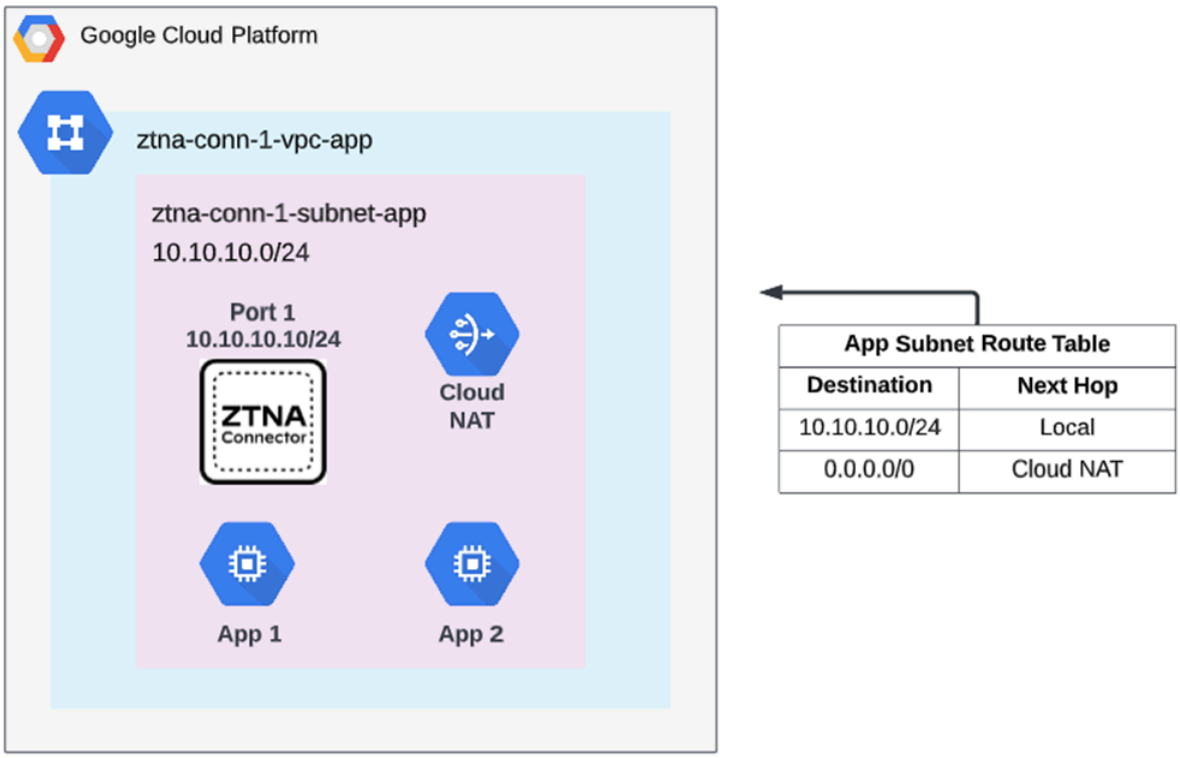
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Une fois le déploiement terminé, sélectionnez **Go to resource (Accéder à la ressource)**.

Déploiements de Google Cloud Platform pris en charge par le connecteur ZTNA

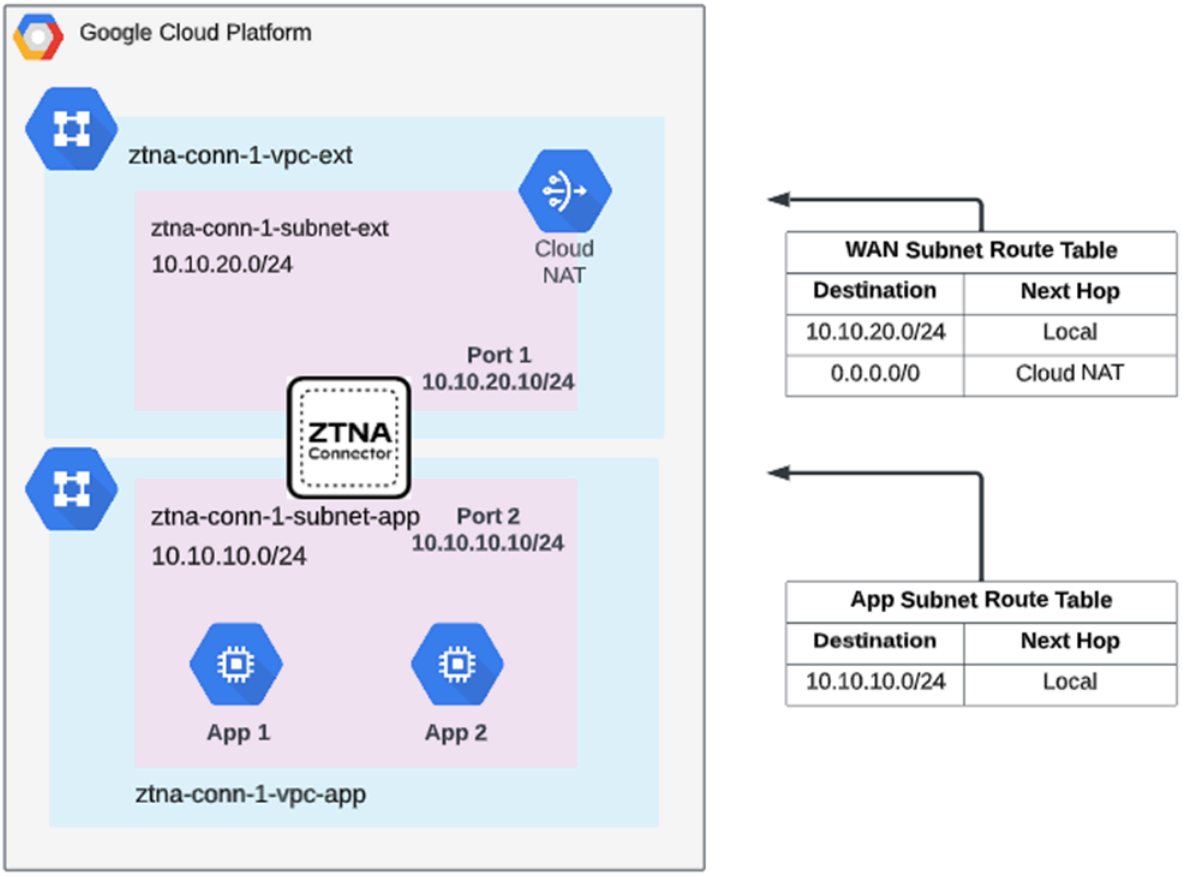
Le déploiement de réseau via le connecteur ZTNA de Prisma Access dans Google Cloud Platform (GCP) prend en charge deux déploiements et un modèle correspondant pour chaque déploiement.

Le diagramme suivant montre un exemple de déploiement via le connecteur ZTNA de Prisma Access dans GCP à l'aide du mode one-arm avec une passerelle NAT.



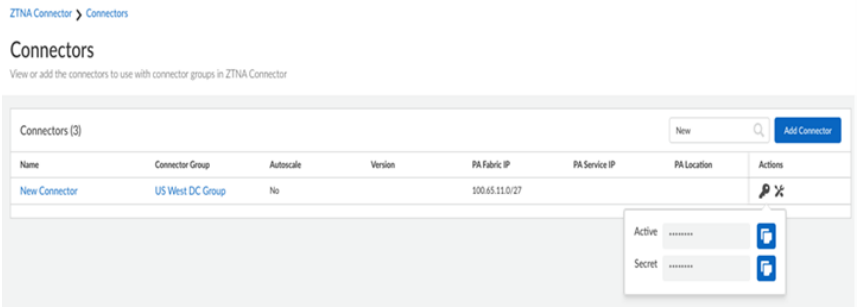
Le diagramme suivant montre un exemple de déploiement via le connecteur ZTNA de Prisma Access dans GCP à l'aide du mode two-arm avec une passerelle NAT.

 ©2025 Palo Alto Networks, Inc.



Intégrer un connecteur ZTNA dans Google Cloud Platform

- Passez en revue les Exigences et directives et le FQDN et les ports que vous devez configurer pour utiliser le connecteur ZTNA Prisma Access dans Google Cloud Platform (GCP).
- Récupérez et copiez les valeurs de la clé et du secret du Connecteur sur le portail Prisma SASE : **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)**, recherchez l'objet Connecteur que vous avez créé dans Prisma Access pour l'associer à cette VM, puis sélectionnez **Copy Token (Copier le jeton)**. Ensuite, copiez les valeurs **Key (Clé)** et **Secret**.



Une fois que vous avez rempli toutes les conditions préalables, suivez ces étapes pour intégrer un Connecteur ZTNA Prisma Access dans GCP.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Accédez à GCP Marketplace et recherchez le **Prisma Access ZTNA Connector (Connecteur ZTNA Prisma Access)**.

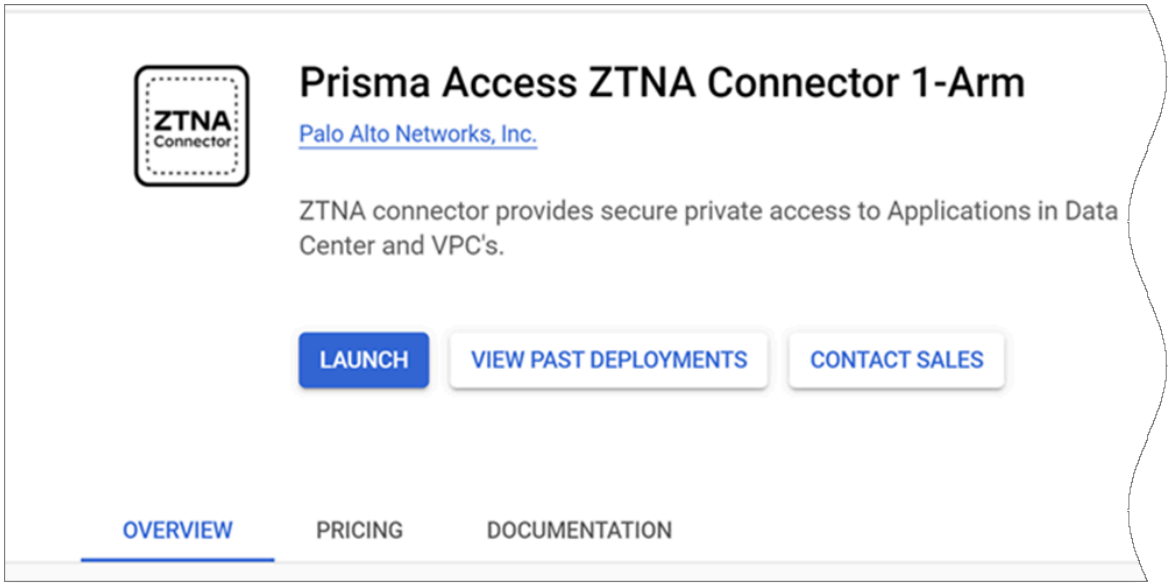
STEP 2 | Choisissez le plan logiciel qui répond le mieux à vos besoins.

- Connecteur ZTNA Prisma Access à un bras
- Connecteur ZTNA Prisma Access à deux bras

Déployer le connecteur ZTNA à un bras dans GCP

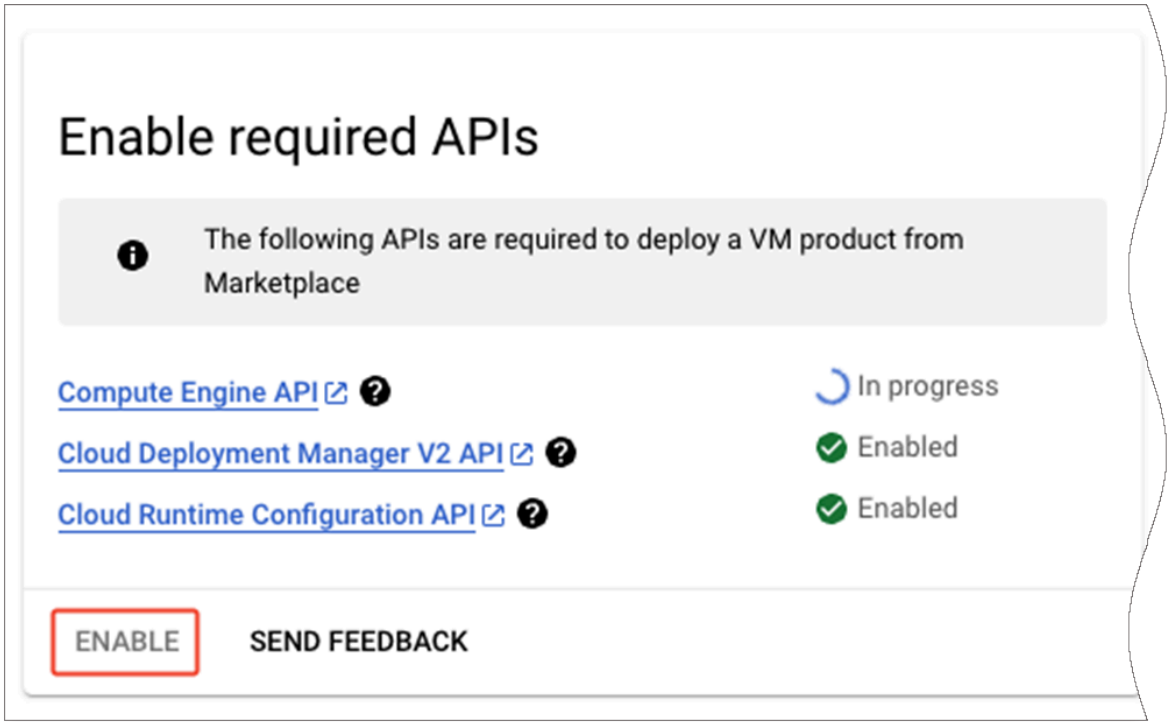
Suivez les étapes suivantes pour déployer le connecteur ZTNA à un bras dans GCP.

STEP 1 | Cliquez sur **LAUNCH (DÉMARRER)** pour configurer le connecteur ZTNA à un bras.



 ©2025 Palo Alto Networks, Inc.

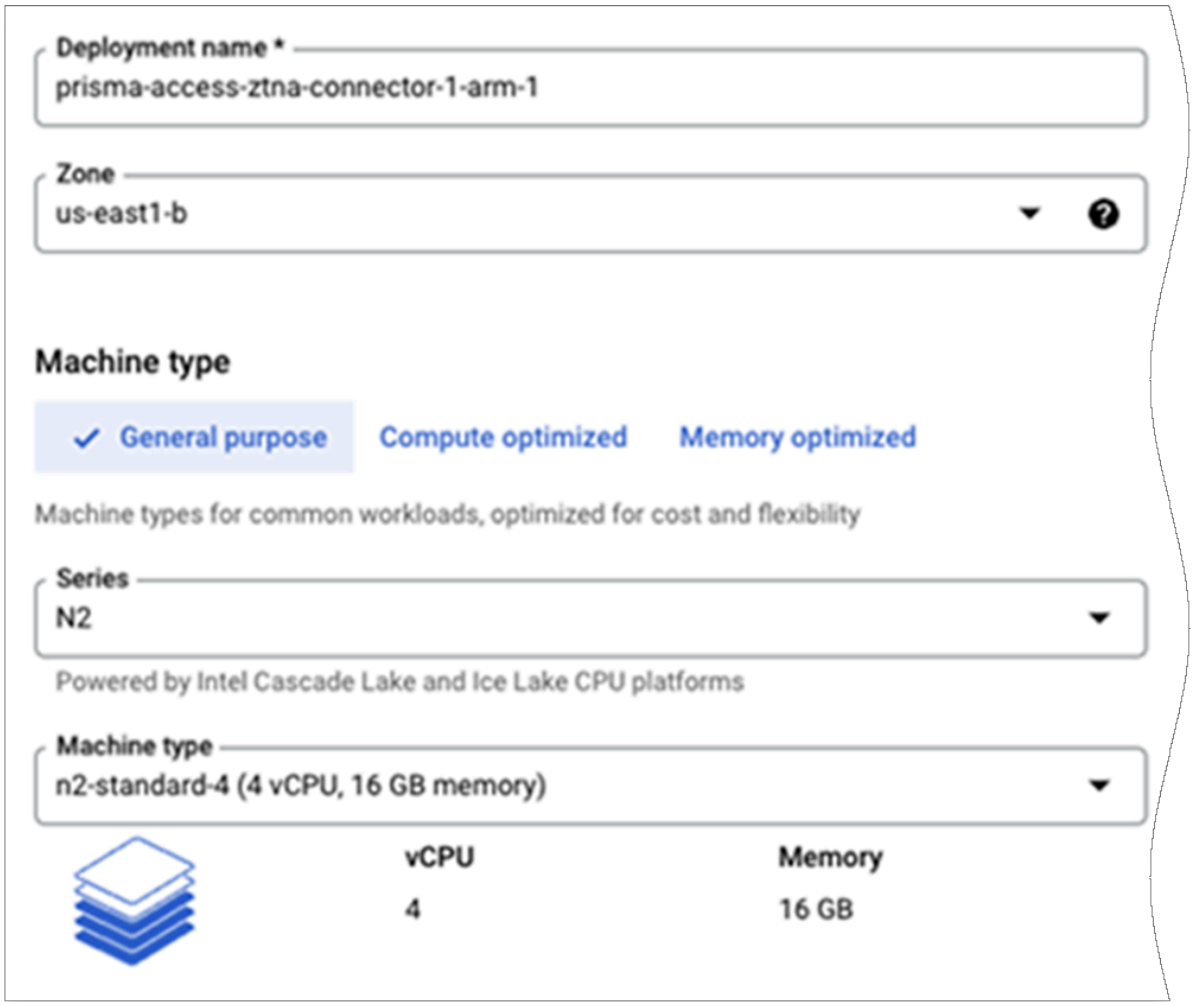
STEP 2 | (Facultatif) Cliquez sur **Enable (Activer)** pour activer les API du GCP nécessaires pour déployer une machine virtuelle depuis le marketplace.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configurez les paramètres suivants :

- Saisissez le **Deployment Name (Nom de déploiement)** qui vous permet d'identifier votre machine virtuelle.
- Sélectionnez la **Zone** où se trouvent les applications pour ce connecteur.
- Utilisez la valeur par défaut pour le **Machine Type (Type de machine)**. Le type de machine qualifié pour ce connecteur est **n2-standard-4**.



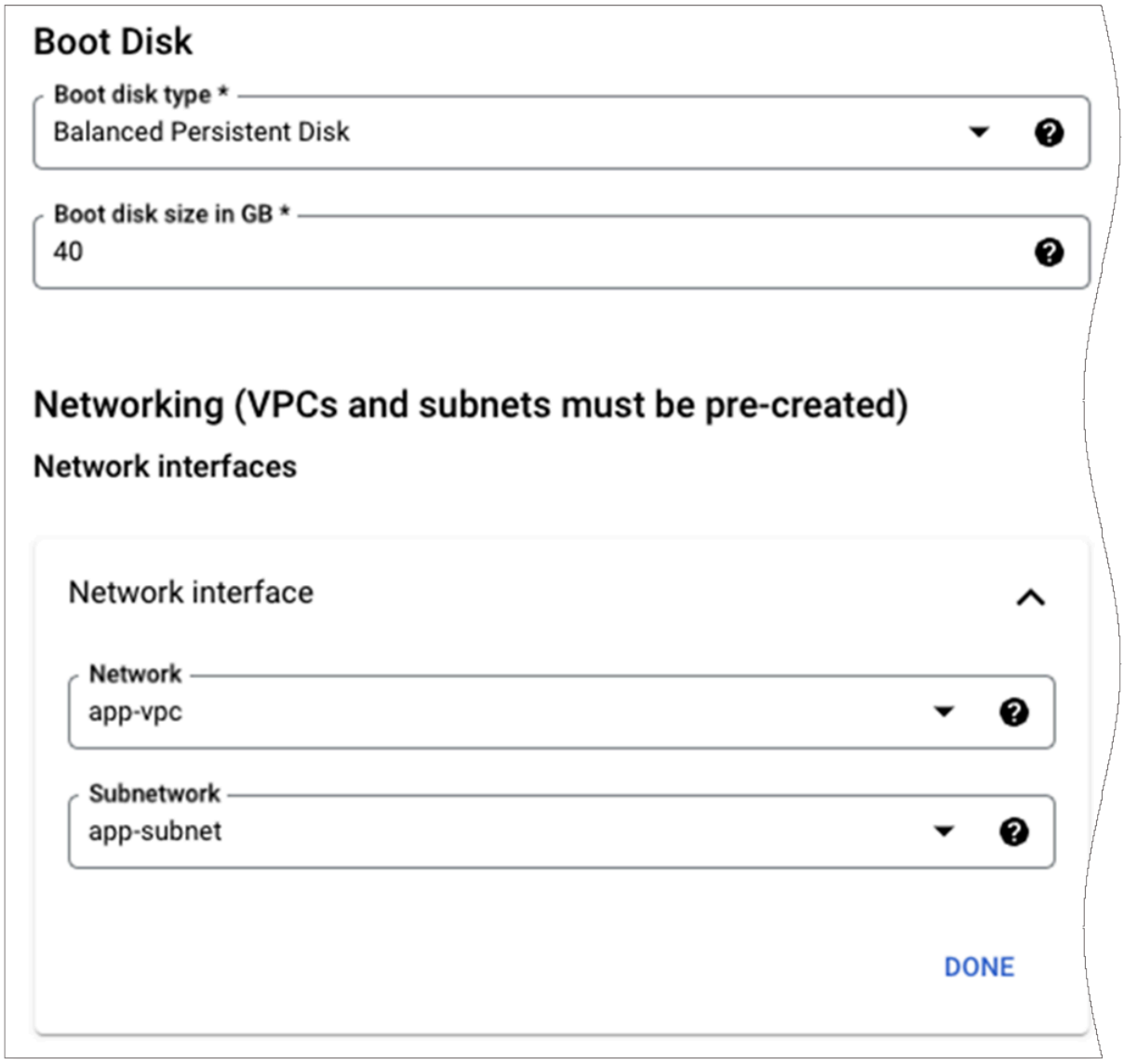
- Saisissez les valeurs de **Prisma ZTNA Connector License Key (Clé de licence du connecteur ZTNA Prisma)** et de **Prisma ZTNA Connector License Secret (Secret de la licence du connecteur ZTNA Prisma)** que vous avez récupérées à partir du portail Prisma SASE.

©2025 Palo Alto Networks, Inc.



- Configurez les éléments suivants dans la section **Boot Disk (Disque de démarrage)** :
  - Utilisez le **Boot disk type (Type de disque de démarrage)** par défaut.
  - Sélectionnez **40 GB (40 Go)** comme**Boot disk size in GB (Taille du disque de démarrage en Go)**.
- Développez la section **Networking (VPCs and subnets must be pre-created) (Réseautage (les VPC et les sous-réseaux doivent être pré-créés))** et sélectionnez les détails de **Network Interface (Interface réseau)**.
  - Sélectionnez le **Network (Réseau)** qui contient le sous-réseau que vous avez créé.
  - Sélectionnez le **Subnetwork (Sous-réseau)** à utiliser par la machine virtuelle.

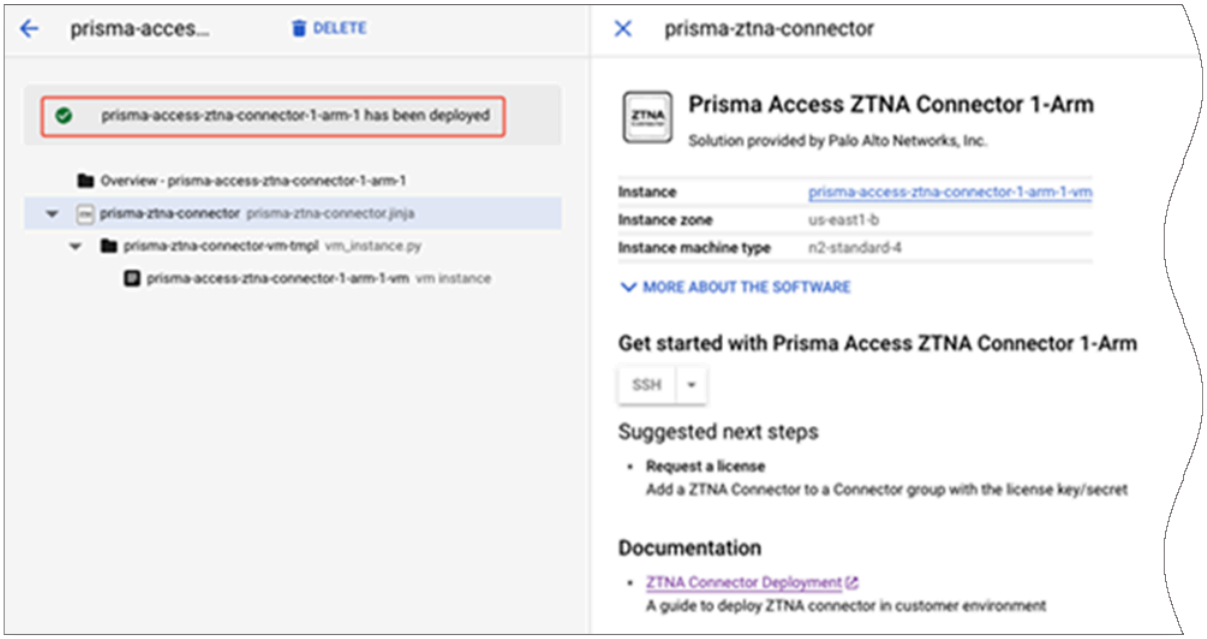
 ©2025 Palo Alto Networks, Inc.



STEP 4 | Cliquez sur **Terminé**.

 ©2025 Palo Alto Networks, Inc.

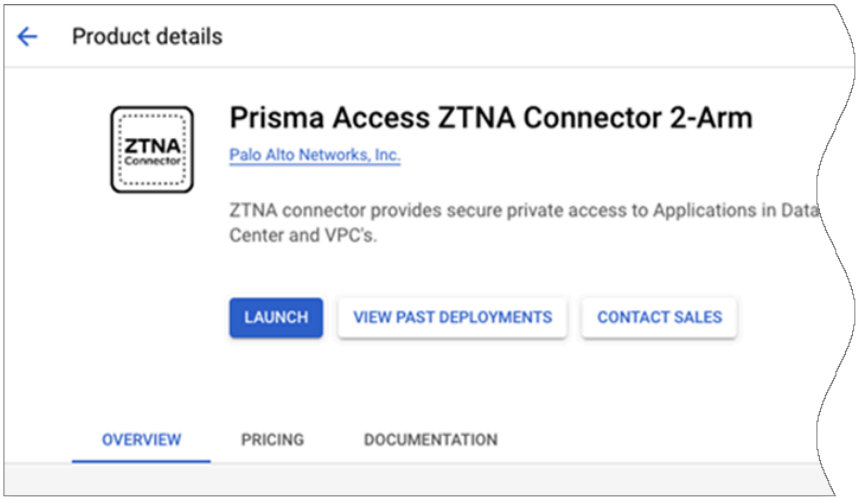
STEP 5 | Cliquez sur **Deploy (Déployer)** pour terminer le processus d'intégration.



Déployer le connecteur ZTNA à deux bras dans GCP

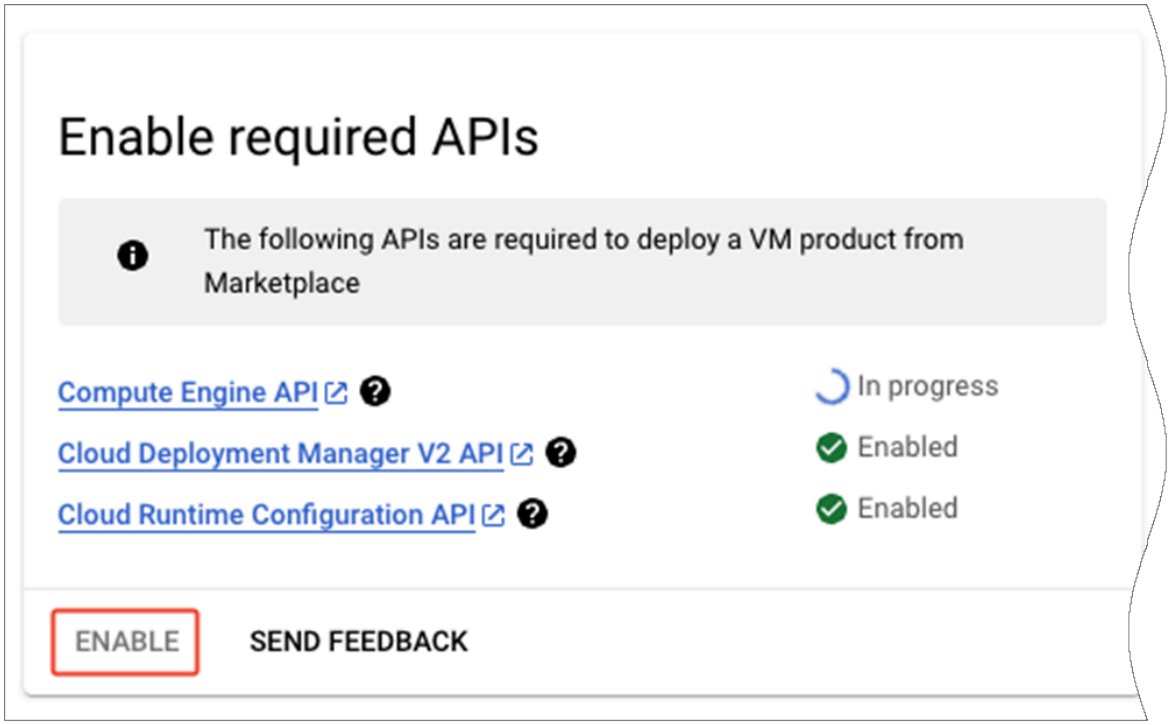
Suivez les étapes suivantes pour déployer le connecteur ZTNA dans GCP.

STEP 1 | Cliquez sur **LAUNCH (DÉMARRER)** pour configurer.



 ©2025 Palo Alto Networks, Inc.

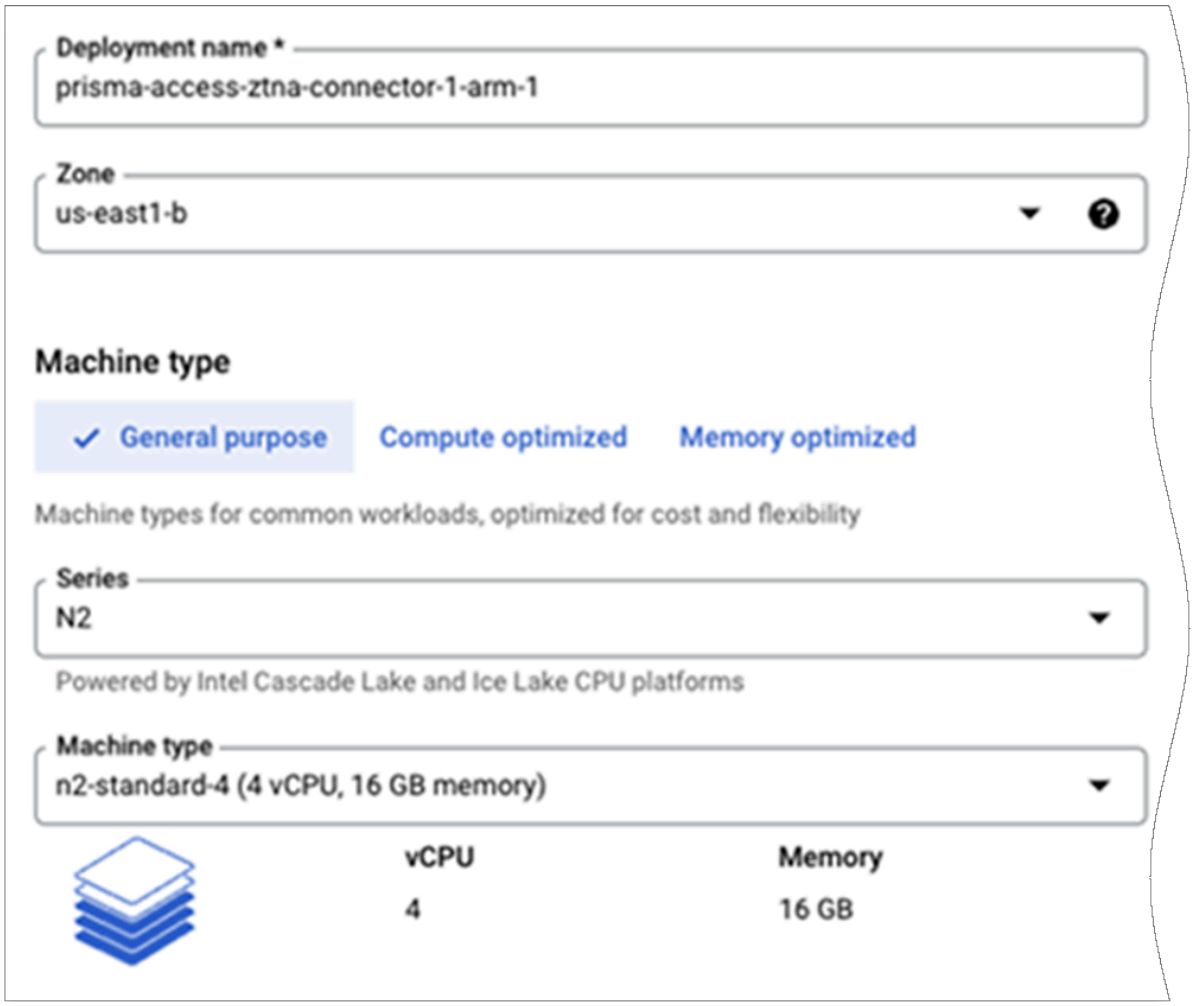
STEP 2 | (Facultatif) Cliquez sur **Enable (Activer)** pour activer les API nécessaires pour déployer une machine virtuelle depuis le marketplace.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configurez les paramètres suivants :

- Saisissez le **Deployment Name (Nom de déploiement)** qui vous permet d'identifier votre machine virtuelle.
- Sélectionnez la **Zone** où se trouvent les applications pour ce connecteur.
- Utilisez la valeur par défaut pour le **Machine Type (Type de machine)**. Le type de machine qualifié pour ce connecteur est **n2-standard-4**.



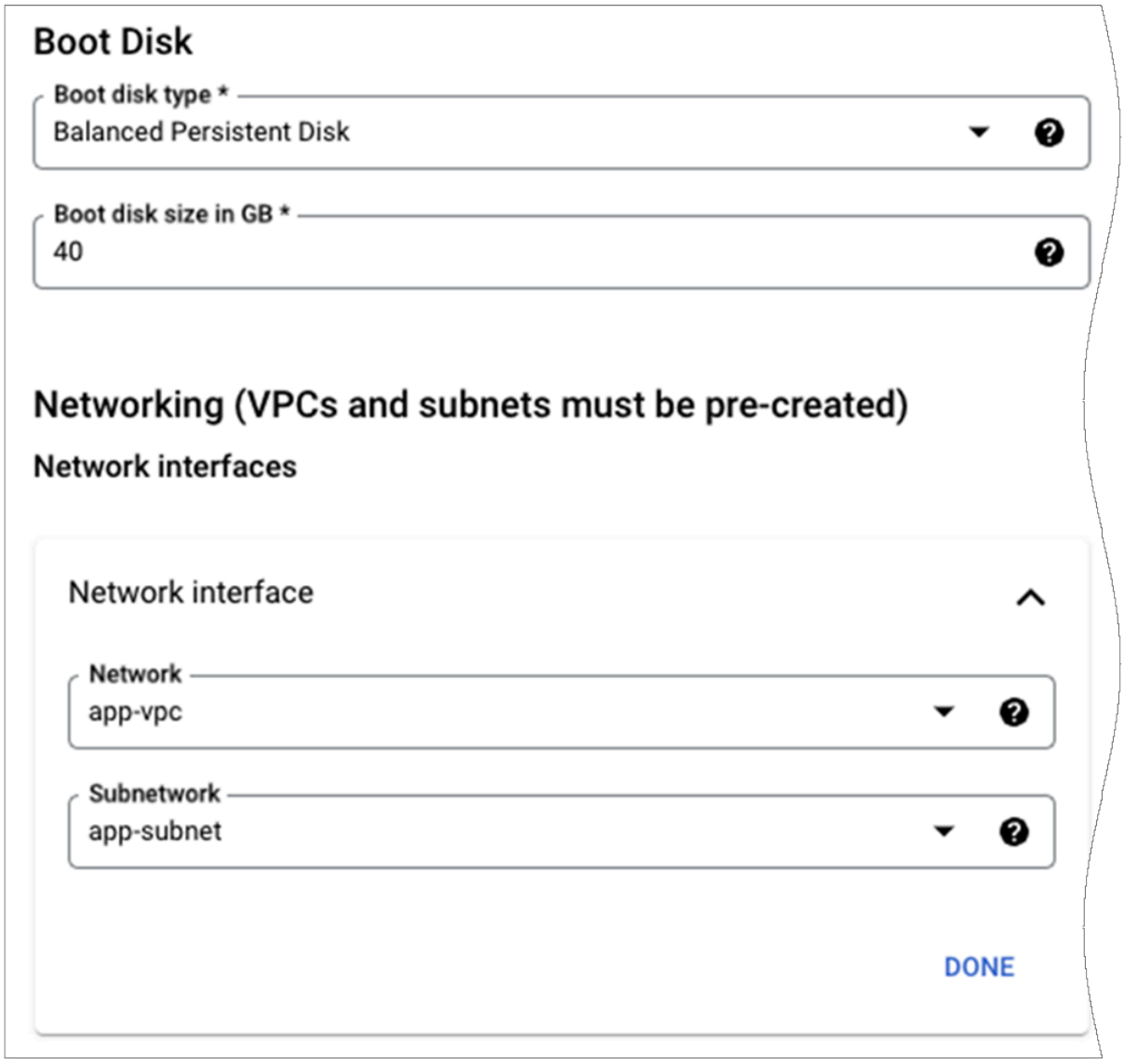
- Saisissez les valeurs de **Prisma ZTNA Connector License Key (Clé de licence du connecteur ZTNA Prisma)** et de **Prisma ZTNA Connector License Secret (Secret de la licence du connecteur ZTNA Prisma)** que vous avez récupérées à partir du portail Prisma SASE.

 ©2025 Palo Alto Networks, Inc.

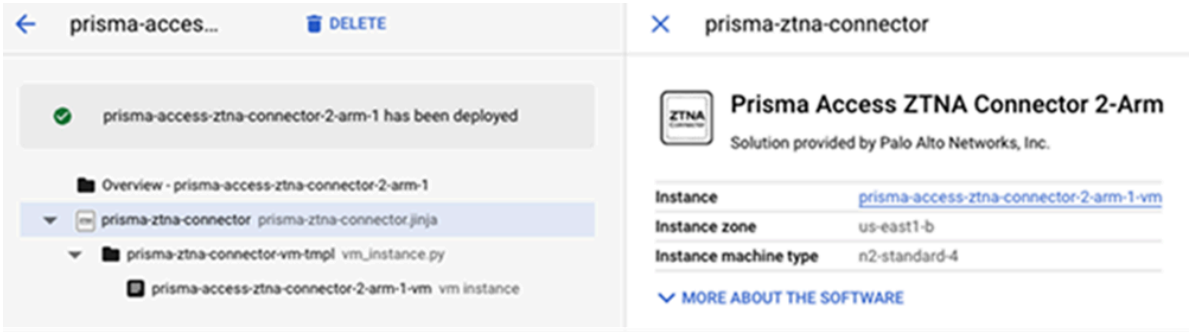


- Dans la section **Boot Disk (Disque de démarrage)** :
  - Utilisez le **Boot disk type (Type de disque de démarrage)** par défaut.
  - Sélectionnez **40 GB (40 Go)** comme**Boot disk size in GB (Taille du disque de démarrage en Go)**.
- Développez la section **Networking (VPCs and subnets must be pre-created) (Réseautage (les VPC et les sous-réseaux doivent être pré-créés))** et sélectionnez les détails de **Network Interface (Interface réseau)**.
  - Sélectionnez le **Network (Réseau)** qui contient le sous-réseau que vous avez créé.
  - Sélectionnez le **Subnetwork (Sous-réseau)** à utiliser par la machine virtuelle.

 ©2025 Palo Alto Networks, Inc.



STEP 4 | Cliquez sur **Deploy (Déployer)** pour terminer le processus d'intégration.

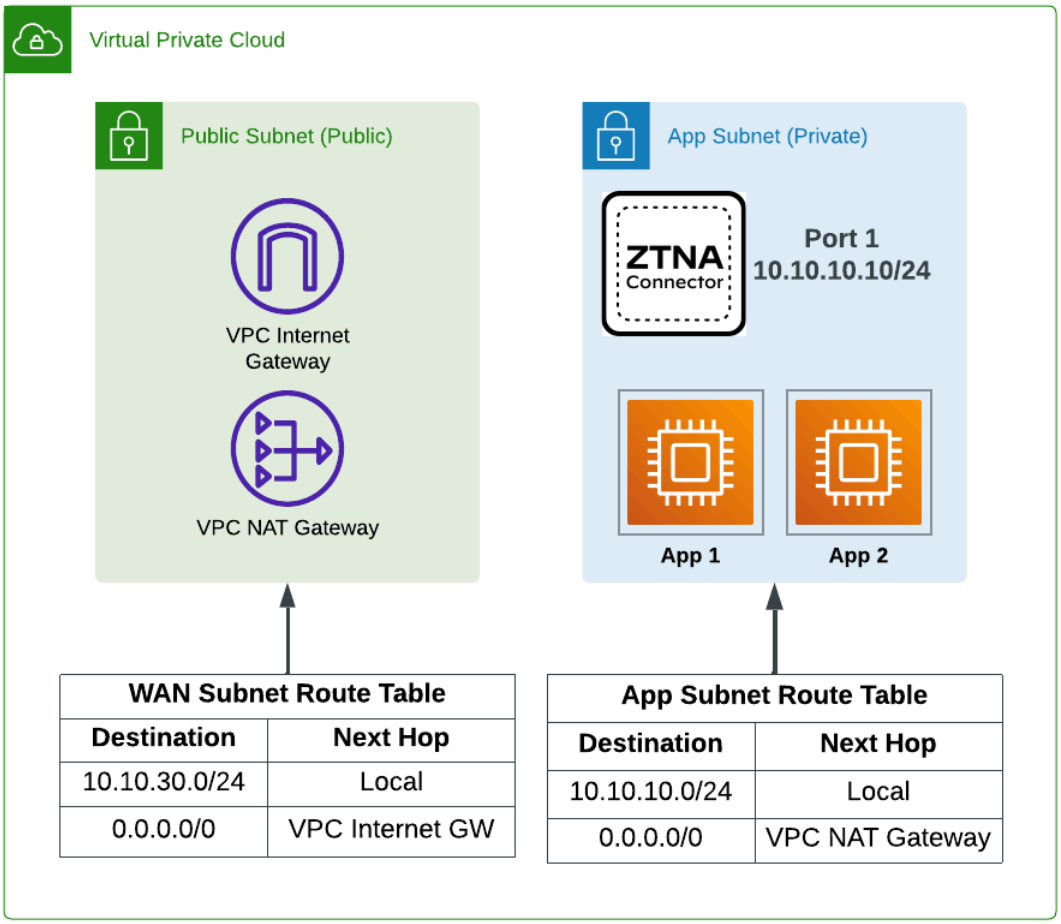


 ©2025 Palo Alto Networks, Inc.

Déploiements d'Amazon Web Services pris en charge par le connecteur ZTNA

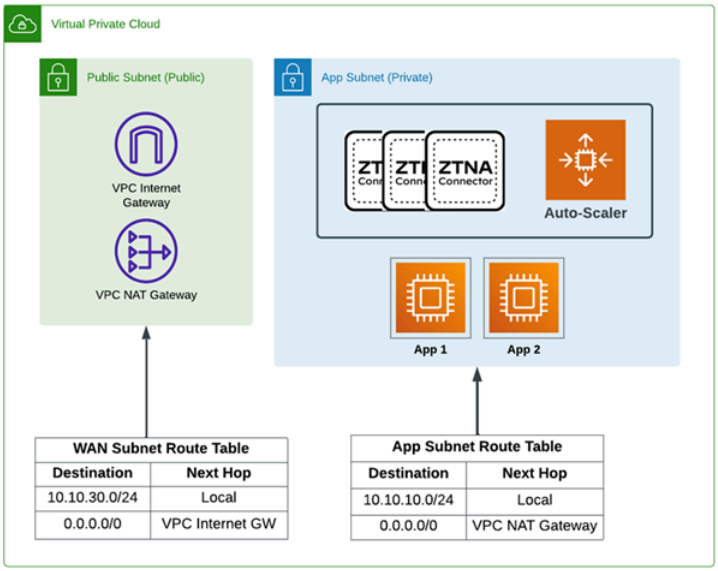
Prisma Access Le déploiement réseau du connecteur ZTNA dans Amazon Web Services (AWS) prend en charge trois déploiements et un modèle correspondant pour chaque déploiement.

Le diagramme suivant montre un échantillon de déploiement du connecteur ZTNA Prisma Access dans AWS à l'aide du mode à un bras avec une passerelle NAT.

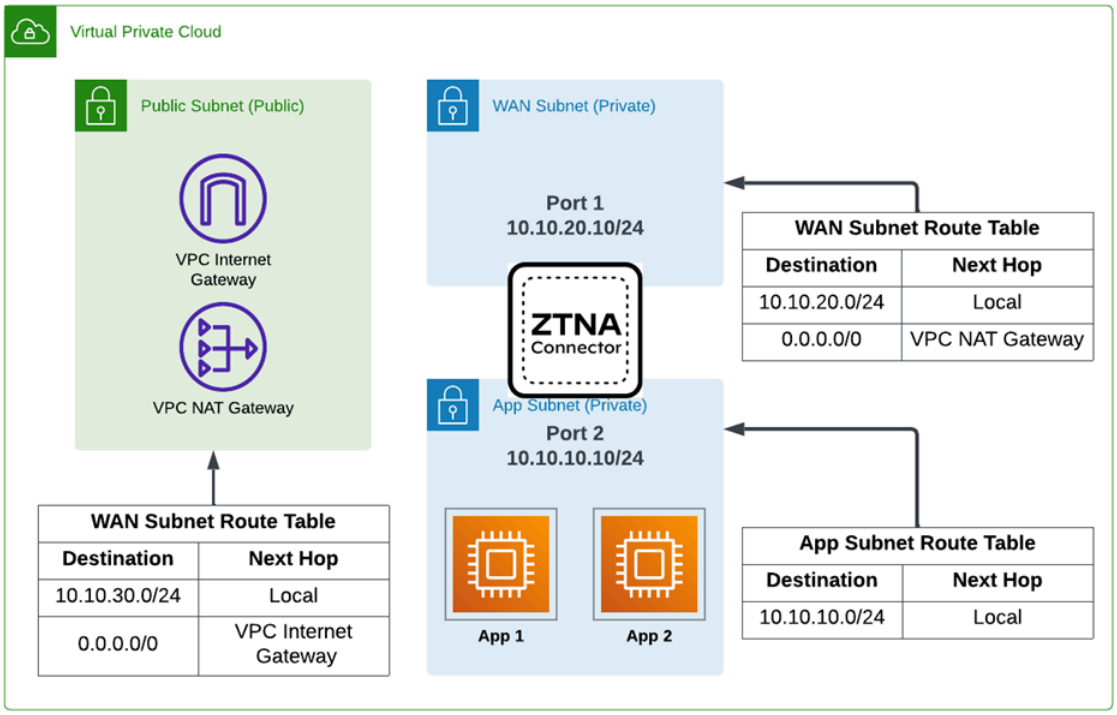


Le diagramme suivant montre un échantillon de déploiement du connecteur ZTNA dans AWS à l'aide d'une mise à l'échelle automatique one-arm avec une passerelle NAT.

 ©2025 Palo Alto Networks, Inc.



Le diagramme suivant montre un échantillon de déploiement du connecteur ZTNA dans AWS à l'aide du mode à deux bras avec une passerelle NAT.

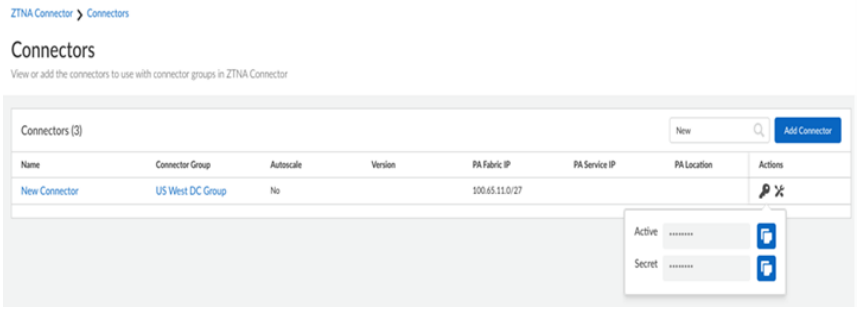


Intégrer un connecteur ZTNA dans Amazon Web Services

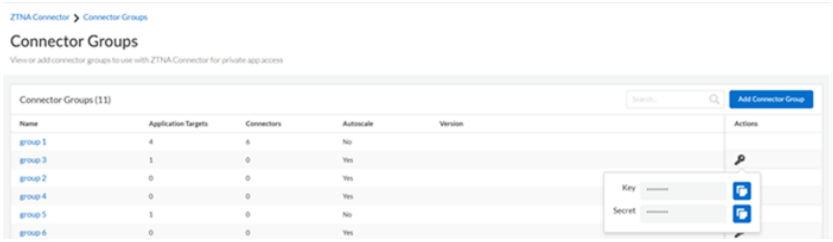
- Passez en revue les Exigences et directives et le FQDN et les ports que vous devez configurer pour utiliser le connecteur ZTNA dans Amazon Web Services (AWS).

 ©2025 Palo Alto Networks, Inc.

- Sur la plateforme Prisma SASE, récupérez et copiez les valeurs de la clé et du secret du connecteur : **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)**, recherchez l'objet Connecteur que vous avez créé dans Prisma Access pour l'associer à cette VM, puis sélectionnez **Copy Token (Copier le jeton)**. Ensuite, copiez les valeurs **Key (Clé)** et **Secret**.



- Pour le déploiement de **la mise à l'échelle automatique du connecteur ZTNA Prisma Access à un bras**, vous devez récupérer et copier les valeurs de la clé et du secret du groupe de connecteurs : **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connector Groups (Groupes de connecteurs)**, recherchez l'objet Groupe de connecteurs que vous avez créé dans Prisma Access pour l'associer à cette VM, puis sélectionnez **Copy Token (Copier le jeton)**. Ensuite, copiez les valeurs **Clé** et **Secret**.



Une fois que vous avez rempli toutes les conditions préalables, suivez ces étapes pour intégrer un Connecteur ZTNA Prisma Access dans AWS.

STEP 1 | Accédez à AWS Marketplace et recherchez **Prisma Access ZTNA Connector (Connecteur ZTNA Prisma Access)**.

STEP 2 | Choisissez le plan logiciel qui répond le mieux à vos besoins.

- Connecteur ZTNA Prisma Access à un bras
- Mise à l'échelle automatique du connecteur ZTNA Prisma Access à un bras
- Connecteur ZTNA Prisma Access à deux bras

Déployer le connecteur ZTNA à un bras dans AWS

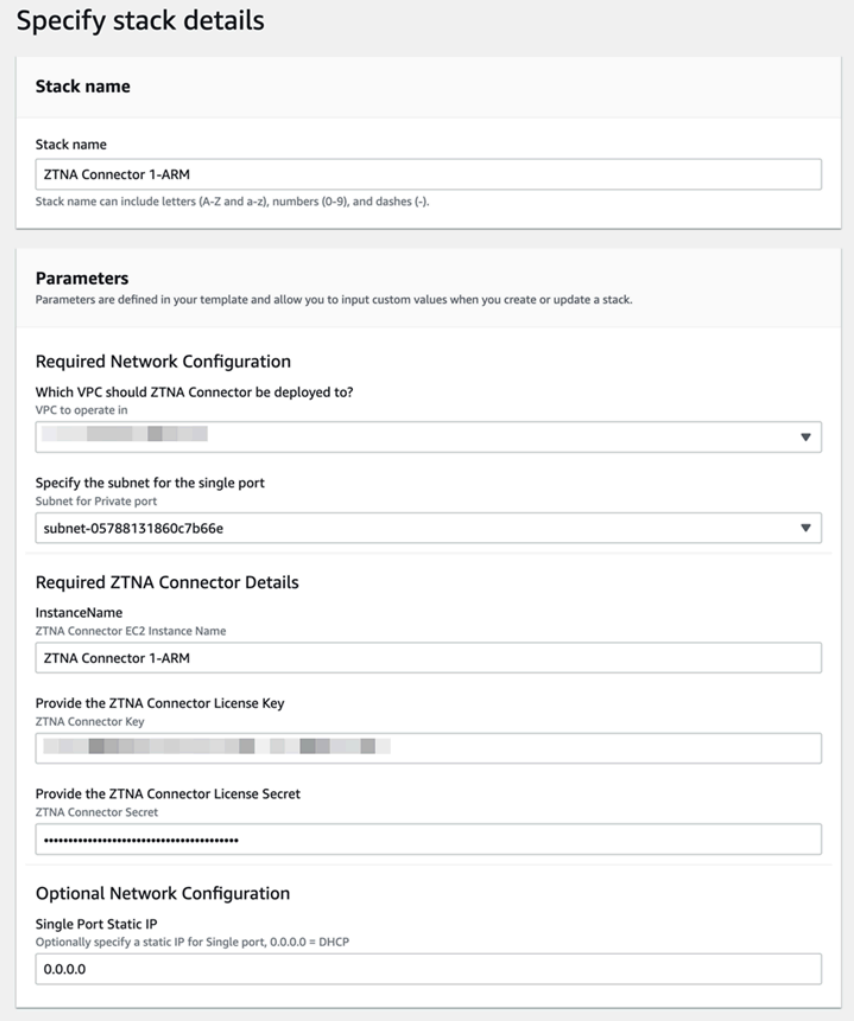
Suivez les étapes suivantes pour déployer le connecteur ZTNA à un bras dans AWS.

STEP 1 | Sélectionnez le modèle Cloud Formation **Prisma Access ZTNA Connector 1-Arm (Connecteur ZTNA Prisma Access à un bras)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configurez-les dans la page **Specify stack details (Spécifier les détails de la pile)** :

- Saisissez le **Stack Name (Nom de la pile)** pour identifier la pile.
- Dans la section **Parameters (Paramètres)**, spécifiez les paramètres définis dans le modèle de pile.
  - Sélectionnez **Which VPC should ZTNA Connector be deployed to (Sur quel VPC le connecteur ZTNA doit être déployé)**.
  - **Specify the subnet for the single port (Spécifiez le sous-réseau pour le port unique)**, où vous avez provisionné des applications à intégrer à ce connecteur. Vous devez avoir accès à Internet à partir de ce sous-réseau via une passerelle NAT.
- Saisissez les valeurs de **ZTNA Connector License Key (Clé de licence du connecteur ZTNA)** Prisma et de **ZTNA Connector License Secret (Secret de la licence du connecteur ZTNA)** Prisma que vous avez récupérées à partir du portail Prisma SASE.



Déployer le connecteur ZTNA à un bras avec mise à l'échelle automatique dans AWS

Suivez les étapes suivantes pour déployer le connecteur ZTNA à un bras avec mise à l'échelle automatique dans AWS.

 ©2025 Palo Alto Networks, Inc.

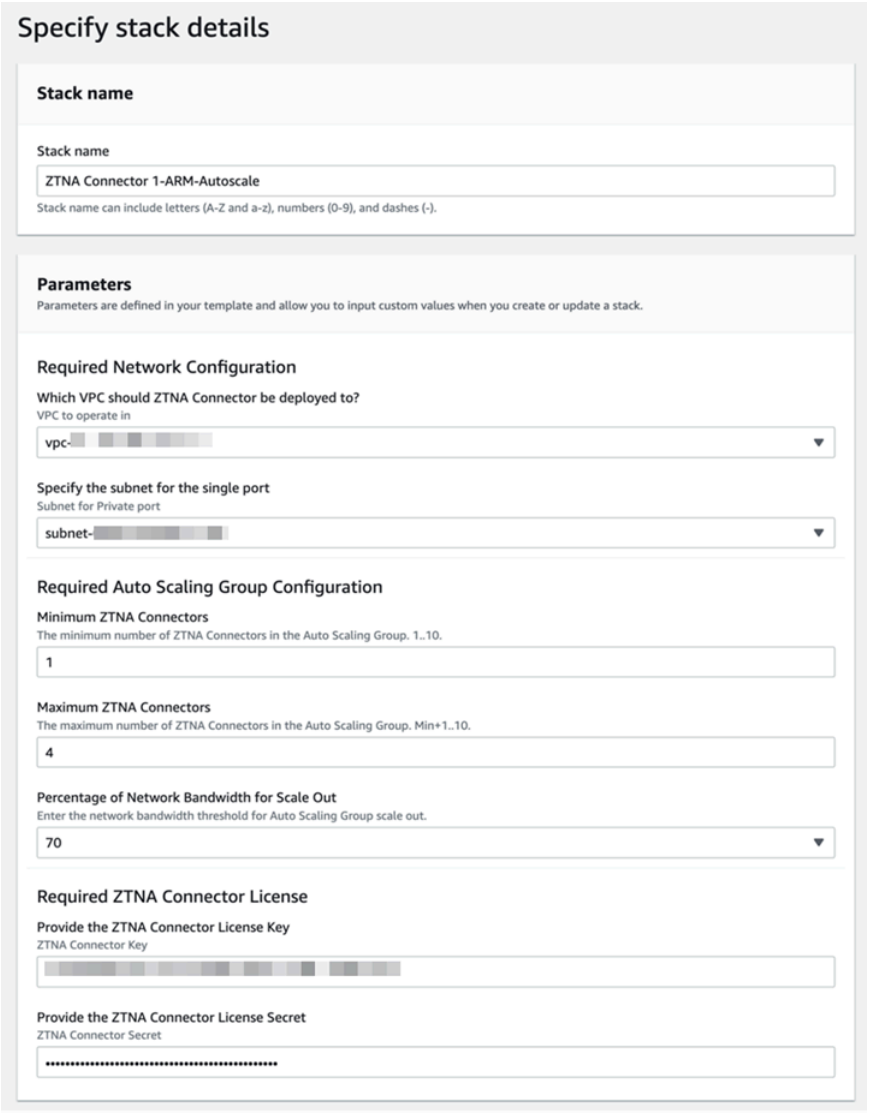
STEP 1 | Sélectionnez le modèle Cloud Formation **Prisma Access ZTNA Connector 1-Arm Auto-Scaling (Mise à l'échelle automatique du connecteur ZTNA Prisma Access à un bras)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configurez ces paramètres dans la page **Specify stack details (Spécifier les détails de la pile)** :

- Saisissez le **Stack Name (Nom de pile)** unique pour le déploiement.
- Spécifiez les paramètres définis dans le modèle de pile dans la section **Parameters (Paramètres)** :
  - Sélectionnez **Which VPC should ZTNA Connector be deployed to (Sur quel VPC le connecteur ZTNA doit être déployé)**.
  - **Specify the subnet for the single port (Spécifiez le sous-réseau pour le port unique)**, où vous avez provisionné des applications à intégrer à ce connecteur. Vous devez avoir accès à Internet à partir de ce sous-réseau via une passerelle NAT.
- Dans **Required Auto Scaling Group Configuration (Configuration requise du groupe de mise à l'échelle automatique)** :
  - Saisissez les **Minimum ZTNA Connectors (Connecteurs ZTNA minimum)** requis dans le groupe de mise à l'échelle automatique.
  - Saisissez les **Minimum ZTNA Connectors (Connecteurs ZTNA minimum)** requis dans le groupe de mise à l'échelle automatique. Le nombre maximal de connecteurs ZTNA autorisés dans le groupe de connecteurs est de 4.
  - Réglez l'option **Percentage of Network Bandwidth for Scale Out (Pourcentage de la bande passante réseau pour la mise à l'échelle)**. La valeur par défaut et recommandée est de 70 %.
- Saisissez les valeurs de **ZTNA Connector License Key (Clé de licence du connecteur ZTNA)** et de **ZTNA Connector License Secret (Secret de la licence du connecteur ZTNA)** Prisma que vous avez récupérées à partir du portail Prisma SASE.

 ©2025 Palo Alto Networks, Inc.



Déployer le connecteur ZTNA à deux bras dans AWS

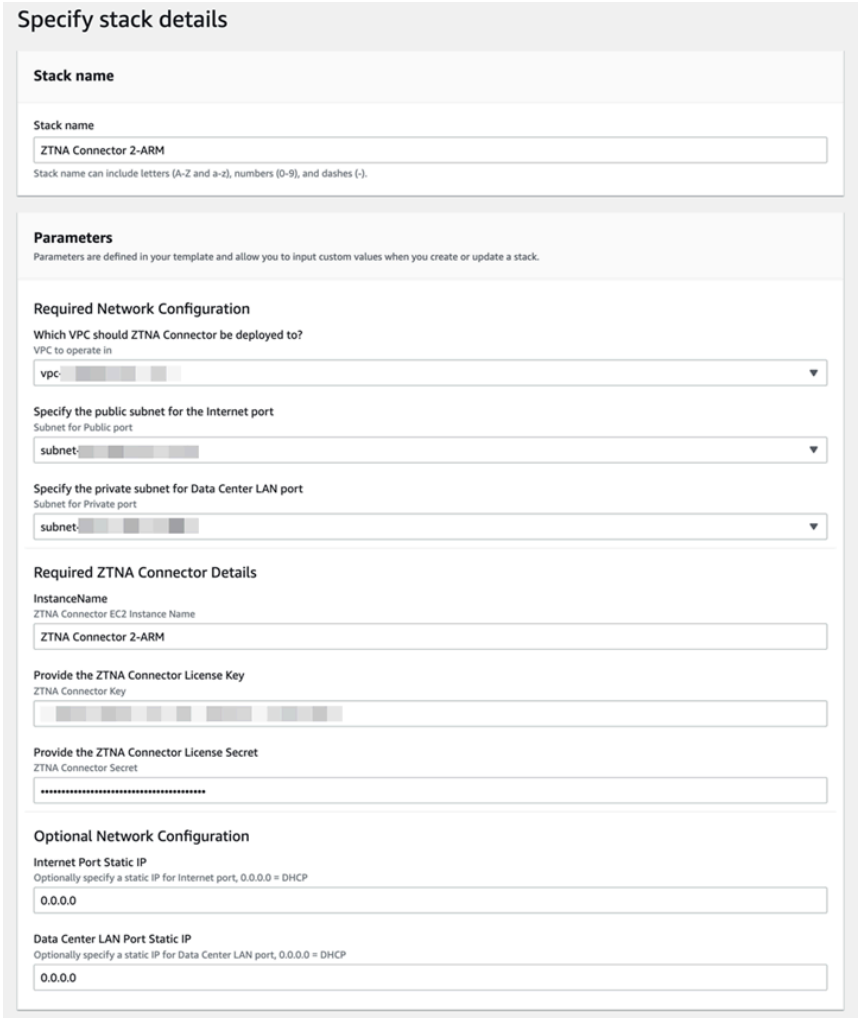
Suivez les étapes suivantes pour déployer le connecteur ZTNA à deux bras dans AWS.

STEP 1 | Sélectionnez le modèle Cloud Formation du déploiement du connecteur ZTNA Prisma Access à un bras.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Sur la page **Specify stack details (Spécifier les détails de la pile)** :

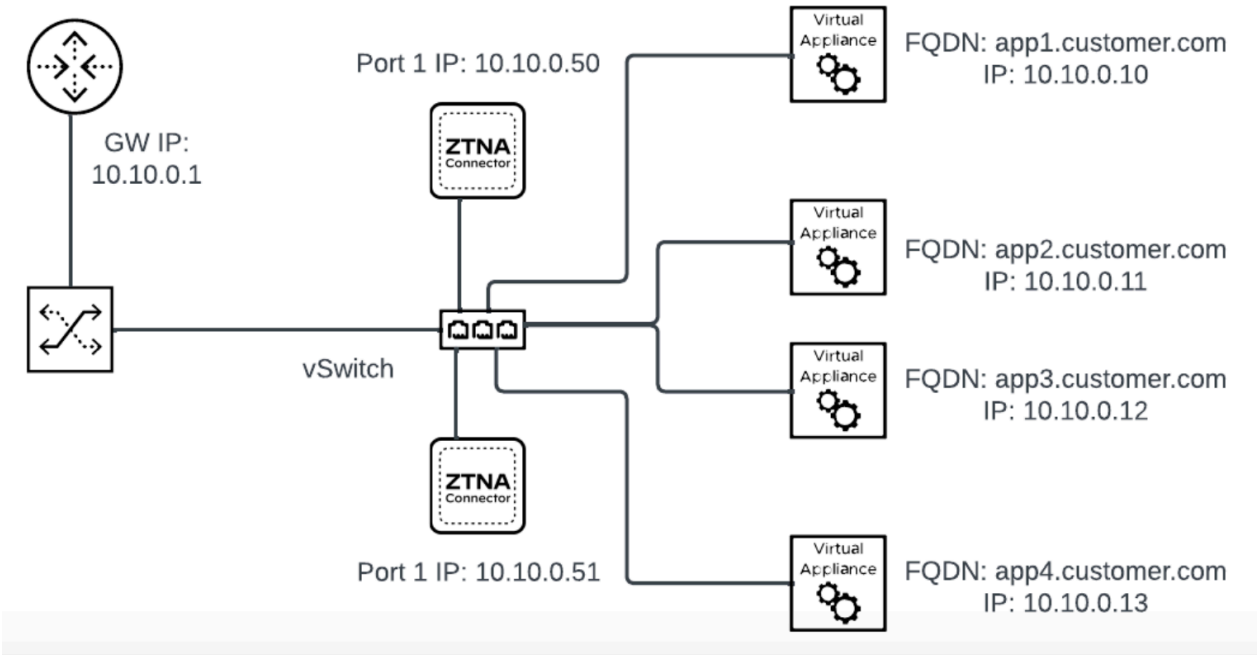
- Saisissez le **Stack Name (Nom de pile)** pour le déploiement.
- Spécifiez les paramètres définis dans votre modèle de pile dans la section **Parameters (Paramètres)**.
  - Sélectionnez **Which VPC should ZTNA Connector be deployed to (Sur quel VPC le connecteur ZTNA doit être déployé)**.
  - **Specify the public subnet for the Internet port (Spécifier le sous-réseau public pour le port Internet)** pour la connectivité WAN à IPSec. Ce sous-réseau doit être associé à une passerelle NAT pour la connectivité Internet.
  - **Specify the private subnet for Data Center LAN port (Spécifier le sous-réseau privé pour le port LAN du centre de données)**, où vous avez provisionné des applications à intégrer à ce connecteur.
- Saisissez **Instance Name (Nom de l'instance)**
- Saisissez les valeurs de **ZTNA Connector License Key (Clé de licence du connecteur ZTNA)** Prisma et de **ZTNA Connector License Secret (Secret de la licence du connecteur ZTNA)** Prisma que vous avez récupérées à partir du portail Prisma SASE.



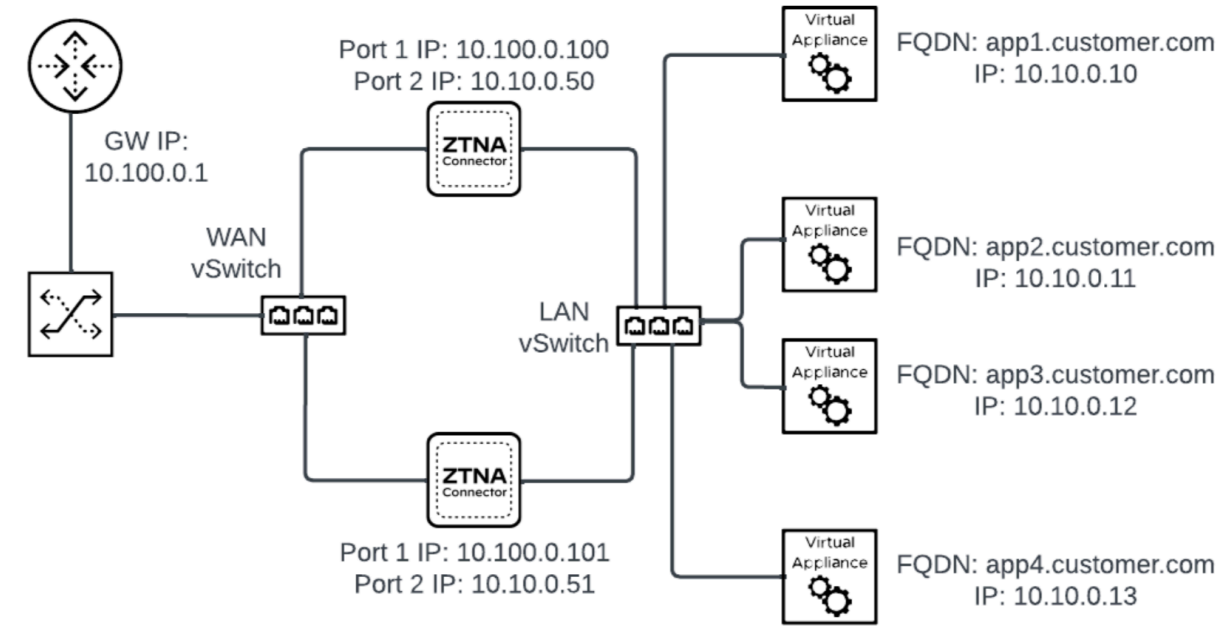
 ©2025 Palo Alto Networks, Inc.

Déploiements VMware ESXi pris en charge par le connecteur ZTNA Prisma Access

Le diagramme suivant montre un exemple de déploiement réseau du connecteur ZTNA utilisant VMware ESXi en mode à un bras avec une passerelle NAT.



Le diagramme suivant montre un exemple de déploiement réseau du connecteur ZTNA utilisant VMware ESXi en mode à deux bras avec une passerelle NAT.



 ©2025 Palo Alto Networks, Inc.

Intégrer un connecteur ZTNA dans VMware ESXi

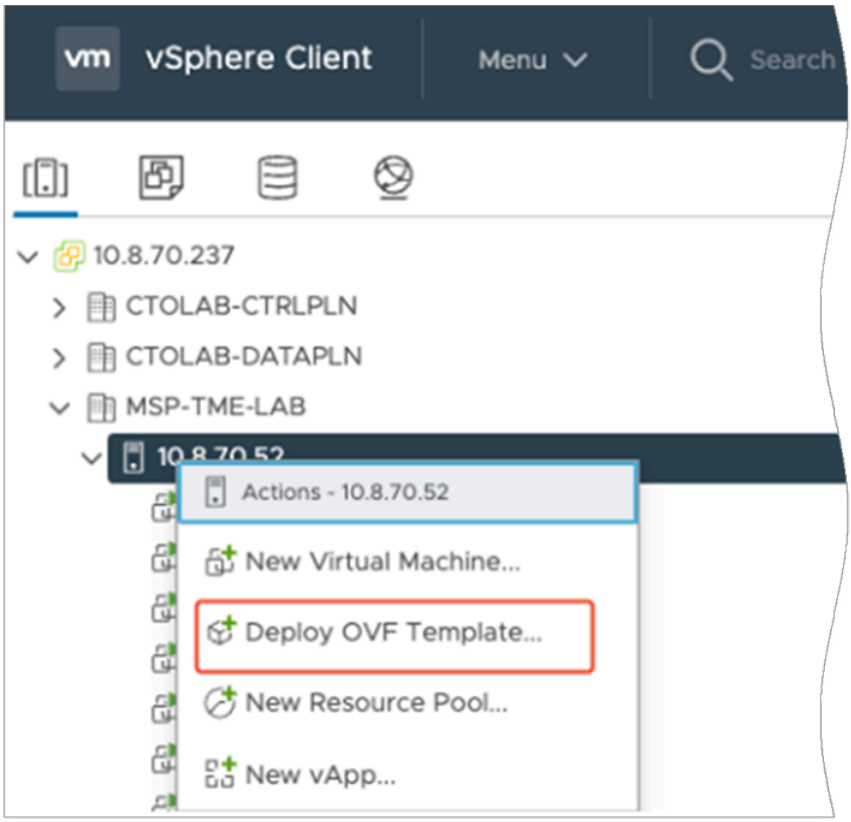
Pour intégrer un connecteur ZTNA dans VMware ESXi, procédez comme suit. Avant de commencer, assurez-vous de passer en revue les Exigences et directives pour les déploiements ZTNA en général et VMware ESXi en particulier.

Avant de commencer, passez en revue les Exigences et directives et le FQDN et les ports que vous devez configurer pour utiliser le connecteur ZTNA avec VMware ESXi.

STEP 1 | Téléchargez l'image VMware ESXi du connecteur ZTNA à partir du Portail de support client (CSP) sous **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)** > **Prisma Access ZTNA Connector for VMware (Connecteur ZTNA Prisma Access pour VMware)**.

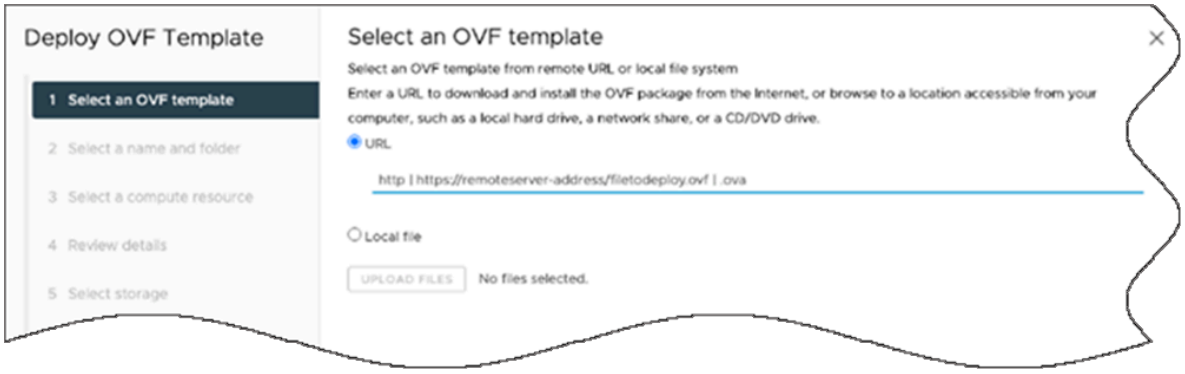
Téléchargez un fichier de version à une carte d'interface réseau pour un déploiement à un bras et un fichier de version à deux cartes d'interface réseau pour un déploiement à deux bras.

STEP 2 | Ouvrez VMware vCenter, sélectionnez, faites un clic droit sur l'hôte, puis sélectionnez **Deploy OVF Template (Déployer le modèle OVF)**.

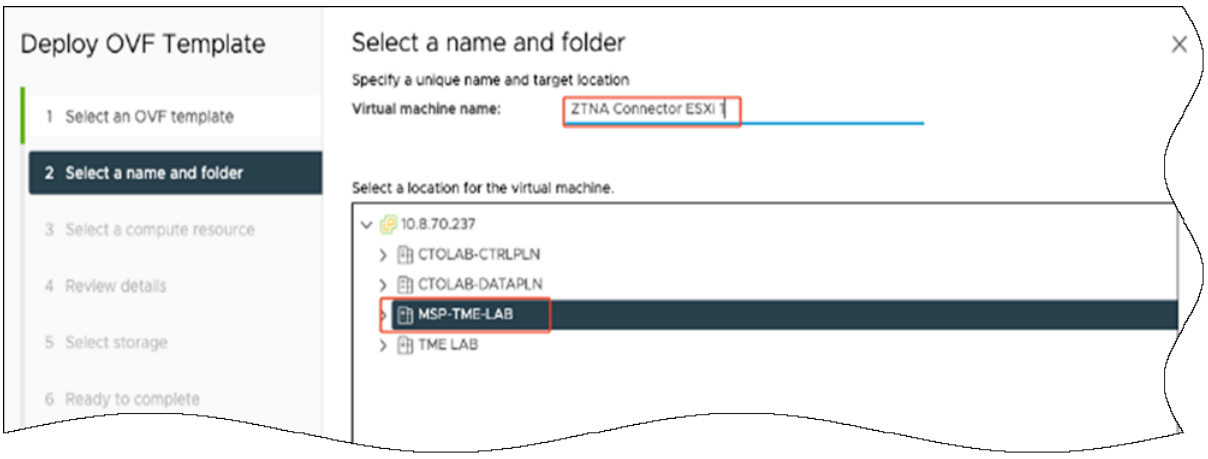


 ©2025 Palo Alto Networks, Inc.

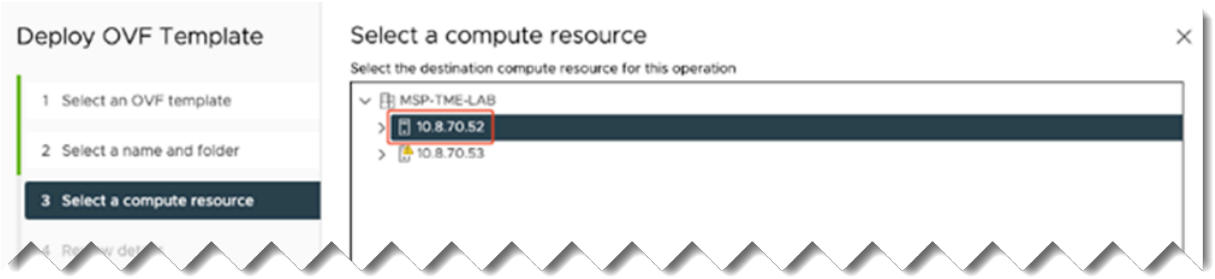
STEP 3 | Sélectionnez l'emplacement dans l'OVA du connecteur (soit une URL, soit un fichier local) et sélectionnez **Next (Suivant)**.



STEP 4 | Saisissez un nom de machine virtuelle (VM) et un emplacement pour la VM.

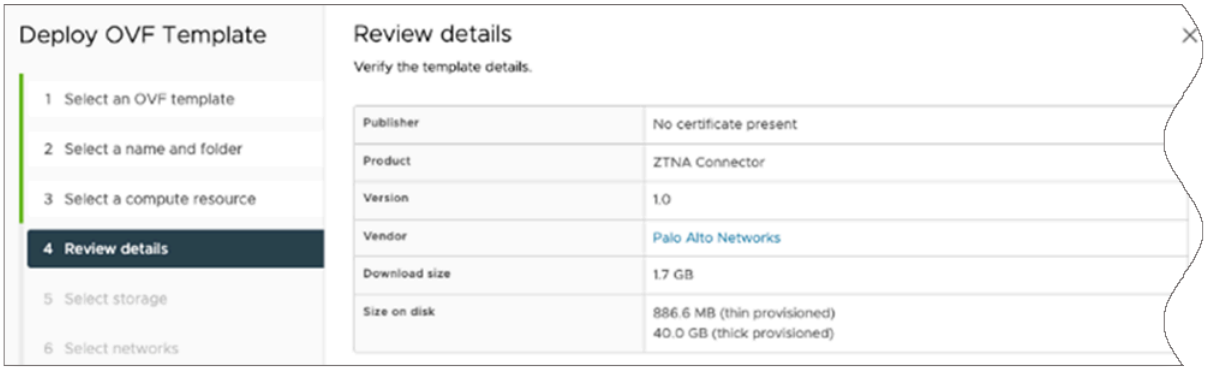


STEP 5 | Sélectionnez la ressource de calcul pour la VM.

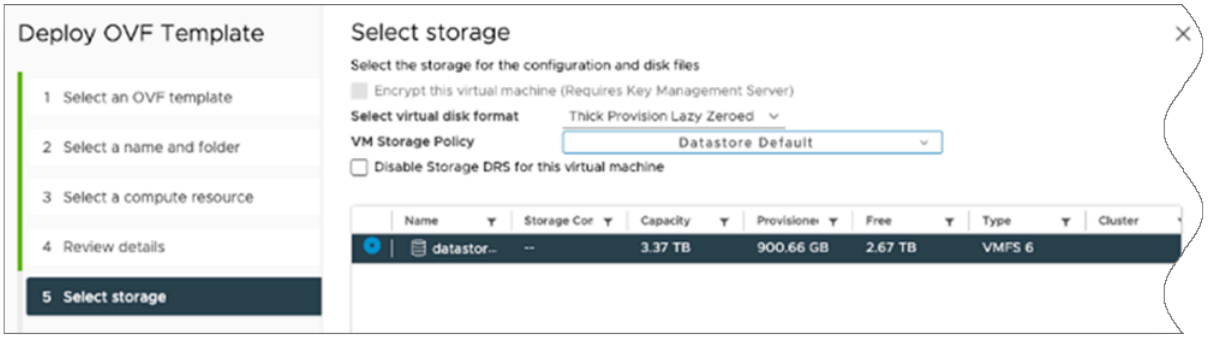


 ©2025 Palo Alto Networks, Inc.

STEP 6 | Passez en revue les détails du modèle et sélectionnez **Next (Suivant)**.



STEP 7 | Sélectionnez **Thick Provision Lazy Zeroed (Allocation statique avec mise à zéro tardive)** pour le format de disque virtuel et le magasin de données approprié pour la VM du connecteur ZTNA.



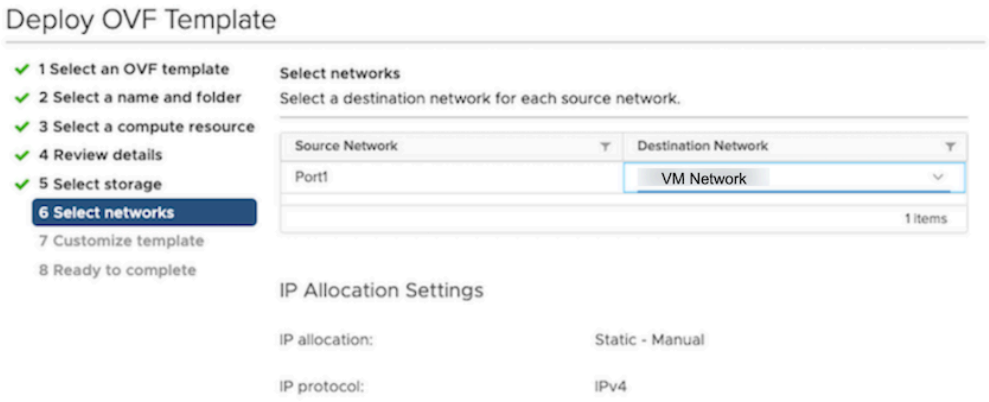
Facultatif Sélectionnez **Thin Provision (Allocation dynamique)** pour le format de disque virtuel et le magasin de données approprié pour la VM du connecteur ZTNA, où, en fonction des besoins, le serveur alloue uniquement l'espace requis par l'hôte.



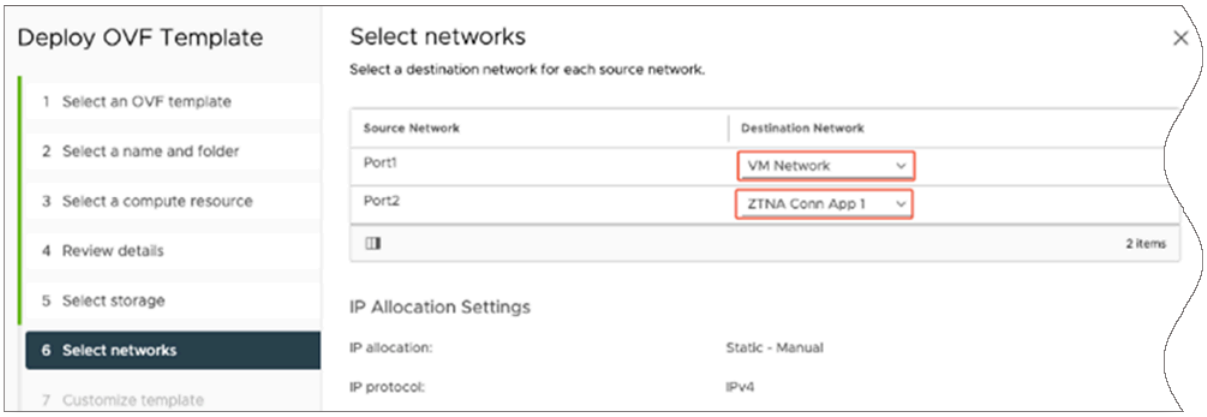
 ©2025 Palo Alto Networks, Inc.

STEP 8 | Sélectionnez les réseaux (pour le port 1 et le port 2) pour les interfaces que vous avez créées à l'aide du modèle de configuration OVA.

1. Si vous déployez un connecteur à un bras, le **Port 1** est le réseau capable d'atteindre les serveurs d'applications WAN et LAN. Sélectionnez le réseau WAN/LAN pour le **Port 1**.



2. Si vous déployez un connecteur à deux bras, sélectionnez le port orienté vers Internet pour le **Port 1** et le réseau orienté vers le serveur d'applications pour le **Port 2**.
   - Le port 1 est le port orienté WAN pour la connectivité IPSec Prisma Access.
   - Le port 2 est le port orienté vers l'application.



STEP 9 | Si ce n'est pas déjà fait, accédez à **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)**, recherchez l'objet Connecteur que vous

 ©2025 Palo Alto Networks, Inc.

avez créé dans Prisma Access pour l'associer à cette VM, puis sélectionnez **Copy Token (Copier le jeton)** de l'onglet **Actions** (icône clé) ; puis copiez les valeurs **Key (Clé)** et **Secret**.



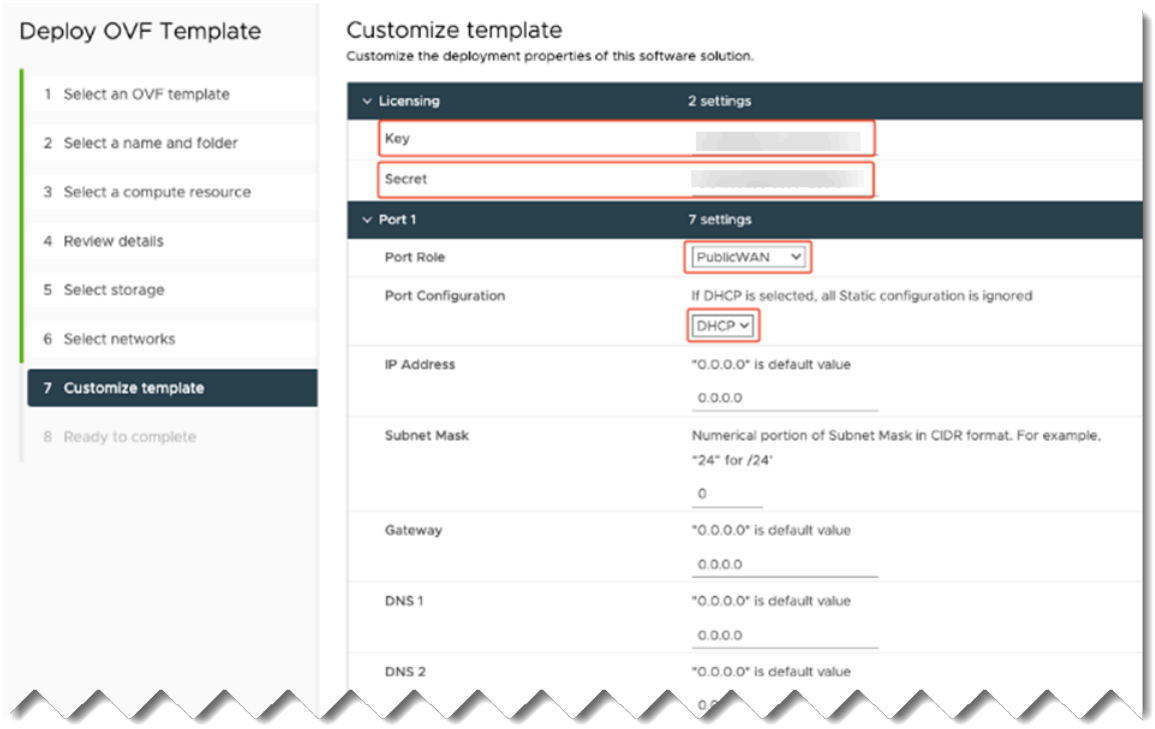
 ©2025 Palo Alto Networks, Inc.

STEP 10 | Dans l'écran **Customize template (Personnaliser le modèle)**, effectuez les modifications de configuration suivantes :

- Zone **Licensing (Octroi de licences)** : saisissez les valeurs **Key (Clé)** et **Secret** que vous avez récupérées à partir du portail Prisma SASE.
- **Port 1** (le port orienté vers Prisma Access) : effectuez les modifications suivantes :
  - **Role (Rôle)** : WAN public.
  - **Port Configuration (Configuration du port)** : soit **DHCP** ou **Static (Statique)**.

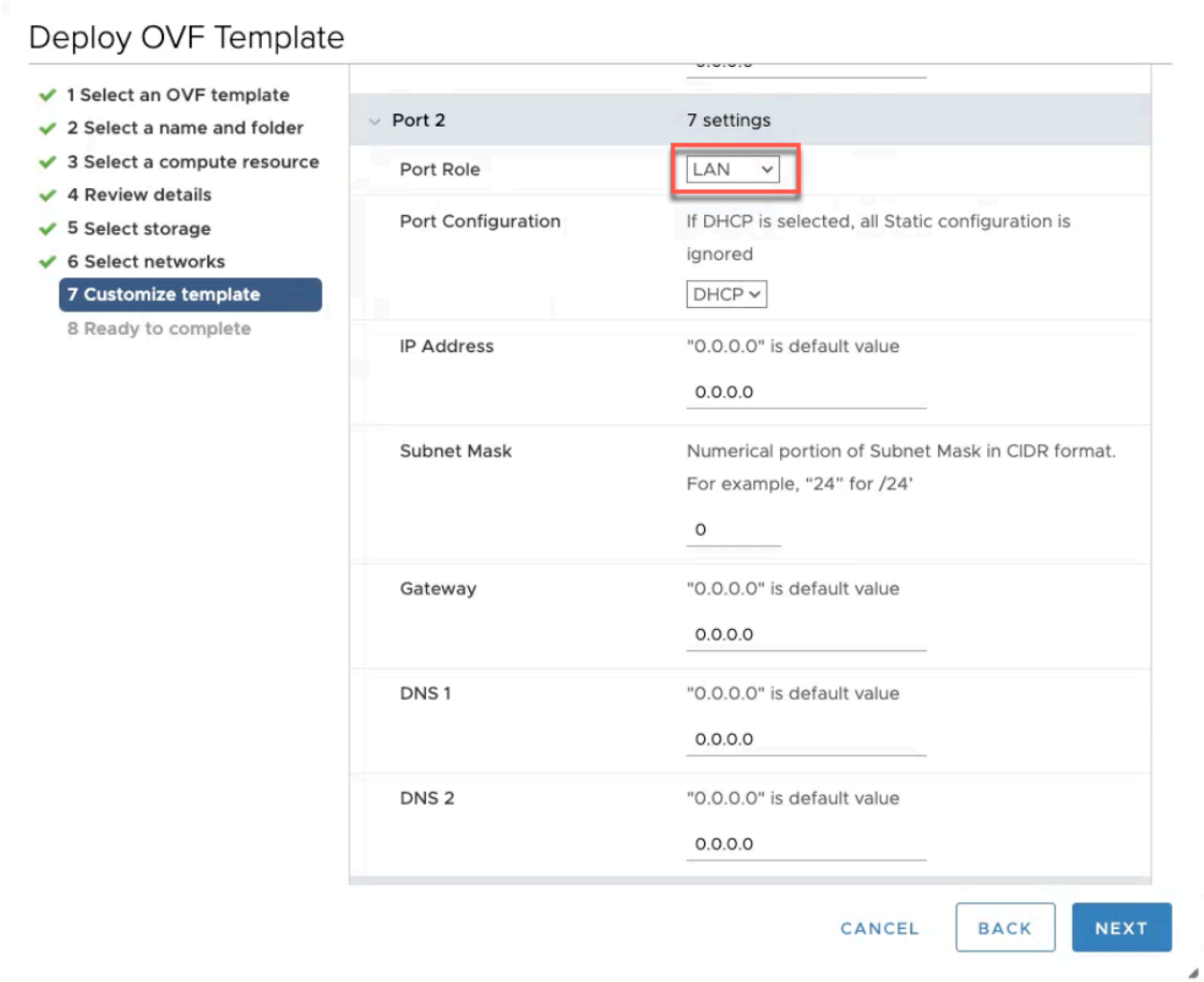
    Si vous sélectionnez **Static (Statique)**, saisissez l'adresse IP, le masque de sous-réseau, la passerelle et une ou deux valeurs de serveur DNS.

    Si vous utilisez DHCP, laissez les zéros par défaut dans les champs, comme indiqué dans la capture d'écran suivante.



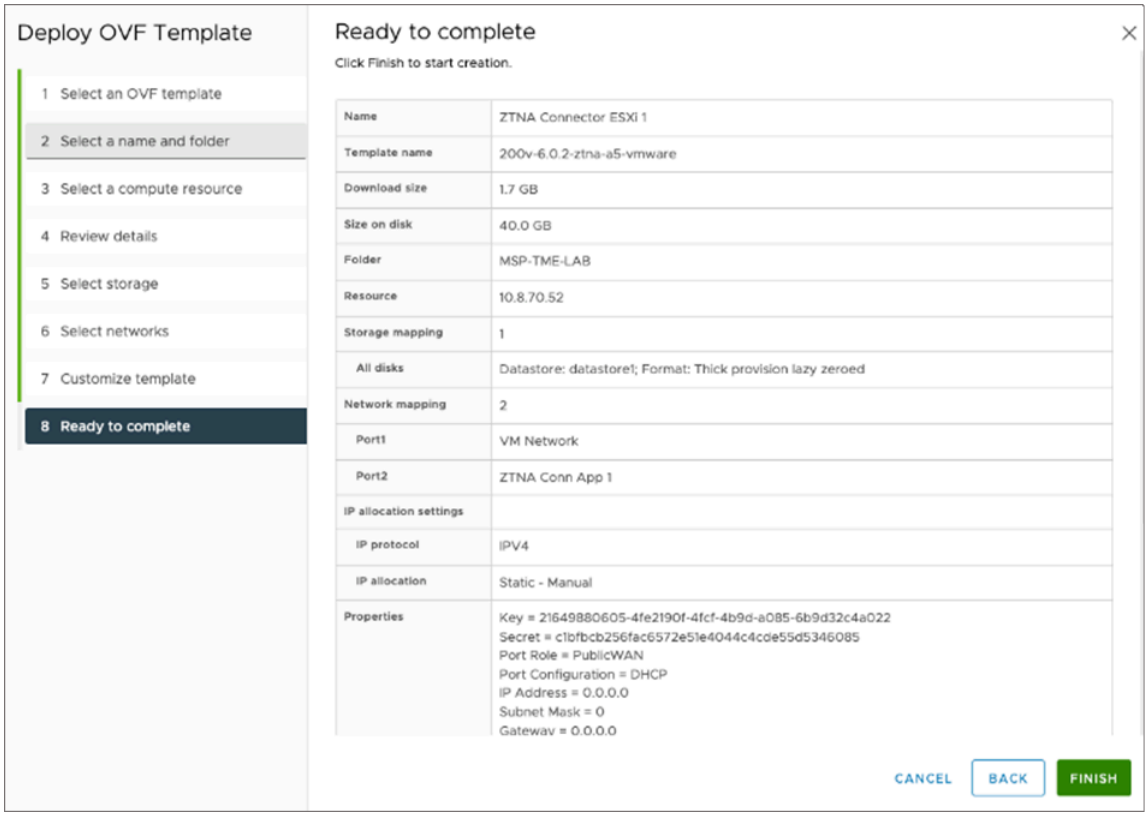
- Déploiements ESXi à deux bras uniquement Si vous avez un déploiement à deux bras, configurez l'interface IP LAN du **Port 2** avec les mêmes règles appliquées pour le **Port 1** à l'étape 10.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

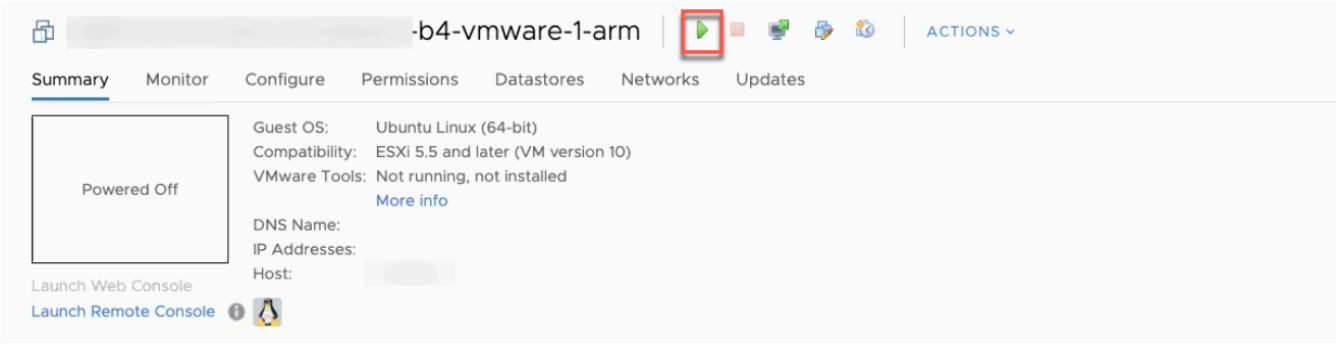
STEP 11 | Passez en revue le résumé, puis sélectionnez **Finish (Terminer)**.



 ©2025 Palo Alto Networks, Inc.

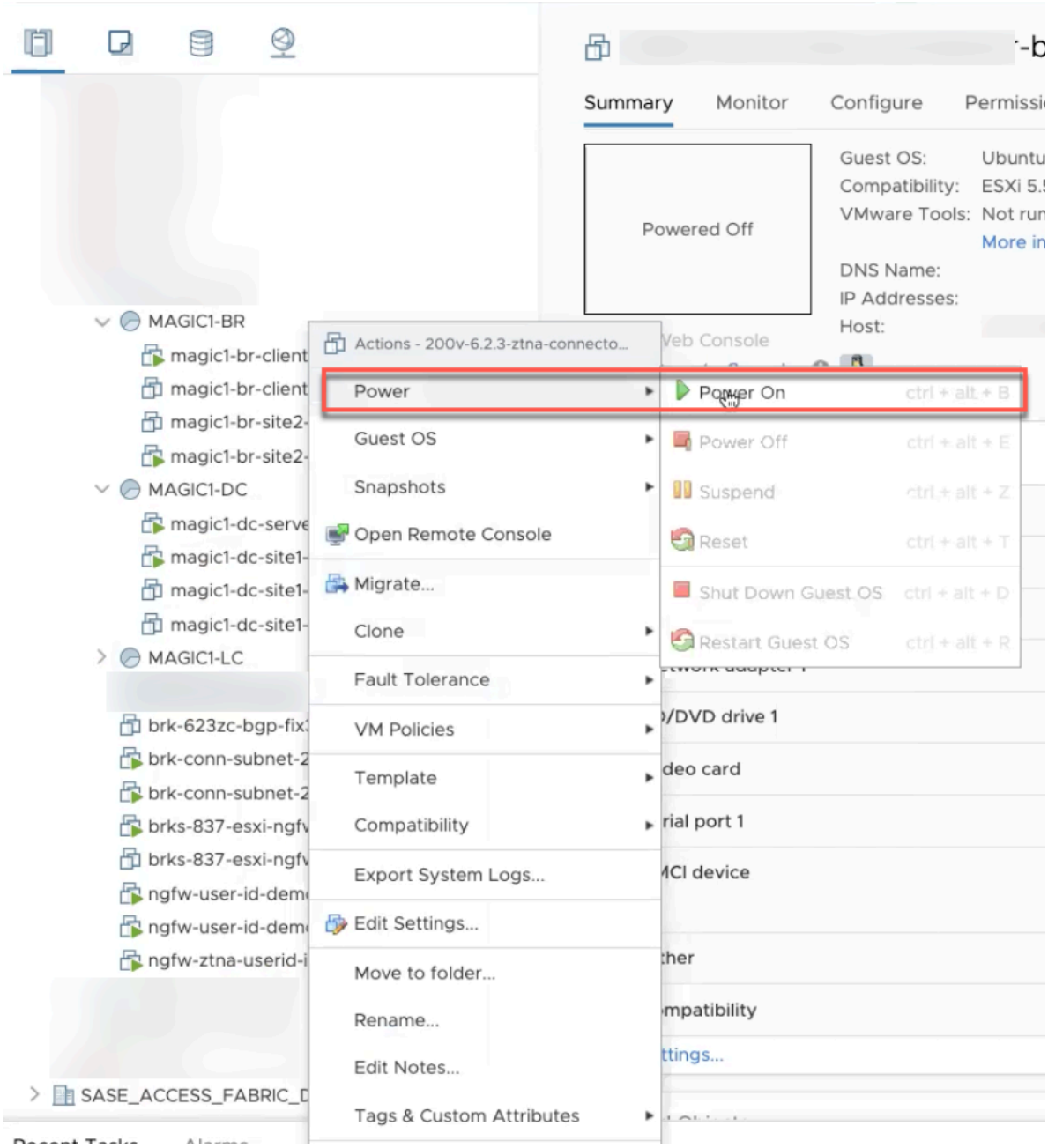
STEP 12 | Mettez la VM sous tension par l'une des méthodes suivantes.

- Sélectionnez **Power On (Mise sous tension)** pour démarrer le serveur virtuel.



- Faites un clic droit sur l'interface, puis sélectionnez **Power On (Mise sous tension)** (**Power (Alimentation)** > **Power On (Mise sous tension)**).

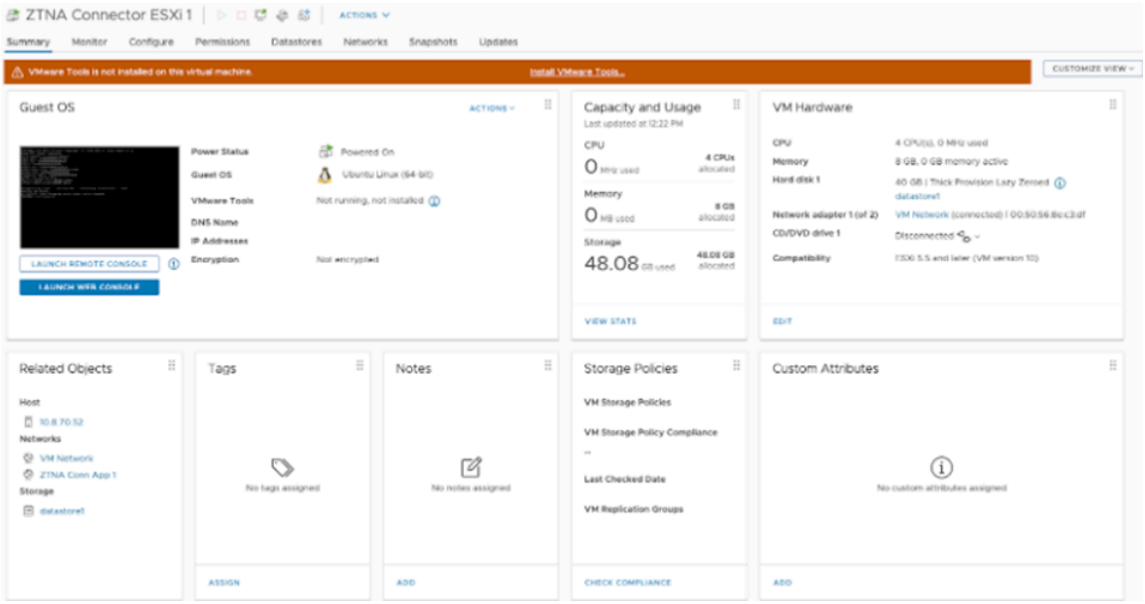
 ©2025 Palo Alto Networks, Inc.



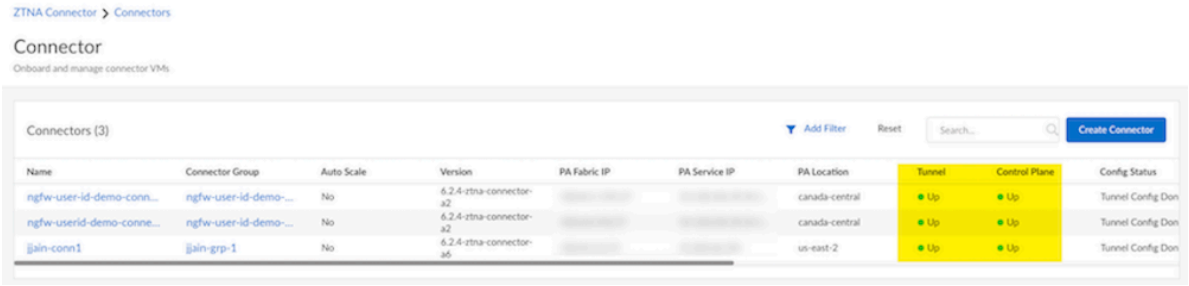
 ©2025 Palo Alto Networks, Inc.

STEP 13 | Après avoir déployé la VM, vérifiez qu'elle est activée.

Une fois que le serveur virtuel ESXi est activé, Prisma Access termine la configuration du périphérique à utiliser comme connecteur ZTNA.



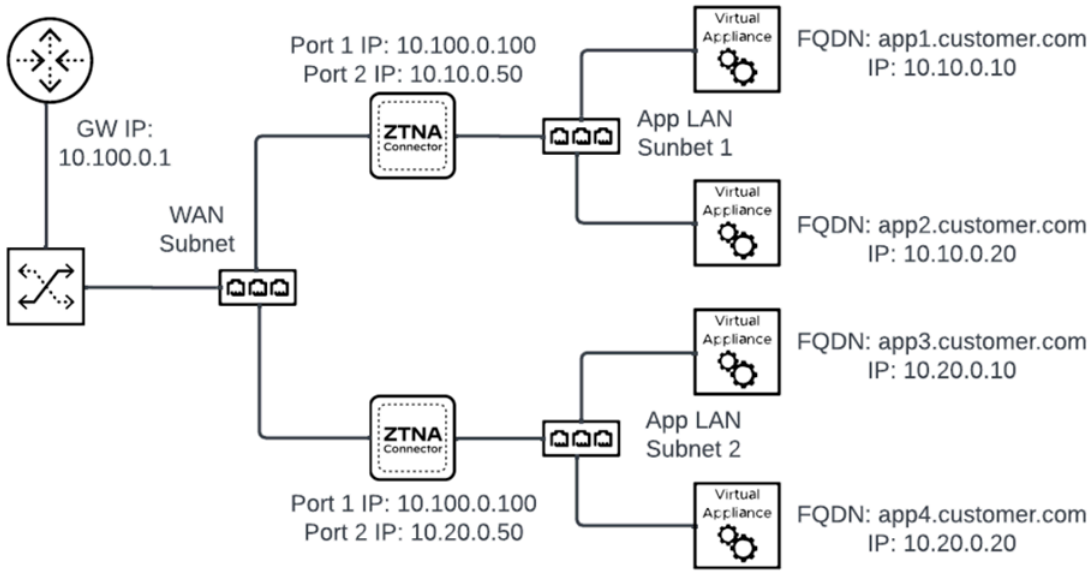
STEP 14 | Sur le portail Prisma SASE, accédez à **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)**, recherchez le connecteur que vous souhaitez utiliser et vérifiez qu'il affiche **tunnel up (tunnel vers le haut)**.



Déploiements de KVM pris en charge par le connecteur ZTNA Prisma Access

Vous déployez une machine virtuelle basée sur le noyau (Kernel-based Virtual Machine – KVM) à l'aide d'un déploiement à deux bras. Le diagramme suivant montre un exemple de déploiement réseau du connecteur ZTNA à l'aide d'une KVM en mode à deux bras avec une passerelle NAT.

 ©2025 Palo Alto Networks, Inc.



Intégrer un connecteur ZTNA à l'aide de KVM

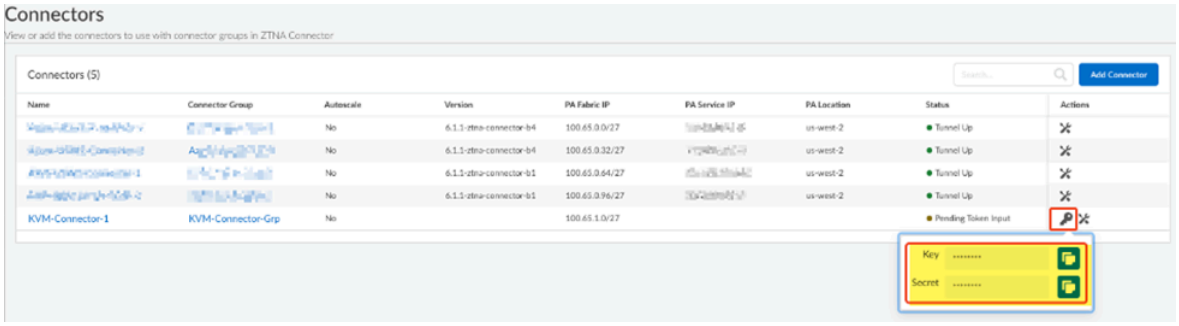
Pour intégrer un connecteur ZTNA à l'aide d'une machine virtuelle basée sur noyau (KVM), procédez comme suit.

Avant de commencer, assurez-vous de disposer des conditions préalables suivantes :

- Téléchargez l'image KVM du connecteur ZTNA à partir du portail de support client (CSP) sous **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)** > **Prisma Access ZTNA Connector for KVM (Connecteur ZTNA Prisma Access pour Hyper-V)**.
- Vérifiez que vous disposez d'un hôte KVM qui répond aux environnements d'hébergement minimaux pour le connecteur ZTNA.

STEP 1 | Créez un groupe de connecteurs et un connecteur pour l'hôte KVM.

STEP 2 | Sélectionnez **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)**et recherchez le connecteur que vous avez créé pour l'hôte KVM, puis cliquez sur **Copy Token (Copier le jeton)** dans la zone **State (État)** et copiez les valeurs de **Key (Clé)** et du **Secret**.



STEP 3 | Chargez l'image **qcow** que vous avez téléchargée depuis le CSP vers l'hôte KVM.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Si vous ne l'avez pas déjà fait, créez et associez les interfaces de pont virtuel sur l'hôte KVM et préparez l'hôte en saisissant les commandes suivantes :

- `brctl addbr virbr0`
- `brctl addbr virbr0`
- `brctl addbr virbr1`
- `brctl addif virbr1 ens192`

STEP 5 | Déployez la VM sur l'hôte KVM en exécutant la commande `virt-install` avec les options suivantes définies :

- `-name` désigne le nom de la machine virtuelle.
- `-vcpu` est **4**.
- `-memory` est **16384** (16 Go).
- `-disk` désigne l'emplacement et le nom de l'image **qcow** sur l'hôte KVM.
- `-network` fait référence aux interfaces virtuelles à attacher à cette VM (vous devez déployer des interfaces pour un connecteur ZTNA).

La commande suivante est un exemple utilisé pour déployer l'hôte KVM, où <kvm-file-name> désigne le nom du fichier qcow que vous avez téléchargé depuis le CSP :

```
virt-install --name ztna-conn-1 --vcpus 4 --memory 16384 --disk ./
<kvm-file-name> --import --network bridge=virbr0,model=virtio --
network bridge=virbr1,model=virtio
```

STEP 6 | Connectez-vous à la console VM en saisissant la commande suivante :

```
virsh console ztna-conn-1
```

Un programme d'installation CLI interactif s'initialise.

STEP 7 | Configurez le modèle ION, la clé et le secret.

1. Sélectionnez **1** (un modèle ION de **ion 200v**) parmi les choix qui s'affichent.

```
root@ubuntu-kvm-vm:/home/ubuntu-kvm/Desktop# virsh console
 ztna-conn-1 Connecté au domaine ztna-conn-1 Le caractère
 d'échappement est ^] Sélectionnez un modèle ION : 1) ion
 200v 2) ion 3102v 3) ion 3104v 4) ion 3108v 5) ion 7108v
 6) ion 7116v 7) ion 7132v 8) ion 9100v Choisissez un
 numéro ou (Q)uitter : 1 Processeur : Réussite (nécessite 4)
 Mémoire : Réussite (nécessite 8,0 Go) Disque : Impossible
 de vérifier (nécessite 40,0 G) Réseau : Réussite (nécessite
 1) Sélectionnez un élément à modifier ou soumettez la
 configuration : 1) Modèle : ion 200v 2) Clé ION : 3) Clé
 secrète : 4) Contrôleur 1 : Contrôleur — DHCP 5) Port 1 :
 Désactivé/Non utilisé 6) Port 2 : Désactivé/Non utilisé
 7) Port 3 : Désactivé/Non utilisé 8) Port 4 : Désactivé/
Non utilisé 9) Port 5 : Désactivé/Non utilisé 10) Port 6 :
 Désactivé/Non utilisé 11) Port 7 : Désactivé/Non utilisé 12)
 Port 8 : Désactivé/Non utilisé 13) Port 9 : Désactivé/Non
 utilisé 14) Soumettre et redémarrer
```

 ©2025 Palo Alto Networks, Inc.

2. Saisissez la clé du connecteur en sélectionnant l'option **2** et en saisissant la clé que vous avez enregistrée à partir de l'interface utilisateur du connecteur ZTNA.

```
Choisissez un numéro ou (Q)uitter : 2 Saisissez la clé ION
 [Aucune] : xxxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl
 Sélectionnez un élément à modifier ou soumettez la
 configuration : 1) Modèle : ion 200v 2) Clé ION : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Clé secrète : 4)
 Contrôleur 1 : Contrôleur – DHCP 5) Port 1 : Désactivé/
Non utilisé 6) Port 2 : Désactivé/Non utilisé 7) Port 3 :
 Désactivé/Non utilisé 8) Port 4 : Désactivé/Non utilisé 9)
 Port 5 : Désactivé/Non utilisé 10) Port 6 : Désactivé/Non
 utilisé 11) Port 7 : Désactivé/Non utilisé 12) Port 8 :
 Désactivé/Non utilisé 13) Port 9 : Désactivé/Non utilisé 14)
 Soumettre et redémarrer
```

3. Saisissez le secret du connecteur ZTNA en sélectionnant l'option **3** et en saisissant le secret que vous avez enregistré à partir de l'interface utilisateur du connecteur ZTNA.

```
Choisissez un numéro ou (Q)uitter : 3 Saisissez le secret
 ION [Aucun] : abcde12345 Sélectionnez un élément à modifier
 ou soumettez la configuration : 1) Modèle : ion 200v 2) Clé
 ION : xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Clé
 secrète : abcde12345 4) Contrôleur 1 : Contrôleur – DHCP
 5) Port 1 : Désactivé/Non utilisé 6) Port 2 : Désactivé/
Non utilisé 7) Port 3 : Désactivé/Non utilisé 8) Port 4 :
 Désactivé/Non utilisé 9) Port 5 : Désactivé/Non utilisé
 10) Port 6 : Désactivé/Non utilisé 11) Port 7 : Désactivé/
Non utilisé 12) Port 8 : Désactivé/Non utilisé 13) Port 9 :
 Désactivé/Non utilisé 14) Soumettre et redémarrer
```

STEP 8 | Configurez les options du port WAN.

1. Sélectionnez l'option **5** (Port 1).

```
Choisissez un numéro ou (Q)uitter : 5 Port 1 : 1) Rôle :
 Désactiver 2) Annuler les changements de port 3) Appliquer et
 revenir
```

2. Sélectionnez l'option **1** (Public/WAN).

```
Choisissez un numéro ou (Q)uitter : 1 Sélectionnez le
 rôle du port : 1) Port Internet (PublicWAN) 2) Port WAN
 privé (PrivateWAN) 3) Paire de ports de contournement 1
 (port WAN) 4) Paire de ports de contournement 1 (port
 LAN) 5) Paire de ports de contournement 2 (port WAN) 6)
 Paire de ports de contournement 2 (port LAN) 7) Paire
 de ports de contournement 3 (port WAN) 8) Paire de
 ports de contournement 3 (port LAN) 9) Paire de ports
 de contournement 4 (port WAN) 10) Paire de ports de
 contournement 4 (port LAN) 11) Désactivé/Non utilisé
```

 ©2025 Palo Alto Networks, Inc.

3. (Facultatif) Si vous avez besoin de définir une adresse IP statique, choisissez l'option **2** et définissez les paramètres de l'adresse IP, de la passerelle et du serveur DNS ; sinon, sélectionnez **1**.

```
Choisissez un numéro ou (Q)uitter : 1 Port 1 : 1) Rôle :
 PublicWAN 2) Configuration via : DHCP 3) Annuler les
 changements de port 4) Appliquer et revenir
```

4. Sélectionnez l'option **4** pour revenir au menu principal.

```
Choisissez un numéro ou (Q)uitter : 4 Sélectionnez un élément
 à modifier ou soumettez la configuration : 1) Modèle :
 ion 200v 2) Clé ION : xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) Clé secrète : abcde12345 4) Contrôleur 1 :
 Contrôleur – DHCP 5) Port 1 : PublicWAN – DHCP 6) Port 2 :
 Désactivé/Non utilisé 7) Port 3 : Désactivé/Non utilisé 8)
 Port 4 : Désactivé/Non utilisé 9) Port 5 : Désactivé/Non
 utilisé 10) Port 6 : Désactivé/Non utilisé 11) Port 7 :
 Désactivé/Non utilisé 12) Port 8 : Désactivé/Non utilisé
 13) Port 9 : Désactivé/Non utilisé 14) Soumettre et
 redémarrer Sélectionnez un élément à modifier ou soumettez
 la configuration : 1) Modèle : ion 200v 2) Clé ION :
 xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Clé
 secrète : abcde12345 4) Contrôleur 1 : Contrôleur – DHCP 5)
 Port 1 : PublicWAN – DHCP 6) Port 2 : Désactivé/Non utilisé
 7) Port 3 : Désactivé/Non utilisé 8) Port 4 : Désactivé/
Non utilisé 9) Port 5 : Désactivé/Non utilisé 10) Port 6 :
 Désactivé/Non utilisé 11) Port 7 : Désactivé/Non utilisé 12)
 Port 8 : Désactivé/Non utilisé 13) Port 9 : Désactivé/Non
 utilisé 14) Soumettre et redémarrer
```

STEP 9 | Configurez les options du port LAN.

1. Sélectionnez l'option **6** (Port 2).

```
Choisissez un numéro ou (Q)uitter : 6 Port 2 : 1) Rôle :
 Désactiver 2) Annuler les changements de port 3) Appliquer et
 revenir
```

2. Sélectionnez l'option **2** (PrivateWAN).

```
Choisissez un numéro ou (Q)uitter : 2 Sélectionnez le
 rôle du port : 1) Port Internet (PublicWAN) 2) Port WAN
 privé (PrivateWAN) 3) Paire de ports de contournement 1
 (port WAN) 4) Paire de ports de contournement 1 (port
 LAN) 5) Paire de ports de contournement 2 (port WAN) 6)
 Paire de ports de contournement 2 (port LAN) 7) Paire
 de ports de contournement 3 (port WAN) 8) Paire de
 ports de contournement 3 (port LAN) 9) Paire de ports
 de contournement 4 (port WAN) 10) Paire de ports de
 contournement 4 (port LAN) 11) Désactivé/Non utilisé
```

 ©2025 Palo Alto Networks, Inc.

3. (Facultatif) Si vous avez besoin de définir une adresse IP statique, choisissez l'option **2** et définissez les paramètres de l'adresse IP, de la passerelle et du serveur DNS ; sinon, sélectionnez **1**.

```
Choisissez un numéro ou (Q)uitter : 2 Port 2 : 1) Rôle :
 PrivateWAN 2) Configuration via : DHCP 3) Annuler les
 changements de port 4) Appliquer et revenir
```

4. Sélectionnez l'option **4** pour revenir au menu principal.

```
Choisissez un numéro ou (Q)uitter : 4 Sélectionnez un élément
 à modifier ou soumettez la configuration : 1) Modèle :
 ion 200v 2) Clé ION : xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) Clé secrète : abcde12345 4) Contrôleur 1 :
 Contrôleur – DHCP 5) Port 1 : PublicWAN – DHCP 6) Port 2 :
 PrivateWAN – DHCP 7) Port 3 : Désactivé/Non utilisé 8)
 Port 4 : Désactivé/Non utilisé 9) Port 5 : Désactivé/Non
 utilisé 10) Port 6 : Désactivé/Non utilisé 11) Port 7 :
 Désactivé/Non utilisé 12) Port 8 : Désactivé/Non utilisé 13)
 Port 9 : Désactivé/Non utilisé 14) Soumettre et redémarrer
```

STEP 10 | Enregistrez et redémarrez le connecteur.

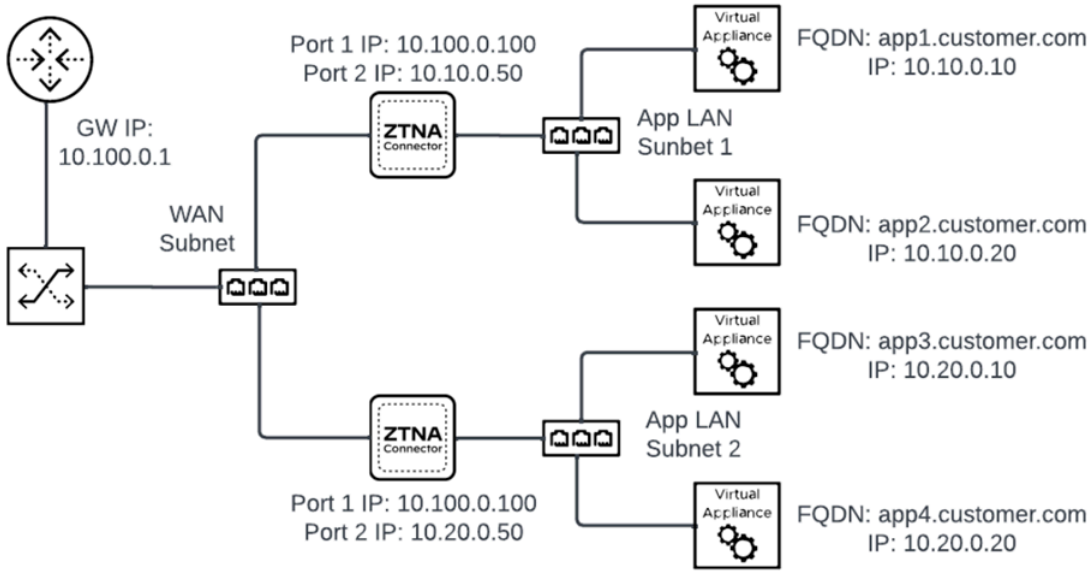
```
Choisissez un numéro ou (Q)uitter : 14 AVERTISSEMENT ! Une
 fois cette configuration soumise, tout le matériel sera signé,
 enregistré et lié de manière permanente à la clé ION/clé secrète
 dans le contrôleur cloud Prisma SDWAN. CELA SIGNIFIE que le
 matériel ne peut pas être ajouté/supprimé (disques, cartes
 réseau) après la fonction de « SOUMISSION ». Si des modifications
 matérielles sont nécessaires après cette « SOUMISSION », l'ION
 devra être redéployé avec une nouvelle clé ION et une nouvelle
 clé secrète. S'il est nécessaire d'ajouter ou de supprimer
 du matériel, veuillez répondre par « N » ci-dessous, arrêter
 l'ION et effectuer les modifications maintenant. Soumettre
 ces modifications maintenant ? [N] : y Configuration de
 construction... [VFF:CFG] Démarrage de la configuration ZeroTouch
 – analyseur du fichier de configuration [VFF:CFG] Tentative
 de chargement/analyse en tant que fichier de configuration/
INI. [VFF:CFG] Fichier de style de configuration chargé avec
 succès. [VFF:CFG] Contrôleur 1 défini avec succès sur CONTRÔLEUR/
DHCP. [VFF:CFG] Port 1 défini avec succès sur PUBLICWAN/DHCP.
 [VFF:CFG] Port 2 défini avec succès sur PRIVATEWAN/DHCP. [VFF:CFG]
 AVERTISSEMENT : Le port 3 n'avait pas de section de configuration.
 La valeur par défaut est Désactiver. [VFF:CFG] AVERTISSEMENT :
 Le port 4 n'avait pas de section de configuration. La valeur
 par défaut est Désactiver. [VFF:CFG] AVERTISSEMENT : Le port 5
 n'avait pas de section de configuration. La valeur par défaut est
 Désactiver. [VFF:CFG] AVERTISSEMENT : Le port 6 n'avait pas de
 section de configuration. La valeur par défaut est Désactiver.
 [VFF:CFG] AVERTISSEMENT : Le port 7 n'avait pas de section de
 configuration. La valeur par défaut est Désactiver. [VFF:CFG]
 AVERTISSEMENT : Le port 8 n'avait pas de section de configuration.
 La valeur par défaut est Désactiver. [VFF:CFG] AVERTISSEMENT :
 Le port 9 n'avait pas de section de configuration. La valeur
 par défaut est Désactiver. [VFF:CFG] Réussite de l'analyseur
```

 ©2025 Palo Alto Networks, Inc.

```
de fichiers Config/INI. [VFF:KVM] Fin de la configuration du
menu, poursuite du démarrage normal... Motif du redémarrage :
fabrication
```

Déploiements Hyper-V pris en charge par le connecteur ZTNA de Prisma Access

Vous déployez un hyperviseur Microsoft Hyper-V à l'aide d'un déploiement à deux bras. Le diagramme suivant montre un exemple de déploiement réseau de connecteur ZTNA à l'aide d'Hyper-V en mode two-arm avec une passerelle NAT.



Intégrer un connecteur ZTNA à l'aide d'Hyper-V

Pour intégrer un connecteur ZTNA à l'aide d'une machine virtuelle (VM) Microsoft Hyper-V, procédez comme suit.

Avant de commencer, assurez-vous de disposer des conditions préalables suivantes :

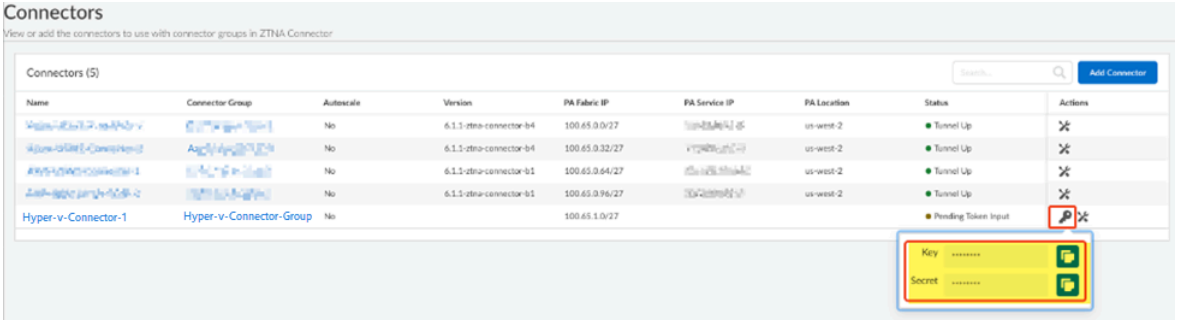
- Téléchargez l'image Hyper-V du connecteur ZTNA à partir du portail de support client (CSP) sous **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)** > **Prisma Access ZTNA Connector for Hyper-V (Connecteur ZTNA Prisma Access pour Hyper-V)**.
- Vérifiez que vous disposez d'une VM Hyper-V qui répond aux environnements d'hébergement minimaux pour le connecteur ZTNA.

STEP 1 | Créez un groupe de connecteurs et un connecteur pour la VM Hyper-V.

STEP 2 | Sélectionnez **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)**et recherchez le connecteur que vous avez créé pour la VM

 ©2025 Palo Alto Networks, Inc.

Hyper-V, puis cliquez sur **Copy Token (Copier le jeton)** dans la zone **State (État)** et copiez les valeurs de **Key (Clé)** et du **Secret**.



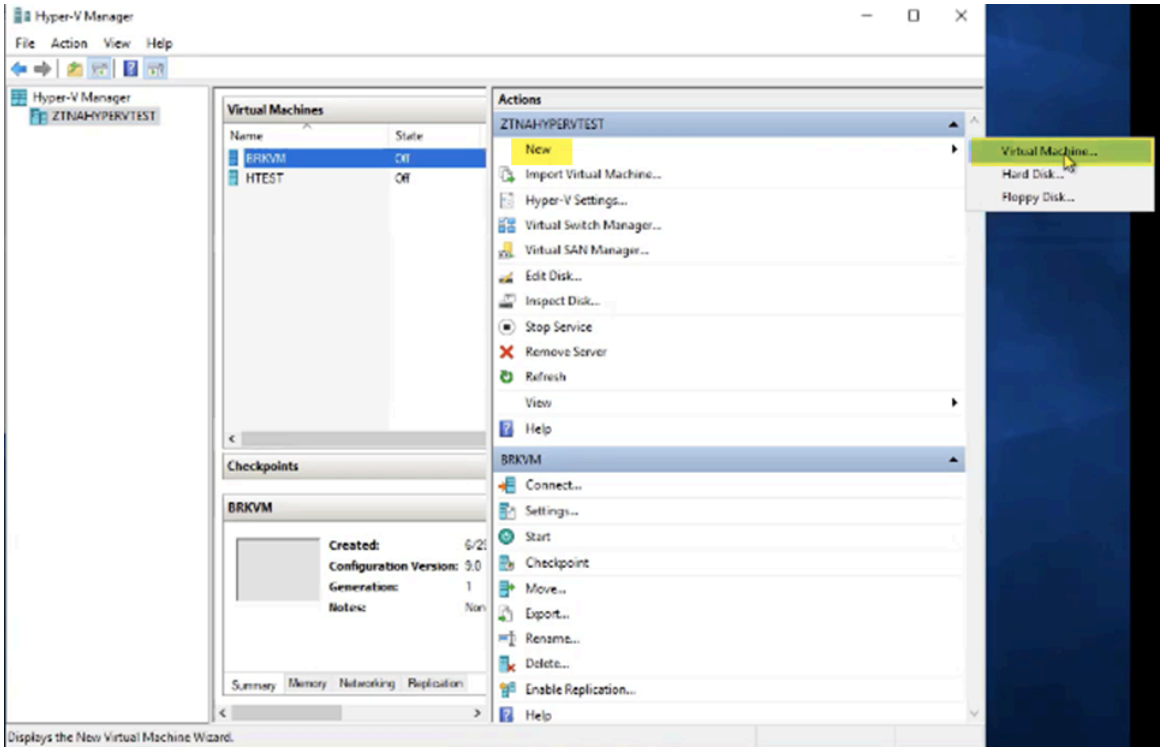
STEP 3 | Chargez l'image **vhd** que vous avez téléchargée depuis le CSP vers la VM Hyper-V.

Veillez à choisir un emplacement qui soit accessible depuis la VM Hyper-V.

Un fichier (vhd) est requis pour chaque VM Hyper-V.

STEP 4 | Accédez au Hyper-V Manager et créez une nouvelle machine virtuelle en sélectionnant **Actions** > **New (Nouvelle)** > **Virtual Machine (Machine virtuelle)**.

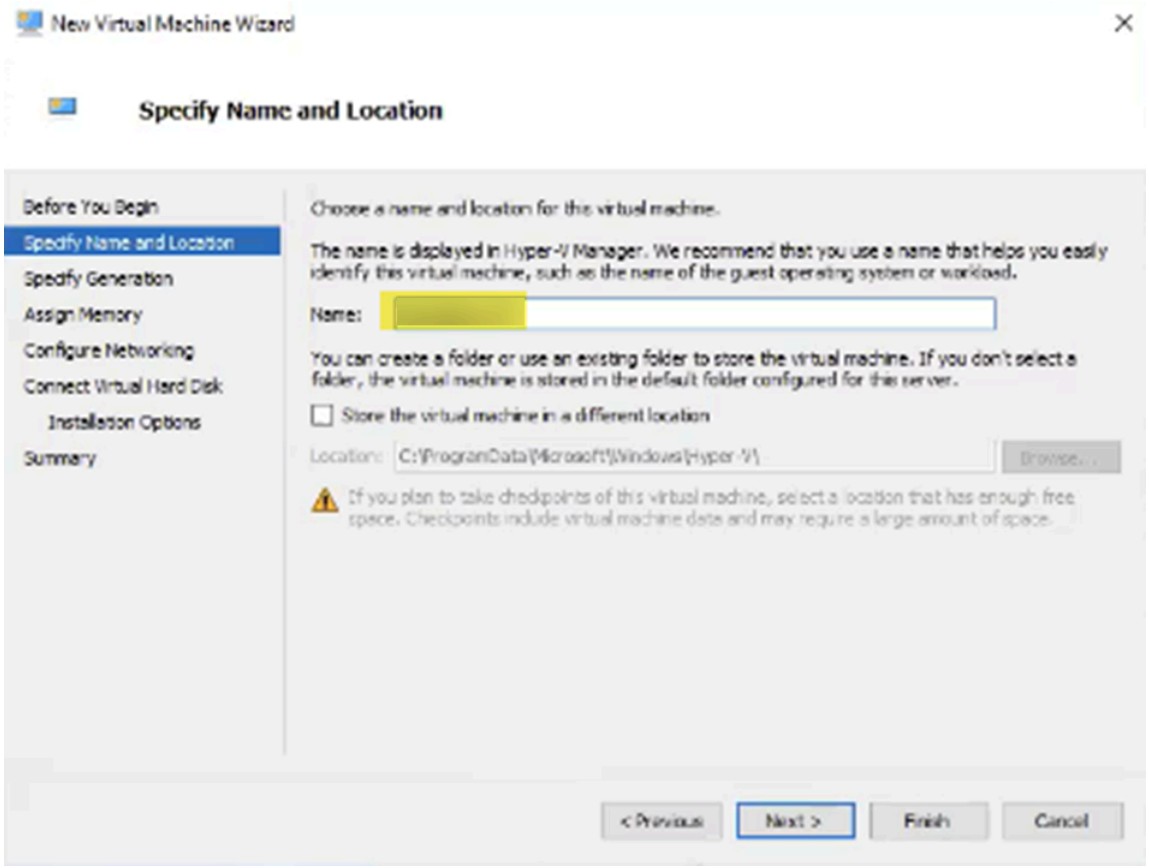
Ce flux de travail montre les étapes à effectuer pour déployer des VM Hyper-V sur un serveur Microsoft. L'interface utilisateur Hyper-V peut sembler différente dans votre environnement.



STEP 5 | Accédez à l'écran **Next (Suivant)** et saisissez un nom unique pour la VM, puis accédez à la page **Next (Suivante)**.

 ©2025 Palo Alto Networks, Inc.

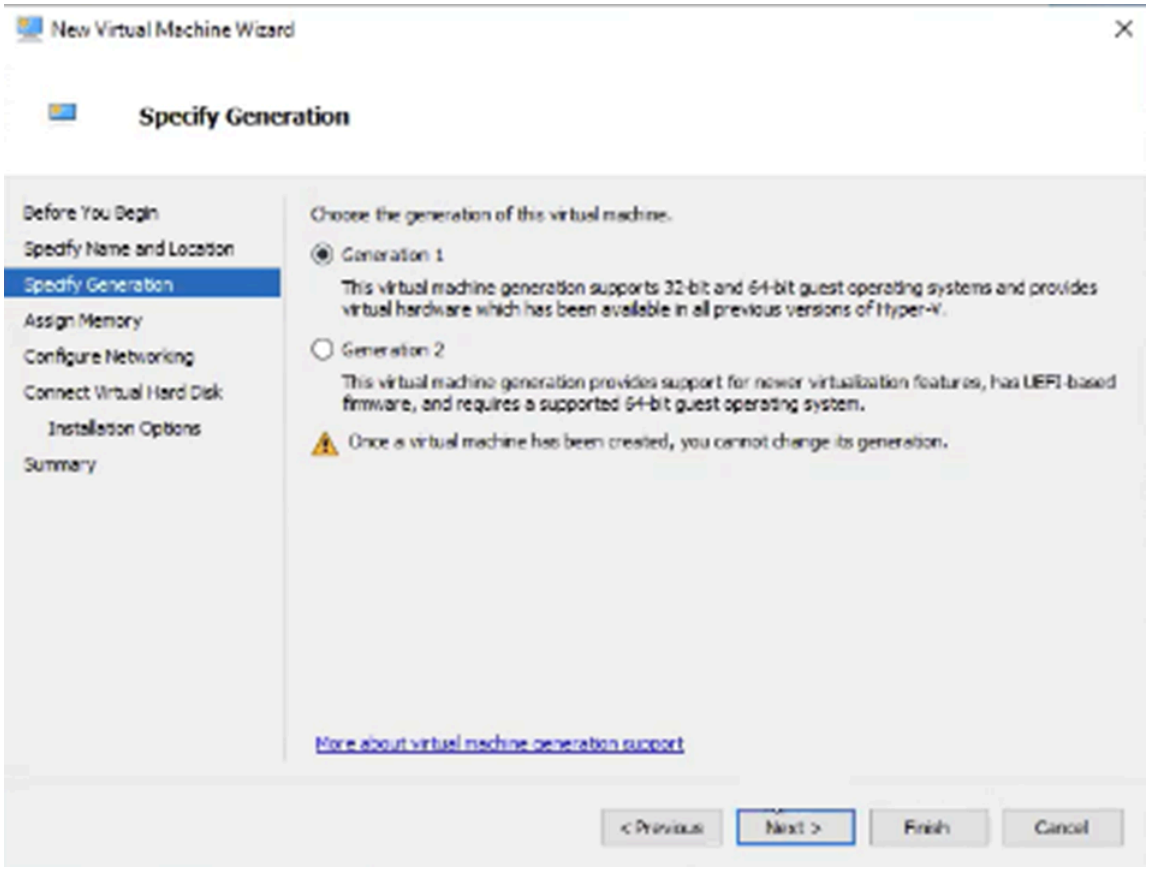
STEP 6 | (Facultatif) Pour changer l'emplacement de la VM, sélectionnez **Store the virtual machine in a different location (Stocker la machine virtuelle dans un autre emplacement)** et sélectionnez l'emplacement.



 ©2025 Palo Alto Networks, Inc.

STEP 7 | Sélectionnez **Generation 1 (Génération 1)** comme génération de VM et accédez à la page **Next (Suivant)**.

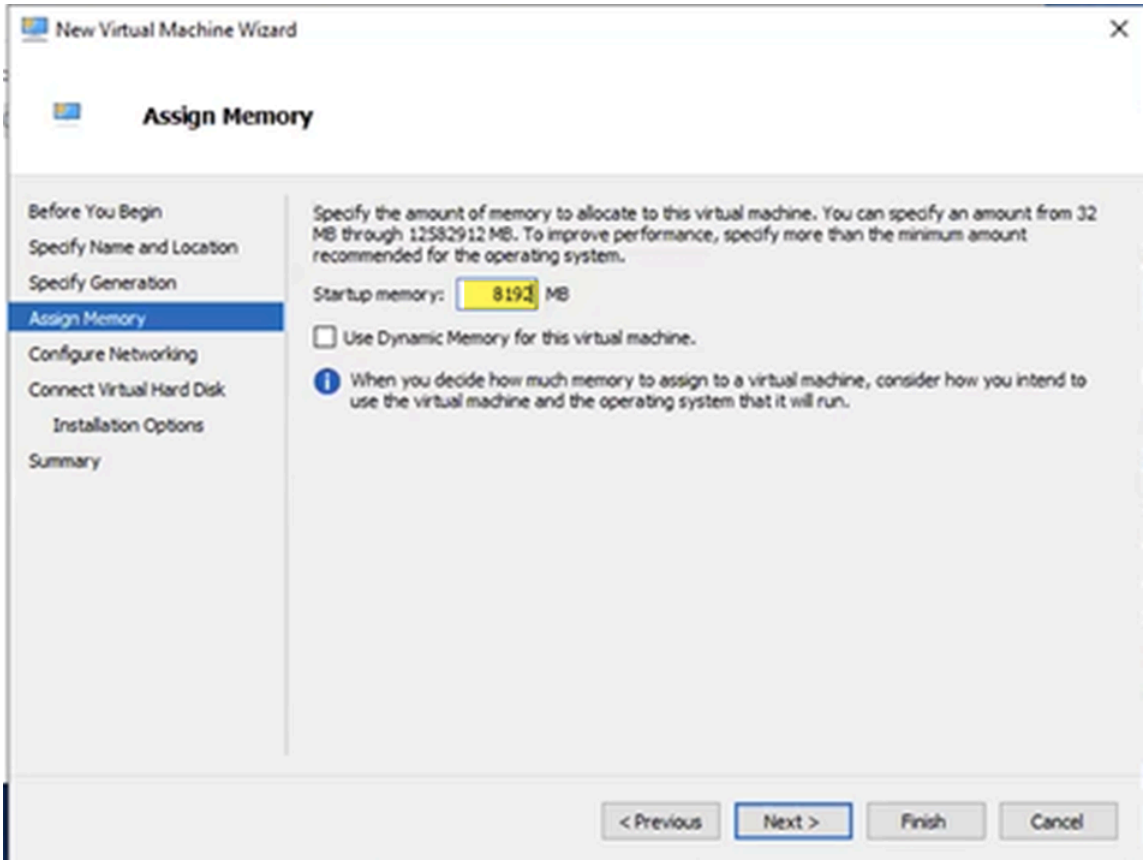
Il s'agit de la génération prise en charge par le fichier vhd du connecteur ZTNA.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | Attribuez de la mémoire à la VM.

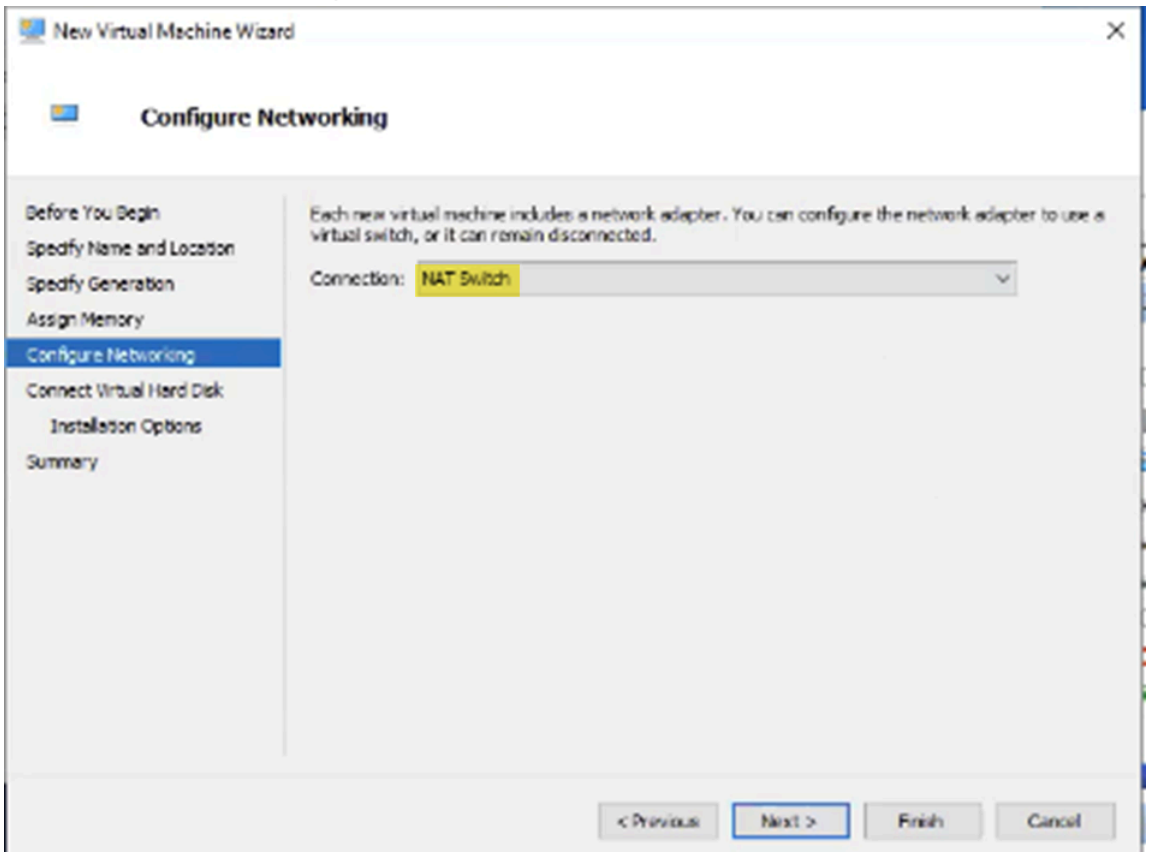
Allouez une mémoire minimale de **8 192** Mo (8 Go), ce qui répond aux exigences minimales d'une VM Hyper-V et accédez à la page **Next (Suivant)**.



 ©2025 Palo Alto Networks, Inc.

STEP 9 | Configurez la mise en réseau de votre VM, puis passez à la page **Next (Suivant)**.

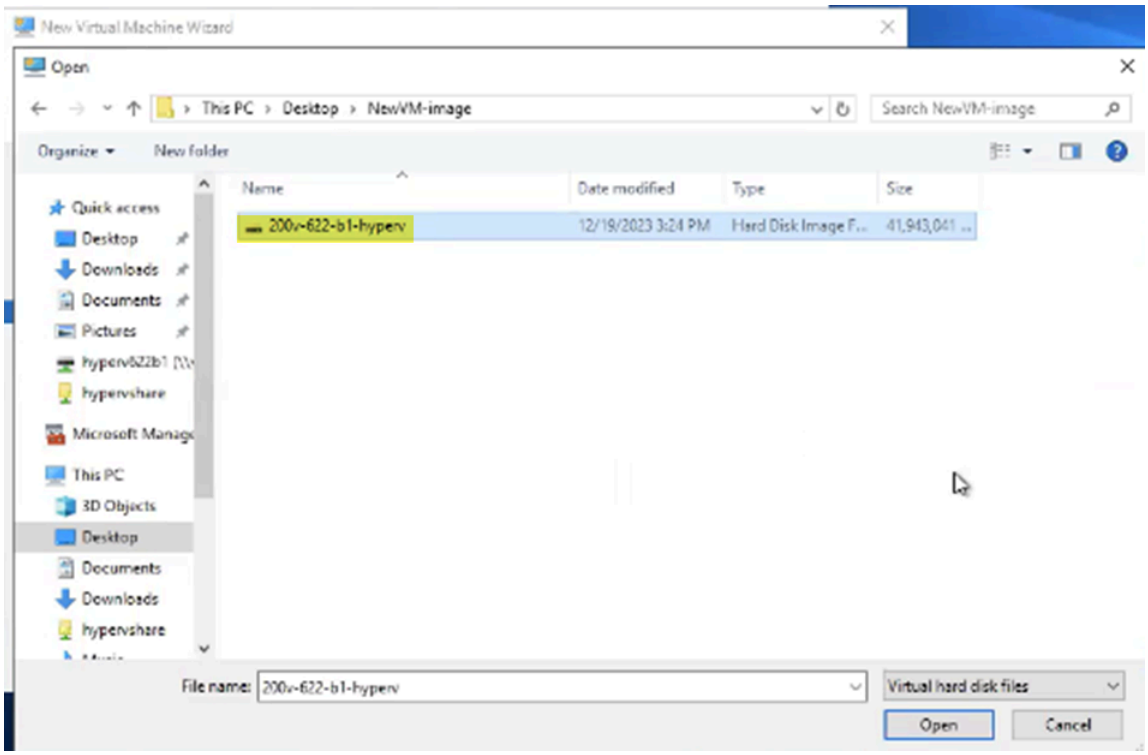
La mise en réseau que vous utilisez dépend de votre configuration. Cet exemple utilise un **NAT Switch (Commutateur NAT)** pour la mise en réseau.



 ©2025 Palo Alto Networks, Inc.

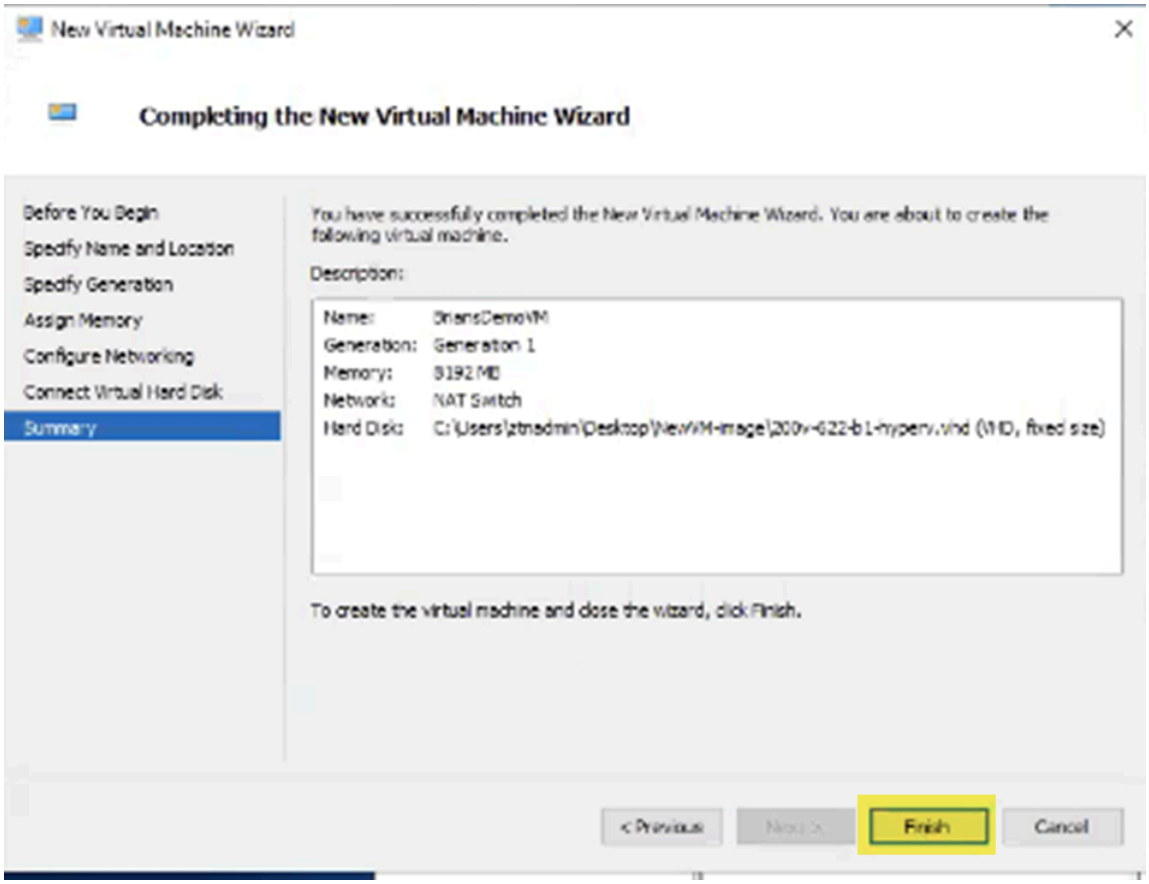
STEP 10 | Connectez le disque dur virtuel.

1. Sélectionnez **Use an existing virtual hard disk (Utiliser un disque dur virtuel existant)** et cliquez sur **Browse (Parcourir)** pour rechercher le fichier vhd que vous avez téléchargé
2. Sélectionnez le fichier vhd que vous avez téléchargé, cliquez sur **Open (Ouvrir)** pour l'ouvrir, puis passez à la page **Next (Suivant)**.



 ©2025 Palo Alto Networks, Inc.

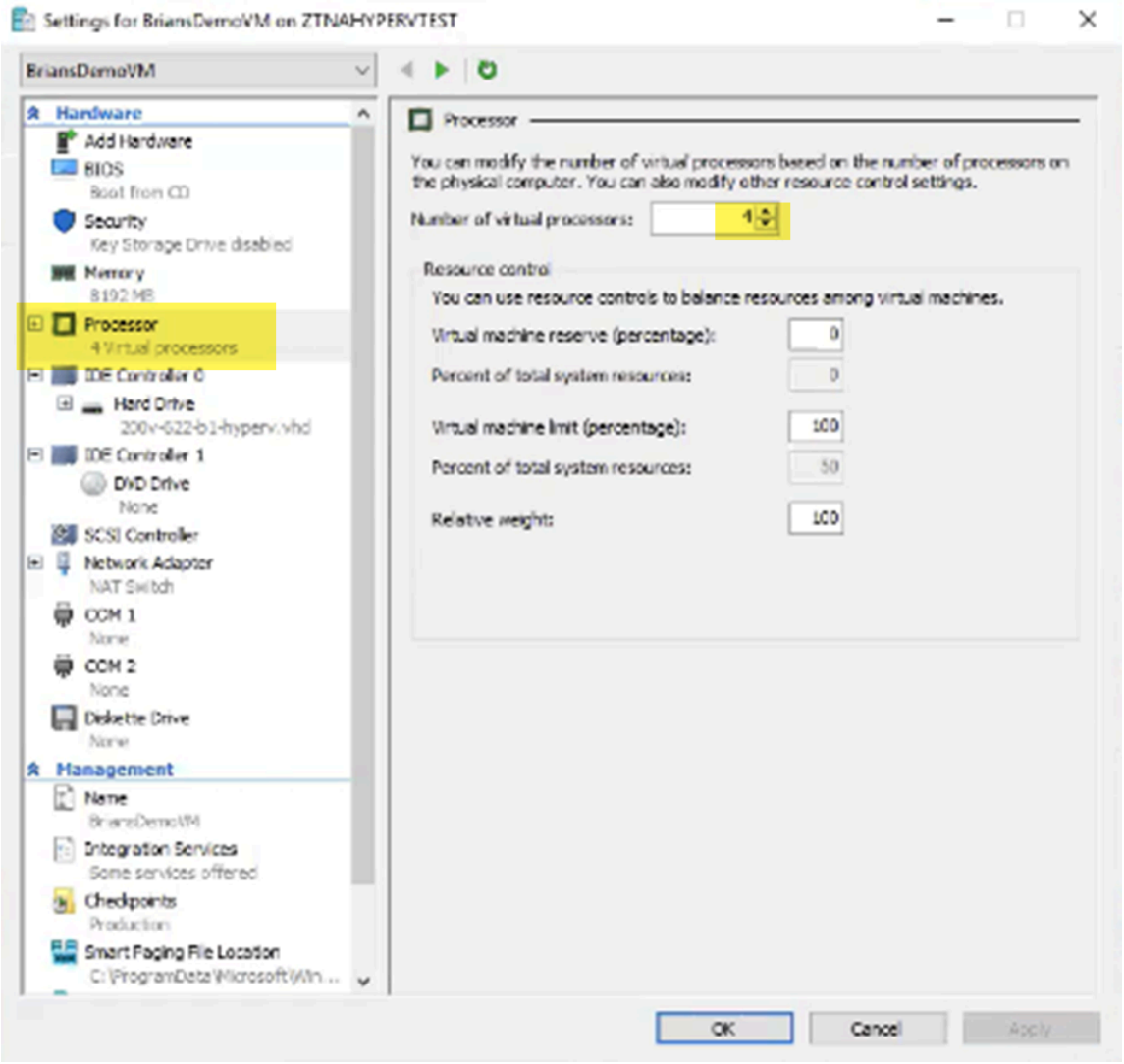
STEP 11 | Cliquez sur **Finish (Terminer)** pour terminer l'assistant de nouvelle VM.



Hyper-V crée la VM.

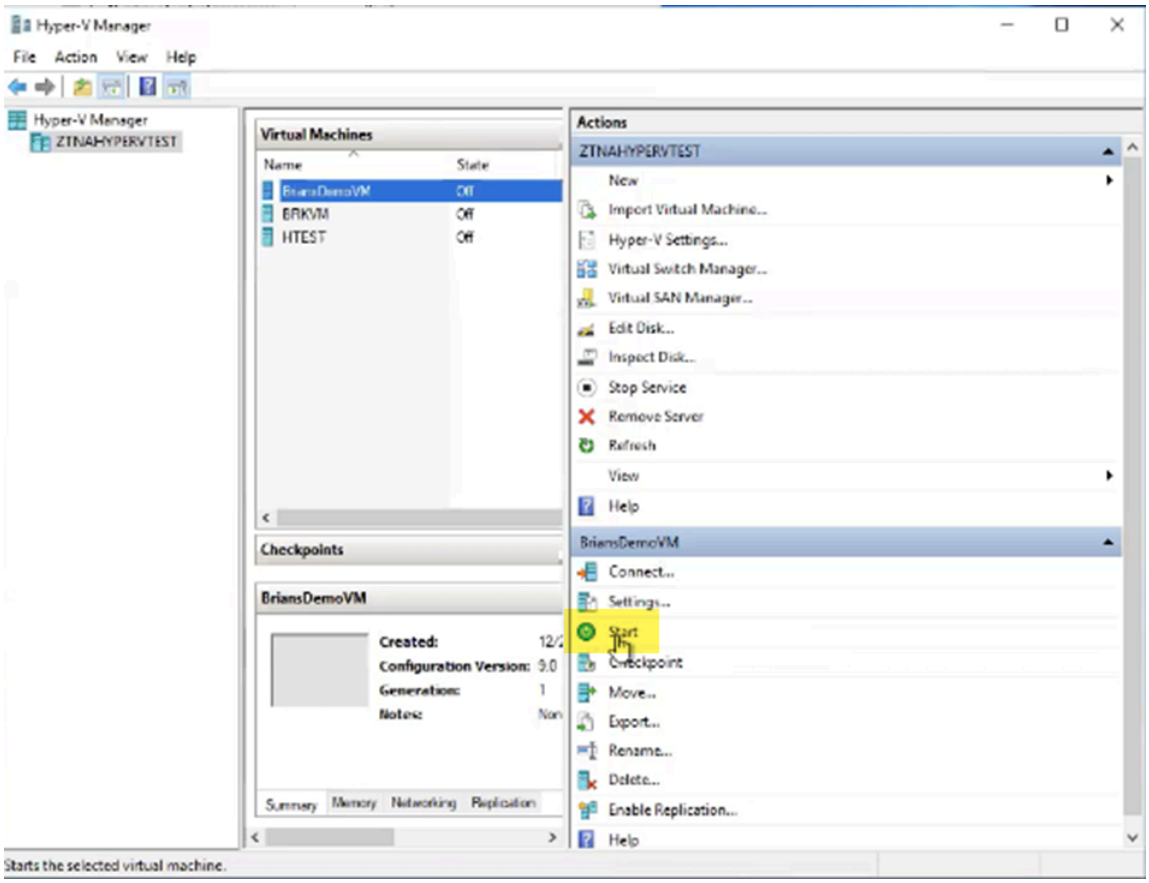
 ©2025 Palo Alto Networks, Inc.

STEP 12 | Vérifiez que votre VM dispose d'au moins quatre processeurs en accédant à la zone **Processor (Processeur)** et en vous assurant de sélectionner au moins **4** processeurs virtuels.

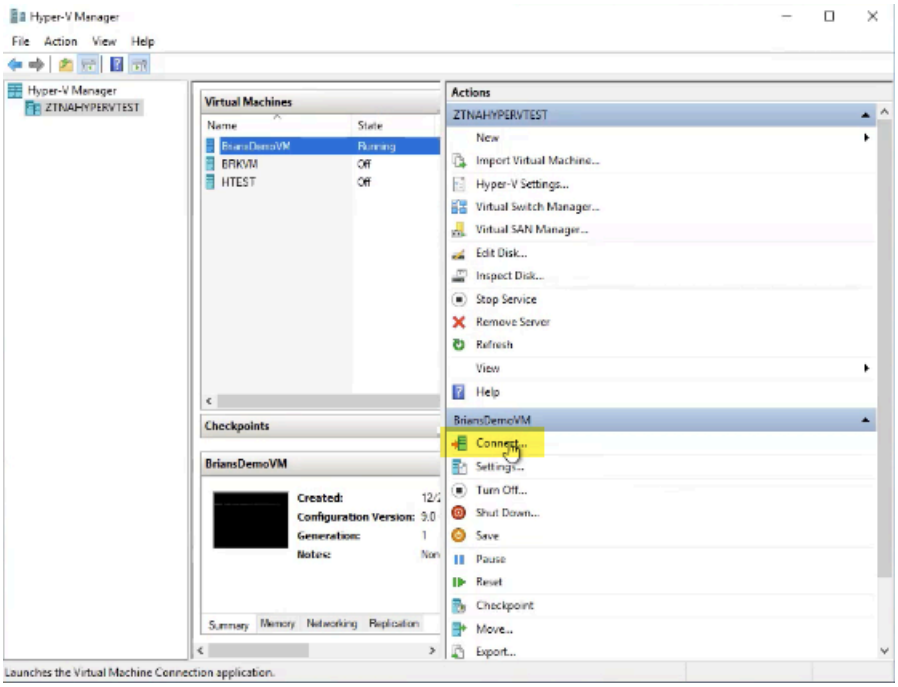


 ©2025 Palo Alto Networks, Inc.

STEP 13 | Start (Démarrez) la VM.



STEP 14 | Connect (Connectez-vous) à la console en série.



 ©2025 Palo Alto Networks, Inc.

STEP 15 | Attendez que le programme d'installation interactif CLI s'initialise, puis configurez le modèle, la clé et le secret ION.

1. Sélectionnez **1** (un modèle ION de **ion 200v**) parmi les choix qui s'affichent.

```
Sélectionnez un modèle ION : 1) ion 200v 2) ion 3102v 3) ion
 3104v 4) ion 3108v 5) ion 7108v 6) ion 7116v 7) ion 7132v 8)
 ion 9100v Choisissez un numéro ou (Q)uitter : 1 Processeur :
 Réussite (nécessite 4) Mémoire : Réussite (nécessite 8,0 Go)
 Disque : Impossible de vérifier (nécessite 40,0 G) Réseau :
 Réussite (nécessite 1) Sélectionnez un élément à modifier
 ou soumettez la configuration : 1) Modèle : ion 200v 2) Clé
 ION : 3) Clé secrète : 4) Contrôleur 1 : Contrôleur – DHCP
 5) Port 1 : Désactivé/Non utilisé 6) Port 2 : Désactivé/
Non utilisé 7) Port 3 : Désactivé/Non utilisé 8) Port 4 :
 Désactivé/Non utilisé 9) Port 5 : Désactivé/Non utilisé
 10) Port 6 : Désactivé/Non utilisé 11) Port 7 : Désactivé/
Non utilisé 12) Port 8 : Désactivé/Non utilisé 13) Port 9 :
 Désactivé/Non utilisé 14) Soumettre et redémarrer
```

2. Saisissez la clé du connecteur en sélectionnant l'option **2** et en saisissant la clé que vous avez enregistrée à partir de l'interface utilisateur du connecteur ZTNA.

```
Choisissez un numéro ou (Q)uitter : 2 Saisissez la clé ION
 [Aucune] : xxxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl
 Sélectionnez un élément à modifier ou soumettez la
 configuration : 1) Modèle : ion 200v 2) Clé ION : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Clé secrète : 4)
 Contrôleur 1 : Contrôleur – DHCP 5) Port 1 : Désactivé/
Non utilisé 6) Port 2 : Désactivé/Non utilisé 7) Port 3 :
 Désactivé/Non utilisé 8) Port 4 : Désactivé/Non utilisé 9)
 Port 5 : Désactivé/Non utilisé 10) Port 6 : Désactivé/Non
 utilisé 11) Port 7 : Désactivé/Non utilisé 12) Port 8 :
 Désactivé/Non utilisé 13) Port 9 : Désactivé/Non utilisé 14)
 Soumettre et redémarrer
```

3. Saisissez le secret du connecteur ZTNA en sélectionnant l'option **3** et en saisissant le secret que vous avez enregistré à partir de l'interface utilisateur du connecteur ZTNA.

```
Choisissez un numéro ou (Q)uitter : 3 Saisissez le secret
 ION [Aucun] : abcde12345 Sélectionnez un élément à modifier
 ou soumettez la configuration : 1) Modèle : ion 200v 2) Clé
 ION : xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Clé
 secrète : abcde12345 4) Contrôleur 1 : Contrôleur – DHCP
 5) Port 1 : Désactivé/Non utilisé 6) Port 2 : Désactivé/
Non utilisé 7) Port 3 : Désactivé/Non utilisé 8) Port 4 :
 Désactivé/Non utilisé 9) Port 5 : Désactivé/Non utilisé
 10) Port 6 : Désactivé/Non utilisé 11) Port 7 : Désactivé/
Non utilisé 12) Port 8 : Désactivé/Non utilisé 13) Port 9 :
 Désactivé/Non utilisé 14) Soumettre et redémarrer
```

 ©2025 Palo Alto Networks, Inc.

STEP 16 | Configurez les options du port WAN.

1. Sélectionnez l'option **5** (Port 1).

```
Choisissez un numéro ou (Q)uitter : 5 Port 1 : 1) Rôle :
 Désactiver 2) Annuler les changements de port 3) Appliquer et
 revenir
```

2. Sélectionnez l'option **1** (Public/WAN).

```
Choisissez un numéro ou (Q)uitter : 1 Sélectionnez le
 rôle du port : 1) Port Internet (PublicWAN) 2) Port WAN
 privé (PrivateWAN) 3) Paire de ports de contournement 1
 (port WAN) 4) Paire de ports de contournement 1 (port
 LAN) 5) Paire de ports de contournement 2 (port WAN) 6)
 Paire de ports de contournement 2 (port LAN) 7) Paire
 de ports de contournement 3 (port WAN) 8) Paire de
 ports de contournement 3 (port LAN) 9) Paire de ports
 de contournement 4 (port WAN) 10) Paire de ports de
 contournement 4 (port LAN) 11) Désactivé/Non utilisé
```

3. (Facultatif) Si vous avez besoin de définir une adresse IP statique, choisissez l'option **2** et définissez les paramètres de l'adresse IP, de la passerelle et du serveur DNS ; sinon, sélectionnez **1**.

```
Choisissez un numéro ou (Q)uitter : 1 Port 1 : 1) Rôle :
 PublicWAN 2) Configuration via : DHCP 3) Annuler les
 changements de port 4) Appliquer et revenir
```

4. Sélectionnez l'option **4** pour revenir au menu principal.

```
Choisissez un numéro ou (Q)uitter : 4 Sélectionnez un élément
 à modifier ou soumettez la configuration : 1) Modèle :
 ion 200v 2) Clé ION : xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) Clé secrète : abcde12345 4) Contrôleur 1 :
 Contrôleur – DHCP 5) Port 1 : PublicWAN – DHCP 6) Port 2 :
 Désactivé/Non utilisé 7) Port 3 : Désactivé/Non utilisé 8)
 Port 4 : Désactivé/Non utilisé 9) Port 5 : Désactivé/Non
 utilisé 10) Port 6 : Désactivé/Non utilisé 11) Port 7 :
 Désactivé/Non utilisé 12) Port 8 : Désactivé/Non utilisé
 13) Port 9 : Désactivé/Non utilisé 14) Soumettre et
 redémarrer Sélectionnez un élément à modifier ou soumettez
 la configuration : 1) Modèle : ion 200v 2) Clé ION :
 xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Clé
 secrète : abcde12345 4) Contrôleur 1 : Contrôleur – DHCP 5)
 Port 1 : PublicWAN – DHCP 6) Port 2 : Désactivé/Non utilisé
 7) Port 3 : Désactivé/Non utilisé 8) Port 4 : Désactivé/
Non utilisé 9) Port 5 : Désactivé/Non utilisé 10) Port 6 :
 Désactivé/Non utilisé 11) Port 7 : Désactivé/Non utilisé 12)
 Port 8 : Désactivé/Non utilisé 13) Port 9 : Désactivé/Non
 utilisé 14) Soumettre et redémarrer
```

 ©2025 Palo Alto Networks, Inc.

STEP 17 | Configurez les options du port LAN.

1. Sélectionnez l'option **6** (Port 2).

```
Choisissez un numéro ou (Q)uitter : 6 Port 2 : 1) Rôle :
 Désactiver 2) Annuler les changements de port 3) Appliquer et
 revenir
```

2. Sélectionnez l'option **2** (PrivateWAN).

```
Choisissez un numéro ou (Q)uitter : 2 Sélectionnez le
 rôle du port : 1) Port Internet (PublicWAN) 2) Port WAN
 privé (PrivateWAN) 3) Paire de ports de contournement 1
 (port WAN) 4) Paire de ports de contournement 1 (port
 LAN) 5) Paire de ports de contournement 2 (port WAN) 6)
 Paire de ports de contournement 2 (port LAN) 7) Paire
 de ports de contournement 3 (port WAN) 8) Paire de
 ports de contournement 3 (port LAN) 9) Paire de ports
 de contournement 4 (port WAN) 10) Paire de ports de
 contournement 4 (port LAN) 11) Désactivé/Non utilisé
```

3. (Facultatif) Si vous avez besoin de définir une adresse IP statique, choisissez l'option **2** et définissez les paramètres de l'adresse IP, de la passerelle et du serveur DNS ; sinon, sélectionnez **1**.

```
Choisissez un numéro ou (Q)uitter : 2 Port 2 : 1) Rôle :
 PrivateWAN 2) Configuration via : DHCP 3) Annuler les
 changements de port 4) Appliquer et revenir
```

4. Sélectionnez l'option **4** pour revenir au menu principal.

```
Choisissez un numéro ou (Q)uitter : 4 Sélectionnez un élément
 à modifier ou soumettez la configuration : 1) Modèle :
 ion 200v 2) Clé ION : xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) Clé secrète : abcde12345 4) Contrôleur 1 :
 Contrôleur – DHCP 5) Port 1 : PublicWAN – DHCP 6) Port 2 :
 PrivateWAN – DHCP 7) Port 3 : Désactivé/Non utilisé 8)
 Port 4 : Désactivé/Non utilisé 9) Port 5 : Désactivé/Non
 utilisé 10) Port 6 : Désactivé/Non utilisé 11) Port 7 :
 Désactivé/Non utilisé 12) Port 8 : Désactivé/Non utilisé 13)
 Port 9 : Désactivé/Non utilisé 14) Soumettre et redémarrer
```

STEP 18 | Enregistrez et redémarrez le connecteur.

```
Choisissez un numéro ou (Q)uitter : 14 AVERTISSEMENT ! Une
 fois cette configuration soumise, tout le matériel sera signé,
 enregistré et lié de manière permanente à la clé ION/clé secrète
 dans le contrôleur cloud Prisma SDWAN. CELA SIGNIFIE que le
 matériel ne peut pas être ajouté/supprimé (disques, cartes
 réseau) après la fonction de « SOUMISSION ». Si des modifications
 matérielles sont nécessaires après cette « SOUMISSION », l'ION
 devra être redéployé avec une nouvelle clé ION et une nouvelle
 clé secrète. S'il est nécessaire d'ajouter ou de supprimer
 du matériel, veuillez répondre par « N » ci-dessous, arrêter
 l'ION et effectuer les modifications maintenant. Soumettre
 ces modifications maintenant ? [N] : y Configuration de
```

 ©2025 Palo Alto Networks, Inc.

```
 construction... [VFF:CFG] Démarrage de la configuration ZeroTouch
 – analyseur du fichier de configuration [VFF:CFG] Tentative
 de chargement/analyse en tant que fichier de configuration/
INI. [VFF:CFG] Fichier de style de configuration chargé avec
 succès. [VFF:CFG] Contrôleur 1 défini avec succès sur CONTRÔLEUR/
DHCP. [VFF:CFG] Port 1 défini avec succès sur PUBLICWAN/DHCP.
 [VFF:CFG] Port 2 défini avec succès sur PRIVATEWAN/DHCP. [VFF:CFG]
 AVERTISSEMENT : Le port 3 n'avait pas de section de configuration.
 La valeur par défaut est Désactiver. [VFF:CFG] AVERTISSEMENT :
 Le port 4 n'avait pas de section de configuration. La valeur
 par défaut est Désactiver. [VFF:CFG] AVERTISSEMENT : Le port 5
 n'avait pas de section de configuration. La valeur par défaut est
 Désactiver. [VFF:CFG] AVERTISSEMENT : Le port 6 n'avait pas de
 section de configuration. La valeur par défaut est Désactiver.
 [VFF:CFG] AVERTISSEMENT : Le port 7 n'avait pas de section de
 configuration. La valeur par défaut est Désactiver. [VFF:CFG]
 AVERTISSEMENT : Le port 8 n'avait pas de section de configuration.
 La valeur par défaut est Désactiver. [VFF:CFG] AVERTISSEMENT :
 Le port 9 n'avait pas de section de configuration. La valeur
 par défaut est Désactiver. [VFF:CFG] Réussite de l'analyseur
 de fichiers Config/INI. [VFF:KVM] Fin de la configuration du
 menu, poursuite du démarrage normal... Motif du redémarrage :
 fabrication
```

 ©2025 Palo Alto Networks, Inc.

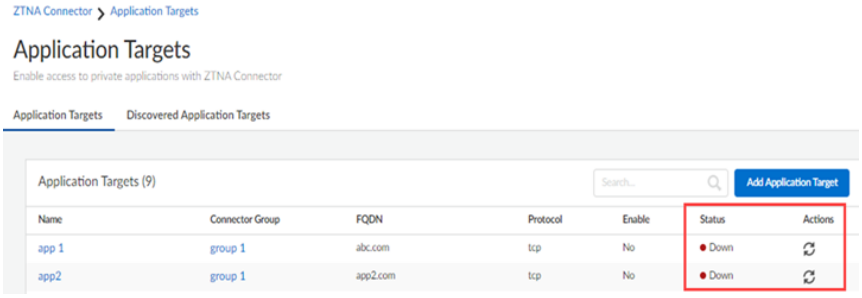
Surveiller le connecteur ZTNA

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend 200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

Tous les composants du connecteur ZTNA fournissent des informations d'état claires, des journaux et des outils de diagnostic pour vous aider à résoudre les problèmes qui surviennent. Utilisez les outils suivants pour surveiller le déploiement du connecteur ZTNA.

©2025 Palo Alto Networks, Inc.

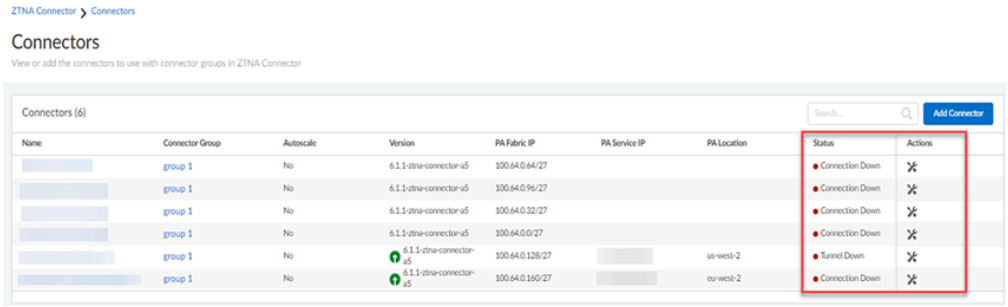
- Vous pouvez consulter l'état des applications et connecteurs depuis la plateforme Prisma SASE.
  - Sélectionnez **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Application Targets (Cibles d'application)** et vérifiez que le **Status (État)** de toutes les cibles d'application indique **Up (Actif)**.



Si l'état indique **Down (Inactif)**, le connecteur ne peut pas atteindre l'application. Après avoir résolu le problème avec l'application, cliquez sur le bouton d'actualisation de l'état dans la colonne **Action** et vérifiez que le **Status (État)** passe à **Up (Actif)** (l'état s'actualise automatiquement une fois par minute).

L'état indique également Up (Actif) si l'application est accessible depuis le connecteur ZTNA (sur la base du dernier résultat de résolution DNS réussi), mais que la résolution DNS du FQDN de l'application échoue depuis le connecteur ZTNA.

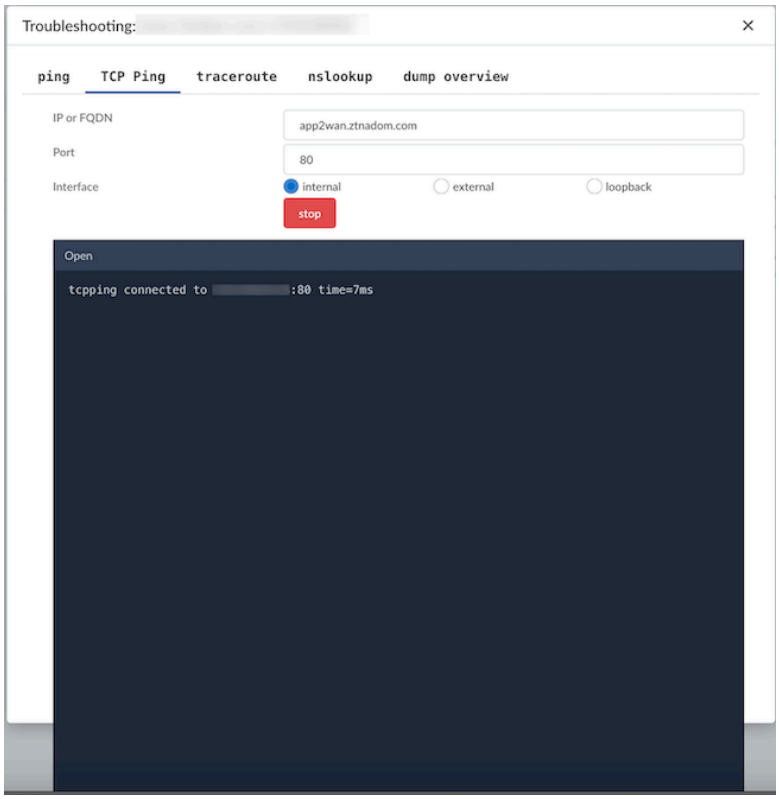
- Sélectionnez **Workflows (Flux de travail)** > **ZTNA Connector (Connecteur ZTNA)** > **Connectors (Connecteurs)** et vérifiez que le **Status (État)** de tous les connecteurs indique **Up (Actif)**.



Si le **Status (État)** indique **Tunnel Down (Tunnel inactif)**, cela signifie que le tunnel IPSec entre la VM du connecteur et Prisma Access est inactif. Si le **Status (État)** indique **Connection Down (Connexion inactive)**, cela signifie que la VM du connecteur est inactive. Cliquez sur l'icône de diagnostic pour lancer une connexion shell distante au connecteur pour résoudre le problème. Vous pouvez exécuter une requête **`ping`**, **`TCP`**

 ©2025 Palo Alto Networks, Inc.

`Ping`, **`traceroute`**, **`nslookup`** ou **`dump overview`** pour vous aider à diagnostiquer le problème de connectivité.



 ©2025 Palo Alto Networks, Inc.

Afficher les journaux du connecteur ZTNA

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ Licence complémentaire du connecteur ZTNA La licence Essential avec la licence complémentaire comprend 8 connecteurs ZTNA, 100 FQDN et 4 fonctionnalités de sous-réseau IP. La licence Advanced avec la licence complémentaire comprend 40 connecteurs ZTNA, 300 FQDN et 1 024 fonctionnalités de sous-réseau IP. La licence Premium avec la licence complémentaire comprend 200 connecteurs ZTNA, 4 000 FQDN et 1 024 fonctionnalités de sous-réseau IP. ❑ Si vous n'achetez pas la licence complémentaire du connecteur ZTNA, les licences Prisma Access incluent quatre connecteurs, 40 FQDN et quatre sous-réseaux IP. Cette fonctionnalité est fournie dans le but d'essayer les connecteurs ZTNA dans votre environnement.

Tout le trafic du connecteur ZTNA est enregistré dans le Strata Logging Service. Pour stocker des journaux Prisma Access dans Strata Logging Service, vous devez estimer et acheter la quantité appropriée de stockage de journaux dans Strata Logging Service. Nous vous recommandons d'augmenter le pourcentage de votre capacité de stockage totale Strata Logging Service de 10 % pour stocker les journaux du connecteur ZTNA.

Assurez-vous d'avoir configuré un profil de transfert de journaux qui transfère les types de journaux souhaités au service de journalisation Strata. Strata Logging Service enverra une notification par e-mail pour acheter plus de stockage lorsque le quota de stockage des journaux atteindra 90 %. Si vous n'achetez pas plus de stockage, les anciens journaux seront supprimés.

Indépendamment de l'interface de gestion que vous utilisez pour Prisma Access (Panorama ou Cloud Management), vous pouvez consulter vos journaux dans Prisma Access (Managed by Strata Cloud Manager) sous **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)**.

Le connecteur ZTNA fournit les journaux réseau suivants.

 ©2025 Palo Alto Networks, Inc.

- Les **journaux d'audit** sont disponibles via la plateforme Prisma SASE et fournissent des enregistrements des modifications de configuration des administrateurs dans le connecteur ZTNA. Vous pouvez utiliser ces journaux à des fins de conformité et de résolution de problèmes.

  Vous pouvez filtrer les journaux d'audit par intervalle de temps, site, périphérique et type. Les journaux d'audit fournissent les détails suivants :

  - Nombre de tentatives de connexion à un portail d'entreprise par un utilisateur spécifique depuis une adresse IP particulière.
  - S'il s'agit d'une application ou d'un connecteur d'application qui est intégré(e) ou supprimé(e).
  - Lorsqu'une mise à niveau du connecteur est planifiée.
  - Affichage de toutes les modifications du système et des accès tentés.

  Les journaux d'audit du connecteur ZTNA ne sont pas disponibles dans l'interface Web Prisma Access. Pour consulter les journaux d'audit, vous devez ouvrir une demande d'assistance auprès du support technique de Palo Alto Networks.
- **Les journaux de trafic** affichent une entrée au début et à la fin de chaque session. Chaque entrée contient la date et l'heure, les zones source et de destination, des adresses et des ports, le nom de l'application, le nom de la règle de sécurité appliquée au flux, l'action de la règle (allow (autoriser), deny (refuser) ou drop (supprimer)), l'interface d'entrée et de sortie, ainsi que le nombre d'octets et le motif de fin de session.
  - La colonne Type indique si l'entrée correspond au début ou à la fin de la session.
  - La colonne Action indique si le pare-feu a autorisé, refusé ou supprimé la session.
  - Une suppression indique que la règle de sécurité qui bloquait le trafic a spécifié n'importe quelle application, alors qu'un refus indique que la règle a identifié une application spécifique.
  - Si le pare-feu supprime le trafic avant d'identifier l'application, comme lorsqu'une règle supprime l'ensemble du trafic d'un service spécifique, la colonne Application (Application) affiche non-applicable.
  - L'App-ID pour un connecteur ZTNA est l'App-ID personnalisé.
  - Si le trafic atteint la passerelle d'utilisateur mobile, la colonne **Destination Address (Adresse de destination)** affiche l'adresse IP RFC 6598.
- **Les journaux de configuration** affichent des entrées pour des modifications de la configuration du connecteur ZTNA. Chaque entrée inclut la date et l'heure, le nom d'utilisateur de l'administrateur, l'adresse IP correspondant à l'emplacement où l'administrateur a apporté une modification, le type de client, le type de commande exécutée, l'état de la commande (réussite ou échec), le chemin de la configuration et les valeurs avant et après la modification.
- Strata Cloud Manager
- Panorama

Afficher les journaux du connecteur ZTNA (Panorama)

Utilisez le flux de travail suivant pour afficher les journaux du connecteur ZTNA dans Prisma Access (Managed by Panorama) Access.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Connectez-vous à Prisma Access.

STEP 2 | Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)**.

STEP 3 | Sélectionnez un type de journal dans la liste : Journaux **Audit**, **Traffic (Trafic)**et **Config (Configuration)** Journaux.

STEP 4 | Cliquez sur la flèche qui se trouve à la droite des en-têtes des colonnes, puis sélectionnez **Columns (Colonnes)** .

STEP 5 | Sélectionnez les colonnes à afficher dans la liste. Le journal se met à jour automatiquement pour correspondre à vos sélections.

STEP 6 | Cliquez sur l'icône **Spyglass (Longue-vue)** pour une entrée de journal spécifique. La **Detailed Log View (Vue détaillée du journal)** contient plus d'informations sur la source et la destination de la session ainsi qu'une liste de sessions associée à l'entrée du journal.

Afficher les journaux du connecteur ZTNA (Strata Cloud Manager)

Utilisez le workflow suivant pour afficher les journaux du connecteur ZTNA dans Prisma Access géré par le cloud.

STEP 1 | Connectez-vous à Prisma Access (Managed by Strata Cloud Manager).

STEP 2 | Sélectionnez **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)**.

STEP 3 | Sélectionnez le type de journal que vous souhaitez afficher : Journaux d'audit, de pare-feu/trafic et de configuration.

STEP 4 | Sélectionnez un intervalle de temps pour laquelle vous souhaitez afficher les journaux.

STEP 5 | Fournissez cette chaîne de requête pour affiner la liste des journaux du connecteur ZTNA : **Subtype = 'netflow' AND Device Name = 'PA_CONN' (Sous-type = 'netflow' ET Nom du périphérique = 'PA_CONN')**.

Les journaux incluent les détails suivants :

- Horodatage
- Nom du connecteur
- Adresse IP source d'origine du client
- Port source d'origine du client
- Adresse IP traduite du connecteur
- Port traduit du connecteur
- Adresse IP de destination traduite
- Port de destination traduit

 ©2025 Palo Alto Networks, Inc.

Préserver le mappage User-ID pour les connexions de connecteurs ZTNA avec le source NAT

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 5.1.1

Vous pouvez utiliser le connecteur ZTNA dans Prisma Access pour sécuriser des applications privées. Pour limiter l'accès aux applications en fonction de User-ID, vous pouvez déployer un pare-feu nouvelle génération (NGFW) dans le centre de données ou dans l'emplacement du siège où se trouvent les applications privées ; puis, configurez les règles de politique sur le NGFW en fonction du mappage de User-ID.

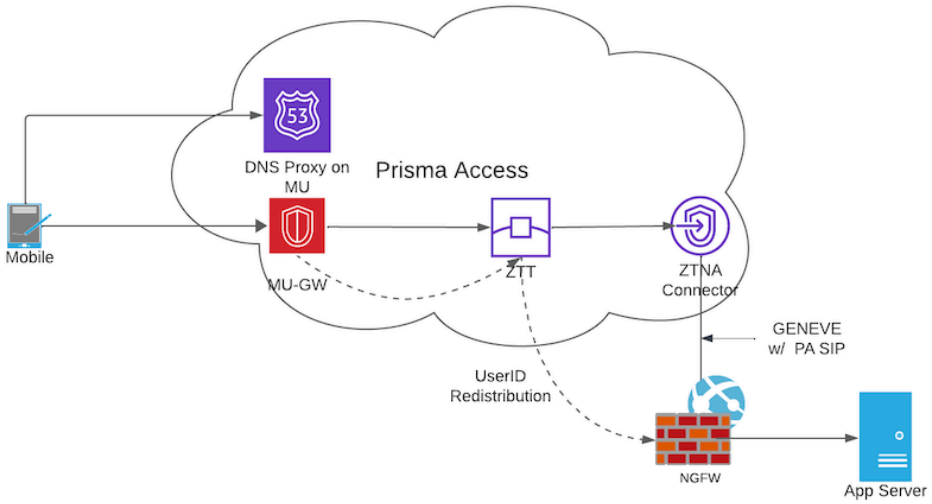
Si votre déploiement utilise un pare-feu nouvelle génération (NGFW) dans le centre de données ou l'emplacement du siège où se trouvent les applications privées, et que le connecteur ZTNA Connector le NAT source, le NGFW ne peut pas récupérer le mappage User-ID. Le NAT source sur le connecteur ZTNA empêche NGFW d'obtenir l'adresse IP du client, ce qui est essentiel pour le mappage. Si le NGFW ne peut pas récupérer cette adresse IP client, il ne peut pas appliquer les règles de politique de sécurité basées sur les zones que vous avez créées sur lui en fonction du mappage User-ID.

Le connecteur ZTNA a les responsabilités suivantes pour activer User-ID au sein du centre de données sécurisé du NGFW :

1. Fournir une connexion sécurisée du NGFW aux terminateurs de tunnel de connecteurs (ZTT) régionaux ZTNA pour que le NGFW puisse se connecter à son agent de redistribution User-ID.
2. Pour les applications FQDN, la sonde d'état étant réglée sur tcpping, l'application sonde les applications du centre de données pour déterminer si l'application est en place et accessible depuis ce connecteur individuel.
3. Encapsulez les paquets IP post NAT de l'espace de centre de données utilisateur à application dans un paquet Geneve incluant l'adresse IP source d'origine en option.

Le diagramme suivant illustre les éléments de réseau qui fournissent l'adresse IP source au mappage User-ID au NGFW et fournissent des paquets de données encapsulés Generic Network Virtualization Encapsulation (Geneve), y compris l'option originale d'adresse IP source Prisma Access au NGFW. Ces éléments permettent à la NGFW d'appliquer efficacement les règles de politique de sécurité basées sur User-ID.

 ©2025 Palo Alto Networks, Inc.



Restrictions :

- Le support User-ID avec le connecteur ZTNA n'est disponible qu'après ces versions :
  - Plan de données Prisma Access : Version 10.2.4 et versions ultérieures
  - Saas_agent : Version 5.1.0 et versions ultérieures
  - Version de NGFW : Version 11.2.0 et versions ultérieures
  - Version du connecteur : 6.2.4-ztna-connector-b3 version et versions ultérieures
- Le sondage ICMP n'est pas pris en charge pour les cibles FQDN, qui sont attachées à des groupes de connecteurs basés sur User-ID.
- La configuration d'itinéraire de service NGFW pour un agent UID ne prend en charge que les interfaces avec des adresses IP statiques. Si l'interface NGFW est configurée pour être en mode dynamique (attribution d'adresse IP via DHCP), le canal User-ID de NGFW à ZTT ne peut pas établir la prise en charge de User-ID du connecteur ZTNA. Pour résoudre ce problème, vous devez configurer l'interface à utiliser pour l'agent UID sur NGFW avec une adresse IP statique.
- Les outils de diagnostic comme ping et traceroute ne sont pas pris en charge pour les connecteurs basés sur User-ID.

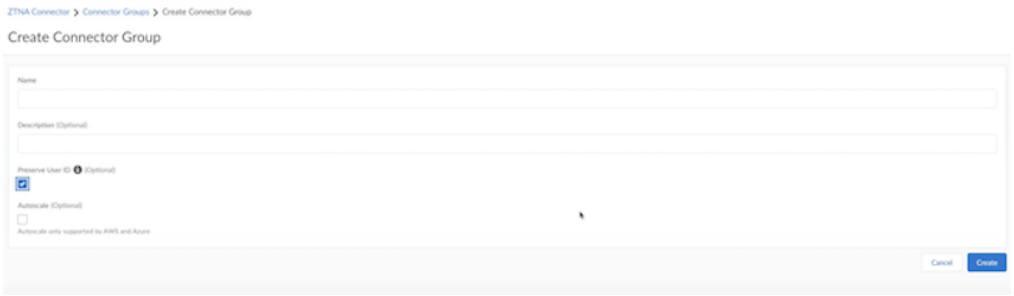
Cette procédure suppose que vous disposez des configurations réseau suivantes :

- Vous avez déployé un NGFW au siège ou au centre de données où se trouvent les applications privées.
- Vous avez appliqué des règles de politique de sécurité sur NGFW en fonction des zones (zone non approuvée et zone approuvée) que vous avez créées dans la NGFW. Ces règles de politique de sécurité incluent l'application de User-ID.

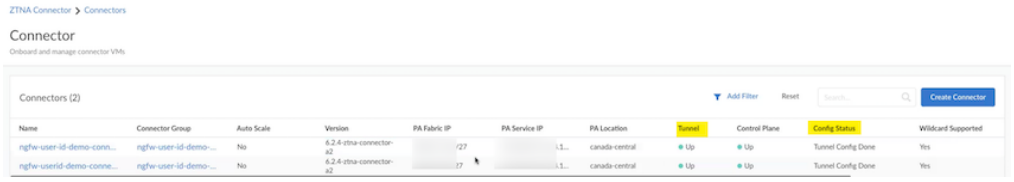
Pour vous assurer que votre réseau distribue le mappage User-ID au siège ou au centre de données, suivez la procédure indiquée ci-dessous, qui permet à NGFW d'appliquer les règles de politique de sécurité basées sur le mappage User-ID qu'elle apprend de GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

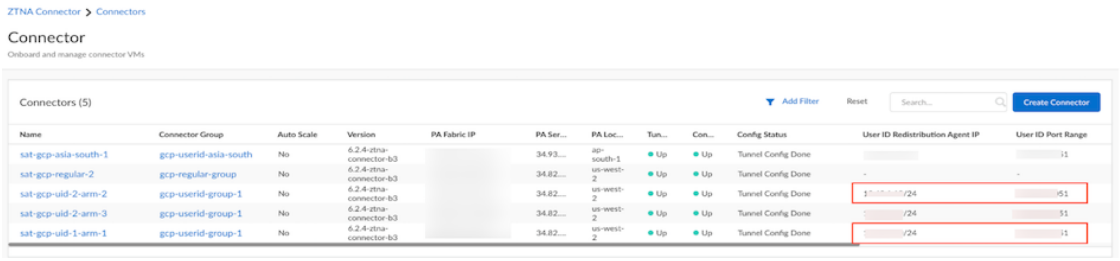
STEP 1 | Créez un groupe de connecteurs, activez **Preserve User ID (Préserver User-ID)** et ajoutez les connecteurs.



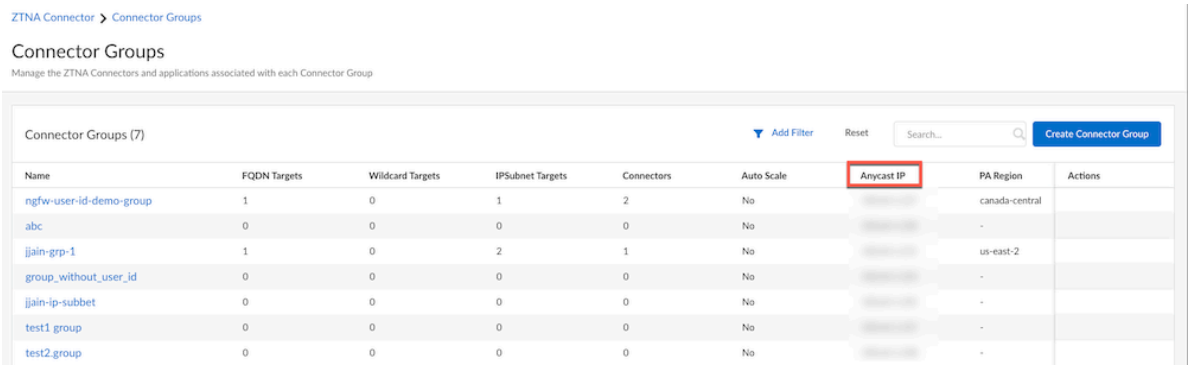
STEP 2 | Déployez et embarquez les connecteurs dans votre centre de données et vérifiez si les tunnels sont actifs et fonctionnent.



STEP 3 | Accédez à **Connector (Connecteur)** et notez l'**User ID Redistribution Agent IP (Adresse IP de redistribution User-ID)** et la **User ID Port Range (Plage de ports User-ID)** pour votre connecteur. Vous avez besoin de ces adresses IP et plages de ports pour configurer les agents de redistribution User-ID sur NGFW.



Allez également dans **Connector Groups (Groupes de connecteurs)** et notez **Anycast IP (Adresse IP Anycast)**. Cette adresse IP est requise pour configurer les règles de politique de sécurité NGFW afin d'autoriser le sondage d'applications TCP à partir de cette adresse IP source.



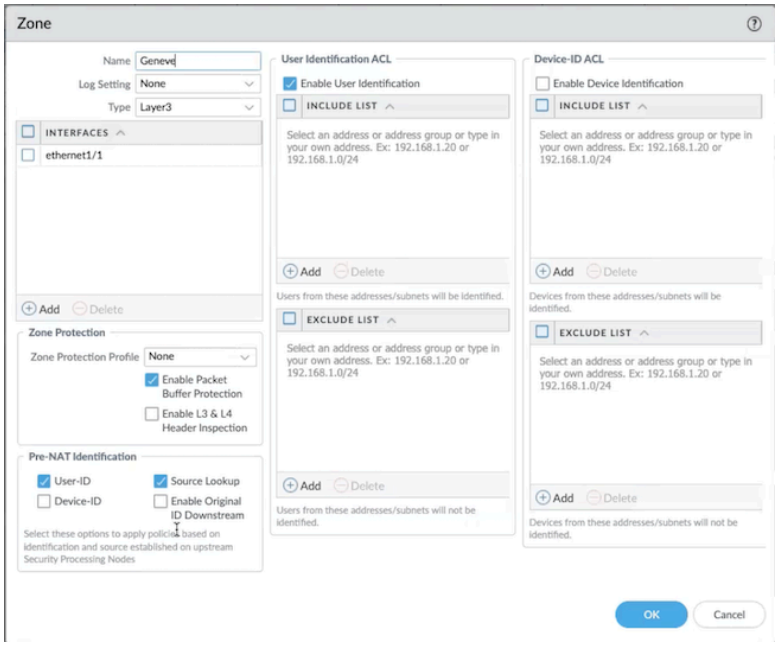
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Saisissez les paramètres d'identification pré-NAT sur NGFW.

1. Connectez-vous à l'interface utilisateur NGFW, allez dans **Network (Réseau)** > **Zones** et **Add (Ajoutez)** deux zones (zone pour l'interface de connexion du connecteur ZTNA et zone pour l'interface de connexion du serveur d'applications) ou sélectionnez l'existante.

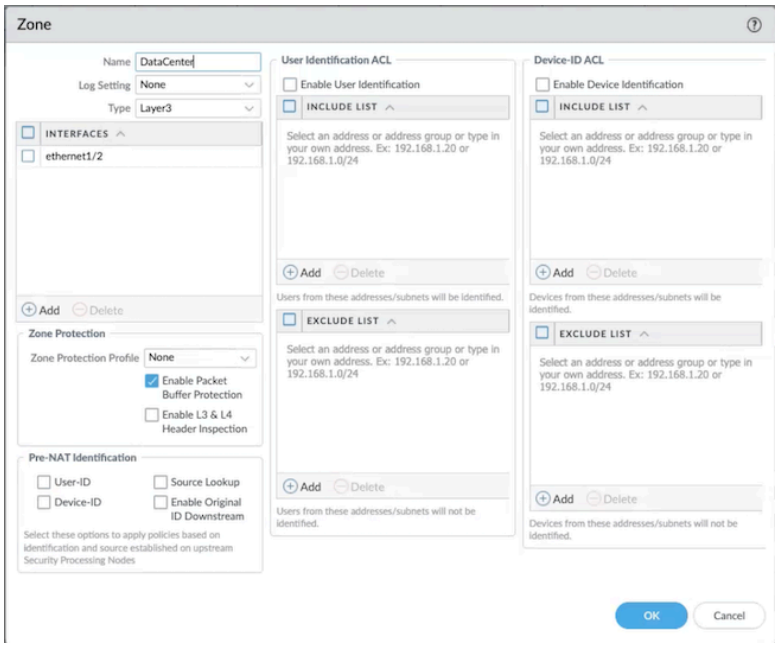
   1. Sélectionnez les paramètres **Pre-NAT Identification (Identification pré-NAT)** suivants pour la zone avec l'interface de connexion du connecteur ZTNA :

      - **User-ID** : préserve le mappage User-ID de l'utilisateur mobile utilisé avant la NAT des adresses IP. Activez cette option si vous utilisez User-ID dans les règles de politique de sécurité.
      - **Source Lookup (Recherche de source)** : vous permet de faire correspondre l'adresse IP source d'origine reçue de GlobalProtect.

   2. Pour l'interface se connectant à la zone du serveur d'applications, vous n'avez pas à sélectionner de paramètres **Pre-NAT Identification (Identification pré-NAT)**.

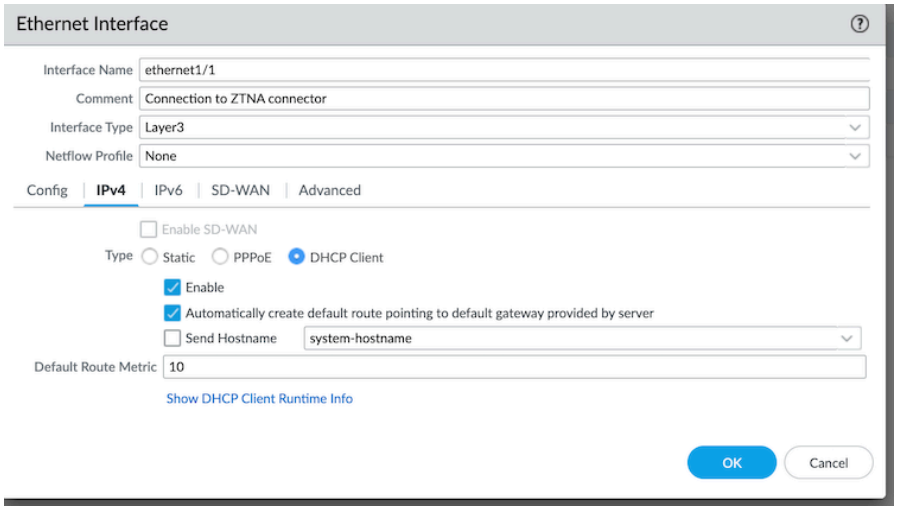
 ©2025 Palo Alto Networks, Inc.



3. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

2. Ajoutez les adresses IP aux interfaces.

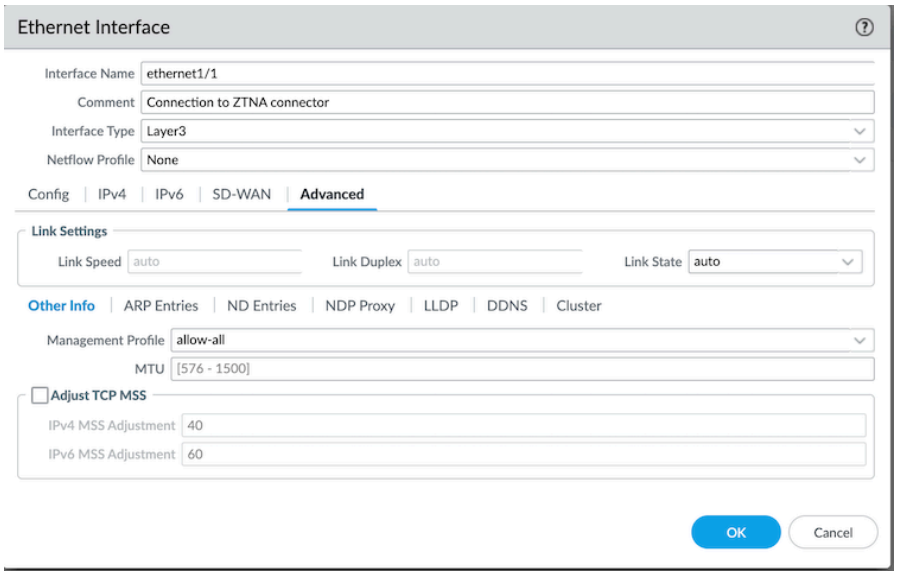
   1. Accédez à **Network (Réseau)** > **Interfaces** > **Ethernet**.
   2. Sélectionnez l'interface qui se connecte au connecteur ZTNA et au serveur d'applications, puis configurez-les. Ajoutez l'**Interface name (Nom de l'interface)** et l'**Interface type (Type d'interface)** au **Layer 3 (Calque 3)**.



   3. Pour l'interface Ethernet connectée au serveur d'applications, désactivez la case à cocher **Automatically create default route pointing to default gateway provided by**

 ©2025 Palo Alto Networks, Inc.

server (Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur).



3. Allez dans **Interfaces** et ajoutez les adresses IP statiques aux interfaces. Ajoutez l'interface orientée connecteur ZTNA dans la zone du connecteur ZTNA (Geneve) et l'interface orientée serveur d'applications dans la zone du serveur d'applications (centre de données).

STEP 5 | Créez une session d'interface en ligne de commande (CLI) avec NGFW et saisissez la commande suivante dans le mode de configuration :

```
set deviceconfig setting preserve-prenat-feature yes
```

Si vous devez désactiver cette fonctionnalité à l'avenir, saisissez `set deviceconfig setting preserve-prenat-feature no`.

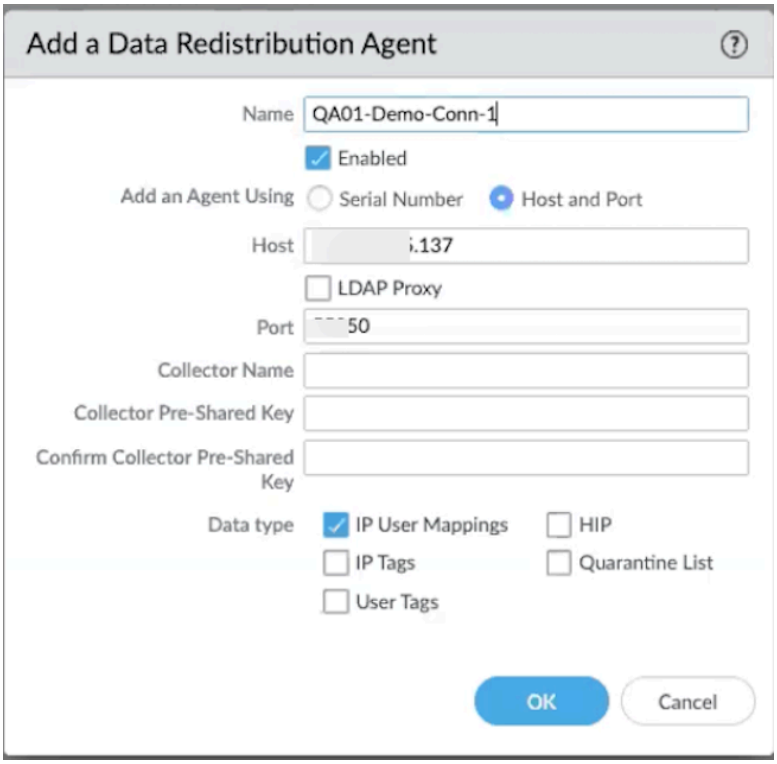
 ©2025 Palo Alto Networks, Inc.

STEP 6 | *Lors de la configuration de la redistribution User-ID, vous devez ajouter une entrée d'agent de redistribution pour chaque port dans la plage spécifiée à partir de l'étape 3* ***User ID Port Range (Plage de ports User-ID)****. Par exemple, si la plage est 55050-55055, vous devez configurer 6 entrées, alignées sur le nombre de régions de connecteur ZTNA que vous avez déployées.*

Pour chaque port de la plage, sélectionnez une adresse IP dans ***User ID Redistribution Agent IP (Adresse IP de l'agent de redistribution User-ID)*** *à l'étape 3 pour le champ* ***Host (Hôte)****. Si vous souhaitez une redondance au niveau du connecteur ZTNA, vous pouvez choisir deux adresses à partir de* ***User ID Redistribution Agent IP (Adresse IP de l'agent de redistribution User ID)*** *et appliquer la plage de ports complète pour les deux adresses IP. Alternativement, tous les ports sur toutes les adresses IP dans* ***User ID Redistribution Agent IP (Adresse IP de l'agent de redistribution User ID)*** *peuvent être configurés.*

Ajoutez un agent de redistribution pour chacun des ports de la plage **User ID Port Range (Plage de ports User-ID)** avec une ou plusieurs des adresses dans **User ID Redistribution Agent IP (Adresse IP de l'agent de redistribution User ID)**.

1. Sur l'interface utilisateur NGFW, accédez à **Device (Périphérique)**, puis sélectionnez **Data Redistribution (Redistribution des données)**.
2. Cliquez sur **Add (Ajouter)**, ajoutez le **Name (Nom)** et cochez la case **Enabled (Activé)** .
3. Sélectionnez **Host and Port (Hôte et port)**, ajoutez **User ID Redistribution Agent IP (Adresse IP de l'agent de redistribution User ID)** de l'étape 3 dans **Host (Hôte)** et ajoutez la **User ID Port Range (Plage de ports User-ID)** copiée à l'étape 3.
4. Activez la case à cocher **IP User Mappings (Mappages des utilisateurs IP)** et cliquez sur **OK**.

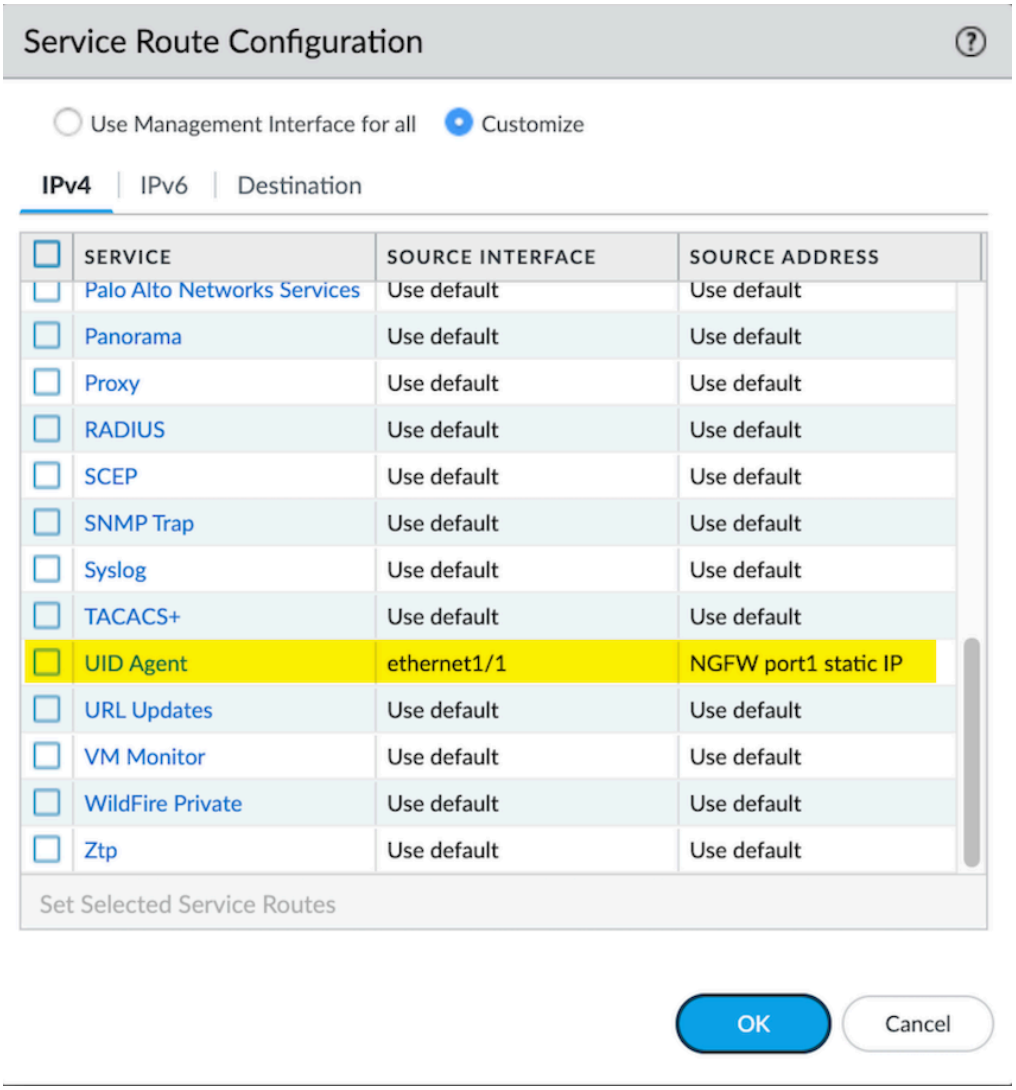


 ©2025 Palo Alto Networks, Inc.

5. Cliquez sur **Commit (Valider)** pour enregistrer la configuration.

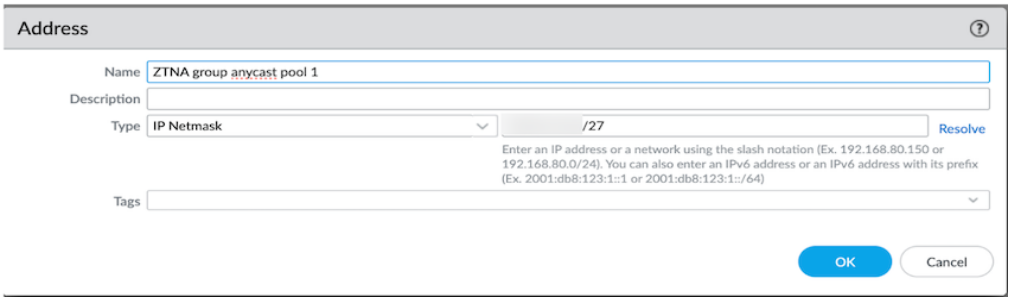
STEP 7 | Sur l'interface utilisateur NGFW, accédez à **Device (Périphérique)** > **Setup (Configuration)** > **Services** > **Service Route Configuration (Configuration d'itinéraire de service)** > **Customize (Personnaliser)** > **UID agent (Agent UID)**.

1. Sous **IPv4**, sélectionnez **SOURCE INTERFACE (INTERFACE SOURCE)** comme **Ethernet1/1** (interface orientée connecteur ZTNA), et ajoutez la **SOURCE ADDRESS (ADRESSE SOURCE)**.



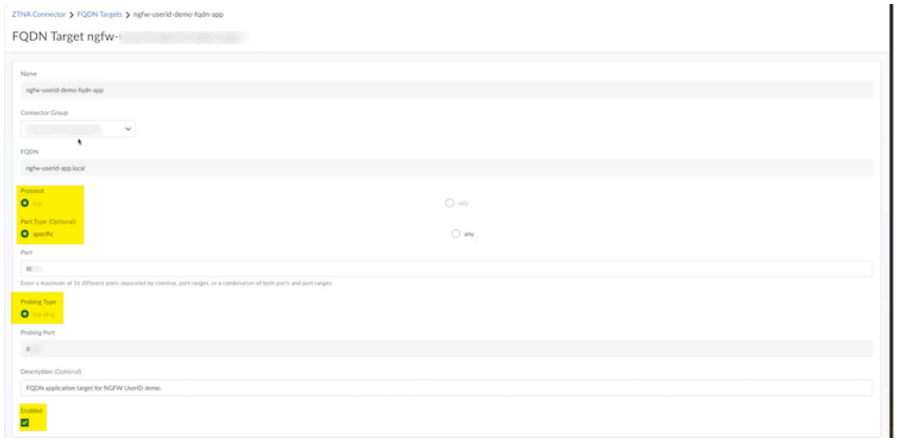
 ©2025 Palo Alto Networks, Inc.

STEP 8 | Ajoutez une règle de politique de sécurité pour autoriser les paquets TCP avec l'adresse IP source. Ajoutez l'adresse IP source, qui est l'adresse IP Anycast copiée à l'étape 3 et cliquez sur **OK**.

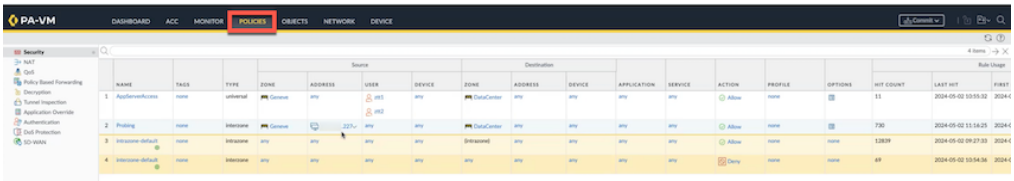


STEP 9 | (Facultatif) Activez le sondage TCP.

1. Pour créer une cible FQDN :
    1. Accédez à **Workflows (Flux de travail)** > **Application Targets (Cibles d'application)** > **FQDN Targets (Cibles FQDN)** et cliquez sur **Create FQDN Target (Créer une cible FQDN)**.
    2. Ajoutez un **Nom (Name)** et sélectionnez le **Connector Group (Groupe de connecteurs)**.
    3. Activez **tcp**, **specific (spécifique)**, **tcp ping** et **Enabled (Activé)**. Ajoutez le **Port** et cliquez sur **Create (Créer)**.



STEP 10 | Sur l'interface utilisateur NGFW, accédez à **Policies (Politiques)** et définissez les politiques basées sur User-ID.



 ©2025 Palo Alto Networks, Inc.

Configurer les paramètres d'accès à privilèges dynamique

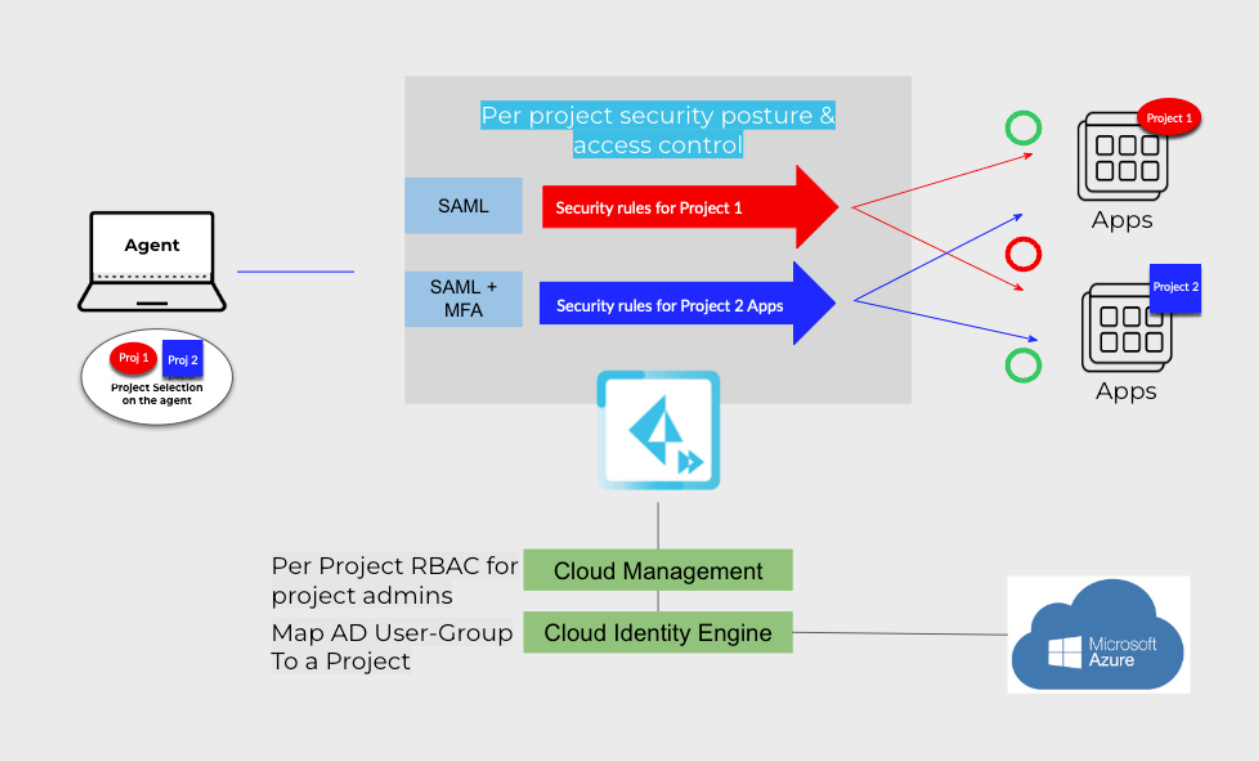
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access ❑ Prisma Access 5.1 ❑ Rôle : Super utilisateur

Pour les entreprises d'informatique et de services informatiques (IT Enabled Services, ITES) qui doivent contrôler les utilisateurs ayant accès aux projets de leurs clients, *Dynamic Privilege Access (Accès à privilèges dynamique)* fournit à vos utilisateurs un moyen transparent, sécurisé et compartimenté d'accéder uniquement aux projets qui leur sont affectés. Ces entreprises attribuent généralement plusieurs projets client à des employés et fournissent un accès isolé à ces projets afin qu'un utilisateur autorisé ne puisse accéder qu'à un seul projet client à la fois.

Qu'est-ce que l'accès à privilèges dynamique ?

L'accès à privilèges dynamique est une fonctionnalité de Prisma Access qui fournit des privilèges dynamiques à vos utilisateurs en fonction du flux de travail ou du projet qu'ils sélectionnent dans l'application Prisma Access Agent. Vos utilisateurs peuvent disposer de privilèges dynamiques basés sur la combinaison du groupe d'utilisateurs et du pool d'adresses IP attribué à un projet. Cette combinaison unique définit un projet. Avec l'accès à privilèges dynamique, vous pouvez isoler des ressources de votre réseau afin qu'elles ne soient accessibles à vos utilisateurs qu'en fonction des projets auxquels ils sont affectés.

Un nouveau rôle prédéfini appelé **Project Admin (Administrateur de projet)** est disponible sur Prisma Access pour permettre aux administrateurs de projet de créer et de gérer des définitions de projet. Les administrateurs de projet ont la possibilité de mapper les projets pour sélectionner des groupes d'emplacements Prisma Access, et de créer des attributions d'adresses IP à l'aide de DHCP en fonction du projet et du groupe d'emplacements. Les administrateurs de projet ne peuvent gérer que les projets auxquels ils sont affectés dans Strata Cloud Manager.



Lorsque vos utilisateurs finaux se connectent à un Prisma Access Agent qui est activé pour l'accès à privilèges dynamique sur leurs périphériques gérés, le flux de travail suivant a lieu :

1. Votre utilisateur final sélectionne un projet auquel il est affecté (par exemple, Projet 1).
2. Son identité est authentifiée dans Cloud Identity Engine, qui mappe le groupe d'utilisateurs de l'utilisateur au projet.
3. Une fois l'authentification réussie et que son groupe d'utilisateurs correspond aux critères de projet configurés par l'administrateur de projet, l'utilisateur a accès aux ressources du réseau via des paramètres spécifiques au Projet 1 et des règles de sécurité qui fournissent une posture de sécurité ainsi qu'un contrôle d'accès par projet. L'infrastructure de sécurité applique

 ©2025 Palo Alto Networks, Inc.

des règles de sécurité pour restreindre l’accès des utilisateurs uniquement aux ressources et applications appartenant à ce projet. L’accès aux ressources et aux applications d’autres projets n’est pas autorisé.

4. Lorsque l’utilisateur bascule vers un autre projet (par exemple, Projet 2), il est déconnecté du projet précédent (Projet 1). Il peut ensuite accéder aux ressources du deuxième projet en fonction des paramètres spécifiques au projet et de ses règles de sécurité.

Vous pouvez gagner en visibilité sur votre déploiement Prisma Access Agent à l’aide de Strata Cloud Manager pour surveiller l’activité de vos utilisateurs sur le projet, et afficher la consommation des services ainsi que la posture de sécurité de votre réseau.

 ©2025 Palo Alto Networks, Inc.

Activer l'accès à privilèges dynamique pour Prisma Access via Common Services

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access avec abonnement d'utilisateur mobile ❑ Lien d'activation ❑ Strata Logging Service ❑ Moteur d'identité sur le cloud ❑ Prisma Access Agent ❑ Role (Rôle) : Super utilisateur multi-locataire ou Super utilisateur avec accès au portail de support client

Avec l'accès à privilèges dynamique, les administrateurs informatiques peuvent associer les utilisateurs finaux à plusieurs projets clients. Un utilisateur autorisé n'est autorisé à accéder qu'à un seul projet client à la fois.

Le **Dynamic Privilege Access (Accès à privilèges dynamique)** est une fonctionnalité optionnelle lors de l'activation d'un nouveau locataire Prisma Access. Après avoir activé cette fonctionnalité et le locataire, le DPA est défini pour la durée de vie du locataire, et vous ne pouvez pas le désactiver.

L'option d'activation du DPA n'est disponible qu'une seule fois lors de la première activation d'un nouveau locataire. Après l'activation du locataire, l'option est cachée pour toutes les activations suivantes, y compris les options supplémentaires et les renouvellements. Elle n'est pas disponible pour les locataires existants.

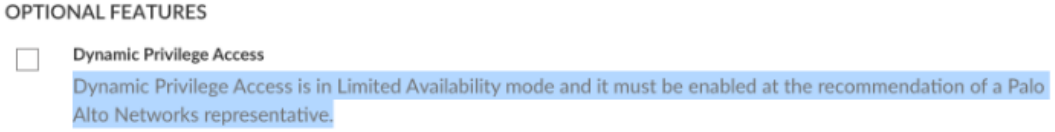
STEP 1 | Contactez votre représentant de compte Palo Alto Networks pour activer cette fonctionnalité pour votre locataire.

STEP 2 | Activez la licence pour votre Prisma Access (Managed by Strata Cloud Manager).

STEP 3 | -vous d'allouer des licences, de planifier vos connexions aux services et d'ajouter des emplacements supplémentaires en conséquence.

STEP 4 | Activez les modules complémentaires disponibles.

STEP 5 | Cochez la case **Dynamic Privilege Access (Accès à privilèges dynamique)**.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | Cliquez sur **Agree to the Terms and Conditions (Accepter les termes et conditions)** et sur

STEP 7 | **Activate Now (Activer maintenant)**. Les produits et les modules complémentaires que vous activez (comme Prisma Access ou Strata Logging Service) sont maintenant provisionnés. Alors que les abonnements s'activent, l'état d'avancement s'affiche. Lorsque le processus est terminé, l'état du locataire s'affiche comme `Up (Actif)`. Vous avez maintenant un locataire provisionné avec des instances des produits que vous avez achetés. Le locataire a un utilisateur, le compte que vous avez utilisé lorsque vous avez commencé ce processus.

STEP 8 | Pour compléter la configuration des produits restants, vous devez accéder aux produits que vous avez achetés et effectuer toute configuration post-installation requise. Pour des informations sur vos produits, consultez :

- API ouvertes
- Guide de démarrage de Strata Logging Service
- Guide d'administrateurs de Prisma Access (Managed by Strata Cloud Manager)
- Guide de démarrage de Cloud Identity Engine

STEP 9 | Ajoutez l'accès utilisateur et attribuez des rôles.

Accordez l'accès aux utilisateurs en tant que **Project Admin (Administrateur de projet)** en fonction des projets.

 ©2025 Palo Alto Networks, Inc.

Autoriser le mappage des groupes d’utilisateurs dans Cloud Identity Engine pour l’accès à privilèges dynamiques

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access ❑ Version minimale requise de Prisma Access : 5.1 ❑ Rôle : Super utilisateur

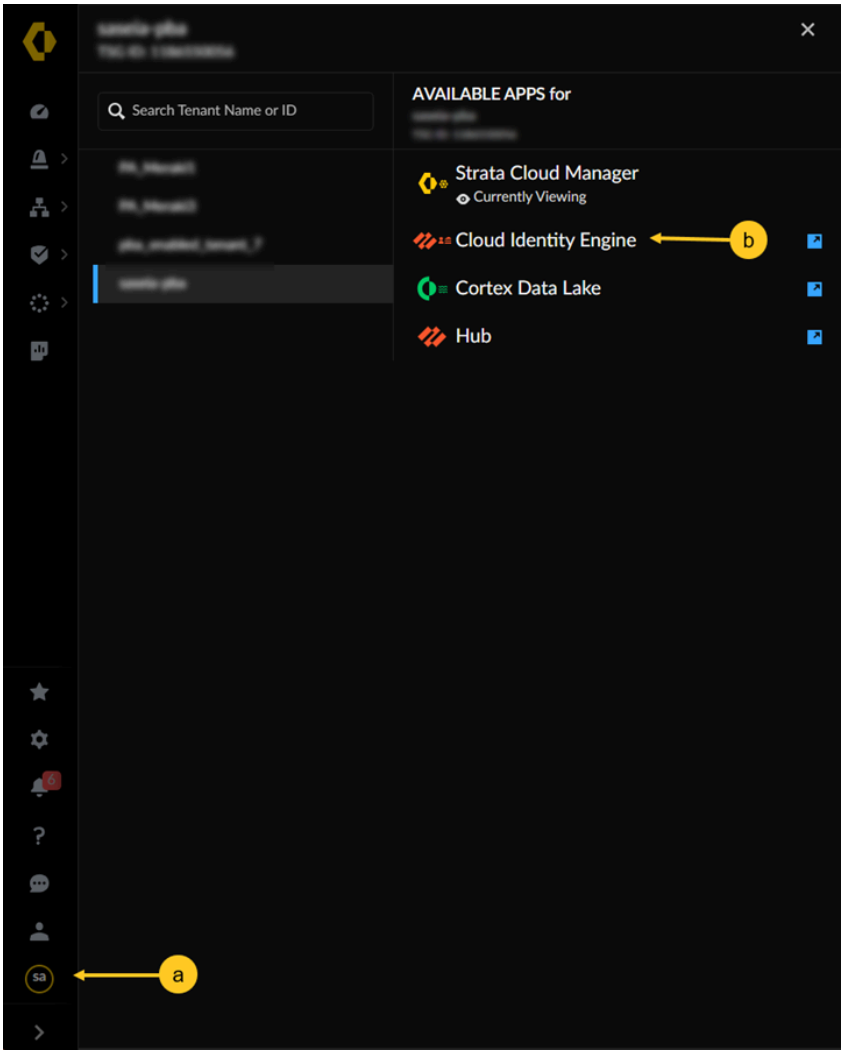
Avant de commencer, assurez-vous d’avoir rempli les conditions préalables suivantes :

- Contactez votre représentant de compte Palo Alto Networks pour activer la fonctionnalité d’accès à privilèges dynamiques
- Activez Cloud Identity Engine et créez votre premier locataire.
- Configurez Cloud Identity Engine.

Dans ce flux de travail, nous avons utilisé Azure comme IdP. Vous pouvez également utiliser Okta comme IdP.

©2025 Palo Alto Networks, Inc.

STEP 1 | Depuis Strata Cloud Manager, ouvrez l’application Cloud Identity Engine associée à votre locataire.



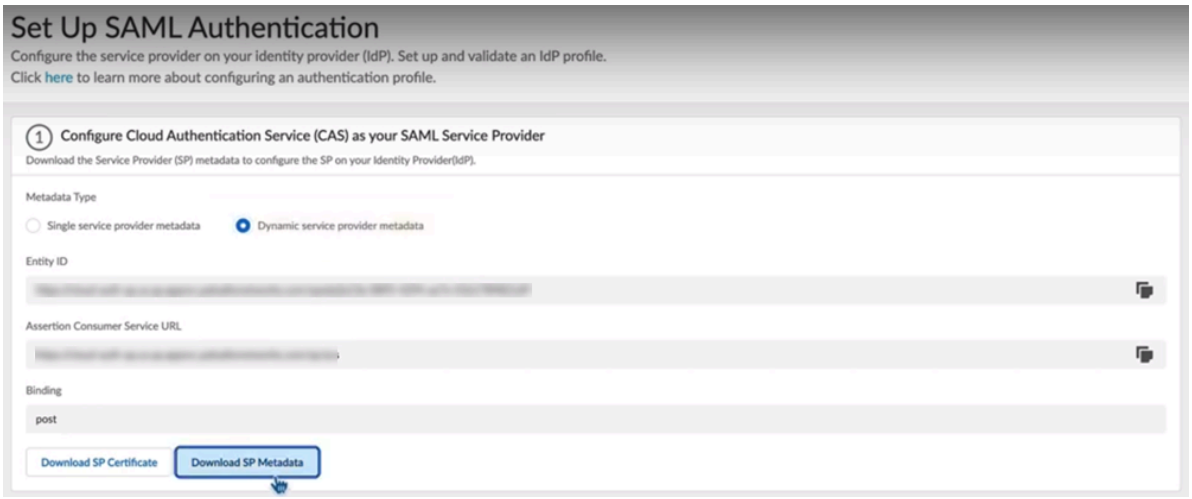
STEP 2 | Ajoutez un répertoire Azure ou un répertoire Okta comme IdP pour les utilisateurs mobiles.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Téléchargez les métadonnées SP dans l'application Cloud Identity Engine.

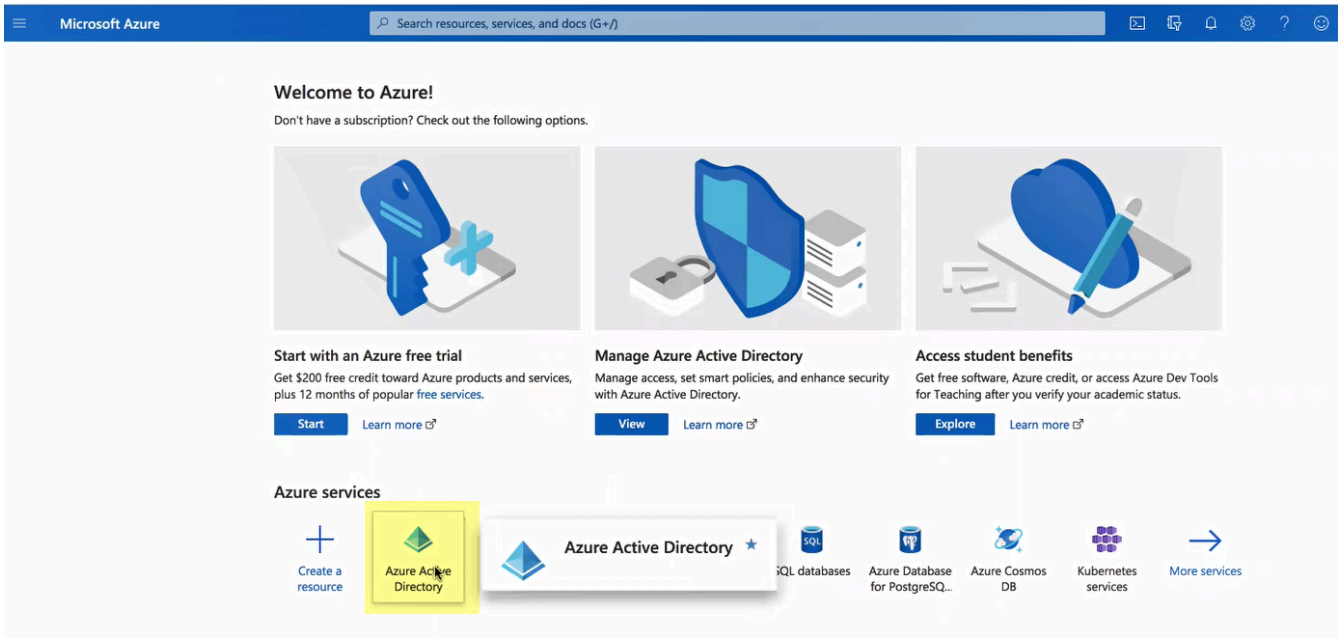
1. Accédez à **Authentication (Authentification)** > **Authentication Types (Types d'authentification)** > **Add New Authentication Type (Ajouter un nouveau type d'authentification)**.
2. Utilisez la fonction **Set Up (Configurer)** pour configurer un type d'authentification SAML 2.0.

   Sélectionnez **Dynamic service provider metadata (Métadonnées du fournisseur de services dynamiques)**.
3. Cliquez sur **Download SP Metadata (Télécharger les métadonnées SP)**.



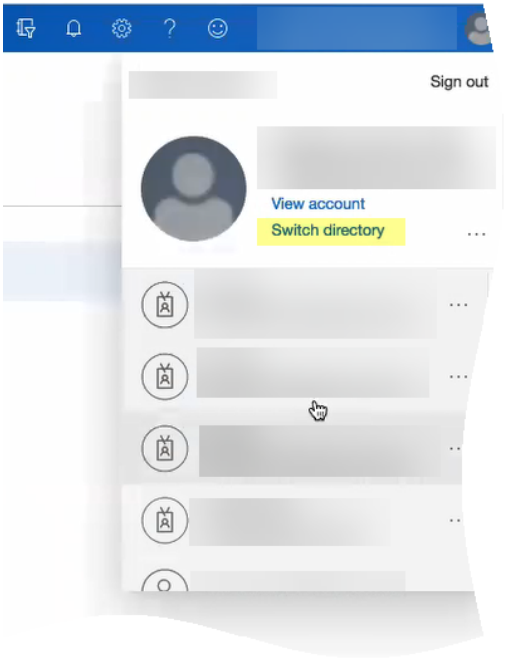
4. Connectez-vous au portail Azure et sélectionnez **Azure Active Directory**.

   Assurez-vous de suivre toutes les étapes nécessaires dans le portail Azure.

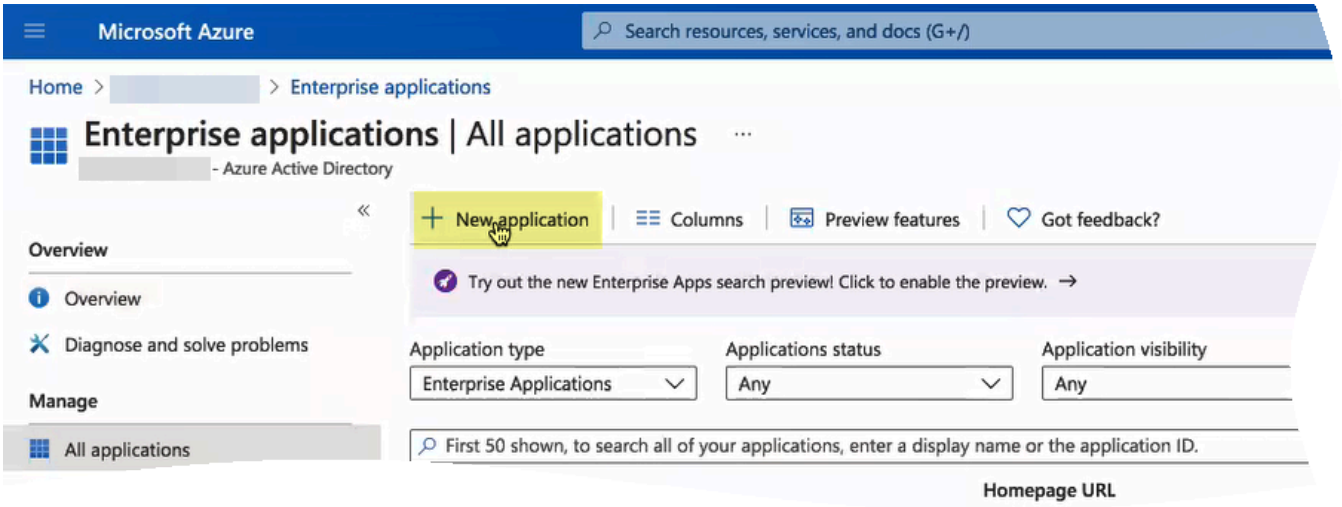


   Si vous disposez de plusieurs répertoires, utilisez la fonction **Switch directory (Basculer entre les répertoires)** pour sélectionner le répertoire que vous souhaitez utiliser avec Cloud Identity Engine.

 ©2025 Palo Alto Networks, Inc.



5. Sélectionnez **Enterprise applications (Applications d’entreprise)** et cliquez sur **New application (Nouvelle application)**.



6. Recherchez **`Palo Alto Networks Cloud Identity Engine - Cloud Authentication Service (Cloud Identity Engine Palo Alto Networks`**

 ©2025 Palo Alto Networks, Inc.

- Service d'authentification de cloud) et créez l'intégration d'ouverture de session unique SSO Active Directory (AD) Azure.

Personnalisez le nom de l'application si nécessaire lors de la création de l'application.

7. Une fois l'application chargée, sélectionnez **Users and groups (Utilisateurs et groupes)**, puis **Add user/group (Ajouter un utilisateur/groupe)** pour les attribuer à cette application à l'aide de la fonction **Assign (Attribuer)**.

   Sélectionnez les utilisateurs et les groupes que vous souhaitez utiliser avec l'IdP Azure dans Cloud Identity Engine pour l'authentification.

   Assurez-vous d'attribuer le compte que vous utilisez afin de pouvoir tester la configuration une fois celle-ci terminée. Vous devrez peut-être actualiser la page après avoir ajouté des comptes pour terminer le test avec succès.
8. Utilisez la fonction **Set up single sign-on (Configurer l'ouverture de session unique SSO),** puis sélectionnez **SAML**.
9. Utilisez la fonction **Upload Metadata File (Télécharger le fichier de métadonnées)** en recherchant le fichier de métadonnées que vous avez téléchargé à partir de l'application Cloud Identity Engine à l'étape 3.c et cliquez sur **Add (Ajouter)**.
10. Une fois les métadonnées téléchargées, saisissez votre terminal régional comme **Sign-on URL (URL d'ouverture de session)** en utilisant le format suivant : https://<RegionUrl>.paloaltonetworks.com/sp/acs (où <RegionUrl> est votre terminal régional).

    Vous pouvez également copier l'URL de réponse dans l'URL d'ouverture de session.
11. Cliquez sur **Save (Enregistrer)** pour enregistrer votre configuration.

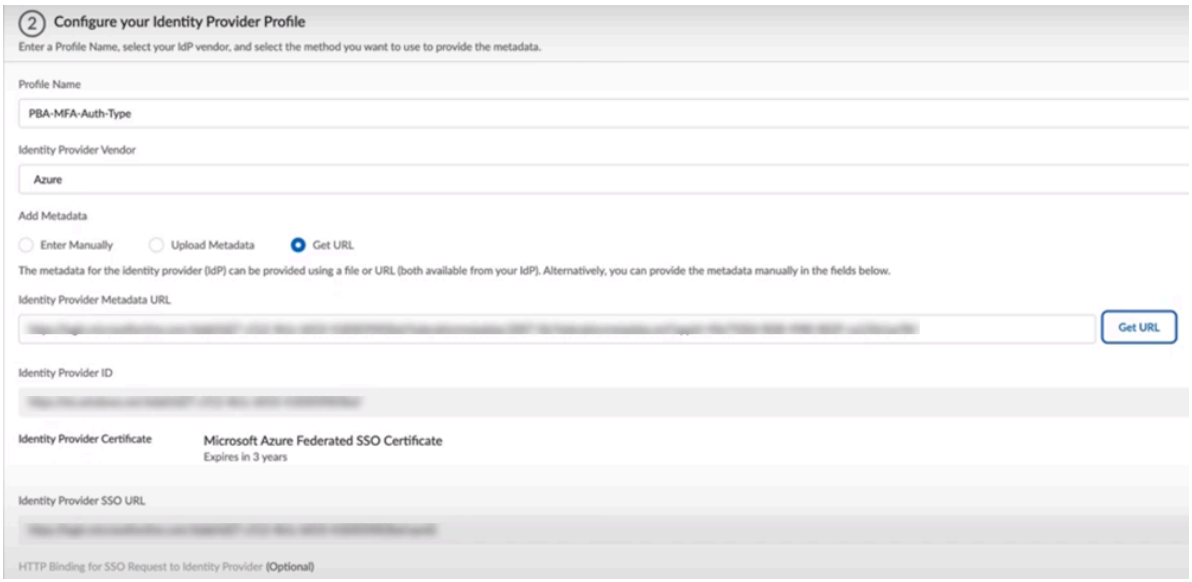
STEP 4 | Configurez la politique d'accès conditionnel pour activer l'authentification multifacteur pour les groupes d'utilisateurs sélectionnés.

1. Dans votre application, accédez à **Overview (Vue d'ensemble)** > **Conditional Access (Accès conditionnel)** > **Create a policy (Créer une politique)**.
2. Ajouter une **New Policy (Nouvelle politique)**.
3. Nommez la politique.
4. Dans la section **Users (Utilisateurs)**, incluez **Select users and groups (Sélectionner les utilisateurs et les groupes)** et choisissez vos groupes de projets en conséquence.
5. Vérifiez les **Target resources (Ressources cibles)**.
6. Sélectionnez les **Conditions** qui déclenchent la politique.
7. Cliquez sur **Grant (Accorder)** pour accorder l'accès dans **Access Controls (Contrôles d'accès)** à l'aide de l'option **Require multifactor authentication (Exiger une authentification multifacteur)**.
8. Activez la politique en basculant le sélecteur sur **On (Activé)** et cliquez sur **Create (Créer)** pour créer l'accès conditionnel.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Ajoutez votre fournisseur IdP comme type d'authentification.

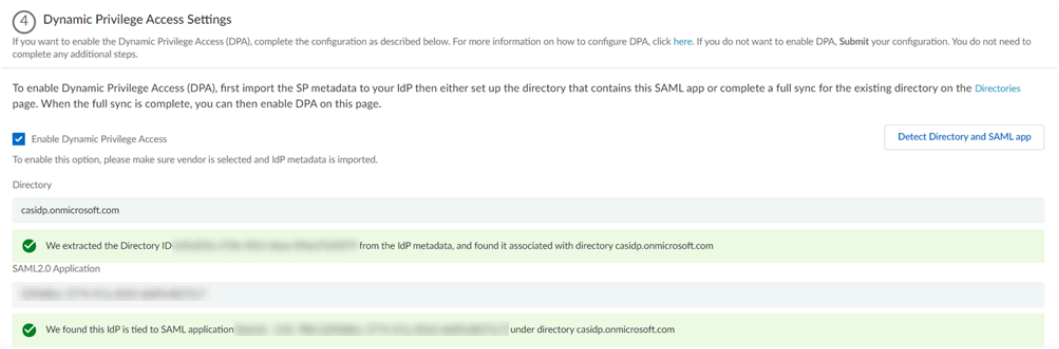
1. Sélectionnez **Single sign-on (Ouverture de session unique SSO)** > **SAML Certificates (Certificats SAML)** et copiez l'**App Federation Metadata URL (URL des métadonnées de la fédération d'applications)**.
2. Dans l'application Cloud Identity Engine, sélectionnez **Authentication (Authentification)** > **Authentication Types (Types d'authentification)** > **Add New Authentication Type (Ajouter un nouveau type d'authentification)**.
3. Utilisez la fonction **Set Up (Configurer)** pour configurer un type d'authentification SAML 2.0.
4. Sous **Configure your Identity Provider Profile (Configurer le profil de votre fournisseur d'identité)**, entrez un **Profile Name (Nom de profil)**.
5. Sélectionnez **Azure** comme **IDP Vendor (Fournisseur IDP)**.
6. Sélectionnez **Get URL (Obtenir l'URL)**, collez l'URL de l'étape 5.a et sélectionnez **Get URL (Obtenir l'URL)** pour obtenir les métadonnées.



7. Activez l'option **Multi-factor Authentication is Enabled on the Identity Provider (L'authentification multifacteur est activée sur le fournisseur d'identité)**.
8. Utilisez la fonction **Test SAML Setup (Tester la configuration SAML)** pour vérifier la configuration du profil.
9. Sélectionnez les attributs SAML que vous souhaitez que Prisma Access utilise pour l'authentification.
10. Activez **Dynamic Privilege Access (Accès à privilèges dynamiques)**.

    Assurez-vous de synchroniser le répertoire que vous avez ajouté à l'étape 2 et l'application SAML.

 ©2025 Palo Alto Networks, Inc.



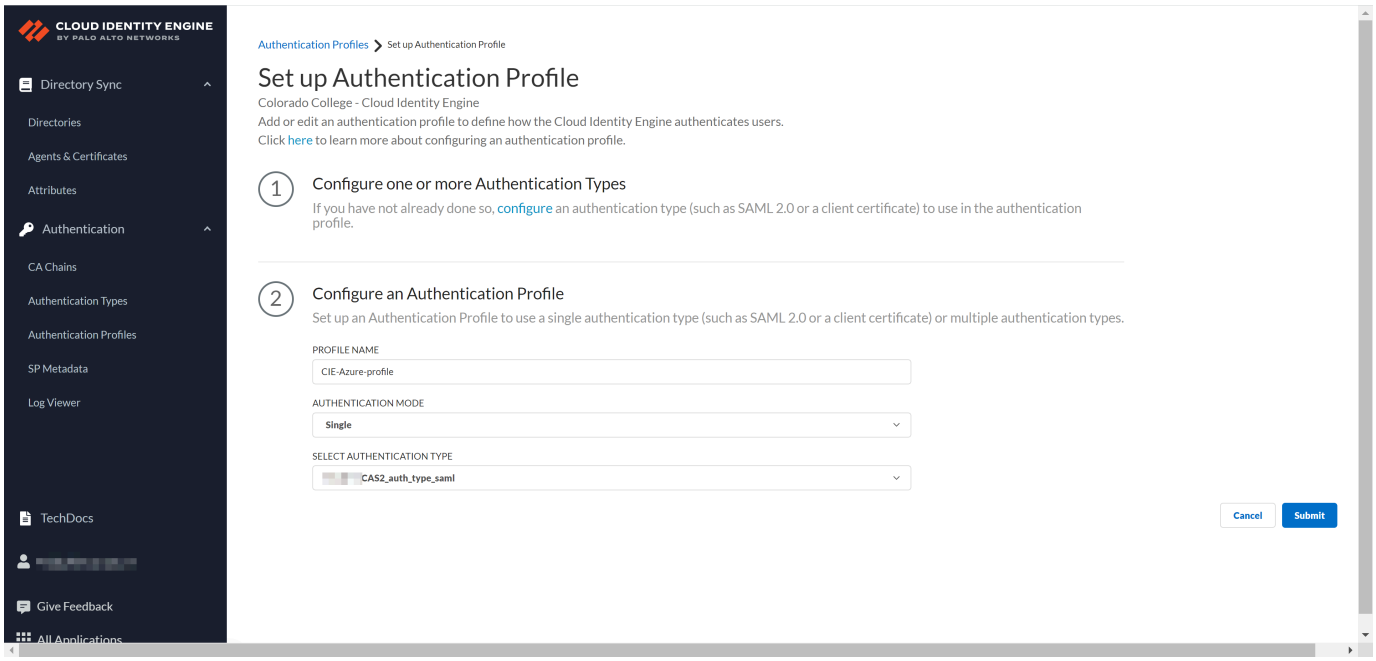
11. Cliquez sur **Submit (Envoyer)** pour envoyer le profil IdP.

STEP 6 | Répétez les étapes de 3 à 5 pour configurer l'application SAML pour les groupes d'utilisateurs qui ne nécessitent pas d'authentification multifacteur.

N'activez pas l'authentification multifacteur à l'étape 5.g pour les groupes d'utilisateurs qui ne nécessitent pas d'authentification multifacteur.

STEP 7 | Ajoutez un profil d'authentification pour les groupes d'utilisateurs qui utilisent l'authentification multifacteur et les groupes d'utilisateurs qui ne l'utilisent pas.

1. Sélectionner **Authentication (Authentification)** > **Authentication Profiles (Profils d'authentification)** > **Add Authentication Profile (Ajouter un profil d'authentification)**.
2. Saisissez un **PROFILE NAME (NOM DE PROFIL)**.
3. Sélectionnez un **Authentication Mode (Mode d'authentification)** :
4. Sélectionnez le **Authentication Type (Type d'authentification)** de l'étape 5 ou 6, en fonction des groupes d'utilisateurs nécessitant l'authentification multifacteur, puis cliquez sur **Submit (Envoyer)**.

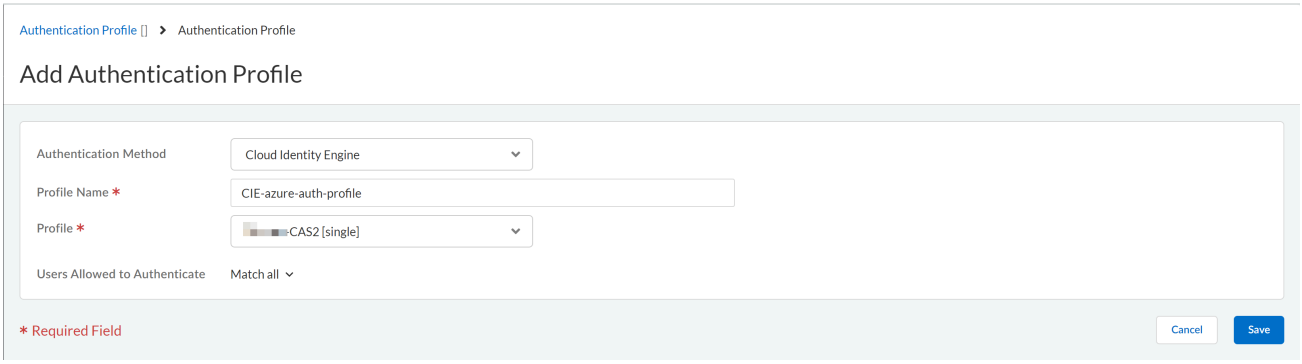


 ©2025 Palo Alto Networks, Inc.

STEP 8 | Ajoutez le profil d'authentification depuis Cloud Identity Engine à Prisma Access.

1. Dans Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Authentication (Authentification)** > **Authentication Profiles (Profils d'authentification)**.

   Assurez-vous de définir l'étendue de la configuration sur le conteneur d'utilisateurs mobiles de l'**Access Agent (Agent d'accès)**.
2. Cliquez sur **Add Profile (Ajouter un profil)**.
3. Sélectionnez **Cloud Identity Engine** comme **Authentication Method (Méthode d'authentification)**.
4. Saisissez un **Profile Name (Nom de profil)**.
5. Sélectionnez le **Profile (Profil)** que vous avez ajouté dans l'application Cloud Identity Engine à l'étape 7.
6. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.



STEP 9 | Joignez l'authentification aux utilisateurs mobiles.

1. Lancez Prisma Access depuis votre Strata Cloud Manager.
2. Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)**.
3. Définissez l'étendue sur l'extrait de projet que vous avez créé et accédez à **Security Services (Services de sécurité)** > **Security policy (Politique de sécurité)**.
4. Créez une politique pour autoriser le trafic uniquement à partir d'une plage DHCP de projet particulière et de ce groupe d'utilisateurs basé sur le projet.

©2025 Palo Alto Networks, Inc.

Activer l’agent d’accès

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Licence Prisma Access avec l’abonnement Utilisateur mobile ❑ Rôle : Super utilisateur

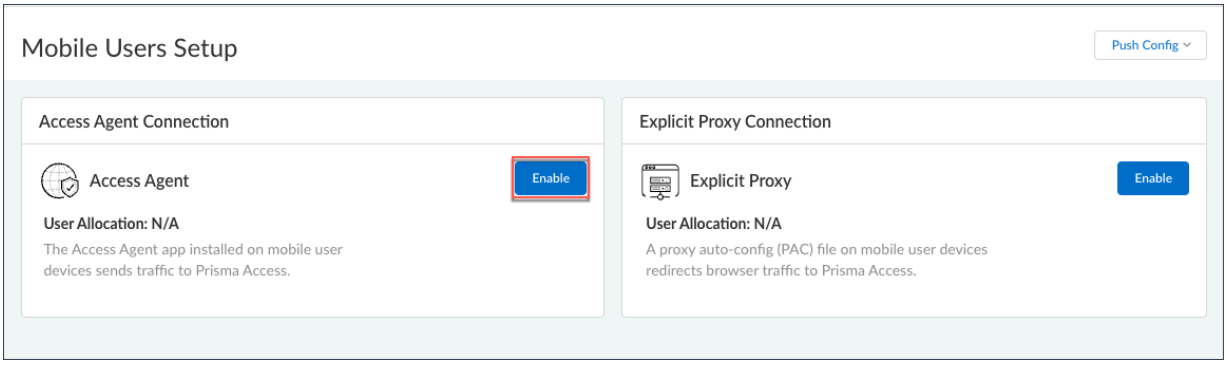
Avant de pouvoir intégrer vos utilisateurs, vous devez activer **Access Agent (Agent d’accès)** en tant que type de connexion d’utilisateur mobile à l’aide de Strata Cloud Manager. Après avoir activé le type de connexion, les Prisma Access Agents installés sur les périphériques des utilisateurs mobiles pourront envoyer du trafic à Prisma Access.

Avant de commencer à activer le Prisma Access Agent, assurez-vous que vous Autoriser le mappage des groupes d’utilisateurs dans Cloud Identity Engine pour l’accès à privilèges dynamiques.

STEP 1 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Configuration (Configuration Prisma Access)** > **Mobile Users (Utilisateurs mobiles)**.

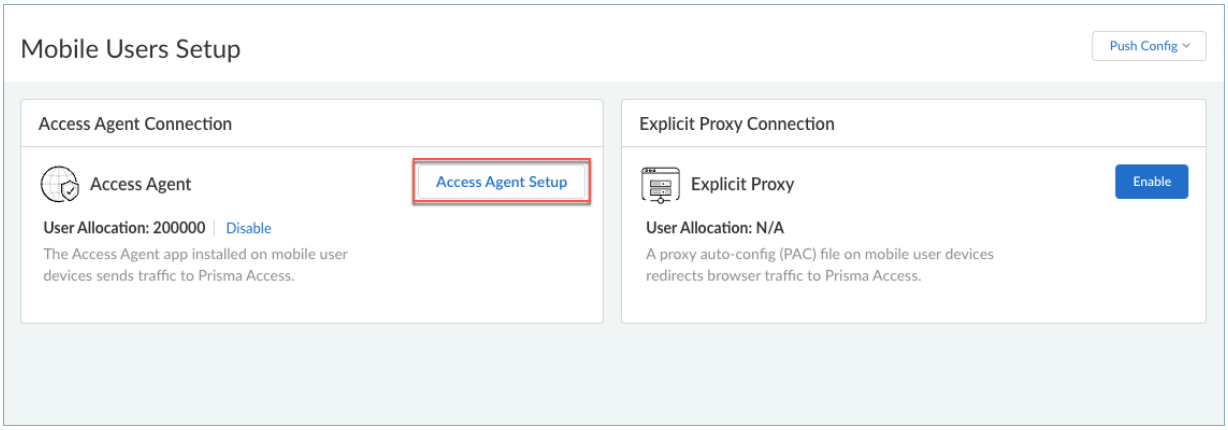
STEP 2 | **Enable (Activez)** l’agent d’accès.

Le proxy explicite n’est pas pris en charge pour Prisma Access Agent.

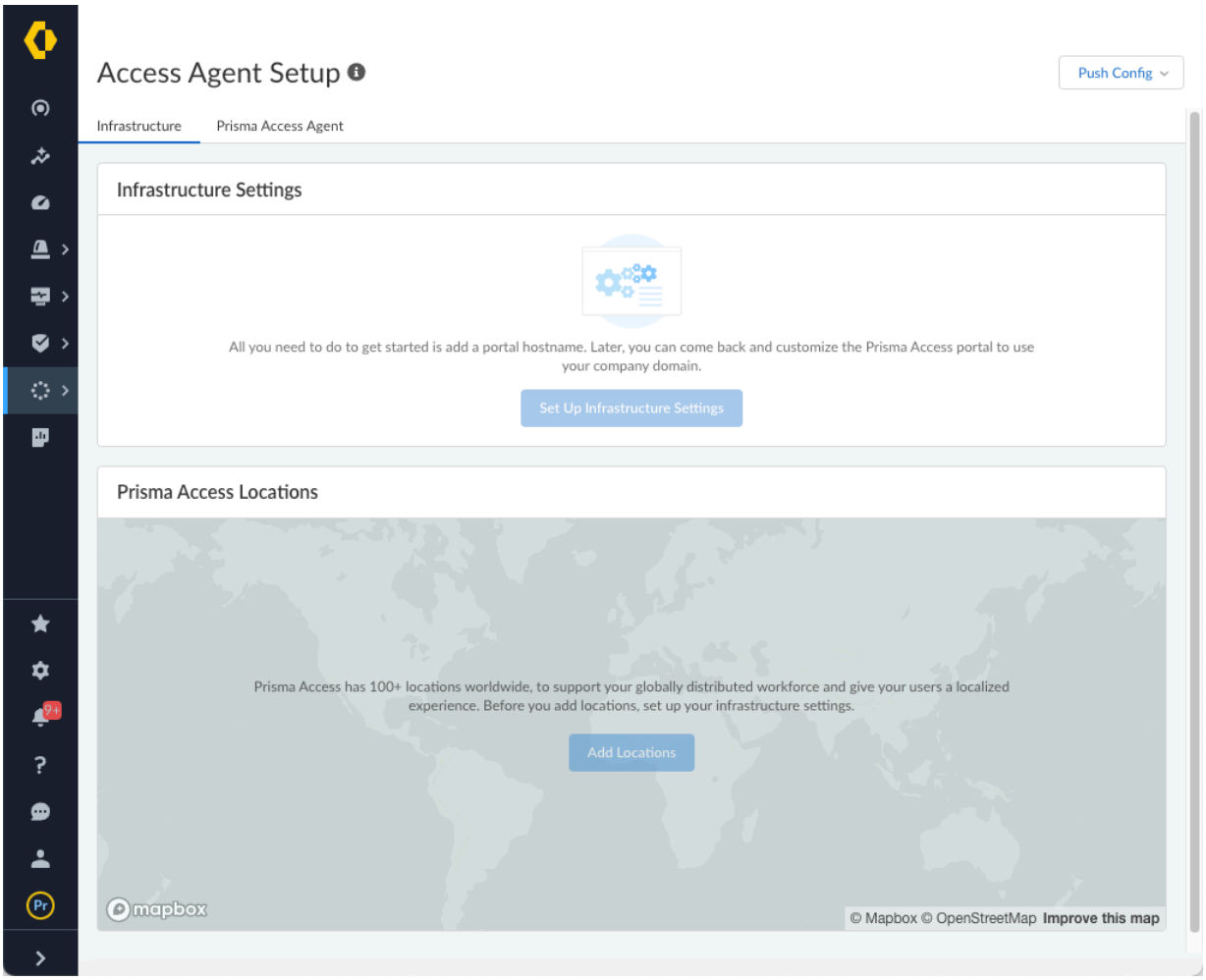


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Cliquez sur **Access Agent Setup (Configuration de l'agent d'accès)** pour commencer l'intégration de vos utilisateurs mobiles.



La page de configuration de l'agent d'accès s'affiche.



 ©2025 Palo Alto Networks, Inc.

Configurer l'infrastructure de l'agent pour l'accès à privilèges dynamique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Rôle : Super utilisateur

Configurez les paramètres d'infrastructure pour l'Prisma Access Agent afin que Prisma Access puisse approvisionner votre environnement d'utilisateur mobile. Ensuite, sélectionnez les emplacements de Prisma Access auxquels vos utilisateurs d'Prisma Access Agent se connecteront.

Vous pouvez également éventuellement activer le support SC-NAT pour l'accès à privilèges dynamique si vous avez créé des connexions aux services pour accéder aux applications privées dans leur centre de données ou à l'emplacement du siège, ou activer le résumé de l'itinéraire pour l'accès à privilèges dynamique afin de réduire le nombre d'itinéraires envoyés au réseau.

Configurer les paramètres d'infrastructure

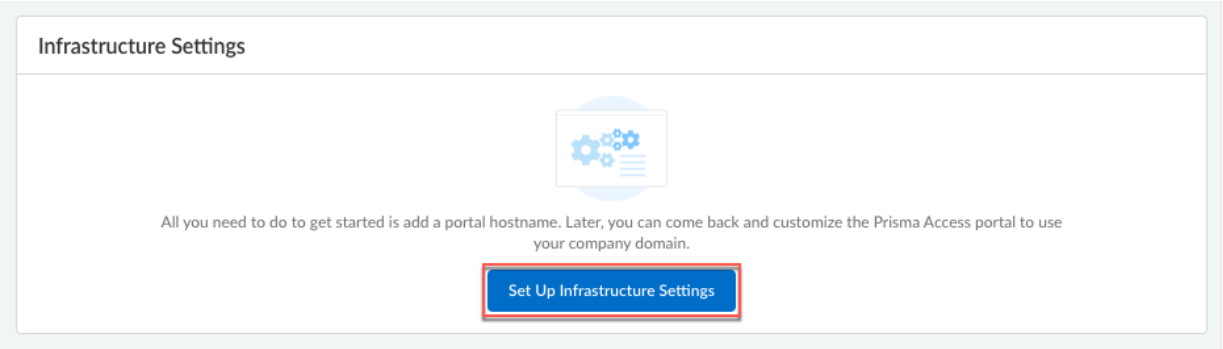
Pour activer Prisma Access pour l'accès à Internet uniquement pour les utilisateurs, Prisma Access fournit un pool d'adresses IP par défaut et un serveur DNS par défaut dans le cloud. Toutefois, si vous souhaitez que vos utilisateurs mobiles accèdent à des ressources internes depuis votre siège, depuis vos centres de données ou depuis des sites de réseaux distants que vous avez intégrés à Prisma Access, vous devez allouer des pools d'adresses IP clients. Prisma Access utilise les pools d'adresses IP pour attribuer des adresses IP à vos utilisateurs mobiles et configurer l'infrastructure de service Prisma Access.

Avant de configurer les paramètres de l'infrastructure, assurez-vous de configurer au moins un projet. Sinon, lorsque vous essayez de valider et d'appliquer les paramètres de l'infrastructure, la validation échoue. Pour en savoir plus, reportez-vous à la section Créer un projet.

STEP 1 | Dans Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Access Agent (Agent d'accès)** > **Infrastructure**.

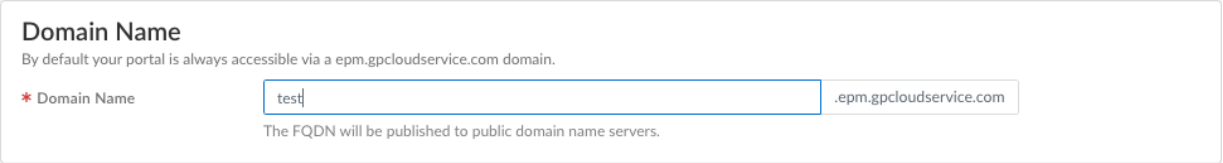
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Si vous configurez l'infrastructure pour la première fois, cliquez sur **Set Up Infrastructure Settings (Configurer les paramètres de l'infrastructure)**. Sinon, modifiez les **Infrastructure Settings (Paramètres de l'infrastructure)**.



STEP 3 | Ajoutez un nom d'hôte au **Domain Name (Nom de domaine)** pour le service auquel les agents Prisma Access se connectent.

Par défaut, les utilisateurs peuvent accéder au service à l'aide d'un FQDN basé sur votre nom d'hôte et le domaine **`.epm.gpcloudservice.com`**.

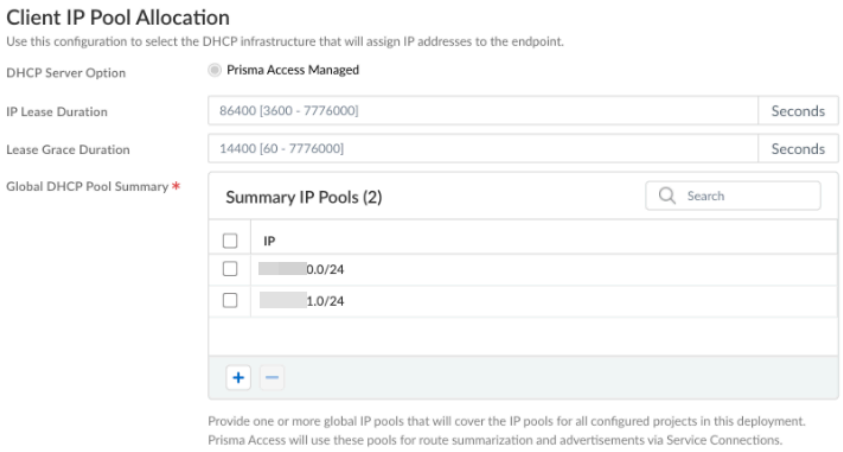


STEP 4 | Dans **Client IP Pool Allocation (Allocation de pool d'adresses IP client)**, Prisma Access fournit un serveur DHCP qui gérera l'affectation des adresses IP à vos terminaux pour l'accès à privilèges dynamique.

Le nom du projet et l'ID du groupe d'emplacements de Prisma Access font partie de la requête DHCP. Chaque Prisma Access Agent se connectant à un projet spécifique se voit attribuer une adresse IP à partir du sous-réseau IP de ce projet. Lorsqu'un utilisateur change

 ©2025 Palo Alto Networks, Inc.

pour un projet différent, une adresse IP différente est attribuée à l'Prisma Access Agent à partir du sous-réseau IP du projet.



Vous pouvez configurer les options suivantes :

- **IP Lease Duration (Durée du bail IP)** : spécifiez la durée (en secondes) pendant laquelle le serveur DHCP alloue une adresse réseau à un Prisma Access Agent. La durée du bail IP par défaut est de 86 400 secondes.
- **Lease Grace Duration (Durée appropriée du bail)** : indiquez la durée pendant laquelle l'Prisma Access Agent peut continuer à utiliser son adresse IP après l'expiration du bail. La durée appropriée du bail par défaut est de 14 400 secondes.
- **Global DHCP Pool Summary (Résumé du pool DHCP global)** : sélectionnez le pool d'adresses IP sur lequel vous souhaitez activer SC-NAT ou configurez et sélectionnez les pools d'adresses IP récapitulatifs globaux pour le résumé de l'itinéraire.

STEP 5 | Cliquez sur **Save (Enregistrer)** pour enregistrer les paramètres d'infrastructure.

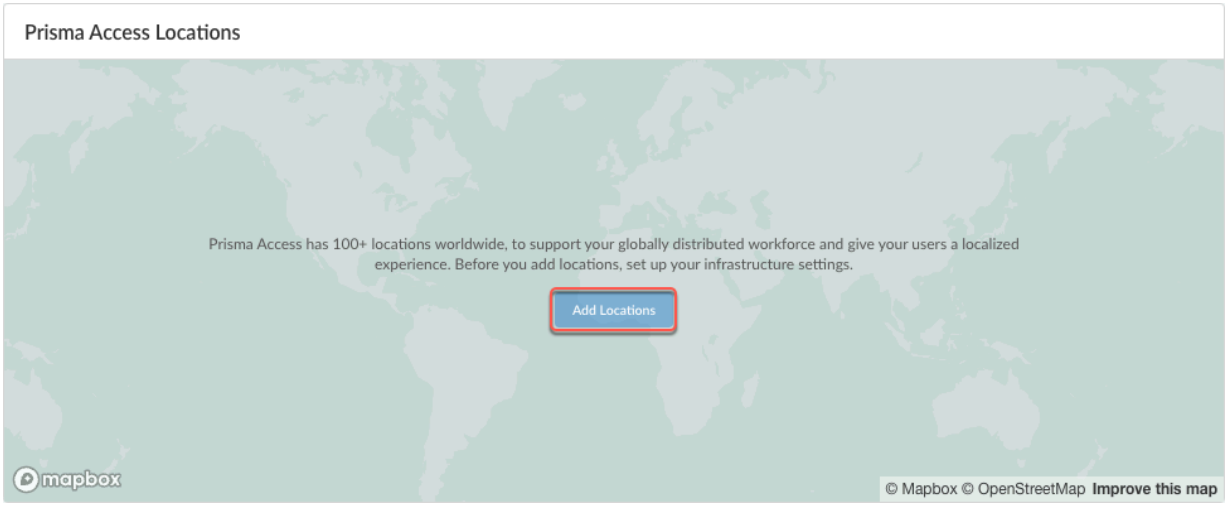
Sélectionner les emplacements Prisma Access

Sélectionnez les emplacements Prisma Access où vous souhaitez prendre en charge les utilisateurs d'Prisma Access Agent. Les groupes d'emplacements sont utilisés pour l'accès à privilèges dynamique.

STEP 1 | Dans Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Access Agent (Agent d'accès)** > **Infrastructure**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Si vous configurez l'infrastructure pour la première fois, cliquez sur **Add Locations (Ajouter des emplacements)**. Sinon, modifiez les **Prisma Access Locations (Emplacements d'accès Prisma)**.



STEP 3 | Sélectionnez les emplacements Prisma Access auxquels vos utilisateurs mobiles vont se connecter.

En fonction de votre contrat de licence, vous pouvez sélectionner des emplacements locaux ou universels. La carte montre les régions dans lesquelles vous pouvez déployer Prisma Access pour les utilisateurs. En outre, Prisma Access fournit plusieurs emplacements dans chaque région pour s'assurer que vos utilisateurs peuvent se connecter à un emplacement qui offre une expérience utilisateur adaptée à la région des utilisateurs. Pour des performances optimales, cliquez sur **Select All (Sélectionner tout)**. Sinon, sélectionnez des emplacements spécifiques dans chaque région sélectionnée où vos utilisateurs auront besoin d'accès. En limitant votre déploiement à une seule région, vous pouvez avoir un contrôle plus granulaire sur vos régions déployées et exclure les régions requises par votre politique ou les règles de l'industrie.

Pour les agents Prisma Access, vous pouvez déployer Prisma Access dans les régions Strata Logging Service suivantes :

- *États-Unis*
- *Allemagne*
- *Inde*

Cette liste sera mise à jour au fur et à mesure que d'autres régions seront disponibles.

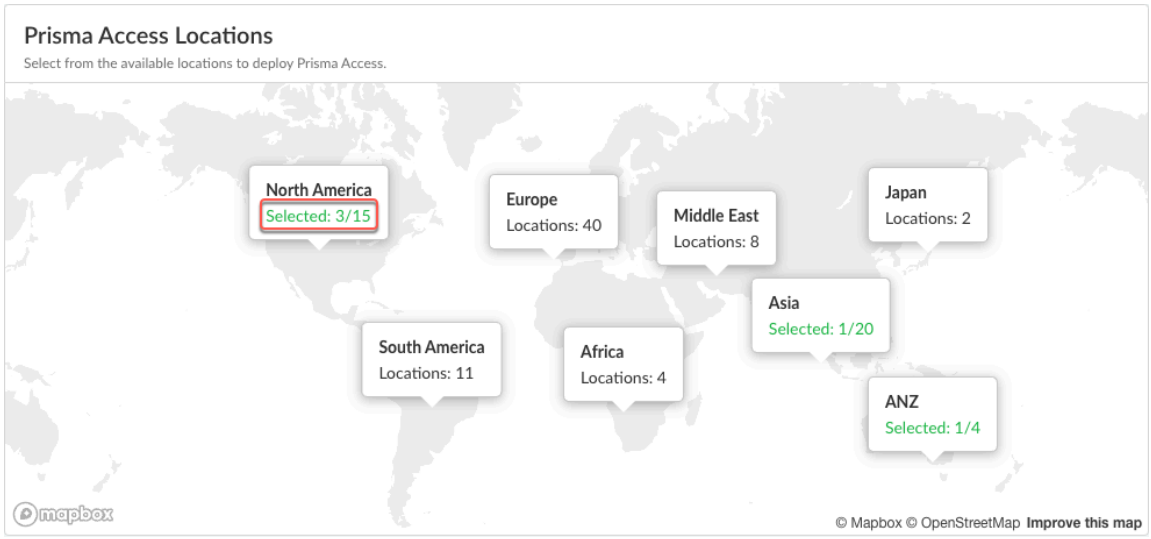
Pour une expérience utilisateur optimale, si vous limitez le nombre d'emplacements, choisissez les emplacements les plus proches ou situés dans le même pays que vos utilisateurs. Si aucun

 ©2025 Palo Alto Networks, Inc.

emplacement n'est disponible dans le pays où résident vos utilisateurs mobiles, choisissez l'emplacement le plus proche de vos utilisateurs pour obtenir les meilleures performances.

Les images de cette section sont fournies à titre indicatif seulement.

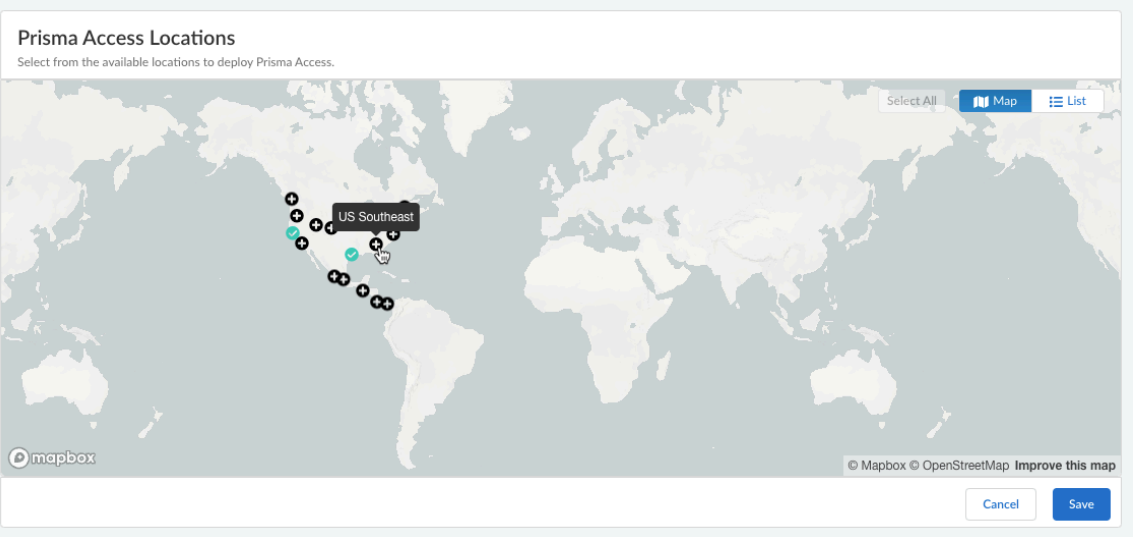
1. Sélectionnez une région disponible sur la carte.



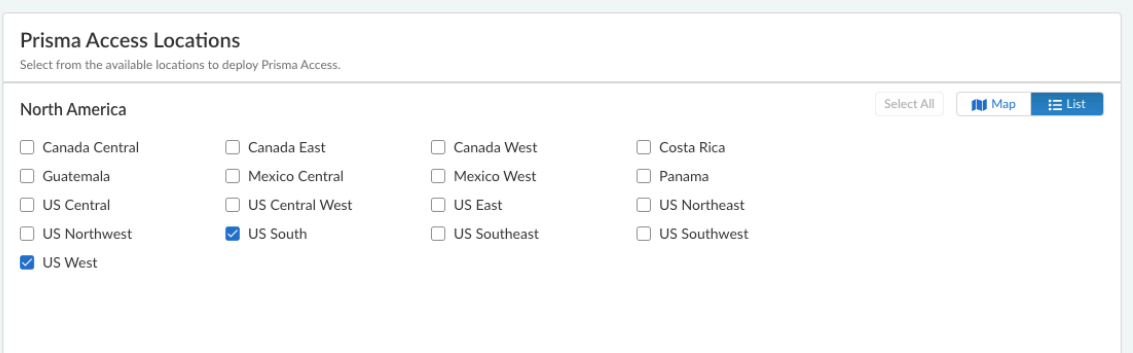
 ©2025 Palo Alto Networks, Inc.

2. Cliquez sur le signe **+** sur les emplacements que vous souhaitez ajouter.

   Vous pouvez basculer entre les vues **Map (Carte)** et **List (Liste)**. Vous pouvez également cliquer sur **Select All (Sélectionner tous)** pour sélectionner tous les emplacements.



   Dans la vue de liste, vous pouvez sélectionner dans la liste d'emplacements disponibles pour déployer Prisma Access. Vous pouvez sélectionner **All (Tous)** les sites au sein d'une région.



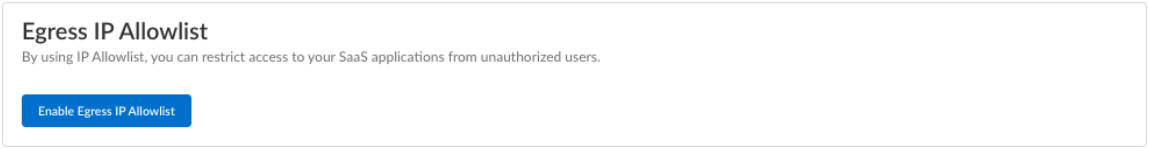
3. Cliquez sur **Save (Enregistrer)** pour enregistrer les paramètres de votre emplacement Prisma Access.

STEP 4 | (Facultatif) Empêchez l'accès à vos applications SaaS pour les utilisateurs non autorisés.

Vous pouvez activer les listes d'adresses IP de sortie autorisées pour les déploiements d'utilisateurs mobiles existants et lors de l'intégration de nouveaux utilisateurs. Si vous activez les listes d'adresses IP de sortie autorisées pour les déploiements Prisma Access existants, Prisma Access migre toutes les adresses IP de sortie déjà allouées à vos emplacements vers les listes d'adresses IP de sortie autorisées. Pour les nouveaux déploiements Prisma Access, activez la liste d'adresses IP de sortie autorisées lors de l'intégration des utilisateurs mobiles de Prisma Access Agent. Chaque fois que vous ajoutez un emplacement ou que vous avez un événement de mise à l'échelle automatique, vous devez récupérer les nouvelles adresses IP de sortie allouées par Prisma Access et les ajouter aux listes autorisées dans vos applications

SaaS. Vous pouvez ensuite transmettre la configuration à votre déploiement Prisma Access pour confirmer les listes d'adresses IP de sortie autorisées allouées à vos emplacements.

1. **Enable Egress IP Allowlist (Activez la liste d'adresses IP de sortie autorisées)** pour afficher les adresses IP des emplacements Prisma Access intégrés.



2. Copiez et ajoutez les adresses allouées aux listes autorisées de vos applications SaaS.
3. **Migrate (Migrez)** pour confirmer les adresses IP allouées aux emplacements intégrés dans Prisma Access.
4. Récupérez les adresses IP des nouveaux emplacements intégrés ou lors d'un événement de mise à l'échelle automatique.
    1. Sélectionnez le nom de **Location (Emplacement)** pour rechercher les nouvelles adresses IP de sortie allouées à l'emplacement.
    2. Ajoutez ces adresses IP aux listes autorisées de vos applications SaaS avant de les confirmer dans Prisma Access.
    3. Cliquez sur **Save (Enregistrer)** pour enregistrer les adresses IP de sortie allouées.

Activer le support SC-NAT pour l'accès à privilèges dynamique

Utilisez le support SC-NAT pour l'accès à privilèges dynamique (DPA) si vous utilisez le DPA et avez créé des connexions aux services pour accéder aux applications privées dans le site de votre centre de données ou de votre siège. Plusieurs projets dans votre environnement DPA peuvent subir un épuisement des adresses IP si les adresses IP du sous-réseau d'infrastructure se chevauchent. Pour résoudre ce problème, Prisma Access peut implémenter le NAT source (SNAT) pour les adresses IP, qui :

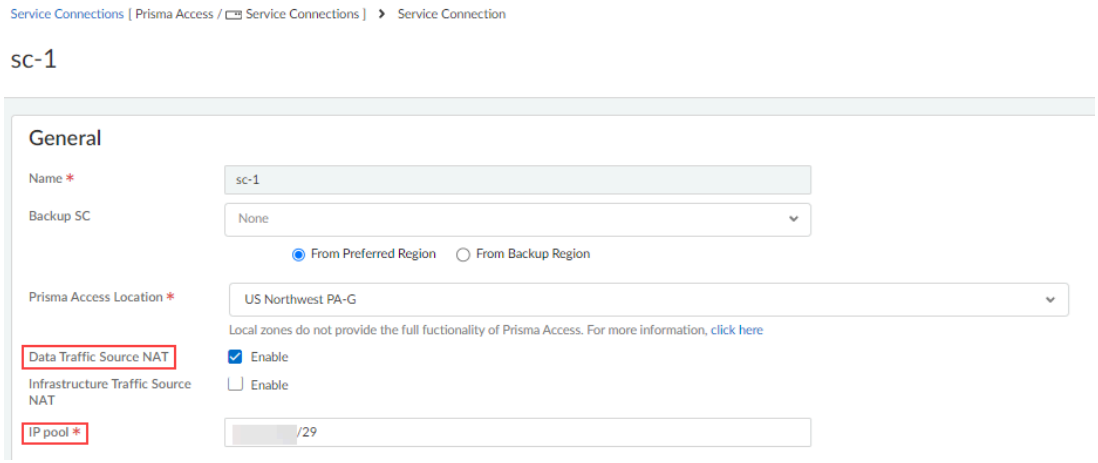
- Permet à Prisma Access de cartographier une seule adresse IP pour un utilisateur mobile accédant à des applis privées à l'aide d'une connexion de service
- Vous fournit SNAT pour faciliter le routage
- Élimine le chevauchement de pools IP
- Élimine l'épuisement IPv4 entre Prisma Access et le site de votre centre de données ou de votre siège

Les clients DPA peuvent intégrer des emplacements de clients à Prisma Access en utilisant des connexions aux services. Cependant, plusieurs projets peuvent avoir de grands pools d'IP sur plusieurs centres de données, conduisant à un épuisement potentiel des pools d'adresses IP privées. Pour résoudre ce problème, l'accès à privilèges dynamique dans Prisma Access offre le support SC-NAT avec des pools définis. Les clients ont la possibilité d'utiliser SC-NAT au lieu du sous-réseau d'infrastructure afin de diviser les pools d'adresses IP. Si vous activez SC-NAT pour une connexion aux services-nœud d'accès d'entreprise (SC-CAN), SC-NAT sera toujours pris en charge pour cette connexion aux services.

Avec DPA activé, vous pouvez activer SC-NAT (pour utiliser SC-NAT) ou le désactiver (pour utiliser le sous-réseau d'infrastructure) par projet.

 ©2025 Palo Alto Networks, Inc.

1. Dans Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connections (Connexions aux services)**.
2. Sélectionnez une connexion aux services dans le tableau **Service Connections (Connexions aux services)**.
3. Cochez la case correspondant à **Data Traffic Source NAT (NAT de source de trafic de données)**.
4. Après avoir coché la case **Data Traffic Source NAT (NAT de source de trafic de données)**, le champ obligatoire **IP Pool (Pool d'adresses IP)** s'affiche. Saisissez les sous-réseaux pour lesquels vous souhaitez activer SC-NAT.
5. **Save (Enregistrez)** vos modifications.



Activer le résumé de l'itinéraire pour l'accès à privilèges dynamique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.2 Innovation ❑ Version du plan de données Prisma Access minimum : 11.2.3 ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Rôle : Super utilisateur

Pour les entreprises qui disposent de matériel sur site avec une capacité limitée, comme de simples routeurs cloud qui ne peuvent accueillir que quelques centaines d'itinéraires, Prisma Access peut résumer les itinéraires des utilisateurs mobiles (MU) lors de l'annonce des itinéraires vers le réseau sur site. Le résumé des itinéraires minimise les exigences sur ces périphériques en restant dans la capacité des itinéraires sur le centre de données.

Pour activer le résumé des itinéraires, vous pouvez configurer des pools récapitulatifs globaux composés de listes de grands pools d'adresses IP utilisables sur plusieurs projets. Lorsqu'un utilisateur se connecte à un projet à l'aide de l'agent Prisma Access et que l'agent se voit attribuer une adresse IP dans la plage d'un pool récapitulatif global, la connexion aux services Prisma Access annonce le pool récapitulatif global au lieu de l'itinéraire agrégé plus petit.

 ©2025 Palo Alto Networks, Inc.

Pour illustrer le résumé des itinéraires pour les projets, envisagez le scénario suivant :

- Vous configurez un pool récapitulatif global 10.10.0.0/16 et activez l'option de résumé des itinéraires sur la connexion aux services **SC-A**.
- L'**User-A** (utilisateur A) se connecte au **Project-A** (projet A), auquel est assigné le pool d'adresses IP de projet 10.10.10.0/24. Lors de la connexion, l'agent Prisma Access acquiert l'adresse IP 10.10.10.10/32.
- L'**User-B** (utilisateur B) se connecte au **Project-B** (projet B), auquel est assigné le pool d'adresses IP de projet 10.10.11.0/24. Lors de la connexion, l'agent Prisma Access acquiert l'adresse IP 10.10.11.10/32.
- Dans ce cas, la connexion aux services annonce un seul sous-réseau (le pool récapitulatif global 10.10.0.0/16) au lieu des itinéraires agrégés /24 vers le réseau sur site via eBGP.



- *Prisma Access ne résume pas les pools d'adresses IP qui ne font pas partie d'un projet.*
- *Les pools d'adresses IP de projet au sein d'un projet peuvent se chevaucher, et les pools d'adresses IP récapitulatifs globaux peuvent également se chevaucher.*
- *Les pools récapitulatifs globaux doivent être de grands pools d'adresses IP contenant les pools d'adresses IP de projet associés à plusieurs projets.*

Pour activer le résumé des itinéraires pour les projets dans Strata Cloud Manager :

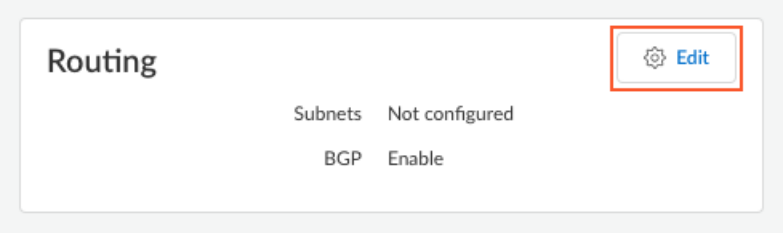
STEP 1 | Configurez les pools d'adresses IP de projet dans les paramètres du projet dans **Manage (Gérer)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **<Snippet>** > **Objects (Objets)** > **Dynamic Privilege Access (Accès à privilèges dynamique)** > **Projects (Projets)**.

STEP 2 | Configurez les pools d'adresses IP récapitulatifs globaux dans **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Access Agent (Agent d'accès)** > **Infrastructure Settings (Paramètres d'infrastructure)**.

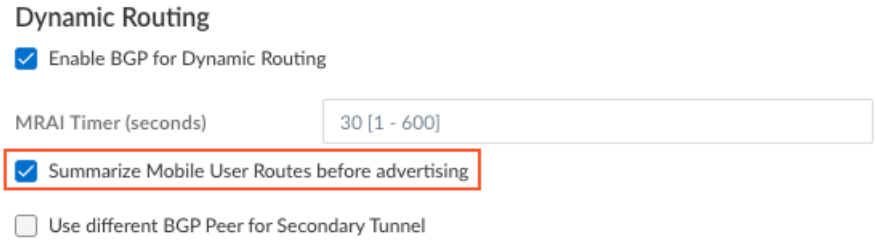
 ©2025 Palo Alto Networks, Inc.

STEP 3 | Activez le résumé des itinéraires dans la connexion aux services.

1. Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connections (Connexions aux services)**.
2. Sélectionnez une connexion aux services dans le tableau **Service Connections (Connexions aux services)**.
3. **Edit (Modifiez)** les paramètres de routage.



4. Sélectionnez **Summarize Mobile User Routes before advertising (Résumer les itinéraires des utilisateurs mobiles avant de publier)**.



STEP 4 | **Save (Enregistrez)** les paramètres de routage.

STEP 5 | **Save (Enregistrez)** les paramètres de connexion aux services.

STEP 6 | Appliquez une configuration à tous les administrateurs de Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Créer un extrait

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Rôle : Super utilisateur

Vous pouvez créer un extrait pour regrouper les configurations de Prisma Access Agents que vous pouvez rapidement transférer vers vos déploiements. Les extraits sont utilisés pour normaliser une configuration de base commune pour un ensemble de déploiements basés sur les projets, ce qui permet d'intégrer rapidement de nouveaux périphériques avec une bonne configuration connue et de réduire le temps nécessaire à l'intégration d'un nouveau périphérique.

Après avoir créé l'extrait, vous associerez l'extrait à une étendue, vous affecterez un utilisateur à l'étendue et vous accorderez à l'utilisateur le rôle administrateur de projet. L'utilisateur peut ensuite se connecter en tant qu'administrateur de projet et utiliser l'extrait pour gérer les paramètres du projet pour Prisma Access Agent. L'administrateur du projet ne peut modifier que les paramètres de Prisma Access Agent pour les extraits auxquels ils sont affectés.

Pour créer un extrait, procédez comme suit :

STEP 1 | Connectez-vous à Strata Cloud Manager en tant que super utilisateur.

STEP 2 | Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)**.

STEP 3 | Sélectionnez **Overview (Aperçu)** et développez la portée de la configuration pour afficher les **Snippets (Extraits)**.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Cliquez sur **Add Snippet (Ajouter un extrait)** et saisissez les détails suivants :

1. Saisissez un **Name (Nom)** pour l'extrait.
2. (Facultatif) Saisissez une **Description** pour l'extrait.
3. (Facultatif) Attribuer une ou plusieurs **Labels (Étiquettes)**.

   Vous pouvez sélectionner une étiquette existante ou en créer une nouvelle en saisissant l'étiquette que vous souhaitez créer.
4. Pour garantir que les noms d'objet sont uniques dans un extrait, l'option **Add prefix to object names (Ajouter un préfixe aux noms d'objet)** est activée par défaut.

   Cliquez sur **Auto (Automatique)** pour générer automatiquement un préfixe aléatoire ou sur **Manual (Manuel)** et ajoutez votre propre **Prefix Value (Valeur de préfixe)**. La valeur du préfixe peut être alphanumérique et comporter un maximum de six caractères.

   Le préfixe aura le format **xxxxxx-**. Lorsque vous ajoutez un objet, Strata Cloud Manager préremplit le nom de l'objet avec le préfixe.
5. Cliquez sur **Create (Créer)** pour créer les extraits.

   Après avoir créé l'extrait, vous êtes dans la portée de configuration de l'extrait. Toutes les configurations que vous créez dans le champ d'application de l'extrait ne s'appliquent qu'à cet extrait.

STEP 5 | Associez l'extrait au dossier **Access Agent (Agent d'accès)**.

1. Dans la page Overview (Aperçu) de votre extrait, sélectionnez les paramètres **Snippet Associations (Associations d'extraits)**.
2. Sélectionnez **Access Agent (Agent d'accès)** dans les **Config trees (Arborescences de configuration)**.
3. Cliquez sur **X** pour fermer la fenêtre Snippet Associations (Associations d'extraits).

   L'option **Access Agent (Agent d'accès)** apparaît dans la liste des associations d'extraits.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Si vous ne l'avez pas déjà fait, créez une identité pour l'utilisateur qui gérera les projets et attribuez-lui le rôle Transmission de l'administrateur de projet.

1. Depuis Strata Cloud Manager, sélectionnez **Settings (Paramètres)** > **Identity & Access (Identité et accès)**.
2. Sélectionnez **Add Identity (Ajouter une identité)**.
3. Saisissez l'adresse **Identity Address (Adresse d'identité)** de l'utilisateur qui sera l'administrateur du projet et cliquez sur **Next (Suivant)**.
4. Sélectionnez **Add Access (Ajouter un accès)** > **Prisma Access & NGFW Configuration (Configuration de Prisma Access & NGFW)** et sélectionnez le rôle **Project Admin Push (Transmission de l'administrateur de projet)** pour l'utilisateur.
5. Cliquez sur **Submit (Envoyer)**.

STEP 7 | Créez une étendue de gestion pour l'extrait et attribuez un utilisateur à cette étendue.

1. Sélectionnez **Manage (Gestion)** > **Access Control (Contrôle d'accès)** > **Scope Management (Gestion de la portée)**.
2. **Créer une nouvelle étendue**
3. Saisissez un **Name (Nom)** pour l'étendue et affichez les **Snippets (Extraits)**.
4. Associez l'extrait à l'étendue. Sélectionnez l'extrait que vous avez créé et cliquez sur **Add (Ajouter)** pour l'ajouter.
5. Dans les objets de l'étendue, cliquez sur **Assign Users (Attribuer des utilisateurs)** pour les attribuer à l'étendue que vous avez créée pour votre extrait.
6. Attribuez un utilisateur à l'étendue en sélectionnant un utilisateur dans la liste et en lui attribuant le rôle **Project Admin (Administrateur de projet)**.
7. **Close (Fermez)** la fenêtre.
8. Transmettez la configuration.
   1. Sélectionnez **Manage (Gestion)** > **Operations (Opérations)** > **Push Config (Transmettre la configuration)**.
   2. Sélectionnez l'étendue de l'administrateur **All Admins (Tous les administrateurs)** et sélectionnez **Push Config (Transmettre la configuration)** > **Push (Transmettre)**.

   Une fois l'opération de transmission de configuration terminée, l'extrait est créé et les rôles sont associés à l'extrait.

   L'utilisateur attribué (administrateur du projet) peut désormais se connecter à Strata Cloud Manager et configurer des paramètres Prisma Access Agent spécifiques au projet en utilisant l'extrait que vous avez créé. L'utilisateur peut afficher d'autres étendues auxquelles il n'est pas attribué, mais il ne peut pas interagir avec elles, par exemple en modifiant des configurations.

 ©2025 Palo Alto Networks, Inc.

Configurer les paramètres Prisma Access Agent spécifiques au projet

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Rôle : Administrateur de projet

Une fois que l'administrateur super utilisateur a configuré l'infrastructure, créé un extrait et vous l'a attribué, vous pouvez vous connecter en tant qu'administrateur de projet pour configurer les paramètres Prisma Access Agents spécifiques au projet, tels que l'IP privée, le tunnel partagé et les informations DNS qui seront assignées aux terminaux lorsqu'ils se connectent à un projet à l'aide de Prisma Access Agent.

Vous pouvez créer des paramètres spécifiques au projet pour un ou plusieurs Prisma Access Agents ou utiliser les paramètres par défaut de l'agent. Vous pouvez utiliser un agent différent pour chaque projet que vous avez géré, ou partager un agent avec plusieurs projets.

Configurer les profils de transfert pour gérer le trafic des agents pour les agents d'accès à privilège dynamique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Rôle : Administrateur de projet

Les profils de transfert fournissent une interface unique pour configurer et gérer les règles de transfert du trafic et l'application du trafic, telles que la configuration des paramètres de tunnel fractionné et la gestion du trafic en dehors de la connexion au tunnel. Les profils de transfert améliorent la configuration disjointe des politiques de trafic rencontrées avec d'autres agents d'accès mobiles et étendent considérablement la limite du nombre de règles et d'entrées que

 ©2025 Palo Alto Networks, Inc.

vous pouvez configurer. En simplifiant les configurations associées et en améliorant la clarté, vous pouvez vous concentrer sur la manière dont vous souhaitez que le trafic des terminaux soit acheminé et appliqué.

Le profil de transfert est un type de profil qui contient plusieurs sections logiques et ordonnées. Ces sections illustrent les différentes phases d'une connexion avant que l'agent détermine comment celle-ci doit être dirigée. Cette structure organisationnelle peut vous aider à comprendre les raisons pour lesquelles le trafic est acheminé d'une certaine manière en présentant les entrées ordonnées dans chaque section. Vous pouvez ajouter, modifier, supprimer ou réorganiser des entrées dans chaque section.

Une fois les profils de transfert sont configurés, vous pouvez les attribuer à des utilisateurs ou à des groupes d'utilisateurs dans la page Paramètres de l'agent.

Les règles de transfert de trafic sont appliquées de haut en bas dans le profil de transfert. Par conséquent, configurez le profil de transfert de manière descendante, par exemple en commençant par la configuration des règles les plus spécifiques et en terminant par les règles les moins spécifiques.

Règles de transfert

Un profil de transfert se compose d'un ensemble de règles de transfert de trafic qui spécifient quel trafic d'application source ou de domaine de destination et d'adresse IP de destination passe par le tunnel ou en dehors du tunnel, s'il faut fractionner le trafic DNS et quelle application du trafic est en vigueur. Le trafic correspondant à une règle est transmis à Prisma Access conformément aux spécifications de transfert de trafic. Les spécifications d'une règle de transfert sont organisées dans les sections suivantes :

- **Source Applications (Applications sources)** : spécifie les applications privées ou SaaS auxquelles la règle s'applique. Lorsque le trafic provenant d'un terminal correspond à l'appli source, le trafic est acheminé conformément à la règle de transfert.
- **Destinations** : spécifie les domaines et les adresses IP auxquels la règle s'applique. Lorsque le trafic correspond aux destinations (spécifiées sous forme de FQDN ou d'adresses IP), le trafic est acheminé conformément à la règle de transfert.

Contrôle de la circulation

Chaque profil de transfert contient également des paramètres d'application du trafic qui vous autorisent à :

- Bloquer tout le trafic sortant qui ne correspond à aucune règle de transfert
- Bloquer l'accès au LAN sortant lorsque l'agent est connecté au tunnel
- Bloquer l'accès entrant lorsque l'agent est connecté au tunnel

Pour configurer un profil de transfert, suivez les étapes suivantes :

STEP 1 | Connectez-vous à Strata Cloud Manager en tant qu'administrateur du projet.

STEP 2 | Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)** et développez la Configuration Scope (Portée de configuration) pour afficher les **Snippets (Extraits)**.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Sélectionnez l’extrait que l’administrateur du super utilisateur vous a attribué.

Vous pouvez également afficher les extraits qui ne vous sont pas attribués, mais vous ne pouvez pas interagir avec eux, par exemple pour modifier la configuration.

STEP 4 | Sélectionnez **Objects (Objets)** > **Dynamic Privilege Access (Accès à privilèges dynamique)** pour ouvrir les paramètres d’accès à privilèges dynamique.

STEP 5 | Sélectionnez **Forwarding Profiles (Profils de transfert)** et modifiez la **Forwarding Profiles Setup (Configuration des profils de transfert)**.

 ©2025 Palo Alto Networks, Inc.

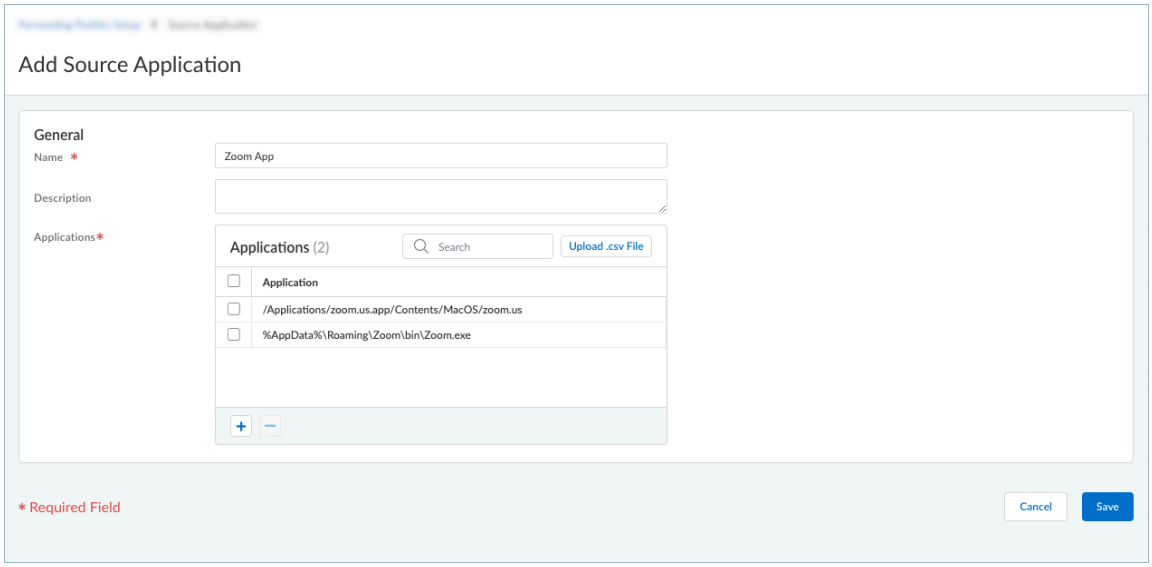
STEP 6 | Configurez les **Source Applications (Applications sources)** si vous souhaitez créer des tunnels fractionnés en fonction du nom de l'application SaaS ou cloud public.

1. Dans la page Configuration des profils de transfert, sélectionnez **Source Applications (Applications sources)** > **Add Source Application (Ajouter une application source)**.

2. Saisissez un **Name (Nom)** significatif pour l'application que vous souhaitez ajouter.
3. Cliquez sur le signe **+** dans le tableau **Applications** et saisissez le chemin complet de l'application. Vous pouvez ajouter une ou plusieurs applications pour gérer l'exclusion ou l'inclusion du trafic de l'application dans le tunnel.

   Si vous choisissez d'exclure le trafic de l'application (en sélectionnant la connectivité **Direct (directe)** dans la règle de transfert), le trafic de ces applications est envoyé sur les terminaux via l'adaptateur physique plutôt que via le tunnel (l'adaptateur virtuel).

   Si vous choisissez d'inclure le trafic de l'application (en sélectionnant la connectivité **Tunnel** dans la règle de transfert), le trafic de ces applications est acheminé vers Prisma Access, même s'il répond aux critères d'exclusion du trafic.



   Par exemple, pour gérer le trafic depuis l'application Zoom, ajoutez les chemins complets suivants :

   - terminaux Windows : **`%AppData%\Roaming\Zoom\bin\Zoom.exe`**
   - terminaux macOS : **`/Applications/zoom.us.app/Contents/MacOS/zoom.us`**

   Si vous avez une liste d'applications dans un fichier texte au format de valeurs séparées par des virgules (`.csv`), vous pouvez **Upload .csv File (Charger un fichier .csv)**.
4. Cliquez sur **Save (Enregistrer)** pour enregistrer l'application source.
5. Répétez ces étapes pour ajouter d'autres applications sources.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Configurez les **Destinations** si vous souhaitez créer des tunnels fractionnés en fonction du domaine de destination ou des itinéraires d'accès.

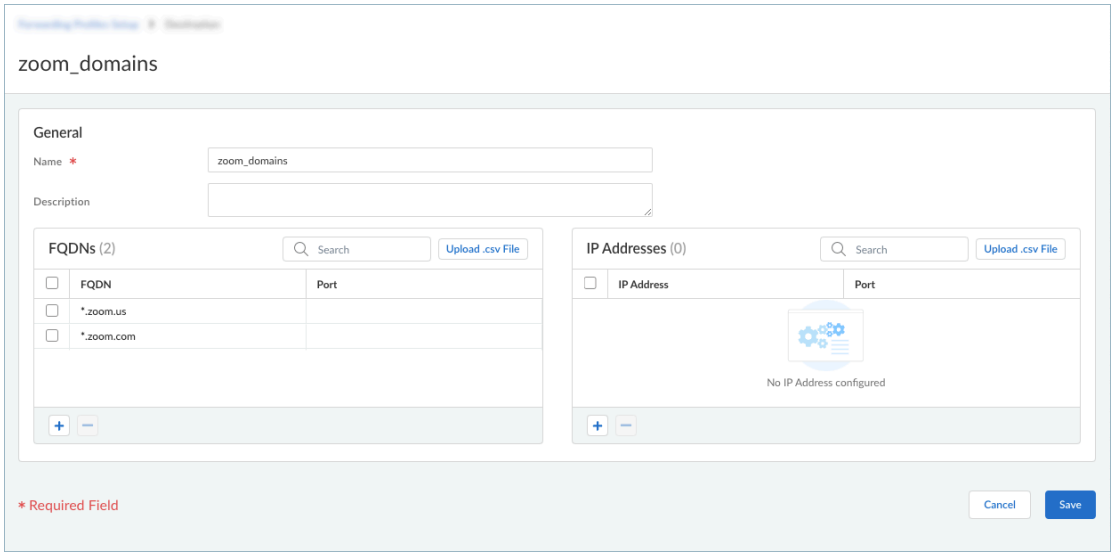
1. Dans la page Configuration des profils de transfert, sélectionnez **Destinations** > **Add Destination (Ajouter une destination)**.

2. Saisissez un **Name (Nom)** significatif pour la destination que vous souhaitez ajouter.
3. Ajoutez une destination en spécifiant le nom de domaine, l'itinéraire d'accès ou les deux.

   - Pour ajouter un domaine de destination, cliquez sur le signe **+** dans le tableau des **FQDN** et saisissez le FQDN du domaine de destination. Vous pouvez éventuellement ajouter un port. Si vous ne spécifiez pas de port, tous les ports du domaine spécifié sont soumis à la règle de transfert. Vous pouvez ajouter un ou plusieurs domaines pour la gestion du trafic.

     Si vous choisissez d'exclure le trafic en fonction du nom de domaine (en sélectionnant la connectivité **Direct (directe)** dans la règle de transfert), le trafic du domaine est envoyé sur les terminaux via l'adaptateur physique plutôt que via le tunnel (l'adaptateur virtuel).

     Si vous choisissez d'inclure le trafic en fonction du nom de domaine (en sélectionnant la connectivité **Tunnel** dans la règle de transfert), le trafic du domaine est acheminé vers Prisma Access, même s'il répond aux critères d'exclusion de trafic.



   - Pour ajouter un itinéraire d'accès, cliquez sur le signe **+** dans le tableau **IP Addresses (Adresses IP)** et saisissez un sous-réseau de destination. Vous pouvez ajouter une ou plusieurs itinéraires d'accès pour la gestion du trafic.

     N'incluez pas de caractères génériques dans l'adresse IP. Les caractères génériques dans les adresses IP ne sont pas pris en charge dans les profils de transfert.

     Si vous n'incluez ni n'excluez d'itinéraires ou d'applications, chaque demande est acheminée via le tunnel (sans un tunnel fractionné). En outre, tout le trafic est

 ©2025 Palo Alto Networks, Inc.

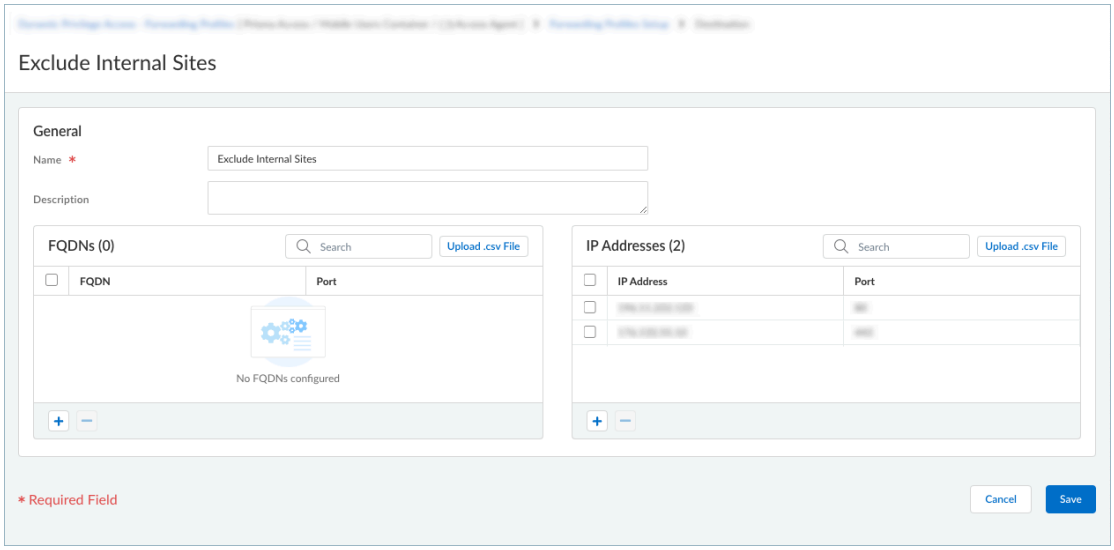
inspecté et soumis à l'application des politiques à chaque fois que les utilisateurs se connectent à Prisma Access.

Lorsque vous définissez le trafic de tunnel fractionné pour exclure des itinéraires d'accès (en sélectionnant la connectivité **Direct (directe)** dans la règle de transfert), ces itinéraires sont envoyés sur le terminal via l'adaptateur physique au lieu d'être envoyés via le tunnel via l'adaptateur virtuel (le tunnel). En excluant le trafic du tunnel fractionné par les itinéraires d'accès, vous pouvez envoyer le trafic sensible à la latence ou à bande passante élevée en dehors du tunnel, tandis que tout autre trafic est acheminé via le tunnel pour inspection et application des politiques par la passerelle Prisma Access.

Lorsque vous définissez le trafic de tunnel fractionné pour inclure des itinéraires d'accès (en sélectionnant la connectivité **Tunnel** dans la règle de transfert), la passerelle Prisma Access envoie ces itinéraires aux terminaux des utilisateurs distants afin de spécifier le trafic que ces terminaux peuvent envoyer via le tunnel.

Spécifiez des itinéraires exclus qui sont plus spécifiques que les itinéraires inclus. Sinon, vous risqueriez d'exclure plus de trafic que prévu.

Si vous avez une liste d'adresses IP dans un fichier texte au format `.csv`, vous pouvez **Upload .csv File (Charger un fichier .csv)**.



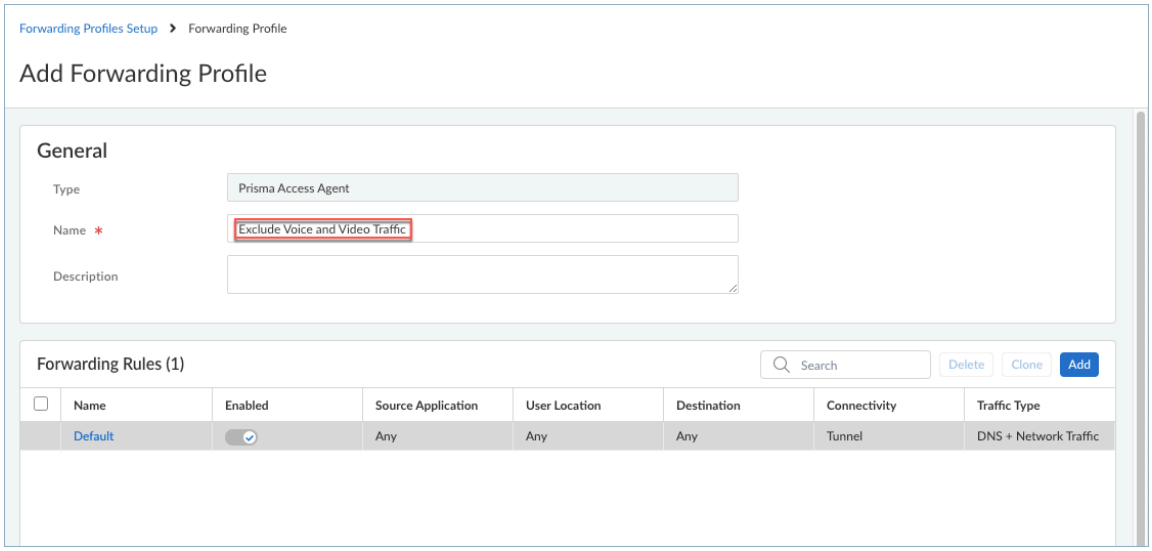
4. Cliquez sur **Save (Enregistrer)** pour enregistrer les destinations.
5. Répétez ces étapes pour ajouter d'autres destinations.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Créez un profil de transfert qui autorise ou exclut le trafic en fonction des applications ou des destinations sources que vous avez configurées.

1. Pour ajouter un profil de transfert, sélectionnez **Forwarding Profiles (Profils de transfert)** > **Add Forwarding Profile (Ajouter un profil de transfert)** > **Prisma Access Agent**.

   Pour modifier un profil de transfert, sélectionnez le nom du profil dans le tableau Profils de transfert.
2. Saisissez un **Name (Nom)** significatif pour le profil de transfert.
3. Cliquez sur **Add (Ajouter)** pour ajouter une règle de transfert.

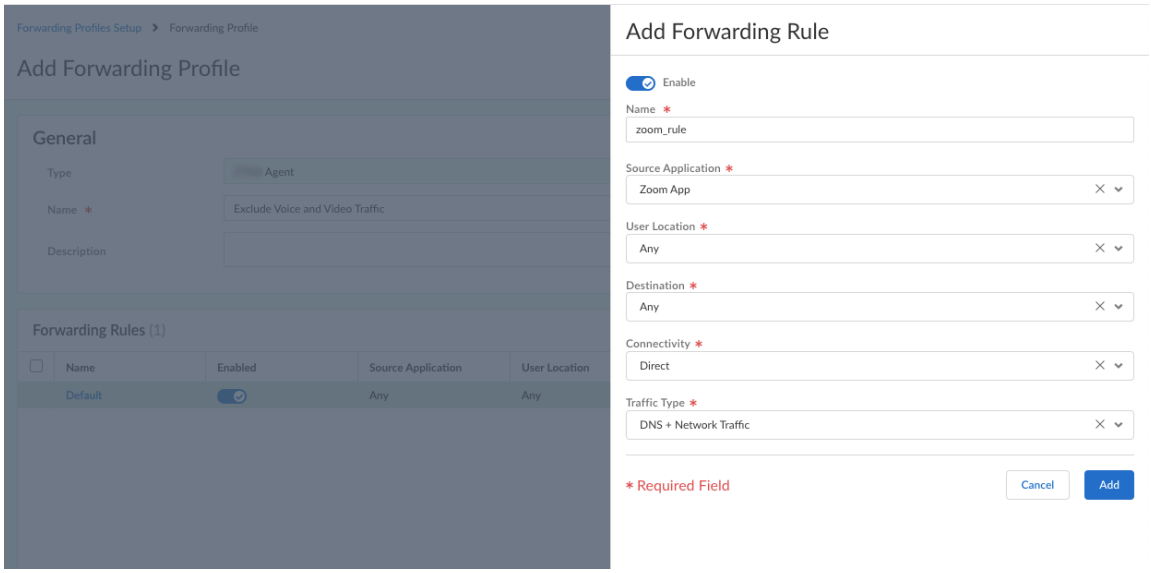


Le tableau Règles de transfert affiche les règles qui composent le profil de transfert. Tous les profils de transfert contiennent la règle de transfert **Default (Par défaut)** qui envoie tout le trafic DNS et réseau via le tunnel. Toutes les nouvelles règles que vous ajoutez sont placées au-dessus de la règle par défaut. Vous ne pouvez pas supprimer

 ©2025 Palo Alto Networks, Inc.

ou déplacer la règle de transfert par défaut, mais vous pouvez modifier son paramètre **Connectivity (Connectivité)**.

4. Saisissez les spécifications de la règle de transfert.



1. **Enable (Activez)** la règle.
2. Donnez un **Name (Nom)** à la règle.
3. Sélectionnez la **Source Application (Application source)** que vous avez définie précédemment. Si vous sélectionnez **Any (Indifférent)**, la règle de transfert s'appliquera au trafic provenant de n'importe quelle application source.

   La règle correspondra uniquement si la connexion est établie par l'application source spécifiée.
4. Sélectionnez un **User Location (Emplacement de l'utilisateur)**. Si vous n'avez pas configuré d'emplacement d'utilisateur ou si vous autorisez la règle à correspondre

 ©2025 Palo Alto Networks, Inc.

à n'importe quel emplacement d'utilisateur, sélectionnez **Any (Indifférent)**. (Ne s'applique pas aux agents compatibles Dynamic Privilege Access.)

La règle correspondra uniquement si un terminal est connecté à l'emplacement d'utilisateur que vous spécifiez.

5. Sélectionnez une **Destination** que vous avez définie précédemment. Si vous sélectionnez **Any (Indifférent)**, la règle de transfert s'appliquera au trafic provenant de n'importe quel domaine de destination ou adresse IP.

   La règle correspondra uniquement si la destination de connexion correspond au domaine de destination ou à l'adresse IP spécifiés.

6. Sélectionnez la **Connectivity (Connectivité)** :

   - **Direct (Directe)** : envoie le trafic en dehors du tunnel. Tout le trafic de l'application ou de la destination sélectionnée est envoyé directement à l'adaptateur physique sur le terminal sans inspection.
   - **Tunnel** : envoie le trafic via le tunnel. Tout le trafic allant vers l'application ou la destination sélectionnée est envoyé via le tunnel vers Prisma Access pour inspection et application des politiques.

7. Sélectionnez le **Traffic Type (Type de trafic)** :

   indiquez si vous souhaitez utiliser un DNS fractionné pour autoriser les utilisateurs à diriger leurs requêtes DNS vers les applications et les ressources via le tunnel ou en dehors du tunnel en plus du trafic réseau.

   - **DNS + Network Traffic (trafic DNS et réseau)** :veille à ce que le tunnel fractionné sur la base du domaine de destination que vous avez indiqué pour les inclusions et les exclusions soit appliqué au trafic DNS et au trafic de l'application du réseau associé pour ce domaine.
   - **Network Traffic (Trafic réseau)** : inclut ou exclut les règles qui sont appliquées uniquement au trafic de l'application réseau et non au trafic DNS. Tout le trafic

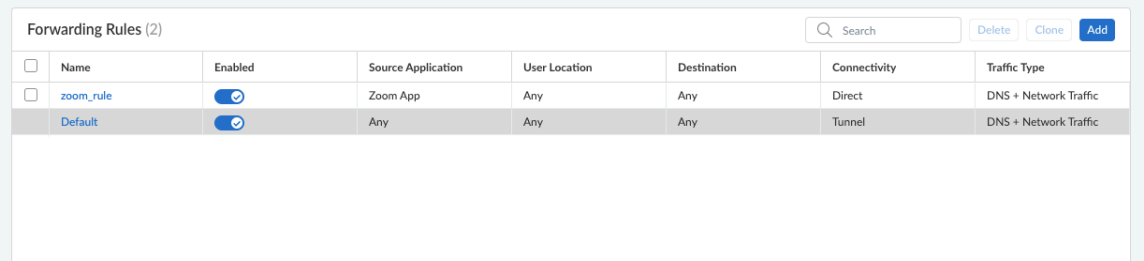
 ©2025 Palo Alto Networks, Inc.

DNS passe par le tunnel quel que soit le tunnel fractionné basé sur le domaine de destination que vous avez indiqué pour les inclusions ou les exclusions.

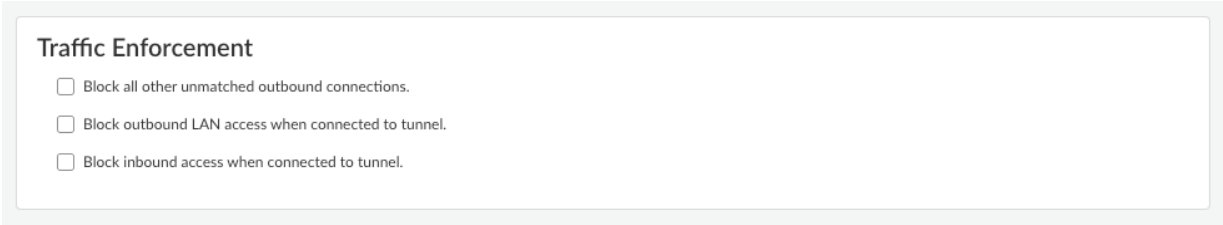
*Pour les agents Windows, l'option de tunnel fractionné **DNS + Network Traffic (DNS + trafic réseau)** n'est pas prise en charge pour les règles de tunnel fractionné basées sur les applications. Si vous configurez le tunneling fractionné pour inclure ou exclure le trafic du tunnel en fonction des noms d'applications et sélectionnez **DNS + Network Traffic (DNS + Trafic réseau)**, les paquets de requête DNS pour les applications exclues et incluses ne respecteront pas la règle de tunnel fractionné.*

5. Cliquez sur **Add (Ajouter)** pour ajouter la règle de transfert.

   La règle est ajoutée au tableau Règles de transfert. Vous pouvez ajouter plusieurs règles au profil de transfert.



STEP 9 | Configurez les options **Traffic Enforcement (Application du trafic)** pour déterminer la manière dont vous souhaitez appliquer le trafic.



*Assurez-vous de **désélectionner toutes** ces options, car elles ne sont pas recommandées pour l'accès à privilèges dynamique.*

- **Block all other unmatched outbound connections (Bloquer toutes les autres connexions sortantes non correspondantes)** : lorsque cette option est activée, elle bloque toutes les connexions qui ne correspondent à aucune des règles de transfert. Le trafic ne sera pas envoyé via le tunnel.
- **Block outbound LAN access when connected to the tunnel (Bloquer l'accès LAN sortant lors de la connexion au tunnel)** : lorsque cette option est activée, elle bloque l'accès direct au réseau local lorsque l'agent est connecté au tunnel.

  Le blocage de l'accès à votre réseau local entraîne l'envoi de tout le trafic à l'adaptateur local. En outre, vos utilisateurs ne pourront pas accéder aux ressources du sous-réseau

 ©2025 Palo Alto Networks, Inc.

local, telles que les imprimantes. Le trafic du tunnel fractionné en fonction de l'itinéraire d'accès, du domaine de destination et de l'application fonctionne toujours comme prévu.

Si vous désactivez cette option, vos utilisateurs finaux peuvent accéder aux ressources locales sans avoir à se connecter d'abord à Prisma Access à l'aide de Prisma Access Agent.

- **Block inbound access when connected to the tunnel (Bloquer l'accès entrant lors de la connexion au tunnel)** : lorsque cette option est activée, elle bloque toutes les connexions entrantes provenant du tunnel.

STEP 10 | Cliquez sur **Save (Enregistrer)** pour enregistrer votre profil de transfert.

STEP 11 | Transmettez la configuration en sélectionnant **Push Config (Transmettre la configuration) > Push (Transmettre)**. Cette action rendra votre profil de transfert disponible à la sélection dans la page Paramètres de l'agent.

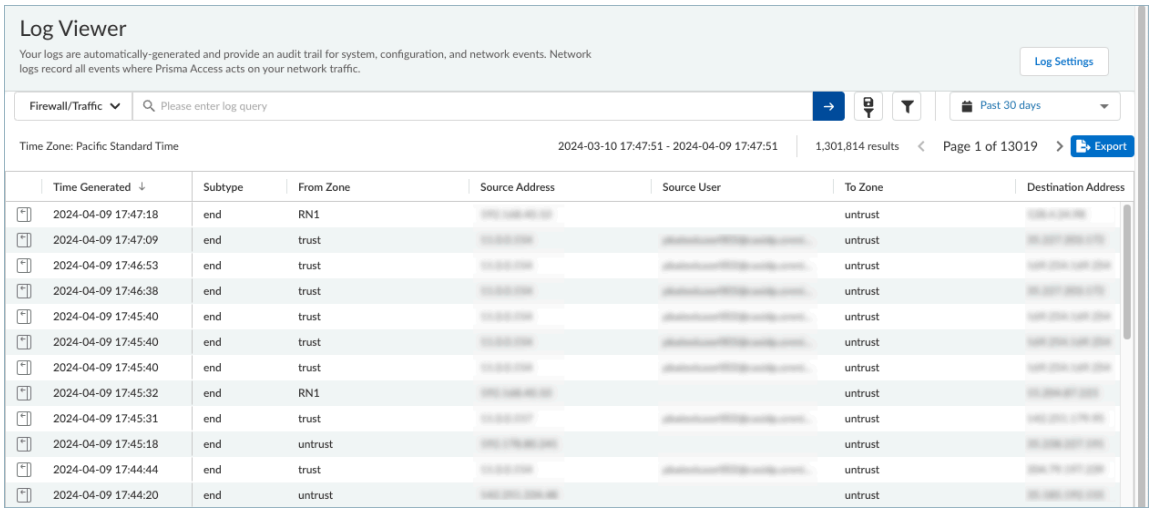
Vérifier et résoudre les problèmes des configurations de profil de transfert pour les agents de l'accès à privilèges dynamiques.

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (géré par Strata Cloud Manager)	☐ Prisma Access 5.1 version préférée ou innovation ☐ Licence Prisma Access avec l'abonnement Utilisateur mobile ☐ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ☐ Rôle : Super utilisateur

Après avoir configuré un profil de transfert, vous pouvez vérifier si le trafic est dirigé comme prévu en affichant les fichiers journaux du trafic. Vous pouvez afficher les journaux du trafic dans la visionneuse de journaux de Strata Cloud Manager ou en utilisant l'outil de ligne de commande de Prisma Access (PACli) sur un terminal.

 ©2025 Palo Alto Networks, Inc.

- Pour afficher les fichiers journaux du trafic à partir de la visionneuse de journaux de Strata Cloud Manager :
  1. Sélectionnez **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)**.
  2. Consultez les journaux **Firewall/Traffic (Pare-feu/trafic)** pour plus de détails.



 ©2025 Palo Alto Networks, Inc.

- Pour afficher les fichiers journaux du trafic sur un terminal :
  1. Démarrez le shell à distance dans **Manage (Gérer)** > **Prisma Access Agent** ou ouvrez une invite de commande Windows ou une fenêtre de terminal macOS sur le périphérique d'un utilisateur final.
  2. Pour afficher les règles de transfert dans un profil de transfert, utilisez la commande suivante :
     - Sous Windows :

       ```
       "C:\Program Files\Palo Alto Networks\Prisma Access Agent
       \pacli" traffic show
       ```

     - Sous macOS :

       ```
       /Applications/Prisma\ Access\ Agent.app/Contents/Helpers/
       pacli traffic show
       ```

       *Si vous configurez une variable d'environnement pour l'outil PACli (`pacli`), vous pouvez simplement saisir **`pacli traffic show`**.*



L'exemple de sortie de ligne de commande PACli affiche un tableau contenant les règles de transfert en vigueur dans le profil de transfert, y compris les priorités des règles de transfert. Les sélections d'application du trafic pour le profil de transfert sont également

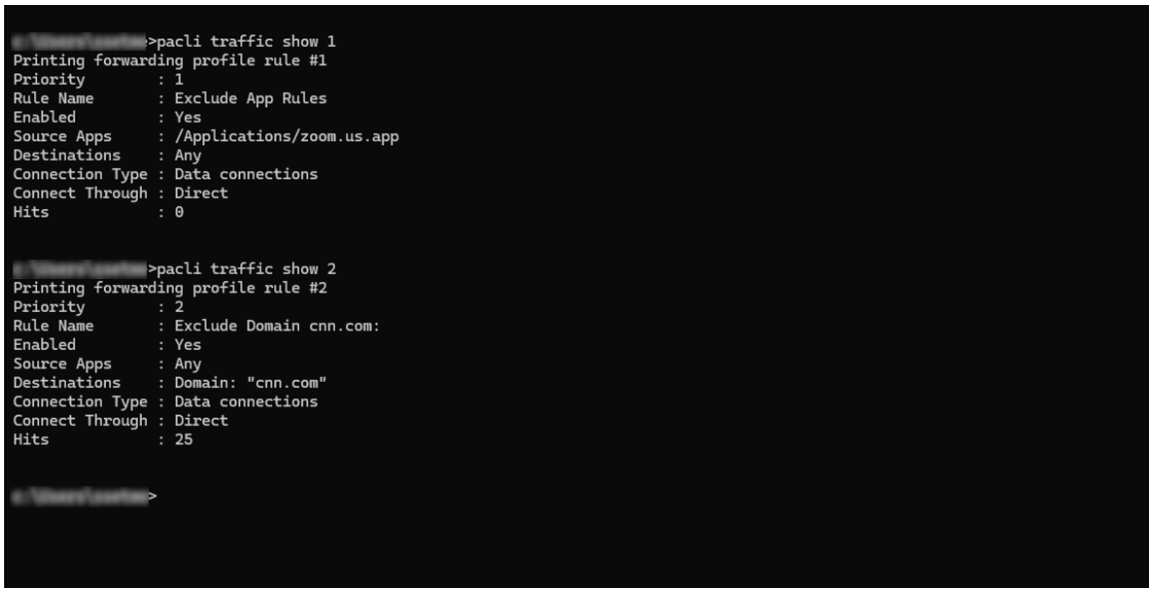
 ©2025 Palo Alto Networks, Inc.

affichées. Ce tableau correspond aux règles de transfert que vous configurez dans votre profil de transfert.

3. Pour afficher les détails d'une règle de transfert, utilisez la commande suivante :

```
pacli traffic show <number>
```

Où **<number>** est le numéro dans la colonne `Priority`, par exemple :

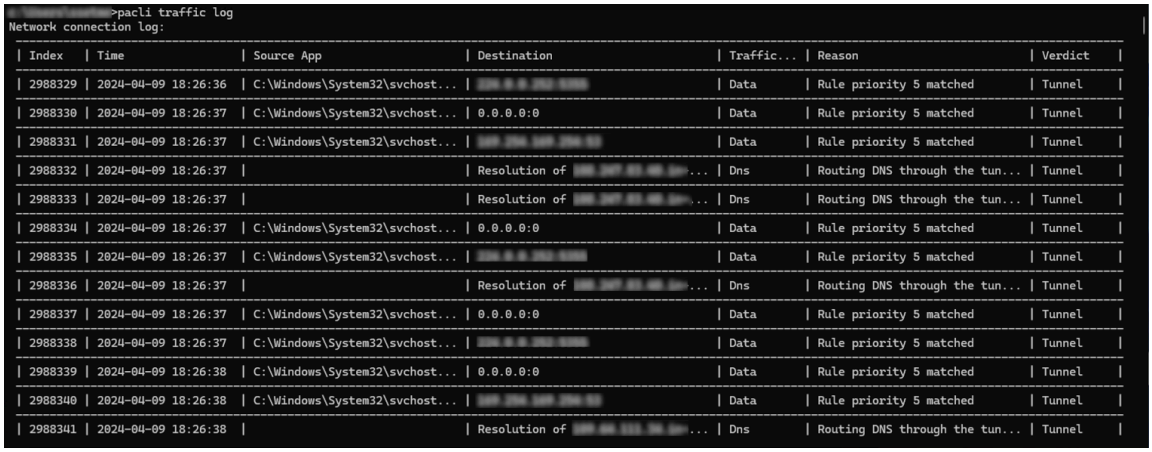


4. Pour résoudre les problèmes de tunnel fractionné, vous pourriez devoir examiner quel trafic d'agent se trouve à l'intérieur ou à l'extérieur du tunnel. Vous pouvez le faire

 ©2025 Palo Alto Networks, Inc.

en affichant le journal des connexions de Prisma Access Agent. Utilisez la commande suivante :

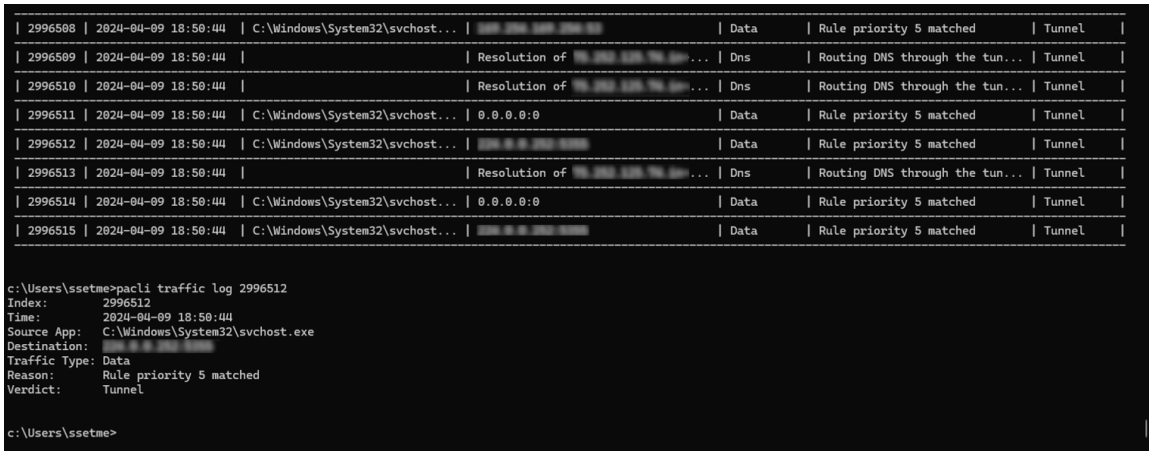
```
pacli traffic log
```



Pour afficher une entrée de journal individuelle, utilisez la commande suivante :

```
pacli traffic log <index>
```

Où **<index>** correspond au numéro d’index de l’entrée. Par exemple :



Vous pouvez également exporter le journal des connexions vers un fichier pour une analyse plus approfondie en utilisant :

```
pacli traffic log export <filename>
```

 ©2025 Palo Alto Networks, Inc.

Configurer les paramètres de l'application Prisma Access Agent pour l'accès à privilèges dynamique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Rôle : Administrateur de projet

Strata Cloud Manager fournit les configurations par défaut de l'application Prisma Access Agent qui s'appliquent à tous les groupes d'utilisateurs dans tous les projets. Vous pouvez ajouter une configuration de l'application pour personnaliser la façon dont vos utilisateurs finaux d'un projet interagissent avec l'application Prisma Access Agent.

STEP 1 | Connectez-vous à Strata Cloud Manager en tant qu'administrateur du projet.

STEP 2 | Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)** et développez la Configuration Scope (Portée de configuration) pour afficher les **Snippets (Extraits)**.

STEP 3 | Sélectionnez l'extrait que l'administrateur du super utilisateur vous a attribué.

Vous pouvez également afficher les extraits qui ne vous sont pas attribués, mais vous ne pouvez pas interagir avec eux, par exemple pour modifier la configuration.

STEP 4 | Sélectionnez **Objects (Objets)** > **Dynamic Privilege Access (Accès à privilèges dynamique)** pour ouvrir les paramètres d'accès à privilèges dynamique.

STEP 5 | Sélectionnez l'onglet **Agent Settings (Paramètres de l'agent)**.

STEP 6 | Strata Cloud Manager vous fournit les paramètres d'agent par défaut. Si vous ne souhaitez pas utiliser les paramètres par défaut, cliquez sur **Add Agent Settings (Ajouter les paramètres de l'agent)**.

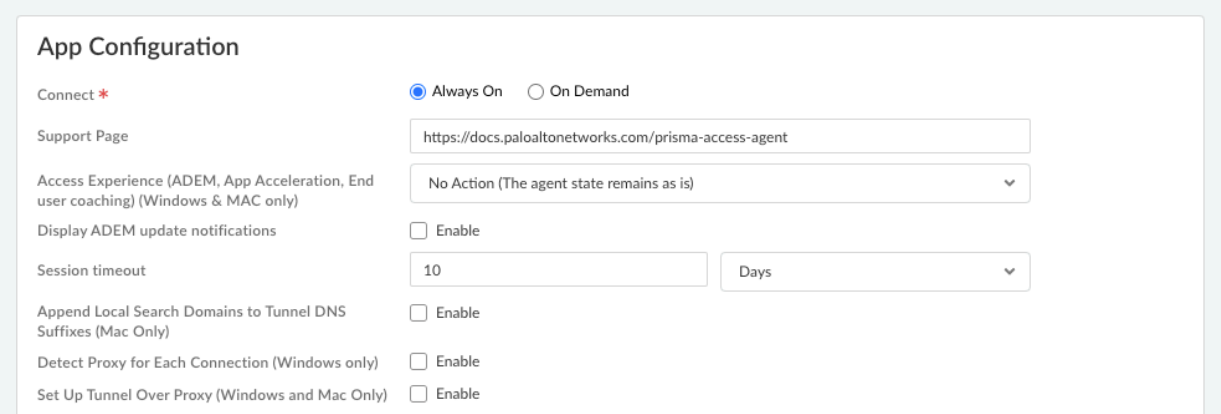
Pour modifier les paramètres d'un agent, sélectionnez le nom d'un agent dans le tableau.

©2025 Palo Alto Networks, Inc.

STEP 7 | Créez une règle de configuration d'appli. La règle de configuration associe un ou plusieurs projets à certains paramètres spécifiques à ces projets.

1. Donnez un **Name (Nom)** à la règle.
2. Spécifiez les **Match Criteria (Critères de correspondance)** en ajoutant des **Projects (Projets)**. Les utilisateurs et groupes qui correspondent au **Project (Projet)** recevront les paramètres de l'application lorsqu'ils se connecteront au projet à l'aide de l'application Prisma Access Agent.
   - Pour déployer la configuration sur tous les utilisateurs, définissez **Projects (Projets)** sur **Any (N'importe lequel)**.
   - Pour déployer la configuration auprès des utilisateurs qui se connectent à des projets spécifiques, définissez **Projects (Projets)** sur **Add Projects (Ajouter des projets)** et sélectionnez-les dans la liste des projets.

STEP 8 | Configurez les paramètres d'appli de Prisma Access Agent.



- **Connect (Connecter)** : spécifiez comment Prisma Access Agent se connecte à Prisma Access. Ce paramètre est obligatoire.
  - Sélectionnez **Always on (Toujours actif)** pour établir automatiquement une connexion à Prisma Access Agent chaque fois que l'utilisateur se connecte à un terminal.
  - Sélectionnez **On demand (Sur demande)** pour se connecter à Prisma Access Agent uniquement lorsque l'utilisateur se connecte à Prisma Access Agent en cliquant sur le bouton de verrouillage.
- **Support Page (Page d'assistance)** : saisissez le site web auquel les utilisateurs peuvent accéder pour obtenir de l'aide lorsqu'ils cliquent sur **Support Resources (Ressources d'assistance)** dans Prisma Access Agent.

  La page d'assistance par défaut est le site web de la documentation de Prisma Access Agent.
- **Access Experience (ADEM, App Acceleration, End user coaching) (Windows & MAC only) (Expérience d'accès (ADEM, accélération d'applis, coaching de l'utilisateur final) (Windows et MAC uniquement))**: spécifiez s'il faut installer l'agent de terminal Autonomous DEM (ADEM) lors de l'installation de l'appli Prisma Access Agent et autoriser les utilisateurs finaux à activer ou désactiver les tests d'expérience utilisateur à partir de l'appli.
  - **Installer l'agent**

 ©2025 Palo Alto Networks, Inc.

- **Désinstaller l'agent**
- **No action (The agent state remains as is) (Aucune action (l'état de l'agent reste tel quel))** (Il s'agit de la valeur par défaut)

Pour plus d'informations sur la prise en main d'ADEM sur Cloud Managed Prisma Access, consultez Get Started with Autonomous DEM (Premiers pas avec Autonomous DEM).

- **Display ADEM update notifications (Afficher les notifications de mise à jour de l'ADEM)** : **Enable (Activer)** ce paramètre pour afficher les notifications de l'ADEM lorsqu'une mise à jour est disponible sur le terminal.
- **Session timeout (Délai d'expiration de la session)** : les sessions utilisateur de Prisma Access Agent sont créées lorsqu'un utilisateur se connecte à la passerelle (emplacement) Prisma Access et s'authentifie avec succès. La session est ensuite attribuée à une passerelle spécifique qui détermine le trafic à mettre en tunnel en fonction des règles définies du tunnel fractionné. La version minimale du plan de données pour Prisma Access doit être la 11.2.

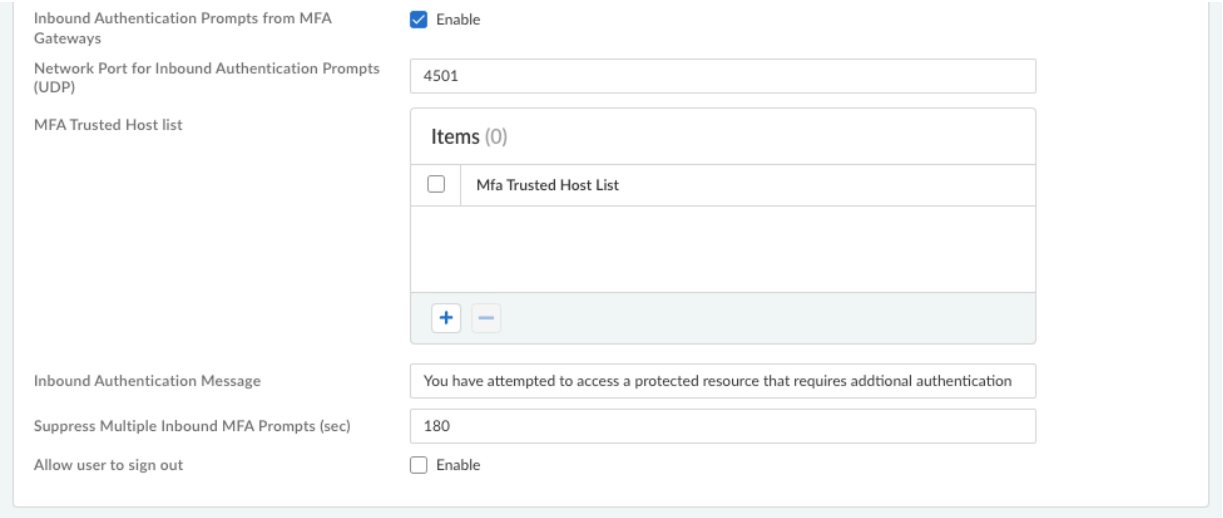
  Spécifiez la durée qui doit s'écouler avant que la session n'expire en raison d'une inactivité. Ce paramètre est obligatoire.

  *Si vous utilisez le plan de données Nebula (10.2) dans Prisma Access, la valeur du **Session timeout (Délai d'expiration de la session)** n'est pas configurable et est définie par défaut sur 7 jours.*
- **Append Local Search Domains to Tunnel DNS Suffixes (Mac only) (Ajouter des domaines de recherche locaux aux suffixes DNS de tunnel (Mac uniquement))** : **Enable (Activer)** ce paramètre pour ajouter des domaines de recherche DNS de tunnel aux domaines de recherche DNS locaux sur les terminaux macOS. L'ajout de domaines de recherche de tunnel aux domaines de recherche DNS locaux d'un terminal autorise les utilisateurs à accéder rapidement aux sites web et aux serveurs d'entreprise locaux et distants qu'ils visitent fréquemment sans saisir l'adresse complète.
- **Detect Proxy for Each Connection (Windows only) (Détecter le proxy pour chaque connexion (Windows uniquement))** : **Enable (Activer)** ce paramètre permet de détecter automatiquement le proxy à chaque connexion. Désactivez ce paramètre si vous souhaitez détecter automatiquement le proxy pour la connexion à la passerelle et l'utiliser pour les connexions ultérieures à Prisma Access.
- **Set Up Tunnel Over Proxy (Windows and Mac Only) (Configurer le tunnel sur le proxy (Windows et Mac uniquement))** : **Enable (Activer)** ce paramètre pour configurer le comportement du trafic réseau en fonction de l'utilisation du proxy Prisma Access Agent. Sélectionnez **Enable (Activer)** pour exiger que Prisma Access Agent utilise des proxys. Désactivez ce paramètre si vous souhaitez que Prisma Access Agent contourne les proxys. En fonction de l'utilisation des proxys par Prisma Access Agent, du système d'exploitation des terminaux et du type de tunnel, le trafic réseau fonctionnera différemment.

  Si vous désactivez cette option, Prisma Access Agent contournera les proxys. Tout le trafic HTTP ou HTTPS correspondant aux règles de fichier proxy ou PAC doit traverser le tunnel de Prisma Access Agent avant d'atteindre la destination prévue. En contournant les proxys,

 ©2025 Palo Alto Networks, Inc.

vous pouvez empêcher les utilisateurs de configurer un proxy personnel pour accéder aux ressources web sans passer par le tunnel pour inspection et application des politiques.



- **Optimized MTU (MTU optimisé)** : l'unité de transmission maximale (MTU) est la plus grande taille de paquet pouvant être envoyée dans un paquet au cours d'une transmission. **Enable (Activer)** cette option permet de déterminer automatiquement la meilleure MTU à utiliser pour les transmissions de paquets.

  Les connexions à Prisma Access Agent peuvent passer par plusieurs ISP et sauts de réseau avec des valeurs de MTU inférieures aux 1 500 octets standard. Lorsque la valeur de MTU de l'agent statique est inférieure à celle qui est proposée par un ISP, une fragmentation excessive et une surcharge supplémentaire se produisent, entraînant une baisse du débit. Les paquets abandonnés dans le chemin d'accès au réseau de l'ISP déclenchent également des retransmissions qui contribuent aux performances sous-optimales.

  L'activation de l'option **Optimized MTU (MTU optimisée)** peut vous aider à éviter une détermination et une configuration manuelles fastidieuses de la valeur optimale de la MTU, et à empêcher les utilisateurs d'avoir des performances médiocres qui affectent leur productivité.

  L'option **Optimized MTU (MTU optimisée)** est activée par défaut. Si vous la désactivez, vous pouvez configurer la MTU manuellement. La plage de la **Configurable MTU (bytes) (MTU configurable (octets))** est comprise entre 256 et 1 420 octets. La valeur par défaut est 1400 octets.
- **Inbound Authentication Prompts from MFA Gateways (Invites d'authentification entrantes à partir de passerelles MFA)** : pour prendre en charge l'authentification multifacteur (MFA), un terminal Prisma Access Agent doit recevoir et accepter les invites UDP entrantes de la passerelle. **Enable (Activer)** ce paramètre autorise un terminal Prisma Access Agent de recevoir et d'accepter les invites UDP. Ce paramètre est activé par défaut. Désactivez ce paramètre pour bloquer les invites UDP de la passerelle.
- **Network Port for Inbound Authentication Prompts (UDP) (Port réseau pour les invites d'authentification entrantes (UDP))** : spécifie le numéro de port qu'un terminal Prisma Access Agent utilise pour recevoir les invites d'authentification entrantes des passerelles MFA. Le port par défaut est 4501. Pour changer de port, indiquez un chiffre entre 1 et 65535.

 ©2025 Palo Alto Networks, Inc.

- **MFA Trusted Host list (Liste des hôtes fiables MFA)** : **Add (Ajouter)** les hôtes des pare-feu ou des passerelles d’authentification qu’un terminal Prisma Access Agent peut approuver pour l’authentification multifacteur. Lorsqu’un terminal reçoit un message UDP sur le port réseau spécifié, le Prisma Access Agent affiche un message d’authentification uniquement si l’invite UDP provient d’une passerelle de confiance.
- **Inbound Authentication Messages (Messages d’authentification entrants)** : personnalisez un message de notification à afficher lorsque les utilisateurs tentent d’accéder à une ressource qui nécessite une authentification supplémentaire.

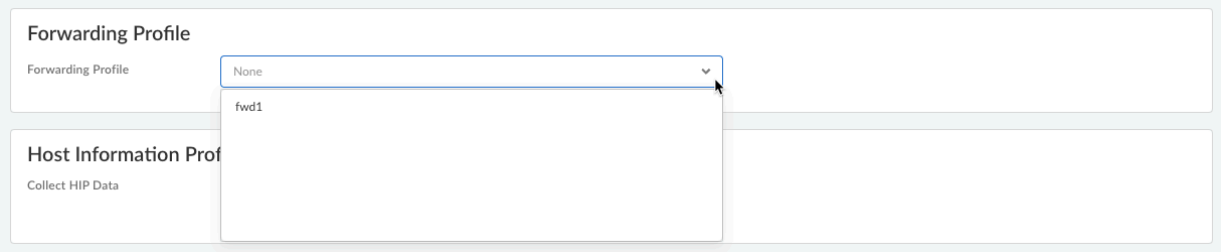
  Lorsque les utilisateurs tentent d’accéder à une ressource qui nécessite une authentification supplémentaire, Prisma Access Agent reçoit un paquet UDP contenant l’invite d’authentification entrante et affiche ce message. Le paquet UDP contient également l’URL vers la page du Portail d’authentification que vous avez précisée lors de la configuration de l’authentification multifacteur. Prisma Access Agent ajoute automatiquement l’URL au message.

  Par exemple :

  ```
  Vous avez tenté d’accéder à une ressource protégée qui
   nécessite une authentification supplémentaire. Procédez à
   l’authentification sur
  ```

  Le message peut comporter 255 caractères au maximum.
- **Suppress Multiple Inbound MFA Prompts (sec) (Supprimer plusieurs invites MFA entrantes (s))** : spécifiez le nombre de secondes à attendre avant que Prisma Access Agent puisse supprimer plusieurs invites UDP entrantes. La valeur par défaut est 180 secondes.
- **Allow user to sign out (Autoriser l’utilisateur à se déconnecter)** : **Enable (Activer)** ce paramètre pour autoriser vos utilisateurs à se déconnecter de Prisma Access Agent. Ce paramètre est désactivé par défaut.

STEP 9 | Sélectionnez un **Forwarding Profile (Profil de transfert)** que vous avez configuré précédemment pour gérer la circulation du trafic entre l’agent et Prisma Access.



STEP 10 | Configurez les paramètres DNS pour l’accès à privilèges dynamique.

STEP 11 | Configurer les paramètres du profil d’informations sur l’hôte

STEP 12 | Lorsque vous avez terminé de configurer les paramètres de l’application Prisma Access Agent, cliquez sur **Save (Enregistrer)**.

 ©2025 Palo Alto Networks, Inc.

Configurer les paramètres DNS pour l'accès à privilèges dynamique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Rôle : Administrateur de projet

Vous pouvez configurer les serveurs DNS pour permettre à Prisma Access de résoudre vos domaines internes.

STEP 1 | Depuis Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)** et développez la Configuration Scope (Portée de configuration) pour afficher les **Snippets (Extraits)**.

STEP 2 | Sélectionnez l'extrait que l'administrateur du super utilisateur vous a attribué.

STEP 3 | Sélectionnez **Objects (Objets)** > **Dynamic Privilege Access (Accès à privilèges dynamique)** pour ouvrir les paramètres d'accès à privilèges dynamique.

STEP 4 | Sélectionnez l'onglet **Agent Settings (Paramètres de l'agent)**.

STEP 5 | Cliquez sur **Add Agent Settings (Ajouter les paramètres de l'agent)** pour ajouter des paramètres ou sélectionnez un paramètre existant dans le tableau Agent Setting (Paramètres de l 'agent).

STEP 6 | Entrez le serveur **Primary DNS (DNS principal)** et le serveur **Secondary DNS (DNS secondaire)** que Prisma Access doit utiliser pour résoudre les noms de domaine internes.

STEP 7 | Vous pouvez ajouter une **Client DNS Suffix List (Liste de suffixes DNS client)** pour spécifier le suffixe que le client doit utiliser localement lorsqu'un nom d'hôte non qualifié est saisi et qu'il ne peut pas résoudre, par exemple, **`acme.local`**.

Ne saisissez pas de caractère générique (*) avant le suffixe de domaine (par exemple, acme.com). Vous pouvez ajouter plusieurs suffixes.

 ©2025 Palo Alto Networks, Inc.

Configurer les paramètres de collecte de données HIP pour l'accès à privilèges dynamique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Rôle : Administrateur de projet

Prisma Access Agent collecte des informations sur l'hôte sur lequel il s'exécute et soumet ces informations sur l'hôte à l'emplacement Prisma Access (passerelle) dès que la connexion est établie. La passerelle fait correspondre ces informations brutes sur l'hôte soumises par Prisma Access Agent à tous les objets du profil d'informations sur l'hôte (HIP) et les profils HIP que vous avez définis. Si elle trouve une correspondance, elle génère une entrée dans le journal des correspondances HIP. En outre, si elle trouve une correspondance de profil HIP dans une règle de politique, elle met applique la politique de sécurité correspondante.

Dans l'onglet **HIP Notifications (Notifications HIP)** de la page Modifier les paramètres globaux de l'agent, vous pouvez créer des notifications HIP, créer et gérer des objets HIP, ainsi que créer et gérer des profils HIP qui s'appliquent à Prisma Access Agent sur tous les terminaux.

Ici, vous pouvez définir les données HIP personnalisées que vous souhaitez faire collecter ou exclure par Prisma Access Agent. Lorsque cette option est activée, Prisma Access Agent collecte des données à partir des périphériques exécutant les systèmes d'exploitation macOS ou Windows.

Par exemple, une vérification personnalisée pourrait vous permettre de savoir si une certaine application est installée ou en cours d'exécution sur un terminal. Les données que vous définissez pour être collectées dans une vérification personnalisée sont incluses dans les données d'informations brutes de l'hôte collectées par Prisma Access Agent puis soumises à Prisma Access lors de la connexion de Prisma Access Agent.

STEP 1 | Depuis Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)** et développez la Configuration Scope (Portée de configuration) pour afficher les **Snippets (Extraits)**.

STEP 2 | Sélectionnez l'extrait que l'administrateur du super utilisateur vous a attribué.

STEP 3 | Sélectionnez **Objects (Objets)** > **Dynamic Privilege Access (Accès à privilèges dynamique)** pour ouvrir les paramètres d'accès à privilèges dynamique.

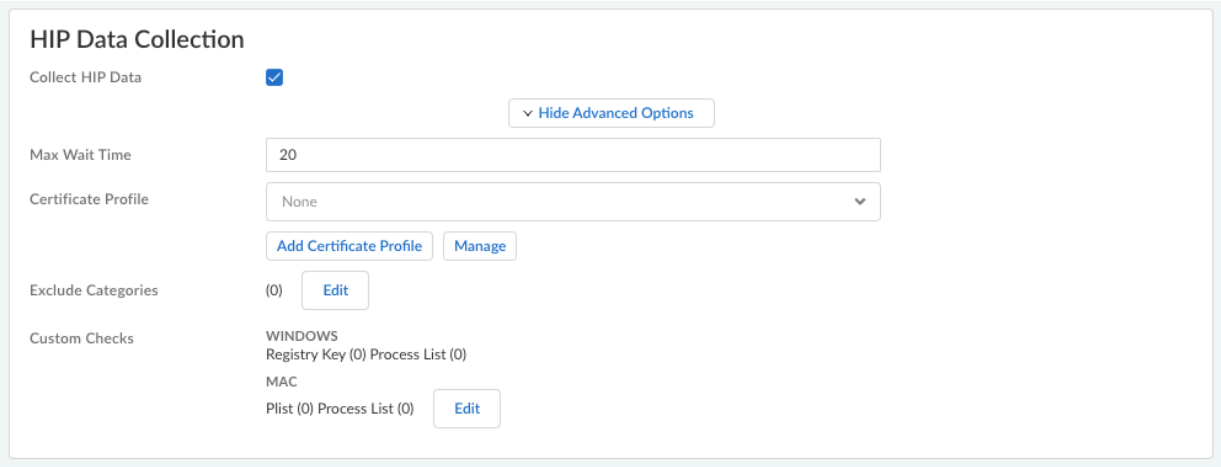
STEP 4 | Sélectionnez l'onglet **Agent Settings (Paramètres de l'agent)**.

STEP 5 | Sélectionnez **Add Agent Settings (Ajouter les paramètres de l'agent)** ou bien une configuration existante dans le tableau Agent Setting (Paramètres de l'agent).

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Dans la section Profil d'informations sur l'hôte (HIP), sélectionnez **Collect HIP Data (Collecter les données HIP)** pour activer la collecte de données HIP sur les terminaux connectés à l'aide d'un projet.

STEP 7 | Sélectionnez **Show Advanced Options (Afficher les options avancées)**.



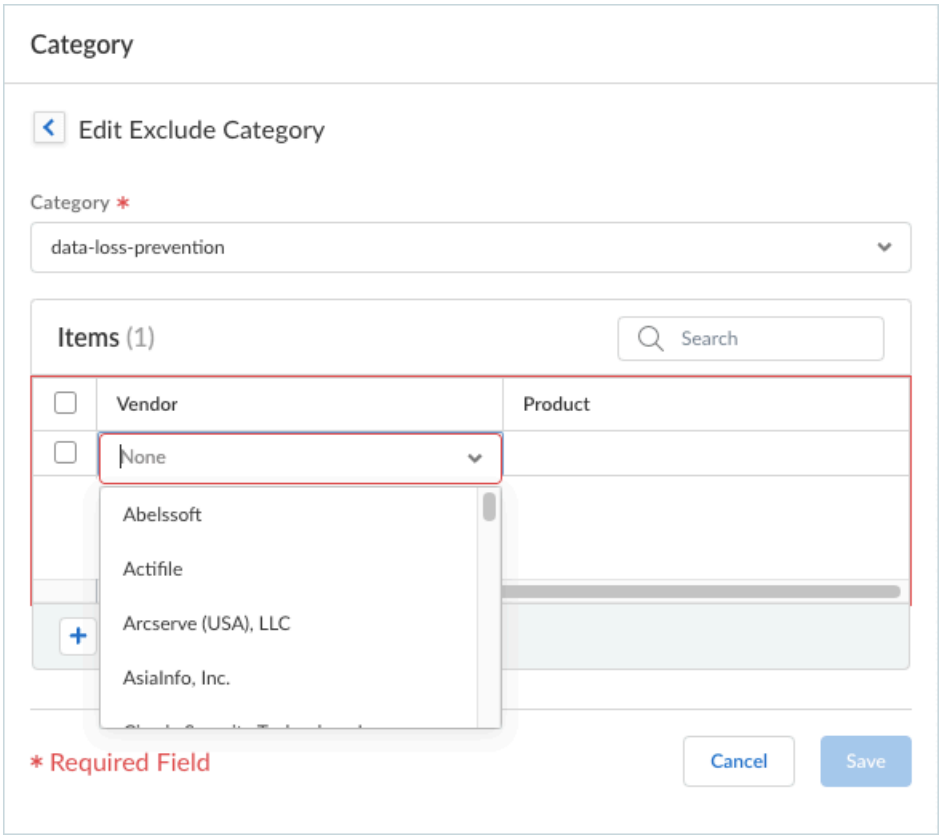
STEP 8 | Spécifiez le **Max Wait Time (Délai d'attente maxi** (en secondes) pendant lequel Prisma Access Agent doit rechercher des données HIP avant de soumettre les données disponibles. La plage est de 10 à 60 secondes, avec une valeur par défaut de 20 secondes.

STEP 9 | **Edit (Modifiez)** les catégories d'exclusion pour exclure des catégories et/ou des fournisseurs, des applications ou des versions spécifiques dans une catégorie de la collecte de données HIP.

Sélectionnez une **Category (Catégorie)** (comme la prévention des pertes de données) à exclure de la collecte HIP. Après avoir sélectionné une catégorie, vous pouvez **Add (Ajouter)** un **Vendor (Fournisseur)** particulier, puis vous pouvez **Add (Ajouter)** des **Products (Produits)** spécifiques provenant du fournisseur pour affiner l'exclusion au besoin. Vous pouvez ajouter

 ©2025 Palo Alto Networks, Inc.

de multiples fournisseurs et produits à la liste d'exclusion. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres dans chaque boîte de dialogue.



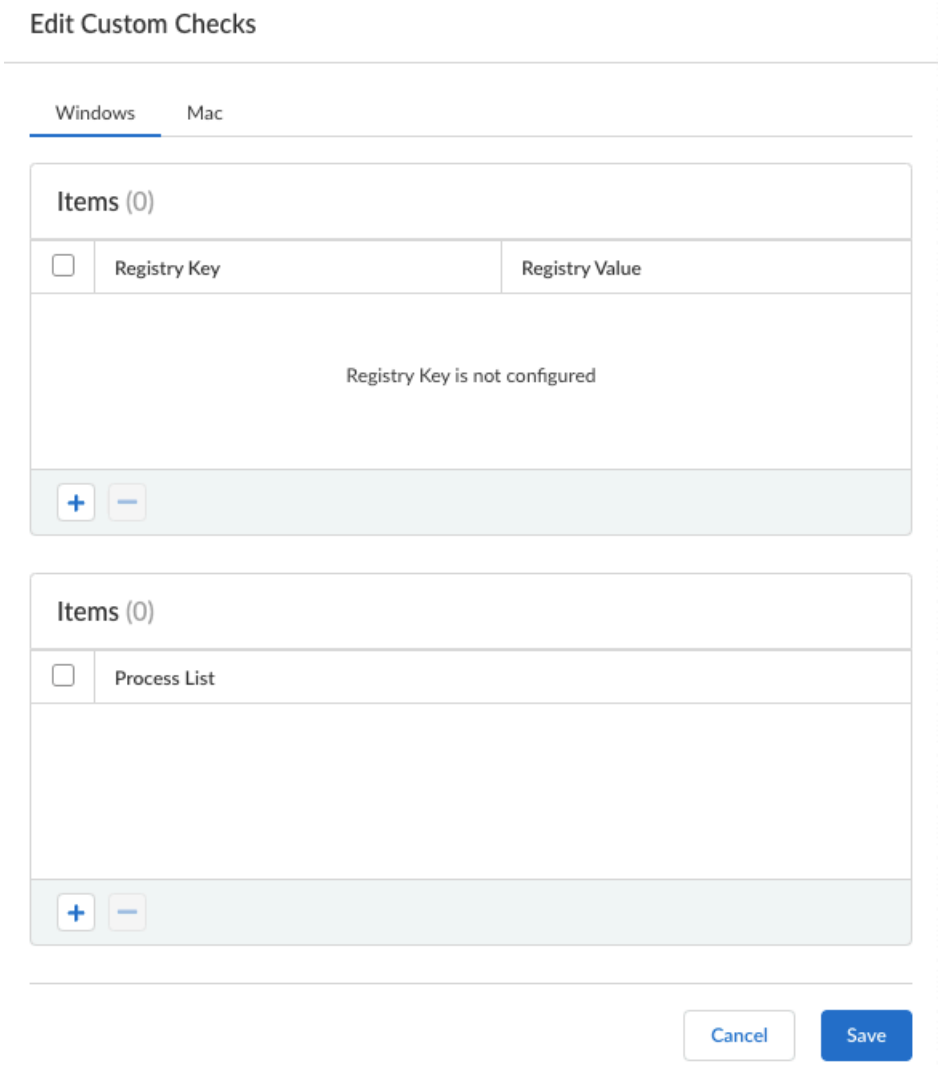
Si vous ne souhaitez pas exclure un fournisseur complet, vous pouvez exclure des correctifs spécifiques d'un fournisseur. Après avoir ajouté le fournisseur, vous pouvez spécifier le nom ou le numéro du correctif et éventuellement la date jusqu'à laquelle vous souhaitez exclure les mises à jour du correctif du rapport HIP en suivant le format suivant :

```
Exclure :[kb-article-id1 : MM/JJ/AAAA], [kb-article-id2 : MM/JJ/
AAAA]
```

Où **<kb-article-id>** est le nom ou le numéro de l'attribut (par exemple**<kb-article-id> 2267602</kb-article-id>**) et la **MM/JJ/AAAA** spécifie la date jusqu'à laquelle le correctif est exclu du rapport HIP. Si vous ne fixez pas de date, le correctif sera exclu du rapport HIP indéfiniment. Si vous choisissez de définir une date, le correctif sera exclu jusqu'à la date spécifiée.

 ©2025 Palo Alto Networks, Inc.

STEP 10 | **Edit (Modifiez)** les vérifications personnalisées pour définir toutes les données personnalisées que vous souhaitez collecter auprès des hôtes exécutant cette configuration.



Par exemple, si vous disposez d'applications non incluses dans les listes de fournisseurs et/ou de produits, qui sont requises pour la création d'objets HIP, vous pouvez créer une vérification personnalisée qui vous permet de déterminer si l'application est installée (doit avoir une clé de registre Windows ou Plist Mac correspondante) ou est présentement en cours d'exécution (a un processus en cours d'exécution correspondant) :

- **Windows** : **Add (Ajouter)** une vérification d’une clé de registre et/ou d’une valeur de registre particulière. Pour restreindre la collecte de données à une valeur de registre spécifique, cliquez sur **Add (Ajouter)**, puis définissez des valeurs de registre spécifiques.
- **Mac** : **Add (Ajouter)** une vérification d’une clé **Plist** ou d’une valeur de **Key (Clé)** particulière. Pour restreindre la collecte de données à des valeurs clés particulières, cliquez sur **Add (Ajouter)** pour ajouter les valeurs des clés. Cliquez sur OK pour enregistrer les paramètres.
- **Process List (Liste des processus)** : **Add (Ajouter)** les processus que vous souhaitez vérifier sur les terminaux de l'utilisateur pour voir s'ils sont en cours d'exécution. Par exemple, pour déterminer si une application est en cours d'exécution, ajoutez le nom du fichier exécutable

 ©2025 Palo Alto Networks, Inc.

à la liste des processus. Vous pouvez ajouter une liste de processus dans l'onglet **Windows** ou **Mac**.

Cliquez sur **Save (Enregistrer)** quand vous aurez terminé pour enregistrer les paramètres de vérification personnalisée.

STEP 11 | Une fois que vous avez terminé de configurer les paramètres Prisma Access Agent spécifiques au projet, cliquez sur **Save (Enregistrer)** pour enregistrer la configuration.

 ©2025 Palo Alto Networks, Inc.

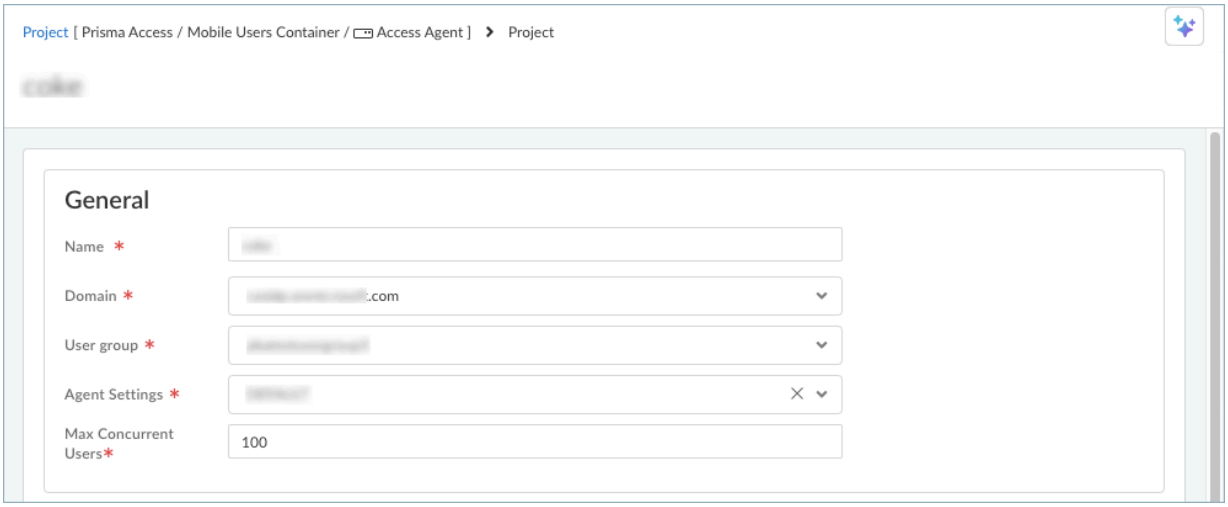
Créer un projet

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access ❑ Version minimale requise de Prisma Access : 5.1 ❑ Rôle : Super utilisateur

Ajoutez des projets auxquels des utilisateurs doivent pouvoir accéder à l'aide de Prisma Access Agent. Seul un admin de projet peut créer et gérer les définitions de projet.

STEP 1 | Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)**.

STEP 2 | Définissez l'étendue sur l'extrait de projet que vous avez créé, puis accédez à **Objects (Objets)** > **Dynamic Privilege Access (Accès à privilèges dynamiques)** > **Projects (Projets)** > **Add Project (Ajouter un projet)**.



1. Donnez un nom au projet dans **Name (Nom)**.
2. Sélectionnez le **Domain (Domaine)** que vous avez ajouté dans Cloud Identity Engine ainsi que le **User Group (Groupe d'utilisateurs)** mappé au répertoire.
3. Sélectionnez les **Agent Settings (Paramètres de l'agent)** que vous avez ajoutés précédemment ainsi que le **Max Concurrent Users (Nombre maximal d'utilisateurs simultanés)** pour le projet.
4. Sélectionnez **Prisma Access Location Groups (Groupes d'emplacements Prisma Access)**. Les groupes d'emplacements qui s'affichent dans la liste dépendent des emplacements où vous avez ajouté les passerelles GlobalProtect.

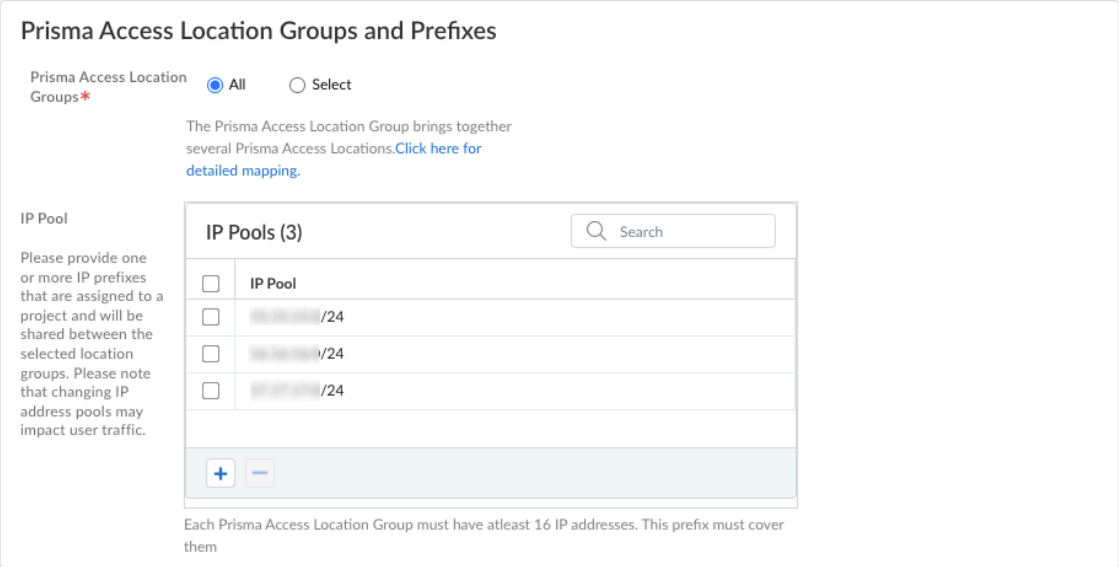
   Le projet que vous créez est associé à des pools d'adresses IP et à des groupes d'emplacements. Les utilisateurs acquerront les adresses IP en fonction du projet et de l'emplacement de calcul Prisma Access auxquels ils se connectent avec Prisma Access Agent. Un projet ne peut se connecter qu'à un emplacement du groupe d'emplacements

 ©2025 Palo Alto Networks, Inc.

associé au projet. Vous pouvez sélectionner **Click here for detailed mapping (Cliquez**

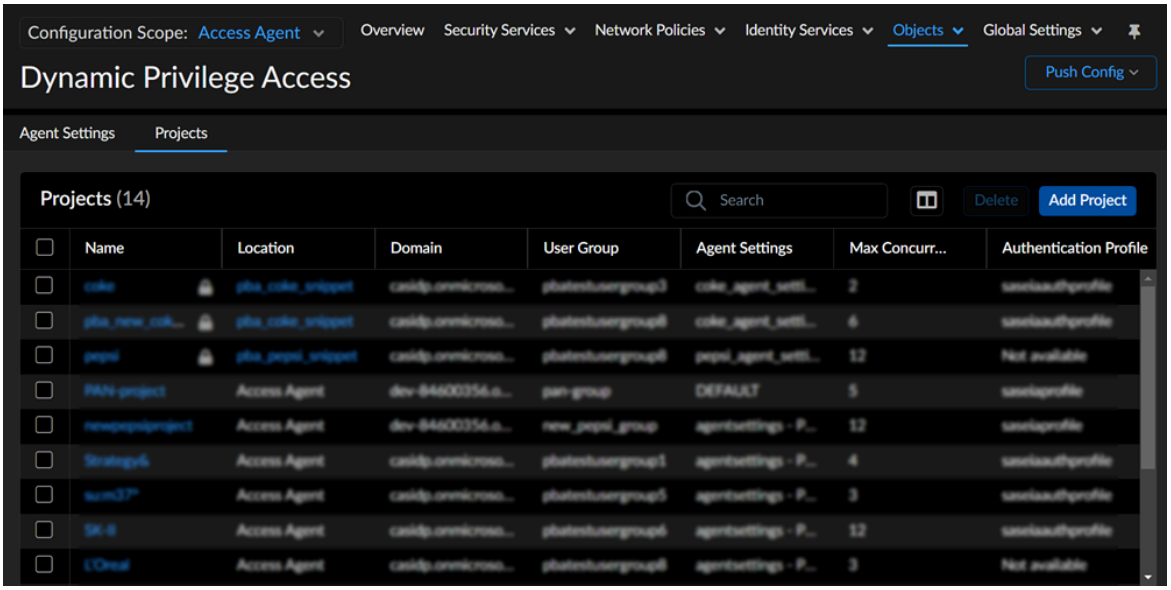
 ©2025 Palo Alto Networks, Inc.

ici pour un mappage détaillé) pour voir le mappage entre les groupes d'emplacements Prisma Access et les emplacements de calcul Prisma Access.



5. Ajoutez ou sélectionnez des **IP Pools (Pools d'adresses IP)** pour votre projet. Les préfixes IP sont attribués à votre projet et seront partagés entre les groupes d'emplacements Prisma Access que vous avez sélectionnés.

   Ces pools d'adresses IP de projet peuvent être résumés pour que le nombre de routes envoyées au réseau soit réduit.
6. Sélectionnez **Save (Enregistrer)** pour enregistrer les paramètres du projet.



 ©2025 Palo Alto Networks, Inc.

- *Lorsque vous sélectionnez un extrait de projet dans la portée de configuration, vous ne pouvez accéder qu’aux paramètres et aux détails liés à ce projet particulier.*
- *Lorsque vous vous connectez à Strata Cloud Manager en tant qu’admin de projet ou admin push de projet, vous ne pouvez afficher que les détails du projet auxquels vous avez accès. Si vous sélectionnez la portée de configuration d’un autre extrait de projet, vous ne pouvez pas accéder aux paramètres et aux détails d’un autre projet.*
- *Pour passer d’un projet à l’autre, vous devez vous reconnecter à Strata Cloud Manager en tant qu’un autre admin de projet ou admin push de projet push à l’aide des informations d’identification du projet concerné.*

STEP 3 | **Push (Appliquez)** vos changements.

Une fois qu’un projet a été créé dans Prisma Access, il peut s’écouler jusqu’à 15 minutes avant que l’utilisateur puisse s’authentifier sur ce projet à l’aide de Prisma Access Agent.

 ©2025 Palo Alto Networks, Inc.

Redirection du trafic pour l'accès à privilèges dynamique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access ❑ Version de Prisma Access minimale requise : 5.1 ❑ Rôle : Administrateur de projet

Utilisez la redirection du trafic pour transférer le trafic d'un projet vers une connexion aux services et des itinéraires spécifiques au projet.

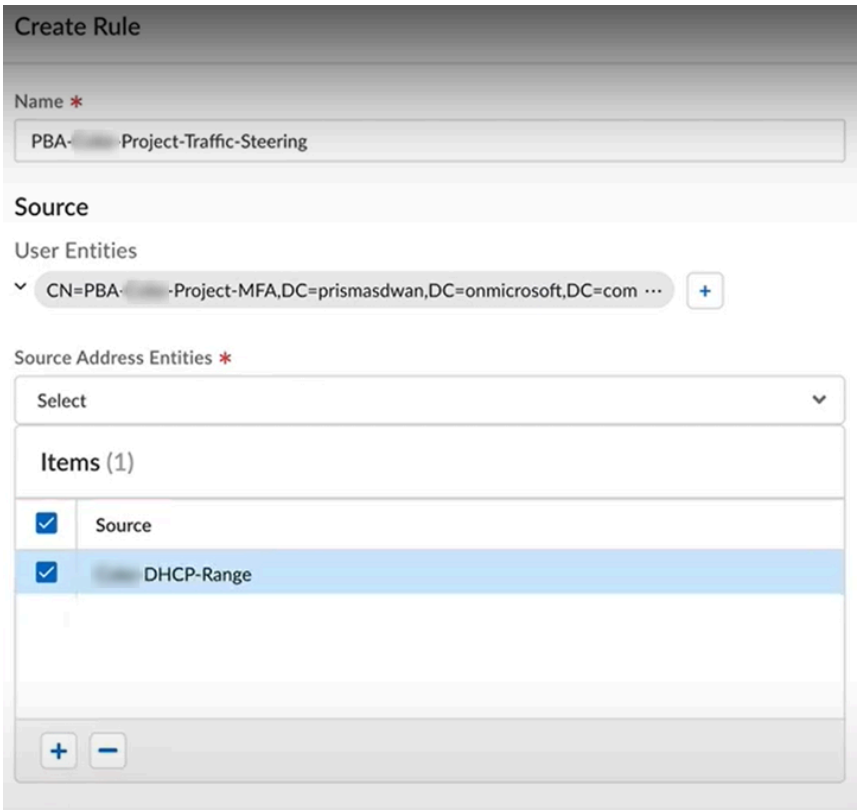
STEP 1 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connections (Connexions aux services)**.

STEP 2 | Ajoutez une connexion aux services.

STEP 3 | Modifiez les **Advanced Settings (Paramètres avancés)** pour acheminer le trafic.

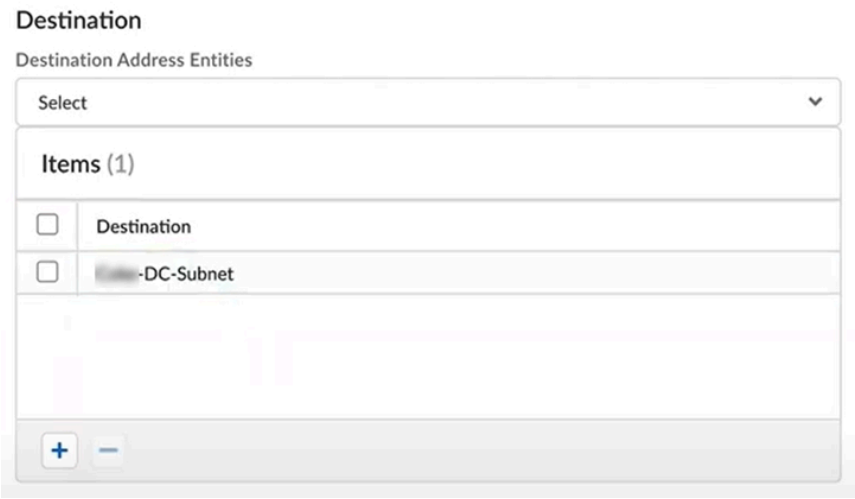
STEP 4 | **Add Rule (Ajoutez une règle)** sous **Traffic Steering (Redirection du trafic)** pour vos projets.

STEP 5 | Associez la **Source** avec les utilisateurs et ajoutez la plage DHCP du projet en tant que **Source Address Entities (Entités d'adresse source)**.

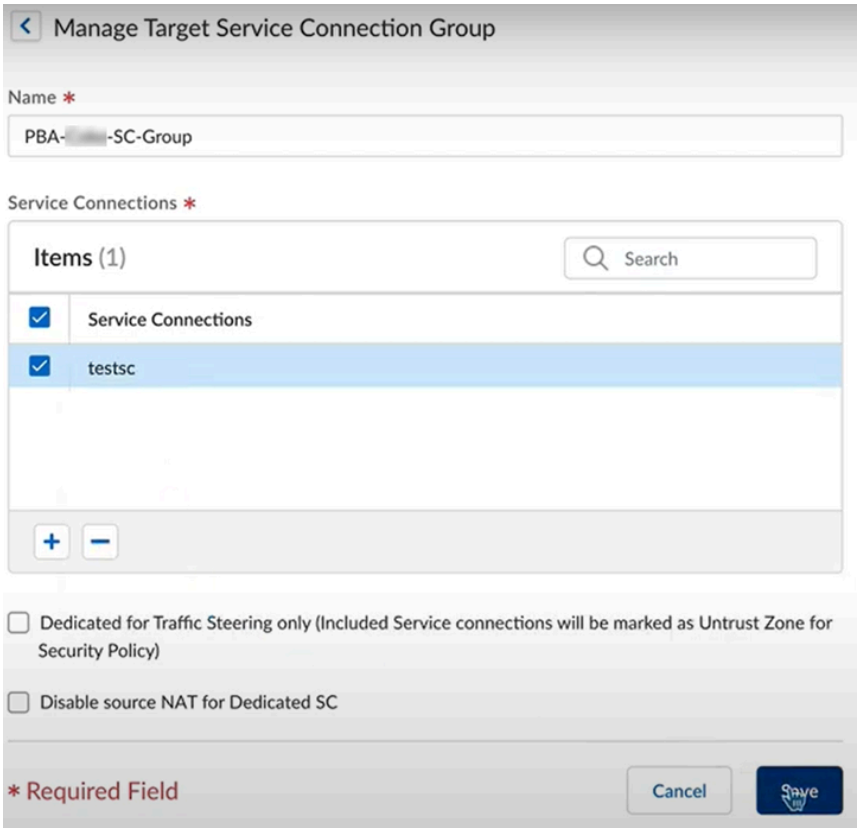


 ©2025 Palo Alto Networks, Inc.

STEP 6 | Associez les entités d'adresse de **Destination**.



STEP 7 | Sélectionnez les services et les actions.



STEP 8 | Enregistrez et appliquez les modifications.

 ©2025 Palo Alto Networks, Inc.

Configurer le Prisma Access Agent pour l'accès à privilèges dynamique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Rôle : Super utilisateur

Vos utilisateurs finaux utiliseront l'Prisma Access Agent pour accéder au réseau de votre organisation en fonction des projets clients auxquels vos utilisateurs sont assignés.

Après avoir configuré les paramètres de l'agent spécifiques au projet et créé les projets, vous pouvez configurer d'autres paramètres d'Prisma Access Agent tels que les déploiements par étapes et les paramètres globaux de l'agent.

Vous pouvez configurer les paramètres d'Prisma Access Agent suivants :

- Configurer les déploiements par étapes pour l'agent Prisma Access
- Configurer les paramètres globaux généraux des agents Prisma Access
- Configurer les notifications HIP pour l'agent Prisma Access

Configurer les déploiements par étapes pour le Prisma Access Agent

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (géré par Strata Cloud Manager)	❑ Prisma Access 5.1 version préférée ou innovation ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Rôle : Super utilisateur

©2025 Palo Alto Networks, Inc.

La fonctionnalité de déploiement de la mise à niveau de Prisma Access Agent permet aux administrateurs de mettre à niveau des groupes de périphériques dans un ordre spécifique. Grâce aux déploiements de mises à niveau, vous n’avez plus besoin de compter sur les logiciels de gestion des appareils mobiles (MDM), tels que Jamf Pro et Microsoft Intune pour mettre à niveau les agents Prisma Access.

Les déploiements de mise à niveau par étapes ne peuvent avoir lieu qu’après le déploiement initial ou l’installation de Prisma Access Agent sur les périphériques de vos utilisateurs finaux.

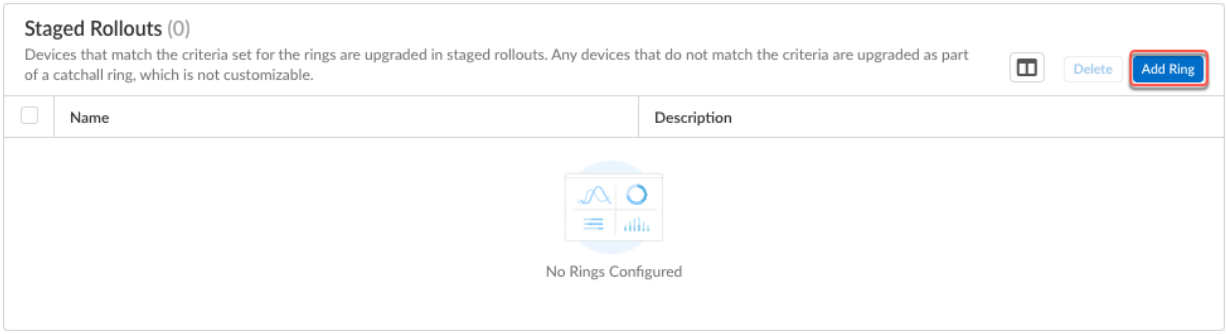
Pour préparer le déploiement des mises à niveau de Prisma Access Agent, vous pouvez configurer des anneaux de mise à niveau avec des critères de correspondance basés sur les utilisateurs, les groupes et les systèmes d’exploitation. Les périphériques qui correspondent aux critères sont mis à niveau dans l’ordre des anneaux de mise à niveau (Anneau 0 à Anneau 4, Anneau par défaut).

Vous pouvez éventuellement définir des anneaux de mise à niveau lors de l’intégration des utilisateurs mobiles à l’aide de la page de configuration de l’agent d’accès de Prisma Access Agent. Si vous choisissez de ne pas définir d’anneaux de mise à niveau lors de la configuration initiale de l’agent, tous les périphériques sont placés dans l’anneau par défaut. Vous pouvez revenir à la page de configuration de Prisma Access Agent ultérieurement pour définir les anneaux de mise à niveau et transmettre la configuration à Prisma Access. Ces modifications prendront effet lors du prochain déploiement par étapes, ou une fois que vous aurez arrêté et démarré un déploiement par étapes.

Pour configurer un anneau de mise à niveau :

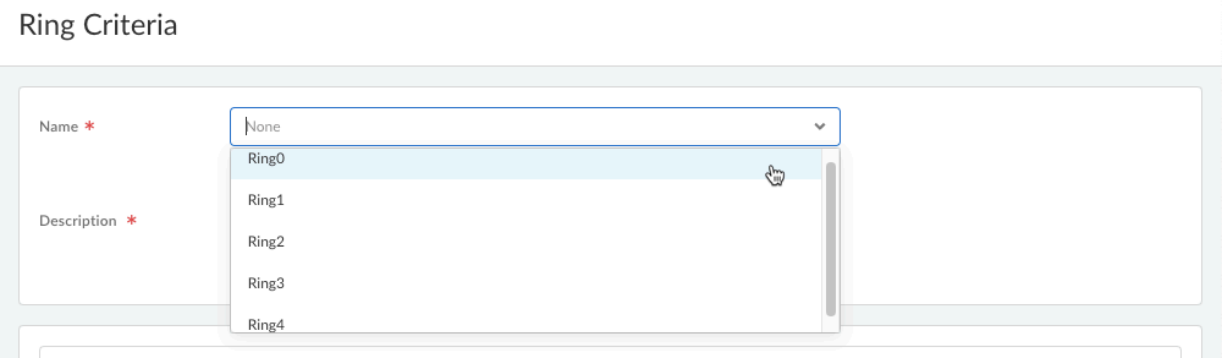
STEP 1 | Dans Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Access Agent (Agent d’accès)** > **Prisma Access Agent**.

STEP 2 | Dans la section **Staged Rollouts (Déploiements par étapes)**, cliquez sur **Add Ring (Ajouter un anneau)**.



 ©2025 Palo Alto Networks, Inc.

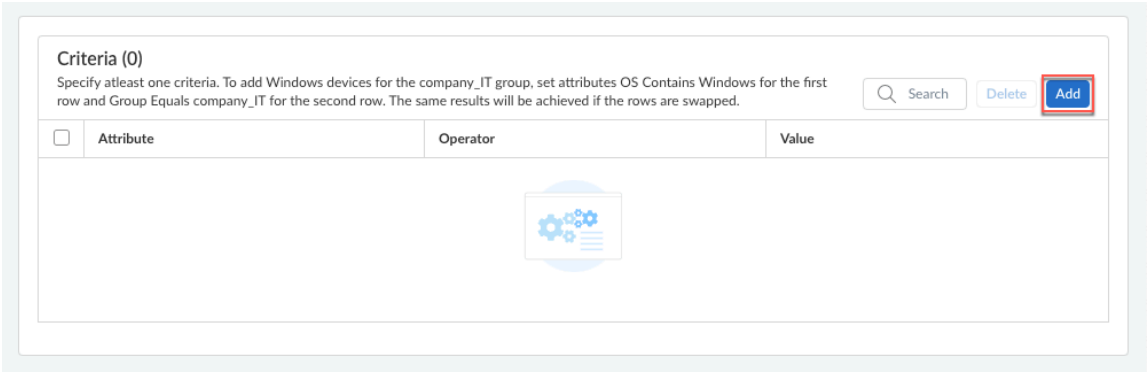
STEP 3 | Sélectionnez un **Name (Nom)** prédéfini pour l'anneau Vous pouvez choisir de **Ring0 (Anneau0)** à **Ring4 (Anneau4)**. Le premier anneau que vous allez ajouter est **Ring0 (Anneau0)**.



STEP 4 | Ajoutez une **Description** significative pour l'anneau.

STEP 5 | Spécifiez les critères de l'anneau en fonction des attributs **User (Utilisateur)**, **Groups (Groupes)** ou **Device OS (Système d'exploitation du périphérique)**.

1. Cliquez sur **Add (Ajouter)** pour ajouter un critère.



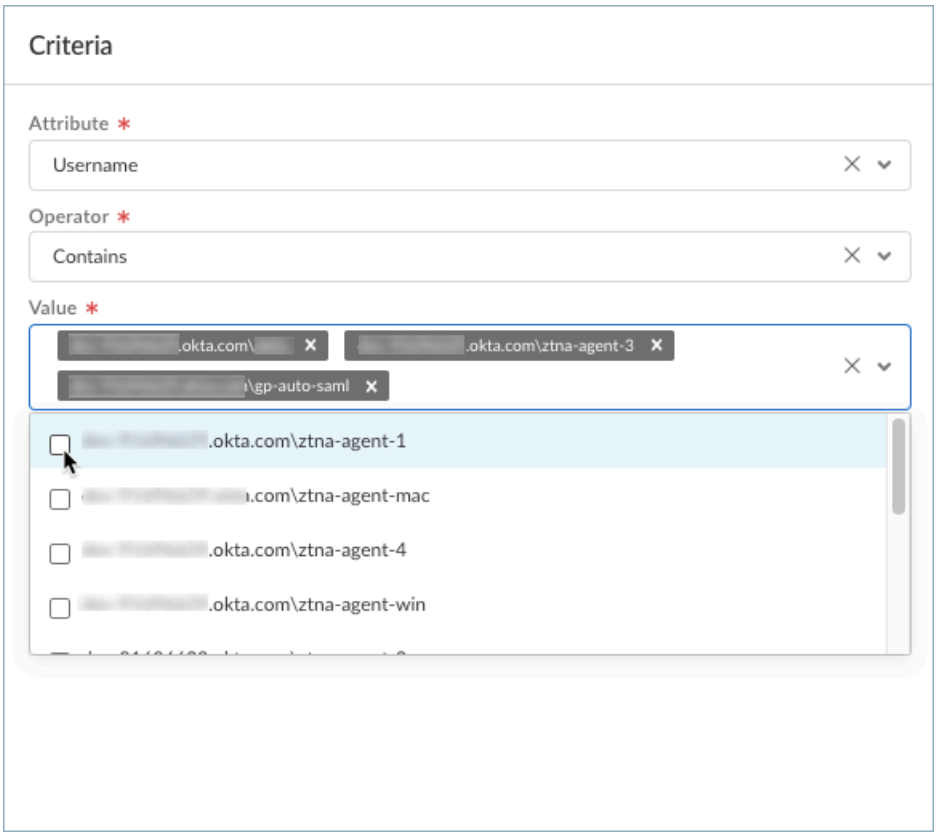
2. Pour chaque critère, sélectionnez un **Attribute (Attribut)**, un **Operator (Opérateur)**, une **Value (Valeur)**, puis cliquez sur **Add (Ajouter)**.

   Vous ne pouvez sélectionner qu'un seul attribut et un seul opérateur par critère. La valeur dépend de ce que vous avez sélectionné pour l'attribut et l'opérateur :

   - Pour l'attribut **Username (Nom d'utilisateur)** :
     - Si vous sélectionnez **Operator (Opérateur)** > **Contains (Contient)**, sélectionnez ou recherchez un nom d'utilisateur dans la liste **Value (Valeurs)**. Pour lancer une

 ©2025 Palo Alto Networks, Inc.

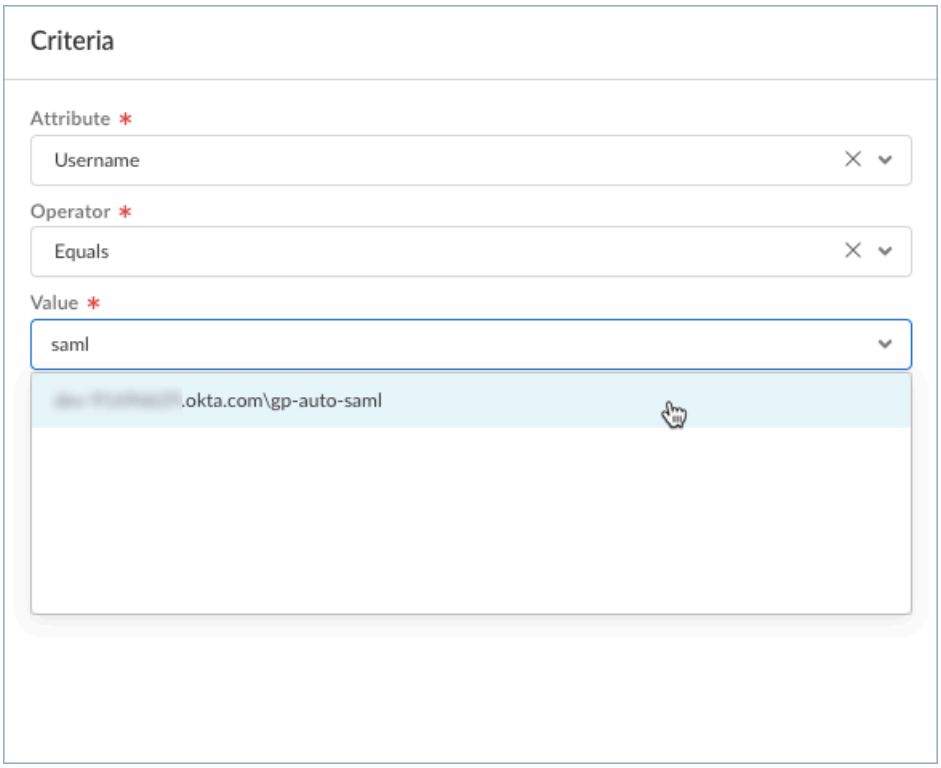
recherche, commencez à taper le nom d’utilisateur. Vous pouvez sélectionner un ou plusieurs noms d’utilisateurs dans la liste.



- Si vous sélectionnez **Operator (Opérateur)** > **Equals (Égal)**, sélectionnez ou recherchez un nom d’utilisateur dans la liste **Value (Valeurs)**. Pour lancer une

 ©2025 Palo Alto Networks, Inc.

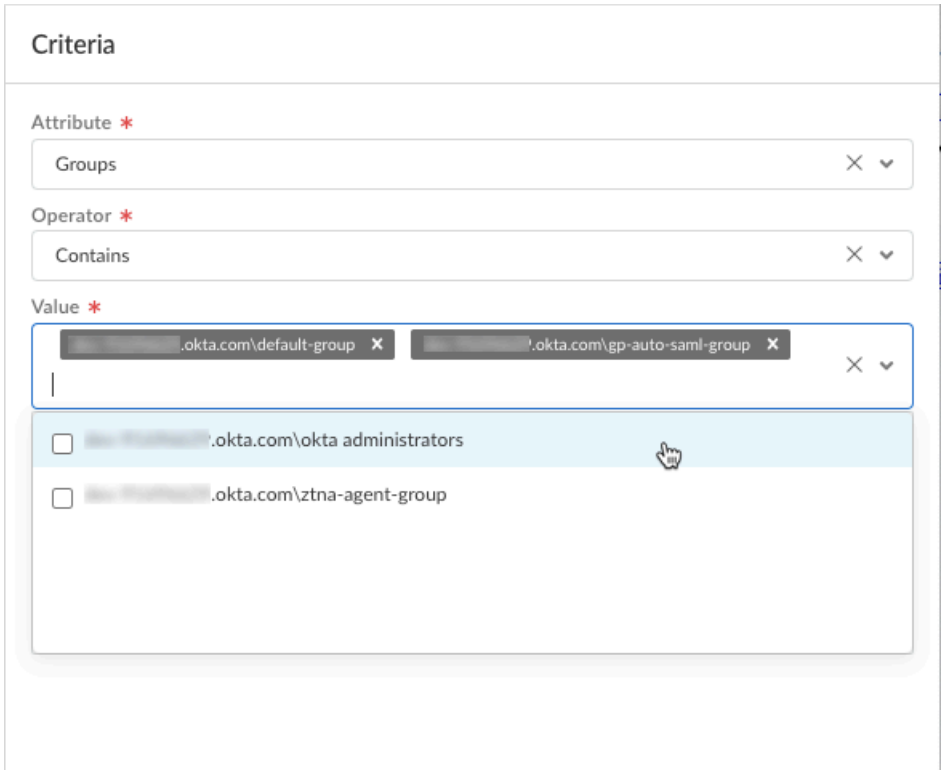
recherche, commencez à taper le nom d'utilisateur. Vous pouvez sélectionner un nom d'utilisateur dans la liste.



- Pour l'attribut **Group (Groupe)** :
  - Si vous sélectionnez **Operator (Opérateur)** > **Contains (Contient)**, sélectionnez ou recherchez un groupe dans la liste **Value (Valeurs)**. Pour lancer une recherche,

 ©2025 Palo Alto Networks, Inc.

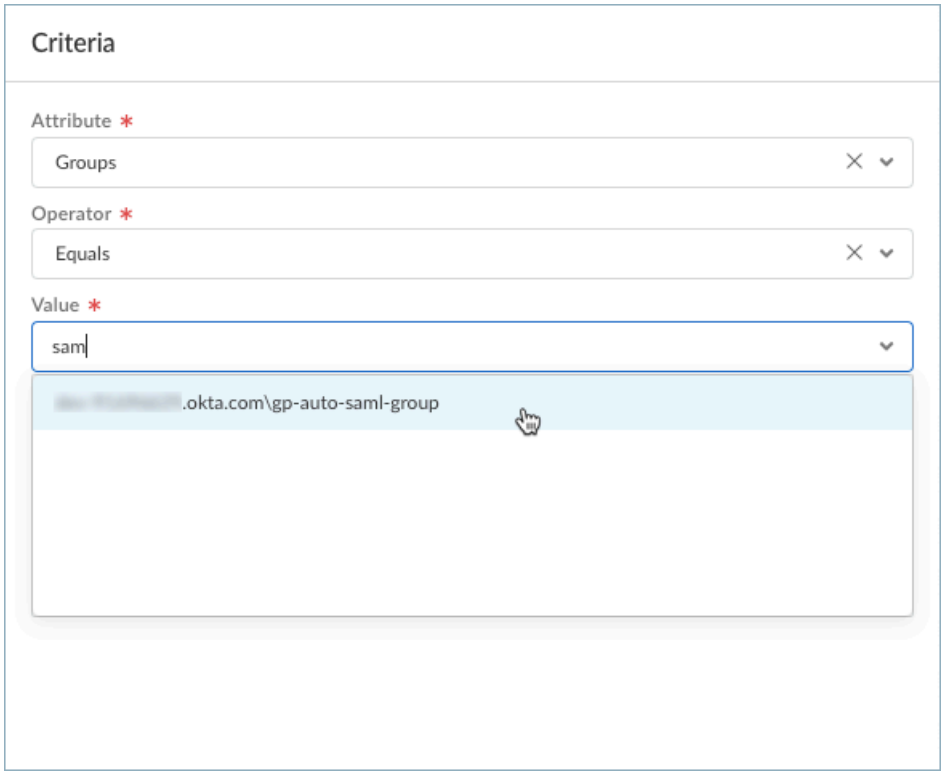
commencez à taper le nom du groupe. Vous pouvez sélectionner un ou plusieurs groupes dans la liste.



- Si vous sélectionnez **Operator (Opérateur)** > **Equals (Égal)**, sélectionnez ou recherchez un groupe dans la liste **Value (Valeurs)**. Pour lancer une recherche,

 ©2025 Palo Alto Networks, Inc.

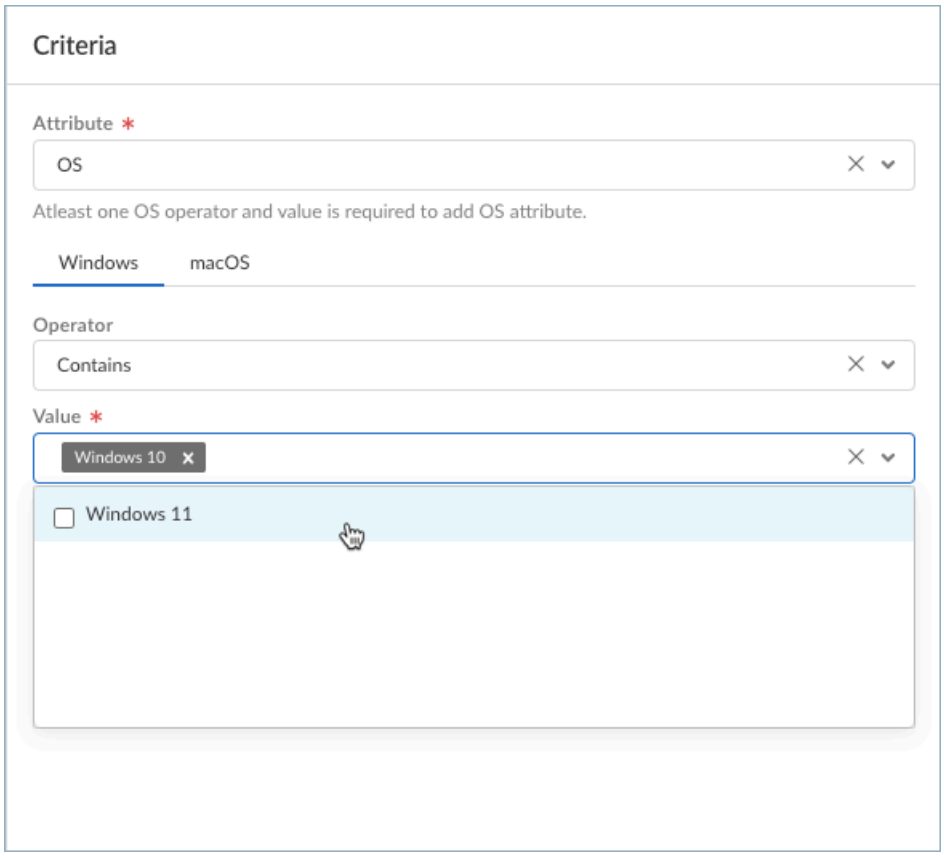
commencez à taper le nom du groupe. Vous pouvez sélectionner un groupe dans la liste.



- Pour l'attribut **OS (Système d'exploitation)**, sélectionnez un type de système d'exploitation (**Windows** ou **macOS**). Ensuite :
  - Si vous sélectionnez **Operator (Opérateur)** > **Contains (Contient)**, recherchez ou sélectionnez une ou plusieurs versions du système d'exploitation dans la liste **Value (Valeurs)**. Pour lancer une recherche, commencez à taper le système d'exploitation

 ©2025 Palo Alto Networks, Inc.

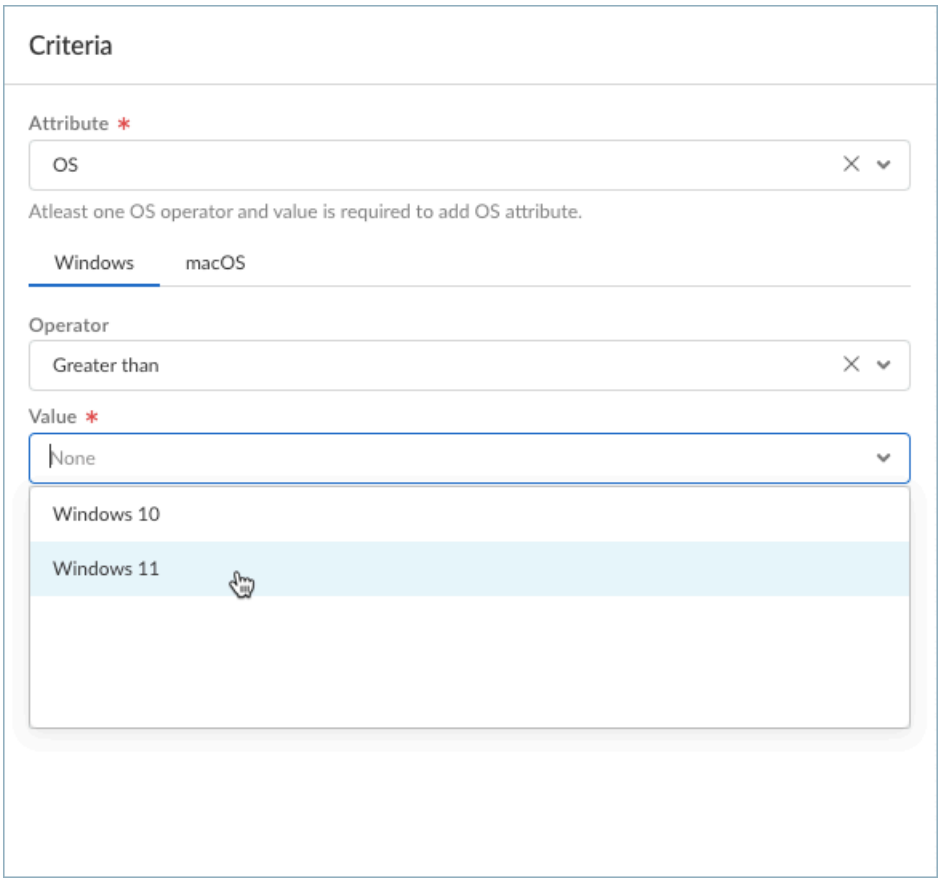
et la version. Vous pouvez sélectionner une ou plusieurs versions de système d'exploitation dans la liste.



- Si vous sélectionnez l'opérateur **Greater than (Supérieur à)** ou **Less than (Inférieur à)**, recherchez ou sélectionnez une version de système d'exploitation dans la liste **Value (Valeurs)**. Pour lancer une recherche, commencez à taper le système

 ©2025 Palo Alto Networks, Inc.

d'exploitation et la version. Vous pouvez sélectionner une version de système d'exploitation dans la liste.



3. Si nécessaire, cliquez sur **Add (Ajouter)** pour ajouter plus de critères. Vous pouvez spécifier jusqu'à trois critères par anneau.

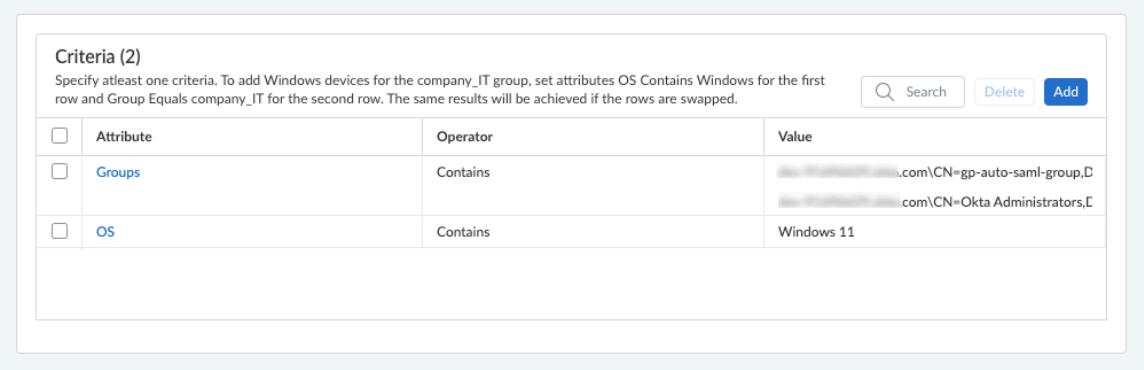
   Vous ne pouvez utiliser un attribut qu'une seule fois par anneau. Une fois que vous avez ajouté un critère à l'aide d'un attribut, cet attribut ne sera plus affiché dans la liste déroulante **Attribute (Attribut)**.

   Une fois les critères ajoutés, ils s'affichent dans le tableau **Criteria (Critères)** dans la page Critères d'anneau. Lorsque Prisma Access évalue les critères, les valeurs énumérées dans

©2025 Palo Alto Networks, Inc.

la même cellule sont évaluées à l'aide de l'opérateur logique OR, tandis que les attributs et les valeurs situés entre les lignes sont évalués à l'aide de l'opérateur logique AND.

Par exemple, les critères de l'image suivante correspondront aux périphériques du groupe **`gp-auto-saml-group`** ou **`Okta Administrators (Administrateurs Okta)`** et exécutent le système d'exploitation Windows 11.



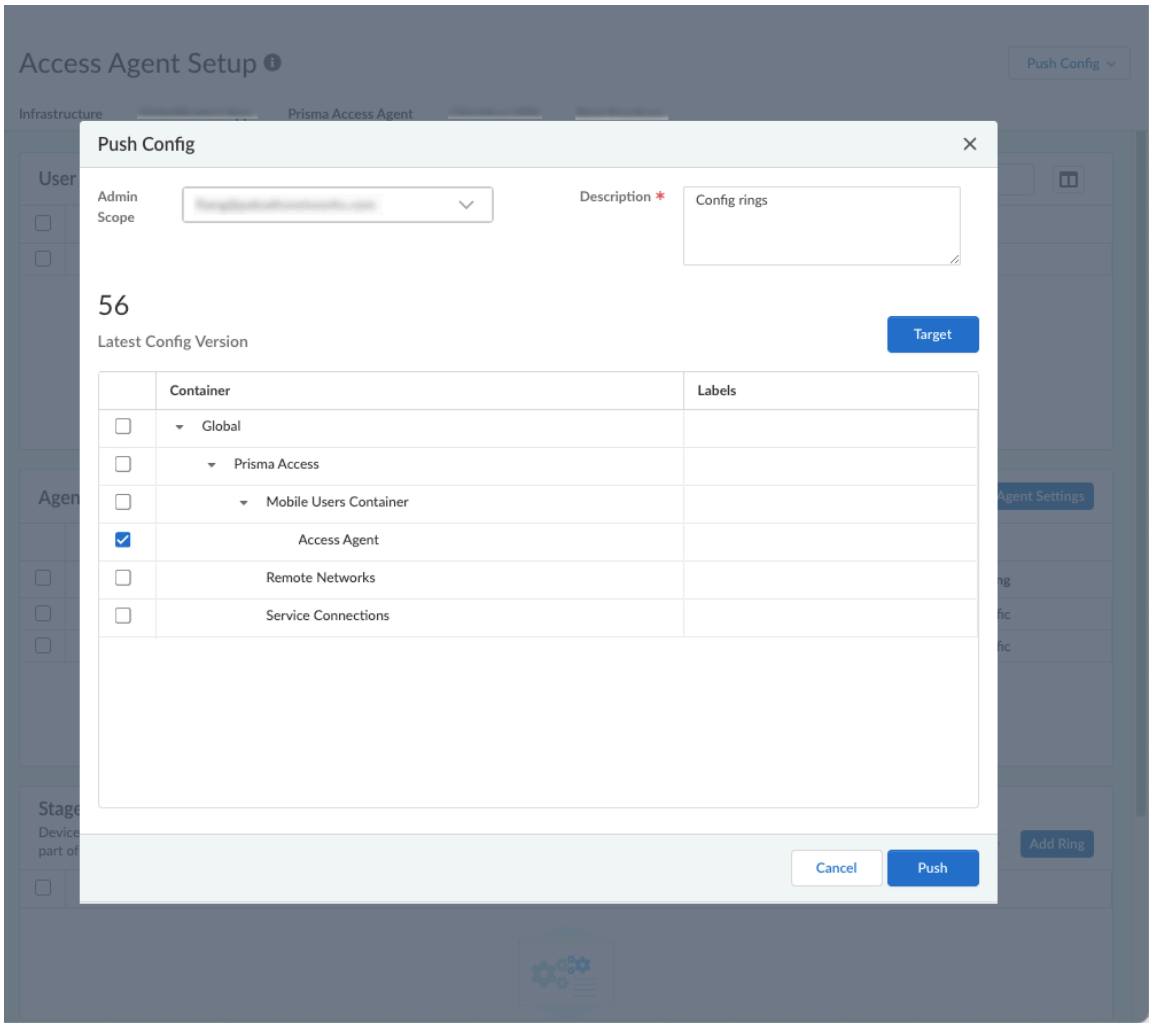
4. Cliquez sur **Save (Enregistrer)** pour enregistrer les critères de l'anneau.

STEP 6 | Pour créer d'autres anneaux, répétez les étapes 2 à 5. Vous pouvez créer un total de cinq anneaux (Anneau 0 à Anneau 4).

 ©2025 Palo Alto Networks, Inc.

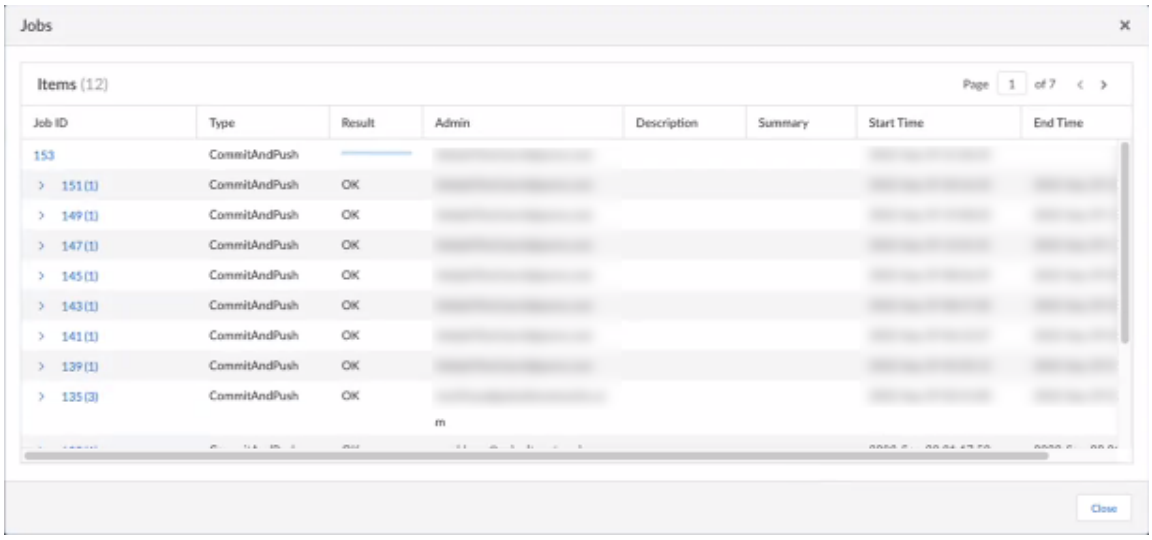
STEP 7 | Transmettez la configuration à Prisma Access.

1. Sélectionnez **Push Config (Transmettre la configuration)** > **Push (Transmettre)**.
2. Saisissez une **Description** de la tâche.
3. Sélectionnez le conteneur **Global (Mondial)** > **Prisma Access** > **Mobile Users (Utilisateurs mobiles)** > **Access Agent (Agent d’accès)** et cliquez sur **Push (Transmettre)**.



4. Attendez la fin de la tâche et cliquez sur **Close (Fermer)** pour fermer la boîte de dialogue des tâches.

 ©2025 Palo Alto Networks, Inc.



STEP 8 | Vous pouvez surveiller le déploiement par étapes dans **Manage (Gérer)** > **Prisma Access Agent** dans Strata Cloud Manager.

Configurez les paramètres globaux généraux pour Prisma Access Agents

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Rôle : Super utilisateur

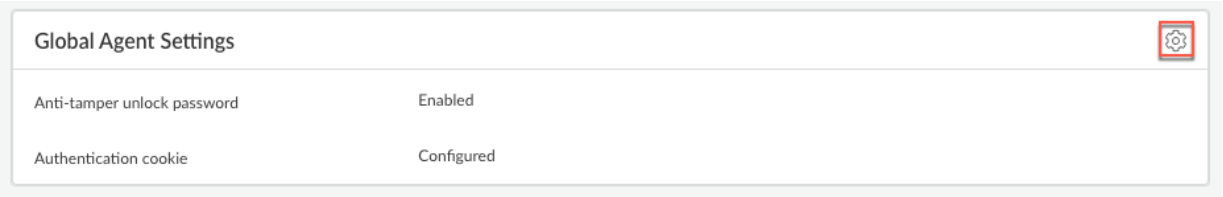
Vous pouvez personnaliser les paramètres globaux de l'agent qui s'appliquent aux agents Prisma Access sur tous les terminaux.

Les paramètres globaux généraux de l'agent incluent la configuration de la fonctionnalité anti-altération qui empêche les utilisateurs d'altérer Prisma Access Agent, notamment sa désinstallation du périphérique d'un utilisateur final. En outre, vous pouvez configurer les paramètres de remplacement de l'authentification, le paramètre de délai d'inactivité et le blocage de la connexion des périphériques en quarantaine.

STEP 1 | À partir de Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Access Agent (Agent d'accès)** > **Prisma Access Agent**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Modifier les **Global Agent Settings (Configurer les paramètres globaux de l'agent)**.



STEP 3 | Sélectionnez **General (Général)**.

STEP 4 | Configurez un mot de passe de déverrouillage anti-altération.

Vous pouvez protéger Prisma Access Agent en activant la fonctionnalité anti-altération, qui empêche tout utilisateur non autorisé d'effectuer des altérations à Prisma Access Agent. La fonctionnalité anti-altération peut protéger les ressources Prisma Access Agent suivantes sur vos terminaux :

- Dossiers et fichiers Prisma Access Agent : les utilisateurs non autorisés ne peuvent supprimer ou renommer tout fichier et dossier associé à Prisma Access Agent.
- Services et processus de profil d'informations sur l'hôte (HIP) de Prisma Access Agent : les utilisateurs non autorisés ne peuvent arrêter aucun service et processus HIP associé à Prisma Access Agent. Les processus HIP recueillent des informations sur l'hôte exécutant Prisma Access Agent et soumettent les informations sur l'hôte à Prisma Access pour inspection. Si un utilisateur tente d'arrêter un processus, il doit fournir le mot de passe de déverrouillage anti-altération.
- Clés de registre Prisma Access Agent (sous Windows) ou fichier `.plist` (sous macOS) : les utilisateurs non autorisés ne peuvent pas supprimer ou mettre à jour les clés de registre Windows ou le fichier `.plist` pour Prisma Access Agent.
- Interface de ligne de commande PACli : les utilisateurs non autorisés ne peuvent pas désactiver Prisma Access Agent ou la fonctionnalité anti-altération à l'aide de l'interface de ligne de commande PACli. Les administrateurs et les utilisateurs autorisés qui doivent effectuer certaines actions de dépannage au niveau de la ligne de commande doivent fournir le mot de passe de déverrouillage (superviseur) anti-altération à l'invite.

Pour déverrouiller la fonctionnalité anti-altération afin de dépanner Prisma Access Agent, vous devez configurer un mot de passe de déverrouillage anti-altération (également appelé mot de passe superviseur).

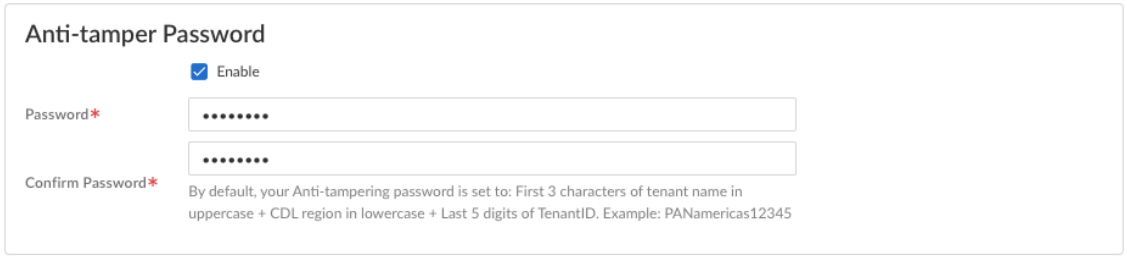
1. **Enable (Activez)** le mot de passe anti-altération.

   Si vous n'activez pas le mot de passe anti-altération, aucun mot de passe n'est attribué et un utilisateur peut saisir n'importe quel mot de passe (y compris un mot de passe vide) à l'invite de la ligne de commande Prisma Access Agent.

   Si vous désactivez le mot de passe anti-altération après l'avoir activé, les utilisateurs peuvent exécuter certaines commandes PACli sur l'agent, telles que les commandes **`pacli disable`**, **`pacli hip status`**, **`pacli protect disable`** et **`pacli switchto GlobalProtect`**, sans fournir le mot de passe superviseur. Ils n'ont qu'à appuyer sur **Enter (Entrée)** lorsque le mot de passe leur est demandé.

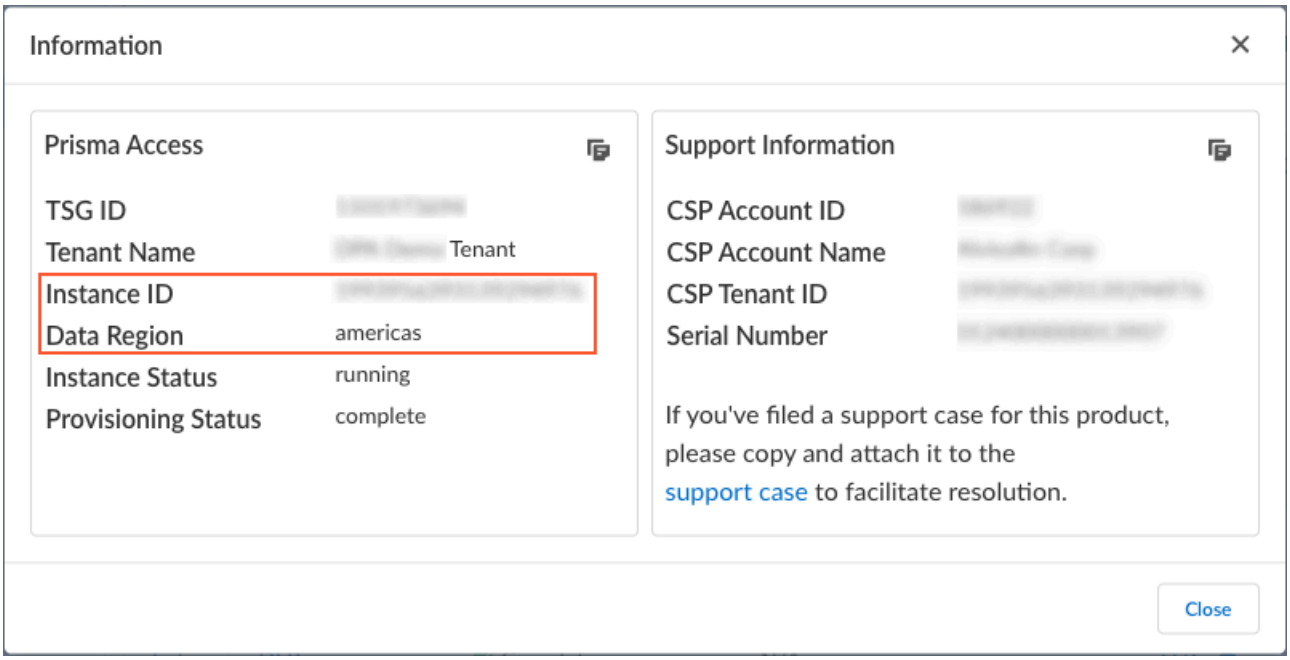
 ©2025 Palo Alto Networks, Inc.

2. Saisissez le **Password (Mot de passe)**, puis **Confirm Password (Confirmez le mot de passe)** en le saisissant à nouveau. Le mot de passe doit comporter un minimum de huit caractères alphanumériques.



Si vous ne fournissez pas un mot de passe, le mot de passe par défaut sera utilisé. Par défaut, le mot de passe anti-altération est défini sur les trois premiers caractères du nom du locataire Prisma Access en majuscules, plus la **Data Region (Région de données)** Prisma Access en minuscules, plus les cinq derniers chiffres de l'**Instance ID (ID d'instance)** Prisma Access, par exemple : **PANamericas56789**.

Vous pouvez obtenir l'**Instance ID (ID d'instance)** et la **Data Region (Région de données)** en sélectionnant **Settings (Paramètres)** > **Tenants (Locataires)** > **<your_tenant>** et en sélectionnant l'infobulle **View Support Info (Afficher les informations de support)** à côté du numéro de série de Prisma Access.

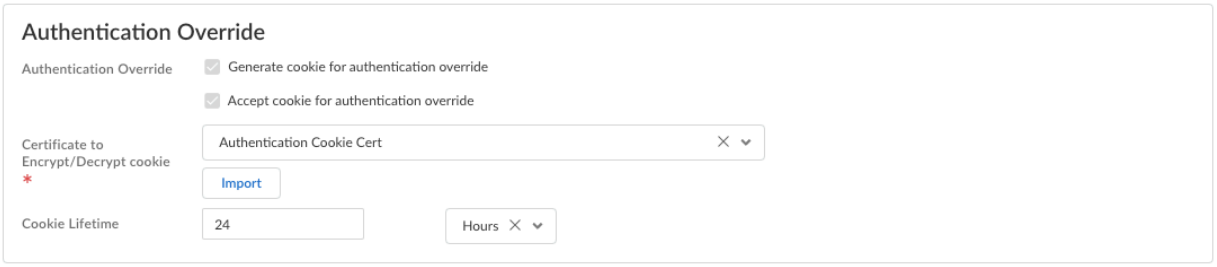


Pour assurer un niveau de sécurité plus élevé à vos agents, configurez un nouveau mot de passe de déverrouillage anti-altération pour remplacer le mot de passe par défaut, car ce dernier pourrait ne pas être le plus sécurisé.

STEP 5 | Configurez les paramètres de **Authentification Override (Remplacement de l'authentification)** pour autoriser Prisma Access à générer et à accepter des cookies sécurisés et cryptés pour l'authentification des utilisateurs. Le remplacement de l'authentification

 ©2025 Palo Alto Networks, Inc.

autorise l'utilisateur à fournir des informations d'identification de connexion une seule fois pendant la **Cookie Lifetime (Durée de vie des cookies)** spécifiée.



- **Generate cookie for authentication override (Générer un cookie pour remplacer l'authentification)** : permet à Prisma Access de générer des cookies cryptés spécifiques au terminal et d'émettre les cookies d'authentification au terminal.
- **Accept cookie for authentication override (Accepter un cookie pour remplacer l'authentification)** : permet à Prima Access d'authentifier les utilisateurs au moyen d'un cookie crypté valide. Lorsque l'appli présente un cookie valide, Prisma Access vérifie que le cookie a été crypté par Prisma Access à l'origine, décrypte le cookie, puis authentifie l'utilisateur.
- **Certificate to Encrypt/Decrypt Cookie (Certificat pour crypter/décrypter le cookie)** : sélectionnez un certificat RSA à utiliser pour crypter et décrypter le cookie.
- **Cookie Lifetime (Durée de vie des cookies)** : spécifie les heures, les jours ou les semaines pendant lesquelles le cookie est valide (la valeur par défaut est 24 heures). La plage des heures est de 1 à 72 ; la plage des semaines est de 1 à 52 ; et la plage des jours est de 1 à 365. Après l'expiration du cookie, l'utilisateur doit saisir à nouveau ses informations d'identification de connexion. Prisma Access crypte alors un nouveau cookie à envoyer à l'agent. Cette valeur peut être identique ou différente de la durée de vie des cookies que vous configurez.

STEP 6 | Saisissez le nombre de minutes de la **Inactivity Logout (Déconnexion en cas d'inactivité)** pour spécifier la durée après laquelle les utilisateurs inactifs sont déconnectés de Prisma Access Agent.

Vous pouvez utiliser la période de déconnexion en cas d'inactivité pour appliquer une politique de sécurité afin de surveiller le trafic à partir des terminaux lorsque vous êtes connecté à Prisma Access et de déconnecter rapidement les sessions Prisma Access Agent inactives. Vous pouvez imposer une période de déconnexion d'inactivité plus courte. Les utilisateurs sont déconnectés si Prisma Access Agent n'a pas acheminé le trafic via le tunnel ou si la passerelle ne reçoit pas une vérification HIP du terminal au cours de la période configurée.

STEP 7 | **Block Login for Quarantined Devices (Bloquer la connexion pour les périphériques en quarantaine)** afin d'empêcher les utilisateurs de Prisma Access Agent de se connecter à partir de périphériques en quarantaine.

Si un utilisateur tente de se connecter à partir d'un périphérique en quarantaine lorsque ce paramètre est activé, Prisma Access Agent l'informe que le périphérique est en quarantaine et qu'il ne peut pas se connecter à partir du périphérique en question. Si ce paramètre n'est pas activé, l'utilisateur reçoit la notification mais peut se connecter depuis ce périphérique.

STEP 8 | Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

 ©2025 Palo Alto Networks, Inc.

Configurer les notifications HIP pour l'accès à privilèges dynamique Prisma Access Agent

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Rôle : Super utilisateur

Dans l'onglet **HIP Notifications (Notifications HIP)** de la page Modifier les paramètres globaux de l'agent, vous pouvez créer des notifications de profil d'informations sur l'hôte, créer et gérer des objets HIP et créer et gérer des profils HIP qui s'appliquent à Prisma Access Agent sur tous les terminaux.

Prisma Access Agent collecte des informations sur l'hôte sur lequel il s'exécute et soumet ces informations sur l'hôte à l'emplacement Prisma Access (passerelle) dès que la connexion est établie. La passerelle fait correspondre ces informations brutes sur l'hôte soumises par Prisma Access Agent à tous les objets HIP et profils HIP que vous avez définis. Si elle trouve une correspondance, elle génère une entrée dans le journal des correspondances HIP. En outre, si elle trouve une correspondance de profil HIP dans une règle de politique, elle met applique la politique de sécurité correspondante.

Les vérifications HIP sont effectuées lorsque l'appli se connecte à la passerelle et les vérifications ultérieures sont effectuées toutes les heures pendant que Prisma Access Agent est connecté. Prisma Access Agent peut demander un rapport HIP mis à jour si la vérification HIP antérieure a changé. Seul le dernier rapport HIP est conservé sur la passerelle par terminal.

L'utilisation des profils d'informations sur l'hôte pour la mise en œuvre d'une stratégie active la sécurité granulaire qui garantit que les hôtes distants accédant à vos ressources vitales sont adéquatement maintenus et qu'ils respectent vos normes de sécurité avant de les autoriser à accéder à vos ressources réseau. Par exemple, avant d'autoriser l'accès à vos systèmes de données les plus sensibles, vous devrez vérifier que le cryptage de disque est activé sur les disques durs des hôtes accédant aux données. Vous pouvez mettre en œuvre cette stratégie en créant une règle de sécurité qui autorise l'accès à l'application uniquement si le cryptage de disque est activé sur le système de points de terminaison.

En outre, pour les terminaux qui ne respectent pas cette règle, vous pouvez créer un message de notification qui alerte les utilisateurs sur les raisons pour lesquelles l'accès leur a été refusé. Vous pouvez également fournir un lien vers l'emplacement où ils peuvent accéder au programme d'installation du logiciel de cryptage manquant. Pour autoriser l'utilisateur à accéder à ce partage de fichiers, vous devrez créer une règle de sécurité correspondante qui autoriserait l'accès au partage particulier pour les hôtes ayant cette correspondance spécifique de profil HIP.

Vous pouvez effectuer les tâches suivantes :

 ©2025 Palo Alto Networks, Inc.

- Créer une notification HIP pour l'accès à privilèges dynamique Prisma Access Agent
- Créer et gérer des objets HIP pour l'accès à privilèges dynamique Prisma Access Agent
- Créer et gérer des profils HIP pour l'accès à privilèges dynamique Prisma Access Agent

Créer une notification HIP pour l'accès à privilèges dynamique Prisma Access Agent

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Rôle : Super utilisateur

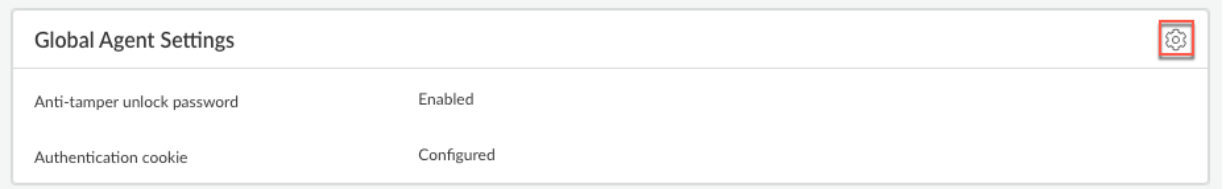
Vous pouvez définir les messages de notification à afficher aux utilisateurs finaux lors de l'application d'une règle de sécurité dotée d'un profil HIP.

La décision d'afficher ou non un message de notification lors de la correspondance ou non de l'utilisateur à un profil HIP dans la politique dépend en grande partie de votre politique et de ce que signifie une correspondance (ou non-correspondance) HIP pour l'utilisateur. Autrement dit, une correspondance signifie-t-elle que l'utilisateur bénéficie d'un accès complet aux ressources de votre réseau ou qu'il dispose d'un accès limité en raison d'un problème de non-conformité ?

Par exemple, supposons que vous créez un profil HIP qui correspond si l'antivirus d'entreprise et les logiciels anti-spyware requis ne sont pas installés. Vous pouvez créer un message de notification HIP pour les utilisateurs qui correspondent au profil HIP pour leur indiquer qu'ils doivent installer le logiciel. Sinon, si votre profil HIP correspond alors que ces mêmes applications sont installées, vous pourriez créer le message aux utilisateurs qui ne correspondent pas au profil.

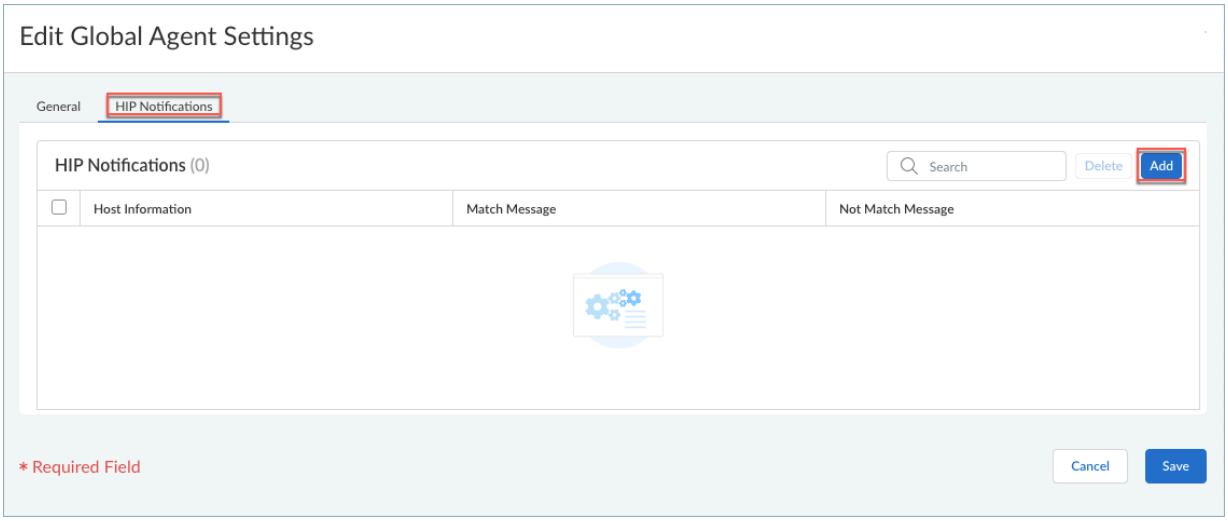
STEP 1 | À partir de Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Access Agent (Agent d'accès)** > **Prisma Access Agent**.

STEP 2 | **Edit (Modifier)** les **Global Agent Settings (Paramètres globaux de l'agent)**.

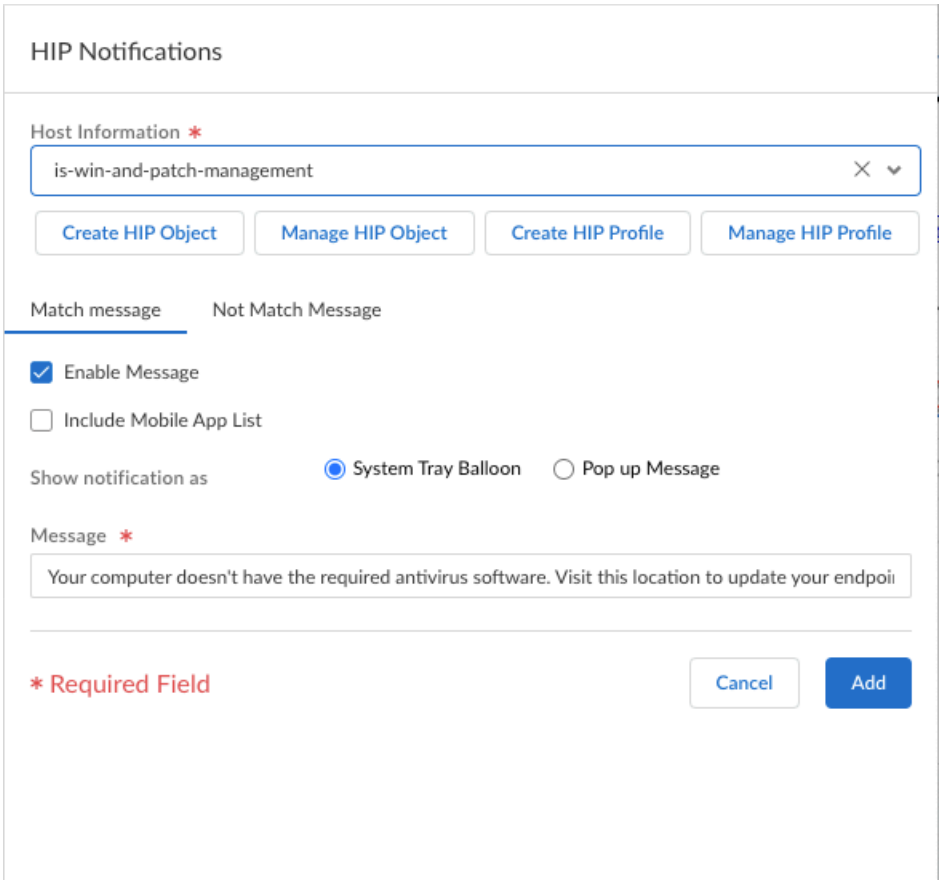


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Sélectionnez **HIP Notifications (Notifications HIP)** et cliquez sur **Add (Ajouter)**.



STEP 4 | Sélectionnez le profil HIP auquel ce message s'applique dans la liste déroulante **Host Information (Informations sur l'hôte)**.



S'il n'y a pas de profils HIP, vous devez en créer un.

STEP 5 | Selon que vous souhaitiez afficher le message lorsque le profil HIP correspondant est mis ou non en correspondance, sélectionnez **Match Message (Message de correspondance)** ou **Not Match Message (Message de non-correspondance)**. Dans certains cas, vous pourriez

 ©2025 Palo Alto Networks, Inc.

créer des messages à la fois pour une correspondance et pour une non-correspondance, en fonction des objets que vous souhaitez faire correspondre et des objectifs que vous avez définis pour la politique.

STEP 6 | Sélectionnez **Enable Message (Activer le message)**, puis sélectionnez si vous souhaitez afficher le message sous la forme d'une **System Tray Balloon (infobulle dans la barre des tâches)** ou en tant que **Pop Up Message (message contextuel)**.

STEP 7 | Saisissez le texte de votre **Message** puis cliquez sur **Add (Ajouter)**.

STEP 8 | Répétez cette procédure pour chaque message que vous souhaitez définir.

Créer et gérer des objets HIP pour l'accès à privilèges dynamique Prisma Access Agent

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licence Prisma Access avec l'abonnement Utilisateur mobile ❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Rôle : Super utilisateur

Vous pouvez définir les attributs d'hôte que vous souhaitez surveiller ou utiliser pour l'application de politiques en créant des objets HIP et des profils HIP sur la passerelle Prisma Access.

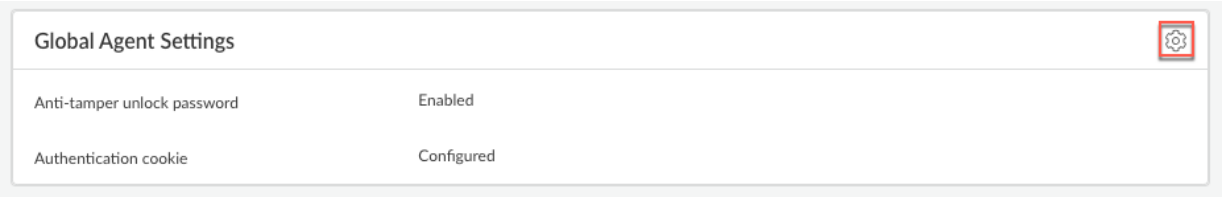
Les objets HIP sont des critères de correspondance utilisés pour filtrer les informations sur l'hôte que vous souhaitez utiliser pour appliquer la politique à partir des données brutes rapportées par Prisma Access Agent. Par exemple, bien que les données brutes sur l'hôte puissent inclure des informations sur plusieurs modules antivirus installés sur le terminal, vous pourriez n'êtes intéressé que par une application particulière. Dans ce cas, créez un objet HIP qui doit correspondre à l'application spécifique que vous souhaitez mettre en œuvre.

Le meilleur moyen de définir les objets HIP dont vous avez besoin consiste à déterminer la manière dont vous prévoyez utiliser les informations sur l'hôte que vous collectez dans l'application de la politique. N'oubliez pas que les objets HIP forment simplement des blocs qui vous autorisent à créer les profils HIP utilisés dans vos politiques de sécurité. Par conséquent, essayez de garder vos objets simples en correspondant un élément, comme la présence d'un type particulier de logiciel requis, l'abonnement à un domaine spécifique ou la présence d'un système d'exploitation particulier. Cela vous permettra de disposer de la souplesse nécessaire pour créer une politique HIP enrichie et granulaire.

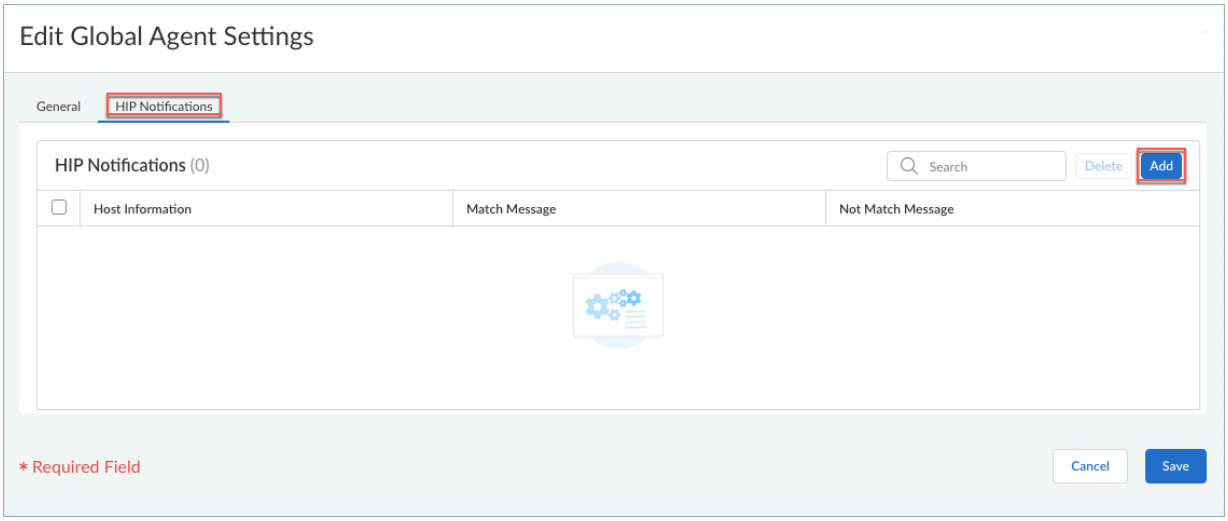
STEP 1 | À partir de Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Access Agent (Agent d'accès)** > **Prisma Access Agent**.

 ©2025 Palo Alto Networks, Inc.

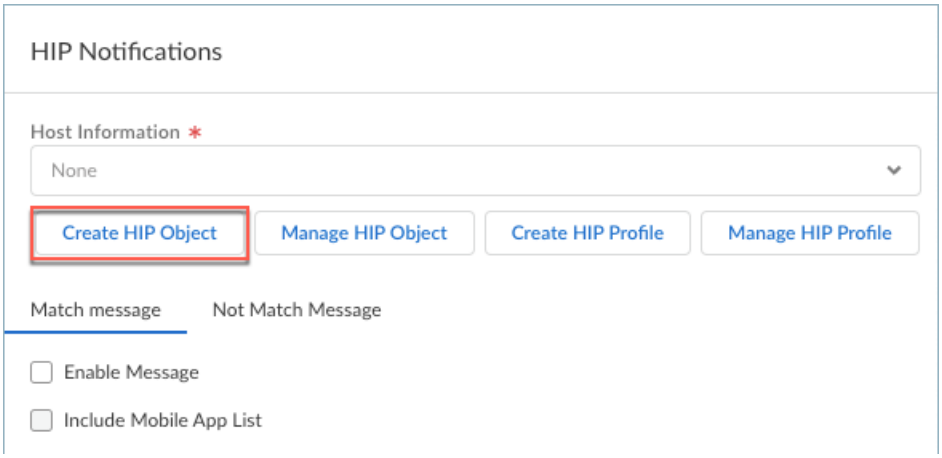
STEP 2 | **Edit (Modifier)** les **Global Agent Settings (Paramètres globaux de l'agent)**.



STEP 3 | Sélectionnez **HIP Notifications (Notifications HIP)** et cliquez sur **Add (Ajouter)**.



STEP 4 | Cliquez sur **Create HIP Object (Créer un objet HIP)**.



STEP 5 | Saisissez un **Name (Nom)** et une **Description** pour l'objet.

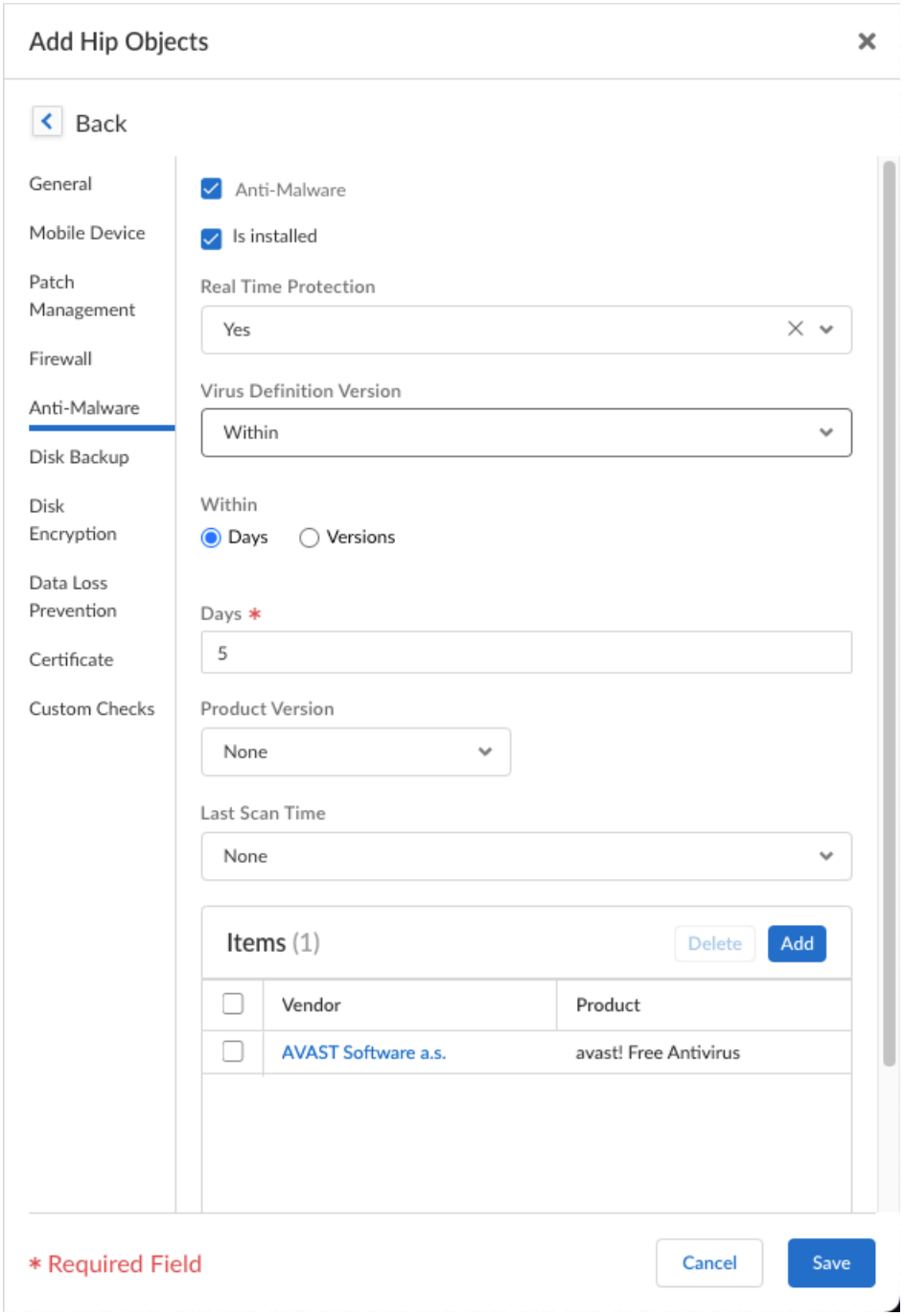
STEP 6 | Sélectionnez l'onglet correspondant à la catégorie d'informations sur l'hôte qui vous intéressent, puis cochez la case pour activer la mise en correspondance de l'objet avec la catégorie.

Par exemple, pour créer un objet qui cherche des informations sur le logiciel antivirus ou antispyware, sélectionnez l'onglet **Anti-Malware (Anti-logiciels malveillants)**, puis cochez

 ©2025 Palo Alto Networks, Inc.

la case **Anti-Malware (Anti-logiciels malveillants)** pour activer les champs correspondants. Remplissez les champs pour définir les critères de correspondance souhaités.

Par exemple, l'image suivante illustre comment créer un objet HIP qui correspondra si le l'application logicielle antivirus AVAST gratuite est installée sur le terminal, si la **Real Time Protection (Protection en temps réel)** est activée, et si les définitions de logiciels malveillants ont été mises à jour au cours des 5 derniers jours.



Répétez cette étape pour chaque catégorie que vous souhaitez faire correspondre dans cet objet. Pour plus d'informations, consultez le Tableau : Catégories de collecte de données.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Cliquez sur **Save (Enregistrer)**, puis sur **Add (Ajouter)** pour enregistrer et ajouter votre objet HIP.

STEP 8 | Pour gérer vos objets HIP, vous pouvez sélectionner un objet existant dans le tableau des notifications HIP ou cliquer sur **Add (Ajouter)** dans la page Modifier les paramètres globaux de l'agent pour ouvrir la fenêtre des notifications HIP.

Ensuite, cliquez sur **Manage HIP Object (Gérer l'objet HIP)** pour afficher la liste des objets HIP que vous avez configurés. Vous pouvez sélectionner un objet HIP et le **Delete (Supprimer)**, le **Clone (Cloner)** ou le **Move (Déplacer)**.

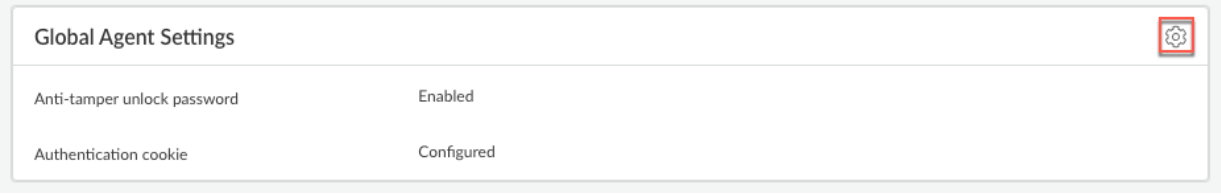
Créer et gérer des profils HIP pour l'accès à privilèges dynamique Prisma Access Agent

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access 5.1 Innovation ☐ Licence Prisma Access avec l'abonnement Utilisateur mobile ☐ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ☐ Rôle : Super utilisateur

Un profils HIP est une collection d'objets de profils d'informations sur l'hôte qui sont évalués ensemble, pour la surveillance ou l'application de politiques de sécurité. Lors de la création de profils HIP, vous pouvez combiner des objets HIP et les profils HIP précédemment créés à l'aide d'une logique booléenne, comme lorsqu'un flux de trafic est évalué en fonction du profil HIP résultant, auquel il peut correspondre ou non. En cas de correspondance, la règle de politique correspondante est mise en œuvre. S'il n'y a pas de correspondance, le flux est évalué en fonction de la règle suivante, comme avec tout autre critère de correspondance de politique.

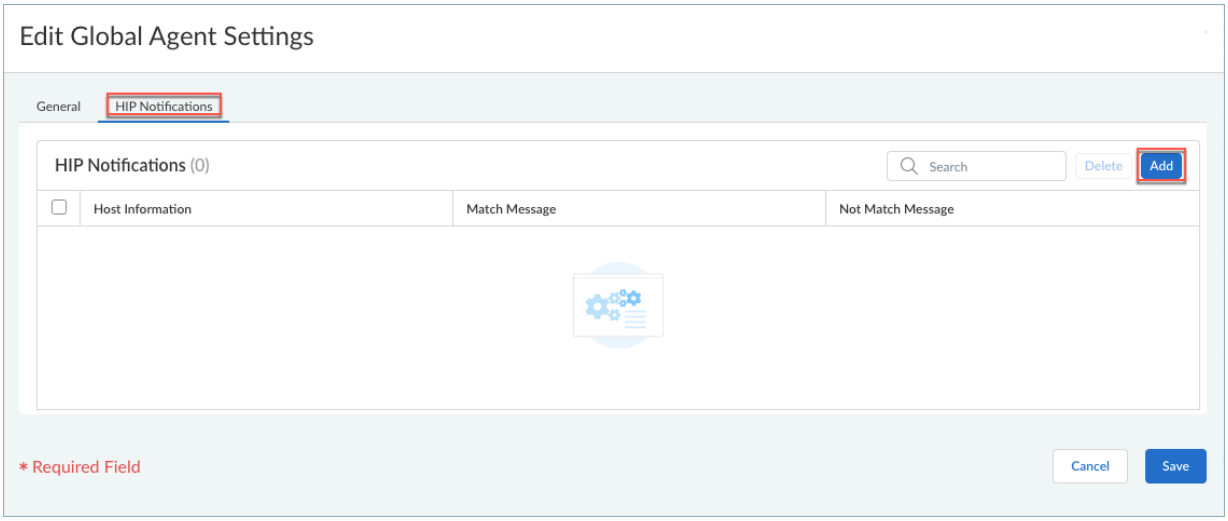
STEP 1 | À partir de Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Access Agent (Agent d'accès)** > **Prisma Access Agent**.

STEP 2 | **Edit (Modifier)** les **Global Agent Settings (Paramètres globaux de l'agent)**.

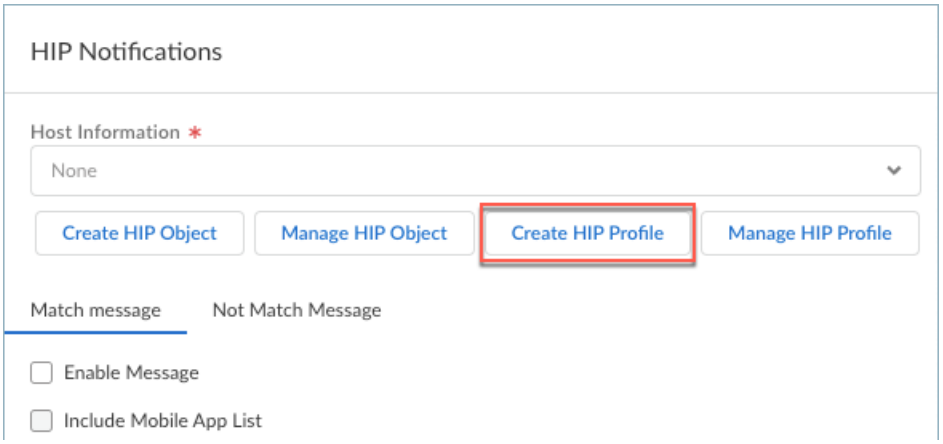


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Sélectionnez **HIP Notifications (Notifications HIP)** et cliquez sur **Add (Ajouter)**.



STEP 4 | Cliquez sur **Create HIP Profile (Créer un profil HIP)**.



STEP 5 | Saisissez un **Name (Nom)** et une **Description** pour identifier le profil.

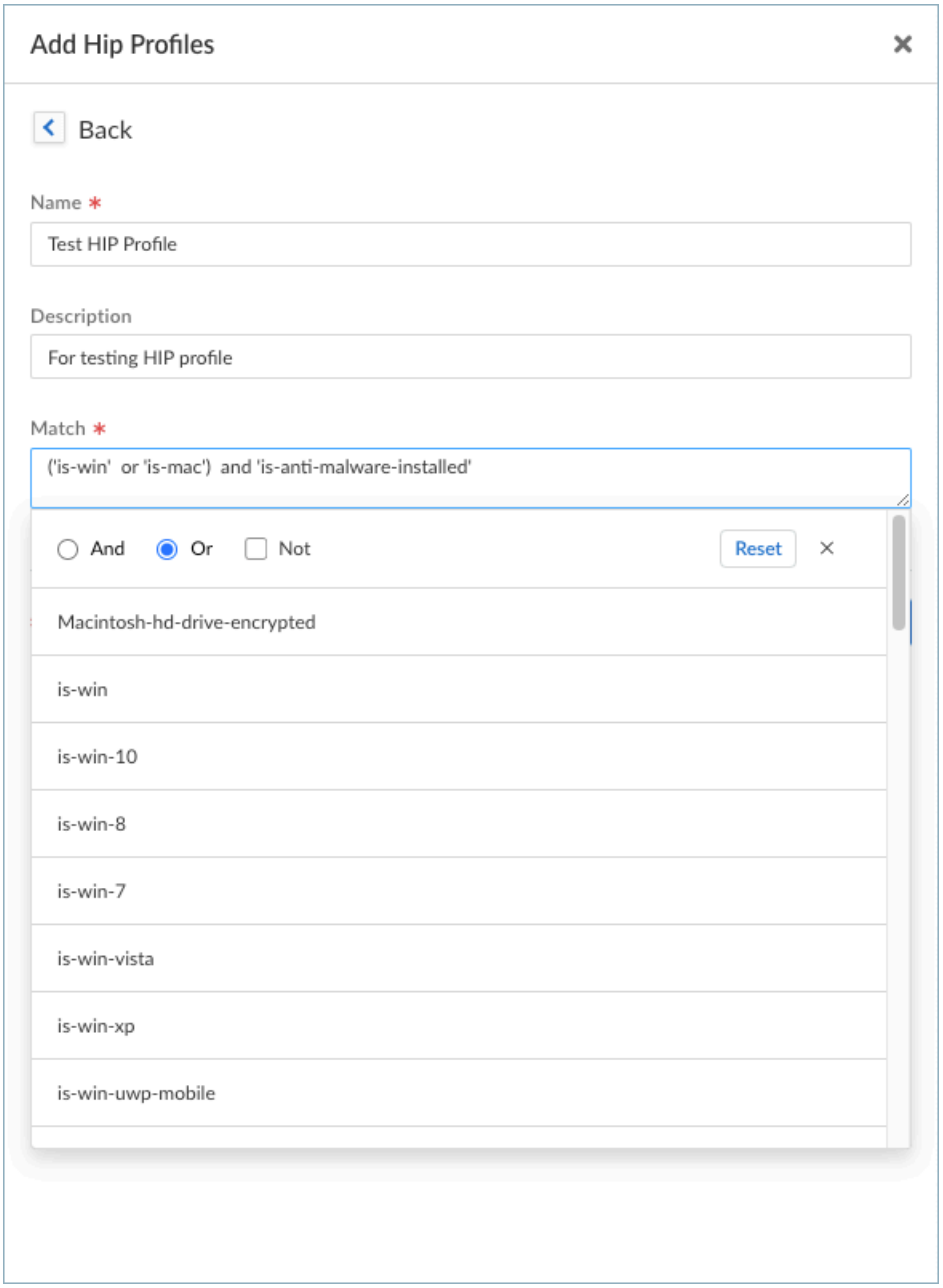
STEP 6 | Cliquez dans le champ **Match (Faire correspondre)** pour ouvrir le générateur de profil HIP.

1. Sélectionnez l'objet ou le profil HIP que vous souhaitez utiliser comme critères de correspondance dans la liste.
2. Sélectionnez un opérateur booléen (**And (Et)**, **And (Et)**). Si vous souhaitez que le profil HIP évalue l'objet comme une correspondance uniquement lorsque les critères de l'objet ne sont pas vrais pour un flux, cochez la case **Not (Ne pas)** avant d'ajouter l'objet.
3. Sélectionnez un autre objet ou profil HIP à évaluer par rapport au premier objet HIP.

STEP 7 | Continuez d'ajouter des critères de correspondance pour le profil que vous créez, en vous assurant de sélectionner la case d'option de l'opérateur booléen correspondant (**And (Et)** ou **And (Et)**) entre chaque ajout, et en cochant la case **Not (Ne pas)**, le cas échéant. Le profil HIP peut contenir jusqu'à 2 048 caractères.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Si vous créez une expression booléenne complexe, vous devez ajouter manuellement les parenthèses aux bons endroits dans la zone de texte **Match (Faire correspondre)** pour que le profil HIP soit évalué à l'aide de la logique souhaitée.



STEP 9 | Cliquez sur **Save (Enregistrer)**, puis sur **Add (Ajouter)** pour enregistrer et ajouter votre profil HIP.

STEP 10 | Pour gérer vos profils HIP, vous pouvez sélectionner un profil existant dans le tableau Notifications HIP ou cliquer sur **Add (Ajouter)** dans la page Modifier les paramètres globaux de l'agent pour ouvrir la fenêtre Notifications HIP.

Ensuite, cliquez sur **Manage HIP Profile (Gérer le profil HIP)** pour afficher la liste des profils HIP que vous avez configurés. Vous pouvez sélectionner un profil HIP et le **Delete (Supprimer)**,

 ©2025 Palo Alto Networks, Inc.

le **Clone (Cloner)** ou le **Move (Déplacer)**. Vous pouvez également **Add (Ajouter)** un profil HIP à partir d’ici.

 ©2025 Palo Alto Networks, Inc.

Transmettez les Prisma Access Agent la configuration.

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access 5.1 Innovation ☐ Licence Prisma Access avec l’abonnement Utilisateur mobile ☐ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ☐ Rôle : Super utilisateur

Après avoir terminé la configuration de Prisma Access Agent ou mis à jour la configuration, vous devez pousser la configuration à Prisma Access.

Créez au moins un projet avant de pouvoir transmettre la validation, sinon la validation échouera.

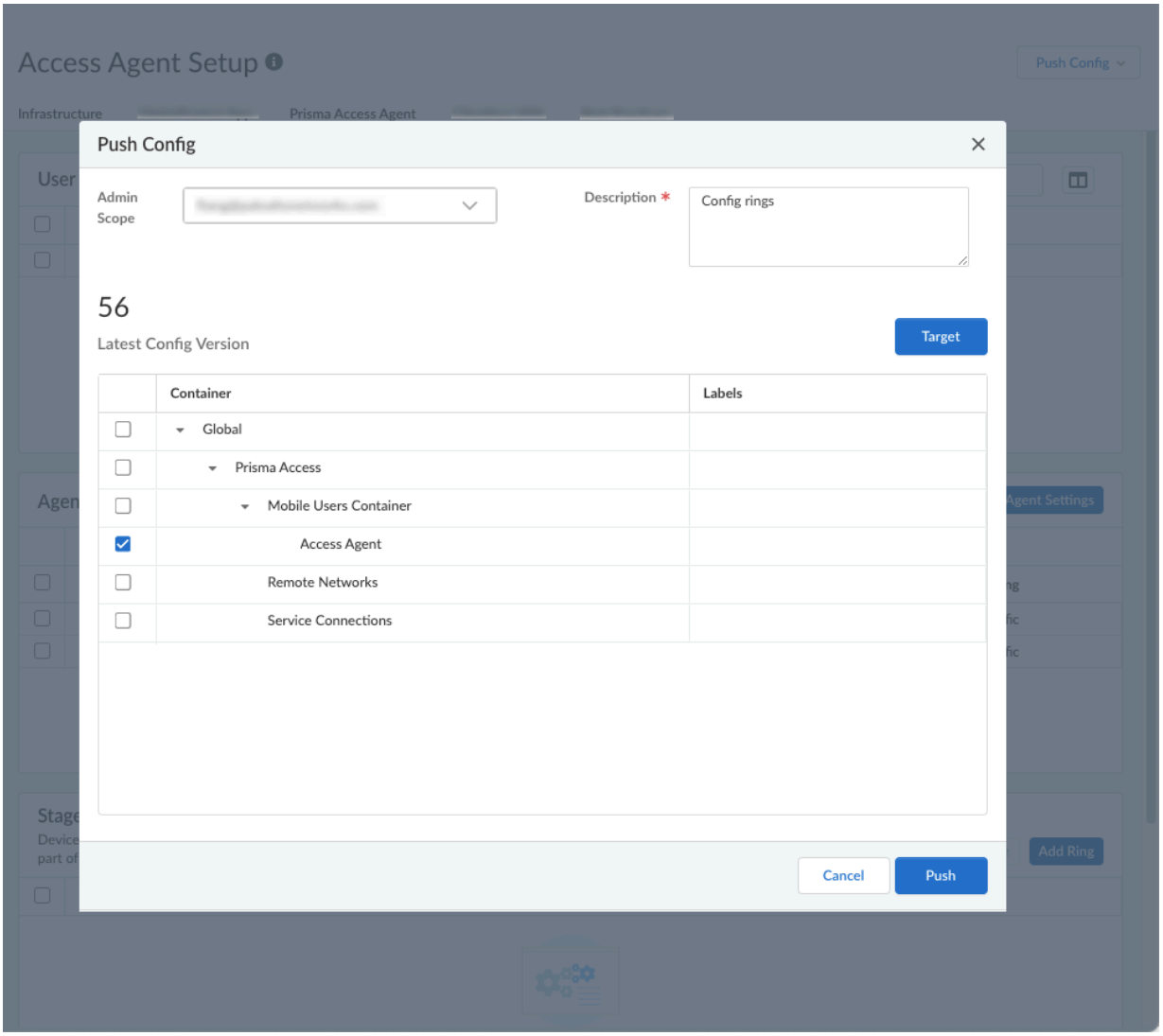
STEP 1 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Access Agent (Agent d’accès)**.

STEP 2 | Sélectionnez **Push Config (Transmettre la configuration)** > **Push (Transmettre)**.

STEP 3 | Saisissez une **Description** de la tâche.

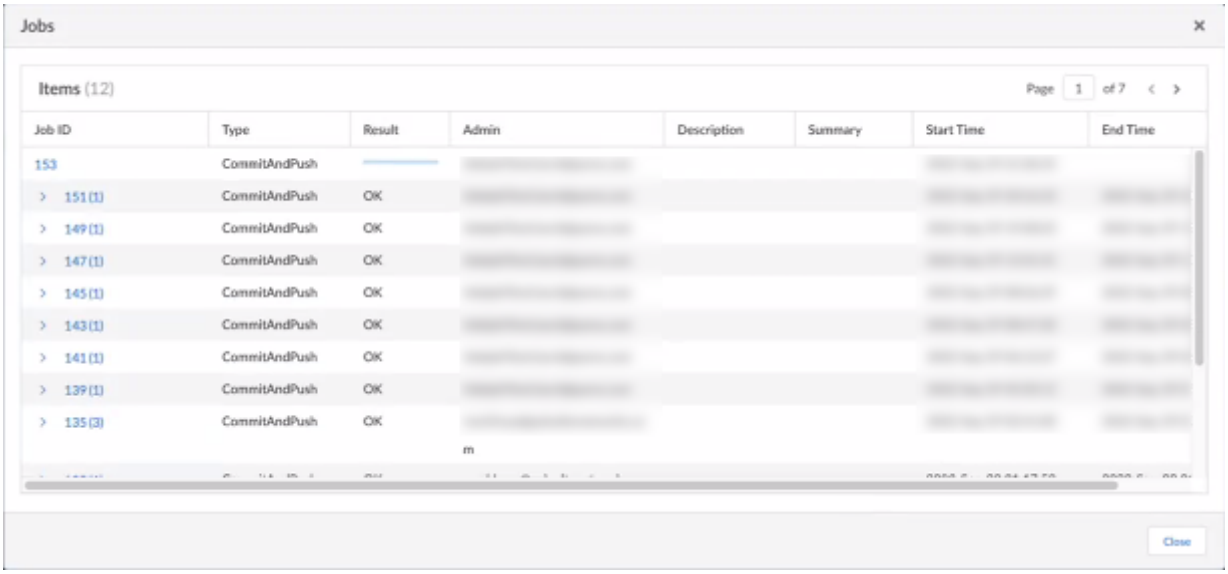
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Sélectionnez le conteneur **Global (Mondial)** > **Prisma Access** > **Mobile Users (Utilisateurs mobiles)** > **Access Agent (Agent d’accès)** et cliquez sur **Push (Pousser)**.



 ©2025 Palo Alto Networks, Inc.

STEP 5 | Attendez la fin de la tâche et cliquez sur **Close (Fermer)** pour fermer la boîte de dialogue des tâches.



 ©2025 Palo Alto Networks, Inc.

Télécharger le package Prisma Access Agent activé par accès à privilèges dynamique

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ Licence Prisma Access avec l’abonnement Utilisateur mobile ❑ Rôle : Super utilisateur

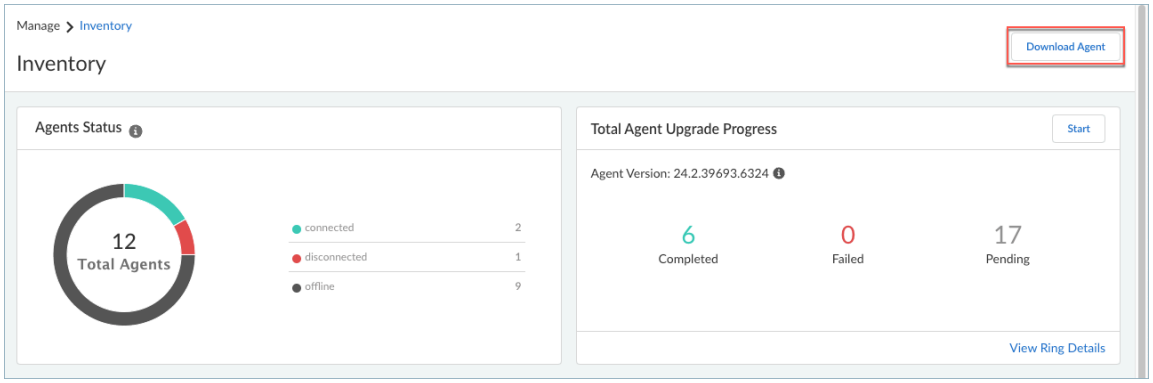
Une fois que vous avez configuré le Prisma Access Agent et les paramètres Prisma Access Agent spécifiques au projet, vous pouvez télécharger le package Prisma Access Agent afin que vos utilisateurs finaux puissent le télécharger et l’installer.

De plus, assurez-vous de télécharger le fichier de configuration. Vos configurations d’agent et d’agent spécifiques au projet, ainsi que l’ID de locataire Prisma Access et le domaine du serveur, sont enregistrées dans le fichier de configuration Prisma Access Agent. Le fichier de configuration sera utilisé lors de l’installation et de l’enregistrement de Prisma Access Agent.

 ©2025 Palo Alto Networks, Inc.

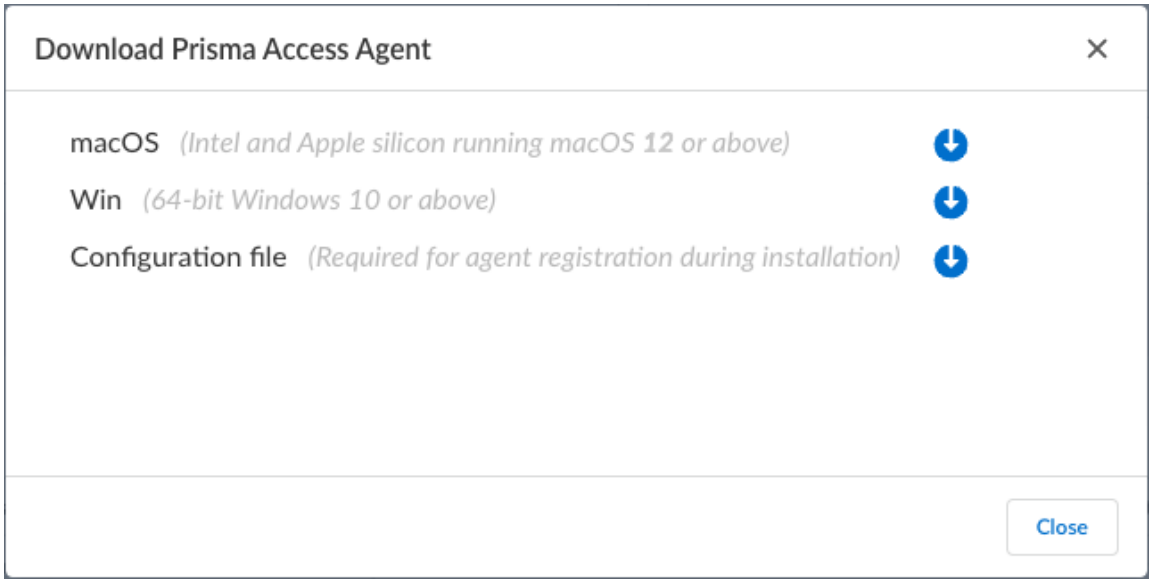
STEP 1 | Téléchargez le package Prisma Access Agent et le fichier de configuration.

1. Sélectionnez **Manage (Gérer)** > **Prisma Access Agent** > **Inventory (Inventaire)**.
2. Cliquez sur **Download Agent (Agent de téléchargement)**.



3. Cliquez sur la flèche vers le bas correspondant aux éléments que vous souhaitez télécharger.

   Assurez-vous de télécharger le **Configuration file (Fichier de configuration)**, car il sera utilisé lors de l'installation et de l'enregistrement du Prisma Access Agent.



4. Enregistrez le package à un emplacement sur votre système et cliquez sur **Close (Fermer)** pour fermer la boîte de dialogue Download Agent (Agent de téléchargement).

STEP 2 | Téléchargez le package à un emplacement central dans le réseau de votre organisation ou distribuez-le afin que vos utilisateurs finaux puissent télécharger et installer le Prisma Access Agent.

 ©2025 Palo Alto Networks, Inc.

Utiliser le Prisma Access Agent pour accéder à vos projets

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access Agent	❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Accès à internet

Si votre organisation est une société informatique ou de services informatiques (ITES) qui doit contrôler quels utilisateurs ont accès à ses projets clients, l'accès à privilèges dynamique offre un moyen transparent, sécurisé et compartimenté pour vous permettre d'accéder uniquement aux projets qui vous sont attribués.

Si votre administrateur a configuré Prisma Access et le Prisma Access Agent pour l'accès à privilèges dynamique, vous pouvez utiliser le Prisma Access Agent pour accéder et travailler sur les projets qui vous sont attribués.

Une fois connecté à votre projet, vous pouvez accéder au réseau de votre organisation, aux ressources du réseau ou aux applications Software-as-a-Service (SaaS) spécifiques au projet. Apprenez comment :

- Se connecter à l'agent Prisma Access compatible avec l'accès à privilèges dynamique
- Afficher l'état de votre connexion
- Modifier les préférences de l'agent Prisma Access compatible avec l'accès à privilèges dynamique
- Se connecter à un autre emplacement Prisma Access
- Afficher les notifications de l'application

De plus, si vous êtes affecté à différents projets, vous pouvez passer à un autre projet ou connecter l'agent Prisma Access à un autre serveur.

Installer Prisma Access Agent

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access Agent	❑ Périphériques de bureau macOS 12 ou version ultérieure, ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 avec privilèges admin ❑ Accès à internet

©2025 Palo Alto Networks, Inc.

Si votre administrateur n'a pas appliqué Prisma Access Agent sur votre périphérique, vous pouvez installer manuellement le Prisma Access Agent sur votre périphérique macOS ou Windows.

Prisma Access Agent et l'application GlobalProtect peuvent coexister sur le même périphérique, mais un seul peut se connecter à Prisma Access. Si l'application GlobalProtect est également installée et activée sur votre périphérique, l'installation de Prisma Access Agent désactivera automatiquement l'application GlobalProtect. Pour utiliser l'application GlobalProtect après avoir installé Prisma Access Agent, vous devrez passer à l'application GlobalProtect.

- macOS
- Windows

Installer Prisma Access Agent (macOS)

Pour installer Prisma Access Agent manuellement sur votre périphérique macOS :

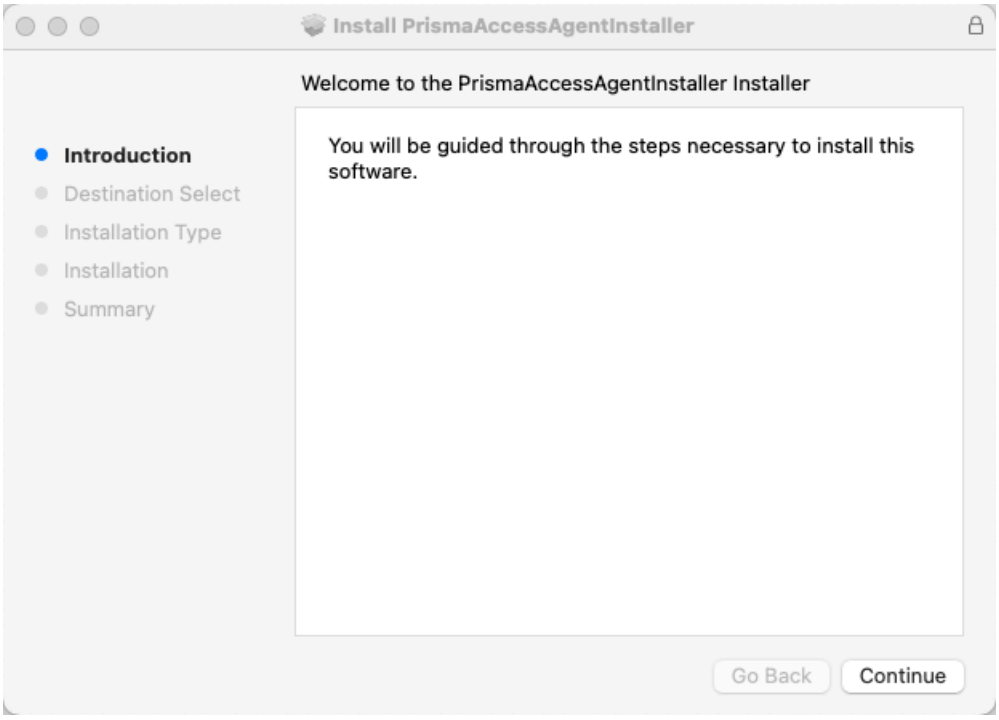
STEP 1 | Obtenez le package Prisma Access Agent que votre administrateur vous a fourni. Le nom du package est selon le format suivant :

`PrismaAccessAgentInstaller_<version>.pkg`

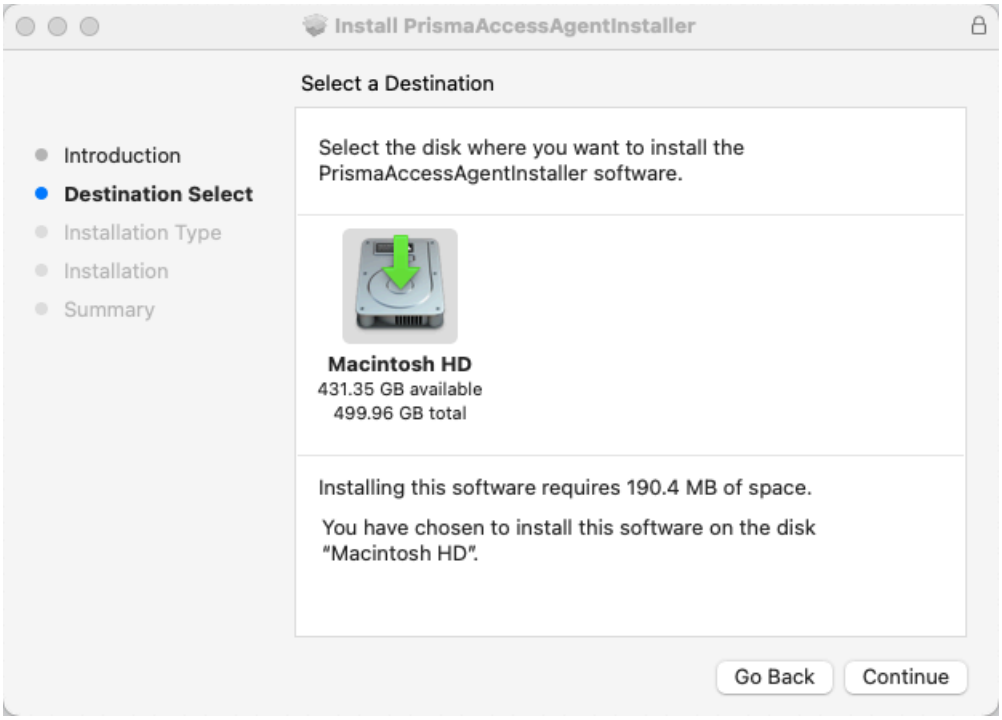
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Dans votre dossier Téléchargements (ou celui dans lequel vous avez placé le package d'installation), ouvrez le package d'installation et suivez les instructions pour installer Prisma Access Agent.

1. Dans le programme d'installation, cliquez sur **Continue (Continuer).**

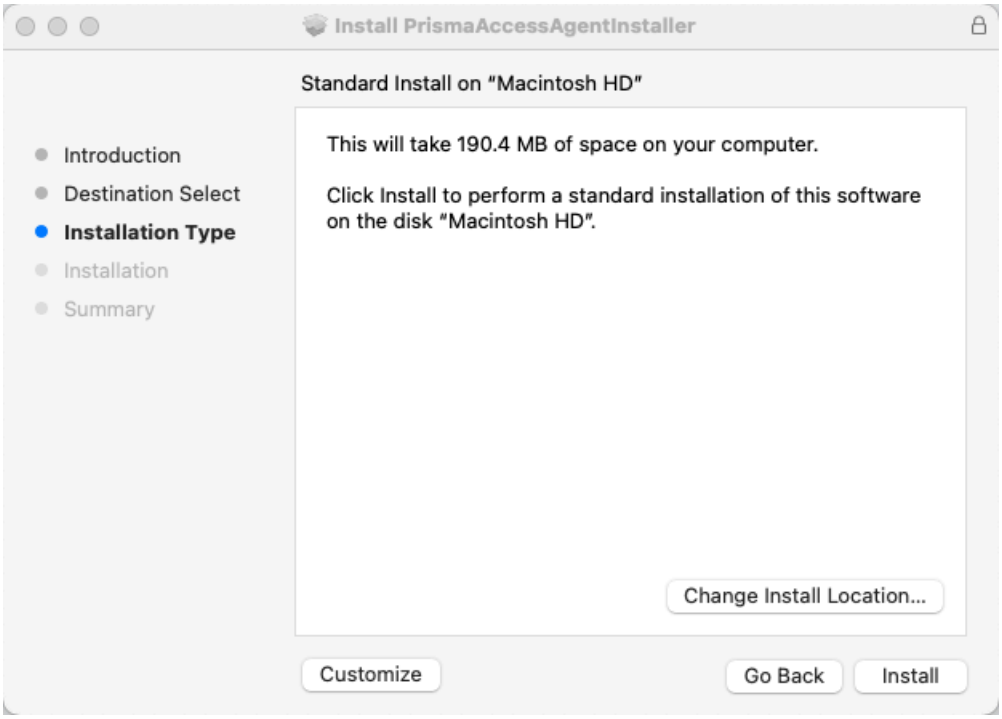


2. Sélectionnez le dossier d'installation de Prisma Access Agent et cliquez sur **Continue (Continuer)**.



 ©2025 Palo Alto Networks, Inc.

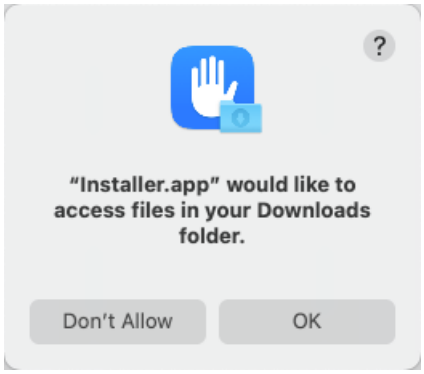
3. Passez en revue les informations dans la page Type d'installation et cliquez sur **Install (Installer)**.



4. À l'invite, saisissez votre **User Name (Nom d'utilisateur)** et votre **Password (Mot de passe)**, puis cliquez sur **Install Software (Installer le logiciel)** pour commencer l'installation.

   Vous pouvez également utiliser Touch ID (si activé) pour terminer cette étape.

5. Lorsque vous êtes invité à autoriser le programme d'installation à accéder aux fichiers du dossier dans lequel vous avez téléchargé le package d'installation, cliquez sur **OK**.



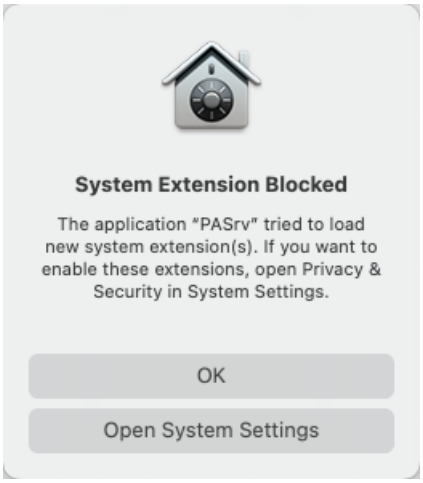
6. Par défaut, macOS bloque les extensions du système Prisma Access Agent. Les extensions du système ou du réseau s'affichent si votre administrateur a configuré Prisma Access Agent avec des règles de transfert de trafic pour :

   - Tunnellisation fractionnée : dirige le trafic réseau à travers ou en dehors de la connexion Prisma Access.
   - DNS fractionné : dirige les requêtes DNS pour les applications et les ressources via Prisma Access ou en dehors de Prisma Access en plus du trafic réseau.

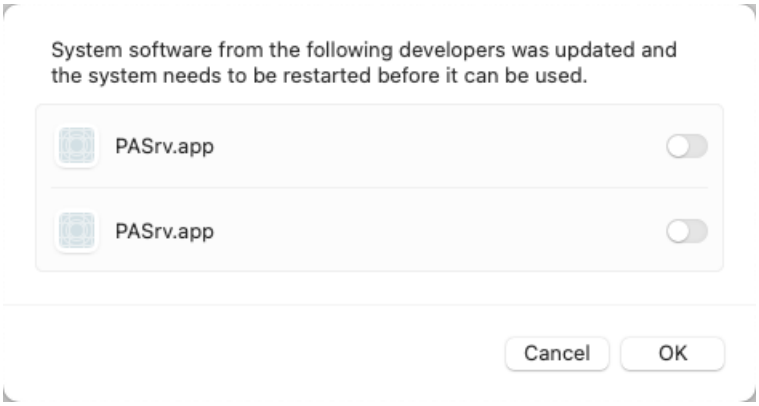
 ©2025 Palo Alto Networks, Inc.

Pour que Prisma Access Agent fonctionne, vous devez activer les extensions du système :

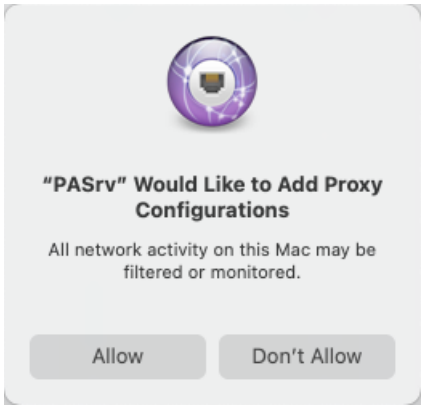
1. Cliquez sur **Open System Settings (Ouvrir les paramètres du système**.



2. Dans la fenêtre Confidentialité et sécurité, cliquez sur **Details (Détails)** pour **Some system software requires your attention before it can be used (Certains logiciels système nécessitent votre attention avant d'être utilisés).**
3. Activez les deux applications **PASrv.app** et cliquez sur **OK**.



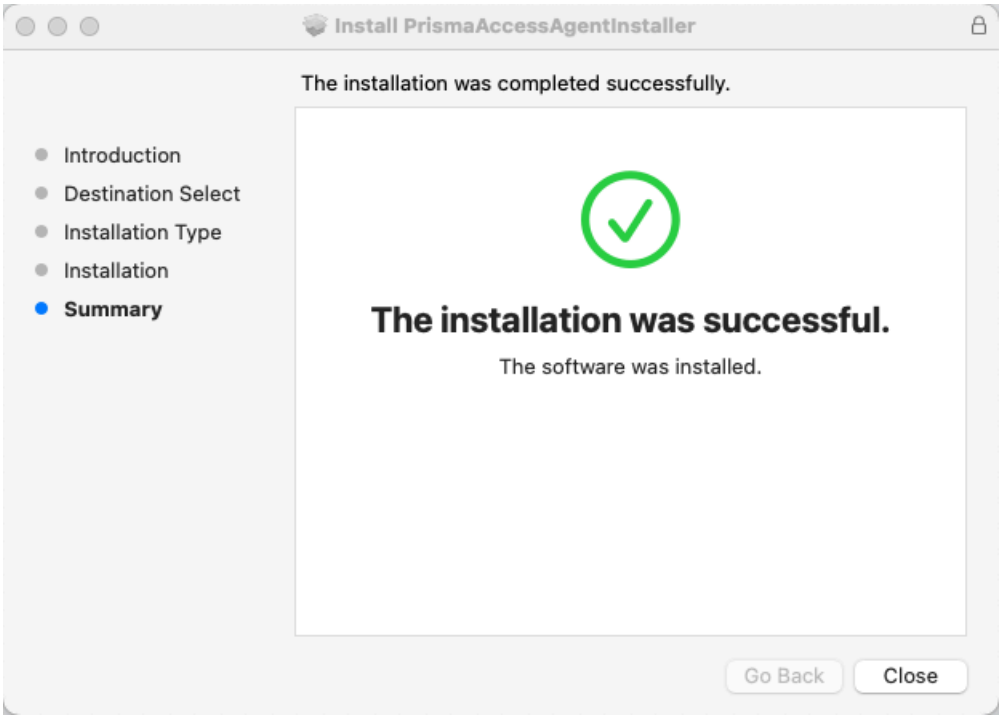
7. Si votre administrateur a activé la fonctionnalité pour appliquer les connexions Prisma Access pour l'accès au réseau, vous serez invité à ajouter une configuration pour filtrer le contenu du réseau. Pour continuer, cliquez sur **Allow (Autoriser)**.



 ©2025 Palo Alto Networks, Inc.

En faisant cela, vos connexions réseau seront filtrées et surveillées à des fins de sécurité.

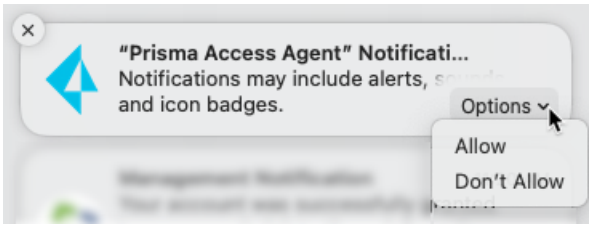
8. Une fois l'installation terminée, cliquez sur **Close (Fermer)** pour fermer le programme d'installation.



9. Si votre administrateur a configuré l'agent pour qu'il installe l'agent DEM autonome avec Prisma Access Agent, cliquez sur **OK** pour ne plus être invité.
10. Cliquez sur la fenêtre contextuelle Notifications de Prisma Access Agent pour ouvrir la fenêtre des préférences Notifications.

STEP 3 | Si vous y êtes invité, activez les notifications de Prisma Access Agent.

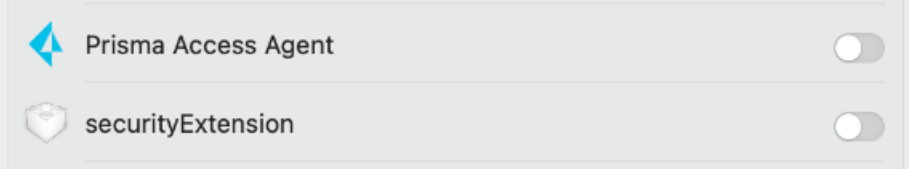
Lorsque la fenêtre contextuelle Notifications de Prisma Access Agent s'affiche sur votre bureau, déplacez votre curseur sur la fenêtre contextuelle et sélectionnez **Options** > **Allow (Autoriser)**.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Pour que Prisma Access Agent puisse accéder aux données dans le navigateur Safari, vous devez accorder un accès complet au disque à l'Extension de sécurité et à Prisma Access Agent.

1. Dans macOS, sélectionnez **System Settings (Paramètres système)** > **Privacy & Security (Confidentialité et sécurité)** > **Full Disk Access (Accès complet au disque)**. Activez **Prisma Access Agent** et **securityExtension** dans la liste des applications.



2. À l'invite, cliquez sur **Quit & Reopen (Quitter et rouvrir)** Prisma Access Agent pour que les modifications prennent effet.

Installer Prisma Access Agent (Windows)

Pour installer Prisma Access Agent manuellement sur votre périphérique Windows :

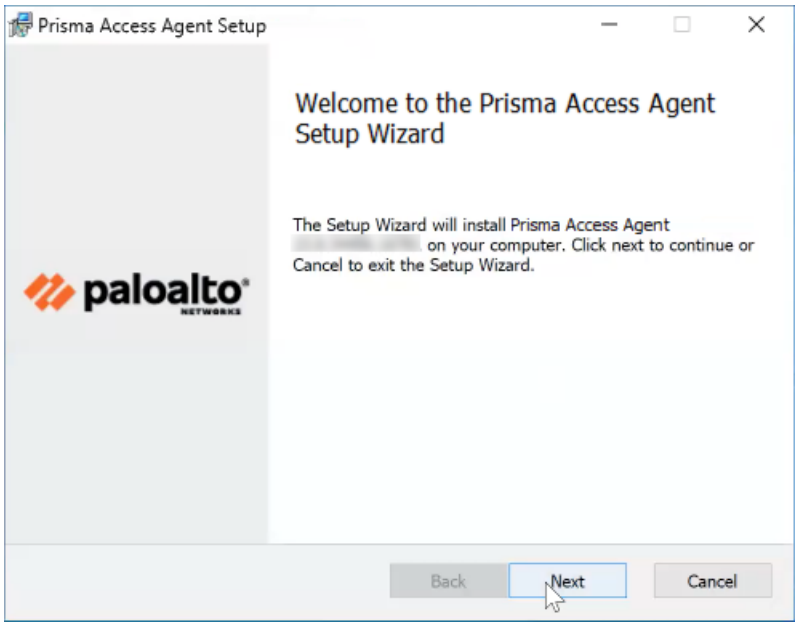
STEP 1 | Obtenez le package Prisma Access Agent que votre administrateur vous a fourni. Le nom du package est selon le format suivant :

`PrismaAccessAgent_x64_<version>.msi`

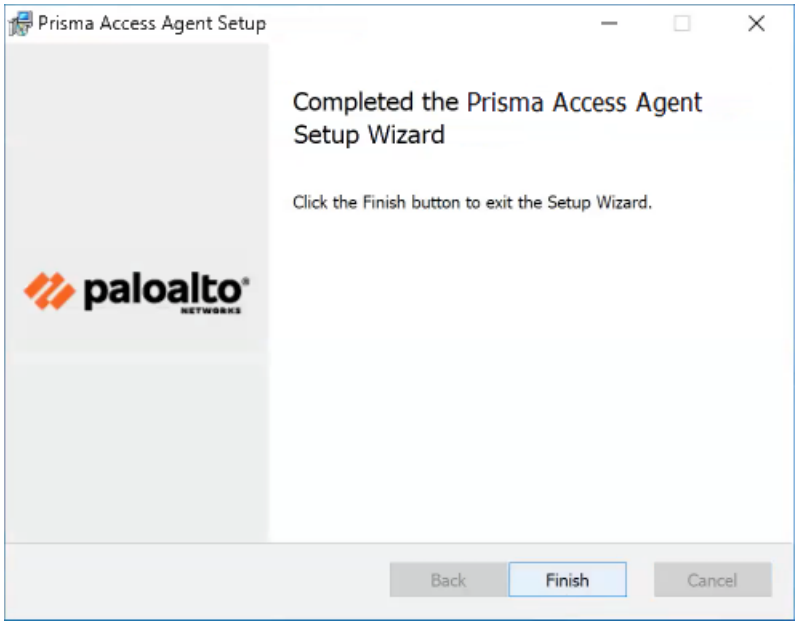
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Dans votre dossier Téléchargements (ou celui dans lequel vous avez placé le package d'installation), double-cliquez sur l'icône du package d'installation et suivez les instructions pour installer Prisma Access Agent.

1. Lorsque l'assistant d'installation s'affiche, cliquez sur **Next (Suivant)** pour continuer.



2. Passez en revue le contrat de licence de l'utilisateur final, sélectionnez **I accept the terms in the License Agreement (J'accepte les termes du contrat de licence)**, puis cliquez sur **Next (Suivant)**.
3. Cliquez sur **Install (Installer)** pour démarrer l'installation.
4. Lorsque vous êtes invité à **allow this app to make changes to your device (autoriser cette application à apporter des modifications à votre périphérique)**, cliquez sur **Yes (Oui)**.
5. Une fois l'installation terminée, cliquez sur **Finish (Terminer)**.



 ©2025 Palo Alto Networks, Inc.

6. Si votre administrateur a configuré l'agent pour qu'il installe l'agent DEM autonome avec Prisma Access Agent, cliquez sur **OK** pour ne plus être invité.

Se connecter à Prisma Access Agent compatible avec l'accès à privilèges dynamique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access Agent	❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Accès à internet

Pour accéder au réseau, aux ressources, aux applications SaaS ou à l'Internet de votre organisation, connectez-vous à Prisma Access Agent à l'aide de vos informations d'identification de connexion.

Après vous être connecté à Prisma Access Agent, vous êtes automatiquement connecté à votre réseau à l'aide du meilleur emplacement Prisma Access (parfois appelé passerelle). Le meilleur emplacement est automatiquement choisi pour vous fournir les meilleures performances afin de permettre une meilleure expérience, comme la visualisation de sites web dans votre propre langue. Lorsque votre périphérique est situé en dehors du réseau de votre organisation, l'agent trouve le meilleur emplacement pour vous offrir les meilleures performances lors de la connexion au réseau.

Avant de commencer, Prisma Access Agent doit être installé sur votre périphérique. En règle générale, votre administrateur déploiera Prisma Access Agent sur le périphérique que vous utilisez pour accéder au réseau, aux ressources et aux applications de votre organisation. L'agent est configuré en fonction des règles de politique définies par votre administrateur et déployées sur votre périphérique. Toutefois, si votre administrateur n'a pas déployé Prisma Access Agent sur votre périphérique, vous devrez l'installer manuellement.

Selon la façon dont Prisma Access est configuré dans votre organisation, votre administrateur doit vous fournir les informations de connexion suivantes :

- Le nom du serveur Prisma Access hébergeant le service qui gère votre Prisma Access Agent. Il peut y avoir plusieurs serveurs en fonction de la configuration de Prisma Access.
- Le nom des projets sur lesquels vous travaillez si votre organisation utilise l'*accès à privilèges dynamique*. L'accès à privilèges dynamique vous permet d'accéder au réseau et aux ressources de votre organisation en fonction du projet auquel vous êtes affecté. Ainsi, vous ne risquez pas d'accéder accidentellement aux ressources d'un autre projet. Si vous travaillez sur plusieurs projets, vous pouvez facilement changer de projet.



Selon les paramètres de votre système d'exploitation, les icônes et l'interface de l'application peuvent s'afficher en mode sombre ou en mode clair.

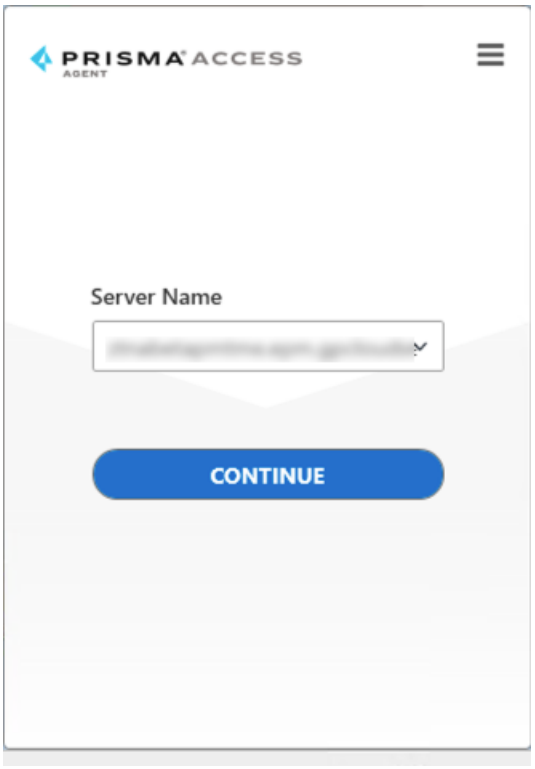
Connectez-vous à Prisma Access Agent en procédant comme suit :

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Lancez Prisma Access Agent en cliquant sur l'icône Prisma Access Agent dans la barre de menus macOS ou la barre des tâches Windows.

STEP 2 | Si vous y êtes invité, saisissez ou sélectionnez le **Server Name (Nom du serveur)** du serveur Prisma Access fourni par votre administrateur, puis cliquez sur **Continue (Continuer)**.

Le format du nom du serveur est **<example.domain.com>** sans le protocole **https://**. La longueur maximale du nom du serveur est de 256 caractères.



STEP 3 | Saisissez le nom du projet que votre administrateur vous a envoyé, puis sélectionnez **Continue (Continuer)**.

La longueur maximale du nom du projet est de 32 caractères.

STEP 4 | Dans la page de connexion qui s'affiche dans votre navigateur web par défaut, connectez-vous à l'application d'ouverture de session unique (SSO) de votre organisation, comme Okta ou Azure Active Directory (AD), en saisissant vos informations d'identification de connexion pour votre organisation.

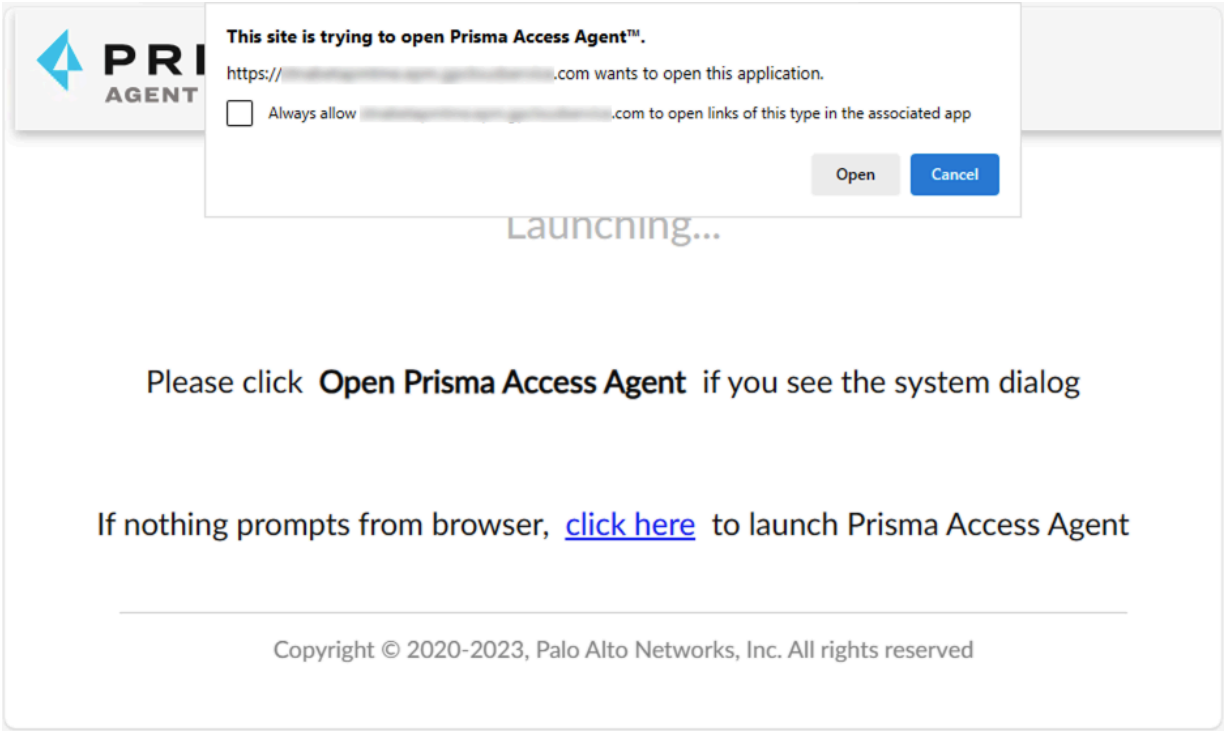
Si votre administrateur a activé l'authentification multifacteur (MFA), vous devrez effectuer une vérification supplémentaire dans le navigateur lorsque vous vous connectez.

STEP 5 | Lorsque votre navigateur web vous y invite, cliquez sur **Open (Ouvrir)**.

Si vous ne souhaitez pas que le navigateur vous invite à vous connecter la prochaine fois, sélectionnez **Always allow (Toujours autoriser) <site> to open these types of links in the**

 ©2025 Palo Alto Networks, Inc.

associated app (à ouvrir ce type de liens dans l'application associée), puis cliquez sur **Open (Ouvrir)** (si cela est pris en charge par votre navigateur web).



STEP 6 | Patientez pendant que Prisma Access Agent se connecte à Prisma Access.



 ©2025 Palo Alto Networks, Inc.

STEP 7 | Après vous être connecté, vous êtes automatiquement connecté au meilleur emplacement Prisma Access disponible. Si vous vous êtes connecté au moyen d'un projet, vous êtes connecté au meilleur emplacement disponible pour ce projet.

Vous pouvez désormais accéder aux ressources et aux applications SaaS de votre organisation, et de bénéficier d'un accès sécurisé à Internet.

*Si votre administrateur a activé le mode **Always On (Toujours actif)** pour Prisma Access Agent, vous ne pouvez pas vous déconnecter de Prisma Access en raison de la politique de votre organisation. Cependant, vous pouvez toujours changer d'emplacement Prisma Access.*

*Si votre administrateur a activé le mode **On Demand (À la demande)** pour Prisma Access Agent, vous devez cliquer sur l'icône en forme de cadenas pour vous connecter à Prisma Access.*

Modifier les préférences pour l'accès à privilèges dynamiques activé Prisma Access Agent

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access Agent	☐ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ☐ Accès à internet

Utilisez la fenêtre des préférences du Prisma Access Agent pour afficher des informations sur votre périphérique et modifier les options de votre agent, telles que l'activation des notifications sur le bureau.

STEP 1 | Lancez Prisma Access Agent en cliquant sur l'icône Prisma Access Agent dans la barre de menu de macOS ou la barre des tâches de Windows.

STEP 2 | Cliquez sur le menu hamburger pour ouvrir la fenêtre des préférences.

STEP 3 | Dans la fenêtre des préférences, vous pouvez consulter les informations suivantes :

Icône	Description
	Votre nom d'utilisateur.

 ©2025 Palo Alto Networks, Inc.

Icône	Description
	L'emplacement Prisma Access auquel votre périphérique est connecté.
	L'adresse IP de l'emplacement Prisma Access.
	Le nom d'hôte ou l'adresse IP de l'interface d'administration (serveur) à laquelle vous êtes connecté. Vous pouvez cliquer sur l'icône plus (**+**) pour vous connecter à un autre serveur.
	Le projet auquel vous êtes connecté.

STEP 4 | Pour recevoir des notifications Prisma Access Agent dans la barre de menus (sous macOS) ou la barre des tâches (sous Windows), sélectionnez **Allow desktop notifications (Autoriser les notifications sur le bureau)**. Ce paramètre est activé par défaut.

Les notifications du bureau respecteront tous les paramètres « Ne pas déranger » que vous avez définis au moment de l'installation. Le système d'exploitation vous demandera d'autoriser les notifications de l'application Prisma Access Agent au moment de l'installation.

STEP 5 | Pour comprendre quelles données Prisma Access Agent collecte et la manière dont les informations sont utilisées, voir **Our Privacy Policy (Notre politique de confidentialité)**.

STEP 6 | Pour obtenir de l'aide lorsque vous rencontrez des difficultés avec l'application Prisma Access Agent, cliquez sur **Support Resources (Ressources d'assistance)**.

STEP 7 | Si votre administrateur le permet, vous pouvez cliquer sur**Sign Out (Se déconnecter)** pour vous déconnecter de Prisma Access Agent.

STEP 8 | Si votre administrateur a activé cette fonctionnalité, vous pouvez **Disable (Désactiver)** l'application Prisma Access Agent afin que vous puissiez passer à l'application GlobalProtect (si elle est installée sur votre périphérique).

STEP 9 | Consultez la version de votre Prisma Access Agent.

STEP 10 | Pour fermer la fenêtre, cliquez sur l'icône **X**.

Connecter l'accès à privilèges dynamique activé Prisma Access Agent vers un autre emplacement

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access Agent	❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Accès à internet

 ©2025 Palo Alto Networks, Inc.

Après vous être connecté à Prisma Access Agent, vous êtes automatiquement connecté au meilleur emplacement Prisma Access disponible. Si vous souhaitez modifier les emplacements, vous pouvez le faire à l'aide de la liste déroulante **Location (Emplacement)**.

STEP 1 | Lancez Prisma Access Agent en cliquant sur l'icône Prisma Access Agent dans la barre de menu de macOS ou la barre des tâches de Windows.

STEP 2 | Sélectionnez un autre **Location (Emplacement)**. Vous pouvez **Search (Rechercher)** un emplacement ou choisir un emplacement dans la liste.

La liste des emplacements disponibles est triée en fonction de la meilleure expérience en fonction du temps de réponse, de la disponibilité et d'autres facteurs. L'emplacement qui offre la meilleure expérience est répertorié comme **Best Location (Meilleur emplacement)**.

STEP 3 | Si votre administrateur a activé le mode **On Demand (À la demande)** pour Prisma Access Agent, cliquez sur l'icône de verrouillage pour vous connecter à l'emplacement nouvellement sélectionné. Sinon, Prisma Access Agent procède à des changements d'emplacement.

Changer de projet

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access Agent	❑ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ❑ Accès à internet

Si vous êtes affecté à plusieurs projets dans votre organisation, vous pouvez basculer vers un autre projet pour accéder au réseau et aux ressources associés à ce projet.

Si le projet vers lequel vous essayez de basculer est accessible depuis un serveur différent, vous devrez d'abord basculer sur ce serveur.

STEP 1 | Lancez Prisma Access Agent en cliquant sur l'icône Prisma Access Agent dans la barre de menu de macOS ou la barre des tâches de Windows.

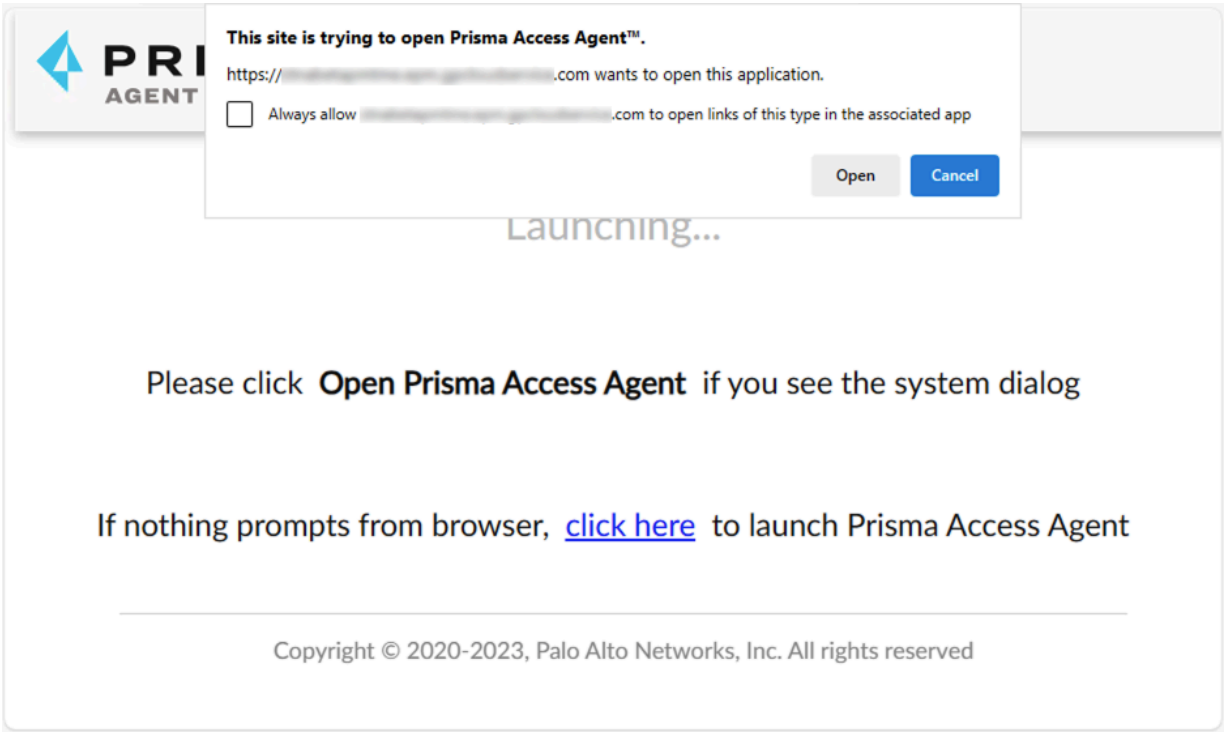
STEP 2 | Sélectionnez un autre **Project (Projet)**. Vous pouvez **Search (Rechercher)** un emplacement ou choisir un emplacement dans la liste.

Vous devez être attribué au projet vers lequel vous basculez.

STEP 3 | Si votre administrateur a activé le mode **On Demand (À la demande)** pour Prisma Access Agent, cliquez sur l'icône de verrouillage pour changer de projet. Sinon, Prisma Access Agent procède au changement de projet.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Chaque fois que vous changez de projet, Prisma Access Agent se déconnecte du projet en cours et se connecte au projet nouvellement sélectionné. Vous pourriez être invité à **Open (Ouvrir)** Prisma Access Agent à nouveau.



Connecter l'accès à privilèges dynamique activé Prisma Access Agent vers un autre serveur

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access Agent	☐ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ☐ Accès à internet

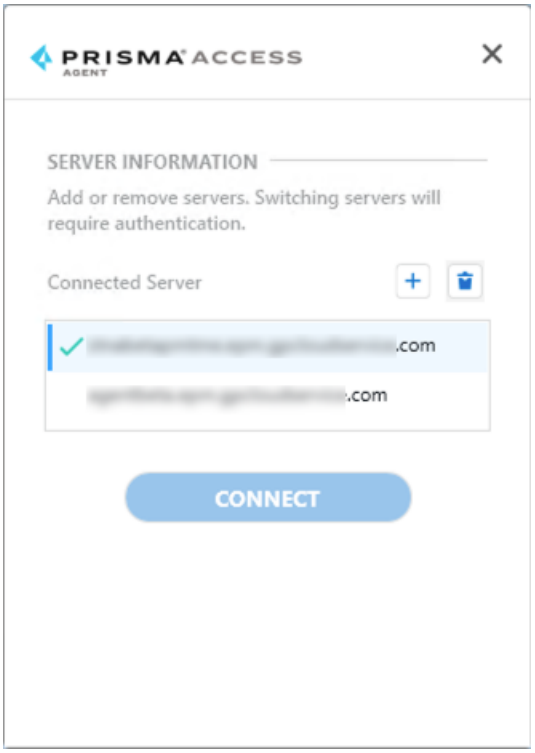
Une instance du serveur Prisma Access est également appelée *locataire*. Si vos administrateurs configurent plusieurs serveurs Prisma Access, vous pouvez vous connecter à un autre serveur pour accéder au réseau ou aux ressources via ce serveur.

Par exemple, vous devez travailler sur un autre projet, mais ce projet n'est accessible que sur un autre serveur. Vous devrez vous connecter à ce serveur avant de pouvoir passer à ce projet.

STEP 1 | Lancez Prisma Access Agent en cliquant sur l'icône Prisma Access Agent dans la barre de menu de macOS ou la barre des tâches de Windows.

STEP 2 | Modifiez les paramètres du serveur en sélectionnant l'icône de gestion du serveur.

STEP 3 | La fenêtre d’informations sur le serveur affiche le serveur auquel vous êtes connecté. Si d’autres serveurs sont répertoriés, vous pouvez en sélectionner un et vous y **Connect (Connecter)**.

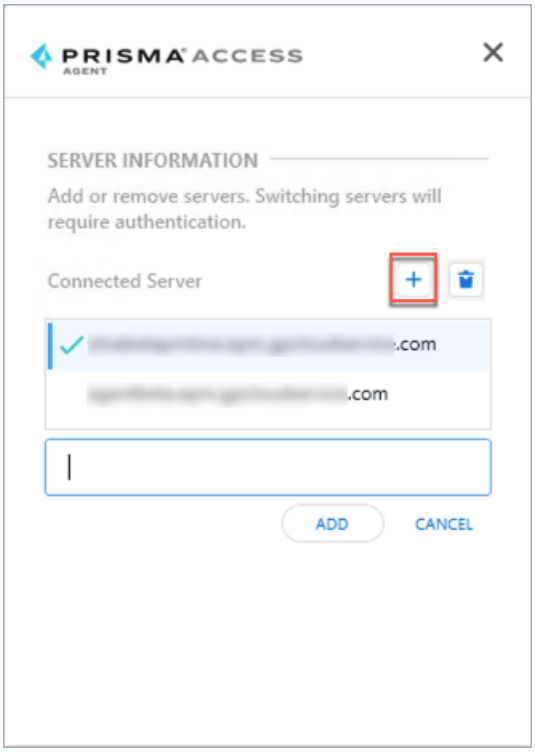


 ©2025 Palo Alto Networks, Inc.

STEP 4 | Si vous devez ajouter un serveur, suivez les étapes suivantes :

1. Cliquez sur le signe **+**.
2. Saisissez le nom du nouveau serveur (fourni par votre administrateur) et cliquez sur **Add (Ajouter)** pour l'ajouter.

   L nom du serveur est au format **<example.domain.com>** sans **https://**. La longueur maximale du nom du serveur est de 256 caractères. Le nombre maximum de serveurs autorisés sur cette page est de 20.



3. Après avoir ajouté le serveur, sélectionnez-le et cliquez sur **Connect (Se connecter)**.

STEP 5 | Lorsque la fenêtre de confirmation s'affiche, cliquez sur **Yes (Oui)** pour vous déconnecter du serveur actuel et vous connecter à l'autre serveur. Vous devrez fournir de nouveau vos identifiants d'ouverture de session unique.

STEP 6 | Lorsque vous y êtes invité, identifiez-vous au nouveau serveur en fournissant le nom du projet (le cas échéant).

Basculer entre Prisma Access Agent et l'application GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access Agent	☐ Périphériques de bureau macOS 12 ou version ultérieure ou périphériques de bureau Windows 10 version 2024 ou ultérieure ou Windows 11 ☐ Accès à internet

 ©2025 Palo Alto Networks, Inc.

Dans certaines organisations, Prisma Access Agent est installé sur des périphériques utilisateurs sur lesquels l'application GlobalProtect est déjà installée. Après l'installation de Prisma Access Agent, vous pouvez basculer entre Prisma Access Agent et l'application GlobalProtect au besoin.

Après être passé à l'application GlobalProtect, l'agent Prisma Access est à l'état désactivé. À l'état désactivé :

- Tout le trafic vers les emplacements Prisma Access est désactivé et l'authentification multifacteur (MFA) est désactivée.

  L'agent Prisma Access et GlobalProtect utilisent tous deux le même port GlobalProtect pour écouter les requêtes MFA (pour une authentification supplémentaire pour certaines applications), mais un seul agent peut utiliser le port à la fois. Lorsque vous désactivez l'agent Prisma Access, le port est libéré pour être utilisé par GlobalProtect.
- La communication avec le serveur persiste, de sorte que l'agent peut continuer à recevoir des mises à niveau de déploiement échelonné, des notifications ADEM et des requêtes shell à distance de l'administrateur et effectuer des vérifications HIP.
- Si elle a été configurée par l'administrateur, la fonction anti-altération continue de fonctionner pour protéger l'agent contre toute altération non autorisée.
- Sur les périphériques macOS, les extensions système et réseau de l'agent Prisma Access restent actives, de même que le filtre de contenu.
- Si vous passez à un autre serveur, l'agent Prisma Access est automatiquement réactivé. Si vous essayez de vous connecter à un emplacement Prisma Access alors que l'agent est désactivé, l'agent se connecte au meilleur emplacement.

Vous pouvez utiliser l'application de l'agent Prisma Access ou l'outil de ligne de commande Prisma Access (PACli) pour basculer entre les deux applications.

- Application de l'agent Prisma Access
- Ligne de commande Prisma Access (PACli)

Basculer entre Prisma Access Agent et l'application GlobalProtect (à l'aide de l'agent Prisma Access)

Basculer entre Prisma Access Agent et l'application GlobalProtect (à l'aide de l'outil PACli)

 ©2025 Palo Alto Networks, Inc.

Afficher et surveiller les utilisateurs de l’accès à privilèges dynamiques

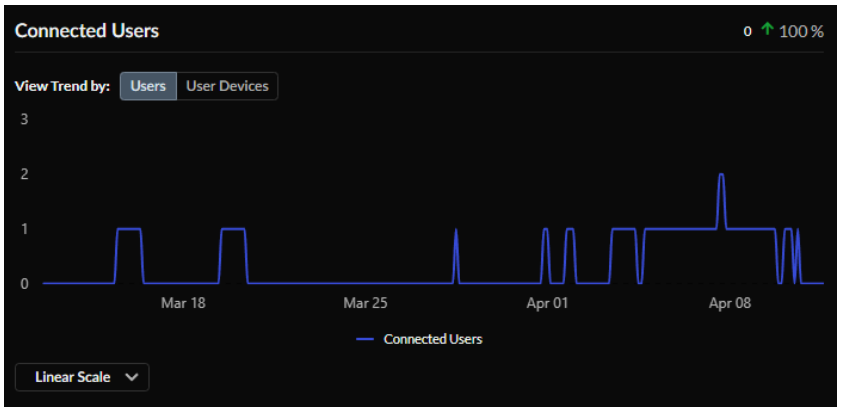
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access

L’accès à privilèges dynamiques permet à Prisma Access d’appliquer différentes règles de réseau et de politique de sécurité aux flux d’utilisateurs mobiles en fonction du projet sur lequel travaillent vos utilisateurs. Accédez à **Insights** > **Users (Utilisateurs)** dans le centre de commandes de Strata Cloud Manager pour afficher les informations d’accès basées sur les utilisateurs dans votre environnement.

Utilisateurs connectés

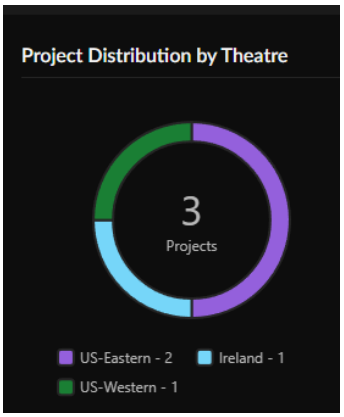
Affichez les **Connected Users (Utilisateurs connectés)** pour consulter les utilisateurs actuellement connectés ou les périphériques utilisateur connectés. La flèche vers le haut ou vers le bas compare cet intervalle de temps avec un intervalle de temps précédent pour déterminer la différence, en pourcentage, du nombre d’utilisateurs ou de périphériques connectés.

Sélectionnez **View Trend by Users (Afficher la tendance par utilisateurs)** pour afficher le nombre d’utilisateurs actuellement connectés à l’agent Prisma Access, puis cliquez sur **View Trend by User Devices (Afficher la tendance par périphérique utilisateur)** pour voir le nombre de périphériques utilisateur actuellement connectés à l’agent Prisma Access.

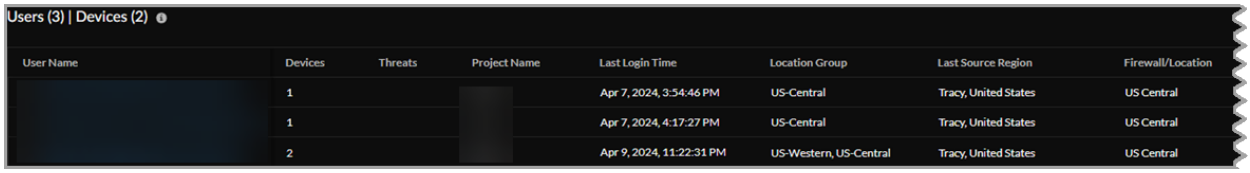


Consultez la **Project Distribution by Theatre (Répartition des projets par théâtre)** pour voir le nombre de projets par emplacement ou par salle.

 ©2025 Palo Alto Networks, Inc.



Le tableau **Users | Devices (Utilisateurs | Périphériques)** affiche le **Project Name (Nom du projet)** associé à chaque utilisateur et périphérique. Vous pouvez également voir combien de périphériques sont connectés par utilisateur, l'heure de la dernière connexion, le dernier emplacement source, le dernier emplacement Prisma Access connecté, le protocole Internet source et la famille et la version du système d'exploitation.

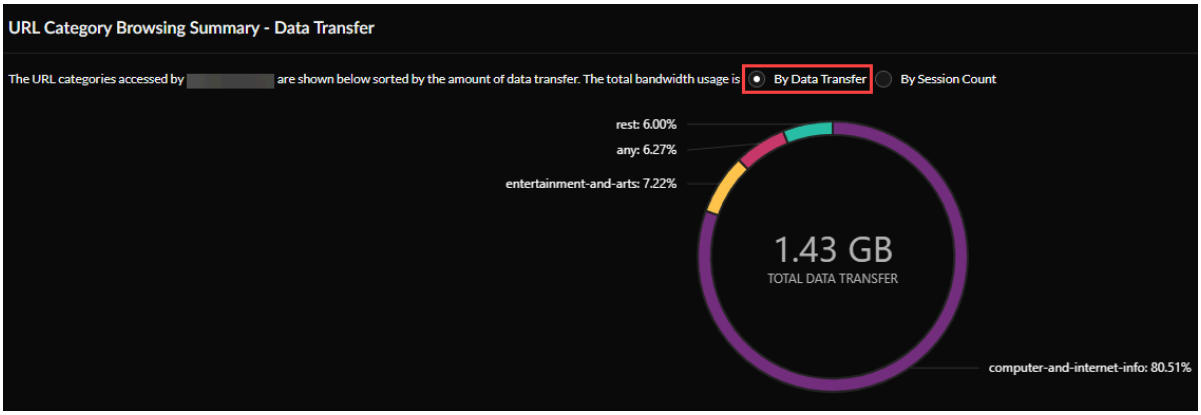


Sélectionnez n'importe quel **Project Name (Nom de projet)** pour accéder à la page **Projects (Projets)**.

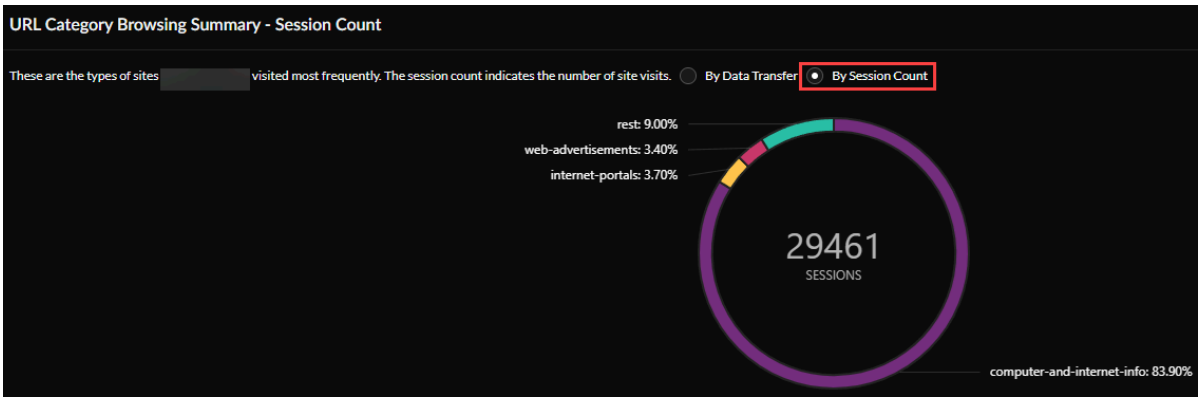
Sélectionnez n'importe quel **User Name (Nom d'utilisateur)** pour afficher les détails de l'utilisateur tels que **Activity (Activité)** et **Connectivity (Connectivité)**.

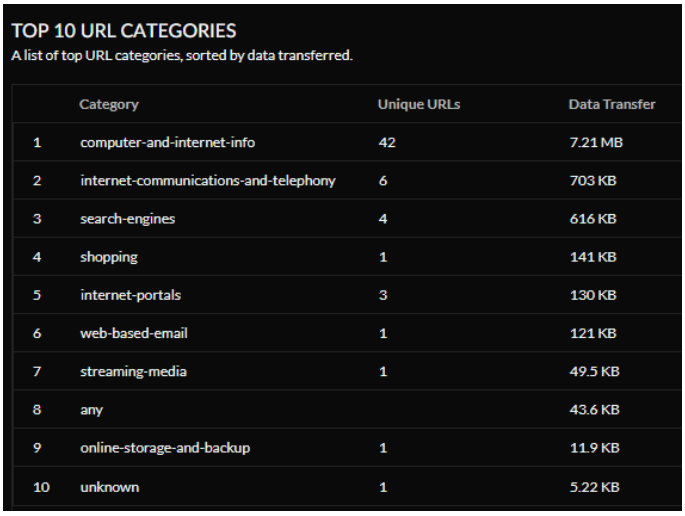
Activité

URL Browsing Category Summary – Data Transfer (Résumé de la catégorie de navigation URL) : affichez le résumé du transfert de données de votre catégorie de navigation **By Data Transfer (Par transfert de données)** ou **By Session Count (Par nombre de sessions)**. Vous pouvez également consulter une liste des **Top 10 URL Categories (Top 10 des catégories d'URL)**, triées par données transférées.



 ©2025 Palo Alto Networks, Inc.





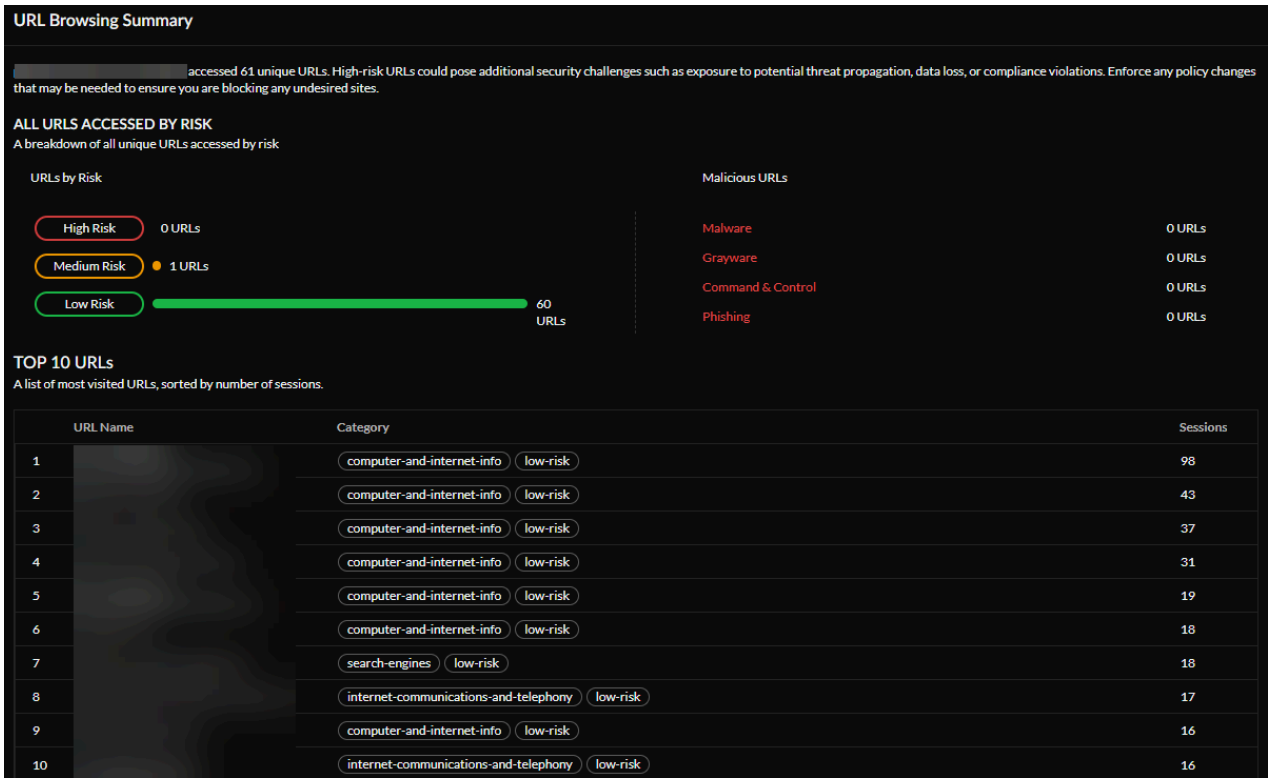
TOP 10 URL CATEGORIES

A list of top URL categories, sorted by data transferred.

	Category	Unique URLs	Data Transfer
1	computer-and-internet-info	42	7.21 MB
2	internet-communications-and-telephony	6	703 KB
3	search-engines	4	616 KB
4	shopping	1	141 KB
5	internet-portals	3	130 KB
6	web-based-email	1	121 KB
7	streaming-media	1	49.5 KB
8	any		43.6 KB
9	online-storage-and-backup	1	11.9 KB
10	unknown	1	5.22 KB

URL Browsing Summary (Résumé de navigation URL) : consultez votre résumé de navigation URL, y compris toutes les URL auxquelles vous avez accédé par risque. Vous pouvez afficher une répartition des URL par risque (élevé, moyen ou faible) et voir à combien d’URL malveillantes vous avez accédé. Vous pouvez également afficher une liste des **Top 10 URLs (Top 10 des URL)** visitées et le nombre de fois que vous avez visité chaque URL.

 ©2025 Palo Alto Networks, Inc.

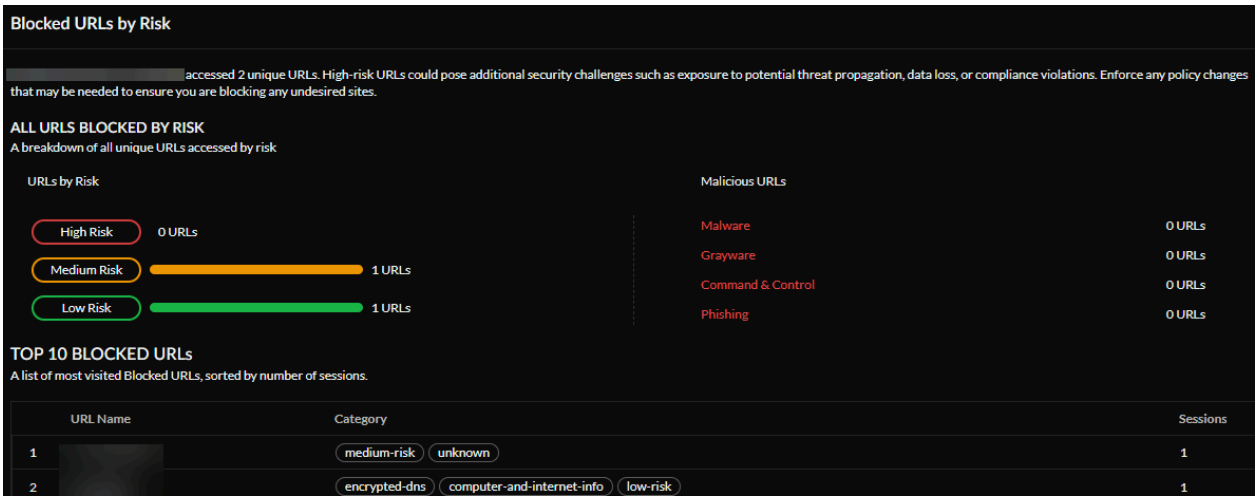


View URL Filtering Logs (Afficher les journaux de filtrage d’URL) : sélectionnez **View URL Filtering Logs (Afficher les journaux de filtrage d’URL)** pour afficher les détails sur le total des données transférées. Les journaux fournissent une piste d’audit pour les événements de système, de configuration et de réseau. Les journaux de réseau enregistrent tous les événements où Prisma Access agit sur votre réseau.

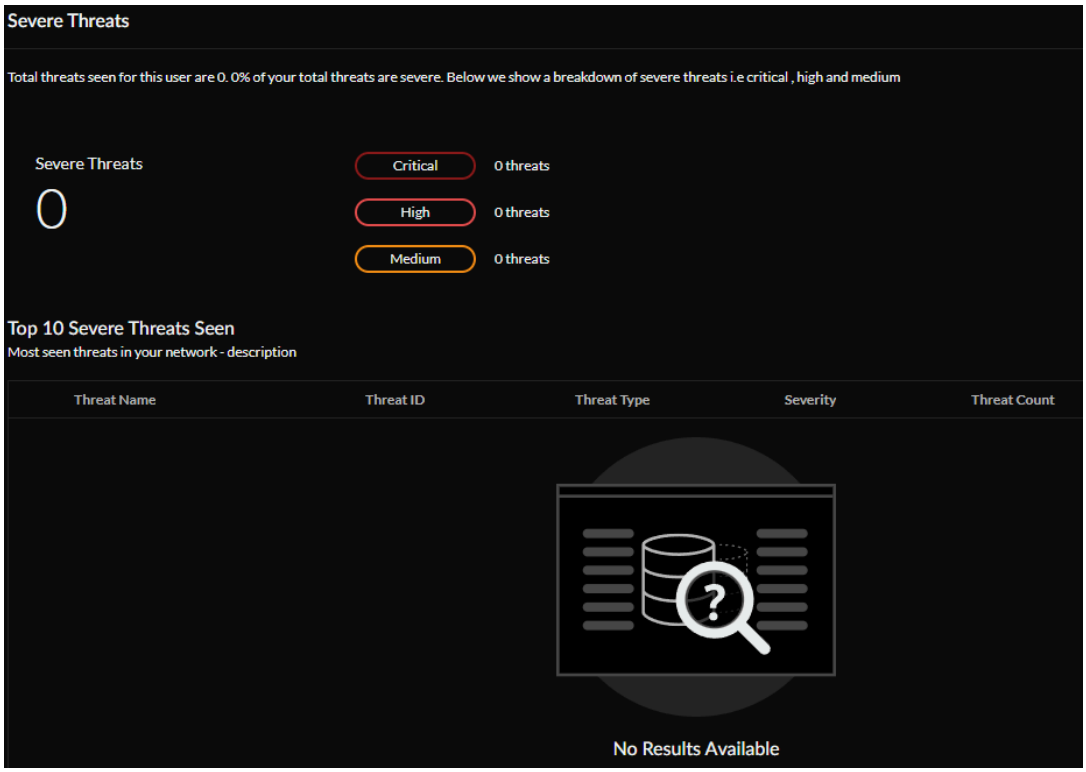
- Affichez toutes les données de journaux ou utilisez la liste déroulante pour filtrer par **Firewall/ URL (Pare-feu/URL)**, **Common (Commun)**ou **Endpoint (Terminal)**. Chacun de ces filtres dispose également de plusieurs sous-filtres parmi lesquels choisir.
- Saisissez une requête de journal. Cliquez dans ce champ pour afficher une sélection de requêtes pour commencer et créer votre requête.
- Sélectionnez une plage horaire. La valeur par défaut est supérieure à 60 minutes.
- Sélectionnez **Log Settings (Paramètres des journaux)** pour afficher le tableau de bord du service de journalisation Strata. Le service de journalisation Strate gère le mécanisme de fourniture des journaux.

Blocked URLs by Risk (URL bloquées par risque) : vérifiez si vous avez accédé ou tenté d’accéder à des URL bloquées par risque. Les URL à haut risque pourraient poser des problèmes de sécurité supplémentaires, tels que l’exposition à la propagation potentielle des menaces, la perte de données ou les violations de conformité. Appliquez toutes les modifications de politique nécessaires pour bloquer tous les sites indésirables. Vous pouvez également voir une liste des **Top 10 Blocked URLs (Top 10 des URL bloquées)** que vous avez le plus visitées, classées par nombre de sessions.

 ©2025 Palo Alto Networks, Inc.



Severe Threats (Menaces graves) : découvrez combien de vos menaces sont graves. Les menaces graves sont subdivisées en menaces critiques, élevées et moyennes. Vous pouvez également consulter une liste des **Top 10 Severe Threats Seen (Top 10 des menaces graves observées)** dans votre environnement.



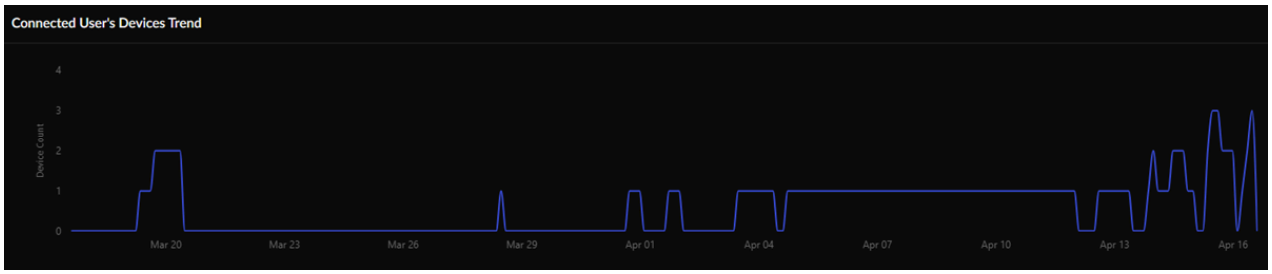
Connectivité

Sélectionnez n'importe quel nom de **User (Utilisateur)** pour afficher des informations sur la **Connectivity (Connectivité)** de l'utilisateur pendant la **Time Range (Plage horaire)** sélectionnée.

Active Projects (Projets actifs) : vous pouvez voir quels projets étaient actifs pendant la période sélectionnée et la date à laquelle chaque projet est devenu actif.

 ©2025 Palo Alto Networks, Inc.

Connected User's Devices Trend and Connected User's Devices (Tendance des périphériques des utilisateurs connectés et périphériques des utilisateurs connectés) : sur la page principale Users (Utilisateurs), vous pouvez voir tous les utilisateurs connectés et leurs projets. Sur la page **Connectivity (Connectivité)**, affichez la tendance des **Connected User's Devices (Périphériques de vos utilisateurs connectés)** individuels pendant l'intervalle de temps sélectionné et les détails sur **Connected User's Devices (Périphériques de vos utilisateurs connectés)**, tels que le nom du périphérique, la dernière adresse IP source de l'utilisateur, la dernière adresse IP privée, l'emplacement du dernier utilisateur, l'heure de la dernière connexion, l'heure de la dernière déconnexion et la durée de la dernière session.





Project Activity (Activité du projet) : affichez l'activité du projet d'un utilisateur par session. Vous pouvez voir l'état actuel d'une session, quand l'utilisateur s'est connecté à chaque projet, quand il s'est déconnecté et combien de temps a duré chaque session.



Total User Activity by Project (Activité totale de l'utilisateur par projet) : affichez le temps qu'un utilisateur a passé sur chaque projet pendant l'intervalle de temps sélectionné.

 ©2025 Palo Alto Networks, Inc.

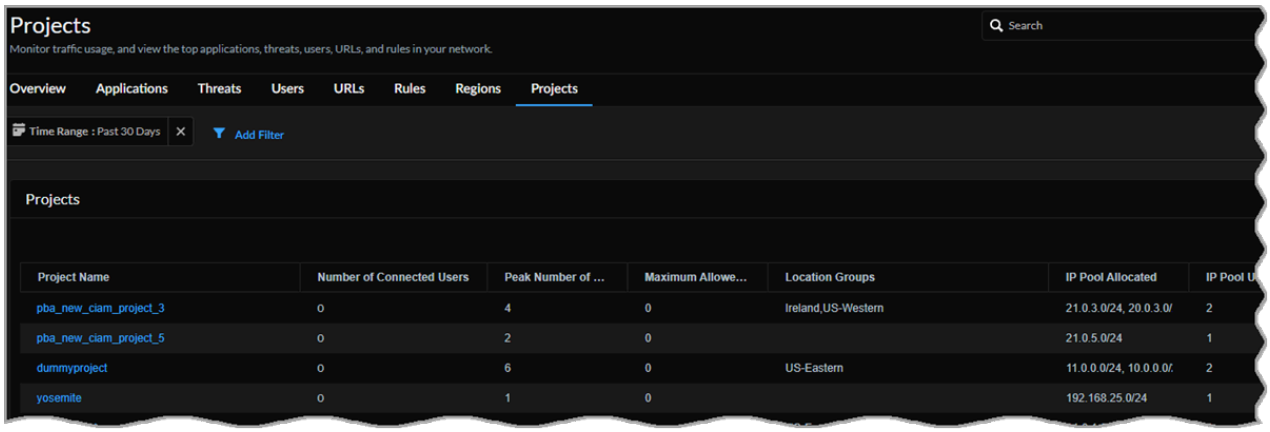
Afficher et surveiller les projets de l’accès à privilèges dynamiques

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Obtenez une visibilité sur votre déploiement de l’agent Prisma Access en utilisant Strata Cloud Manager pour surveiller l’activité des projets de vos utilisateurs. Accédez à **Activity Insights (Informations sur l’activité)** > **Projects (Projets)** dans le centre de commande de Strata Cloud Manager pour afficher les informations d’accès basées sur les projets dans votre environnement.

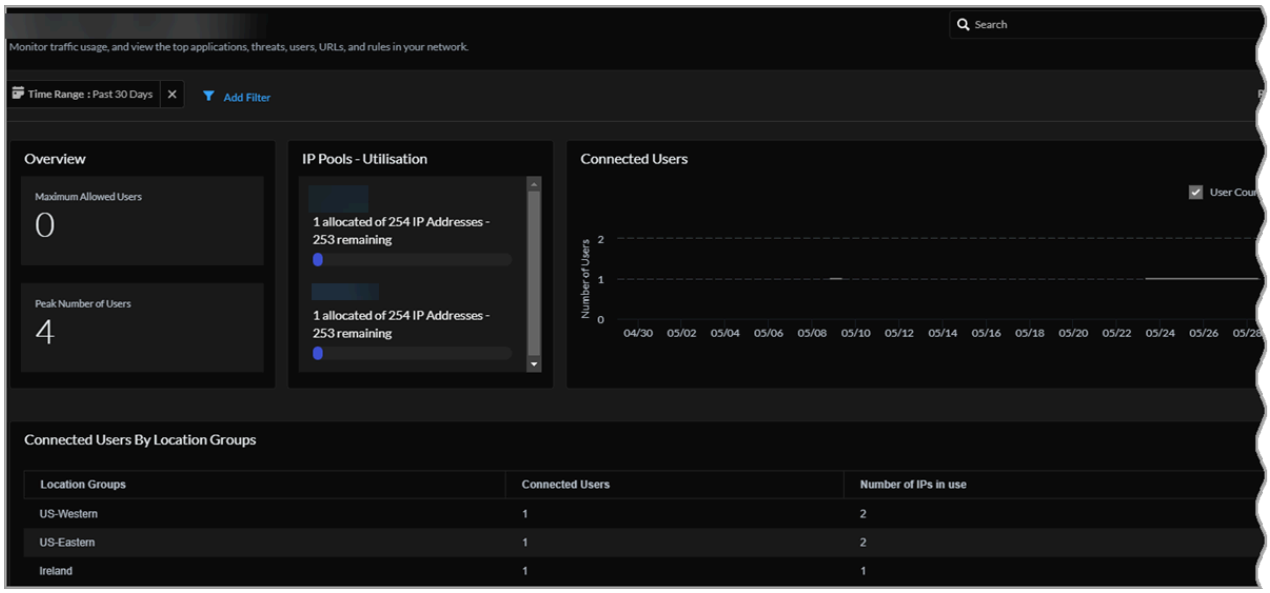
Projets

Le tableau **Projects (Projets)** fournit une vue d’ensemble des projets auxquels vos utilisateurs accèdent à l’aide de Prisma Access au cours de l’intervalle de temps sélectionné. Vous pouvez voir le nombre d’utilisateurs connectés de chaque projet, le nombre maximal d’utilisateurs, le nombre maximal d’utilisateurs autorisés, les groupes d’emplacements Prisma Access, le pool d’adresses IP alloué, le pool d’adresses IP utilisé, le nombre d’adresses IP disponibles et le dernier emplacement Prisma Access connecté.



Sélectionnez un **Project Name (Nom du projet)** pour accéder à la page de détails de ce projet. Le nom du projet (flouté dans l’image suivante) apparaît dans le coin supérieur gauche de la page.

©2025 Palo Alto Networks, Inc.

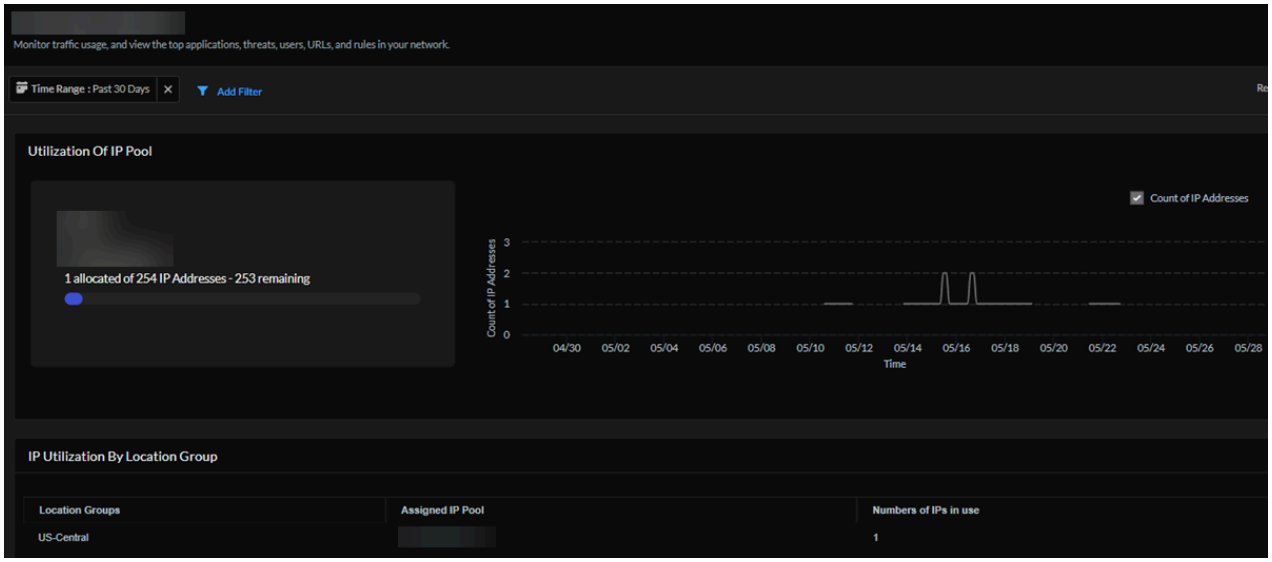


Vue d’ensemble

Sur la page des détails du projet, **Overview (Vue d’ensemble)** affiche le nombre maximal d’utilisateurs autorisés pour ce projet et le nombre maximal d’utilisateurs au cours de l’intervalle de temps sélectionné.

Pools d’adresses IP – Utilisation

Affichez le nombre d’adresses IP utilisées et le nombre d’adresses IP encore disponibles pour les pools de ce projet. Sélectionnez un pool d’adresses IP spécifique pour accéder à sa page de détails (voir l’image suivante), où vous pouvez voir l’utilisation de ce pool d’adresses IP, le nombre d’adresses IP utilisées et l’utilisation des adresses IP par groupe d’emplacements Prisma Access.



Utilisateurs connectés

Affichez un graphique des utilisateurs connectés pendant l’intervalle de temps sélectionné. Passez la souris sur n’importe quel point du graphique pour voir le nombre d’utilisateurs à ce point.

 ©2025 Palo Alto Networks, Inc.

Utilisateurs connectés par groupes d’emplacements

Consultez le nombre d’utilisateurs par le **Location Group (Groupe d’emplacements)** Prisma Access dans lequel ils se trouvent. Vous pouvez également voir le nombre d’adresses IP utilisées pour chaque **Location Group (Groupe d’emplacements)**.

©2025 Palo Alto Networks, Inc.

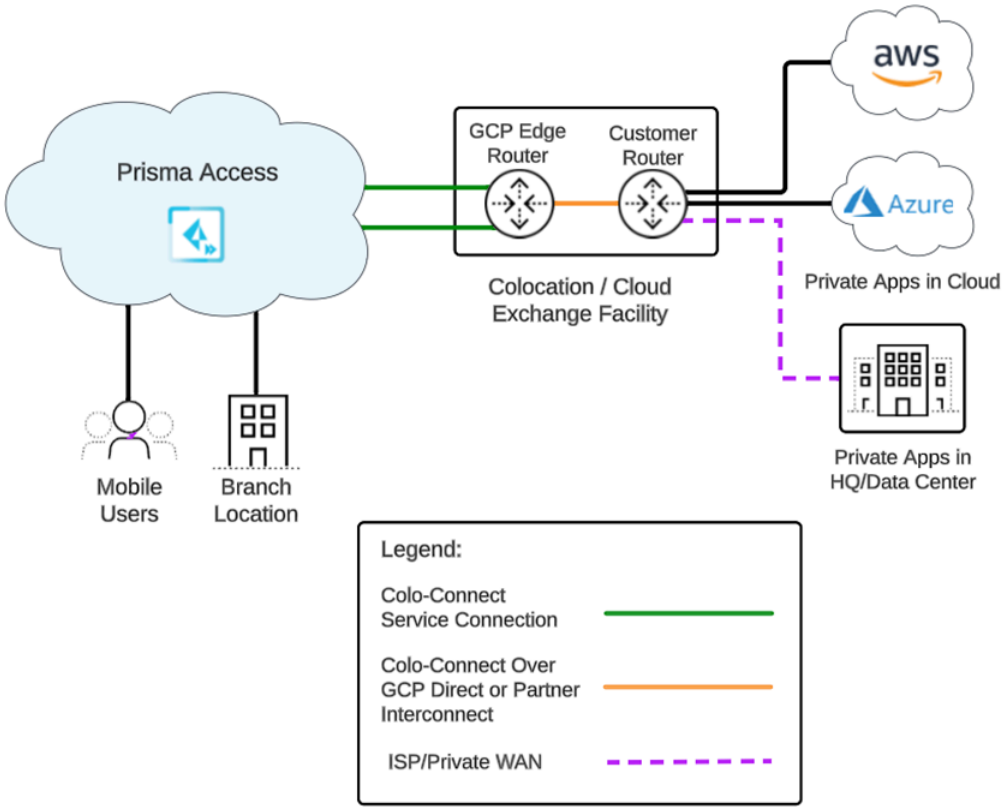
 ©2025 Palo Alto Networks, Inc.

Prisma Access Colo-Connect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Un déploiement Prisma Access (Managed by Panorama) exécutant une version minimale du plug-in Cloud Services 4.1 et une version minimale du plan de données 10.2.4 ❑ Une licence complémentaire Colo-Connect

Aujourd'hui, les grandes entreprises construisent des hubs de performance basés des centres de données en colocation pour atteindre des applications privées dans des architectures hybrides et multicloud en raison des exigences en matière de bande passante large et de faible latence. En règle générale, ces hubs incluent des interconnexions à un ou plusieurs fournisseurs de cloud et des connexions aux centres de données sur site via un WAN privé ou loué. Les hubs de performances peuvent acheminer le trafic entre le cloud public et l'infrastructure sur site à grande vitesse, et ils sont résilients en raison de l'infrastructure d'interconnexion sous-jacente.

Colo-Connect s'appuie sur le concept de hub de performance basé sur des centres de données en colocation, offrant des connexions privées à large bande passante (jusqu'à 20 Gbit/s) ainsi qu'une connectivité transparente de couche 2/3 à Prisma Access à partir de hubs performants existants. La figure suivante montre l'intégration de Prisma Access dans une instance GCP à l'aide de connexions aux services et d'interconnexions directes ou partenaires. Cette configuration limite l'exposition à Internet et permet l'utilisation de connexions privées pour la connectivité d'applications privées.



Prisma Access Colo-Connect exploite la technologie d'interconnexion GCP native du cloud pour fournir des connexions aux services à large bande passante à vos applications privées avec les capacités suivantes :

- Large bande passante (jusqu'à 20 Gbit/s) par région pour l'accès aux applications privées
- Prise en charge des interconnexions dédiées et partenaires à l'aide de Google Cloud Platform (GCP)
- Prise en charge de plusieurs rattachements VLAN par liaison d'interconnexion.
- Redondance régionale

 ©2025 Palo Alto Networks, Inc.

Cas d'utilisation de Colo-Connect

Prisma Access Colo-Connect fournit une connectivité bidirectionnelle à large bande passante pour sécuriser des applications privées, comme illustré dans les cas d'utilisation suivants.

Accès à large bande passante aux applications privées

Si votre organisation dispose d'une présence réseau dans un centre de données en colocation et que vous exploitez les installations de centres de données en colocation pour créer une connectivité privée aux applications hébergées sur site, dans le cloud public ou les deux, Prisma Access peut faire partie de cette infrastructure de centre de données en colocation via Colo-Connect. Vous pouvez configurer Colo-Connect à l'aide d'une interconnexion dédiée ou partenaire fournie par GCP pour obtenir un débit allant jusqu'à 20 Gbit/s par région pour l'accès aux applications privées.

Par exemple, vous avez un ou plusieurs centres de données ou emplacements du siège qui disposent d'une connectivité directe au centre de données en colocation, et vous souhaitez vous connecter à Prisma Access pour obtenir un accès sécurisé à large bande passante aux applications. Dans ce cas, vous pouvez utiliser une interconnexion partenaire avec Prisma Access Colo-Connect pour fournir aux utilisateurs un accès sécurisé aux applications. Étant donné que l'équipement du centre de données en colocation est appairé au cloud public ainsi qu'à votre centre de données, vous pouvez également fournir l'accès à toutes les applications privées hébergées dans le cloud public.

Colo-Connect coexiste avec les connexions aux services basées sur des tunnels IPSec existantes, donc si vous avez besoin de fournir un accès aux applications privées à des centres de données plus petits qui ne nécessitent pas de large bande passante et de débit multi-gigabit, vous pouvez également utiliser des connexions aux services vers ces centres de données. Vous pouvez configurer les connexions aux services à l'aide du routage BGP pour rendre votre réseau compatible avec les connexions aux services et les connexions Colo-Connect.

Connectivité privée pour les applications privées

Colo-Connect peut tirer parti d'un réseau privé pour que les utilisateurs puissent accéder aux applications privées au lieu d'y accéder via Internet, ajoutant ainsi un niveau supplémentaire de contrôle et de sécurité pour les applications privées.

Utilisation d'un fournisseur NaaS tiers

Dans ce cas d'utilisation, vous exploitez des fournisseurs de réseau en tant que service (Network as a Service, NaaS) tiers tels que Megaport et PacketFabric pour connecter le centre de données en colocation à vos applications exécutées dans des clouds publics ou avec des fournisseurs SaaS tels que salesforce.com ou Box. Vous souhaitez établir une connectivité réseau entre les réseaux tiers et Prisma Access pour fournir un accès à large bande passante aux services, clouds et applications connectés. Vous pouvez :

- Utiliser l'équipement réseau d'un fournisseur NaaS en tant que hub pour fournir une connectivité entre les utilisateurs et les applications s'exécutant dans des VPC de cloud public ou des fournisseurs SaaS publics dans une région donnée ;
- Établir une session BGP entre l'équipement réseau du fournisseur NaaS et Prisma Access.

 ©2025 Palo Alto Networks, Inc.

L'utilisation de solutions NaaS tierces avec Prisma Access Colo-Connect n'a pas été validée par Palo Alto Networks. Il est conseillé d'évaluer les fonctionnalités prises en charge auprès du fournisseur tiers, y compris la configuration d'une interconnexion à GCP et la création de tunnels GRE vers Prisma Access pour les connexions aux services Colo-Connect.

 ©2025 Palo Alto Networks, Inc.

En quoi Colo-Connect est-il différent des connexions aux services et du connecteur ZTNA ?

Palo Alto Networks propose trois façons de sécuriser l'accès aux applications privées : les connexions aux services, le connecteur ZTNA et Colo-Connect. Les connexions aux services et le connecteur ZTNA sécurisent tous les deux l'accès aux applications privées sur Internet, tandis que Colo-Connect établit une connexion privée vers votre centre de données. Consultez le tableau ci-dessous pour une comparaison de la bande passante et des facteurs de différenciation.

Type de déploiement			
Fonctionnalité	**Colo-Connect**	**Connecteur ZTNA**	**Connexions aux services**
Bande passante maximale par région de calcul	20 Gbit/s	10 Gbit/s	5 Gbit/s
Débit	Connectivité privée bidirectionnelle de 20 Gbit/s au centre de données	Jusqu'à 10 Gbit/s par centre de données	1 Gbit/s par connexion
Compatible avec les fournisseurs SDN/ NaaS tels qu'Equinix Cross-Connect et Megaport	Oui	Non	Non
Réseaux superposés dans les centres de données	Non	Oui	Non
Autres avantages	Intégration simple dans les déploiements existants hybrides et multicloud via Colo	Intégration simplifiée des applications privées dans les déploiements hybrides et multicloud	Prend en charge Active Directory sur site
Nécessite un déploiement sur site ?	Non	Oui	Non

©2025 Palo Alto Networks, Inc.

Caractéristiques et fonctionnalités non prises en charge par Colo-Connect

Les caractéristiques et fonctionnalités suivantes ne sont pas prises en charge par Colo-Connect :

- Configuration d'une connexion aux services Colo-Connect en tant que connexion aux services cible lors de l'utilisation de la redirection du trafic
- Prise en charge d'IPv6 pour l'accès aux applications privées
- Appairage eBGP sur IPv6

 ©2025 Palo Alto Networks, Inc.

Exigences et conditions préalables pour Prisma Access Colo-Connect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Un Prisma Access (Managed by Panorama) déploiement exécutant une version minimale du plug-in Cloud Services 4.1 et une version minimale du plan de données de 10.2.4 ❑ Une licence complémentaire Colo-Connect

Avant de commencer l'intégration et la configuration de Colo-Connect, prenez connaissance des informations requises et des conditions préalables en suivant cette liste de contrôle.

- ❑ Assurez-vous d'avoir accès au fournisseur d'installations Colo (par exemple, vous avez accès au portail client Equinix).
- ❑ Assurez-vous que votre CPE peut prendre en charge GRE et BGP.

  Les connexions aux services Colo-Connect utilisent des tunnels GRE.
- ❑ Décidez du type d'interconnexion que vous utiliserez pour Colo-Connect (un partenaire ou interconnexion dédiée).
  - **Interconnexion des partenaires**—Une touche d'appairage de Prisma Access est requise pour les interconnexions de partenaires. Vous recevez cette clé lors de l'intégration Prisma Access.

    Si vous créez une interconnexion de partenaires, assurez-vous que le fournisseur de services (SP) est un SP approuvé avec GCP et la connectivité entre le SP et le GCP est déjà établie.
  - **Interconnexion dédiée**—
    - Déterminez l'emplacement du Colo où le câble de connexion croisée sera connecté avant que vous ne commenciez l'intégration dans Prisma Access. L'emplacement Colo est nécessaire pour que Palo Alto Networks puisse commander le lien dédié
    - Familiarisez-vous avec le réseau de base Interconnexions afin de pouvoir configurer les circuits.
    - Après avoir provisionné l'interconnexion dédiée, vous devez la tester.
- ❑ **Exigences du sous-réseau**—Déterminez les sous-réseaux IPv4 RFC-1918 que vous utiliserez pour chaque connexion Colo-Connect par région. Prisma Access utilise ces sous-réseaux pour la communication interne et la mise en réseau.

  Rendez les sous-réseaux uniques parmi toutes les régions Colo-Connect d'un locataire donné. Le sous-réseau Colo-Connect ne peut pas chevaucher le Prisma Access sous-réseau infra et le pool d'utilisateurs mobiles. Utilisez une taille de sous-réseau minimale de /28.

 ©2025 Palo Alto Networks, Inc.

- **Exigences relatives à la liaison (interconnexion)**—Suivez ces instructions lors de la configuration des liens :
  - Chaque licence complémentaire Colo-Connect comprend une liaison d'une capacité de 10 Gbits/s. Vous avez besoin d'un minimum de deux liens, ce qui signifie que vous devez acheter un minimum de deux licences dans un déploiement Colo-Connect.
  - Intégrez deux liens dans chaque région.

    Ces deux liens doivent se trouver dans des zones de disponibilité différentes (domaines périphériques).
  - (Déploiements d'interconnexion dédiés uniquement) Si vous souhaitez intégrer plus de six liens dans un locataire, contactez votre représentant de compte ou partenaire Palo Alto Networks, qui contactera l'équipe d'ingénierie de la fiabilité du site (SRE) et soumettra une demande d'augmentation du quota pour un locataire donné.

- **Exigences de connexion**—
  - Embarquez deux connexions dans chaque région.

    Les deux connexions doivent se trouver dans des domaines de périphérie différents.
  - Les connexions en mode actif/sauvegarde ou actif/actif doivent avoir la même bande passante.
  - Décidez si vous souhaitez configurer vos connexions dans une configuration active/active ou active/sauvegarde.
- **Exigences de connexion aux services Colo-Connect**—
  - Chaque connexion aux services nécessite deux connexions.
  - Chaque connexion pour une connexion aux services donnée doit se trouver sur une liaison différente et un domaine de périphérie différent.
  - Notez les adresses que vous utiliserez comme adresses IP BGP avec colo-routeur et les adresses IP locales du tunnel GRE. Vous utilisez ces adresses lors de la création de la connexion aux services.
  - Les connexions aux services doivent se trouver sur le même type de liaison (liaisons d'interconnexion partenaires ou liaisons d'interconnexion dédiées).
- **Interopérabilité avec les connexions de service IPSec existantes**—Palo Alto Networks vous recommande vivement de déployer des connexions aux services basées sur des tunnels Colo-Connect et IPSec dans différentes régions. En outre, si vous migrez d'une connexion aux services basée sur un tunnel IPSec vers une connexion aux services Colo-Connect, vous devez planifier une fenêtre de maintenance. Une fois que vous avez migré d'une connexion aux services basée sur un tunnel IPSec vers une connexion de service Colo-Connect, supprimez la connexion aux services basée sur IPSec une fois que la connexion aux services Colo-Connect est opérationnelle et avant l'expiration de la fenêtre de maintenance.

 ©2025 Palo Alto Networks, Inc.

Configurer Prisma Access Colo-Connect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Un déploiement Prisma Access (Managed by Panorama) exécutant une version minimale du plug-in Cloud Services 4.1 et une version minimale du plan de données 10.2.4 ❑ Une licence complémentaire Colo-Connect

Prisma Access Colo-Connect comporte les composants suivants :

- **Colo** : l'installation de colocalisation qui fournit de l'espace de rack, de l'alimentation et de la connectivité aux réseaux hôtes, aux infrastructures de cloud privé et public, comme Equinix.
- **Interconnexion dédiée** : la connexion physique de couche 2 ou 3 dédiée entre votre routeur et un routeur de périphérie GCP dans une région de calcul GCP donnée. Une interconnexion dédiée fournit une connexion physique directe entre votre réseau sur site et le réseau Google.

  Les interconnexions sont appelées *Liens* dans l'interface utilisateur Prisma Access.
- **Attachement VLAN GCP** : connexion logique de couche 2 sur le lien qui sépare le trafic de toutes les autres connexions logiques partageant le même lien.

  Les attachements VLAN sont appelés *Connexions* dans l'interface utilisateur Prisma Access.
- **Interconnexion partenaire** : connexion physique de couche 3 entre un routeur appartenant à un fournisseur de services et un routeur de périphérie GCP dans une région de calcul GCP donnée. Une interconnexion partenaire fournit une connectivité entre vos réseaux sur site et VPC par le biais d'un fournisseur de services pris en charge.

  Colo-Connect prend en charge les interconnexions dédiées et partenaires.
- **Routeur Colo (client)** : le périphérique de routage de l'installation de Colo qui établit eBGP avec le routeur cloud GCP sur l'interconnexion de l'installation de Colo, ainsi qu'eBGP avec la connexion aux services Colo-Connect via le tunnel GRE. Il s'agit d'un routeur client pour une interconnexion dédiée, ou si le fournisseur de services dispose d'une connectivité de couche 2 avec GCP sur l'interconnexion partenaire. Le fournisseur de services est propriétaire du routeur Colo lorsqu'il dispose d'une connectivité de couche 3 avec le routeur cloud GCP.
- **Routeur de périphérie GCP** : l'équipement de périphérie du réseau GCP pour fournir une connectivité physique entre GCP et le réseau client/partenaire via Colo.
- **Routeur cloud** : la construction logicielle GCP dans le cloud qui établit des sessions BGP avec le périphérique réseau (par exemple, un routeur ou un pare-feu de couche 3) dans Colo et achemine le trafic entre Prisma Access et votre réseau. Vous n'êtes pas obligé de configurer ce composant. Cela se fait automatiquement par Prisma Access.

Pour configurer Colo-Connect, vous devez d'abord recueillir des informations sur votre environnement réseau existant et vous assurer que tous les composants réseau requis sont en place. Assurez-vous d'avoir tous les prérequis ; puis déployez Colo-Connect dans le réseau de votre organisation à l'aide d'un partenaire ou d'une interconnexion dédiée.

 ©2025 Palo Alto Networks, Inc.

- Strata Cloud Manager
- Panorama

Configurer Prisma Access Colo-Connect (Strata Cloud Manager)

Pour configurer Colo-Connect, vous devez d'abord rassembler des informations sur votre environnement réseau existant et vous assurer que vous disposez de tous les composants réseau requis. Assurez-vous d'avoir tous les prérequis ; puis déployez Colo-Connect dans le réseau de votre organisation à l'aide d'un partenaire ou d'une interconnexion dédiée.

Configurer Prisma Access Colo-Connect — Déploiements à l'aide d'interconnexions partenaires

Pour configurer Prisma Access Colo-Connect à l'aide d'une interconnexion partenaire, procédez comme suit.

STEP 1 | Créez des sous-réseaux pour vos connexions Colo-Connect.

Vous utilisez les sous-réseaux que vous créez ici dans les connexions et connexions aux services que vous créez dans les étapes ultérieures.

1. Depuis Strata Cloud Manager, accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Colo-Connect**.
2. Cliquez sur **Add Prefix (Ajouter un préfixe)** et ajoutez un sous-réseau Colo-Connect à un emplacement Prisma Access pour celui-ci.

   Consultez ici la liste des emplacements Colo-Connect pris en charge. Entrez un sous-réseau minimum de /28.
3. (Facultatif) Si vous prévoyez de créer des instances Colo-Connect pour plus d'un emplacement, ajoutez d'autres sous-réseaux par emplacement.

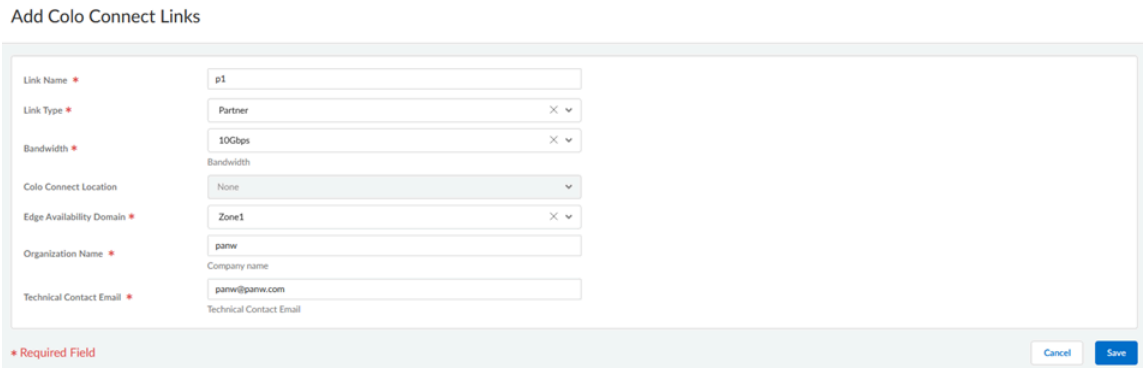
   Vous pouvez configurer un sous-réseau par emplacement.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Ajoutez un nouveau lien Colo-Connect (également appelé *interconnexion*).

1. Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Colo-Connect** et **Add Link (Ajouter un lien)**.
2. Donnez au lien un **Link Name (Nom de lien)** unique.
3. Sélectionnez une interconnexion **Partner (Partenaire)** comme **Link Type (Type de lien)**.
4. Spécifiez les paramètres restants du lien Colo-Connect.
   - Sélectionnez **10Gbps (10 Gbit/s)** ou **20Gbps (20 Gbit/s)** pour la **Bandwidth (Bande passante)**.
   - Sélectionnez **Zone1** ou **Zone2** pour **Edge Availability Domain (Domaine de disponibilité périphérique)**. Prenez cette valeur dans la zone GCP utilisée pour votre domaine de disponibilité périphérique.
   - Entrez l'**Organization Name (Nom de l'organisation)** à utiliser pour ce lien.
   - Entrez l'**Email (E-mail)** à utiliser pour ce lien. Toute adresse e-mail est acceptable.



5. Répétez les étapes 2.a à 2.d et créez un autre lien avec un **Edge Availability Domain (Domaine de disponibilité périphérique)**.

STEP 3 | Créez les connexions (également appelées *attachements VLAN*) pour Colo-Connect.

1. Accédez à **Workflows (Flux de travail)** > **Configuration de Prisma Access (Prisma Access Setup)** > **Colo-Connect** et **Add Connection (Ajouter une connexion)**.
2. Configurez les paramètres de connexion.
   - Entrez un **Connection Name (Nom de connexion)** unique.
   - Sélectionnez un **Link Name (Nom de lien)** parmi les liens que vous avez configurés lors d'une étape précédente.

     Vous n'avez pas besoin d'entrer un **VLAN ID (ID de VLAN)**. Il n'est pas configurable pour les VLAN créés sur des interconnexions partenaires.
   - Sélectionnez une **Bandwidth (Bande passante)** pour la connexion.

     Vous pouvez choisir entre **1 Gbps (1 Gbit/s)**, **2 Gbps (2 Gbit/s)**, **5 Gbps (5 Gbit/s)**, **10 Gbps (10 Gbit/s)** ou **20 Gbps (20 Gbit/s)**.

     Si vous configurez plusieurs connexions pour une interconnexion, assurez-vous que la bande passante totale des connexions ne dépasse pas la bande passante de l'interconnexion. Par exemple, avec une interconnexion partenaire de 10 Gbit/s, vous

 ©2025 Palo Alto Networks, Inc.

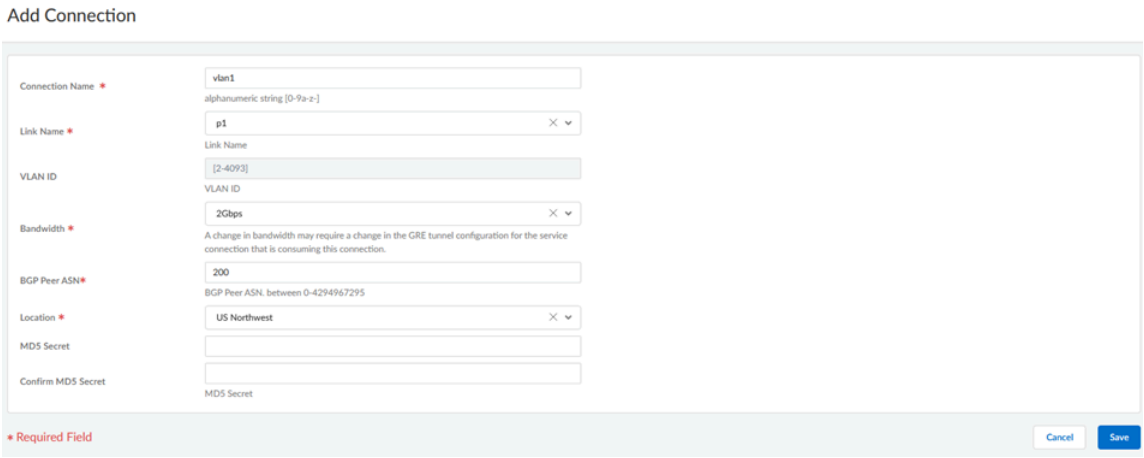
pouvez configurer 10 connexions de 1 Gbit/s chacune, mais vous ne pouvez pas dépasser 10 Gbit/s au total pour toutes les connexions.

Si votre déploiement nécessite plus de 16 connexions, contactez votre équipe de compte Palo Alto Networks, qui ouvrira un dossier SRE pour répondre à la requête.

- Entrez un **BGP Peer ASN (ASN homologue BGP)**.

  Entrez le numéro de système autonome (AS) pour le routeur sur site client dans le Colo. La plage se situe entre 1 et 4294967295.
- Sélectionnez le **Location (Emplacement)** parmi les noms de connexion que vous avez créés lors d'une étape précédente.

  Vous devez avoir déjà ajouté un sous-réseau pour tout emplacement que vous spécifiez.
- (Facultatif) Entrez le **MD5 Secret (Secret MD5)** de BGP.



3. Continuez à créer des connexions jusqu'à ce qu'elles soient terminées.

   Créez deux connexions. Les deux connexions doivent être dans la même région et une connexion doit être dans une zone distincte. Vous utilisez ces connexions dans les connexions aux services que vous créez dans une étape ultérieure.

STEP 4 | **Push Config (Transmettre la configuration)**.

Actualisez le navigateur une fois la tâche de validation terminée pour afficher les clés de couplage sous **Connections (Connexions)**.

STEP 5 | Récupérez la **Pairing Key (Clé de couplage)** et complétez la configuration de votre interconnexion partenaire dans GCP.

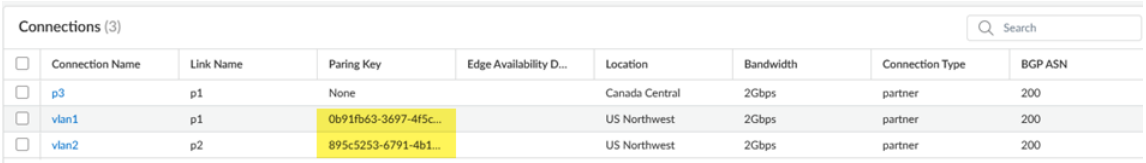
Vous utilisez cette clé de couplage lorsque vous configurez l'interconnexion partenaire dans le Colo.

Lors de la première connexion, le **Status (État)** dans la zone **Connections (Connexions)** affiche un **Status (État)** de **PENDING_PARTNER** et un **BGP Status (État BGP)** de **DOWN (INACTIF)**.

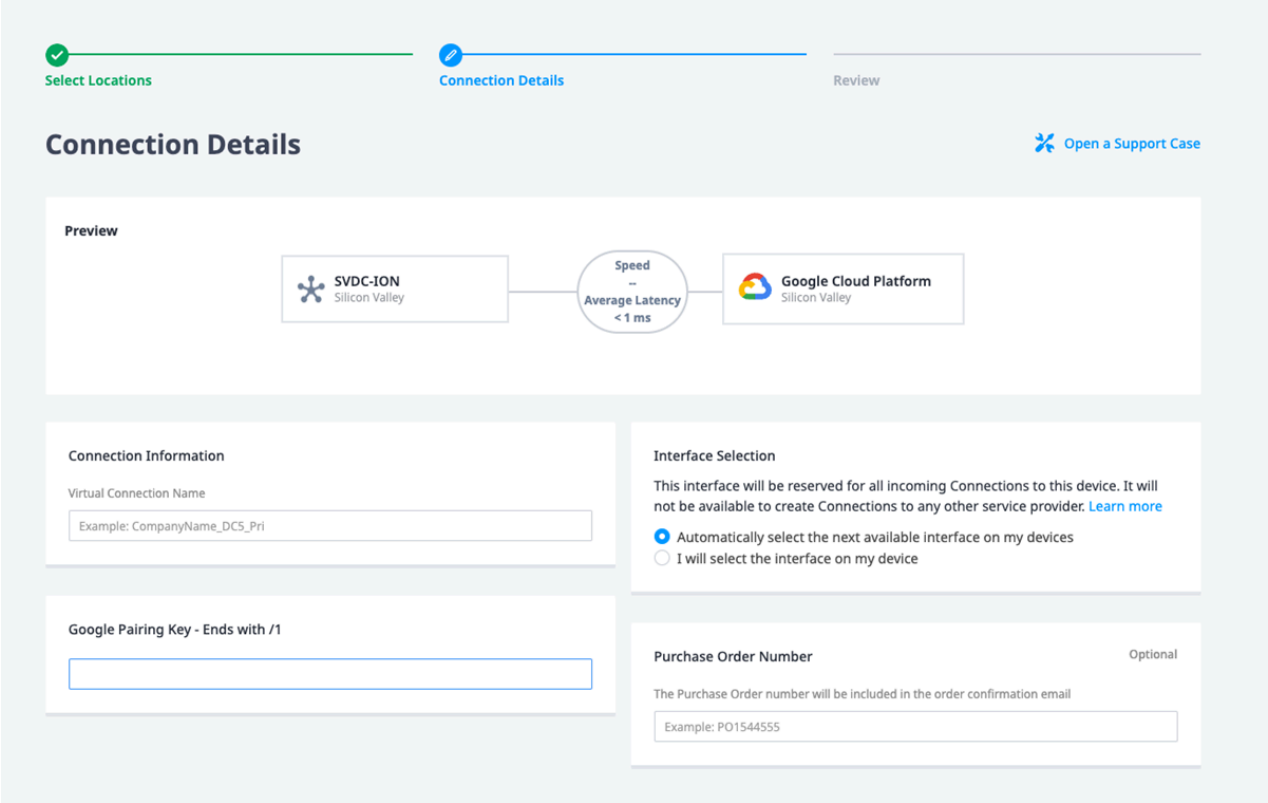
 ©2025 Palo Alto Networks, Inc.

Pour mettre l'état de la connexion sur **ACTIVE (ACTIF)**, récupérez la clé de couplage et l'entrée dans la connexion au Colo.

1. Accédez à **Workflows (Flux de travail)** > **Configuration de Prisma Access (Prisma Access Setup)** > **Colo-Connect** > **Connections (Connexions)** et copiez la **Pairing Key (Clé de couplage)**.



2. Créez une nouvelle connexion VLAN dans le Colo.



3. Collez la clé de couplage dans le VLAN de Colo.

   GCP détecte quand la clé de couplage est consommée, met l'état du VLAN sur **ACTIVE (ACTIF)** et génère l'adresse IP de BGP que vous pouvez configurer sur votre routeur local dans le Colo. Prisma Access utilise ces IP pour lancer une contiguïté eBGP sur chaque VLAN associé entre le routeur Colo et le routeur cloud GCP.

STEP 6 | Créez un routage eBGP sur le routeur client (Colo) pour la connexion Colo-Connect.

Vous devez configurer l'appairage BGP pour assurer la connectivité entre le routeur client et le routeur cloud.

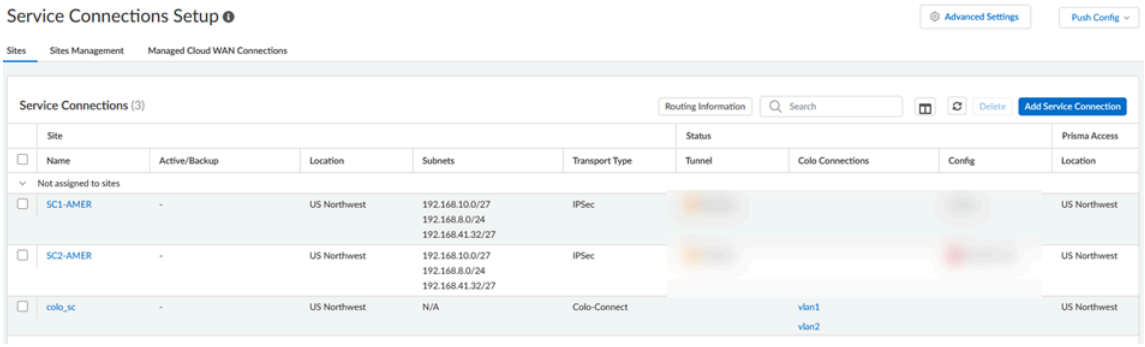
STEP 7 | Configurez les connexions aux services à utiliser avec Colo-Connect.

STEP 8 | **Push Config (Transmettre la configuration)**.

 ©2025 Palo Alto Networks, Inc.

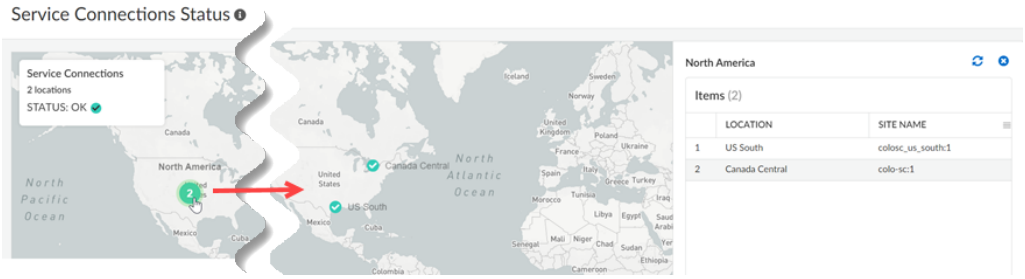
STEP 9 | Vérifiez l'état des connexions Colo-Connect.

1. Pour vérifier l'état d'une connexion aux services utilisée par une connexion Colo-Connect, accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connection (Connexion aux services)**.



2. Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)**. Sélectionnez la **Configuration Scope (Portée de la configuration)** comme étant **Prisma Access**. Sélectionnez l'état **In Sync (En synchronisation)** des **Service Connections (Connexions aux services)** sous l'état de synchronisation de Prisma Access. Sélectionnez la région où une connexion Colo-Connect est déployée.

   - Si la connexion Colo-Connect et le routage BGP sont actifs, l'état affiche **OK**.
   - Si la connexion Colo-Connect est active, mais que le routage BGP est inactif, l'état affiche **Warning (Avertissement)**.
   - Si la connexion Colo-Connect et le routage BGP sont inactifs, l'état s'affiche **Down (Inactif)**.
   - Si la connexion Colo-Connect est inactive, mais que le routage BGP est actif, l'état affiche **Error (Erreur)**.



3. Pour plus d'informations, cliquez sur la zone de région et affichez les informations dans l'onglet **Status (État)**.

STEP 10 | Vérifiez les détails de connexion, y compris la clé de couplage, des connexions Colo-Connect en accédant à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Colo Connect**.

Configurer Prisma Access Colo-Connect — Déploiements à l'aide d'interconnexions dédiées

Pour configurer Prisma Access Colo-Connect à l'aide d'une interconnexion dédiée, procédez comme suit.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Créez des sous-réseaux pour vos connexions Colo-Connect.

Vous utilisez les sous-réseaux que vous créez ici dans les connexions et connexions aux services que vous créez dans les étapes ultérieures.

1. Depuis Strata Cloud Manager, accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Colo-Connect** et cliquez sur l'icône en forme d'engrenage pour modifier les paramètres.
2. Cliquez sur **Add Prefix (Ajouter un préfixe)** pour **Colo-Connect Subnet (Sous-réseau Colo-Connect)** et sélectionnez un emplacement Prisma Access (**PA Location (Emplacement PA)**) pour celui-ci.

   Entrez un sous-réseau minimum de /28.
3. (Facultatif) Si vous prévoyez de créer des instances Colo-Connect pour plus d'un emplacement, ajoutez d'autres sous-réseaux par emplacement.

   Vous pouvez configurer un seul sous-réseau par emplacement.

STEP 2 | Ajoutez un nouveau lien Colo-Connect (également appelé *interconnexion*).

1. Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Colo-Connect** et **Add Link (Ajouter un lien)**.
2. Donnez au lien un **Link Name (Nom de lien)** unique.
3. Sélectionnez une interconnexion **Dedicated (Dédiée)** comme **Link Type (Type de lien)**.
4. Spécifiez les paramètres restants du lien Colo-Connect.
   - Sélectionnez **10Gbps (10 Gbit/s)** ou **20Gbps (20 Gbit/s)** pour la **Bandwidth (Bande passante)**.

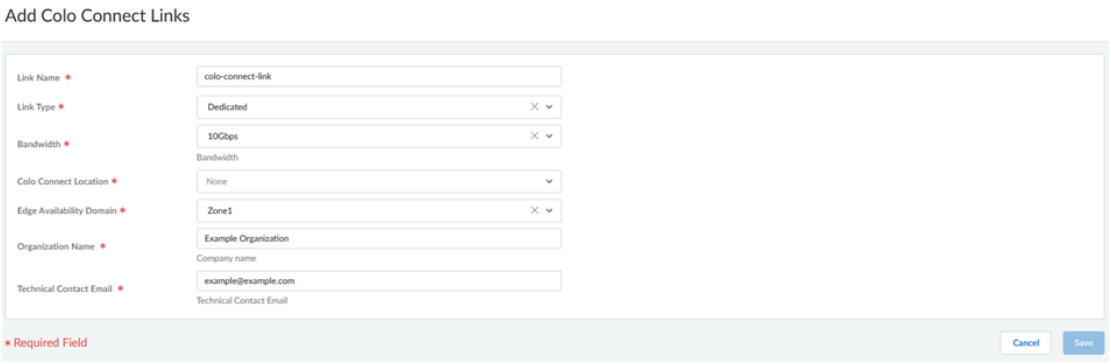
     Si vous sélectionnez 20 Gbit/s, vous devez regrouper le lien d'interconnexion dédiée en deux liens de 10 Gbit/s à l'aide du LACP.

     Vous ne pouvez pas modifier la bande passante d'un lien d'interconnexion dédiée après l'avoir spécifié et validé et appliqué vos modifications.
   - Sélectionnez un **Colo-Connect Location (Emplacement Colo-Connect)** dans la liste déroulante.

     Assurez-vous que vous sélectionnez le même emplacement que celui utilisé pour l'interconnexion dédiée.
   - Sélectionnez **Zone1** ou **Zone2** pour **Edge Availability Domain (Domaine de disponibilité périphérique)**. Prenez cette valeur dans la zone GCP utilisée pour votre domaine de disponibilité périphérique.
   - Entrez l'**Organization Name (Nom de l'organisation)** à utiliser pour ce lien.
   - Entrez l'**Email (E-mail)** où vous souhaitez recevoir les détails LOA-CFA du fournisseur cloud.
     - GCP utilise cet e-mail pour envoyer la lettre d'autorisation et de cession d'installation de raccordement (LOA-CFA). Assurez-vous que la LOA-CFA est

 ©2025 Palo Alto Networks, Inc.

envoyée à votre fournisseur Colo, afin qu'il puisse commencer à installer vos connexions.



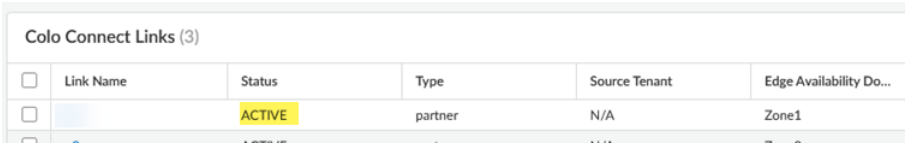
STEP 3 | Après la création de la connexion dédiée, l'installation Colo teste vos connexions et vous informe qu'elles ont été testées et sont prêtes à l'emploi.

Aucune configuration de Prisma Access n'est requise pour cette étape. Ne créez pas les connexions Colo-Connect dans Prisma Access tant que l'installation Colo ne vous a pas informé qu'elles ont été testées.

STEP 4 | Créez les connexions (également appelées *attachements VLAN*) pour Colo-Connect.

1. Assurez-vous que l'état du lien dédié est Active (Actif) en accédant à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Colo-Connect** > **Colo Connect Links (Liens Colo-Connect)**.

   Tant que l'état du lien dédié n'est pas actif, vous ne pouvez pas créer de liens Colo-Connect.

2. Accédez à **Workflows (Flux de travail)** > **Configuration de Prisma Access (Prisma Access Setup)** > **Colo-Connect** et **Add Connection (Ajouter une connexion)**.
3. Configurez les paramètres de connexion.
   - Saisissez un **Name (Nom)** unique pour la connexion.
   - Sélectionnez un **Link Name (Nom de lien)** parmi les liens que vous avez configurés à une étape précédente.
   - (Facultatif) Entrez un **VLAN ID (ID de VLAN)** pour la connexion.

     Les ID de VLAN sont générés par le fournisseur d'interconnexion (GCP) si vous n'entrez pas manuellement une valeur.
   - Sélectionnez une **Bandwidth (Bande passante)** pour la connexion.

     Vous pouvez choisir entre **1 Gbps (1 Gbit/s)**, **2 Gbps (2 Gbit/s)**, **5 Gbps (5 Gbit/s)**, **10 Gbps (10 Gbit/s)** ou **20 Gbps (20 Gbit/s)**.

     Si vous configurez plusieurs connexions pour une interconnexion, assurez-vous que la bande passante totale des connexions ne dépasse pas la bande passante de l'interconnexion. Par exemple, avec une interconnexion dédiée de 20 Gbit/s, vous

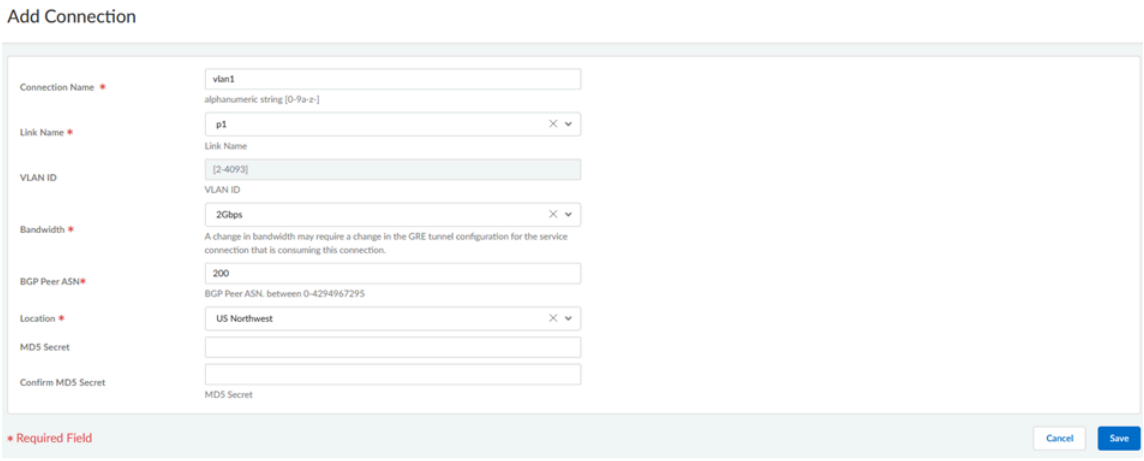
 ©2025 Palo Alto Networks, Inc.

pouvez configurer 10 connexions de 2 Gbit/s chacune, mais vous ne pouvez pas dépasser 20 Gbit/s au total pour toutes les connexions.

- Entrez un **BGP Peer ASN (ASN homologue BGP)**.

  Entrez le numéro de système autonome (AS) pour le routeur sur site client dans le Colo. La plage se situe entre 1 et 4294967295.
- Sélectionnez le **Location (Emplacement)** parmi les noms de connexion que vous avez créés lors d'une étape précédente.

  Vous devez avoir déjà ajouté un sous-réseau pour tout emplacement que vous spécifiez.
- (Facultatif) Entrez le **MD5 Secret (Secret MD5)** de BGP.



4. Continuez à créer des connexions jusqu'à ce qu'elles soient terminées.

   Créez deux connexions. Les deux connexions doivent être dans la même région et une connexion doit être dans une zone distincte. Vous utilisez ces connexions dans les connexions aux services que vous créez dans une étape ultérieure.

STEP 5 | **Push Config (Transmettre la configuration)**.

STEP 6 | Configurez le routage eBGP sur le routeur client.

Vous devez configurer l'appairage BGP pour assurer la connectivité entre le routeur client.

STEP 7 | Configurez les connexions aux services à utiliser avec Colo-Connect.

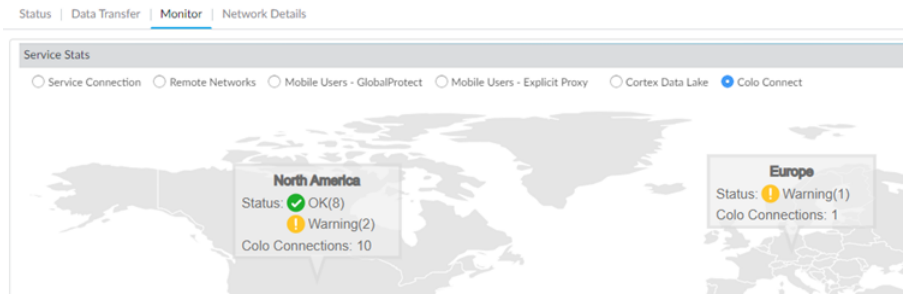
STEP 8 | Cliquez sur **Commit and Push (Valider et appliquer)** pour valider et appliquer vos modifications de configuration, en vous assurant que **Colo-Connect** est sélectionné dans **Push Scope (Étendue de la transmission)**.

STEP 9 | Vérifiez l'état des connexions Colo-Connect.

1. Pour vérifier l'état d'une connexion aux services utilisée par une connexion Colo-Connect, accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)**. Sélectionnez la **Configuration Scope (Portée de la configuration)** comme étant **Prisma Access**.

 ©2025 Palo Alto Networks, Inc.

2. Survolez une région où une connexion Colo-Connect est déployée.
   - Si la connexion Colo-Connect et le routage BGP sont actifs, l'état affiche **OK**.
   - Si la connexion Colo-Connect est active, mais que le routage BGP est inactif, l'état affiche **Warning (Avertissement)**.
   - Si la connexion Colo-Connect et le routage BGP sont inactifs, l'état s'affiche **Down (Inactif)**.
   - Si la connexion Colo-Connect est inactive, mais que le routage BGP est actif, l'état affiche **Error (Erreur)**.



3. Pour plus d'informations, cliquez sur la zone de région et affichez les informations dans l'onglet **Status (État)**.

STEP 10 | Vérifiez les détails du réseau des connexions Colo-Connect en accédant à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Colo-Connect** > **Connections (Connexions)** et en affichant les détails.

Pour les liens dédiés, la **Pairing Key (Clé de couplage)** s'affiche comme **N/A (S.O.)**.



Configurer le routage VLAN eBGP sur le routeur client

GCP crée des adresses IP pour le routeur client (Colo) et le routeur cloud pendant ces étapes de déploiement :

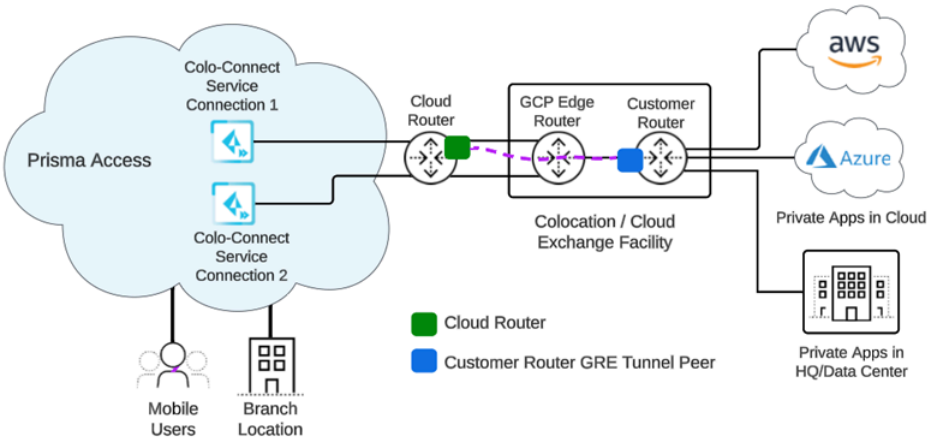
- Pour les interconnexions partenaires, GCP crée les adresses IP une fois la clé de couplage consommée par votre Colo (par exemple, Equinix).
- Pour les interconnexions dédiées, GCP crée les adresses IP une fois que vous avez intégré vos connexions Colo-Connect (attachements VLAN) et validé et appliqué vos modifications.

Pour assurer un routage correct, vous devez :

- Configurer l'adresse IP du routeur Colo (**Colo CPE IP** dans Prisma Access) comme adresse IP eBGP locale
- Configurez l'adresse IP du routeur cloud (**Cloud Router IP (IP du routeur cloud)**) comme adresse de l'homologue eBGP sur votre routeur Colo.

Une fois terminé, eBGP est configuré pour la connexion (attachement VLAN) entre le routeur Colo et le routeur cloud.

 ©2025 Palo Alto Networks, Inc.



La création de ce routage est la première étape de la configuration du routage tunnel GRE. Vous terminez le routage du tunnel GRE lorsque vous configurez les tunnels GRE pendant la configuration de la connexion aux services.

Suivez les étapes suivantes pour configurer le routage entre le Colo et le routeur cloud.

STEP 1 | Depuis Strata Cloud Manager, créez les sous-réseaux, les liens et les connexions et **Push Config (Transmettre la configuration)**.

Utilisez le flux de travail spécifique à votre type d'interconnexion (Partenaire ou Dédiée) Pour les interconnexions partenaires, assurez-vous d'avoir collé la clé de couplage dans le VLAN Colo.

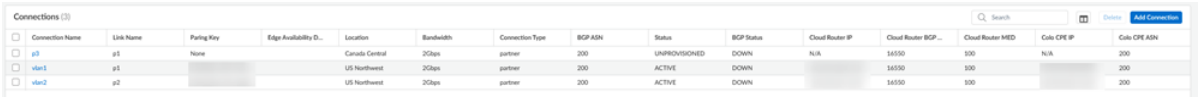
STEP 2 | Accédez à **Workflows (Flux de travail)** > **(Configuration de Prisma Access (Prisma Access Setup)** > **Colo-Connect** > **Connections (Connexions)**.

STEP 3 | Notez les éléments de connexion suivants :

- **Colo CPE IP**
- **IP de routeur cloud**
- **Routeur cloud BGP ASN**

Dans l'exemple suivant :

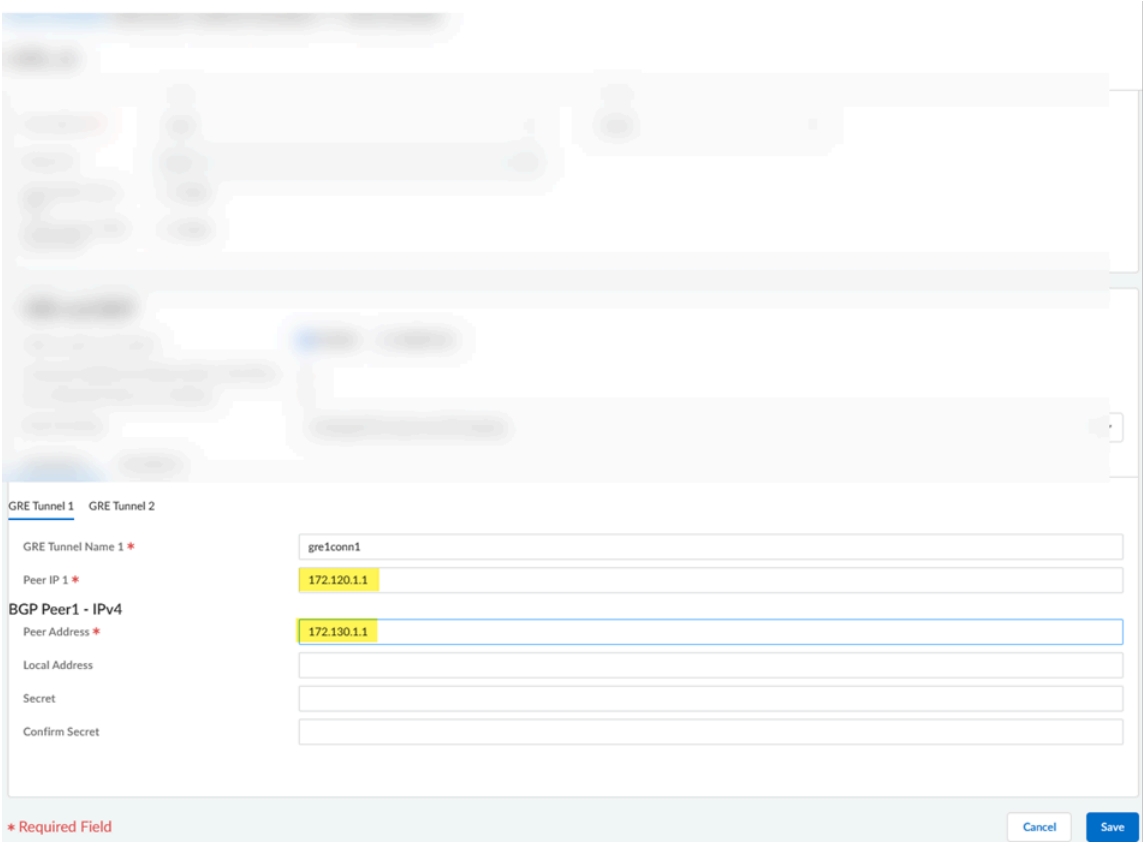
- Pour la connexion vlan-central-1, la **Colo CPE IP** est 169.254.24.170/29, la **Cloud Router IP (IP de routeur cloud)** est 169.254.24.169/29 et le **Cloud Router BGP ASN (Routeur cloud BGP ASN)** est 16550
- Pour la connexion vlan-central-2, la **Colo CPE IP** est 169.254.120.74/29, la **Cloud Router IP (IP de routeur cloud)** est 169.254.120.73/29 et le **Cloud Router BGP ASN (Routeur cloud BGP ASN)** est 16550.
- .



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Déterminez les adresses IP que vous utiliserez pour les adresses IP GRE locales lorsque vous configurerez les connexions aux services Colo-Connect.

Vous les configurez lors de la configuration d'une connexion aux services Colo-Connect (**Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connections (Connexions aux services)**). Dans les zones **Peer IP 1 (IP de l'homologue 1)** et, le cas échéant, **Peer IP 2 (IP de l'homologue 2)**.



Si vous configurez une connexion aux services pour prendre en charge jusqu'à 10 Gbit/s de débit, mettez un tunnel chacun dans la **Connection 1 (Connexion 1)** et la **Connection 2 (Connexion 2)**, pour un total de deux tunnels dans chaque connexion aux services.

Si vous configurez une connexion aux services pour prendre en charge plus de 10 Gbit/s de débit (jusqu'à 20 Gbit/s), mettez deux tunnels chacun dans la **Connection 1 (Connexion 1)** et la **Connection 2 (Connexion 2)**, pour un total de quatre tunnels dans chaque connexion aux services.

Les exemples suivants montrent qu'un tunnel est configuré pour un débit supérieur à 10 Gbit/s. Deux tunnels par connexion sont donc utilisés et ils utilisent les adresses IP de l'homologue suivantes :

- 172.120.1.1 pour la connexion 1
- 172.130.1.1 pour la connexion 1
- 172.121.1.1 pour la connexion 2
- 172.131.1.1 pour la connexion 2

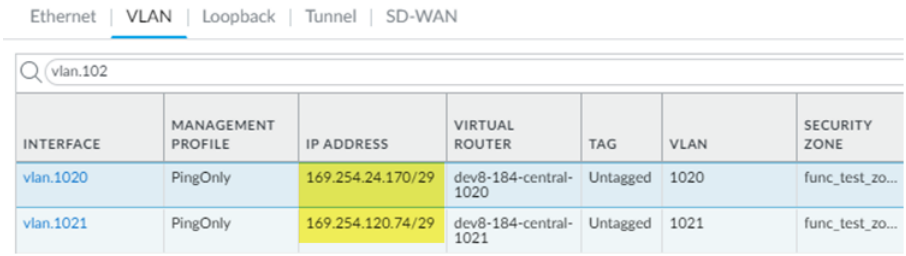
 ©2025 Palo Alto Networks, Inc.

STEP 5 | Connectez-vous au routeur Colo.

Les captures d'écran de configuration suivantes utilisent un pare-feu nouvelle génération Palo Alto Networks comme routeur Colo.

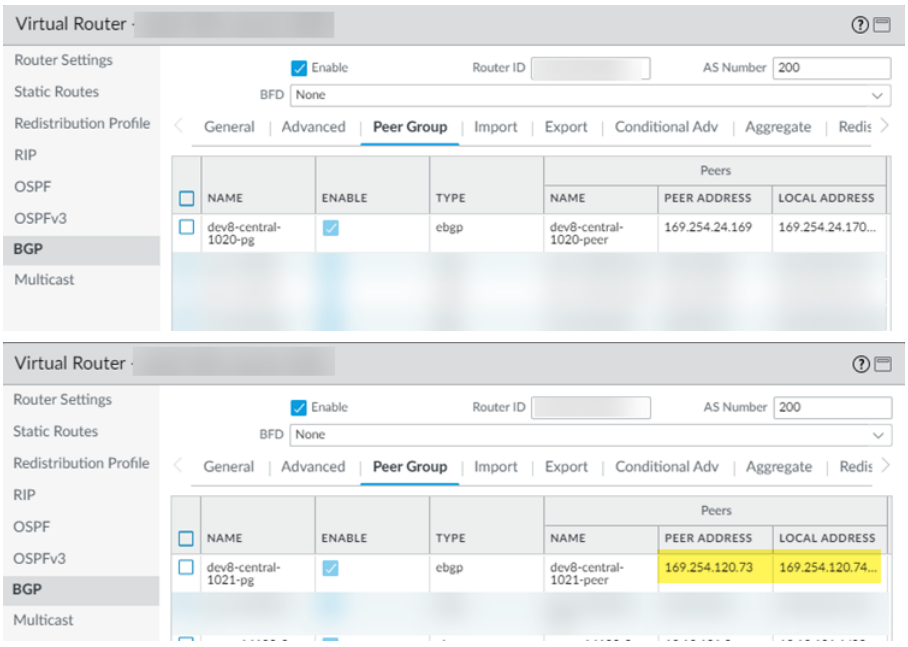
STEP 6 | Ajoutez une interface VLAN, en spécifiant l'adresse **Colo CPE IP** comme adresse IP.

Si vous utilisez un pare-feu nouvelle génération comme routeur Colo, accédez à **Network (Réseau)** > **Interfaces** > **VLAN** et cliquez sur **Add (Ajouter)** pour ajouter l'interface VLAN, en spécifiant le nom du **Virtual Router (Routeur virtuel)**.



STEP 7 | Configurez l'adresse IP du routeur Colo (**Colo CPE IP**) comme adresse IP eBGP locale et configurez l'adresse IP du routeur cloud (**IP de routeur cloud**) comme adresse de l'homologue eBGP sur votre routeur Colo.

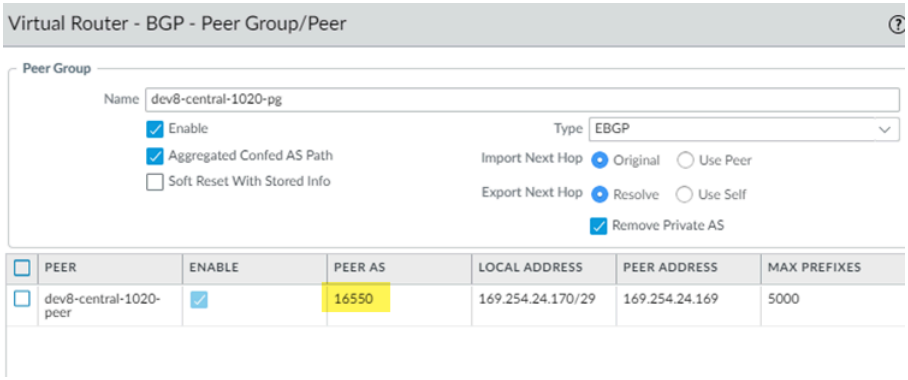
Si vous utilisez un pare-feu nouvelle génération comme routeur Colo, accédez à **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, cliquez sur **Add (Ajouter)** pour ajouter un routeur virtuel, accédez à **BGP** > **Peer Group (Groupe d'homologues)** et entrez **Colo CPE IP** comme **Peer Address (Adresse de l'homologue)** et **Cloud Router IP (IP de routeur cloud)** comme **Local Address (Adresse locale)**.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | Configurez le **Cloud Router BGP ASN (Routeur cloud BGP ASN)** en tant que numéro de système autonome (ASN) de l'homologue eBGP.

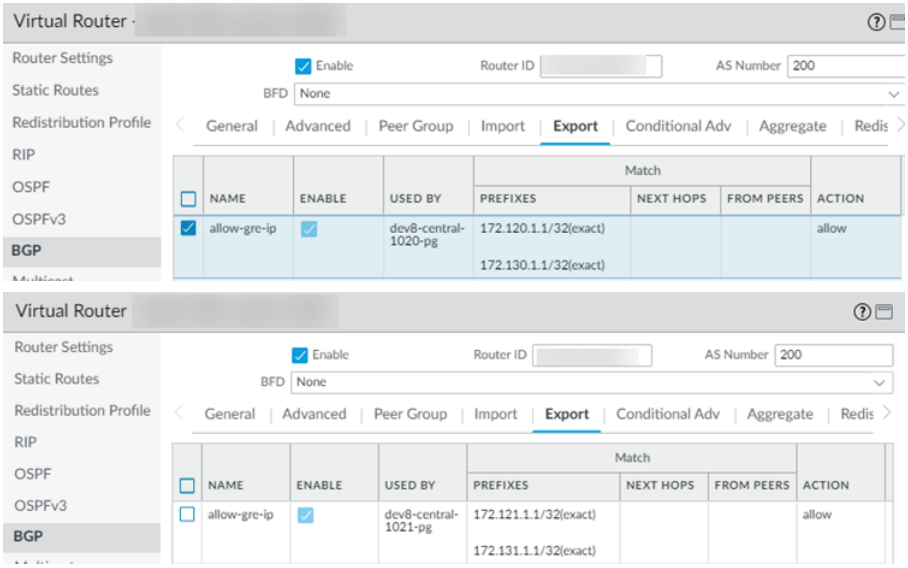
Si vous utilisez un pare-feu nouvelle génération comme routeur Colo, accédez à **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, cliquez sur **Add (Ajouter)** pour ajouter un routeur virtuel, accédez à **BGP** > **Peer Group (Groupe d'homologues)**, **Add (Ajouter)** un groupe d'homologues et sélectionnez un **Peer AS (AS de l'homologue** de **16500**.



STEP 9 | Créez une politique d'exportation BGP qui autorise uniquement l'adresse IP GRE locale à être annoncée à l'adresse IP de l'homologue du routeur cloud.

Puisque les routeurs cloud ne peuvent recevoir qu'un nombre limité d'itinéraires, vous devez créer des politiques afin que seul le routage entre les adresses IP des tunnels GRE de connexion aux services soit envoyé au routeur cloud.

Si vous utilisez un pare-feu nouvelle génération comme routeur Colo, accédez à **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, cliquez sur **Add (Ajouter)** pour ajouter un routeur virtuel, accédez à **BGP** > **Export (Exporter)**, cliquez sur **Add (Ajouter)** pour ajouter une règle d'exportation, et sur **Match (Faire correspondre)** pour faire correspondre les adresses IP utilisées comme adresse IP de l'homologue et créez une **Action Allow (Autorisation)**.



STEP 10 | Créez les connexions aux services Colo-Connect.

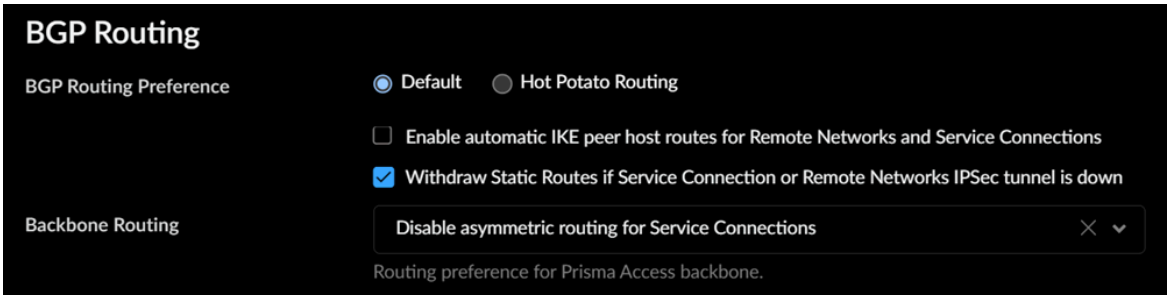
 ©2025 Palo Alto Networks, Inc.

Créer des connexions aux services Colo-Connect

Colo-Connect utilise des connexions aux services, mais elles diffèrent des connexions aux services Prisma Access, car elles utilisent des tunnels GRE au lieu de tunnels IPSec et utilisent toujours BGP pour le routage. Pour configurer les connexions aux services Colo-Connect, procédez comme suit.

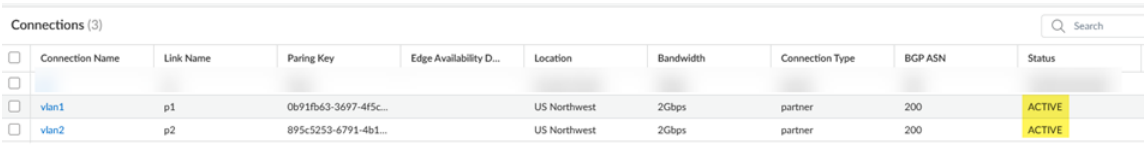
STEP 1 | Assurez-vous que Prisma Access retire les itinéraires statiques en accédant à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connections (Connexions aux services)** > **Advanced Settings (Paramètres avancés)**, et en sélectionnant **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down (Supprimer les itinéraires statiques si la connexion aux services ou le tunnel IPSec du réseau distant est inactif)**.

Sélectionner cette option garantit que, si le tunnel GRE est inactif, l'itinéraire statique utilisé par le tunnel GRE est retiré.



STEP 2 | Accédez à l'onglet **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Colo-Connect** > **Connections (Connexions)** et assurez-vous que les connexions sont dans un état **Active (Actif)** en vérifiant leur **Status (État)**.

Tant que le **Status (État)** de la connexion n'est pas **Active (Actif)**, vous ne pouvez pas configurer les connexions aux services.



STEP 3 | Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** et définissez l'étendue de la configuration sur **Prisma Access**.

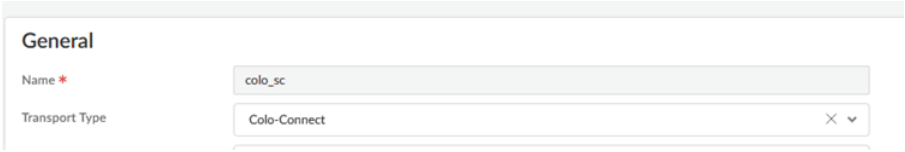
STEP 4 | Actualisez le **Prisma Access Sync Status (État de synchronisation de Prisma Access)** afin que la configuration Colo-Connect soit provisionnée dans la zone des connexions aux services.

STEP 5 | Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connection (Connexion aux services)Add Service Connection (Ajouter**

 ©2025 Palo Alto Networks, Inc.

une connexion aux services), donnez-lui un **Name (Nom)** unique et sélectionnez un **Transport Type (Type de transport)** de **Colo-Connect**.

Assurez-vous que le nom que vous saisissez fait 31 caractères ou moins ; la saisie d'un nom de 32 caractères ou plus provoque une mauvaise cartographie du tunnel dans l'infrastructure Prisma Access.



STEP 6 | Sélectionnez deux connexions à utiliser avec les connexions aux services (**Connection 1 (Connexion 1)** et **Connection 2 (Connexion 2)**).

Ces connexions doivent être dans deux zones différentes.



STEP 7 | Sélectionnez **Active (Actif)** ou **Backup (Sauvegarde)** pour la **Connection 1 (Connexion 1)** et la **Connection 2 (Connexion 2)**.

Utilisez ces directives lors de la configuration des connexions aux services :

- Vous pouvez configurer les connexions dans ces modes :
  - **Active (Actif)/Active (Actif)**
  - **Active (Actif)/Backup (Sauvegarde)**
  - **Backup (Sauvegarde)/Active (Actif)**

  La configuration des deux connexions en mode **Backup (Sauvegarde)/Backup (Sauvegarde)** n'est pas valide et n'est pas prise en charge.
- La bande passante des connexions doit être la même pour tous les modes.
- Les connexions doivent être dans des zones différentes.
- La bande passante maximale que vous pouvez spécifier pour une connexion de service est de 20 Gbit/s. Si vous spécifiez une **Bandwidth (Bande passante)** de **20 Gbps (20 Gbit/s)** pour une connexion, vous ne pouvez pas utiliser cette connexion dans une configuration **Active (Actif)/Active (Actif)** (elle doit être définie comme **Active (Actif)/Backup (Sauvegarde)**).
- Ne mélangez pas les interconnexions dédiées et partenaires dans la même connexion aux services, et assurez-vous que les connexions aux services utilisent des zones différentes. Ce tableau montre les configurations autorisées et interdites pour les connexions aux services,

 ©2025 Palo Alto Networks, Inc.

en supposant que les zones, les emplacements, la bande passante et les rôles suivent les directives et exigences de connexion aux services :

Connection 1 Belongs To (Connexion 1 appartient à)	Connection 2 Belongs To (Connexion 2 appartient à)	Valid Colo-Connect Service Connection Configuration? (Configuration de connexion aux services Colo-Connect valide ?)
Partner Connect 1 (Connexion partenaire 1)	Partner Connect 2 (Connexion partenaire 2)	Yes (Oui)
Dedicated Connect 1 (Connexion dédiée 1)	Dedicated Connect 2 (Connexion dédiée 2)	Yes (Oui)
Partner Connect 1 (Connexion partenaire 1)	Partner Connect 1 (Connexion partenaire 1)	No (Non)
Dedicated Connect 1 (Connexion dédiée 1)	Dedicated Connect 1 (Connexion dédiée 1)	No (Non)
Partner Connect (Connexion partenaire)	Dedicated Connect (Connexion dédiée)	No (Non)

STEP 8 | (Facultatif et pour les déploiements de routage hot potato uniquement) Sélectionnez une connexion aux services à utiliser comme sauvegarde préférée, qui est le **Backup SC (SC de secours)**, dans la configuration de routage hot potato.

Vous ne pouvez sélectionner qu'une connexion aux services configurée en tant que connexion aux services Colo-Connect. Prisma Access utilise la sauvegarde SC que vous sélectionnez comme connexion aux services préférée en cas d'échec de connexion. La sélection d'une connexion de service de sauvegarde peut éviter les problèmes de routage asymétrique si vous avez intégré plus de deux connexions de service.

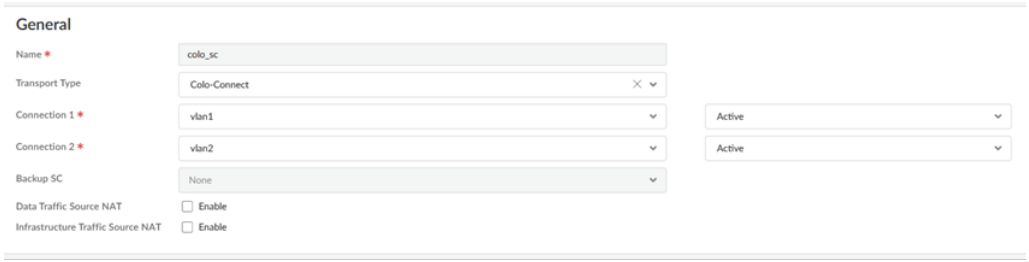
STEP 9 | (Facultatif) Activez le NAT source pour les utilisateurs mobiles : adresses du pool d'adresses IP GlobalProtect, adresses IP dans le sous-réseau Infrastructure, ou les deux.

Vous pouvez spécifier un sous-réseau au niveau d'une ou plusieurs connexions aux services utilisées pour le trafic NAT entre les utilisateurs mobiles Prisma Access GlobalProtect et les applications et ressources privées d'un centre de données.

- **Activer le NAT source de trafic de données** : effectue le NAT sur les adresses du pool d'adresses IP des utilisateurs mobiles afin qu'elles ne soient pas annoncées au centre de données et que seuls les sous-réseaux que vous spécifiez aux connexions aux services soient annoncés et acheminés dans le centre de données.
- **Activer le NAT source de trafic d'infrastructure** : effectue le NAT sur les adresses du sous-réseau d'infrastructure afin qu'elles ne soient pas annoncées au centre de données et que seuls les sous-réseaux que vous spécifiez aux connexions aux services soient annoncés et acheminés dans le centre de données.
- **IP Pool (Pool d'adresses IP)** : spécifie le pool d'adresses IP utilisé pour effectuer le NAT sur le pool d'adresses IP des utilisateurs mobiles, le sous-réseau d'infrastructure ou les

 ©2025 Palo Alto Networks, Inc.

deux. Utilisez un sous-réseau IP privé (RFC 1918) ou un sous-réseau approprié qui est routable dans votre domaine de routage et qui ne chevauche pas le pool d'adresses IP des utilisateurs mobiles – Pool d'adresses IP GlobalProtect ou le sous-réseau d'infrastructure. Entrez un sous-réseau entre /25 et /32.



STEP 10 | Dans la zone **GRE and BGP (GRE et BGP)**, configurez les paramètres du tunnel GRE et du BGP pour la connexion aux services.

BGP est toujours réglé sur **Enable (Activer)**.

1. (Facultatif) Choisissez parmi les options suivantes :

   - Pour ajouter une communauté de **no-export (non-export)** pour les nœuds d'accès d'entreprise (connexions aux services) aux préfixes sortants des homologues eBGP de l'équipement sur site client (CPE), définissez **Add no-export community (Ajouter une communauté de non-export)** sur **Enabled Out (Sortie activée)**. Cette option est **Disabled (Désactivée)** par défaut.

     N'utilisez pas cette option en mode routage hot potato.

   - Pour réduire le nombre de publicités de sous-réseaux IP d'utilisateurs mobiles sur le BGP de votre équipement sur site client (CPE), sélectionnez **Summarize Mobile User Routes before advertising (Résumer les itinéraires des utilisateurs mobiles avant de publier)**.

     Par défaut, Prisma Access publie les pools d'adresses IP des utilisateurs mobiles par blocs de sous-réseaux /24. Si vous les résumez, Prisma Access publie le pool en fonction du sous-réseau que vous avez spécifié. Par exemple, Prisma Access publie un pool d'adresses IP mobiles d'utilisateurs publics de 10.8.0.0/20 en utilisant le sous-réseau /20, plutôt que de diviser le pool en sous-réseaux de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, et ainsi de suite, avant de les publier. Le résumé de ces publicités peut réduire le nombre d'itinéraires stockés dans les tableaux de routage CPE. Par exemple, vous pouvez utiliser le résumé de pool d'adresses IP avec des passerelles VPN cloud (passerelles privées virtuelles [VGW] ou passerelles de transit [TGW]) qui peuvent accepter un nombre limité d'itinéraires.

     Si vous avez activé le routage hot potato et que vous activez le résumé des itinéraires, Prisma Access ne présuppose plus les AS-PATH, ce qui peut provoquer un routage asymétrique. Assurez-vous que votre trafic de retour du centre de données ou de l'emplacement du siège a garanti un retour symétrique avant d'activer le résumé des itinéraires avec le routage hot potato.

 ©2025 Palo Alto Networks, Inc.

- Pour empêcher le pair BGP Prisma Access de transférer des itinéraires dans le réseau de votre organisation. Cliquez sur **Don't Advertise Prisma Access Routes (Ne pas publier les itinéraires Prisma Access)**.

  Par défaut, Prisma Access publie toutes les informations de routage BGP, y compris les itinéraires locaux et tous les préfixes qu'il reçoit d'autres connexions aux services, réseaux distants et sous-réseaux d'utilisateurs mobiles. Cochez cette case pour empêcher Prisma Access d'envoyer des publicités BGP, mais utilisez quand même les informations BGP qu'il reçoit pour apprendre les itinéraires d'autres voisins BGP.

  Puisque Prisma Access n'envoie pas de publicités BGP si vous sélectionnez cette option, vous devez configurer des itinéraires statiques sur l'équipement local pour établir des itinéraires de retour vers Prisma Access.

- Quel est le paramètre « Échange d'itinéraire » ?

2. Configurez le routage pour la connexion aux services en utilisant les tunnels GRE.
3. Depuis Strata Cloud Manager, revenez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connexion (Connexion aux services)** un tunnel GRE pour **Connection 1 (Connexion 1)** en saisissant un **GRE Tunnel Name 1 (Nom de tunnel GRE 1)** et une **Peer IP 1 (Adresse IP de l'homologue 1)** pour la **Connection 1 (Connexion 1)** et, si plus de 10 Gbit/s de bande passante sont requis, en saisissant un**GRE Tunnel Name 2 (Nom de tunnel GRE 2)** et une **Peer IP 2 (Adresse IP de l'homologue 2)** pour le deuxième tunnel pour la connexion 1. Puis, créez un tunnel GRE pour la **Connection 2 (Connexion 2)** en répétant ces mêmes étapes.

   Chaque paire de tunnels GRE dans une connexion prend en charge un maximum de 10 Gbit/s de bande passante. Si vous avez besoin de plus de 10 Gbit/s de bande passante, configurez deux tunnels par connexion. Par exemple :

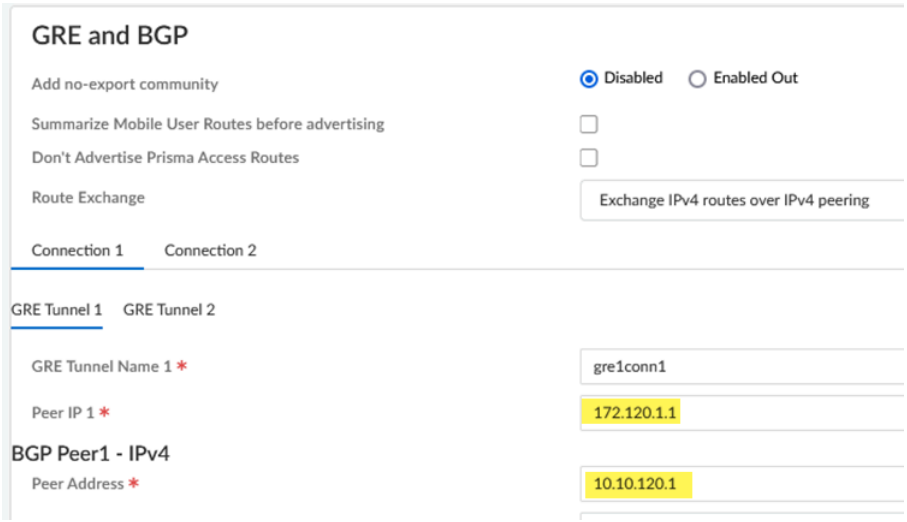
   Pour l'IP de l'homologue, entrez l'adresse IP GRE du routeur sur site dans le Colo.

   Utilisez les adresses IPv4 pour les valeurs BGP ; IPv6 n'est pas pris en charge.
4. Entrez la **Peer Address (Adresse de l'homologue)** et la **Local Address (Adresse locale)** pour l'homologue BGP 1 et, si une seconde est requise pour la connexion 1, l'homologue BGP 2.

   Pour **Peer Address (Adresse de l'homologue)**, entrez l'adresse IP de l'homologue BGP du routeur Colo. Pour **Local Address (Adresse locale)**, entrez l'adresse qui sera utilisée pour l'établissement du réseau BGP sur le tunnel GRE.

©2025 Palo Alto Networks, Inc.

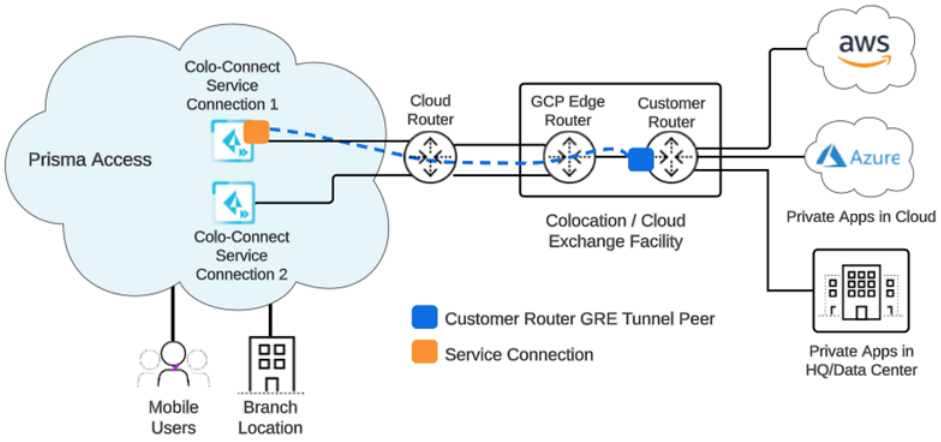
5. (Facultatif) Pour configurer un secret BGP, saisissez les valeurs **Secret** et **Confirm Secret (Confirmer secret)**.



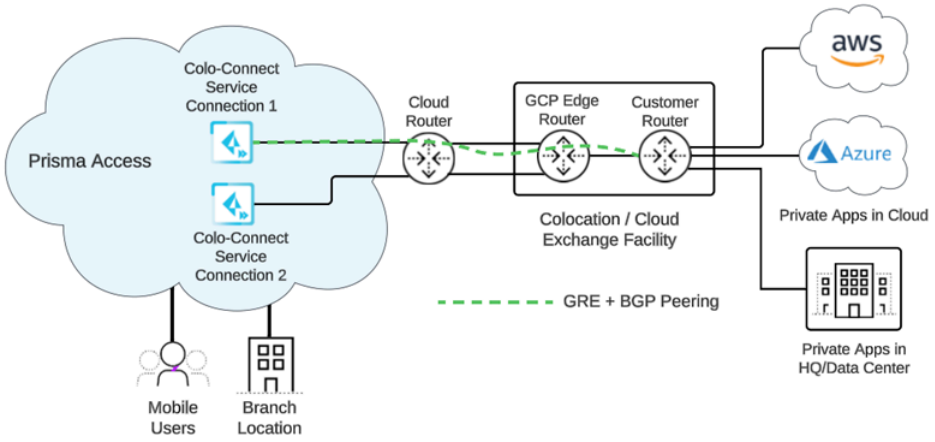
STEP 11 | Cliquez sur **Commit and Push (Valider et appliquer)** pour valider et appliquer vos modifications de configuration, en vous assurant que **Colo-Connect** est sélectionné dans **Push Scope (Étendue de la transmission)**.

Configurer le routage pour la connexion aux services à l'aide des tunnels GRE

Le routeur Colo publie son adresse IP de l'homologue du tunnel GRE au routeur cloud, et apprend le sous-réseau pour le tunnel GRE à partir du routeur cloud. Lorsque vous avez configuré pour la première fois le routage eBGP sur le VLAN du routeur client, vous avez annoncé la possibilité d'atteindre localement les tunnels GRE. Après que le routeur cloud et le routeur Colo aient annoncé et appris les itinéraires pour le sous-réseau Colo et les adresses IP GRE locales l'un de l'autre, les tunnels GRE utilisés par la connexion aux services deviennent actifs.



 ©2025 Palo Alto Networks, Inc.



Pour configurer le routage et ajouter des tunnels GRE aux connexions aux services, suivez les étapes suivantes.

STEP 1 | Notez les adresses IP que vous utiliserez pour la **Peer Address (Adresse de l'homologue)** et la **Local Address (Adresse locale)** pour l'homologue BGP 1 et, si une seconde est nécessaire pour la connexion 1, l'homologue BGP 2.

Les exemples suivants utilisent les adresses homologues et locales suivantes :

- **Peer Address (Adresse de l'homologue)** — 10.10.120.0 et 10.10.130.1 pour la connexion 1, 10.10.120.2 et 10.10.130.2 pour la connexion 2
- **Local Address (Adresse locale)** — 10.10.120.2 et 10.10.130.2 pour la connexion 1, 10.10.121.2 et 10.10.131.2 pour la connexion 2

STEP 2 | Notez les adresses IP que vous utiliserez pour l'adresse **Peer IP 1 (IP de l'homologue 1)** et, si nécessaire, l'adresse **Peer IP 2 (IP de l'homologue 2)** dans les connexions aux services.

Vous utilisez ces adresses IP pour créer une politique de déni qui empêche l'adresse IP GRE locale d'être annoncée à la connexion aux services Colo-Connect.

Tous les exemples de ce document utilisent ces adresses IP :

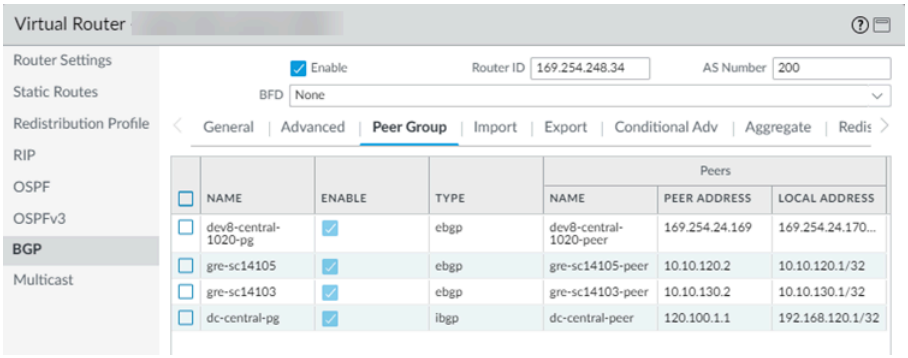
- 172.120.1.1 pour la connexion 1
- 172.121.1.1 pour la connexion 2

STEP 3 | Configurez les groupes d'homologues pour les adresses IP de l'homologue et locales.

Si vous utilisez un pare-feu nouvelle génération comme routeur Colo, accédez à **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, cliquez sur **Add (Ajouter)** pour ajouter un routeur virtuel, accédez à **BGP** > **Peer Group (Groupe d'homologues)**, et saisissez l'adresse

 ©2025 Palo Alto Networks, Inc.

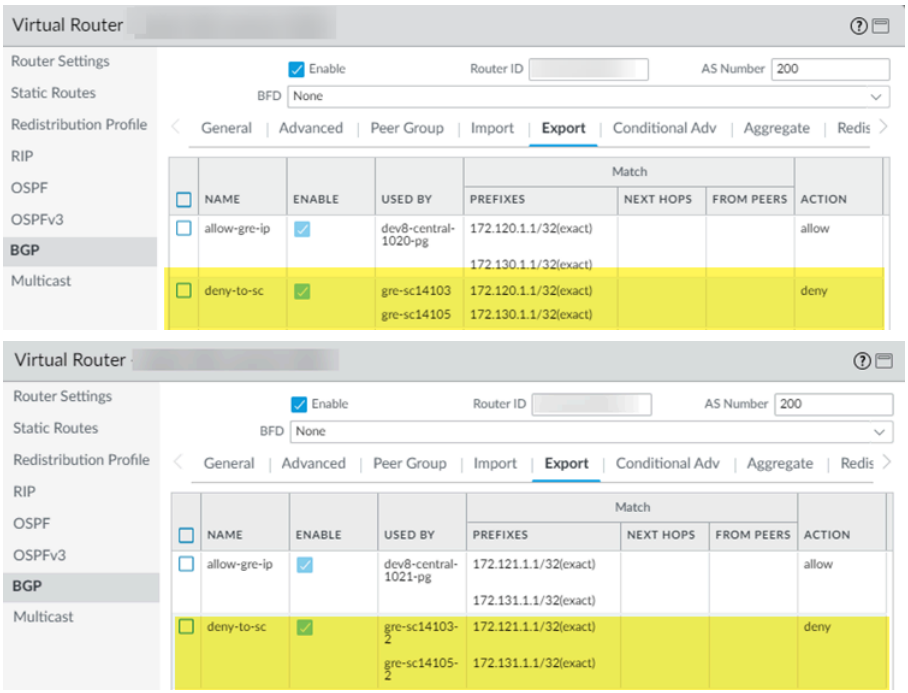
de l'homologue comme **Peer Address (Adresse de l'homologue)** et la **Local Address (Adresse locale)** comme **Local Address (Adresse locale)**.



STEP 4 | Créez une politique d'exportation du BGP pour refuser les adresses IP d'homologues que vous avez configurées (172.120.1.1, 172.130.1.1, 172.121.1.1 et 172.131.1.1) et les appliquer aux groupes d'homologues que vous avez créés.

Cette politique d'exportation place une règle de DÉNI sur les adresses IP d'homologues du tunnel GRE local et permet à tous les autres itinéraires d'être publiés sur la connexion aux services.

Si vous utilisez un pare-feu nouvelle génération comme routeur Colo, accédez à **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, **Add (Ajouter)** un routeur virtuel, accédez à **BGP** > **Export (Exporter)**, cliquez sur **Add (Ajouter)** pour ajouter une règle d'exportation, et sur **Match (Faire correspondre)** pour faire correspondre les adresses IP utilisées comme adresse IP de l'homologue et créez une **Action Deny (Déni)**.



 ©2025 Palo Alto Networks, Inc.

Augmenter ou diminuer la bande passante d'une connexion aux services Colo-Connect

Lorsque vous configurez des connexions aux services, vous configurez la bande passante en fonction des connexions (attachements VLAN) que vous lui associez. Vous allouez deux connexions par connexion aux services, puis vous allouez un ou deux tunnels GRE par connexion.

Alors que chaque connexion aux services Colo-Connect prend en charge un maximum de 20 Gbit/s, chaque tunnel GRE de la connexion aux services prend en charge 10 Gbit/s. Pour cette raison, vous devrez peut-être ajouter ou supprimer les tunnels GRE dans la connexion aux services Colo-Connect, modifier la bande passante totale dans un lien, ce qui entraînera une augmentation de la bande passante de la connexion aux services au-dessus ou en dessous de 10 Gbit/s.

Augmenter la bande passante d'une connexion aux services Colo-Connect

Pour augmenter la bande passante d'une connexion aux services existante au-delà de 10 Gbit/s, procédez comme suit :

STEP 1 | Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Colo-Connect**.

STEP 2 | Sélectionnez le **Link Name (Nom du lien)** associé à la connexion aux services.

STEP 3 | Augmentez la **Bandwidth (Bande passante)** du lien (interconnexion).

STEP 4 | **Push Config (Transmettre la configuration)**.

STEP 5 | Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connection (Connexion aux services)**.

STEP 6 | Ajoutez le tunnel GRE supplémentaire à la connexion aux services Colo-Connect.

STEP 7 | **Push Config (Transmettre la configuration)**.

STEP 8 | Ajoutez les adresses IP locales (d'homologues) GRE à vos politiques d'exportation pour le routage VLAN eBGP et le routage de connexion aux services pour les tunnels GRE.

Diminuer la bande passante d'une connexion aux services Colo-Connect

Pour réduire la bande passante d'une connexion aux services existante supérieure à 10 Gbit/s, procédez comme suit :

STEP 1 | Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Colo-Connect** .

STEP 2 | Sélectionnez le **Link Name (Nom du lien)** associé à la connexion aux services.

STEP 3 | Diminuez la **Bandwidth (Bande passante)** du lien (interconnexion).

STEP 4 | **Push Config (Transmettre la configuration)**.

Vous n'avez pas besoin de reconfigurer la connexion aux services pour supprimer le tunnel GRE supplémentaire. Prisma Access détecte et diminue la bande passante du lien et supprime le tunnel supplémentaire lorsque vous validez et appliquez vos modifications dans l'étendue de la transmission de la connexion aux services.

 ©2025 Palo Alto Networks, Inc.

Supprimer une connexion Colo-Connect

Pour supprimer une connexion Colo-Connect, suivez l'ordre inverse de sa configuration en effectuant les étapes suivantes :

STEP 1 | Supprimez les connexions aux services associées à la connexion en vous accédant à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connections (Connexions aux services)**, en sélectionnant la connexion aux services et cliquez sur **Delete (Supprimer)**.

STEP 2 | **Push Config (Transmettre la configuration)**.

STEP 3 | Supprimez les connexions Colo-Connect associées à la connexion en accédant à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Colo-Connect**, en sélectionnant le **Connection Name (Nom de connexion)** dans la section **Onboarding (Intégration)** et cliquez sur **Delete (Supprimer)**.

STEP 4 | Supprimez le lien Colo-Connect en sélectionnant le **Link Name (Nom du lien)** et **Delete (Supprimer)**.

STEP 5 | Supprimez les adresses IP locales (d'homologues) GRE à vos politiques d'exportation pour le routage VLAN eBGP et le routage de connexion aux services pour les tunnels GRE.

Configurer Prisma Access Colo-Connect (Panorama)

Configurer Prisma Access Colo-Connect — Déploiements à l'aide d'interconnexions partenaires

Pour configurer Prisma Access Colo-Connect à l'aide d'une interconnexion partenaire, procédez comme suit.

STEP 1 | Créez des sous-réseaux pour vos connexions Colo-Connect.

Vous utilisez les sous-réseaux que vous créez ici dans les connexions et connexions aux services que vous créez dans les étapes ultérieures.

1. Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Colo-Connect** et cliquez sur l'icône en forme d'engrenage pour modifier les paramètres.
2. Cliquez sur **Add (Ajouter)** pour ajouter un **Colo-Connect Subnet (Sous-réseau Colo-Connect)** et sélectionnez un emplacement Prisma Access (**PA Location (Emplacement PA**) pour celui-ci.

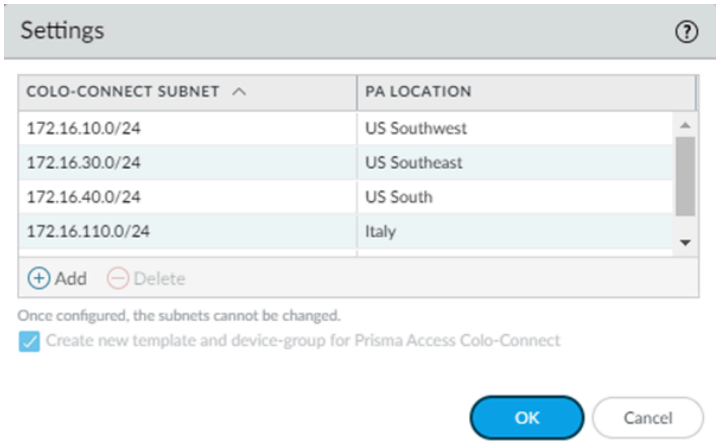
   Entrez un sous-réseau minimum de /28.
3. (Facultatif) Si vous prévoyez de créer des instances Colo-Connect pour plus d'un emplacement, ajoutez d'autres sous-réseaux par emplacement.

   Vous pouvez configurer un sous-réseau par emplacement.
4. Sélectionnez **Create new templates and device-group for Prisma Access Colo-Connect (Créer de nouveaux modèles et un groupe de périphériques pour Prisma Access Colo-Connect)**.

   La première fois que vous configurez un déploiement Colo-Connect, cochez cette case afin que des modèles et des groupes de périphériques (Colo_Connect_Template et

 ©2025 Palo Alto Networks, Inc.

Colo_Connect_Device_Group, respectivement) soient créés pour Colo-Connect. Après avoir créé ces modèles et groupes de périphériques, cette case à cocher est grisée.



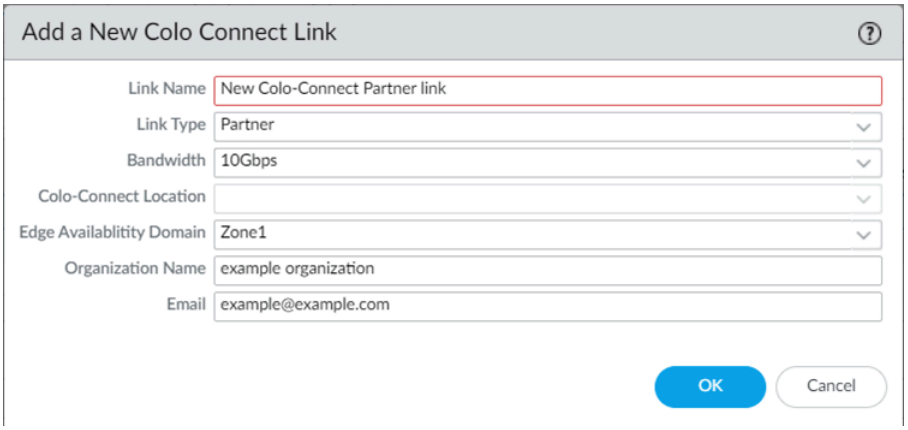
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Ajoutez un nouveau lien Colo-Connect (également appelé *interconnexion*).

1. Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Colo-Connect** > **Colo Connect Link (Lien Colo-Connect)** et cliquez sur **Add (Ajouter)** pour ajouter un lien Colo-Connect.
2. Donnez au lien un **Link Name (Nom de lien)** unique.
3. Sélectionnez une interconnexion **Partner (Partenaire)**.

   Vous n'avez pas besoin de saisir un **VLAN ID (ID de VLAN)**, votre Colo en fournit un lorsqu'il utilise la clé de couplage pour compléter la configuration de votre attachement VLAN.
4. Spécifiez les paramètres restants du lien Colo-Connect.
   - Sélectionnez **10Gbps (10 Gbit/s)** ou **20Gbps (20 Gbit/s)** pour la **Bandwidth (Bande passante)**.

     Vous ne pouvez pas changer la bande passante d'un lien d'interconnexion dédiée après l'avoir spécifié et avoir validé et appliqué vos modifications.
   - Sélectionnez **Zone1** ou **Zone2** pour **Edge Availability Domain (Domaine de disponibilité périphérique)**. Prenez cette valeur dans la zone GCP utilisée pour votre domaine de disponibilité périphérique.
   - Entrez l'**Organization Name (Nom de l'organisation)** à utiliser pour ce lien.
   - Entrez l'**Email (E-mail)** à utiliser pour ce lien. Toute adresse e-mail est acceptable.



STEP 3 | Créez les connexions (également appelées *attachements VLAN*) pour Colo-Connect.

1. Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Colo-Connect** > **Onboarding (Intégration)** et cliquez sur **Add (Ajouter)** pour ajouter une nouvelle connexion.
2. Configurez les paramètres de connexion.
   - Saisissez un **Name (Nom)** unique pour la connexion.
   - Sélectionnez un **Link Name (Nom de lien)** parmi les liens que vous avez configurés à une étape précédente.
   - Sélectionnez une **Bandwidth (Bande passante)** pour la connexion.

     Vous pouvez choisir entre **1 Gbps (1 Gbit/s)**, **2 Gbps (2 Gbit/s)**, **5 Gbps (5 Gbit/s)**, **10 Gbps (10 Gbit/s)** ou **20 Gbps (20 Gbit/s)**.

     Si vous configurez plusieurs connexions pour une interconnexion, assurez-vous que la bande passante totale des connexions ne dépasse pas la bande passante de

 ©2025 Palo Alto Networks, Inc.

l'interconnexion. Par exemple, avec une interconnexion partenaire de 10 Gbit/s, vous pouvez configurer 10 connexions de 1 Gbit/s chacune, mais vous ne pouvez pas dépasser 10 Gbit/s au total pour toutes les connexions.

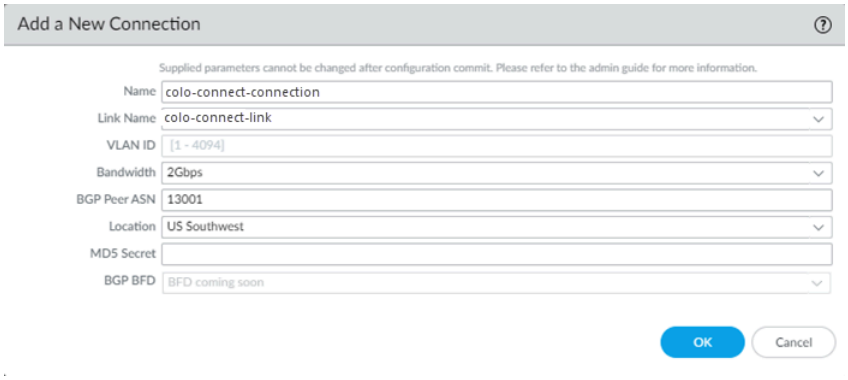
Si votre déploiement nécessite plus de 16 connexions, contactez votre équipe de compte Palo Alto Networks, qui ouvrira un dossier SRE pour répondre à la requête.

- Entrez un **BGP Peer ASN (ASN homologue BGP)**.

  Entrez le numéro de système autonome (AS) pour le routeur sur site client dans le Colo. La plage se situe entre 1 et 4294967295.
- Sélectionnez le **Location (Emplacement)** parmi les noms de connexion que vous avez créés lors d'une étape précédente.

  Vous devez avoir déjà ajouté un sous-réseau pour tout emplacement que vous spécifiez.
- (Facultatif) Entrez le **MD5 Secret (Secret MD5)** de BGP.

*Ignorez le champ **BGP BFD** ; il est réservé pour une future version de Colo-Connect.*



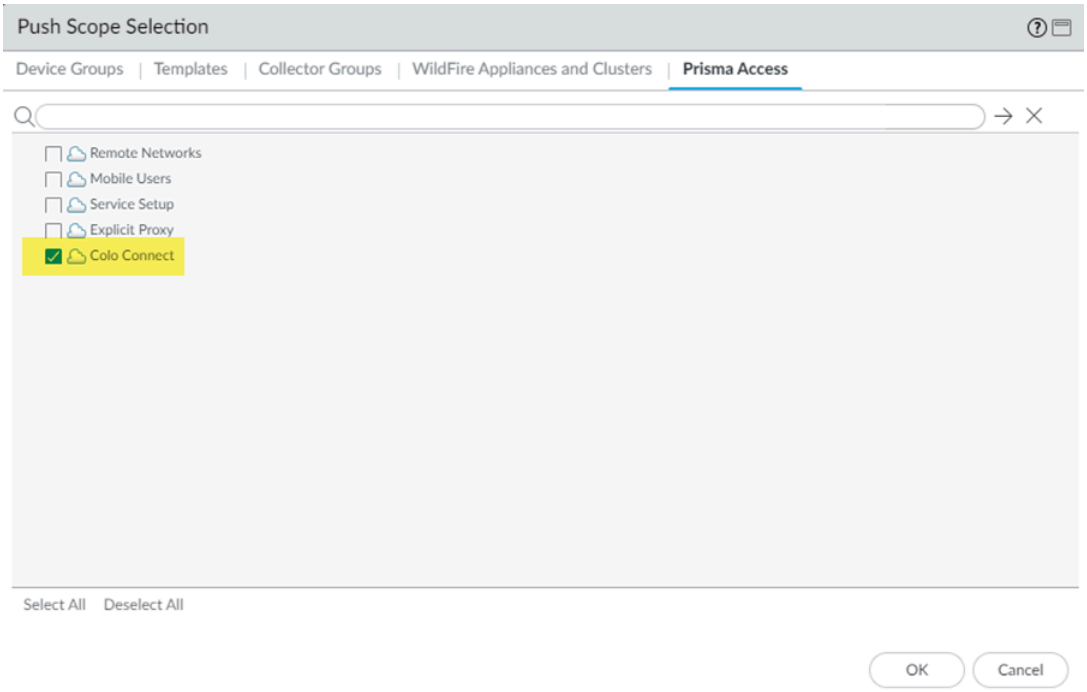
3. Continuez à créer des connexions jusqu'à ce qu'elles soient terminées.

   Vous devez créer deux connexions. Les deux connexions doivent être dans la même région et une connexion doit être dans une zone distincte. Vous utilisez ces connexions dans les connexions aux services que vous créez dans une étape ultérieure.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Validez et appliquez vos modifications.

1. Accédez à **Commit (Valider)** > **Commit and Push (Valider et appliquer)**.
2. Cliquez sur **Edit Selections (Modifier les sélections)** et assurez-vous que Colo-Connect est sélectionné dans l'étendue de la transmission.



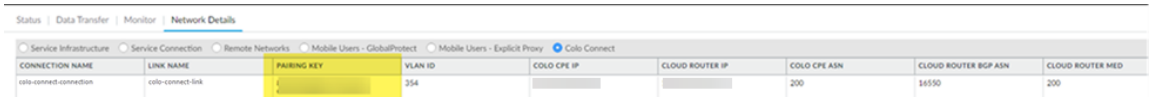
3. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.
4. **Commit and Push (Validez et appliquez)** vos modifications.

STEP 5 | Récupérez la **Pairing Key (Clé de couplage)** et complétez la configuration de votre interconnexion partenaire dans GCP.

Vous utilisez cette clé de couplage lorsque vous configurez l'interconnexion partenaire dans le Colo.

Lors de la première connexion, l'état dans la zone d'intégration Colo-Connect affiche un **Status (État)** de **PENDING_PARTNER** et un **BGP Status (État BGP)** de **DOWN (INACTIF)**. Pour mettre l'état de la connexion sur **ACTIVE (ACTIF)**, récupérez la clé de couplage et l'entrée dans la connexion au Colo.

1. Accédez à **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Colo Connect** et copiez la **Pairing Key (Clé de couplage)**.



2. Créez une nouvelle connexion VLAN dans le Colo (par exemple, Equinix).
3. Collez la clé de couplage dans le VLAN de Colo.

   GCP détecte quand la clé de couplage est consommée, met l'état du VLAN sur **ACTIVE (ACTIF)** et génère l'adresse IP de BGP que vous pouvez configurer sur votre routeur local dans le Colo. Ces actions initient le routage eBGP sur le VLAN entre le routeur Colo et le routeur cloud GCP.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Créez un routage eBGP sur le routeur client (Colo) pour la connexion Colo-Connect.

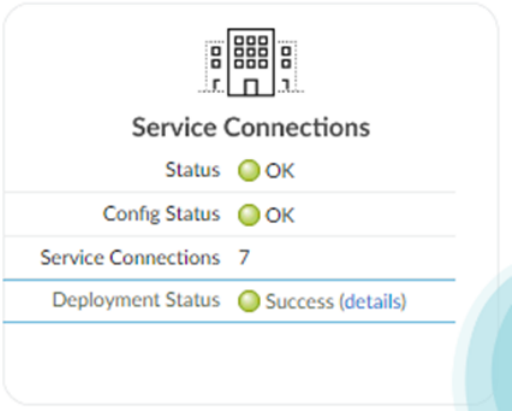
Vous devez configurer l'appairage BGP pour assurer la connectivité entre le routeur client et le routeur cloud.

STEP 7 | Configurez les connexions aux services à utiliser avec Colo-Connect.

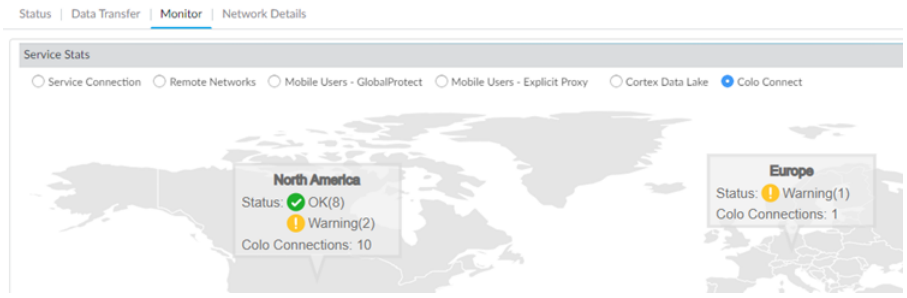
STEP 8 | Cliquez sur **Commit and Push (Valider et appliquer)** pour valider et appliquer vos modifications de configuration, en vous assurant que **Colo-Connect** est sélectionné dans **Push Scope (Étendue de la transmission)**.

STEP 9 | Vérifiez l'état des connexions Colo-Connect.

1. Pour vérifier l'état d'une connexion aux services utilisée par une connexion Colo-Connect, accédez à **Panorama** > **Cloud Services** > **Status (État)** > > **Colo-Connect** > **Monitor (Surveiller)**



2. Survolez une région où une connexion Colo-Connect est déployée.
   - Si la connexion Colo-Connect et le routage BGP sont actifs, l'état affiche **OK**.
   - Si la connexion Colo-Connect est active, mais que le routage BGP est inactif, l'état affiche **Warning (Avertissement)**.
   - Si la connexion Colo-Connect et le routage BGP sont inactifs, l'état s'affiche **Down (Inactif)**.
   - Si la connexion Colo-Connect est inactive, mais que le routage BGP est actif, l'état affiche **Error (Erreur)**.



3. Pour plus d'informations, cliquez sur la zone de région et affichez les informations dans l'onglet **Status (État)**.

 ©2025 Palo Alto Networks, Inc.

STEP 10 | Vérifiez les détails du réseau, y compris la clé de couplage, des connexions Colo-Connect en accédant à **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Colo-Connect** et en consultant les informations dans les champs suivants.

Configurer Prisma Access Colo-Connect — Déploiements à l'aide d'interconnexions dédiées

Pour configurer Prisma Access Colo-Connect à l'aide d'une interconnexion dédiée, procédez comme suit.

STEP 1 | Créez des sous-réseaux pour vos connexions Colo-Connect.

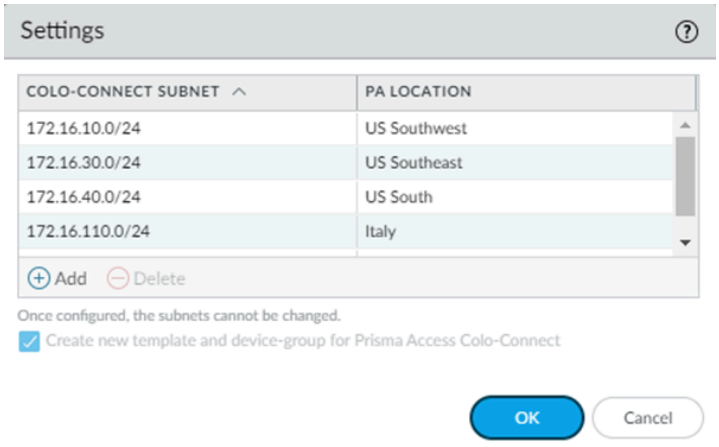
Vous utilisez les sous-réseaux que vous créez ici dans les connexions et connexions aux services que vous créez dans les étapes ultérieures.

1. Depuis le Panorama qui gère Prisma Access, accédez à **Panorama** > **Cloud Services** > **Configuration** > **Colo-Connect** et cliquez sur l'icône en forme d'engrenage pour modifier les paramètres.
2. Cliquez sur **Add (Ajouter)** pour ajouter un **Colo-Connect Subnet (Sous-réseau Colo-Connect)** et sélectionnez un emplacement Prisma Access (**PA Location (Emplacement PA**) pour celui-ci.

   Entrez un sous-réseau minimum de /28.
3. (Facultatif) Si vous prévoyez de créer des instances Colo-Connect pour plus d'un emplacement, ajoutez d'autres sous-réseaux par emplacement.

   Vous pouvez configurer un seul sous-réseau par emplacement.
4. Sélectionnez **Create new templates and device-group for Prisma Access Colo-Connect (Créer de nouveaux modèles et un groupe de périphériques pour Prisma Access Colo-Connect)**.

   La première fois que vous configurez un déploiement Colo-Connect, cochez cette case afin que des modèles et des groupes de périphériques (Colo_Connect_Template et Colo_Connect_Device_Group, respectivement) soient créés pour Colo-Connect. Après avoir créé ces modèles et groupes de périphériques, cette case à cocher est grisée.



 ©2025 Palo Alto Networks, Inc.

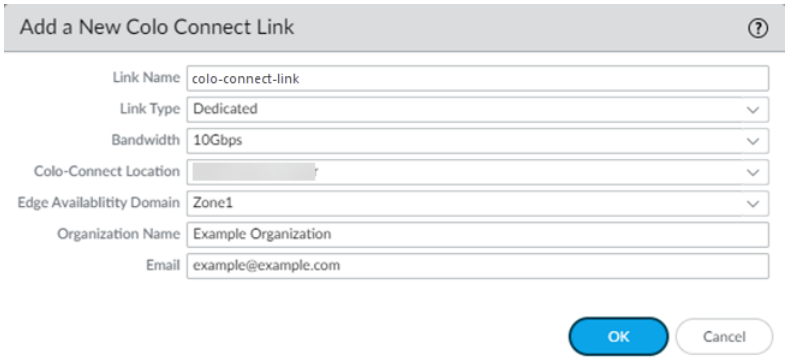
STEP 2 | Ajoutez un nouveau lien Colo-Connect (également appelé *interconnexion*).

1. Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Colo-Connect** > **Colo Connect Link (Lien Colo-Connect)** et cliquez sur **Add (Ajouter)** pour ajouter un lien Colo-Connect.
2. Donnez au lien un **Link Name (Nom de lien)** unique.
3. Sélectionnez une interconnexion **Dedicated (Dédiée)**.
4. Spécifiez les paramètres restants du lien Colo-Connect.
   - Sélectionnez **10Gbps (10 Gbit/s)** ou **20Gbps (20 Gbit/s)** pour la **Bandwidth (Bande passante)**.

     Si vous sélectionnez 20 Gbit/s, vous devez regrouper le lien d'interconnexion dédiée en deux liens de 10 Gbit/s à l'aide du LACP.

     Vous ne pouvez pas changer la bande passante d'un lien d'interconnexion dédiée après l'avoir spécifié et avoir validé et appliqué vos modifications.
   - Sélectionnez un **Colo-Connect Location (Emplacement Colo-Connect)** dans la liste déroulante.

     Assurez-vous que vous sélectionnez le même emplacement que celui utilisé pour l'interconnexion dédiée.
   - Sélectionnez **Zone1** ou **Zone2** pour **Edge Availability Domain (Domaine de disponibilité périphérique)**. Prenez cette valeur dans la zone GCP utilisée pour votre domaine de disponibilité périphérique.
   - Entrez l'**Organization Name (Nom de l'organisation)** à utiliser pour ce lien.
   - Entrez l'**Email (E-mail)** où vous souhaitez recevoir les détails LOA-CFA du fournisseur cloud.
     - GCP utilise cet e-mail pour envoyer la lettre d'autorisation et de cession d'installation de raccordement (LOA-CFA). Assurez-vous que la LOA-CFA est envoyée à votre fournisseur Colo, afin qu'il puisse commencer à installer vos connexions.



STEP 3 | Après la création de la connexion dédiée, l'installation Colo teste vos connexions et vous informe qu'elles ont été testées et sont prêtes à l'emploi.

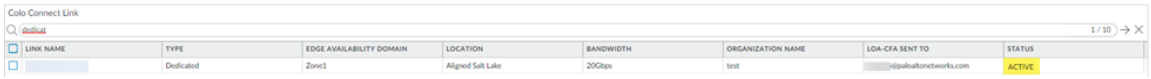
Aucune configuration de Prisma Access n'est requise pour cette étape. Ne créez pas les connexions Colo-Connect dans Prisma Access tant que l'installation Colo ne vous a pas informé qu'elles ont été testées.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Créez les connexions (également appelées *attachements VLAN*) pour Colo-Connect.

1. Assurez-vous que l'état du lien dédié est actif en accédant à **Panorama** > **Cloud Services** > **Configuration** > **Colo-Connect** > **Colo-Connect Link (Lien Colo-Connect**.

   Tant que l'état du lien dédié est actif, vous ne pouvez pas créer de liens Colo-Connect.

2. Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Colo-Connect** > **Onboarding (Intégration)** et cliquez sur **Add (Ajouter)** pour ajouter une nouvelle connexion.
3. Configurez les paramètres de connexion.
   - Saisissez un **Name (Nom)** unique pour la connexion.
   - Sélectionnez un **Link Name (Nom de lien)** parmi les liens que vous avez configurés à une étape précédente.
   - (Facultatif) Entrez un **VLAN ID (ID de VLAN)** pour la connexion.

     Les ID de VLAN sont générés par le fournisseur d'interconnexion (GCP) si vous n'entrez pas manuellement une valeur.
   - Sélectionnez une **Bandwidth (Bande passante)** pour la connexion.

     Vous pouvez choisir entre **1 Gbps (1 Gbit/s)**, **2 Gbps (2 Gbit/s)**, **5 Gbps (5 Gbit/s)**, **10 Gbps (10 Gbit/s)** ou **20 Gbps (20 Gbit/s)**.

     Si vous configurez plusieurs connexions pour une interconnexion, assurez-vous que la bande passante totale des connexions ne dépasse pas la bande passante de l'interconnexion. Par exemple, avec une interconnexion dédiée de 20 Gbit/s, vous

 ©2025 Palo Alto Networks, Inc.

pouvez configurer 10 connexions de 2 Gbit/s chacune, mais vous ne pouvez pas dépasser 20 Gbit/s au total pour toutes les connexions.

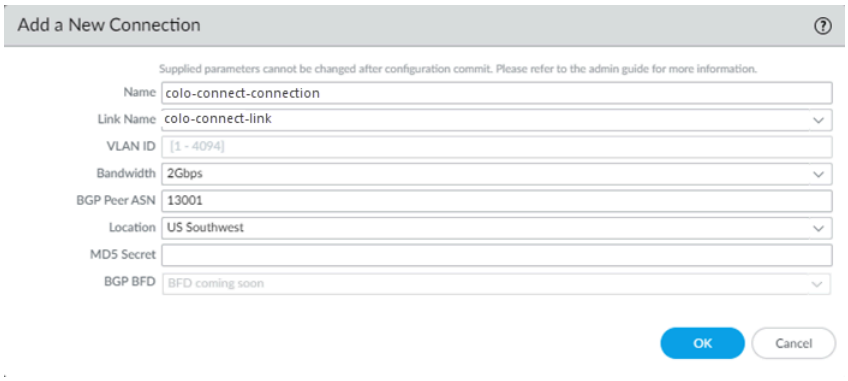
- Entrez un **BGP Peer ASN (ASN homologue BGP)**.

  Entrez le numéro de système autonome (AS) pour le routeur sur site client dans le Colo. La plage se situe entre 1 et 4294967295.

- Sélectionnez le **Location (Emplacement)** parmi les noms de connexion que vous avez créés lors d'une étape précédente.

  Vous devez avoir déjà ajouté un sous-réseau pour tout emplacement que vous spécifiez.

- (Facultatif) Entrez le **MD5 Secret (Secret MD5)** de BGP.



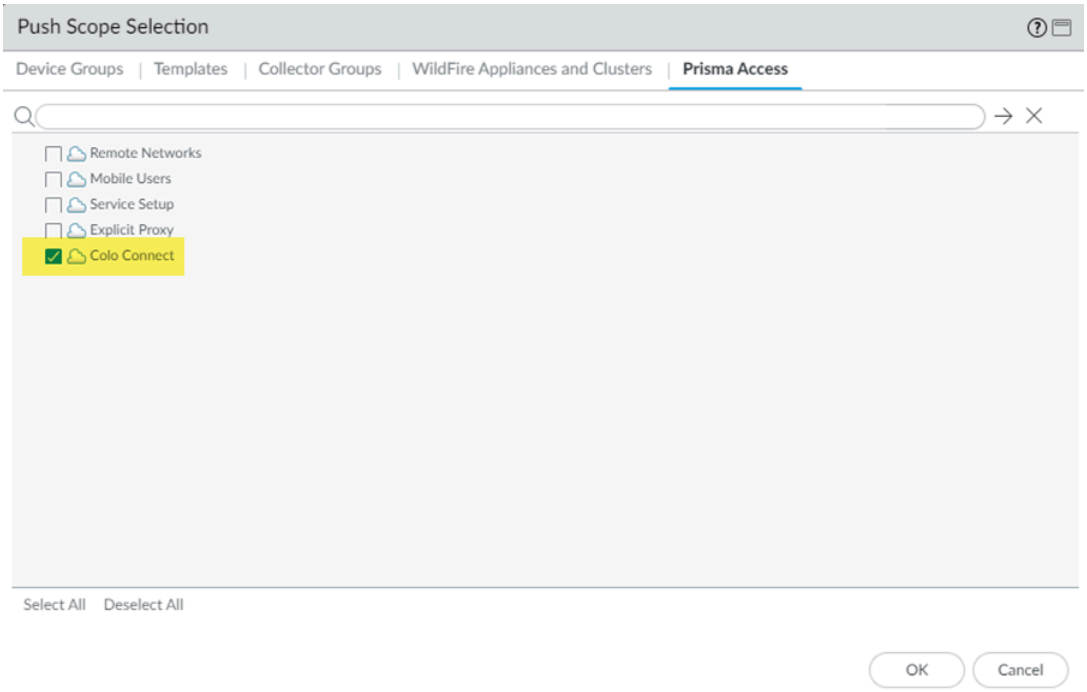
4. Continuez à créer des connexions jusqu'à ce qu'elles soient terminées.

   Vous devez créer deux connexions. Les deux connexions doivent être dans la même région et une connexion doit être dans une zone distincte. Vous utilisez ces connexions dans les connexions aux services que vous créez dans une étape ultérieure.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Validez et appliquez vos modifications.

1. Accédez à **Commit (Valider)** > **Commit and Push (Valider et appliquer)**.
2. Cliquez sur **Edit Selections (Modifier les sélections)** et assurez-vous que Colo-Connect est sélectionné dans l'étendue de la transmission.



3. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.
4. **Commit and Push (Validez et appliquez)** vos modifications.

STEP 6 | Configurez le routage eBGP sur le routeur client.

Vous devez configurer l'appairage BGP pour assurer la connectivité entre le routeur client.

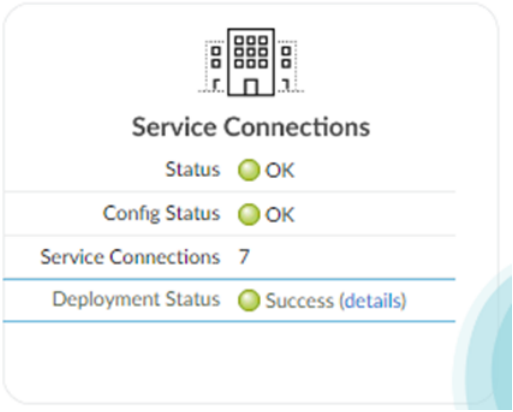
STEP 7 | Configurez les connexions aux services à utiliser avec Colo-Connect.

STEP 8 | Cliquez sur **Commit and Push (Valider et appliquer)** pour valider et appliquer vos modifications de configuration, en vous assurant que **Colo-Connect** est sélectionné dans **Push Scope (Étendue de la transmission)**.

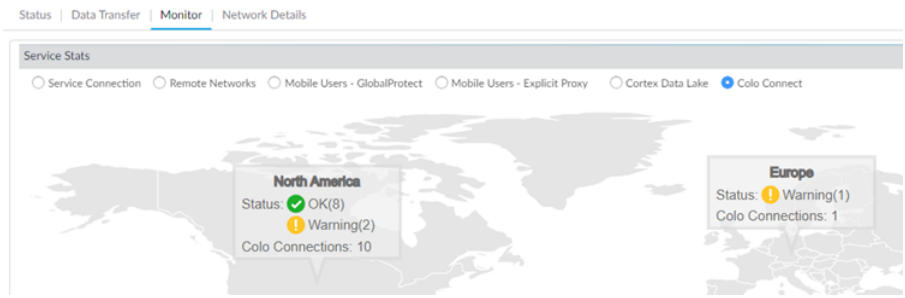
 ©2025 Palo Alto Networks, Inc.

STEP 9 | Vérifiez l'état des connexions Colo-Connect.

1. Pour vérifier l'état d'une connexion aux services utilisée par une connexion Colo-Connect, accédez à **Panorama** > **Cloud Services** > **Status (État)** > > **Colo-Connect** > **Monitor (Surveiller)**.



2. Survolez une région où une connexion Colo-Connect est déployée.
   - Si la connexion Colo-Connect et le routage BGP sont actifs, l'état affiche **OK**.
   - Si la connexion Colo-Connect est active, mais que le routage BGP est inactif, l'état affiche **Warning (Avertissement)**.
   - Si la connexion Colo-Connect et le routage BGP sont inactifs, l'état s'affiche **Down (Inactif)**.
   - Si la connexion Colo-Connect est inactive, mais que le routage BGP est actif, l'état affiche **Error (Erreur)**.

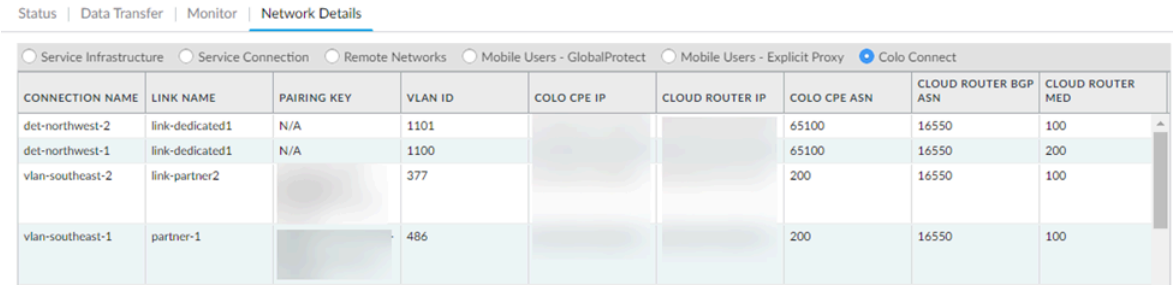


3. Pour plus d'informations, cliquez sur la zone de région et affichez les informations dans l'onglet **Status (État)**.

 ©2025 Palo Alto Networks, Inc.

STEP 10 | Vérifiez les détails du réseau des connexions Colo-Connect en accédant à **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Colo-Connect** et en consultant les détails.

Pour les liens dédiés, la **Pairing Key (Clé de couplage)** s'affiche comme **N/A (S.O.)**.



CONNECTION NAME	LINK NAME	PAIRING KEY	VLAN ID	COLO CPE IP	CLOUD ROUTER IP	COLO CPE ASN	CLOUD ROUTER BGP ASN	CLOUD ROUTER MED
det-northwest-2	link-dedicated1	N/A	1101			65100	16550	100
det-northwest-1	link-dedicated1	N/A	1100			65100	16550	200
vlan-southeast-2	link-partner2		377			200	16550	100
vlan-southeast-1	partner-1		486			200	16550	100

Configurer le routage VLAN eBGP sur le routeur client

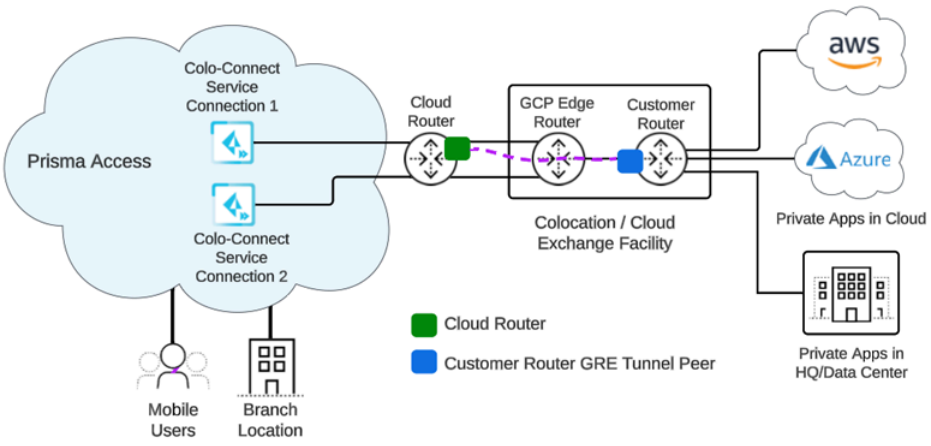
GCP crée des adresses IP pour le routeur client (Colo) et le routeur cloud pendant ces étapes de déploiement :

- Pour les interconnexions partenaires, GCP crée les adresses IP une fois la clé de couplage consommée par votre Colo (par exemple, Equinix).
- Pour les interconnexions dédiées, GCP crée les adresses IP une fois que vous avez intégré vos connexions Colo-Connect (attachements VLAN) et validé et appliqué vos modifications.

Pour assurer un routage correct, vous devez :

- Configurez l'adresse IP du routeur Colo (**Colo CPE IP** dans l'interface utilisateur Prisma Access) comme l'adresse IP VLAN locale et l'adresse IP eBGP locale.
- Configurez l'adresse IP du routeur cloud (**Cloud Router IP (IP du routeur cloud)**) comme adresse de l'homologue eBGP sur votre routeur Colo.

Une fois terminé, eBGP est configuré pour la connexion (attachement VLAN) entre le routeur Colo et le routeur cloud.



La création de ce routage est la première étape de la configuration du routage tunnel GRE. Vous terminez le routage du tunnel GRE lorsque vous configurez les tunnels GRE pendant la configuration de la connexion aux services.

 ©2025 Palo Alto Networks, Inc.

Suivez les étapes suivantes pour configurer le routage entre le Colo et le routeur cloud.

STEP 1 | Depuis le Panorama qui gère Prisma Access, créez les sous-réseaux, les liens et les connexions, puis cliquez sur **Commit and Push (Valider et appliquer)** vos modifications.

Utilisez le flux de travail spécifique à votre type d'interconnexion (Partenaire ou Dédiée) Pour les interconnexions partenaires, assurez-vous d'avoir collé la clé de couplage dans le VLAN Colo.

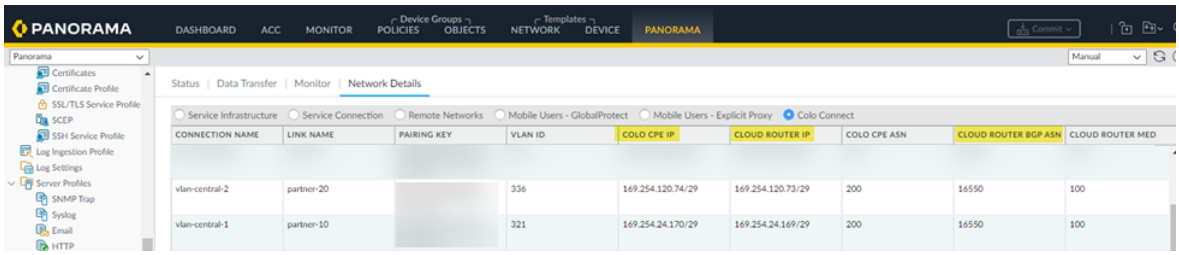
STEP 2 | Accédez à **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Colo-Connect**.

STEP 3 | Notez les éléments de connexion suivants :

- **Colo CPE IP**
- **IP de routeur cloud**
- **Routeur cloud BGP ASN**

Dans l'exemple suivant :

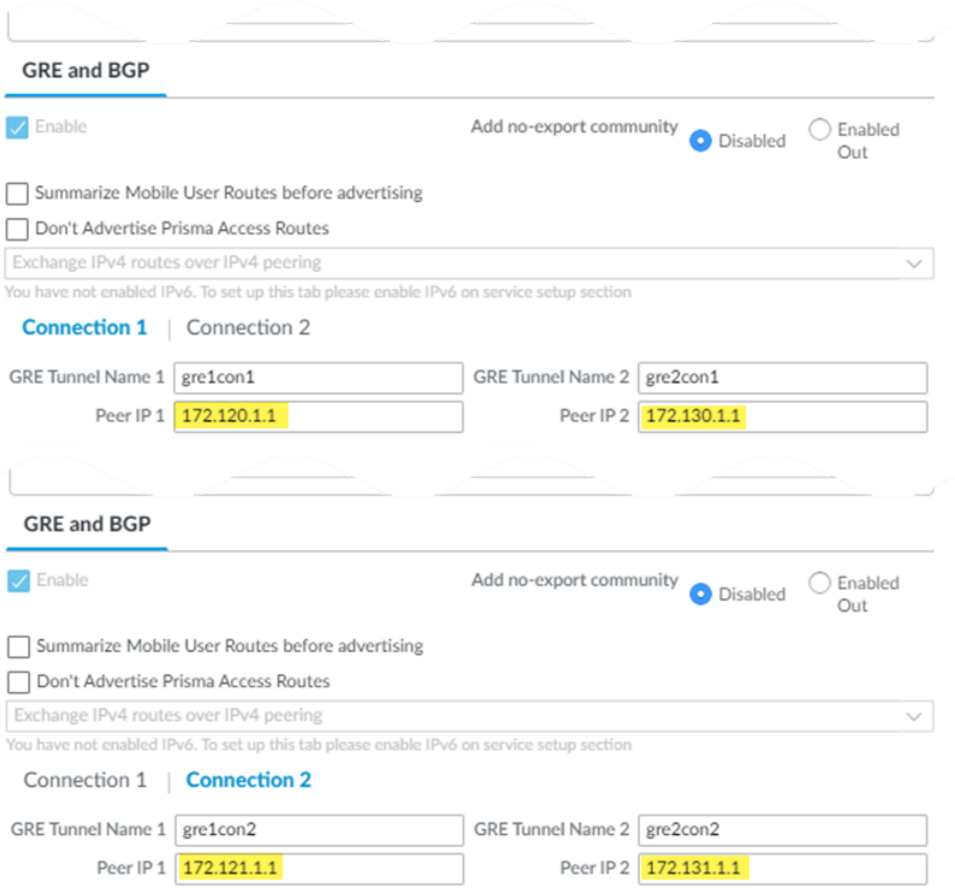
- Pour la connexion vlan-central-1, la **Colo CPE IP** est 169.254.24.170/29, la **Cloud Router IP (IP de routeur cloud)** est 169.254.24.169/29 et le **Cloud Router BGP ASN (Routeur cloud BGP ASN)** est 16550
- Pour la connexion vlan-central-2, la **Colo CPE IP** est 169.254.120.74/29, la **Cloud Router IP (IP de routeur cloud)** est 169.254.120.73/29 et le **Cloud Router BGP ASN (Routeur cloud BGP ASN)** est 16550.
- .



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Déterminez les adresses IP que vous utiliserez pour les adresses IP GRE locales lorsque vous configurerez les connexions aux services Colo-Connect.

Vous les configurez lorsque vous mettez en place une connexion aux services Colo-Connect (**Panorama** > **Cloud Services** > **Configuration** > **Service Connection (Connexion aux services)**) dans les zones **Peer IP 1 (IP de l'homologue 1)** et **Peer IP 2 (IP de l'homologue 2)**.



Si vous configurez une connexion aux services pour prendre en charge jusqu'à 10 Gbit/s de débit, mettez un tunnel chacun dans la **Connection 1 (Connexion 1)** et la **Connection 2 (Connexion 2)**, pour un total de deux tunnels dans chaque connexion aux services.

Si vous configurez une connexion aux services pour prendre en charge plus de 10 Gbit/s de débit (jusqu'à 20 Gbit/s), mettez deux tunnels chacun dans la **Connection 1 (Connexion 1)** et la **Connection 2 (Connexion 2)**, pour un total de quatre tunnels dans chaque connexion aux services.

Les exemples suivants montrent qu'un tunnel est configuré pour un débit supérieur à 10 Gbit/s. Deux tunnels par connexion sont donc utilisés et ils utilisent les adresses IP de l'homologue suivantes :

- 172.120.1.1 pour la connexion 1
- 172.130.1.1 pour la connexion 1
- 172.121.1.1 pour la connexion 2
- 172.131.1.1 pour la connexion 2

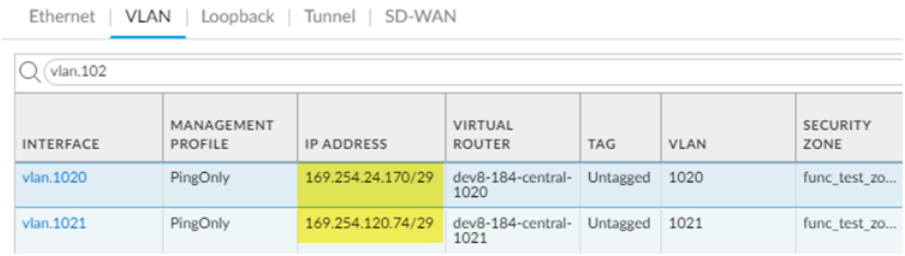
 ©2025 Palo Alto Networks, Inc.

STEP 5 | Connectez-vous au routeur Colo.

Les captures d'écran de configuration suivantes utilisent un pare-feu nouvelle génération Palo Alto Networks comme routeur Colo.

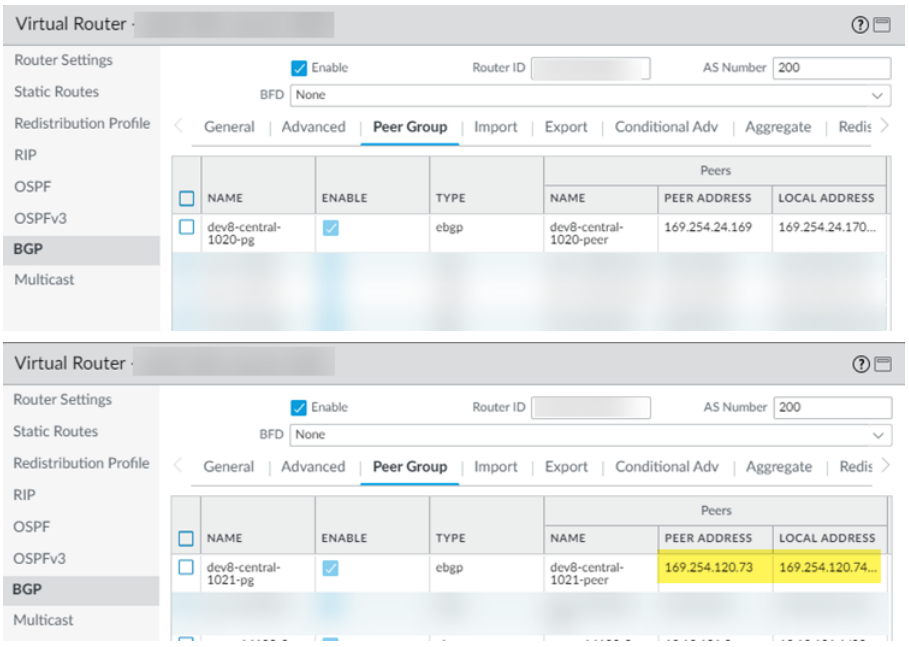
STEP 6 | Ajoutez une interface VLAN, en spécifiant l'adresse **Colo CPE IP** comme adresse IP.

Si vous utilisez un pare-feu nouvelle génération comme routeur Colo, accédez à **Network (Réseau)** > **Interfaces** > **VLAN** et **Add (Ajouter)** l'interface VLAN, en spécifiant le nom du **Virtual Router (Routeur virtuel)**.



STEP 7 | Configurez l'adresse IP du routeur Colo (**Colo CPE IP**) comme adresse IP eBGP locale et configurez l'adresse IP du routeur cloud (**IP de routeur cloud**) comme adresse de l'homologue eBGP sur votre routeur Colo.

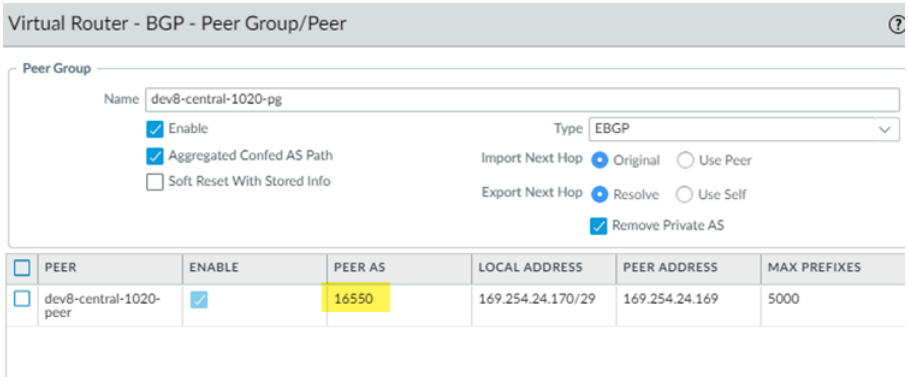
Si vous utilisez un pare-feu nouvelle génération comme routeur Colo, accédez à **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, cliquez sur **Add (Ajouter)** pour ajouter un routeur virtuel, accédez à **BGP** > **Peer Group (Groupe d'homologues)** et entrez **Colo CPE IP** comme **Peer Address (Adresse de l'homologue)** et **Cloud Router IP (IP de routeur cloud)** comme **Local Address (Adresse locale)**.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | Configurez le **Cloud Router BGP ASN (Routeur cloud BGP ASN)** en tant que numéro de système autonome (ASN) de l'homologue eBGP.

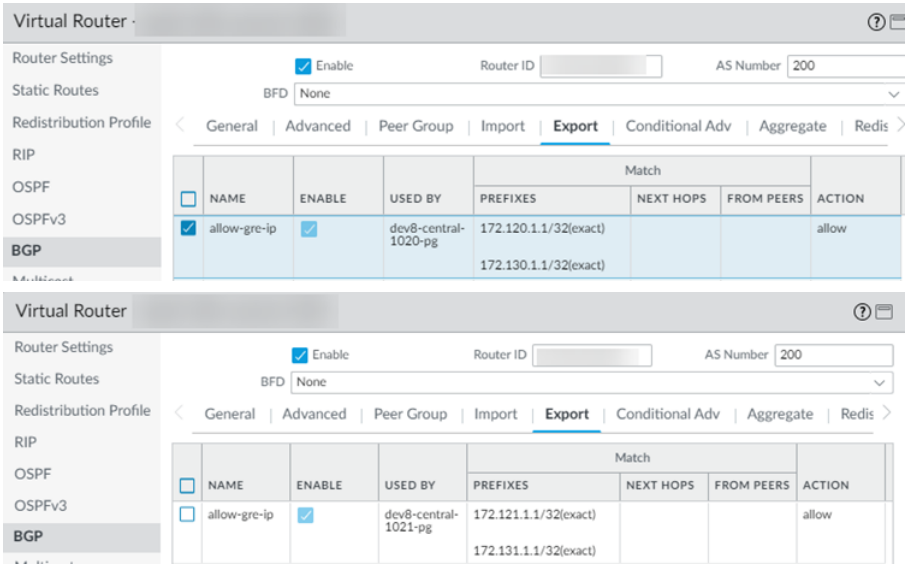
Si vous utilisez un pare-feu nouvelle génération comme routeur Colo, accédez à **Network (Réseau** > **Virtual Routers (Routeurs virtuels)**, **Add (Ajouter)** un routeur virtuel, accédez à **BGP** > **Peer Group (Groupe d'homologues)**, cliquez sur **Add (Ajouter)** pour ajouter un groupe d'homologues et sélectionnez un **Peer AS (AS de l'homologue** de **16500**.



STEP 9 | Créez une politique d'exportation BGP qui autorise uniquement l'adresse IP GRE locale à être annoncée à l'adresse IP de l'homologue du routeur cloud.

Puisque les routeurs cloud ne peuvent recevoir qu'un nombre limité d'itinéraires, vous devez créer des politiques afin que seul le routage entre les adresses IP des tunnels GRE de connexion aux services soit envoyé au routeur cloud.

Si vous utilisez un pare-feu nouvelle génération comme routeur Colo, accédez à **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, **Add (Ajouter)** un routeur virtuel, accédez à **BGP** > **Export (Exporter)**, cliquez sur **Add (Ajouter)** pour ajouter une règle d'exportation, et sur **Match (Faire correspondre)** pour faire correspondre les adresses IP utilisées comme adresse IP de l'homologue et créez une **Action Allow (Autorisation)**.



STEP 10 | Créez les connexions aux services Colo-Connect.

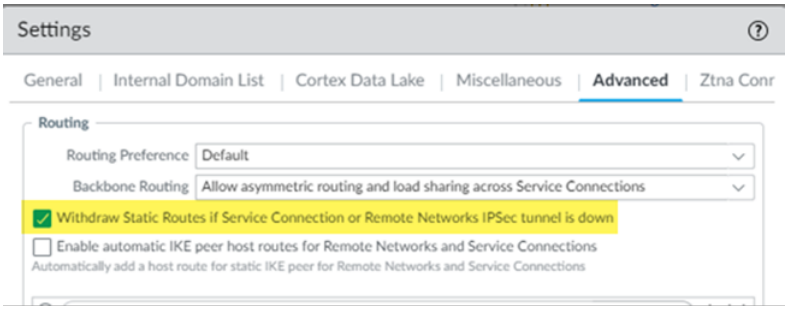
 ©2025 Palo Alto Networks, Inc.

Créer des connexions aux services Colo-Connect

Colo-Connect utilise des connexions aux services, mais elles diffèrent des connexions aux services Prisma Access, car elles utilisent des tunnels GRE au lieu de tunnels IPSec et utilisent toujours BGP pour le routage. Pour configurer les connexions aux services Colo-Connect, procédez comme suit.

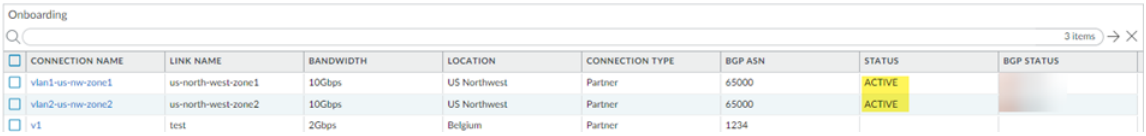
STEP 1 | Depuis le Panorama qui gère Prisma Access, assurez-vous que Prisma Access retire les itinéraires statiques en accédant à **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)**, en cliquant sur l'icône en forme d'engrenage pour modifier les **Settings (Paramètres)** et en sélectionnant **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down (Supprimer les itinéraires statiques si la connexion aux services ou le tunnel IPSec du réseau distant est inactif)**.

Sélectionner cette option garantit que, si le tunnel GRE est inactif, l'itinéraire statique utilisé par le tunnel GRE est retiré.



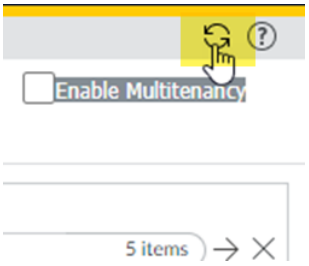
STEP 2 | Accédez à l'onglet **Colo-Connect** et assurez-vous que les connexions sont dans un état **Active (Actif)** en vérifiant le champ **Status (État)** dans la zone d'intégration.

Tant que le **Status (État)** de la connexion est **Active (Actif)**, vous ne pouvez pas configurer les connexions aux services.



STEP 3 | Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Service Connection (Connexion aux services)**

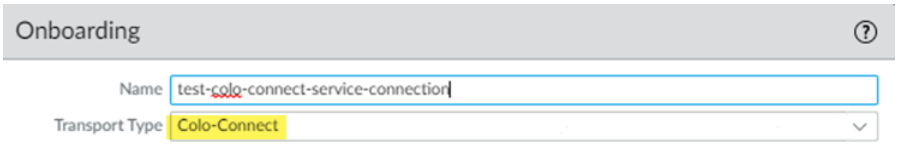
STEP 4 | Cliquez sur **Refresh (Actualiser)** en haut à droite de l'interface utilisateur Panorama afin que la configuration Colo-Connect soit provisionnée dans la zone des connexions aux services.



 ©2025 Palo Alto Networks, Inc.

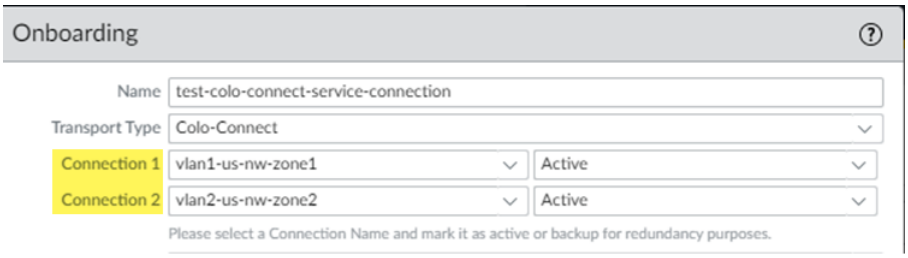
STEP 5 | Cliquez sur **Add (Ajouter)** pour ajouter une connexion aux services, donnez-lui un **Name (Nom)** unique et sélectionnez un **Transport Type (Type de transport) Colo-Connect**.

Assurez-vous que le nom que vous saisissez fait 31 caractères ou moins ; la saisie d'un nom de 32 caractères ou plus provoque une mauvaise cartographie du tunnel dans l'infrastructure Prisma Access.



STEP 6 | Sélectionnez deux connexions à utiliser avec les connexions aux services (**Connection 1 (Connexion 1)** et **Connection 2 (Connexion 2)**).

Ces connexions doivent être dans deux zones différentes.



STEP 7 | Sélectionnez **Active (Actif)** ou **Backup (Sauvegarde)** pour la **Connection 1 (Connexion 1)** et la **Connection 2 (Connexion 2)**.

Utilisez ces directives lors de la configuration des connexions aux services :

- Vous pouvez configurer les connexions dans ces modes :
  - **Active (Actif)/Active (Actif)**
  - **Active (Actif)/Backup (Sauvegarde)**
  - **Backup (Sauvegarde)/Active (Actif)**

  La configuration des deux connexions en mode **Backup (Sauvegarde)/Backup (Sauvegarde)** n'est pas valide et n'est pas prise en charge.
- La bande passante des connexions doit être la même pour tous les modes.
- Les connexions doivent être dans des zones différentes.
- La bande passante maximale que vous pouvez spécifier pour une connexion de service est de 20 Gbit/s. Si vous spécifiez une **Bandwidth (Bande passante)** de **20 Gbps (20 Gbit/s)** pour une connexion, vous ne pouvez pas utiliser cette connexion dans une configuration **Active (Actif)/Active (Actif)** (elle doit être définie comme **Active (Actif)/Backup (Sauvegarde)**).
- Ne mélangez pas les interconnexions dédiées et partenaires dans la même connexion aux services, et assurez-vous que les connexions aux services utilisent des zones différentes. Ce tableau montre les configurations autorisées et interdites pour les connexions aux services,

 ©2025 Palo Alto Networks, Inc.

en supposant que les zones, les emplacements, la bande passante et les rôles suivent les directives et exigences de connexion aux services :

Connection 1 Belongs To (Connexion 1 appartient à)	Connection 2 Belongs To (Connexion 2 appartient à)	Valid Colo-Connect Service Connection Configuration? (Configuration de connexion aux services Colo-Connect valide ?)
Partner Connect 1 (Connexion partenaire 1)	Partner Connect 2 (Connexion partenaire 2)	Yes (Oui)
Dedicated Connect 1 (Connexion dédiée 1)	Dedicated Connect 2 (Connexion dédiée 2)	Yes (Oui)
Partner Connect 1 (Connexion partenaire 1)	Partner Connect 1 (Connexion partenaire 1)	No (Non)
Dedicated Connect 1 (Connexion dédiée 1)	Dedicated Connect 1 (Connexion dédiée 1)	No (Non)
Partner Connect (Connexion partenaire)	Dedicated Connect (Connexion dédiée)	No (Non)

STEP 8 | (Facultatif, déploiements de routage hot potato uniquement) Sélectionnez une connexion aux services à utiliser comme sauvegarde préférée (SC de secours).

Vous ne pouvez sélectionner qu'une connexion aux services configurée en tant que connexion aux services Colo-Connect. Prisma Access utilise la sauvegarde SC que vous sélectionnez comme connexion aux services préférée en cas d'échec de connexion. La sélection d'une connexion de service de sauvegarde peut éviter les problèmes de routage asymétrique si vous avez intégré plus de deux connexions de service.

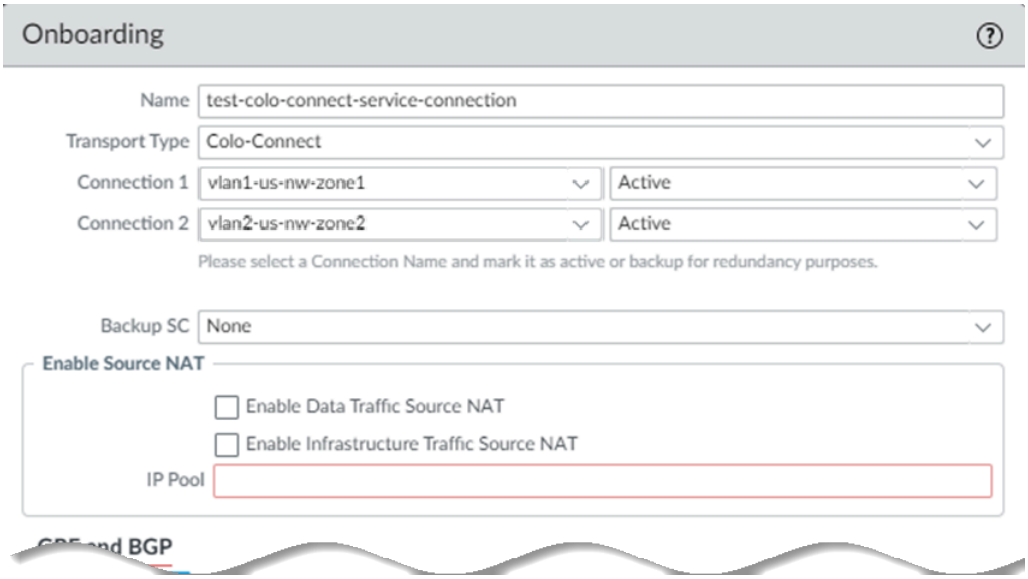
STEP 9 | (Facultatif) Activez le NAT source pour les utilisateurs mobiles : adresses du pool d'adresses IP GlobalProtect, adresses IP dans le sous-réseau Infrastructure, ou les deux.

Vous pouvez spécifier un sous-réseau au niveau d'une ou plusieurs connexions aux services utilisées pour le trafic NAT entre les utilisateurs mobiles Prisma Access GlobalProtect et les applications et ressources privées d'un centre de données.

- **Activer le NAT source de trafic de données** : effectue le NAT sur les adresses du pool d'adresses IP des utilisateurs mobiles afin qu'elles ne soient pas annoncées au centre de données et que seuls les sous-réseaux que vous spécifiez aux connexions aux services soient annoncés et acheminés dans le centre de données.
- **Activer le NAT source de trafic d'infrastructure** : effectue le NAT sur les adresses du sous-réseau d'infrastructure afin qu'elles ne soient pas annoncées au centre de données et que seuls les sous-réseaux que vous spécifiez aux connexions aux services soient annoncés et acheminés dans le centre de données.
- **IP Pool (Pool d'adresses IP)** : spécifie le pool d'adresses IP utilisé pour effectuer le NAT sur le pool d'adresses IP des utilisateurs mobiles, le sous-réseau d'infrastructure ou les deux. Utilisez un sous-réseau IP privé (RFC 1918) ou un sous-réseau approprié qui est

 ©2025 Palo Alto Networks, Inc.

routable dans votre domaine de routage et qui ne chevauche pas le pool d'adresses IP des utilisateurs mobiles – Pool d'adresses IP GlobalProtect ou le sous-réseau d'infrastructure. Entrez un sous-réseau entre /25 et /32.



STEP 10 | Dans la zone **GRE and BGP (GRE et BGP)**, configurez les paramètres du tunnel GRE et du BGP pour la connexion aux services.

BGP est toujours réglé sur **Enable (Activer)**.

1. (Facultatif) Choisissez parmi les options suivantes :

   - Pour ajouter une communauté de **no-export (non-export)** pour les nœuds d'accès d'entreprise (connexions aux services) aux préfixes sortants des homologues eBGP de l'équipement sur site client (CPE), définissez **Add no-export community (Ajouter une communauté de non-export)** sur **Enabled Out (Sortie activée)**. Cette option est **Disabled (Désactivée)** par défaut.

     N'utilisez pas cette option en mode routage hot potato.

   - Pour empêcher le pair BGP Prisma Access de transférer des itinéraires dans le réseau de votre organisation. Cliquez sur **Don't Advertise Prisma Access Routes (Ne pas publier les itinéraires Prisma Access)**.

     Par défaut, Prisma Access publie toutes les informations de routage BGP, y compris les itinéraires locaux et tous les préfixes qu'il reçoit d'autres connexions aux services, réseaux distants et sous-réseaux d'utilisateurs mobiles. Cochez cette case pour empêcher Prisma Access d'envoyer des publicités BGP, mais utilisez quand même les informations BGP qu'il reçoit pour apprendre les itinéraires d'autres voisins BGP.

     Puisque Prisma Access n'envoie pas de publicités BGP si vous sélectionnez cette option, vous devez configurer des itinéraires statiques sur l'équipement local pour établir des itinéraires de retour vers Prisma Access.

   - Pour réduire le nombre de publicités de sous-réseaux IP d'utilisateurs mobiles sur le BGP de votre équipement sur site client (CPE), sélectionnez **Summarize Mobile User**

 ©2025 Palo Alto Networks, Inc.

Routes before advertising (Résumer les itinéraires des utilisateurs mobiles avant de publier).

Par défaut, Prisma Access publie les pools d'adresses IP des utilisateurs mobiles par blocs de sous-réseaux /24. Si vous les résumez, Prisma Access publie le pool en fonction du sous-réseau que vous avez spécifié. Par exemple, Prisma Access publie un pool d'adresses IP mobiles d'utilisateurs publics de 10.8.0.0/20 en utilisant le sous-réseau /20, plutôt que de diviser le pool en sous-réseaux de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, et ainsi de suite, avant de les publier. Le résumé de ces publicités peut réduire le nombre d'itinéraires stockés dans les tableaux de routage CPE. Par exemple, vous pouvez utiliser le résumé de pool d'adresses IP avec des passerelles VPN cloud (passerelles privées virtuelles [VGW] ou passerelles de transit [TGW]) qui peuvent accepter un nombre limité d'itinéraires.

Si vous avez activé le routage hot potato et que vous activez le résumé des itinéraires, Prisma Access ne présuppose plus les AS-PATH, ce qui peut provoquer un routage asymétrique. Assurez-vous que votre trafic de retour du centre de données ou de l'emplacement du siège a garanti un retour symétrique avant d'activer le résumé des itinéraires avec le routage hot potato.

2. Configurez le routage pour la connexion aux services en utilisant les tunnels GRE.
3. Depuis Panorama qui gère Prisma Access, revenez à **Panorama** > **Cloud Service** > **Configuration** > **Service Connexion (Connexion aux services)** un tunnel GRE pour **Connection 1 (Connexion 1)** en saisissant un **GRE Tunnel Name 1 (Nom de tunnel GRE 1)** et une **Peer IP 1 (Adresse IP de l'homologue 1)** pour la **Connection 1 (Connexion 1)** et, si plus de 10 Gbit/s de bande passante sont requis, en saisissant un **GRE Tunnel Name 2 (Nom de tunnel GRE 2)** et une **Peer IP 2 (Adresse IP de l'homologue 2)** pour le deuxième tunnel pour la connexion 1. Puis, créez un tunnel GRE pour la **Connection 2 (Connexion 2)** en répétant ces mêmes étapes.

   Chaque paire de tunnels GRE dans une connexion prend en charge un maximum de 10 Gbit/s de bande passante. Si vous avez besoin de plus de 10 Gbit/s de bande passante, configurez deux tunnels par connexion. Par exemple :

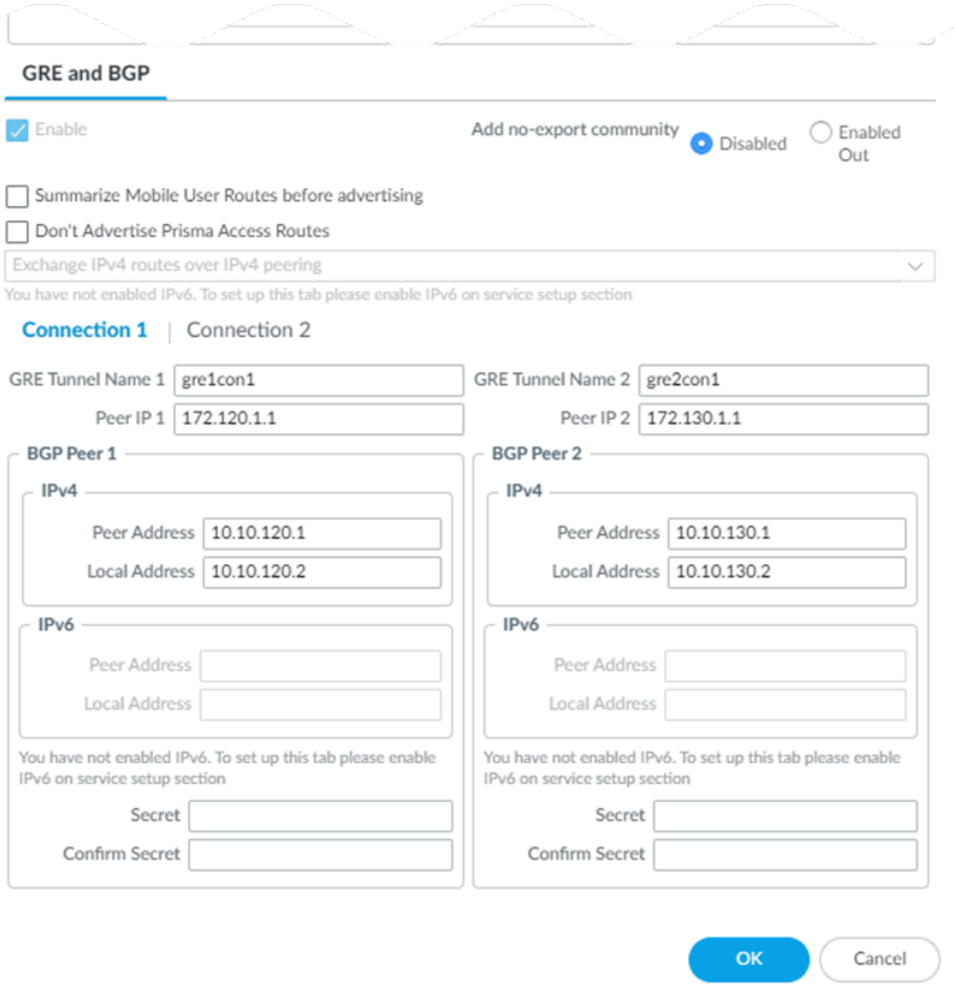
   Pour l'IP de l'homologue, entrez l'adresse IP GRE du routeur sur site dans le Colo.

   Utilisez des adresses IPv4 pour les valeurs BGP ; IPv6 n'est pas pris en charge.
4. Entrez la **Peer Address (Adresse de l'homologue)** et la **Local Address (Adresse locale)** pour l'homologue BGP 1 et, si un second tunnel est requis pour la connexion 1, l'homologue BGP 2.

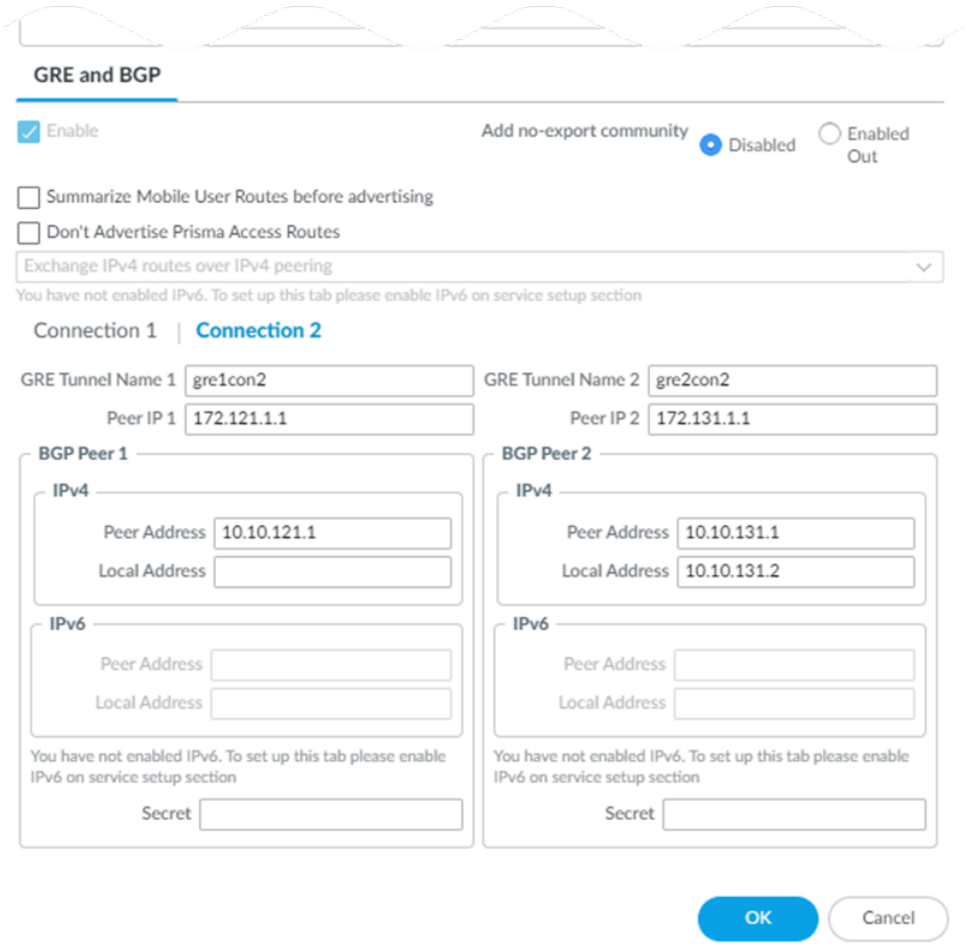
   Pour **Peer Address (Adresse de l'homologue)**, entrez l'adresse IP de l'homologue BGP du routeur Colo. Pour **Local Address (Adresse locale)**, entrez l'adresse qui sera utilisée pour l'établissement du réseau BGP sur le tunnel GRE.

 ©2025 Palo Alto Networks, Inc.

5. (Facultatif) Pour configurer un secret BGP, saisissez les valeurs **Secret** et **Confirm Secret (Confirmer secret)**.



 ©2025 Palo Alto Networks, Inc.

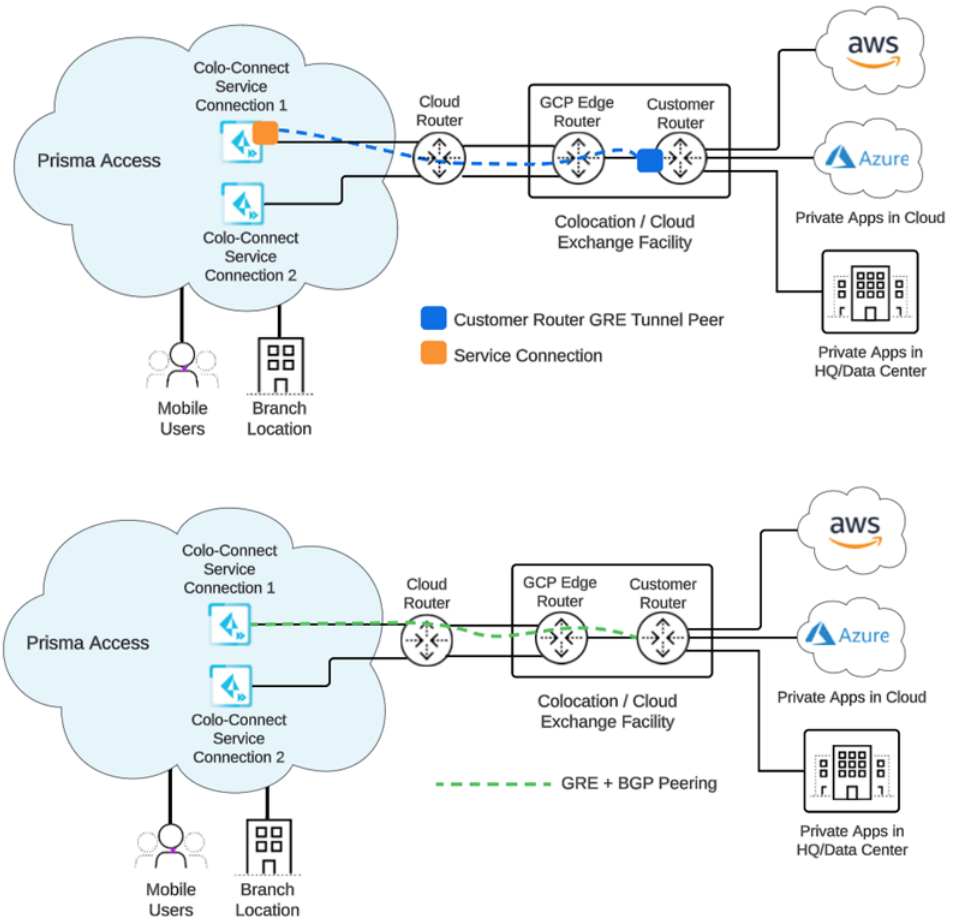


STEP 11 | Cliquez sur **Commit and Push (Valider et appliquer)** pour valider et appliquer vos modifications de configuration, en vous assurant que **Colo-Connect** est sélectionné dans **Push Scope (Étendue de la transmission)**.

Configurer le routage pour la connexion aux services à l'aide des tunnels GRE

Le routeur Colo publie son adresse IP de l'homologue du tunnel GRE au routeur cloud, et apprend le sous-réseau pour le tunnel GRE à partir du routeur cloud. Lorsque vous avez configuré pour la première fois le routage eBGP sur le VLAN du routeur client, vous avez annoncé la possibilité d'atteindre localement les tunnels GRE. Après que le routeur cloud et le routeur Colo aient annoncé et appris les itinéraires pour le sous-réseau Colo et les adresses IP GRE locales l'un de l'autre, les tunnels GRE utilisés par la connexion aux services deviennent actifs.

 ©2025 Palo Alto Networks, Inc.



Pour configurer le routage et ajouter des tunnels GRE aux connexions aux services, suivez les étapes suivantes.

STEP 1 | Notez les adresses IP que vous utiliserez pour la **Peer Address (Adresse de l'homologue)** et la **Local Address (Adresse locale)** pour l'homologue BGP 1 et, si un second tunnel est nécessaire pour la connexion 1, l'homologue BGP 2.

Les exemples suivants utilisent les adresses homologues et locales suivantes :

- **Peer Address (Adresse de l'homologue)** — 10.10.120.0 et 10.10.130.1 pour la connexion 1, 10.10.120.2 et 10.10.130.2 pour la connexion 2
- **Local Address (Adresse locale)** — 10.10.120.2 et 10.10.130.2 pour la connexion 1, 10.10.121.2 et 10.10.131.2 pour la connexion 2

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Notez les adresses IP que vous utiliserez pour l'adresse **Peer IP 1 (IP de l'homologue 1)** et, si nécessaire, l'adresse **Peer IP 2 (IP de l'homologue 2)** dans les connexions aux services.

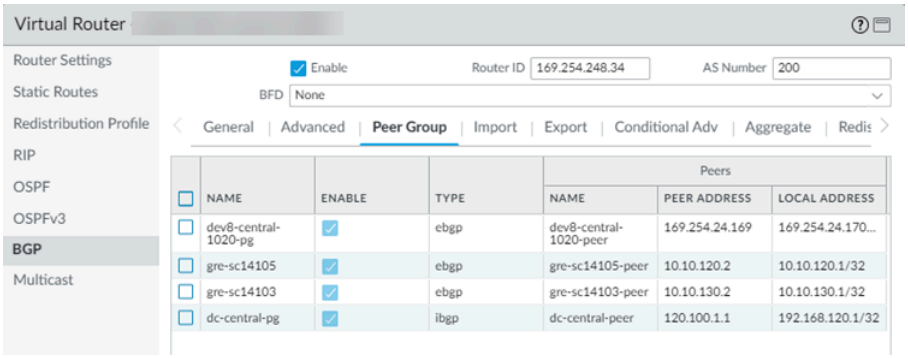
Vous utilisez ces adresses IP pour créer une politique de déni qui empêche l'adresse IP GRE locale d'être annoncée à la connexion aux services Colo-Connect.

Tous les exemples de ce document utilisent ces adresses IP :

- 172.120.1.1 pour la connexion 1
- 172.130.1.1 pour la connexion 1
- 172.121.1.1 pour la connexion 2
- 172.131.1.1 pour la connexion 2

STEP 3 | Configurez les groupes d'homologues pour les adresses IP de l'homologue et locales.

Si vous utilisez un pare-feu nouvelle génération comme routeur Colo, accédez à **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, cliquez sur **Add (Ajouter)** pour ajouter un routeur virtuel, accédez à **BGP** > **Peer Group (Groupe d'homologues)**, et saisissez l'adresse de l'homologue comme **Peer Address (Adresse de l'homologue)** et la **Local Address (Adresse locale)** comme **Local Address (Adresse locale)**.



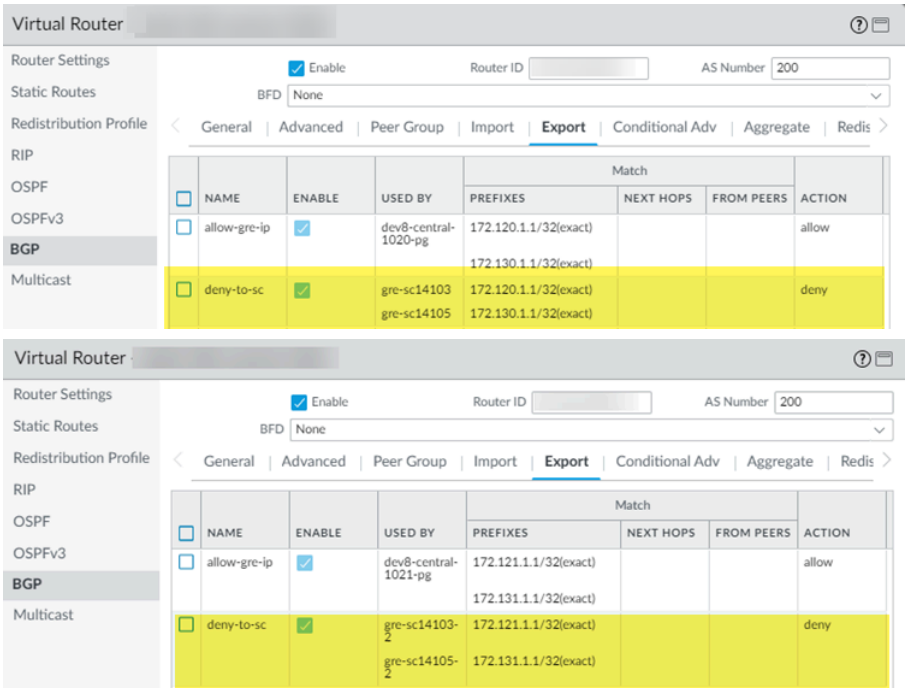
STEP 4 | Créez une politique d'exportation du BGP pour refuser les adresses IP d'homologues que vous avez configurées (172.120.1.1, 172.130.1.1, 172.121.1.1 et 172.131.1.1) et les appliquer aux groupes d'homologues que vous avez créés.

Cette politique d'exportation place une règle de DÉNI sur les adresses IP d'homologues du tunnel GRE local et permet à tous les autres itinéraires d'être publiés sur la connexion aux services.

Si vous utilisez un pare-feu nouvelle génération comme routeur Colo, accédez à **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, cliquez sur **Add (Ajouter)** pour ajouter un routeur virtuel, accédez à **BGP** > **Export (Exporter)**, cliquez sur **Add (Ajouter)** pour ajouter une

 ©2025 Palo Alto Networks, Inc.

règle d'exportation, et sur **Match (Faire correspondre)** pour faire correspondre les adresses IP utilisées comme adresse IP de l'homologue et créez une **Action Deny (Déni)**.



Augmenter ou diminuer la bande passante d'une connexion aux services Colo-Connect

Lorsque vous configurez des connexions aux services, vous configurez la bande passante en fonction des connexions (attachements VLAN) que vous lui associez. Vous allouez deux connexions par connexion aux services, puis vous allouez un ou deux tunnels GRE par connexion.

Alors que chaque connexion aux services Colo-Connect prend en charge un maximum de 20 Gbit/s, chaque tunnel GRE de la connexion aux services prend en charge 10 Gbit/s. Pour cette raison, vous devrez peut-être ajouter ou supprimer les tunnels GRE dans la connexion aux services Colo-Connect ou modifier la bande passante totale dans un lien, ce qui entraînera une augmentation de la bande passante de la connexion aux services au-dessus ou en dessous de 10 Gbit/s.

Augmenter la bande passante d'une connexion aux services Colo-Connect

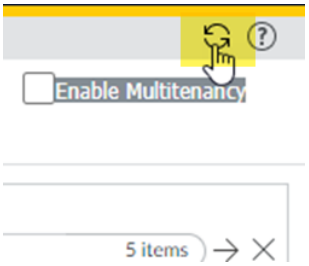
Pour augmenter la bande passante d'une connexion aux services existante au-delà de 10 Gbit/s, procédez comme suit :

STEP 1 | Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Colo-Connect**.

STEP 2 | Accédez **Panorama** > **Cloud Services** > **Configuration** > **Service Connection (Connexion aux services)** et cliquez sur **Refresh (Actualiser)** en haut à droite de l'interface utilisateur

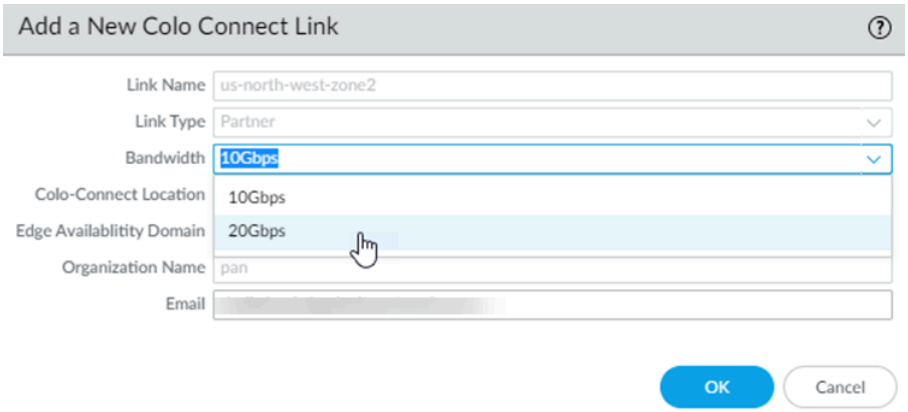
 ©2025 Palo Alto Networks, Inc.

de Panorama afin que la configuration Colo-Connect soit provisionnée dans la zone des connexions aux services.



STEP 3 | Sélectionnez le **Link Name (Nom du lien)** associé à la connexion aux services.

STEP 4 | Augmentez la **Bandwidth (Bande passante)** du lien (interconnexion).

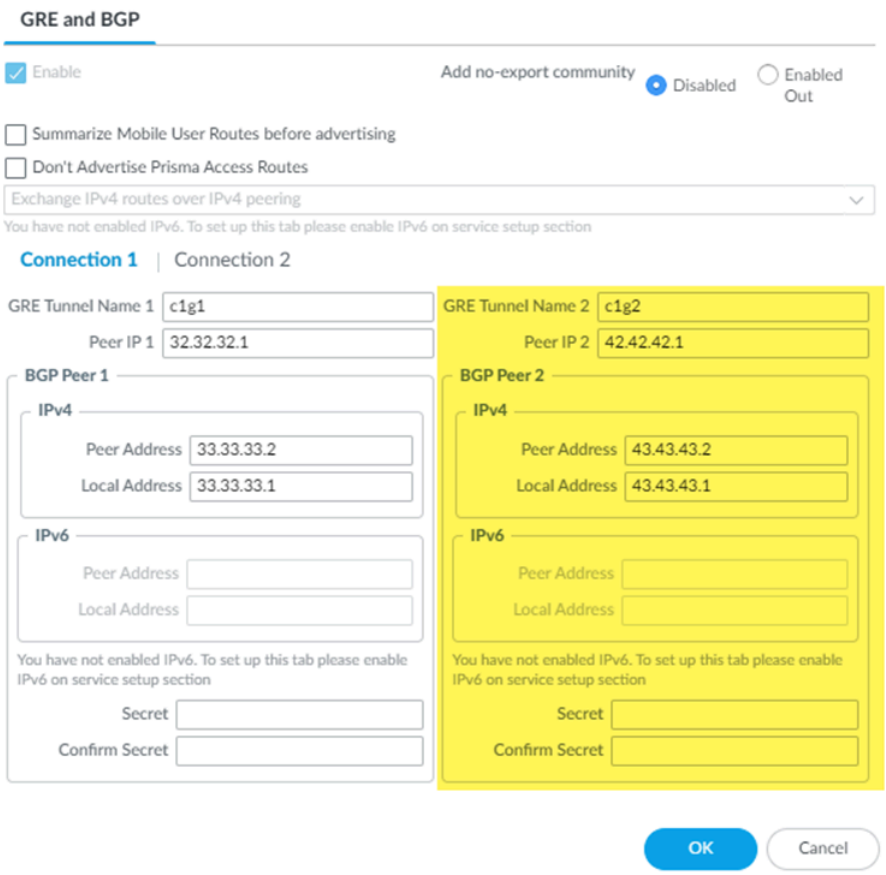


STEP 5 | Cliquez sur **Commit and Push (Valider et appliquer)** pour valider et appliquer vos modifications, en sélectionnant uniquement **Colo-Connect** dans la **Push Scope (Étendue de la transmission)**.

STEP 6 | Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Service Connection (Connexion aux services)** > ***<service-connection-name>*** > **Onboarding (Intégration)**.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Ajoutez le tunnel GRE supplémentaire à la connexion aux services Colo-Connect.



STEP 8 | Cliquez sur **Commit and Push (Valider et appliquer)** pour valider et appliquer vos modifications, en sélectionnant **Service Connections (Connexions aux services)** dans la **Push Scope (Étendue de la transmission)**.

STEP 9 | Ajoutez les adresses IP locales (d'homologues) GRE à vos politiques d'exportation pour le routage VLAN eBGP et le routage de connexion aux services pour les tunnels GRE.

Diminuer la bande passante d'une connexion aux services Colo-Connect

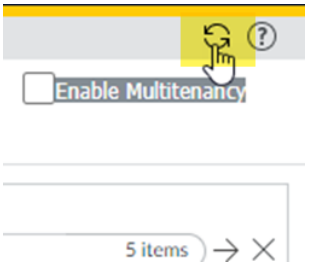
Pour réduire la bande passante d'une connexion aux services existante supérieure à 10 Gbit/s, procédez comme suit :

STEP 1 | Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Colo-Connect**

STEP 2 | Accédez **Panorama** > **Cloud Services** > **Configuration** > **Service Connection (Connexion aux services)** et cliquez sur **Refresh (Actualiser)** en haut à droite de l'interface utilisateur

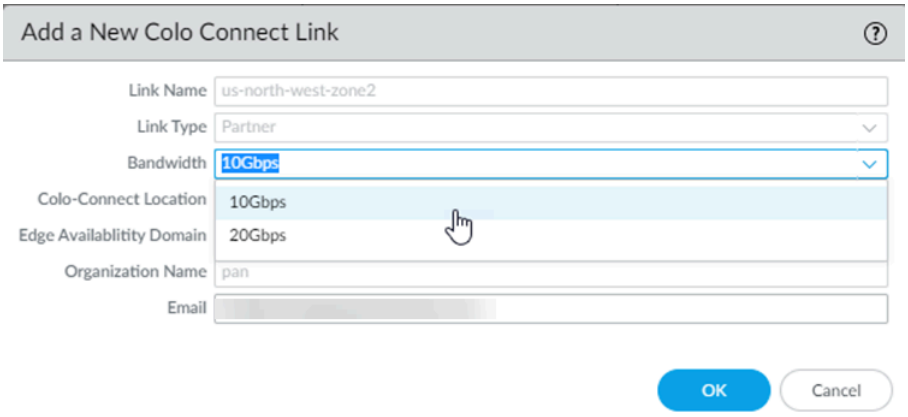
 ©2025 Palo Alto Networks, Inc.

de Panorama afin que la configuration Colo-Connect soit provisionnée dans la zone des connexions aux services.



STEP 3 | Sélectionnez le **Link Name (Nom du lien)** associé à la connexion aux services.

STEP 4 | Diminuez la **Bandwidth (Bande passante)** du lien (interconnexion).



STEP 5 | Cliquez sur **Commit and Push (Valider et appliquer)** pour valider et appliquer vos modifications, en sélectionnant uniquement **Colo-Connect** dans la **Push Scope (Étendue de la transmission)**.

STEP 6 | Cliquez sur **Commit and Push (Valider et appliquer)** pour valider et appliquer vos modifications, en sélectionnant **Service Connections (Connexions aux services)** dans la **Push Scope (Étendue de la transmission)**.

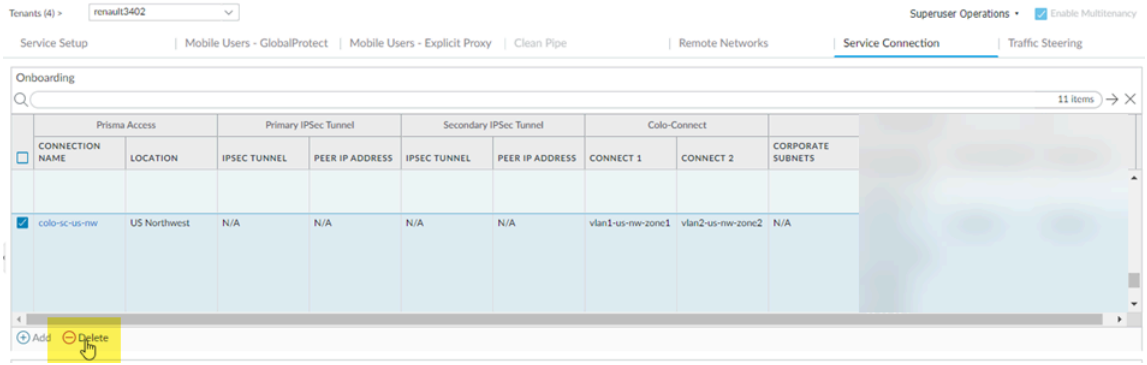
Vous n'avez pas besoin de reconfigurer la connexion aux services pour supprimer le tunnel GRE supplémentaire. Prisma Access détecte et diminue la bande passante du lien et supprime le tunnel supplémentaire lorsque vous validez et appliquez vos modifications dans l'étendue de la transmission de la connexion aux services.

Supprimer une connexion Colo-Connect

Pour supprimer une connexion Colo-Connect, suivez l'ordre inverse de sa configuration en effectuant les étapes suivantes :

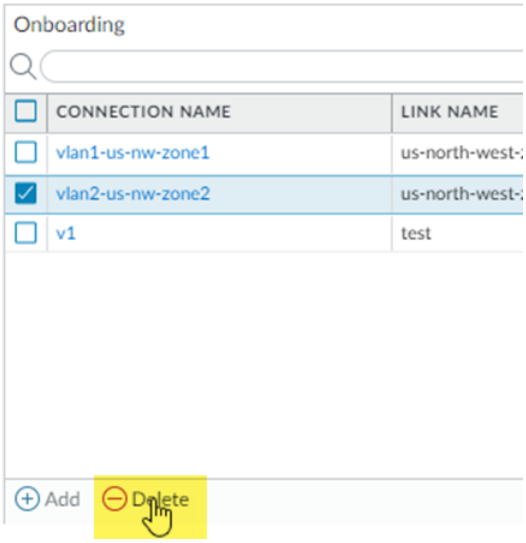
©2025 Palo Alto Networks, Inc.

STEP 1 | Supprimez les connexions aux services associées à la connexion en accédant à **Panorama** > **Cloud Services** > **Configuration** > **Service Connection (Connexion aux services)**, en sélectionnant la connexion aux services et **Delete (Supprimer)**.



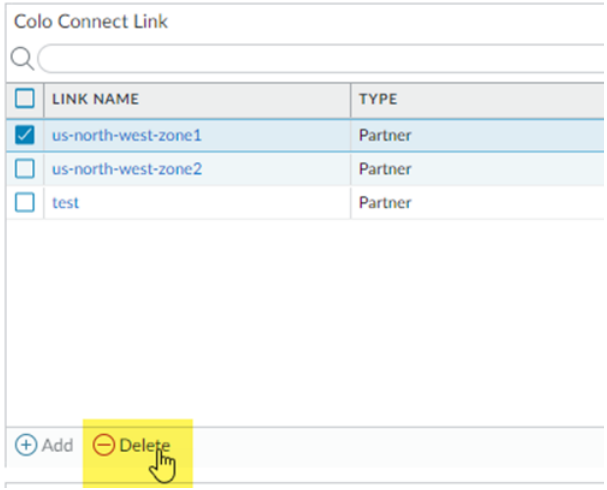
STEP 2 | Cliquez sur **Commit and Push (Valider et appliquer)** pour valider et appliquer vos modifications, en sélectionnant **Service Connections (Connexions aux services)** dans la **Push Scope (Étendue de la transmission)**.

STEP 3 | Supprimez les connexions Colo-Connect associées à la connexion en accédant à **Panorama** > **Cloud Services** > **Configuration** > **Colo-Connect**, en sélectionnant le **Connection Name (Nom de la connexion)** dans la section **Onboarding (Intégration)**, et cliquez sur **Delete (Supprimer)**.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Supprimez le lien Colo-Connect en sélectionnant le **Link Name (Nom du lien)** et **Delete (Supprimer)**.



STEP 5 | Supprimez les adresses IP locales (d'homologues) GRE à vos politiques d'exportation pour le routage VLAN eBGP et le routage de connexion aux services pour les tunnels GRE.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Accélération des applications dans Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Au minimum la version 5.0 d'Innovation Prisma Access ❑ Licence Prisma Access ❑ L'accélération des applications nécessite la version 10.2.10 du plan de données Prisma Access. ❑ Licence complémentaire d'accélération des applications La licence d'accélération des applications inclut une licence d'évaluation de 30 jours pour Autonomous DEM (ADEM) afin que vous puissiez récupérer les mesures de performances de l'accélération des applications à partir d'ADEM.

L'accélération des applications traite directement les causes des mauvaises performances des applications et agit en temps réel pour les atténuer, améliorant considérablement l'expérience des utilisateurs de GlobalProtect et du réseau distant Prisma Access.

Les principales causes d'une mauvaise expérience utilisateur lors de l'accès aux applications sont le contenu dynamique (contenu qui doit être traité pour chaque utilisateur individuellement, à la demande) et les problèmes de connectivité réseau.

L'accélération des applications vous offre les fonctionnalités suivantes :

Accélération pour les principales applications SaaS : l'accélération des applications pour Prisma SASE accélère le contenu dynamique pour améliorer le temps de réponse des principales applications SaaS. Il prépare de manière sécurisée et intelligente le contenu dynamique dont chaque utilisateur a besoin avant que celui-ci ne le demande.

Par conséquent, l'accélération des applications réduit considérablement leur temps de réponse ainsi que celui des API qui les alimentent pour améliorer l'expérience utilisateur et augmenter la productivité.

Les applications accélérées sont répertoriées dans la section Supported Apps (Applications prises en charge).

Accélération du réseau : lorsque vos utilisateurs accèdent aux applications, ils peuvent rencontrer de mauvaises performances dues à une diminution du débit, qui peut être causée par une perte de paquets, une connectivité sans fil dégradée, une congestion du réseau et d'autres facteurs. Ces problèmes de réseau peuvent nuire à l'expérience des employés et réduire leur productivité.

Lors de la conception d'Internet, les réseaux étaient homogènes et la connectivité sans fil en était à ses débuts. Des protocoles fondamentaux comme le protocole TCP ont initialement été créés pour ces réseaux. Aujourd'hui, les réseaux ne sont plus homogènes et la connectivité sans fil crée une expérience utilisateur très variable. Lorsque les utilisateurs rencontrent des conditions de réseau dégradées, le protocole TCP ne peut pas déterminer si le problème est dû à des limitations du périphérique, à des limitations du réseau ou à des contraintes physiques.

Sans nécessiter de modifications de la configuration de votre client ou de vos applications, l'accélération des applications permet de comprendre en toute sécurité les éléments suivants :

- **Capacité du périphérique** : le type de terminal client
- **Capacité du réseau** : le type de réseau
- **Contexte de l'application** : le type d'application utilisé

Grâce à sa compréhension du contexte du périphérique, du réseau et de l'application, l'accélération des applications maximise le débit et s'ajuste en temps réel pour tenir compte de l'évolution des conditions du réseau.

Par rapport à l'accès Internet direct, l'accélération des applications améliore considérablement le débit pour le trafic TCP lors de la connexion via Prisma Access.

Vous pouvez visualiser les améliorations de débit grâce à l'accélération des applications dans les Incidents and Alerts (Incidents et alertes) Prisma SASE. Autonomous DEM alimenté par l'IA (ADEM) s'intègre à l'accélération des applications et vous fournit des mesures telles que le nombre d'applications qui ont été accélérées et l'amélioration globale des performances obtenue.

 ©2025 Palo Alto Networks, Inc.

Exigences et directives en matière d'accélération des applications

Lors de la configuration de l'accélération des applications, prenez note des directives et exigences suivantes :

- **Applications prises en charge** : l'accélération des applications prend en charge les applications suivantes :
  - Amazon S3
  - Azure Storage
  - Box
  - Google Drive
  - Microsoft 365 :
    - Mon contenu
  - Microsoft OneDrive
  - Salesforce
  - SAP Ariba
  - ServiceNow
  - Slack (*téléchargements de fichiers*)
  - Zoom :
    - Téléchargements de fichiers à partir du chat
    - Téléchargements d'enregistrements dans le cloud
    - Zoom Team Chat
- **Emplacements pris en charge** : l'accélération des applications est disponible pour tous les emplacements Prisma Access à l'exception des emplacements suivants :
  - Toutes les zones locales
  - Bahreïn
  - Chine
  - Irlande
  - Afrique du Sud Ouest
  - Suède
  - Émirats arabes unis
- **Téléchargement de CA racine approuvée** : vous devez configurer une CA racine approuvée, la valider et l'appliquer, puis la sélectionner lors de la configuration de l'accélération des applications, comme indiqué dans les procédures suivantes. Si vous utilisez Strata Cloud Manager pour configurer l'accélération des applications, configurez la CA racine dans l'entendue Prisma Access. Si vous modifiez le certificat que vous utilisez, vous devez également valider et appliquer le certificat modifié avant de le sélectionner.

 ©2025 Palo Alto Networks, Inc.

- **Certificat d'approbation de transfert et CA racine approuvée :** activez la CA/le certificat que vous avez téléchargés en tant que certificat d'approbation de transfert et CA racine approuvée, comme indiqué dans les procédures suivantes. Si le déchiffrement SSL est appliqué à des applications accélérées, vous devez marquer le certificat comme certificat d'approbation de transfert et CA racine approuvée, sinon les utilisateurs rencontreront des erreurs SSL lorsqu'ils tenteront d'accéder à ces applications.
- **Fonctionnalité Prisma Access non prise en charge** : la fonctionnalité suivante ne prend pas en charge l'accélération des applications et les déploiements Prisma Access avec ces fonctionnalités activées ne seront pas accélérés :
  - IPv6

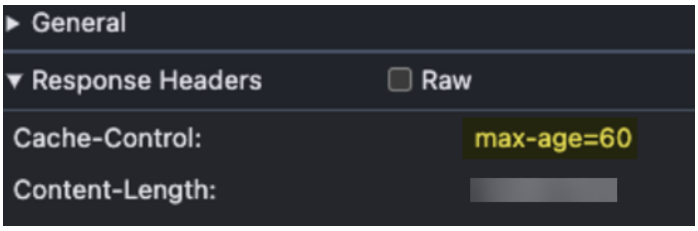
    L'accélération des applications coexiste avec la mise en réseau IPv6 lorsque IPv6 est configuré ; cependant, seul le trafic TCP IPv4 est accéléré. Le trafic IPv6 n'est pas accéléré, mais fonctionne normalement.
  - Réseaux distants qui utilisent des sous-réseaux superposés (pris en charge par défaut dans les déploiements Prisma Access (Managed by Strata Cloud Manager), configurables dans les déploiements Prisma Access (Managed by Panorama)).
- **Directives pour l'accélération des applications**:
  - **Prise en charge du protocole QUIC** : certains navigateurs (tels que Google Chrome) peuvent utiliser le protocole Quick UDP Internet Connections (QUIC) par défaut. L'accélération d'application de couche 7 ne peut pas être utilisée sur le trafic utilisant le protocole QUIC. Comme solution alternative, désactivez le protocole QUIC lorsque vous configurez l'accélération des applications.
  - **Applications SaaS et en-têtes de réponse Zy-*** : les utilisateurs se connectant aux déploiements Prisma Access pour lesquels l'accélération des applications est activée pour les principales applications SaaS peuvent s'attendre à voir des en-têtes de réponse portant le nom Zy-*, tel que Zy-Server et Zy-Accelerated, ainsi qu'un cookie de session zy_sid.

    Si l'en-tête de réponse est Zy-Accelerated, une valeur de **1** indique que la réponse a été accélérée et une valeur de **0** indique que la réponse n'a pas été accélérée.
  - **Localisation de contenu** : si une application SaaS accélérée localise le contenu en fonction uniquement de l'adresse IP ou de l'ID utilisateur, lorsque l'accélération est activée pour cette application, son contenu ne sera pas localisé.
  - **Modification du comportement par défaut des règles de politique de sécurité avec une action définie sur Deny (Refuser)** : si vous avez une règle de politique de sécurité avec une action définie sur **Deny (Refuser)** qui est appliquée au trafic passant par l'accélération des applications à l'aide d'une règle basée sur l'adresse source ou de destination, l'application ou le service, le trafic effectuera une connexion en trois étapes, mais Prisma Access le bloquera et la politique **Deny (Refuser)** fonctionnera comme elle a été configurée.
  - **`Contrôle du cache` Amazon S3 et du stockage Azure Blob** : les compartiments et fichiers Amazon S3 et de stockage Azure Blob ont une série d'en-têtes de réponse HTTP qui leur sont associés. L'une de ces valeurs est `cache-control`. Les fichiers ne sont pas accélérés si la valeur `cache-control` est :
    - Annulé
    - Définir sur une valeur de `max-age=0`

 ©2025 Palo Alto Networks, Inc.

- Définir sur une valeur de `max-age=no-cache`

  Pour bénéficier des avantages de l'accélération des applications pour Amazon S3 et le stockage Azure Blob, définissez la valeur `cache-control` `max-age` sur une valeur supérieure à zéro.



- **Applications avec domaine partagé dans Activity Insights (Informations sur l'activité)** : lorsque vous utilisez l'accélération des applications, l'accélération de couche 7 est basée sur le domaine. Dans certaines conditions, si deux applications partagent le même domaine, les rapports d'application dans Activity Insights (Informations sur l'activité) peuvent attribuer le trafic de couche 7 d'une application à une autre application. Par exemple, si une partie du trafic provenant des applications MS Teams et OneDrive partage le même domaine, les rapports de l'application MS Teams s'afficheront sous OneDrive.
- **Connexions longue durée et journaux système** : l'accélération des applications écrit des journaux de couche 4 lorsqu'une connexion TCP individuelle se termine. Pour les connexions de courte durée, ce comportement est transparent, car des connexions de courte durée sont fréquemment créées par les applications.

  L'accélération des applications recueille des métriques pour toute la période pendant laquelle la connexion est active. Pour les connexions de longue durée telles que celles utilisées par les lecteurs réseau SMB montés, ce comportement peut donner l'impression que les métriques sont uniquement recueillies à la fin de la connexion.

 ©2025 Palo Alto Networks, Inc.

Configurer l’accélération des applications

Pour configurer l’accélération des applications dans Prisma Access, sélectionnez l’un des onglets suivants en fonction de votre déploiement (Prisma Access (Managed by Strata Cloud Manager) ou Prisma Access (Managed by Panorama)).

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

Configurer l’accélération des applications dans Prisma Access (Strata Cloud Manager)

Pour configurer l’accélération des applications dans un déploiement Prisma Access (Managed by Strata Cloud Manager), effectuez cette tâche.

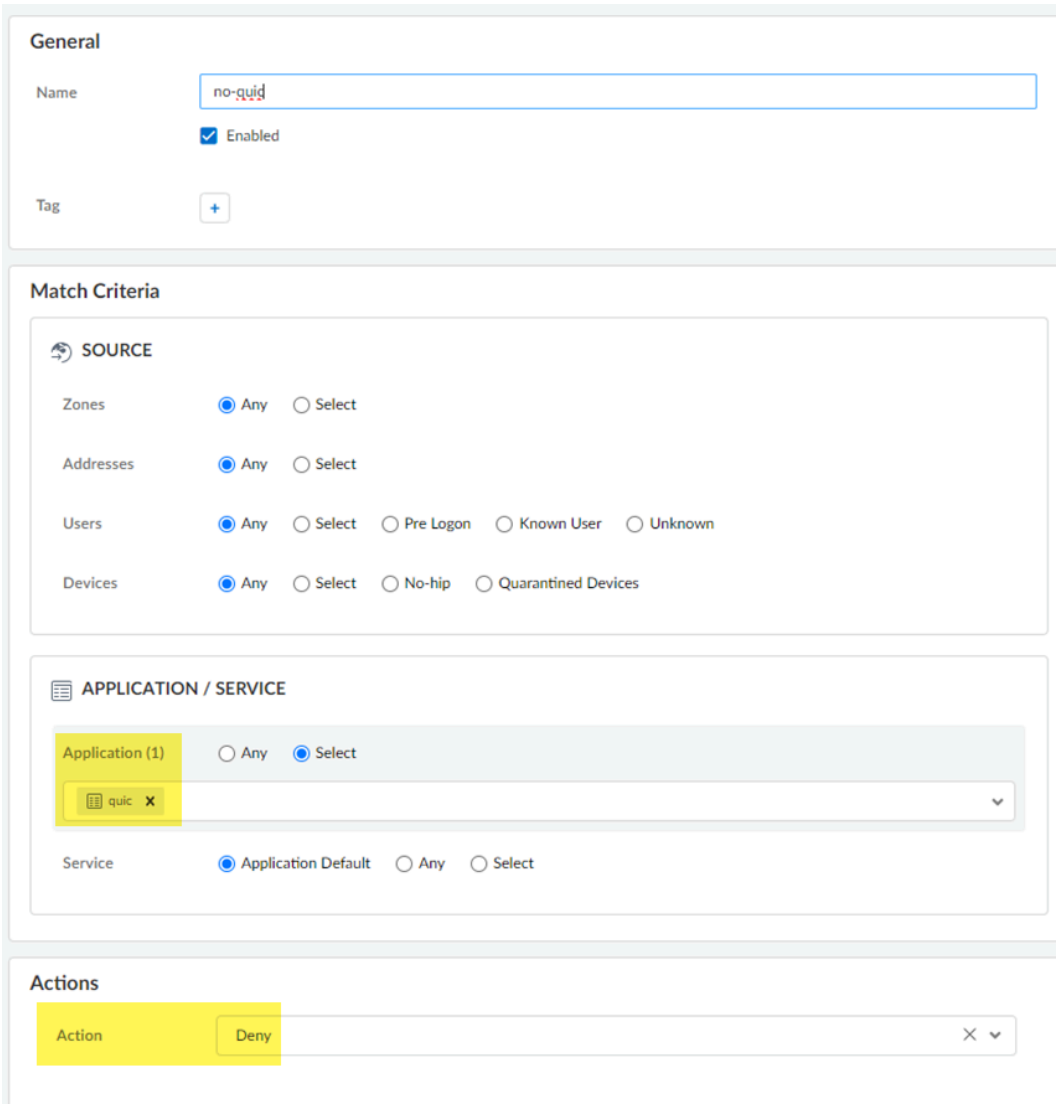
 ©2025 Palo Alto Networks, Inc.

STEP 1 | (Facultatif) Désactivez le protocole de connexions Internet UDP rapides (Quick UDP Internet Connections, QUIC).

L'accélération des applications ne peut pas accélérer les applications au niveau de la couche 7 sans désactiver QUIC.

1. Accédez à **Manage (Gestion)** > **Configuration (Configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** et **Add Rule (Ajouter une règle)** > **Pre Rules (Pré-règles)**.

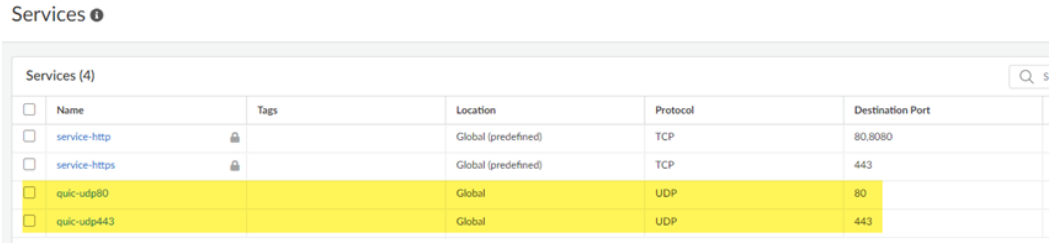
   Créez cette règle de politique de sécurité dans la portée de configuration **Global (Globale)**.
2. Sélectionnez **quic** dans **Application / Service** et **Deny (Refuser)** dans **Actions**.



3. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.
4. Allez dans **Manage (Gérer)** > **Configuration** > **NGFW & Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Services** > **Service** et **Add (Ajouter)** pour le port UDP 80 et le port UDP 443.

 ©2025 Palo Alto Networks, Inc.

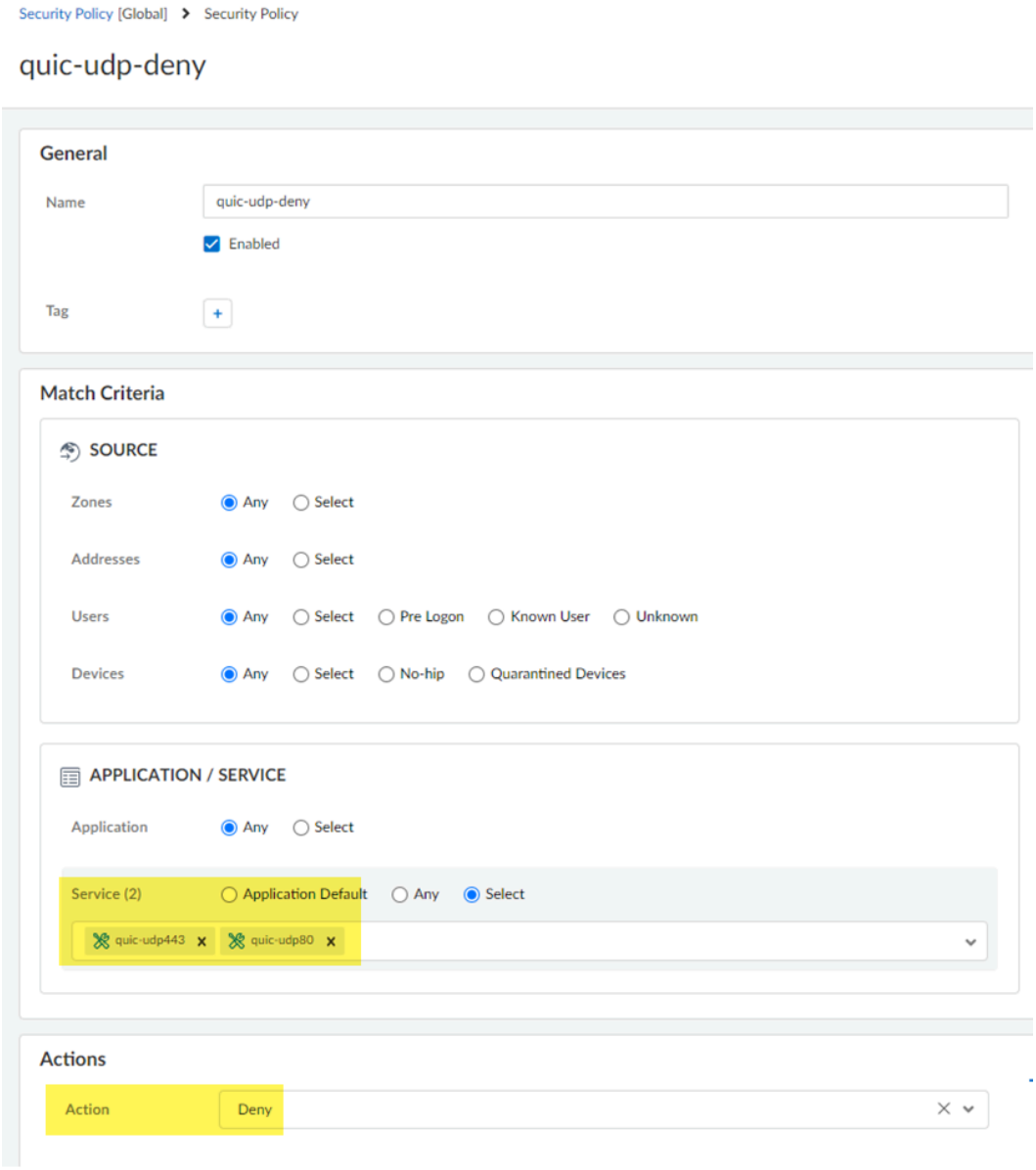
Palo Alto Networks recommande d'ajouter des services pour le port UDP 80 et le port UDP 443 et de créer une politique de sécurité supplémentaire pour bloquer le trafic UDP sur ces ports, car les nouvelles versions QUIC peuvent être identifiées à tort comme **unknown-udp (udp inconnu)**.



5. Revenez à **Manage (Gérer)** > **Configuration** > **NGFW & Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)Add Rule (Ajouter une règle)** pour une deuxième politique de sécurité, en

 ©2025 Palo Alto Networks, Inc.

précisant les services sous **Application / Services** et en sélectionnant **Deny (Refuser)** dans **Action**.



Une fois l'opération terminée, vous disposez de deux politiques de sécurité : L'une qui bloque le protocole QUIC et l'autre qui bloque le trafic sur les ports UDP 80 et 443.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Importez un certificat d'autorité de certification (certificate authority, CA) racine et une clé privée dans Strata Cloud Manager dans l'étendue Prisma Access à utiliser avec l'accélération des applications et appliquez vos modifications.

Une CA/un certificat racines auto-signés est le niveau supérieur d'un certificat dans une chaîne de certificats. L'accélération des applications utilise la CA/les certificats racines pour créer des certificats pour les applications accélérées. Appliquez la CA/le certificat racines dans Prisma Access afin que l'accélération des applications puisse commencer la création des certificats spécifiques à l'application.

La CA/le certificat racines doivent présenter les caractéristiques suivantes :

- La CA doit être une CA de confiance.
- (Recommandé) La CA doit être unique et utilisée uniquement pour l'accélération des applications.
- La CA ne peut pas expirer. Notez la date d'expiration de la CA et renouvelez le certificat avant qu'il n'expire. Si une CA/un certificat utilisé par l'accélération des applications expire, les utilisateurs reçoivent une erreur SSL lorsqu'ils tentent d'accéder aux applications accélérées. Il est essentiel de s'assurer que la CA est valide lorsque l'accélération des applications est utilisée par votre organisation.
- Le certificat doit comporter une clé.
- Il doit utiliser une phrase secrète.
- Il doit être dans l'étendue **Prisma Access**.
- (Utilisateurs mobiles — déploiements GlobalProtect uniquement) Il doit être installé dans le magasin de certificats racines local.

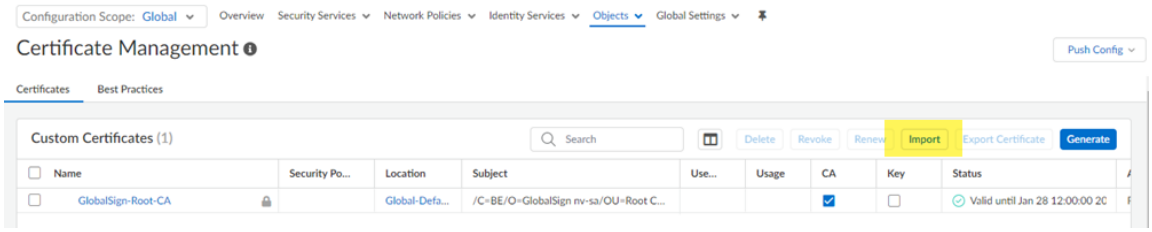
  Vous pouvez effectuer cette installation en l'ajoutant à la liste des certificats de confiance comme décrit dans cette procédure ou, si vous utilisez ActiveDirectory, vous pouvez

 ©2025 Palo Alto Networks, Inc.

distribuer la CA racine à partir d'AD à l'aide d'un objet de politique de groupe (Group Policy Object, GPO) Active Directory.

Si vous devez modifier la CA/le certificat racines, vous devez les télécharger et valider vos modifications avant de pouvoir utiliser le certificat modifié.

1. Accédez à **Manage (Gestion)** > **Configuration (Configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)**.
2. Cliquez sur **Import (Importer)** pour importer un certificat.



3. Sélectionnez les paramètres suivants :
   - Saisissez le **Certificate Name (Nom du certificat)** pour le certificat, par exemple `AppAcceleration_CA`.

     Le nom est sensible à la casse et peut comporter jusqu'à 31 caractères. Dans le nom, n'utilisez que des lettres, chiffres, traits d'union et traits de soulignement.
   - Utilisez la fonction **Choose File (Choisir le fichier)**, recherchez le **Certificate File (Fichier du certificat)** reçu de la CA et cliquez sur **Open (Ouvrir)**.
   - Sélectionnez un **Format** :
     - **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat cryptés (PKCS12))** : il s'agit du format, par défaut et le plus courant, dans lequel la clé et le certificat sont enregistrés dans un conteneur unique (Certificate File (Fichier du certificat)).
     - **Base64 Encoded Certificate (PEM) (Certificat codé en base-64 (PEM))** : vous devez importer la clé séparément du certificat. Si vous sélectionnez ce format, vous devez sélectionner un **Key File (Fichier clé)**.

 ©2025 Palo Alto Networks, Inc.

- Saisissez une **Passphrase (Phrase secrète)** et cliquez sur **Confirm Passphrase (Confirmer la phrase secrète)**.

4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

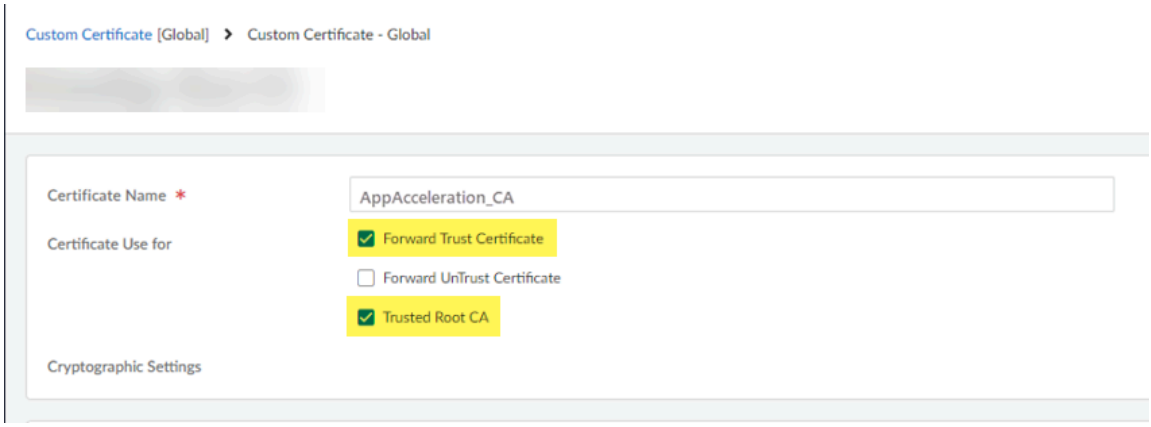


 ©2025 Palo Alto Networks, Inc.

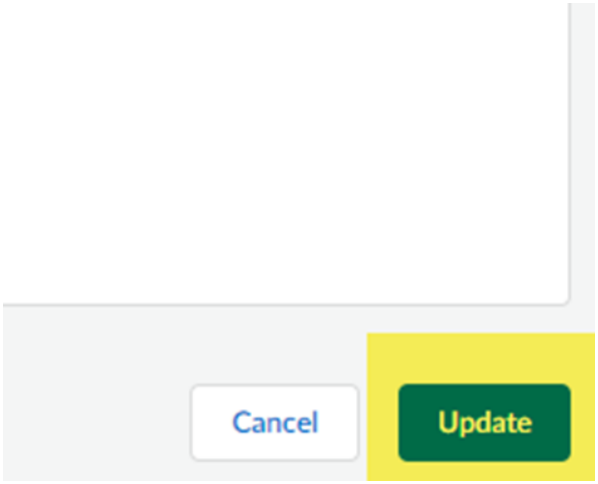
STEP 3 | Marquez la CA/le certificat racines que vous avez ajoutés en tant que certificat d'approbation de transfert et autorité de certification racine fiable.

Si vous ne spécifiez pas le certificat en tant que certificat d'approbation de transfert et CA racine approuvée, les utilisateurs rencontreront des erreurs SSL lorsqu'ils tenteront d'accéder à des applications accélérées lors de l'utilisation du décryptage SSL.

1. Sélectionnez la CA/le certificat racines que vous avez ajoutés.
2. Sélectionnez le certificat en tant que **Forward Trust Certificate (Certificat d'approbation de transfert)** et **Trusted Root CA (CA racine approuvée)**.

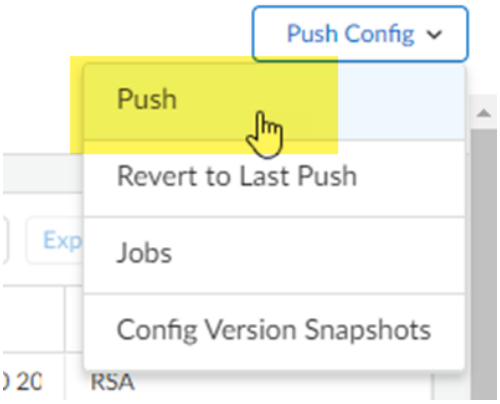


3. Utilisez la fonction **Update (Mettre à jour)** pour mettre à jour le certificat.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | **Push (Appliquez)** vos changements.

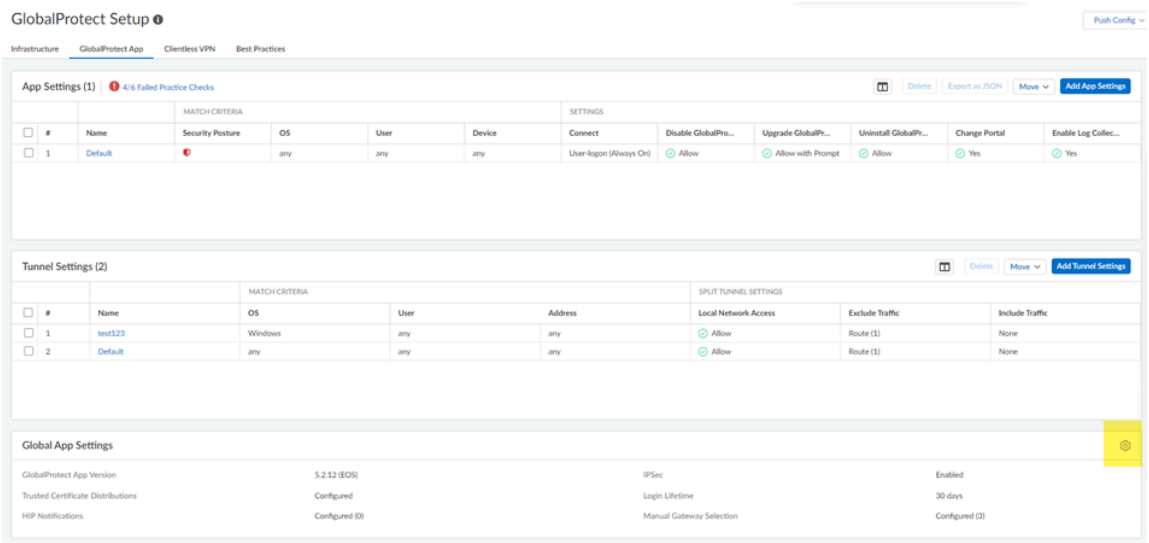


 ©2025 Palo Alto Networks, Inc.

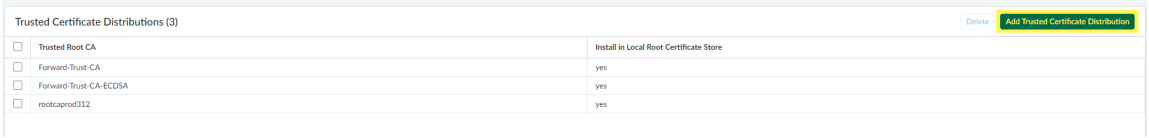
STEP 5 | (Utilisateurs mobiles — déploiements GlobalProtect uniquement) Ajoutez la CA/le certificat racines que vous avez ajoutés à la liste des certificats de confiance GlobalProtect et installez-les dans le magasin de certificats racines local.

Sinon, si vous utilisez ActiveDirectory, vous pouvez distribuer la CA racine à partir d'AD à l'aide d'un GPO Active Directory.

1. Allez dans **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prima Access)** > **GlobalProtect** > **GlobalProtect App (Application GlobalProtect)** > **Global App Settings (Paramètres généraux de l'application)**.
2. Pour modifier les **Settings (Paramètres)**, cliquez sur l'engrenage.



3. Utilisez la fonction **Add Trusted Certificate Distribution (Ajouter une distribution de certificats fiables)**.



4. Sélectionnez la **Trusted Root CA (CA racine approuvée)** que vous avez créée à l'étape précédente et sélectionnez **Install in Local Root Certificate Store (Installer dans le magasin de certificats racines local)**.

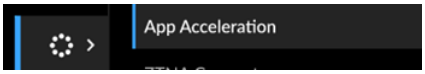


5. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.
6. **Push (Appliquez)** vos changements.

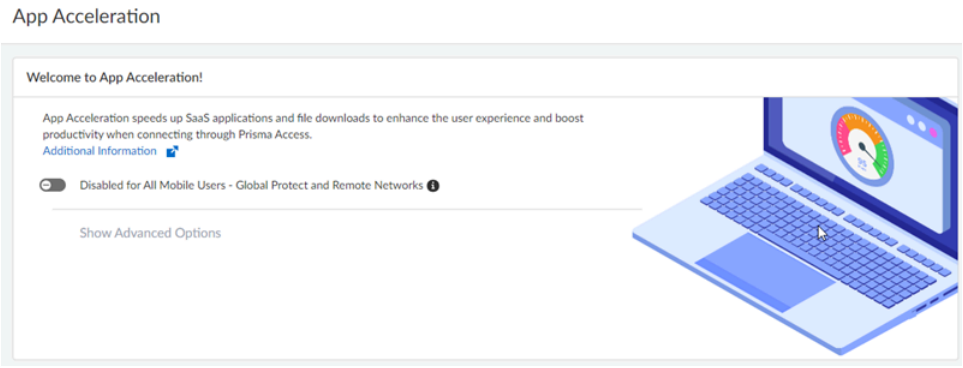
 ©2025 Palo Alto Networks, Inc.

STEP 6 | Activez l'accélération des applications et choisissez le fichier de certificat que vous avez créé.

1. Allez dans **Workflow (Flux de travail)** > **App Acceleration (Accélération des applications)** dans la barre de navigation de gauche.

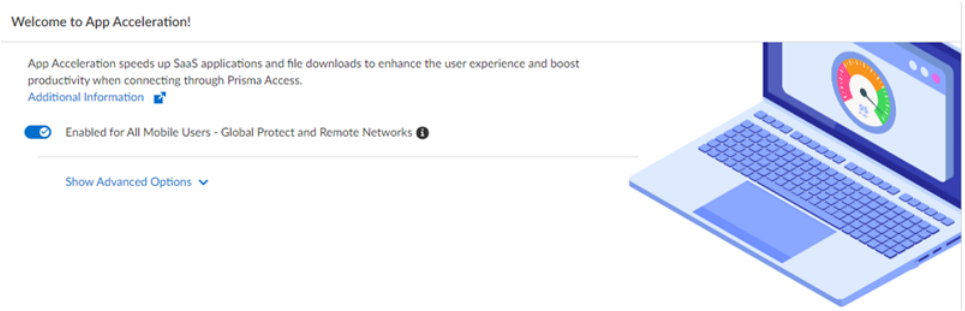


La fenêtre App Acceleration (Accélération des applications) s'affiche.



2. Déplacez le curseur vers la droite pour que l'accélération des applications soit **Enabled for all Mobile Users—GlobalProtect and Remote Networks (Activée pour tous les utilisateurs mobiles — GlobalProtect et réseaux distants)**.

Si les validations sont en cours, les paramètres d'accélération des applications prendront effet une fois toutes les validations terminées.

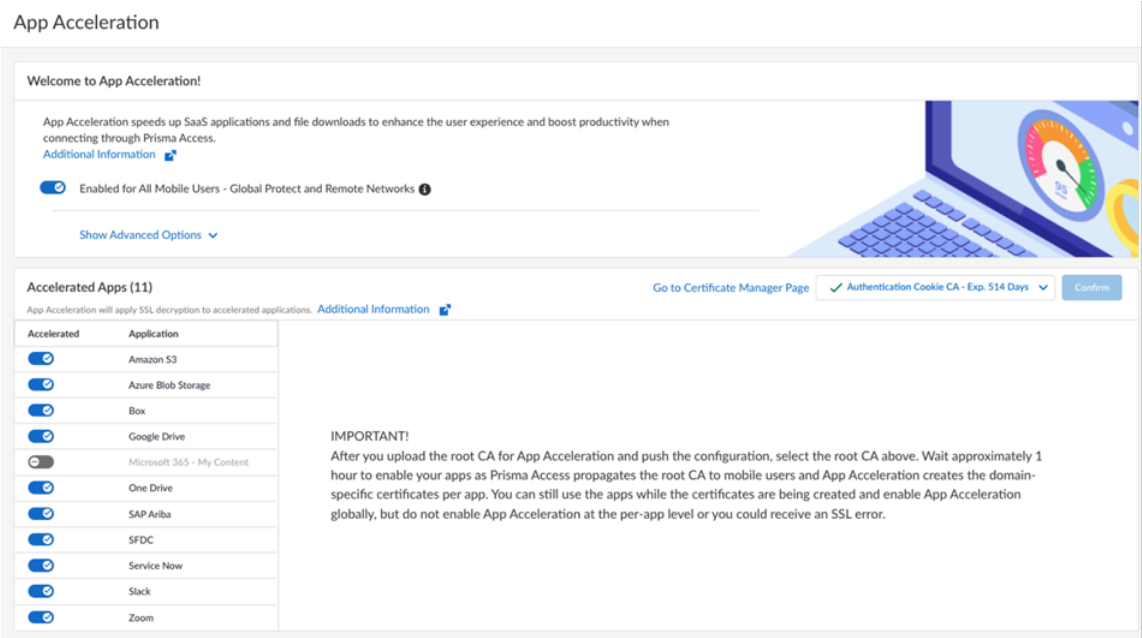


L'accélération des applications sera activée pour tout le trafic TCP. Si vous souhaitez accélérer des applications SaaS, vous devez sélectionner une CA/un certificat racines, comme indiqué à l'étape suivante.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Sélectionnez le certificat que vous avez créé à l'étape précédente.

Si vous devez modifier le certificat d'un certificat existant, assurez-vous d'avoir validé et appliqué le certificat à vos pare-feu et à vos utilisateurs, puis sélectionnez-le ici. Vous devez valider le nouveau certificat avant de le sélectionner.



*Après avoir importé le certificat, vous devez attendre que l'accélération des applications génère des certificats spécifiques au domaine de chaque application. Ce processus peut prendre jusqu'à sept jours. En attendant, vous pouvez déplacer le curseur pour les **Accelerated Apps (Applications accélérées)** à gauche pour désactiver temporairement l'accélération des applications et accéder aux applications jusqu'à ce que les certificats soient générés. Si vous ne le faites pas, vous risquez de recevoir une erreur SSL jusqu'à ce que les certificats soient générés.*

Attendez jusqu'à 10 minutes pour que l'accélération soit active une fois que vous l'avez activée pour une application donnée.

STEP 8 | (Facultatif) Sélectionnez la fonction **Show Advanced Options (Afficher les options avancées)** et modifiez les paramètres de test de métrique.

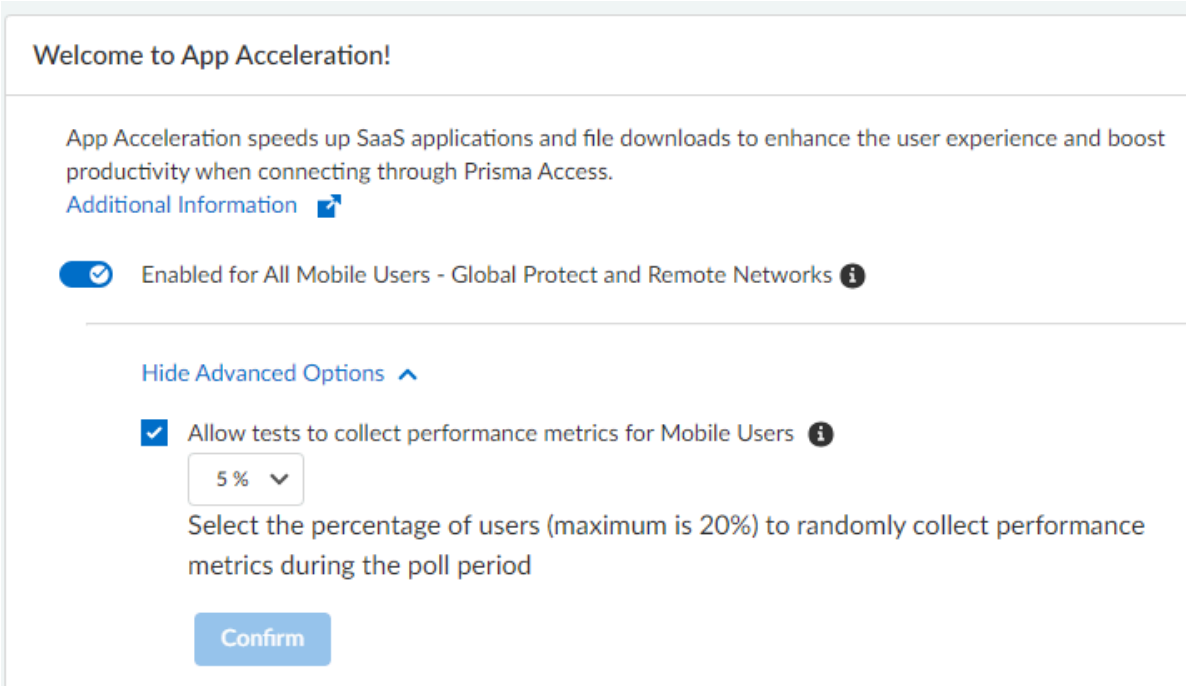
- (Facultatif) Pour désactiver le recueillement de mesures afin d'obtenir des informations sur les performances, désélectionnez **Allow tests to collect performance metrics for Mobile**

 ©2025 Palo Alto Networks, Inc.

Users (Autoriser les tests à recueillir des indicateurs de performance pour les utilisateurs mobiles).

Palo Alto Networks vous recommande d'activer le recueillement de mesures pour observer les améliorations des performances des applications lors de l'utilisation de l'accélération des applications.

- (Facultatif) Pour modifier le pourcentage d'utilisateurs pour lesquels des tests prédictifs sont traités par rapport à la valeur par défaut de 5 %, sélectionnez un autre pourcentage dans la liste déroulante et cliquez sur **Confirm (Confirmer)** pour confirmer les changements.



 ©2025 Palo Alto Networks, Inc.

Configurer l'accélération des applications dans Prisma Access (Panorama)

Pour configurer l'accélération des applications dans un déploiement Prisma Access (Managed by Panorama), effectuez cette tâche.

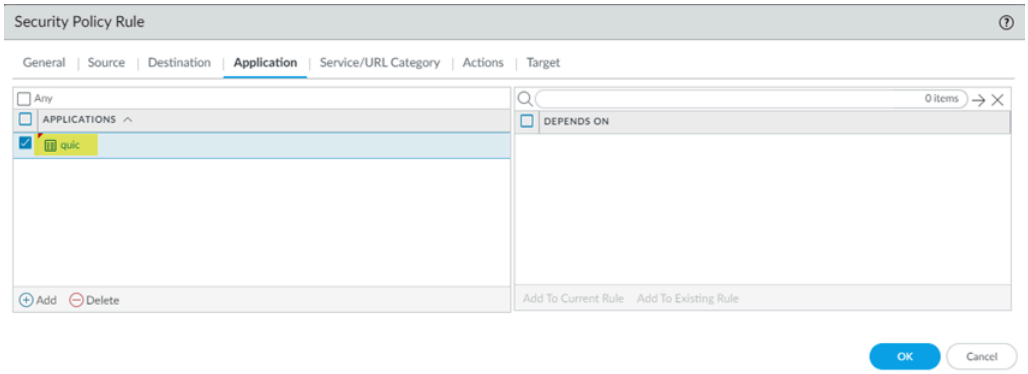
STEP 1 | (Facultatif) Désactivez le protocole de connexions Internet UDP rapides (Quick UDP Internet Connections, QUIC).

L'accélération des applications ne peut pas accélérer les applications au niveau de la couche 7 sans désactiver QUIC.

1. Allez dans **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Pré Règles)** et cliquez sur **Add (Ajouter)** pour ajouter une politique de sécurité.

   Créez cette règle de politique de sécurité dans le groupe de périphériques **Shared (Partagé)**.

2. Sélectionnez **quic** dans **Application** et **Deny (Refuser)** dans **Action**.



3. Cliquez sur **Add (Ajouter)** pour ajouter une deuxième politique de sécurité.

   Les versions les plus récentes de QUIC peuvent être mal identifiées**unknown-udp (udp inconnu)**. Pour cette raison, Palo Alto Networks conseille d'ajouter des services pour le port UDP 80 et le port UDP 443 et de créer une politique de sécurité supplémentaire pour bloquer le trafic UDP sur ces ports.

4. Dans **Service/URL Category (Catégorie de service/URL)**, cliquez sur **Add (Ajouter)** pour ajouter de nouveaux services pour les ports UDP 80 et 443, et sélectionnez **Deny (Refuser)** dans **Action**.

   Une fois l'opération terminée, vous disposez de deux politiques de sécurité : L'une qui bloque le protocole QUIC et l'autre qui bloque le trafic sur les ports UDP 80 et 443.

	NAME	LOCATION	APPLICATION	TAGS	ACTION	SERVICE	PROFILE
1	quic-deny	Shared	quic	none	Deny	application-...	none
2	quic-udp-deny	Shared	any	none	Deny	quic-udp80 quic-udp443	none

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Importez un certificat d'autorité de certification (certificate authority, CA) racine et une clé privée dans Panorama à utiliser avec l'accélération des applications, puis validez et appliquez vos modifications.

Une CA/un certificat racines auto-signés est le niveau supérieur d'un certificat dans une chaîne de certificats. L'accélération des applications utilise la CA/les certificats racines pour créer des certificats pour les applications accélérées. Appliquez la CA/le certificat racines dans Prisma Access afin que l'accélération des applications puisse commencer la création des certificats spécifiques à l'application.

La CA/le certificat racines doivent présenter les caractéristiques suivantes :

- La CA doit être une CA de confiance.
- (Recommandé) La CA doit être unique et utilisée uniquement pour l'accélération des applications.
- La CA ne peut pas expirer. Notez la date d'expiration de la CA et renouvelez le certificat avant qu'il n'expire. Si une CA/un certificat utilisé par l'accélération des applications expire, les utilisateurs reçoivent une erreur SSL lorsqu'ils tentent d'accéder aux applications accélérées. Il est essentiel de s'assurer que la CA est valide lorsque l'accélération des applications est utilisée par votre organisation.
- Le certificat doit comporter une clé.
- Il doit utiliser une phrase secrète.
- (Utilisateurs mobiles — déploiements GlobalProtect uniquement) Il doit être installé dans le magasin de certificats racines local.

  Vous pouvez effectuer cette installation en l'ajoutant à la liste des certificats de confiance comme décrit dans cette procédure ou, si vous utilisez ActiveDirectory, vous pouvez

 ©2025 Palo Alto Networks, Inc.

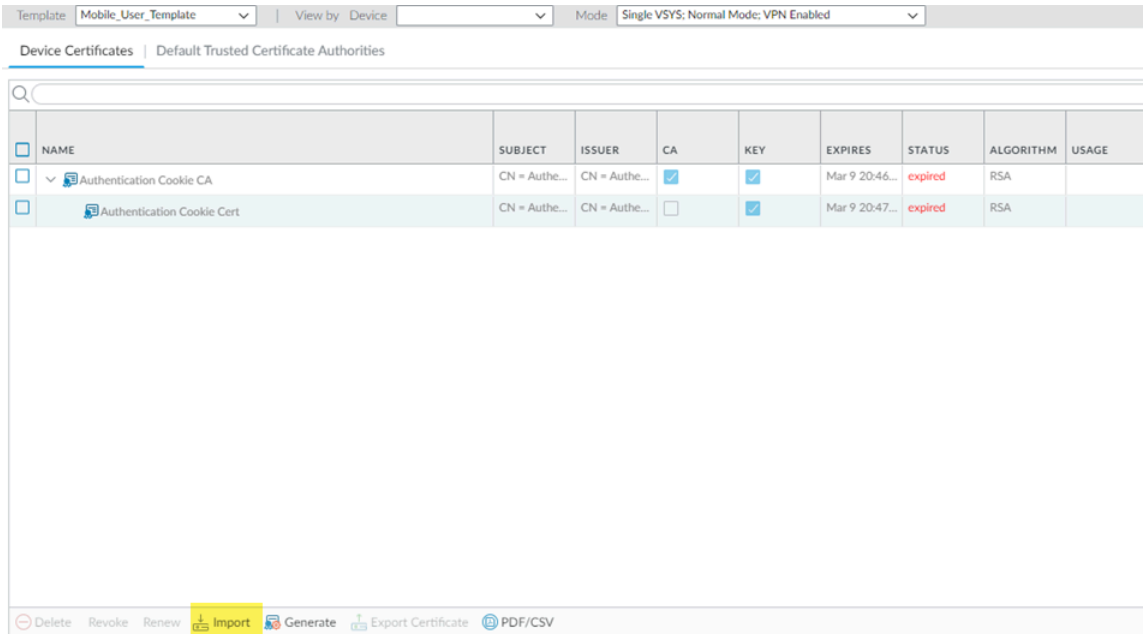
distribuer la CA racine à partir d'AD à l'aide d'un objet de politique de groupe (Group Policy Object, GPO) Active Directory.

Si vous devez modifier la CA/le certificat racines, vous devez les télécharger, puis valider et appliquer vos modifications avant de pouvoir utiliser le certificat modifié.

1. Allez dans **Device (Périphérique)** > **Certificates (Certificats)** > **Certificate Management (Gestion des certificats)**.

   Assurez-vous que vous êtes dans le modèle Mobile_User_Template.

2. Cliquez sur **Import (Importer)** pour importer un certificat.



3. Sélectionnez les paramètres suivants :

   - Saisissez le **Certificate Name (Nom du certificat)** pour le certificat, par exemple `AppAcceleration_CA`.

     Le nom est sensible à la casse et peut comporter jusqu'à 31 caractères. Dans le nom, n'utilisez que des lettres, chiffres, traits d'union et traits de soulignement.

   - Recherchez le **Certificate File (Fichier du certificat)** reçu de la CA et cliquez sur **Open (Ouvrir)** pour l'ouvrir.

   - Sélectionnez un **Format** :

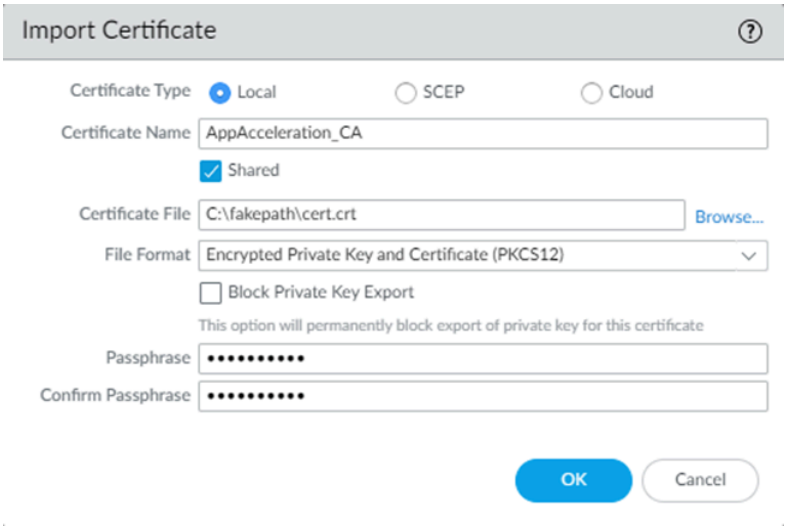
     - **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat cryptés (PKCS12))** : il s'agit du format, par défaut et le plus courant, dans lequel la clé et le certificat sont enregistrés dans un conteneur unique (Certificate File (Fichier du certificat)).

     - **Base64 Encoded Certificate (PEM) (Certificat codé en base-64 (PEM))** : vous devez importer la clé séparément du certificat. Vous devez utiliser la fonction **Import Private Key (Importer la clé privée)** et sélectionner un **Key File (Fichier clé)** si vous choisissez ce format.

 ©2025 Palo Alto Networks, Inc.

- Saisissez une **Passphrase (Phrase secrète)** et cliquez sur **Confirm Passphrase (Confirmer la phrase secrète)**.

4. Cliquez sur **OK**.



5. Répétez ces étapes en remplaçant le modèle Remote_Network_Template par le modèle Mobile_User_Template.

   Vous devez importer ces certificats à la fois dans le modèle Mobile_User_Template et le modèle Remote_Network_Template afin d'accélérer les applications pour vos utilisateurs mobiles et les utilisateurs des sites de réseau distants.

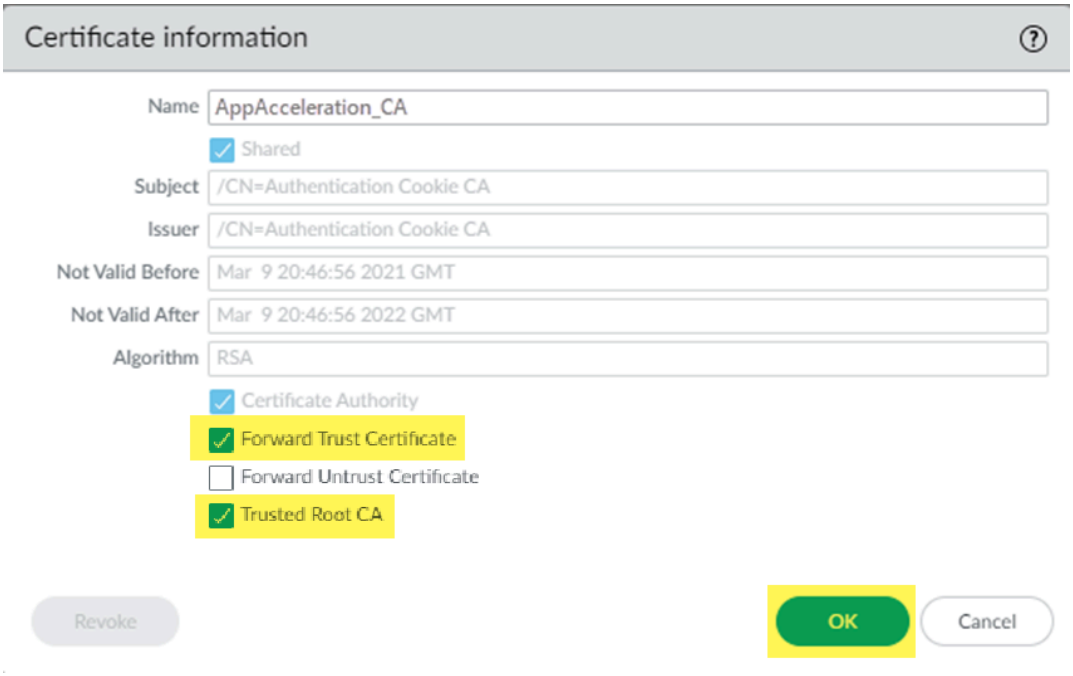
STEP 3 | Marquez la CA/le certificat racines que vous avez ajoutés en tant que certificat d'approbation de transfert et autorité de certification racine fiable.

Si vous ne spécifiez pas le certificat en tant que certificat d'approbation de transfert et CA racine approuvée, les utilisateurs rencontreront des erreurs SSL lorsqu'ils tenteront d'accéder à des applications accélérées lors de l'utilisation du décryptage SSL. Si vous avez des certificats dans le modèle Mobile_User_Template et le modèle Remote_Network_Template, effectuez cette étape dans les deux modèles.

1. Sélectionnez la CA/le certificat racines que vous avez ajoutés.

 ©2025 Palo Alto Networks, Inc.

2. Sélectionnez le certificat en tant que **Forward Trust Certificate (Certificat d'approbation de transfert)** et **Trusted Root CA (CA racine approuvée)**, puis cliquez sur **OK**.



STEP 4 | **Commit and Push (Validez et appliquez)** vos modifications.

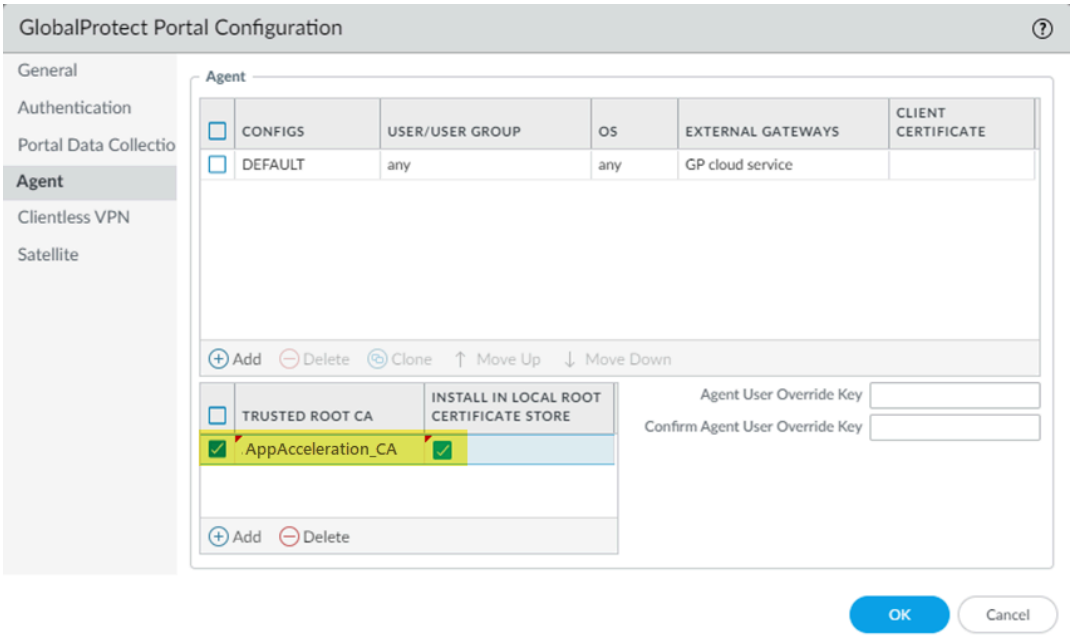
 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Utilisateurs mobiles — Déploiements GlobalProtect uniquement) Ajoutez la CA/le certificat racines que vous avez ajoutés à la liste des certificats de confiance GlobalProtect dans la configuration du portail GlobalProtect.

Sinon, si vous utilisez ActiveDirectory, vous pouvez distribuer la CA racine à partir d'AD à l'aide d'un GPO Active Directory.

1. Allez dans **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **GlobalProtect_Portal** > **Agent**.

   Assurez-vous que vous êtes dans le modèle Mobile_User_Template.
2. Cliquez sur **Add (Ajouter)** pour ajouter la CA racine de confiance que vous avez créée dans une étape précédente.
3. Sélectionnez **Install in Local Root Certificate Store (Installer dans le magasin de certificats racines local)**.
4. Cliquez sur **OK**.

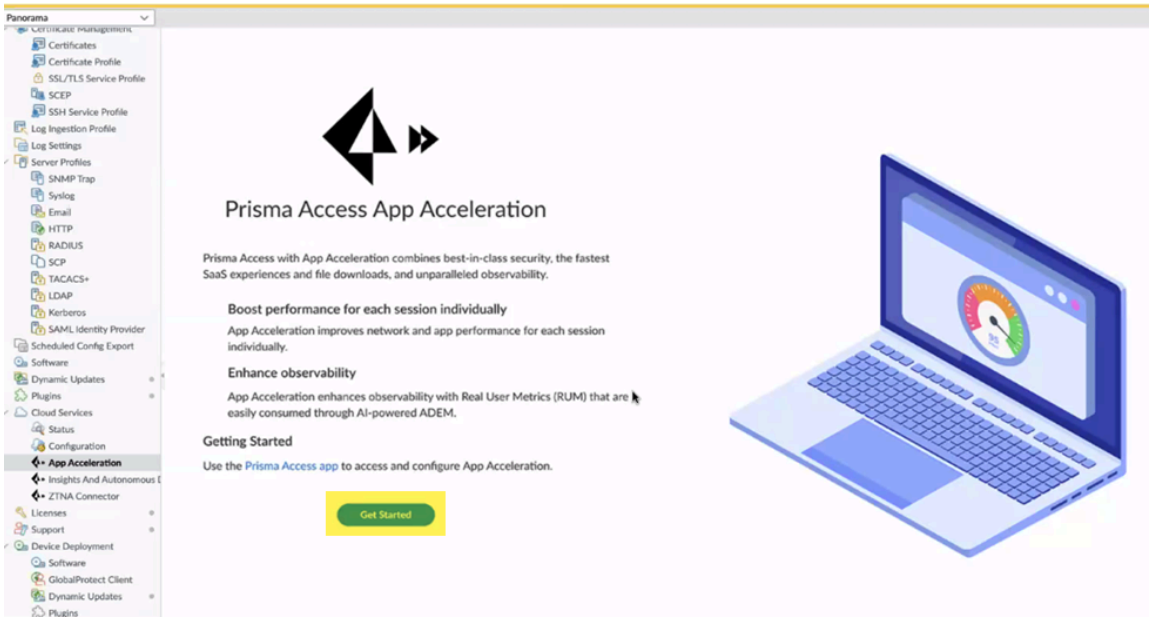


5. **Commit and Push (Validez et appliquez)** vos modifications.

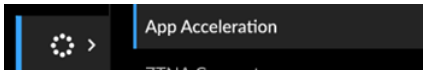
 ©2025 Palo Alto Networks, Inc.

STEP 6 | Activez l'accélération des applications et choisissez le fichier de certificat que vous avez créé.

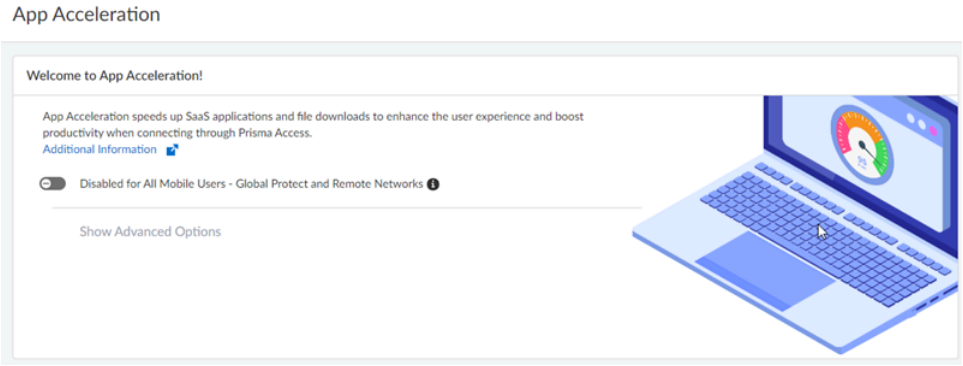
1. Allez dans **Panorama** > **Cloud Services** > **App Acceleration (Accélération des applications)** et sélectionnez **Get Started (Démarrer)** pour démarrer l'accélération des applications.



2. Allez dans **Workflow (Flux de travail)** > **App Acceleration (Accélération des applications)** dans la barre de navigation de gauche.



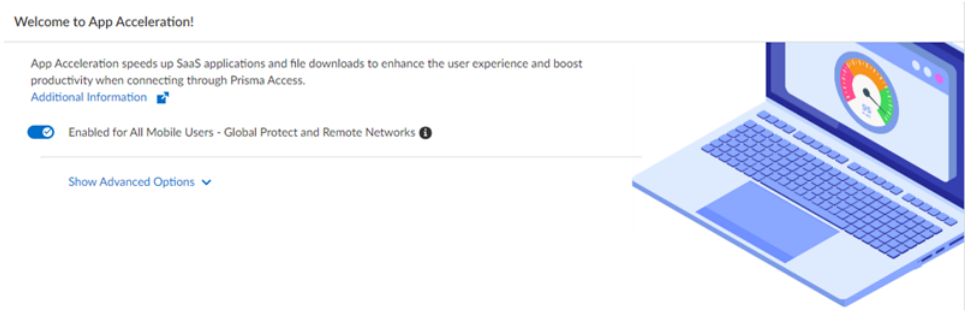
La fenêtre App Acceleration (Accélération des applications) s'affiche.



3. Déplacez le curseur vers la droite pour que l'accélération des applications soit **Enabled for all Mobile Users—GlobalProtect and Remote Networks (Activée pour tous les utilisateurs mobiles — GlobalProtect et réseaux distants)**.

Si les validations sont en cours, les paramètres d'accélération des applications prendront effet une fois toutes les validations terminées.

 ©2025 Palo Alto Networks, Inc.



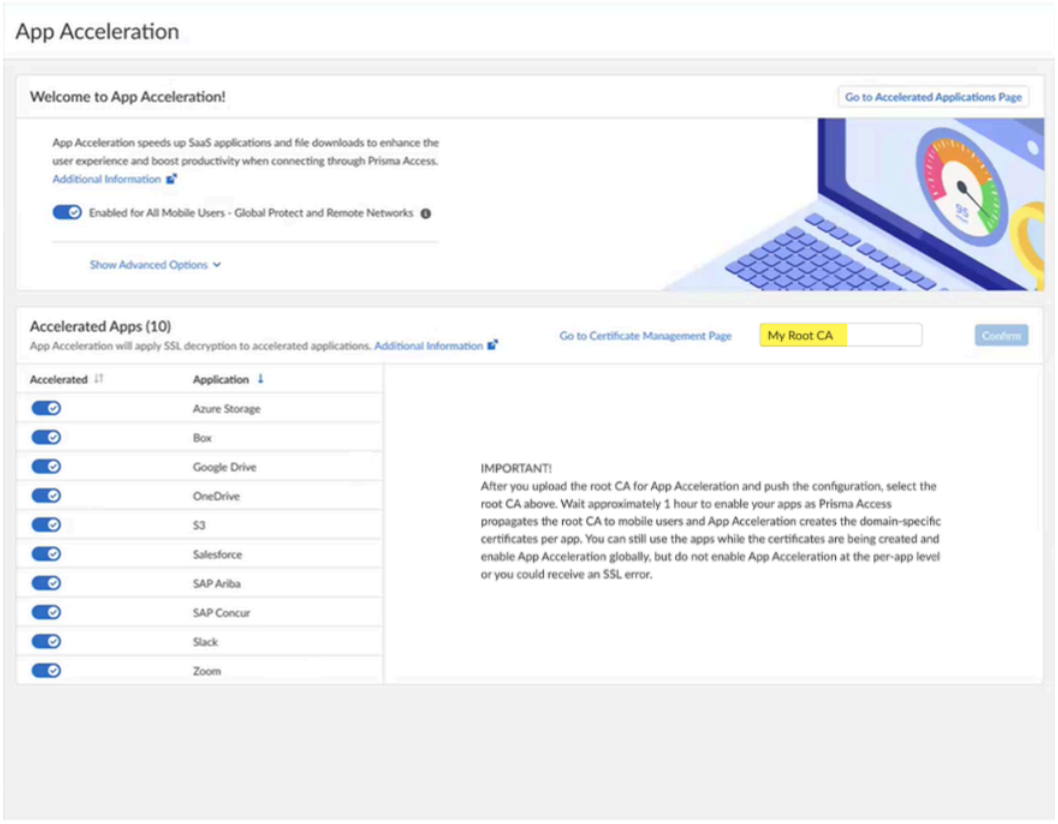
L'accélération des applications sera activée pour tout le trafic TCP. Si vous souhaitez accélérer des applications SaaS, vous devez sélectionner une CA/un certificat racines, comme indiqué à l'étape suivante.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Dans la configuration de l'accélération des applications, tapez le nom du certificat que vous avez créé dans une étape précédente exactement comme il est répertorié dans Panorama.

Assurez-vous d'avoir validé et appliqué le certificat avant de saisir son nom.

Si vous devez changer le certificat d'un certificat existant, tapez son nouveau nom. Vous devez taper son nom (vous ne pouvez pas le sélectionner dans une liste), et vous devez valider et appliquer le nouveau certificat avant d'entrer son nom.



*Après avoir importé le certificat, vous devez attendre que l'accélération des applications génère des certificats spécifiques au domaine de chaque application. Ce processus peut prendre jusqu'à sept jours. En attendant, vous pouvez déplacer le curseur pour les **Accelerated Apps (Applications accélérées)** à gauche pour désactiver temporairement l'accélération des applications et accéder aux applications jusqu'à ce que les certificats soient générés. Si vous ne le faites pas, vous risquez de recevoir une erreur SSL jusqu'à ce que les certificats soient générés.*

Attendez jusqu'à 10 minutes pour que l'accélération soit active une fois que vous l'avez activée pour une application donnée.

STEP 8 | (Facultatif) Sélectionnez la fonction **Show Advanced Options (Afficher les options avancées)** et modifiez les paramètres de test de métrique.

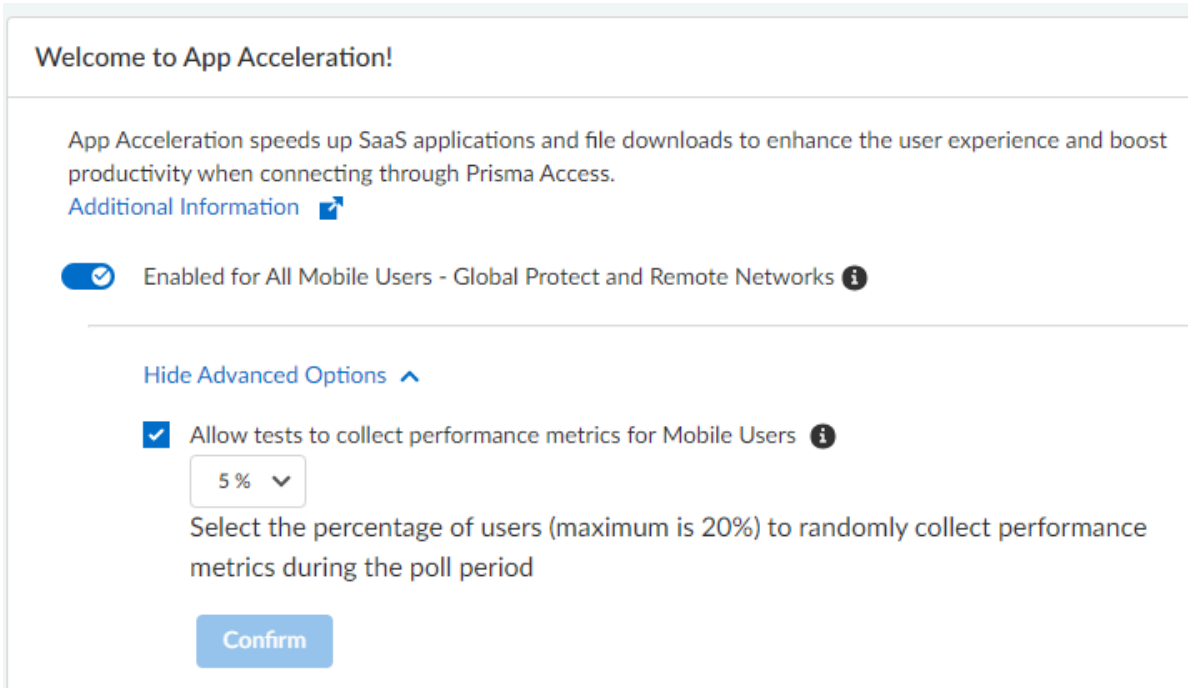
- (Facultatif) Pour désactiver le recueillement de mesures afin d'obtenir des informations sur les performances, désélectionnez **Allow tests to collect performance metrics for Mobile**

 ©2025 Palo Alto Networks, Inc.

Users (Autoriser les tests à recueillir des indicateurs de performance pour les utilisateurs mobiles).

Palo Alto Networks vous recommande d'activer le recueillement de mesures pour observer les améliorations des performances des applications lors de l'utilisation de l'accélération des applications.

- (Facultatif) Pour modifier le pourcentage d'utilisateurs pour lesquels des tests prédictifs sont traités par rapport à la valeur par défaut de 5 %, sélectionnez un autre pourcentage dans la liste déroulante et cliquez sur **Confirm (Confirmer)** pour confirmer les changements.



 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Utilisateurs mobiles Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Prisma Access offre deux méthodes de connexion pour sécuriser les utilisateurs mobiles : les utilisateurs peuvent se connecter Prisma Access à l'aide de l'application GlobalProtect ou en utilisant un fichier de configuration automatique de proxy (PAC).

- **Sécuriser les utilisateurs mobiles avec l'application GlobalProtect**

  Vous pouvez utiliser GlobalProtect dans les modes suivants :

  - Mode Tunnel—Le mode agent par défaut pour GlobalProtect dans Prisma Access. Établit un tunnel (IPSec ou SSL) pour Prisma Accesssécuriser l'accès des utilisateurs mobiles à toutes les applications, ports et protocoles, et pour obtenir une sécurité cohérente que l'utilisateur soit à l'intérieur ou à l'extérieur de votre réseau.

    L'application GlobalProtect installée sur le point de terminaison des utilisateurs sécurise le trafic des utilisateurs vers Internet, les applications SaaS et vos ressources cloud internes et publiques. Déployez l'application GlobalProtect auprès de vos utilisateurs (disponible pour les smartphones, tablettes ou ordinateurs portables fonctionnant sous Microsoft Windows, Apple macOS et iOS, Android, Google Chrome OS et Linux) afin qu'ils puissent acheminer le trafic pour Prisma Access l'application des politiques et la prévention des menaces. L'application GlobalProtect fournit également des rapports sur le profil d'information de l'hôte (HIP) afin que vous puissiez créer des règles granulaires basées sur l'état du périphérique pour garantir que les points de terminaison respectent vos normes de sécurité —par exemple, qu'ils sont équipés des derniers correctifs, du cryptage et de définitions de virus—pour accéder à vos applications les plus sensibles. Ou, pour permettre un accès sécurisé aux utilisateurs sur des périphériques non gérés, vous pouvez activer le VPN sans client. Prisma Access s'adapte dynamiquement en fonction de la région selon l'emplacement de vos utilisateurs à ce moment.
  - Mode Proxy—Ce mode vous permet d'utiliser un agent VPN tiers tout en utilisant Prisma Access comme passerelle web sécurisée pour une sécurité SaaS cohérente et supérieure. Cette méthode de connexion est idéale si vous n'êtes pas encore prêt à remplacer votre VPN d'application privée existant, mais que vous souhaitez remplacer votre passerelle web sécurisée. Par exemple, vous utilisez un agent VPN tiers pour un accès privé, mais vous souhaitez utiliser uniquement Prisma Access pour votre sécurité Internet. Les avantages de cette méthode de connexion incluent :
    - Répond aux exigences de conformité ou de réseau qui nécessitent un proxy
    - Réduit la charge de gestion des fichiers PAC et prend en charge les applications conscientes des proxy au-delà du navigateur.

    - Améliore l'expérience utilisateur en évitant la nécessité de revenir à un proxy web sur site.
  - Mode Tunnel et Proxy— Ce mode vous permet de sécuriser l'accès à Internet et aux applications SaaS via le mode proxy et de sécuriser l'accès aux applications privées via le mode tunnel. Ceci est particulièrement utile si vous avez besoin d'un accès rapide et à faible latence à une application privée et que votre Prisma Access emplacement n'est pas dans votre région.

    Dans ce mode, l'application GlobalProtect évalue d'abord les règles de transfert de proxy explicite que vous avez définies et envoie tout le trafic Internet vers le Prisma Access proxy explicite. Pour tout autre trafic, l'application détermine quel trafic envoyer à travers le tunnel vers la passerelle GlobalProtect, et quel trafic exclure du tunnel, en fonction des règles de tunnel fractionné que vous avez définies. Vous pouvez également utiliser le tunnel pour sécuriser toute application qui n'est pas consciente du proxy.

- **Sécuriser les utilisateurs mobiles en utilisant un fichier PAC**

  En plus de sécuriser les utilisateurs mobiles avec GlobalProtect, vous pouvez configurer un proxy explicite en utilisant Prisma Access. Avec un proxy explicite, un point de terminaison utilise un fichier PAC qui indique à un navigateur web et aux applications compatibles avec le proxy de rediriger le trafic vers le serveur proxy web au lieu du serveur de destination, protégeant ainsi votre trafic internet basé sur le web (HTTP et HTTPS).

  Si le réseau existant de votre organisation utilise déjà des proxys explicites et déploie des fichiers PAC sur vos points de terminaison et serveurs clients, vous pouvez migrer en douceur des solutions SWG basées sur des proxys hérités vers Prisma Access pour sécuriser le trafic Internet sortant des utilisateurs mobiles. Vous pouvez également utiliser un proxy explicite si vous devez utiliser un proxy à des fins d'audit ou de conformité.

- **Sécuriser les utilisateurs mobiles avec Prisma Access Browser Mobile**

  Le navigateur mobile Prisma Access simplifie la sécurisation des utilisateurs mobiles en combinant des contrôles d'accès solides avec une interface claire et intuitive. Il permet aux utilisateurs d'accéder en toute sécurité à des applications privées sans avoir recours aux VPN, aux certificats ou aux systèmes de gestion des périphériques mobiles (MDM), réduisant ainsi la complexité et facilitant la connectivité.

  Conçu pour les environnements Bring Your Own Device (BYOD), il garantit un accès sécurisé aux applications privées sur des périphériques non gérés, permettant aux organisations d'étendre des ressources critiques à l'ensemble de leur personnel. Les tablettes deviennent des alternatives de bureau polyvalentes grâce à Prisma Access Browser Mobile, offrant le même niveau de sécurité et d'accès que les points de terminaison traditionnels.

  Avec Prisma Access Browser Mobile, votre organisation peut rationaliser l'accès aux applications privées, améliorer la productivité sur tablette et maintenir une sécurité fiable sur diverses plateformes mobiles.

 ©2025 Palo Alto Networks, Inc.

Utilisateurs mobiles : GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

GlobalProtect vous permet de protéger les utilisateurs mobiles en installant l'application GlobalProtect sur leurs terminaux et en configurant les paramètres de GlobalProtect dans Prisma Access. GlobalProtect vous permet de sécuriser l'accès des utilisateurs mobiles à l'ensemble des applications, ports et protocoles, et de profiter d'une sécurité cohérente, que l'utilisateur se trouve à l'intérieur ou à l'extérieur de votre réseau.

Lorsque vous sécurisez les utilisateurs mobiles à l'aide de GlobalProtect, vous devez définir les paramètres pour configurer le portail et les passerelles dans le cloud. Par exemple, vous devez définir un nom d'hôte de portail et configurer le pool d'adresses IP pour les utilisateurs mobiles ainsi que les paramètres DNS pour les domaines internes. Vous pouvez utiliser les configurations existantes pour certains des paramètres requis, par exemple pour définir le profil d'authentification à utiliser pour l'authentification des utilisateurs mobiles. Si vous disposez déjà d'un modèle comportant vos profils d'authentification, certificats, profils de certificat et profils de serveur, vous pouvez l'ajouter à la pile de modèles prédéfinie lors de l'intégration pour simplifier le processus de configuration.

En outre, si vous souhaitez que les utilisateurs mobiles puissent se connecter aux emplacements de réseau distant ou si des utilisateurs mobiles se trouvant dans différentes zones géographiques ont besoin d'un accès direct aux terminaux des utilisateurs dans une autre zone, vous devez configurer au moins une connexion aux services avec des valeurs d'espace réservé, même si vous ne prévoyez pas d'utiliser la connexion pour fournir un accès aux emplacements de centre de données ou de siège. Bien que tous les emplacements de réseau distants soient entièrement maillés, cette configuration est nécessaire, car les passerelles Prisma Access (également appelées *emplacements*) se connectent à la connexion aux services dans une architecture en étoile pour fournir un accès aux réseaux internes de votre infrastructure Prisma Access.

- Liste de contrôle de planification pour GlobalProtect sur Prisma Access
- Configurer les utilisateurs mobiles GlobalProtect
- GlobalProtect – Personnaliser les paramètres de tunnel
- Requête de ticket pour désactiver GlobalProtect (Strata Cloud Manager)
- Surveiller les utilisateurs mobiles GlobalProtect
- Pools d'adresses IP pour un déploiement de type Utilisateurs mobiles – GlobalProtect
- Comment l'application GlobalProtect sélectionne des emplacements Prisma Access pour les utilisateurs mobiles
- Liste d'autorisation des utilisateurs mobiles de GlobalProtect
- Mises à niveau de l'application GlobalProtect
- Intégrer Prisma Access à des passerelles GlobalProtect sur site

 ©2025 Palo Alto Networks, Inc.

Liste de contrôle de planification pour GlobalProtect sur Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Si vous employez GlobalProtect pour sécuriser les utilisateurs mobiles, utilisez la liste de contrôle suivante pour vous assurer d'être en mesure d'activer le service et d'appliquer une politique cohérente pour vos utilisateurs mobiles (en protégeant les utilisateurs avec l'application GlobalProtect installée sur leurs terminaux et en autorisant les utilisateurs à accéder en toute sécurité aux applications à l'aide du VPN sans client).

- ☐ **Liste de contrôle de pré-installation :**
  - **Pool d'adresses IP** : pour configurer Prisma Access pour les utilisateurs, vous devez fournir un pool d'adresses IP qui ne chevauche pas d'autres adresses IP que vous utilisez en interne ou le pool d'adresses IP que vous avez désigné pour le sous-réseau d'infrastructure.

    Nous recommandons d'utiliser un pool d'adresses IP conforme à la norme RFC 1918. Bien que l'utilisation d'adresses IP (publiques) non conformes à la norme RFC 1918 soit possible, nous ne la recommandons pas en raison des éventuels conflits avec l'espace public d'adresses IP sur Internet.

    Ne spécifiez aucun sous-réseau qui chevauche les adresses IP et sous-réseaux suivants, car Prisma Access réserve ces adresses IP et sous-réseaux à son usage interne :

    169.254.0.0/16 et 100.64.0.0/10

    Prisma Access utilise ce pool d'adresses IP pour attribuer des adresses IP aux adaptateurs de réseau virtuel des terminaux lorsqu'ils se connectent à Prisma Access à l'aide de l'application GlobalProtect. Chaque périphérique qui se connecte à une passerelle d'utilisateur mobile Prisma Access a besoin de sa propre adresse IP. Vous devez spécifier ces pools durant le processus d'intégration des utilisateurs mobiles.

    Palo Alto Networks recommande que le nombre d'adresses IP dans le pool soit deux fois supérieur au nombre de périphériques d'utilisateurs mobiles qui se connecteront à Prisma Access. Si votre organisation dispose d'une politique BYOD (Bring Your Own Device, apportez votre propre périphérique) ou si un utilisateur unique possède plusieurs comptes utilisateur, veillez à tenir compte de ces périphériques et comptes supplémentaires lorsque vous allouez des pools d'adresses IP. Si le pool d'adresses IP atteint sa limite, les autres périphériques d'utilisateurs mobiles ne pourront pas se connecter.

    Lorsque les périphériques d'utilisateurs mobiles se connectent à une passerelle, Prisma Access récupère les adresses IP des pools que vous avez spécifiés et les alloue à la passerelle dans des blocs /24. Lorsqu'un bloc /24 atteint sa limite à mesure que d'autres périphériques d'utilisateurs se connectent, Prisma Access alloue d'autres blocs /24 du pool à la passerelle. Prisma Access annonce ces sous-réseaux /24 dans sa dorsale, car ils sont alloués en fonction de leurs attributions de passerelle.

 ©2025 Palo Alto Networks, Inc.

- **Modèle** : le déploiement GlobalProtect de Prisma Access crée automatiquement une pile de modèles et un modèle de niveau supérieur. Si vous exécutez déjà GlobalProtect sur site et que vous souhaitez tirer parti de votre configuration existante, vous pouvez ajouter des modèles supplémentaires à la pile pour transmettre les configurations existantes des modèles de portail GlobalProtect, passerelle GlobalProtect, User-ID, profil de serveur (par exemple, pour vous connecter à votre service d'authentification), certificat et profil de service SSL/TLS à Prisma Access pour les utilisateurs. Si vous n'avez pas de modèle avec les paramètres de configuration existants, vous pouvez saisir les paramètres de configuration requis manuellement lors de la configuration de GlobalProtect sur Prisma Access (Managed by Panorama). En outre, tout modèle que vous ajoutez à la pile doit comporter la configuration de zone pour les zones que vous utilisez pour appliquer la politique de sécurité à vos utilisateurs mobiles.
- **Groupe de périphériques parent** : lorsque vous configurez Prisma Access pour les utilisateurs, vous devez spécifier un groupe de périphériques parent à utiliser lors de la transmission de vos groupes d'adresses, politique de sécurité, profils de sécurité, ainsi que d'autres objets de politique (tels que des groupes d'applications et des objets), des objets et profils HIP et la politique d'authentification dont le service a besoin pour appliquer une politique cohérente pour vos utilisateurs distants.
- **Emplacements à intégrer** : Prisma Access vous offre des emplacements dans le monde entier où vous pouvez configurer GlobalProtect sur Prisma Access (Managed by Panorama). Avant d'intégrer vos emplacements, consultez cette liste pour déterminer les emplacements que vous devez intégrer pour le déploiement de vos utilisateurs mobiles.

  Choisissez les emplacements les plus proches de vos utilisateurs ou qui se situent dans le même pays que ceux-ci. Si aucun emplacement n'est disponible dans le pays où vos utilisateurs mobiles résident, vous pouvez choisir un emplacement qui emploie la même langue que vos utilisateurs mobiles.

  Vous pouvez également répartir les emplacements par région géographique. Le fait de conserver tous les emplacements dans une seule région vous permet de spécifier un pool d'adresses IP pour cette région uniquement, ce qui peut être utile si vous disposez d'un nombre limité d'adresses IP que vous pouvez allouer au pool. Un seul pool régional d'adresses IP offre également un contrôle plus granulaire sur les régions déployées et vous permet d'exclure des régions, comme l'exige votre politique ou les réglementations du secteur.

  Si vous avez une licence locale Prisma Access pour les utilisateurs et que vous disposez d'un déploiement GlobalProtect ainsi que d'un déploiement de proxy explicite, vous pouvez déployer un maximum de cinq emplacements pour les deux déploiements combinés. Vous devez allouer les cinq emplacements entre les deux déploiements (par exemple, deux emplacements pour les utilisateurs mobiles (GlobalProtect) et trois emplacements pour les utilisateurs mobiles (proxy explicite). Si vous disposez d'une licence mondiale, il n'y a pas de restrictions quant au nombre maximal d'emplacements.
- **Nom d'hôte du portail** : Prisma Access pour les utilisateurs vous permet de configurer rapidement et facilement le nom d'hôte du portail à l'aide d'un nom de domaine par défaut (`.gpcloudservice.com`). Dans ce cas, le Cloud Service publie automatiquement le nom d'hôte sur les serveurs DNS publics et gère toute la génération de certificats. Toutefois, vous pouvez choisir d'utiliser le nom de domaine de votre propre entreprise dans le nom d'hôte du portail. Si vous envisagez d'utiliser le nom de domaine de votre entreprise, vous devez obtenir vos propres certificats pour le portail et configurer un profil de service

 ©2025 Palo Alto Networks, Inc.

SSL/TLS pour pointer vers le certificat avant de configurer le service. En outre, si vous utilisez votre propre nom de domaine dans le nom d'hôte du portail, vous devez également configurer vos serveurs DNS pour qu'ils pointent vers le CNAME DNS du portail, qui est fourni pendant le processus de configuration.

- **Connexion aux services** : vous devez créer et configurer une connexion aux services si vous souhaitez autoriser vos utilisateurs mobiles à accéder à des ressources, comme les serveurs d'authentification, sur votre réseau interne (par exemple, un serveur d'authentification à l'emplacement de votre centre de données ou de votre siège social) ou à vos emplacements de réseau distant.

  Même si vous ne prévoyez pas d'utiliser la connexion pour fournir un accès à vos ressources internes, vous devez configurer au moins une connexion aux services avec des valeurs d'espace réservé si vous souhaitez que vos utilisateurs mobiles puissent se connecter aux emplacements de réseau distant ou si vous avez des utilisateurs mobiles dans des zones géographiques différentes qui ont besoin d'un accès direct aux terminaux des utilisateurs situés dans une autre zone.
- **Utilisation d'IPv6 dans votre réseau** : déterminez si vous souhaitez effectuer une atténuation du trafic IPv6 dans votre réseau afin de réduire la surface d'attaque. Dans un terminal à double pile capable de traiter à la fois le trafic IPv4 et IPv6, le trafic IPv6 des utilisateurs mobiles n'est pas envoyé à Prisma Access par défaut ; il est plutôt envoyé à la carte réseau locale du terminal. Pour cette raison, Palo Alto Networks vous recommande de configurer Prisma Access sur le trafic de l'entonnoir IPv6.
- **Journalisation des terminaux GlobalProtect** : deux options se présentent pour collecter les journaux des utilisateurs mobiles qui utilisent l'application GlobalProtect :
  - **Collecte manuelle des journaux à partir des terminaux GlobalProtect** : demandez aux utilisateurs mobiles de collecter les journaux de l'application GlobalProtect pour les périphériques Windows, macOS et Linux. Cette option ne nécessite aucune configuration supplémentaire.
  - **Collecte des journaux de l'application GlobalProtect pour le dépannage** : permet à l'application GlobalProtect d'effectuer des tests de diagnostic de bout en bout pour résoudre les problèmes de connexion, de performances et d'accès, et de générer des journaux de dépannage et de diagnostic à envoyer à Strata Logging Service pour une analyse plus approfondie. Vous devez générer un certificat pour que l'application GlobalProtect puisse s'authentifier avec Strata Logging Service pour collecter les journaux de dépannage. Grâce à **Prisma Access (Managed by Strata Cloud Manager)**, vous pouvez activer l'application GlobalProtect pour collecter les journaux Strata Logging Service pour le dépannage. Pour **Prisma Access (Managed by Panorama)**, cette fonctionnalité se trouve sous **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** > **Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM (Générer un certificat pour la collecte de journaux de l'application GlobalProtect et Autonomous DEM)**. Consultez la collecte des journaux d'application GlobalProtect pour le dépannage pour avoir des détails sur la configuration.

☐ **Liste de contrôle de post-installation :**

- **Ajouter les adresses IP publiques à une liste d'autorisation dans votre réseau** : après avoir intégré vos emplacements, vous devez récupérer les adresses IP publiques utilisées par chaque emplacement et les ajouter à une liste d'autorisation dans votre réseau pour autoriser les utilisateurs mobiles à accéder aux applications SaaS ou publiques. Si vous

 ©2025 Palo Alto Networks, Inc.

ajoutez d'autres emplacements, vous devrez également récupérer les nouvelles adresses IP attribuées par Prisma Access à l'emplacement ou aux emplacements nouvellement ajoutés.

- **Cohérence de la dénomination des passerelles** : si vous disposez déjà d'un déploiement GlobalProtect pour les utilisateurs mobiles et que votre organisation exerce une activité de fusions et d'acquisitions, vous aurez peut-être besoin des passerelles existantes pour ne pas faire référence à un nom de marque antérieur ou à un nouveau nom de marque. Dans ce cas, contactez votre équipe de compte Palo Alto Networks qui ouvrira un dossier SRE pour répondre à la requête. Palo Alto Networks vous recommande de programmer ce changement pendant une fenêtre de maintenance ou pendant les heures creuses. Palo Alto Networks met à niveau toutes les passerelles de votre déploiement qui nécessitent un changement de nom pendant la fenêtre de maintenance.

Configurer les utilisateurs mobiles GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Avant de configurer les utilisateurs mobiles, assurez-vous de disposer des licences requises (licence Prisma Access pour les utilisateurs mobiles et une licence Strata Logging Service avec espace de stockage pare-feu approprié). Si les utilisateurs mobiles se connectent à d'autres réseaux connectés, vous aurez besoin de la licence ZTNA (Zero Trust Network Access) ou Enterprise Edition Prisma Access qui fournira le nœud d'accès d'entreprise (CAN) nécessaire pour vous connecter.

Pour configurer Prisma Access pour les utilisateurs mobiles, vous aurez besoin des éléments suivants :

- Prisma Access Licence pour les utilisateurs mobiles Vérifiez que la licence Prisma Access pour les utilisateurs mobiles a été activée.
- Pool d'adresses IP pour les utilisateurs mobiles : Vérifiez que vous disposez d'un ou plusieurs pools d'adresses IP non superposés disponibles pour les utilisateurs mobiles.
- Nom d'hôte du portail : Assurez-vous de connaître le nom de domaine complet (FQDN) du portail.
- Agent GlobalProtect pour les utilisateurs mobiles : Prisma Access pour les utilisateurs mobiles nécessite l'application GlobalProtect sur chaque point de terminaison pris en charge. Vous aurez besoin d'une stratégie de déploiement pour installer GlobalProtect Agent sur les périphériques des utilisateurs mobiles.
- Informations sur les règles de stratégie de sécurité : Vous devez déployer des règles de stratégie de sécurité pour autoriser ou refuser le trafic via Prisma Access. Vous devrez savoir quelles règles déployer lorsque vous configurez Prisma Access pour vos utilisateurs mobiles.
- Emplacements géographiques de vos utilisateurs mobiles : Lorsque vous approvisionnez des utilisateurs mobiles, vous devez sélectionner un emplacement géographique disponible proche de vos utilisateurs mobiles.

 ©2025 Palo Alto Networks, Inc.

Découvrez comment intégrer les utilisateurs mobiles de GlobalProtect à Prisma Access.

- Strata Cloud Manager
- Panorama

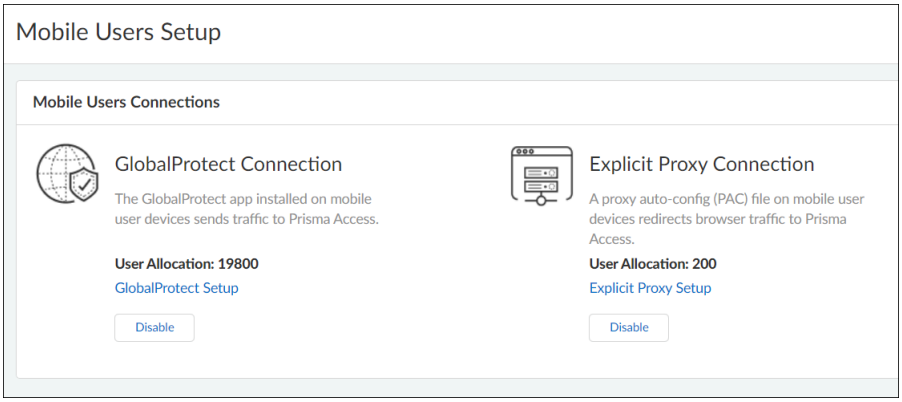
Configurer les utilisateurs mobiles GlobalProtect (Strata Cloud Manager)

En quelques étapes seulement, voici comment commencer l'intégration des utilisateurs mobiles GlobalProtect pour Prisma Access.

1. **Activez GlobalProtect en tant que type de connexion d'utilisateur mobile**

   Allez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Mobile Users (Utilisateurs mobiles)**.

   Vous pouvez diviser votre licence d'utilisateur mobile entre GlobalProtect et les connexions proxy explicites ; certains utilisateurs peuvent se connecter via GlobalProtect et d'autres via proxy explicite. Avec une **Connexion GlobalProtect**, l'application GlobalProtect installée sur les périphériques des utilisateurs mobiles envoie le trafic vers Prisma Access.

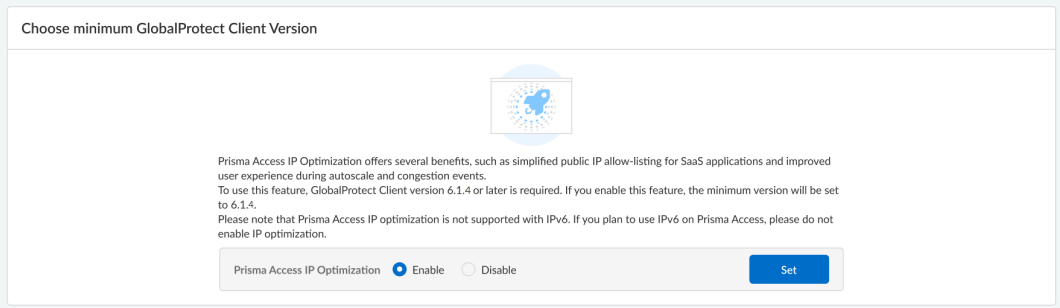


 ©2025 Palo Alto Networks, Inc.

2. **Configurer les paramètres d'infrastructure de base**

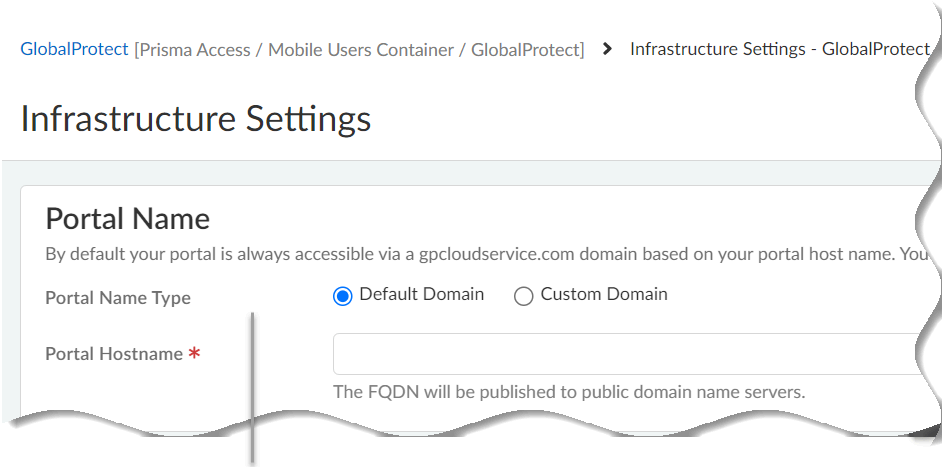
   Configurez les paramètres d'infrastructure spécifiques à GlobalProtect. Il y a quelques paramètres requis que vous devrez remplir au départ, afin que Prisma Access puisse provisionner votre environnement d'utilisateur mobile.

   - *Lorsque vous configurez GlobalProtect pour la première fois, vous décidez d'activer ou non Prisma Access Optimisation IP. Le choix d'activer l'optimisation IP nécessite la version client GlobalProtect 6.1.4 et versions ultérieures, 6.2.3 et versions ultérieures, ou 6.3.0 et versions ultérieures, et ne prend pas en charge IPv6. Choisissez avec soin, car vous ne pourrez pas modifier ce paramètre ultérieurement.*
   - *La fonctionnalité d'optimisation IP est pour les nouveaux Prisma Access déploiements GlobalProtect uniquement. Les déploiements GlobalProtect existants, y compris les nouveaux locataires que vous créez à partir d'un déploiement multi-locataires existant, ne sont pas éligibles.*
   - *Si vous migrez votre déploiement GlobalProtect vers Prisma Access (en dehors de l'utilisation de passerelles et des portails sur site), assurez-vous que tous les utilisateurs exécutent l'application GlobalProtect version 6.1.4 et ultérieure, 6.2.3 et ultérieure ou 6.3 et ultérieure avant d'activer cette fonctionnalité.*



   Allez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **Infrastructure** > **Infrastructure Settings (Paramètres d'infrastructure)**.

 ©2025 Palo Alto Networks, Inc.



GlobalProtect Infrastructure Settings

- Spécifiez le **Portal Name (Nom du portail)**.
  - **Default Domain (Domaine par défaut)**—Si vous sélectionnez cette option, le nom d'hôte de votre portail utilise le nom de domaine par défaut : `.gpcloudservice.com`. Dans ce cas, il suffit d'entrer un **Portal Hostname (Nom d'hôte du portail)** à ajouter au nom de domaine par défaut. Prisma Access pour les utilisateurs créera automatiquement les certificats nécessaires et publiera le nom d'hôte sur les serveurs DNS publics.
  - **Custom Domain (Domaine personnalisé)**—Vous pouvez également personnaliser l'adresse du portail si vous souhaitez que le domaine du nom d'hôte du portail corresponde au nom de domaine de votre entreprise (par exemple, myportal.mydomain.com).
- Saisissez les paramètres de résolution **Client DNS (DNS client)** pour votre déploiement GlobalProtect.
  - Sélectionnez une région pour les **DNS Servers (Serveurs DNS)** (**Add Region (Ajouter une région)**).

    Sélectionnez **Worldwide (Mondial)** ou un théâtre. Si vous spécifiez plusieurs paramètres proxy avec une combinaison de paramètres Mondial et Théâtre, Prisma Access utilise les paramètres du groupe d'emplacement, puis Théâtre, puis Mondial. Prisma Access évalue les règles de haut en bas dans la liste.
  - Choisissez si vous souhaitez ou non que Prisma Access effectue l'opération **Resolve internal domains (Résoudre les domaines internes)** ; si vous le souhaitez, **Add (Ajouter)** une ou plusieurs **Internal Domain Resolve Rules (Règles de résolution de domaine interne)**.
  - Saisissez un **Name (Nom)** unique pour la règle.
  - Sélectionnez **Prisma Access Default (Par défaut Prisma Access)** pour utiliser le serveur DNS Prisma Access par défaut pour résoudre les domaines internes. vous souhaitez que votre serveur DNS interne ne résolve que les domaines que vous spécifiez, entrez les domaines à résoudre dans la **Domain List (Liste des domaines)**. Spécifiez un astérisque

 ©2025 Palo Alto Networks, Inc.

devant le domaine ; par exemple, *.acme.com. Vous pouvez spécifier un maximum de 1 024 entrées de domaine

.

- Si vous disposez d'un serveur DNS **Custom (Personnalisé)** capable d'accéder à vos domaines internes, spécifiez les adresses IP du serveur **Primary DNS (DNS principal)** et **Secondary DNS (DNS secondaire)**.
- Si vous souhaitez que votre serveur DNS interne résolve uniquement les domaines que vous spécifiez, saisissez les domaines à résoudre dans les **Domain Lists (Listes de domaines)**. Spécifiez un astérisque devant le domaine ; par exemple, *.acme.com. Vous pouvez spécifier un maximum de 1 024 entrées de domaine
- **Save (Enregistrer)** vos modifications lorsque vous avez terminé.

- (Facultatif) Spécifiez un **Client IP Pool (Pool d'adresses IP client)**.

  Par défaut, Prisma Access fournit un pool d'adresses IP d'utilisateur mobile par défaut de 100.127.0.0/16 qui peut être utilisé n'importe où dans le monde. Prisma Access attribue une adresse IP de ce pool à chaque périphérique connecté à GlobalProtect. Vous pouvez éventuellement ajouter un pool d'adresses IP par région ici.

  - Saisissez un sous-réseau minimum requis de /23 (512 adresses IP) par emplacement. Les emplacements supplémentaires nécessitent un sous-réseau minimum de /23. Si vous spécifiez un sous-réseau mondial, le sous-réseau minimum requis est /23, mais nous vous recommandons Pools d'adresses IP pour un déploiement de type Utilisateurs mobiles – GlobalProtect pour attribuer un nombre d'adresses IP égal ou supérieur au nombre d'utilisateurs mobiles sous licence afin qu'ils puissent se connecter en même temps.

    Ne spécifiez pas d'adresses qui chevauchent d'autres réseaux que vous utilisez en interne ou avec les pools que vous avez attribués lorsque vous Configurer l'infrastructure de service Prisma Access (Panorama). En outre, n'utilisez pas les adresses IP et sous-réseaux suivants, car Prisma Access réserve ces adresses IP et sous-réseaux à son usage interne :

    - 169.254.0.0/16

 ©2025 Palo Alto Networks, Inc.

- 100.64.0.0/10

Nous recommandons d'utiliser un pool d'adresses IP conforme à la norme RFC 1918. Bien que les adresses IP (publiques) non conformes à la RFC 1918 soient prises en charge pour les utilisateurs mobiles, évitez de les utiliser à cause d'éventuels conflits avec l'espace des adresses IP publiques d'Internet.

- Spécifiez les paramètres DNS pour le **Primary DNS for public domains (DNS principal pour les domaines publics)** et le **Secondary DNS for public domains (DNS secondaire pour les domaines publics)**.
  - **Prisma Access Default (Par défaut Prisma Access)**—Utilisez le serveur DNS Prisma Access par défaut.
  - **Internal DNS (DNS interne)** : utilisez le même serveur que vous utilisez pour résoudre les domaines internes.
  - **Custom (Personnalisé)**—Si vous disposez d'un serveur DNS capable d'accéder à vos domaines publics (externes), saisissez l'adresse du serveur DNS principal dans ce champ.
  - Vous pouvez ajouter un **Client DNS Suffix List (Liste de suffixes DNS client)** pour spécifier le suffixe que le client doit utiliser localement lorsqu'un nom d'hôte non qualifié est saisi et qu'il ne peut pas résoudre, par exemple, acme.local. Ne saisissez pas de caractère générique (*) avant le suffixe de domaine (par exemple, acme.com). Vous pouvez ajouter plusieurs suffixes.

3. Configurez **Advanced Settings (Paramètres avancés)**.
   - (Facultatif) Utilisez **Static Entries (Entrées statiques)** pour résoudre les noms de domaines complets en adresses IP spécifiques.

     Cette fonctionnalité peut être utile si vous disposez de services Internet invités dans votre organisation et que vous souhaitez que vos invités utilisent les moteurs de recherche en toute sécurité, ce qui les empêche de rechercher du contenu potentiellement inapproprié ou offensant qui pourrait être contraire à la politique de l'entreprise. Pour ce faire, saisissez un **Name (Nom)** unique pour la règle d'entrée statique, un **FQDN** et l'**Address (Adresse)** IP vers laquelle la demande FQDN doit être dirigée.

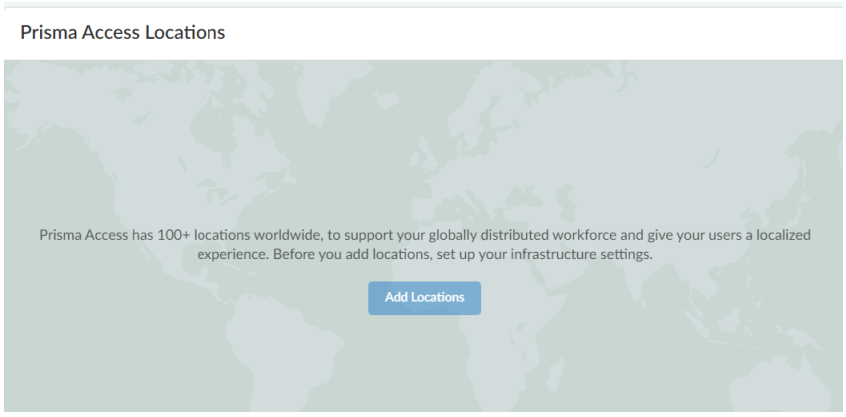
   - Si vous souhaitez que Prisma Access serve de proxy pour les requêtes DNS, configurez les valeurs de **UDP Queries Retries (Tentatives de requêtes UDP)** **(Interval (Sec) (Intervalle (sec))** pour réessayer la requête en secondes et le nombre de **Attempts (Tentatives)** de requête à effectuer.

4. **Sélectionnez l'emplacement Prisma Access auquel vos utilisateurs GlobalProtect se connecteront**

   Ajoutez les emplacements Prisma Access où vous souhaitez prendre en charge les utilisateurs de GlobalProtect. Allez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de**

 ©2025 Palo Alto Networks, Inc.

Prisma Access) > GlobalProtect > Infrastructure > Prisma Access Locations (Emplacements Prisma Access).



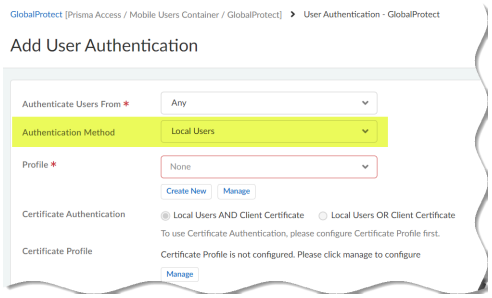
La carte affiche les régions globales où vous pouvez déployer des Prisma Access pour les utilisateurs : En outre, Prisma Access fournit plusieurs emplacements dans chaque région pour s'assurer que vos utilisateurs peuvent se connecter à un emplacement qui offre une expérience utilisateur adaptée à la région des utilisateurs. Pour des performances optimales, cliquez sur **Select All (Sélectionner tout)**. Sinon, sélectionnez les emplacements spécifiques dans chaque région sélectionnée où vos utilisateurs auront besoin d'accès. En limitant votre déploiement à une seule région, vous pouvez avoir un contrôle plus granulaire sur vos régions déployées et exclure les régions requises par votre politique ou les règles de l'industrie.

Pour une expérience utilisateur optimale, si vous limitez le nombre d'emplacements, choisissez les emplacements les plus proches ou situés dans le même pays que vos utilisateurs. Si aucun emplacement n'est disponible dans le pays où résident vos utilisateurs mobiles, choisissez l'emplacement le plus proche de vos utilisateurs pour obtenir les meilleures performances.

5. **Authentifier les utilisateurs GlobalProtect**

   Configurez l'authentification utilisateur de sorte que seuls les utilisateurs légitimes aient accès à vos services et applications. Allez à **Workflows (Flux de travail) > Prisma Access Setup (Configuration de Prisma Access) > GlobalProtect > Infrastructure > User Authentication (Authentification de l'utilisateur)**.

   Pour tester votre configuration, vous pouvez ajouter des utilisateurs que Prisma Access authentifie localement, ou vous pouvez passer directement à la configuration de l'authentification au niveau de l'entreprise. En savoir plus sur la procédure Permettre aux utilisateurs mobiles de s'authentifier auprès de Prisma Access.



 ©2025 Palo Alto Networks, Inc.

6. Prisma Access applique les règles de stratégie de sécurité recommandées par défaut. Ces règles permettent à vos utilisateurs de naviguer en toute sécurité vers des sites Internet généraux. Les utilisateurs sont :
   - Interdits d'accès à des sites Web malveillants connus en fonction de l'URL
   - Interdits de téléversement ou de téléchargement de fichiers connus pour être malveillants
   - Protégés contre des menaces inconnues et inédites
   - Protégés contre les virus, les logiciels espions (attaques de commande et de contrôle) et les vulnérabilités

   Après avoir effectué la configuration initiale, vous pouvez examiner et mettre à jour ces règles par défaut pour répondre aux besoins de votre entreprise.
7. **Vérifiez que la position de l'utilisateur mobile est active**

   Après avoir poussé votre configuration initiale à Prisma Access, Prisma Access commence à approvisionner votre environnement utilisateur mobile GlobalProtect. Cela peut prendre jusqu'à 15 minutes.

   *Vous pouvez également valider votre configuration en sélectionnant **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Paramètres d'infrastructure)** et modifiez les paramètres d'infrastructure pour confirmer qu'une passerelle est configurée dans chacun des emplacements que vous avez approvisionnés.*

GlobalProtect — Personnaliser l'adresse du portail

Prisma Access nécessite uniquement les paramètres minimum pour provisionner l'environnement de votre utilisateur mobile afin que vous puissiez le tester. Si vous préférez utiliser le domaine de votre entreprise dans l'adresse du portail, vous pouvez modifier l'adresse après la configuration initiale de l'environnement.

Par défaut Prisma Access utilise le domaine *gpcloudservice.com* pour configurer Prisma Access l'adresse du portail à laquelle vos utilisateurs mobiles devront se connecter pour un accès sécurisé à Internet, à votre siège social et à vos centres de données. Vous devez utiliser ce domaine par défaut lors de la configuration et du test initiaux de votre environnement. Si vous souhaitez personnaliser le nom de domaine après la configuration initiale pour utiliser le domaine de votre entreprise, vous pouvez revenir en arrière et modifier les paramètres d'environnement afin que l'adresse du portail à laquelle vos utilisateurs se connectent contienne votre propre domaine d'entreprise (par exemple, prisma-access.acme.com).

*Le domaine *.gpcloudservice.com est associé à l'application Palo Alto Networks.*

Pour configurer Prisma Access pour utiliser votre propre domaine, vous devez :

- ☐ Obtenir des certificats pour le service.
- ☐ Créer une entrée DNS CNAME sur vos serveurs DNS qui mappe l'adresse de portail par défaut à l'aide du domaine par défaut à l'adresse de portail personnalisée qui utilise le domaine de votre entreprise. Vous devez le faire parce que Prisma Access publie l'adresse du portail que vous avez configurée sur les serveurs du domaine public lors de l'approvisionnement initial.

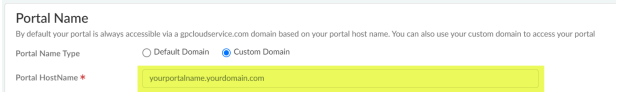
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **Infrastructure** et modifiez les **Infrastructure Settings (Paramètres d'infrastructure)**.

Dans Strata Cloud Manager, la redondance du réseau est activée par défaut entre les portails ou les passerelles et les connexions aux services, ce qui garantit une connectivité redondante pour les utilisateurs mobiles aux services et applications accessibles.

STEP 2 | Définissez le type de nom du portail sur **Custom Domain (Domaine personnalisé)**.

STEP 3 | Entrez le **Portal Hostname (Nom d'hôte du portail)** que vous souhaitez utiliser.



STEP 4 | Ajoutez le **Portal DNS CNAME (CNAME DNS du portail)** auquel mapper les entrées de votre serveur DNS.

STEP 5 | **Import (Importer)** le **Certificate (Certificat)** que vous avez fourni pour votre adresse de portail de domaine personnalisé.

1. Sélectionnez le **Format** de certificat pour le certificat que vous importez :
   - **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat chiffrés (PKCS12))**—La clé et le certificat se trouvent dans un seul conteneur (Fichier de certificat). Cliquez sur **Choose File (Choisir un fichier)** et accédez au fichier PKCS12 à importer.
   - **Base64 Encoded Certificate (PEM) (Certificat codé en base 64 (PEM))**—Si vous sélectionnez cette option, vous devez importer le **Key File (Fichier clé)** séparément du certificat. Pour importer le certificat PEM et le fichier clé, cliquez sur **Choose File (Choisir un fichier)**.
2. Entrez la **Passphrase (Phrase secrète)** pour chiffrer la clé et **Confirm Passphrase (Confirmer la phrase secrète)**, puis cliquez sur **Save (Enregistrer)**.

STEP 6 | Si vous ne l'avez pas déjà fait, configurez vos serveurs DNS pour qu'ils pointent vers le Prisma Access DNS CNAME que vous avez défini.

STEP 7 | **Save (Enregistrer)** la configuration de l'environnement et **Push Config (Transmettre la configuration)** à Prisma Access.

Assurez-vous de sélectionner les deux portée de configuration **Explicit Proxy (Proxy explicite)** et **GlobalProtect**.

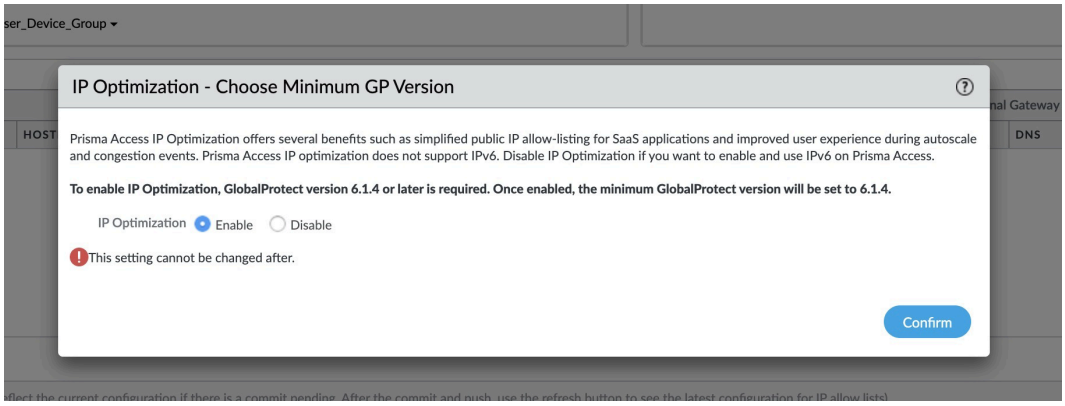
Configurer les utilisateurs mobiles GlobalProtect (Panorama)

Pour configurer un déploiement Utilisateurs mobiles—GlobalProtect, effectuez les étapes suivantes. Avant de commencer, assurez-vous de comprendre comment Prisma Access fonctionne et utilisez la liste de vérification pour planifier votre déploiement GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—GlobalProtect (Utilisateurs mobiles—GlobalProtect)**.

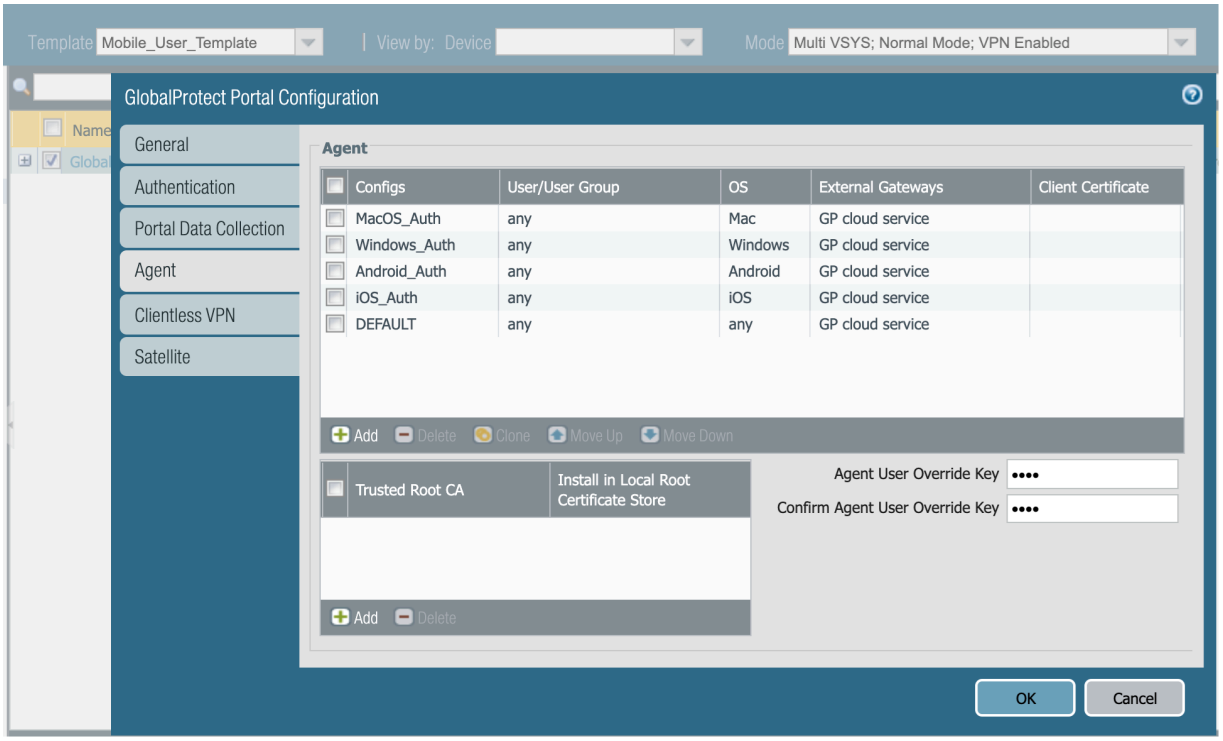
- *Lorsque vous configurez GlobalProtect pour la première fois, il vous sera demandé si vous souhaitez ou non activer l'optimisation IP Prisma Access. Le choix d'activer l'optimisation IP nécessite* la version client GlobalProtect *6.1.4 et versions ultérieures, 6.2.3 et versions ultérieures, ou 6.3.0 et versions ultérieures, et ne prend pas en charge IPv6. Choisissez avec soin, car vous ne pourrez pas modifier ce paramètre ultérieurement.*
- *La fonctionnalité d'optimisation IP est pour les nouveaux Prisma Access déploiements GlobalProtect uniquement. Les déploiements GlobalProtect existants, y compris les nouveaux locataires que vous créez à partir d'un déploiement multi-locataires existant, ne sont pas éligibles.*
- *Si vous migrez votre déploiement GlobalProtect vers Prisma Access (en dehors de l'utilisation de passerelles et des portails sur site), assurez-vous que tous les utilisateurs exécutent l'application GlobalProtect version 6.1.4 et ultérieure, 6.2.3 et ultérieure ou 6.3 et ultérieure avant d'activer cette fonctionnalité*



STEP 2 | (Facultatif) Si vous souhaitez personnaliser la configuration de l'agent que Prisma Access envoie aux clients, modifiez la configuration du portail GlobalProtect dans le Mobile_User_Template pour ajouter une nouvelle configuration d'agent. Après avoir configuré la configuration de l'agent, déplacez-la au-dessus de la configuration de l'agent PAR DÉFAUT qui est prédéfinie dans le modèle pour vous assurer que vos paramètres ont

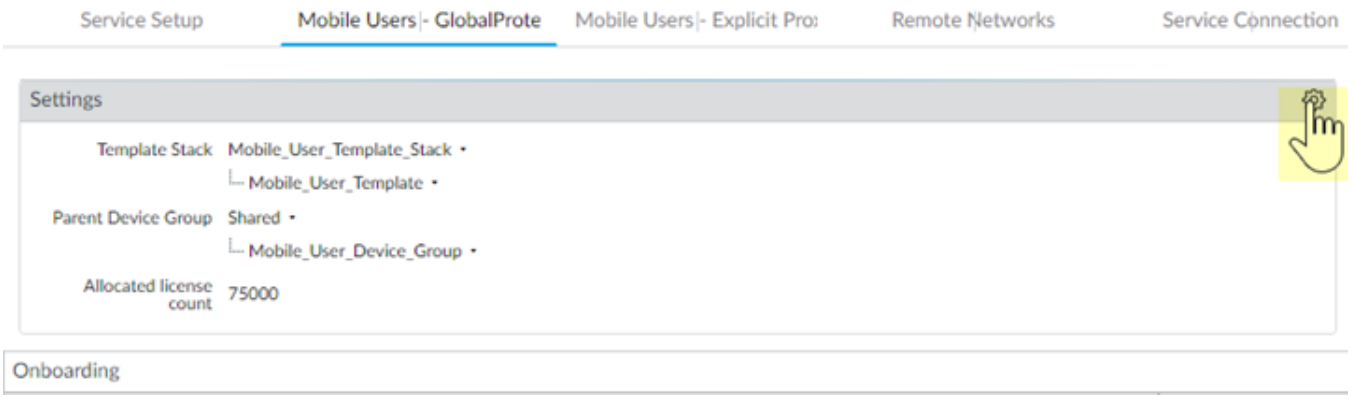
 ©2025 Palo Alto Networks, Inc.

priorité sur les paramètres par défaut. Lorsque vous modifiez ce modèle, ne supprimez pas ou ne modifiez pas l'entrée Passerelle externe.



STEP 3 | Configurez la hiérarchie du groupe de périphériques que le service cloud poussera vers le portail et la passerelle.

1. Modifiez les **Settings (Paramètres)**.



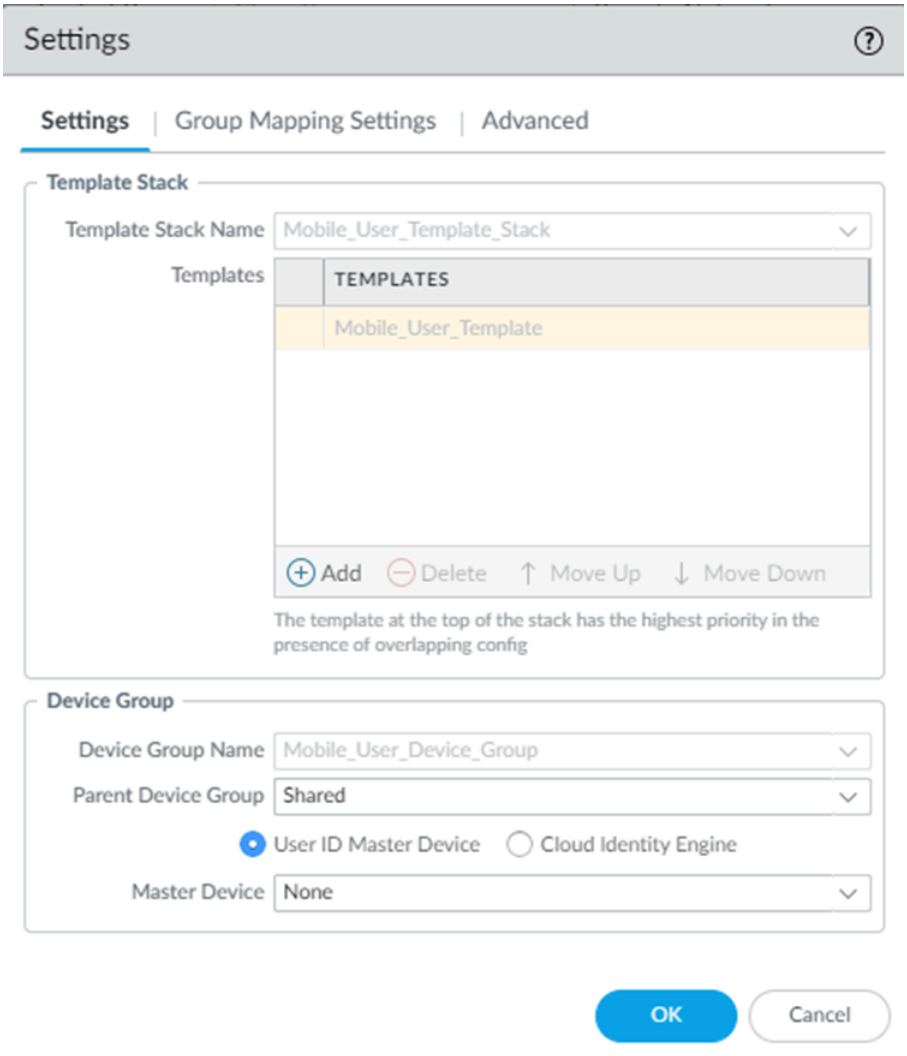
2. Dans la section Groupe de périphériques, sélectionnez le**Parent Device Group (Groupe de périphériques parent)** qui contient les paramètres de configuration que vous souhaitez envoyer à Prisma Access pour les utilisateurs, ou laissez le groupe de

 ©2025 Palo Alto Networks, Inc.

périphériques parent comme **Shared (Partagé)** pour utiliser la hiérarchie partagée du groupe de périphériques Prisma Access.

Vous pousserez toute la configuration – y compris les groupes d'adresses, la stratégie de sécurité, les profils de sécurité et d'autres objets de stratégie (tels que les groupes et objets d'application), les objets et profils HIP et la stratégie d'authentification–dont Prisma Access pour les utilisateurs a besoin pour appliquer une politique cohérente à vos utilisateurs mobiles en utilisant la hiérarchie de groupe de périphériques que vous spécifiez ici. En outre, vous devez vous assurer que vous avez configuré un profil de transfert de journaux qui transfère les types de journaux souhaités à **Panorama/ Strata Logging Service (Panorama/Service de journalisation Strata)** dans un groupe de périphériques qui est poussé à Prisma Access pour les utilisateurs ; c'est la seule façon pour le service cloud de savoir quels journaux transférer à Strata Logging Service.

3. (Facultatif) Si vous avez configuré un pare-feu nouvelle génération comme périphérique principal ou ajouté un profilCloud Identity Engine pour permettre la sélection des informations de l'utilisateur et du groupe dans les stratégies de sécurité, sélectionnez **User-ID Master Device (Périphérique principal User-ID)** ou **Cloud Identity Engine** ; sélectionnez ensuite le profil de Périphérique principal ou de Cloud Identity Engine que vous avez créé.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | (Facultatif) Configurez Prisma Access pour utiliser le composant Synchronisation de répertoire de Cloud Identity Engine pour récupérer les informations d'utilisateur et de groupe.

Vous devez configurer le composant de synchronisation de répertoire du Cloud Identity Engine pour récupérer les informations d'utilisateur et de groupe dans le répertoire cloud ou l'Active Directory (AD) avant d'activer et de configurer l'intégration de la synchronisation de répertoire dans les Prisma Access**Group Mapping Settings (Paramètres de mappage de groupe)**.

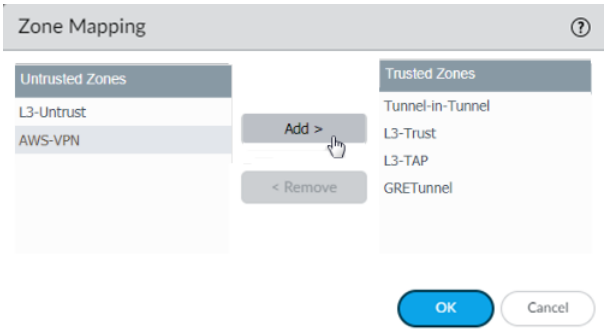
STEP 5 | Cliquez sur **OK** pour enregistrer les paramètres de l'utilisateur mobile.

STEP 6 | Mappez les zones configurées dans la pile de modèles comme fiables ou non.

Sur un pare-feu de la nouvelle génération Palo Alto Networks, la stratégie de sécurité est appliquée entre les zones, qui s'adaptent aux interfaces physiques ou virtuelles du pare-feu. Cependant, avec Prisma Access pour les utilisateurs, l'infrastructure réseau est automatiquement configurée pour vous, ce qui signifie que vous ne devez plus configurer des interfaces et les associer à des zones. Cependant, pour permettre une application cohérente des politiques de sécurité, vous devez cartographier les zones que vous utilisez au sein de votre organisation comme fiables ou non fiables afin que Prisma Access pour utilisateurs puisse traduire les règles de politique que vous appliquez au service cloud vers les zones internes de l'infrastructure réseau.

1. Modifiez les paramètres de mappage de zone.

   Par défaut, toutes les zones de Mobile_User_Template_Stack sont classées comme Zones non fiables.
2. Pour chaque zone que vous souhaitez désigner comme approuvée, sélectionnez-la et cliquez sur **Add (Ajouter)** pour la déplacer vers la liste des **Trusted Zones (Zones approuvées)**.



3. Cliquez sur **OK** pour enregistrer vos modifications.

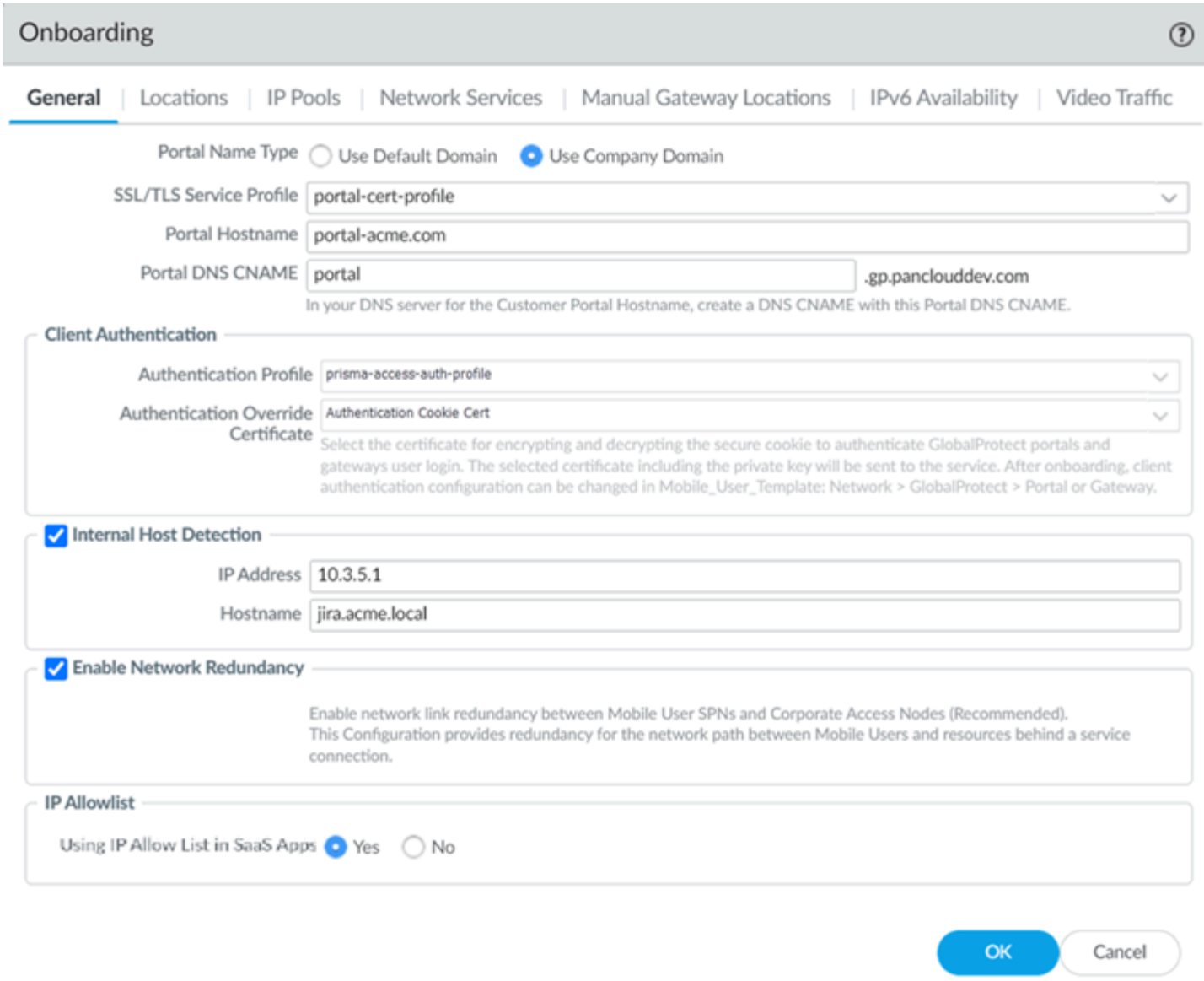
STEP 7 | Configurez le portail GlobalProtect et les paramètres de la passerelle externe.

Vous pouvez configurer les passerelles Prisma Access uniquement en tant que passerelles externes et non en tant que passerelles internes.

1. Dans la section Onboarding (Intégration), cliquez sur **Configure (Configurer)**.
2. Sous l'onglet **General (Général)**, spécifiez le **Portal Name Type (Type de nom de portail)** :
   - **Use Default Domain (Utiliser le domaine par défaut)**—Si vous sélectionnez cette option, le nom d'hôte de votre portail utilise le nom de domaine par défaut : `.gpcloudservice.com`. Dans ce cas, il suffit de saisir un **Portal Hostname (Nom**

 ©2025 Palo Alto Networks, Inc.

d'hôte du portail) à ajouter au nom du domaine par défaut. Prisma Access pour les utilisateurs créera automatiquement les certificats nécessaires et publiera le nom d'hôte sur les serveurs DNS publics.



Si vous avez déjà un déploiement GlobalProtect avec un nom de portail existant et que vous souhaitez continuer à utiliser ce nom de portail, ajoutez une entrée CNAME qui mappe le nom du portail Prisma Access à votre nom de portail existant. Par exemple, si vous avez un portail existant nommé portal.acme.com et que vous souhaitez mapper le nouveau portail Prisma Access à ce même nom, vous ajouteriez un CNAME de gpcs2.gpcloudservice.com à l'entrée DNS de votre portail existant.

*Le domaine *.gpcloudservice.com est associé à l'application Palo Alto Networks.*

- **Use Company Domain (Utiliser le domaine de l'entreprise)**—Sélectionnez cette option si vous souhaitez que le domaine du nom d'hôte du portail corresponde au nom de domaine de votre entreprise (par exemple, myportal.mydomain.com). Si vous

 ©2025 Palo Alto Networks, Inc.

souhaitez utiliser cette option, vous devez d'abord obtenir votre propre certificat et configurer un profil de service SSL/TLS qui pointe vers lui. Ensuite, vous pouvez configurer le nom du portail en sélectionnant le **SSL/TLS Service Profile (Profil de service SSL/TLS)** et en entrant le **Portal Hostname (Nom d'hôte du portail)**. Si vous utilisez cette option, vous devez diriger vos serveurs DNS internes vers le **Portal DNS CNAME (Portail DNS CNAME)**, qui est le nom d'hôte du portail avec le domaine `.gpcloudservice.com` . Par exemple, si vous avez spécifié un nom d'hôte DNS de acme-portal.acme.com, vous devez créer une entrée DNS CNAME qui mappe ce nom d'hôte à acme-portal.gpcloudservice.com sur vos serveurs DNS internes.



*Si vous devez télécharger un nouveau certificat, importez le certificat et la clé privée ; puis, affichez le service SSL/TLS utilisé par Prisma Access sous **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **GlobalProtect_Portal** > **Authentication (Authentification)** et vérifiez le nom **SSL/TLS Service Profile (Profil de service SSL/TLS)**. Ce champ ne s'affiche que si vous utilisez un domaine d'entreprise au lieu du domaine par défaut. Vous pouvez ensuite sélectionner **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Certificate Profile (Profil de certificat SSL/TLS)** et remplacer le certificat dans le profil SSL/TLS utilisé par le portail par le certificat que vous avez importé.*

3. Sélectionnez un **Authentication Profile (Profil d'authentification)** qui précise comment Prisma Access doit authentifier les utilisateurs mobiles ou en créer un nouveau.

   Si vous avez ajouté un groupe de périphériques parent qui contient une configuration de profil d'authentification, vous devriez le voir sur la liste des profils disponibles. Si vous n'avez pas poussé le profil dans le groupe de périphériques, vous pouvez créer un profil d'authentification maintenant.

   *Après avoir validé et poussé vos modifications, vous ne pouvez pas apporter de modifications au profil d'authentification et au certificat de remplacement d'authentification dans ce domaine et les choix deviennent en lecture seule. Pour effectuer des modifications après l'intégration initiale, modifiez ou ajoutez une ou plusieurs configurations d'authentification client sous **Mobile_User_Template**.*

4. Sélectionnez un **Authentication Override Certificate (Certificat de remplacement d'authentification)** pour chiffrer les cookies sécurisés que les utilisateurs mobiles authentifient sur le portail et la passerelle.

   Si vous avez ajouté un groupe de périphériques parent contenant le certificat que vous souhaitez utiliser pour chiffrer les cookies d'authentification, vous devriez le voir sur la liste des certificats disponibles. Si vous n'avez pas poussé de certificat dans le groupe de périphériques, vous pouvez en importer ou en générer un maintenant.

5. (Facultatif) Pour vous assurer que vos utilisateurs mobiles ont toujours accès aux services et applications accessibles à partir des connexions aux services, **Enable Network Redundancy (Activez la redondance réseau)** entre les portails ou passerelles et les connexions aux services.

   Cette fonctionnalité fournit des chemins réseau redondants entre le plan de données des utilisateurs mobiles et les connexions aux services dans différents emplacements de calcul. L'activation de la redondance offre aux utilisateurs un accès plus résilient aux ressources derrière les connexions aux services dans un centre de données ou des

 ©2025 Palo Alto Networks, Inc.

emplacements du siège. Étant donné qu'une connexion aux services est nécessaire pour que les utilisateurs mobiles puissent accéder aux ressources à partir de réseaux distants, les utilisateurs ont également une plus grande résilience pour accéder aux ressources dans des emplacements de réseaux distants.

6. (Facultatif) Si vous n'avez pas besoin que les terminaux GlobalProtect aient des connexions tunnel lorsqu'ils sont sur le réseau interne, activez **Internal Host Detection (Détection d'hôte interne)**.

   1. Sélectionnez la case à cocher **Internal Host Detection (Détection d'hôte interne)**.
   2. Saisissez **IP Address (Adresse IP)** d'un hôte auxquels les utilisateurs ne peuvent accéder que depuis le réseau interne.
   3. Saisissez le **Hostname (Nom d'hôte)** DNS pour l'adresse IP que vous avez saisie. Les clients qui essaient de se connecter effectuent une recherche DNS inversée sur l'adresse spécifiée. Si la recherche échoue, le client détermine qu'il a besoin d'une connexion tunnel à Prisma Access pour les utilisateurs.

   *Prisma Access copie les paramètres de détection d'hôte interne que vous spécifiez ici dans les paramètres par défaut de l'agent dans la configuration du portail GlobalProtect (**Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **<portal-config>** > **Agent** > **DEFAULT (PAR DÉFAUT)** > **Internal (Interne)**). Si vous avez entré les paramètres de détection d'hôte interne pour l'agent par défaut dans le portail GlobalProtect, vous ne pourrez pas modifier les options ici et devez le modifier dans le portail. Si vous avez besoin de plusieurs configurations d'agent, entrez les paramètres de la configuration par défaut de l'agent dans le portail GlobalProtect et utilisez ces paramètres pour Prisma Access, puis sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **<-portal-config>** > **Agent** et **Add (Ajoutez)** une configuration non par défaut, et spécifiez cette configuration dans d'autres parties de votre déploiement.*

7. (Facultatif) Si votre organisation utilise des listes d'autorisation pour contrôler l'accès aux applications publiques ou SaaS, spécifiez si vous **Using IP Allow Lists in SaaS Apps (Utiliser des listes d'autorisation IP dans les applications SaaS)**.

   Pour vous permettre d'ajouter les adresses IP publiques (de sortie) de votre déploiement GlobalProtect—Utilisateur mobile à toute liste d'autorisation d'applications SaaS que vous utilisez au sein de votre entreprise, Prisma Access vous fournit les adresses IP et vous permet de vérifier que vous les avez ajoutées à votre liste d'autorisation avant de les utiliser dans votre environnement. Vous pouvez implémenter les listes d'autorisation pour Prisma Access les adresses IP de sortie pour les déploiements existants et les nouveaux déploiements.

8. (Facultatif) Personnalisez les paramètres de l'application GlobalProtect (par exemple, spécifiez la méthode de connexion utilisée par GlobalProtect) en sélectionnant **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **GlobalProtect_Portal** > **Agent**, en sélectionnant la configuration à personnaliser ou en sélectionnant **DEFAULT (PAR DÉFAUT)**, en sélectionnant **App (Application)**, puis en personnalisant l'application GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

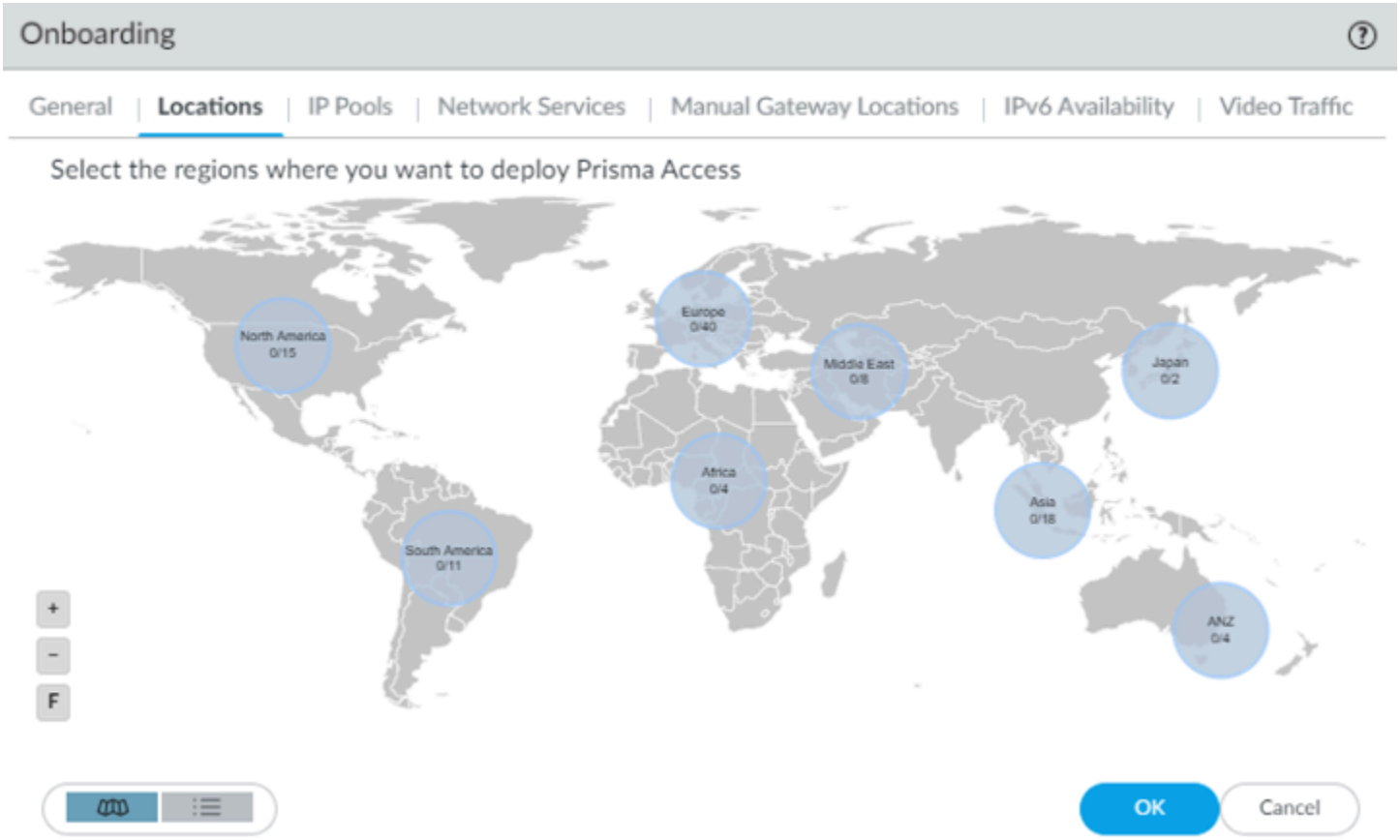
STEP 8 | Sélectionnez les **Locations (Emplacements)** et les régions associés aux emplacements où vous souhaitez déployer vos utilisateurs mobiles.

L'onglet **Locations (Emplacements)** affiche une carte. La mise en surbrillance de la carte affiche les régions du monde (Amériques, Europe et Asie-Pacifique) et les emplacements disponibles dans chaque région. Sélectionnez une région, puis les emplacements que vous souhaitez déployer dans chaque région. Limiter votre déploiement à une seule région offre un contrôle plus granulaire sur les régions déployées et vous permet d'exclure des régions, comme l'exige votre politique ou les réglementations du secteur. Vous pouvez sélectionner un emplacement dans une région qui est la plus proche de vos utilisateurs mobiles, ou sélectionner un emplacement comme l'exige votre politique ou les règlements de l'industrie.

Prisma Access utilise les emplacements Hong Kong, Centre des Pays-Bas et Nord-Ouest des États-Unis comme emplacements de repli pour les utilisateurs mobiles si d'autres emplacements ne sont pas disponibles. Pour cette raison, Palo Alto Networks vous recommande fortement d'activer au moins l'un de ces emplacements lors de l'intégration des utilisateurs mobiles.

Les emplacements notés avec deux astérisques sont des **Local Zones (Zones locales)**. Ces emplacements placent les services de calcul, de stockage, de base de données et d'infrastructure à proximité des grands centres de population et de l'industrie, mais ils ont certaines limites. Pour ajouter une zone locale, contactez votre représentant Palo Alto Networks.

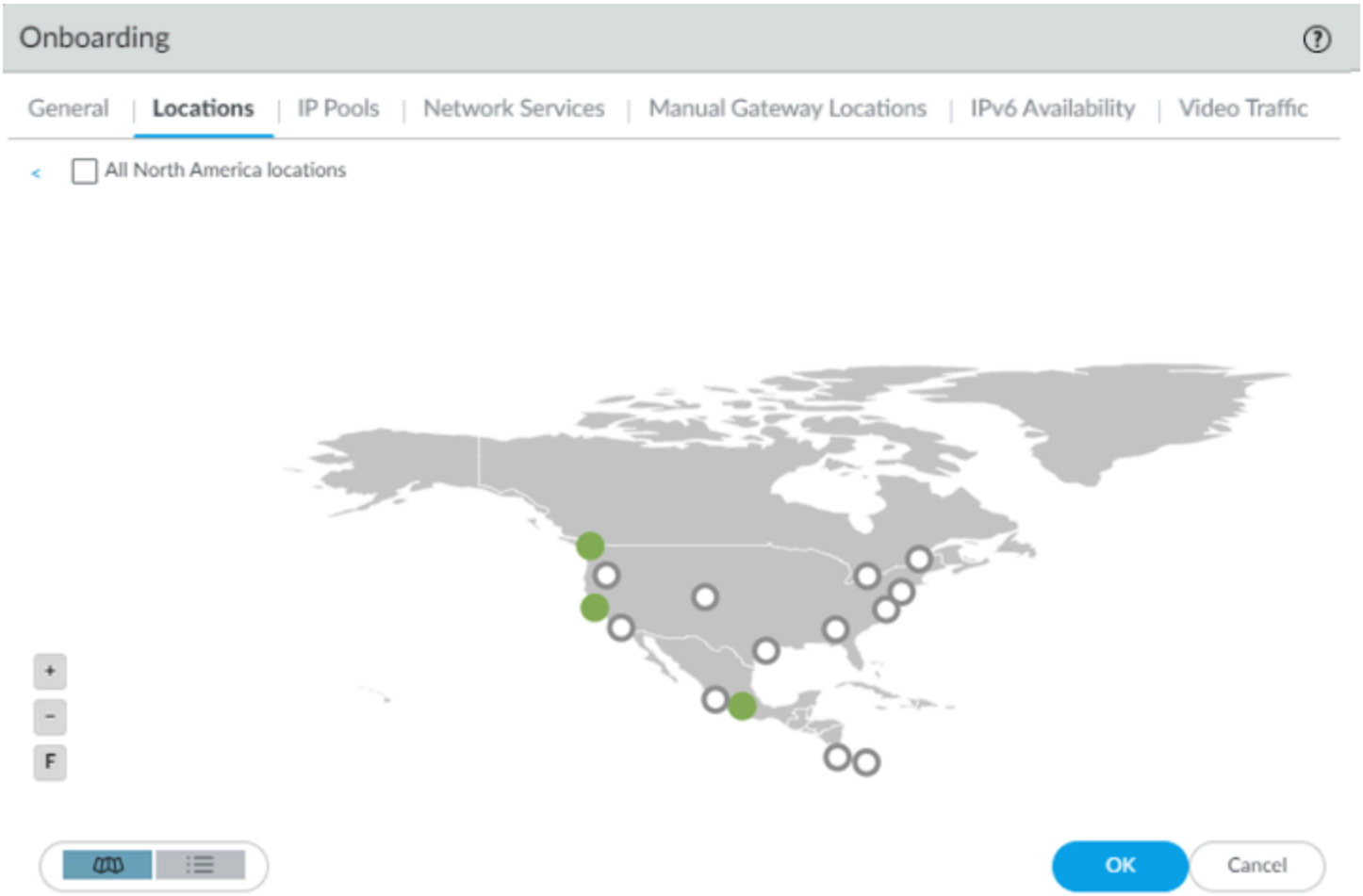
1. Cliquez sur l'onglet **Locations (Emplacements)** et sélectionnez une région.



 ©2025 Palo Alto Networks, Inc.

2. Sélectionnez une ou plusieurs passerelles Prisma Access dans la région sélectionnée à l'aide de la carte.

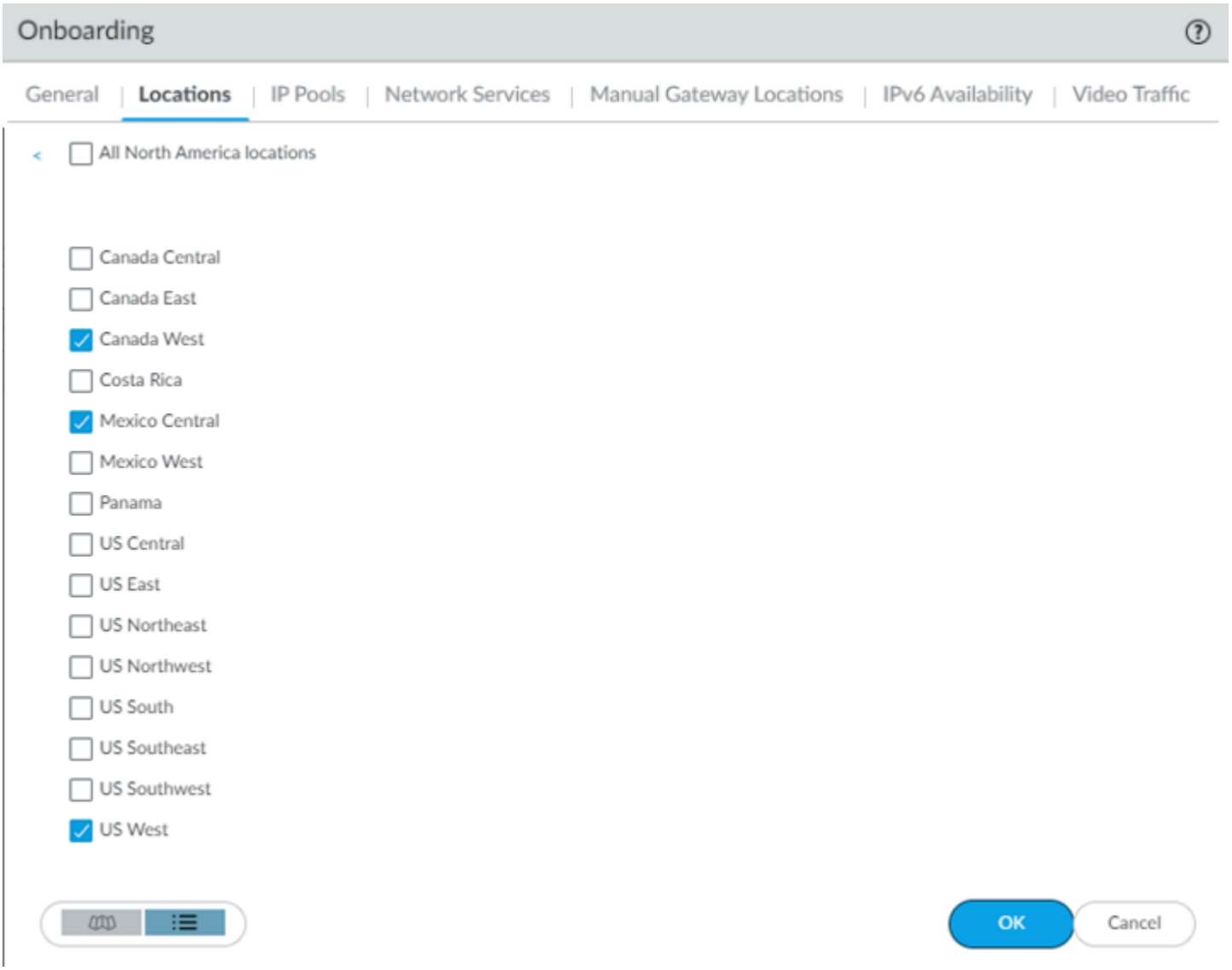
   Passez votre curseur sur un emplacement pour le mettre en surbrillance. Les cercles blancs indiquent un emplacement disponible ; Les cercles verts indiquent que vous avez sélectionné cet emplacement.



   En plus de la vue cartographique, vous pouvez afficher une liste des régions et des emplacements. Choisissez entre la vue carte et la vue liste dans le coin inférieur gauche. Dans la vue liste, la liste affiche les régions triées par colonnes, tous les emplacements

 ©2025 Palo Alto Networks, Inc.

étant triés par région. Vous pouvez sélectionner **All (Tous)** les sites d'une région (en haut de la boîte de dialogue).



STEP 9 | Configurez les pools d'adresses IP utilisés pour attribuer des adresses IP aux terminaux GlobalProtect en sélectionnant l'onglet **IP Pools (Pools IP)** et **Add (Ajouter)** un pool d'adresses IP.

1. Spécifiez une **Region (Région)** pour le pool d'adresses IP.

   Vous pouvez utiliser un pool d'adresses IP unique pour tous les terminaux GlobalProtect dans le monde (**Worldwide (Mondial)**, vous pouvez utiliser des pools distincts pour chaque théâtre où vous avez des utilisateurs mobiles, ou spécifier des pools par groupe d'emplacements (un groupe d'emplacements plus petit que le théâtre). Vous pouvez également spécifier une combinaison de pools d'adresses IP de groupes universels, par théâtre ou par emplacement. Par exemple, vous pouvez ajouter un pool pour un groupe

 ©2025 Palo Alto Networks, Inc.

d'emplacements spécifique, puis ajouter un pool **Worldwide (Mondial)** à utiliser pour tous les autres emplacements.

Utilisez des pools d'adresses IP propres au groupe d'emplacements si vous disposez de services qui dépendent de l'adresse IP source de l'utilisateur pour identifier les détails de ce dernier (tels que les services basés sur l'emplacement ou les services basés sur un groupe d'utilisateurs ou une fonction) afin de pouvoir appliquer des politiques de contrôle d'accès ou d'effectuer des opérations de routage ou de politique dans différents pays si les pays se trouvent dans des régions de calcul différentes. Par exemple, vous pouvez utiliser un pool d'adresses IP distinct pour le Canada et un autre pour le Brésil, qui se trouvent dans des emplacements de calcul différents, afin de fournir des contrôles d'accès et de sécurité distincts.



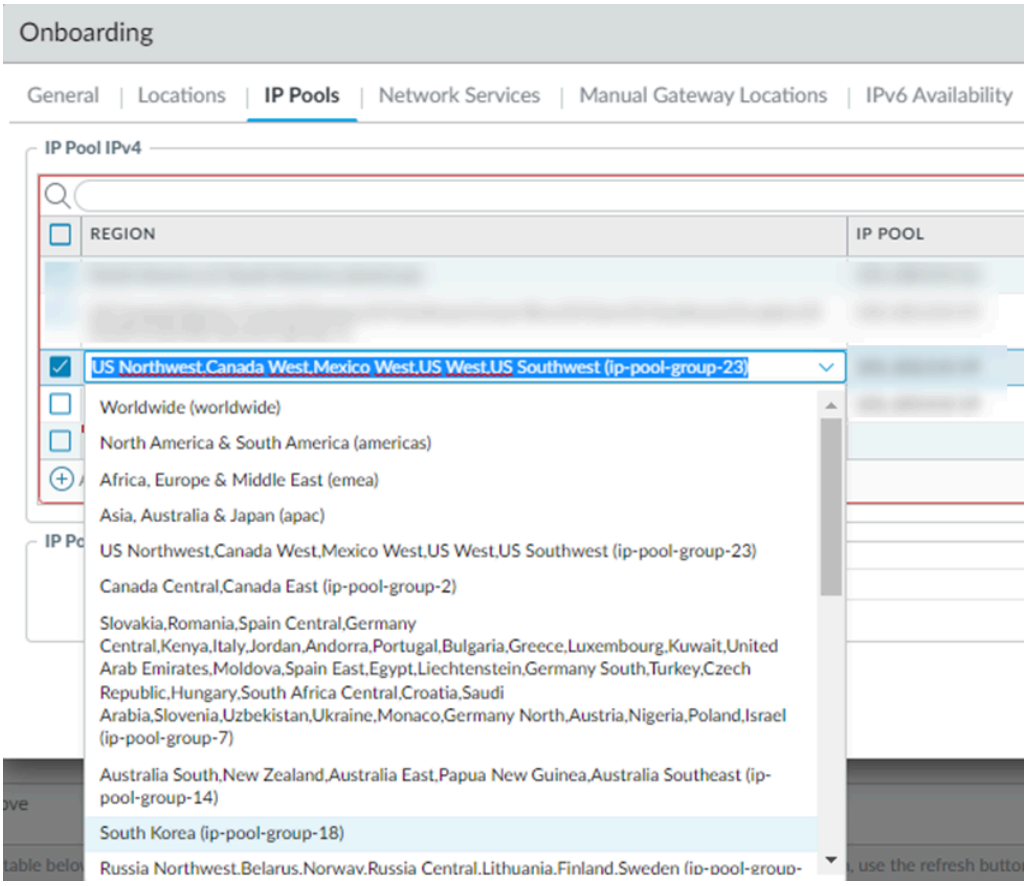
Pour utiliser des pools d'adresses IP spécifiques à un groupe d'emplacements, vous devez également spécifier un pool universel ou spécifique à un théâtre.

Les utilisateurs mobiles GlobalProtect consomment d'abord les adresses IP dans le groupe d'emplacements, puis les adresses IP spécifiques d'un théâtre, puis les adresses IP mondiales. Par exemple, si vous spécifiez un pool pour un groupe d'emplacements et pour le pool mondial, et que vous épuisez ensuite les adresses IP disponibles dans le pool de groupes d'emplacements, Prisma Access prend des adresses IP du pool **Worldwide (Mondial)** pour les utiliser dans ce groupe d'emplacements.

- Pour spécifier les pools IP qui peuvent être utilisés par tous les utilisateurs mobiles GlobalProtect, sélectionnez **Worldwide (Mondial)**.
- Pour spécifier les pools IP qui peuvent être utilisés par les utilisateurs GlobalProtect dans un théâtre spécifique, sélectionnez le théâtre.

 ©2025 Palo Alto Networks, Inc.

- Pour spécifier des pools IP spécifiques au groupe d'emplacements, sélectionnez-le dans la liste.



2. Entrez un **IP Pool (Pool IP)** à affecter aux points de terminaison dans la région que vous avez sélectionnée.

   - Saisissez un sous-réseau minimum requis de /23 (512 adresses IP) par emplacement. Les emplacements supplémentaires nécessitent un sous-réseau minimum de /23. Si vous spécifiez un sous-réseau mondial, le sous-réseau minimum requis est /23, mais nous vous recommandons Pools d'adresses IP pour un déploiement de type Utilisateurs mobiles – GlobalProtect pour attribuer un nombre d'adresses IP égal ou supérieur au nombre d'utilisateurs mobiles sous licence afin qu'ils puissent se connecter en même temps.

     Ne spécifiez pas d'adresses qui chevauchent d'autres réseaux que vous utilisez en interne ou avec les pools que vous avez attribués lorsque vous Configurer l'infrastructure de service Prisma Access (Panorama). En outre, n'utilisez pas les adresses IP et sous-réseaux suivants, car Prisma Access réserve ces adresses IP et sous-réseaux à son usage interne :

     - 169.254.0.0/16

 ©2025 Palo Alto Networks, Inc.

- 100.64.0.0/10

Nous recommandons d'utiliser un pool d'adresses IP conforme à la norme RFC 1918. Bien que les adresses IP (publiques) non conformes à la RFC 1918 soient prises en charge pour les utilisateurs mobiles, évitez de les utiliser à cause d'éventuels conflits avec l'espace des adresses IP publiques d'Internet.

STEP 10 | Pour spécifier les paramètres de résolution DNS pour vos domaines (publics) interne et externe, sélectionnez l'onglet **Network Services (Services réseau)** et **Add (Ajouter)** les paramètres.

Les terminaux GlobalProtect dotés d'une connexion tunnel active utilisent leurs cartes réseau virtuelles plutôt que leurs cartes réseau physiques et nécessitent donc des paramètres de résolution DNS distincts.

Configurez les paramètres réseau dans la fenêtre **Network Services (Services réseau)**.

- Sélectionnez une **Region (Région)** dans la liste déroulante.

  Sélectionnez **Worldwide (Mondial)**, sélectionnez un théâtre ou sélectionnez un groupe d'emplacement pour appliquer les paramètres DNS globalement. Si vous spécifiez plusieurs paramètres proxy avec une combinaison de paramètres spécifiques Mondial, Théâtre et Groupe d'emplacements, Prisma Access utilise les paramètres pour le groupe d'emplacement, puis Théâtre, puis Mondial. Prisma Access évalue les règles de haut en bas dans la liste.
- Cliquez sur **Add (Ajouter)** pour ajouter une ou plusieurs règles pour configurer les paramètres DNS des **Internal Domains (Domaines internes)**.
  - Saisissez un **Rule Name (Nom de règle)** unique pour la règle.
  - Ne saisissez pas une adresse 127.0.0.1 car cela peut causer des problèmes de routage interne Prisma Access.
  - Si vous souhaitez que votre serveur DNS interne résolve uniquement les domaines que vous spécifiez, saisissez les domaines à résoudre dans la **Domain List (Liste de domaines)**. Spécifiez un astérisque devant le domaine ; par exemple, *.acme.com. Vous pouvez spécifier un maximum de 1 024 entrées de domaine.

    *Prisma Access a une règle prédéfinie pour résoudre les domaines *.amazonaws.com, *.aws.amazon.com, *.googleapis.com et *.google.internal en utilisant le serveur Cloud Default. Si vous souhaitez que vos serveurs DNS internes résolvent un domaine plus spécifique (par exemple, *.s3.amazonaws.com au lieu de *.amazonaws.com), entrez l'URL dans la **Domain List (Liste de domaines)**. Prisma Access évalue les noms de domaine du plus long au plus court, puis du haut en bas dans la liste.*
  - Si vous disposez d'un **Custom DNS server (Serveur DNS personnalisé)** capable d'accéder à vos domaines internes, spécifiez les adresses IP du serveur **Primary DNS (DNS principal)** et du serveur **Secondary DNS (DNS secondaire)**, ou sélectionnez **Use Cloud**

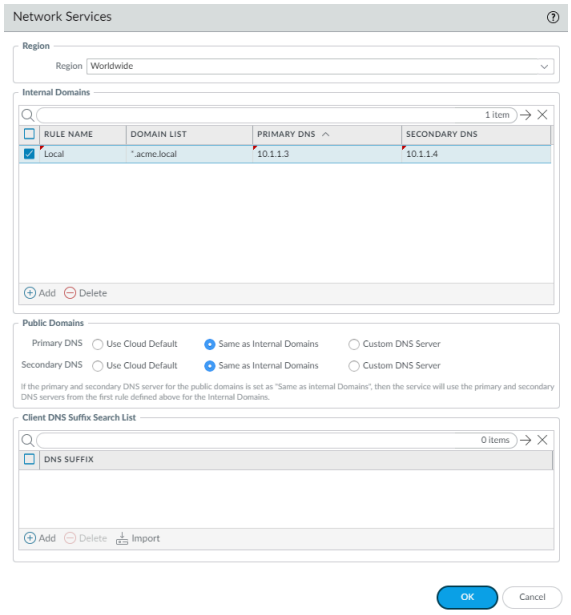
 ©2025 Palo Alto Networks, Inc.

Default (Utiliser la valeur par défaut du cloud) pour utiliser la valeur par défaut du serveur DNS de Prisma Access.

- Spécifiez les paramètres DNS pour les **Public Domains (Domaines publics)**.
  - **Use Cloud Default (Utiliser la valeur par défaut du cloud)** : utilisez la valeur par défaut du serveur DNS de Prisma Access.
  - **Same as Internal Domains (Même valeur que les domaines internes)** : utilisez le même serveur que vous utilisez pour résoudre les domaines internes. Lorsque vous sélectionnez cette option, le serveur DNS utilisé pour résoudre les domaines publics est le même que le serveur configuré pour la première règle dans la section **Internal Domains (Domaines internes)**.
  - **Custom DNS Server (Serveur DNS personnalisé)** : si vous disposez d'un serveur DNS capable d'accéder à vos domaines publics (externes), saisissez l'adresse du serveur DNS principal dans ce champ.

  (Facultatif) Vous pouvez **Add (Ajouter)** un **DNS Suffix (Suffixe DNS)** pour spécifier le suffixe que le client doit utiliser localement lorsqu'un nom d'hôte non qualifié est saisi et qu'il ne peut pas résoudre, par exemple, acme.local. Ne saisissez pas de caractère générique (*) avant le suffixe de domaine (par exemple, acme.com). Vous pouvez ajouter plusieurs suffixes.
- Si vous voulez que Prisma Access utilise un proxy pour les requêtes DNS, configurez les valeurs des requêtes UDP (**Interval (Intervalle)** pour réessayer la requête en quelques secondes et le nombre de nouvelles**Attempts (Tentatives)** à effectuer.

  Pour plus d'informations sur la façon dont Prisma Access utilise un proxy pour les requêtes DNS, consultez Résolution DNS pour utilisateurs mobiles—Déploiements GlobalProtect.

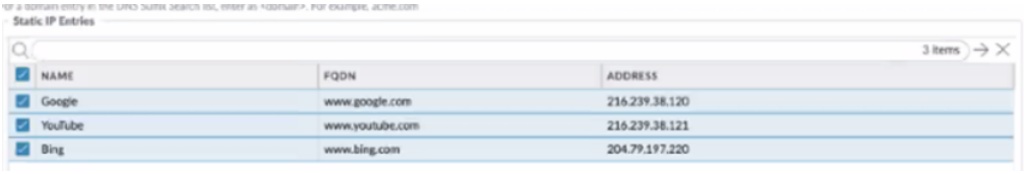


STEP 11 | (Facultatif) Utilisez **Static IP Entries (Entrées IP statiques)** pour résoudre les FQDN en adresses IP spécifiques.

Cette fonctionnalité peut être utile si vous disposez de services Internet pour invités dans votre organisation et que vous souhaitez que vos invités utilisent les moteurs de recherche

 ©2025 Palo Alto Networks, Inc.

en toute sécurité, les empêchant de rechercher du contenu potentiellement inapproprié ou offensant qui pourrait être contraire à la politique de l'entreprise. Pour ce faire, saisissez un **Name (Nom)** unique pour la règle d'entrée statique, un **FQDN** et l'**Address (Adresse)** IP vers laquelle la demande FQDN doit être dirigée.



STEP 12 | (Facultatif) Si votre déploiement utilise Windows Internet Name Service (WINS), vous pouvez spécifier des serveurs WINS pour résoudre le mappage NetBIOS name-to-IP address en sélectionnant **WINS Configuration (Configuration WINS)**, en sélectionnant une région pour le serveur WINS ou en sélectionnant Mondial pour appliquer la configuration WINS dans le monde entier, puis en spécifiant une adresse **Primary WINS (WINS principale)** et, facultativement, une adresse de serveur **Secondary WINS (WINS secondaire)**.

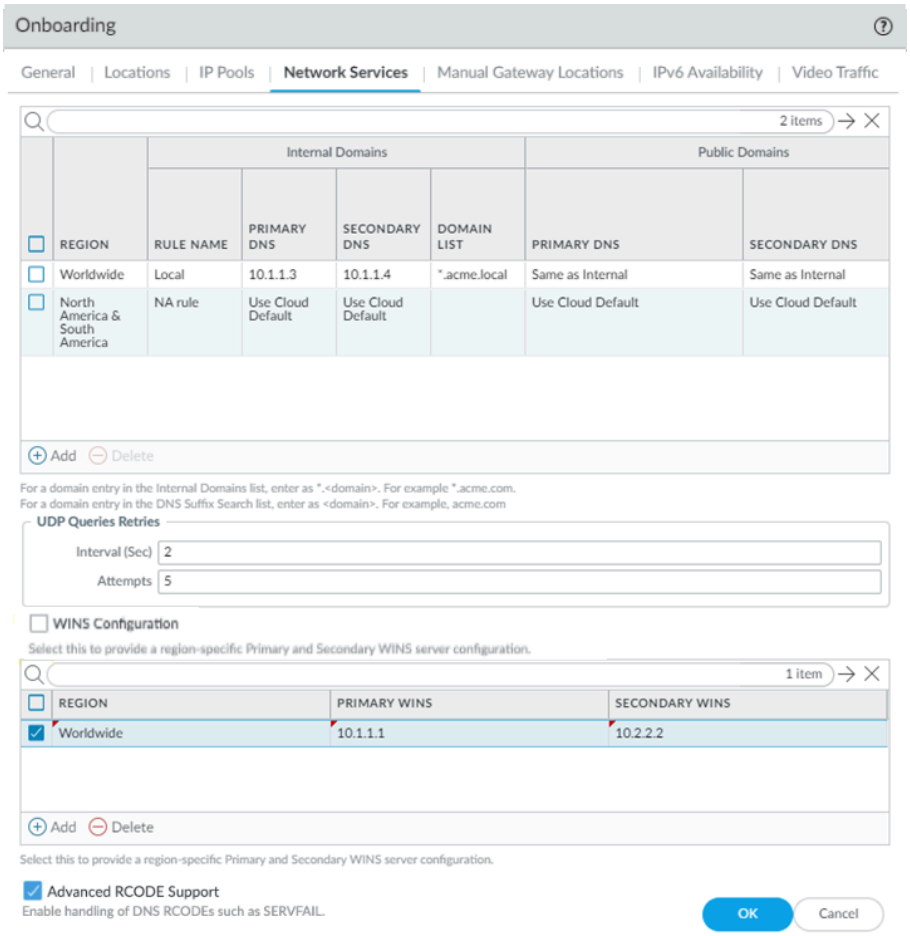
Après avoir activé WINS, Prisma Access peut pousser la configuration WINS vers les terminaux des utilisateurs mobiles via GlobalProtect.

STEP 13 | (Facultatif) Sélectionnez Support RCODE avancé pour autoriser le serveur DNS principal à basculer vers le serveur DNS secondaire en cas de réception d'un code de retour DNS RCODE 2 (SERVFAIL) et RCODE 5 (REFUSED).

Un code de réponse DNS SERVFAIL fait référence à une erreur de communication avec le serveur DNS principal, et un code de réponse DNS REFUSED signifie que le serveur DNS

 ©2025 Palo Alto Networks, Inc.

principal a refusé de fournir les informations demandées. Dans les deux cas, le service bascule vers le serveur DNS secondaire.



STEP 14 | (Facultatif) Si vous autorisez vos utilisateurs mobiles à sélectionner manuellement des passerelles à partir de l'application GlobalProtect, sélectionnez les **Manual Gateway**

 ©2025 Palo Alto Networks, Inc.

Locations (Emplacements de passerelles manuelles) que les utilisateurs peuvent consulter à partir de leur application GlobalProtect.

Le choix d'un sous-ensemble d'emplacements intégrés réduit le nombre de passerelles disponibles que les utilisateurs mobiles peuvent consulter dans leur application GlobalProtect pour la sélection manuelle des passerelles.

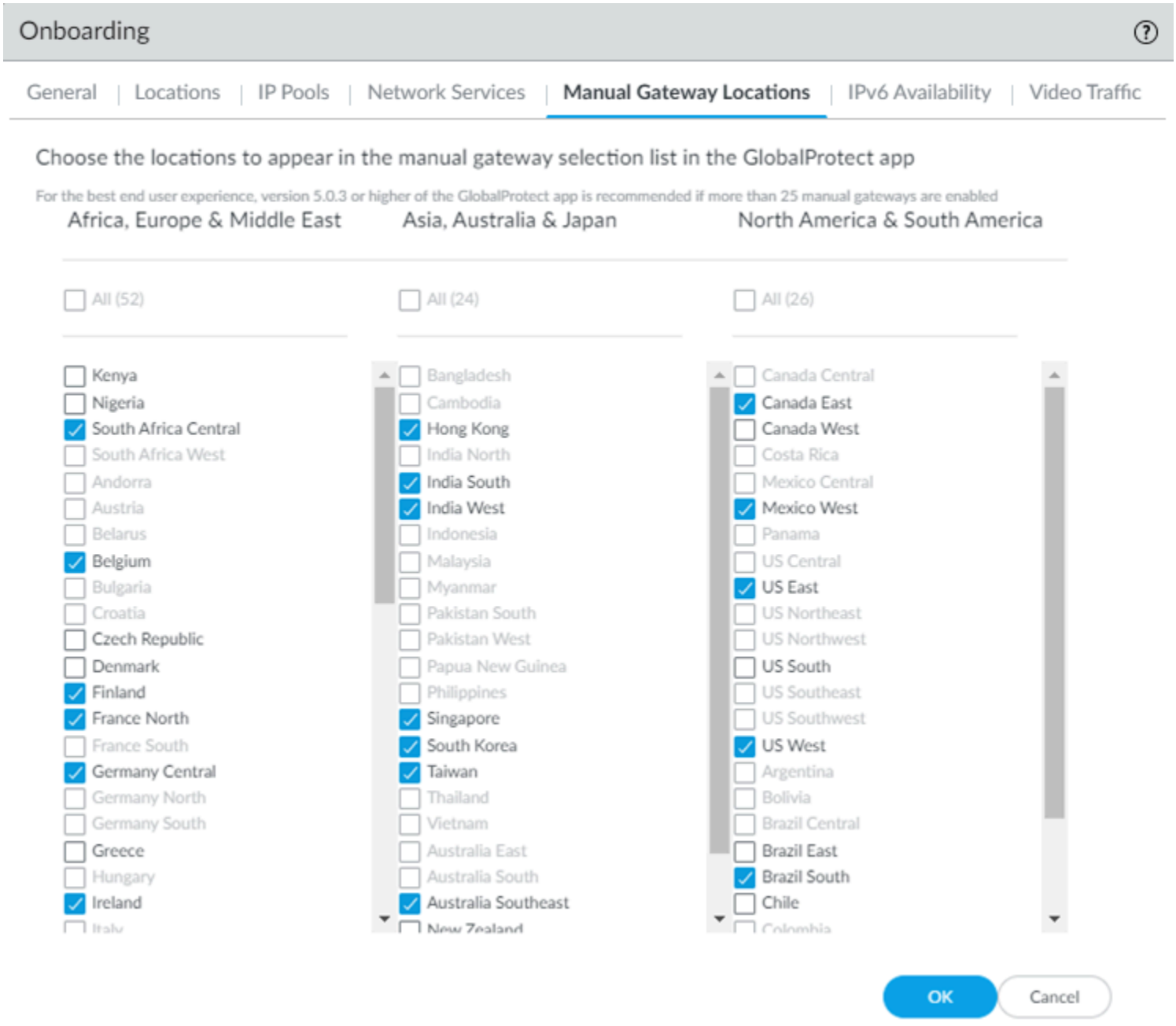
Si vous ne sélectionnez pas de passerelles manuelles dans cet onglet, Prisma Access sélectionne par défaut la liste de passerelles suivante.

- Australie Sud-Est
- Belgique
- Sud du Brésil
- Est du Canada
- Finlande
- Nord de la France
- Allemagne Centre
- Hong Kong
- Ouest de l'Inde
- Irlande
- Israël
- Japon Centre
- Pays-Bas Centre
- Arabie Saoudite
- Singapour
- Afrique du Sud Centre
- Corée du Sud
- Taïwan
- Royaume-Uni
- États-Unis Est
- États-Unis Ouest

Prisma Access vous permet de sélectionner uniquement les passerelles que vous avez intégrées. Par exemple, si vous ne choisissez pas **UK** lorsque vous sélectionnez

 ©2025 Palo Alto Networks, Inc.

des emplacements, vous ne pouvez pas sélectionner **UK** comme passerelle manuelle (l'emplacement est grisé).



*Si vous devez supprimer un emplacement après l'avoir intégré, et qu'il est sélectionné comme l'un des **Manual Gateway Locations (Sélection manuelle des emplacements de passerelle)**, assurez-vous de le désélectionner ici ainsi que dans l'onglet **Locations (Emplacements)**.*

STEP 15 | Cliquez sur **OK** pour enregistrer les paramètres d'intégration.

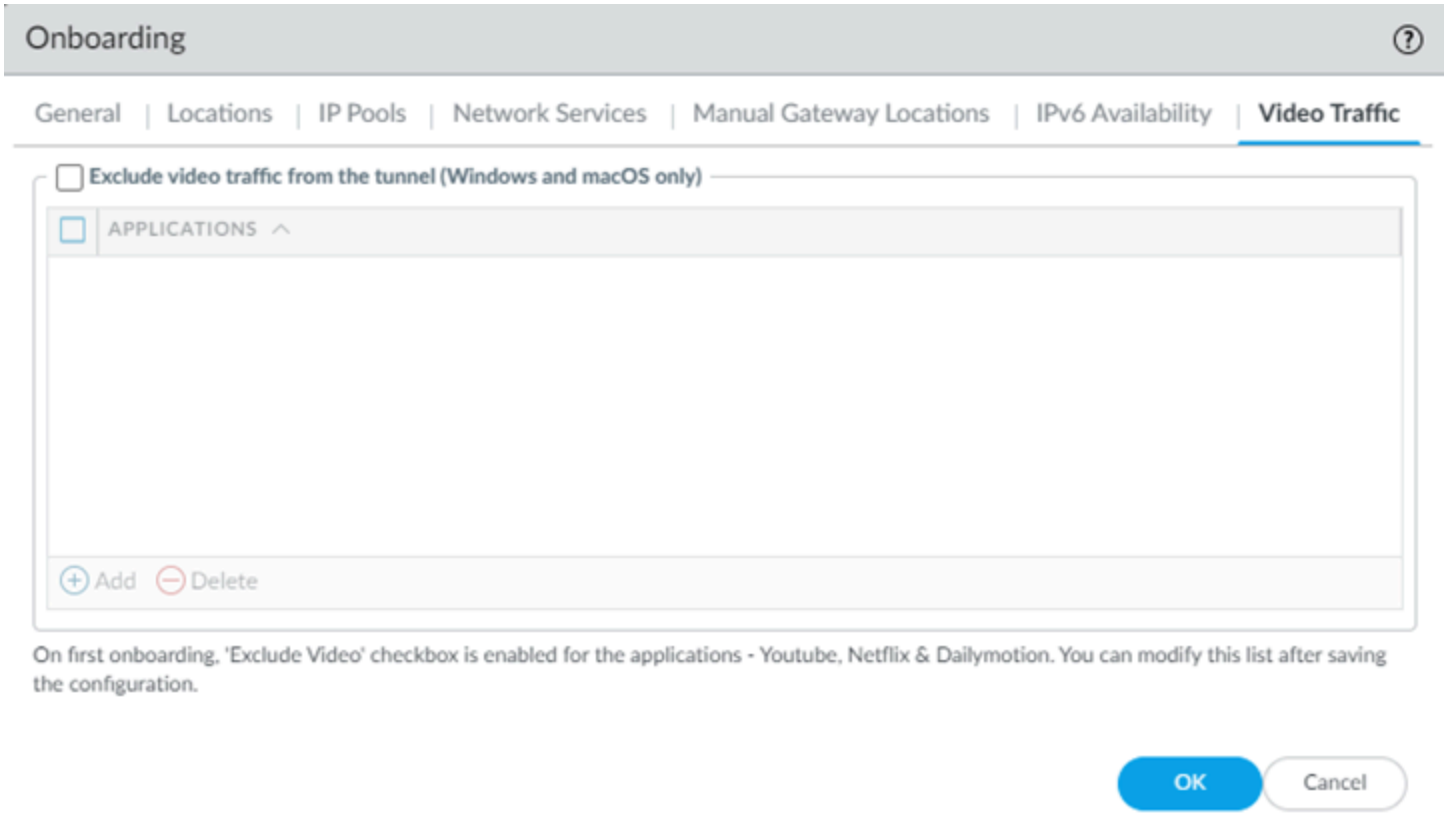
 ©2025 Palo Alto Networks, Inc.

STEP 16 | Configurer les options **IPv6 Availability (Disponibilité IPv6)**.

Si vous utilisez le réseau IPv6 dans votre déploiement Utilisateurs mobiles—GlobalProtect, vous pouvez configurer Prisma Access pour utiliser les adresses IPv6 dans votre réseau utilisateurs mobiles. Vous devez également activer la mise en réseau IPv6 globalement dans votre infrastructure Prisma Access avant de pouvoir utiliser l'adressage IPv6.

STEP 17 | (Facultatif, Windows et macOS uniquement) Exclure le trafic vidéo du tunnel GlobalProtect.

Exclude video traffic from the tunnel (Exclure le trafic vidéo du tunnel) ; puis, **Add (Ajouter)** ou **Delete (Supprimer)** des applications de streaming vidéo que vous souhaitez exclure du tunnel GlobalProtect.



STEP 18 | Créez des règles de stratégie de sécurité pour sécuriser le trafic de vos utilisateurs mobiles.

1. Sélectionnez le **Device Group (Groupe de périphériques)** dans lequel ajouter des règles de stratégie. Vous pouvez sélectionner le groupe Mobile_User_Device_Group ou le groupe de périphériques parent que vous avez sélectionné lors de la configuration de Prisma Access pour les utilisateurs mobiles.
2. Créez des règles de politique de sécurité. Assurez-vous de ne pas définir de règles de politique de sécurité autorisant le trafic de n'importe quelle zone à n'importe quelle zone. Dans les règles de stratégie de sécurité, utilisez les zones que vous avez définies dans la pile de modèles.

 ©2025 Palo Alto Networks, Inc.

STEP 19 | Configurer les journaux à transférer à Strata Logging Service.

Le plugin Cloud Services ajoute automatiquement les paramètres de journalisation suivants (**Device (Périphérique)** > **Log Settings (Paramètres journaux)**) après une nouvelle installation ou lors de la suppression de modèles non Prisma Access d'une pile de modèles Prisma Access :

- Les paramètres des journaux pour les journaux Système (**system-gpcs-default**), User-ID (**userid-gpcs-default**), HIP Match (**hipmatch-gpcs-default**) et GlobalProtect (**gp-prismaaccess-default**) sont ajoutés au modèle Mobile_User_Template.
- Les paramètres des journaux pour les journaux Système (**system-gpcs-default**), User-ID (**userid-gpcs-default**) et GlobalProtect (**gp-prismaaccess-default**) sont ajoutés au Remote_Network_Template.
- Les paramètres des journaux pour les journaux Système (**system-gpcs-default**) et GlobalProtect (**gp-prismaaccess-default**) sont ajoutés au Modèle Service_Conn_Template.

Ces configurations de paramètres de journaux redirigent automatiquement les journaux Système, User-ID et HIP Match vers les Strata Logging Service.

STEP 20 | (Facultatif) Transférer les journaux vers d'autres types de journaux à Strata Logging Service.

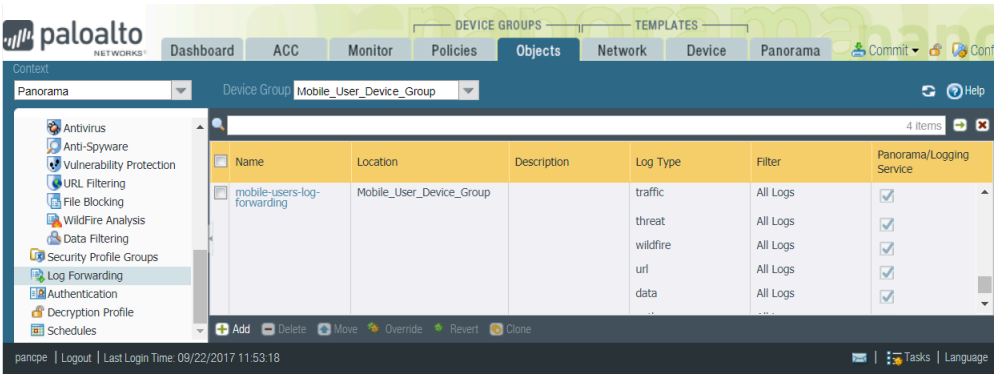
Pour transférer ces journaux, vous devez créer et attacher un profil de transfert de journal à chaque règle de stratégie pour laquelle vous souhaitez transférer les journaux.

1. Sélectionnez le **Device Group (Groupe de périphériques)** dans lequel vous avez ajouté les règles de stratégie.
2. Sélectionnez **Objects (Objets)** > **Log Forwarding (Transfert des journaux)** et **Add (Ajoutez)** un profil. Dans la liste de correspondance du profil de transfert de journaux, **Add (Ajouter)** chaque type de journal que vous souhaitez transférer.

   L'exemple suivant permet le transfert des journaux de trafic, de prévention des menaces, d'envois WildFire, de filtrage des URL, de filtrage des données et des journaux d'authentification.
3. Sélectionnez **Panorama/Strata Logging Service (Service de journalisation Panorama/Strata)** comme méthode de transfert. Lorsque vous sélectionnez Panorama, les journaux sont transmis à Strata Logging Service. Vous pourrez surveiller les journaux et générer des rapports depuis Panorama. Strata Logging Service offre une intégration transparente

 ©2025 Palo Alto Networks, Inc.

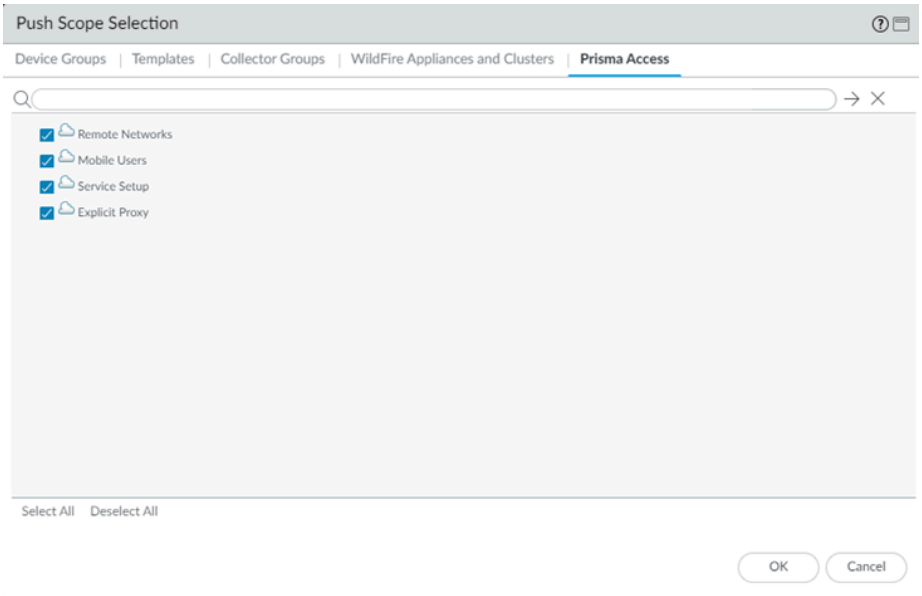
pour stocker les journaux sans les renvoyer à votre Panorama au siège social, et Panorama peut interroger Strata Logging Service selon le besoin.



4. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis modifiez la règle de politique. Dans **Actions (Actions)**, sélectionnez le profil de transfert des journaux que vous avez créé.

STEP 21 | Validez toutes les modifications dans Panorama et appliquez les modifications de configuration sur Prisma Access.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**.
2. **Edit Selections (Modifier les sélections)** et, dans l'onglet **Prisma Access**, assurez-vous que **Mobile Users (Utilisateurs mobiles)** et **Explicit Proxy (Proxy explicite)** sont sélectionnés dans **Push Scope (Étendue de la transmission)**, puis cliquez sur **OK**.



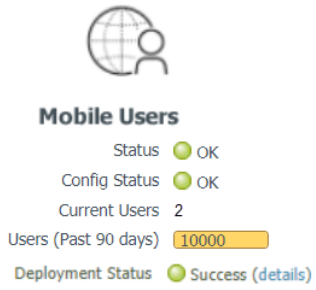
3. Dans l'onglet **Device Groups (Groupes de périphériques)**, assurez-vous d'avoir sélectionné les groupes de périphériques **Explicit Proxy (Proxy explicite)** et **GlobalProtect**.
4. Cliquez sur **Commit and Push (Valider et appliquer)**.

 ©2025 Palo Alto Networks, Inc.

STEP 22 | Pour vérifier que Prisma Access pour les utilisateurs est déployé et actif, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Status (État)**.

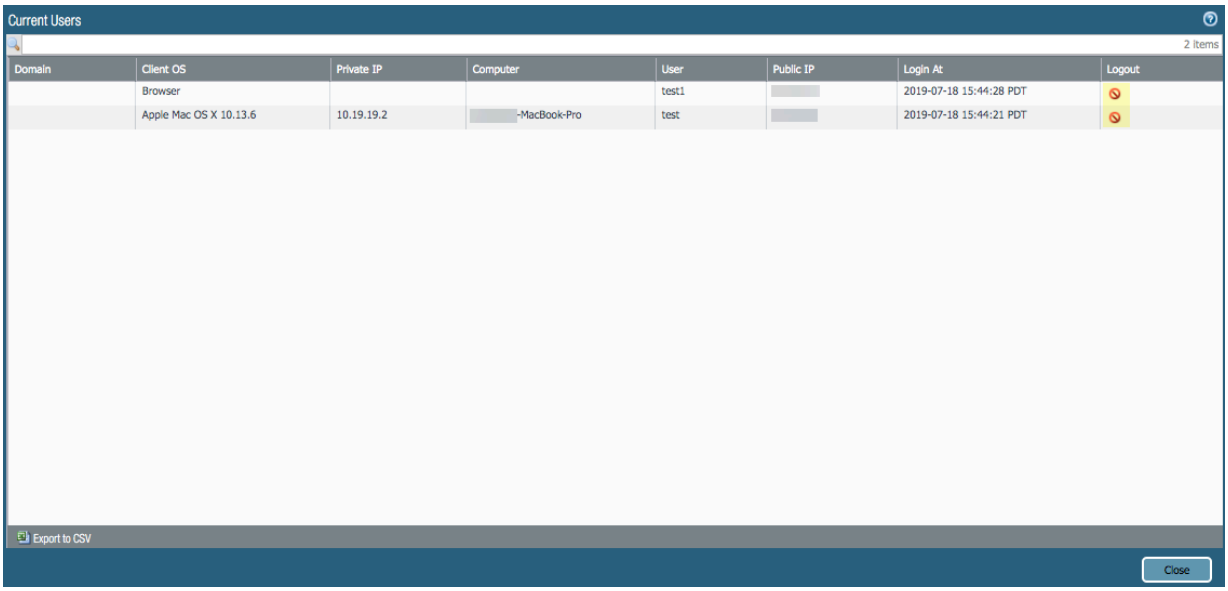
Une fois le provisionnement terminé, le **Status (État)** et le **Config Status (Statut de la configuration)** des utilisateurs mobiles doivent afficher **OK**.

La zone **Deployment Status (État du déploiement)** vous permet d'afficher la progression des tâches d'intégration et de déploiement avant qu'elles ne soient terminées, ainsi que de voir plus d'informations sur l'état des tâches terminées.



Pour afficher le nombre d'utilisateurs uniques qui sont actuellement connectés, ou pour déconnecter un utilisateur connecté, cliquez sur le numéro hypertexte en regard de **Current Users (Utilisateurs actuels)**.

 ©2025 Palo Alto Networks, Inc.

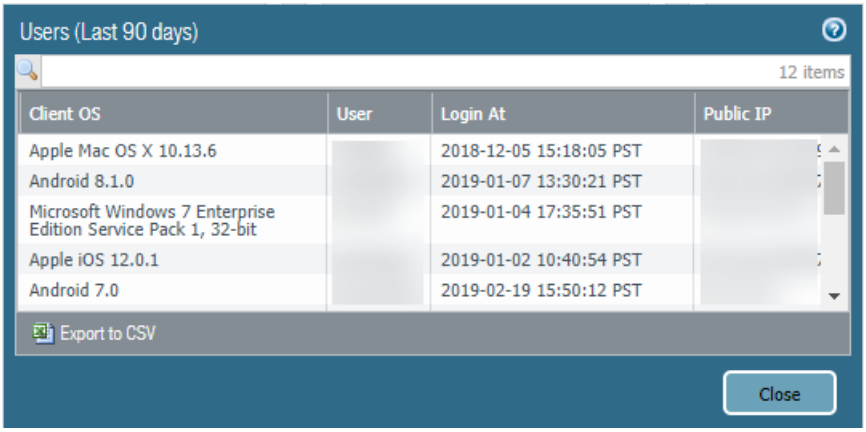


Pour afficher les informations historiques des utilisateurs déjà connectés pour une période de 90 jours, cliquez sur le numéro en regard de **Users (Last 90 days) (Utilisateurs (90 derniers jours))**.

Lorsque le nombre d'utilisateurs dans le champ Utilisateurs (90 derniers jours) atteint 80 % du nombre total de licences, le nombre s'affiche dans une couleur rouge.

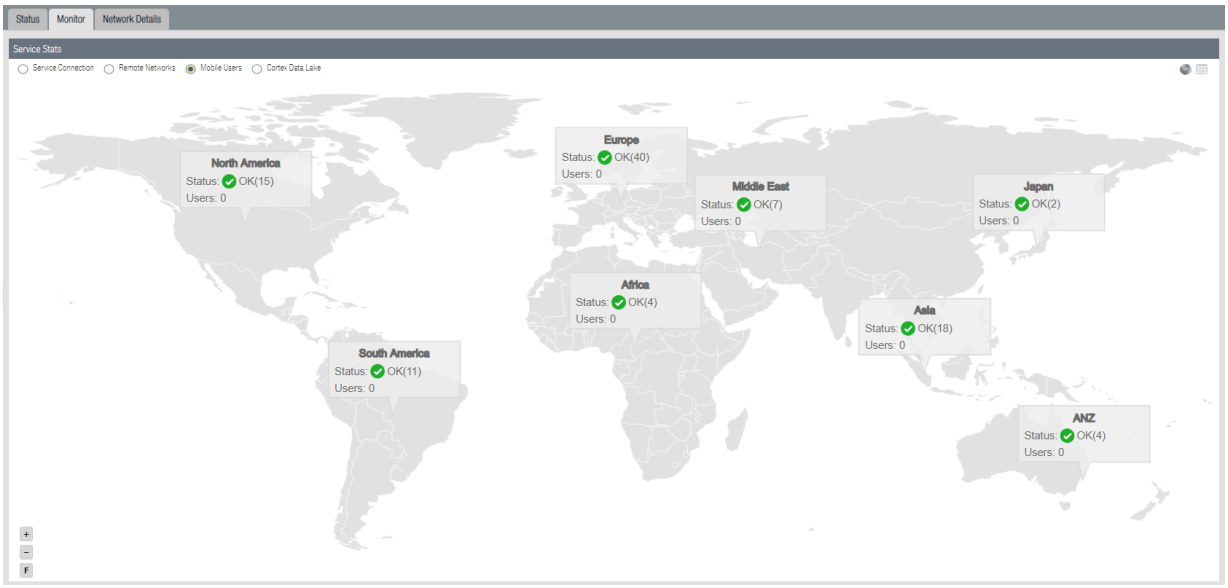
Pour exporter la liste des utilisateurs vers un fichier CSV, sélectionnez **Export to CSV (Exporter vers CSV)**. Notez qu'un maximum de 45 000 utilisateurs peuvent être exportés vers un fichier CSV.

 ©2025 Palo Alto Networks, Inc.



Pour afficher une carte indiquant l'emplacement des portails et passerelles Prisma Access exécutés dans les régions que vous avez sélectionnées, sélectionnez **Monitor (Surveiller)**, puis **Mobile Users (Utilisateurs mobiles)**.

 ©2025 Palo Alto Networks, Inc.



Sélectionnez une région pour obtenir plus de détails sur cette région.

- **Location (Emplacement)**—L'emplacement où votre infrastructure de services cloud est déployée pour sécuriser les utilisateurs mobiles sur votre réseau.

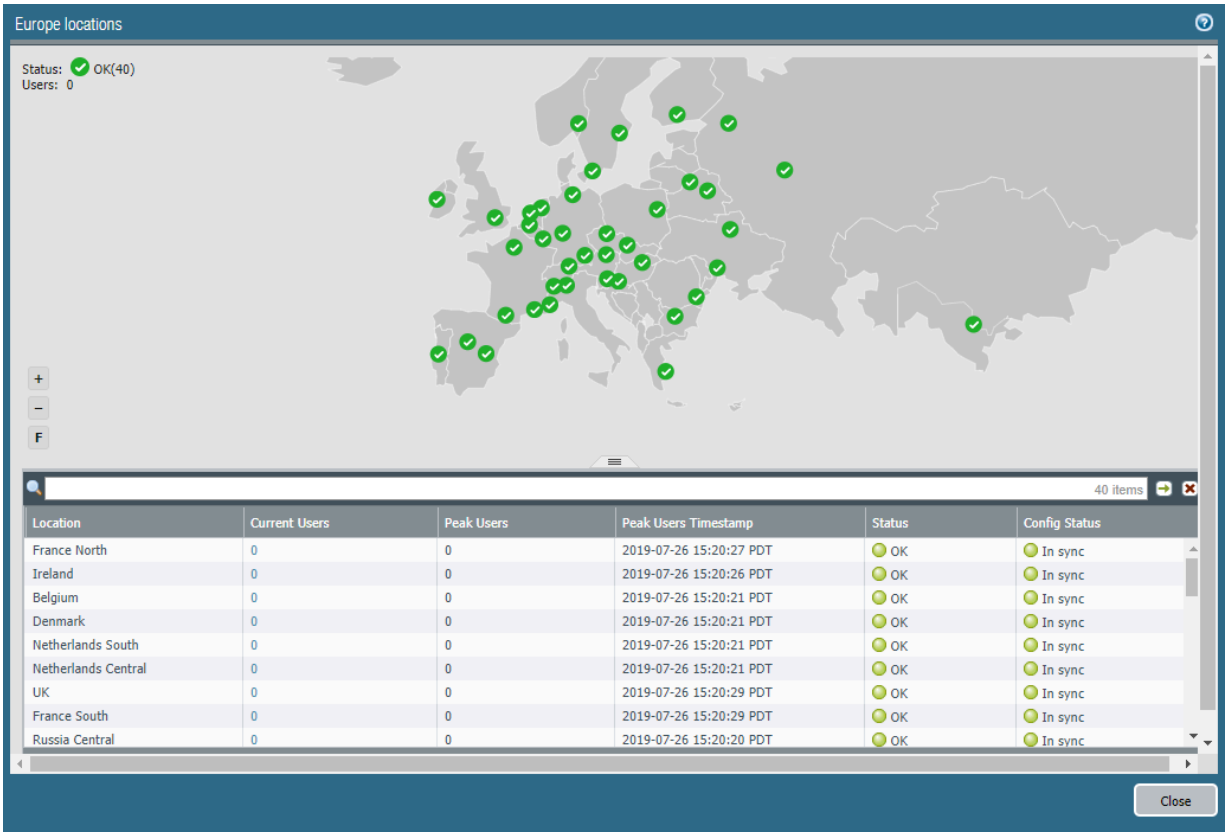
 ©2025 Palo Alto Networks, Inc.

- **Current Users (Utilisateurs actuels)**—Nombre d'utilisateurs connectés et sécurisés par le service.

  Lorsque le nombre actuel d'utilisateurs mobiles atteint 80 % de son nombre total de licences, ce nombre s'affiche en rouge.
- **Peak Users (Pic des utilisateurs)**—Le nombre maximal d'utilisateurs simultanés.
- **Peak Users Timestamp (Horodatage du pic des utilisateurs)**—Horodatage lors de la dernière récupération des données de pic des utilisateurs.
- **Status (État)**—État opérationnel de la connexion entre Prisma Access et vos utilisateurs mobiles.
- **Config Status (État de la configuration)**—État de votre dernière transmission de configuration au service. Si vous avez effectué une modification localement et que vous n'avez pas encore appliqué la configuration au cloud, l'état peut être affiché comme **Out of sync (Désynchronisé)**. Passez la souris sur l'indicateur d'état pour obtenir des informations

 ©2025 Palo Alto Networks, Inc.

plus détaillées. Après avoir validé et transmis la configuration vers Prisma Access, l'état de configuration passe à **In sync (Synchronisé)**.



STEP 23 | Si vous avez choisi **Use Company Domain (Utiliser le domaine de l'entreprise)** pour votre nom d'hôte de portail, vous devez ajouter une entrée DNS sur vos serveurs DNS internes pour cartographier le nom d'hôte du portail que vous avez défini sur le portail DNS CNAME affiché sur l'onglet **Cloud Services** > **Configuration** > **Mobile Users (Utilisateurs mobiles)** > **Onboarding (Intégration)** > **General (Général)** (par exemple, `<portal_hostname>.gpcloudservice.com`).

 ©2025 Palo Alto Networks, Inc.

STEP 24 | Déployez le logiciel Application GlobalProtect pour vos utilisateurs finaux.

Pour les utilisateurs Mac OS ou Windows, vous pouvez diriger les utilisateurs vers l'adresse du portail Prisma Access, où ils peuvent télécharger l'application GlobalProtect à partir du portail.

Prisma Access gère la version de l'application GlobalProtect sur le portail et vous pouvez sélectionner la version active parmi les versions hébergées par Prisma Access, ainsi que contrôler la capacité des utilisateurs à la télécharger.

Alternativement, vous pouvez héberger le logiciel de l'application GlobalProtect sur un serveur Web pour vos utilisateurs Mac OS et Windows. Prisma Access est compatible avec toutes les versions de l'application GlobalProtect qui ne sont pas répertoriées comme en fin de vie.

Les utilisateurs d'applications mobiles peuvent télécharger et installer l'application mobile GlobalProtect à partir de la boutique d'applications appropriée pour leurs systèmes d'exploitation.

GlobalProtect – Personnaliser les paramètres de tunnel

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Personnalisez les paramètres du tunnel VPN que l'application GlobalProtect établit pour se connecter à Prisma Access. Les paramètres du tunnel incluent des options de segmentation de tunnel que vous pouvez utiliser pour définir le trafic que l'application envoie vers Prisma Access et ce qui peut être acheminé localement à la place (comme les applications gourmandes en bande passante qui ne sont pas nécessaires à une utilisation professionnelle).

Les **Match Criteria (Critères de correspondance)** que vous définissez pour les paramètres du tunnel indiquent à Prisma Access les utilisateurs, les périphériques ou les systèmes qui doivent recevoir les paramètres. Par exemple, vous pouvez spécifier qu'une règle de paramètres de tunnel s'applique à toutes les instances de l'application GlobalProtect dans une certaine région. Dans Prisma Access (Managed by Panorama), vous pouvez configurer les paramètres de segmentation de tunnel en fonction de l'itinéraire d'accès, du domaine et de l'application.

- Strata Cloud Manager
- Panorama

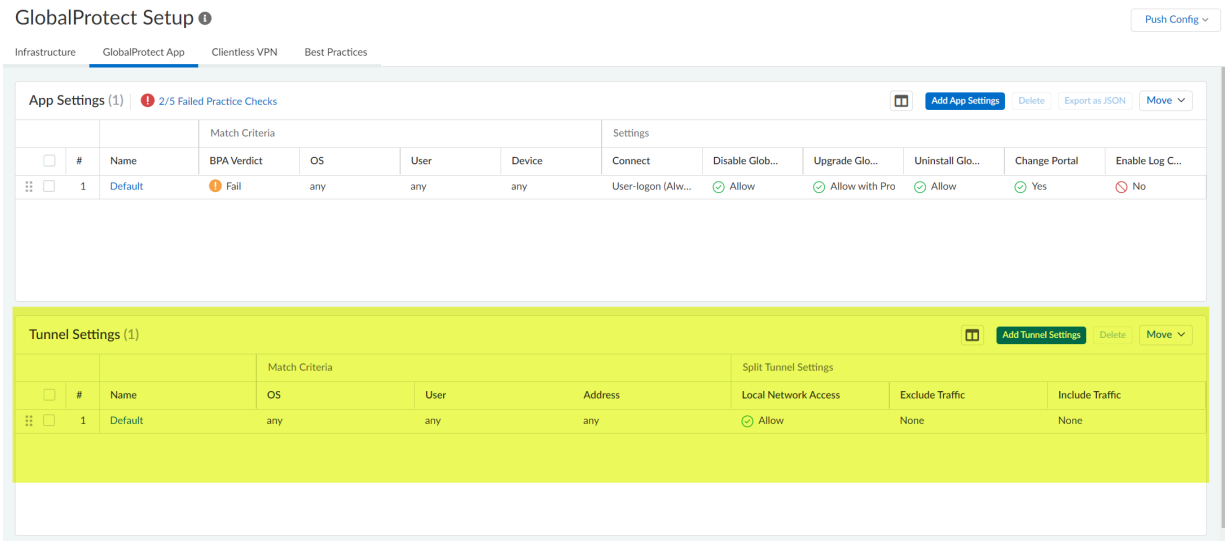
GlobalProtect – Personnaliser les paramètres de tunnel (Strata Cloud Manager)

STEP 1 | Cliquez sur **Manage > Service Setup > Mobile Users > GlobalProtect Setup > GlobalProtect App > Add Tunnel Settings (Gérer > Configuration de service > Utilisateurs mobiles >**

 ©2025 Palo Alto Networks, Inc.

Configuration de GlobalProtect > Application GlobalProtect > Ajouter des paramètres de tunnel).

*Si vous utilisez Strata Cloud Manager, cliquez sur **Workflow > Prisma Access Setup > Mobile User > GlobalProtect Setup > GlobalProtect App > Add Tunnel Settings (Flux de travail > Configuration de Prisma Access > Utilisateur mobile > Configuration de GlobalProtect > Application GlobalProtect > Ajouter des paramètres de tunnel).***



STEP 2 | Saisissez un nom et les **Match Criteria (Critères de correspondance)** pour spécifier les utilisateurs, les périphériques ou les systèmes qui doivent recevoir les paramètres. Par exemple, vous pouvez spécifier qu'une règle de paramètres de tunnel s'applique à toutes les instances de l'application GlobalProtect dans une certaine région.

STEP 3 | Activez **Authentication Override (Contournement de l'authentification)** pour Prisma Access pour générer et accepter des cookies sécurisés et cryptés pour l'authentification de l'utilisateur. Ce paramètre permet à l'utilisateur de ne fournir ses identifiants de connexion qu'une seule fois au cours de la période spécifiée.

- **Generate cookie for authentication override (Générer un cookie pour remplacer l'authentification)** : permet à Prisma Access de générer des cookies cryptés spécifiques au terminal et d'émettre les cookies d'authentification au terminal.
- **Accept cookie for authentication override (Accepter un cookie pour remplacer l'authentification)** : permet à Prisma Access d'authentifier les utilisateurs au moyen d'un cookie crypté qui est valide. Lorsque l'application présente un cookie valide, Prisma Access

 ©2025 Palo Alto Networks, Inc.

vérifie que le cookie a été crypté par Prisma Access à l'origine, décrypte le cookie, puis authentifie l'utilisateur.

L'application GlobalProtect doit connaître le nom d'utilisateur de l'utilisateur qui se connecte pour faire correspondre et récupérer les cookies d'authentification associés à partir du terminal de l'utilisateur. Une fois que l'application a récupéré les cookies, elle les envoie à Prisma Access à des fins d'authentification de l'utilisateur.

STEP 4 | Activez la **Split Tunneling (Segmentation de tunnel)** pour définir le trafic que l'application GlobalProtect autorise ou restreint via le tunnel VPN vers Prisma Access. La segmentation de tunnel permet d'économiser la bande passante en excluant le trafic Prisma Access qui n'est pas critique pour l'entreprise ou qui n'améliore pas la productivité.

- **Local Network Access (Accès au réseau local)** : accordez aux utilisateurs Windows et Mac l'accès aux ressources locales, sans qu'ils aient à se connecter au préalable à Prisma Access.

  Exclude Traffic (Exclure le trafic) : spécifiez le trafic à exclure de l'inspection et l'application des politiques Prisma Access en fonction de l'application, du domaine et de l'itinéraire (par exemple, une adresse IP).

  Customize Include Traffic (Personnaliser Inclure le trafic) : par défaut, l'application GlobalProtect achemine tout le trafic vers Prisma Access, à l'exception de ce qui est indiqué dans la liste d'exclusion. Précisez le trafic que l'application GlobalProtect doit toujours acheminer vers Prisma Access, même lorsqu'il correspond aux critères de la liste d'exclusion.

STEP 5 | **Exclude Video Stream Traffic (Excluez le trafic de diffusion vidéo)** pour ne pas envoyer le trafic de diffusion vidéo des applications répertoriées vers Prisma Access. En excluant la diffusion vidéo à faible risque (comme YouTube et Netflix) du tunnel VPN, vous pouvez diminuer la consommation de bande passante. Les exclusions de diffusion vidéo sont appliquées à tout le trafic que l'application GlobalProtect envoie à Prisma Access, et pas seulement aux critères de correspondance que vous avez définis pour cette règle.

STEP 6 | Enregistrez les paramètres. Répétez les étapes ci-dessus pour ajouter d'autres paramètres de tunnel.

STEP 7 | (Facultatif) **Move (Déplacez)** pour définir l'ordre de priorité dans lequel le paramètre de tunnel VPN sont utilisés lors de la connexion à Prisma Access.

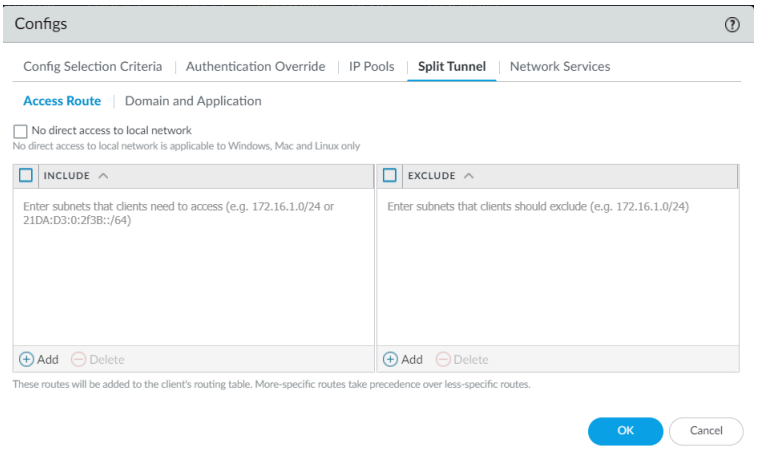
GlobalProtect – Personnaliser les paramètres de tunnel (Panorama)

Vous pouvez configurer les paramètres de segmentation de tunnel en fonction de l'itinéraire d'accès ou du domaine et de l'application.

- Configurez les paramètres de segmentation de tunnel en fonction de l'itinéraire d'accès.
  1. Cliquez sur **Panorama > Network > GlobalProtect > Gateways (Panorama > Réseau > GlobalProtect > Passerelles)** et sélectionnez la passerelle que vous souhaitez personnaliser.
  2. Cliquez sur **Agent > Client Settings (Agent > Paramètres du client)** et sélectionnez la configuration.
  3. Cliquez sur **Split Tunnel > Access Route (Segmentation de tunnel > Itinéraire d'accès)**. Ces paramètres sont assignés à la carte réseau virtuel des terminaux lorsque

 ©2025 Palo Alto Networks, Inc.

l'application GlobalProtect établit un tunnel avec Prisma Access. Vous pouvez inclure ou exclure un trafic du sous-réseau IP de destination spécifique de l'envoi par le tunnel VPN.



4. Activez l'option **No direct access to local network (Pas d'accès direct au réseau local)** pour empêcher les utilisateurs d'envoyer du trafic directement à des proxys ou à des ressources locales lorsqu'ils sont connectés à GlobalProtect.

   *Activez le paramètre **No direct access to local network (Aucun accès direct au réseau local)** pour réduire les risques dans les réseaux non approuvés tels que les points d'accès Wi-Fi malveillants.*

5. Sélectionnez **Include (Inclure)** et **Add (Ajoutez)** les sous-réseaux de destination ou l'objet d'adresse (de type Masque de réseau IP) pour acheminer uniquement certains trafics destinés à votre LAN vers GlobalProtect. Vous pouvez inclure des sous-réseaux IPv6 ou IPv4. Pour inclure tous les sous-réseaux de destination ou les objets d'adresses, **Incluez** 0.0.0.0/0 et ::/0 comme itinéraires d'accès.
6. Sélectionnez **Exclude (Exclure)**, **Add (Ajoutez)** les sous-réseaux de destination ou l'objet d'adresse (de type Masque de réseau IP) que vous souhaitez que l'application exclut. Les itinéraires exclus doivent être plus spécifiques que les itinéraires inclus. Sinon, vous risqueriez d'exclure plus de trafic que prévu. Vous pouvez exclure les sous-réseaux IPv6 ou IPv4.

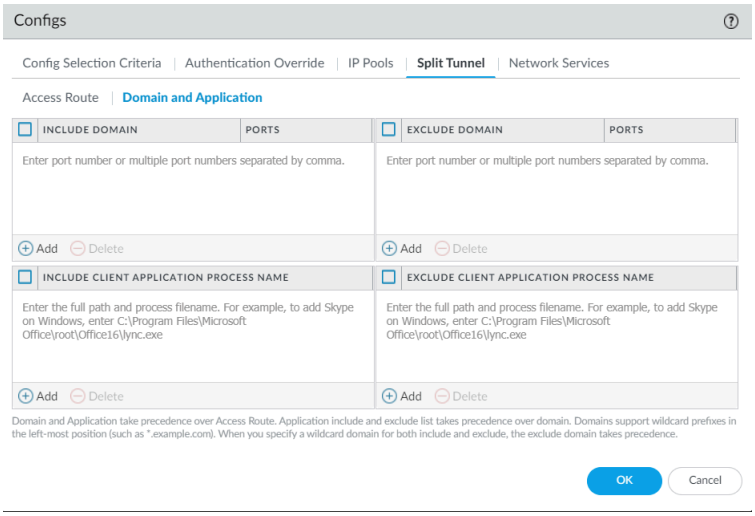
   Vous ne pouvez pas exclure les itinéraires d'accès pour les terminaux exécutant Android sur les Chromebooks. Seuls les itinéraires IPv4 sont pris en charge sur les Chromebooks.

7. Enregistrez les paramètres du tunnel.

 ©2025 Palo Alto Networks, Inc.

- Configurez les paramètres de segmentation de tunnel en fonction du domaine et de l'application.
  1. Cliquez sur **Panorama > Network > GlobalProtect > Gateways (Panorama > Réseau > GlobalProtect > Passerelles)** et sélectionnez la passerelle que vous souhaitez personnaliser.
  2. Cliquez sur **Agent > Client Settings (Agent > Paramètres du client)** et sélectionnez la configuration.
  3. Cliquez sur **Split Tunnel > Domain and Application (Segmentation de tunnel > Domaine et application)** pour configurer les paramètres de segmentation de tunnel en fonction du domaine de destination.

     Vous pouvez rencontrer des problèmes d'incompatibilité lors de l'utilisation d'un produit de sécurité de terminal tiers tel que Sophos sur les terminaux macOS.



  - (Facultatif) Sélectionnez **Include Domain (Inclure le domaine)** et **Add (Ajoutez)** les applications SaaS ou sur le cloud public que vous souhaitez acheminer vers GlobalProtect via la connexion VPN en utilisant le domaine et le port de destination. Vous pouvez ajouter un maximum de 200 entrées à la liste. Par exemple, ajoutez *.gmail.com pour autoriser tout le trafic Gmail à passer par le tunnel VPN.
  - (Facultatif) Sélectionnez **Exclude Domaine (Exclure le domaine)** et **Add (Ajoutez)** les applications SaaS ou sur le cloud public que vous souhaitez exclure du tunnel VPN en utilisant le domaine et le port de destination. Vous pouvez ajouter un maximum de 200

 ©2025 Palo Alto Networks, Inc.

entrées à la liste. Par exemple, ajoutez *.target.com pour exclure tout le trafic Target du tunnel VPN.

4. Configurez les paramètres de segmentation de tunnel en fonction de l'application.

   Le trafic Safari ne peut pas être ajouté à la règle de segmentation de tunnel basée sur une application sur les terminaux macOS.

   Vous pouvez utiliser des variables d'environnement pour configurer une segmentation de tunnel basée sur l'application sur les terminaux Windows et macOS.

   - (Facultatif) Sélectionnez **Include Client Application Process Name (Inclure le Nom de processus de l'application client)** et **Add (Ajoutez)** les applications SaaS ou sur le cloud public que vous souhaitez acheminer vers GlobalProtect via la connexion VPN en utilisant le nom de processus de l'application. Vous pouvez ajouter un maximum de 200 entrées à la liste.
   - (Facultatif) Sélectionnez **Exclude Client Application Process Name (Exclure le Nom de processus de l'application client)** et **Add (Ajoutez)** les applications SaaS ou sur le cloud public que vous souhaitez exclure du tunnel VPN en utilisant le nom de processus de l'application. Vous pouvez ajouter un maximum de 200 entrées à la liste.

5. Enregistrez les paramètres du tunnel.

GlobalProtect – Personnaliser les paramètres de l'application

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Personnalisez la manière dont vos utilisateurs finaux interagissent avec l'application GlobalProtect.

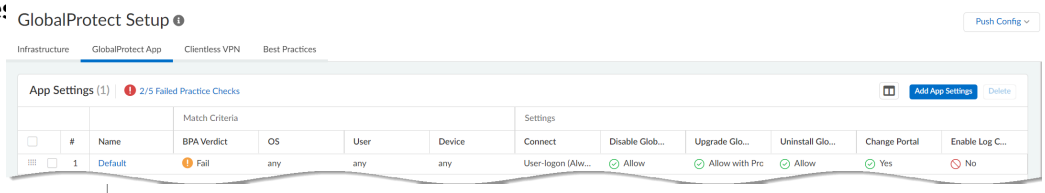
Il existe certains paramètres que vous pouvez personnaliser globalement. Ces **global app settings (paramètres d'application globaux)** s'appliquent à l'application GlobalProtect sur tous les périphériques. Les autres paramètres de l'application GlobalProtect sont définis par défaut. Vous pouvez ensuite personnaliser ces options et, en fonction des **critères de correspondance**, les cibler sur des utilisateurs et des périphériques spécifiques. Les critères de correspondance que vous définissez pour les paramètres de l'application indiquent à Prisma Access les utilisateurs, périphériques ou systèmes qui doivent recevoir les paramètres. Par exemple, vous pouvez spécifier qu'une règle s'applique uniquement aux périphériques dont les numéros de série correspondent aux entrées Active Directory.

Paramètres de l'application GlobalProtect	
Explorez et personnalisez les paramètres de l'application ici (exemples de	Prisma Access (Managed by Strata Cloud Manager)

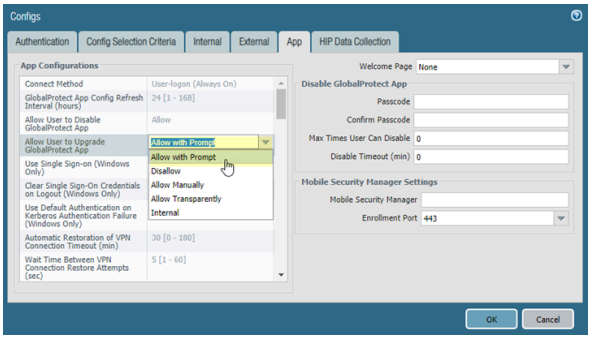
 ©2025 Palo Alto Networks, Inc.

Paramètres de l’application GlobalProtect

Cloud Management pré: ci-dessous)—>

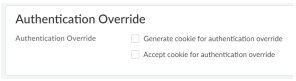


Panorama Managed Prisma Access



Contournement d'Authentification

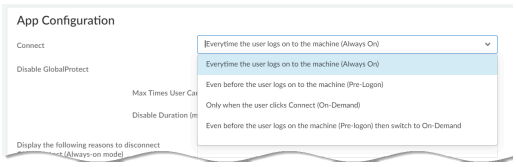
Permettez à Prisma Access de générer et d’accepter des cookies sécurisés et cryptés pour l’authentification des utilisateurs. L’activation de cette option permet à l’utilisateur de fournir ses informations de connexion une seule fois pendant la période spécifiée.



- **Generate cookie for authentication override (Générer un cookie pour remplacer l’authentification)** : permet à Prisma Access de générer des cookies cryptés, spécifiques au terminal et d’émettre les cookies d’authentification au terminal.
- **Accept cookie for authentication override (Accepter un cookie pour remplacer l’authentification)** : permet à Prisma Access d’authentifier les utilisateurs au moyen d’un cookie crypté qui est valide. Lorsque l’application présente un cookie valide, Prisma Access vérifie que le cookie a été crypté par Prisma Access à l’origine, décrypte le cookie, puis authentifie l’utilisateur.

> *L’application GlobalProtect doit connaître le nom d’utilisateur de l’utilisateur qui se connecte afin de faire correspondre et d'extraire les cookies d’authentification associés du point de terminaison de l’utilisateur. Une fois que l’application a récupéré les cookies, elle les envoie à Prisma Access à des fins d’authentification de l’utilisateur.*

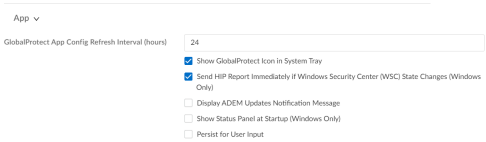
 ©2025 Palo Alto Networks, Inc.

Paramètres de l'application GlobalProtect	
	• **Cookie Lifetime (Durée de vie des cookies)** : spécifie les heures, les jours ou les semaines pendant lesquelles le cookie est valide (la valeur par défaut est 24 heures). La plage des heures est de 1 à 72 ; des semaines, de 1 à 52 ; et des jours, de 1 à 365. Après l'expiration du cookie, l'utilisateur doit saisir de nouveau ses informations d'identification. Prisma Access crypte ensuite un nouveau cookie à envoyer à l'application. Cette valeur peut être identique ou différente de la Cookie Lifetime (Durée de vie des cookies) que vous configurez. • **Certificate to Encrypt/Decrypt Cookie (Certificat pour chiffrer/décrypter le cookie)** : sélectionnez le certificat RSA utilisé pour chiffrer et décrypter le cookie.
Paramètres de connexion	Spécifiez la méthode utilisée par l'application GlobalProtect pour **Connect (Se connecter)** à Prisma Access.  • **User-logon (Always On) (Connexion utilisateur (Toujours activée))** : l'application GlobalProtect se connecte automatiquement à Prisma Access dès que l'utilisateur se connecte. Lorsqu'elle est utilisée en association avec la SSO (terminaux Windows uniquement), la connexion est transparente pour l'utilisateur final. *Sur les terminaux iOS, ce paramètre empêche les applications One-Time Password (Mot de passe à usage unique - OTP) de fonctionner, car l'application GlobalProtect force tout le trafic à traverser le tunnel.* • **Pre-logon (Always On) (Préouverture de session (Toujours activée))** : l'application GlobalProtect authentifie l'utilisateur et établit un tunnel VPN vers Prisma Access avant que l'utilisateur ne se connecte. Cette option requiert que vous utilisiez une solution PKI externe pour pré-déployer un certificat de machine à chaque périphérique qui reçoit ces paramètres. • **On-demand (Manual user initiated connection) (À la demande (connexion manuelle initiale de l'utilisateur))** : les utilisateurs doivent lancer manuellement l'application pour se connecter à GlobalProtect. • **Pre-logon then On-demand (Préouverture de session puis à la demande)** : semblable à la méthode de connexion

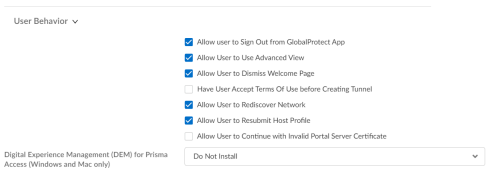
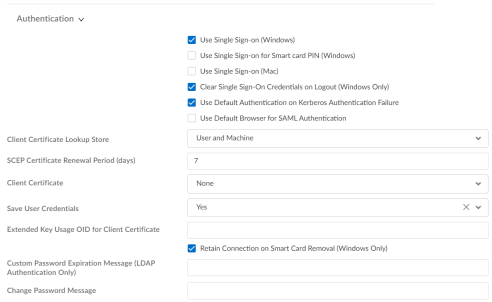
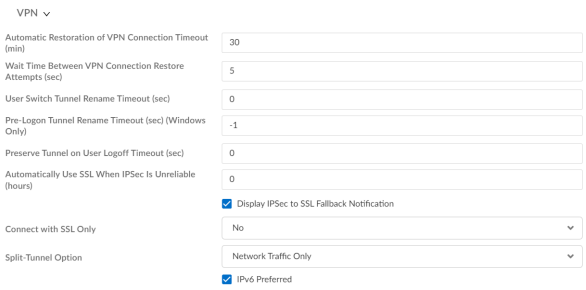
 ©2025 Palo Alto Networks, Inc.

Paramètres de l'application GlobalProtect	
	Pre-logon (Always On) (préouverture de session (toujours activée)), cette méthode de connexion (qui nécessite la version de contenu 590-3397 ou ultérieure) permet à l'application GlobalProtect d'authentifier l'utilisateur et d'établir un tunnel VPN vers Prisma Access avant que l'utilisateur ne se connecte au terminal. Contrairement à la méthode de connexion de préouverture de session, une fois que l'utilisateur se connecte, les utilisateurs doivent lancer manuellement l'application pour se connecter à GlobalProtect si la connexion est terminée pour une raison quelconque. L'avantage de cette option est que vous pouvez permettre aux utilisateurs de spécifier un nouveau mot de passe après expiration du mot de passe ou s'ils oublient leur mot de passe, mais que l'on exige toujours des utilisateurs d'initier manuellement la connexion après qu'ils se connectent.
GlobalProtect	Décidez quels paramètres de l'application GlobalProtect l'utilisateur peut ajuster : • **Disable GlobalProtect (Désactiver GlobalProtect)** : décidez si les utilisateurs peuvent ou non désactiver l'application GlobalProtect. Les utilisateurs qui désactivent l'application GlobalProtect ne peuvent pas se connecter à Prisma Access (et aux ressources protégées de votre entreprise) jusqu'à ce qu'ils réactivent l'application. • **Upgrade GlobalProtect (Mettre à niveau GlobalProtect)** : spécifiez comment les mises à niveau de l'application doivent fonctionner, notamment si les utilisateurs peuvent lancer des mises à jour. Si vous souhaitez contrôler la mise à niveau des utilisateurs, vous pouvez personnaliser la mise à niveau de l'application en fonction de la configuration. Par exemple, si vous souhaitez tester une version sur un petit groupe d'utilisateurs avant de la déployer sur l'ensemble de votre base d'utilisateurs, vous pouvez créer une configuration s'appliquant uniquement aux utilisateurs de votre groupe informatique, leur permettant ainsi de mettre à niveau et de tester tout en désactivant la mise à niveau dans toutes les autres configurations utilisateur / groupe. Après avoir complètement testé la nouvelle version, vous pouvez modifier les configurations logicielles pour le reste de vos utilisateurs et les autoriser à procéder à la mise à niveau. • **Allow with Prompt (Autoriser avec invite)** : invitez les utilisateurs à effectuer une mise à niveau lorsqu'une nouvelle version de l'application est disponible.

 ©2025 Palo Alto Networks, Inc.

Paramètres de l’application GlobalProtect	
	• **Allow Transparently (Autoriser de manière transparente)** : les mises à jour ont lieu automatique sans aucune interaction avec l’utilisateur. • **Internal (Interne)** : les mises à niveau se produisent automatiquement sans interaction de l’utilisateur lorsque l’utilisateur est connecté à Prisma Access. • **Disallow (Interdire)** : empêchez les mises à niveau de l’application. • **Allow Manually (Autoriser manuellement)** : permet aux utilisateurs de lancer les mises à niveau de l’application depuis l’application GlobalProtect. • **Uninstall GlobalProtect (Désinstaller GlobalProtect)** : autorisez les utilisateurs à désinstaller l’application GlobalProtect, empêchez-les de désinstaller l’application GlobalProtect ou autorisez-les à la désinstaller spécifiquement au travers d’un mot de passe que vous créez. • **User Can Change Portal (L’utilisateur peut modifier le portail)** : permet aux utilisateurs de modifier le portail que l’application GlobalProtect utilise pour se connecter à Prisma Access.
Configuration de l’application – Options avancées	
Paramètres de l’application	• Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Windows Only) (Envoyer le rapport HIP immédiatement si les modifications d’état du Centre de sécurité Windows (WSC) changent (Windows Uniquement)) : sélectionnez No (Non) pour empêcher l’application GlobalProtect d’envoyer des données HIP lorsque l’état du Centre de sécurité Windows (WSC) change. Sélectionnez Yes (Oui) pour envoyer immédiatement les données HIP lorsque le statut du WSC change. 
Paramètres de comportement de l’utilisateur	Les paramètres de comportement de l’utilisateur incluent :

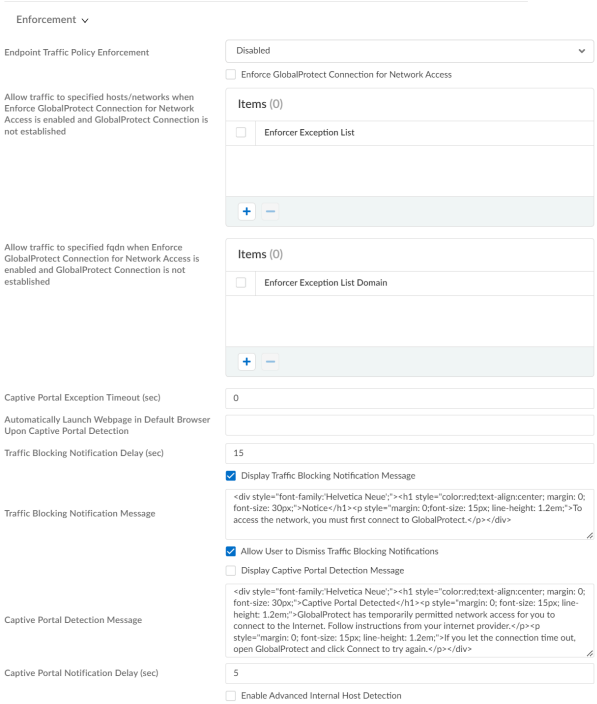
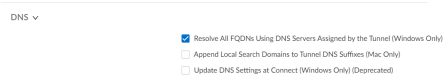
 ©2025 Palo Alto Networks, Inc.

Paramètres de l'application GlobalProtect	
	
Paramètres d'authentification	Les paramètres d'authentification incluent : 
Paramètres VPN	Configurez le délai d'expiration du VPN et les paramètres du tunnel : • **Display IPSec to SSL Fallback Notification (Afficher la notification de repli IPSec vers SSL)** : sélectionnez **No (Non)** pour empêcher les notifications contextuelles lorsque l'application GlobalProtect ne parvient pas à établir une connexion avec un tunnel IPSec et revient à un tunnel SSL. Sélectionnez **Yes (Oui)** (par défaut) pour autoriser les notifications contextuelles lorsque la connexion change. 
Paramètres d'application	Appliquer les paramètres pour le trafic spécifié : • **Allow traffic to specified FDQN when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is established (Autoriser le trafic vers le FDQN spécifié lorsque l'application de la connexion GlobalProtect pour l'accès réseau est activée et que la connexion GlobalProtect est établie).** En savoir plus. • **Automatically Launch Webpage in Default Browser Upon Captive Portal Detection (Lancer automatiquement**

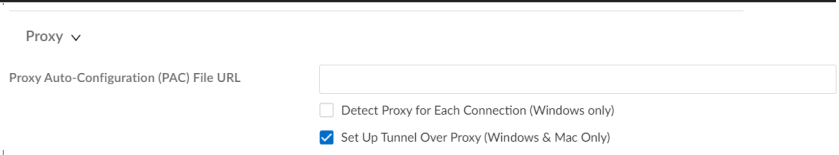
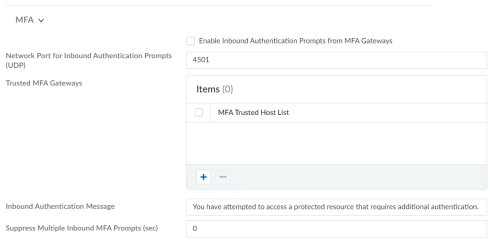
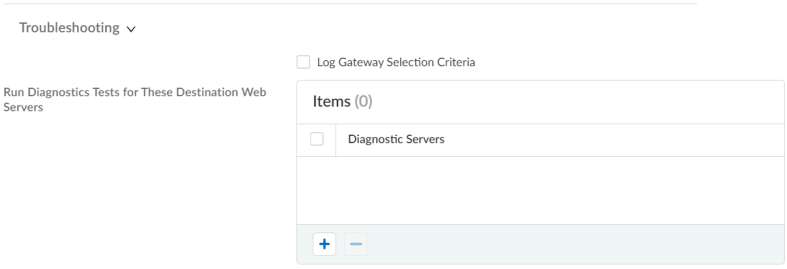
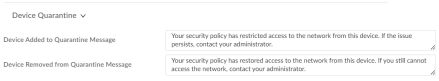
 ©2025 Palo Alto Networks, Inc.

Paramètres de l’application GlobalProtect	
	la page Web dans le navigateur par défaut lors de la détection du portail captif) : pour lancer automatiquement vos navigateurs Web par défaut afin que les utilisateurs puissent se connecter facilement au portail d’authentification, saisissez le Fully Qualified Domain Name (nom de domaine complet - FQDN) ou l’adresse IP du site Web que vous souhaitez utiliser pour la tentative de connexion initiale qui initie le trafic Web lors du lancement du navigateur Web par défaut (longueur maximale de 256 caractères). Le portail d’authentification intercepte alors cette tentative de connexion et redirige le navigateur Web par défaut vers la page de connexion au portail d’authentification. Si ce champ est vide (par défaut), Prisma Access ne lance pas automatiquement le navigateur Web par défaut lors de la détection du portail d’authentification. • **Enable Advance Internal Host Detection (Activer la détection avancée d’hôte interne)** : activez la détection avancée d’hôte interne pour ajouter une couche de sécurité supplémentaire lors de la détection d’hôte interne par l’application GlobalProtect. Avec la détection avancée d’hôte interne, l’application valide le certificat de serveur des passerelles internes en plus d’effectuer une recherche DNS inversée de l’hôte interne pour déterminer si l’application se trouve à l’intérieur du réseau d’entreprise. L’activation de la détection avancée d’hôte interne empêche les acteurs malveillants d’usurper la réponse du serveur DNS inversé pendant la détection d’hôte interne et empêche ainsi l’accès non autorisé aux terminaux du réseau d’entreprise. Si vous n’activez pas

 ©2025 Palo Alto Networks, Inc.

Paramètres de l'application GlobalProtect	
	la détection avancée d'hôte interne, la détection d'hôte interne existante fonctionne comme prévu. 
Paramètres de comportement de connexion	Les paramètres de comportement de connexion incluent :  En savoir plus.
Paramètres DNS	Les paramètres DNS incluent : 
Paramètres du proxy	Spécifiez la **Proxy Auto-Configuration (PAC) File URL (URL du fichier PAC (Proxy Auto-Configuration))** que vous souhaitez transmettre au terminal pour configurer les paramètres de proxy. La longueur maximale de l'URL est de 256 caractères. Les méthodes d'URL de fichier PAC (Proxy Auto-Configuration) suivantes sont prises en charge : • Norme PAC (Proxy Auto-Config) (par exemple, http://pac.<hostname or IP>/proxy.pac). • Norme WPAD (Web Proxy Auto-Discovery Protocol) (par exemple, http://wpad.<hostname or IP>/wpad.dat).

 ©2025 Palo Alto Networks, Inc.

Paramètres de l'application GlobalProtect	
	
Paramètres MFA	Les paramètres MFA incluent : 
Paramètres de dépannage	Les paramètres de dépannage incluent : 
Paramètres de mise en quarantaine des périphériques	Les paramètres de mise en quarantaine des périphériques incluent : 
Détection d'hôte interne	Si vous ne souhaitez pas que vos utilisateurs mobiles se connectent à Prisma Access lorsqu'ils se trouvent sur le réseau interne, activez la détection d'hôte interne pour permettre à l'application GlobalProtect de déterminer s'il se trouve sur un réseau interne ou externe. • Saisissez l'adresse IP (IPv4 ou IPv6) d'un hôte qui peut être résolue uniquement depuis le réseau interne. • Saisissez le nom d'hôte DNS correspondant à l'adresse IP que vous avez saisie. Lorsqu'un utilisateur mobile se connecte à Prisma Access, l'application GlobalProtect tente d'effectuer une recherche DNS inversée sur l'adresse spécifiée. Si la recherche échoue, l'application GlobalProtect détermine

 ©2025 Palo Alto Networks, Inc.

Paramètres de l'application GlobalProtect	
	qu'elle se trouve sur le réseau externe et initie ensuite une connexion à Prisma Access.
Activer la détection d'hôte interne	Si vous souhaitez que l'application GlobalProtect retente la découverte du réseau lorsqu'une passerelle interne et une détection d'hôte interne sont configurées sans passerelle externe et que la détection d'hôte interne échoue, définissez le paramètre **Enable Intelligent Internal Host Detection (Activer la détection intelligente d'hôte interne)** sur Yes (Oui).
Passerelles	Par défaut, toutes les passerelles de vos emplacements Prisma Access sont disponibles pour les utilisateurs. Si vous disposez de passerelles GlobalProtect supplémentaires (internes ou externes) auxquelles vous souhaitez que vos utilisateurs puissent se connecter, vous pouvez ajouter ces passerelles ici.
Collecte de données HIP	Définissez les données de Host Information Profile (profil d'informations sur l'hôte - HIP) que l'application devra collecter ou exclure de la collecte. Lorsque cette option est activée, l'application collecte des données à partir de périphériques exécutant les systèmes d'exploitation Windows, Mac ou Linux. Par exemple, une vérification personnalisée peut vous permettre de savoir si une certaine application est installée ou en cours d'exécution sur un terminal. Les données que vous définissez comme devant être collectées dans une vérification personnalisée sont incluses dans les données d'informations brutes de l'hôte que l'application GlobalProtect collecte puis soumet à Prisma Access lorsque l'application se connecte. Pour surveiller les données collectées avec des vérifications personnalisées, vous pouvez créer un objet HIP. Vous pouvez ensuite ajouter l'objet HIP à un profil HIP afin d'utiliser les données collectées pour mettre en correspondance les données et le trafic du point de terminaison, et mettre en œuvre des règles de sécurité. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **HIP** et **HIP Objects (Objets HIP)** ou **HIP Profiles (Profils HIP)**. Sélectionnez la portée de configuration **Prisma Access** > **Mobile Users Container (Conteneur d'utilisateurs mobiles)** > **GlobalProtect**.
Paramètres de délai d'expiration	• Sur la page GlobalProtect Setup (Configuration de GlobalProtect), sélectionnez l'icône d'engrenage dans la zone Global App Settings (Paramètres globaux de l'application).

 ©2025 Palo Alto Networks, Inc.

Paramètres de l'application GlobalProtect	
	• Modifiez la **Login Lifetime (Durée de vie de connexion)** maximale d'une session de connexion d'une seule passerelle (la valeur par défaut est de 30 jours). Pendant la durée de vie, l'utilisateur reste connecté tant que la passerelle reçoit une vérification HIP à partir du terminal dans la période de **Inactivity Logout (Déconnexion d'inactivité)**. Après cette période, la session de connexion se termine automatiquement. • Définissez le délai de préavis à fournir aux utilisateurs pour indiquer que leurs sessions d'application sont sur le point d'expirer en raison de l'expiration de la durée de vie de la connexion. La valeur par défaut est 30 minutes. La plage acceptée est de 0 à 60 minutes. • Personnalisez le message de notification de délai d'expiration. • Modifiez la période de **Inactivity Logout (Déconnexion d'inactivité)** pour spécifier la durée après laquelle les utilisateurs inactifs sont déconnectés de GlobalProtect. Vous pouvez appliquer une politique de sécurité pour surveiller le trafic des terminaux lorsque vous êtes connecté à GlobalProtect et pour vous déconnecter rapidement des sessions GlobalProtect inactives en définissant une période de déconnexion d'inactivité plus courte. Les utilisateurs sont déconnectés de GlobalProtect si l'application GlobalProtect n'a pas acheminé le trafic via le tunnel VPN ou si la passerelle ne reçoit pas de vérification HIP du terminal au cours de la période configurée. La valeur par défaut est 180 minutes. La plage acceptée est de 5 à 43 200 minutes. • Définissez le délai de préavis à fournir aux utilisateurs pour indiquer que leurs sessions d'application sont sur le point d'expirer en raison d'une inactivité. La valeur par défaut est 30 minutes. La plage acceptée est de 0 à 60 minutes. • Personnalisez le message de notification d'inactivité. • Spécifiez si vous souhaitez avertir les utilisateurs finaux si leur administrateur les déconnecte et définissez le message d'affichage. • Cliquez sur **Save (Enregistrer)**.
Application de l'adresse IP source pour les cookies d'authentification	Configurez les paramètres de connexion VPN et les restrictions d'utilisation des cookies d'authentification pour une posture de sécurité améliorée. • Sur la page GlobalProtect Setup (Configuration de GlobalProtect), sélectionnez l'icône d'engrenage dans

 ©2025 Palo Alto Networks, Inc.

Paramètres de l'application GlobalProtect	
	la zone Global App Settings (Paramètres globaux de l'application). • Configurez la restauration automatique des tunnels VPN SSL. Si la Automatic Restoration of VPN Connection (Restauration automatique de la connexion VPN) est activée sur le portail GlobalProtect, vous pouvez la désactiver pour cette passerelle en sélectionnant **Disable Automatic Restoration of SSL VPN (Désactiver la restauration automatique du VPN SSL)**. • Configurez l'application de l'adresse IP source pour les cookies d'authentification. Vous pouvez configurer la passerelle ou le portail GlobalProtect pour qu'ils acceptent les cookies des terminaux uniquement lorsque l'adresse IP du terminal correspond aux adresses IP source d'origine pour lesquelles le cookie a été émis ou lorsque l'adresse IP du terminal correspond à une plage d'adresses IP de réseau spécifique. Vous pouvez définir la plage d'adresses IP de réseau à l'aide d'un masque de sous-réseau CIDR, comme /24 ou /32. Par exemple, si un cookie d'authentification a été initialement émis vers un terminal avec l'adresse IP source publique 201.109.11.10 et que le masque de sous-réseau de la plage d'adresses IP réseau est défini sur /24, le cookie d'authentification est ensuite valide sur les terminaux avec des adresses IP source publiques dans la plage d'adresses IP réseau 201.109.11.0/24. Dans la section Authentication Cookie Usage Restrictions (Restrictions d'utilisation des cookies d'authentification), sélectionnez **Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override) (Restreindre l'utilisation des cookies d'authentification (pour la restauration automatique du tunnel VPN ou le contournement d'authentification))**, puis configurez l'une des conditions suivantes : • Si vous sélectionnez **The original Source IP for which the authentication cookie was issued (L'adresse IP source d'origine pour laquelle le cookie d'authentification a été émis)**, le cookie d'authentification n'est valide que si l'adresse IP source publique du terminal qui tente d'utiliser le cookie est identique à l'adresse IP source publique du terminal pour laquelle le cookie a initialement été émis.

 ©2025 Palo Alto Networks, Inc.

Paramètres de l'application GlobalProtect	
	• Si vous sélectionnez **The original Source IP network range (La plage réseau de l'adresse IP source d'origine)**, le cookie d'authentification n'est valide que si l'adresse IP source publique du terminal qui tente d'utiliser le cookie se situe dans la plage désignée d'adresses IP réseau. Saisissez un Source IPv4 Netmask (Masque réseau IPv4 source) ou un Source IPv6 Netmask (Masque réseau IPv6 source) pour définir le masque de sous-réseau de la plage d'adresses IP réseau pour laquelle le cookie d'authentification est valide (par exemple 32 ou 128).

Requête de ticket pour désactiver GlobalProtect

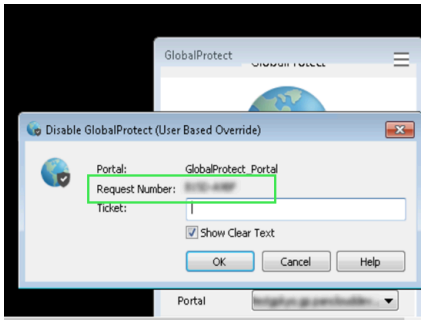
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Au lieu de permettre aux utilisateurs de désactiver directement GlobalProtect, vous pouvez autoriser un utilisateur à créer un ticket afin de désactiver GlobalProtect. L'administrateur GlobalProtect peut alors décider d'autoriser ou non chaque utilisateur spécifique à désactiver GlobalProtect.

Comment cela fonctionne

Une fois que vous avez configuré cette fonctionnalité, voici le flux de travail d'une requête de ticket visant à désactiver GlobalProtect :

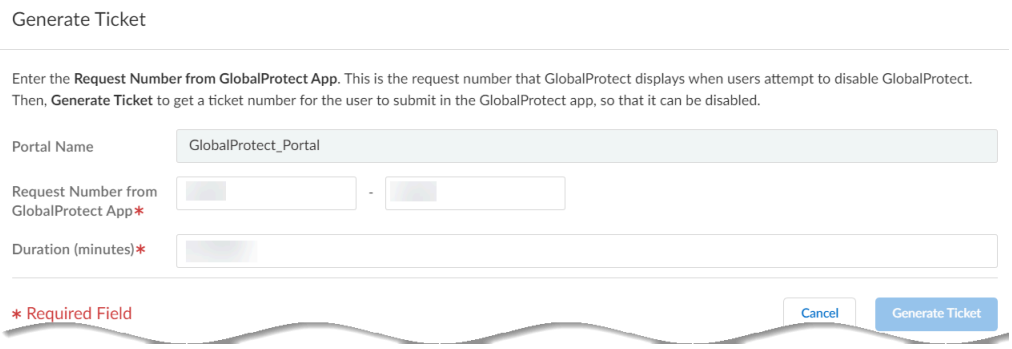
- Un utilisateur tente de désactiver GlobalProtect dans l'application GlobalProtect. GlobalProtect présente un numéro de requête à l'utilisateur.



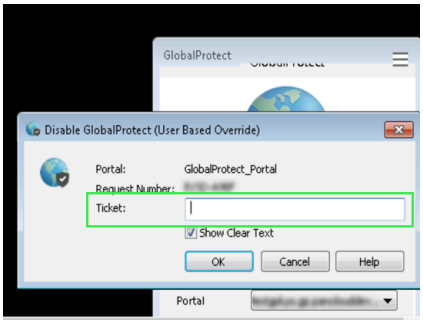
- L'utilisateur partage le numéro de requête avec l'administrateur GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

- L'administrateur GlobalProtect se connecte à Prisma Access (Managed by Strata Cloud Manager) et utilise le numéro de requête pour générer un ticket.



- L'administrateur GlobalProtect partage le numéro de ticket avec l'utilisateur. L'utilisateur saisit le numéro de ticket dans l'application pour désactiver GlobalProtect.



Configurer cette fonctionnalité

- Strata Cloud Manager
- Panorama

Requête de ticket pour désactiver GlobalProtect (Strata Cloud Manager)

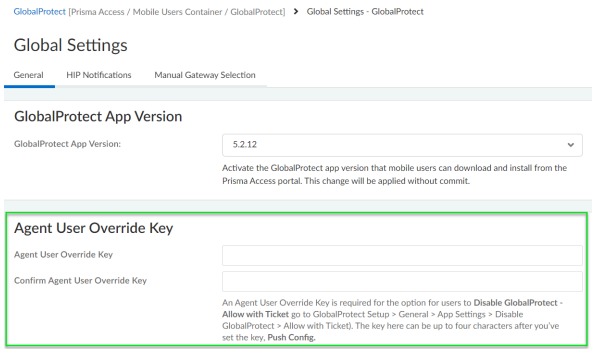
STEP 1 | Définir une clé de remplacement de l'agent

Pour activer l'option permettant aux utilisateurs d'envoyer une requête de ticket pour désactiver GlobalProtect, vous devez d'abord définir une clé de remplacement d'utilisateur de l'agent.

Allez dans **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Application GlobalProtect)** > **Global App**

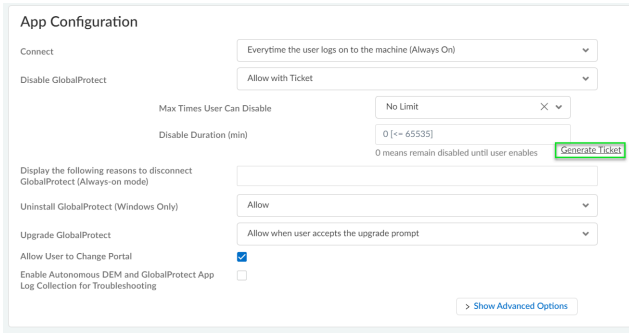
 ©2025 Palo Alto Networks, Inc.

Settings (Paramètres généraux de l'application) et sélectionnez une clé à quatre caractères pour définir la **Agent Override Key (Clé de remplacement de l'agent)**.



STEP 2 | Permettre à GlobalProtect d'être désactivé avec un ticket

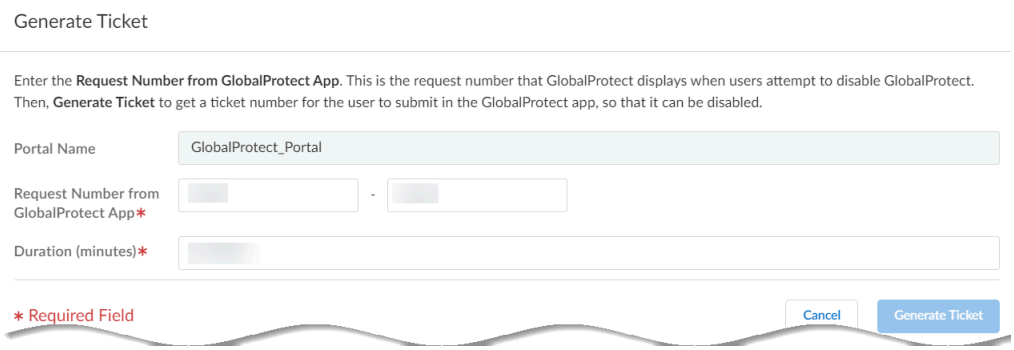
Allez dans **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)** > **App Configuration (Configuration de l'application)** > **Disable GlobalProtect (Désactiver GlobalProtect)** et définissez l'option sur **Allow with Ticket (Autoriser avec ticket)**.



STEP 3 | Générer un ticket

Après avoir défini la **Agent Override Key (Clé de remplacement de l'agent)** et la possibilité de **Allow with Ticket (Autoriser avec ticket)**, vous pourrez sélectionner **Generate Ticket (Générer un ticket)**.

Lorsqu'un utilisateur tente de désactiver GlobalProtect dans l'application, GlobalProtect lui présente un numéro de requête. Soumettez ce numéro de requête ici pour générer un ticket de désactivation de GlobalProtect pour cet utilisateur.



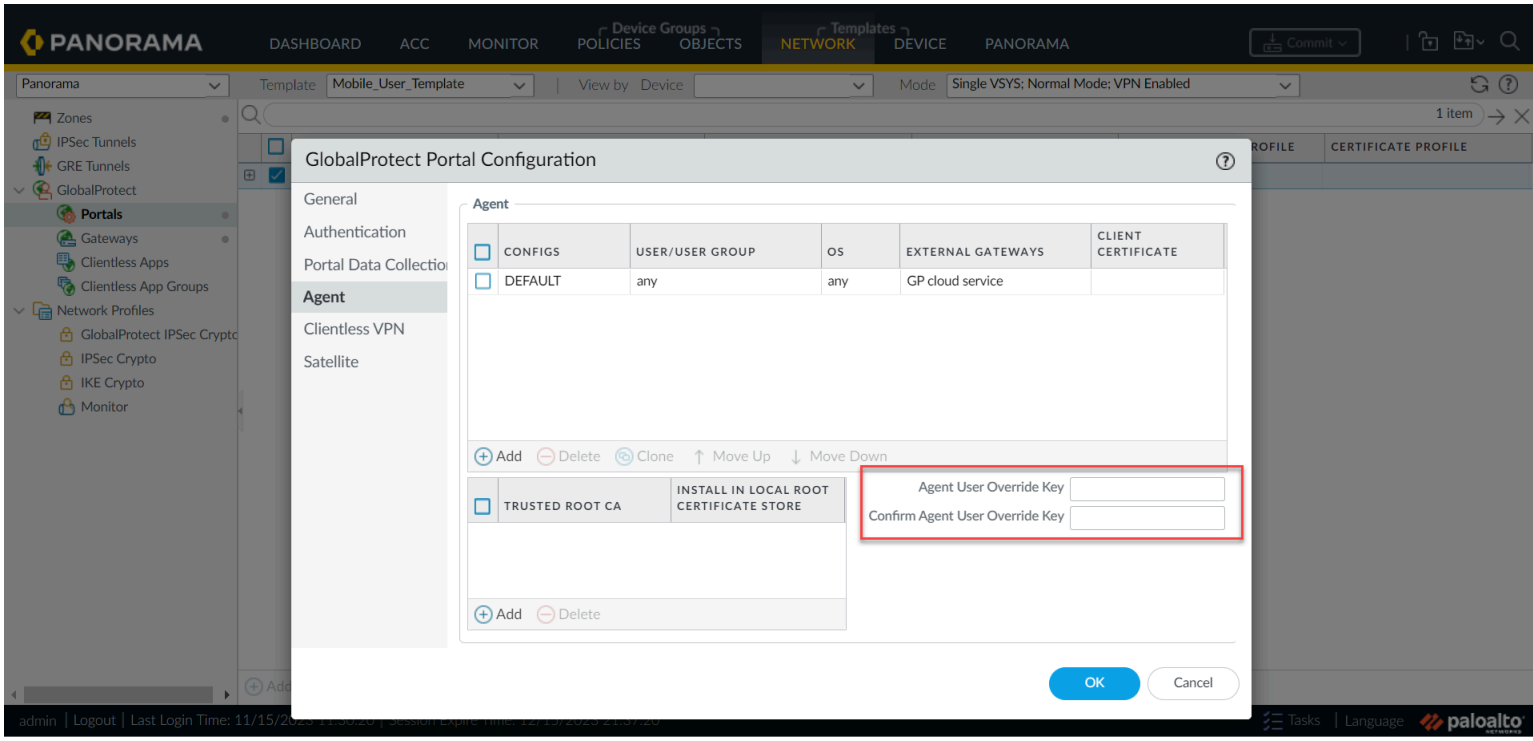
 ©2025 Palo Alto Networks, Inc.

Requête de ticket pour désactiver GlobalProtect (Panorama)

STEP 1 | Définir une clé de remplacement de l'agent

Pour activer l'option permettant aux utilisateurs d'envoyer une requête de ticket pour désactiver GlobalProtect, vous devez d'abord définir une clé de remplacement d'utilisateur de l'agent.

Allez dans **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** et sélectionnez le nom de la connexion pour laquelle vous souhaitez définir une clé de remplacement. Sélectionnez **Agent**, puis entrez une clé pour définir la **Agent Override Key (Clé de remplacement de l'agent)**.

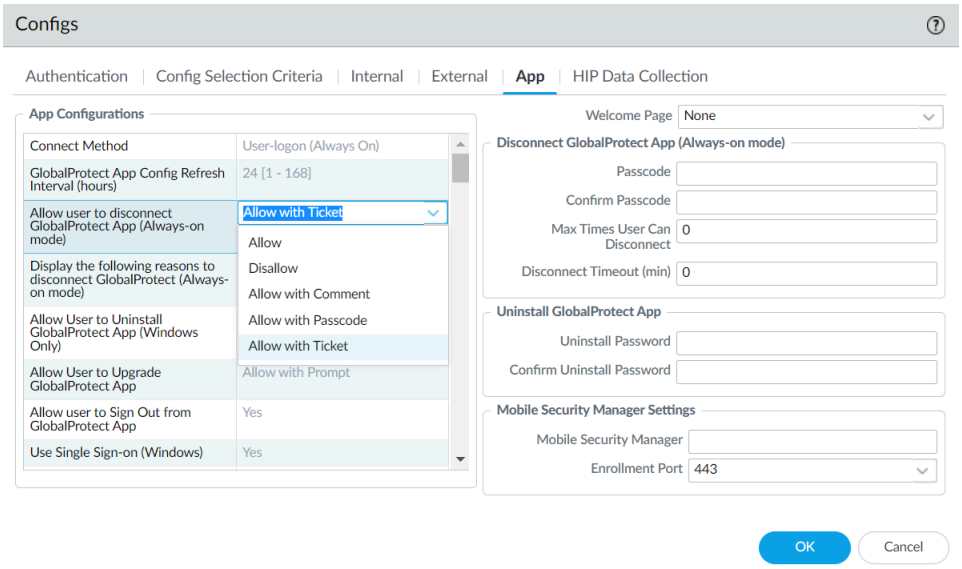


STEP 2 | Permettre à GlobalProtect d'être désactivé avec un ticket

Allez dans **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** et sélectionnez le nom de la connexion dont vous souhaitez vous déconnecter. Sélectionnez **Agent**, choisissez une **Config**, sélectionnez **App (Application)** > **App Configurations (Configurations d'application)** > **Allow user to disconnect GlobalProtect App (Always-on mode) (Autoriser l'utilisateur à déconnecter**

 ©2025 Palo Alto Networks, Inc.

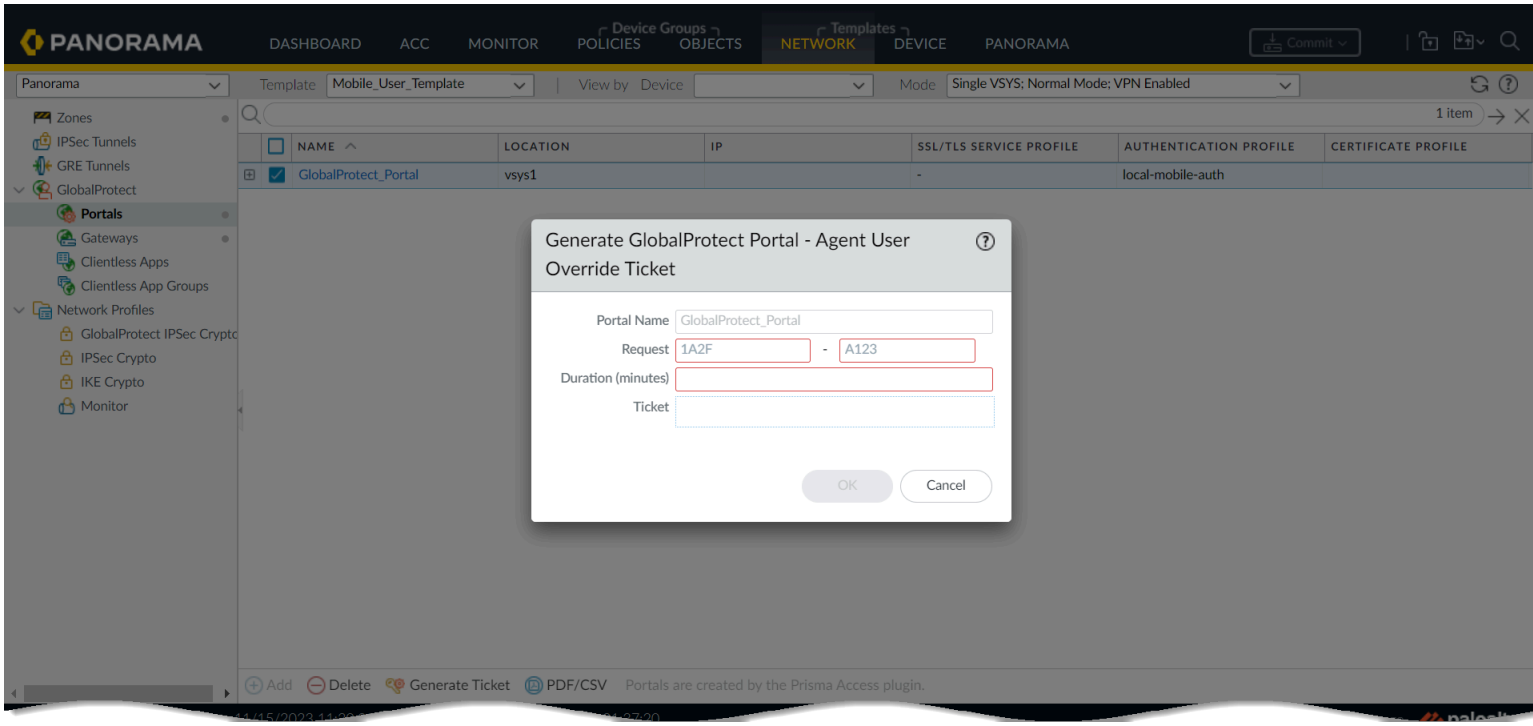
l'application GlobalProtect App (mode toujours actif)) et définissez l'option sur **Allow with Ticket (Autoriser avec ticket)**.



STEP 3 | Générer un ticket

Après avoir défini la **Agent Override Key (Clé de remplacement de l'agent)** et la possibilité de **Allow with Ticket (Autoriser avec ticket)**, vous pourrez sélectionner **Generate Ticket (Générer un ticket)**.

Lorsqu'un utilisateur tente de désactiver GlobalProtect dans l'application, GlobalProtect lui présente un numéro de requête. Soumettez ce numéro de requête ici pour générer un ticket de désactivation de GlobalProtect pour cet utilisateur.



 ©2025 Palo Alto Networks, Inc.

Préouverture de session GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access ❑ Accès administrateur au terminal pour l'installation du certificat machine ❑ Certificat PKI de confiance déployé sur le terminal

La préouverture de session est une méthode de connexion qui établit un tunnel VPN avant qu'un utilisateur ne se connecte. Le but de la préouverture de session est d'authentifier le terminal, et non l'utilisateur, puis d'activer les scripts de domaine et d'autres tâches de votre choix à exécuter dès que le terminal est activé. Les certificats machine permettent au point de terminaison d'établir un tunnel VPN à la passerelle GlobalProtect. Une pratique courante pour les administrateurs informations consiste à installer le certificat de machine tout en mettant en scène le point de terminaison pour l'utilisateur. Un tunnel VPN de préouverture de session utilise un nom d'utilisateur de préouverture de session générique, car l'utilisateur n'est pas connecté. Pour autoriser les terminaux à accéder aux ressources, vous devez créer des règles de politique de sécurité qui correspondent à l'utilisateur de préouverture de session. Ces règles de politique doivent autoriser l'accès uniquement aux services de base pour le démarrage du système ; par exemple, DHCP, DNS, des services Active Directory spécifiques, des antivirus ou d'autres services de mise à jour. Après que l'utilisateur s'authentifie à la passerelle, l'application GlobalProtect réaffecte le tunnel VPN à cet utilisateur. Le mappage de l'adresse IP sur Prisma Access passe du terminal de préouverture de session à l'utilisateur authentifié.

Le certificat utilisé pour l'authentification préouverture de session réside dans le magasin de certificats personnel du terminal. Utilisez une CA tierce de confiance, une CA auto-signée ou une CA PKI interne pour émettre un certificat machine. Vous devez configurer un certificat machine en tant que méthode d'authentification pour établir un tunnel à partir d'un terminal avant de vous connecter à Prisma Access, puis créez un profil de certificat qui inclut le certificat CA de préouverture de session.

- Strata Cloud Manager
- Panorama

Préouverture de session GlobalProtect (Strata Cloud Manager)

Importer un certificat CA racine tiers

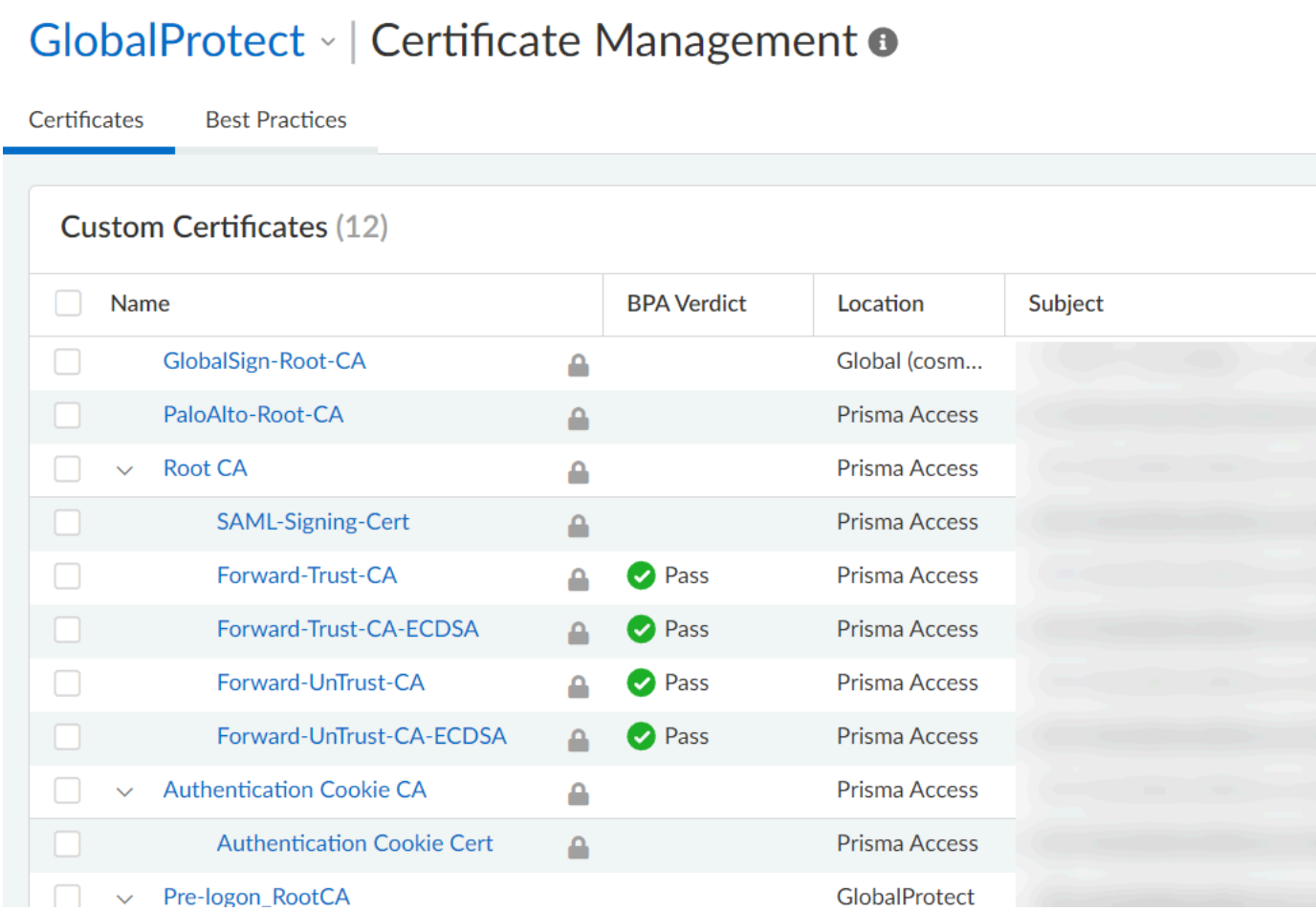
Utilisez un certificat machine comme méthode d'authentification pour établir un tunnel depuis un terminal avant de vous connecter à Prisma Access.

STEP 1 | Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)**. Sélectionnez la portée de la configuration **Prisma Access**.

Assurez-vous d'importer le certificat pour les utilisateurs mobiles de GlobalProtect.

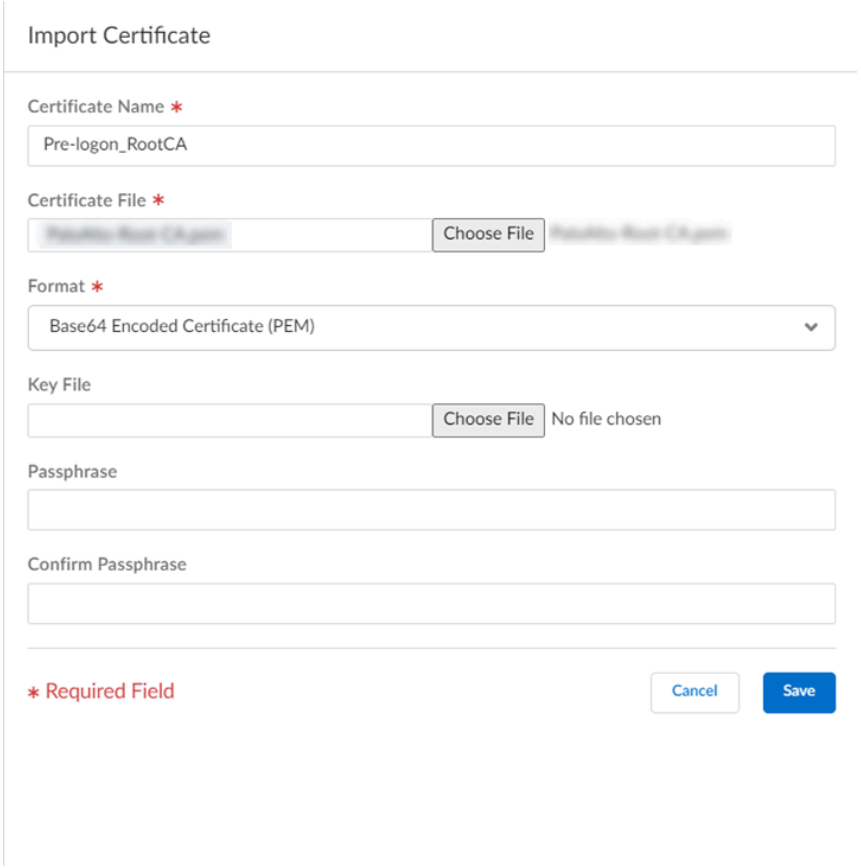
 ©2025 Palo Alto Networks, Inc.

STEP 2 | **Import (Importez)** un certificat personnalisé.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Saisissez les valeurs et **Save (Enregistrez)** les paramètres du certificat.



Créer un profil de certificat de préouverture de session

Créez un profil de certificat et incluez la CA racine auto-signée. Cette CA valide le certificat machine par l'utilisateur mobile GlobalProtect lors de la préouverture de session.

STEP 1 | Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)**. Sélectionnez la portée de la configuration **Prisma Access**.

STEP 2 | **Add Profile (Ajoutez un profil)**.

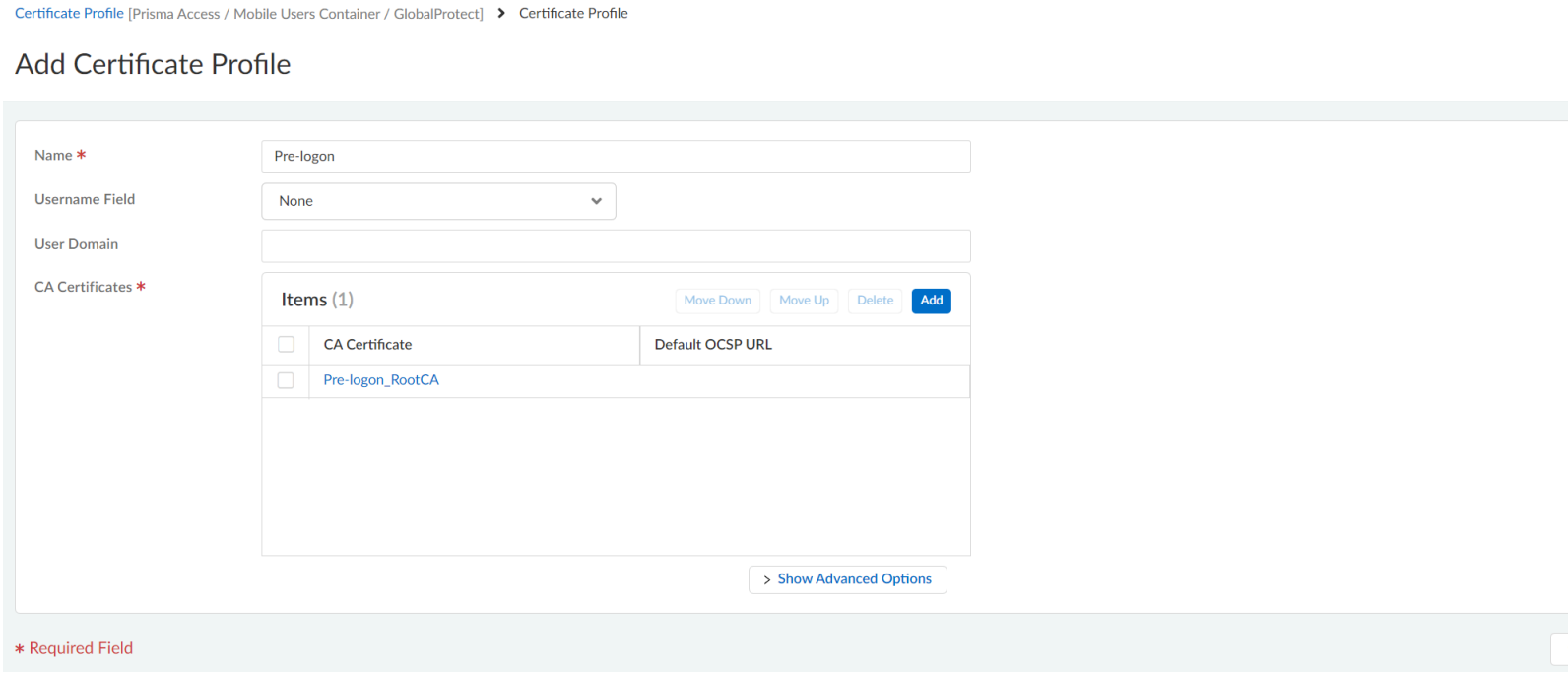
 ©2025 Palo Alto Networks, Inc.

STEP 3 | Saisissez les valeurs.

1. Assurez-vous que le **Username Field (Champ Nom d'utilisateur)** est **None (Vide)** pour empêcher le certificat de mapper à un utilisateur.

   *Le **Username Field (Champ Nom d'utilisateur)** ne peut pas être **None (Vide)** si vous authentifiez votre certificat par une méthode d'authentification **OR (OU)** un certificat client comme mentionné à l'étape 2.*

2. **Add (Ajoutez)** le certificat CA de préouverture de session racine que vous avez importé à l'étape 1.
3. **Save (Enregistrez)** les paramètres de profil de certificat.



Configurer le portail GlobalProtect pour la préouverture de session

Configurez le portail GlobalProtect pour authentifier les connexions avec un certificat machine.

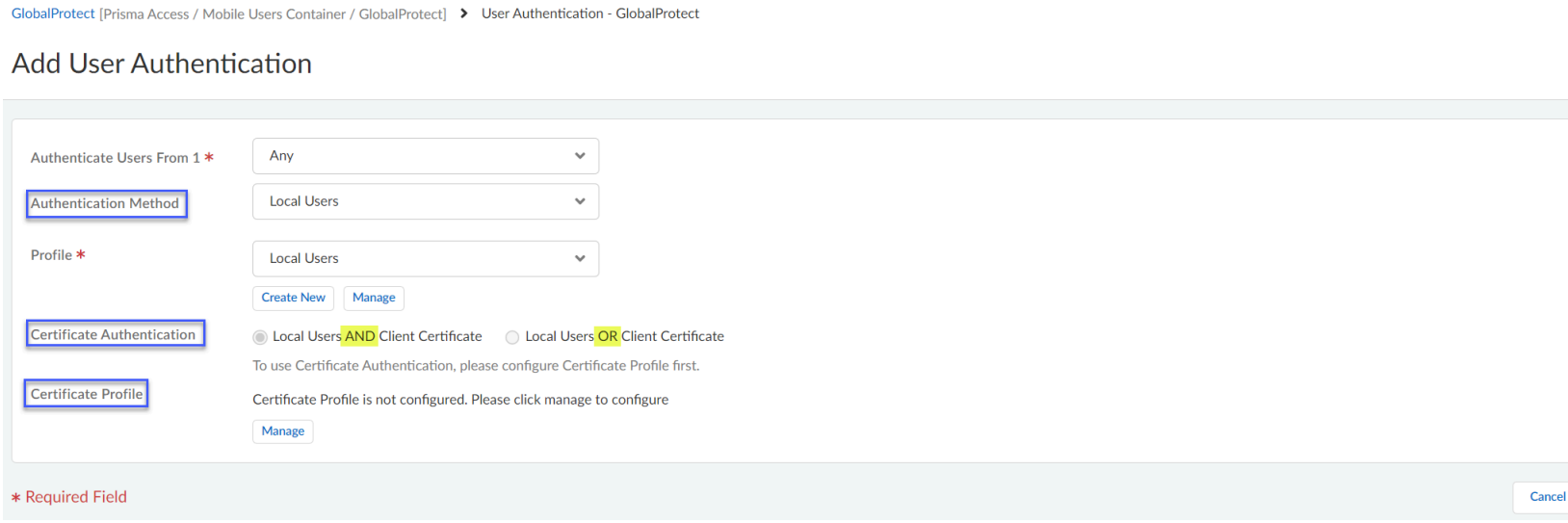
STEP 1 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **Infrastructure**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Modifiez les paramètres de configuration de l'authentification de l'utilisateur.

Sélectionnez une méthode d'authentification prise en charge par GlobalProtect, le profil de certificat de préouverture de session que vous avez créé et l'authentification par certificat.

Choisissez toute authentification par certificat que GlobalProtect prend en charge.

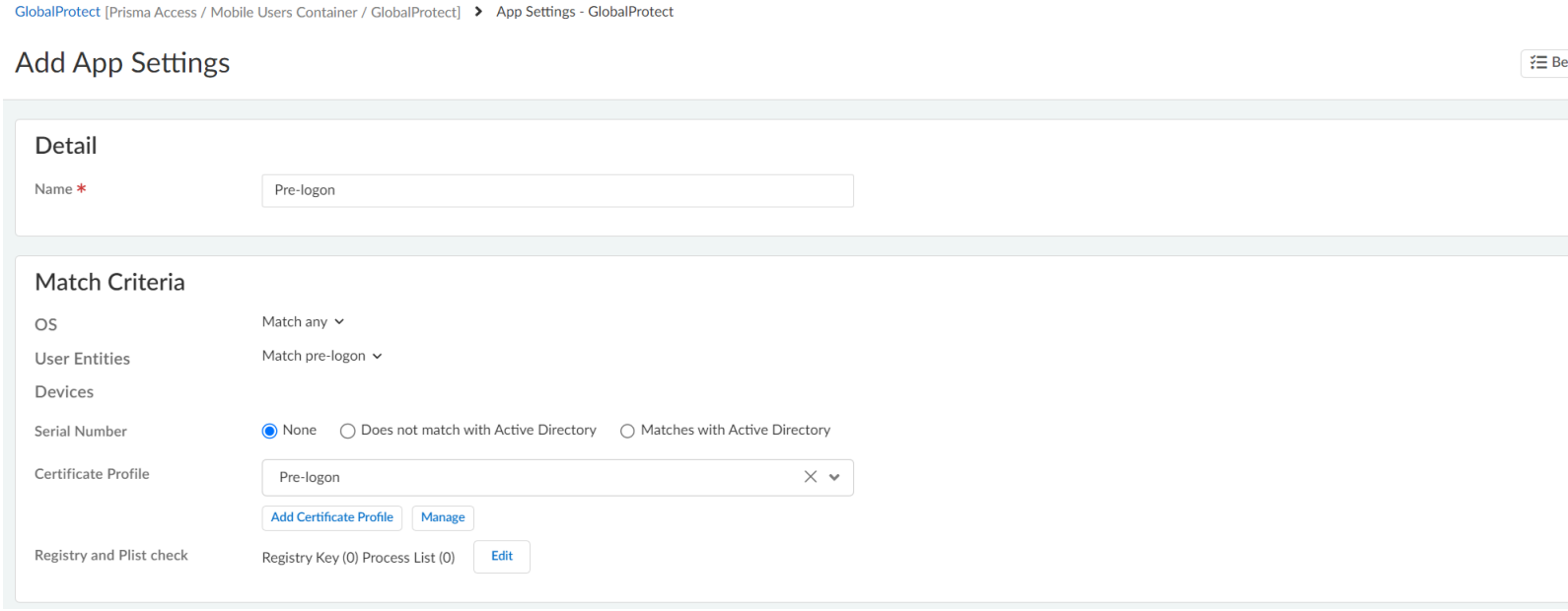


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configurez les paramètres de l'application GlobalProtect pour correspondre aux critères de préouverture de session.

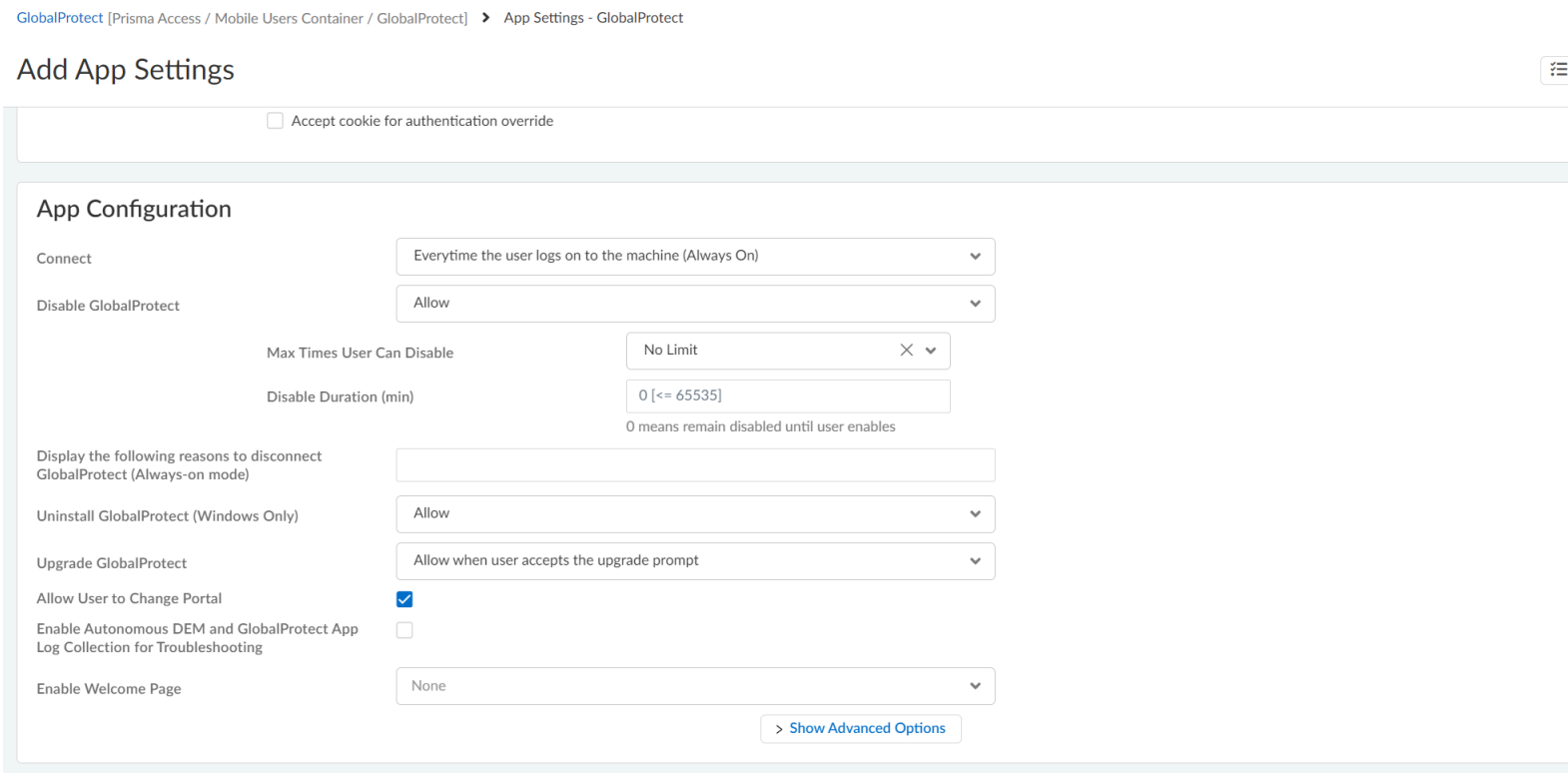
1. Naviguez vers l'onglet **GlobalProtect App (Application GlobalProtect)**.
2. **Ajoutez les paramètres de l'application.**

   *Lorsque vous saisissez des valeurs, assurez-vous de **Match pre-logon user entities (Faire correspondre les entités utilisateur de préouverture de session)** et le profil de certificat de préouverture de session.*



- Sélectionnez une méthode de connexion de préouverture de session.

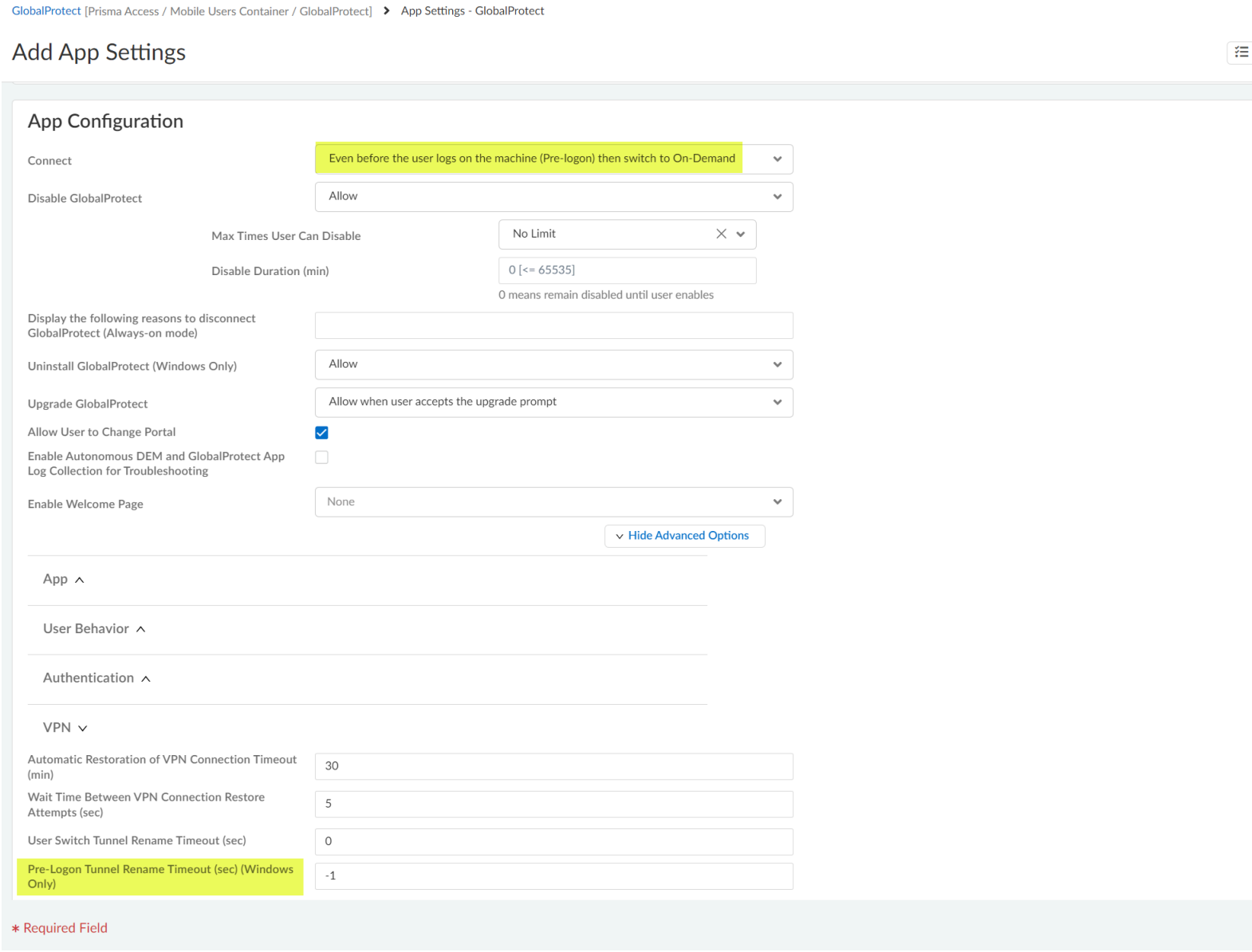
 ©2025 Palo Alto Networks, Inc.



- Si vous sélectionnez **Even before the user logs on the machine (Pre-logon) then switch to On-Demand (Même avant que l'utilisateur ne se connecte à la machine (Préouverture de session), puis passer à À la demande)**, définissez la valeur du **Pre-logon Tunnel Rename Timeout (Délai d'expiration de renommage du tunnel**

 ©2025 Palo Alto Networks, Inc.

de préouverture de session) sur –1. Consultez les options avancées du VPN pour modifier ce champ.



3. Déplacez le paramètre de l'application de préouverture de session au-dessus des autres paramètres d'application.
4. Modifiez tous les autres paramètres de l'application pour les utilisateurs authentifiés.

   Mettez à jour la méthode de connexion et le profil de certificat.

STEP 4 | Transmettez les modifications vers Prisma Access.

Installer un certificat machine – Windows

Installez le certificat machine au niveau du terminal, qui est utilisé pour l'authentification.

STEP 1 | Exportez le certificat CA racine auto-signé de votre PKI au format **Binary Encoded Certificate (DER) (Certificat encodé binaire (DER))**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Transférez les fichiers de certificat sur une machine Windows.

STEP 3 | Installez le certificat CA de préouverture de session racine dans le magasin **Trusted Root Certification Authorities (Autorités de certification racines de confiance)** de votre machine locale.

STEP 4 | Installez le certificat machine de préouverture de session dans l'emplacement du magasin de la machine locale.

STEP 5 | Procédez à l'installation, saisissez la phrase secrète lorsque vous y êtes invité, et terminez l'installation.

STEP 6 | Connectez-vous au portail GlobalProtect et supprimez tous les cookies de l'hôte.

STEP 7 | (Facultatif) Déconnectez-vous de votre machine et consultez les journaux GlobalProtect pour vérifier la connexion préouverture de session.

Préouverture de session GlobalProtect (Panorama)

Configurer le certificat et le profil de préouverture de session

Configurez un certificat machine en tant que méthode d'authentification pour établir un tunnel à partir d'un terminal avant de vous connecter à Prisma Access, puis créez un profil de certificat qui inclut le certificat CA de préouverture de session.

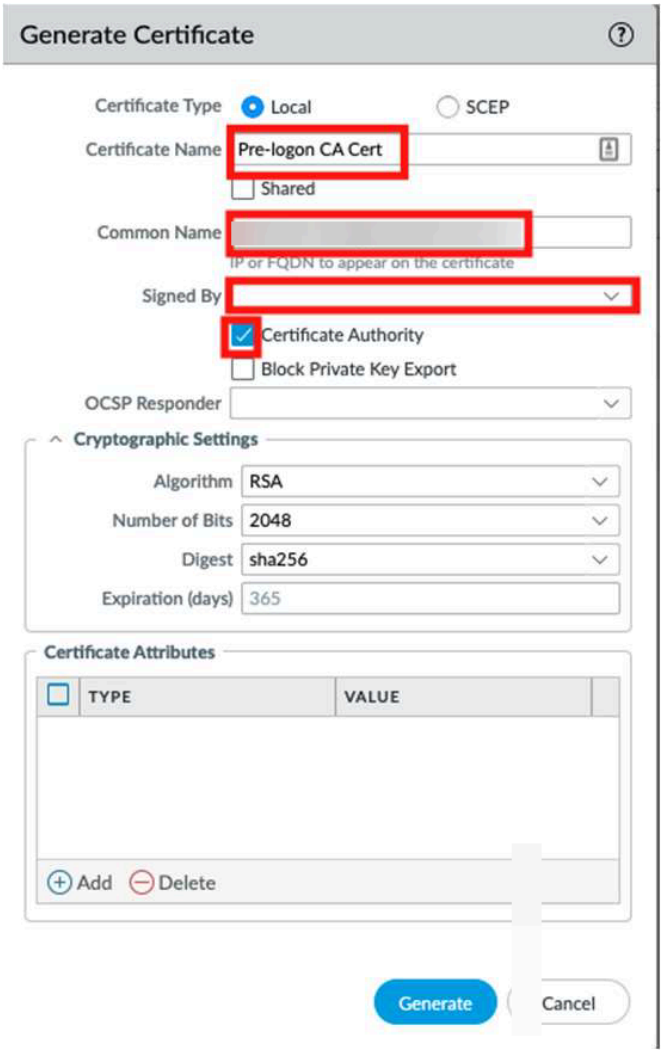
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Configurez une CA auto-signée et utilisez-la pour générer un certificat machine dans le modèle Mobile User (Utilisateur mobile). Accédez à **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**.

Assurez-vous que vous êtes dans le **Mobile_User_Template (Modèle Utilisateur Mobile)** et que le **Location (Emplacement)** est défini sur **Shared (Partagé)**.

1. Nommez le certificat ; par exemple **Certificat CA de préouverture de session**.
2. Saisissez un **Common Name (Nom commun - CN)**.

   Le Common Name (nom commun - CN) est le nom de domaine, tel que www.yourdomainname.com, que vous souhaitez sécuriser avec votre certificat.
3. Laissez le champ **Signed By (Signé par)** vide, puis cliquez sur la case à cocher **Certificate Authority (autorité de certification - CA)**.
4. **Generate (Générez)** le certificat à utiliser dans les connexions préouverture de session.

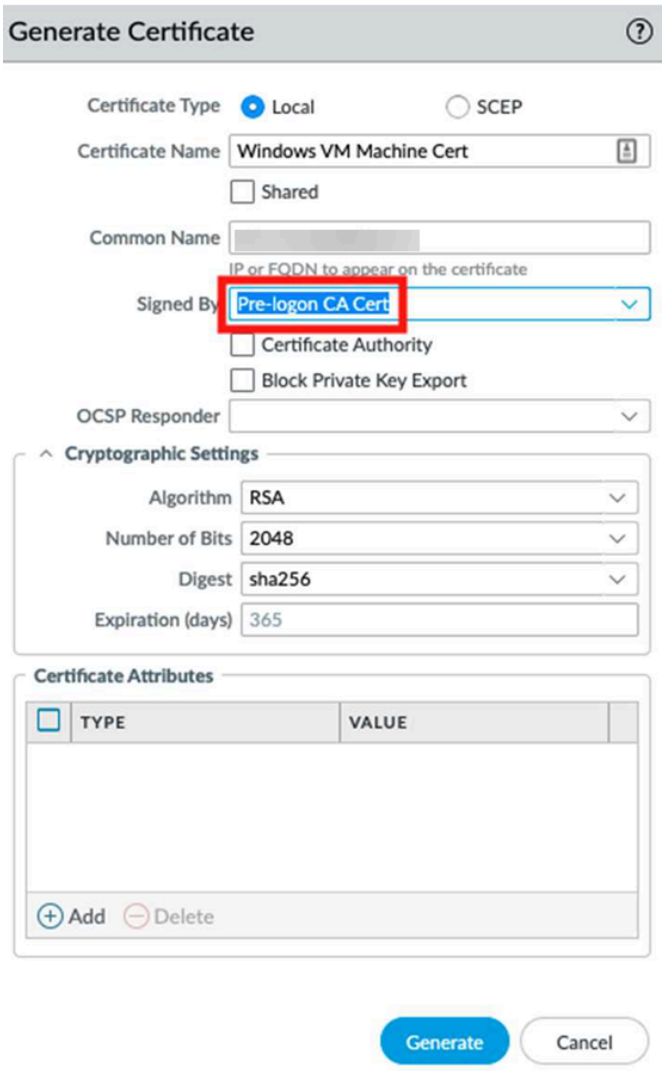


 ©2025 Palo Alto Networks, Inc.

STEP 2 | Après avoir configuré la CA auto-signée, générez le certificat machine.

1. Saisissez un **Certificate Name (Nom de certificat)** et un **Common Name (nom commun - CN)**.
2. Dans la liste déroulante **Signed By (Signé par)**, sélectionnez le **Pre-logon CA Cert (Certificat CA de préouverture de session)** que vous avez créé à l'étape 1.
3. **Generate (Générez)** le **Windows VM Machine Certificate (Certificat de VM Windows)** que vous installerez ultérieurement sur une machine Windows.

   Ce certificat est un enfant de la CA de préouverture de session.

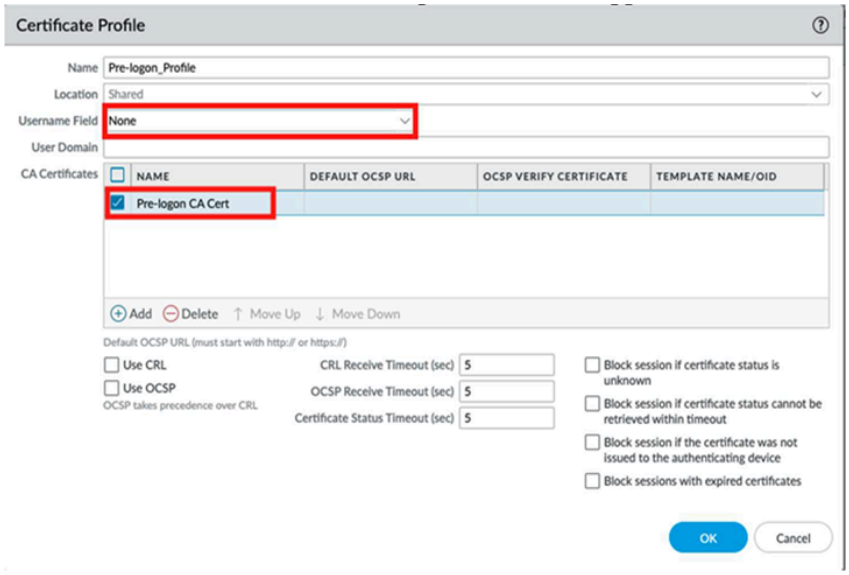


STEP 3 | Pour créer un profil de certificat qui inclut le certificat CA de préouverture de session, accédez à **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**.

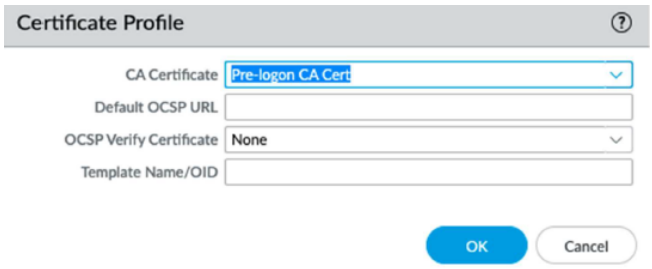
Utilisez cette CA pour valider le certificat machine présenté par le client GlobalProtect lors de l'initialisation du tunnel de préouverture de session.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Créez et nommez le profil. Assurez-vous que le **Username Field (Champ Nom d'utilisateur)** est **None (Vide)** pour empêcher le mappage du certificat à un utilisateur.



STEP 5 | Sous **CA Certificates (Certificats CA)**, sélectionnez **Add (Ajouter)** et sélectionnez **Pre-logon CA Cert (Certificat CA de préouverture de session)** dans la liste déroulante.



STEP 6 | Sélectionnez **OK**, puis sélectionnez **OK** une nouvelle fois.

Configurer le portail GlobalProtect pour la préouverture de session

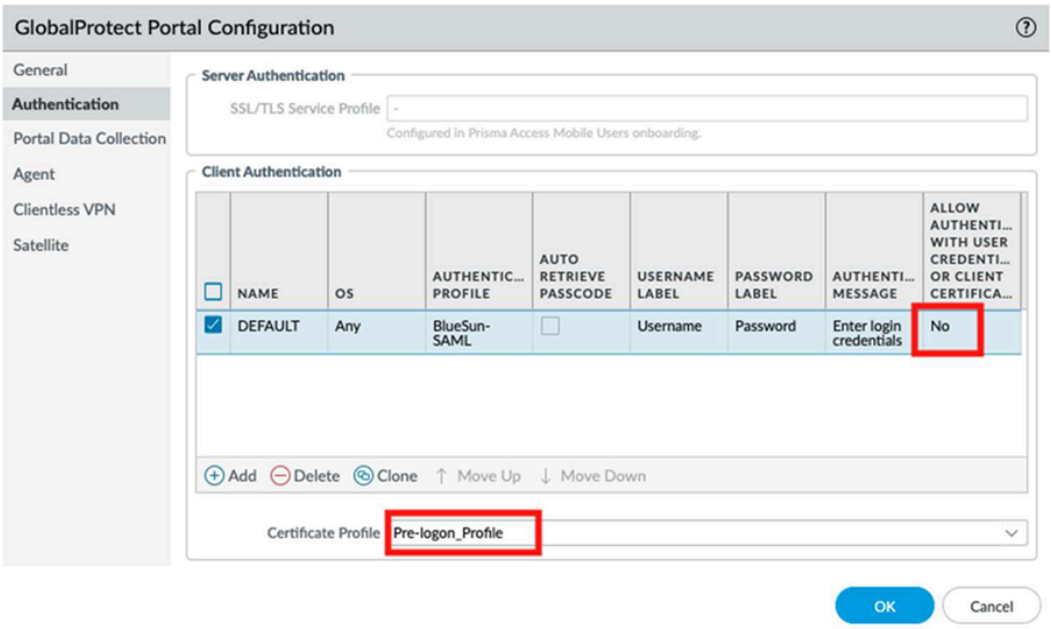
Configurez le portail GlobalProtect pour authentifier les connexions avec un certificat machine.

STEP 1 | Accédez à **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **GlobalProtect_Portal (Portail GlobalProtect)** > **Authentication (Authentification)**.

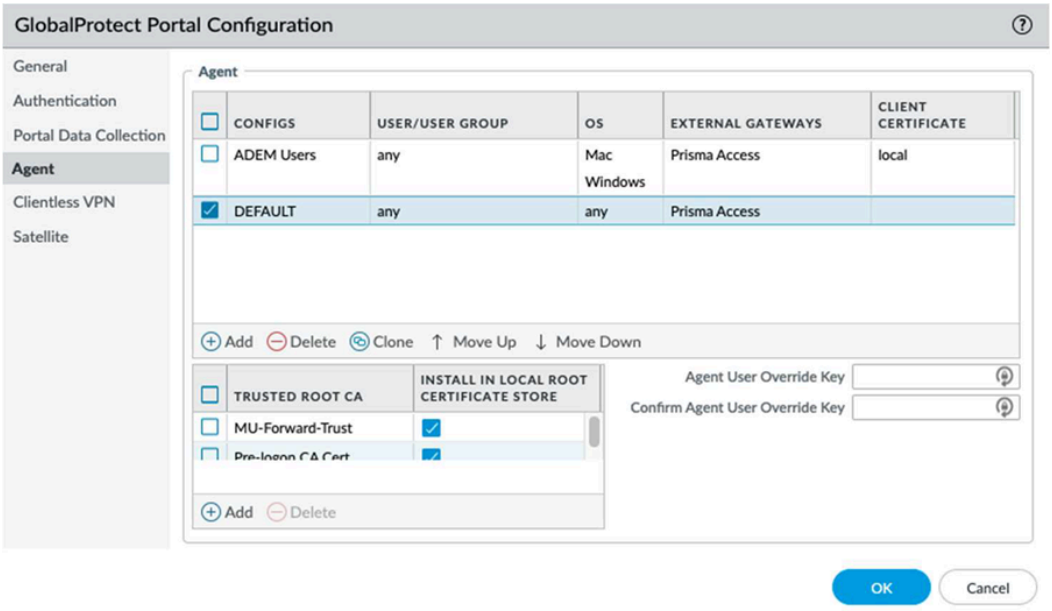
STEP 2 | Sous **Allow Authentication with User Credentials OR Client Certificate (Autoriser l'authentification avec les informations d'identification de l'utilisateur OU le certificat client)**, sélectionnez **No (Non)** pour appliquer uniquement l'authentification basée sur un certificat.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Pour **Certificate Profile (Profil de certificat)**, sélectionnez le **Pre-logon_Profile (Profil de préouverture de session)** que vous avez créé, puis cliquez sur **OK**.



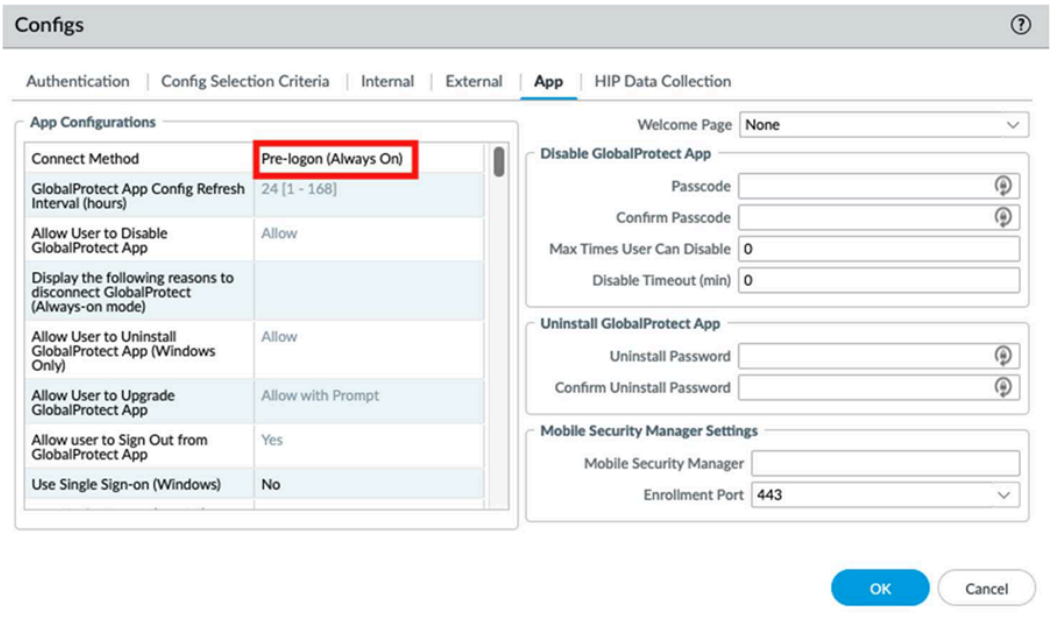
STEP 4 | Sélectionnez **Agent** et ouvrez la configuration de l'Agent pour les utilisateurs authentifiés.



STEP 5 | Sélectionnez l'onglet **App (Applications)**.

 ©2025 Palo Alto Networks, Inc.

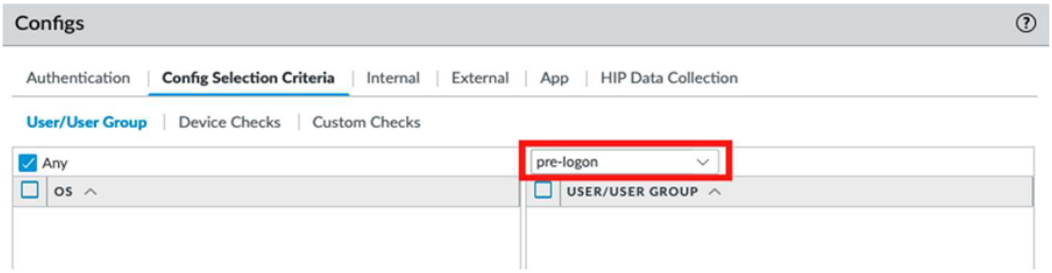
STEP 6 | Sélectionnez **Pre-logon (Always On) (Préouverture de session (Toujours active))**, puis sélectionnez **OK** pour revenir à la zone Agent.



STEP 7 | Dans la zone Agent, **Clone (Clonez)** la configuration par défaut. Remplacez le nom de la configuration par **Pre-logon (Préouverture de session)** pour correspondre à la méthode de connexion pour l'authentification par certificat machine.

STEP 8 | Sélectionnez la configuration de l'agent nouvellement clonée.

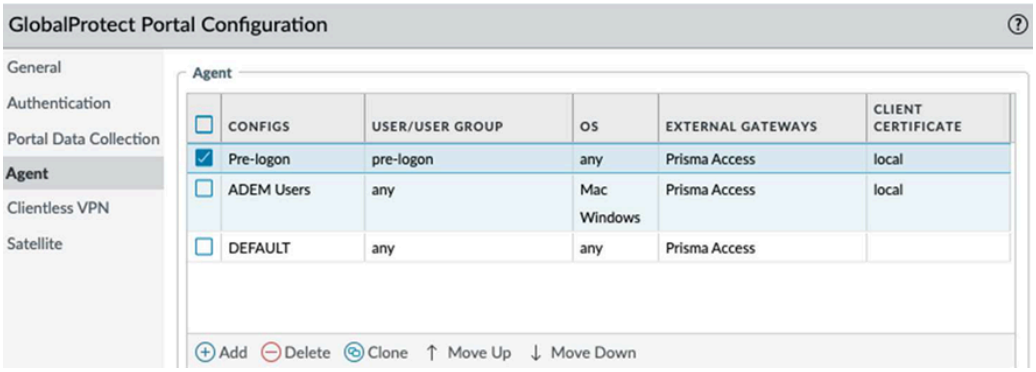
STEP 9 | Sélectionnez **Config Selection Criteria (Critères de sélection de configuration)**. Dans la configuration **User/User Group (Utilisateur/Groupe d'utilisateurs)**, sélectionnez **pre-logon (préouverture de session)** dans la liste déroulante au-dessus de la case de configuration **USER/USER Group (UTILISATEUR/Groupe d'UTILISATEURS)**, et assurez-vous que la configuration est définie sur **Any (Indifférent)**.



STEP 10 | Configurez les paramètres de l'application selon vos besoins et sélectionnez **OK**. Assurez-vous de sélectionner une méthode de connexion préouverture de session pour la configuration de préouverture de session et la configuration actuelle.

 ©2025 Palo Alto Networks, Inc.

STEP 11 | Déplacez la configuration de l'agent de préouverture de session en haut de la liste **CONFIGS (CONFIGURATIONS)** pour vous assurer qu'elle correspond d'abord à la condition de préouverture de session.



STEP 12 | Cliquez sur **OK** pour enregistrer la configuration de client.

Configurer les passerelles GlobalProtect de Prisma Access

Configurez les passerelles GlobalProtect dans Panorama Managed Prisma Access.

Cette configuration applique uniquement l'authentification basée sur un certificat.

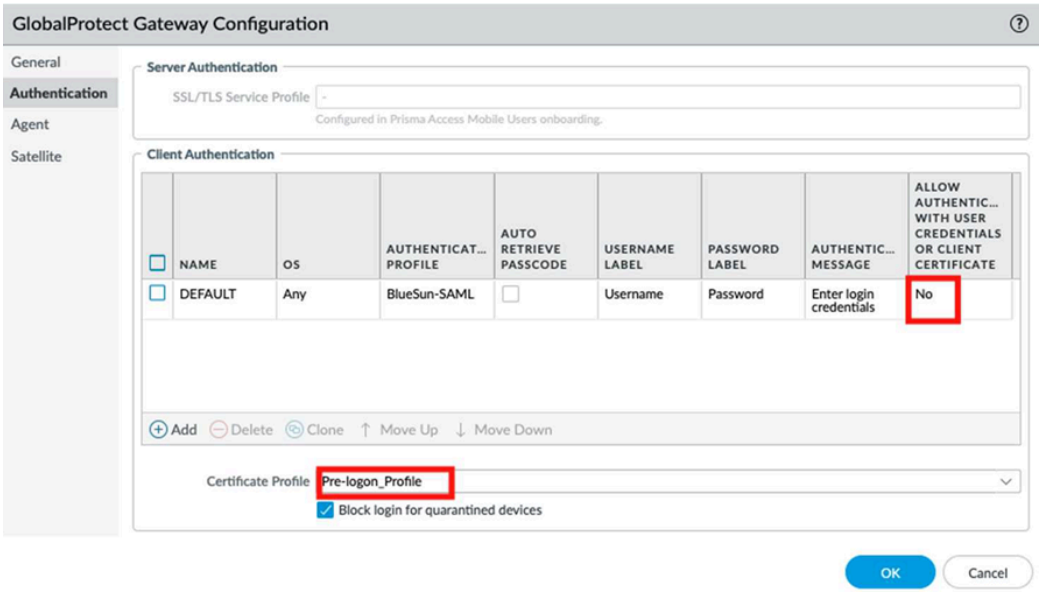
STEP 1 | Accédez à **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > **GlobalProtect_External_Gateway (Passerelle externe GlobalProtect)** > **Authentication (Authentification)**.

STEP 2 | Sélectionnez la méthode d'authentification **Default (Par défaut)**.

Si vous avez déjà configuré une authentification client (telle que SAML), sélectionnez-la à la place de **Default (Par défaut)**.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Sous **Allow Authentication with User Credentials or Client Certificate (Autoriser l'authentification à l'aide des informations d'identification de l'utilisateur ou du certificat client)**, sélectionnez **No (Non)**, puis sélectionnez **OK** pour enregistrer la configuration.



Installer un certificat machine – Windows

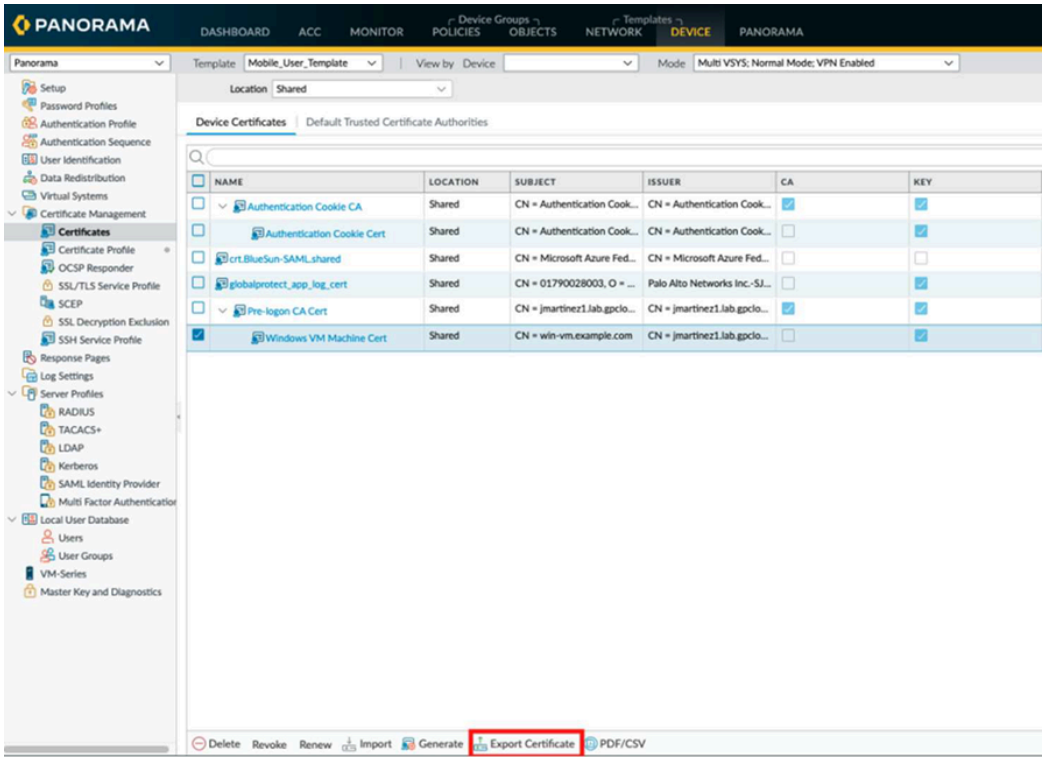
Installez le certificat machine sur les terminaux des utilisateurs mobiles, qui sont utilisés pour l'authentification.

STEP 1 | Accédez à **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**.

STEP 2 | Assurez-vous que vous êtes toujours dans le Mobile_User_Template (Modèle Utilisateur Mobile). Sélectionnez le **Windows VM Machine Cert (Certificat de machine virtuelle**

 ©2025 Palo Alto Networks, Inc.

Windows) que vous avez créé précédemment, puis sélectionnez **Export Certificate (Exporter le certificat)** pour le télécharger sous forme de fichier PKCS12 avec une phrase secrète.



STEP 3 | Exportez le certificat CA de préouverture de session en tant que certificat encodé en base64.

STEP 4 | Transférez les fichiers de certificat sur une machine Windows.

STEP 5 | Installez le certificat CA de préouverture de session racine dans le magasin **Trusted Root Certification Authorities (Autorités de certification racines de confiance)** de votre machine locale.



STEP 6 | Installez le certificat machine de préouverture de session dans l'emplacement du magasin de la machine locale. Complétez les autorisations, puis sélectionnez **Next (Suivant)** pour procéder à l'installation.

STEP 7 | Validez le nom de fichier du certificat, puis sélectionnez **Next (Suivant)**.

STEP 8 | Saisissez le mot de passe, qui est la phrase secrète que vous avez utilisée lors de l'exportation du certificat à partir de Panorama, puis sélectionnez **Next (Suivant)**.

 ©2025 Palo Alto Networks, Inc.

STEP 9 | Dans la boîte de dialogue **Certificate Store (Magasin de certificats)**, sélectionnez **Place all certificates in the following store (Placer tous les certificats dans le magasin suivant)**, puis sélectionnez **Browse (Parcourir)**.

STEP 10 | Sélectionnez le **Personal folder (Dossier personnel)** à l'emplacement où vous souhaitez installer le certificat machine, puis sélectionnez **OK**.

STEP 11 | Sélectionnez **Next (Suivant)** pour procéder à l'installation.

STEP 12 | Connectez-vous au portail GlobalProtect et supprimez tous les cookies de l'hôte.

STEP 13 | (Facultatif) Déconnectez-vous de votre machine et consultez les journaux GlobalProtect pour vérifier la connexion préouverture de session.

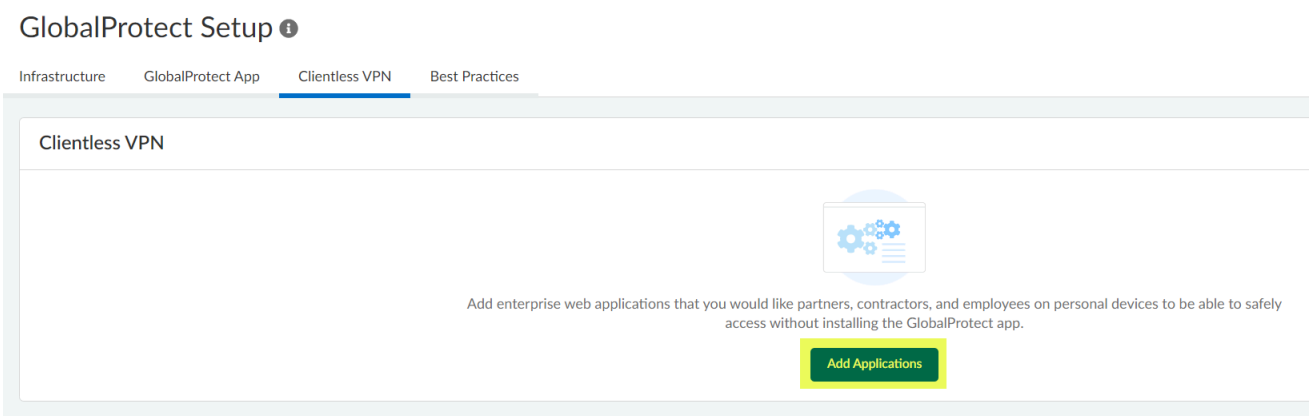
GlobalProtect — VPN sans client

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Le VPN sans client permet un accès à distance sécurisé aux applications d 'entreprise à partir de navigateurs web sur lesquels SSL est activé. Avec un VPN sans client, les utilisateurs finaux ne sont pas obligés d 'installer le logiciel de l 'application GlobalProtect sur leurs terminaux, ce qui est utile lorsque vous devez permettre à un partenaire ou à un sous-traitant d 'accéder aux applications et d 'activer en toute sécurité des actifs non gérés, y compris des terminaux personnels.

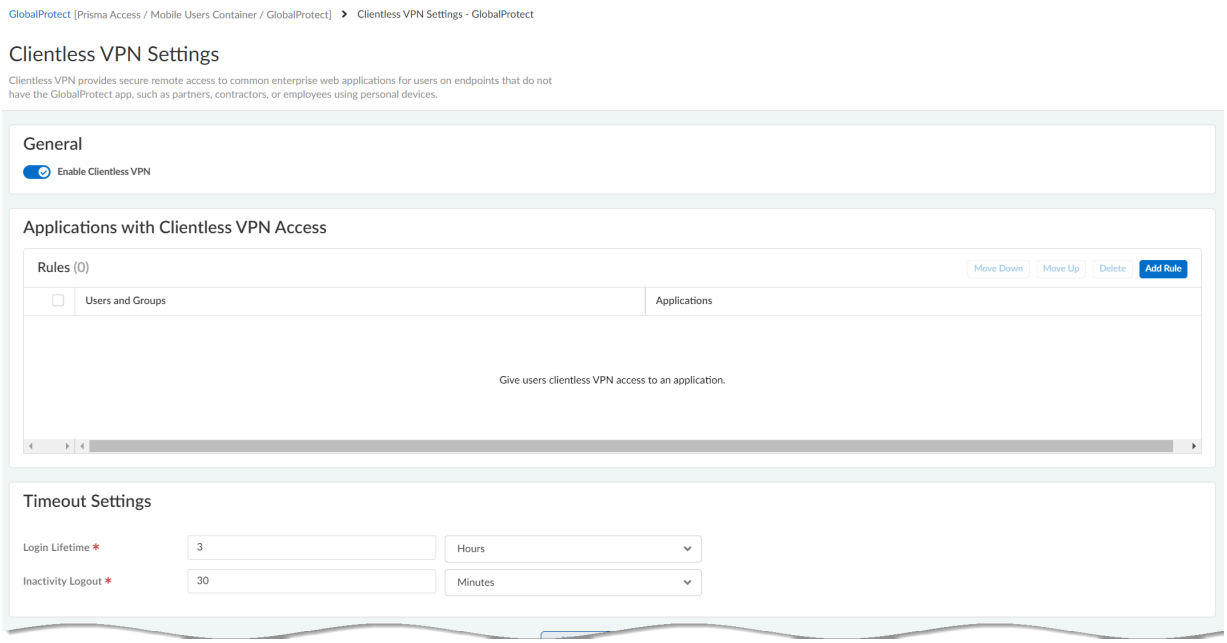
Suivez les étapes suivantes pour configurer un VPN sans client pour Prisma Access :

STEP 1 | Accédez à **Settings (Paramètres)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **GlobalProtect Setup (Configuration de GlobalProtect)** > **Clientless VPN (VPN sans client)** et **Add Applications (Ajouter des applications)**.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Cliquez sur **Enable Clientless VPN (Activer le VPN sans client)**.



STEP 3 | Ajouter des règles de VPN sans client.

Spécifiez les utilisateurs et les applications qui peuvent utiliser le VPN sans client.

STEP 4 | Si les utilisateurs doivent accéder aux applications via un serveur proxy, cliquez sur **Add Proxy (Ajouter un proxy)** pour ajouter un proxy.

Seule l'authentification de base au proxy est prise en charge (nom d'utilisateur et mot de passe). Vous pouvez ajouter plusieurs configurations de serveur proxy, une pour chaque ensemble de domaines. Certains des paramètres à ajouter incluent :

- **Domains (Domaines)** : ajoutez les domaines servis par le serveur proxy. Vous pouvez utiliser un caractère générique (*) au début du nom de domaine pour indiquer plusieurs domaines.
- **Enable Proxy (Activer le proxy)** : affectez un serveur proxy afin de fournir l'accès aux domaines.
- **Server (Serveur)** : spécifiez l'adresse IP ou le nom d'hôte du serveur proxy.
- **Port** : spécifiez un port de communication avec le serveur proxy.
- **User and Password (Utilisateur et mot de passe)** : spécifiez les informations d'identification de l'utilisateur et le mot de passe nécessaires pour se connecter au serveur proxy. Saisissez à nouveau le mot de passe pour le vérifier.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Modifiez les **Crypto Settings (Paramètres de crypto)** par défaut pour spécifier les algorithmes d 'authentification et de cryptage pour les sessions SSL entre Prisma Access et les applications utilisant un VPN sans client.

STEP 6 | Ajoutez des domaines à la **Rewrite Exclude Domain List (Liste des domaines à exclure de la réécriture)**.

Le VPN sans client agit comme un proxy inversé et modifie les pages Web renvoyées par les applications Web publiées. Il réécrit toutes les URL et présente une page réécrite aux utilisateurs à distance de telle sorte que lorsqu 'ils accèdent à l 'une de ces URL, les requêtes passent par le portail GlobalProtect. Dans certains cas, l'application peut avoir des pages qui n'ont pas besoin d'être accessibles via le portail (par exemple, l'application peut inclure un code de titre de yahoo.finance.com). Vous pouvez exclure ces pages. Les domaines que vous ajoutez à la **Rewrite Exclude Domain List (Liste des domaines à exclure de la réécriture)** sont exclus des règles de réécriture et ne peuvent pas être réécrits. Les chemins ne sont pas pris en charge dans les noms de domaine. Le caractère générique (*) pour les noms de domaine ne peut apparaître qu'au début du nom (par exemple, *.etrade.com).

Surveiller les utilisateurs mobiles GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Prisma Access (Managed by Strata Cloud Manager)

Les utilisateurs Prisma Access (Managed by Strata Cloud Manager) peuvent accéder à **Monitor (Surveiller)** > **Users (Utilisateurs)** et sélectionner la méthode de connexion **GlobalProtect** ou **Explicit Proxy (Proxy explicite)**. La page **Mobile Users (Utilisateurs mobiles)** dépend de la méthode de connexion utilisée.

Prisma Access (Managed by Panorama)

Vous pouvez consulter la liste des utilisateurs connectés à plusieurs endroits dans Panorama. Vous pouvez afficher les utilisateurs uniques, l'emplacement auquel les utilisateurs sont connectés et des tableaux qui fournissent des informations supplémentaires. Vous devez également comprendre comment Prisma Access compte le nombre d'utilisateurs à chaque emplacement dans un déploiement de type Utilisateurs mobiles – GlobalProtect.

Vous pouvez obtenir une vue détaillée des utilisateurs à plusieurs endroits :

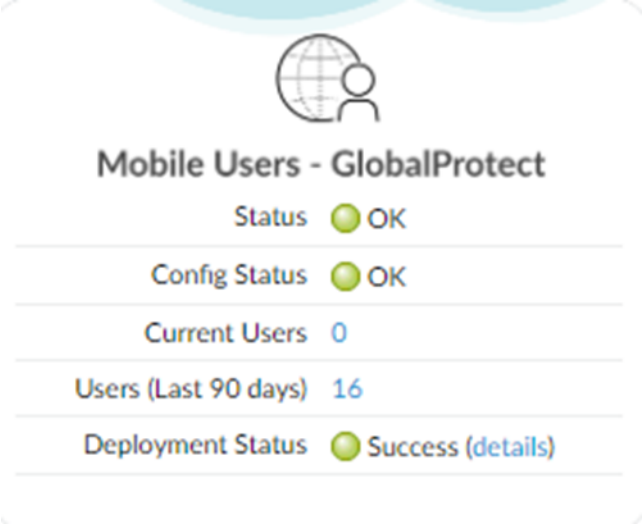
- Pour obtenir une vue globale des utilisateurs et ouvrir un tableau qui vous permet d'afficher et de déconnecter les utilisateurs connectés, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Status (État)**.
- Pour obtenir une vue graphique des utilisateurs dans une carte et afficher les utilisateurs par région et par emplacement, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Service Stats (Statistiques de service)** > **Mobile Users—GlobalProtect (Utilisateurs mobiles – GlobalProtect)**.

 ©2025 Palo Alto Networks, Inc.

- Vous pouvez également en apprendre davantage sur la façon dont Prisma Access compte les utilisateurs mobiles.

Afficher les utilisateurs mobiles GlobalProtect à partir de l'onglet Status (État)

Pour afficher le nombre total d'utilisateurs uniques actuellement connectés sur tous les emplacements, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Status (État)** > **Mobile Users—GlobalProtect (Utilisateurs mobiles – GlobalProtect)**.



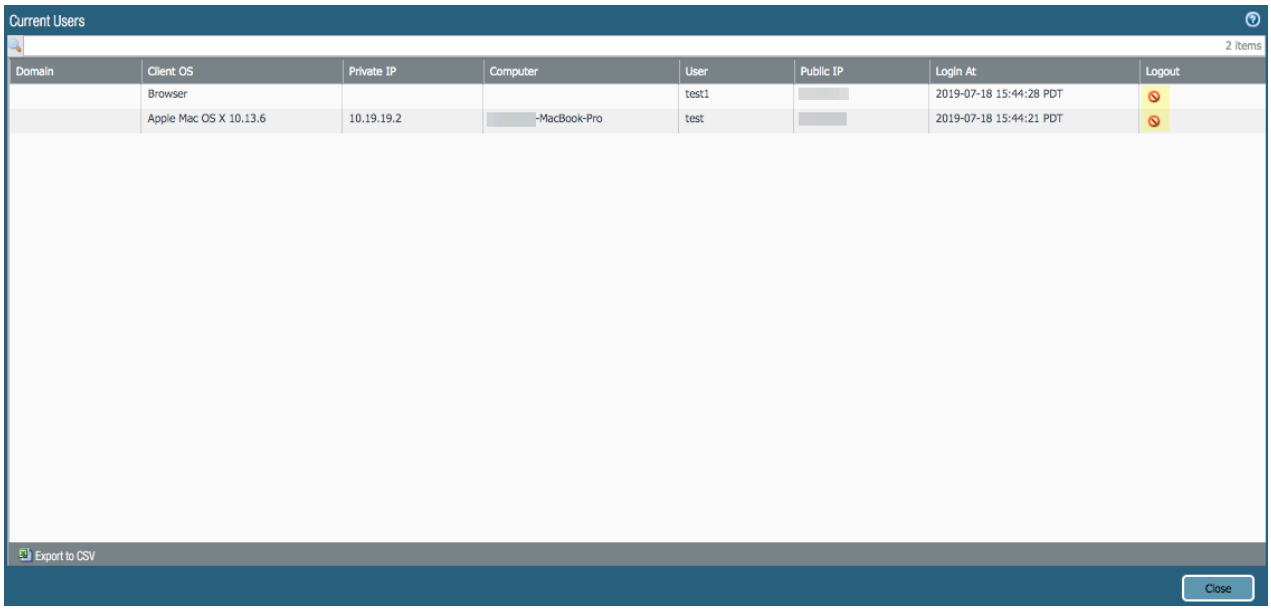
Pour voir plus de détails sur les utilisateurs actuellement connectés, cliquez sur le numéro (lien hypertexte) à côté de **Current Users (Utilisateurs actuels)** pour afficher le tableau **Current Users (Utilisateurs actuels)**.

Le nombre total d'utilisateurs affiché sur la page Status (État) et le nombre affiché dans le tableau contextuel peuvent être différents ; le nombre affiché dans le tableau *peut être plus grand.*

Vous pouvez déconnecter les utilisateurs actifs à partir du tableau **Current Users (Utilisateurs actuels)**. Pour ce faire, sélectionnez l'utilisateur et cliquez sur **Logout (Déconnexion)**. Notez que vous devrez peut-être fermer puis rouvrir l'écran pour que Prisma Access supprime l'utilisateur déconnecté de la page **Current Users (Utilisateurs actuels)**.

L'écran suivant montre les utilisateurs qui se sont connectés avec l'application GlobalProtect et avec le VPN sans client. Il indique le nom d'utilisateur des utilisateurs, l'adresse IP publique et l'heure de la dernière connexion. Si l'utilisateur est connecté avec l'application GlobalProtect, l'écran indique également le système d'exploitation du client, l'adresse IP privée et le nom de l'ordinateur.

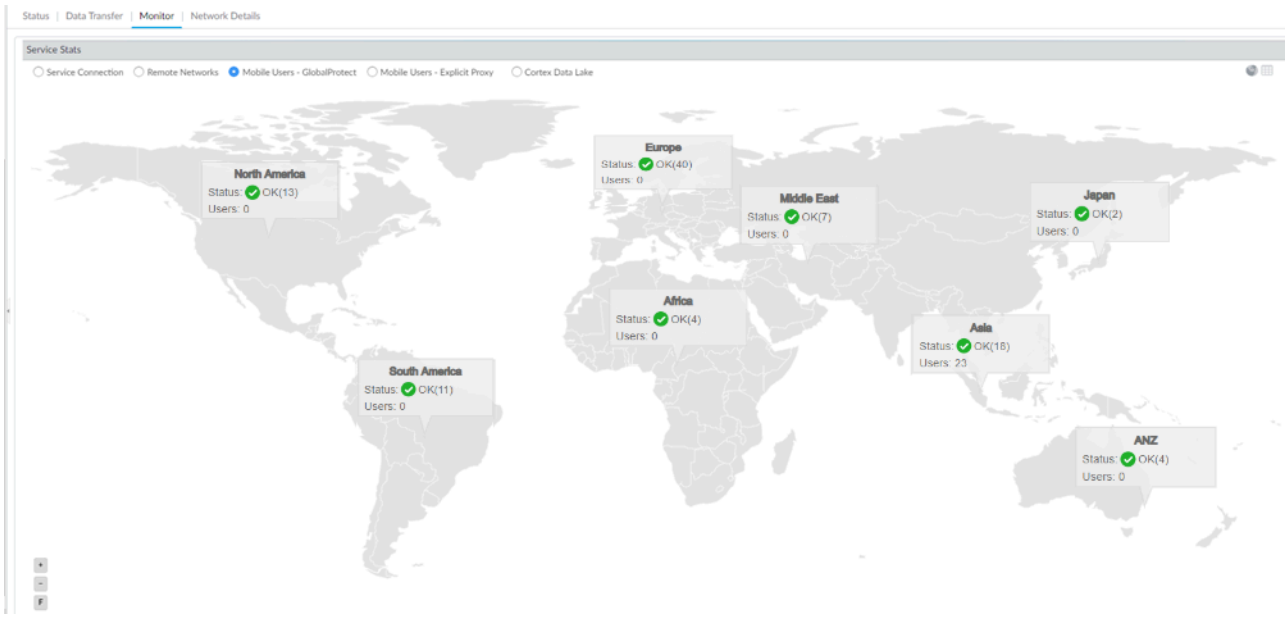
 ©2025 Palo Alto Networks, Inc.



Afficher les utilisateurs mobiles GlobalProtect à partir de l'onglet Monitor (Surveiller)

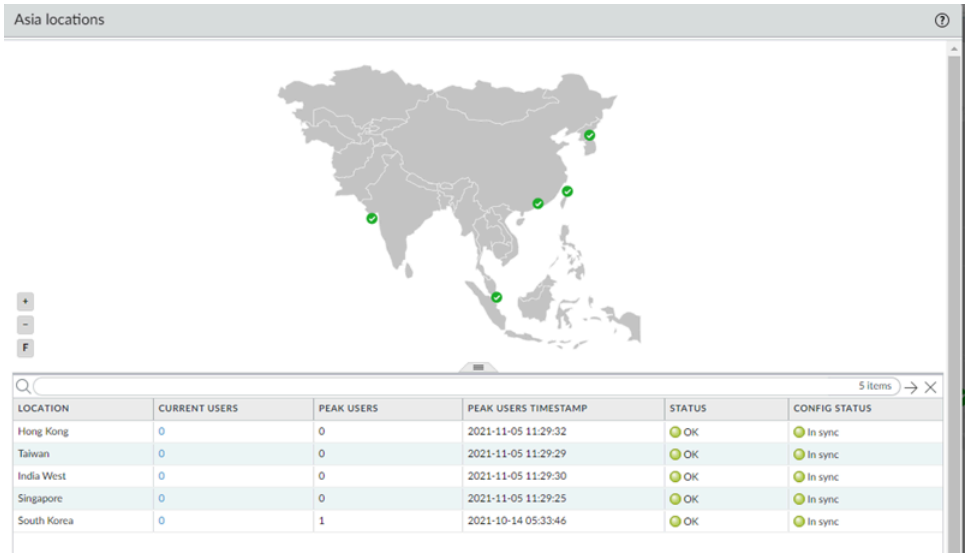
Pour afficher le nombre d'utilisateurs uniques connectés par région, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Service Stats (Statistiques de service)** > **Mobile Users—GlobalProtect (Utilisateurs mobiles – GlobalProtect)**.

 ©2025 Palo Alto Networks, Inc.



Pour afficher les détails des emplacements dans une région, cliquez sur la région.

Le nombre d'utilisateurs affiché sur la carte mondiale et le nombre affiché dans le tableau par région peuvent être différents ; le nombre affiché dans le tableau *peut être plus grand.*



Comment Prisma Access compte les utilisateurs mobiles GlobalProtect

Le nombre total d'utilisateurs affiché dans les zones d'état peut être différent du nombre affiché dans les tableaux associés. La section suivante décrit les différences.

- Onglet **Status (État)** (**Panorama** > **Cloud Services** > **Status (État)** > **Status (État)**) : le nombre d'utilisateurs affiché sur la page principale, dans la zone **Mobile Users—GlobalProtect (Utilisateurs mobiles – GlobalProtect)**, peut être différent du nombre affiché dans le tableau lorsque vous cliquez sur le lien hypertexte **Current Users (Utilisateurs actuels)**. Le nombre affiché dans la zone **Mobile Users—GlobalProtect (Utilisateurs mobiles – GlobalProtect)** compte le nombre d'utilisateurs uniques, tandis que la liste des utilisateurs dans le tableau

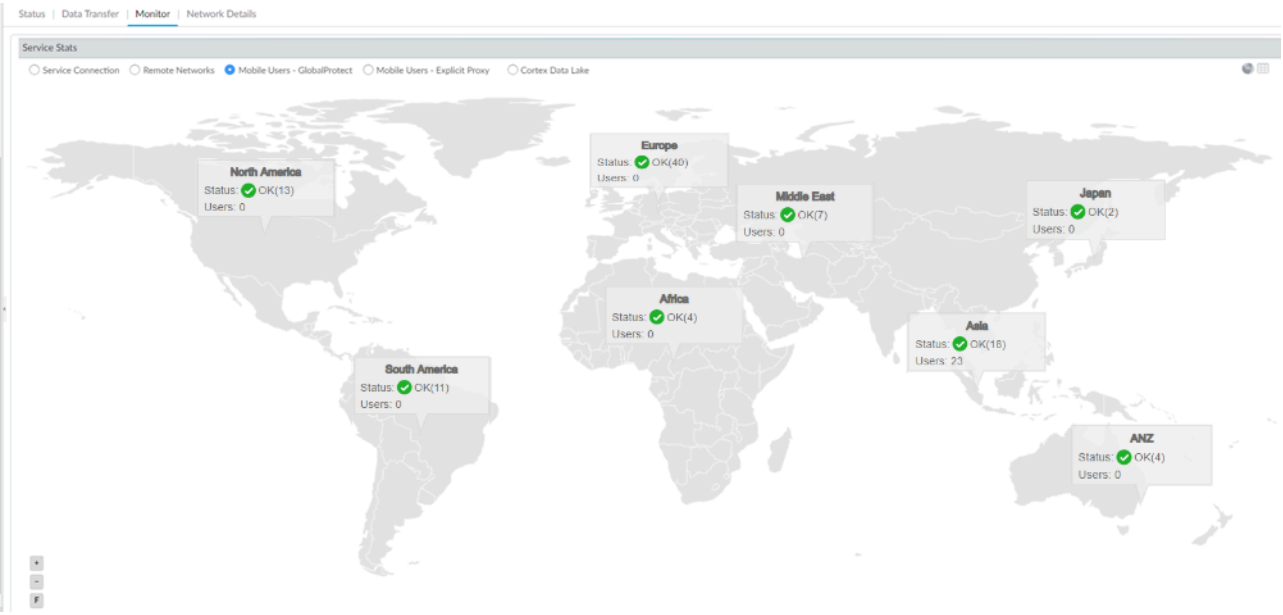
 ©2025 Palo Alto Networks, Inc.

Current Users (Utilisateurs actuels) compte tous les utilisateurs par connexion. Si un même utilisateur est connecté à plusieurs passerelles ou est connecté sur plusieurs périphériques, le nombre dans le tableau peut être plus grand.

Imaginez par exemple que l'utilisateur **user1** est connecté à deux passerelles situées dans l'emplacement **United Kingdom (Royaume-Uni)**, peut-être parce que Prisma Access a automatiquement ajouté des passerelles lorsqu'un grand nombre d'utilisateurs se sont connectés au même emplacement. Dans ce cas, Prisma Access compte **user1** une fois dans la zone **Mobile Users—GlobalProtect (Utilisateurs mobiles – GlobalProtect)**, mais deux fois dans le tableau **Current Users (Utilisateurs actuels)**.

- Onglet **Monitor (Surveiller)** (**Panorama** > **Cloud Services** > **Status (État)** > **Service Stats (Statistiques de service)** > **Mobile Users—GlobalProtect (Utilisateurs mobiles – GlobalProtect)**) : le nombre affiché à côté de **Users (Utilisateurs)** sur la carte mondiale peut être différent du nombre affiché dans le tableau lorsque vous sélectionnez une région. Un utilisateur connecté à plusieurs passerelles ou connecté sur plusieurs périphériques peut apparaître plusieurs fois dans le tableau.

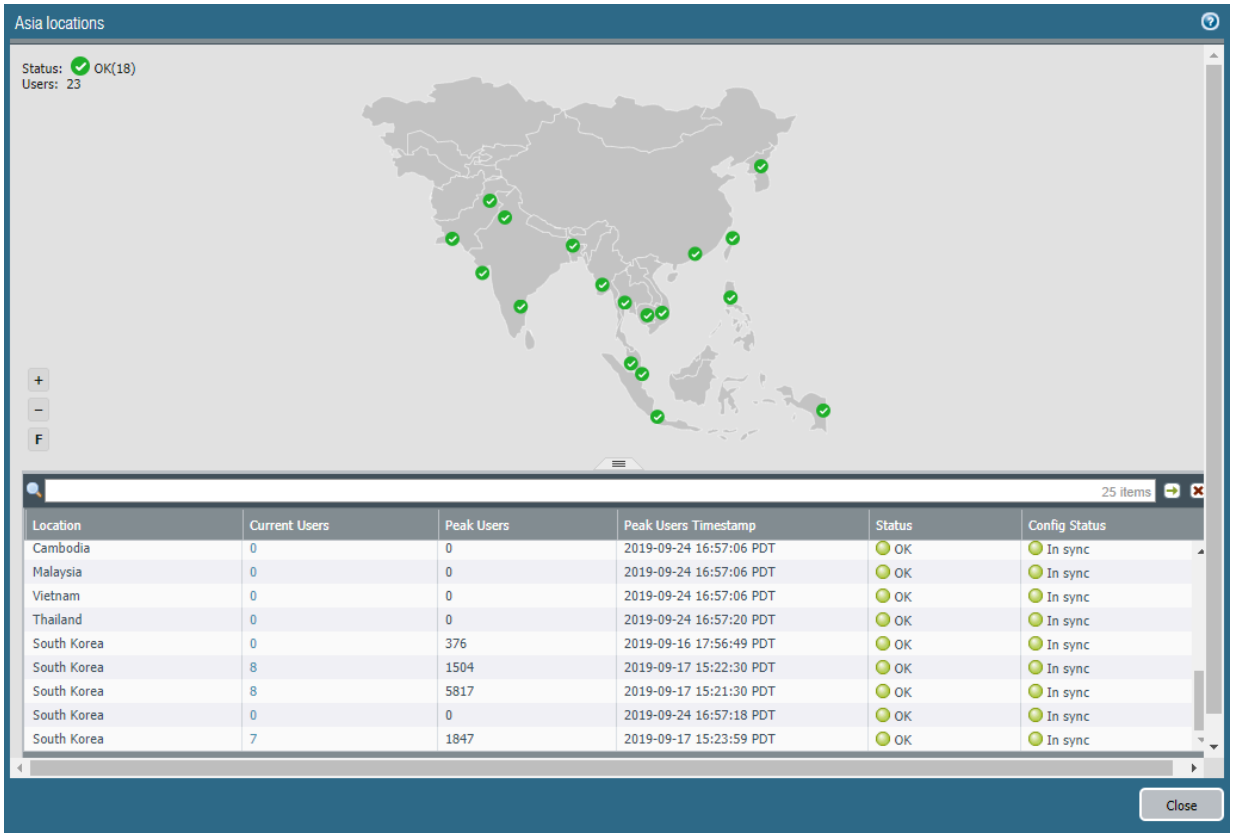
  Les captures d'écran suivantes fournissent un exemple. Comme le montre la carte mondiale, 23 utilisateurs uniques sont connectés à la région **Asia (Asie)**.



Si vous sélectionnez la région **Asia (Asie)**, Prisma Access affiche le nombre d'utilisateurs uniques (23) en haut à gauche de la page de la région. Cependant, deux utilisateurs sont connectés via plusieurs périphériques dans l'emplacement **South Korea (Corée du Sud)** (par exemple, sur un smartphone et un ordinateur). Comme les utilisateurs ont deux connexions

 ©2025 Palo Alto Networks, Inc.

distinctes, Prisma Access les compte deux fois dans le tableau, ce qui donne un nombre total de 25 dans le tableau.



 ©2025 Palo Alto Networks, Inc.

Pools d'adresses IP pour un déploiement de type Utilisateurs mobiles – GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Assurez-vous d'avoir spécifié un pool d'adresses IP qui permet une couverture suffisante pour les utilisateurs mobiles de votre organisation. Notez bien que chaque utilisateur unique peut utiliser plusieurs périphériques en même temps pour se connecter à Prisma Access, et que chaque périphérique connecté nécessite une adresse IP unique du pool. Les adresses de ce pool ne doivent pas chevaucher d'autres pools d'adresses que vous utilisez en interne ou le sous-réseau IP que vous attribuez lorsque vous activez l'infrastructure de service.

Nous vous recommandons d'avoir un nombre d'adresses IP dans le pool 2 fois supérieur au nombre de périphériques d'utilisateurs mobiles qui se connecteront à Prisma Access. Si votre organisation dispose d'une politique BYOD (Bring Your Own Device, apportez votre propre périphérique) ou si un utilisateur unique possède plusieurs comptes utilisateur, veillez à tenir compte de ces appareils et comptes supplémentaires lorsque vous allouez des pools d'adresses IP. Si l'espace de pool est limité, vous pouvez spécifier un pool d'adresses plus petit. Toutefois, si le pool d'adresses IP atteint sa limite, les périphériques d'utilisateurs mobiles supplémentaires ne pourront pas se connecter.

L'interface utilisateur vérifie que vous entrez des sous-réseaux IP valides (par exemple, si vous entrez un pool avec un sous-réseau inférieur à /23, il vous sera demandé de le modifier). Cependant, elle ne vérifie pas que vous avez alloué suffisamment d'adresses IP pour le déploiement.

Cette validation n'est pas disponible si vous configurez des emplacements à l'aide de la CLI. Si vous déployez tous les emplacements à l'aide de la CLI, nous vous recommandons d'ajouter une adresse /18 au pool mondial pour les utilisateurs mobiles.

Prisma Access contrôle votre configuration pour vérifier que vous avez spécifié le pool d'adresses IP minimal suivant :

- Un minimum de /23 (512 adresses IP) est requis pour un pool d'adresses mondial ou régional.
- Si un emplacement existant est converti en emplacement de calcul, il aura besoin d'un sous-réseau /23 au minimum après la conversion.
- Si vous n'intégrez aucune passerelle Prisma Access dans une région, vous n'avez pas besoin d'un pool d'adresses IP pour cette région. Par exemple, si vous spécifiez des passerelles dans les emplacements USA Est, USA Nord-Ouest et USA Nord-Est, vous devez uniquement spécifier un pool d'adresses IP pour la région Amérique du Nord et Amérique du Sud. À l'inverse, si vous activez des emplacements d'utilisateurs mobiles en Europe sans spécifier un pool d'adresses mondial ou un pool d'adresses IP dans la région Afrique, Europe et Moyen-Orient, le déploiement échouera.

 ©2025 Palo Alto Networks, Inc.

- Les utilisateurs mobiles GlobalProtect consomment d'abord les adresses IP dans le groupe d'emplacements, puis les adresses IP spécifiques d'un théâtre, puis les adresses IP mondiales. Par exemple, si vous spécifiez un pool pour un groupe d'emplacements et pour le pool mondial, et que vous épuisez ensuite les adresses IP disponibles dans le pool de groupes d'emplacements, Prisma Access prend des adresses IP du pool **Worldwide (Mondial)** pour les utiliser dans ce groupe d'emplacements.

  Si vous spécifiez plusieurs blocs de pools d'adresses IP, Prisma Access utilise les pools dans l'ordre dans lequel vous les avez saisis lors de la configuration des utilisateurs mobiles.

Allocation d'adresse IP statique pour les utilisateurs mobiles : déploiements GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access version 5.2.1 • Version 11.2.4 du plan de données PAN-OS inclut Activity Insights (Informations sur l'activité), User Group (Groupe d'utilisateurs) et Location Group (Groupe d'emplacements) • GlobalProtect Version 6.1.4 *Il s'agit d'une version à disponibilité limitée. Pour activer cette fonctionnalité, contactez votre représentant de compte Palo Alto Networks après avoir activé le locataire.*

Certains réseaux existants utilisent une autorisation basée sur l'adresse IP pour restreindre l'accès des utilisateurs aux ressources internes ou externes. Un déploiement de GlobalProtect Prisma Access pour les utilisateurs mobiles attribue aux utilisateurs une adresse IP à partir du pool d'adresses IP des utilisateurs mobiles que vous attribuez lors de l'intégration, et ce mappage d'adresse IP à un utilisateur peut changer lors des connexions ultérieures. Pour conserver le mappage d'adresse IP à un utilisateur, Prisma Access permet d'attribuer des adresses IP statiques aux utilisateurs.

Cette fonctionnalité est disponible pour les nouveaux déploiements Prisma Access uniquement.

Pour créer un profil de Pool d'adresses IP, utilisez un ou plusieurs de ces critères :

- **Théâtre** : attribuez des adresses IP en fonction du théâtre dans lequel se trouvent vos utilisateurs. Par exemple, vous pouvez créer un sous-réseau /30 pour un théâtre spécifique. Ces adresses IP sont statiques pour ce théâtre. Vous pouvez appliquer l'accès aux ressources

 ©2025 Palo Alto Networks, Inc.

en fonction du théâtre en créant des règles de politique de sécurité à l'aide des adresses IP que vous spécifiez pour ce théâtre.

- **Utilisateur** : allouez des adresses IP en fonction d'un ID utilisateur en configurant une adresse /30 ou /32 dans le pool d'adresses IP d'utilisateur mobile et en utilisant des critères de correspondance pour associer cet utilisateur à une adresse IP. De cette façon, vous attribuez une adresse IP statique que Prisma Access conserve pour un utilisateur spécifique, vous permettant de conserver vos règles de politique de sécurité basées sur l'adresse IP actuelle pour contrôler l'accès d'un utilisateur aux ressources.
- **Groupe d'utilisateurs** : allouez des adresses IP en fonction du groupe d'utilisateurs. L'utilisateur obtiendra l'adresse IP du sous-réseau du pool d'adresses IP défini s'il fait partie du groupe d'utilisateurs configuré.
- **Groupe d'emplacements** : allouez des adresses IP en fonction du groupe d'emplacements défini dans le profil de pool d'adresses IP.

Utilisez les directives suivantes lors de l'attribution d'adresses IP statiques :

- Si vous spécifiez plusieurs pools d'adresses IP, Prisma Access évalue les règles de haut en bas et attribue des adresses IP en fonction de la première correspondance dans la liste des règles.
- Intégrez votre déploiement Prisma Access avec Cloud Identity Engine si vous souhaitez utiliser l'ID utilisateur ou le groupe d'utilisateurs comme critère pour faire correspondre les pools d'adresses IP.
- Les allocations maximales suivantes sont prises en charge par locataire :
  - 20 000 utilisateurs
  - 5 000 groupes d'utilisateurs avec 50 000 utilisateurs par groupe d'utilisateurs
  - 10 000 profils de pool d'adresses IP
  - 10 000 pools d'adresses IP
- Entrez une longueur de préfixe comprise entre /23 et /32.
- Pour chaque profil **Client IP Pool (Pool d'adresses IP de client)** d'utilisateur mobile que vous créez :
  - Jusqu'à 10 préfixes IP pris en charge.
  - Jusqu'à 256 utilisateurs pris en charge.

 ©2025 Palo Alto Networks, Inc.

- L'adresse IP statique utilise une **Lease Period (Période de location)** et une **Grace Period (Période de grâce)** pour spécifier la durée pendant laquelle Prisma Access conserve une association utilisateur-adresse IP.
  - La **Lease Period (Période de location)** correspond à la durée pendant laquelle le mappage utilisateur-adresse IP est valide après son allocation.

    La période de location par défaut est de 86 400 secondes (24 heures).

    La durée minimale de location est de 3 600 secondes (1 heure).

    La durée maximale de location est de 7 776 000 secondes (90 jours).
  - La **Grace Period (Période de grâce)** est la durée pendant laquelle, après l'expiration d'une période de location, Prisma Access conserve ce mappage utilisateur-adresse IP sans l'attribuer à un autre utilisateur.

    La période de grâce par défaut est de 14 400 secondes (4 heures).

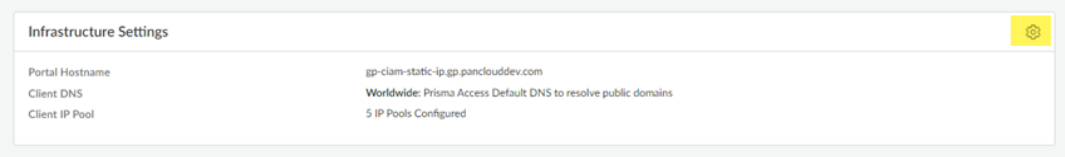
    Le délai de grâce minimum est de 60 secondes.

    La période de grâce maximale est de 7 776 000 secondes (90 jours).

Configurer l'allocation d'adresse IP statique

Pour configurer une allocation d'adresse IP statique dans un déploiement , procédez comme suit.

STEP 1 | Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** et cliquez sur l'engrenage pour mettre en surbrillance les **Infrastructure Settings (Paramètres d'infrastructure)**.



STEP 2 | Dans le pool d'adresses IP client, cliquez sur **Add IP Pool (Ajouter un pool d'adresses IP)** pour les adresses IP statiques.

STEP 3 | Attribuer une adresse IP statique à un théâtre, un groupe d'emplacements Prisma Access ou un utilisateur.

1. Donnez au pool d'adresses IP un **Name (Nom)** unique.
2. **Select (Sélectionnez)** un ou plusieurs **Theatres (Théâtres)** pour autoriser l'utilisation du pool dans ces théâtres, ou sélectionnez **Any (N'importe lequel)** pour autoriser l'utilisation du pool dans tous les théâtres.
3. **Select (Sélectionnez)** un ou plusieurs **Prisma Access Location Groups (Groupes d'emplacements Prisma Access)** pour autoriser l'utilisation du pool dans ce groupe

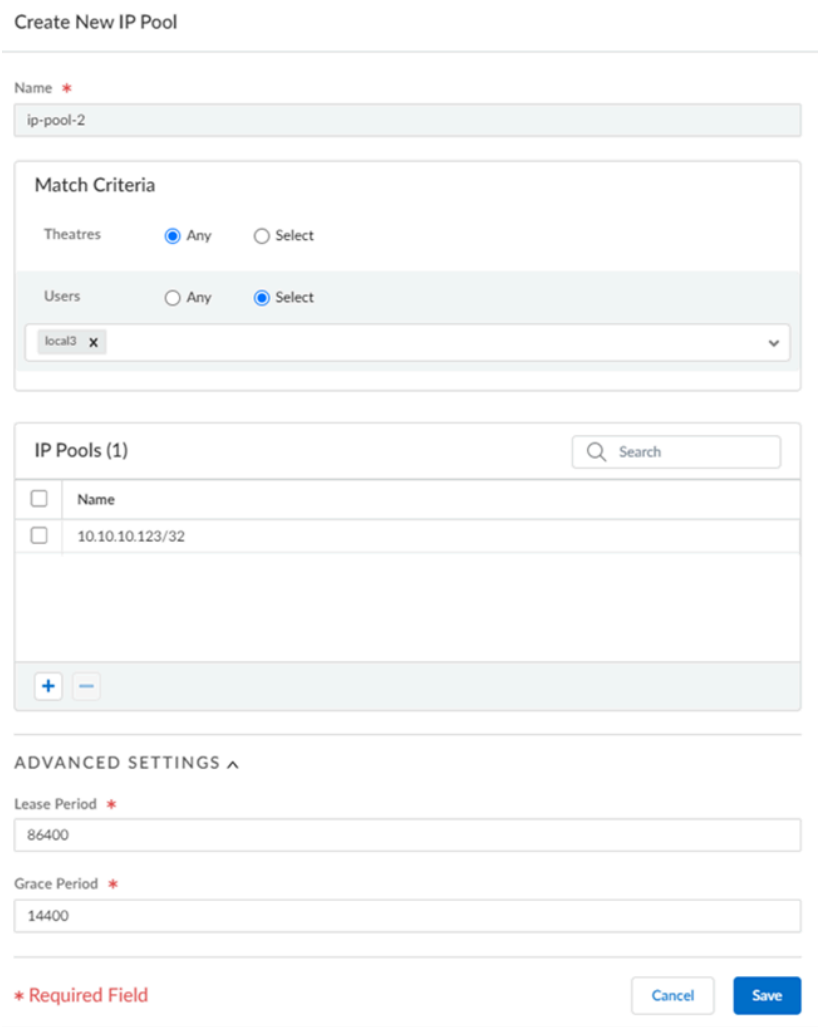
 ©2025 Palo Alto Networks, Inc.

d'emplacements, ou sélectionnez **Any (Tout)** pour autoriser l'utilisation du pool dans tous les groupes d'emplacements.

4. **Select (Sélectionnez)** un utilisateur ou un groupe d'utilisateurs, ou sélectionnez **Any (Tout)** pour autoriser l'utilisation du pool pour n'importe quel utilisateur ou groupe d'utilisateurs.
   - Pour affecter un ou plusieurs utilisateurs à un pool d'adresses IP, sélectionnez l'utilisateur dans l'onglet **Users (Utilisateurs)**.
   - Pour affecter un ou plusieurs groupes d'utilisateurs à un pool d'adresses IP, sélectionnez l'utilisateur dans l'onglet **User Groups (Groupes d'utilisateurs)**.
5. Dans la zone **IP Pools (Pools d'adresses IP)**, entrez un pool d'adresses IP.

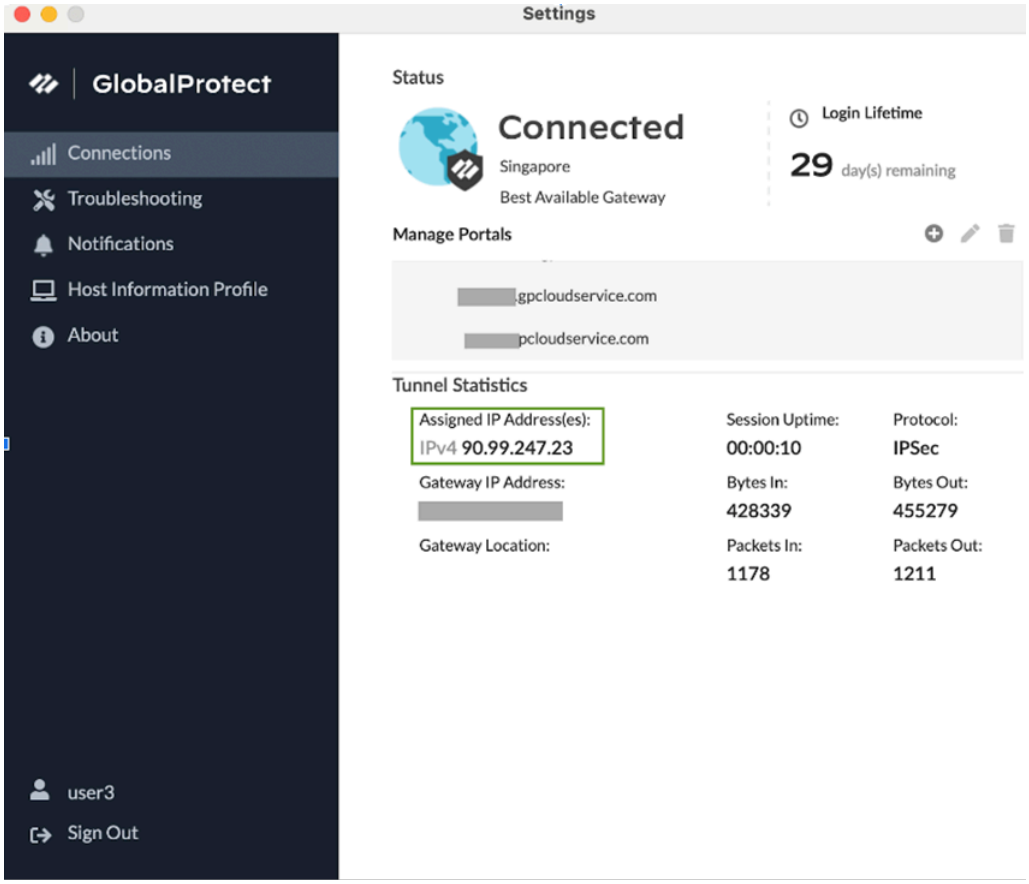
   Pour limiter un utilisateur à une seule adresse IP, spécifiez une adresse IP /30 ou /32 ; Prisma Access attribue l'utilisateur à cette adresse. Étant donné qu'un sous-réseau /32 ne fournirait qu'une seule adresse IP, nous recommandons un sous-réseau minimum de /30 et de restreindre l'utilisateur à ce sous-réseau.
6. (Facultatif) Entrez une **Lease Period (Période de location)** et une **Grace Period (Période de grâce)** pour le mappage utilisateur-adresse IP.
7. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Vérifiez vos modifications en accédant aux **GlobalProtect** > **Settings** sur la machine client, en affichant les **Tunnel Statistics (Statistiques du tunnel)**et en vérifiant les **Assigned IP Address(es) (Adresses IP attribuées)**.



Comment l'application GlobalProtect sélectionne des emplacements Prisma Access pour les utilisateurs mobiles

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Lorsqu'un utilisateur mobile se connecte à un emplacement Prisma Access, l'application utilise le processus de sélection suivant pour déterminer à quel emplacement il se connecte.

Vous activez les emplacements d'utilisateur mobile où vous souhaitez que Prisma Access soit présent pendant l'intégration de l'utilisateur mobile. Si vous ne sélectionnez pas l'emplacement lors de l'intégration, Prisma Access ne l'utilise pas dans votre déploiement.

- Si l'utilisateur mobile se connecte dans un pays qui dispose d'un emplacement Prisma Access, l'utilisateur se connecte à l'emplacement dans ce pays.

 ©2025 Palo Alto Networks, Inc.

- Si l'utilisateur mobile ne peut pas se connecter à un emplacement dans le pays pour une raison quelconque, Prisma Access sélectionne l'un des emplacements d'utilisateurs mobiles suivants pour connecter l'utilisateur en fonction de la région.
  - **Asie, Australie et Japon** : Hong Kong, Japon Centre ou Japon Sud
  - **Afrique, Europe et Moyen-Orient** : Pays-Bas Centre
  - **Amérique du Nord et Amérique du Sud** : États-Unis Nord-Ouest

  Palo Alto Networks vous recommande d'activer au moins l'un de ces emplacements dans leurs régions respectives lors de l'intégration des utilisateurs mobiles afin d'assurer la redondance. Si vous avez des utilisateurs mobiles qui se connectent à Prisma Access depuis un pays qui n'a pas d'emplacement Prisma Access, vous devez activer au moins l'un des emplacements de repli de la liste précédente.

  Les emplacements de Hong Kong, du Centre du Japon, du Sud du Japon, du Pays-Bas Centre et des États-Unis Nord-Ouest peuvent accepter des connexions client de n'importe où et sont connus sous le nom de *Emplacements de repli mondiaux*. En plus de ces emplacements, vous pouvez activer un ou plusieurs des emplacements suivants qui servent également d'emplacements de repli mondiaux :
  - Bahreïn
  - France Nord
  - Irlande
  - Afrique du Sud Ouest
  - Corée du Sud
- Palo Alto Networks vous recommande d'activer les emplacements dans plus d'un emplacement de calcul à des fins de redondance.
- Si vous utilisez des passerelles sur site avec des emplacements Prisma Access, vous pouvez spécifier des priorités dans Prisma Access pour permettre aux utilisateurs mobiles de se connecter à une passerelle GlobalProtect sur site spécifique ou à un emplacement Prisma Access. Reportez-vous à la section Gérer les priorités pour Prisma Access et les passerelles sur site pour plus de détails.
- Lorsque les utilisateurs mobiles se connectent, l'application GlobalProtect n'utilise pas les emplacements Prisma Access suivants dans le processus de sélection automatique de passerelle, même si vous avez sélectionné les emplacements Prisma Access dans le plug-in lors de l'intégration. Cependant, les utilisateurs mobiles peuvent toujours sélectionner manuellement l'un de ces emplacements et le définir comme emplacement préféré (passerelle) tant que vous les autorisez à sélectionner manuellement ces emplacements lors de l'intégration de l'utilisateur mobile :
  - Australie : Est de l'Australie
  - Brésil : Brésil Est et Brésil Centre
  - France : France Sud
  - Allemagne : Allemagne Nord et Allemagne Sud
  - Inde : Inde Sud
  - Mexique : Mexique Ouest
  - Pays-Bas : Pays-Bas Sud

 ©2025 Palo Alto Networks, Inc.

- Pakistan : Pakistan Ouest
- Russie : Russie Nord-Ouest
- Espagne : Espagne Est

*Vous devrez peut-être modifier votre **Connect Method (Méthode de connexion)** par **On-Demand (À la demande)** pour que l'utilisateur mobile se connecte manuellement à une passerelle.*

Liste d'autorisation des utilisateurs mobiles de GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version : 3.0 Préféré

Découvrez comment activer les listes d'adresses IP de sortie autorisées pour les utilisateurs mobiles existants.

Pour vous permettre d'ajouter les adresses IP publiques (de sortie) pour votre déploiement de GlobalProtect — Utilisateur mobile dans les listes d'autorisation de n'importe quelle application SaaS que vous utilisez au sein de votre organisation, Prisma Access fournit les adresses IP et vous permet de vérifier que vous les avez ajoutées à votre liste d'autorisation avant de les utiliser dans votre environnement. Si vous activez les listes d'adresses IP de sortie autorisées pour des déploiements Prisma Access existants, Prisma Access migre toutes les adresses IP de sortie déjà allouées à vos emplacements vers les listes d'adresses IP de sortie autorisées. Pour les nouveaux déploiements de Prisma, activez la liste d'adresses IP de sortie autorisées lors de l'intégration des utilisateurs mobiles Global Protect.

Après avoir ajouté les adresses IP de sortie aux listes d'autorisation de votre organisation, vous revenez à l'interface utilisateur Prisma Access, vérifiez que les adresses IP de sortie de GlobalProtect sont répertoriées comme étant autorisées et sélectionner **Push (Appliquer)** pour appliquer vos modifications. Prisma Access libère ensuite ces adresses IP de sortie et les ajoute à votre déploiement. Si Prisma Access ajoute d'autres adresses IP après la configuration initiale à la suite d'un événement de mise à l'échelle automatique, vous confirmez que les nouvelles adresses IP de sortie ont été ajoutées avant que Prisma Access les ajoute à votre déploiement.

Une fois activé, le tableau de la liste d'adresses IP de sortie autorisées fournit des informations sur les adresses IP confirmées ou à confirmer, ainsi que sur leur état d'approvisionnement.

- Strata Cloud Manager
- Panorama

Liste d'autorisation des utilisateurs mobiles de GlobalProtect (Strata Cloud Manager)

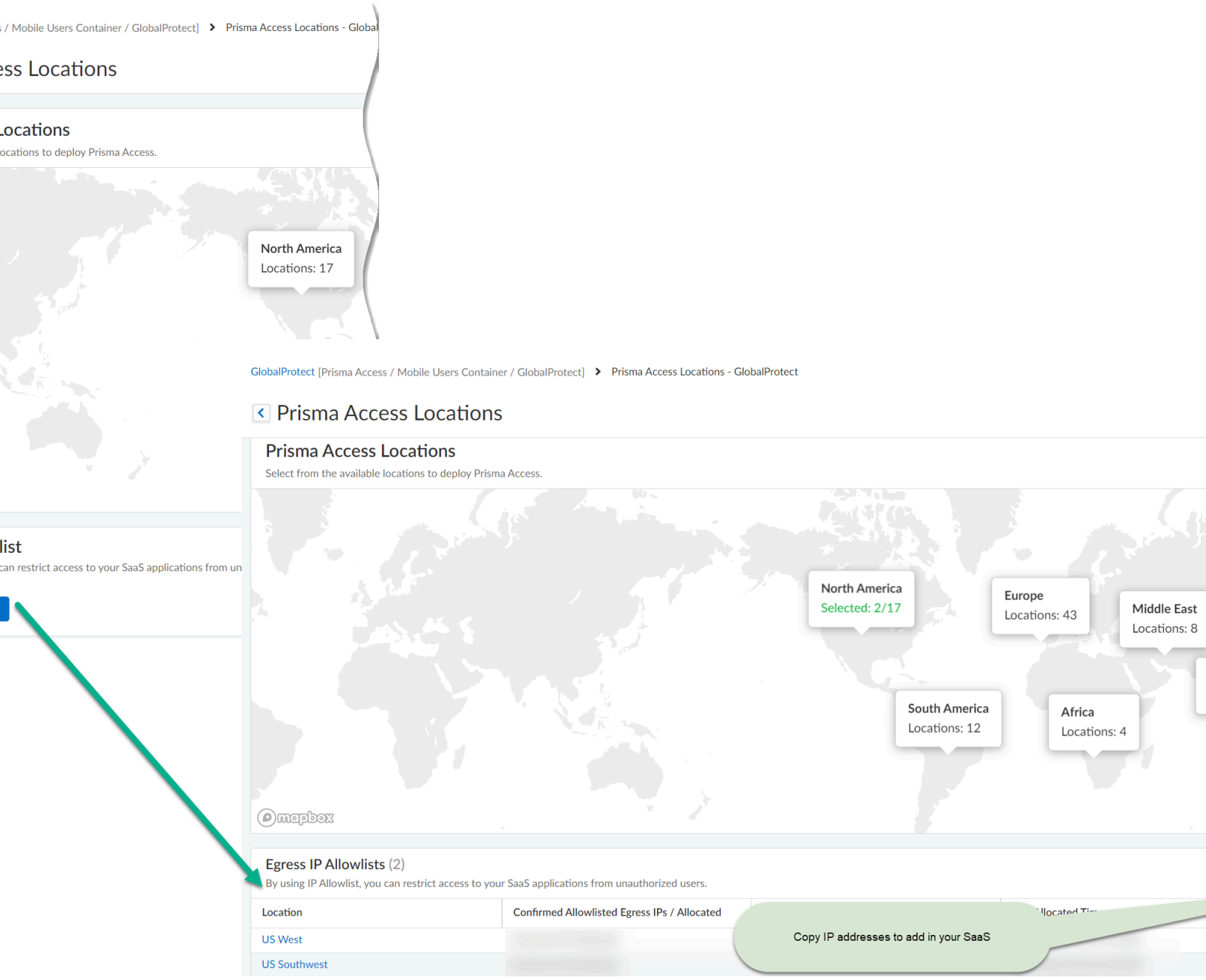
Activer Prisma Access pour afficher les adresses IP de sortie pour le trafic Prisma Access. Utilisez ces adresses IP dans les listes d'adresses IP autorisées pour vos applications SaaS, où vous limitez l'utilisation aux utilisateurs ou sources autorisés.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Allez dans **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **Infrastructure** et modifiez **Prisma Access Locations (Emplacements Prisma Access)**.

STEP 2 | Affichez les adresses IP des emplacements Prisma Access.

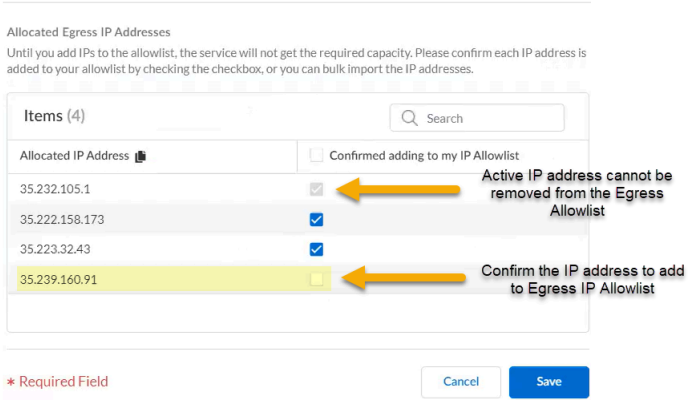
1. Cliquez sur **Enable (Activer)** la liste d'adresses IP de sortie autorisées pour les emplacements Prisma Access intégrés.
2. Copiez et ajoutez les adresses IP allouées aux listes d'autorisation de vos applications SaaS.
3. Cliquez sur **Migrate (Migrer)** pour confirmer les adresses IP allouées aux emplacements intégrés dans Prisma Access.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Récupérez les adresses IP du nouvel emplacement intégré ou lors d'un événement de mise à l'échelle automatique.

1. Sélectionnez le nom de **Location (Emplacement)** pour rechercher les nouvelles adresses IP de sortie allouées à l'emplacement.
2. Sélectionnez **Confirmed adding to my IP Allowlist (Confirmer l'ajout à ma liste d'adresses IP autorisées)** pour ajouter ces adresses IP aux listes d'autorisation de vos applications Saas avant de les confirmer dans Prisma Access.



Si vous avez des adresses IPv6, sélectionnez **Confirmed adding to my IPv6 Allowlist (Confirmer l'ajout à ma liste d'adresses IPv6 autorisées)**.



STEP 4 | Appliquez vos modifications à Prisma Access.

États des adresses IP de sortie allouées

La colonne d'état des listes d'adresses IP de sortie autorisées indique si toutes les adresses IP allouées aux emplacements sont approvisionnées pour votre déploiement. Lisez la suite pour en savoir plus sur chaque état.

- **Provisioned (Approvisionnée)** : vous avez ajouté les adresses IP de sortie aux listes d'autorisation de vos applications SaaS, confirmé les adresses IP dans Prisma Access et appliqué vos modifications pour qu'elles soient entièrement approvisionnées.

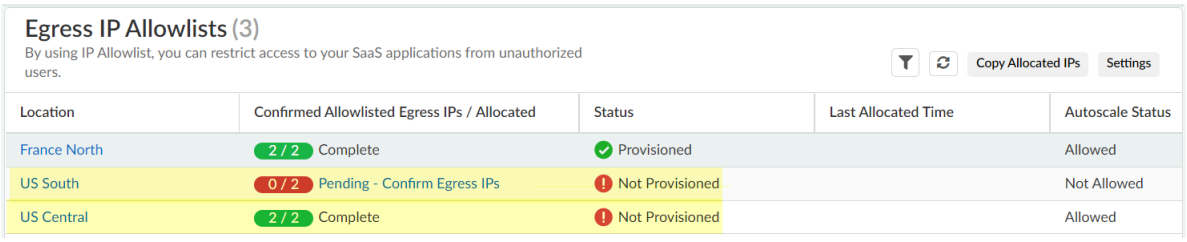
- **Partially Provisioned (Partiellement approvisionnée)** : vous avez ajouté le premier ensemble d'adresses IP de sortie, vous les avez confirmées dans Prisma Access et vous avez appliqué vos modifications. Toutefois Prisma Access a ajouté un autre ensemble d'adresses IP dans le cadre d'un événement de mise à l'échelle automatique et ces adresses IP ne sont pas confirmées dans Prisma Access.

- **Not Provisioned (Non approvisionnée)** : Prisma Access a alloué des adresses IP à l'emplacement, et vous avez ajouté les adresses IP de sortie aux listes d'autorisation de vos applications SaaS et les avez confirmées dans Prisma Access, mais vous n'avez pas encore intégré cet emplacement.

 ©2025 Palo Alto Networks, Inc.

- **Cannot be Provisioned (Ne peut pas être approvisionnée)** : vous avez intégré cet emplacement, mais vous n'avez pas encore procédé à la confirmation dans Prisma Access et appliqué vos modifications.

Le tableau des listes d'adresses IP de sortie autorisées indique également le nombre d'adresses IP confirmées et qui doivent encore être confirmées dans Prisma Access. Par exemple, 1/2 signifie que 1 adresse IP sur 2 adresses IP allouées pour l'emplacement est confirmée dans Prisma Access.



Liste d'autorisation des utilisateurs mobiles de GlobalProtect (Panorama)

Pour vous permettre d'ajouter les adresses IP publiques (de sortie) pour votre déploiement de GlobalProtect — Utilisateur mobile dans les listes d'autorisation de n'importe quelle application SaaS que vous utilisez au sein de votre organisation, Prisma Access fournit les adresses IP et vous permet de vérifier que vous les avez ajoutées à votre liste d'autorisation avant de les utiliser dans votre environnement.

Cette méthode d'attribution d'adresses IP de sortie présente les avantages suivants :

- Elle garantit que Prisma Access ne fournit que les adresses IP apparaissant dans la liste des adresses que vous avez autorisées.
- Elle empêche les utilisateurs mobiles de tenter de se connecter à Prisma Access à partir d'une adresse IP bloquée par le réseau de votre organisation. Prisma Access ne libère pas d'adresses IP pour votre déploiement tant que vous n'avez pas confirmé qu'elles apparaissaient dans votre liste d'autorisation.
- Elle permet de récupérer vos adresses IP de sortie actuelles sans utiliser l'API.

Prisma Access alloue des adresses IP de sortie dans les situations suivantes :

- Lorsque vous intégrez vos emplacements pendant l'intégration des utilisateurs mobiles.

  Prisma Access alloue deux adresses IP de passerelle pour chaque emplacement que vous intégrez.

  *Si vous intégrez un emplacement et que d'autres emplacements du même emplacement de calcul font l'objet d'un événement de mise à l'échelle automatique, Prisma Access peut allouer plus de deux adresses IP au nouvel emplacement. Dans ce cas, assurez-vous d'ajouter toutes ces adresses IP à vos listes d'autorisation et de confirmer que toutes les adresses comme étant **Added to My Allow List (Ajoutées à ma liste d'autorisation)**.*

 ©2025 Palo Alto Networks, Inc.

- Lors d'un événement de mise à l'échelle important.

  Si le nombre d'utilisateurs mobiles dépasse la capacité des deux adresses IP pré-attribuées, Prisma Access alloue un ensemble supplémentaire de deux adresses IP.

  Les événements de mise à l'échelle automatique affectent tous les emplacements intégrés dans un emplacement de calcul. Lorsqu'un événement de mise à l'échelle automatique se produit pour un emplacement et que vous n'avez pas encore confirmé les adresses comme étant ajoutées à vos listes d'autorisation, l'**Autoscale Status (État de la mise à l'échelle automatique)** de tous les emplacements de cet emplacement de calcul sera **Not Allowed (Non autorisée)**.

  Autoscale Status (État de la mise à l'échelle automatique) *affiche l'état de la mise à l'échelle automatique dans Prisma Access.*

  - ***Allowed (Autorisée)*** *: vous avez ajouté les adresses IP aux listes d'autorisation. Si un grand nombre d'utilisateurs mobiles se connectent à un seul emplacement et déclenchent un événement de mise à l'échelle automatique, Prisma Access utilisera les adresses IP autorisées pour l'événement de mise à l'échelle automatique.*
  - ***Not Allowed (Non autorisée)*** *: vous n'avez pas spécifié toutes les adresses IP comme étant ajoutées à vos listes d'autorisation dans l'interface utilisateur de Prisma Access ou vous n'avez pas validé et appliqué vos modifications après les avoir marquées comme ajoutées. Si Prisma Access déclenche un événement de mise à l'échelle automatique, Prisma Access ne fournira pas d'adresses IP supplémentaires pour ajouter plus de capacité à l'emplacement.*

    Chaque fois que vous ajoutez un lieu, ou chaque fois que Prisma Access ajoute des adresses IP à la suite d'un événement de mise à l'échelle automatique, vous devez actualiser la page qui contient le tableau ***Egress IP Allow List (Liste des adresses IP de sortie autorisées)****, spécifier* ***Added to My Allow List (Ajoutée à ma liste d'autorisation)*** *pour marquer les adresses IP comme étant ajoutées aux listes d'autorisation de votre organisation et cliquer sur* ***Commit and Push (Valider et appliquer)*** *pour valider vos modifications.*

  Pour vous tenir informé de toute adresse IP que Prisma Access ajoute à la suite d'un événement de mise à l'échelle automatique, vous pouvez configurer une URL où Prisma Access vous informera des changements d'adresse IP.

Vous n'êtes pas obligé d'activer cette fonctionnalité ; vous choisissez de laisser ou non Prisma Access libérer les adresses IP jusqu'à ce que vous ayez confirmé qu'elles sont répertoriées comme étant autorisées dans l'interface utilisateur.

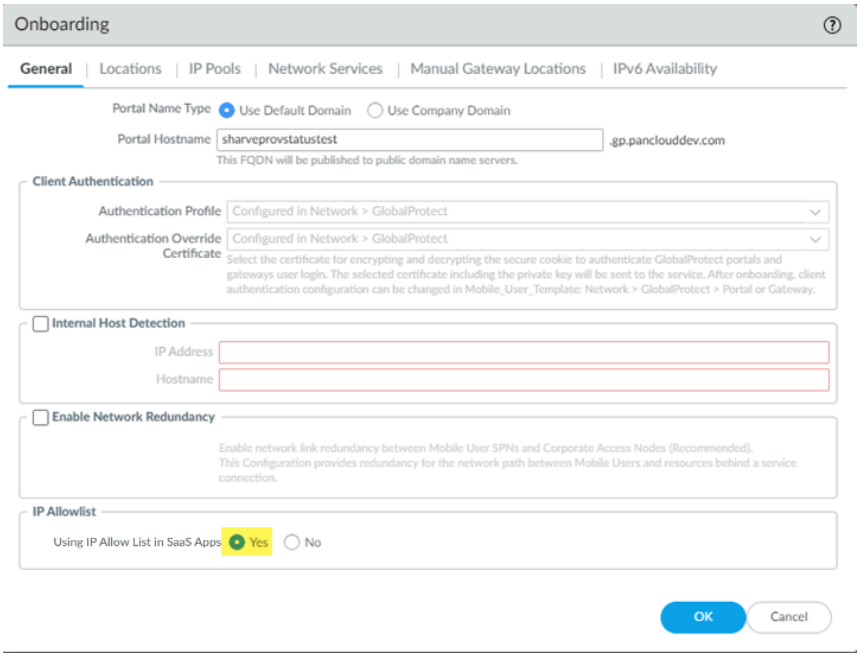
Pour empêcher Prisma Access de fournir des adresses IP GlobalProtect (de sortie) publiques à votre déploiement jusqu'à ce que vous les ayez ajoutées à vos listes d'autorisation, spécifiez **Yes (Oui)** dans le paramètre **Using IP Allow List in SaaS Apps (Utilisation de la liste d'adresses IP autorisées dans les applications SaaS)** pendant l'intégration Utilisateurs mobiles — GlobalProtect. Confirmez que vous les avez ajoutées dans l'interface utilisateur Prisma Access en effectuant la tâche suivante.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—GlobalProtect (Utilisateurs mobiles — GlobalProtect)**.

STEP 2 | Sélectionnez votre **Hostname (Nom d'hôte)**. Puis, vous devez le**Configure (Configurer)** (pour un déploiement existant) ou bien**Configure (Configurer)** votre déploiement pour la première fois (pour un nouveau déploiement).

STEP 3 | Sélectionnez **Yes (Oui)** dans **Using IP Allow List in SaaS Apps (Utilisation de la liste d'adresses IP autorisées dans les applications SaaS)**.



STEP 4 | Poursuivez votre l'intégration Prisma Access, y compris la sélection des emplacements à utiliser dans votre déploiement Utilisateurs Mobiles — GlobalProtect, puis cliquez sur **Commit and Push (Valider et appliquer)** pour valider vos modifications.

Il peut s'écouler jusqu'à une minute avant que les modifications ne soient reflétées dans l'interface utilisateur. Si vous consultez la **Egress IP Allow List (Liste des adresses IP de sortie autorisées)** avant de valider et d'appliquer vos modifications, elle affiche l'état **0/0 Egress IPs Confirmed Allow Listed (0/0 adresse IP de sortie autorisée confirmée)** parce que Prisma Access n'a attribué aucune adresse IP de sortie à votre déploiement.

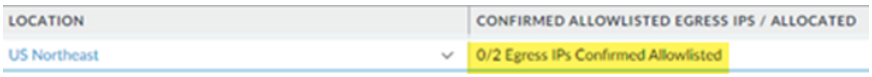
STEP 5 | Consultez le tableau **Egress IP Allow List (Liste des adresses IP de sortie autorisées)** et notez les adresses IP de sortie qui doivent être ajoutées à vos listes d'autorisation.

Vous pouvez afficher les adresses IP de sortie dans le champ **Confirmed Allow Listed Egress IPs / Allocated (Adresses IP de sortie autorisées confirmées/allouées)** du tableau **Egress IP Allow List (Liste des adresses IP de sortie autorisées)**. Le premier chiffre indique si l'ajout de l'adresse IP à vos listes d'autorisation a été confirmé ou non.

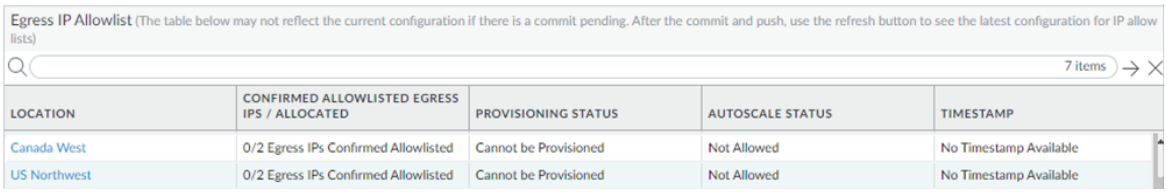
L'exemple suivant montre les adresses IP de l'emplacement nord-est des États-Unis. La description `0/2 Egress IPs Confirmed Allow Listed (0/2 adresse IP de`

 ©2025 Palo Alto Networks, Inc.

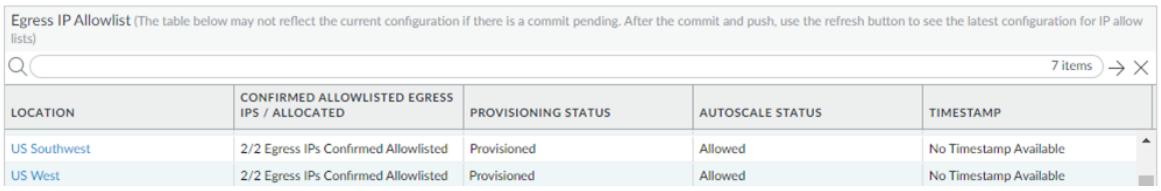
`sortie autorisée confirmée)` indique qu'aucune des deux adresses IP de sortie n'a été marquée comme étant ajoutée à vos listes d'autorisation et que vous devez l'ajouter.



Si vous avez un nouveau déploiement Prisma Access, ou si vous avez ajouté des emplacements ou si vous avez eu un événement de mise à l'échelle automatique, le tableau indique qu'aucune des adresses IP de sortie n'a été ajoutée à la liste d'autorisation de votre organisation.

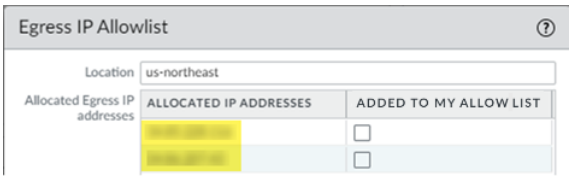


Si vous disposez d'un déploiement Prisma Access existant, le tableau affiche le **Provisioning Status (État de l'approvisionnement) Provisioned (Approvisionnée)** et l'**Autoscale Status (État de la mise à l'échelle automatique) Allowed (Autorisée)**, ce qui indique que Prisma Access a marqué les adresses IP de sortie comme ajoutées.



Prisma Access attribuera deux adresses pour chaque nouvel emplacement ajouté. Si un emplacement existant a déjà fait l'objet d'un événement de mise à l'échelle automatique lorsqu'un grand nombre d'utilisateurs mobiles se sont connectés à un seul emplacement en même temps, Prisma Access alloue une adresse IP de sortie supplémentaire par multiples de deux et un emplacement existant peut avoir quatre adresses ou plus.

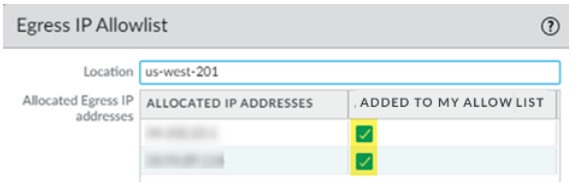
STEP 6 | Recherchez les nouvelles adresses IP de sortie qui doivent être ajoutées aux listes d'autorisation de votre organisation en sélectionnant le nom du **Location (Emplacement)** dans le tableau.



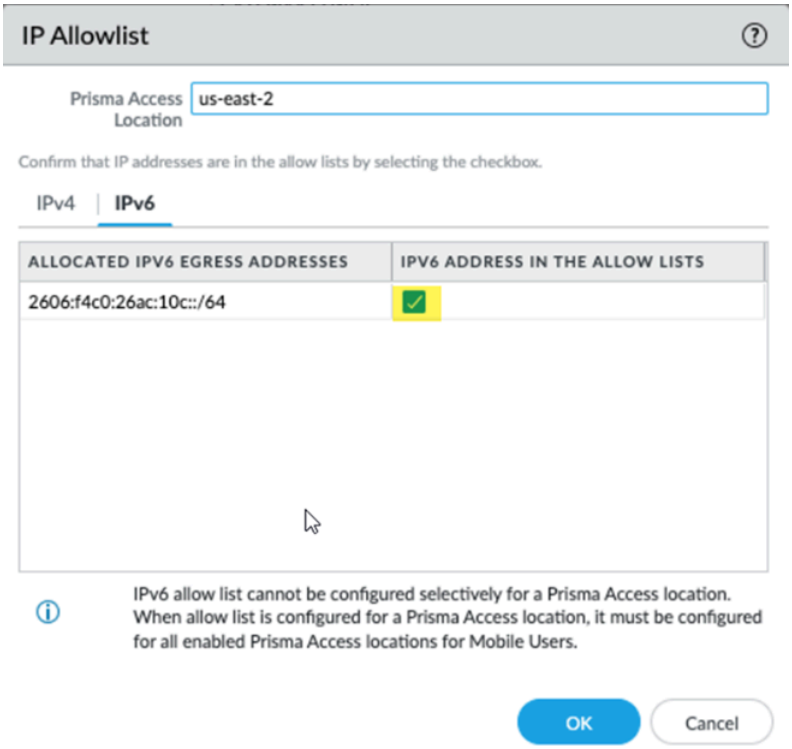
STEP 7 | Ajoutez ces adresses IP de sortie aux listes d'autorisation de votre organisation.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Une fois que vous avez autorisé l'adresse IP de sortie, revenez à la zone IP de sortie et indiquez que vous l'avez ajoutée à vos listes d'autorisation en sélectionnant **Added to My Allow List (Ajoutée à ma liste d'autorisation)**.



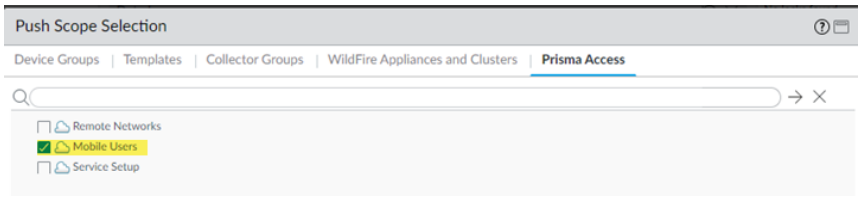
Si vous avez des adresses IPv6, sélectionnez **IPv6 Address in the Allow Lists (Adresse IPv6 dans les listes d'autorisation)**.



 ©2025 Palo Alto Networks, Inc.

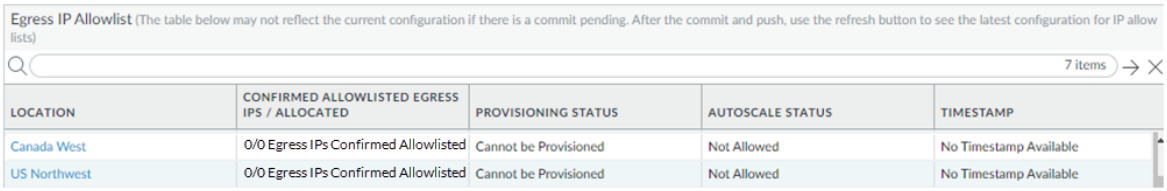
STEP 9 | Validez et appliquez vos modifications pour les rendre actives dans Prisma Access.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
2. Sélectionnez **Prisma Access**, puis assurez-vous que l'option **Mobile Users (Utilisateurs mobiles)** est sélectionnée.



3. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.
4. Sélectionnez **Commit (Valider)** et **Push (Pousser)** pour valider et transmettre les modifications.

Si vous consultez le tableau **Egress IP Allow List (Liste des adresses IP de sortie autorisées)** avant de valider et d'appliquer vos modifications, la colonne Confirmed (Confirmé) affiche l'état **0/0 Egress IPs Confirmed Allow Listed (0/0 adresse IP de sortie autorisée confirmée)** parce que Prisma Access n'a attribué aucune adresse IP à votre déploiement tant que vous n'avez pas cliqué sur **Commit and Push (Valider et appliquer)**.



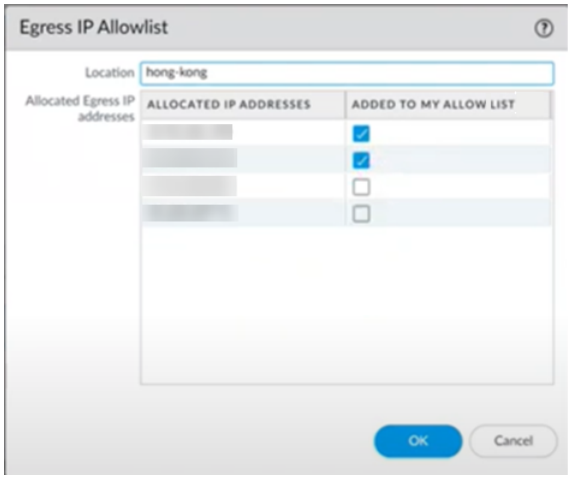
Le tableau **Egress IP Allow List (Liste des adresses IP de sortie autorisées)** contient les champs supplémentaires suivants :

Champ	Description
Emplacement	L'emplacement de l'utilisateur mobile intégré.
Liste des adresses IP de sortie autorisées confirmées/allouées	Le nombre d'adresses IP de sortie dont l'autorisation a été confirmée et le nombre d'adresses IP de sortie allouées.
Configuration de l'état	L'état de la liste d'autorisation des adresses IP de sortie. • **Provisioned (Approvisionnée)** : vous avez ajouté les adresses IP de sortie aux listes d'autorisation de votre organisation, vous avez confirmé qu'elles avaient été ajoutées dans l'interface utilisateur Prisma Access en vérifiant le champ **Added to My Allow List (Ajoutée à ma liste d'autorisation)**, et vous avez validé et

 ©2025 Palo Alto Networks, Inc.

Champ	Description
	appliqué vos modifications pour qu'elles soient entièrement approvisionnées. • **Not Provisioned (Non approvisionnée)** : Prisma Access a alloué des adresses IP à l'emplacement, et vous avez ajouté les adresses IP de sortie aux listes d'autorisation de votre organisation et confirmé qu'elles avaient été ajoutées dans l'interface utilisateur de Prisma Access, mais vous n'avez pas encore intégré cet emplacement. • **Cannot be Provisioned (Ne peut pas être approvisionnée)** : vous avez intégré cet emplacement, mais vous n'avez pas encore vérifié le champ **Add to My Allow List (Ajoutée à ma liste d'autorisation)** ni confirmé et appliqué vos modifications. Jusqu'à ce que vous spécifiiez dans Prisma Access que vous avez ajouté ces adresses IP de sortie aux listes d'autorisation de votre organisation et que vous ayez cliqué sur **Commit and Push (Valider et appliquer)** pour appliquer vos modifications, Prisma Access n'approvisionnera pas ces adresses IP pour votre déploiement. • **Provisioned with partial capacity (Approvisionnée avec une capacité partielle)** : vous avez ajouté le premier ensemble d'adresses IP de sortie, vous avez confirmé qu'elles avaient été ajoutées dans l'interface utilisateur Prisma Access, et avez validé et appliqué vos modifications. Toutefois Prisma Access a ajouté un autre ensemble d'adresses IP dans le cadre d'un événement de mise à l'échelle automatique et ces adresses IP n'ont pas été spécifiées comme ajoutées à vos listes d'autorisation dans l'interface utilisateur Prisma Access. La capture d'écran suivante montre un exemple de déploiement qui afficherait l'état **Provisioned with partial capacity (Approvisionnée avec une capacité partielle)**. Deux adresses IP ont été marquées comme **Added to My Allow List (Ajoutées à ma liste d'autorisation)**. Toutefois, Prisma Access a ajouté deux autres adresses IP à cet

 ©2025 Palo Alto Networks, Inc.

Champ	Description
	emplacement et ceux-ci n'ont pas été ajoutés dans l'interface utilisateur. 
État de la mise à l'échelle	Affiche l'état de la mise à l'échelle automatique dans Prisma Access. • **Allowed (Autorisée)** : vous avez ajouté les adresses IP aux listes d'autorisation. Si un grand nombre d'utilisateurs mobiles se connectent à un seul emplacement et déclenchent un événement de mise à l'échelle automatique, Prisma Access utilisera les adresses IP autorisées pour l'événement de mise à l'échelle automatique. • **Not Allowed (Non autorisée)** : vous n'avez pas spécifié toutes les adresses IP comme étant ajoutées à vos listes d'autorisation dans l'interface utilisateur Prisma Access ou vous n'avez pas validé et appliqué vos modifications après les avoir marquées comme ajoutées. Si Prisma Access déclenche un événement de mise à l'échelle automatique, Prisma Access ne fournira pas d'adresses IP supplémentaires pour ajouter plus de capacité à l'emplacement. Chaque fois que vous ajoutez un lieu, ou chaque fois que Prisma Access ajoute des adresses IP à la suite d'un événement de mise à l'échelle automatique, vous devez actualiser la page qui contient le tableau **Egress IP Allow List (Liste des adresses IP de sortie autorisées)**, spécifier **Added to My Allow List (Ajoutée à ma liste d'autorisation)** pour marquer les adresses IP comme étant

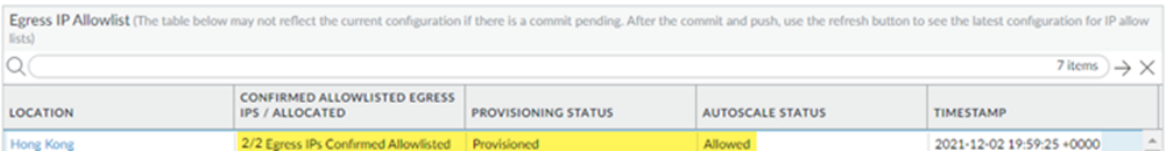
 ©2025 Palo Alto Networks, Inc.

Champ	Description
	ajoutées aux listes d'autorisation de votre organisation et cliquer sur **Commit and Push (Valider et appliquer)** pour valider vos modifications. *Pour vous tenir informé de toute adresse IP que Prisma Access ajoute à la suite d'un événement de mise à l'échelle automatique, vous devez configurer une URL où Prisma Access vous informera des changements d'adresse IP.*
Horodatage	Dernière heure connue à laquelle une adresse IP a été attribuée à cette région en temps universel coordonné (UTC).

Après avoir cliqué sur **Commit and Push (Valider et appliquer)**, la colonne Confirmed (Confirmé) affichera l'état **0/2 Egress IPs Confirmed Allow Listed (0/2 adresse IP de sortie autorisée confirmée)**, car vous n'avez pas encore confirmé que les adresses IP ont été répertoriées dans la liste d'autorisation dans l'interface utilisateur Prisma Access.

Lorsque vous intégrez l'emplacement d'un utilisateur mobile, Prisma Access vous fournit deux adresses IP de sortie : une adresse IP active et une adresse à utiliser en cas d'événement de mise à l'échelle automatique. Voici des exemples de la façon dont Prisma Access alloue et fournit les adresses IP de sortie après un événement de mise à l'échelle automatique.

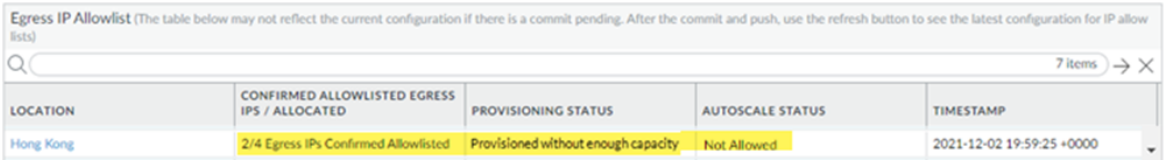
Événement de mise à l'échelle automatique : si un grand nombre d'utilisateurs mobiles se connectent à un emplacement d'utilisateur mobile en même temps, Prisma Access peut allouer un ensemble supplémentaire de deux adresses IP de sortie afin de prendre en charge le grand nombre d'utilisateurs. Une fois que vous avez répertorié les deux premières adresses IP de sortie dans la liste d'autorisation, l'état avant un événement de mise à l'échelle automatique indique que les deux adresses IP de sortie sont autorisées avec l'état confirmé **2/2 Egress IPs Confirmed Allow Listed (2/2 adresses IP de sortie autorisées confirmées)**, l'état d'approvisionnement **Provisioned (Approvisionnée)** et l'état de mise à l'échelle automatique **Allowed (Autorisée)**, comme indiqué dans l'emplacement de Hong Kong dans la capture d'écran suivante.



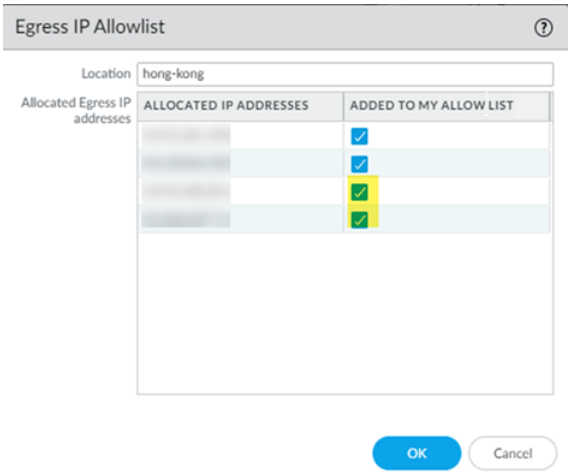
Si un grand nombre d'utilisateurs mobiles se connectent en même temps à l'emplacement de Hong Kong, Prisma Access active l'adresse IP de sortie de secours, alloue deux autres adresses IP et active l'une d'entre elles. Lorsqu'un événement de mise à l'échelle automatique se produit,

 ©2025 Palo Alto Networks, Inc.

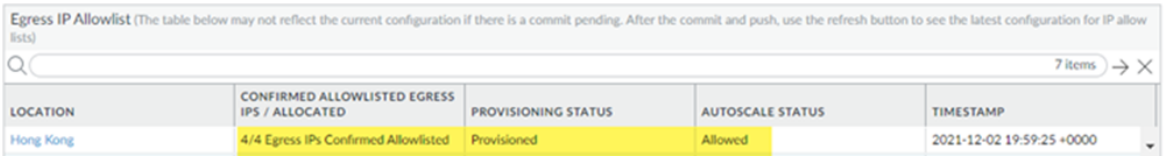
les adresses IP de sortie ont été allouées, mais elles n'ont pas été approvisionnées, l'état confirmé est **2/4 Egress IPs Confirmed Allow Listed (2/4 adresses IP de sortie autorisées confirmées)** et l'état d'approvisionnement indique **Provisioned without enough capacity (Approvisionnée sans capacité suffisante)**. De plus, l'état de la mise à l'échelle automatique indique **Not Allowed (Non autorisée)**, ce qui signifie que Prisma Access ne fournira pas l'adresse IP de sortie supplémentaire pour votre déploiement si un événement de mise à l'échelle automatique se produit.



Après avoir ajouté les nouvelles adresses IP de sortie à vos listes d'autorisation, sélectionnez le nom de l'emplacement. Ensuite, sélectionnez **Added to My Allow List (Ajoutée à ma liste d'autorisation)** pour les deux adresses IP qui ont été ajoutées et cliquez sur **Commit and Push (Valider et appliquer)** pour appliquer vos modifications.



Une fois l'opération terminée, l'emplacement de Hong Kong indique que les quatre adresses IP de sortie sont confirmées et provisionnées, et que la mise à l'échelle automatique est active.



Mises à niveau de l'application GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	• Licence Prisma Access

 ©2025 Palo Alto Networks, Inc.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	

Prisma Access héberge la version de l'application GlobalProtect que les utilisateurs macOS et Windows de votre organisation peuvent télécharger à partir du portail Prisma Access. Prisma Access propose plusieurs versions de l'application GlobalProtect, et vous pouvez choisir de faire de l'une d'entre elles la version active. Vous pouvez également gérer l'accès des utilisateurs mobiles à l'application GlobalProtect ou effectuer des mises à niveau échelonnées.

- Sélectionnez la version active de l'application GlobalProtect pour Prisma Access
- Autoriser les utilisateurs à mettre à niveau l'application GlobalProtect
- Échelonner les mises à jour de l'application GlobalProtect

Sélectionnez la version active de l'application GlobalProtect pour Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Prisma Access gère la version de l'application GlobalProtect pour les utilisateurs Windows et macOS de votre organisation. Alors que Prisma Access héberge plusieurs versions de l'application GlobalProtect, une seule des versions hébergées est active. Lorsque les utilisateurs mobiles se connectent au portail Prisma Access, la version active est celle que les utilisateurs mobiles peuvent télécharger et installer sur leurs périphériques Windows et macOS.

Vous pouvez sélectionner plusieurs versions de GlobalProtect dans un déploiement multi-locataires. Les paramètres de version de l'application GlobalProtect que vous appliquez le sont par locataire et non globaux ; vous contrôlez la version de l'application pour chaque locataire.

Certaines fonctionnalités, telles que l'optimisation IP, nécessitent que les utilisateurs disposent de versions suffisamment mises à jour de GlobalProtect. Continuez à lire pour savoir comment sélectionner la version active de l'application GlobalProtect dans Prisma Access.

- Strata Cloud Manager
- Panorama

Sélectionnez la version active de l'application GlobalProtect pour Prisma Access (Managed by Strata Cloud Manager)

Vous pouvez remplacer la version active actuelle par une autre version hébergée depuis la page de configuration du service en réalisant les étapes suivantes.

STEP 1 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Mobile Users (Utilisateurs mobiles)**, puis localisez le panneau **GlobalProtect Connection (Connexion GlobalProtect)**.

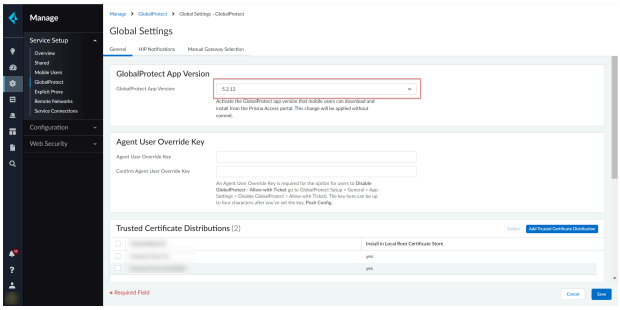
STEP 2 | Sélectionnez **GlobalProtect Setup (Configuration de GlobalProtect)** ou **Enable (Activer)** > **GlobalProtect Setup (Configuration de GlobalProtect)** si GlobalProtect n'est pas déjà activé.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Sélectionnez l'onglet **App GlobalProtect (Application GlobalProtect)**, puis modifiez les **Global App Settings (Paramètres de l'Application Global)**.

STEP 4 | Dans l'onglet **General (Général)** de la page **Global Settings (Paramètres globaux)**, sélectionnez la **GlobalProtect App Version (Version de l'application GlobalProtect)** que vous souhaitez autoriser les utilisateurs mobiles à télécharger et à installer depuis le portail Prisma Access.

La version active est indiquée dans la liste déroulante.



Sélectionnez la version active de l'application GlobalProtect pour Prisma Access (Managed by Panorama)

Si votre version actuellement active est en fin de vie, Prisma Access vous en informe et vous demande d'activer une version prise en charge.

Vous pouvez remplacer la version active actuelle par une autre version hébergée à partir de la page Configuration du service en exécutant les étapes suivantes.

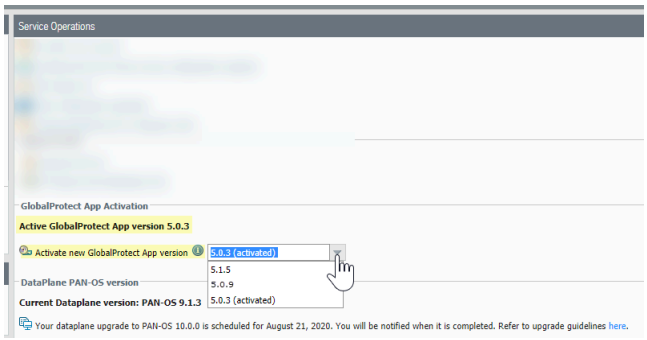
Si vous utilisez Prisma Access dans un environnement FedRAMP, vous devez utiliser la version certifiée FIPS de GlobalProtect, qui est la version 5.1.4. Si vous modifiez la version GlobalProtect par défaut de 5.1.4, vous ne pouvez pas sélectionner la version 5.1.4 à partir de l'interface utilisateur Panorama et vous devrez ouvrir une demande d'assistance auprès du support technique de Palo Alto Networks pour la rajouter.

STEP 1 | Sélectionnez **Panorama** > **Cloud Services (Services Cloud)** > **Configuration** > **Service Setup (Configuration du service)**.

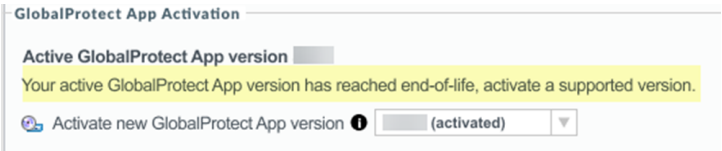
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Sélectionnez **Activate new GlobalProtect app version (Activer la nouvelle version de l'application GlobalProtect)**.

La version active est indiquée dans la liste déroulante.

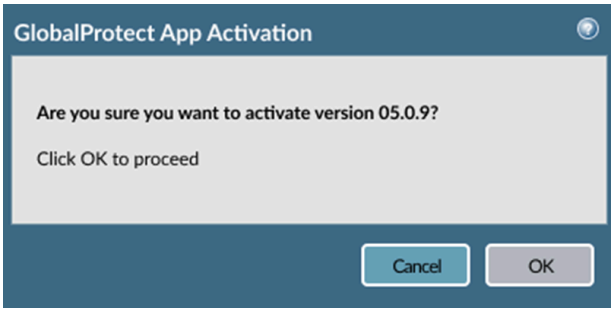


Si votre version actuelle de GlobalProtect est en fin de vie (EoL), un message s'affiche dans cette zone sur la page Configuration du service ; si vous recevez ce message, mettez à niveau votre version de l'application GlobalProtect en passant à l'étape suivante.

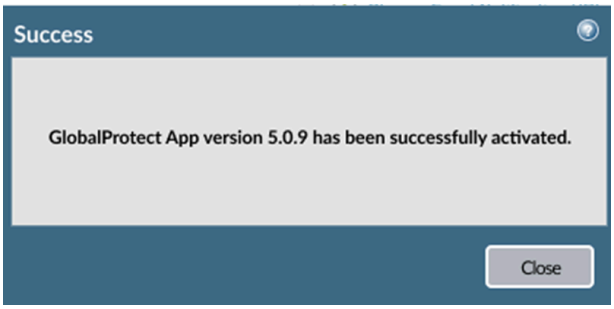


STEP 3 | Sélectionnez la version vers laquelle vous souhaitez effectuer la mise à niveau et cliquez sur **OK**.

Une fenêtre s'affiche pour vérifier votre choix.



Une fois l'application activée, vous recevez un message de réussite.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Affichez la page System Status (État du système) pour vérifier la **Active GlobalProtect App version (Version de l'application GlobalProtect active)**.

Autoriser les utilisateurs à mettre à niveau l'application GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Découvrez comment contrôler l'accès de votre utilisateur mobile à la version de l'application GlobalProtect pour les déploiements GlobalProtect Prisma Access.

- Strata Cloud Manager
- Panorama

Autoriser les utilisateurs à mettre à niveau l'application GlobalProtect (Strata Cloud Manager)

Vous pouvez gérer l'accès des utilisateurs mobiles à la version active de l'application GlobalProtect hébergée par Prisma Access. Pour effectuer cela dans Prisma Access (Managed by Strata Cloud Manager), configurez le paramètre **Upgrade Global Protect (Mettre à niveau Global Protect)**. Pour Prisma Access (Managed by Strata Cloud Manager), suivez les étapes suivantes.

STEP 1 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Mobile Users (Utilisateurs mobiles)**, puis localisez le panneau **GlobalProtect Connection (Connexion GlobalProtect)**.

STEP 2 | Sélectionnez **GlobalProtect Setup (Configuration de GlobalProtect)** ou **Enable (Activer)** > **GlobalProtect Setup (Configuration de GlobalProtect)** si GlobalProtect n'est pas déjà activé.

STEP 3 | Sélectionnez l'onglet **App GlobalProtect (Application GlobalProtect)**, puis **Add App Settings (Ajouter les paramètres de l'application)**.

STEP 4 | Dans la zone **App Configuration (Configuration de l'application)**, sélectionnez une option dans **Upgrade GlobalProtect App (Mettre à niveau l'application GlobalProtect)** pour spécifier si les utilisateurs mobiles peuvent mettre à niveau leur version de l'application GlobalProtect vers la version active hébergée sur Prisma Access et, si cela est possible, s'ils peuvent choisir le moment de la mise à niveau :

- **Allow when user accepts the upgrade Prompt (Autoriser lorsque l'utilisateur accepte l'invite de mise à niveau)** (par défaut) : envoyer une invite aux utilisateurs lorsqu'une nouvelle version est activée et permettre aux utilisateurs de mettre à niveau leur logiciel lorsqu'ils le souhaitent.
- **Disallow (Désactiver)** – Empêche les utilisateurs de mettre à niveau le logiciel de l'application.
- **Allow Manually (Autoriser manuellement)** – Autoriser les utilisateurs à vérifier manuellement les mises à niveau et à les lancer en sélectionnant **Check Version (Vérifier Version)** dans l'application GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

- **Allow Transparently (Permettre avec transparence)** – Met automatiquement à niveau le logiciel de l'application lorsqu'une nouvelle version est disponible sur le portail.
- **Allow when the user is in the corporate network (Autoriser lorsque l'utilisateur se trouve dans le réseau de l'entreprise)** : mettre automatiquement à niveau le logiciel de l'application chaque fois qu'une nouvelle version est disponible sur le portail. Cependant, vous devez attendre que le terminal soit connecté en interne au réseau de l'entreprise. Cela empêche les retards causés par les mises à niveau sur les connexions à bande passante étroite.

Autoriser les utilisateurs à mettre à niveau l'application GlobalProtect (Panorama)

Vous pouvez gérer l'accès des utilisateurs mobiles à la version active de l'application GlobalProtect hébergée par Prisma Access. Pour effectuer cela dans Prisma Access (Managed by Strata Cloud Manager), configurez le paramètre **Upgrade Global Protect (Mettre à niveau Global Protect)**. Pour Prisma Access (Managed by Panorama), suivez les étapes suivantes.

STEP 1 | Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**.

STEP 2 | Sélectionnez la **Mobile_User_Template** dans la liste déroulante **Template (Modèle)**.

STEP 3 | Sélectionnez **GlobalProtect_Portal** pour modifier la configuration du portail Prisma Access.

STEP 4 | Sélectionnez l'onglet **Agent** et sélectionnez la configuration de l'application.

STEP 5 | Sélectionnez l'onglet **App (Applications)**.

STEP 6 | Dans la zone **App Configurations (Configurations d'application)**, sélectionnez une option dans **Allow User to Upgrade GlobalProtect App (Autoriser l'utilisateur à mettre à niveau l'application GlobalProtect)** pour spécifier si les utilisateurs mobiles peuvent mettre à niveau leur version de l'application GlobalProtect vers la version active hébergée sur Prisma Access et, si cela est possible, s'ils peuvent choisir quand effectuer la mise à niveau :

- **Allow with Prompt (Autoriser avec invite)** (par défaut) : envoyer une invite aux utilisateurs lorsqu'une nouvelle version est activée et permettre aux utilisateurs de mettre à niveau leur logiciel lorsqu'ils le souhaitent.
- **Disallow (Désactiver)** – Empêche les utilisateurs de mettre à niveau le logiciel de l'application.
- **Allow Manually (Autoriser manuellement)** – Autoriser les utilisateurs à vérifier manuellement les mises à niveau et à les lancer en sélectionnant **Check Version (Vérifier Version)** dans l'application GlobalProtect.
- **Allow Transparently (Permettre avec transparence)** – Met automatiquement à niveau le logiciel de l'application lorsqu'une nouvelle version est disponible sur le portail.
- **Internal (Interne)** – Mettre automatiquement à niveau le logiciel de l'application chaque fois qu'une nouvelle version est disponible sur le portail. Cependant, vous devez attendre que le terminal soit connecté en interne au réseau de l'entreprise. Cela empêche les retards causés par les mises à niveau sur les connexions à bande passante étroite.

 ©2025 Palo Alto Networks, Inc.

Échelonner les mises à jour de l'application GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• Licence Prisma Access

Si vous gérez une grande entreprise, vous souhaiterez peut-être aider les utilisateurs mobiles à obtenir la dernière version de l'application GlobalProtect par étapes. Par exemple, vous pouvez affecter un groupe plus petit à la mise à jour de l'application GlobalProtect avant de la déployer à tous les membres de votre organisation. Pour cela, vous pouvez effectuer la tâche suivante.

STEP 1 | Si vous ne l'avez pas encore fait, créez un groupe d'utilisateurs pour le premier groupe d'utilisateurs à qui vous souhaitez déployer la mise à jour de l'application GlobalProtect.

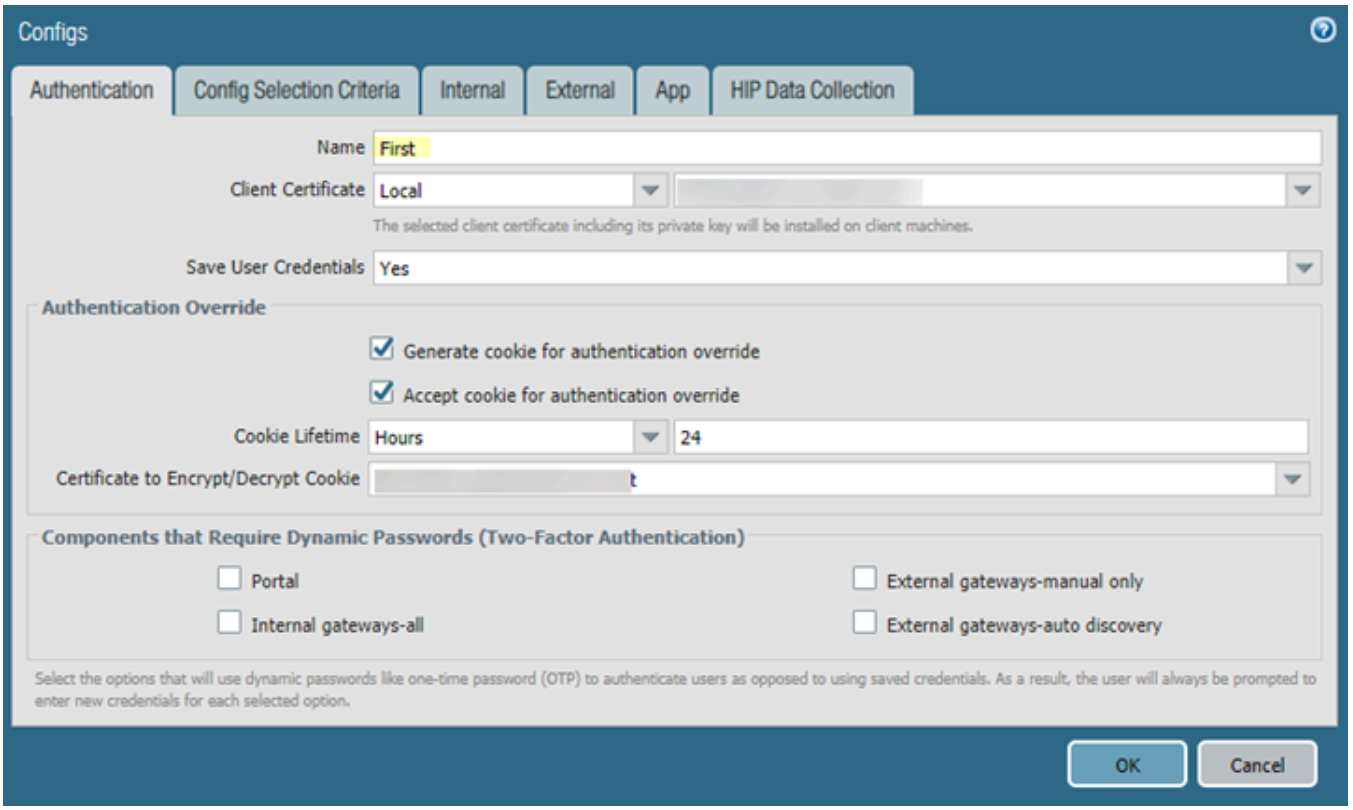
Vous pouvez utiliser User-ID pour mapper les utilisateurs à des groupesou sélectionnez **Device (Périphérique)** > **Local User Database (Base de données d'utilisateurs locale)** > **User Groups (Groupes d'utilisateurs)** pour créer manuellement un groupe.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Créez une nouvelle configuration de l'agent GlobalProtect à utiliser pour le premier groupe d'utilisateurs.

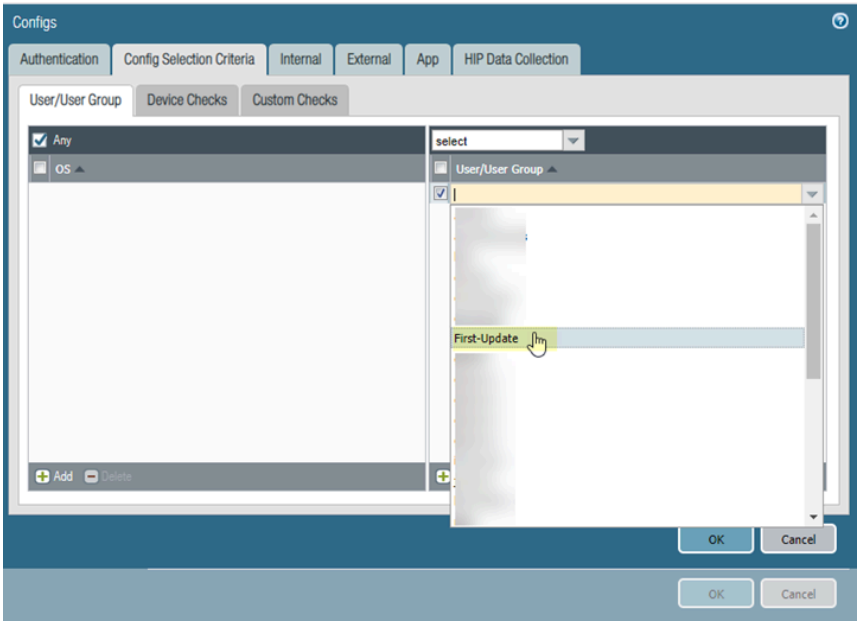
1. Dans Panorama, sélectionnez **Network (réseau)** > **GlobalProtect** > **Portals (Portails)**.
2. Sélectionnez la **Mobile_User_Template** dans la liste déroulante **Template (Modèle)**.
3. Sélectionnez **GlobalProtect_Portal** pour modifier la configuration du portail Prisma Access.
4. Sélectionnez l'onglet **Agent.**
5. Sélectionnez la configuration par **DEFAULT (DÉFAUT)** et sélectionnez **Clone (Cloner)**.

   Vous pouvez également sélectionner **Add (Ajouter)** pour ajouter une nouvelle configuration ; mais le clonage de la configuration existante copie les informations requises pour la nouvelle configuration.
6. Saisissez un **Name (Nom)** pour la configuration.



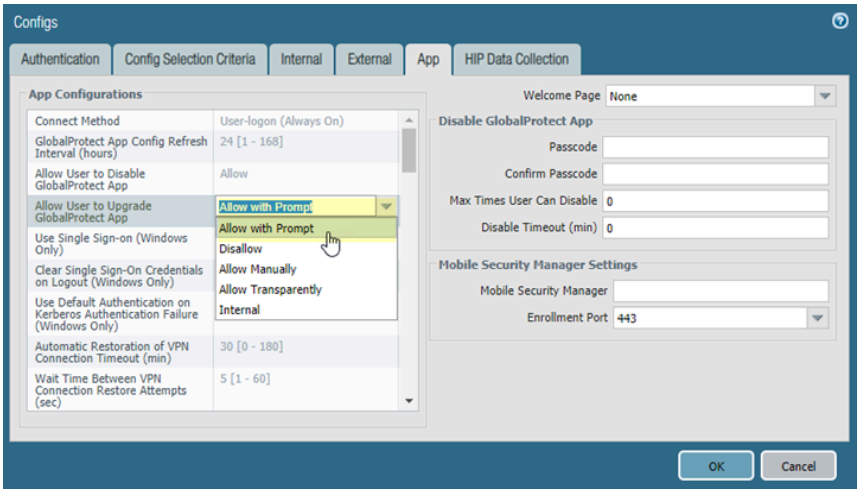
7. Sélectionnez l'onglet **Config Selection Criteria (Critères de sélection de la configuration)**
8. Dans la zone **User/User Group (Utilisateur/Groupe d'utilisateurs)**, sélectionnez l'utilisateur que vous avez créé à l'étape 1.

 ©2025 Palo Alto Networks, Inc.



9. Sélectionnez l'onglet **App (Applications)**.
10. Modifiez **Allow User to Upgrade GlobalProtect App (Autoriser l'utilisateur à mettre à niveau l'application GlobalProtect)** par **Allow with Prompt (Autoriser avec message)** ou **Allow Transparently (Autoriser en transparence)**.

    La fonction **Allow with Prompt (Autoriser avec message)** avertit les utilisateurs lorsqu'une nouvelle version est activée et leur permet de mettre à niveau leur logiciel lorsque cela leur convient ; la fonction **Allow Transparently (Autoriser en transparence)** met automatiquement à jour le logiciel de l'application chaque fois qu'une nouvelle version est disponible sur le portail.



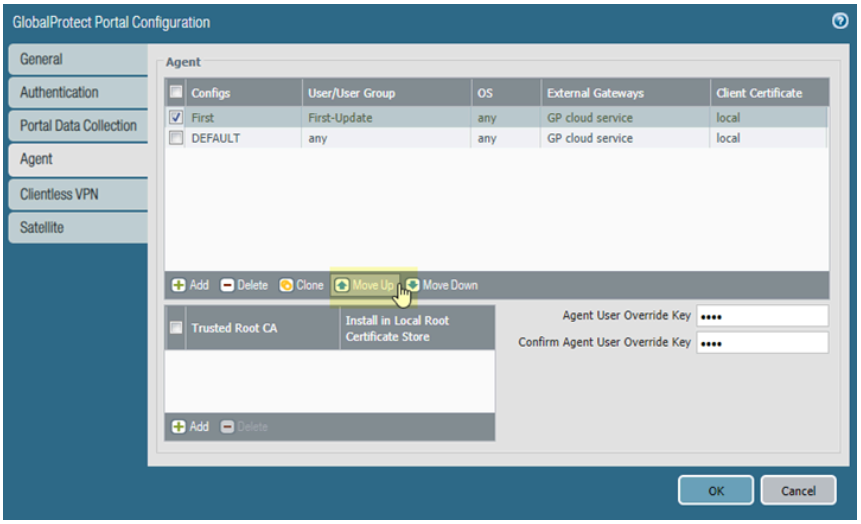
11. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 3 | Sélectionnez **Move Up (Monter)** pour déplacer votre configuration au-dessus de la configuration par défaut.

Dès qu'une application se connecte, le portail compare les informations sources dans le paquet aux configurations d'agent que vous avez définies. Comme avec l'évaluation des règles de

 ©2025 Palo Alto Networks, Inc.

sécurité, le portail recherche une correspondance en commençant par le début de la liste. Lorsqu'il trouve une correspondance, il fournit la configuration correspondante à l'application.



STEP 4 | Répétez ces étapes pour la configuration par **DEFAULT (DÉFAUT)**, mais modifiez la fonction **Allow User to Upgrade GlobalProtect App (Autoriser l'utilisateur à mettre à niveau l'application GlobalProtect)** par **Disallow (Interdire)** pour empêcher les utilisateurs d'effectuer la mise à jour vers la dernière version du logiciel de l'application GlobalProtect.

STEP 5 | Lorsque vous souhaitez permettre au reste des utilisateurs de mettre à jour leurs applications, modifiez **Allow User to Upgrade GlobalProtect App (Autoriser l'utilisateur à mettre à niveau l'application GlobalProtect)** dans la configuration par **DEFAULT (DÉFAUT)** à une sélection qui le lui permet (soit **Allow with Prompt (Autoriser avec message)** ou **Allow Transparently (Autoriser en transparence)**).

Intégrer Prisma Access à des passerelles GlobalProtect sur site

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Licence Prisma Access

Prisma Access vous permet d'étendre la plateforme de sécurité de Palo Alto Networks aux emplacements réseau distants et aux utilisateurs mobiles sans avoir à créer votre propre infrastructure de sécurité globale et à étendre votre capacité opérationnelle. Si vous avez déjà déployé des passerelles GlobalProtect dans des régions où vous disposez déjà de l'infrastructure nécessaire pour les gérer, vous pouvez tirer parti de cet investissement en configurant Prisma Access pour diriger les utilisateurs mobiles vers vos passerelles externes existantes, le cas échéant.

Vous pouvez gérer les priorités des passerelles Prisma Access et sur site afin de spécifier des priorités pour les passerelles Prisma Access et sur site. Les administrateurs ne peuvent pas forcer les utilisateurs mobiles à se connecter à une passerelle Prisma Access précise, mais ils peuvent

 ©2025 Palo Alto Networks, Inc.

permettre aux utilisateurs mobiles de sélectionner manuellement des passerelles Prisma Access spécifiques à l'aide de l'application GlobalProtect.

Vous ne pouvez pas utiliser votre propre portail avec Prisma Access. Vous ne pouvez utiliser le portail déployé que si votre Prisma Access pour les utilisateurs mobiles est provisionné.

- Strata Cloud Manager
- Panorama

Intégrer Prisma Access à des passerelles GlobalProtect sur site (Prisma Access (Managed by Strata Cloud Manager))

STEP 1 | Ajoutez votre passerelle sur site à la liste des passerelles dans la configuration de l'agent.

1. Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration Prisma Access)** > **GlobalProtect** et sélectionnez l'onglet **GlobalProtect App (Application GlobalProtect)**.
2. Sélectionnez **Add App Settings (Ajouter les paramètres de l'application)**.
3. Sélectionnez **Add (Ajouter)** pour ajouter une passerelle externe

   *Si vous ajoutez une nouvelle configuration d'agent et que vous souhaitez ajouter les passerelles Prisma Access à la liste des passerelles externes dans cette configuration, vous devez définir le **Name (Nom)** sur **GP cloud service (Service cloud GP)** et l'**Address (Adresse)** sur **gpcloudservice.com**. Entrez ces valeurs exactement comme indiqué. Vous ne pouvez pas utiliser ces valeurs pour des passerelles non Prisma Access.*
4. Saisissez le **Name (Nom)** de la passerelle et spécifiez l'adresse **FQDN** ou **IP** de la passerelle dans le champ **Address (Adresse)** ; cette valeur doit correspondre exactement au nom commun (Common Name – CN) dans le certificat de la passerelle.
5. (Facultatif) Si vous souhaitez que les utilisateurs mobiles ne se connectent à la passerelle que s'ils se trouvent dans la région correspondante, sélectionnez **Add (Ajouter)** et ajoutez la **Source Region (Région source)** à laquelle vous souhaitez limiter la passerelle.

 ©2025 Palo Alto Networks, Inc.

Par exemple, si vous avez une passerelle en France, vous devez sélectionner FR (France). Si vous avez une passerelle en Suède, vous devez sélectionner (SE) Suède.

Ainsi, les utilisateurs pourront accéder à une passerelle qui permet d'accéder à des ressources Internet dans leur propre langue.

6. (Facultatif) Spécifiez les priorités dans la configuration de votre passerelle.

   Vous pouvez accorder une priorité plus élevée ou plus basse à la passerelle sur site.

   - Pour donner à la passerelle sur site une priorité plus basse que celle de la passerelle Prisma Access par défaut, définissez la **Priority (Priorité)** sur **High (Élevée)** ou **Medium (Moyenne)**.

     Si vous ajoutez d'autres passerelles et que vous souhaitez définir des priorités différentes pour chaque passerelle, vous pouvez définir la **Priority (Priorité)** sur **High (Élevée)**, **Medium (Moyenne)**, **Low (Basse)** ou **Lowest (La plus basse)**.
   - Pour donner à la passerelle sur site une priorité plus élevée que celle de la passerelle par défaut, définissez la **Priority (Priorité)** sur **Highest (La plus élevée)**.

     Si vous souhaitez accorder à la passerelle sur site une priorité plus élevée, vous devez également modifier la passerelle **Prisma Access** par défaut et définir la **Priority (Priorité)** sur un niveau inférieur à **Highest (La plus élevée)**.

7. Sélectionnez **Manual (Manuel)**.

   Cochez cette case pour permettre aux utilisateurs de GlobalProtect de sélectionner manuellement cette passerelle externe dans leur application GlobalProtect.

STEP 2 | Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

STEP 3 | **Push Config (Transmettre la configuration)**.

Intégrer Prisma Access à des passerelles GlobalProtect sur site (Prisma Access (Managed by Panorama))

Pour configurer l'un de ces déploiements Prisma Access hybrides, vous devez modifier la configuration GlobalProtect_Portal dans Mobile_User_Template pour ajouter les passerelles locales aux régions appropriées.

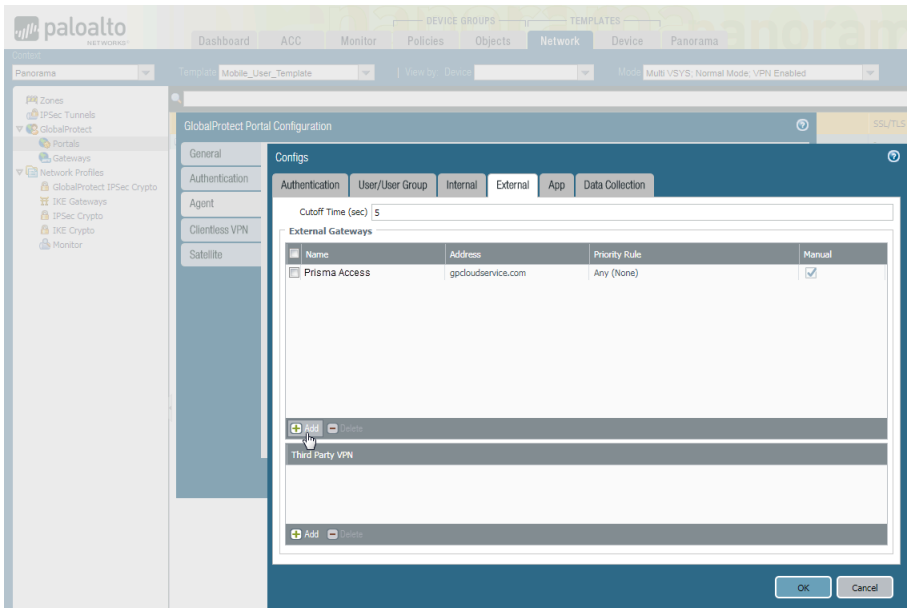
STEP 1 | Modifiez la configuration du portail Prisma Access.

1. Pour ajouter une passerelle existante à la liste des passerelles disponibles, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
2. Sélectionnez **Mobile_User_Template** dans la liste déroulante **Template (Modèle)**.
3. Sélectionnez **GlobalProtect_Portal** pour modifier la configuration du portail Prisma Access.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Ajoutez votre passerelle sur site à la liste des passerelles dans la configuration de l'agent.

1. Sélectionnez l'onglet **Agent**, puis choisissez la configuration d'agent **DEFAULT (PAR DÉFAUT)** ou sélectionnez **Add (Ajouter)** pour ajouter un nouvel agent.
2. Sélectionnez l'onglet **External (Externe)**, puis choisissez **Add (Ajouter)** pour ajouter la passerelle sur site.



> *Si vous ajoutez une nouvelle configuration d'agent et que vous souhaitez ajouter les passerelles Prisma Access à la liste des passerelles externes dans cette configuration, vous devez définir le **Name (Nom)** sur **GP cloud service (Service cloud GP)** et l'**Address (Adresse)** sur **gpcloudservice.com**. Vous devez entrer ces valeurs exactement comme indiqué. Vous ne pouvez pas utiliser ces valeurs pour des passerelles non Prisma Access.*

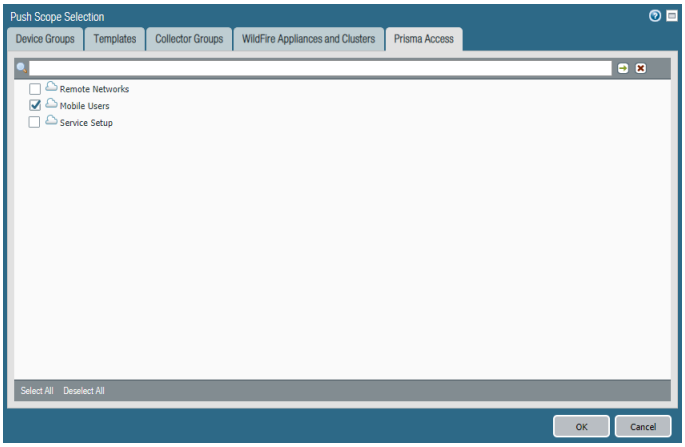
3. Saisissez le **Name (Nom)** de la passerelle et spécifiez l'adresse **FQDN** ou **IP** de la passerelle dans le champ **Address (Adresse)** ; cette valeur doit correspondre exactement au nom commun (Common Name – CN) dans le certificat de la passerelle.
4. (Facultatif) Si vous souhaitez que les utilisateurs mobiles ne se connectent à la passerelle que s'ils se trouvent dans la région correspondante, sélectionnez **Add (Ajouter)** et ajoutez la **Source Region (Région source)** à laquelle vous souhaitez limiter la passerelle. Par exemple, si vous avez une passerelle en France, vous devez sélectionner FR (France). Si vous avez une passerelle en Suède, vous devez sélectionner (SE) Suède.

   Ainsi, les utilisateurs pourront accéder à une passerelle qui permet d'accéder à des ressources Internet dans leur propre langue.
5. (Facultatif) Définissez la priorité de la passerelle.
6. Configurez d'autres paramètres d'agent si nécessaire pour terminer la configuration de l'agent.
7. Cliquez sur **OK** pour enregistrer la configuration de client.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Validez toutes les modifications dans Panorama et appliquez les modifications de configuration sur Prisma Access.

1. Cliquez sur **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.
2. Cliquez sur **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)**, puis sur **Edit Selections (Modifier les sélections)**.
3. Dans l'onglet **Prisma Access**, vérifiez que **Prisma Access for users (Prisma Access pour les utilisateurs)** est sélectionné, puis cliquez sur **OK**.



4. Cliquez sur **Push (Pousser)**.

Définir la priorité pour les passerelles Prisma Access et sur site

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• Licence Prisma Access

Vous pouvez sélectionner une passerelle sur site qui est physiquement la plus proche de vos utilisateurs mobiles et permettre aux utilisateurs de se connecter à une passerelle différente (sur site ou dans le cloud) pour garantir un accès sécurisé aux utilisateurs mobiles s'ils changent d'emplacement. Vous pouvez également spécifier la priorité pour les passerelles qui se trouvent dans le même pays ou la même zone linguistique que vos utilisateurs mobiles.

Si vous souhaitez que les utilisateurs se connectent à une passerelle Prisma Access spécifique, vous pouvez autoriser les utilisateurs mobiles à sélectionner manuellement des passerelles Prisma Access spécifiques. Les utilisateurs mobiles choisissent l'une des passerelles Prisma Access à l'aide de l'application GlobalProtect installée sur leur terminal.

Terminez le flux de travail suivant pour configurer les priorités de passerelles dans Prisma Access.

- Définir des priorités égales pour les passerelles sur site et Prisma Access
- Définir une priorité de passerelle plus élevée pour une passerelle sur site
- Définir des priorités plus élevées pour plusieurs passerelles sur site
- Configurer les priorités pour les passerelles Prisma Access et sur site

 ©2025 Palo Alto Networks, Inc.

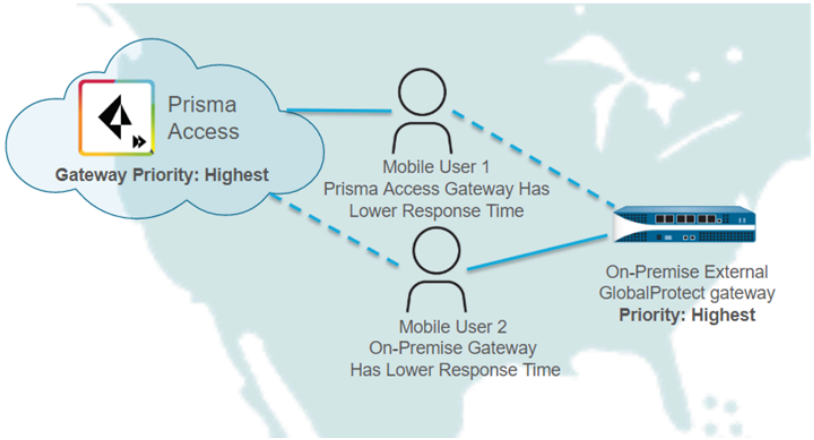
Définir des priorités égales pour les passerelles sur site et Prisma Access

Pour permettre un accès sécurisé à vos employés mobiles, où qu'ils se trouvent, vous pouvez définir des priorités égales pour les passerelles GlobalProtect sur site et les passerelles Prisma Access. L'application GlobalProtect utilise la Priorité de passerelle dans une configuration de passerelle multiple pour déterminer la passerelle préférée.

Vous pouvez utiliser cette configuration si vos utilisateurs mobiles sont le plus souvent plus proches d'une passerelle sur site. Lorsque les utilisateurs changent d'emplacement, l'application GlobalProtect choisit une autre passerelle (sur site ou Prisma Access) en fonction de la priorité la plus élevée et du temps de réponse le plus faible.

La figure suivante illustre un exemple de configuration avec deux utilisateurs mobiles en Amérique du Nord. Vous définissez la priorité de passerelle sur **Highest (Plus élevée)** pour les passerelles Prisma Access et les passerelles sur site.

Dans cet exemple, l'application GlobalProtect de l'utilisateur 1 détermine que la passerelle Prisma Access a un temps de réponse inférieur à celui de la passerelle sur site, et l'application GlobalProtect de l'utilisateur 2 détermine que la passerelle sur site a un temps de réponse inférieur. Puisque toutes les passerelles ont la même priorité, l'utilisateur 1 se connecte à la passerelle Prisma Access et l'utilisateur 2 se connecte à la passerelle sur site, en fonction du temps de réponse le plus faible.



Définir une priorité de passerelle plus élevée pour une passerelle sur site

Dans les situations où vous souhaitez demander aux utilisateurs mobiles d'utiliser une passerelle sur site au lieu des passerelles Prisma Access, spécifiez les passerelles sur site avec une région source et une priorité plus élevée que la passerelle Prisma Access.

La figure suivante illustre un exemple de configuration pour les utilisateurs mobiles en Indonésie. Pour éviter la possibilité que les utilisateurs mobiles soient connectés à la passerelle Prisma Access la plus proche à Singapour, vous définissez la priorité de passerelle sur **Highest (Plus élevée)** pour la passerelle sur site en Indonésie et définissez la priorité sur **Medium (Moyenne)** pour les passerelles Prisma Access.

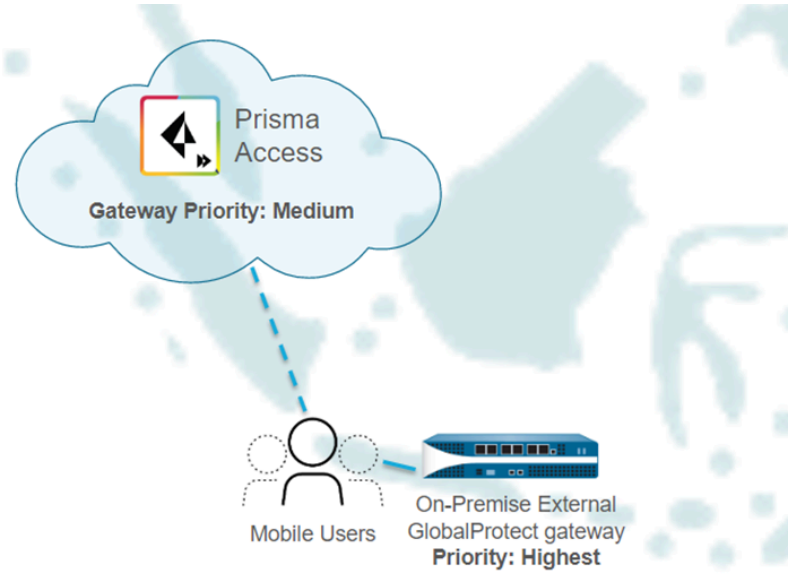
Cet exemple spécifie également une région source en Indonésie pour la passerelle sur site. Nous recommandons de spécifier une région source pour les raisons suivantes :

- Spécifier une région source pour une passerelle sur site permet aux utilisateurs d'une région d'accéder à cette passerelle et empêche les utilisateurs en dehors de cette région de se connecter à cette passerelle. Dans cet exemple, seuls les utilisateurs mobiles en Indonésie

 ©2025 Palo Alto Networks, Inc.

peuvent se connecter à la passerelle sur site avec la région source de l'Indonésie, et la priorité plus élevée signifie que la passerelle sur site a priorité sur les passerelles Prisma Access.

- Si vous définissez une région source **Any (Indifférent)** pour la passerelle sur site en Indonésie, chaque utilisateur mobile de votre organisation préférerait la passerelle sur site en Indonésie, en raison de sa priorité plus élevée et de son accessibilité mondiale. Cette configuration signifie que les utilisateurs mobiles pourraient ne jamais se connecter aux passerelles Prisma Access.



Définir des priorités plus élevées pour plusieurs passerelles sur site

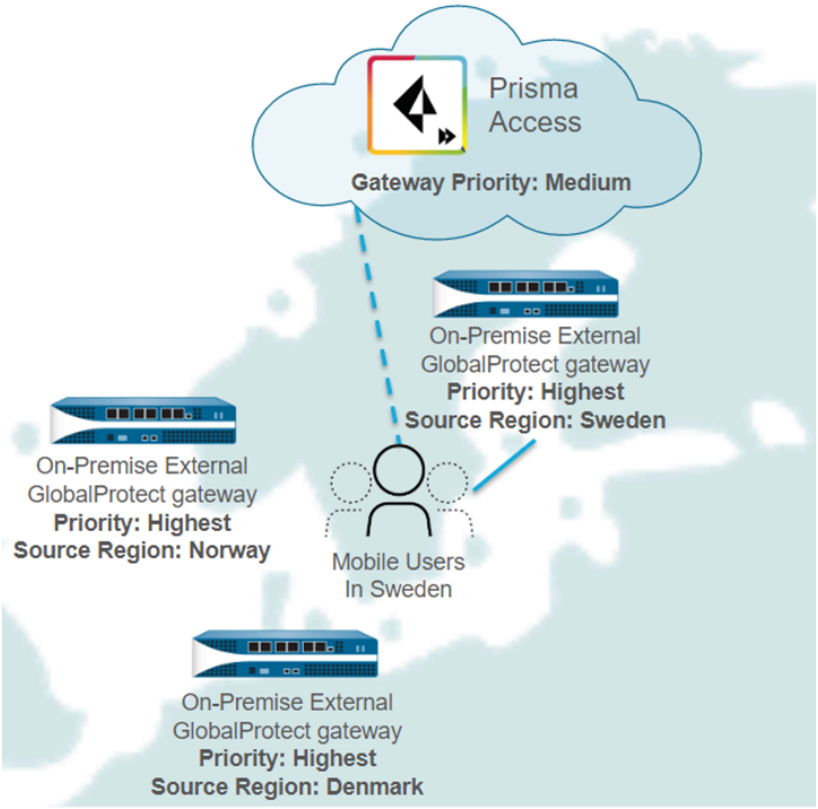
Pour vous assurer que le trafic vers Internet reste dans des régions spécifiques à la langue, vous pouvez configurer plusieurs passerelles dans plusieurs régions sources, en définissant la priorité des passerelles sur site sur **Highest (Plus élevée)** et la priorité des passerelles Prisma Access sur **Medium (Moyenne)**.

La figure suivante illustre un exemple de configuration pour les utilisateurs mobiles en Scandinavie. Avec cette configuration, lorsque les utilisateurs mobiles accèdent à des sites Web sur Internet, les sites Web utilisent le jeu de codage de caractères spécifique à leurs langues.

Dans cet exemple, vous configurez des passerelles sur site avec des régions sources au Danemark, en Norvège et en Suède. Vous définissez la priorité de ces passerelles sur **Highest (Plus élevée)** et définissez la priorité des passerelles Prisma Access sur **Medium (Moyenne)**. Spécifier une région source pour les passerelles sur site permet aux utilisateurs de ces régions d'accéder à ces passerelles et empêche les utilisateurs en dehors de ces régions de se connecter à ces passerelles.

Dans cet exemple, l'application GlobalProtect pour les utilisateurs mobiles en Suède sélectionne la passerelle sur site en Suède en raison de la région source et de la priorité plus élevée de la passerelle.

 ©2025 Palo Alto Networks, Inc.



Configurer les priorités pour les passerelles Prisma Access et sur site

Utilisez ce flux de travail pour configurer les priorités pour un déploiement qui utilise des passerelles sur site avec Prisma Access.

STEP 1 | Connectez-vous à Prisma Access.

STEP 2 | Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** dans le modèle **Mobile_User_Template**.

STEP 3 | Cliquez sur le nom du portail dans le champ **Name (Nom)**.

STEP 4 | Cliquez sur l'onglet **Agent**.

STEP 5 | Cliquez sur le nom de l'agent à configurer.

L'agent par défaut est nommé **DEFAULT**.

STEP 6 | Cliquez sur l'onglet **External (Externe)**.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Définissez la priorité des passerelles Prisma Access.

1. Cliquez sur **GP cloud service (Service cloud GP)**.
2. Définissez la priorité pour votre configuration préférée.
   - Pour Définir des priorités égales pour les passerelles sur site et Prisma Access, changez la priorité de **None (Aucune)** à **Highest (Plus élevée)**.
   - Pour Définir une priorité de passerelle plus élevée pour une passerelle sur site ou Définir des priorités plus élevées pour plusieurs passerelles sur site, changez la priorité de **None (Aucune)** à **Medium (Moyenne)**.
3. Assurez-vous que la case **Manual (Manuel)** est cochée.

   Cocher la case **Manual (Manuel)** permet aux utilisateurs mobiles de sélectionner une passerelle Prisma Access spécifique si nécessaire.

   N'ajoutez pas de région source pour les passerelles Prisma Access ; toute région que vous spécifiez n'est pas appliquée à la configuration.
4. Cliquez sur **OK**.

STEP 8 | **Add (Ajoutez)** une ou plusieurs passerelles externes sur site à votre configuration.

1. Donnez un **Name (Nom)** descriptif à la passerelle.

   Le nom que vous saisissez ici doit correspondre au nom que vous avez défini lorsque vous avez configuré la passerelle et il doit être suffisamment descriptif pour que les utilisateurs sachent l'emplacement de la passerelle à laquelle ils sont connectés.
2. Saisissez le FQDN ou l'adresse IP de l'interface sur laquelle la passerelle est configurée dans le champ Address (Adresse).

   Vous pouvez configurer une adresse IPv4. L'adresse que vous spécifiez doit correspondre exactement au nom commun (NC) dans le certificat de serveur de passerelle.
3. Ajoutez une ou plusieurs **Source Regions (Régions sources)** pour la passerelle sur site, ou sélectionnez **Any (Indifférent)** pour rendre la passerelle accessible à toutes les régions.

   *Si vous définissez la priorité des passerelles externes sur site au-dessus de celle des passerelles Prisma Access, nous vous recommandons de spécifier des régions sources pour les passerelles externes. Si vous spécifiez **Any (Indifférent)** pour la région, l'application GlobalProtect pourrait ne jamais sélectionner de passerelles Prisma Access par rapport aux passerelles sur site en raison de la priorité plus élevée accordée aux passerelles sur site.*
4. Cochez la case **Manual (Manuelle)** pour autoriser les utilisateurs à passer manuellement sur la passerelle.
5. Définissez la **Priority (Priorité)** de la passerelle sur site sur **Highest (Plus élevée)** (la valeur par défaut).
6. Cliquez sur **OK**.

 ©2025 Palo Alto Networks, Inc.

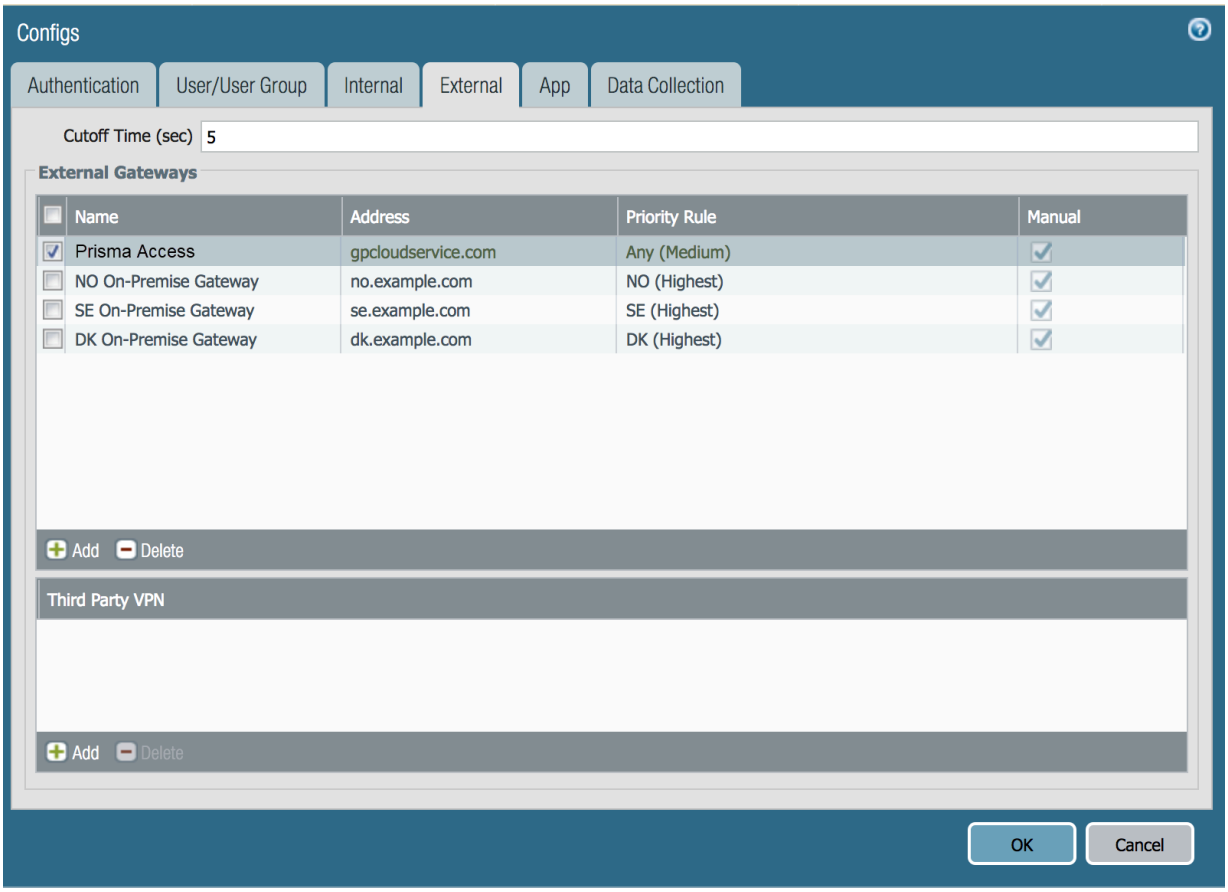
STEP 9 | (Facultatif) Définissez la priorité pour les passerelles supplémentaires en répétant l'étape 8.

Assurez-vous de spécifier les bonnes régions sources.

La figure suivante illustre un exemple de configuration avec plusieurs passerelles qui ont des régions sources en Norvège, en Suède et au Danemark. Notez que la case **Manual (Manuel)**

 ©2025 Palo Alto Networks, Inc.

est cochée, ce qui indique qu'un utilisateur mobile peut sélectionner manuellement n'importe laquelle de ces passerelles.



 ©2025 Palo Alto Networks, Inc.

Utilisateurs mobiles : Proxy explicite

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Prisma Access de Palo Alto Networks est une solution SSE (Security Service Edge) qui offre des fonctionnalités SWG cloud de premier ordre, y compris un filtrage avancé des URL, un décryptage SSL, un contrôle des applications SaaS et une prévention avancée des menaces. Prisma Access opérationnalise les déploiements de sécurité de nouvelle génération avec une infrastructure cloud native omniprésente et toujours active, entièrement gérée par Palo Alto Networks. Les utilisateurs mobiles et les sites distants peuvent accéder en toute sécurité à Internet et aux applications SaaS conformément aux politiques de l'entreprise. Prisma Access offre des options de connectivité flexibles (fichiers PAC, agent, sans agent et IPSec de site à site) permettant de migrer toute architecture de proxy cloud héritée ou autre vers Prisma Access avec un minimum de changements dans la mise en réseau.

Proxy explicite

Prisma Access fournit une capacité SWG (passerelle web sécurisée) cloud complète, y compris une méthode de connexion par proxy explicite basée dans le cloud. Si le réseau existant de votre organisation utilise déjà des proxys explicites et déploie des fichiers PAC sur vos terminaux clients, vous pouvez effectuer en toute simplicité la migration des solutions SWG basées sur des proxys héritées vers Prisma Access pour sécuriser le trafic Internet sortant des utilisateurs mobiles. Vous pouvez également utiliser un proxy explicite si vous avez besoin d'un proxy pour des raisons de conformité. Le proxy explicite utilise la licence d'utilisateur mobile.

Si vous utilisez plusieurs fichiers PAC pour définir la façon de diriger le trafic web pour différents utilisateurs ou systèmes, Prisma Access vous donne la possibilité d'associer ces fichiers PAC à des profils de transfert afin que vous puissiez utiliser plusieurs fichiers PAC à la fois. De plus, les profils de transfert vous permettent de configurer des règles de transfert simples pour définir la direction du trafic web. Ainsi, vous n'avez même plus besoin de créer des fichiers PAC.

- Emplacements pris en charge
- Proxy explicite avec l'application GlobalProtect
  - GlobalProtect en mode proxy
  - GlobalProtect en mode tunnel et proxy
- Proxy explicite avec fichiers PAC
  - Configuration avec SAML
  - Configuration avec Kerberos

 ©2025 Palo Alto Networks, Inc.

- Profils de transfert
  - Prise en charge de plusieurs fichiers PAC
  - Règles de transfert
  - Profils de transfert avec GlobalProtect

Fonctionnalités du proxy explicite Prisma Access

Fonctionnalité	Description
App-ID	Classifie en continu toutes les applications indépendamment du port, du cryptage TLS/SSL ou de la technique utilisée par un attaquant pour échapper à la détection. Contrairement aux solutions héritées qui dépendent des couches 3 et 4 comme premières couches de contrôle avant que la classification des applications ne soit appliquée, Prisma Access applique App-ID avec d'autres contrôles de couche 7, tels que User-ID.
User-id	S'intègre à un large éventail de référentiels d'identité d'utilisateur afin que vos politiques suivent vos utilisateurs et groupes, peu importe leur emplacement.
Décryptage SSL	Inspecte le trafic crypté TLS/SSL et y applique la politique. Pour des raisons de confidentialité et de conformité réglementaire, vous pouvez activer ou désactiver le décryptage de manière flexible en fonction de l'URL, de la source, de la destination, de l'utilisateur, du groupe d'utilisateurs et du port.
Détection basée sur l'IA et le ML	Fournit une détection en ligne des attaques sans signature et une prévention des exploitations de type « zero-day ». Contrairement aux mises à jour programmées, Prisma Access peut s'adapter en fonction des menaces et offre une protection instantanée en temps réel. Il empêche instantanément jusqu'à 95 % des menaces inconnues, avec une livraison de signature de moins de 10 secondes, ce qui entraîne une réduction de 99,5 % des systèmes infectés.
Sécurité DNS	Applique des protections en temps réel et un apprentissage automatique en ligne pour perturber les rappels C2 et d'autres attaques utilisant le DNS. Intégré nativement à Prisma Access, Advanced DNS Security fournit des protections automatisées, empêchant les attaquants de contourner les mesures de sécurité, et élimine la nécessité d'utiliser des outils indépendants ou de modifier le routage DNS.
URL Filtering avancé	Protection supérieure contre les menaces web, telles que l'hameçonnage, les logiciels malveillants et les attaques C2, qui associe de puissantes protections de base de données à un moteur de sécurité web alimenté par le ML qui catégorise et bloque les nouvelles URL malveillantes en temps réel. La protection contre l'hameçonnage à la pointe du secteur s'attaque aux causes les plus

 ©2025 Palo Alto Networks, Inc.

Fonctionnalité	Description
	courantes des violations, vous permettant de reprendre le contrôle de votre trafic web grâce à des paramètres de politique et des contrôles granulaires qui automatisent les actions de sécurité en fonction des utilisateurs, des cotes de risque et des catégories de contenu.
Prévention avancée des menaces	Arrêtez les menaces de type « zero-day », les exploitations connues, les logiciels malveillants, les logiciels espions et les techniques de commande et contrôle (C2) malveillantes grâce à une prévention des menaces à la pointe du secteur. Prévenez 60 % d'attaques par injection inconnues en plus et 48 % de trafic C2 hautement évasif en plus qu'avec un système de prévention des intrusions traditionnel.
Advanced WildFire	Assurez la sécurité des fichiers en empêchant automatiquement les logiciels malveillants connus, inconnus et très évasifs 60 fois plus rapidement grâce au plus grand moteur de renseignements sur les menaces et de prévention des logiciels malveillants du secteur.
NG-CASB*	Obtenez une visibilité SaaS proactive, une protection contre les erreurs de configuration et une protection des données en temps réel pour une sécurité SaaS de premier ordre.
Data Loss Prevention (prévention des pertes de données – DLP)*	Comprend un ensemble d'outils et de processus qui vous permettent de protéger les informations sensibles contre les utilisations abusives et les accès, les extractions et les partages non autorisés. La DLP sur Prisma Access vous permet d'appliquer des politiques de sécurité des données et d'empêcher la perte de données sensibles chez les utilisateurs mobiles et sur les réseaux distants.
Prise en charge de l'isolation de navigateur à distance	Grâce à CloudBlades, cette fonctionnalité s'intègre aux clouds RBI tiers en tirant parti des fonctionnalités de catégorisation d'URL et de réécriture d'URL NGFW existantes pour rediriger le trafic Internet, en tout ou en partie, vers le cloud RBI. Cette capacité offre une expérience utilisateur fluide tout en transférant certains trafics (inconnus ou à haut risque) à RBI pour un examen supplémentaire, tandis que le reste du trafic peut être inspecté par Prisma Access et sortir directement sur Internet.
Création de rapports	Comprend par défaut un rapport détaillé et personnalisable sur l'utilisation des applications SaaS qui fournit un aperçu de tout le trafic SaaS (qu'il soit autorisé ou non) sur votre réseau. Vous pouvez également créer des rapports personnalisés en fonction de vos besoins et les programmer, les télécharger et les partager facilement avec d'autres personnes de votre organisation.
Authentification de l'utilisateur	Prend en charge toutes les méthodes d'authentification PAN-OS existantes, y compris Kerberos, RADIUS, SAML, LDAP, les certificats clients et une base de données d'utilisateurs locale. Avec PAC uniquement, prend en charge Kerberos et SAML.

 ©2025 Palo Alto Networks, Inc.

Fonctionnalité	Description
VPN IPsec de site à site	Prend en charge les tunnels de site à site sur IPv4 et IKEv1/IKEv2 pour garantir la compatibilité. Si vous avez plusieurs sites de connexion, le routage ECMP peut offrir une redondance supplémentaire et améliorer la rentabilité en équilibrant les sessions sur les connexions Internet disponibles.
de journalisation	Affiche la journalisation globale du trafic, des applications, des utilisateurs, des menaces, des URL et des filtres de données pour faciliter l'organisation des données via Strata Logging Service, un service de journalisation basé sur le cloud.
Profils de transfert	Permet l'utilisation de plusieurs fichiers PAC pour différents groupes d'utilisateurs ou systèmes. Prend également en charge la création de règles de transfert pour la définition de la direction du trafic web afin de fournir une solution plus simple que la création et à la maintenance d'un fichier PAC.

* Nécessite une licence de module complémentaire.

Pour obtenir une description détaillée des fonctionnalités et des capacités du produit, consultez la fiche technique de Prisma Access.

Directives de configuration du proxy explicite

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Configuration système requise et fonctionnalités prises en charge

Il s'agit de la configuration système requise et des fonctionnalités prises en charge pour les différentes méthodes de connexion que vous pouvez utiliser avec le proxy explicite.

	SAML sans agent	**Kerberos sans agent**	**Mode proxy sur l'agent (nécessite GP 6.2 ou version ultérieure)**	**Mode proxy sur les réseaux distants**
Prise en charge des applications et des systèmes d'exploitation				
Type de trafic	Trafic Internet et SaaS public uniquement	Trafic Internet et SaaS public uniquement	Trafic Internet et SaaS public uniquement	Trafic Internet et SaaS public uniquement

 ©2025 Palo Alto Networks, Inc.

Supports de protocole	Proxy prenant en charge HTTP ou HTTPS	Proxy prenant en charge HTTP ou HTTPS	Proxy prenant en charge HTTP ou HTTPS	Proxy prenant en charge HTTP ou HTTPS
Canal de transport vers Prisma Access	Connexion HTTP	Connexion HTTP	Connexion HTTP dans TLS	Connexion HTTP dans IPSec de la branche au nœud de traitement de sécurité (SPN, security processing node) du réseau distant
Environnements pris en charge	Windows, Mac, Linux, ChromeOS, VDI	Windows, Mac, Linux, ChromeOS, VDI	Windows et Mac	Windows, Mac, Linux, ChromeOS, VDI
Prises en charge des applications	Applications HTTP(s) prenant en charge le proxy	Toute application qui respecte un fichier PAC ou un paramètre de proxy système et qui prend en charge Kerberos	Applications HTTP(s) prenant en charge le proxy	Applications HTTP(s) prenant en charge le proxy
Prise en charge des navigateurs	Chrome#, Edge, Firefox version 115 ou ultérieure	Chrome#, Edge, Firefox version 115 ou ultérieure	Chrome#, Edge, Firefox version 115 ou ultérieure*	Chrome#, Edge, Firefox version 115 ou ultérieure
Prise en charge d'O365†	Navigateur et applications clientes	Navigateur et applications clientes	Navigateur et applications clientes	Navigateur et applications clientes
Identité				
User-ID‡	Trafic CORS déchiffré et non HTTP	Tout le trafic pris en charge	Tout le trafic pris en charge	Selon que vous utilisez SAML ou Kerberos : trafic d'utilisateur X-authentifié déchiffré/non CORS

©2025 Palo Alto Networks, Inc.

Authentification prise en charge	SAML (n'importe quel IDP SAML 2.0 ou via CIE)	Kerberos	Toutes les authentifications prises en charge par GlobalProtect	SAML, Kerberos, basé sur l'utilisateur X-authentifié
Ignorer l'authentification	Par domaine et par adresse IP source	Par domaine et par adresse IP source	Par domaine	Par domaine et par adresse IP source
Annuaire de groupes d'utilisateurs	Tous les annuaires pris en charge par CIE	Tous les annuaires pris en charge par CIE	Tous les annuaires pris en charge par CIE	Tous les annuaires pris en charge par CIE
Licence	Unité d'utilisateur mobile par utilisateur	Unité d'utilisateur mobile par utilisateur	Unité d'utilisateur mobile par utilisateur	Unité d'utilisateur mobile par utilisateur ou appareil sans tête et unités NET pour la bande passante pour les réseaux distants
Gestion				
Panorama multilocataire	Pris en charge sur le premier locataire	Pris en charge sur le premier locataire	Pris en charge sur le premier locataire	Pris en charge sur le premier locataire
Cloud Management multilocataire	Pris en charge	Pris en charge	Pris en charge	Pris en charge
Services de sécurité				
SaaS Inline	Pris en charge	Pris en charge	Pris en charge	Pris en charge
DLP	Pris en charge	Pris en charge	Pris en charge	Pris en charge
Sécurité DNS§	Pris en charge	Pris en charge	Pris en charge	Pris en charge
URL Filtering avancé	Pris en charge	Pris en charge	Pris en charge	Pris en charge
Advanced WildFire	Pris en charge	Pris en charge	Pris en charge	Pris en charge

 ©2025 Palo Alto Networks, Inc.

Prévention avancée des menaces	Pris en charge	Pris en charge	Pris en charge	Pris en charge
Isolation du navigateur distant	Pris en charge	Pris en charge	Pris en charge	Pris en charge
Visibilité et application d'adresse IP privée	Non pris en charge	Non pris en charge	Pris en charge pour les sites ou les branches connus	Pris en charge
NAT de sortie	Pris en charge	Pris en charge	Pris en charge	Pris en charge
Accès privé de l'application	Non pris en charge	Non pris en charge	Pris en charge via les connexions aux services	Non pris en charge
Tout le trafic TCP	Non pris en charge	Non pris en charge	Pris en charge (avec GlobalProtect version 6.3.1)	Non pris en charge
Connecteur ZTNA	Non pris en charge	Non pris en charge	Pris en charge	Non pris en charge
Colo Connect	Non pris en charge	Non pris en charge	Pris en charge	Non pris en charge
Connexions aux services	Pris en charge	Pris en charge	Pris en charge	Pris en charge
Prise en charge HIP (mode tunnel et proxy)	Non pris en charge	Non pris en charge	Pris en charge	Non pris en charge

Pour le navigateur Chrome, suivez les instructions ci-dessous pour désactiver TLS 1.3 Kyber, si le décryptage est activé :

1. Ouvrez le navigateur Chrome.
2. Ajoutez `chrome://flags/#enable-tls13-kyber` dans la barre d'adresse et désactivez-le.
3. Cliquez sur **Relaunch (Relancer)**.

* Pour le mode proxy sur l'agent, Firefox nécessite une règle de politique manuelle via Mobile Device Management (Gestion des appareils mobiles - MDM) qui lui ordonne de respecter le proxy système

 ©2025 Palo Alto Networks, Inc.

† Le proxy explicite ne prend en charge que le trafic HTTP, et non UDP. Avec SAML, le proxy explicite ne fournit pas User-ID pour les flux d'applications clientes. Pour le proxy de l'agent, vous devez utiliser un fichier PAC pour envoyer les flux d'authentification de l'application cliente au proxy cloud.

‡ Aucun User-ID n'est disponible pour le contournement d'authentification.

§ Vous ne pouvez pas appliquer de profils de sécurité DNS aux flux de proxy explicite. Bloquez les domaines à la place.

Considérations relatives à la prise en charge des applications

1. Le proxy explicite ne prend pas en charge les applications qui nécessitent une affinité IP. L'application doit prendre en charge le trafic provenant de plusieurs adresses IP pour une session utilisateur donnée.
2. Le proxy explicite rétrograde les flux HTTP/2 déchiffrés vers HTTP/1.
3. Le proxy explicite ne récupère pas les listes dynamiques externes locales.
4. SAML sans agent uniquement :
    1. Configurez une politique de décryptage SSL pour autoriser le contournement de l'authentification par domaine pour le proxy explicite basé sur PAC sans agent avec authentification SAML

        Le décryptage est nécessaire pour que Prisma Access puisse lire le cookie d'état d'authentification configuré par Prisma Access sur le navigateur de l'utilisateur mobile. Le fait de ne pas appliquer le décryptage permet d'abuser du proxy explicite en tant que proxy ouvert que les attaquants peuvent utiliser comme service de transfert pour les attaques par déni de service.
    2. Dans les journaux du trafic, le proxy explicite affichera les journaux de trafic des utilisateurs mobiles non décryptés et HTTP-CORS en tant qu'utilisateurs authentifiés SWG.
    3. Prenez note des exigences et des directives d'utilisation suivantes pour les navigateurs :
        - Si vous utilisez un proxy explicite, ne désactivez pas les cookies dans votre navigateur. Si vous le faites, vous ne pouvez pas parcourir les pages Web.
        - Si vous utilisez un proxy explicite avec Microsoft Edge, veillez à définir **Settings (Paramètres)** > **Privacy, Search, and Services (Confidentialité, recherche et services)** > **Tracking prevention (Prévention du suivi)** sur **Basic (Basique)**.

Exigences de connectivité

Si les utilisateurs mobiles se connectent à partir de sites distants, de sièges sociaux ou de centres de données à l'aide d'un proxy explicite, le terminal de l'utilisateur mobile doit être en mesure d'atteindre et d'acheminer vers l'IdP, le FQDN ACS, l'URL du proxy explicite et l'URL du fichier PAC hébergé par Prisma Access.

Exigences et directives relatives aux fichiers PAC : suivez la section Directives relatives aux fichiers PAC lorsque vous configurez le fichier PAC à utiliser avec le proxy explicite.

Directives de chaînage de proxy : si vous utilisez le chaînage de proxy d'un proxy tiers vers un proxy explicite, spécifiez l'**Explicit Proxy URL (URL du proxy explicite)** dans le proxy tiers pour transférer le trafic vers le proxy explicite

 ©2025 Palo Alto Networks, Inc.

Prise en charge sur site : le proxy explicite est une solution de proxy basée sur le cloud et non un produit sur site. Pour une solution de proxy sur site, configurez un proxy Web PAN-OS.

GlobalProtect en mode proxy

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager) Si vous souhaitez utiliser cette fonctionnalité dans votre Prisma Access environnement, contactez votre équipe de compte pour en savoir plus.	• Prisma Access 5.2 • Application GlobalProtect version 6.2 pour Windows ou macOS • Version du contenu 8700-7994 • Licence d'utilisateur mobile Prisma Access

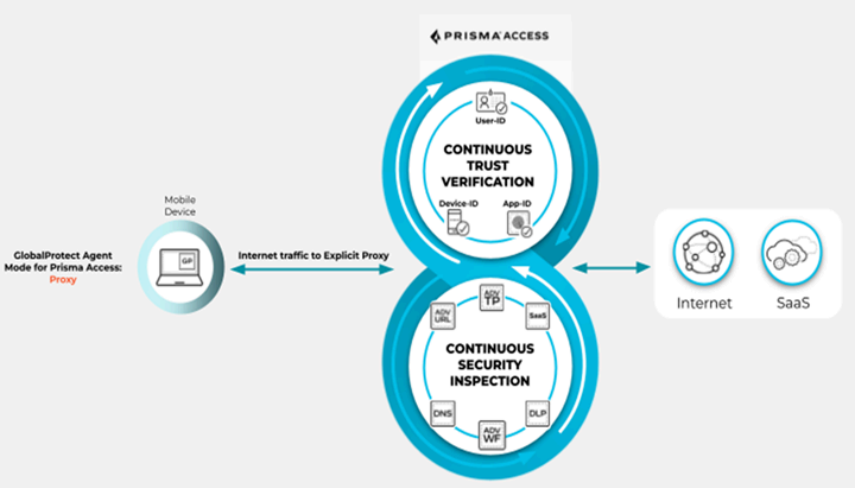
Avec le mode **Proxy**, l'application GlobalProtect assure une sécurité Internet permanente. Dans ce mode, l'application GlobalProtect transmet par proxy le trafic vers Prisma Access selon les règles de transfert et la logique du fichier PAC, hébergé dans Prisma Access ou dans votre environnement. Cela est utile si vous disposez d'une architecture proxy existante (héritée) ou si vous devez la maintenir pour des raisons réglementaires ou de conformité.

La fonctionnalité de proxy basé l'agent facilite la coexistence et l'interopérabilité de l'application GlobalProtect avec les VPN tiers, dans lesquels vous pouvez sécuriser le trafic Internet de vos utilisateurs mobiles via l'application GlobalProtect vers le proxy explicite et utiliser le VPN tiers de votre choix pour sécuriser l'accès aux applications privées.

Vous avez besoin de Strata Cloud Manager et l'agent GlobalProtect version 6.3.0 pour le canal proxy GlobalProtect afin de prendre en charge toutes les connexions TCP IPv4, y compris le trafic non envoyé au proxy. Pour garantir une fonctionnalité fluide, le DNS configuré sur les terminaux doit être en mesure de résoudre le FQDN de destination.

Dans ce scénario, l'application GlobalProtect envoie le trafic Internet à Prisma Access en fonction des règles du fichier PAC que vous définissez, tandis que le terminal achemine l'accès à vos applications privées via un VPN tiers à l'aide d'un tunnel IPSec/TLS.

 ©2025 Palo Alto Networks, Inc.



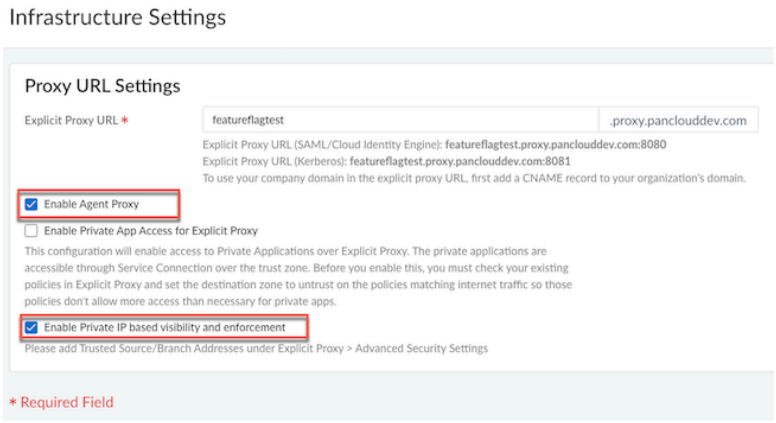
- Strata Cloud Manager
- Panorama

GlobalProtect en mode proxy (Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Activez la fonctionnalité de proxy basé sur l'agent pour les utilisateurs mobiles sur Prisma Access.

1. Activez le proxy explicite.
   1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Mobile Users (Utilisateurs mobiles)** et cliquez sur **Explicit Proxy Setup (Configuration du proxy explicite)**.
   2. Dans la zone Infrastructure Settings (Paramètres d'infrastructure), cliquez sur **Setup Proxy Settings (Configurer les paramètres de proxy)** et spécifiez une **Explicit Proxy URL (URL de proxy explicite)**.
2. Sélectionnez les options **Enable Agent Proxy (Activer le proxy de l'agent)** et, optionnellement, **Enable Private IP based visibility and enforcement (Activer la visibilité et l'application basées sur l'IP privée)**, puis cliquez sur **Save (Enregistrer)**.



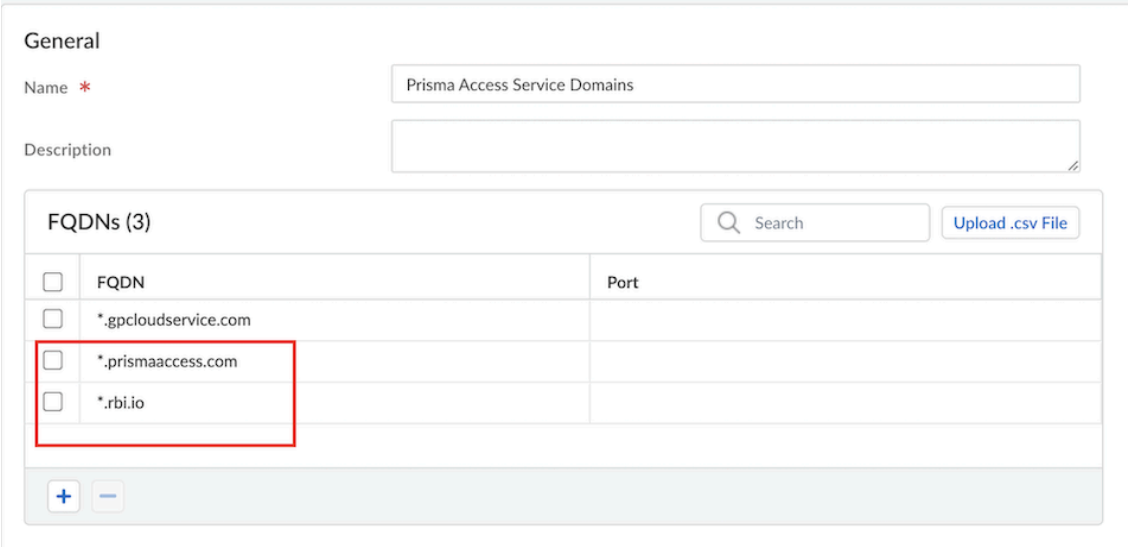
3. Sélectionnez les emplacements Prisma Access où vous souhaitez prendre en charge les utilisateurs mobiles.

   Pour une expérience utilisateur optimale, si vous limitez le nombre d'emplacements, choisissez les emplacements les plus proches de vos utilisateurs finaux. Si aucun

 ©2025 Palo Alto Networks, Inc.

emplacement n'est disponible dans le pays où résident vos utilisateurs mobiles, choisissez l'emplacement le plus proche des utilisateurs mobiles.

4. Créez un profil de transfert pour définir le trafic que vous souhaitez envoyer via le proxy explicite. Lors de la configuration du profil de transfert, ignorez les domaines *.prismaaccess.com et *.gpcloudservice.com



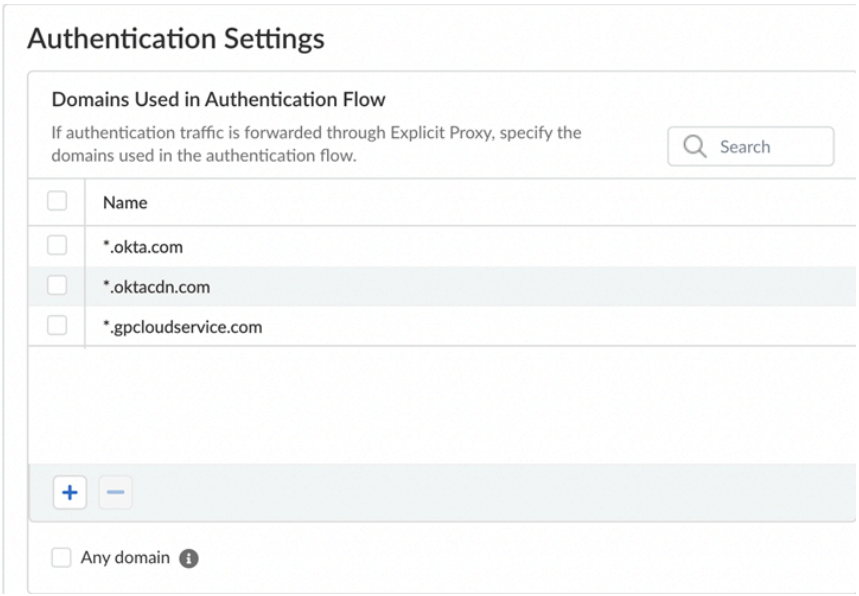
5. Associez le profil de transfert à la configuration de votre application GlobalProtect.
6. Sélectionnez **Workflows (Flux de travail)** > **Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Advanced Security Settings (Paramètres de sécurité**

 ©2025 Palo Alto Networks, Inc.

avancés) > **Authentication Settings (Paramètres d'authentification)** et ajoutez les domaines que vous devez contourner.

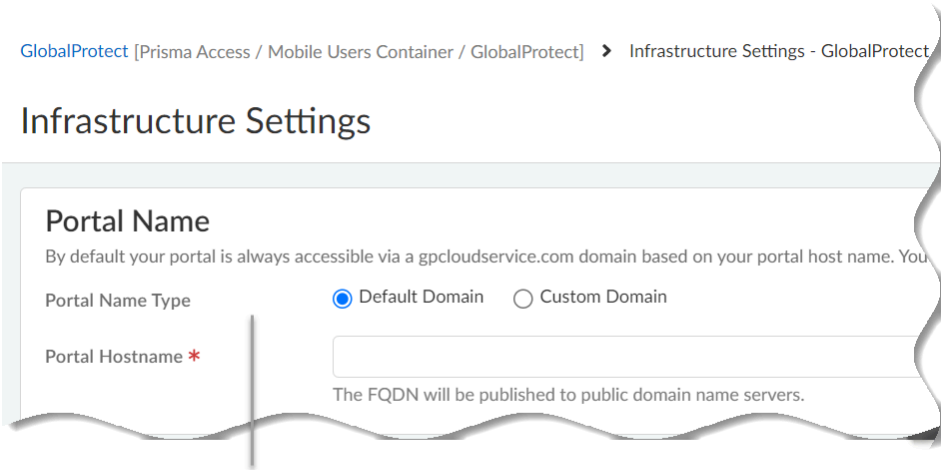
Toutes les requêtes adressées au proxy sont soumises à une authentification. Cependant, si vous transmettez des flux IdP via le proxy, vous devez les contourner pour que l'authentification réussisse.

Dans cet exemple, nous contournons le portail GlobalProtect et Okta, mais veuillez les personnaliser en fonction des IdP que vous utilisez.



STEP 2 | Configurez le portail GlobalProtect, l'authentification et le mode proxy pour l'application GlobalProtect.

1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **Infrastructure** > **Infrastructure Settings (Paramètres d'infrastructure)** et indiquez le **Portal Name (Nom du portail)**.



GlobalProtect Infrastructure Settings

- **Default Domain (Domaine par défaut)** : si vous sélectionnez cette option, le nom d'hôte de votre portail utilise le nom du domaine par défaut :

 ©2025 Palo Alto Networks, Inc.

`.gpcloudservice.com`. Dans ce cas, il suffit de saisir un **Portal Hostname (Nom d'hôte du portail)** à ajouter au nom du domaine par défaut. Prisma Access pour les utilisateurs créera automatiquement les certificats nécessaires et publiera le nom d'hôte sur les serveurs DNS publics.

- **Custom Domain (Domaine personnalisé)** : vous pouvez également personnaliser l'adresse du portail si vous souhaitez que le domaine du nom d'hôte du portail corresponde au nom du domaine de votre entreprise (par exemple, myportal.mydomain.com).

2. Permettez aux utilisateurs mobiles de s'authentifier auprès de Prisma Access.
3. Activez le mode proxy GlobalProtect pour Prisma Access dans les paramètres de l'application GlobalProtect pour envoyer du trafic Internet au proxy basé sur l'agent.

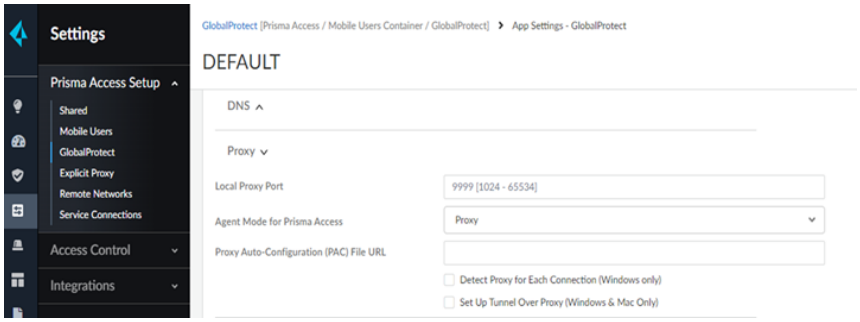
   La méthode de connexion GlobalProtect ne s'applique pas en mode proxy, car elle est toujours activée.

   - Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect**.
   - Dans l'onglet **GlobalProtect App (Application GlobalProtect)**, cliquez sur **Default (Par défaut)** pour personnaliser les paramètres de l'application ou **Add App Settings (Ajouter les paramètres de l'application)** pour ajouter une nouvelle configuration.
   - Cliquez sur **Show Advanced Options (Montrer les options avancées)** ainsi que dans la section **App Configuration (Configuration de l'application)**.
   - Définissez l'option **Agent Mode for Prisma Access (Mode Agent pour Prisma Access)** sur **Proxy** pour demander à l'application GlobalProtect d'envoyer le trafic Internet au proxy explicite sur Prisma Access.
   - (Facultatif) Configurez le port de proxy local. La plage de ports est comprise entre 1024 et 65534 et le port par défaut est 9999. Si le port par défaut n'est pas disponible, GlobalProtect essaiera 10 autres ports dans la plage de 9999 à 10009 et utilisera le port qui est disponible. Vous pouvez également choisir votre propre numéro de port dans la plage.
   - (Facultatif) Configurez l'URL du fichier de configuration automatique (PAC) si vous souhaitez transmettre une nouvelle URL PAC pour les paramètres de proxy au terminal. L'URL PAC transmet vers le terminal une fois que l'utilisateur se connecte. Lorsque l'utilisateur déconnecte l'application GlobalProtect, les configurations de proxy de terminal sont automatiquement désactivées et reviennent aux paramètres précédents.
   - (Facultatif) Autorisez l'utilisateur à redécouvrir le réseau si vous souhaitez que l'utilisateur vérifie le portail pour tout nouveau paramètre.
   - (Facultatif) Configurez l'intervalle de rafraîchissement de configuration de l'application GlobalProtect (heures). Par défaut, le client GlobalProtect actualise la configuration

 ©2025 Palo Alto Networks, Inc.

du portail mise en cache toutes les 24 heures. Vous pouvez changer l'intervalle de rafraîchissement en fonction de vos besoins commerciaux.

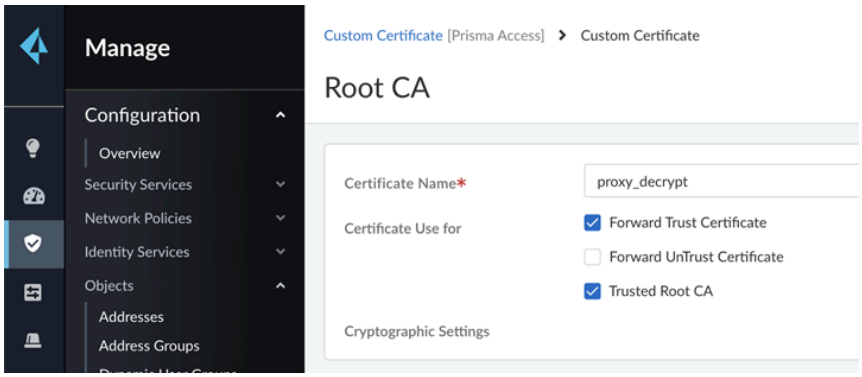
- Désactivez l'option **Set Up Tunnel Over Proxy (Windows & Mac Only) (Définir le proxy du tunnel (Windows et Mac uniquement))**.



4. Activez la sécurité Internet toujours active en configurant les paramètres suivants sur la page **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Application GlobalProtect)** > **Add App Settings (Ajouter les paramètres de l'application)** :
   1. Définissez l'option Disable GlobalProtect (Désactiver GlobalProtect) sur **Disallow (Ne pas autoriser)**, **Allow with Passcode (Autoriser avec mot de passe)** ou **Allow with Ticket (Autoriser avec ticket)**.
   2. Désactivez l'option Allow user to Sign Out from GlobalProtect App (Autoriser l'utilisateur à se déconnecter de l'application GlobalProtect).

STEP 3 | Configurez le décryptage pour le trafic proxy explicite.

- Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Decryption (Décryptage)**.
- Si vous activez le décryptage, assurez-vous de configurer le certificat de décryptage en tant que CA racine approuvée.



STEP 4 | Configurez les règles de politique de sécurité pour le trafic du proxy explicite.

- Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)**.
- Suivez les meilleures pratiques des politiques de sécurité des passerelles Internet.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Facultatif) Configurez l'application GlobalProtect en mode proxy dans réseau d'itinéraires autre que celui par défaut.

- (Facultatif) Hébergez un fichier PAC en interne et ajoutez le FQDN du proxy explicite Prisma Access en tant que proxy dans le fichier PAC ou hébergez le fichier PAC dans un Forwarding Profile (Profil de transfert) et ajoutez des itinéraires à votre réseau pour PAC service IP addresses (Adresses IP de service PAC).
- Dans le fichier PAC, transférez l'URL de l'IdP et l'URL du portail Prisma Access vers le proxy explicite.
- Sur le proxy explicite, excluez l'URL de l'IdP et du portail des paramètres d'authentification. Ajoutez l'URL de l'IdP et du portail au domaine utilisé dans les flux d'authentification.
- Configurez des itinéraires vers le FQDN du proxy explicite ou des adresses IP sur les périphériques de périmètre pour permettre aux utilisateurs d'accéder à Internet via le proxy explicite.
- (Facultatif) Ajoutez des enregistrements DNS pour résoudre le FQDN du proxy explicite Prisma Access à une adresse IP interne si les utilisateurs ne peuvent pas résoudre les domaines publics dans le réseau de succursales, et ajoutez le NAT de destination pour l'adresse IP interne au FQDN du proxy explicite ou à l'adresse IP.

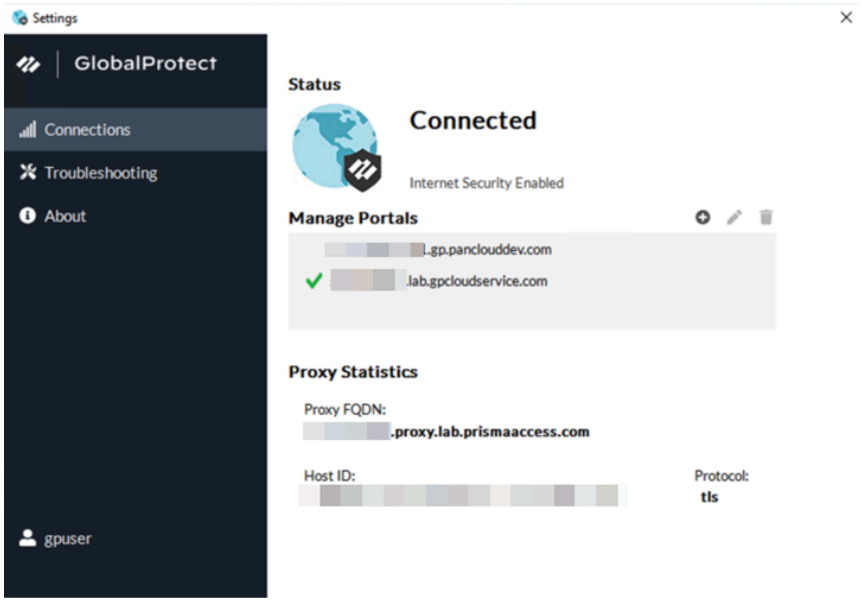
STEP 6 | Cliquez sur **Save (Enregistrer)** et sélectionnez **Push Config (Transmettre la configuration)** à **GlobalProtect** et à l'**Explicit Proxy (Proxy explicite)**.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Vérifiez et dépannez le déploiement du proxy de l'agent.

1. Vérifiez les informations relatives à votre connexion réseau dans l'onglet **Connections (Connexions)** sous **Settings (Paramètres)** de l'application GlobalProtect.

   1. Ouvrez l'application GlobalProtect.
   2. Sélectionnez **Settings (Paramètres)** pour ouvrir le panneau GlobalProtect Settings (Paramètres de GlobalProtect), puis sélectionnez **Connections (Connexions)**.



2. Affichez et collectez les journaux GlobalProtect.

   Consultez le journal PanGPS pour vérifier la configuration du mode proxy sur le portail GlobalProtect.

   Vous pouvez vérifier que le mode proxy est configuré en recherchant l'événement suivant dans le journal PanGPS :

   ```
   OnProxyAgentMode : mode proxy uniquement
   ```

   Pour afficher les journaux GlobalProtect dans , sélectionnez **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)** et :

   - **GlobalProtect** pour les journaux d'authentification, et
   - **Traffic (Trafic)** et **Decryption (Décryptage)** pour les journaux d'accès utilisateur.

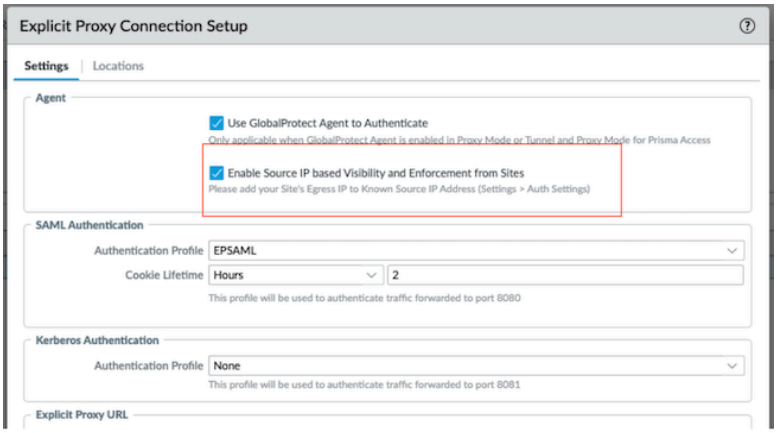
GlobalProtect en mode proxy (Panorama)

Si vous convertissez un déploiement à locataire unique Prisma Access (Managed by Panorama) en déploiement multilocataire, seul le premier locataire (le locataire que vous avez migré) prend en charge cette fonctionnalité. En outre, dans ce premier locataire, vous devez configurer vos règles de politique dans le Explicit_Proxy_Device_Group prédéfini plutôt que dans un groupe de périphériques personnalisé. Aucun des locataires que vous créez ensuite pour le déploiement multilocataire après le premier ne prend en charge cette fonctionnalité.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Activez la fonctionnalité de proxy basé sur l'agent pour les utilisateurs mobiles.

1. Activez le proxy explicite.
   1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—Explicit Proxy (Utilisateurs mobiles — proxy explicite)**.
   2. Vous devez **Configure (Configurer)** la configuration du proxy explicite pour spécifier une **Explicit Proxy URL (URL de proxy explicite)**.
2. Sélectionnez **Use GlobalProtect app to Authenticate (Utiliser l'application GlobalProtect pour s'authentifier)** pour activer la fonctionnalité de proxy basé sur l'agent et, optionnellement, **Enable Source IP based Visibility and Enforcement from Sites (Activer la visibilité et l'application basées sur l'adresse IP source à partir des sites)**.



3. Entrez l'URL du **PAC (Proxy Auto-Configuration) File (Fichier PAC (Proxy Auto-Configuration))**. Assurez-vous d'entrer un port de 8080 dans le fichier PAC.
   - Assurez-vous d'entrer un port de 8080 dans le fichier PAC.
   - L'énoncé du proxy dans le fichier PAC doit utiliser le FQDN Prisma Access que vous avez configuré ci-dessus.
   - Le fichier PAC doit être configuré pour contourner le trafic VPN tiers.

   Échantillon de fichier PAC :

```
function FindProxyForURL (url, host) { /* Bypass localhost
 and Private IPs * / var resolved_ ip = dnsResolve (host) ;
 if (isplainHostName (host) || shExpMatch (host,"* ,local")
 || isInNet (resolved_ip,"10.0.0.0", "255.0.0.0") ||
 isInNet (resolved ip,"172.16.0.0","255.240.0.0") ||
 isInNet (resolved_ip,"192.168.0.0","255.255.0.0") ||
 isInNet (resolved ip, "127.0.0.0", "255.255.255.0" ))
 return "DIRECT"; /* Bypass Non-HTTP * / if (url.substring
 (0,4) == "ftp: ") return "DIRECT"; /* Bypass VPN */ if
 (shExpMatch (host, "vpn. acme.com") || shExpMatch (host,
 "gateway. acme.com" )) return "DIRECT"; /* Bypass Private
 Apps */ if (shExpMatch (host,"internalapps. acme.com" ) )
 return "DIRECT"; /* Forward to  */ return "PROXY acme-
demo.proxy.prismaaccess.com: 8080";}
```

4. Sélectionnez le **Connection Name (Nom de connexion)** pour la configuration du proxy explicite que vous avez configuré.

 ©2025 Palo Alto Networks, Inc.

5. Sélectionnez les **Locations (Emplacements)** et les régions dans lesquels vous souhaitez déployer votre proxy explicite pour les utilisateurs mobiles.

   Prisma Access ajoute un nœud proxy à chaque emplacement que vous sélectionnez. Le proxy explicite prend en charge un sous-ensemble de tous les emplacements Prisma Access. Pour une expérience utilisateur optimale, si vous limitez le nombre d'emplacements, choisissez les emplacements les plus proches de vos utilisateurs finaux. Si aucun emplacement n'est disponible dans le pays où résident vos utilisateurs mobiles, choisissez l'emplacement le plus proche des utilisateurs mobiles.

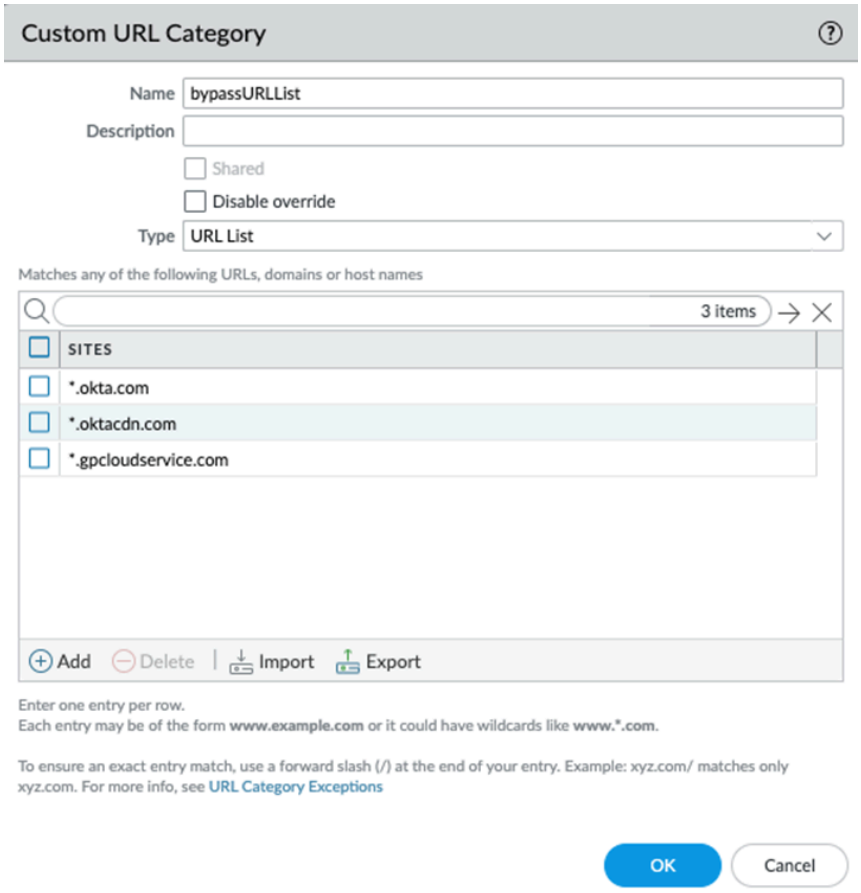
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Contournez les fournisseurs d'identité (IDP).

Toutes les requêtes adressées au proxy sont authentifiées. Cependant, si vous transmettez des flux IDP via le proxy, vous devez les contourner pour que l'authentification réussisse.

Dans cet exemple, nous contournons le portail GlobalProtect et Okta, mais veuillez les personnaliser en fonction des IDP que vous utilisez.

1. Avec **Explicit_Proxy_Device_Group** sélectionné, sélectionnez **Object (Objet)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)** et créez une catégorie d'URL personnalisée.
2. Dans la catégorie Custom URL (URL personnalisée), ajoutez tous les domaines FQDN qui doivent être contournés depuis l'authentification EP.



3. Sélectionnez **Cloud Services** > **Configuration** > **Mobile Users (Utilisateurs mobiles)** > **Explicit Proxy (Proxy explicite)** > **Settings (Paramètres)** > **Authentication Settings (Paramètres d'authentification)** et joignez la catégorie Custom URL (URL personnalisée).



4. Validez et appliquez vers le **Explicit_Proxy_Device_Group**.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configurez le portail GlobalProtect.

En mode proxy, la méthode de connexion que vous définissez ne modifie pas le comportement de la fonctionnalité proxy. Même si vous définissez une méthode de connexion à la demande, tout le trafic Internet passera toujours par le proxy pour une sécurité Internet permanente.

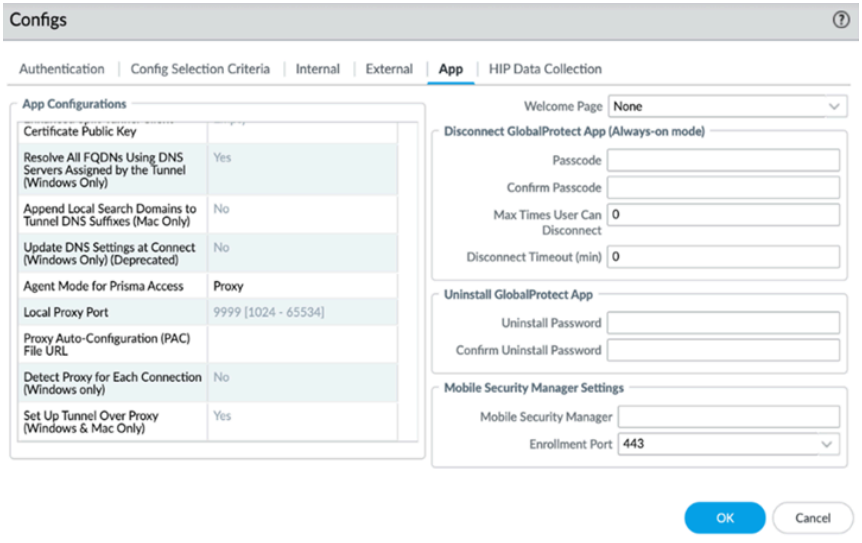
1. Dans la section Onboarding (Intégration), cliquez sur **Configure (Configurer)**.
2. Dans l'onglet **General (Général)**, spécifiez le**Portal Name Type (Type de nom de portail)** :

   Use Default Domain (Utiliser le domaine par défaut) : si vous sélectionnez cette option, le nom d'hôte de votre portail utilise le nom du domaine par défaut : .gpcloudservice.com. Dans ce cas, il vous suffit d'entrer un nom d'hôte de portail à ajouter au nom du domaine par défaut. Prisma Access créera automatiquement les certificats nécessaires et publiera le nom d'hôte sur les serveurs DNS publics.

   Use Company Domain (Utiliser le domaine de l'entreprise) : sélectionnez cette option si vous souhaitez que le domaine dans le nom d'hôte du portail corresponde au nom du domaine de votre entreprise (par exemple, myportal.mydomain.com).
3. Sélectionnez un **Authentication Profile (Profil d'authentification)** qui précise comment Prisma Access doit authentifier les utilisateurs mobiles ou en créer un nouveau.
4. (Facultatif) Sélectionnez un **Authentication Override Certificate (Certificat de remplacement de l'authentification)** pour crypter les cookies sécurisés que les utilisateurs mobiles utilisent pour s'authentifier sur le portail et la passerelle.

STEP 4 | Activez le mode proxy sur GlobalProtect.

1. Sélectionnez **Network (Réseau)** > **GlobalProtect Portals (Portails Globalprotect)**.
2. Sélectionnez la configuration du portail à laquelle vous ajoutez la configuration de l'agent, puis sélectionnez l'onglet **Agent**.
3. Dans l'onglet **Agent**, sélectionnez **App (Application)**.
4. Dans la zone App Configurations (Configurations de l'application), définissez l'option **Agent Mode for Prisma Access (Mode agent pour Prisma Access)** sur **Proxy** pour envoyer le trafic Internet au proxy basé sur l'agent GlobalProtect.



 ©2025 Palo Alto Networks, Inc.

STEP 5 | Effectuez des configurations facultatives.

1. (Facultatif) Configurez le port de proxy local. La plage de ports est comprise entre 1024 et 65534 et le port par défaut est 9999. Si le port par défaut n'est pas disponible, GlobalProtect essaiera 10 autres ports dans la plage de 9999 à 10009 et utilisera le port qui est disponible. Vous pouvez également choisir votre propre numéro de port dans la plage.
2. (Facultatif) Configurez l'URL du fichier de configuration automatique (PAC) si vous souhaitez transmettre une URL PAC personnalisée pour les paramètres de proxy au terminal. L'URL PAC transmet vers le terminal une fois que l'utilisateur se connecte. Lorsque l'utilisateur déconnecte l'application GlobalProtect, les configurations de proxy de terminal sont automatiquement désactivées et reviennent aux paramètres précédents.
3. (Facultatif) Autorisez l'utilisateur à redécouvrir le réseau si vous souhaitez que l'utilisateur vérifie le portail pour tout nouveau paramètre.
4. (Facultatif) Configurez l'intervalle de rafraîchissement de configuration de l'application GlobalProtect (heures). Par défaut, le client GlobalProtect actualise la configuration du portail mise en cache toutes les 24 heures. Vous pouvez changer l'intervalle de rafraîchissement en fonction de vos besoins commerciaux.

STEP 6 | Activez la sécurité Internet toujours active en configurant les paramètres suivants :

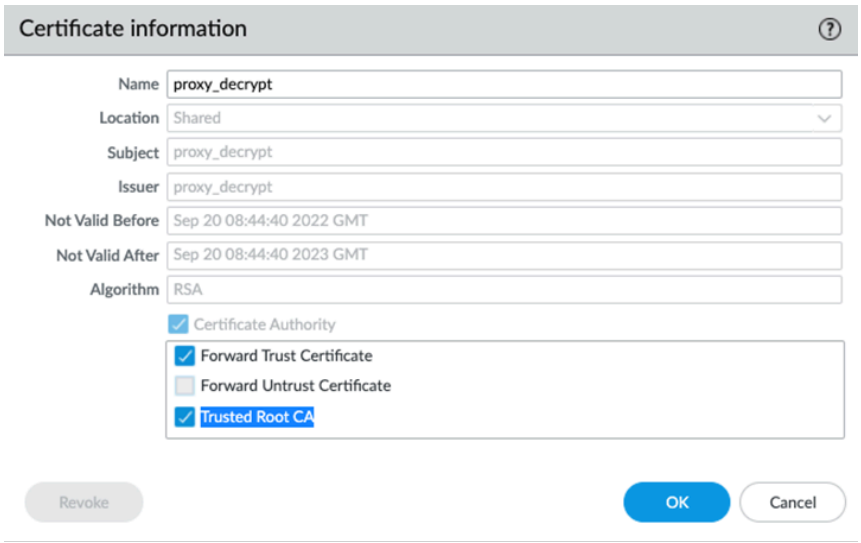
1. Définissez l'option Allow User to Disable GlobalProtect (Autoriser l'utilisateur à désactiver GlobalProtect) sur **Disallow (Ne pas autoriser)**, **Allow with Passcode (Autoriser avec mot de passe)** ou **Allow with Ticket (Autoriser avec ticket)**.
2. Définissez l'option Allow user to Sign Out from GlobalProtect App (Autoriser l'utilisateur à se déconnecter de l'application GlobalProtect) sur **No (Non)**.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | (Facultatif) Configurez la politique de décryptage pour le trafic proxy explicite.

Si vous activez le décryptage, assurez-vous que le certificat de décryptage est également configuré en tant que CA racine approuvée.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** et créez un certificat qui est une CA racine approuvée et un certificat d'approbation de transfert.



2. Créez une règle de décryptage sous **Explicit_Proxy_Device Group** avec un proxy de transfert SSL.

STEP 8 | Configurez les règles de politique de sécurité pour le trafic du proxy explicite.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Définissez **Device Group (Groupe de périphériques)** sur **Explicit_Proxy_Device_Group**.
3. Suivez les meilleures pratiques des politiques de sécurité des passerelles Internet.

STEP 9 | (Facultatif) Configurez l'application GlobalProtect en mode proxy dans un réseau d'itinéraires autre que celui par défaut.

- (Facultatif) Hébergez un fichier PAC en interne et ajoutez le FQDN du proxy explicite Prisma Access en tant que proxy dans le fichier PAC ou hébergez le fichier PAC dans un Forwarding Profile (Profil de transfert) et ajoutez des itinéraires à votre réseau pour PAC service IP addresses (Adresses IP de service PAC).
- Dans le fichier PAC, transférez l'URL de l'IdP et l'URL du portail Prisma Access vers le proxy explicite.
- Sur le proxy explicite, excluez l'URL de l'IdP et du portail des paramètres d'authentification. Ajoutez l'URL de l'IdP et du portail au domaine utilisé dans les flux d'authentification.
- Configurez des itinéraires vers le FQDN du proxy explicite ou des adresses IP sur les périphériques de périmètre pour permettre aux utilisateurs d'accéder à Internet via le proxy explicite.
- (Facultatif) Ajoutez des enregistrements DNS pour résoudre le FQDN du proxy explicite Prisma Access à une adresse IP interne si les utilisateurs ne peuvent pas résoudre les

 ©2025 Palo Alto Networks, Inc.

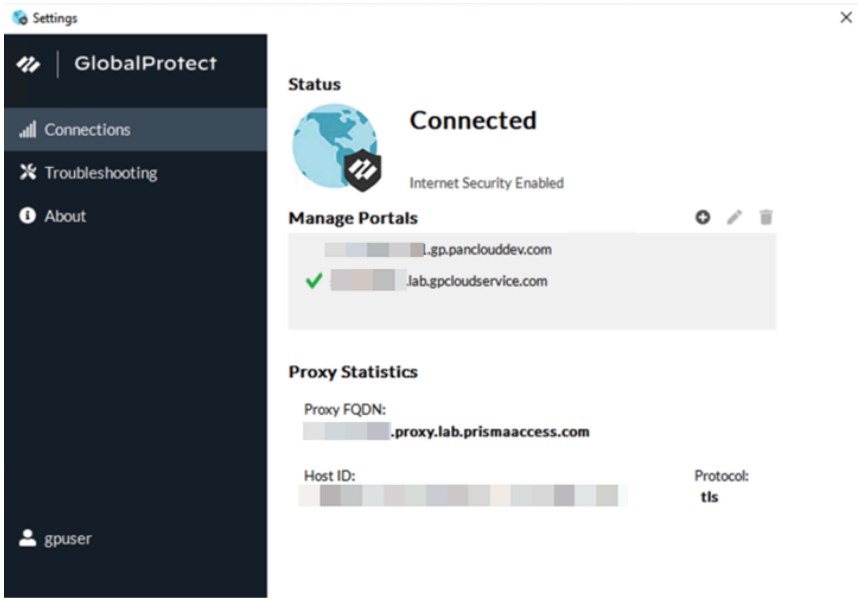
domaines publics dans le réseau de succursales, et ajoutez le NAT de destination pour l'adresse IP interne au FQDN du proxy explicite ou à l'adresse IP.

STEP 10 | Sélectionnez l'option **Commit (Valider)** pour valider les modifications que vous avez apportées à Panorama et **Commit et Push (Valider et appliquer)** pour les modifications apportées à la configuration des **Mobile Users (Utilisateurs mobiles)** et de l'**Explicit Proxy (Proxy explicite)** de Prisma Access.

STEP 11 | Vérifiez et dépannez le déploiement du proxy de l'agent.

1. Vérifiez les informations relatives à votre connexion réseau dans l'onglet **Connections (Connexions)** sous **Settings (Paramètres)** de l'application GlobalProtect.

   1. Ouvrez l'application GlobalProtect.
   2. Sélectionnez **Settings (Paramètres)** pour ouvrir le panneau GlobalProtect Settings (Paramètres de GlobalProtect), puis sélectionnez **Connections (Connexions)**.



2. Afficher et collecter les journaux GlobalProtect

   Consultez le journal PanGPS pour vérifier la configuration du mode proxy sur le portail GlobalProtect.

   Vous pouvez vérifier que le mode proxy est configuré en recherchant l'événement suivant dans le journal PanGPS :

   ```
   OnProxyAgentMode : mode proxy uniquement
   ```

   Pour afficher les journaux GlobalProtect dans Panorama, sélectionnez **Monitor (Surveiller)** > **Logs (Journaux)** et :

   - **GlobalProtect** pour les journaux d'authentification, et
   - **Traffic (Trafic)** et **Decryption (Décryptage)** pour les journaux d'accès utilisateur.

 ©2025 Palo Alto Networks, Inc.

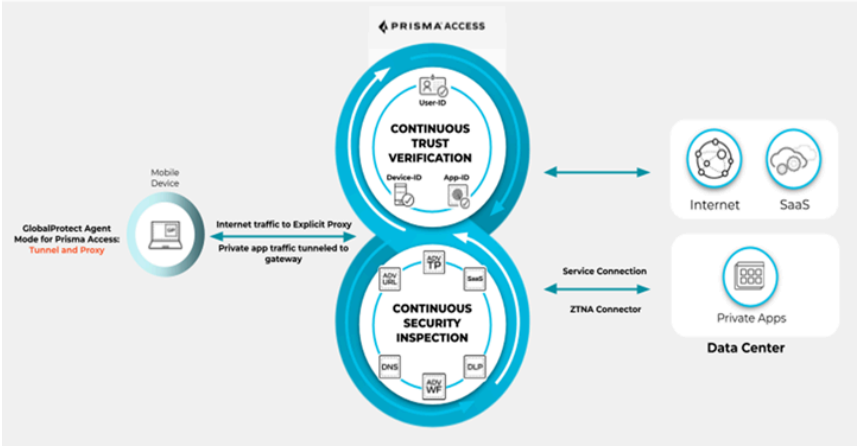
GlobalProtect en mode tunnel et proxy

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager) Si vous souhaitez utiliser cette fonctionnalité dans votre Prisma Access environnement, contactez votre équipe de compte pour en savoir plus.	• Prisma Access 5.2 • Application GlobalProtect version 6.2 pour Windows ou macOS • Version du contenu 8700-7994 • Licence d'utilisateur mobile Prisma Access

Dans le mode **Tunnel and Proxy (Tunnel et proxy)**, l'application GlobalProtect envoie le trafic Internet au proxy explicite en fonction des règles que vous définissez dans un fichier PAC. Pour le trafic restant, elle utilise les règles de segmentation de tunnel et la logique définies dans le fichier PAC pour déterminer le trafic à envoyer via le tunnel et le trafic qui peut le contourner. Si vous n'avez pas défini de règles de segmentation de tunnel, l'application envoie tout le trafic restant via le tunnel.

Lors de l'exécution de l'application GlobalProtect en mode tunnel et proxy, la fonctionnalité Host Information Profile (profil d'informations sur l'hôte - HIP) n'est prise en charge que pour le trafic via un tunnel GlobalProtect.

Vous avez besoin de Strata Cloud Manager et de l'agent GlobalProtect version 6.3.0 pour le canal proxy GlobalProtect afin de prendre en charge toutes les connexions TCP IPv4, y compris le trafic non compatible avec le proxy. Pour garantir une fonctionnalité fluide, le DNS configuré sur les terminaux doit être en mesure de résoudre le FQDN de destination.



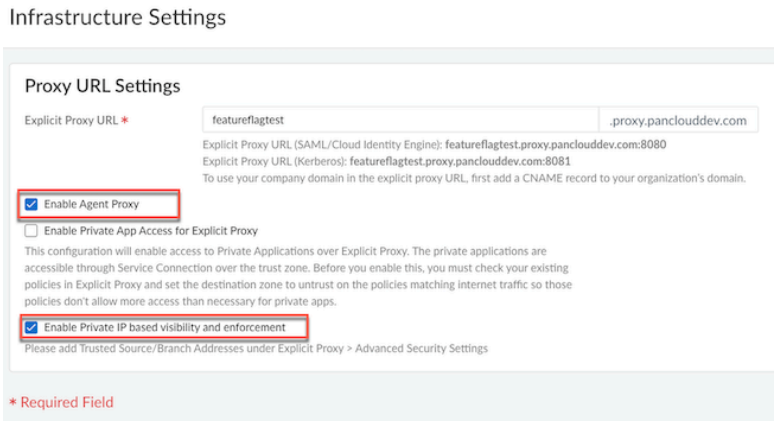
- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

GlobalProtect en mode tunnel et proxy (Strata Cloud Manager)

STEP 1 | Activez la fonctionnalité de proxy basé sur l'agent pour les utilisateurs mobiles sur Prisma Access.

1. Activez le proxy explicite.
   1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)**.
   2. Dans la zone Infrastructure Settings (Paramètres d'infrastructure), cliquez sur **Setup Proxy Settings (Configurer les paramètres de proxy)** et spécifiez une **Explicit Proxy URL (URL de proxy explicite)**.
2. Sélectionnez les options **Enable Agent Proxy (Activer le proxy de l'agent)** et, optionnellement, **Enable Private IP based visibility and enforcement (Activer la visibilité et l'application basées sur l'IP privée)**, puis cliquez sur **Save (Enregistrer)**.



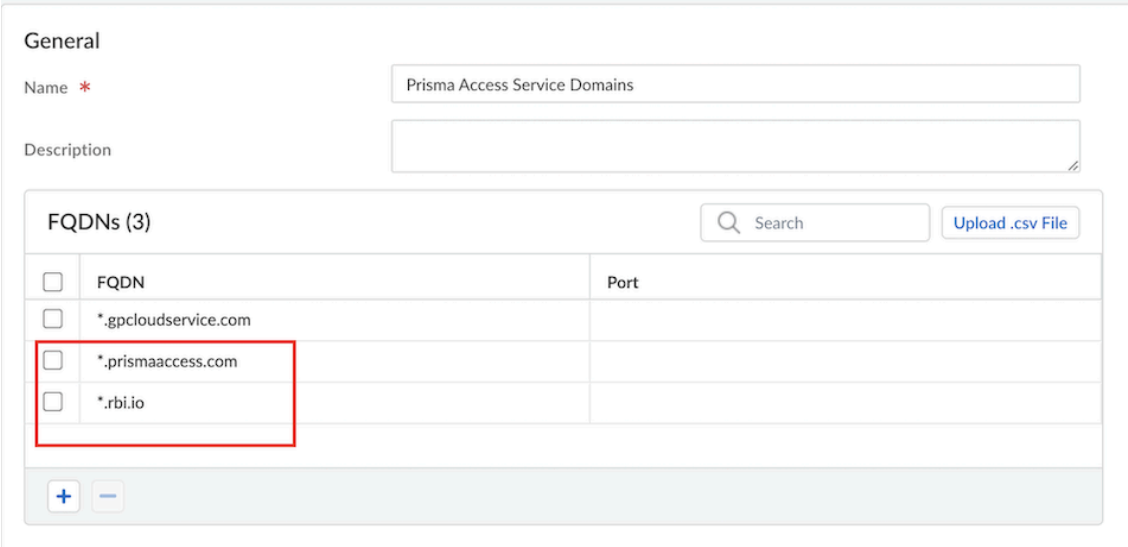
3. Sélectionnez les emplacements Prisma Access où vous souhaitez prendre en charge les utilisateurs mobiles.

   Pour une expérience utilisateur optimale, si vous limitez le nombre d'emplacements, choisissez les emplacements les plus proches de vos utilisateurs finaux. Si aucun

 ©2025 Palo Alto Networks, Inc.

emplacement n'est disponible dans le pays où résident vos utilisateurs mobiles, choisissez l'emplacement le plus proche des utilisateurs mobiles.

4. Créez un profil de transfert pour définir le trafic que vous souhaitez envoyer via le proxy explicite. Lors de la configuration du profil de transfert, ignorez les domaines *.prismaaccess.com et *.gpcloudservice.com



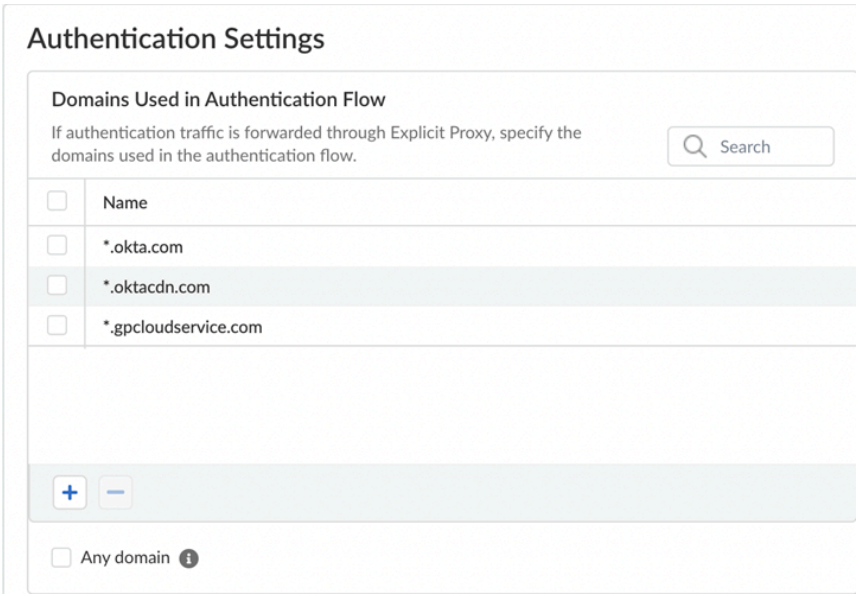
5. Associez le profil de transfert à la configuration de votre application GlobalProtect.
6. Sélectionnez **Workflows (Flux de travail)** > **Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Advanced Security Settings (Paramètres de sécurité**

 ©2025 Palo Alto Networks, Inc.

avancés) > **Authentication Settings (Paramètres d'authentification)** et ajoutez les domaines que vous devez contourner.

Toutes les requêtes adressées au proxy sont soumises à une authentification. Cependant, si vous transmettez des flux IdP via le proxy, vous devez les contourner pour que l'authentification réussisse.

Dans cet exemple, nous contournons le portail GlobalProtect et Okta, mais veuillez les personnaliser en fonction des IdP que vous utilisez.

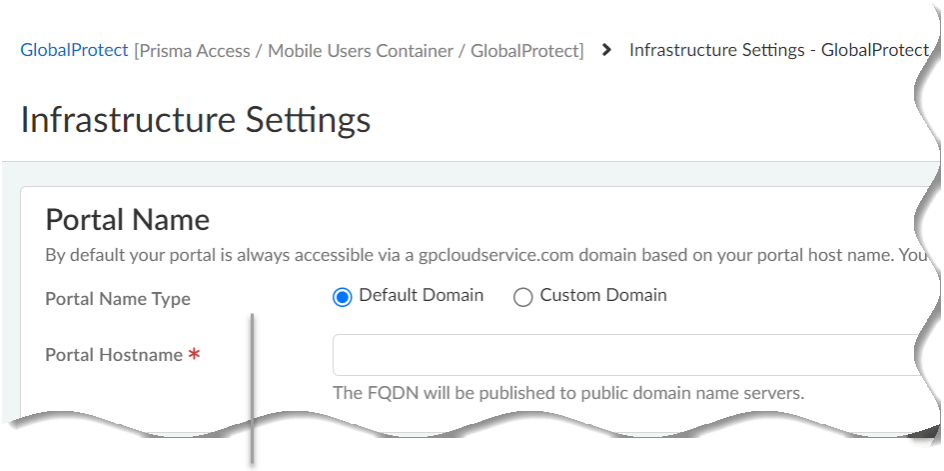


 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configurez le mode tunnel et proxy pour l'application GlobalProtect sur Prisma Access.

Dans le mode tunnel et proxy, la méthode de connexion que vous définissez s'applique uniquement au trafic tunnelisé via GlobalProtect. La fonctionnalité de proxy basé sur l'agent fournira une sécurité Internet toujours active. Même si vous définissez une méthode de connexion à la demande, tout le trafic Internet passera toujours par le proxy pour une sécurité Internet permanente, même lorsque les utilisateurs déconnectent l'application GlobalProtect.

1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **Infrastructure** > **Infrastructure Settings (Paramètres d'infrastructure)** et indiquez le **Portal Name (Nom du portail)**.



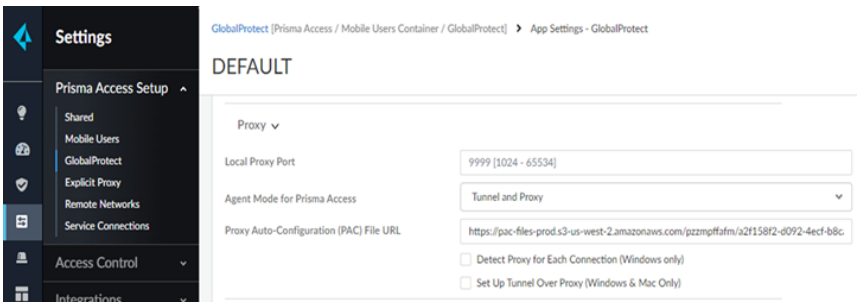
GlobalProtect Infrastructure Settings

- **Default Domain (Domaine par défaut)** : si vous sélectionnez cette option, le nom d'hôte de votre portail utilise le nom du domaine par défaut : `.gpcloudservice.com`. Dans ce cas, il suffit de saisir un **Portal Hostname (Nom d'hôte du portail)** à ajouter au nom du domaine par défaut. Prisma Access pour les utilisateurs créera automatiquement les certificats nécessaires et publiera le nom d'hôte sur les serveurs DNS publics.
- **Custom Domain (Domaine personnalisé)** : vous pouvez également personnaliser l'adresse du portail si vous souhaitez que le domaine du nom d'hôte du portail corresponde au nom du domaine de votre entreprise (par exemple, myportal.mydomain.com).

2. Permettez aux utilisateurs mobiles de s'authentifier auprès de Prisma Access.

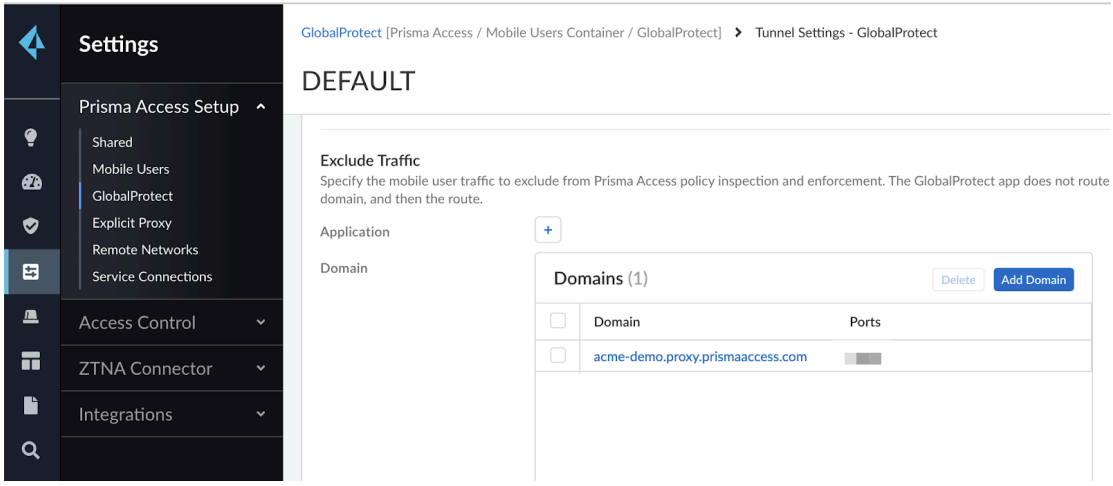
 ©2025 Palo Alto Networks, Inc.

3. Activez le mode tunnel et proxy GlobalProtect pour Prisma Access dans les paramètres de l'application GlobalProtect pour envoyer du trafic Internet au proxy basé sur l'agent.
   - Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect**.
   - Dans l'onglet **GlobalProtect App (Application GlobalProtect)**, cliquez sur **Default (Par défaut)** pour personnaliser les paramètres de l'application ou **Add App Settings (Ajouter les paramètres de l'application)** pour ajouter une nouvelle configuration.
   - Cliquez sur **Show Advanced Options (Montrer les options avancées)** ainsi que dans la section **App Configuration (Configuration de l'application)**.
   - Dans la section **Proxy**, définissez **Agent Mode for Prisma Access (Mode agent pour Prisma Access)** sur **Tunnel and Proxy (Tunnel et proxy)** pour demander à l'application GlobalProtect d'envoyer le trafic Internet au proxy explicite sur Prisma Access et le trafic d'applications privées vers le VPN. Après avoir configuré le mode **Tunnel and Proxy (Tunnel et proxy)** sur Prisma Access, les utilisateurs peuvent accéder en toute sécurité à Internet via Prisma Access même lorsqu'ils déconnectent ou désactivent l'application GlobalProtect.
   - (Facultatif) Configurez le port de proxy local. La plage de ports est comprise entre 1024 et 65534 et le port par défaut est 9999. Si le port par défaut n'est pas disponible, GlobalProtect essaiera 10 autres ports dans la plage de 9999 à 10009 et utilisera le port qui est disponible. Vous pouvez également choisir votre propre numéro de port dans la plage.
   - (Facultatif) Configurez l'URL du fichier de configuration automatique (PAC) si vous souhaitez transmettre une nouvelle URL PAC pour les paramètres de proxy au terminal. L'URL PAC transmet vers le terminal une fois que l'utilisateur se connecte. Lorsque l'utilisateur déconnecte l'application GlobalProtect, les configurations de proxy de terminal sont automatiquement désactivées et reviennent aux paramètres précédents.
   - (Facultatif) Autorisez l'utilisateur à redécouvrir le réseau si vous souhaitez que l'utilisateur vérifie le portail pour tout nouveau paramètre.
   - (Facultatif) Configurez l'intervalle de rafraîchissement de configuration de l'application GlobalProtect (heures). Par défaut, le client GlobalProtect actualise la configuration du portail mise en cache toutes les 24 heures. Vous pouvez changer l'intervalle de rafraîchissement en fonction de vos besoins commerciaux.
   - Désactivez l'option **Set Up Tunnel Over Proxy (Windows & Mac Only) (Définir le proxy du tunnel (Windows et Mac uniquement))**.



 ©2025 Palo Alto Networks, Inc.

4. Dans la configuration de la **Split Tunnel (Segmentation du tunnel)**, excluez le FQDN du proxy explicite et le FQDN du fichier PAC.
   - Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect**.
   - Dans l'onglet **GlobalProtect App (application GlobalProtect)**, cliquez sur **Default (Par défaut)** pour personnaliser les paramètres du tunnel ou **Add Tunnel Settings (Ajouter les paramètres du tunnel)** pour ajouter une nouvelle configuration.
   - Sous **Exclude Traffic (Exclure le trafic)**, **Add Domain (Ajouter un domaine)**.



 ©2025 Palo Alto Networks, Inc.

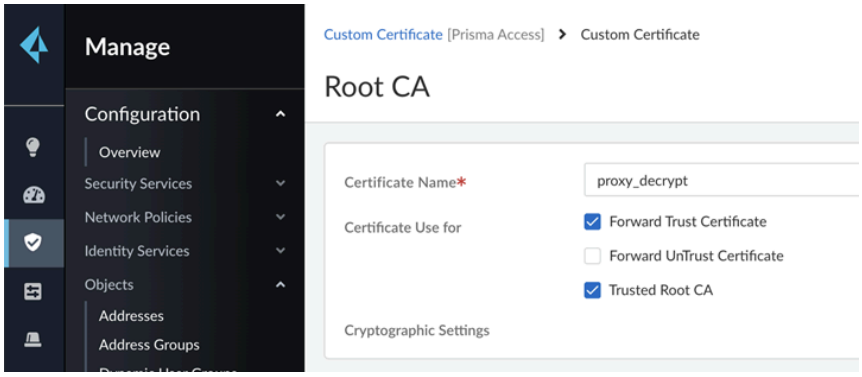
Remplacez le FQDN dans l'image par le FQDN votre proxy.

STEP 3 | Activez la sécurité toujours active en configurant les paramètres suivants sur la page **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Application GlobalProtect)** > **Add App Settings (Ajouter les paramètres de l'application)** :

1. Définissez l'option Disable GlobalProtect (Désactiver GlobalProtect) sur **Disallow (Ne pas autoriser)**, **Allow with Passcode (Autoriser avec mot de passe)** ou **Allow with Ticket (Autoriser avec ticket)**.
2. Désactivez l'option Allow user to Sign Out from GlobalProtect App (Autoriser l'utilisateur à se déconnecter de l'application GlobalProtect).

STEP 4 | Configurez le décryptage pour le trafic proxy explicite.

- Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Decryption (Décryptage)**.
- Si vous activez le décryptage, assurez-vous de configurer le certificat de décryptage en tant que CA racine approuvée.



STEP 5 | Configurez les règles de politique de sécurité pour le trafic du proxy explicite.

- Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)**.
- Suivez les meilleures pratiques des politiques de sécurité des passerelles Internet.

STEP 6 | (Facultatif) Configurez l'application GlobalProtect en mode proxy et tunnel dans un réseau d'itinéraires autre que celui par défaut.

- (Facultatif) Hébergez un fichier PAC en interne et ajoutez le FQDN du proxy explicite Prisma Access en tant que proxy dans le fichier PAC ou hébergez le fichier PAC dans un Forwarding Profile (Profil de transfert) et ajoutez des itinéraires à votre réseau pour PAC service IP addresses (Adresses IP de service PAC).
- Transférez les requêtes d'authentification vers Internet pour les FQDN du portail et de la passerelle et pour les URL d'IdP.

 ©2025 Palo Alto Networks, Inc.

- Configurez des itinéraires vers le FQDN du proxy explicite ou des adresses IP sur les périphériques de périmètre pour permettre aux utilisateurs d'accéder à Internet via le proxy explicite.
- (Facultatif) Ajoutez des enregistrements DNS pour résoudre le FQDN du proxy explicite Prisma Access à une adresse IP interne si les utilisateurs ne peuvent pas résoudre les domaines publics dans le réseau de succursales, et ajoutez le NAT de destination pour l'adresse IP interne au FQDN du proxy explicite ou à l'adresse IP.
- Pour permettre aux utilisateurs d'accéder directement à des applications privées lorsqu'ils sont au bureau :
  - **Direct Access (Accès direct) :** Activez la détection de l'hôte interne et laissez la liste des passerelles internes vide.

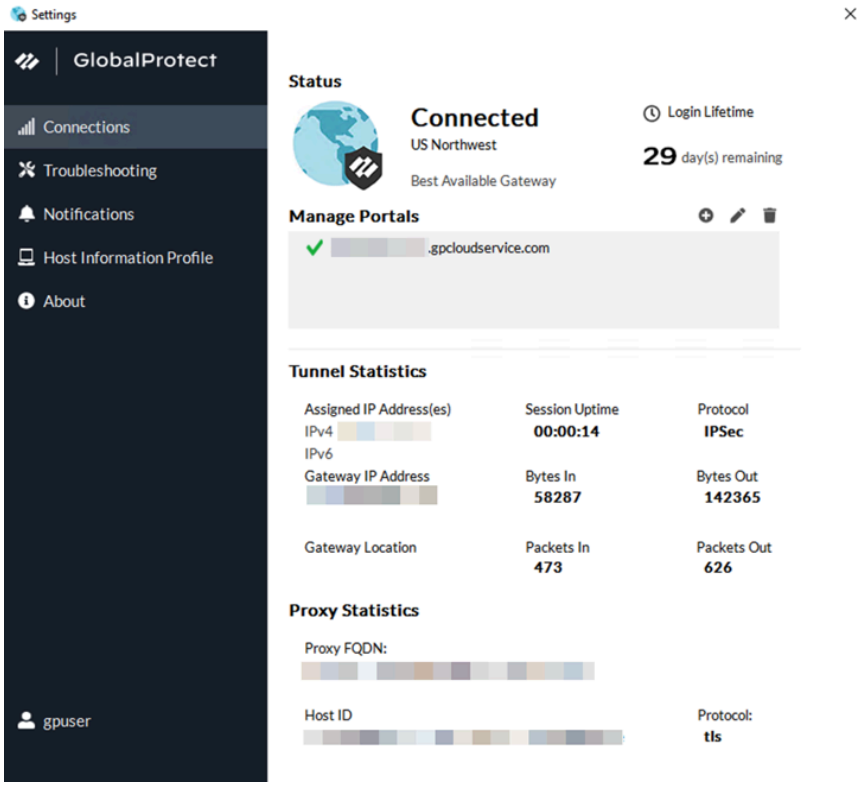
STEP 7 | Cliquez sur **Save (Enregistrer)** et sélectionnez **Push Config (Transmettre la configuration)** à **GlobalProtect** et à l'**Explicit Proxy (Proxy explicite)**.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Vérifiez et dépannez le déploiement du proxy de l'agent.

1. Vérifiez les informations relatives à votre connexion réseau dans l'onglet **Connections (Connexions)** sous **Settings (Paramètres)** de l'application GlobalProtect.

   1. Ouvrez l'application GlobalProtect.
   2. Sélectionnez **Settings (Paramètres)** pour ouvrir le panneau GlobalProtect Settings (Paramètres de GlobalProtect), puis sélectionnez **Connections (Connexions)**.



2. Affichez et collectez les journaux GlobalProtect.

   Consultez le journal PanGPS pour vérifier la configuration du mode proxy sur le portail GlobalProtect.

   Vous pouvez vérifier que le mode proxy est configuré en recherchant l'événement suivant dans le journal PanGPS :

   ```
   OnProxyAgentMode : mode hybride
   ```

   Pour afficher les journaux GlobalProtect dans , sélectionnez **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)** et :

   - **GlobalProtect** pour les journaux d'authentification, et
   - **Traffic (Trafic)** et **Decryption (Décryptage)** pour les journaux d'accès utilisateur.

Déconnecter et désactiver le mode tunnel et proxy avec la méthode de connexion Toujours actif

À partir de la version 6.3.1 de GlobalProtect, lorsque vous configurez le mode **Tunnel and Proxy (Tunnel et proxy)** pour l'application GlobalProtect avec le mode **Always-On (Toujours**

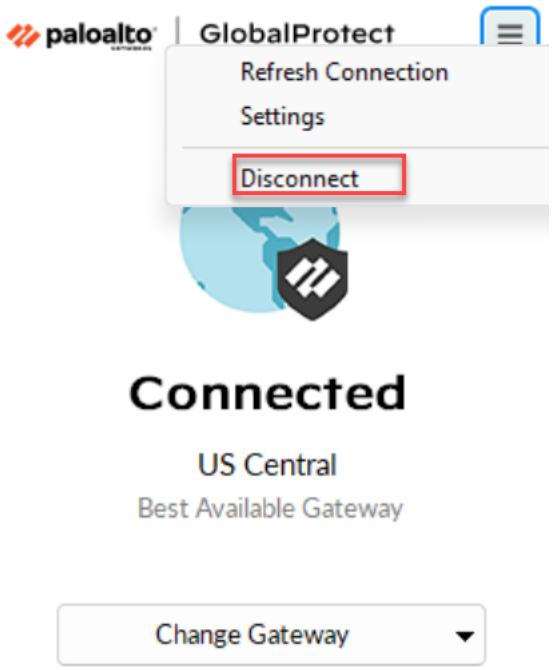
 ©2025 Palo Alto Networks, Inc.

actif) comme méthode de connexion et que vous souhaitez déconnecter le mode tunnel et proxy, vous devez effectuer les étapes suivantes :

1. Déconnectez l'application GlobalProtect pour déconnecter la connexion du tunnel (VPN). Lorsque vous déconnectez l'application, la connexion du tunnel (VPN) est déconnectée et l'application est toujours connectée via le mode proxy.
2. Désactivez l'application GlobalProtect pour déconnecter le mode tunnel et le mode proxy. Lorsque vous désactivez l'application, le mode tunnel et le mode proxy sont tous les deux déconnectés et l'application n'est plus connectée.

Pour déconnecter et désactiver l'application GlobalProtect configurée avec le mode **Tunnel and Proxy (Tunnel et proxy)** (mode hybride) et la méthode de connexion **Always-On (Toujours actif)**, vous devez :

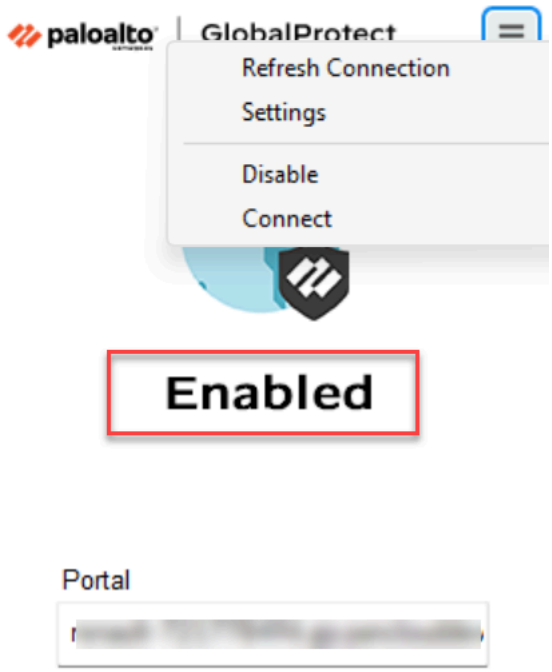
1. Déconnectez l'application GlobalProtect à l'aide de l'option **Disconnect (Déconnecter)** dans le menu hamburger. Lorsque vous déconnectez l'application, la connexion du tunnel (VPN) est déconnectée.



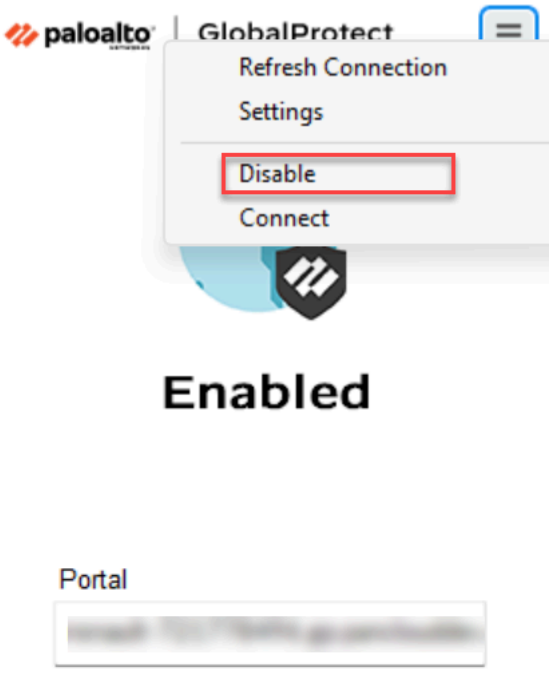
Une fois que vous avez déconnecté l'application, la connexion VPN est déconnectée, mais le mode proxy est activé. L'application sera toujours connectée via le mode proxy et l'application affiche l'état **Enabled (Activée)**.

*Si vous souhaitez reconnecter la connexion du tunnel (VPN), vous pouvez utiliser l'option **Connect (Connecter)** dans le menu hamburger.*

 ©2025 Palo Alto Networks, Inc.

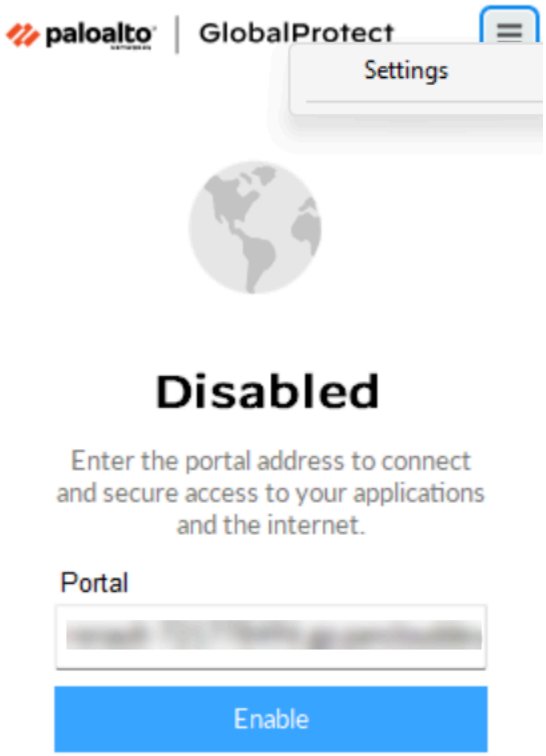


2. Désactivez l'application GlobalProtect à l'aide de l'option **Disable (Désactiver)** dans le menu hamburger. Une fois que vous avez désactivé l'application, la connexion du tunnel et la connexion du proxy sont toutes les deux déconnectées.



L'application sera désactivée et affichera l'état **Disabled (Désactivée)**.

 ©2025 Palo Alto Networks, Inc.



GlobalProtect en mode tunnel et proxy (Panorama)

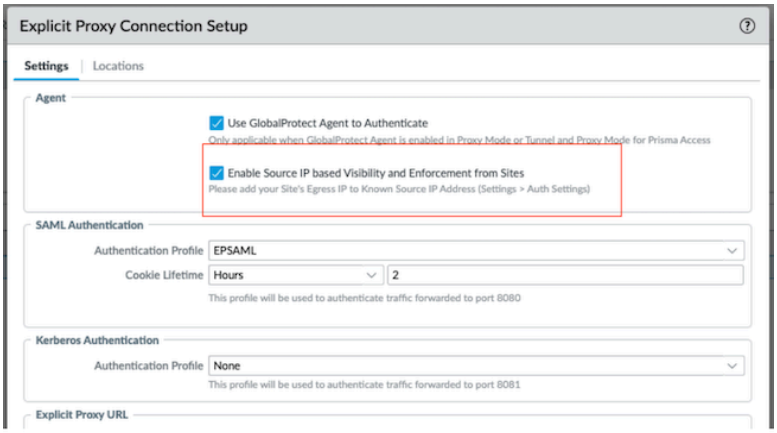
Si vous convertissez un déploiement à locataire unique Prisma Access (Managed by Panorama) en déploiement multilocataire, seul le premier locataire (le locataire que vous avez migré) prend en charge cette fonctionnalité. En outre, dans ce premier locataire, vous devez configurer vos règles de politique dans le Explicit_Proxy_Device_Group prédéfini plutôt que dans un groupe de périphériques personnalisé. Aucun des locataires que vous créez ensuite pour le déploiement multilocataire après le premier ne prend en charge cette fonctionnalité.

STEP 1 | Activez la fonctionnalité de proxy basé sur l'agent pour les utilisateurs mobiles.

1. Activez le proxy explicite.
    1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—Explicit Proxy (Utilisateurs mobiles — proxy explicite)**.
    2. Vous devez **Configure (Configurer)** la configuration du proxy explicite pour spécifier une **Explicit Proxy URL (URL de proxy explicite)**.
2. Sélectionnez **Use GlobalProtect app to Authenticate (Utiliser l'application GlobalProtect pour s'authentifier)** pour activer la fonctionnalité de proxy basé sur l'agent et,

 ©2025 Palo Alto Networks, Inc.

optionnellement, **Enable Source IP based Visibility and Enforcement from Sites (Activer la visibilité et l'application basées sur l'adresse IP source à partir des sites)**.



3. Entrez l'URL du **PAC (Proxy Auto-Configuration) File (Fichier PAC (Proxy Auto-Configuration))**. Assurez-vous d'entrer un port de 8080 dans le fichier PAC.
   - L'énoncé du proxy dans le fichier PAC doit utiliser le FQDN Prisma Access que vous avez configuré ci-dessus.
   - Le fichier PAC doit être configuré pour exclure les passerelles GlobalProtect (*.gp.gpcoudservice.com).
4. Sélectionnez le **Connection Name (Nom de connexion)** pour la configuration du proxy explicite que vous avez configuré.
5. Sélectionnez les **Locations (Emplacements)** et les régions dans lesquels vous souhaitez déployer votre proxy explicite pour les utilisateurs mobiles.

   Prisma Access ajoute un nœud proxy à chaque emplacement que vous sélectionnez. Le proxy explicite prend en charge un sous-ensemble de tous les emplacements Prisma Access. Pour une expérience utilisateur optimale, si vous limitez le nombre d'emplacements, choisissez les emplacements les plus proches de vos utilisateurs finaux. Si aucun emplacement n'est disponible dans le pays où résident vos utilisateurs mobiles, choisissez l'emplacement le plus proche des utilisateurs mobiles.

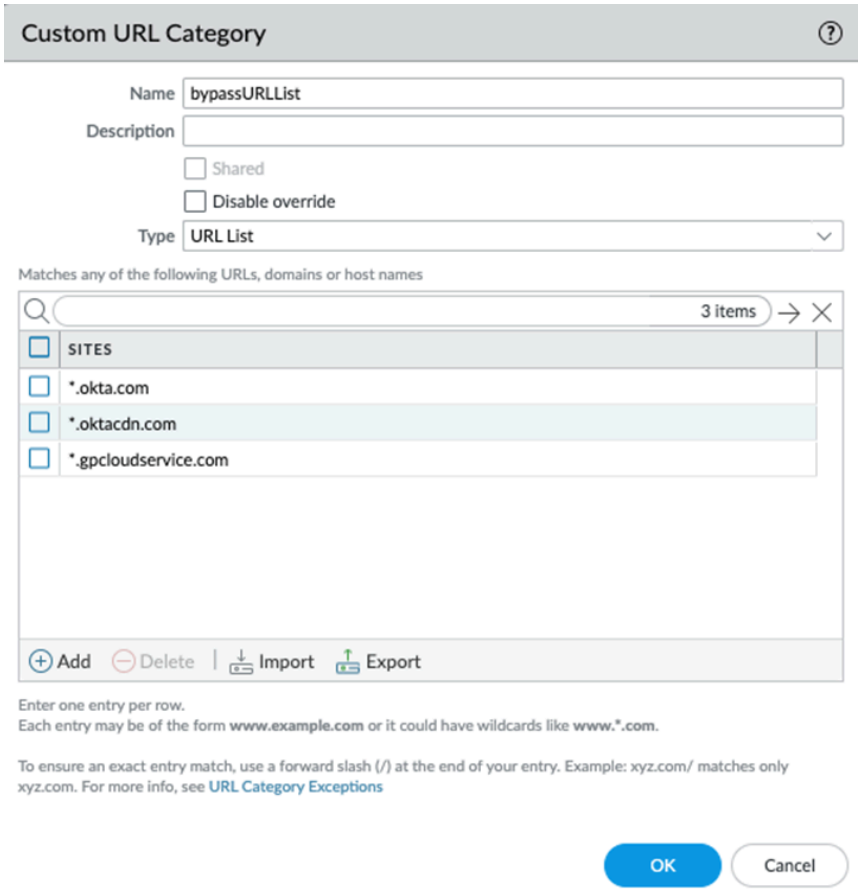
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Contournez les fournisseurs d'identité (IDP).

Toutes les requêtes adressées au proxy sont authentifiées. Cependant, si vous transmettez des flux IDP via le proxy, vous devez les contourner pour que l'authentification réussisse.

Dans cet exemple, nous contournons le portail GlobalProtect et Okta, mais veuillez les personnaliser en fonction des IDP que vous utilisez.

1. Avec **Explicit_Proxy_Device_Group** sélectionné, sélectionnez **Object (Objet)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)** et créez une catégorie d'URL personnalisée.
2. Dans la catégorie Custom URL (URL personnalisée), ajoutez tous les domaines FQDN qui doivent être contournés depuis l'authentification EP.



3. Sélectionnez **Cloud Services** > **Configuration** > **Mobile Users (Utilisateurs mobiles)** > **Explicit Proxy (Proxy explicite)** > **Settings (Paramètres)** > **Authentication Settings (Paramètres d'authentification)** et joignez la catégorie Custom URL (URL personnalisée).



4. Validez et appliquez vers le **Explicit_Proxy_Device_Group**.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configurez le portail GlobalProtect.

Dans le mode tunnel et proxy, la méthode de connexion que vous définissez s'applique uniquement au trafic tunnelisé via GlobalProtect. La fonctionnalité de proxy basé sur l'agent fournira une sécurité Internet toujours active. Même si vous définissez une méthode de connexion à la demande, tout le trafic Internet passera toujours par le proxy pour une sécurité Internet permanente, même lorsque les utilisateurs déconnectent l'application GlobalProtect.

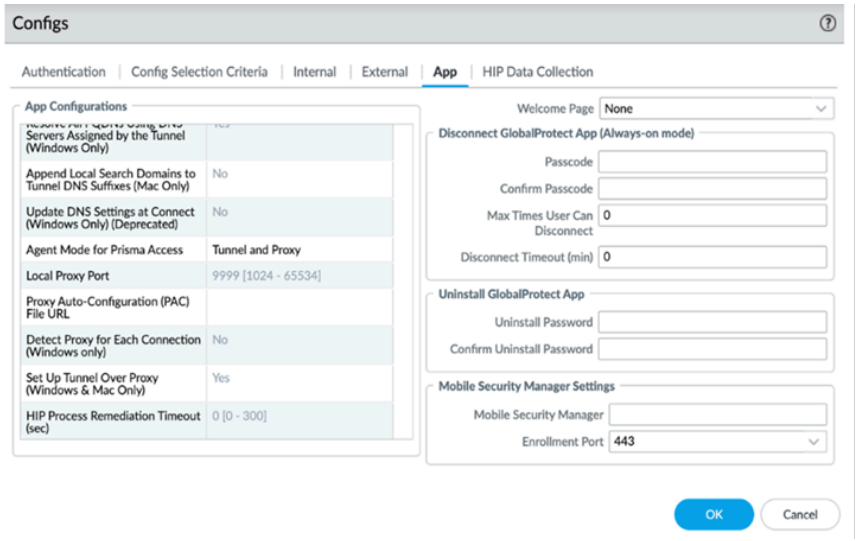
1. Dans la section Onboarding (Intégration), cliquez sur **Configure (Configurer)**.
2. Dans l'onglet **General (Général)**, spécifiez le**Portal Name Type (Type de nom de portail)** :

   Use Default Domain (Utiliser le domaine par défaut) : si vous sélectionnez cette option, le nom d'hôte de votre portail utilise le nom du domaine par défaut : .gpcloudservice.com. Dans ce cas, il vous suffit d'entrer un nom d'hôte de portail à ajouter au nom du domaine par défaut. Prisma Access créera automatiquement les certificats nécessaires et publiera le nom d'hôte sur les serveurs DNS publics.

   Use Company Domain (Utiliser le domaine de l'entreprise) : sélectionnez cette option si vous souhaitez que le domaine dans le nom d'hôte du portail corresponde au nom du domaine de votre entreprise (par exemple, myportal.mydomain.com).
3. Sélectionnez un **Authentication Profile (Profil d'authentification)** qui précise comment Prisma Access doit authentifier les utilisateurs mobiles ou en créer un nouveau.
4. (Facultatif) Sélectionnez un **Authentication Override Certificate (Certificat de remplacement de l'authentification)** pour crypter les cookies sécurisés que les utilisateurs mobiles utilisent pour s'authentifier sur le portail et la passerelle.
   1. Activez le mode tunnel et proxy sur GlobalProtect.
      1. Sélectionnez **Network (Réseau)** > **GlobalProtect Portals (Portails Globalprotect)**.
      2. Sélectionnez la configuration du portail à laquelle vous ajoutez la configuration de l'agent, puis sélectionnez l'onglet **Agent**.
      3. Dans l'onglet **Agent**, sélectionnez **App (Application)**.
      4. Dans la zone App Configurations (Configurations de l'application), définissez le **Agent Mode for Prisma Access (Mode agent pour Prisma Access)** sur **Tunnel and Proxy**

 ©2025 Palo Alto Networks, Inc.

(Tunnel et proxy) pour envoyer le trafic Internet vers le proxy explicite de Prisma Access et le trafic des applications privées vers le VPN.



2. Effectuez des configurations facultatives.
    1. (Facultatif) Configurez le port de proxy local. La plage de ports est comprise entre 1024 et 65534 et le port par défaut est 9999. Si le port par défaut n'est pas disponible, GlobalProtect essaiera 10 autres ports dans la plage de 9999 à 10009 et utilisera le port qui est disponible. Vous pouvez également choisir votre propre numéro de port dans la plage.
    2. (Facultatif) Configurez l'URL du fichier de configuration automatique (PAC) si vous souhaitez transmettre une URL PAC personnalisée pour les paramètres de proxy au terminal. L'URL PAC transmet vers le terminal une fois que l'utilisateur se connecte. Lorsque l'utilisateur déconnecte l'application GlobalProtect, les configurations de proxy de terminal sont automatiquement désactivées et reviennent aux paramètres précédents.
    3. (Facultatif) Autorisez l'utilisateur à redécouvrir le réseau si vous souhaitez que l'utilisateur vérifie le portail pour tout nouveau paramètre.
    4. (Facultatif) Configurez l'intervalle de rafraîchissement de configuration de l'application GlobalProtect (heures). Par défaut, le client GlobalProtect actualise la configuration du portail mise en cache toutes les 24 heures. Vous pouvez changer l'intervalle de rafraîchissement en fonction de vos besoins commerciaux.
3. Dans la configuration de la segmentation du tunnel, excluez le FQDN du proxy explicite et le FQDN du fichier PAC.

STEP 4 | Activez la sécurité Internet toujours active en configurant les paramètres suivants :

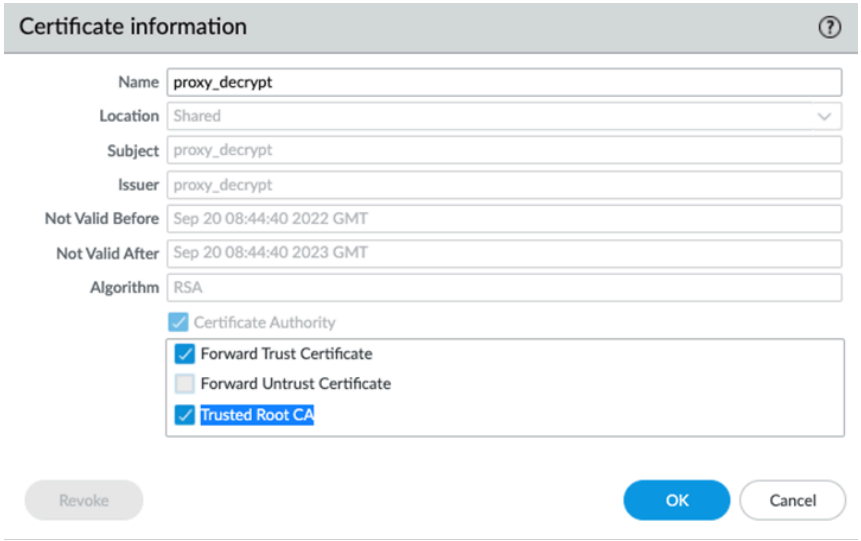
1. Définissez l'option Allow User to Disable GlobalProtect (Autoriser l'utilisateur à désactiver GlobalProtect) sur **Disallow (Ne pas autoriser)**, **Allow with Passcode (Autoriser avec mot de passe)** ou **Allow with Ticket (Autoriser avec ticket)**.
2. Définissez l'option Allow user to Sign Out from GlobalProtect App (Autoriser l'utilisateur à se déconnecter de l'application GlobalProtect) sur **No (Non)**.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Facultatif) Configurez la politique de décryptage pour le trafic proxy explicite.

Si vous activez le décryptage, assurez-vous que le certificat de décryptage est également configuré en tant que CA racine approuvée.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** et créez un certificat qui est une CA racine approuvée et un certificat d'approbation de transfert.



2. Créez une règle de décryptage sous **Explicit_Proxy_Device Group** avec un proxy de transfert SSL.

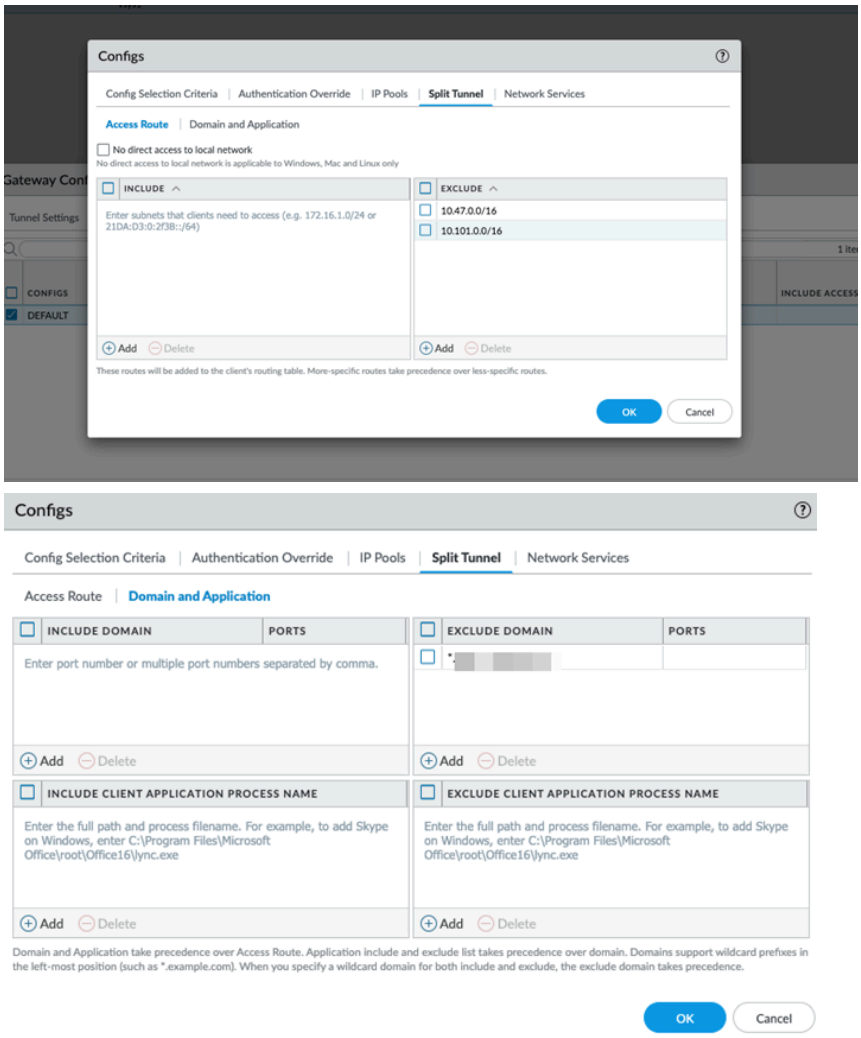
STEP 6 | Configurez les règles de politique de sécurité pour le trafic du proxy explicite.

- Sélectionnez **Manage (Gérer)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** > ..
- Suivez les meilleures pratiques des politiques de sécurité des passerelles Internet.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Configurez la segmentation du tunnel sur Panorama.

1. Sélectionnez **Network (Réseau)** > **Mobile User Template (Modèle d'utilisateur mobile)** > **Gateways (Passerelles)** > **GlobalProtect_ExternalGateway** > **Agent** > **Client Settings (Paramètres du client)** > **Split (Segmenter)**.
2. Configurez le tunnel en fonction des itinéraires et des domaines.



STEP 8 | (Facultatif) Configurez l'application GlobalProtect en mode tunnel et proxy dans un réseau d'itinéraires autre que celui par défaut.

- (Facultatif) Hébergez un fichier PAC en interne et ajoutez le FQDN du proxy explicite Prisma Access en tant que proxy dans le fichier PAC ou hébergez le fichier PAC dans un Forwarding Profile (Profil de transfert) et ajoutez des itinéraires à votre réseau pour PAC service IP addresses (Adresses IP de service PAC).
- Vérifiez que l'URL du portail GlobalProtect et les URL d'IdP sont redirigées vers le proxy explicite Prisma Access.
- Configurez des itinéraires vers le FQDN du proxy explicite ou des adresses IP sur les périphériques de périmètre pour permettre aux utilisateurs d'accéder à Internet via le proxy explicite.

 ©2025 Palo Alto Networks, Inc.

- (Facultatif) Ajoutez des enregistrements DNS pour résoudre le FQDN du proxy explicite Prisma Access à une adresse IP interne si les utilisateurs ne peuvent pas résoudre les domaines publics dans le réseau de succursales, et ajoutez le NAT de destination pour l'adresse IP interne au FQDN du proxy explicite ou à l'adresse IP.
- Pour permettre aux utilisateurs d'accéder directement à des applications privées lorsqu'ils sont au bureau :
  - **Direct access (Accès direct)** : activez la détection de l'hôte interne et laissez la liste des passerelles internes vide.

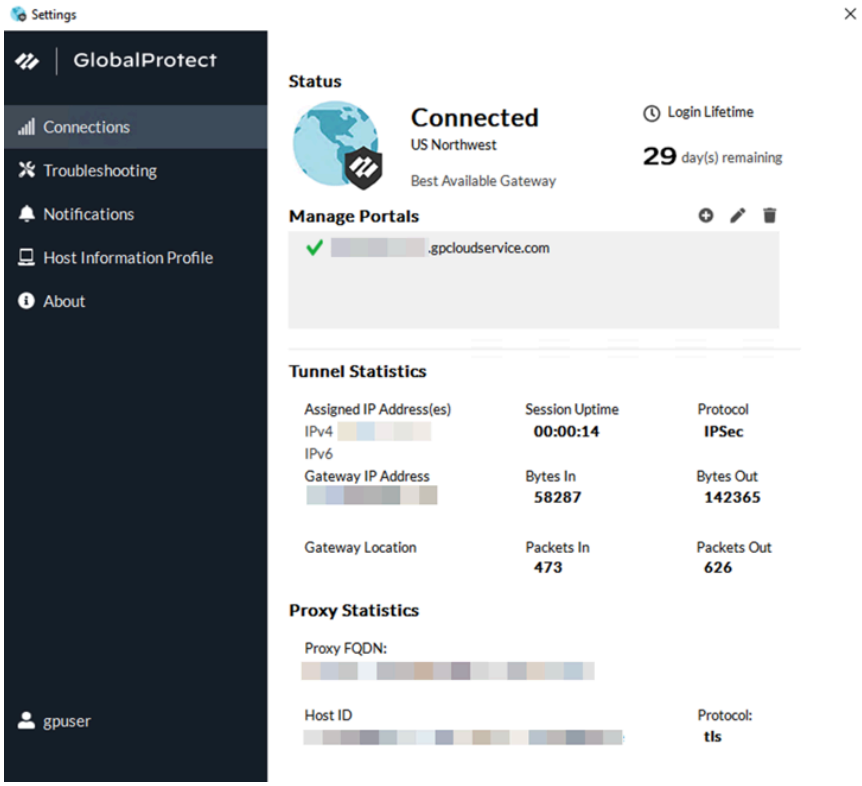
STEP 9 | Sélectionnez l'option **Commit (Valider)** pour valider les modifications que vous avez apportées à Panorama et **Commit et Push (Valider et appliquer)** pour les modifications apportées à la configuration des **Mobile Users (Utilisateurs mobiles)** et de l'**Explicit Proxy (Proxy explicite)** de Prisma Access.

 ©2025 Palo Alto Networks, Inc.

STEP 10 | Vérifiez et dépannez le déploiement du proxy de l'agent.

1. Vérifiez les informations relatives à votre connexion réseau dans l'onglet **Connections (Connexions)** sous **Settings (Paramètres)** de l'application GlobalProtect.

   1. Ouvrez l'application GlobalProtect.
   2. Sélectionnez **Settings (Paramètres)** pour ouvrir le panneau GlobalProtect Settings (Paramètres de GlobalProtect), puis sélectionnez **Connections (Connexions)**.



2. Afficher et collecter les journaux GlobalProtect

   Consultez le journal PanGPS pour vérifier la configuration du mode proxy sur le portail GlobalProtect.

   Vous pouvez vérifier que le mode proxy est configuré en recherchant l'événement suivant dans le journal PanGPS :

   ```
   OnProxyAgentMode : mode hybride
   ```

   Pour afficher les journaux GlobalProtect dans Panorama, sélectionnez **Monitor (Surveiller)** > **Logs (Journaux)** et :

   - **GlobalProtect** pour les journaux d'authentification, et
   - **Traffic (Trafic)** et **Decryption (Décryptage)** pour les journaux d'accès utilisateur.

Déconnecter et désactiver le mode tunnel et proxy avec la méthode de connexion Toujours actif

À partir de la version 6.3.1 de GlobalProtect, lorsque vous configurez le mode **Tunnel and Proxy (Tunnel et proxy)** pour l'application GlobalProtect avec le mode **Always-On (Toujours**

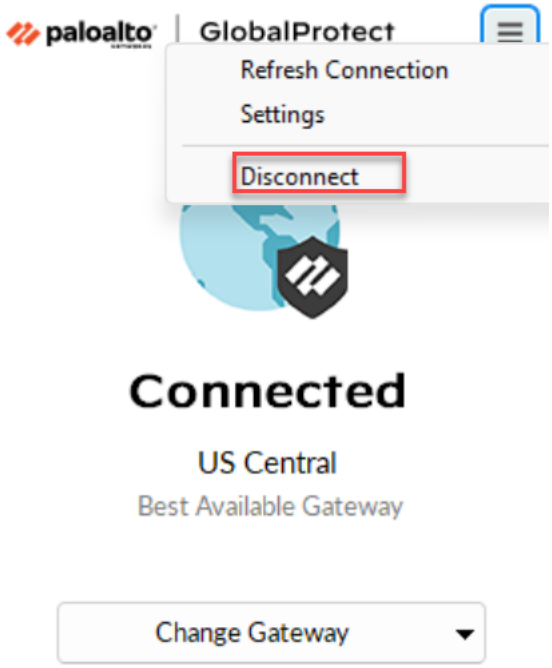
 ©2025 Palo Alto Networks, Inc.

actif) comme méthode de connexion et que vous souhaitez déconnecter le mode tunnel et proxy, vous devez effectuer les étapes suivantes :

1. Déconnectez l'application GlobalProtect pour déconnecter la connexion du tunnel (VPN). Lorsque vous déconnectez l'application, la connexion du tunnel (VPN) est déconnectée et l'application est toujours connectée via le mode proxy.
2. Désactivez l'application GlobalProtect pour déconnecter le mode tunnel et le mode proxy. Lorsque vous désactivez l'application, le mode tunnel et le mode proxy sont tous les deux déconnectés et l'application n'est plus connectée.

Pour déconnecter et désactiver l'application GlobalProtect configurée avec le mode **Tunnel and Proxy (Tunnel et proxy)** (mode hybride) et la méthode de connexion **Always-On (Toujours actif)**, vous devez :

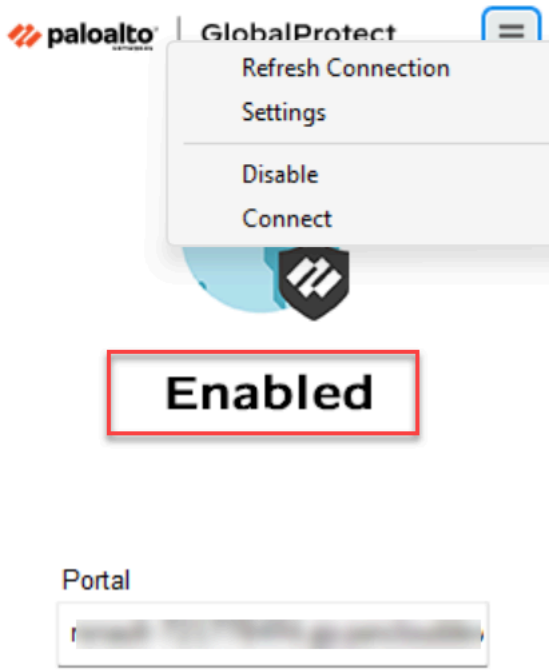
1. Déconnectez l'application GlobalProtect à l'aide de l'option **Disconnect (Déconnecter)** dans le menu hamburger. Lorsque vous déconnectez l'application, la connexion du tunnel (VPN) est déconnectée.



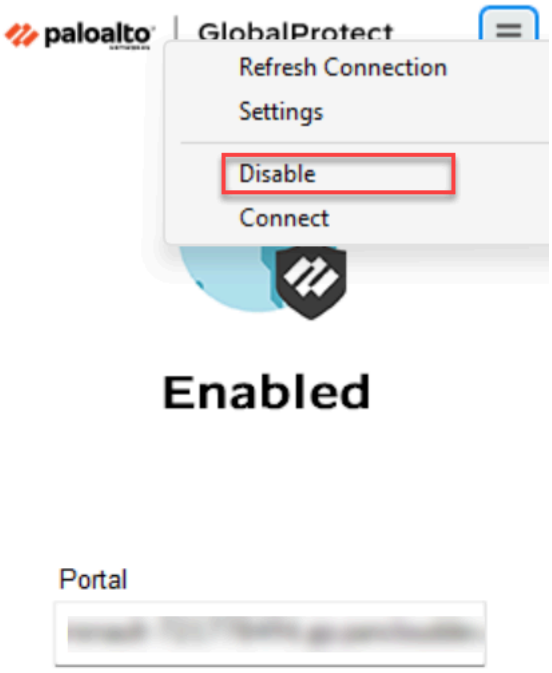
Une fois que vous avez déconnecté l'application, la connexion VPN est déconnectée, mais le mode proxy est activé. L'application sera toujours connectée via le mode proxy et l'application affiche l'état **Enabled (Activée)**.

*Si vous souhaitez reconnecter la connexion du tunnel (VPN), vous pouvez utiliser l'option **Connect (Connecter)** dans le menu hamburger.*

 ©2025 Palo Alto Networks, Inc.

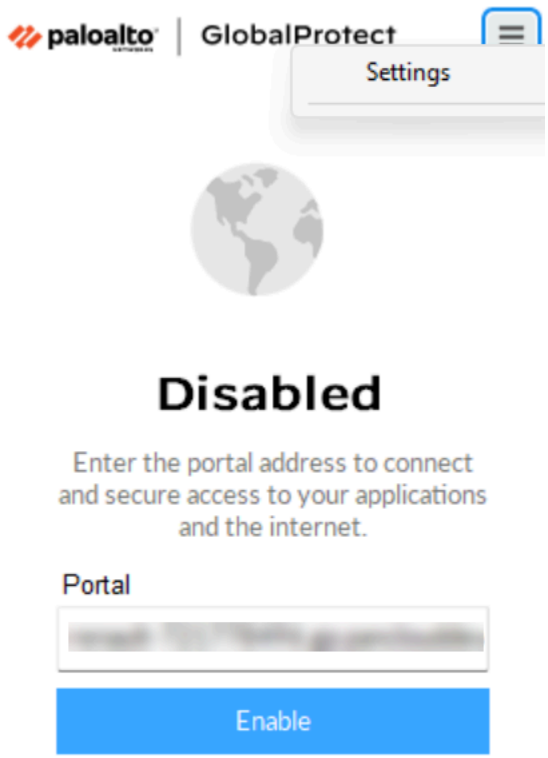


2. Désactivez l'application GlobalProtect à l'aide de l'option **Disable (Désactiver)** dans le menu hamburger. Une fois que vous avez désactivé l'application, la connexion du tunnel et la connexion du proxy sont toutes les deux déconnectées.



L'application sera désactivée et affichera l'état **Disabled (Désactivée)**.

 ©2025 Palo Alto Networks, Inc.



Visibilité et application de l'adresse IP privée pour le trafic de proxy basé sur l'agent

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access 5.2 • Application GlobalProtect version 6.3.1 pour Windows ou macOS • Plan de données Prisma Access 10.2.4 • Licence d'utilisateur mobile Prisma Access • Plugin Panorama version 5.2.0

Les utilisateurs qui se connectent au proxy explicite Prisma Access via l'agent GlobalProtect à partir de succursales peuvent exploiter les adresses IP privées des terminaux pour la journalisation ou pour l'application basée sur l'adresse IP.

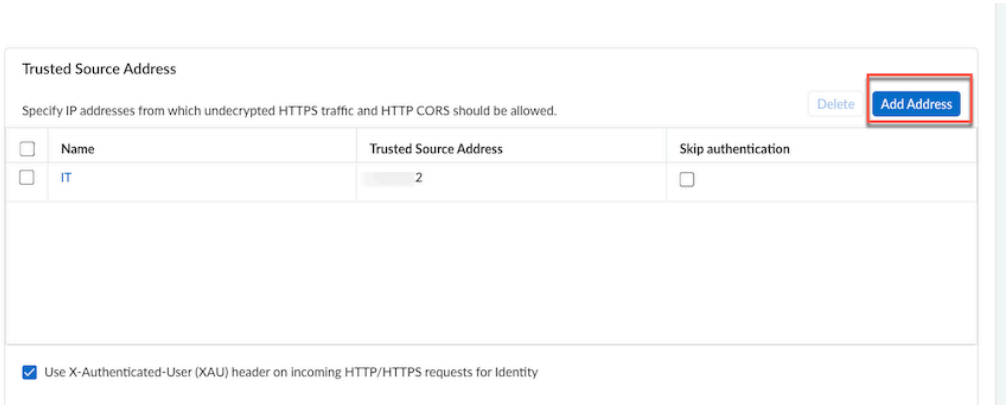
- Strata Cloud Manager
- Panorama

Visibilité et application de l'adresse IP privée pour le trafic de proxy basé sur l'agent (Strata Cloud Manager)

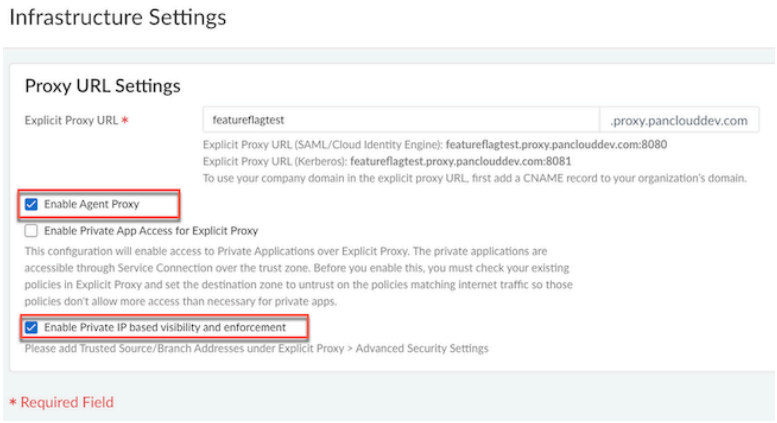
STEP 1 | Activez la fonctionnalité de proxy basé sur l'agent (Proxy mode (Mode proxy) ou Tunnel and Proxy mode (Mode tunnel et proxy)) pour les utilisateurs mobiles.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Advanced Security Settings (Paramètres de sécurité avancés)**, puis cliquez sur l'icône des paramètres. Sous **Trusted Source Address (Adresse source fiable)**, ajoutez l'adresse IP de sortie de la branche.



STEP 3 | Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Infrastructure Settings (Paramètres d'infrastructure)**. Sous **Proxy URL Settings (Paramètres d'URL de proxy)**, activez **Enable Source IP based visibility and enforcement (Activer la visibilité et l'application basées sur l'IP source)**, puis cliquez sur **Save (Enregistrer)**.



STEP 4 | (Facultatif) Configurez les règles de sécurité avec l'adresse IP source du terminal.

STEP 5 | Définissez l'option **Push Config (Transmettre la configuration)** sur **Explicit Proxy (Proxy explicite)**.

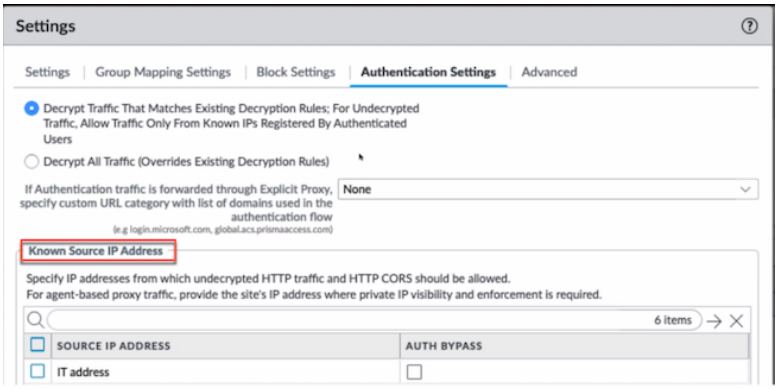
Visibilité et application de l'adresse IP privée pour le trafic de proxy basé sur l'agent (Panorama)

STEP 1 | Activez la fonctionnalité de proxy basé sur l'agent (Proxy mode (Mode proxy) et Tunnel and Proxy mode (Mode tunnel et proxy)) pour les utilisateurs mobiles.

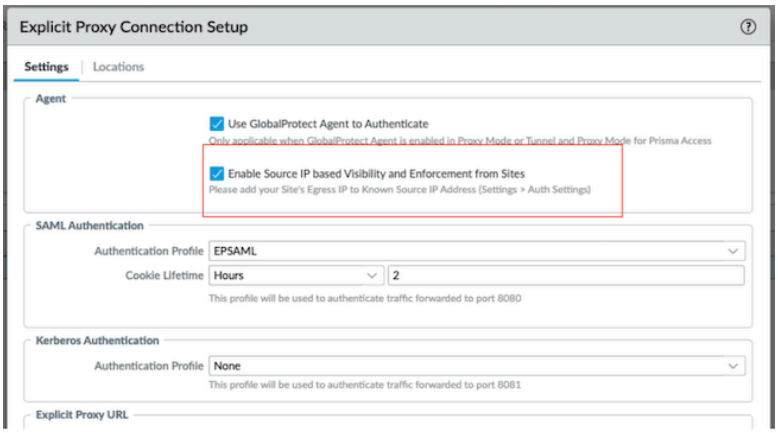
STEP 2 | Accédez à **Cloud Services** > **Configuration** > **Mobile Users (Utilisateurs mobiles)** > **Explicit Proxy (Proxy explicite)** > **Settings (Paramètres)** > **Authentication Settings (Paramètres**

 ©2025 Palo Alto Networks, Inc.

d'authentification) et ajoutez l'adresse IP de sortie de la branche sous **Known Source IP Address (Adresse IP source connue)**.



STEP 3 | Accédez à **Cloud Services** > **Configuration** > **Mobile Users-Explicit Proxy (Utilisateurs mobiles-Proxy explicite)**. Sous **Agent**, activez **Enable Source IP based Visibility and Enforcement from Sites (Activer la visibilité et l'application basées sur l'adresse IP source à partir des sites)**, puis cliquez sur **OK**.



STEP 4 | (Facultatif) Configurez les règles de sécurité avec l'adresse IP source du terminal.

STEP 5 | Validez et appliquez vers le **Explicit_Proxy_Device_Group**.

Authentification SAML pour le proxy explicite

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

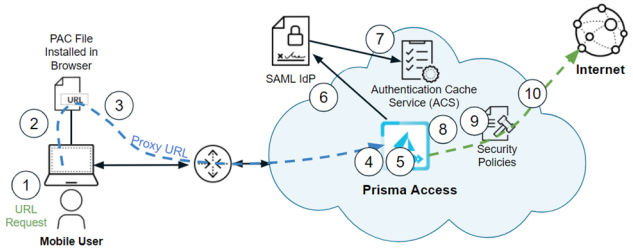
Découvrez comment fonctionne le proxy explicite avec SAML et comment le configurer.

- Comment le proxy explicite avec SAML traite le trafic
- Configurer le proxy explicite avec SAML

 ©2025 Palo Alto Networks, Inc.

Comment le proxy explicite avec SAML traite le trafic

Voici comment fonctionne le proxy explicite avec SAML. Suivez- pour voir le chemin emprunté par le trafic :



STEP 1 | L'utilisateur mobile navigue sur Internet ou accède à l'application SaaS en saisissant l'URL ou l'adresse IP à l'aide d'un navigateur Web.

STEP 2 | Le navigateur sur le terminal des utilisateurs mobiles vérifie le fichier PAC.

Ce fichier PAC spécifie que l'URL ou la requête SaaS doit être envoyée au proxy explicite de Prisma Access.

STEP 3 | Le client HTTPS (le navigateur sur le terminal de l'utilisateur mobile) transmet la demande d'URL à l'URL du proxy.

STEP 4 | Le trafic est redirigé vers le proxy explicite, qui décrypte le trafic.

STEP 5 | Le proxy inspecte le trafic et vérifie la présence du cookie d'authentification mis en place par le proxy explicite de Prisma Access.

Le cookie contient des informations qui identifient l'utilisateur mobile et utilise le cookie pour authentifier l'utilisateur.

STEP 6 | Si, lors de l'inspection du cookie, Prisma Access détermine que l'utilisateur n'est pas authentifié, il le redirige pour l'authentification.

STEP 7 | Une fois que l'IdP a authentifié l'utilisateur, Prisma Access stocke l'état d'authentification de l'utilisateur dans le service de cache d'authentification (ACS, Authentication Cache Service). La durée de validité de l'authentification est basée sur la valeur **Cookie Lifetime (Durée de vie des cookies)** que vous spécifiez lors de la configuration du proxy explicite.

STEP 8 | Le proxy explicite vérifie la présence et la validité de notre cookie. Si le cookie n'est pas présent ou n'est pas valide, l'utilisateur est redirigé vers l'ACS. Une fois que l'ACS a confirmé l'authentification de l'utilisateur, celui-ci est redirigé vers le proxy explicite à l'aide d'un jeton. Le proxy valide ensuite ce jeton et définit le cookie pour ce domaine et pour cet utilisateur.

STEP 9 | Prisma Access applique l'application de la sécurité en fonction des règles de politique de sécurité que l'administrateur a configurées.

STEP 10 | Si l'URL n'est pas bloquée par les règles de politique de sécurité, Prisma Access envoie la requête d'URL à Internet.

STEP 11 | (Facultatif) Configurez la connectivité du proxy explicite dans GlobalProtect pour une sécurité Internet permanente. Activez cette fonctionnalité pour assurer une sécurité

 ©2025 Palo Alto Networks, Inc.

permanente du trafic Internet, tout en fournissant un accès à la demande aux applications privées via GlobalProtect ou un VPN tiers.

Configurer le proxy explicite avec SAML

Suivez ces étapes pour configurer le proxy explicite avec l'authentification SAML.

- Strata Cloud Manager
- Panorama

Configurer un proxy explicite avec SAML (Strata Cloud Manager)

STEP 1 | Configurez un proxy explicite.

STEP 2 | (Facultatif) Configurez Cloud Identity Engine l'authentification pour le proxy explicite.

STEP 3 | Configurez des règles de politique de sécurité.

1. Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGSW et Prima Access)** > **Configuration Scope: Explicit Proxy (Étendue de la configuration : proxy explicite)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)**.
2. Personnalisez les règles de politique par défaut en fonction de vos besoins et des meilleures pratiques en matière de politique de sécurité des passerelles Internet.

   *Avec Prisma Access 5.1 et un plan de données PAN-OS 10.2.10 ou d'une version ultérieure, vous n'aurez besoin que de la règle de politique de sécurité **Allow Web Access to Known Users (Autoriser l'accès web aux utilisateurs connus)**.*

STEP 4 | Appliquez les modifications apportées à la configuration.

Configurer un proxy explicite avec SAML (Panorama)

STEP 1 | Configurez un proxy explicite.

STEP 2 | (Facultatif) Configurez Cloud Identity Engine l'authentification pour le proxy explicite.

STEP 3 | En fonction de votre version de Prisma Access et de la version votre de plan de données, configurez soit une seule règle de politique, soit plusieurs.

Exigences en matière de version	Configuration
Prisma Access 5.1 ou une version ultérieure et un plan de données PAN-OS 10.2.10 ou une version ultérieure.	Configurez une règle de politique de sécurité pour le trafic utilisateur avant authentification. **1.** Sélectionnez le **Explicit_Proxy_Device_Group**. **2.** Créez un filtre d'application à l'aide de l'étiquette **Web App (Application web)**.

 ©2025 Palo Alto Networks, Inc.

Exigences en matière de version	Configuration
	3. Sélectionnez **Policies (Politiques)** > **Pre Rules (Pré-règles)** > **Add (Ajouter)**. 4. Créez la règle. 1. Cliquez sur **Add (Ajouter)** pour ajouter la règle. 2. Donnez-lui un nom descriptif. Par exemple, **`allow-pre-auth`** . 3. Sous l'onglet **Application**, cliquez sur **Add (Ajouter)** pour ajouter le filtre d'application **Web App (Application web)**. 4. Sous l'onglet **Source**, cliquez sur **Add (Ajouter)** pour ajouter un **Known-user (Utilisateur connu)**.
Toutes les autres versions de Prisma Access et du plan de données.	Configurez des règles de politique de sécurité en fonction de vos besoins et des meilleures pratiques en matière de politique de sécurité des passerelles Internet.

STEP 4 | **Commit (Validez)** la configuration.

Configurer un proxy explicite

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) Si vous souhaitez activer la visibilité et l'application basées sur l'IP de source privée sur le proxy explicite dans votre environnement Prisma Access, contactez votre équipe de compte pour en savoir plus.	• Licence Prisma Access

Utilisez le proxy explicite pour sécuriser les utilisateurs mobiles en redirigeant le trafic du navigateur vers Prisma Access.

Directives d'intégration—Utilisez les instructions suivantes lors de l'octroi d'une licence et de l'intégration de votre déploiement de proxy explicite :

- Le proxy explicite prend en charge un sous-ensemble d'emplacements Prisma Access.

 ©2025 Palo Alto Networks, Inc.

- Vous ne pouvez pas ajouter des emplacements signalés par deux astérisques. il s'agit de zones locales qui ne sont pas prises en charge avec Prisma Access.
- Si vous disposez d'une licence locale ou d'évaluation pour Prisma Access pour les utilisateurs et que vous disposez d'un déploiement Utilisateurs mobiles GlobalProtect et d'un déploiement Utilisateurs mobiles Proxy explicite, vous pouvez déployer un maximum de cinq emplacements pour chacun (cinq emplacements maximum pour Utilisateurs mobiles GlobalProtect et cinq emplacements maximum pour Utilisateurs mobiles Proxy explicite). Si vous disposez d'une licence mondiale, il n'y a pas de restrictions quant au nombre maximal d'emplacements.
- Le proxy explicite prend en charge les multi-locataires dans les conditions suivantes : si vous disposez d'un déploiement non multi-locataires Prisma Access et si vous le convertissez en déploiement multi-locataires, seul le premier locataire (le locataire que vous avez migré) prend en charge le proxy explicite. Aucun des locataires que vous créez ensuite pour le déploiement multilocataire après le premier ne prend en charge le proxy explicite.
- Lors de l'intégration d'un déploiement de proxy explicite, Palo Alto Networks recommande que toute la configuration soit effectuée dans un seul navigateur. Vous pouvez toutefois ajouter des stratégies de sécurité à partir de plusieurs navigateurs ou sessions de navigateur.
- Actions de filtrage d'URL de **continue (continuer)** ou **override (remplacer)** ne sont pas pris en charge et ne fonctionnent pas avec le proxy explicite.

Découvrez comment configurer le proxy explicite.

- Strata Cloud Manager
- Panorama

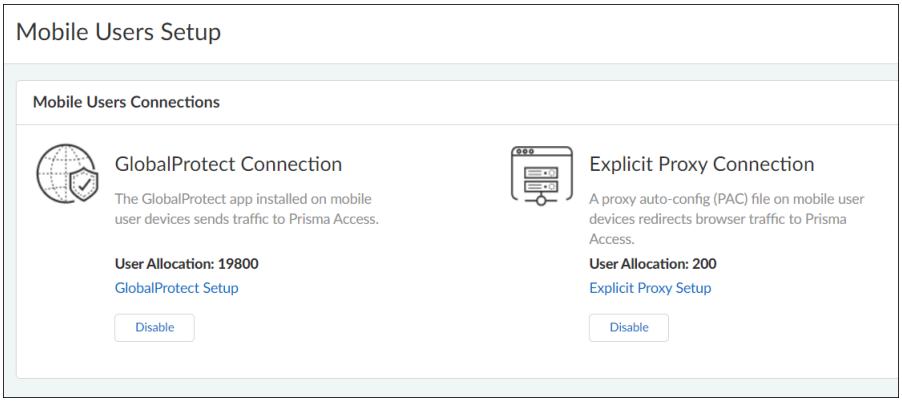
Cloud Management

Configurer une connexion proxy explicite pour les utilisateurs mobiles ; avec un proxy explicite, un fichier PAC (Proxy Auto-Config) sur les périphériques des utilisateurs mobiles redirige le trafic du navigateur vers Prisma Access.

Avant de commencer, assurez-vous de passer en revue les lignes directrices du proxy explicite.

STEP 1 | Activer le proxy explicite et allouer des utilisateurs

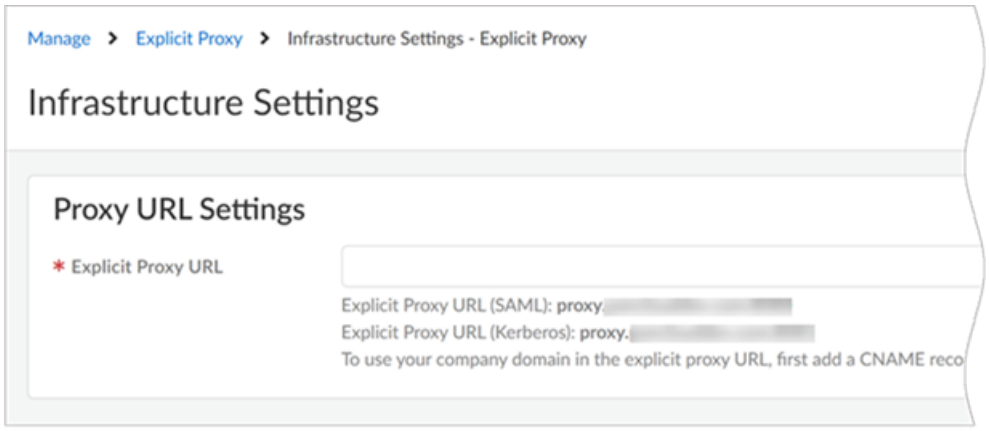
Allez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Mobile Users (Utilisateurs mobiles)** pour commencer la configuration du proxy explicite. Lorsque vous activez le proxy explicite, vous êtes invité à spécifier le nombre d'utilisateurs mobiles qui utiliseront ce type de connexion.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Ajoutez les paramètres de proxy que les utilisateurs mobiles utiliseront pour se connecter à Prisma Access

Allez dans les **Infrastructure Settings (Paramètres d'infrastructure)**.



1. Spécifiez une URL de proxy explicite.

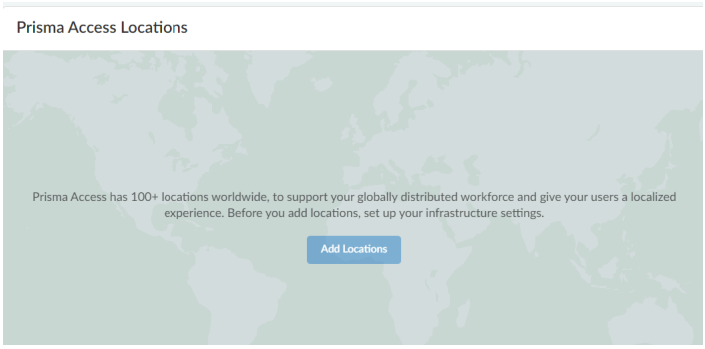
   Par défaut, le nom est *nom du proxy*.proxy.prismaaccess.com, où *nom du proxy* est le sous-domaine que vous spécifiez et utilise le port 8080. Pour utiliser le domaine de votre entreprise dans l'URL de proxy explicite ajoutez un enregistrement CNAME au domaine de votre organisation.

   Vous pouvez utiliser les types d'authentification SAML ou Kerberos pour authentifier les utilisateurs mobiles.
2. (Facultatif) Sélectionnez **Enable Agent Proxy (Activer le proxy de l'agent)** pour activer la fonctionnalité de proxy basée sur l'agent.

   Activez cette fonctionnalité pour configurer le proxy explicite en Mode proxy ou Mode tunnel et proxy.
3. Utiliser les règles de transfert pour créer un fichier PAC qui répond à vos besoins ou télécharger votre propre fichier PAC dans un profil de redirection..

STEP 3 | Sélectionnez l'emplacement Prisma Access auquel vos utilisateurs mobiles se connecteront

Ajoutez les emplacements Prisma Access où vous souhaitez prendre en charge les utilisateurs mobiles.



La carte affiche les emplacements Prisma Access.

Pour une expérience utilisateur optimale, si vous limitez le nombre d'emplacements, choisissez les emplacements les plus proches ou situés dans le même pays que vos utilisateurs. Si un

 ©2025 Palo Alto Networks, Inc.

emplacement n'est pas disponible dans le pays où résident vos utilisateurs mobiles, choisissez l'emplacement le plus proche de vos utilisateurs pour obtenir les meilleures performances.

Vous devez activer les emplacements de proxy explicite dans au moins deux régions pour garantir la redondance régionale.

STEP 4 | Authentifiez les utilisateurs mobiles

Configurez **User Authentication (Authentification utilisateur)** de sorte que seuls les utilisateurs légitimes aient accès à vos services et applications.

SAML et Kerberos sont les protocoles d'authentification pris en charge. Prisma Access prend en charge PingOne, Azure AD et Okta en tant que fournisseurs d'authentification SAML, mais vous devez pouvoir utiliser n'importe quel fournisseur qui prend en charge SAML 2.0 en tant que fournisseur d'identité SAML (IdP). En savoir plus sur comment Permettre aux utilisateurs mobiles de s'authentifier auprès de Prisma Access.

STEP 5 | Passez en revue les règles de sécurité recommandées qui sont activées par défaut

Prisma Access applique les règles de stratégie de sécurité recommandées par défaut. Ces règles permettent à vos utilisateurs de naviguer en toute sécurité vers des sites Internet généraux. Les utilisateurs sont :

- Interdits d'accès à des sites Web malveillants connus en fonction de l'URL
- Interdits de téléversement ou de téléchargement de fichiers connus pour être malveillants
- Protégés contre des menaces inconnues et inédites
- Protégés contre les virus, les logiciels espions (attaques de commande et de contrôle) et les vulnérabilités

Après avoir effectué la configuration initiale, vous pouvez examiner et mettre à jour ces règles par défaut pour répondre aux besoins de votre entreprise.

STEP 6 | Vérifiez que la position des utilisateurs mobiles est active

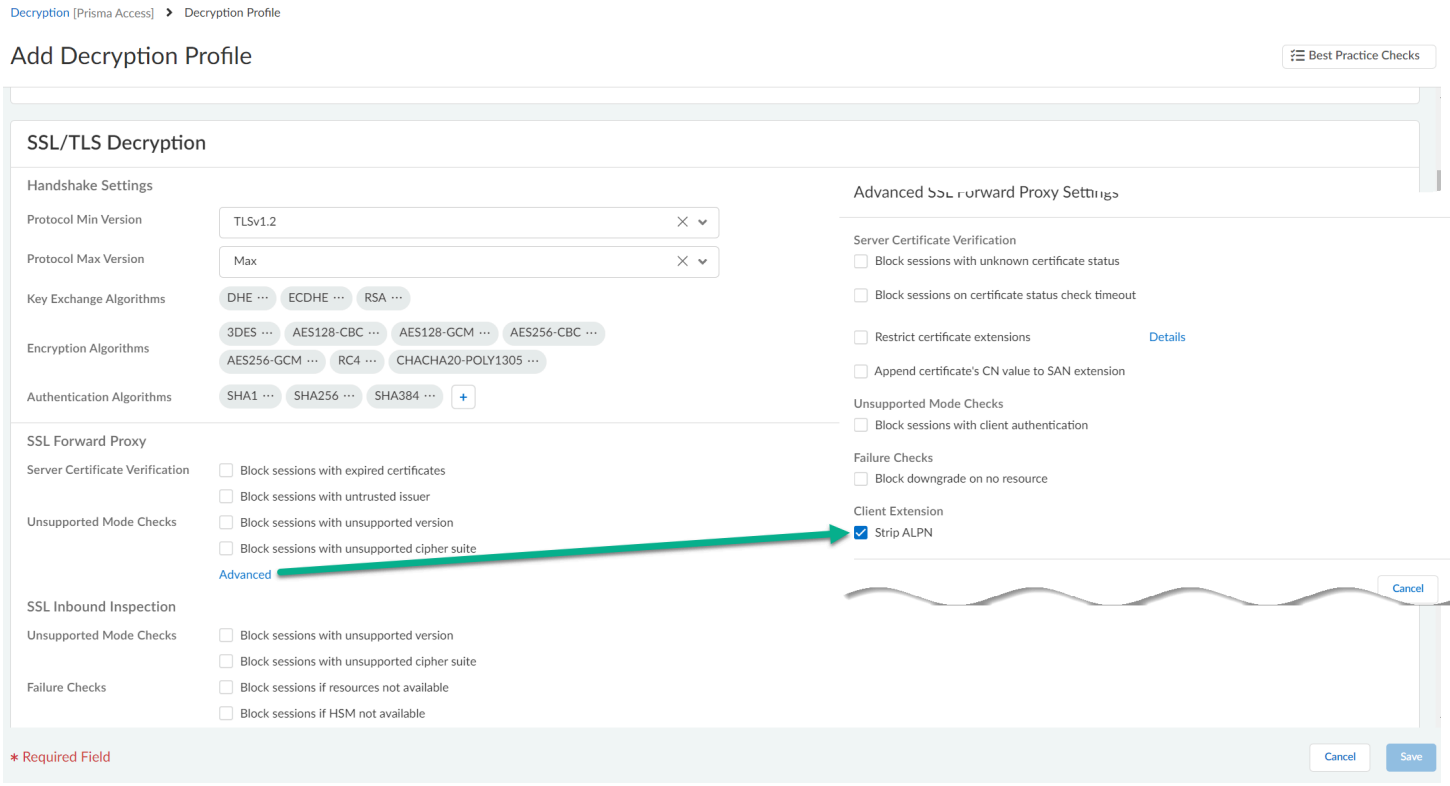
Après avoir poussé votre configuration initiale à Prisma Access, Prisma Access commence à approvisionner votre environnement utilisateur mobile. Cela peut prendre jusqu'à 15 minutes. Une fois que vos emplacements d'utilisateurs mobiles sont opérationnels, vous pouvez les vérifier sur les pages de configuration des utilisateurs mobiles, dans la vue d'ensemble et dans Informations.

*Vous pouvez également valider votre configuration en sélectionnant **Manage (Gérer)** > **Service Setup (Configuration du service)** > **Mobile Users (Utilisateurs mobiles)** et modifiez les paramètres d'infrastructure pour confirmer qu'une passerelle est configurée dans chacun des emplacements que vous avez approvisionnés.*

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Activer le déchiffrement pour le trafic proxy explicite

- Définissez la version TLS maximale prise en charge sur 1.2.
- Définissez **Strip ALPN (Enlever l'ALPN)** (Paramètres avancés de proxy de transfert SSL), car le proxy explicite ne prend pas en charge HTTP/2 natif et vous devez supprimer les en-têtes ALPN.



STEP 8 | Téléchargez la CA racine et installez-la sur votre point de terminaison pour le décryptage SSL.

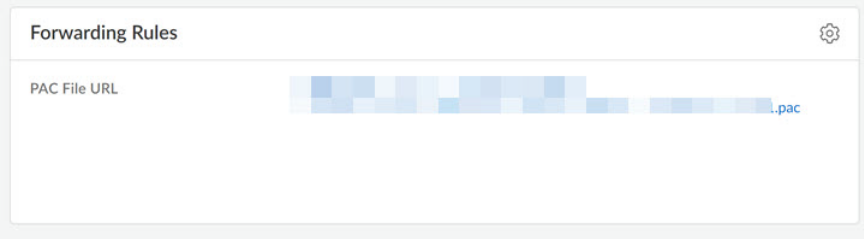
 ©2025 Palo Alto Networks, Inc.

STEP 9 | **Edit the PAC file content (Modifier le contenu du fichier PAC).**

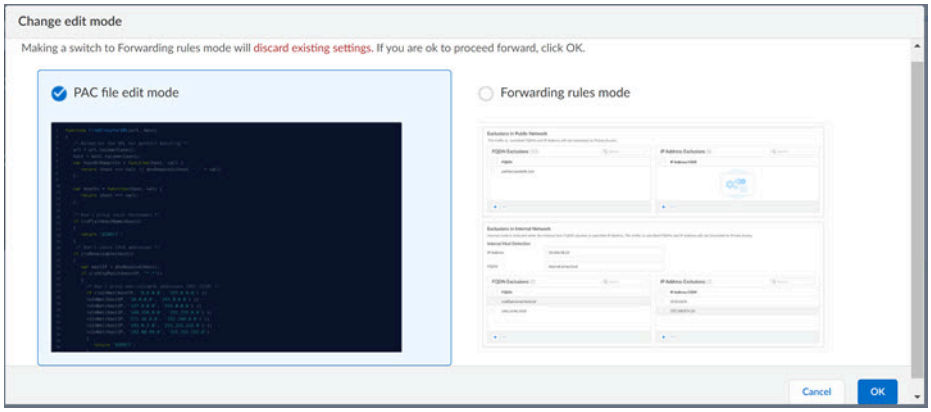
Utilisez Profils de transfert pour gérer les fichiers PAC.

Modifiez un fichier de configuration automatique de proxy (PAC) pour un proxy explicite qui répond à vos besoins. L'application GlobalProtect transmet par proxy le trafic vers Prisma Access sur la base des règles de transfert et la logique du fichier PAC.

Allez dans les **Forwarding Rules (Règles de transfert)** :



1. Téléchargez le fichier PAC et personnalisez-le pour qu'il réponde à vos besoins. Ensuite, importez-le de nouveau ici et nous vous donnerons l'URL de l'emplacement où Prisma Access héberge le fichier PAC.
2. Modifiez le fichier PAC à l'aide du**PAC File Editor (Éditeur de fichier PAC)** ou du **Forwarding rules mode (Mode de règles de transfert)**.
3. Le mode **PAC File Editor (Éditeur de fichier PAC)** est sélectionné par défaut. Cliquez sur **OK** pour modifier dans le mode d'édition du fichier PAC.
4. Sélectionnez **Forwarding rules mode (Mode de règles de transfert)** et cliquez sur **OK** pour modifier dans le mode de règles de transfert. Le passage en mode de règles de transfert supprime les paramètres existants.



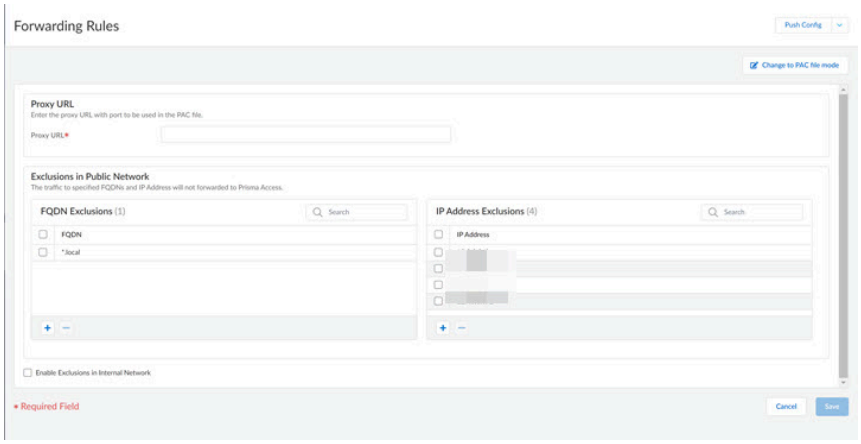
- Spécifiez une **Explicit Proxy URL (URL de proxy explicite)** avec le port à utiliser dans le fichier PAC.

  Par défaut, le nom est proxyname.proxy.prismaaccess.com, où proxyname est le sous-domaine que vous spécifiez et utilise port 8080.
- Configurez **Exclusions in Public Network (Exclusions dans le réseau public)** lorsque vos utilisateurs mobiles de proxy explicite se connectent à Prisma Access à partir d'un réseau public.

 ©2025 Palo Alto Networks, Inc.

- Configurez **FQDN Exclusions (Exclusions de FQDN)** et **IP Address Exclusions (Exclusions d'adresses IP)**. Les noms de domaines complets et les adresses IP exclus ne seront pas transférés à partir de Prisma Access.

- **Enable Exclusions in Internal Network (Activer les exclusions dans le réseau interne)** pour configurer des exclusions pour des adresses IP ou des noms de domaines complets spécifiques lorsque les utilisateurs mobiles de proxy explicite se connectent à Prisma Access sur le réseau interne.
  - Spécifiez les exclusions ci-dessous pour avoir des exclusions de trafic différentes lorsque l'utilisateur se trouve sur le réseau interne.
    - Saisissez la **IP Address (Adresse IP)** d'un hôte qui peut être résolue uniquement depuis le réseau interne.
    - Saisissez le **FQDN** qui correspond à l'adresse IP que vous entrez.
  - Configurez des exclusions pour des noms de domaine complets et des adresses IP spécifiques. Le trafic vers les noms de domaine complets et les adresses IP spécifiés ne sera pas transféré à partir de Prisma Access.
- **Save (Enregistrez)** les modifications.

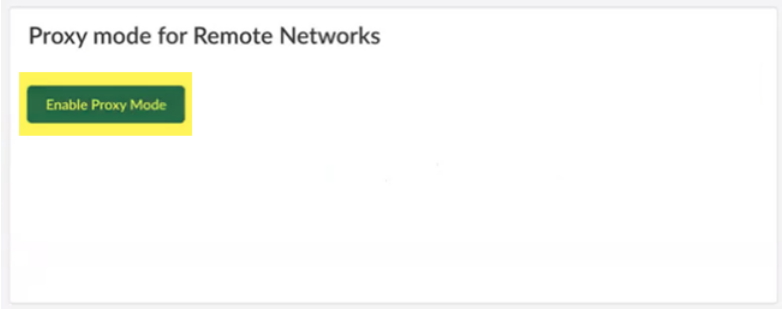


STEP 10 | Configurez les **Advanced Security Settings (Paramètres de sécurité avancés)**.

- Si vous souhaitez transférer le trafic vers le proxy explicite de vos succursales via un tunnel IPSec sécurisé, **Enable Proxy Mode (Activer le mode proxy)** et récupérez les adresses IP

 ©2025 Palo Alto Networks, Inc.

anycast si vous souhaitez utiliser le proxy explicite en conjonction avec un réseau distant Prisma Access.



Cette solution utilise des adresses anycast avec un tunnel IPSec de réseau distant pour permettre l'utilisation d'un proxy explicite pour les utilisateurs et les périphériques d'un site réseau distant ou d'une succursale.

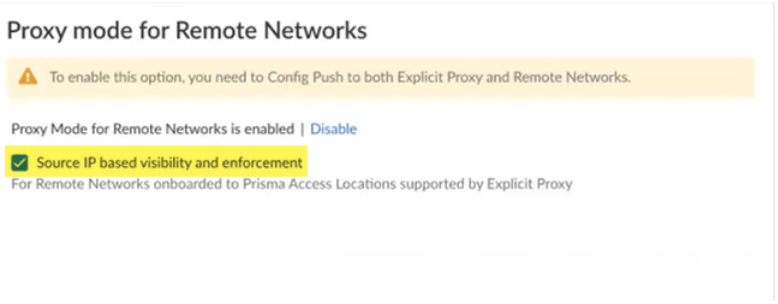
- Déploiements en mode proxy uniquement Si le mode proxy est activé sur vos réseaux distants, ajoutez une stratégie pour autoriser le trafic lié à des adresses IP anycast et unicast sur des réseaux distants. Si vous avez activé **Source IP visibility and enforcement (Visibilité et application basées sur l'IP source)**, utilisez le champ **Source IP (IP Source)** dans les Stratégies de sécurité dans le proxy explicite pour sécuriser le trafic. Vous avez besoin de stratégies supplémentaires dans les réseaux distants.

 ©2025 Palo Alto Networks, Inc.

- (Facultatif) Si vous activez le mode proxy, pour exploiter les adresses IP privées des systèmes de vos succursales qui transfèrent le trafic vers le proxy explicite, sélectionnez **Source IP based visibility and enforcement (Visibilité et application basées sur l'IP source)**.

  Cette fonctionnalité a ces exigences :

  - Un Prisma Access plan de données minimum de 10.2.4
  - Un déploiement Prisma Access (Managed by Panorama) avec un plug-in Services Cloud minimum de 4.1
  - Les adresses IP sources ne s'affichent que pour les emplacements du réseau distant qui sont pris en charge avec le proxy explicite.



- Spécifiez **Block Sources (Bloquer les sources)**.

  Ajoutez tout trafic d'adresse IP source qui doit être bloqué à la liste **Block Source Address (Bloquer l'adresse source)**.

  Spécifiez une adresse, un groupe d'adresses ou une liste EDL.

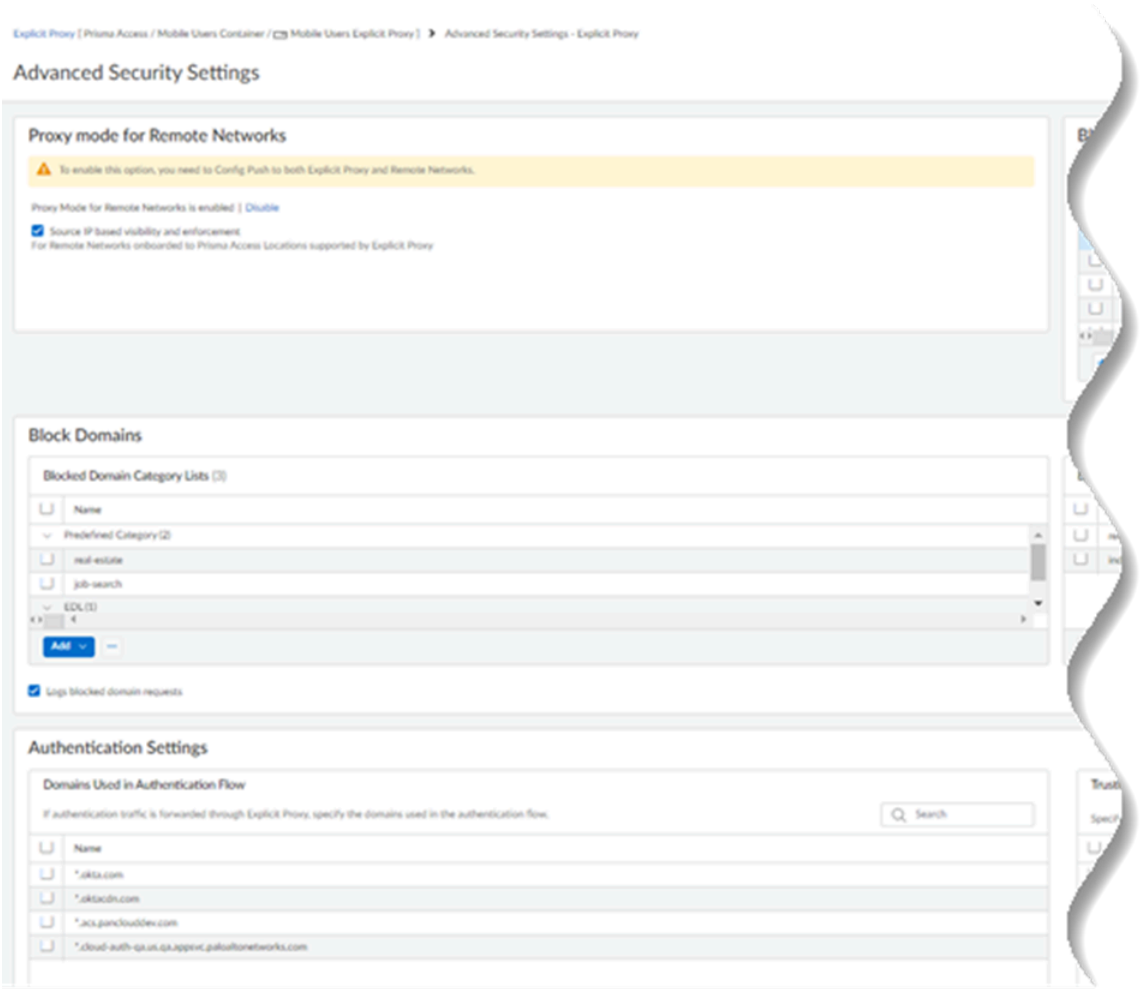
  Pour exclure les entrées de la liste d'adresses IP de l'application, **Add Exception (Ajouter une exception)** et sélectionnez les adresses IP à exclure du blocage.
- Spécifiez **Blocked Domains (Domaines bloqués)**.

  Spécifiez les domaines ou les catégories de domaine pour les sites Web malveillants ou pour les sites Web auxquels vous ne souhaitez pas que les utilisateurs puissent accéder. Prisma Access empêche les utilisateurs d'accéder aux URL et aux adresses IP que vous spécifiez dans cette zone lorsqu'ils lancent un HTTP GET (pour les requêtes non chiffrées)

 ©2025 Palo Alto Networks, Inc.

ou HTTP CONNECT (pour les requêtes chiffrées). Les utilisateurs sont redirigés vers une page de blocage lorsqu'ils tentent d'accéder à des sites web bloqués.

- Si vous souhaitez exempter des domaines inclus dans une liste de catégories de domaines bloqués, spécifiez-les dans la **Exception List (Liste des exceptions)**.

  Tous les domaines entrés sont exemptés d'être bloqués, même s'ils apparaissent dans une catégorie de domaine que vous avez bloquée.
- Le proxy explicite nécessite un déchiffrement pour authentifier les utilisateurs. Saisissez les **Domains used in the authentication flow (Domaines utilisés dans le flux d'authentification)**.
- 

- Entrez toutes les adresses IP à partir desquelles le trafic CORS (Cross-Origin Resource Sharing) HTTPS ou HTTP non déchiffré peut être autorisé pour **Trusted Source Address (Adresse de source fiable)**.
- Pour contourner l'authentification des adresses de source fiables que vous avez saisies, sélectionnez **Skip authentication (Ignorer l'authentification)**.

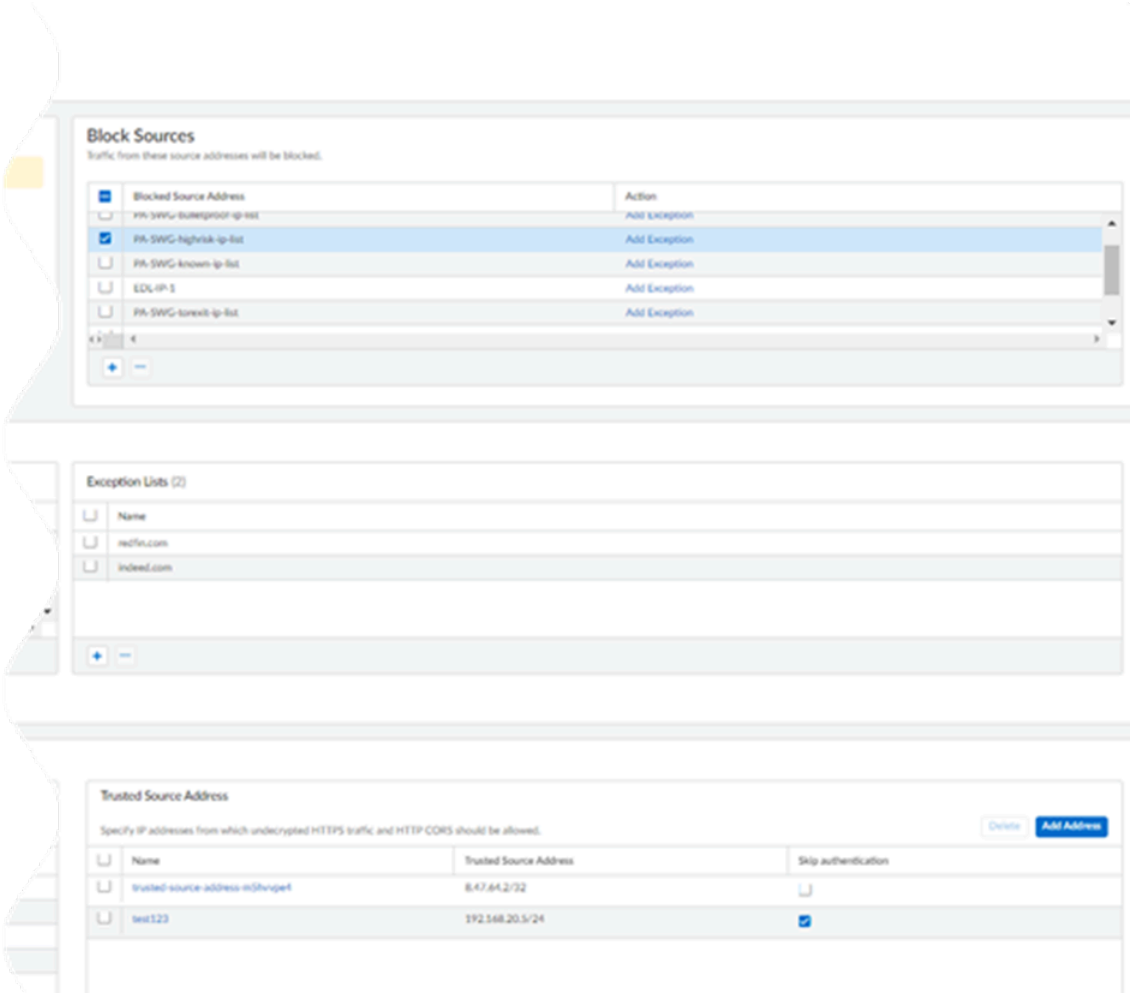
  Vous pouvez utiliser **Skip authentication (Ignorer l'authentification)** avec **Source IP based visibility and enforcement (Visibilité et application basées sur l'IP source)** pour ignorer

 ©2025 Palo Alto Networks, Inc.

l'authentification des systèmes sans tête qui ne peuvent pas s'authentifier, configurer des stratégies de sécurité et obtenir une visibilité du trafic sur le proxy explicite Prisma Access.

Vous pouvez ajouter des adresses IP ou des sous-réseaux. Un maximum de 100 000 adresses IP est pris en charge après l'extension des sous-réseaux.

Si vous sélectionnez **Skip authentication (Ignorer l'authentification)** pour ignorer l'authentification d'un objet d'adresse, et que vous souhaitez ensuite activer l'authentification en désélectionnant **Skip authentication (Ignorer l'authentification)** pour cet objet d'adresse, il peut s'écouler jusqu'à 24 heures avant que la modification ne prenne effet une fois que vous avez effectué la modification et que vous avez validé et poussé vos modifications.

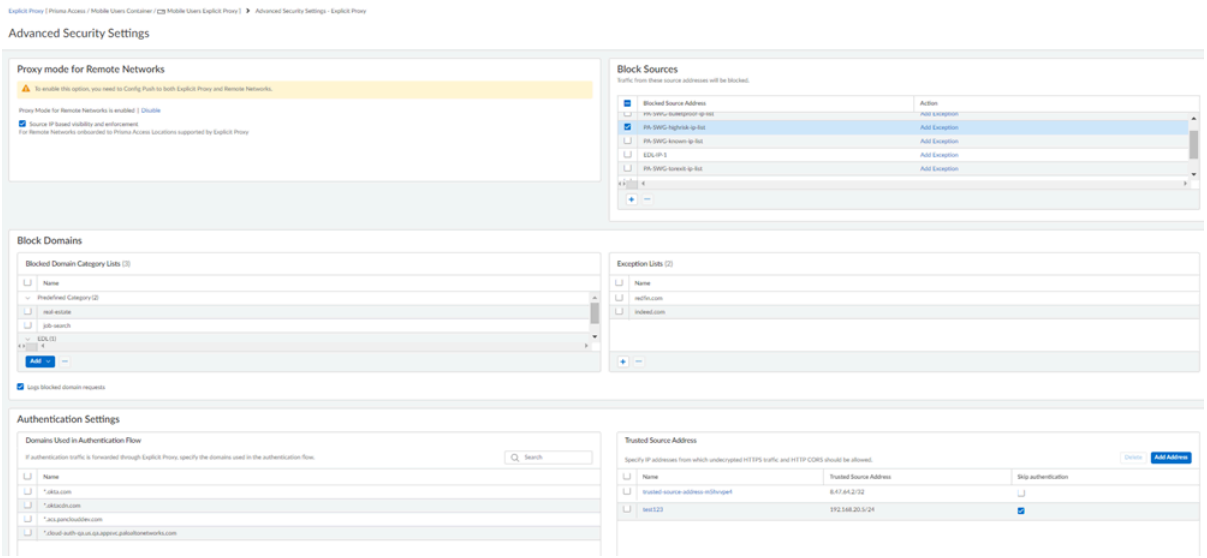
- 

- Si vous disposez d'un déploiement de proxy explicite et que vous avez ajouté une liste d'adresses IP sources fiables, vous pouvez **Use X-Authenticated-User (XAU) headers on incoming HTTP/HTTPS requests for identity (Utiliser les en-têtes X-Authenticated-User (XAU) sur les requêtes HTTP/HTTPS entrantes pour l'identité)**. Utilisez cette fonctionnalité

 ©2025 Palo Alto Networks, Inc.

pour autoriser les utilisateurs connectés à partir d'un autre proxy qui utilisent des en-têtes XAU pour l'authentification.

*Vous devez cliquer sur **Save (Enregistrer)** pour que le paramètre XAU prenne effet.*



Configurer un proxy explicite (Panorama)

Pour sécuriser les utilisateurs mobiles à l'aide d'un proxy explicite, procédez comme suit.

Avant de configurer le proxy explicite, parcourez la liste de contrôle de planification et apprenez à configurer le fichier PAC de proxy explicite.

STEP 1 | Configurez l'authentification pour le proxy explicite.

SAML et Kerberos sont les types d'authentification pris en charge.

Utilisez les instructions suivantes lors de la configuration de l'authentification SAML pour l'IdP et dans Panorama :

- **Lignes directrices de Panorama :**
  - Configurez un **SAML Identity Provider (Fournisseur d'identité SAML)** et un **Authentication profile (Profil d'authentification)** pour Prisma Access. Vous spécifiez le profil d'authentification que vous créez à une étape ultérieure.
  - Assurez-vous de configurer le profil d'authentification sous **Explicit_Proxy_Template**.
  - Utilisez **mail (courrier)** en tant qu'attribut utilisateur dans le profil de serveur IdP et dans le **Authentication profile (Profil d'authentification)** sur Panorama.
  - Le proxy explicite ne prend pas en charge **Sign SAML Message to IdP (Signer un message SAML vers IdP)** dans le profil serveur du fournisseur d'identité SAML.
  - Lorsque vous configurez Cloud Identity Engine pour récupérer les informations de mappage d'utilisateur et de groupe, utilisez **mail (courrier)** ou **userPrincipalName** comme **SamAccountName** dans le mappage de groupe.
  - Lors de la configuration de **Group mapping Settings (Paramètres de mappage de groupe)** lors de la configuration du proxy explicite, utilisez le même attribut de répertoire

 ©2025 Palo Alto Networks, Inc.

pour le nom d'utilisateur principal et l'adresse e-mail, ou Prisma Access ne reflète pas précisément le nombre d'utilisateurs. Par exemple, étant donné le profil d'utilisateur suivant :

```
sAMAccountName : muser Netbios : exemple userPrincipalName :
 muser@example.com mail : mobile.user@example.com
```

Si, dans la configuration de Cloud Identity Engine, vous utilisez un **Primary Username (Nom d'utilisateur principal)** `userPrincipalName` et un **E-Mail (Courriel)** `mail (courrier)`, les informations sur l'utilisateur que Strata Logging Service renvoie dans les journaux de trafic et les informations utilisateur renvoyées par ACS dans les journaux d'authentification seront différentes. Dans cet exemple, ACS envoie l'attribut **mail (courrier)** (mobile.user@example.com) aux journaux d'authentification et Strata Logging Service envoie l'attribut **userPrincipalName** (muser@example.com) aux journaux de trafic. En raison de cette incohérence, votre nombre d'utilisateurs ne sera pas exact dans les champs **Current Users (Utilisateurs actuels)** et **Users (Last 90 days) (Utilisateurs (90 derniers jours))** lors de la vérification du statut Proxy explicite dans le Statut (**Panorama** > **Cloud Services** > **Status (État)** > **Status (État)**). Pour cette raison, utilisez le même attribut de répertoire pour **Primary Username (Nom d'utilisateur principal)** et **E-Mail (Courriel)** (par exemple, **mail (courrier)**) lors de la spécification des **Group Mapping Settings (Paramètres de mappage de groupe)**.

- Lors de l'utilisation de Panorama pour gérer Prisma Access, Cloud Identity Engine ne renseigne pas automatiquement les informations sur l'utilisateur et le groupe dans les règles de stratégie de sécurité.

- **Directives IdP :**
  - Utilisez les URL suivantes lors de la configuration de SAML :

    Service consommateur d'assertion SAML URL: **`https://global.acs.prismaaccess.com/saml/acs`**

    ID d'entité URL: **`https://global.acs.prismaaccess.com/saml/metadata`**
  - Si vous utilisez Okta comme IdP, utilisez **EmailAddress** pour le paramètre **Name ID Format (Format de l'ID de nom)**.
  - Entrez une URL d'ouverture de session unique `https://global.acs.prismaaccess.com/saml/acs`.
  - La déconnexion unique (SLO) n'est pas prise en charge.
  - Pour résoudre les problèmes d'authentification de l'IdP, utilisez les fonctionnalités de surveillance et de dépannage de l'IdP. L'ACS n'enregistre pas les échecs d'authentification IdP.
  - Lors de la création d'un **Authentication profile (Profil d'authentification)** pour l'IdP SAML, dans l'onglet **Advanced (Avancé)**, sélectionnez **all (tout)** dans la **Allow List (Liste d'autorisation)** ou le proxy explicite ne sera pas en mesure de récupérer le mappage de groupe.

 ©2025 Palo Alto Networks, Inc.

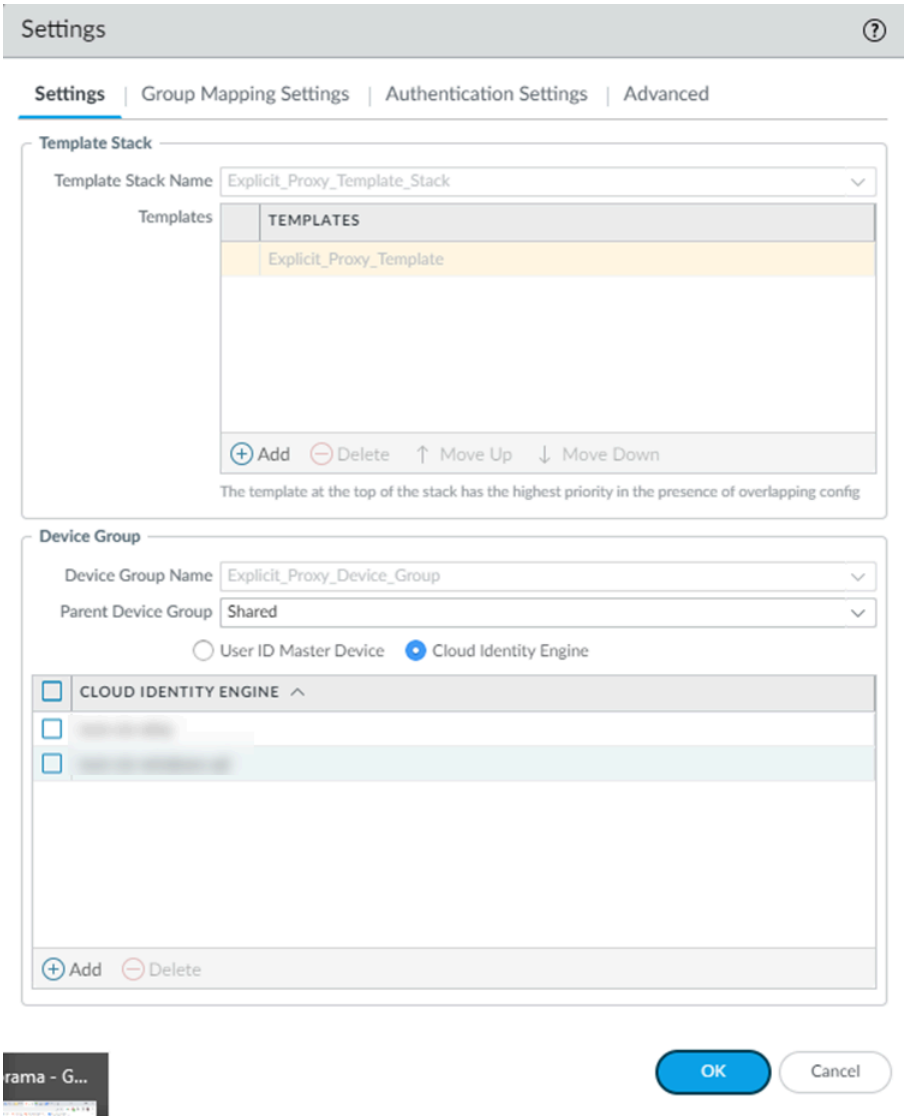
STEP 2 | Configurer les paramètres de proxy explicite.

1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—Explicit Proxy (Utilisateurs mobiles—Proxy explicite)** et cliquez sur l'icône d'engrenage pour modifier les **Settings (Paramètres)** du proxy explicite.
2. Dans l'onglet **Settings (Paramètres)**, modifiez les paramètres suivants :
   - (Facultatif) Vérifiez les noms du modèle et de la pile de modèles.

     Par défaut Prisma Access crée une nouvelle pile de modèles **Explicit_Proxy_Template_Stack** et un nouveau modèle **Explicit_Proxy_Template**. Assurez-vous d'utiliser ce modèle lorsque vous créez et modifiez les paramètres de votre **Device (Périphérique)** dans Panorama.
   - Dans la section Groupe de périphériques, sélectionnez **Parent Device group (Groupe de périphériques parent)** qui contient les paramètres de configuration que vous souhaitez envoyer pour le proxy explicite, ou laissez le groupe de périphériques parent comme **Shared (Partagé)** pour utiliser la hiérarchie partagée du groupe de périphériques Prisma Access. Le **Device group Name (Nom du groupe de périphériques)** ne peut pas être modifié.
   - (Facultatif) Si vous avez configuré un pare-feu de la nouvelle génération en tant que périphérique principal ou ajouté un profil Cloud Identity Engine pour renseigner les informations d'utilisateur et de groupe dans les règles de stratégie de sécurité, sélectionnez le périphérique principal User-ID ou Cloud Identity Engine ; sélectionnez ensuite le périphérique principal ou le profil Cloud Identity Engine que vous avez créé.

 ©2025 Palo Alto Networks, Inc.

- Dans la section Allocation de licences, spécifiez le nombre d'utilisateurs mobiles à allouer pour le proxy explicite.



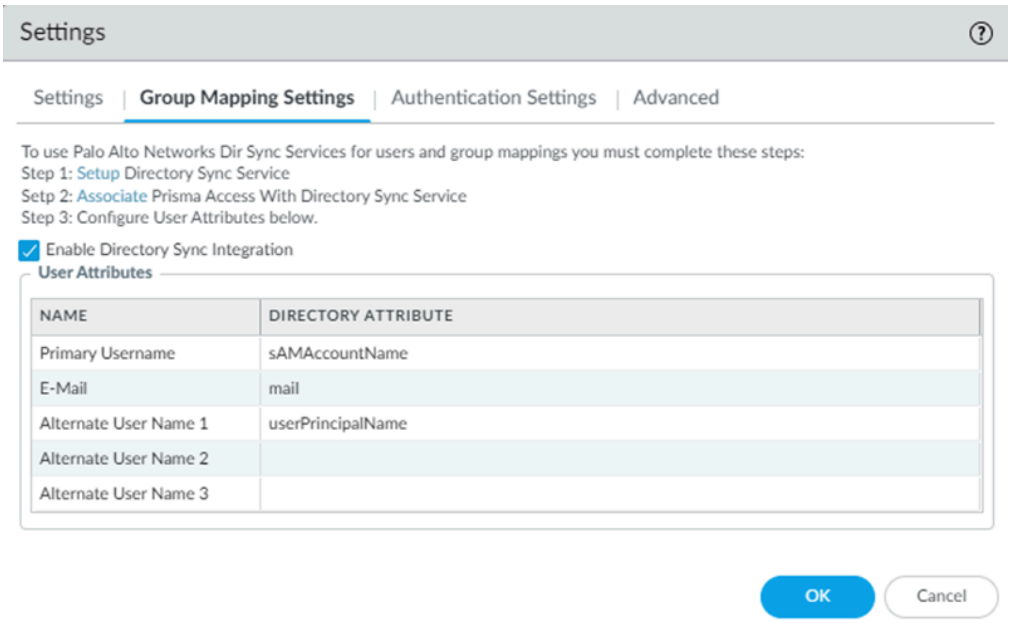
3. Dans l'onglet **Group Mapping Settings (Paramètres de mappage de groupe)**, **Enable Directory Sync Integration (Activer l'intégration de la synchronisation de répertoire)** (désormais connu sous le nom deCloud Identity Engine) pour configurer Prisma Access

©2025 Palo Alto Networks, Inc.

de façon à utiliser Cloud Identity Engine pour récupérer des informations sur les utilisateurs et les groupes.

Vous utilisez Cloud Identity Engine pour renseigner les informations de mappage des utilisateurs et des groupes pour un déploiement de proxy explicite.

Saisissez **mail (courrier)** pour l'attribut de répertoire dans le champ **Primary Username (Nom d'utilisateur principal)** et **mail (courrier)** pour le champ **E-mail (Courriel)**.



4. Sélectionnez **OK** lorsque vous avez terminé.

STEP 3 | (Facultatif) Configurez les Paramètres de blocage.

Utilisez les paramètres de blocage pour bloquer l'accès à une destination Internet à l'étape de résolution DNS.

Pour restreindre l'accès au proxy explicite à des adresses IP sources spécifiques, vous pouvez également utiliser des objets spéciaux. Ces objets d'adresse, groupes d'adresses et listes EDL externes qui utilisent des noms spécifiques autorisent les adresses IP que vous spécifiez pour le trafic Internet et bloquent toutes les autres adresses IP.

STEP 4 | Dans l'onglet **Authentication Settings (Paramètres d'authentification)**, configurez le décryptage, X-Authenticated-User (XAU) et les paramètres d'authentification.

1. Configurez vos paramètres pour le trafic déchiffré.
   - Sélectionnez **Decrypt Traffic That Matches Existing Decryption rules; For Undecrypted Traffic, Allow Traffic Only From Known IPs Registered By Authenticated Users (Déchiffrer le trafic qui correspond aux règles de déchiffrement existantes ; Pour le trafic non déchiffré, n'autorisez le trafic qu'à partir d'adresses IP**

 ©2025 Palo Alto Networks, Inc.

connues enregistrées par des utilisateurs authentifiés) pour configurer les règles de déchiffrement suivantes :

- Le trafic qui correspond aux règles de stratégie de déchiffrement que vous avez configurées avec une **Action Decrypt (Déchiffrer)** ou **Decrypt and Forward (Déchiffrer et transférer)** sera déchiffré.

  Si un utilisateur accède à un site HTTPS non déchiffré et qu'il ne s'est pas encore authentifié auprès du proxy explicite à partir de cette adresse IP, l'utilisateur est bloqué. Cependant, l'utilisateur peut accéder à un site déchiffré, effectuer l'authentification, puis accéder à des sites non déchiffrés.
- Le trafic non déchiffré est autorisé à partir d'adresses IP à partir desquelles l'utilisateur mobile s'est déjà authentifié.

Le proxy explicite nécessite un déchiffrement pour authentifier les utilisateurs. Entrez les domaines qui peuvent être déchiffrés dans une catégorie d'URL personnalisée ; spécifiez ensuite ces catégories dans **If Authentication traffic is forwarded through Explicit Proxy, specify the domains used in the authentication flow (Si le trafic d'authentification est transféré via un proxy explicite, spécifiez les domaines utilisés dans le flux d'authentification)**.

Ajoutez uniquement les domaines requis pour l'authentification à la catégorie d'URL personnalisée que vous spécifiez, y compris tous les noms de domaine complets ACS et IdP. Vous devez ajouter des URL d'authentification à la catégorie URL personnalisée, même si vous les avez ajoutées à une stratégie de déchiffrement.

- Pour autoriser le déchiffrement de tout le trafic, sélectionnez **Decrypt All traffic (Overrides Existing Decryption Rules) (Déchiffrer tout le trafic (remplace les règles de déchiffrement existantes)**.

  Si vous choisissez ce bouton radio, assurez-vous que :

  - Vous n'avez pas d'exceptions dans votre politique de déchiffrement.
  - Vous appliquez des restrictions basées sur l'adresse IP source dans votre stratégie de sécurité.

  Le non-respect de ces recommandations permet l'utilisation abusive du proxy explicite en tant que proxy ouvert qui peut être largement utilisé à mauvais escient en tant que service de transfert pour mener des attaques par déni de service.

  - Vous disposez d'au moins un certificat de proxy de transfert SSL spécifié en tant que **Forward Trust Certificate (Certificat d'approbation de transfert)**.

    Si vous n'avez pas de certificat d'approbation de transfert, créez-en un sur Panorama ; et **Commit and Push (Valider et pousser)** vos modifications à Prisma Access. Si vous ne disposez pas d'un certificat d'approbation de transfert, une erreur de validation s'affiche lorsque vous validez les modifications apportées à votre proxy explicite.

2. (Facultatif) Entrez toutes les adresses IP à partir desquelles le trafic HTTP non déchiffré ou HTTP Cross-Origin Resource Sharing (CORS) doit être autorisé pour le **Trusted**

 ©2025 Palo Alto Networks, Inc.

Source Address Auth Bypass (Contournement de l'authentification de l'adresse de source fiable).

Ajoutez les adresses IP aux objets d'adresse basés sur l'adresse IP et **Add (Ajouter)** les objets d'adresse dans le champ.

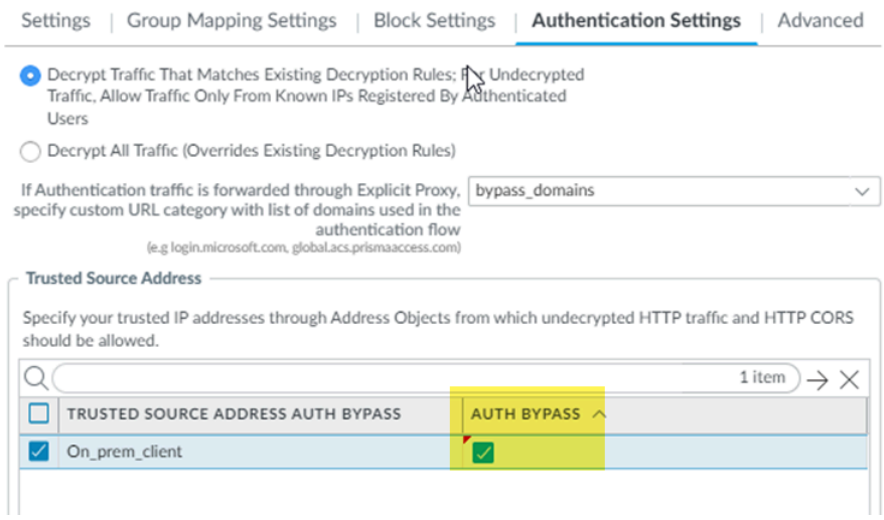
Saisissez un maximum de 100 000 adresses. Assurez-vous que l'objet d'adresse utilise uniquement des adresses IP.

3. (Facultatif) Pour contourner l'authentification de toute adresse source fiable que vous avez saisie, sélectionnez **Auth Bypass (Contournement d'authentification)**.

   Vous pouvez utiliser **Auth Bypass (Contournement d'authentification)** avec une **Source IP based visibility and enforcement (Visibilité et application basées sur l'IP source)** pour sauter l'authentification des systèmes sans tête qui ne peuvent pas authentifier, configurer des stratégies de sécurité et obtenir une visibilité du trafic sur le proxy explicite Prisma Access.

   Vous pouvez ajouter des adresses IP ou des sous-réseaux. Un maximum de 100 000 adresses IP sont prises en charge après extension des sous-réseaux.

   Si vous sélectionnez **Auth Bypass (Contournement d'authentification)** pour ignorer l'authentification pour un objet d'adresse, et que vous souhaitez ensuite activer l'authentification en désélectionnant **Auth Bypass (Contournement d'authentification)** pour cet objet d'adresse, il peut s'écouler jusqu'à 24 heures avant que la modification ne prenne effet une fois que vous avez effectué la modification et que vous avez validé et poussé vos modifications.



4. (Facultatif) Pour permettre aux adresses IP de l'adresse source fiable d'utiliser XAU pour l'identité, sélectionnez **Use X-Authenticated-User (XAU) header on incoming HTTP/**

 ©2025 Palo Alto Networks, Inc.

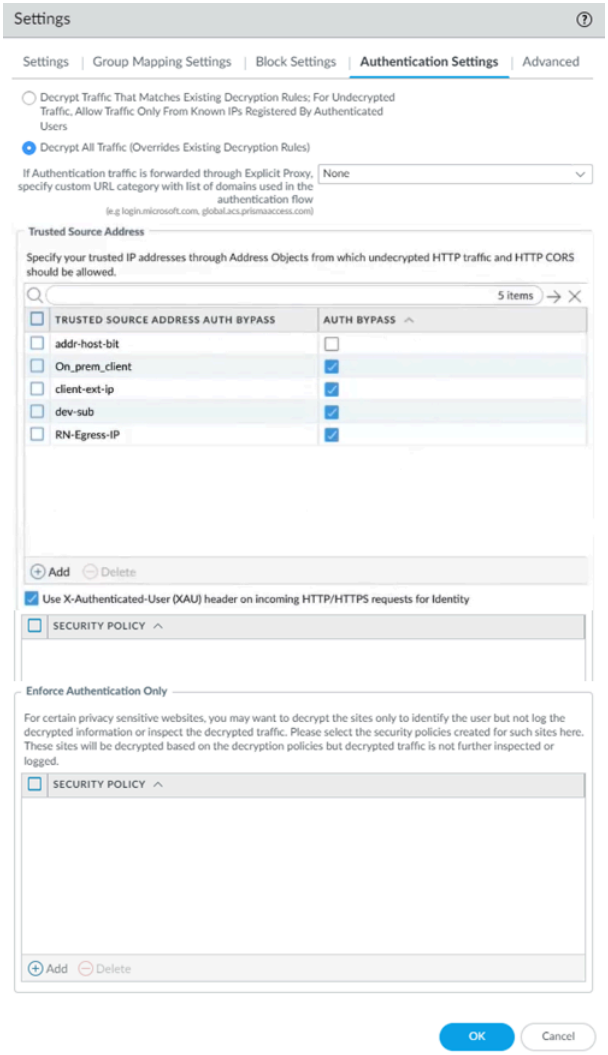
HTTPS requests for Identity (Utiliser l'en-tête X-Authenticated-User (XAU) sur les requêtes HTTP/HTTPS entrantes pour l'identité).

Sélectionnez cette option si vous utilisez le chaînage de proxy d'un proxy tiers vers un proxy explicite, si les utilisateurs se sont authentifiés dans ce proxy et si le proxy utilise des en-têtes XAU.

Les en-têtes XAU sont les seuls en-têtes HTTP pris en charge pour l'ingestion d'en-têtes de proxy explicite. Les en-têtes X-Forwarded-For (XFF) ne sont pas pris en charge.

5. (Facultatif) Spécifiez les paramètres des sites Web sensibles à la vie privée en créant des règles de politique de sécurité pour ces sites, puis en spécifiant la **Security policy (Politique de sécurité)** ou les politiques pour ces sites dans la zone **Enforce Authentication Only (Appliquer l'authentification uniquement)**.

   Pour tous les sites Web que vous spécifiez dans la **Security Policy (Politique de sécurité)** ou les politiques que vous ajoutez, le proxy explicite déchiffre les sites Web en fonction des stratégies de déchiffrement, mais n'inspecte ni n'enregistre le trafic déchiffré.



 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Facultatif) Configurez les paramètres **Advanced (Avancés)**.

1. Si vous souhaitez transférer le trafic vers le proxy explicite de vos succursales via un tunnel IPSec sécurisé, **Enable Proxy Mode (Activer le mode proxy)** et récupérez les adresses IP anycast si vous souhaitez utiliser le proxy explicite en conjonction avec un réseau distant Prisma Access.

   Cette solution utilise des adresses anycast avec un tunnel IPSec de réseau distant pour permettre l'utilisation d'un proxy explicite pour les utilisateurs et les périphériques d'un site réseau distant ou d'une succursale.
2. (Facultatif) Pour exploiter les adresses IP privées des systèmes de vos succursales qui transfèrent du trafic vers le proxy explicite, sélectionnez **Source IP based visibility and enforcement (Visibilité et application basées sur l'IP source)**.

   Cette fonctionnalité a ces exigences :

   - Un Prisma Access plan de données de minimum 10.2.4
   - Un Prisma Access (Managed by Panorama) déploiement avec un plug-in Cloud Services minimum de 4.1
   - Les adresses IP sources ne s'affichent pour les adresses IP d'un réseau distant que lorsque vous avez configuré un déploiement Réseaux distants-Proxy explicite et uniquement les adresses sources dans les emplacements des réseaux distants qui sont pris en charge avec le proxy explicite.
3. Déploiements en mode proxy uniquement Si le mode proxy est activé sur vos réseaux distants, ajoutez une stratégie pour autoriser le trafic lié à des adresses IP anycast et unicast sur des réseaux distants. Si vous avez activé **Source IP visibility and enforcement (Visibilité et application basées sur l'IP source)**, utilisez le champ **Source IP (IP Source)** dans les Stratégies de sécurité dans le proxy explicite pour sécuriser le trafic. Vous avez besoin de stratégies supplémentaires dans les réseaux distants.
4. Cliquez sur **OK**.

STEP 6 | Cliquez sur **Configure (Configurer)** pour configurer la configuration du proxy explicite.

1. Spécifiez un **Explicit Proxy FQDN (Nom de domaine complet du proxy explicite)**.

   Par défaut, le nom est *nom du proxy*.proxy.prismaaccess.com, où *nom du proxy* est le sous-domaine que vous spécifiez et utilise le port 8080. Si vous souhaitez utiliser le nom de domaine de votre organisation dans l'URL du proxy explicite (par exemple, thisproxy.proxy.mycompany.com), entrez un enregistrement CNAME pour le domaine de votre organisation.

   Par exemple, pour mapper une URL de proxy nommée thisproxy.prismaaccess.com à un proxy nommé thisproxy.proxy.mycompany.com, vous devez ajouter un CNAME de thisproxy.proxy.prismaaccess.com à l'enregistrement CNAME dans le domaine de votre organisation.
2. (Facultatif) Sélectionnez **Use GlobalProtect Agent to Authenticate (Utiliser l'agent GlobalProtect pour s'authentifier)** pour activer la fonctionnalité de proxy basée sur un agent.

   Activez cette fonctionnalité pour configurer le proxy explicite en mode proxy ou en mode tunnel et proxy. Vous devez également cocher cette case pour activer **Source IP based visibility and enforcement (Visibilité et application basées sur l'IP source)**.

 ©2025 Palo Alto Networks, Inc.

3. Spécifiez un **Authentication Profile (Profil d'authentification)** et **Cookie Lifetime (Durée de vie des cookies)**.

   - Spécifiez le SAML **Authentication profile (Profil d'authentification)** que vous avez utilisé à l'étape 1, ou ajoutez un **New (Nouveau)** profil d'authentification à utiliser avec Prisma Access.

     Vous devez configurer l'authentification SAML, y compris la configuration d'un **SAML Identity Provider (Fournisseur d'identité SAML)** (IdP) et un **Authentication profile (Profil d'authentification)**, pour utiliser un proxy explicite.

   - (Facultatif) Spécifiez une **Cookie Lifetime (Durée de vie des cookies)** pour le cookie qui stocke les identifiants d'authentification des utilisateurs.

     Prisma Access met en cache les identifiants de l'utilisateur et les stocke sous la forme d'un cookie. Pour modifier la valeur, spécifiez la durée à utiliser en secondes, minutes, heures ou jours.

     Pour éviter les problèmes empêchant les utilisateurs de télécharger des fichiers volumineux avant l'expiration de la durée de vie du cookie, ou l'expiration du cookie lorsque les utilisateurs accèdent à un seul site web pendant une longue période, Palo Alto Networks vous recommande de configurer une Durée de vie de cookie d'au moins un jour. Si les utilisateurs du proxy explicite rencontrent un problème d'expiration de la durée de vie des cookies, ils peuvent accéder à un autre site Web pour s'authentifier à nouveau auprès d'ACS et actualiser le cookie ACS.

     Si vous téléchargez un fichier et que le téléchargement du fichier prend plus de temps que la **Cookie Lifetime (Durée de vie des cookies)**, le téléchargement du fichier s'arrêtera à l'expiration de la durée de vie. Pour cette raison, envisagez d'utiliser une plus longue **Cookie Lifetime (Durée de vie des cookies)** si vous téléchargez des fichiers volumineux dont le téléchargement prend beaucoup de temps.

STEP 7 | Sélectionnez **Locations (Emplacements)** et les régions associées à ces emplacements où vous souhaitez déployer votre proxy explicite pour les utilisateurs mobiles. Prisma Access ajoute un nœud proxy à chaque emplacement que vous sélectionnez.

Le proxy explicite prend en charge un sous-ensemble de tous les emplacements Prisma Access. Voir Directives de configuration du proxy explicite pour la liste des emplacements.

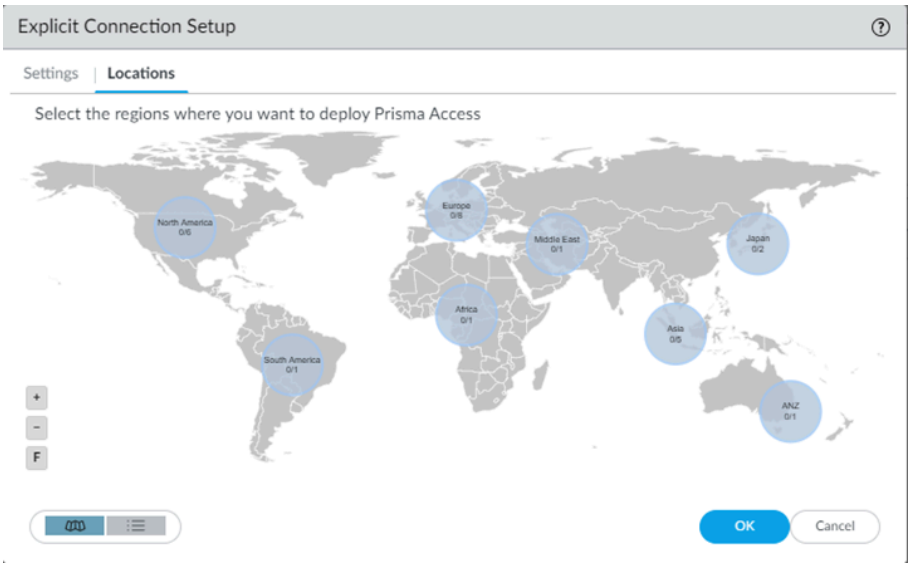
L'onglet **Locations (Emplacements)** affiche une carte. La mise en surbrillance de la carte affiche les régions du monde (Amériques, Europe et Asie-Pacifique) et les emplacements disponibles

 ©2025 Palo Alto Networks, Inc.

dans chaque région. Sélectionnez une région, puis les emplacements que vous souhaitez déployer dans chaque région.

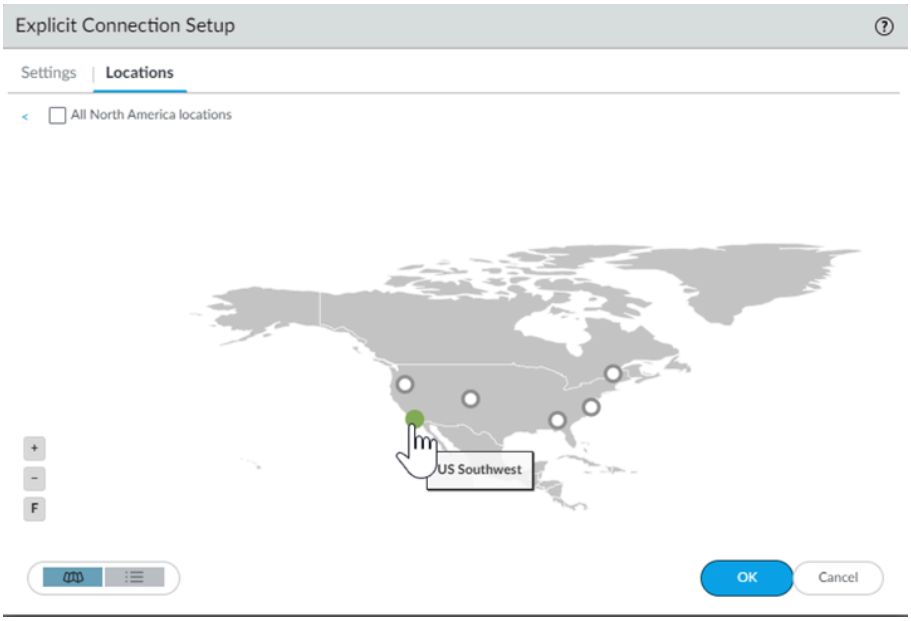
Vous devez activer les emplacements de proxy explicite dans au moins deux régions pour garantir la redondance régionale.

1. Cliquez sur l'icône **Locations (Emplacements)** et sélectionnez une région.



2. Sélectionnez un ou plusieurs emplacements de proxy explicite dans la région sélectionnée à l'aide de la carte.

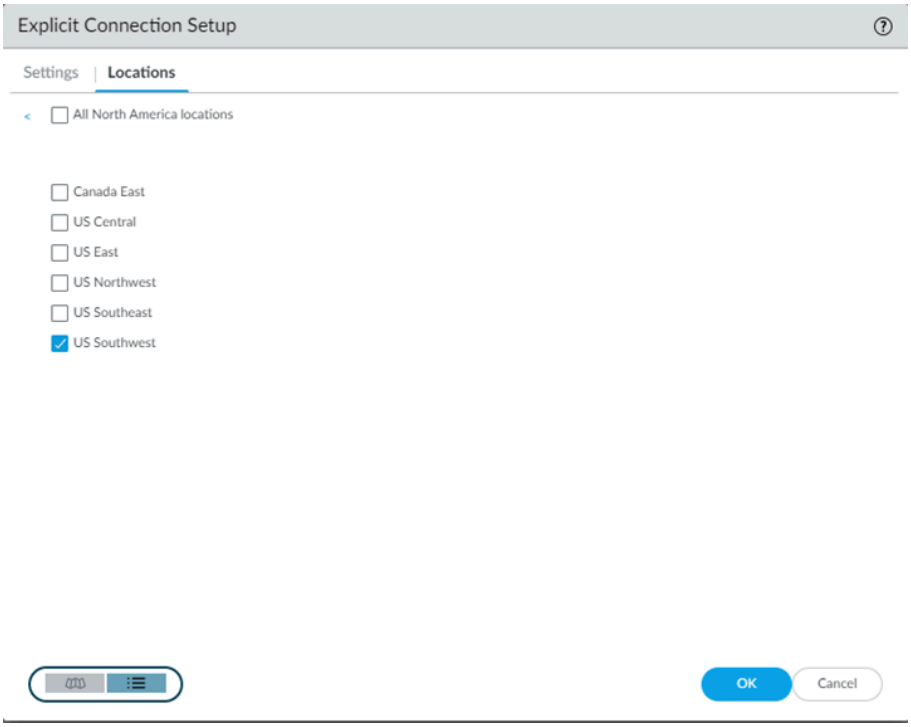
   Passez votre curseur sur un emplacement pour le mettre en surbrillance. Les cercles blancs indiquent un emplacement disponible ; Les cercles verts indiquent que vous avez sélectionné cet emplacement.



   En plus de la vue cartographique, vous pouvez afficher une liste des régions et des emplacements. Choisissez entre la vue carte et la vue liste dans le coin inférieur gauche.

 ©2025 Palo Alto Networks, Inc.

Dans la vue liste, la liste affiche les régions triées par colonnes, tous les emplacements étant triés par région. Vous pouvez sélectionner **All (Tous)** les sites d'une région (en haut de la boîte de dialogue).



3. Cliquez sur **OK** pour ajouter les emplacements.

STEP 8 | Configurez des règles de stratégie de sécurité pour appliquer les stratégies de sécurité de votre organisation.

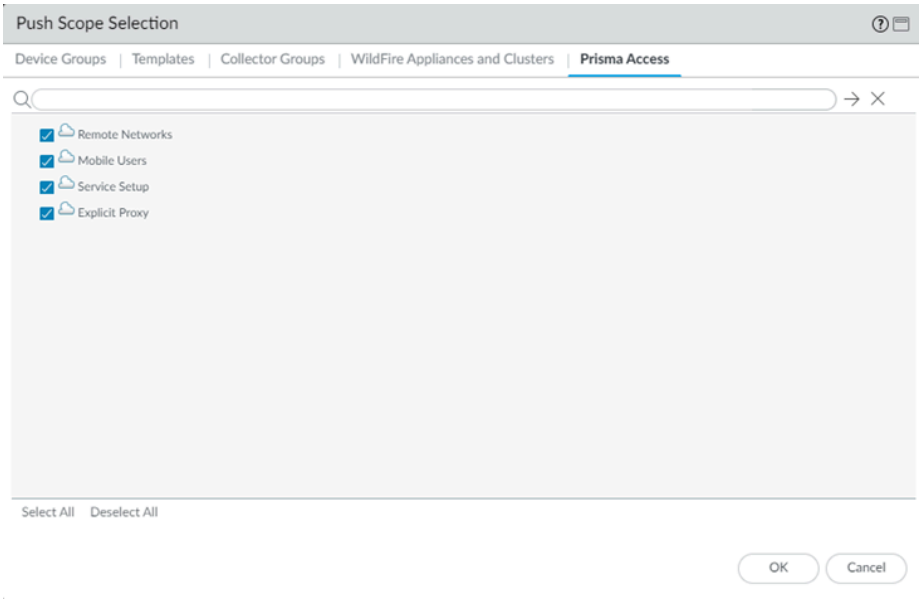
Pour apporter les modifications de configuration requises et contrôler les URL auxquelles les utilisateurs mobiles peuvent accéder à partir du proxy explicite, utilisez des stratégies de sécurité. Utilisez les instructions et exigences suivantes lors de la configuration de vos stratégies de sécurité :

- En fonction de vos objectifs commerciaux, créez des stratégies de sécurité pour les applications Internet et SaaS approuvées à l'aide d'App-ID et les groupes d'utilisateurs qui ont besoin d'accéder à ces applications.
- Associez des profils de sécurité à toutes les règles de stratégie de sécurité afin de prévenir les menaces connues et inconnues suivant les bonnes pratiques en matière de profil de sécurité.

 ©2025 Palo Alto Networks, Inc.

STEP 9 | Validez vos modifications sur Panorama et appliquez les modifications de configuration à Prisma Access.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**.
2. **Edit Selections (Modifier les sélections)** et, dans l'onglet **Prisma Access**, assurez-vous que **Explicit Proxy (Proxy explicite)** est sélectionné dans **Push Scope (Étendue de la transmission)**, puis cliquez sur **OK**.



3. Cliquez sur **Commit and Push (Valider et appliquer)**.

STEP 10 | Sélectionnez le fichier PAC à utiliser avec le proxy explicite.

1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users (Utilisateurs mobiles)** > **Explicit Proxy (Proxy explicite)**.

   Assurez-vous d'entrer un port de 8080 dans le fichier PAC.
2. Sélectionnez **Connection Name (Nom de la connexion)** pour la configuration du proxy explicite que vous venez de configurer.
3. Entrez le **PAC (Proxy Auto-Configuration) File (Fichier PAC (Proxy Auto-Configuration))** à utiliser pour le proxy explicite.

   Assurez-vous de comprendre comment fonctionnent les fichiers PAC et comment les modifier avant de les télécharger sur Prisma Access.



   Browse (Parcourir) et téléchargez le fichier.

   Prisma Access vous fournit un exemple de fichier PAC ; vous pouvez **Download sample PAC file (Télécharger un exemple de fichier PAC)**, modifier les valeurs et télécharger ce fichier. Voir Configurer votre fichier PAC proxy explicite pour les exigences et les directives du fichier PAC comme une description du contenu de l'exemple de fichier PAC.

 ©2025 Palo Alto Networks, Inc.

Authentification Kerberos pour les déploiements de proxy explicite

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Les déploiements Utilisateurs mobiles – Proxy explicite de Prisma Access prennent en charge l'authentification Kerberos. Si vous avez des serveurs, des périphériques IoT ou des machines sans périphérique de contrôle qui ne peuvent pas s'authentifier avec SAML, vous pouvez utiliser l'authentification Kerberos à la place.

Si votre déploiement utilise à la fois SAML et Kerberos pour l'authentification, vous pouvez configurer les deux types d'authentification dans un seul déploiement de proxy explicite. De cette manière, vous pouvez authentifier les utilisateurs mobiles avec SAML tout en authentifiant les serveurs, les appareils IoT ou les machines sans périphérique de contrôle avec Kerberos. Le proxy explicite Prisma Access traite l'authentification en fonction du port utilisé pour le trafic d'authentification :

- Si le trafic d'authentification utilise le port 8080, le proxy explicite utilise l'authentification SAML.
- Si le trafic d'authentification utilise le port 8081, le proxy explicite utilise l'authentification Kerberos.

Si un seul port est configuré, le port qui n'est pas configuré utilise le même profil d'authentification que le port configuré.

La SSO Kerberos n'est disponible que pour les terminaux et les systèmes ayant accès à votre infrastructure Kerberos. Les terminaux et les systèmes qui n'ont pas accès à l'infrastructure Kerberos doivent utiliser la SSO SAML.

- Configuration requise et recommandations pour le déploiement de Kerberos pour les déploiements de proxy explicites
- Créer un fichier keytab Kerberos
- Configurer l'authentification Kerberos pour les déploiements de proxy explicite

Configuration requise et recommandations pour le déploiement de Kerberos pour les déploiements de proxy explicites

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Licence Prisma Access ☐ Version du plan de données requis minimum : PAN-OS 10.1.3 ou versions ultérieures

©2025 Palo Alto Networks, Inc.

Avant de créer un keytab Kerberos pour implémenter Kerberos dans un déploiement de proxy explicite, assurez-vous que votre déploiement Kerberos présente les exigences et conditions préalables suivantes :

- Mettez à jour votre plan de données vers PAN-OS 10.1.3 ou versions ultérieures.
- Assurez-vous de disposer d'un compte Kerberos que vous pouvez utiliser pour permettre à Prisma Access d'authentifier des serveurs ou des périphériques.

  Un compte est nécessaire pour créer un keytab Kerberos qui est un fichier contenant le nom principal et le mot de passe Kerberos chiffré.
- Assurez-vous que les serveurs et les points de terminaison sont joints à un domaine, ce qui permet aux utilisateurs et aux machines de se connecter en toute sécurité à leur domaine de travail à l'aide de leurs informations d'identification du réseau de travail.
- Veillez à transférer le trafic d'authentification Kerberos vers le port 8081 dans le fichier PAC des utilisateurs mobiles ou dans vos paramètres de proxy sur le point de terminaison ou les serveurs.

  Le proxy explicite utilise le port 8081 pour l'authentification Kerberos et le port 8080 pour l'authentification SAML.
- Assurez-vous que votre administrateur Kerberos est en mesure de créer et d'exporter des fichiers keytab.
- Assurez-vous que vous disposez des adresses IP de sortie de la succursale ou du campus où se trouvent vos serveurs, vos périphériques IoT ou vos machines sans tête.

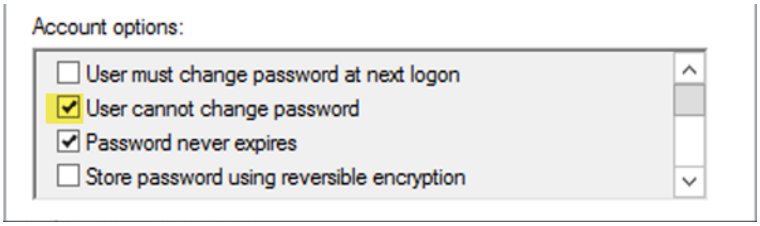
  Vous ajoutez ces adresses IP à la liste des adresses approuvées par le proxy explicite.
- Suivez les bonnes pratiques en matière d'authentification et de création d'utilisateurs Kerberos.

  Il est de la responsabilité de l'administrateur de compte Kerberos de suivre les meilleures pratiques pour protéger son environnement Kerberos et empêcher la compromission des mots de passe. Utilisez les bonnes pratiques suivantes lors de la création des comptes d'utilisateur, du mot de passe et des ServicePrincipalNames (SPN).

  Bonnes pratiques de création de compte d'utilisateur Kerberos :

  - Ne réutilisez pas les comptes d'utilisateur administrateur.

    Créez un nom de compte unique pour le compte Kerberos à utiliser avec lePrisma Access proxy explicite.
  - Ne partagez pas ce compte avec un autre service ; utilisez un compte d'utilisateur dédié pour le Prisma Access proxy explicite.
  - Assurez-vous que l'utilisateur ne peut pas modifier le mot de passe du compte Kerberos.

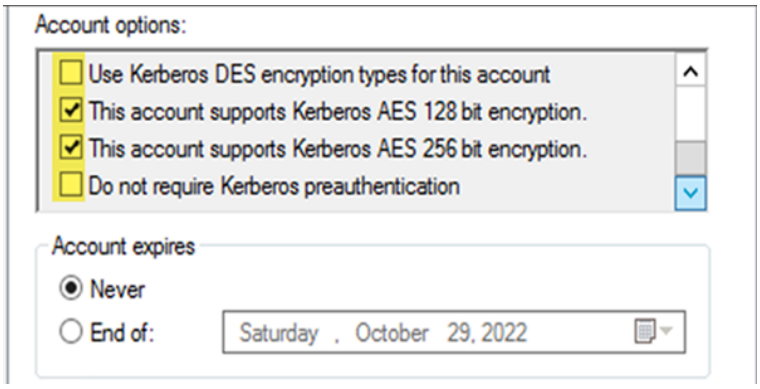
    

  - Lorsque vous sélectionnez les options du compte Kerberos, désélectionnez **Use Kerberos DES encryption types for this account (Utiliser les types de chiffrement Kerberos DES**

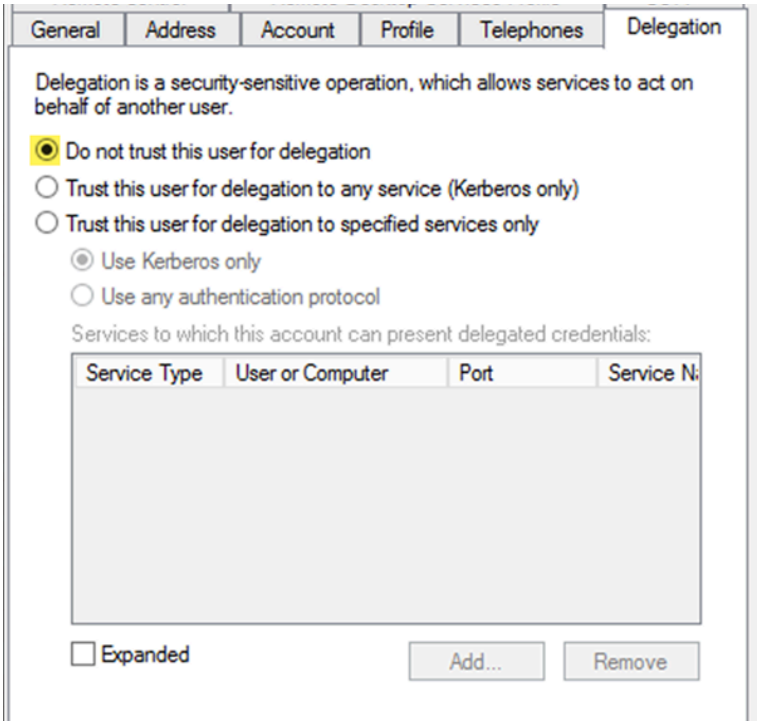
 ©2025 Palo Alto Networks, Inc.

pour ce compte) et **Do not require Kerberos preauthentication (N'exige pas de pré-authentification Kerberos)**.

- Activer le chiffrement AES-128 et AES-256 bits.

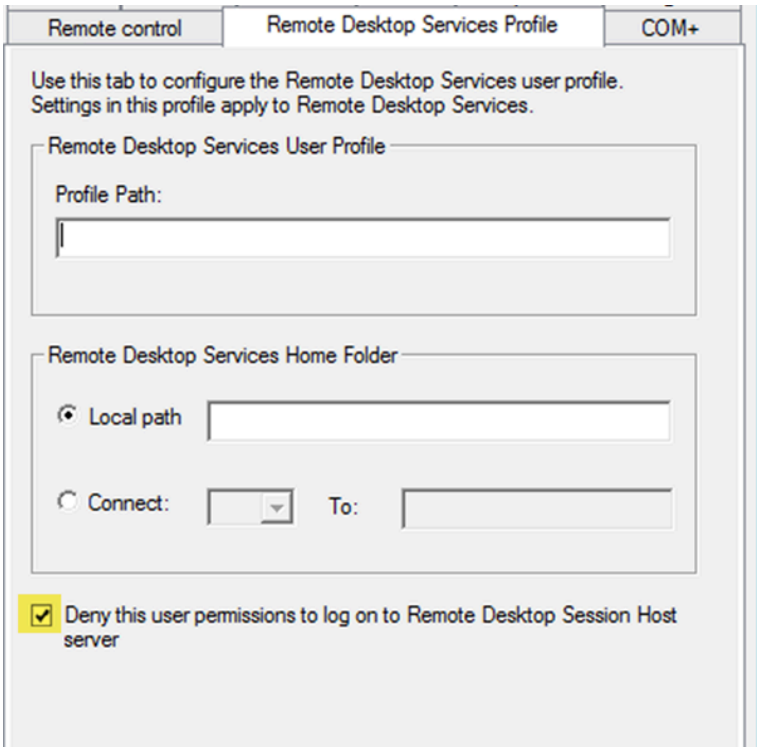


- Désactiver la délégation pour les utilisateurs.

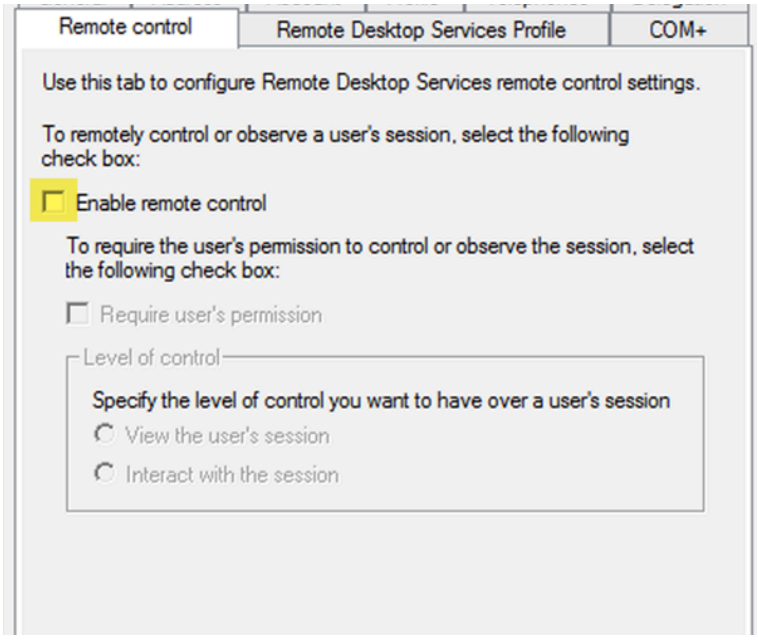


- Refuser la possibilité de se connecter à une session de bureau à distance.

 ©2025 Palo Alto Networks, Inc.

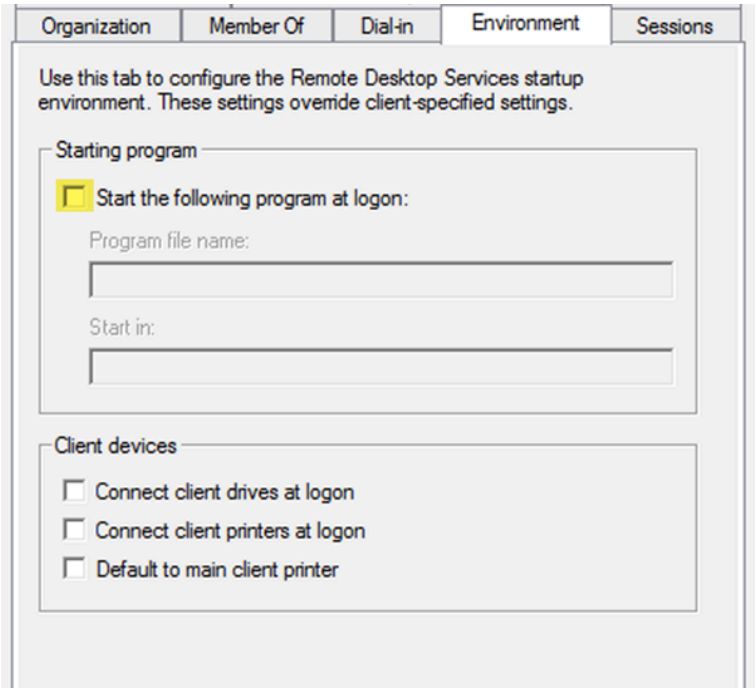


- Ne pas activer la commande à distance.



- Ne pas autoriser les utilisateurs à démarrer des programmes à l'ouverture de session.

 ©2025 Palo Alto Networks, Inc.



- Vous pouvez spécifier des utilisateurs ou des groupes d'utilisateurs dans la liste d'autorisation du profil d'authentification que vous créez afin de limiter l'authentification aux seuls utilisateurs ou machines qui ont des besoins professionnels légitimes.

Bonnes pratiques SPN et Keytab :

- Assurez-vous que le SPN n'est pas associé à plusieurs comptes d'utilisateur, ce qui pourrait entraîner des échecs de SPN en double.
- RC4-HMAC-NT utilise un hachage NTML faible. Suivez les stratégies et directives de sécurité de votre organisation pour inclure ou exclure le chiffrement RC5.
- Les chiffrements DES-CBC-CRC et DES-CBC-MD5 sont obsolètes et ne sont pas pris en charge par Prisma Access.
- Effectuez régulièrement une rotation du mot de passe du SPN. Suivez les stratégies de sécurité et les directives de votre organisation en matière de rotation des mots de passe.
- Suivez les pratiques de votre organisation en matière de complexité des mots de passe (par exemple, créez les mots de passe SPN d'une manière vraiment aléatoire qui ne peut pas être lue ou devinée par l'homme).
- Si vous modifiez le mot de passe de l'utilisateur du service ou tout autre attribut, mettez à jour et générez à nouveau le nouveau keytab et téléchargez-le dans Prisma Access.
- Si vous intégrez une nouvelle région PA, vous devez générer un nouveau keytab pour cette région, comme indiqué dans les étapes suivantes.

L'exemple suivant montre un compte créé à l'aide des meilleures pratiques Kerberos.

```
PS C:\Users\Administrator> Get-ADUser example -Properties "*"
 AccountNotDelegated : True AllowReversiblePasswordEncryption :
 False CannotChangePassword : True CN : example Deleted :
 DoesNotRequirePreAuth : False Enabled : True GivenName :
 PrismaAccess EP Service User KerberosEncryptionType :
```

 ©2025 Palo Alto Networks, Inc.

```
 {AES128, AES256} msDS-SupportedEncryptionTypes : 24 Name :
 example PasswordExpired : False PasswordNeverExpires : True
 PasswordNotRequired : false PrincipalsAllowedToDelegateToAccount :
 {} ProtectedFromAccidentalDeletion : True SamAccountName :
 example servicePrincipalName : {HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM, HTTP/us-east-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM, HTTP/us-south-1.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM} ServicePrincipalNames :
 {HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM,
 HTTP/us-east-2.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM,
 HTTP/us-south-1.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM}
 SmartcardLogonRequired : False TrustedForDelegation :
 False TrustedToAuthForDelegation : False UseDESKeyOnly :
 False UserPrincipalName : HTTP/us-south-1.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM
```

Créer un fichier keytab Kerberos

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access ❑ Version minimale requise du plan de données : PAN-OS 10.1.3 ou versions ultérieures

Après avoir examiné les exigences et recommandations pour le déploiement de Kerberos pour le proxy explicite, vous êtes prêt à créer un fichier keytab Kerberos.

Pour des performances optimales, la taille du fichier keytab doit être inférieure à 60 Ko.

STEP 1 | Configurez le déploiement de votre proxy explicite.

STEP 2 | Obtenez le FQDN, les FQDN du proxy et les CNAME DNS requis pour configurer votre authentification Kerberos.

L'authentification Kerberos utilise les informations extraites du Prisma Accessscript API pour créer et configurer les fichiers keytab Kerberos. Le script API récupère les informations suivantes :

- **ep_geo_lb_fqdn** : le FQDN DNS du proxy explicite utilisé dans la configuration de l'équilibreur de charge réseau du proxy explicite. Ce nom de domaine complet est identique à **Explicit Proxy URL (URL du proxy explicite)** du proxy explicite dans l'interface utilisateur Prisma Access sous **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Infrastructure Settings (Paramètres d'infrastructure)** > **Explicit Proxy URL (URL du proxy explicite)**.
- **ep_geo_lb_cname** : CNAME DNS pour le locataire du proxy explicite.
- **ep_regional_fqdn** : les FQDN utilisés pour les emplacements de proxy explicite intégrés.

  Le proxy explicite attribue à chaque emplacement une adresse IP publique pour l'équilibreur de charge réseau ; « ep_regional_fqdn » est le FQDN associé à cette adresse IP. Si plusieurs

 ©2025 Palo Alto Networks, Inc.

emplacements partagent la même adresse IP publique, ces emplacements utilisent le même FQDN régional.

1. Générez une clé API à utiliser dans le cadre d'une commande curl.
   - Sur Prisma Access (Managed by Strata Cloud Manager), sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Paramètres d'infrastructure)** > **Generate New API Key (Générer une nouvelle clé API)**.
   - Sur Panorama Managed Prisma Access, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** > **Generate API Key (Générer une clé API)**
2. Créez un fichier .txt et entrez les options de commande suivantes dans le fichier :

   ```
   { "serviceType": "swg_proxy", "location": "deployed",
    "addrType": "network_load_balancer" }
   ```

3. Entrez la commande suivante pour récupérer les FQDN requis pour utiliser l'authentification Kerberos :

   ```
   curl -X POST --data @option.txt -H header-api-key:Current-
   API-Key "https://api.prod.datapath.prismaaccess.com/
   getPrismaAccessIP/v2"
   ```

   Où `option.txt` est le fichier .txt que vous avez créé lors d'une étape précédente et `Current-API-Key` est la clé API de Prisma Access.
4. Notez les FQDN.

   Il y en a au moins un **ep_geo_lb_fqdn**, un **ep_geo_lb_cname** et un **ep_regional_fqdn** par emplacement intégré.

STEP 3 | Créez un nouvel utilisateur pour Prisma Access dans l'Active Directory (AD) de votre organisation en entrant la commande suivante :

```
New-ADUser -Name "USER_NAME" -GivenName "USER_GIVEN_NAME"
 -SamAccountName "USER_SAMACCOUNTNAME" -UserPrincipalName
 "USER_NAME@DNS_DOMAIN_NAME" -Path "X_500_PATH" –AccountPassword
```

 ©2025 Palo Alto Networks, Inc.

```
(ConvertTo-SecureString “PASSWORD” -AsPlainText -force) -Enabled
$true -KerberosEncryptionType RC4,AES128,AES256
```

Où :

- *USER_NAME* est le nom de l’objet utilisateur.
- *USER_GIVEN_NAME* est le prénom de l’utilisateur.
- *USER_SAMACCOUNTNAME* est le nom du responsable de compte de sécurité (SAM) de l’utilisateur.
- *USER_NAME@DNS_DOMAIN_NAME* est le nom d’utilisateur principal (UPN) de l’utilisateur.
- *X_500_PATH* est le chemin X.500 de l’UO ou du conteneur dans lequel le nouvel objet est créé (par exemple, `DC=EXAMPLE,DC=COM`.)
- *PASSWORD* est le mot de passe à utiliser pour le compte.

L’exemple CLI suivant a un nom d’utilisateur `example`, un nom SAM `example`, un prénom `PrismaAccess EP Service User`, un UPN `example@exmp.com`, un chemin d’accès `DC=EXMP,DC=COM`, et un mot de passe Ex@mple123:

```
New-ADUser -Name "example" -GivenName "PrismaAccess EP
 Service User" -SamAccountName "example" -UserPrincipalName
 "example@exmp.com" -Path "DC=EXMP,DC=COM" –AccountPassword
 (ConvertTo-SecureString “Ex@mple123” -AsPlainText -force) -Enabled
 $true -KerberosEncryptionType RC4,AES128,AES256
```

La commande précédente spécifie un type de chiffrement RC4, qui utilise un hachage NTLM faible. Suivez les politiques et directives de sécurité de votre organisation pour inclure ou exclure RC4 dans cette commande.

STEP 4 | Entrez la commande suivante pour empêcher l’expiration du mot de passe et pour empêcher sa modification :

```
Get-ADUser USER_NAME|Set-ADUser -PasswordNeverExpires:$True -
CannotChangePassword:$true
```

Suivez les politiques de sécurité et les directives de votre organisation en matière d’expiration et de rotation des mots de passe.

STEP 5 | Entrez la commande suivante pour afficher le compte utilisateur nouvellement créé :

```
Get-ADUser USER_NAME -property msDS-KeyVersionNumber
```

STEP 6 | Associez les SPN et exportez les fichiers keytab à utiliser avec l’authentification Kerberos dans votre Windows AD.

Un fichier keytab permet au proxy explicite de valider les jetons d’authentification Kerberos fournis pendant les flux de trafic à partir d’utilisateurs, de serveurs, de périphériques IoT ou d’autres systèmes sans tête. Lors de la création du fichier keytab, le proxy explicite exige que les valeurs que vous avez récupérées à l’aide de l’API lors d’une étape précédente soient

 ©2025 Palo Alto Networks, Inc.

associées en tant que ServicePrincipalNames (SPN) au compte utilisateur que vous avez créé au cours de l'étape suivante.

Utilisez les valeurs **ep_geo_lb_fqdn**, **ep_geo_lb_cname** et **ep_regional_fqdn**. Ces valeurs permettent au proxy explicite d'authentifier les flux de trafic vers l'un de ces domaines proxy.

1. Générez et exportez un fichier keytab à l'aide de la valeur **ep_geo_lb_fqdn** comme nom de principal de service (SPN) en entrant les commandes suivantes :

   ```
   ktpass -princ HTTP/ep_geo_lb_fqdn@REALM -
   mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
    -pass PASSWORD -out KEYTAB_NAME_1.keytab
   ```

   Où :

   - *ep_geo_lb_fqdn* est la valeur **ep_geo_lb_fqdn** renvoyée par le script de l'API du proxy explicite.
   - *REALM* est le realm (par exemple, EXMP.COM).

     Dans la plupart des cas, vous entrez realm à l'aide de lettres majuscules.
   - *DOMAIN\USER_NAME* est le nom d'ouverture de session au niveau du domaine (par exemple, EXMP\example).
   - *PASSWORD* est le mot de passe à utiliser pour le fichier keytab. Ce mot de passe n'a pas besoin de correspondre au mot de passe de l'utilisateur, mais doit correspondre à la valeur que vous créez pour les SPN **ep_geo_lb_cname** et **ep_regional_fqdn** dans les étapes suivantes.
   - *KEYTAB_NAME_1* est le nom du fichier keytab. Le nom du fichier keytab doit être unique à ce SPN.

   Veillez à suivre les meilleures pratiques de création de SPN et de mots de passe.

   L'exemple CLI suivant comporte un *ep_geo_lb_fqdn* example.proxy.prismaaccess.com, un *REALM* EXMP.COM, un

 ©2025 Palo Alto Networks, Inc.

DOMAIN\USER_NAME EXMP\example*un PASSWORD* Ex@mple123, et un nom de fichier keytab exporté exmp1.keytab :

```
ktpass -princ HTTP/example.proxy.prismaaccess.com@EXMP.COM -
mapuser EXMP\example -ptype KRB5_NT_PRINCIPAL -crypto all -
pass Ex@mple123 -out exmp1.keytab
```

2. Générez et exportez un fichier keytab à l'aide de la valeur **ep_geo_lb_cname** comme SPN en entrant les commandes suivantes :

```
ktpass -princ HTTP/ep_geo_lb_cname@REALM -
mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
 -pass PASSWORD -out KEYTAB_NAME_2.keytab
```

Où :

- *ep_geo_lb_cname* est la valeur **ep_geo_lb_cname** renvoyée par le script de l'API du proxy explicite.
- *REALM* est le realm par exemple, EXMP.COM
- *DOMAIN\USER_NAME* est le nom d'ouverture de session au niveau du domaine (par exemple, EXMP\example).
- *PASSWORD* est le mot de passe à utiliser pour le fichier keytab. Ce mot de passe doit correspondre aux mots de passe SPN **ep_geo_lb_fqdn** et **ep_regional_fqdn**.
- *KEYTAB_NAME_2* est le nom du fichier keytab que vous souhaitez exporter. Ce nom doit être différent des autres noms de fichier keytab SPN que vous créez.

L'exemple CLI suivant comporte un *ep_geo_lb_cname* prisma-abcde12345.proxy.prismaaccess.com, un *REALM* EXMP.COM, un *DOMAIN\USER_NAME* EXMP\example, un *PASSWORD* Ex@mple123 et un nom de fichier keytab exporté exmp2.keytab :

```
ktpass -princ HTTP/prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
```

 ©2025 Palo Alto Networks, Inc.

```
\example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
 -out exmp2.keytab
```

3. Générez et exportez un fichier keytab à l'aide de la valeur **ep_regional_fqdn** comme SPN en entrant les commandes suivantes :

   ```
   ktpass -princ HTTP/ep_regional_fqdn@REALM -
   mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
    -pass PASSWORD -out KEYTAB_NAME_3.keytab
   ```

   Où :

   - *ep_regional_fqdn* est la valeur **ep_regional_fqdn** renvoyée par le script de l'API du proxy explicite.
   - *REALM* est le realm (par exemple, `EXMP.COM`).
   - *DOMAIN\USER_NAME* est le nom d'ouverture de session au niveau du domaine (par exemple, `EXMP\example`).
   - *PASSWORD* est le mot de passe à utiliser pour le fichier keytab. Ce mot de passe doit correspondre aux mots de passe SPN **ep_geo_lb_fqdn** et **ep_geo_lb_cname**.
   - *KEYTAB_NAME_3* est le nom du fichier keytab que vous souhaitez exporter. Ce nom doit être différent des autres noms de fichier keytab SPN que vous créez.

   L'exemple CLI suivant comporte un *ep_regional_fqdn* `prisma-abcde12345.proxy.prismaaccess.com`, un *REALM* `EXMP.COM`, un *DOMAIN\USER_NAME* `EXMP\example`, un *PASSWORD* `Ex@mple123` et un nom de fichier keytab exporté `exmp3.keytab` :

   ```
   ktpass -princ HTTP/us-west-2.prisma-
   abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
   \example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
    -out exmp3.keytab
   ```

4. (Facultatif) Si vous avez d'autres emplacements qui utilisent différentes valeurs **ep_regional_fqdn** et que vous souhaitez créer des fichiers keytab pour ces emplacements, générez et exportez un ou plusieurs fichiers keytab supplémentaires en répétant l'étape 6.c, à l'aide de la valeur **ep_regional_fqdn** pour ces emplacements.

   Créez un nom de fichier keytab unique pour chaque **ep_regional_fqdn**. Par exemple, si la valeur **ep_regional_fqdn** pour un autre emplacement est `us-east-2.prisma-abcde12345.proxy.prismaaccess.com`, entrez l'exemple CLI suivant avec un nom de fichier keytab exporté unique :

   ```
   ktpass -princ HTTP/us-east-2.prisma-
   abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
   \example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
    -out exmp4.keytab
   ```

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Supprimez les chiffrements non pris en charge dans les fichiers keytab créés en saisissant les commandes `ktutil` suivantes dans Ubuntu.

La sortie système suivante fournit des exemples de nettoyage de divers chiffrements :

```
slot KVNO Principal ---- ----
 ---------------------------------------------------------------------
 1 3 HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@PANW.COM (des-cbc-crc) 2 3
 HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@PANW.COM
 (des-cbc-md5) 3 3 HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@PANW.COM (arcfour-hmac) 4 3
 HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@PANW.COM
 (aes256-cts-hmac-sha1-96) 5 3 HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@PANW.COM (aes128-cts-hmac-
sha1-96)
```

```
# display all keytabs, get the key entry numbers to remove DES-
CBC-MD5 and DES-CBC-CRC. # Also, enable or disable RC4-HMAC based
 on your organization's policy. for i in `ls keytab_name*.keytab`;
 do echo $i; klist -Kte -k $i; done # cleanup unsupported
 ciphers # entry #1 is typically des-cbc-crc # entry #2 is
 typically des-cbc-md5 # entry #3 is typically arcfour-hmac ktutil
 rkt KEYTAB_NAME_1.keytab delent 2 delent 1 wkt new1.keytab quit
 ktutil rkt KEYTAB_NAME_2.keytab delent 2 delent 1 wkt new2.keytab
 quit ktutil rkt KEYTAB_NAME_3.keytab delent 2 delent 1 wkt
 new3.keytab quit
```

Où les fichiers *KEYTAB_NAME_1*.keytab, *KEYTAB_NAME_2*.keytab et *KEYTAB_NAME_3*.keytab sont les fichiers keytab que vous avez créés à l'étape précédente.

STEP 8 | (Facultatif) Si vous avez créé d'autres fichiers keytab pour d'autres régions, supprimez les chiffrements non pris en charge sur ces fichiers keytab en entrant la commande `ktutil` précédente, en substituant *KEYTAB_NAME_1*.keytab avec le nom du fichier keytab que vous avez utilisé pour la ou les régions et en spécifiant un fichier de sortie différent (par exemple, `new4.keytab`, `new5.keytab`, et ainsi de suite).

STEP 9 | Fusionnez les fichiers keytab que vous avez créés en saisissant la commande `ktutil` suivante, où new1.keytab, new2.keytab et new3.keytab sont les fichiers keytab que vous avez créés à l'étape précédente, assurez-vous d'inclure tous les fichiers keytab spécifiques à la région dans cette commande :

```
ktutil rkt new1.keytab rkt new2.keytab rkt new3.keytab # if you
 created any additional region-specific keytab files, add them
 here. wkt papxv1.keytab quit
```

Une fois l'opération terminée, utilisez le fichier keytab que vous avez créé (`papxv1.keytab` dans cet exemple) comme fichier keytab à utiliser avec le proxy explicite.

 ©2025 Palo Alto Networks, Inc.

Configurer l'authentification Kerberos pour les déploiements de proxy explicite

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

- Strata Cloud Manager
- Panorama

Configurer l'authentification Kerberos pour les déploiements de proxy explicite (Strata Cloud Manager)

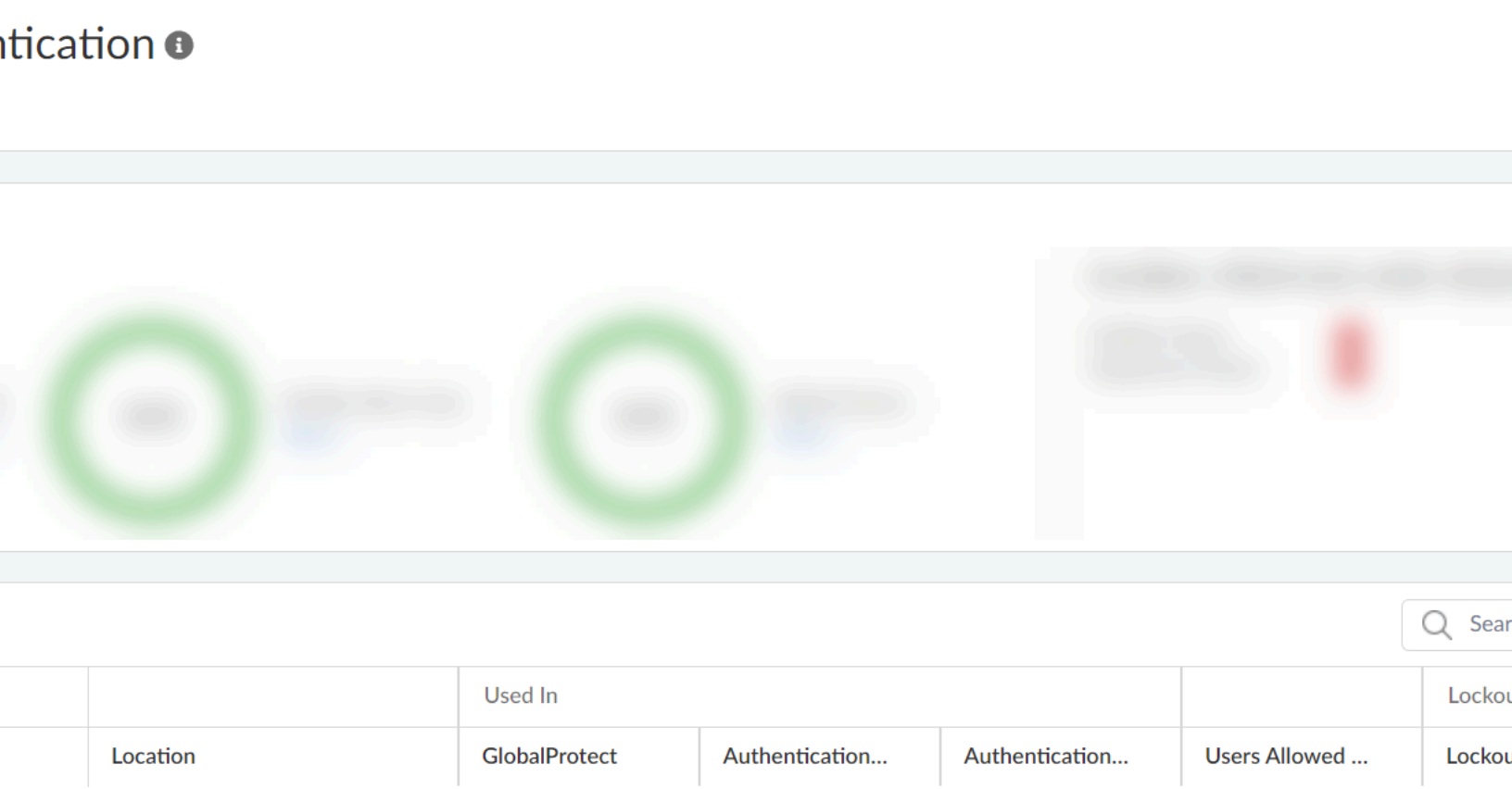
STEP 1 | Configurez un profil d'authentification Kerberos.

Le profil définit la façon dont le proxy explicite se connecte au serveur Kerberos pour l'authentification des utilisateurs mobiles.

1. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Authentication**

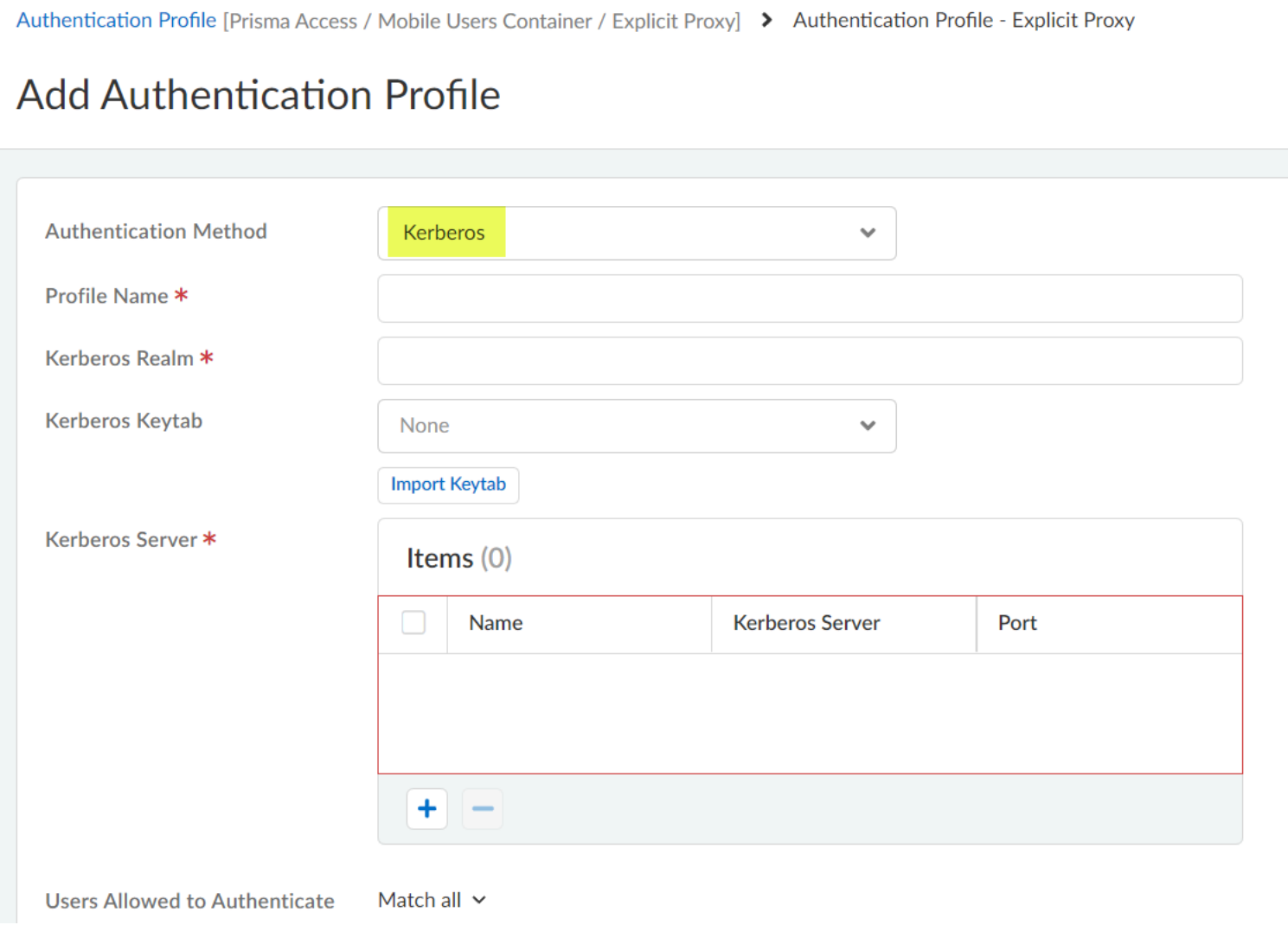
 ©2025 Palo Alto Networks, Inc.

(Authentication) > **Authentication Profiles (Profils d'authentification)** et **Add Profile (Ajouter un profil)**.



2. Sélectionnez **Authentication Method (Méthode d'authentification)** : **Kerberos**.

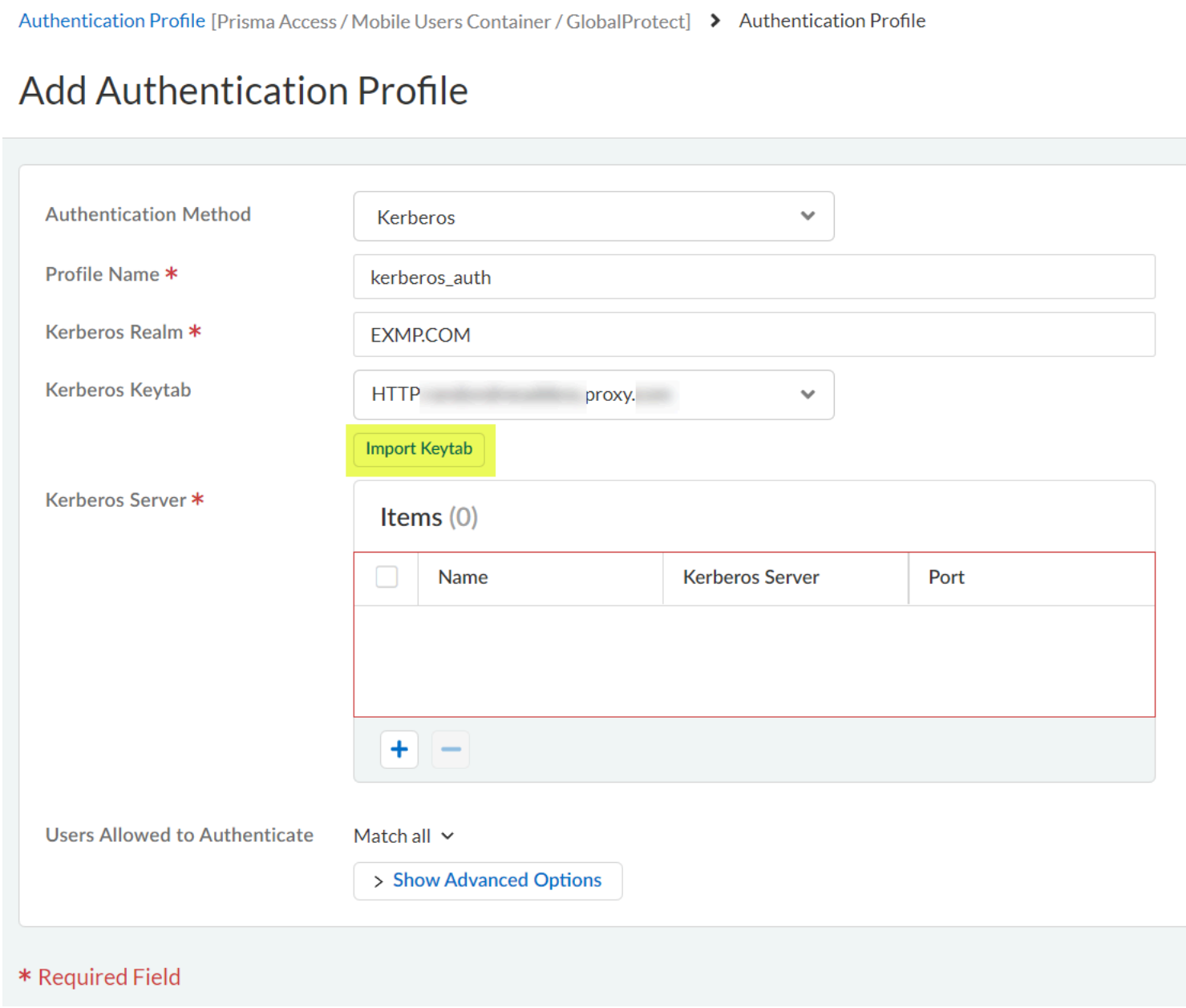
 ©2025 Palo Alto Networks, Inc.



3. Entrez le **Nom du profil** pour identifier le profil du serveur.

   Le profil d'authentification spécifie le profil du serveur pour le portail ou les passerelles à utiliser lorsqu'ils authentifient les utilisateurs.
4. Saisissez la **Kerberos Realm (Partition Kerberos)** (maximum de 127 caractères) afin de spécifier la portion nom d'hôte du nom de connexion de l'utilisateur. Par exemple, le nom du compte d'utilisateur user@EXMP.COM présente le domaine EXMP.COM.
5. Importez le **Kerberos Keytab (Keytab Kerberos)** (**Import Keytab (Importer Keytab)**) que vousavez créé plus tôt.

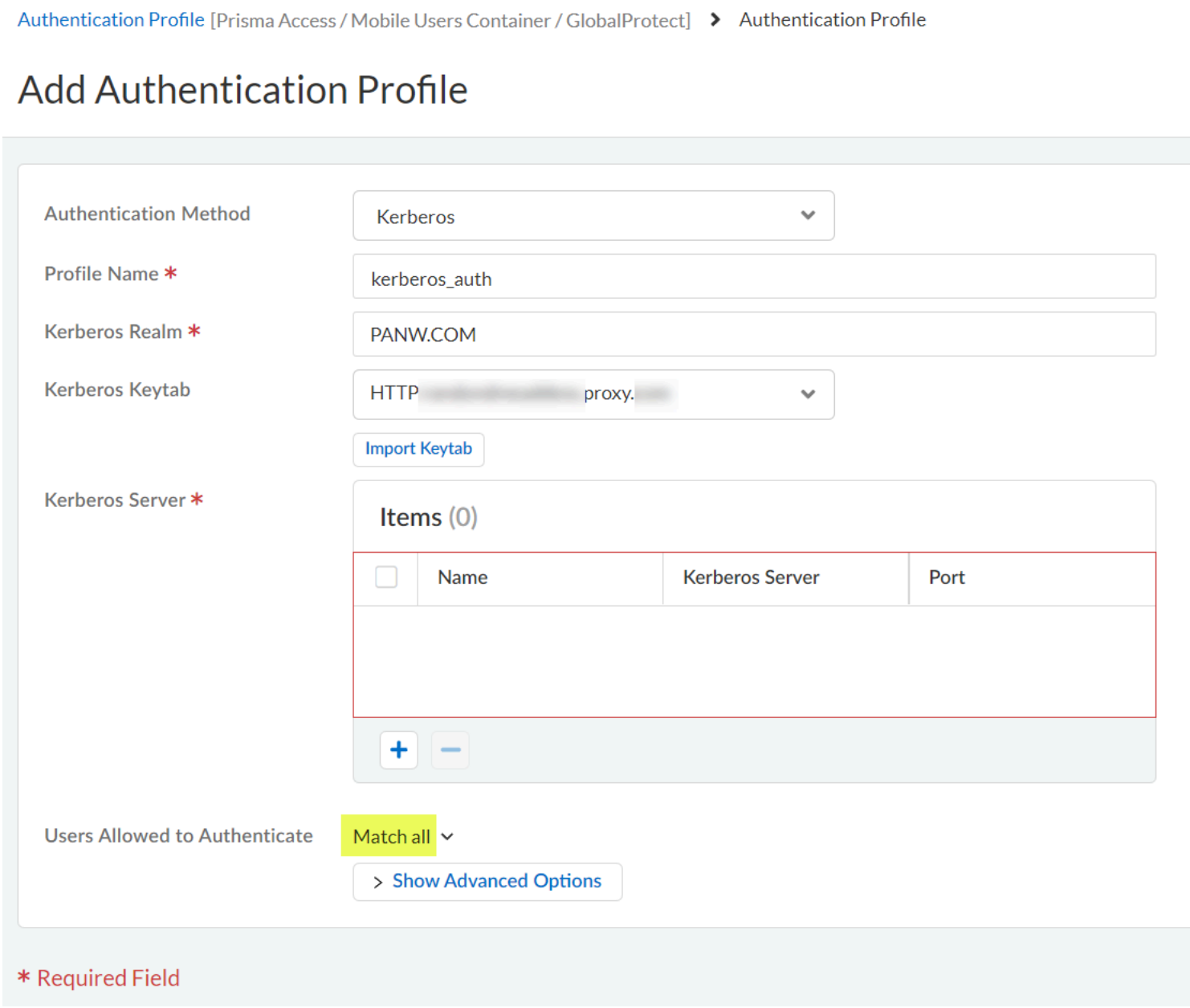
©2025 Palo Alto Networks, Inc.



6. Ajoutez les **Users Allowed to Authenticate (Utilisateurs autorisés à s'authentifier)** avec ce profil.
   - Pour sélectionner tous les utilisateurs, cliquez sur **Match all (Correspondre à tout)**.
   - Si vous utilisez Cloud Identity Engine pour remplir la liste des utilisateurs, sélectionnez-les dans une liste ou sélectionnez **All (Tous)** pour permettre à tous les utilisateurs de s'authentifier.
   - Pour ajouter des utilisateurs locaux qui peuvent se connecter à l'aide de Kerberos, cliquez sur **Add Local User (Ajouter un utilisateur local)**, ajoutez son **Name (Nom)** et créez un **Password (Mot de passe)**.

 ©2025 Palo Alto Networks, Inc.

- Lors de la configuration de l'authentification et du mappage d'utilisateur, utilisez le format userPrincipalName (UPN). Les autres formats (tels que samAccountName) ne sont pas pris en charge.
- Les noms d'utilisateur avec des caractères unicode ne sont pas pris en charge.

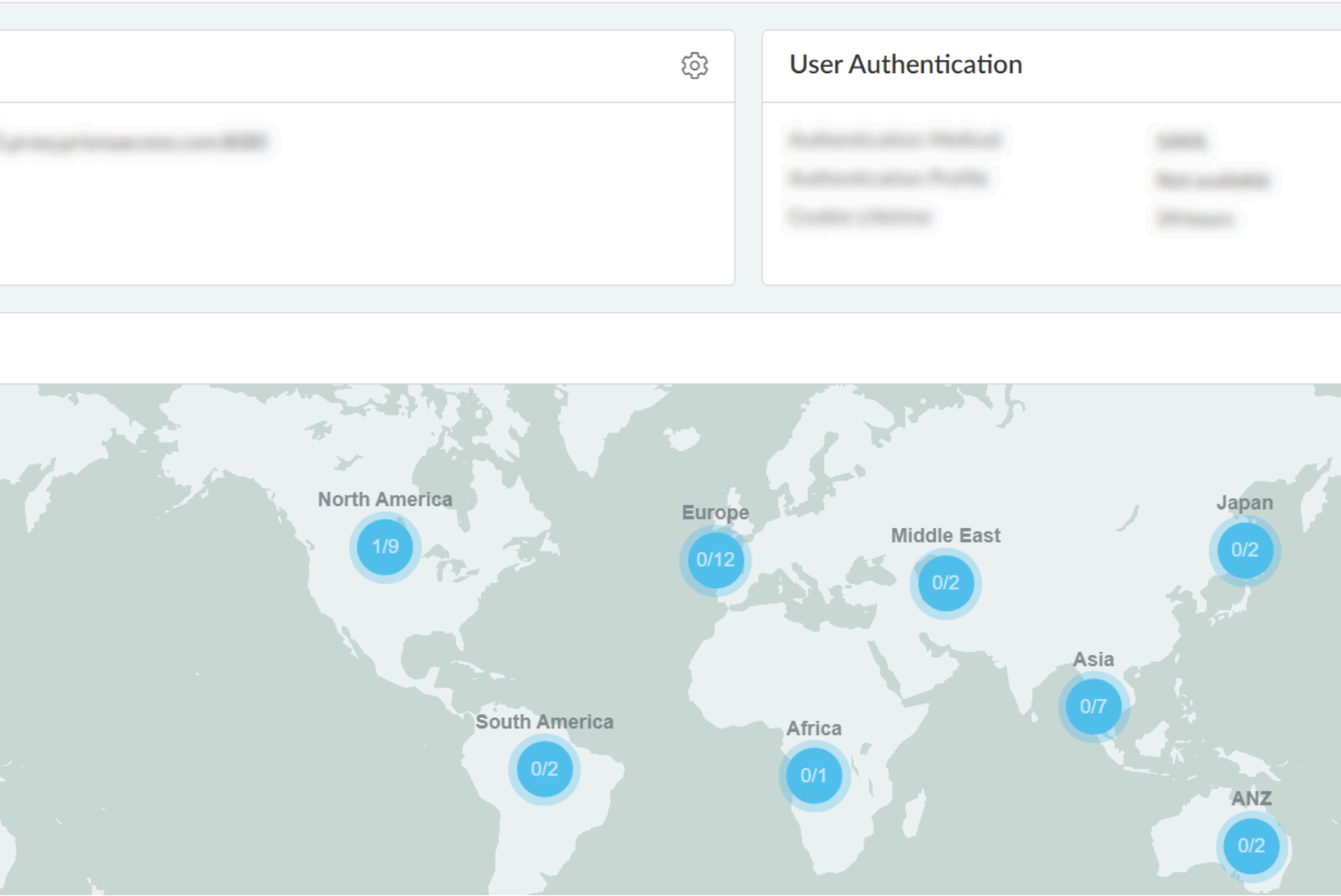


7. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

 ©2025 Palo Alto Networks, Inc.

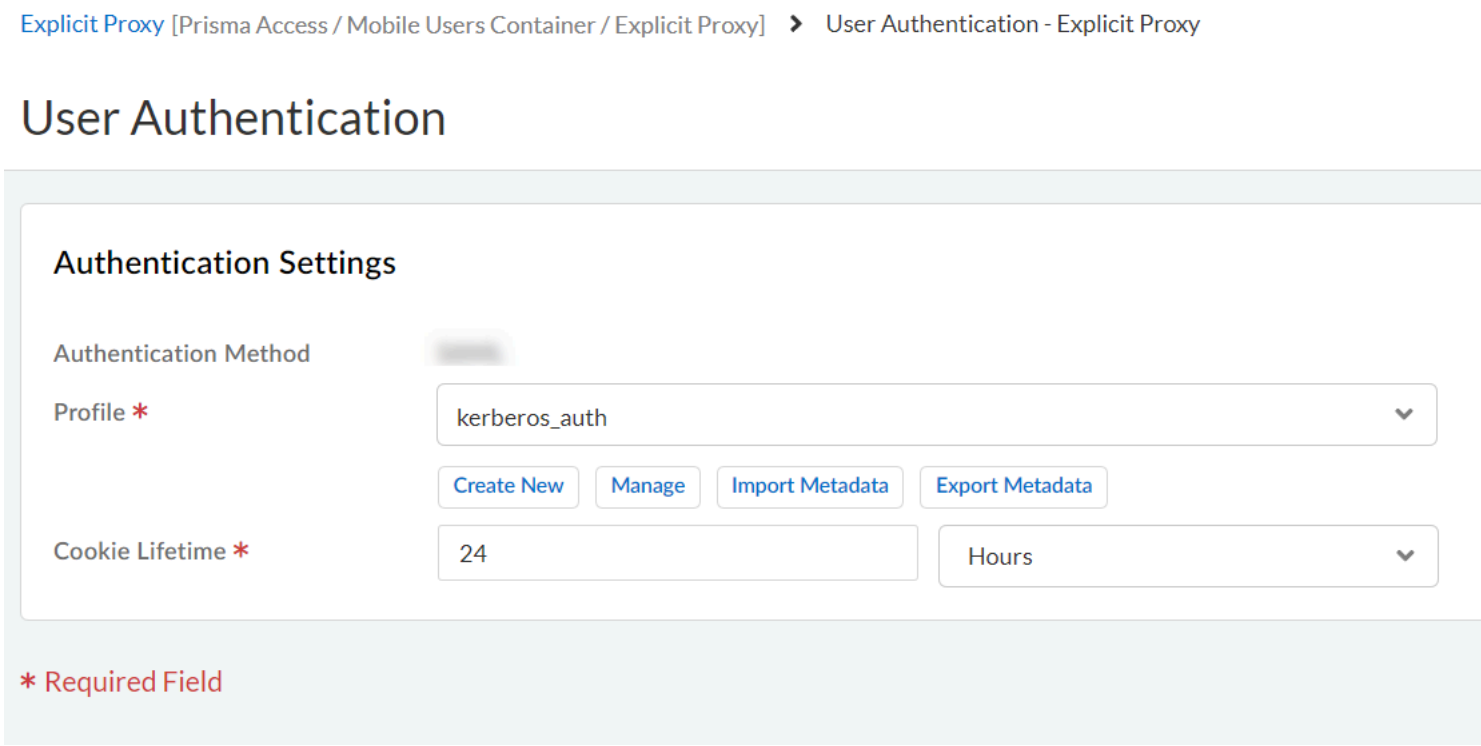
STEP 2 | Associez le profil d'authentification à une méthode d'authentification.

1. Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **User Authentication (Authentification de l'utilisateur)**.



2. Sélectionnez le **Connection Name (Nom de la connexion)**.
3. Sélectionnez l'**Authentication Method (Méthode d'authentification) Kerberos** et sélectionnez le **Profile (Profil)** Kerberos que vous avez créé.

 ©2025 Palo Alto Networks, Inc.



4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

STEP 3 | (Facultatif) Ajoutez les adresses IP de sortie de la succursale ou de l'emplacement de campus où se trouvent vos utilisateurs, serveurs, périphériques IoT ou machines sans périphérique de contrôle à la liste des adresses de proxy explicite approuvées.

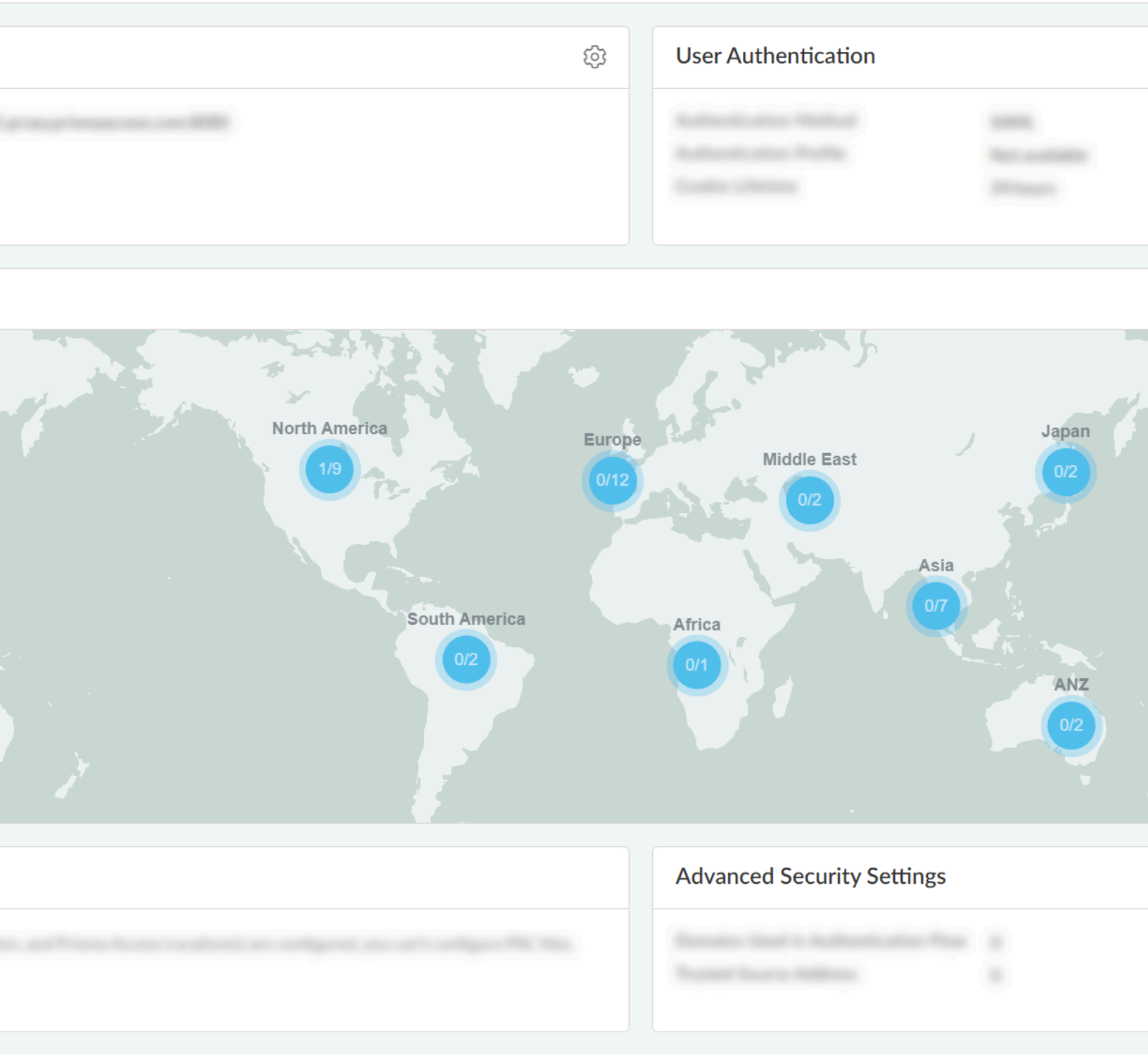
Vous n'avez besoin de faire cela que si vous souhaitez **Skip Authentication (Ignorer l'authentification)** pour des adresses IP spécifiques ou **Use X-Authenticated User (XAU)**

 ©2025 Palo Alto Networks, Inc.

header on incoming HTTP/HTTPS requests for identity (Utiliser l'en-tête des utilisateurs authentifiés X (XAU) sur les requêtes HTTP/HTTPS entrantes pour l'identité).

1. Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Advanced Security Settings (Paramètres de sécurité avancés)**.

 ©2025 Palo Alto Networks, Inc.

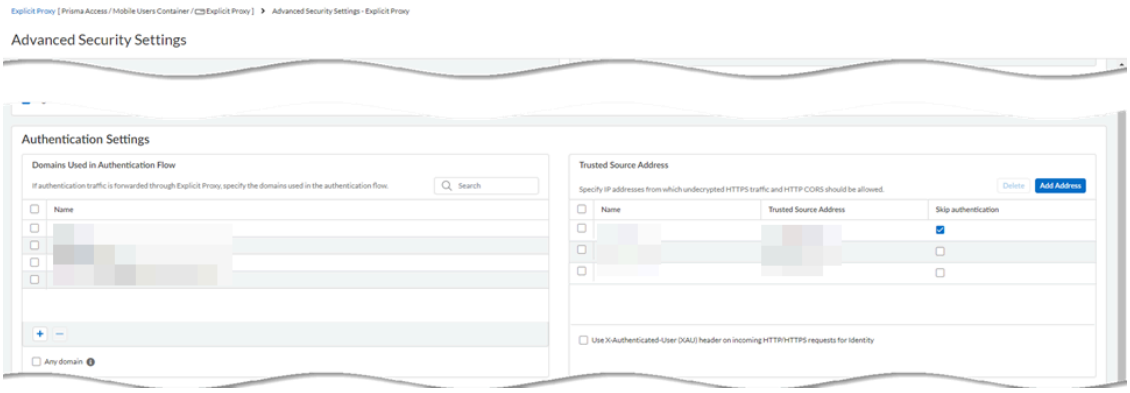


2. Cliquez sur **Add Address (Ajouter une adresse)** pour ajouter une ou plusieurs adresses au champ **Trusted Source Address (Adresse source approuvée)**.

 ©2025 Palo Alto Networks, Inc.

Si vous n'ajoutez pas les adresses IP du terminal de sortie à la liste des adresses approuvées, le proxy explicite force les utilisateurs et les machines à s'authentifier avec SAML et Kerberos.

Saisissez au maximum 100 000 adresses IP.



3. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

STEP 4 | Créez une règle de politique d'autorisation totale pour l'authentification de l'utilisateur.

1. Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** > **Add Rule (Ajouter une règle)** > **Pre Rules (Pré-règles)** > **..**
2. Nommez la règle.
3. Définissez tous les critères de correspondance requis sur **Any (N'importe lequel)**.
4. Définissez Users (Utilisateurs) sur **Known (Connu)**
5. Définissez Action sur **Allow (Autoriser)**.
6. **Save (Enregistrez)** la règle.

STEP 5 | Enregistrez les modifications de configuration.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Vérifiez que l'authentification Kerberos fonctionne avec Prisma Access en consultant les journaux de trafic et d'authentification.

1. (Trafic déchiffré uniquement) Accédez à **Activity (Activité)** > **Log Viewer (Visionneuse de journaux)** > **Firewall/Traffic (Pare-feu/Trafic)** et vérifiez que l'authentification Kerberos fonctionne.

   *Si vous utilisez Strata Cloud Manager, accédez à **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)** > **Firewall/Traffic (Pare-feu/Trafic)**.*

   Le trafic déchiffré affiche le nom d'utilisateur dans les journaux de trafic.

2. (Trafic non déchiffré uniquement) Accédez à **Activity (Activité)** > **Log Viewer (Visionneuse de journaux)** > **Firewall/Authentication (Pare-feu/Authentification)** et vérifiez que l'authentification Kerberos fonctionne correctement.

   *Si vous utilisez Strata Cloud Manager, accédez à **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)** > **Firewall/Authentication (Pare-feu/Authentification)**.*

   Les champs suivants fournissent plus d'informations sur l'événement d'authentification :

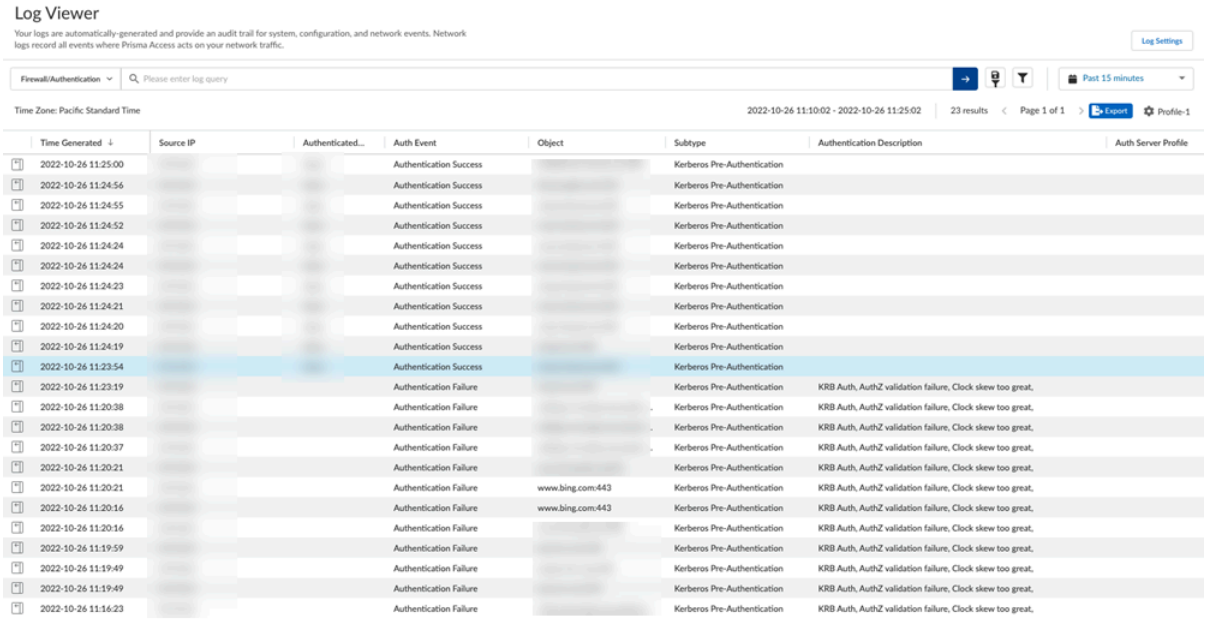
   - **Object (Objet)** : le site web auquel l'utilisateur tentait d'accéder avant d'être redirigé vers Kerberos pour s'authentifier.
   - **Auth Event (Événement d'authentification)** : l'état de la tentative d'authentification.

     Authentication Success (Authentification réussie) indique que l'événement d'authentification a réussi ; **Authentication Failure (Échec de l'authentification)** indique que la tentative a échoué et génère un journal.
   - **Authentication Description (Description de l'authentification)** : des informations supplémentaires sur le type d'échec en cas d'échec de la tentative d'authentification.

     Par exemple, **User not allowed (Utilisateur non autorisé)** indique que l'utilisateur ou le groupe n'est pas autorisé à utiliser Kerberos pour s'authentifier, peut-être

 ©2025 Palo Alto Networks, Inc.

parce qu'il n'a pas été ajouté à la **Allow List (Liste d'autorisations)** dans le profil d'authentification.



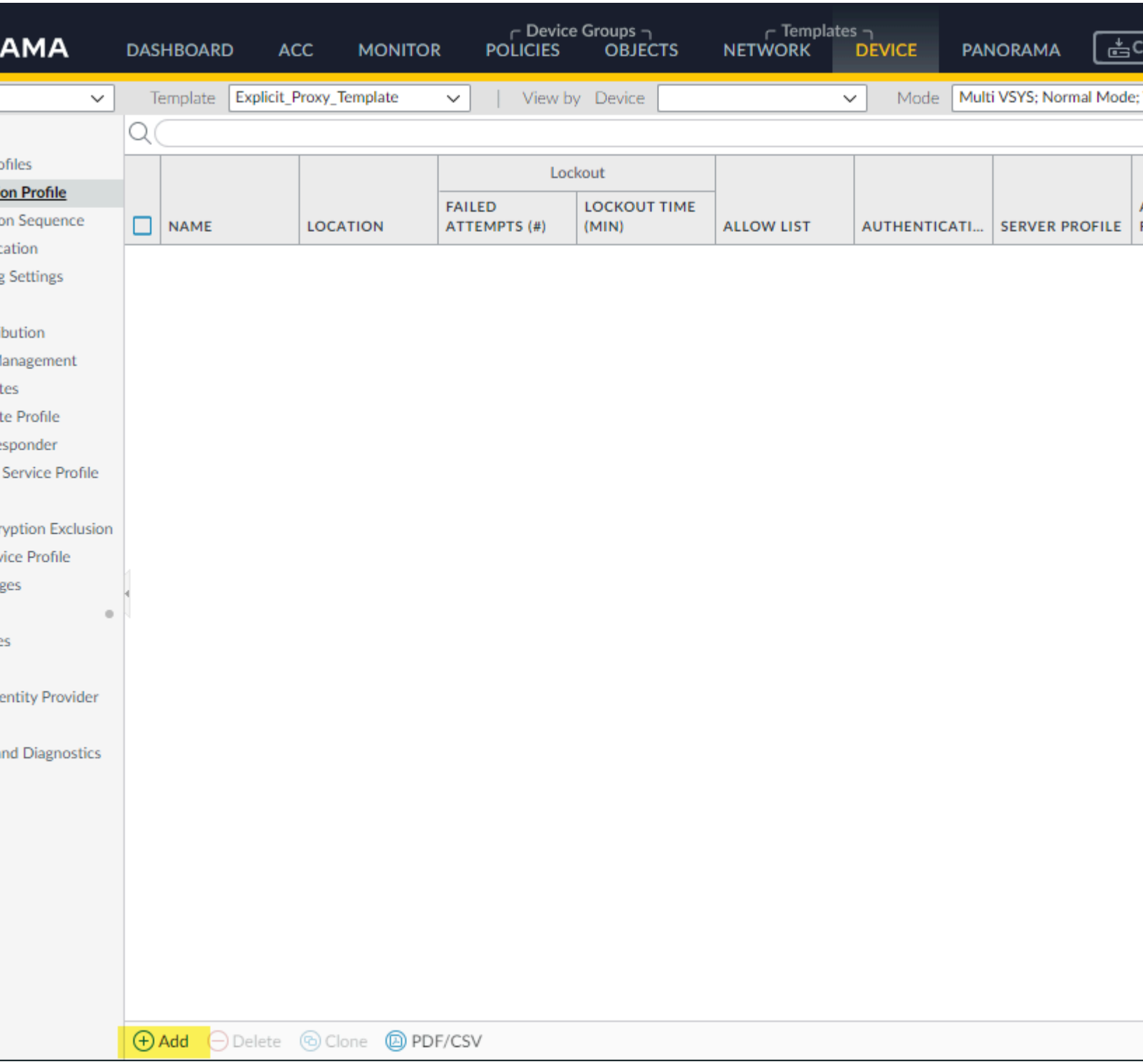
Configurer l'authentification Kerberos pour les déploiements de proxy explicite (Panorama)

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Configurez un profil d'authentification Kerberos.

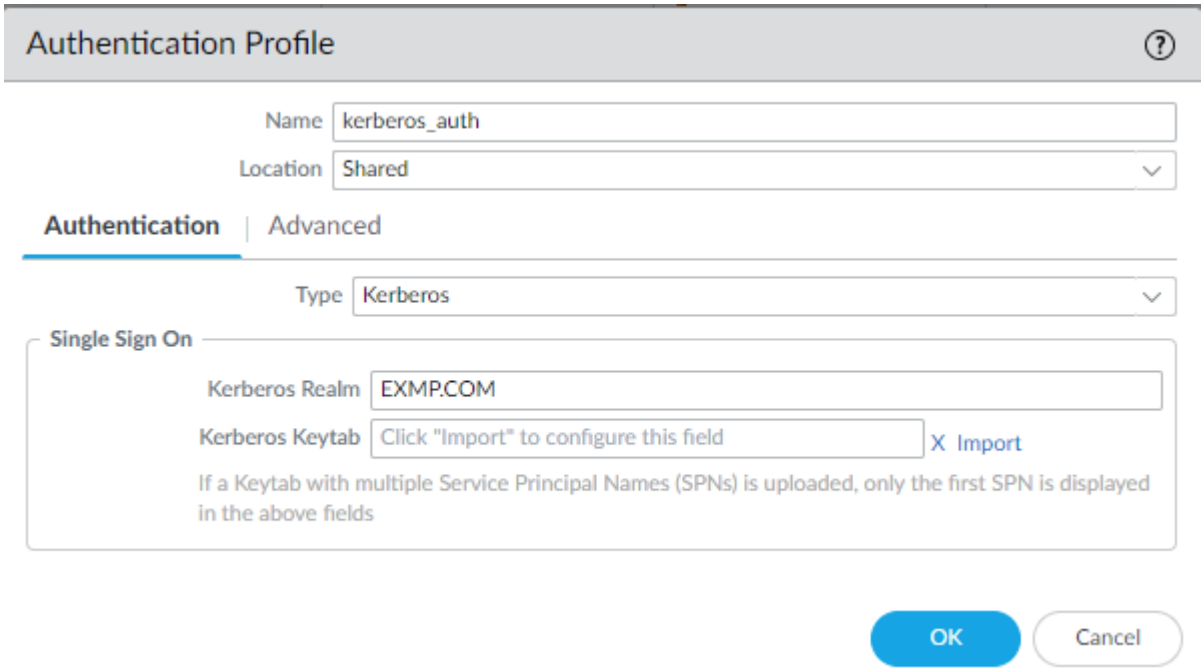
Le profil définit la façon dont le proxy explicite se connecte au serveur Kerberos pour l'authentification des utilisateurs mobiles.

1. Accédez à **Device (Périphériques)** > **Authentication Profile (Profil d'authentification)** > **+ Add (+ Ajouter)**.

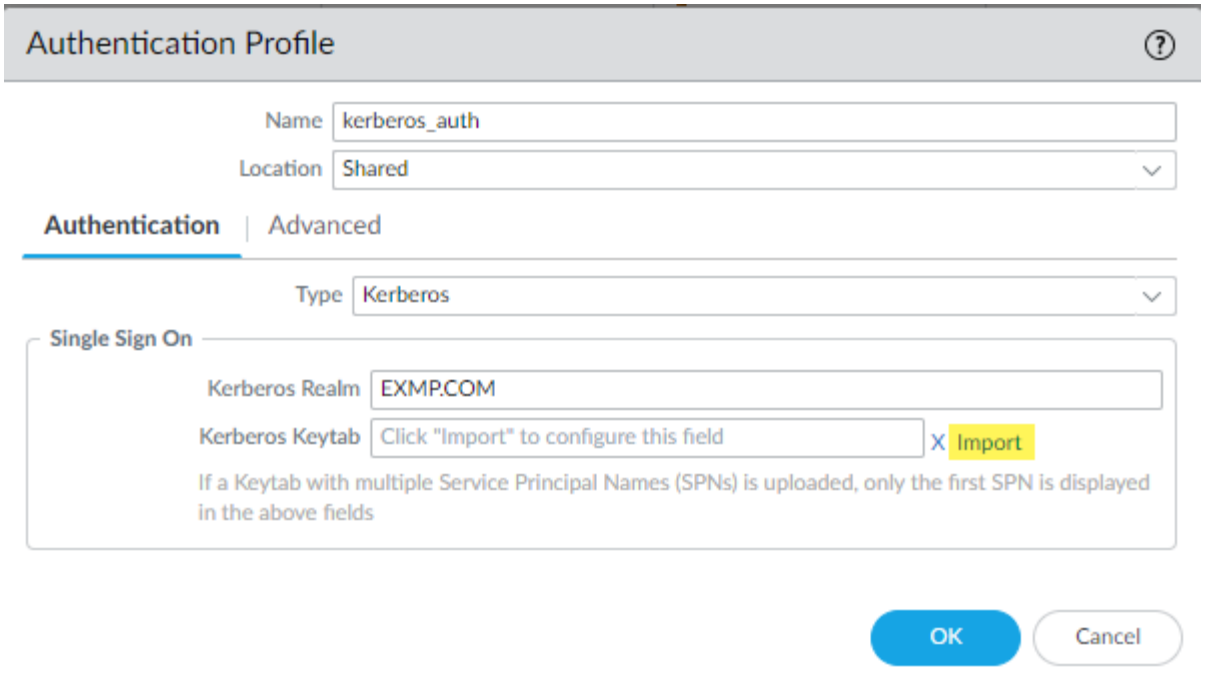


 ©2025 Palo Alto Networks, Inc.

2. Sélectionnez le **Type** : **Kerberos**.



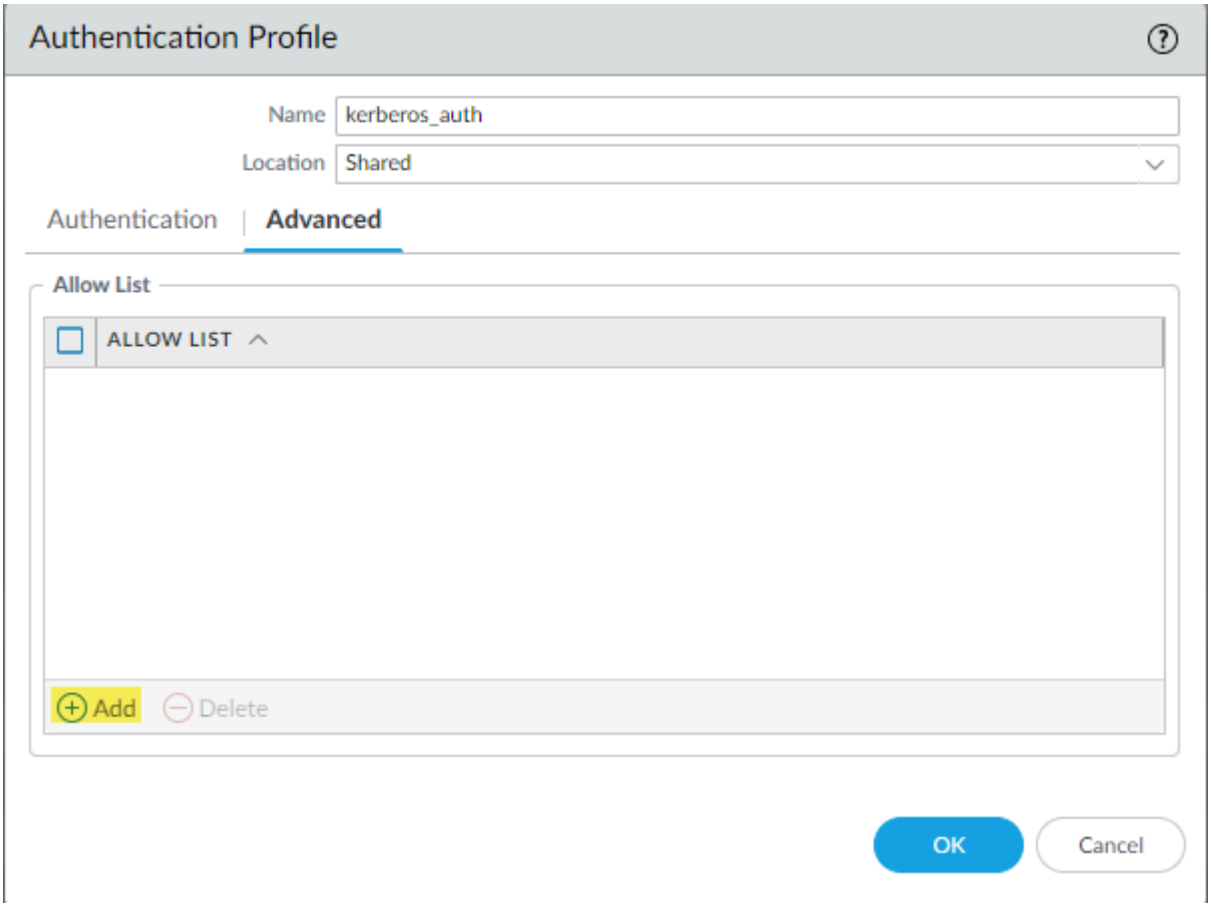
3. Entrez un **Name (Nom)** pour identifier le profil d'authentification.
4. Saisissez la **Kerberos Realm (Partition Kerberos)** (maximum de 127 caractères) afin de spécifier la portion nom d'hôte du nom de connexion de l'utilisateur. Par exemple, le nom du compte d'utilisateur user@EXMP.COM présente le domaine EXMP.COM.
5. Cliquez sur **Import (Importer)** pour importer le Keytab Kerberos que vous avez créé plus tôt.



6. Ajoutez des utilisateurs autorisés à s'authentifier avec ce profil.

©2025 Palo Alto Networks, Inc.

- Sélectionnez **Advanced (Avancé)** > **+ Add (+ Ajouter)**
- Pour sélectionner tous les utilisateurs, sélectionnez **All (Tous)**.
- Si vous utilisez Cloud Identity Engine pour remplir la liste des utilisateurs, sélectionnez-les dans une liste ou sélectionnez **All (Tous)** pour permettre à tous les utilisateurs de s'authentifier.
- Pour ajouter des utilisateurs locaux qui peuvent se connecter à l'aide de Kerberos, tapez leurs noms d'utilisateur.
  - Lors de la configuration de l'authentification et du mappage d'utilisateur, utilisez le format userPrincipalName (UPN). Les autres formats (tels que samAccountName) ne sont pas pris en charge.
  - Les noms d'utilisateur avec des caractères unicode ne sont pas pris en charge.



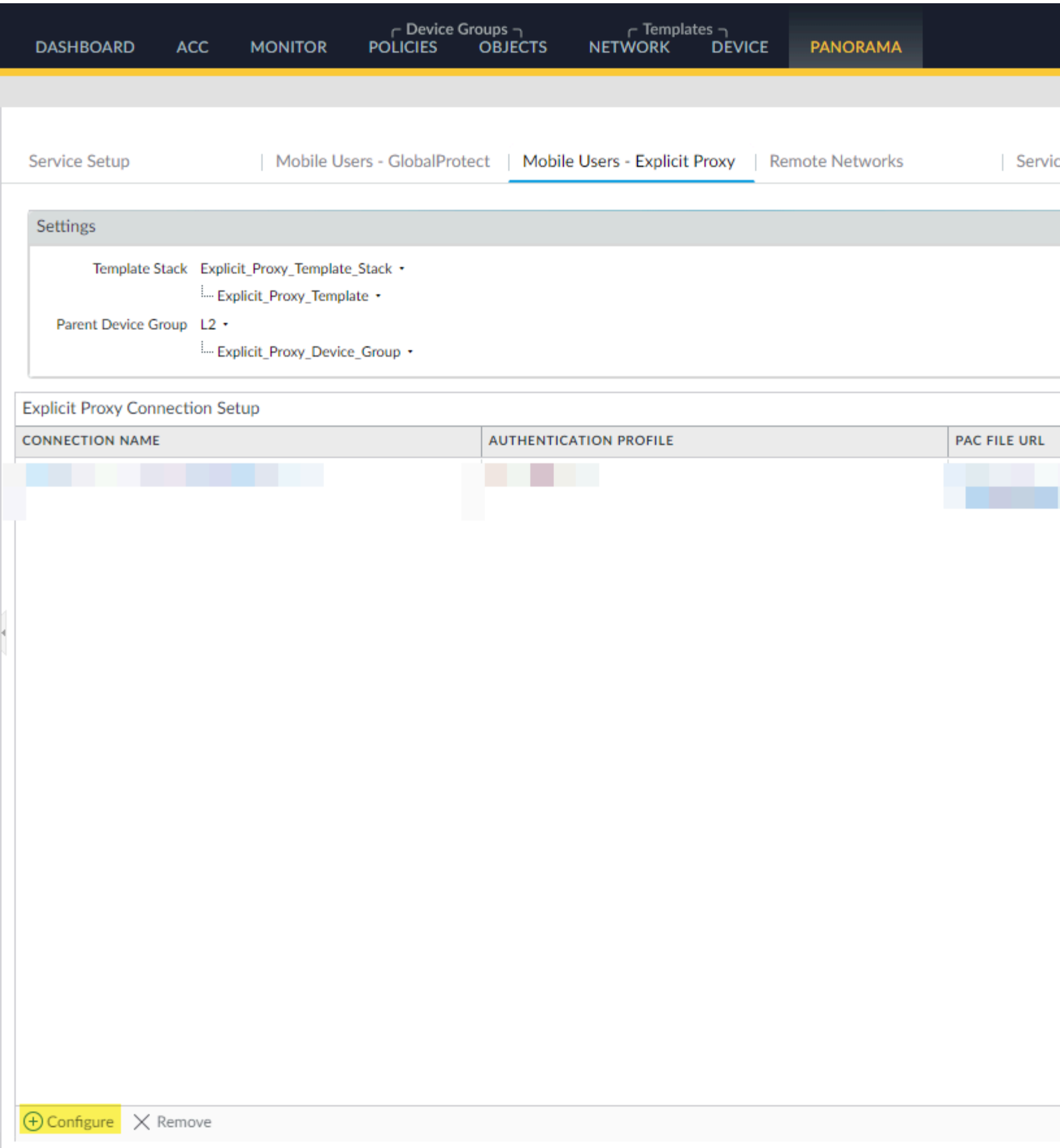
7. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

©2025 Palo Alto Networks, Inc.

STEP 2 | Associez le profil d'authentification à une méthode d'authentification.

1. Accédez à **Panorama** > **Cloud Services** > **Configuration** > **+ Configure (+ Configurer)**.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

2. Définissez le **Explicity Proxy FQDN (FQDN du proxy explicite)**.
3. Sélectionnez le **Profile (Profil)** Kerberos que vous avez créé.
4. Sélectionnez **OK** pour enregistrer vos modifications.

STEP 3 | (Facultatif) Ajoutez les adresses IP de sortie de la succursale ou de l'emplacement de campus où se trouvent vos utilisateurs, serveurs, périphériques IoT ou machines sans périphérique de contrôle à la liste des adresses de proxy explicite approuvées.

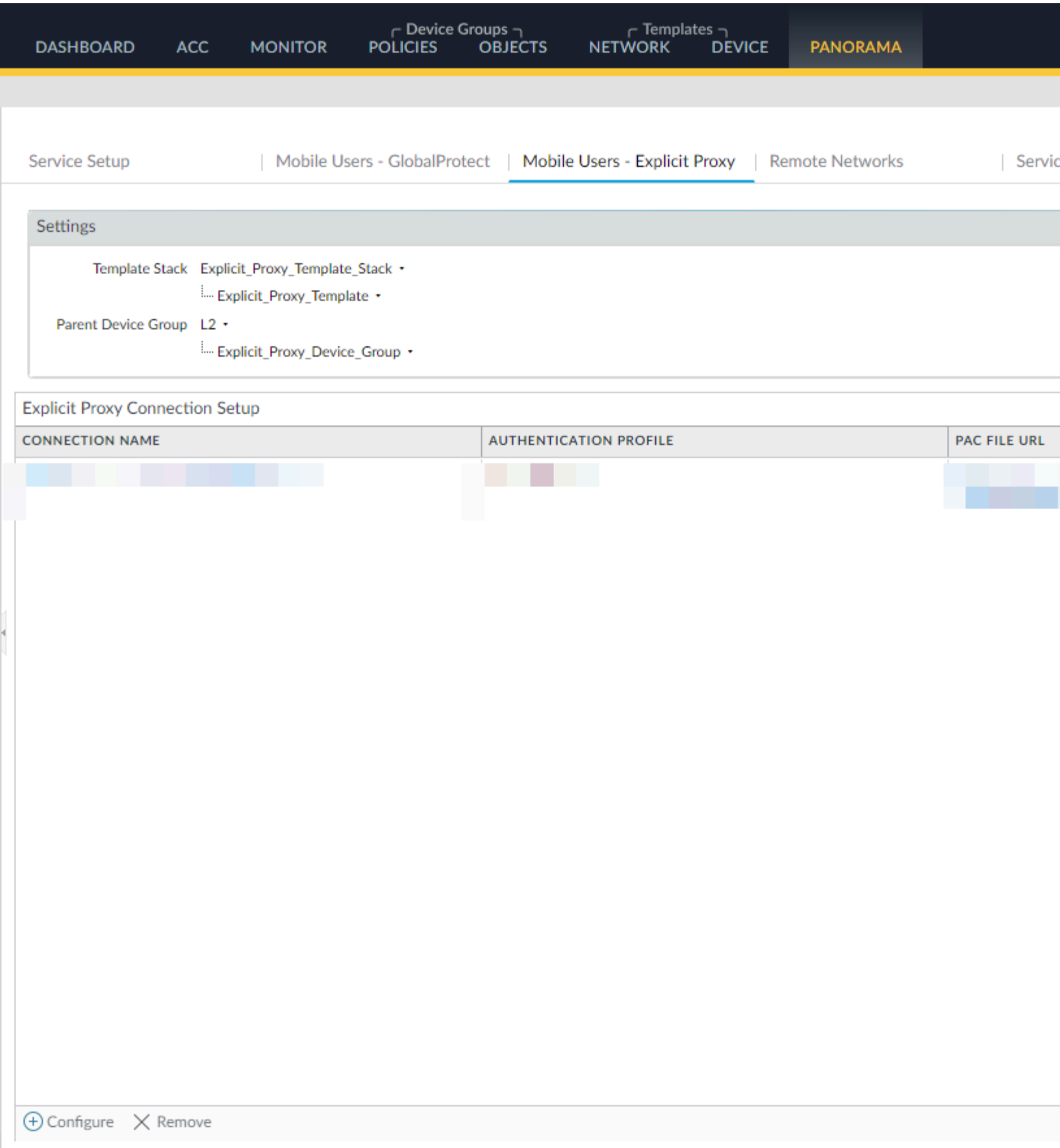
Vous n'avez besoin de faire cela que si vous souhaitez **Skip Authentication (Ignorer l'authentification)** pour des adresses IP spécifiques ou **Use X-Authenticated User (XAU)**

 ©2025 Palo Alto Networks, Inc.

header on incoming HTTP/HTTPS requests for identity (Utiliser l'en-tête des utilisateurs authentifiés X (XAU) sur les requêtes HTTP/HTTPS entrantes pour l'identité).

1. Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Settings gear (Engrenage de réglage)** > **Authentication Settings (Paramètres d'authentification)**.

 ©2025 Palo Alto Networks, Inc.



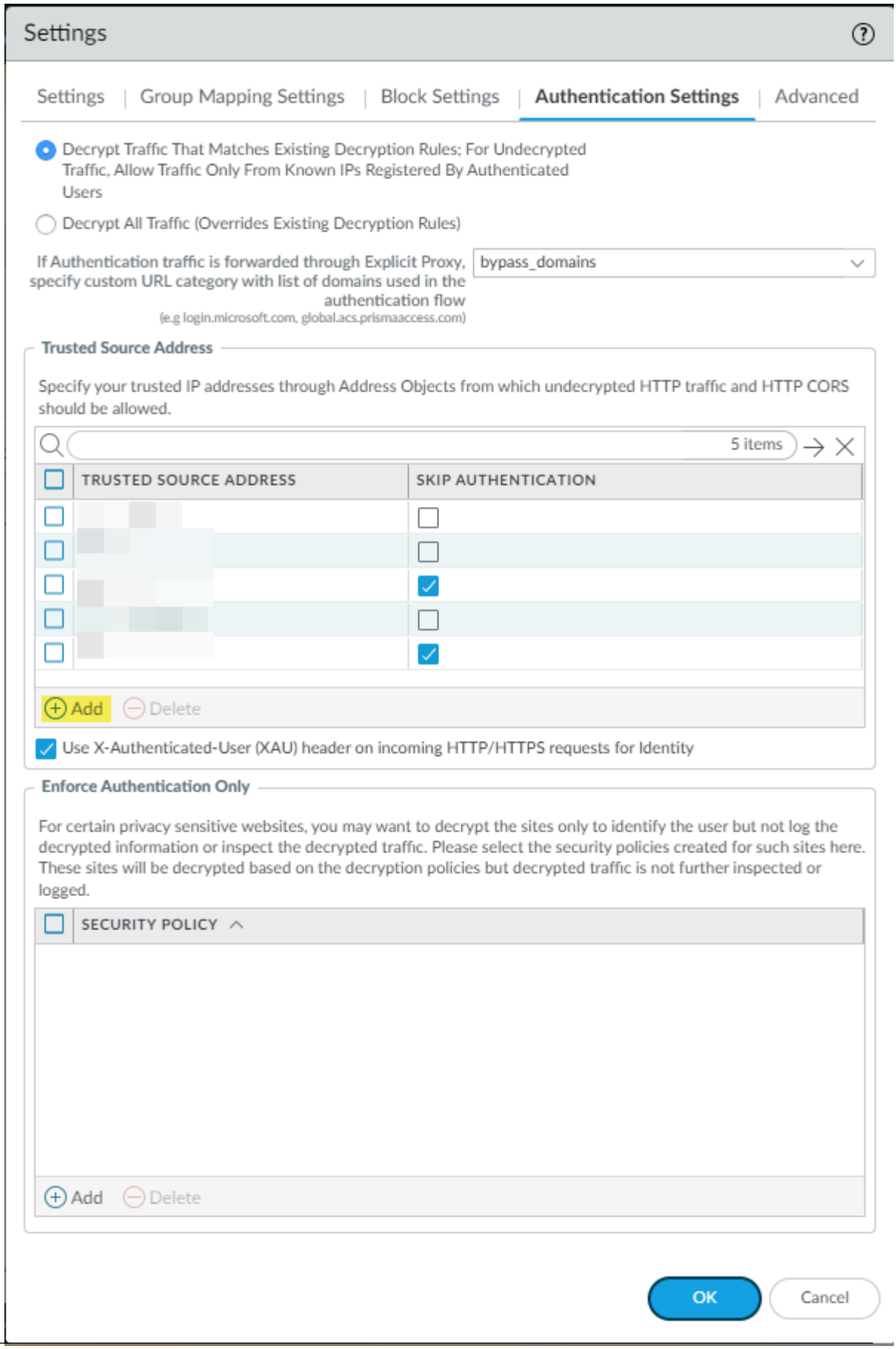
 ©2025 Palo Alto Networks, Inc.

2. Cliquez sur **Add (Ajouter)** pour ajouter des adresses au champ **Trusted Source Address (Adresse source approuvée)**.

   Si vous n'ajoutez pas les adresses IP du terminal de sortie à la liste des adresses approuvées, le proxy explicite force les utilisateurs et les machines à s'authentifier avec SAML et Kerberos.

   Saisissez au maximum 100 000 adresses IP.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

3. Sélectionnez **OK** pour enregistrer vos modifications.

STEP 4 | Créez une règle de politique d'autorisation totale pour l'authentification de l'utilisateur.

1. Sélectionnez **Policies (Politiques)** > **Pre Rules (Pré-règles)** > **+ Add (+ Ajouter)**.
2. Nommez la règle.
3. Sélectionnez **Source**
4. Définir Source User (Utilisateur source) sur **Known-user (Utilisateur connu)**
5. Définissez toutes les autres valeurs requises sur **Any (N'importe lequel)**.
6. Cliquez sur **OK** pour enregistrer la règle.

STEP 5 | Validez et appliquez les modifications apportées à votre configuration.

STEP 6 | Vérifiez que l'authentification Kerberos fonctionne avec Prisma Access en consultant les journaux de trafic et d'authentification.

1. (Trafic déchiffré uniquement) Accédez à **Monitor (Surveiller)** > **(Logs) Journaux** > **Traffic (Trafic)** et vérifiez que l'authentification Kerberos fonctionne.

   Le trafic déchiffré affiche le nom d'utilisateur dans les journaux de trafic.

2. (Trafic non déchiffré uniquement) Accédez à **Monitor (Surveiller)** > **Logs (Journaux)** > **Authentication (Authentification)** et vérifiez que l'authentification Kerberos fonctionne correctement.

   Les champs suivants fournissent plus d'informations sur l'événement d'authentification :

   - **Object (Objet)** : le site web auquel l'utilisateur tentait d'accéder avant d'être redirigé vers Kerberos pour s'authentifier.
   - **Auth Event (Événement d'authentification)** : l'état de la tentative d'authentification.

     Authentication Success (Authentification réussie) indique que l'événement d'authentification a réussi ; **Authentication Failure (Échec de l'authentification)** indique que la tentative a échoué et génère un journal.
   - **Authentication Description (Description de l'authentification)** : des informations supplémentaires sur le type d'échec en cas d'échec de la tentative d'authentification.

     Par exemple, **User not allowed (Utilisateur non autorisé)** indique que l'utilisateur ou le groupe n'est pas autorisé à utiliser Kerberos pour s'authentifier, peut-être parce qu'il n'a pas été ajouté à la **Allow List (Liste d'autorisations)** dans le profil d'authentification.

Authentification Cloud Identity Engine pour les déploiements de proxy explicite

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

 ©2025 Palo Alto Networks, Inc.

Utilisez Cloud Identity Engine pour fournir à la fois l'identification et l'authentification des utilisateurs mobiles dans le cadre d'un déploiement Prisma Access — Proxy explicite.

Cloud Identity Engine fournit l'identification et l'authentification des utilisateurs pour une solution centralisée basée sur le cloud dans des environnements de réseau sur site, basés sur le cloud ou hybrides. Cloud Identity Engine vous permet d'écrire une politique de sécurité basée sur les utilisateurs et les groupes, et contribue à sécuriser vos réseaux en appliquant des actions de sécurité basées sur le comportement.

En synchronisant en permanence les informations de vos répertoires, qu'ils soient sur site, basés sur le cloud ou hybrides, vous garantissez que les informations de vos utilisateurs sont exactes et à jour, et que l'application des politiques se poursuit en fonction des mappages, même si le fournisseur d'identité cloud est temporairement indisponible.

- Authentification Cloud Identity Engine pour les déploiements de proxy explicite (Strata Cloud Manager)
- Authentification Cloud Identity Engine pour les déploiements de proxy explicite (Panorama)

Authentification Cloud Identity Engine pour les déploiements de proxy explicite (Strata Cloud Manager)

L'application Cloud Identity Engine fournit à la fois l'identification et l'authentification des utilisateurs mobiles dans le cadre d'un déploiement Prisma Access — Proxy explicite. L'application Cloud Identity Engine s'intègre au service de cache d'authentification (Authentication Cache Service, ACS) du proxy explicite. Elle utilise des fournisseurs d'identité SAML (Identity Provider, IdP) pour fournir une authentification aux utilisateurs mobiles de proxy explicite.

Pour configurer l'authentification pour un déploiement Utilisateurs mobiles — Proxy explicite à l'aide de Cloud Identity Engine, procédez comme suit.

STEP 1 | Dans Prisma Access (Managed by Strata Cloud Manager), configurez le proxy explicite pour votre locataire.

Avant de configurer le proxy explicite, tenez compte du fonctionnement du proxy explicite et des lignes directrices à respecter lorsque vous le configurez.

Si vous avez plusieurs locataires, configurez le proxy explicite pour chacun de vos locataires qui en a besoin.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Connectez-vous au hub et, à partir de l'application Cloud Identity Engine, configurez un type d'authentification et un fournisseur d'authentification.

Vous pouvez afficher les applications dans le hub par locataire ou par compte support.

1. Configurez un type d'authentification SAML dans Cloud Identity Engine.

   Le guide de démarrage de Cloud Identity Engine contient les procédures dont vous avez besoin pour configurer un idP SAML dans le Cloud Identity Engine :

   - Configurez Azure en tant qu'IdP dans Cloud Identity Engine
   - Configurez Okta en tant qu'IdP dans Cloud Identity Engine
   - Configurez PingOne en tant qu'IdP dans Cloud Identity Engine
   - Configurez PingFederate en tant qu'IdP dans Cloud Identity Engine
   - Configurez Google en tant qu'IdP dans le Cloud Identity Engine

   Ne configurez pas la déconnexion unique, elle n'est pas prise en charge.
2. Configurez un profil d'authentification dans Cloud Identity Engine, puis sélectionnez les utilisateurs et les groupes qui peuvent utiliser cette méthode d'authentification.

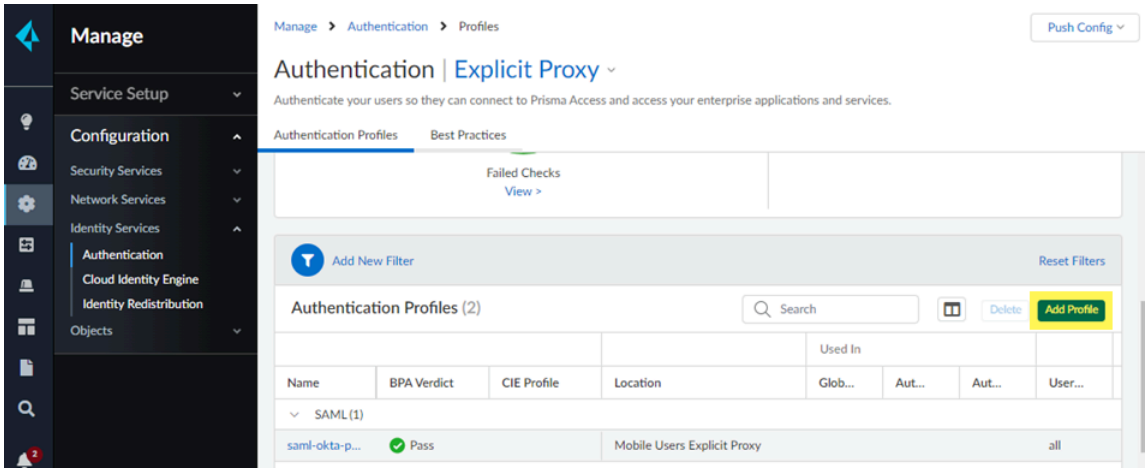
   Vous spécifierez ce profil lorsque vous créerez un profil d'authentification dans Prisma Access (Managed by Strata Cloud Manager) dans une étape ultérieure.

STEP 3 | Revenez à Prisma Access (Managed by Strata Cloud Manager) et créez un profil d'authentification à utiliser avec Cloud Authentication Engine.

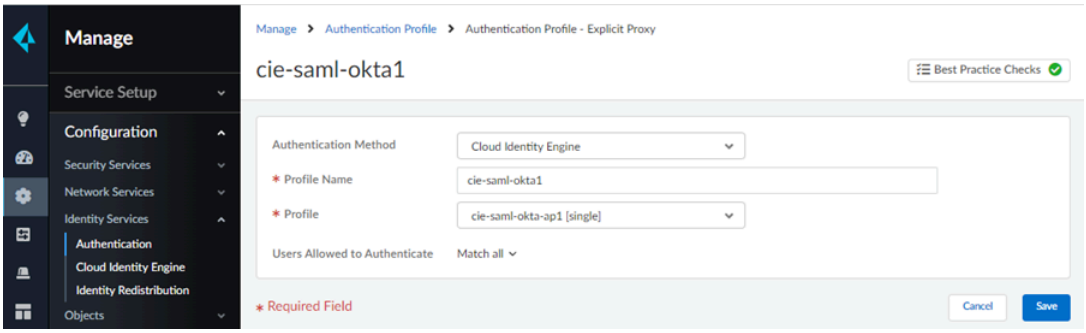
1. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Authentication**

 ©2025 Palo Alto Networks, Inc.

(Authentification), puis définissez la portée sur **Explicit Proxy (Proxy explicite)** et ajoutez un profil d'authentification (**Add Profile (Ajouter un profil)**).



2. Sélectionnez l'**Authentication Method (Méthode d'authentification) Cloud Identity Engine**.
3. Donnez au profil un **Profile Name (Nom du profil)**.
4. Sélectionnez le profil d'authentification Cloud Identity Engine que vous avez créé à l'étape précédente.

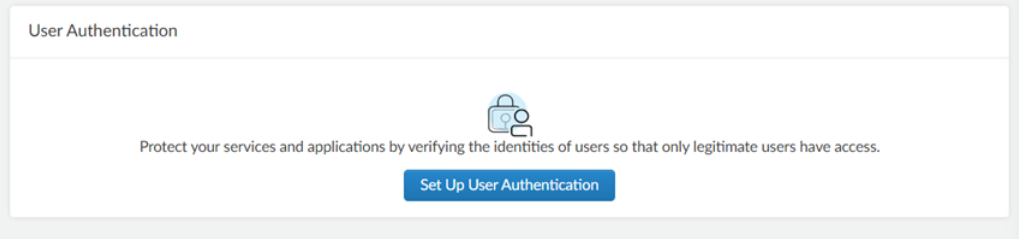


5. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Configurez l'authentification de l'utilisateur dans le proxy explicite.

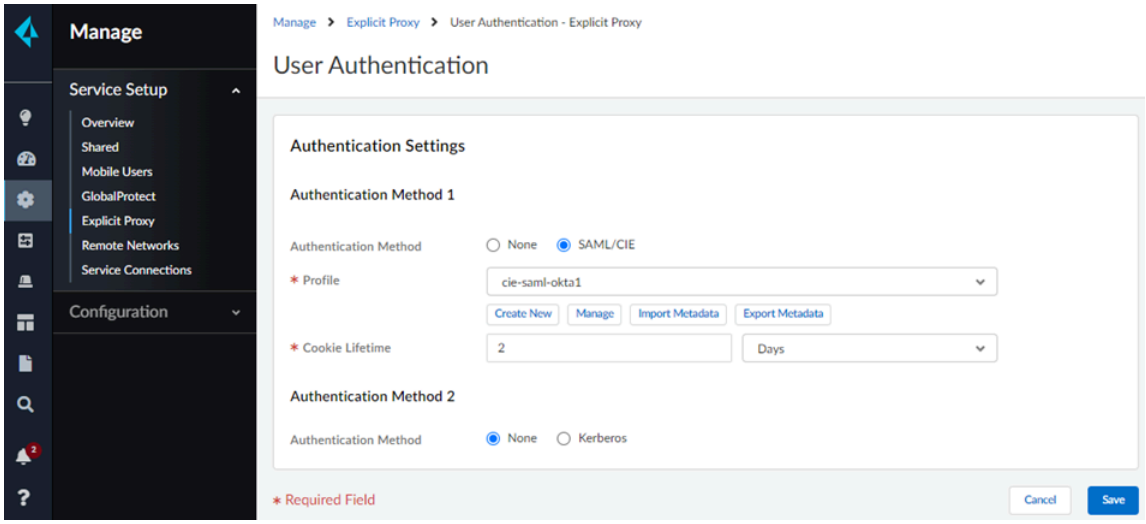
1. Allez dans **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** et **Set Up User Authentication (Configurer l'authentification de l'utilisateur)**.



2. Sélectionnez l'**Authentication Method (Méthode d'authentification) SAML/CIE**.
3. Sélectionnez le profil d'authentification que vous avez créé dans Cloud Managed Prisma Access.
4. Spécifiez une **Cookie Lifetime (Durée de vie de cookie)** pour le cookie qui stocke les informations d'authentification des utilisateurs.

   Une fois que l'IdP a authentifié l'utilisateur, Prisma Access stocke l'état d'authentification de l'utilisateur dans le service de cache d'authentification (Authentication Cache Service, ACS). La période de validité de l'authentification est basée sur la valeur de durée de vie du cookie que vous spécifiez ici.

   Pour éviter les problèmes empêchant les utilisateurs de télécharger des fichiers volumineux avant l'expiration de la durée de vie du cookie, ou l'expiration du cookie lorsque les utilisateurs accèdent à un seul site web pendant une longue période, Palo Alto Networks vous recommande de configurer une **Cookie Lifetime (Durée de vie de cookie)** d'au moins un jour. Si les utilisateurs de proxy explicite rencontrent un problème d'expiration de la durée de vie des cookies, ils peuvent accéder à un autre site web pour se réauthentifier auprès d'ACS et actualiser le cookie ACS.

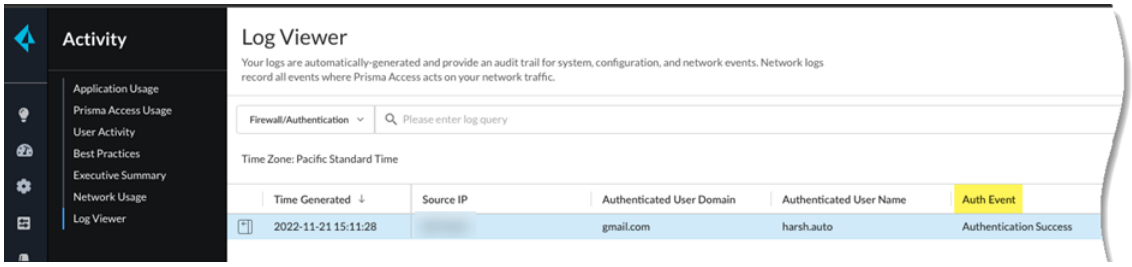


5. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

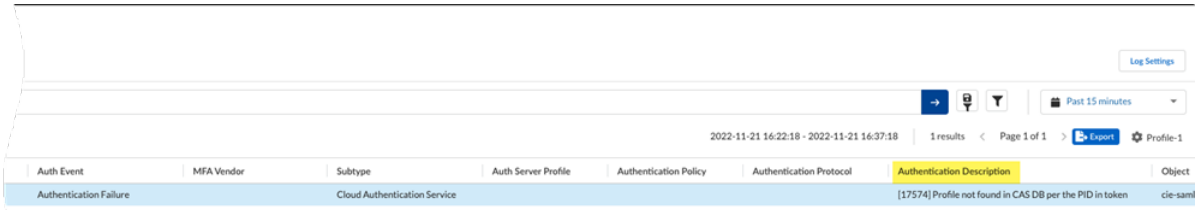
 ©2025 Palo Alto Networks, Inc.

STEP 5 | Vérifiez que Cloud Identity Engine authentifie correctement vos utilisateurs mobiles de proxy explicite.

1. Depuis Prisma Access (Managed by Strata Cloud Manager), sélectionnez **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)** > **Firewall/ Authentication (Pare-feu/Authentification)**.
2. Consultez l'état de l'**Auth Event (Événement d'authentification)**.

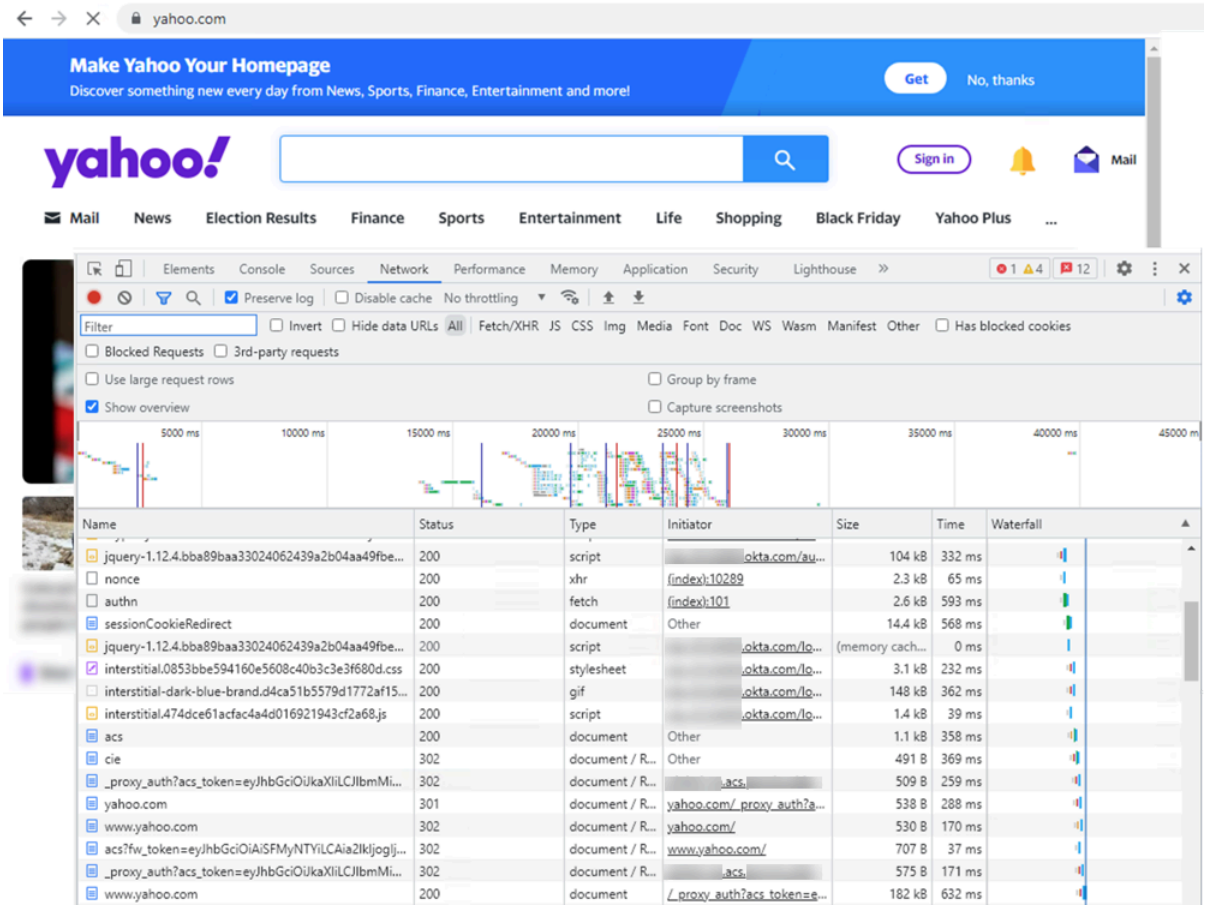


Si l'authentification échoue, consultez l'**Authentication Description (Description de l'authentification)** pour obtenir plus de détails sur l'échec.



3. À partir du terminal de l'utilisateur mobile, utilisez les outils de développement pour afficher le flux d'authentification Cloud Identity Engine.

 ©2025 Palo Alto Networks, Inc.



Authentification Cloud Identity Engine pour les déploiements de proxy explicite (Panorama)

Authentifier les utilisateurs mobiles du proxy explicite Prisma Access (Managed by Panorama) avec Cloud Identity Engine

Mode proxy sur les réseaux distants

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) Si vous souhaitez activer la visibilité et l'application basées sur l'IP de source privée sur le proxy explicite dans votre environnement Prisma Access, contactez votre équipe de compte pour en savoir plus.	• Licence Prisma Access Une licence Prisma Access Utilisateurs mobiles et une licence Prisma Access Réseau distant sont requises pour le mode proxy pour les réseaux distants.

Le mode proxy sur les réseaux distants permet de sécuriser le trafic internet sortant pour les utilisateurs et les serveurs de vos succursales qui ont besoin d'une méthode de connexion basée sur PAC pour des raisons de mise en réseau ou de conformité.

 ©2025 Palo Alto Networks, Inc.

Vous pouvez utiliser le mode proxy pour les réseaux distants pour :

- Sécurisez le trafic Internet à partir de sites de succursales qui utilisent des itinéraires non par défaut.
- Sécurisez le trafic Internet à partir de vos succursales sans le réacheminer vers un centre de données ou ule siège social.
- Connectez-vous à Prisma Access proxy explicite sur des adresses IP privées.

  Prisma Access vous fournit quatre adresses IP anycast à l'échelle mondiale, et une adresse IP unicast par réseau distant, que vous utilisez pour transférer le trafic vers le proxy explicite.
- Appliquez les contrôles de sécurité et obtenez une visibilité basée sur l'IP source pour les systèmes de la succursale.
- Passez l'authentification pour les serveurs en fonction de l'adresse IP Source.
- Connectez-vous à Prisma Access depuis votre succursale via un tunnel IPSec.
- Si vous avez besoin de plus de 1 000 Mbits/s de bande passante, vous pouvez créer une connexion réseau distant à large bande passante en utilisant plusieurs connexions réseau distant et spécifier les adresses anycast et unicast du proxy explicite dans chaque connexion.

Le diagramme suivant montre un réseau distant qui a été configuré pour un site qui n'a pas d'itinéraire par défaut configuré. Pour protéger les utilisateurs et les périphériques sans tête sur le site à l'aide du proxy explicite, l'administrateur a effectué les modifications de configuration suivantes :

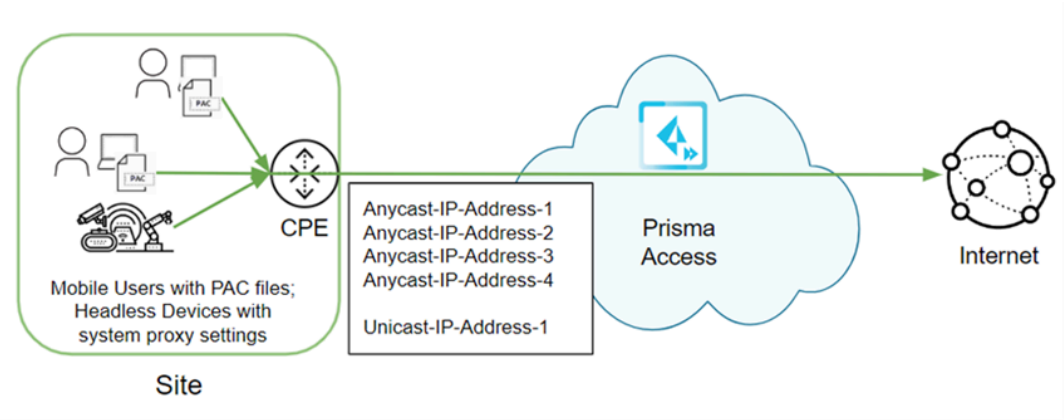
- Réseaux distants intégrés et emplacements de proxy explicite et avoir récupéré les adresses IP anycast et unicast que Prisma Access prend de son sous-réseau d'infrastructure.

  Vous pouvez également créer un nom d'hôte pour le trafic dirigé par le proxy explicite et ajouter les adresses IP unicast et anycast du proxy explicite à ce nom d'hôte.
- Configuration du CPE pour transférer le trafic du proxy explicite vers ces adresses anycast et unicast.

  Utilisez les adresses IP anycast dans le fichier PAC pour que Prisma Access sélectionne à partir de n'importe quel tunnel réseau distant intégré pour transférer le trafic vers le proxy explicite. Utilisez l'adresse unicast pour que Prisma Access transfère le trafic à travers un tunnel de réseau distant spécifique. Dans cet exemple, vous pouvez utiliser des adresses anycast ou unicast, puisque le trafic ne passe que par un tunnel IPSec du réseau distant.
- Spécifié ces adresses IP dans les fichiers PAC des terminaux des utilisateurs et dans les paramètres proxy système des périphériques sans tête.

Une fois la configuration terminée, Prisma Access transfère le trafic du tunnel du réseau distant vers le proxy explicite.

 ©2025 Palo Alto Networks, Inc.



- Strata Cloud Manager
- Panorama

Mode proxy sur les réseaux distants (Strata Cloud Manager)

Pour sécuriser les utilisateurs sur les réseaux distants à l'aide d'un proxy explicite dans Prisma Access géré dans le cloud, procédez comme suit.

STEP 1 | Configurez votre configuration de proxy explicite et intégrez les emplacements de proxy explicite que vous souhaitez ajouter.

STEP 2 | Intégrez vos réseaux distants si vous ne l'avez pas déjà fait.

Vous devez activer Prisma Access Réseaux distants dans les emplacements qui sont pris en charge avec le proxy explicite.

STEP 3 | **Push Config (Transmettre la configuration)**, étant sûr que **Mobile Users—Remote Workforce (Utilisateurs mobiles—Main-d'œuvre à distance)** et **Remote Networks (Réseaux distants)** sont sélectionnés dans la portée **Push (Pousser)**.

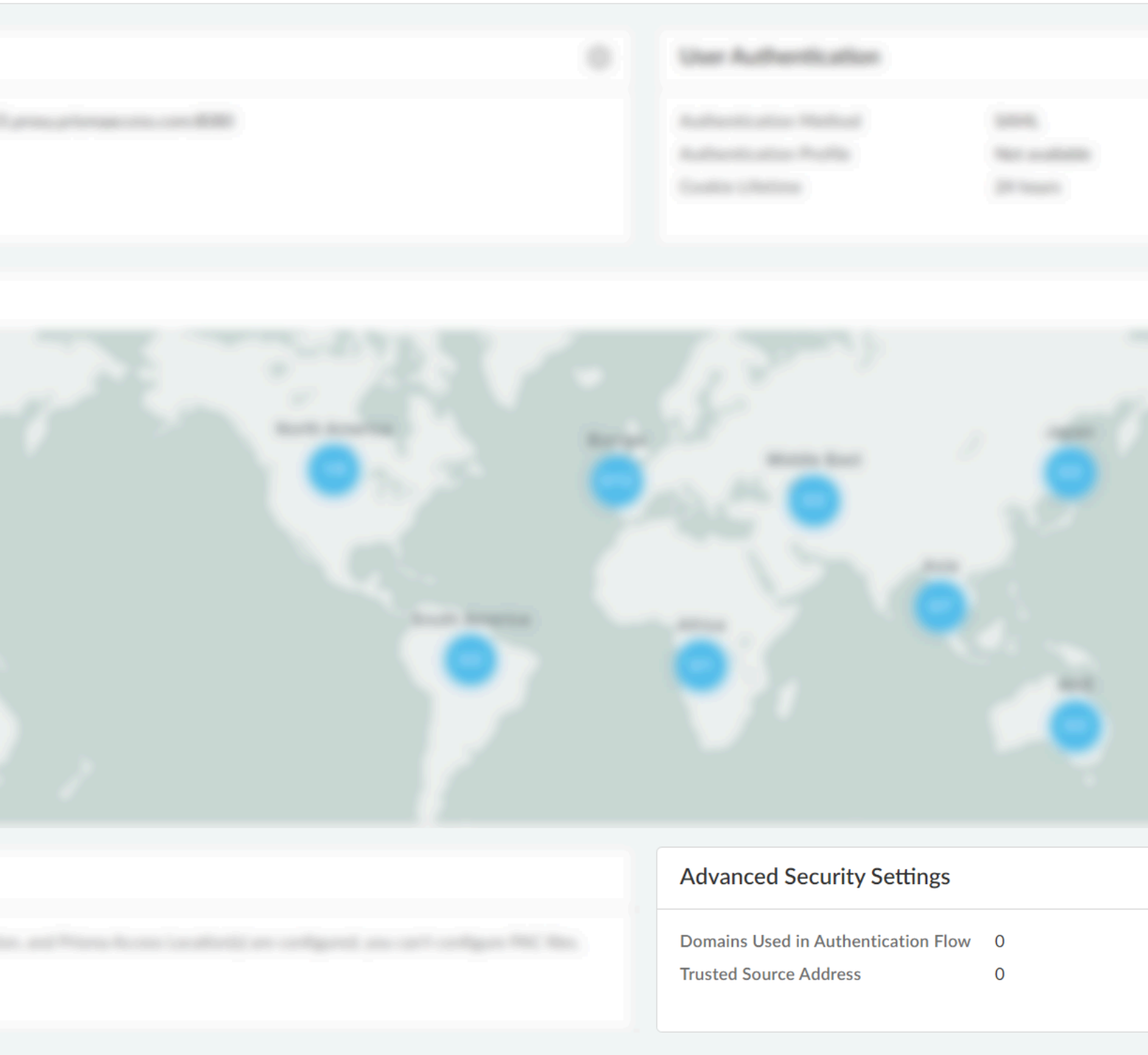
L'opération de transmission récupère les adresses Anycast dont vous avez besoin pour intégrer le proxy explicite au réseau distant.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Obtenez les adresses IP anycast que vous utilisez pour votre déploiement de proxy explicite/réseau distant.

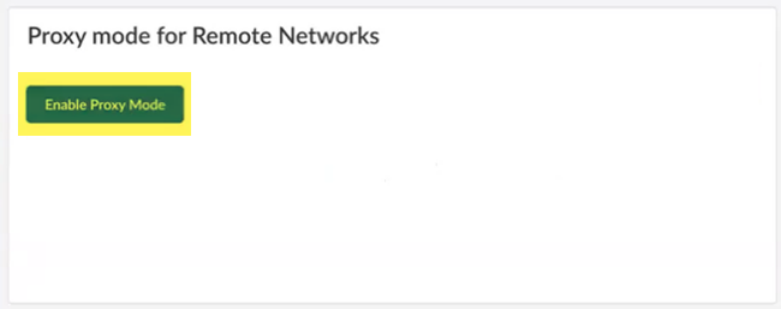
1. Allez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Advanced Security Settings (Paramètres de sécurité avancés)**.

 ©2025 Palo Alto Networks, Inc.



2. **Enable Proxy Mode (Activer le mode proxy).**

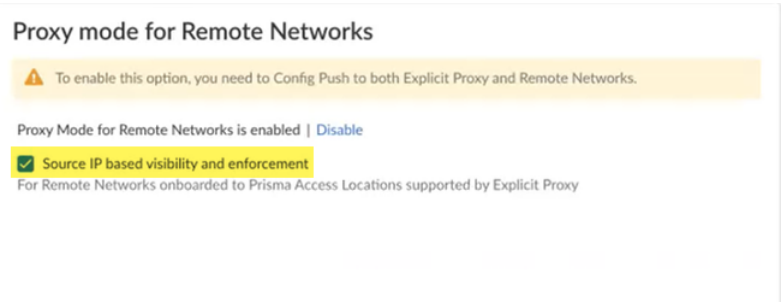
 ©2025 Palo Alto Networks, Inc.



3. Pour exploiter les adresses IP sources des systèmes de vos succursales qui transfèrent le trafic vers le proxy explicite, sélectionnez **Source IP based visibility and enforcement (Visibilité et application basées sur l'IP source)**.

   Cette fonctionnalité présente les exigences suivantes :

   - Un plan de données Prisma Access minimum de 10.2.4
   - Vous ne devez utiliser que des emplacements réseau distants pris en charge avec proxy explicite.



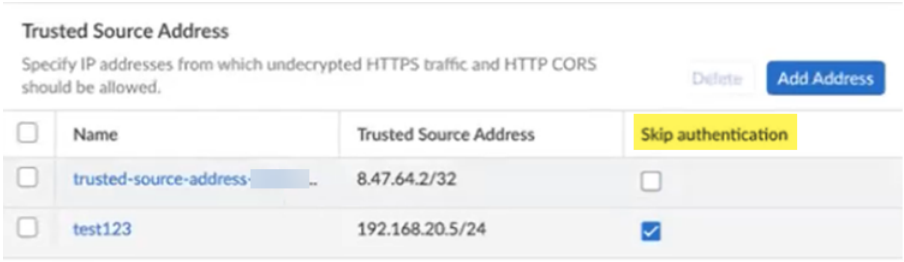
4. Ajoutez une stratégie pour autoriser le trafic lié à des adresses IP anycast et unicast sur des réseaux distants. Si vous avez activé **Source IP visibility and enforcement (Visibilité et application basées sur l'IP source)**, utilisez le champ **Source IP (IP Source)** dans les Stratégies de sécurité dans le proxy explicite pour sécuriser le trafic. Vous avez besoin de stratégies supplémentaires dans les réseaux distants.
5. (Facultatif) Pour contourner l'authentification des adresses sources fiables que vous avez saisies, spécifiez les adresses IP dont l'authentification doit être ignorée dans la zone **Trusted Source Address (Adresse de la source fiable)** et sélectionnez **Skip authentication (Ignorer l'authentification)**.

   Vous pouvez utiliser **Skip authentication (Ignorer l'authentification)** avec **Source IP based visibility and enforcement (Visibilité et application basées sur l'IP source)** pour ignorer l'authentification des systèmes sans tête qui ne peuvent pas s'authentifier,

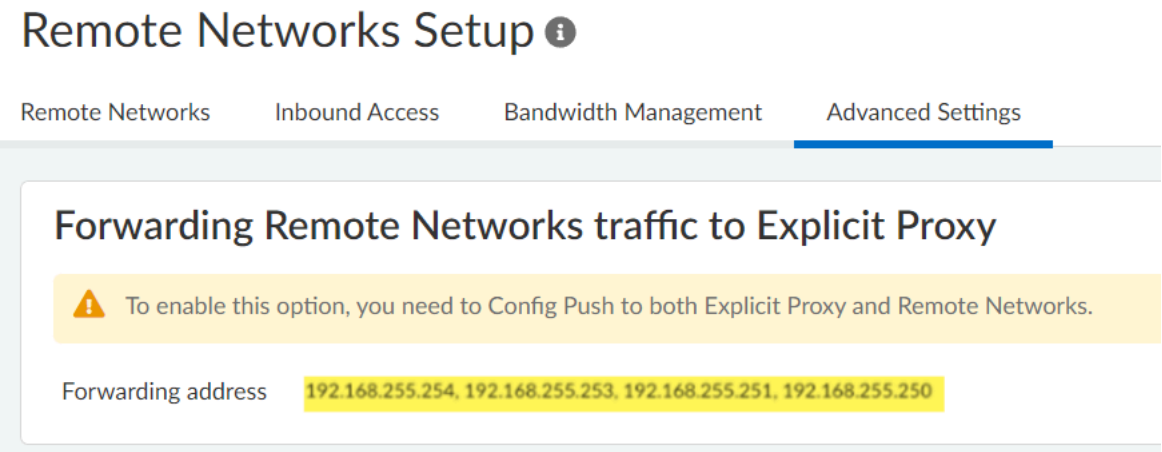
 ©2025 Palo Alto Networks, Inc.

configurer des stratégies de sécurité et obtenir une visibilité du trafic sur le proxy explicite Prisma Access.

Vous pouvez ajouter des adresses IP ou des sous-réseaux. Un maximum de 100 000 adresses IP est pris en charge après l'extension des sous-réseaux.



6. Allez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Remote Networks (Réseaux distants)**.
7. **Push Config (Transmettre la configuration)**, étant sûr que **Mobile Users—Remote Workforce (Utilisateurs mobiles—Main-d'œuvre à distance)** et **Remote Networks (Réseaux distants)** sont sélectionnés dans la portée **Push (Pousser)**.
8. Allez à **Advanced Settings (Paramètres avancés)** dans la configuration de vos réseaux distants et recherchez les adresses IP anycast utilisées pour transférer le trafic vers le proxy explicite.



STEP 5 | (Facultatif) Recherchez l'adresse de monodiffusion à utiliser pour votre déploiement de proxy explicite/réseau distant.

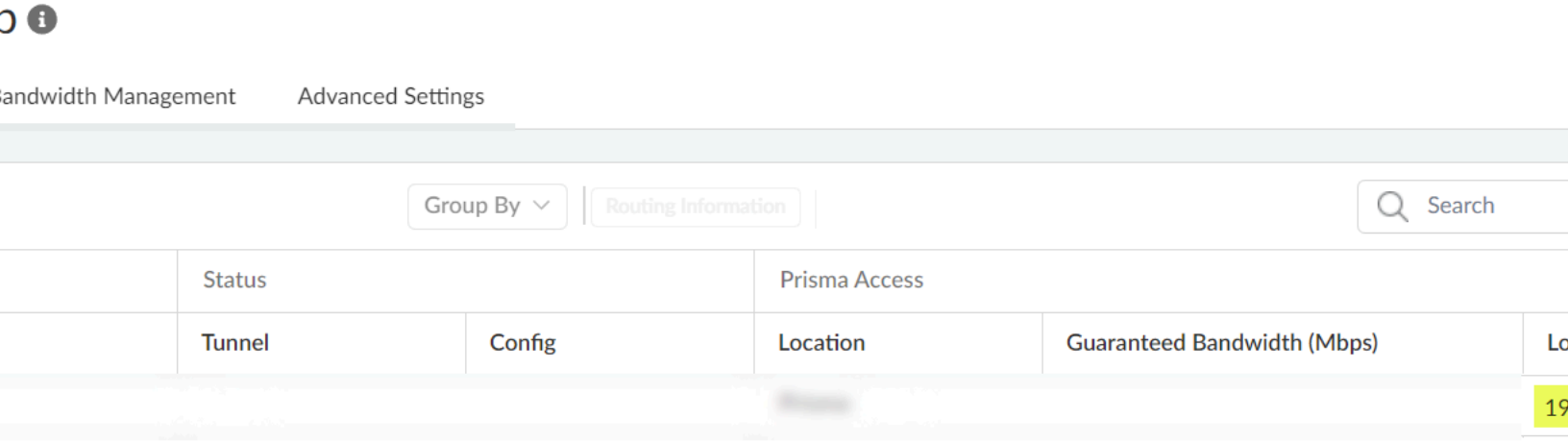
Utilisez l'adresse IP de monodiffusion dans le fichier PAC uniquement si vous souhaitez cibler un réseau distant spécifique pour transférer le trafic vers le proxy explicite. Si vous souhaitez

 ©2025 Palo Alto Networks, Inc.

utiliser tous les réseaux distants déployés pour transférer le trafic vers le proxy explicite, utilisez les adresses anycast.

1. Allez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Remote Networks (Réseaux distants)**.
2. Prenez note de la **Loopback IP address (Adresse IP de bouclage)**.

   Si vous avez des adresses IPv4 et IPv6, notez l'adresse IPv4.



Mode proxy sur les réseaux distants (Panorama)

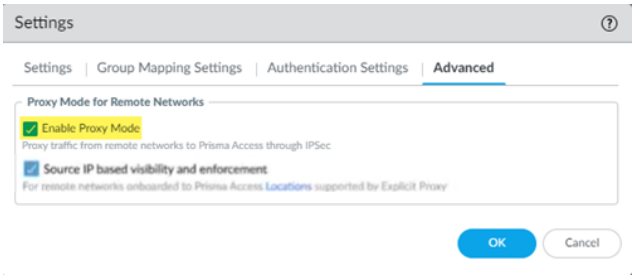
Pour sécuriser les utilisateurs sur les réseaux distants à l'aide du proxy explicite dans Prisma Access (Managed by Panorama) Access, procédez comme suit.

STEP 1 | Configurez le déploiement de votre proxy explicite et intégrez les emplacements de proxy explicite que vous souhaitez ajouter.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Récupérez les adresses IP anycast que vous utilisez pour votre déploiement de proxy explicite/réseau distant.

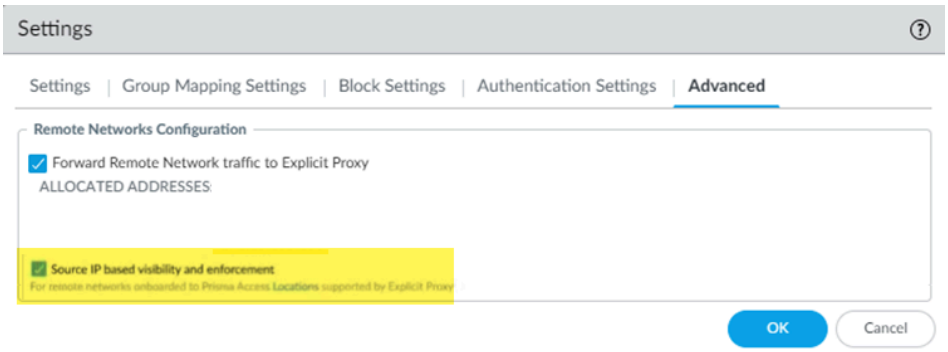
1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—Explicit Proxy (Utilisateurs mobiles—Proxy explicite)**.
2. Sélectionnez l'icône d'engrenage pour modifier les **Settings (Paramètres)**.
3. Sélectionnez **Enable Proxy Mode (Activer le mode proxy)**.



4. Pour exploiter les adresses IP privées des systèmes de vos succursales qui transfèrent du trafic vers le proxy explicite, sélectionnez **Source IP based visibility and enforcement (Visibilité et application basées sur l'IP source)** .

   Cette fonctionnalité a ces exigences :

   - Un plan de données Prisma Access minimum de 10.2.4
   - Un déploiement Prisma Access (Managed by Panorama) avec un plugin Cloud Services minimum de 4.1
   - Vous devez utiliser uniquement les emplacements réseau distants pris en charge par le proxy explicite.



5. Ajoutez une stratégie pour autoriser le trafic lié à des adresses IP anycast et unicast sur des réseaux distants. Si vous avez activé **Source IP visibility and enforcement (Visibilité et application basées sur l'IP source)**, utilisez le champ **Source IP (IP Source)** dans les Stratégies de sécurité dans le proxy explicite pour sécuriser le trafic. Vous avez besoin de stratégies supplémentaires dans les réseaux distants.
6. (Facultatif) Sous **Authentication Settings (Paramètres d'authentification)**, entrez toutes les adresses IP à partir desquelles le trafic HTTP ou Cross-Origin Resource Sharing

 ©2025 Palo Alto Networks, Inc.

(CORS) non déchiffré doit être autorisé vers le **Trusted Source Address Auth Bypass (Contournement d'authentification d'adresse source fiable)**.

Ajoutez les adresses IP aux objets d'adresse basés sur l'adresse IP et **Add (Ajouter)** les objets d'adresse dans le champ.

Saisissez un maximum de 100 000 adresses. Assurez-vous que l'objet d'adresse utilise uniquement des adresses IP.

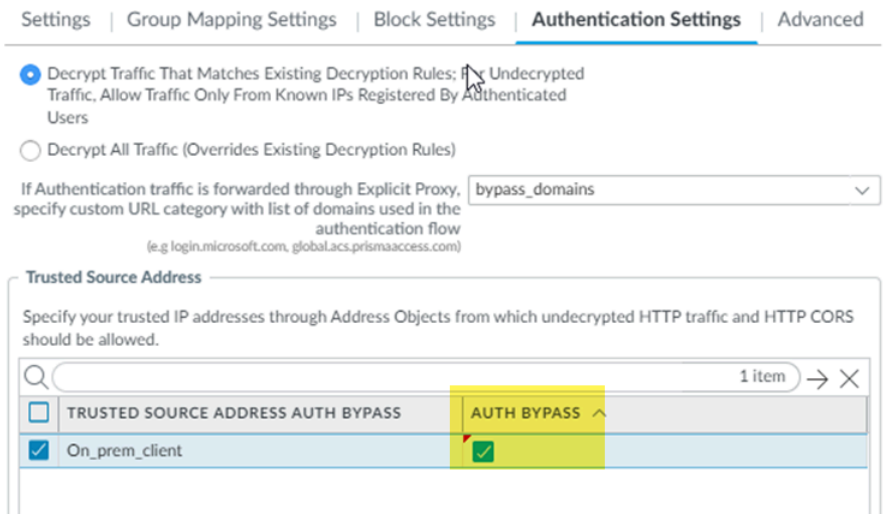
7. (Facultatif) Pour contourner l'authentification de toute adresse source fiable que vous avez saisie, sélectionnez **Auth Bypass (Contournement d'authentification)**.

   Vous pouvez utiliser **Auth Bypass (Contournement d'authentification)** avec une **Source IP based visibility and enforcement (Visibilité et application basées sur l'IP source)** pour sauter l'authentification des systèmes sans tête qui ne peuvent pas authentifier,

 ©2025 Palo Alto Networks, Inc.

configurer des stratégies de sécurité et obtenir une visibilité du trafic sur le proxy explicite Prisma Access.

Vous pouvez ajouter des adresses IP ou des sous-réseaux. Un maximum de 100 000 adresses IP sont prises en charge après extension des sous-réseaux.



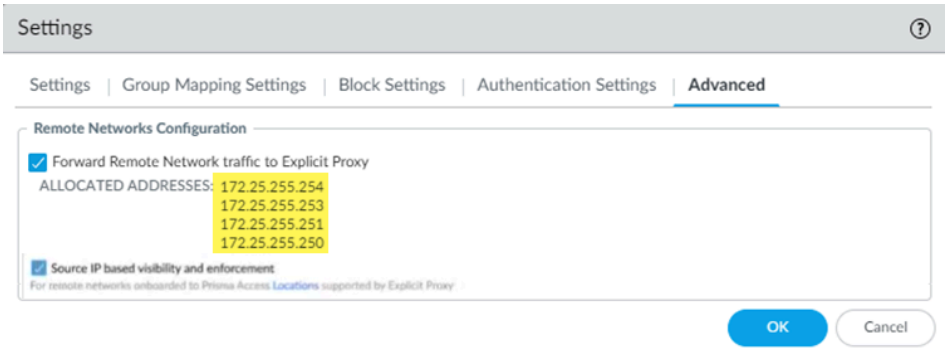
8. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**.
9. Intégrez vos emplacements réseaux distants si vous ne l'avez pas déjà fait.

   Vous devez activer Prisma Access Réseaux distants dans les emplacements qui sont pris en charge avec le proxy explicite.
10. Cliquez sur **Commit (Valider)** > **Commit and Push (Valider et transmettre)**.
11. Vous devez **Edit Selections (Modifier les sélections)** et, dans l'onglet **Prisma Access**, assurez-vous que l'option **Prisma Access for networks (Prisma Access pour les réseaux)** est sélectionnée dans **Push Scope (Étendue de la transmission)**, puis cliquez sur **OK**.
12. **Commit and Push (Validez et appliquez)** vos modifications.

    Vous devez effectuer une validation et pousser pour que vos réseaux distants pour Prisma Access récupèrent les adresses IP utilisées dans un déploiement de proxy explicite/réseau distant.
13. Revenez au proxy explicite **Settings (Paramètres)** (**Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—Explicit Proxy (Utilisateurs mobiles—Proxy explicite)** > **Settings (Paramètres)** > **Advanced (Avancé)**) et notez les **ALLOCATED ADDRESSES**

©2025 Palo Alto Networks, Inc.

(ADRESSES ALLOUÉES) qui s'affichent dans **Remote Networks Configuration (Configuration des réseaux distants)**.



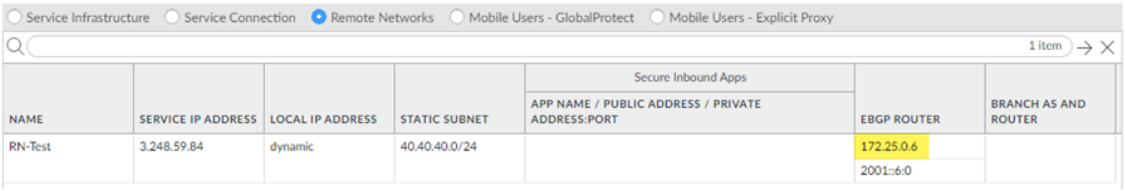
STEP 3 | (Facultatif) Trouvez l'adresse unicast que vous utilisez pour votre déploiement de proxy explicite/réseau distant.

Utilisez l'adresse IP de monodiffusion dans le fichier PAC uniquement si vous souhaitez cibler un réseau distant spécifique pour transférer le trafic vers le proxy explicite. Si vous souhaitez utiliser tous les réseaux distants déployés pour transférer le trafic vers le proxy explicite, utilisez les adresses anycast.

1. Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Remote Networks (Réseaux distants)**.
2. Notez l'adresse du **EBGP Router (Routeur EBGP)**.

   Si vous avez des adresses IPv4 et IPv6, notez l'adresse IPv4.

   Cette adresse est également connue sous le nom d'adresse de bouclage. Si vous avez effectué des modifications de configuration qui ont modifié l'adresse du routeur EBGP, vous pouvez récupérer l'adresse IP de bouclage à l'aide de l'API héritée Prisma Access.



STEP 4 | Assurez-vous que le CPE de votre réseau est correctement configuré pour les terminaux afin de transférer le trafic vers le proxy explicite via les adresses IP anycast et unicast.

Comment le proxy explicite identifie les utilisateurs

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

©2025 Palo Alto Networks, Inc.

Le proxy explicite identifie les utilisateurs dans les journaux du trafic en fonction de la manière dont les utilisateurs s'authentifient auprès du proxy, comme indiqué dans le tableau suivant.

Type d'authentification	Identification de l'utilisateur dans les journaux du trafic
Utilisateurs qui se connectent en utilisant l'authentification SAML et le décryptage	Le nom d'utilisateur.
Les utilisateurs qui se connectent depuis un autre proxy utilisant les en-têtes X-Authenticated-User (XAU)	Informations d'en-tête XAU. Le proxy explicite n'autorise que le trafic provenant d'adresses IP spécifiques qui utilisent XAU pour l'authentification. Vous créez un objet d'adresse et spécifiez les adresses IP où vous autorisez XAU pour l'authentification ; puis, ajoutez l'objet d'adresse dans le champ **Trusted Source Address (Adresse source de confiance)** lors de la configuration du proxy explicite.
Requêtes de partage de ressources entre origines authentifiées (CORS)	L'utilisateur `swg-authenticated-ip-user`. Une partie du trafic provient d'utilisateurs authentifiés dont les navigateurs ne peuvent pas envoyer de cookies ou effectuer une redirection d'authentification, comme les requêtes CORS. Dans de tels cas, le proxy explicite ajoute l'utilisateur `swg-authenticated-ip-user` aux journaux du trafic.
Trafic non décrypté (si vous avez autorisé le proxy explicite à autoriser le trafic non décrypté des adresses IP où les utilisateurs se sont précédemment authentifiés)	L'utilisateur `swg-authenticated-ip-user`. Vous pouvez spécifier un proxy explicite pour autoriser le trafic non décrypté des adresses IP où les utilisateurs se sont authentifiés ; pour ce faire, spécifiez **Decrypt traffic that matches existing decryption rules; for undecrypted traffic, allow traffic only from known IPs registered by authenticated users (Déchiffrer le trafic qui correspond aux règles de décryptage existantes ; pour le trafic non décrypté, autoriser le trafic uniquement des adresses IP connues enregistrées par des utilisateurs authentifiés)** lorsque vous configurez le proxy explicite. Dans ces configurations, le proxy explicite ajoute l'utilisateur `swg-authenticated-ip-user` aux journaux du trafic.
Trafic pour les domaines pour lesquels vous avez choisi de contourner l'authentification	L'utilisateur *swg-known-auth-bypass*. Lorsque vous configurez un proxy explicite, vous pouvez choisir de contourner l'authentification pour des domaines spécifiques. Le nom d'utilisateur pour le trafic provenant de ces domaines apparaîtra dans les journaux sous le nom *swg-known-auth-bypass*.

 ©2025 Palo Alto Networks, Inc.

Profils de transfert de proxy explicite

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access Utilisateurs mobiles

Les profils de transfert de proxy explicite vous permettent d'utiliser plusieurs fichiers PAC pour définir le trafic à transférer à Prisma Access. Les profils de transfert vous offrent également la possibilité de créer des règles de transfert faciles à utiliser au lieu de gérer la complexité de la création et de la maintenance d'un fichier PAC.

- Utiliser des profils de transfert pour définir plusieurs fichiers PAC
- Définir le trafic à transférer vers un proxy explicite avec des règles de transfert
- Associer les profils de transfert à la configuration de l'application GlobalProtect

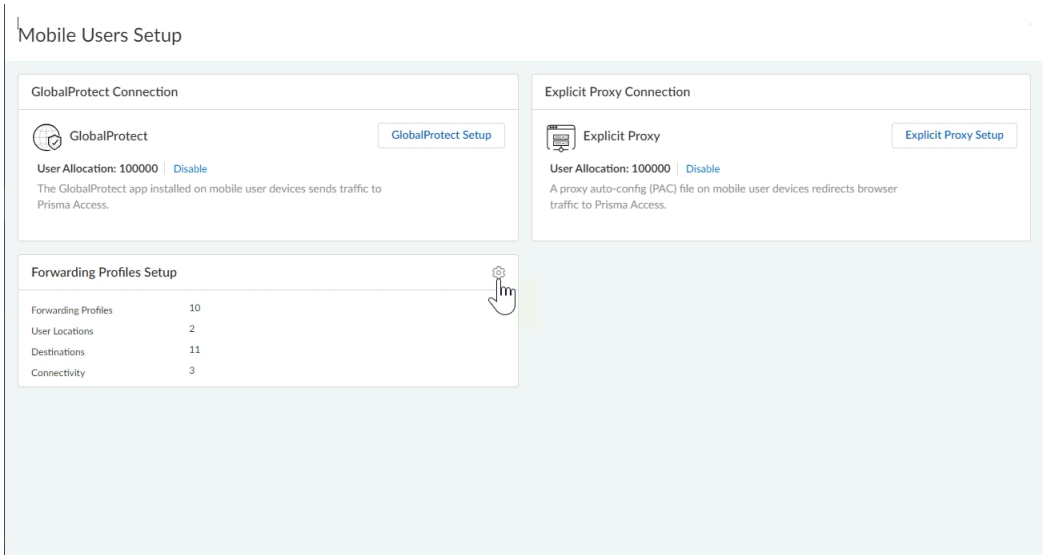
Utiliser des profils de transfert pour définir plusieurs fichiers PAC

Les profils de transfert vous permettent d'utiliser simultanément plusieurs fichiers PAC dans votre déploiement pour pouvoir définir quel trafic transférer vers Prisma Access.

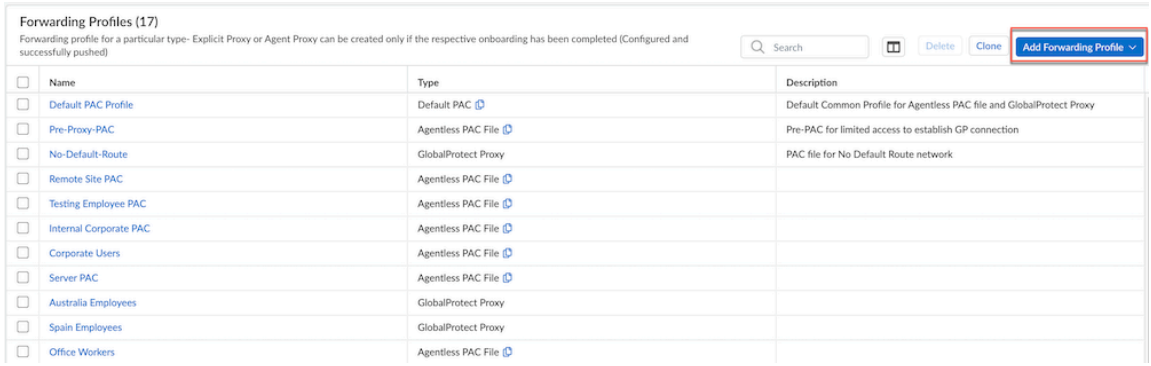
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Créez un profil de transfert.

1. Depuis Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Mobile Users (Utilisateurs mobiles)** > **Forwarding Profiles Setup (Configuration des profils de transfert)** .



2. **Add Forwarding Profile (Ajouter un profil de transfert)**.



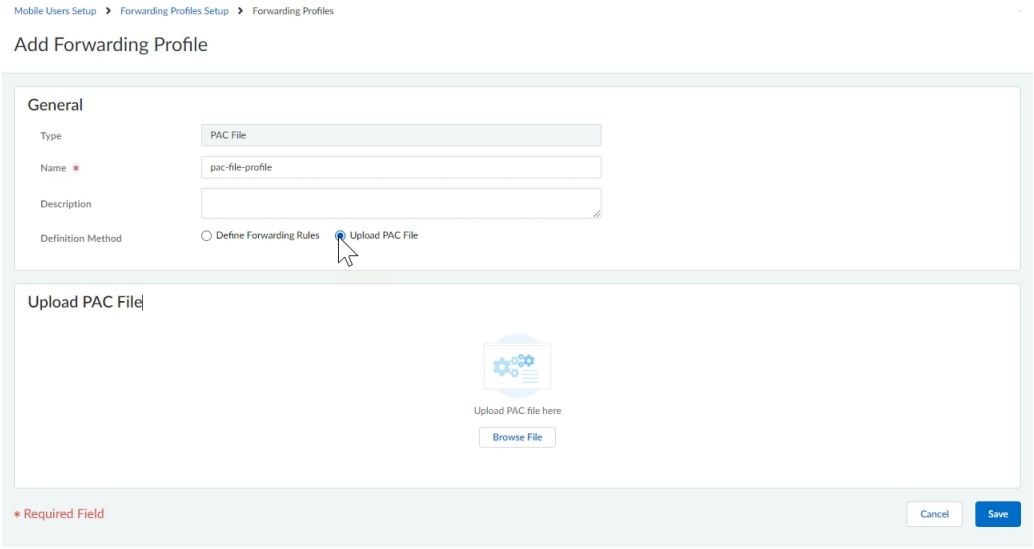
STEP 2 | Sélectionnez **PAC File (Fichier PAC)**.

Le **PAC File (Fichier PAC)** est pour le proxy explicite Prisma Access. Le **GlobalProtect Proxy (Proxy GlobalProtect)** permet d'utiliser GlobalProtect en mode proxy.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Téléchargez un fichier PAC.

1. Sélectionnez **Upload PAC File (Télécharger un fichier PAC)** pour télécharger un fichier PAC existant ou créez un fichier PAC en utilisant les directives relatives aux fichiers PAC.



2. Utilisez **Browse file (Parcourir le fichier)** pour parcourir votre système de fichiers à la recherche du fichier PAC.
3. **Enregistrez** le profil.

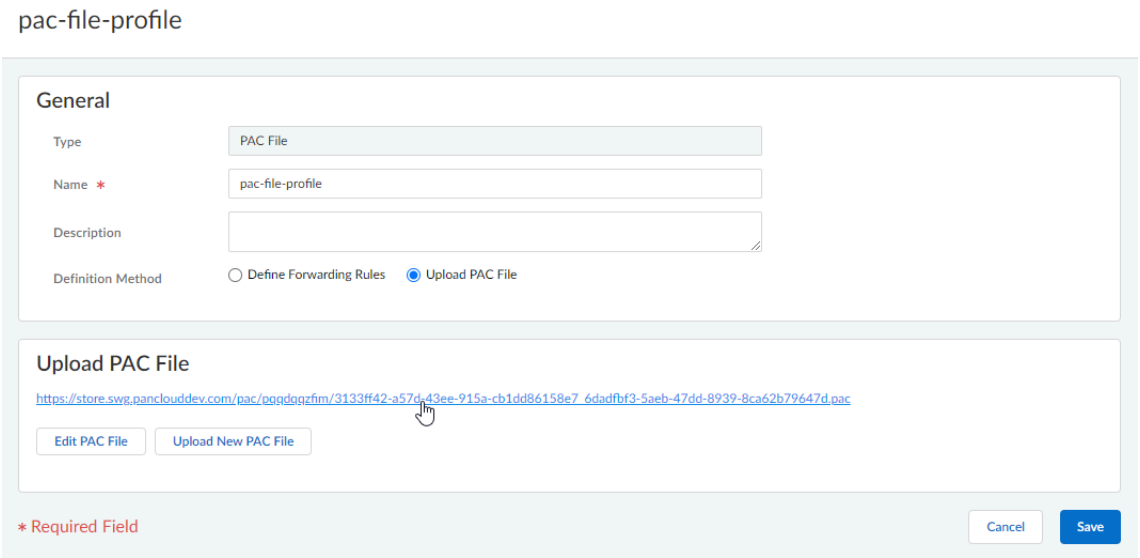
STEP 4 | Répétez les deux étapes précédentes pour créer un autre profil de transfert avec un fichier PAC différent.

Les deux fichiers PAC fonctionnent désormais simultanément dans votre déploiement.

STEP 5 | Récupérez l'URL du fichier PAC.

1. Revenez au profil sur lequel vous avez téléchargé le fichier PAC.

   Vous devriez voir l'URL où le fichier PAC est hébergé.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | (Facultatif) Modifiez le fichier PAC.

Pour apporter rapidement des modifications au fichier PAC, vous pouvez le modifier directement dans l'interface Web

1. Depuis le profil de transfert, **Edit PAC File (Modifiez le fichier PAC)**.
2. Apportez des modifications et cliquez sur **Save (Enregistrer)**.



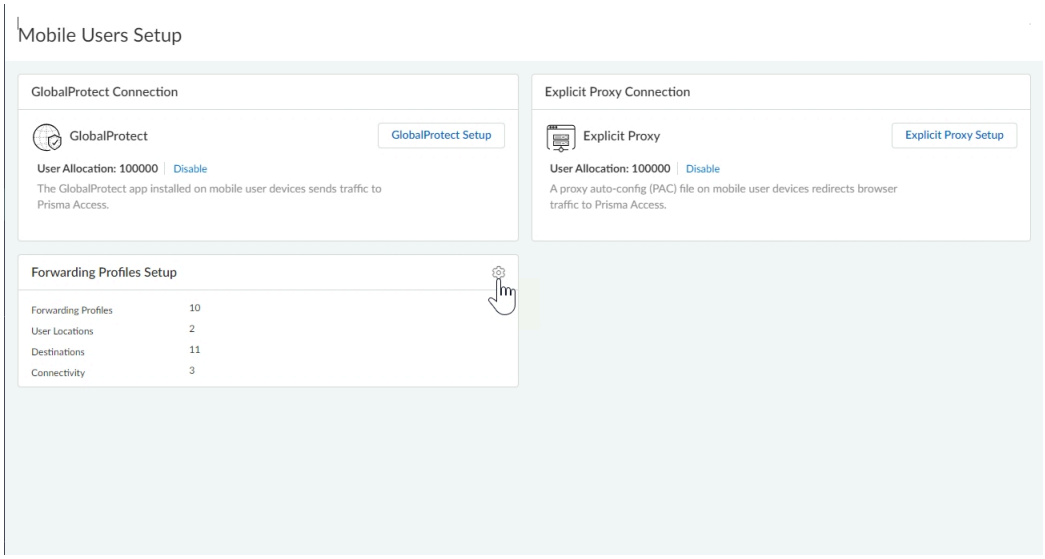
Définir le trafic à transférer vers un proxy explicite avec des règles de transfert

Au lieu de créer votre propre fichier PAC à partir de zéro, vous pouvez créer des règles de transfert simples pour générer un fichier PAC.

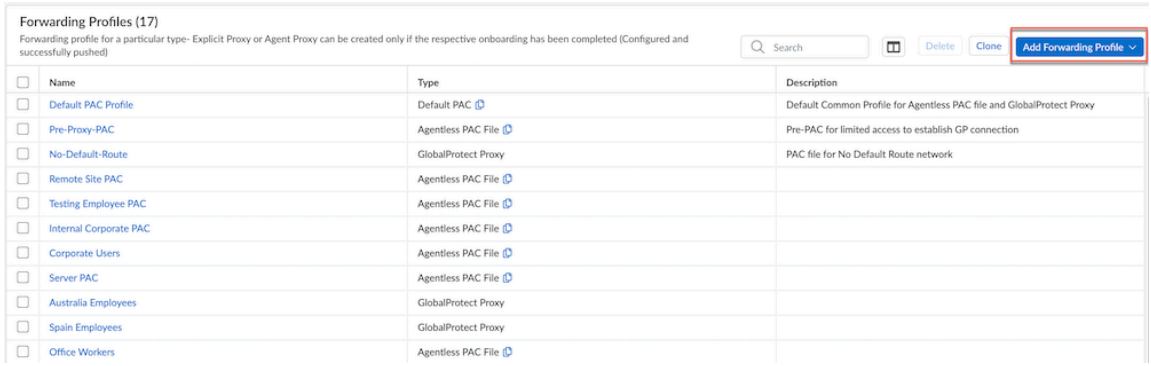
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Créez un profil de transfert.

1. Depuis Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Mobile Users (Utilisateurs mobiles)** > **Forwarding Profiles Setup (Configuration des profils de transfert)** .



2. **Add Forwarding Profile (Ajouter un profil de transfert)**.



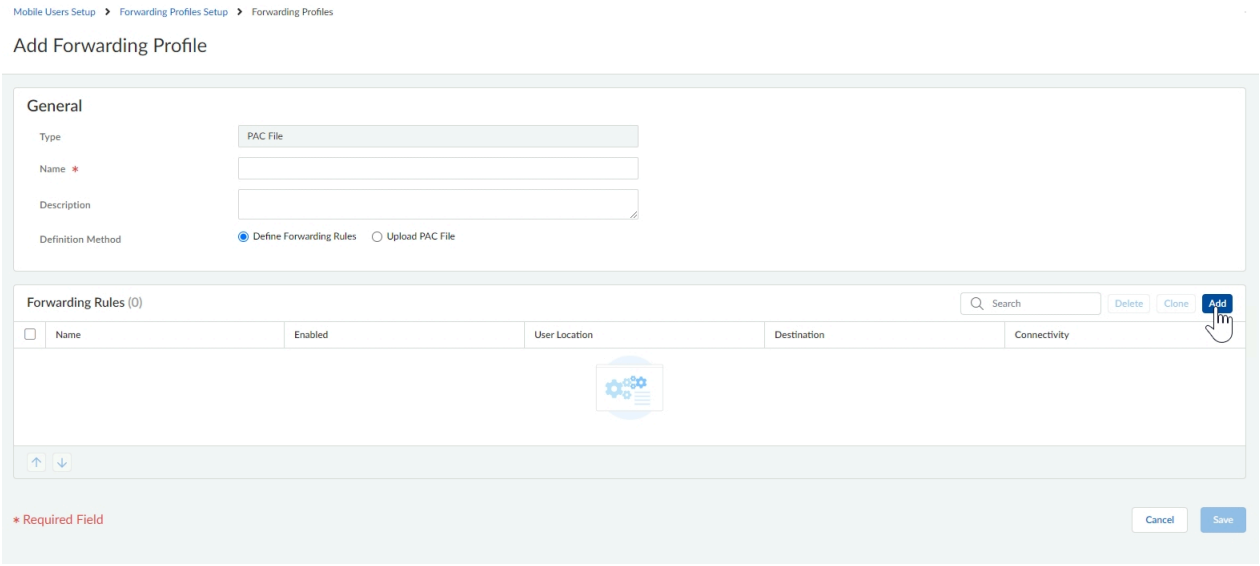
STEP 2 | Sélectionnez **PAC File (Fichier PAC)**.

Le **PAC File (Fichier PAC)** est pour le proxy explicite Prisma Access. Le **GlobalProtect Proxy (Proxy GlobalProtect)** permet d'utiliser GlobalProtect en mode proxy.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Ajoutez une règle de transfert.

1. Sélectionnez **Add (Ajouter)**.



2. Remplissez les champs obligatoires :

Nom	Nom du profil.
Emplacements des utilisateurs	Emplacement des utilisateurs pour lesquels vous créez la règle de transfert. Vous pouvez créer des emplacements personnalisés à partir de **Workflows (Flux de travail** > **Prisma Access Setup (Configuration de Prisma Access)** > **Mobile Users (Utilisateurs mobiles)** > **Forwarding Profiles Setup (Configuration des profils de transfert)** > **User Locations (Emplacements des utilisateurs)**. *Vous ne pouvez pas utiliser de caractères génériques lors de la configuration d'emplacements d'utilisateurs personnalisés en fonction de l'adresse IP.*
Destinations	Destination du trafic Web. Vous pouvez sélectionner parmi des destinations prédéfinies ou créer des destinations personnalisées à partir de **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Mobile Users (Utilisateurs mobiles)** > **Forwarding**

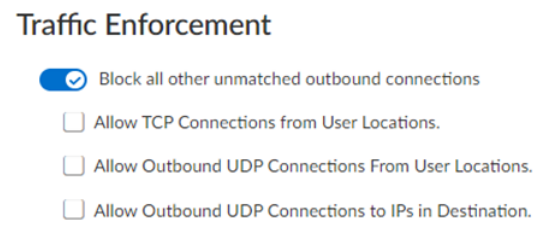
 ©2025 Palo Alto Networks, Inc.

	Profiles Setup (Configuration des profils de transfert) > **Destinations**.
Connectivité	**Direct** fait en sorte que le trafic contourne le proxy. **Global Proxy (proxy global)** fait passer le trafic via le proxy.

3. Sélectionnez **Add (Ajouter)** lorsque vous avez terminé.
4. Activez **Traffic Enforcement (Application du trafic)** si vous souhaitez bloquer tout le trafic sortant (tel que UDP) qui ne correspond pas aux règles de transfert. Cette option nécessite la version 6.3.1 de l'agent GlobalProtect et est désactivée par défaut. Si vous avez des applications qui nécessitent que vous autorisiez les connexions UDP, vous pouvez ajouter ces exceptions à l'aide des objets **Emplacement de l'utilisateur** ou **Destination**.

   Vous pouvez personnaliser vos actions de blocage comme suit :

   - Bloquez toutes les connexions sortantes UDP depuis les terminaux.
   - Autoriser TCP à partir d'emplacements spécifiques. Par exemple, vous pouvez autoriser tout le trafic TCP de votre bureau.
   - Autoriser UDP à partir d'emplacements spécifiques. Par exemple, vous pouvez autoriser tout le trafic TCP de votre bureau.
   - Si certaines applications nécessitent des connexions UDP, vous pouvez autoriser les connexions UDP sortantes vers des destinations spécifiques.

5. **Save (Enregistrez)** le profil avec la règle de transfert que vous avez créée.

   Le profil s'affiche dans votre liste de profils de transfert. Lorsque vous l'ouvrez, vous voyez une URL vers le fichier PAC généré à partir de la règle. **View PAC file (Consultez le fichier PAC)** pour voir son contenu.

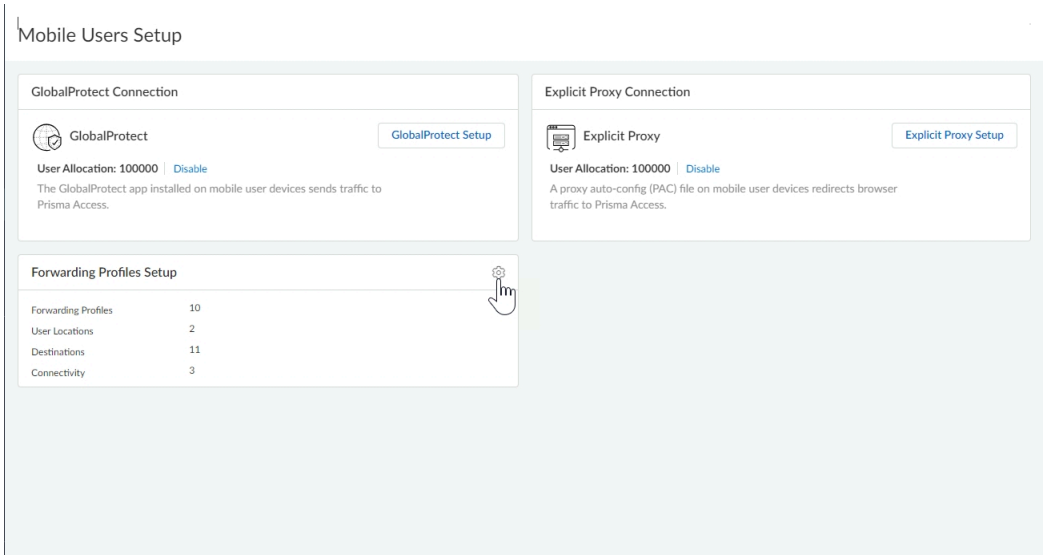
Associer les profils de transfert à la configuration de l'application GlobalProtect

Vous pouvez utiliser les profils de transfert pour simplifier la configuration de votre proxy d'application GlobalProtect.

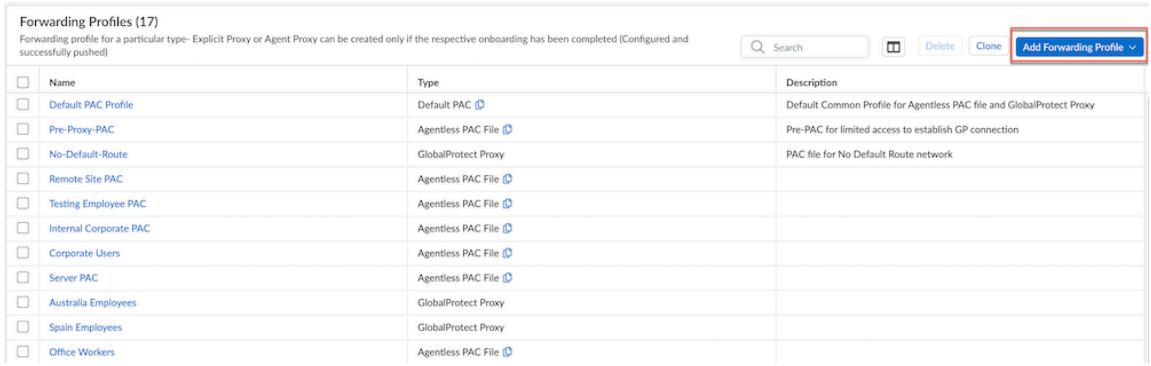
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Créez un profil de transfert.

1. Depuis Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Mobile Users (Utilisateurs mobiles)** > **Forwarding Profiles Setup (Configuration des profils de transfert)** .



2. **Add Forwarding Profile (Ajouter un profil de transfert)**.



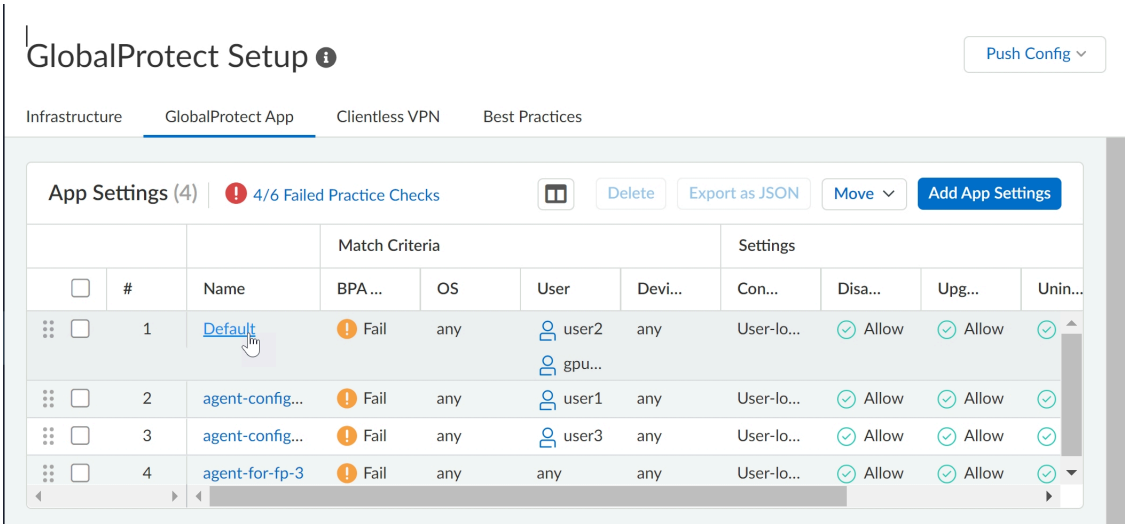
STEP 2 | Sélectionnez **GlobalProtect Proxy (Proxy GlobalProtect)**.

STEP 3 | Configurez le profil de transfert en téléchargeant un fichier PAC ou en créant des règles de transfert.

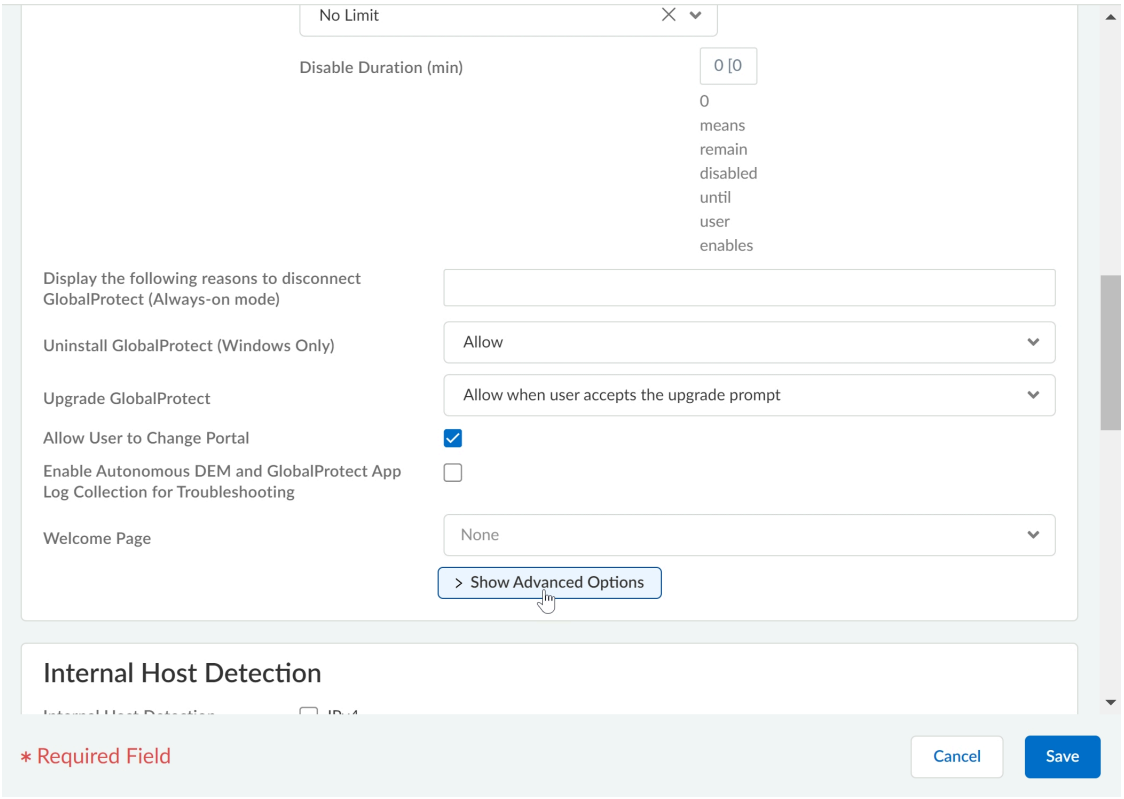
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Ajoutez le profil de transfert à votre configuration de proxy GlobalProtect app.

1. Sélectionnez **Workflows (Flux de travail > Prisma Access Setup (Configuration de Prisma Access) > GlobalProtect > GlobalProtect App (Application GlobalProtect)**.
2. Sélectionnez un fichier de configuration.



3. Sous App Configuration (Configuration de l'application), sélectionnez **Show Advanced Options (Afficher les options avancées)**.

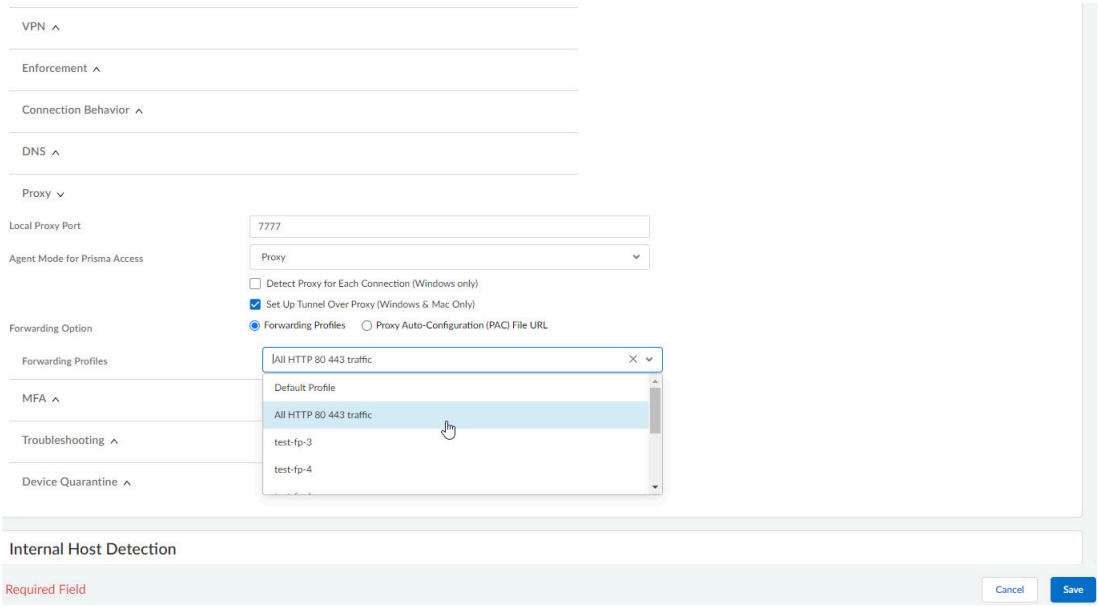


4. Développez les paramètres **Proxy**.
5. Sélectionnez **Proxy** ou **Tunnel and Proxy (Tunnel et proxy)** en fonction de votre mode d'agent GlobalProtect

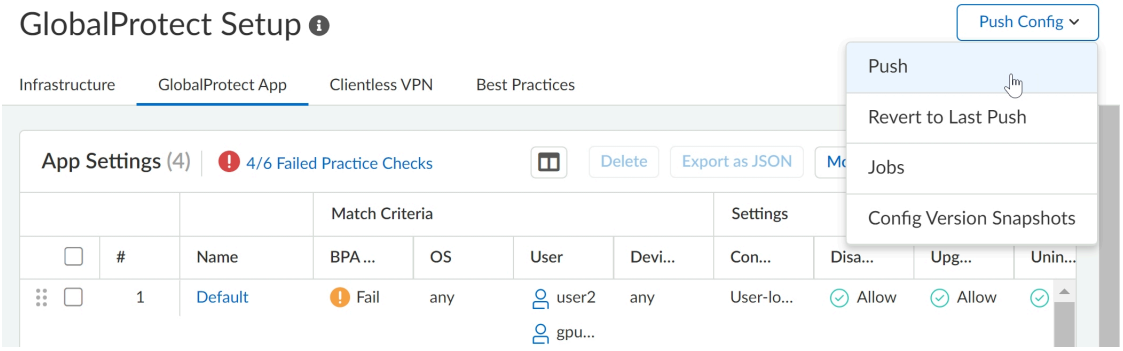
 ©2025 Palo Alto Networks, Inc.

*Vous ne pouvez pas ajouter de profil de transfert si vous sélectionnez le mode **Tunnel**.*

6. Sélectionnez **Forwarding Profiles (Profils de transfert)** et choisissez le profil de transfert que vous souhaitez utiliser.



7. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.
8. Sélectionnez **Push Config (Transmettre la configuration)** > **Push (Transmettre)**.



Directives relatives aux fichiers PAC

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

Directives relatives aux fichiers PAC (Strata Cloud Manager)

Utilisez les directives et exigences suivantes lors de la configuration du fichier PAC à utiliser avec le proxy explicite :

- Notez que si vous utilisez l'agent GlobalProtect en mode proxy, l'agent distribuera le fichier PAC à vos hôtes. L'agent accède au fichier PAC via HTTPS. Le fichier PAC est public.
- Les fichiers PAC dirigent le trafic utilisateur vers le proxy explicite.
- Vous ne pouvez héberger qu'un seul fichier PAC à utiliser avec Prisma Access et le fichier PAC du proxy explicite est hébergé aux États-Unis. Si vous avez besoin d'un autre accès au fichier PAC en dehors des États-Unis, vous pouvez héberger le fichier PAC dans votre entreprise.
- Pour accéder au fichier PAC, vérifiez que vos terminaux peuvent atteindre les adresses IP suivantes :
  - 34.111.7.85
  - 34.160.172.204
  - 34.110.206.116
  - 34.95.107.244
  - 34.149.8.36

  Si vous avez un Réseau sans itinéraire par défaut, vous devez ajouter des itinéraires pour que ces adresses IP puissent accéder au fichier PAC.
- Seul le format texte ASCII est pris en charge pour les fichiers PAC. Palo Alto Networks vous recommande de créer et d'enregistrer le fichier PAC dans un éditeur de texte tel que VI ou Vim.
- Une fois que vous avez créé votre configuration de proxy explicite et que vous avez validé et transmis vos modifications, chargez votre fichier PAC ou spécifiez votre configuration PAC dans l'éditeur de fichiers PAC.
- Vous devez avoir au moins une URL de proxy explicite au début de l'instruction `return"PROXY foo.proxy.prismaaccess.com:8080";` pour le trafic entrant vers Prisma Access. Utilisez soit un domaine configuré utilisé lorsque vous transmettez vos modifications, soit une adresse IPv4 valide ou un mot-clé DIRECT tel que PROXY `paloaltonetworks-245139.proxy.prismaaccess.com:8080` ou PROXY `1.2.3.4:8080`, et ainsi de suite.
- Si le proxy n'est pas contourné, vous devez alors fournir un mot-clé PROXY. Une instruction de proxy valide est requise si aucun mot-clé `DIRECT` n'est configuré pour le contournement de proxy.
- Si une instruction PROXY valide est trouvée avant une instruction PROXY non valide, le proxy explicite ignore le contrôle de validité sur toutes les instructions PROXY après la première. Par exemple, un fichier PAC avec l'instruction valide PROXY `paloaltonetworks-245139.proxy.prismaaccess.com:8080` suivie de l'instruction non valide PROXY `foo.proxy.prismaaccess.com:8080` serait considéré comme valide, car le proxy explicite ignore le contrôle de validité de `foo .proxy.prismaaccess.com:8080`.
- Si vous utilisez une instruction PROXY pour que le trafic ACS contourne le proxy Prisma Access, l'instruction PROXY ne doit pas utiliser l'URL de proxy explicite. Dans cette configuration, le proxy explicite donne un message d'erreur, mais vous permet de charger le

 ©2025 Palo Alto Networks, Inc.

fichier PAC. Vous pouvez diriger le trafic ACS vers d'autres proxys à l'aide d'un FQDN ou d'une adresse IPv4 valide, ou directement vers Internet, à l'aide du mot clé `DIRECT`.

- Seules les adresses IPv4 sont prises en charge dans les instructions PROXY. N'utilisez pas d'adresses IPv6 dans les instructions PROXY.
- La taille maximale d'un fichier PAC est de 750 Ko.
- Si le trafic ACS/IdP doit passer par un proxy explicite, ajoutez ces domaines à une liste de contournement d'authentification et à une Règle de politique sans décryptage.
- Si vous configurez le proxy explicite dans un environnement d'itinéraire par défaut, vous devez exclure le portail, la passerelle et les FQDN SAML. Vous pouvez utiliser le fichier PAC pour contourner les FQDN.
- Vous ne pouvez pas supprimer un fichier PAC une fois que vous l'avez chargé. Vous pouvez toutefois charger un nouveau fichier PAC ou le modifier dans l'éditeur de fichiers PAC pour remplacer le fichier existant.

Le proxy explicite vous fournit un exemple de fichier PAC que vous pouvez modifier et utiliser comme fichier PAC pour votre déploiement de proxy explicite. L'exemple de fichier PAC fourni par Prisma Access contient les données suivantes :

```
function FindProxyForURL(url, host) { /* Bypass localhost and Private
 IPs */ var resolved_ip = dnsResolve(host); if (isPlainHostName(host)
 || shExpMatch(host, "*.local") || isInNet(resolved_ip, "10.0.0.0",
 "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0")
 || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||
 isInNet(resolved_ip, "127.0.0.0", "255.255.255.0")) return
 "DIRECT"; /* Bypass FTP */ if (url.substring(0,4) == "ftp:")
 return "DIRECT"; /* Bypass SAML, e.g. Okta */ if (shExpMatch(host,
 "*.okta.com") || shExpMatch(host, "*.oktacdn.com"))
 return "DIRECT"; /* Bypass ACS */ if (shExpMatch(host,
 "*.acs.prismaaccess.com")) return "DIRECT"; /* Forward to Prisma
 Access */ return "PROXY foo.proxy.prismaaccess.com:8080";
```

Si vous souhaitez utiliser le fichier PAC par défaut fourni par Prisma Access, vous pouvez éventuellement modifier les champs du fichier PAC comme décrit dans le tableau suivant.

Texte	Description
`var resolved_ip = dnsResolve(host); ... retourne « DIRECT » ;`	Si vous ne modifiez pas les données de ce fichier, les noms d'hôte et adresses IP suivants contournent le proxy explicite : • `if (isPlainHostName(host)` : contourne le proxy explicite pour les noms d'hôte qui ne contiennent pas de points (par exemple, http://intranet). • `shExpMatch(host, "*.local") ||` : contourne le proxy pour tous les noms d'hôte hébergés dans le réseau interne (localhost).

 ©2025 Palo Alto Networks, Inc.

Texte	Description
	• `isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") || isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))` : contourne le proxy explicite pour toutes les adresses IP qui se trouvent dans la plage d'adresses IP privée ou de bouclage.
`if (url.substring(0,4) == "ftp:" ) retourne « DIRECT » ;`	Contourne le proxy explicite pour les sessions FTP.
`if (shExpMatch(host, "*.okta.com ") || shExpMatch(host, "*.oktacd n.com")) retourne « DIRECT » ;`	Contourne le proxy explicite pour l'IdP SAML. Veillez à ajouter tous les FQDN utilisés par l'IdP. Si vous utilisez Okta comme l'IdP utilisé pour l'authentification SAML, saisissez **`*.okta.com`** et **`*.oktacdn.com`**.
`if (shExpMatch(host, "*.acs.pris maaccess.com")) retourne « DIREC T » ;`	Contourne le proxy explicite pour le Service de cache d'authentification (ACS) Prisma Access. Au lieu d'utiliser un caractère générique, vous pouvez ajouter le **ACS FQDN (FQDN ACS)** pour votre déploiement. Recherchez ce FQDN sous **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Mobile Users—Explicit Proxy (Utilisateurs mobiles : proxy explicite)** > **ACS FQDN (FQDN ACS)**.
`retourne « PROXY foo.proxy.prism aaccess.com:8080 »`	Contourne le proxy explicite pour l'URL du proxy explicite. Vous devez avoir au moins une URL de proxy explicite à l'instruction `return"PROXY foo.proxy.prismaaccess.com:8080";` pour le trafic entrant vers Prisma Access. Utilisez soit un domaine configuré utilisé lorsque vous transmettez vos modifications, soit une adresse IPv4 valide ou un mot-clé DIRECT tel que PROXY

 ©2025 Palo Alto Networks, Inc.

Texte	Description
	`paloaltonetworks-245139.proxy.prismaaccess.c` ou PROXY `1.2.3.4:8080`.

Directives relatives aux fichiers PAC (Panorama)

Utilisez les directives et exigences suivantes lors de la configuration du fichier PAC à utiliser avec le proxy explicite :

- Notez que si vous utilisez l'agent GlobalProtect en mode proxy, l'agent distribuera le fichier PAC à vos hôtes. L'agent accède au fichier PAC via HTTPS. Le fichier PAC est public.
- Les fichiers PAC dirigent le trafic utilisateur vers le proxy explicite.
- Vous ne pouvez héberger qu'un seul fichier PAC à utiliser avec Prisma Access et le fichier PAC du proxy explicite est hébergé aux États-Unis. Si vous avez besoin d'un autre accès au fichier PAC en dehors des États-Unis, vous pouvez héberger le fichier PAC dans votre entreprise.
- Pour accéder au fichier PAC, vérifiez que vos terminaux peuvent atteindre les adresses IP suivantes :
  - 34.111.7.85
  - 34.160.172.204
  - 34.110.206.116
  - 34.95.107.244
  - 34.149.8.36
- Seul le format texte ASCII est pris en charge pour les fichiers PAC. Palo Alto Networks vous recommande de créer et d'enregistrer le fichier PAC dans un éditeur de texte tel que VI ou Vim.
- Chargez le fichier PAC après avoir créé votre configuration de proxy explicite et validé et transmis vos modifications. Après avoir chargé votre fichier PAC, une opération de validation et de transmission n'est pas requise.
- Vous devez avoir au moins une URL de proxy explicite au début de l'instruction `return"PROXY foo.proxy.prismaaccess.com:8080";` pour le trafic entrant vers Prisma Access. Utilisez soit un domaine configuré utilisé lorsque vous transmettez vos modifications, soit une adresse IPv4 valide ou un mot-clé DIRECT tel que PROXY `paloaltonetworks-245139.proxy.prismaaccess.com:8080` ou PROXY `1.2.3.4:8080`, et ainsi de suite.
- Si le proxy n'est pas contourné, vous devez alors fournir un mot-clé PROXY. Une instruction de proxy valide est requise si aucun mot-clé `DIRECT` n'est configuré pour le contournement de proxy.
- Si une instruction PROXY valide est trouvée avant une instruction PROXY non valide, le proxy explicite ignore le contrôle de validité sur toutes les instructions PROXY après la première. Par exemple, un fichier PAC avec l'instruction valide PROXY `paloaltonetworks-245139.proxy.prismaaccess.com:8080` suivie de l'instruction non valide PROXY `foo.proxy.prismaacess.com:8080` serait considéré comme valide, car le proxy explicite ignore le contrôle de validité de `foo .proxy.prismaacess.com:8080`.

 ©2025 Palo Alto Networks, Inc.

- Si vous utilisez une instruction PROXY pour que le trafic ACS contourne le proxy Prisma Access, l'instruction PROXY ne doit pas utiliser l'URL de proxy explicite. Dans cette configuration, le proxy explicite donne un message d'erreur, mais vous permet de charger le fichier PAC. Vous pouvez diriger le trafic ACS vers d'autres proxys à l'aide d'un FQDN ou d'une adresse IPv4 valide, ou directement vers Internet, à l'aide du mot clé `DIRECT`.
- Seules les adresses IPv4 sont prises en charge dans les instructions PROXY. N'utilisez pas d'adresses IPv6 dans les instructions PROXY.
- La taille maximale d'un fichier PAC est de 256 Ko.
- Si le trafic ACS/IdP doit passer par un proxy explicite, ajoutez ces domaines à une liste de contournement d'authentification et à une Règle de politique sans décryptage.
- Si vous configurez le proxy explicite dans un environnement d'itinéraire par défaut, vous devez exclure le portail, la passerelle et les FQDN SAML. Vous pouvez utiliser le fichier PAC pour contourner les FQDN.
- Vous ne pouvez pas supprimer un fichier PAC une fois que vous l'avez chargé. Vous pouvez cependant charger un nouveau fichier PAC pour remplacer le fichier existant.
- Si vous modifiez l'URL du proxy explicite dans Prisma Access sans modifier le fichier PAC pour refléter la modification, la modification ne sera pas appliquée. Vous devez charger un nouveau fichier PAC spécifiant la nouvelle URL de proxy explicite.

Le proxy explicite vous fournit un exemple de fichier PAC que vous pouvez modifier et utiliser comme fichier PAC pour votre déploiement de proxy explicite. L'exemple de fichier PAC fourni par Prisma Access contient les données suivantes :

```
function FindProxyForURL(url, host) { /* Bypass localhost and Private
 IPs */ var resolved_ip = dnsResolve(host); if (isPlainHostName(host)
 || shExpMatch(host, "*.local") || isInNet(resolved_ip, "10.0.0.0",
 "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0")
 || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||
 isInNet(resolved_ip, "127.0.0.0", "255.255.255.0")) return
 "DIRECT"; /* Bypass FTP */ if (url.substring(0,4) == "ftp:")
 return "DIRECT"; /* Bypass SAML, e.g. Okta */ if (shExpMatch(host,
 "*.okta.com") || shExpMatch(host, "*.oktacdn.com"))
 return "DIRECT"; /* Bypass ACS */ if (shExpMatch(host,
 "*.acs.prismaaccess.com")) return "DIRECT"; /* Forward to Prisma
 Access */ return "PROXY foo.proxy.prismaaccess.com:8080";
```

Si vous souhaitez utiliser le fichier PAC par défaut fourni par Prisma Access, vous pouvez éventuellement modifier les champs du fichier PAC comme décrit dans le tableau suivant.

Texte	Description
`var resolved_ip = dnsResolve(hos t); ... retourne « DIRECT » ;`	Si vous ne modifiez pas les données de ce fichier, les noms d'hôte et adresses IP suivants contournent le proxy explicite : • `if (isPlainHostName(host)` : contourne le proxy explicite pour les noms d'hôte qui ne contiennent pas de points (par exemple, http://intranet).

 ©2025 Palo Alto Networks, Inc.

Texte	Description
	• `shExpMatch(host, "*.local") ||`: contourne le proxy pour tous les noms d'hôte hébergés dans le réseau interne (localhost). • `isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") || isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))`: contourne le proxy explicite pour toutes les adresses IP qui se trouvent dans la plage d'adresses IP privée ou de bouclage.
`if (url.substring(0,4) == "ftp:" ) retourne « DIRECT » ;`	Contourne le proxy explicite pour les sessions FTP.
`if (shExpMatch(host, "*.okta.com ") || shExpMatch(host, "*.oktacd n.com")) retourne « DIRECT » ;`	Contourne le proxy explicite pour l'IdP SAML. Veillez à ajouter tous les FQDN utilisés par l'IdP. Si vous utilisez Okta comme l'IdP utilisé pour l'authentification SAML, saisissez **`*.okta.com`** et **`*.oktacdn.com`**.
`if (shExpMatch(host, "*.acs.pris maaccess.com")) retourne « DIREC T » ;`	Contourne le proxy explicite pour le Service de cache d'authentification (ACS) Prisma Access. Au lieu d'utiliser un caractère générique, vous pouvez ajouter le **ACS FQDN (FQDN ACS)** pour votre déploiement. Recherchez ce FQDN sous **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Mobile Users—Explicit Proxy (Utilisateurs mobiles : proxy explicite)** > **ACS FQDN (FQDN ACS)**.
`retourne « PROXY foo.proxy.prism aaccess.com:8080 »`	Contourne le proxy explicite pour l'URL du proxy explicite. Vous devez avoir au moins une URL de proxy explicite à l'instruction `return"PROXY foo.proxy.prismaaccess.com:8080";` pour le trafic entrant vers Prisma Access. Utilisez soit un domaine configuré

 ©2025 Palo Alto Networks, Inc.

Texte	Description
	utilisé lorsque vous transmettez vos modifications, soit une adresse IPv4 valide ou un mot-clé DIRECT tel que PROXY `paloaltonetworks-245139.proxy.prismaaccess.c` ou PROXY `1.2.3.4:8080`.

Bonnes pratiques en matière de proxy explicite

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Utilisez les bonnes pratiques recommandées lors de la mise en œuvre de votre déploiement de proxy explicite pour des performances optimales et une expérience utilisateur idéale :

- **Bonnes pratiques générales de déploiement de proxy explicite** :
  - Déployez le proxy explicite dans au moins deux régions à des fins de redondance.
  - Si tous vos utilisateurs se trouvent derrière un périphérique NAT et si le proxy explicite voit l'adresse IP du périphérique NAT comme adresse IP source, vous devez allouer une adresse IP NAT pour 500 utilisateurs mobiles.
  - Utilisez des profils de transfert pour configurer un fichier PAC.
- **Bonnes pratiques en matière de fichiers PAC** : lors de la configuration du fichier PAC, contournez toutes les URL SAML, CIE et ACS (Authentication Cache Service).
- **Bonnes pratiques d'authentification SAML** :
  - Définissez la **Cookie Lifetime (Durée de vie des cookies)** de l'authentification SAML sur 24 heures pour avoir la meilleure expérience utilisateur sans interruption d'authentification.
  - Si vous avez configuré GlobalProtect en mode proxy ou GlobalProtect en mode tunnel et proxy, définissez la **Cookie Lifetime (Durée de vie des cookies)** sur le portail GlobalProtect sur 12 heures.
- **Bonnes pratiques d'authentification Kerberos** : la taille du fichier keytab doit être inférieure à 60 Ko.
- **Bonnes pratiques relatives à la règle de politique de sécurité** : utilisez les bonnes pratiques en matière de règles de politique de sécurité en réglant l'**Action** dans les politiques sur **Deny (Déni)** au lieu de **Drop (Abandon)** ou **Reset (Réinitialisation)**. Cette action permet de libérer rapidement les ressources à l'intérieur du nœud de traitement de sécurité de proxy explicite (EP-SPN) pour des performances optimales.
- **Bonnes pratiques de décryptage** : configurez au moins une politique de décryptage et un certificat de décryptage.

 ©2025 Palo Alto Networks, Inc.

- **Bonnes pratiques en matière d'adresse IP source** : pour restreindre l'accès du proxy explicite à des adresses IP sources spécifiques, utilisez des objets spéciaux, qui incluent les objets d'adresse, les groupes d'adresses et les listes dynamiques externes (EDL).

Surveiller et dépanner le proxy explicite

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Apprenez à surveiller et à dépanner votre déploiement de proxy explicite Prisma Access.

- Strata Cloud Manager
- Panorama

Surveiller et dépanner le proxy explicite (Strata Cloud Manager)

Surveillez les détails du déploiement de proxy explicite Prisma Access pour faciliter la résolution des problèmes.

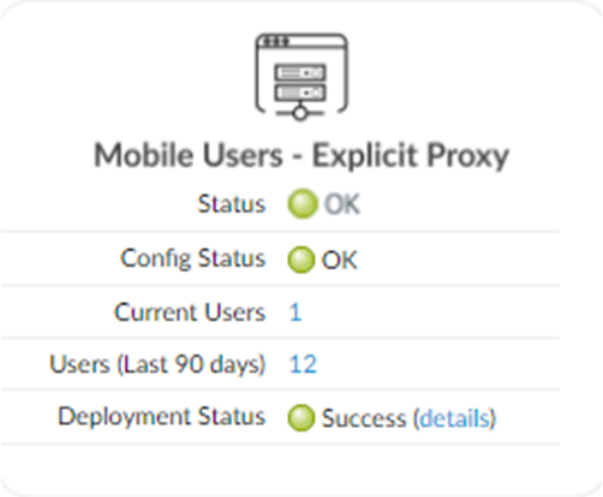
- Cliquez sur **Monitor (Surveiller)** > **Users (Utilisateurs)** et sélectionnez la méthode de connexion **Explicit Proxy (Proxy explicite)**.
- Cliquez sur **Monitor (Surveiller)** > **Users (Utilisateurs)** et sélectionnez la méthode de connexion **Explicit Proxy (Proxy explicite)** pour afficher les utilisateurs mobiles qui se connectent aux services de sécurité Prisma Access par l'intermédiaire du proxy explicite sur un navigateur web sur leur périphérique.
- Sélectionnez **Monitor (Surveiller) > Prisma Access Locations (Emplacements Prisma Access) > Explicit Proxy Mobile Users (Utilisateurs mobiles de proxy explicite)** pour avoir un aperçu de l'intégrité de tous les emplacements Prisma Access pour les utilisateurs mobiles.
- Vérifiez les journaux du trafic (**Incidents & Alerts (Incidents et alertes) > Log Viewer (Visionneuse de journaux)** et sélectionnez le type de journal **Traffic (Trafic)**) et les journaux d'authentification (**Incidents & Alerts (Incidents et alertes) > Log Viewer (Visionneuse de journaux)** et sélectionnez le type de journal **Authentication (Authentification)**) pour résoudre les problèmes liés à l'authentification.

Surveiller et dépanner le proxy explicite (Panorama)

Une fois que vous avez configuré le proxy explicite pour les utilisateurs mobiles, surveillez l'état et résolvez les problèmes en vérifiant l'état du déploiement de proxy explicite Prisma Access.

 ©2025 Palo Alto Networks, Inc.

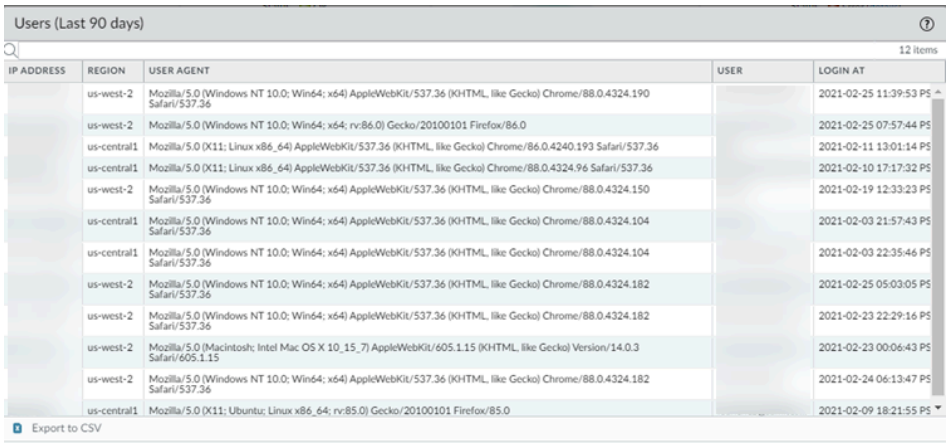
- Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Status (État)** pour voir l'état du proxy explicite.



Les champs **Status (État)** et **Config Status (État de la configuration)** indiquent si la connexion entre Prisma Access et les utilisateurs mobiles est **OK**, s'il n'est pas possible de récupérer l'état sur le tunnel (**Warning (Avertissement)**) ou si les utilisateurs mobiles ne peuvent pas se connecter au proxy explicite (**Error (Erreur)**).

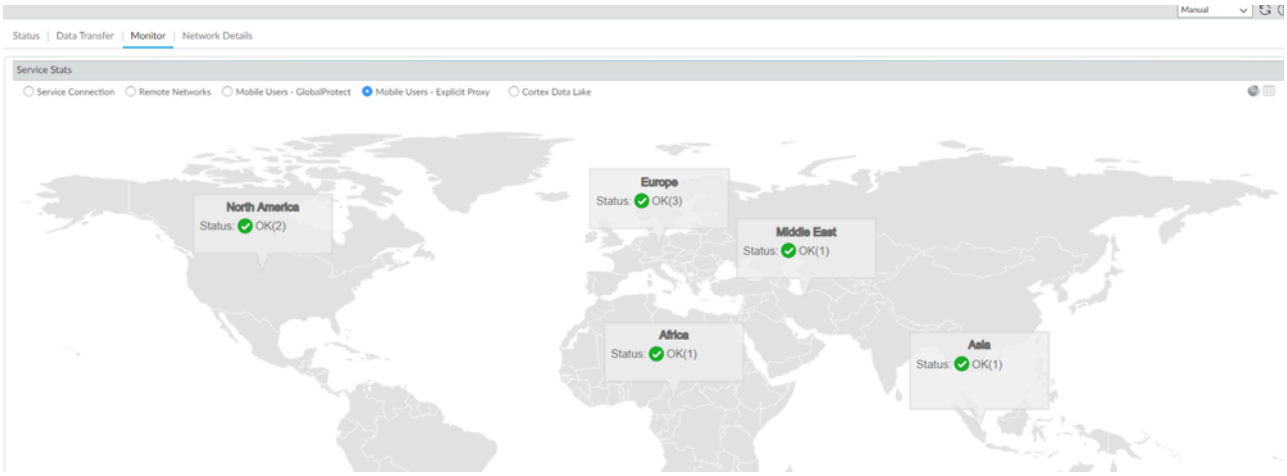
Cliquez sur le lien hypertexte à côté de **Current Users (Utilisateurs actuels)** et de **Users (Last 90 days) (Utilisateurs (90 derniers jours))** pour obtenir plus d'informations sur les utilisateurs mobiles.

- **Current Users (Utilisateurs actuels)** : le nombre actuel d'utilisateurs authentifiés qui ont parcouru du trafic au cours des cinq dernières minutes.
- **Users (Last 90 days) (Utilisateurs (90 derniers jours))** : le nombre d'utilisateurs uniques authentifiés du proxy explicite au cours des 90 derniers jours.

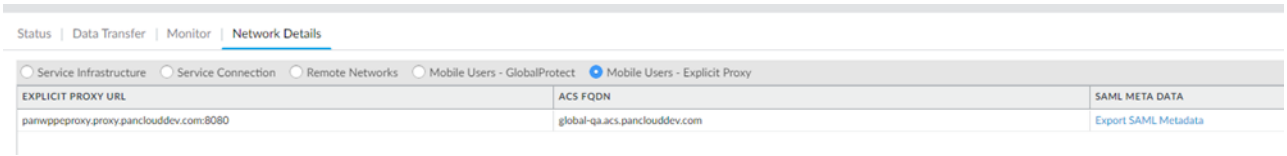


 ©2025 Palo Alto Networks, Inc.

- Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Monitor (Surveiller)** > **Mobile Users—Explicit Proxy (Utilisateurs mobiles – Proxy explicite)** pour afficher une carte des emplacements de proxy explicite déployés.



- Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Mobile Users—Explicit Proxy (Utilisateurs mobiles – Proxy explicite)** pour afficher les détails suivants :



  - **Explicit Proxy URL (URL de proxy explicite)** : l'URL utilisée pour le proxy explicite.
  - **ACS FQDN (FQDN ACS)** : le FQDN d'ACS.
  - **SAML Meta Data (Métadonnées SAML)** : les métadonnées du profil d'authentification utilisées par SAML. Vous pouvez sélectionner **Export SAML Metadata (Exporter les métadonnées SAML)** pour enregistrer le fichier de métadonnées.
- Pour résoudre les problèmes liés à l'authentification, consultez les journaux du trafic (**Monitor (Surveiller)** > **Logs (Journaux)** > **Traffic (Trafic)**) et les journaux d'authentification (**Monitor (Surveiller)** > **Logs (Journaux)** > **Authentication (Authentification)**). Le proxy explicite affiche les adresses IP et les emplacements suivants dans les journaux :
  - **Adresses IP** : si les utilisateurs mobiles contournent le FQDN ACS dans le fichier PAC, l'adresse IP affichée dans la colonne **Source** des journaux du trafic et dans la colonne **IP Address (Adresse IP)** des journaux d'authentification, lorsque vous les consultez sous **Explicit_Proxy_Device_Group**, sera identique à l'adresse IP de l'utilisateur mobile. Si les utilisateurs ne contournent pas le FQDN ACS dans le fichier PAC, l'adresse IP source correspond à l'adresse IP publique du pare-feu cloud du proxy explicite où les redirections sont dirigées vers ACS.
  - **Emplacements** : si les utilisateurs mobiles contournent le FQDN ACS dans le fichier PAC, le nom de la région affiché dans la colonne **Region (Région)** dans **Authentication Logs (Journaux d'authentification)**, **Current Users (Utilisateurs actuels)** et **Users (Last 90 days) (Utilisateurs (90 derniers jours))** correspond à l'une des cinq régions (us-west-2, us-east-1, eu-west-2, eu-west-3, ap-south-1) où ACS est déployé et indique la région dans laquelle le proxy explicite effectue les redirections à partir du navigateur du client. Si les utilisateurs

 ©2025 Palo Alto Networks, Inc.

ne contournent pas le FQDN ACS dans le fichier PAC, le nom de la région affiché dans la colonne **Region (Région)** dans **Authentication Logs (Journaux d'authentification)**, **Current Users (Utilisateurs actuels)** et **Users (Last 90 days) (Utilisateurs (90 derniers jours))** correspond à l'une des cinq régions (us-west-2, us-east-1, eu-west-2, eu-west-3, ap-south-1) où ACS est déployé et indique la région dans laquelle le proxy explicite effectue les redirections à partir du pare-feu du proxy explicite.

Paramètres de blocage pour le proxy explicite

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	• Licence Prisma Access

Pour activer cette fonctionnalité, contactez votre représentant ou partenaire de compte Palo Alto Networks, qui contactera l'équipe d'ingénierie de fiabilité du site (Site Reliability Engineering, SRE) et soumettra une requête.

Lorsque les utilisateurs accèdent à une destination Internet en utilisant un proxy explicite, la résolution DNS de la destination Internet est effectuée par le proxy explicite. Pour bloquer l'accès à une destination Internet au stade de la résolution DNS, vous pouvez utiliser les paramètres de blocage. Vous effectuez des blocages en fonction des catégories de sécurité DNS, des catégories de filtrage des URL ou des listes dynamiques externes (External Dynamic Lists, EDL).

Pour les domaines que vous bloquez, Prisma Access bloque les domaines et les utilisateurs sont redirigés vers une page de blocage lors de la requête HTTP GET (pour les sites web non cryptés) ou HTTP Connect (pour les sites web cryptés), ce qui signifie que les domaines sont bloqués lors de la requête de connexion initiale. Lorsque vous bloquez l'accès au site, l'utilisateur est redirigé vers une page de blocage après être passé par le flux d'authentification, et son nom d'utilisateur est capturé pour d'autres flux de travail forensiques et du centre des opérations de sécurité (Security Operations Center, SOC).

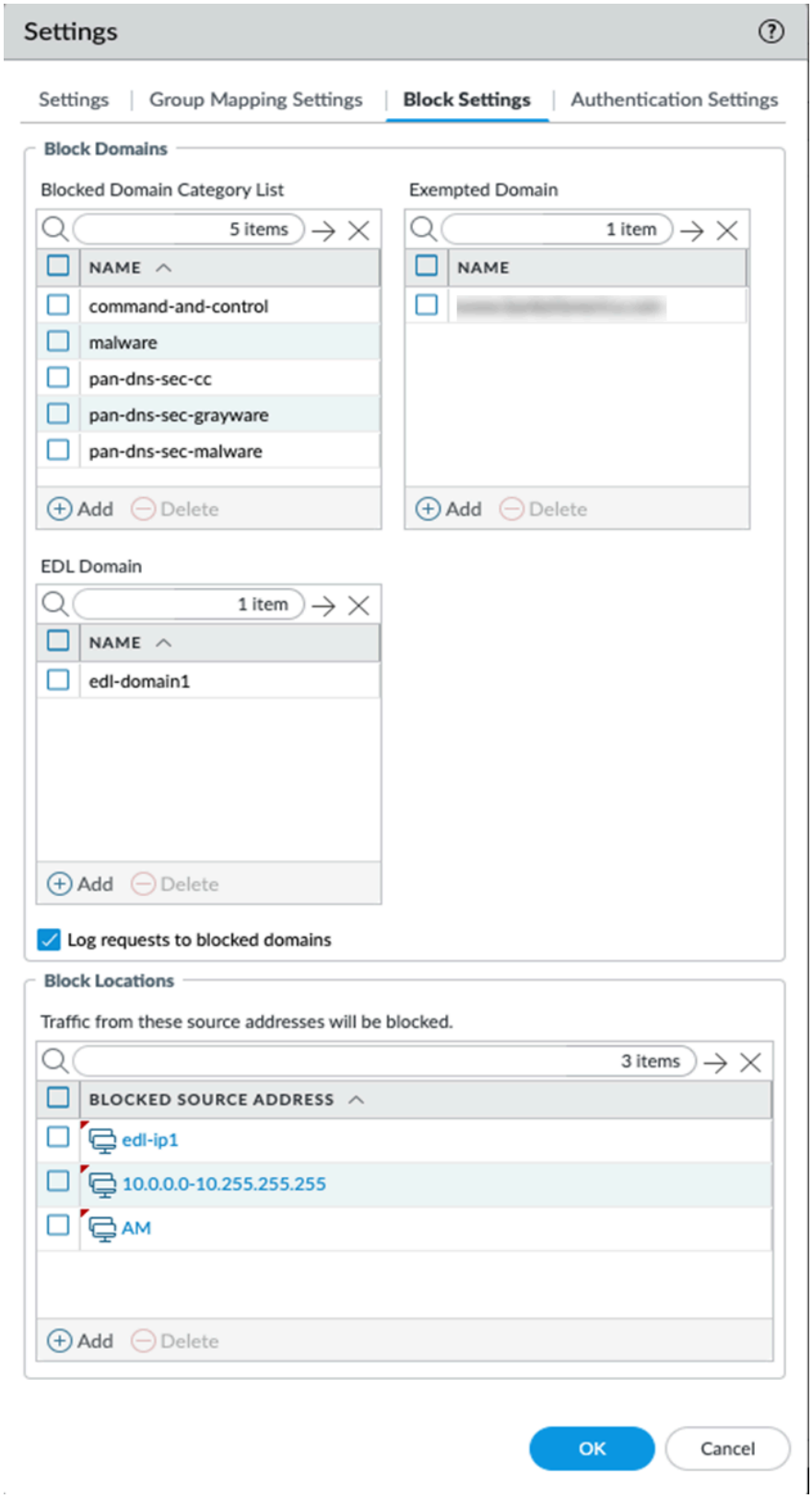
Si vous utilisez Prisma Access (Managed by Strata Cloud Manager), reportez-vous à l'étape 8 de la section Configurer un proxy explicite. Pour configurer les paramètres de blocage Prisma Access Panorama Manage, suivez les étapes suivantes.

STEP 1 | Configurez les **Block Settings (Paramètres de blocage)** pour bloquer les domaines ou les catégories de domaine.

Spécifiez les domaines ou catégories de domaines pour les sites web malveillants ou pour tous les sites web auxquels vous ne souhaitez pas que les utilisateurs accèdent. Prisma Access empêche les utilisateurs d'accéder aux URL et adresses IP que vous spécifiez dans cette zone lorsque les utilisateurs lancent une requête HTTP GET (pour les requêtes non cryptées) ou

 ©2025 Palo Alto Networks, Inc.

HTTP CONNECT (pour les requêtes cryptées). Les utilisateurs sont redirigés vers une page de blocage lorsqu'ils tentent d'accéder à des sites web bloqués.



 ©2025 Palo Alto Networks, Inc.

1. Dans **Blocked Domain Category List (Liste des catégories de domaines bloqués)**, saisissez les catégories prédéfinies à bloquer.

   Les catégories d'URL personnalisées ne sont pas prises en charge.
2. Dans **EDL Domain (Domaine EDL)**, saisissez des listes dynamiques externes (External Dynamic Lists, EDL) basées sur le domaine à bloquer.

   Vous ne pouvez sélectionner que les listes EDL présentant le type d'EDL **Dynamic Domain Lists (Listes de domaines dynamiques)** ; les listes d'adresses IP dynamiques et les listes d'URL dynamiques ne sont pas autorisées.
3. Si vous souhaitez exempter des domaines inclus dans une **Blocked Domain Category List (Liste des catégories de domaines bloqués)**, spécifiez-les comme **Exempted Domain (Domaine exempté)**.

   Tous les domaines entrés sont exemptés d'être bloqués, même s'ils apparaissent dans une catégorie de domaine que vous avez bloquée.

   - Vous pouvez entrer un maximum de 100 domaines.
   - La longueur maximale d'enregistrement du domaine est de 256 caractères.

STEP 2 | Sélectionnez les adresses IP à bloquer dans la zone **Blocked Source Address (Adresse source bloquée)**.

Vous pouvez cliquer sur **Add (Ajouter)** pour ajouter des adresses, des groupes d'adresses, des EDL basées sur des adresses IP ou des adresses IP régionales et nationales.

Utilisez les directives suivantes pour les adresses IP :

- Utilisez des EDL uniquement avec le **Type IP List (Liste IP)** ou **Predefined IP List (Liste IP prédéfinie)**.
- Utilisez uniquement les objets d'adresse avec le type **IP Range (Plage IP)** ou **IP Netmask (Masque réseau IP)**.
- Les groupes d'adresses avec appartenance à des objets dynamiques ne sont pas pris en charge.
- N'utilisez pas de régions personnalisées dans les objets d'adresse IP ; utilisez plutôt des régions prédéfinies.

STEP 3 | Sélectionnez **Log requests to blocked domains (Journaliser les requêtes de domaines bloqués)** pour que Prisma Access journalise les requêtes de domaines bloqués.

Étant donné que les journaux de domaine bloqués peuvent générer beaucoup de trafic à partir des botnets, soyez prudent lorsque vous activez la journalisation ou utilisez-la uniquement à des fins de dépannage. Si vous limitez l'utilisation de votre proxy (par exemple, si vous limitez l'utilisation à des adresses IP spécifiques), vous pouvez activer la journalisation sans restriction.

 ©2025 Palo Alto Networks, Inc.

Utiliser des objets spéciaux pour limiter le trafic Internet proxy explicite à des adresses IP spécifiques

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Le proxy explicite vous fournit des objets d'adresse, des groupes d'adresses et des listes dynamiques externes (EDL) spéciaux pour restreindre l'accès au proxy explicite à des adresses IP sources spécifiques. Lorsque vous créez un ou plusieurs de ces objets spéciaux à l'aide des noms exacts suivants, le proxy explicite autorise les adresses IP sources que vous spécifiez et bloque toutes les autres adresses IP :

- **Address Object (Objet d'adresse)** : sélectionnez **Objects (Objets)** > **Addresses (Adresses)** dans le Explicit_Proxy_Device_Group et créez un objet nommé **Palo Alto Networks Explicit Proxy Allowed Source Address (Adresse source autorisée du proxy explicite de Palo Alto Networks)**.
- **Address Group (Groupe d'adresses)** : sélectionnez **Objects (Objets)** > **Address Groups (Groupes d'adresses)** dans le Explicit_Proxy_Device_Group et créez un objet nommé **Palo Alto Networks Explicit Proxy Allowed Source Address Group (Groupe d'adresses sources autorisées du proxy explicite de Palo Alto Networks)**.
- **Liste dynamique externe (EDL)** : sélectionnez **Objects (Objets)** > **External Dynamic Lists (Listes dynamiques externes)** dans le Explicit_Proxy_Device_Group et créez une liste EDL nommée **Palo Alto Networks Explicit Proxy Allowed Source List (Liste de sources autorisées du proxy explicite de Palo Alto Networks)** et créez une liste EDL avec le type **Liste des adresses IP**.

Vous pouvez spécifier des adresses IP telles que les adresses IP de sortie des succursales.

L'utilisation de caractères génériques (tels que *.*) pour ignorer l'authentification par proxy explicite pour un grand nombre de domaines n'est pas autorisée, sauf si vous limitez votre trafic source à des adresses IP sources spécifiques à l'aide de l'un de ces objets spéciaux.

Utilisez des objets d'adresse, des groupes d'adresses ou des listes EDL séparément ou conjointement ; par exemple, vous pouvez créer uniquement un groupe d'adresses sans créer d'objet d'adresse ou d'EDL.

Accéder au centre de données à l'aide d'un proxy explicite

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	☐ (Pour le connecteur ZTNA et Colo-Connect) Prisma Access version 5.2.1 ☐ (Pour les connexions aux services) Prisma Access version 5.0

 ©2025 Palo Alto Networks, Inc.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
	❑ (Pour l'accès aux applications privées et partenaires) GlobalProtect app version 6.2 pour Windows ou macOS

Vous pouvez utiliser des connexions aux services, un connecteur ZTNA ou Colo-Connect pour accéder aux ressources de votre centre de données, telles que des listes dynamiques externes ou des applications privées et partenaires, tout en bénéficiant d'une connexion au proxy explicite.

Les adresses IP RFC 6598 suivantes ne sont pas prises en charge pour l'accès aux applications privées par un proxy explicite via des connexions aux services, Colo-Connect ou le connecteur ZTNA :

- *100.64.0.0/15*
- *100.88.0.0/15*
- *100.72.0.0/15*

Les connecteurs ZTNA existants qui utilisent ces adresses IP dans les blocs IP d'application ou les blocs IP de connecteur des connecteurs ZTNA ne peuvent pas utiliser Prisma Access Browser ou l'agent GlobalProtect en mode proxy via un proxy explicite. Vous devez contacter votre représentant Palo Alto Networks pour migrer vos adresses IP vers un autre bloc.

- Strata Cloud Manager
- Panorama

Accéder au centre de données à l'aide d'un proxy explicite (Strata Cloud Manager)

STEP 1 | Configurez une connexion aux services, Colo-Connect ou le connecteur ZTNA dans Prisma Access en fonction de vos besoins.

STEP 2 | Configurez les paramètres DNS.

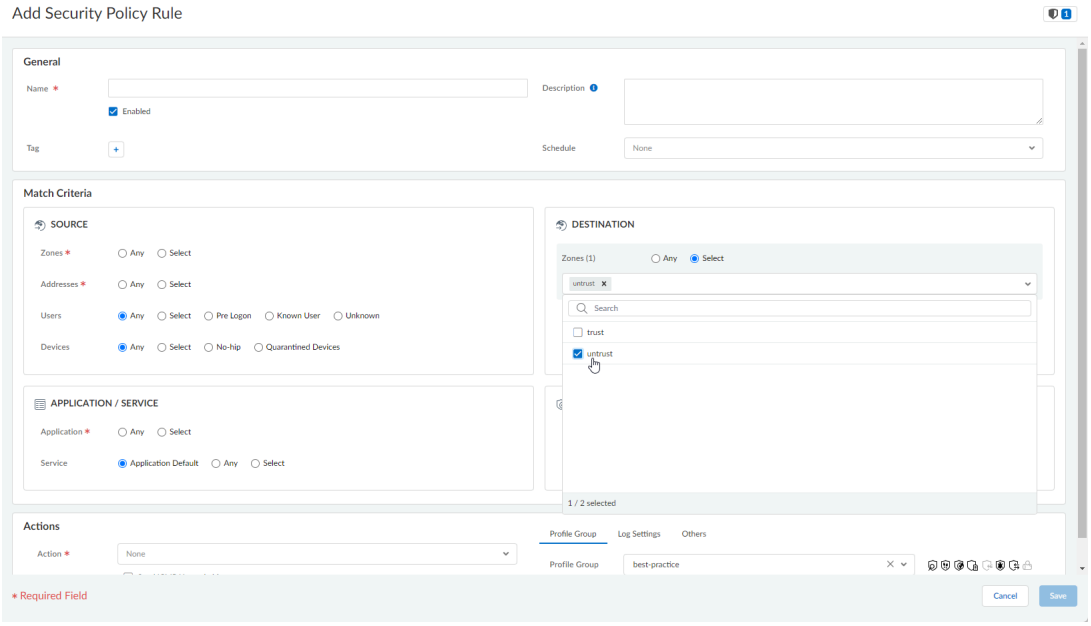
STEP 3 | Assurez-vous que les **DESTINATION Zones (Zones de DESTINATION)** pour le trafic Internet sont définies sur **untrust (non approuvées)** au lieu de **any (tout)**.

Si vous n'effectuez pas cette étape, vous risquez de créer un accès indésirable à votre centre de données.

1. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)**, définissez le paramètre **Configuration Scope (Portée de la configuration)** sur **Prisma Access** > **Mobile Users Container (Conteneur d'utilisateurs mobiles)** > **Explicit Proxy (Proxy explicite)**, puis sélectionnez **Security Policy (Politique de sécurité)** > **Security Services (Services de sécurité)**.

 ©2025 Palo Alto Networks, Inc.

2. Ouvrez une règle pour le trafic Internet.
3. Assurez-vous que le paramètre **Zones** sous **DESTINATION** est défini sur **untrust (non approuvées)**.



4. Répétez l'opération pour toutes vos règles de trafic Internet.

STEP 4 | Activez l'accès aux applications privées.

- Activez l'accès aux applications privées à l'aide de Prisma Access Browser.

  1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Infrastructure Settings (Paramètres d'infrastructure)** et **Enable (Activer)** Prisma Access Browser. Sous **Proxy URL Settings (Paramètres d'URL de proxy)**, sélectionnez **Enable Private App Access for Explicit Proxy (Activer l'accès aux applications privées pour le proxy explicite)**.

- Activez l'accès aux applications privées à l'aide d'un navigateur standard.

  1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Infrastructure Settings (Paramètres d'infrastructure)** > **Enable Agent Proxy (Activer le proxy de l'agent)** > **Enable Private App Access for Explicit Proxy (Activer l'accès aux applications privées pour le proxy explicite)**.

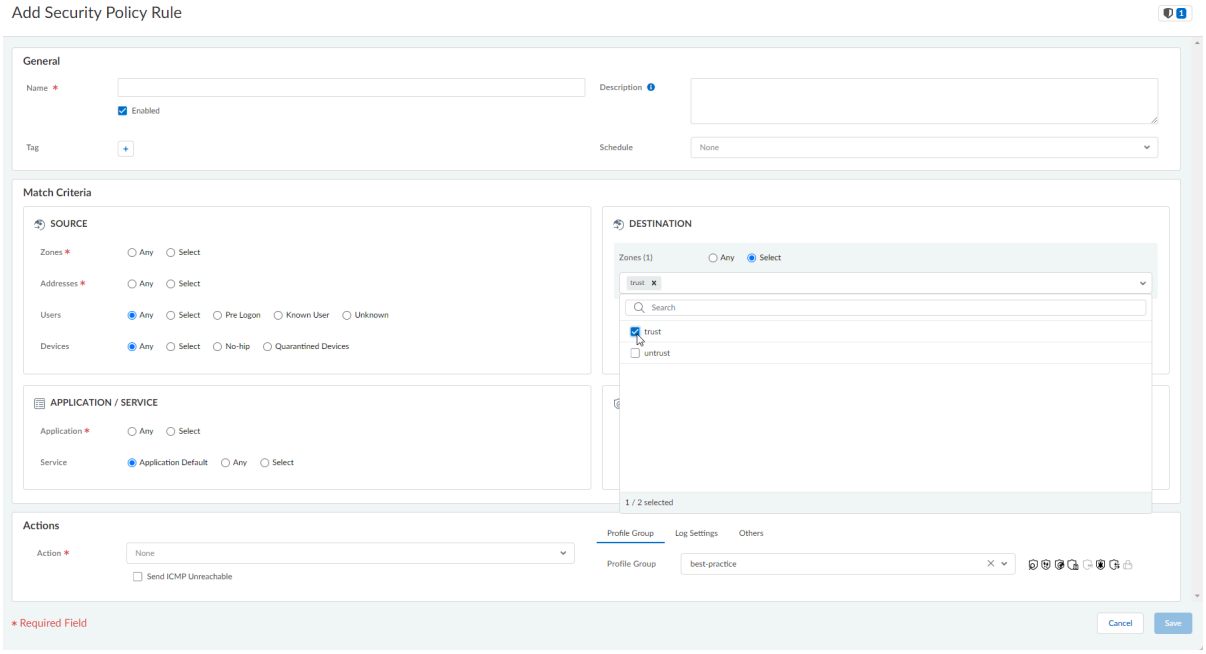
STEP 5 | Créez des règles de politique de sécurité pour les ressources du centre de données auxquelles vous souhaitez accéder.

1. Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)**, définissez le paramètre **Configuration Scope (Portée de la configuration)** sur **Prisma Access** > **Mobile Users Container (Conteneur d'utilisateurs mobiles)** > **Explicit Proxy (Proxy explicite)**, puis sélectionnez **Security Policy (Politique de sécurité)** > **Security Services (Services de sécurité)**.

 ©2025 Palo Alto Networks, Inc.

2. Créez des règles de politique de sécurité.

Dans les règles d'accès au centre de données, assurez-vous que le paramètre **Zones** sous `DESTINATION` est défini sur **trust (approuvées)**.



STEP 6 | Si vous activez l'accès aux applications privées sous Explicit Proxy (Proxy explicite), utilisez l'option **Push Config (Transmettre la configuration)** pour enregistrer vos modifications de configuration après l'intégration du connecteur ZTNA.

Accéder au centre de données à l'aide d'un proxy explicite (Panorama)

STEP 1 | Configurez une connexion aux services, Colo-Connect ou le connecteur ZTNA dans Prisma Access en fonction de vos besoins.

STEP 2 | Configurez les paramètres DNS.

STEP 3 | Configurez les mappages de zones.

1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users - Explicit Proxy (Utilisateurs mobiles - Proxy explicite)** > **Zone Mapping (Mappage de zone)**
2. Ajoutez les zones que vous utiliserez pour accéder aux ressources du centre de données à **Trusted Zones (Zones approuvées)**.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Vérifiez que la `Destination ZONE (ZONE de destination)` dans les règles de politique pour le trafic Internet est définie sur une zone non approuvée au lieu de `any (tout)`.

> *Si vous n'effectuez pas cette étape, vous risquez de créer un accès indésirable à votre centre de données.*

1. Sélectionnez **Policies (Politiques)**.
2. Définissez `Device Group (Groupe de périphériques)` sur **Explicit_Proxy_Device_Group**.
3. Modifiez la `Destination ZONE (ZONE de destination)` et définissez-la sur l'une des zones non approuvées que vous avez configurées à l'étape précédente au lieu de `any (tout)`.

STEP 5 | Activez l'accès aux applications privées.

- Activez l'accès aux applications privées à l'aide de Prisma Access Browser.
  1. Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users - Explicit Proxy (Utilisateurs mobiles - Proxy explicite)** > **Settings (Paramètres)** > **Advanced (Avancé)** > **Enable Prisma Access Browser (Activer Prisma Access Browser)** > **Enable Private Application Access (Activer l'accès aux applications privées)**

- Activez l'accès aux applications privées à l'aide d'un navigateur standard.
  1. Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users - Explicit Proxy (Utilisateurs mobiles - Proxy explicite)** > **Settings (Paramètres)** > **Advanced (Avancé)** > **Use GlobalProtect Agent to Authenticate (Utiliser l'agent GlobalProtect pour s'authentifier)** > **Enable Private Application Access (Activer l'accès aux applications privées)**

STEP 6 | Créez des règles de politique de sécurité pour les ressources du centre de données auxquelles vous souhaitez accéder.

1. Sélectionnez **Policies (Politiques)**.
2. Définissez `Device Group (Groupe de périphériques)` sur **Explicit_Proxy_Device_Group**.
3. Créez des règles de politique de sécurité.

   Dans les règles d'accès au centre de données, vérifiez que vous utilisez les zones **Trusted (Approuvées)** que vous avez configurées auparavant.

Intégration d'Office 365 basée sur une application avec le proxy explicite

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	• Licence d'utilisateur mobile

 ©2025 Palo Alto Networks, Inc.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	

Découvrez comment intégrer la version d'Office 365 basée sur un navigateur avec le proxy explicite.

- Strata Cloud Manager
- Panorama

Intégration d'Office 365 basée sur une application avec le proxy explicite (Panorama)

Le proxy explicite Prisma Access prend en charge la version d'Office 365 (M365) basée sur un navigateur, y compris Office Online (office.com). Suivez les étapes suivantes pour intégrer la version d'Office 365 basée sur un navigateur avec le proxy explicite.

Bien que le proxy explicite ne prenne pas en charge la version d'Office 365 basée sur une application, vous pouvez suivre ces directives pour utiliser le proxy explicite avec des politiques basées sur l'application Office 365.

Configurer l'intégration d'Office 365 basé sur un navigateur avec le proxy explicite Prisma Access

Si vous utilisez la version d'Office 365 basée sur un navigateur, effectuez la tâche suivante pour intégrer Office 365 avec le proxy explicite.

STEP 1 | (Facultatif) si vous souhaitez appliquer des restrictions basées sur le client (limiter le contrôle d'accès à Office 365 uniquement à un certain nombre de locataires), utilisez l'option Insertion de l'en-tête HTTP avec une catégorie d'URL personnalisée pour permettre à des locataires spécifiques d'accéder à Office 365.

STEP 2 | Ajoutez des politiques de décryptage pour les URL utilisées pour Office 365.

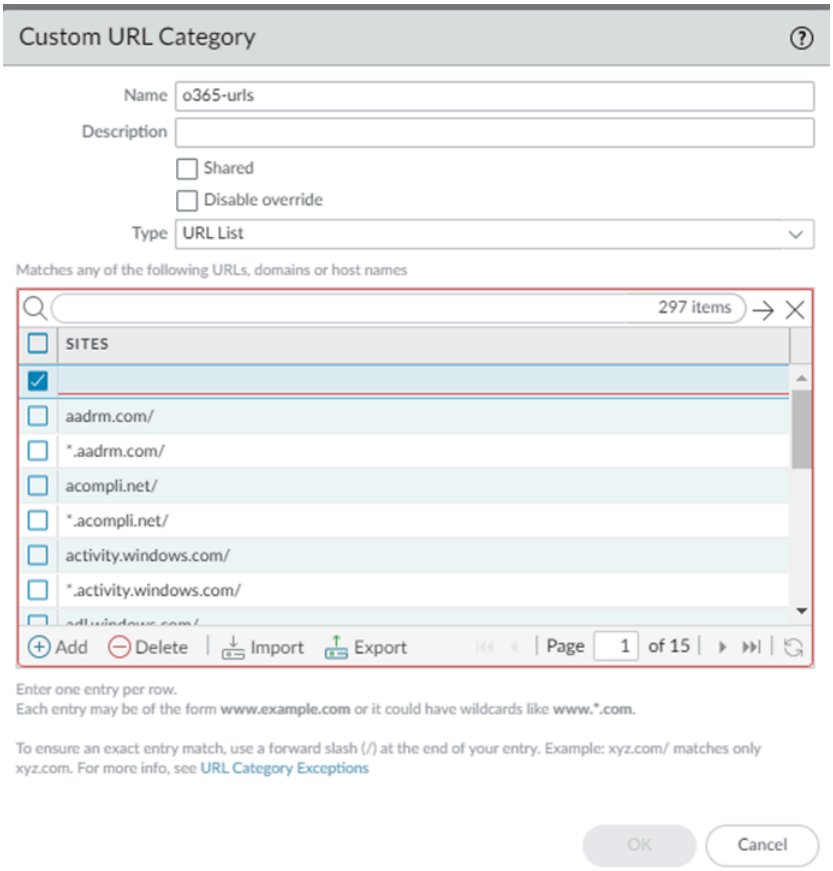
1. Sélectionnez **Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)** et cliquez sur **Add (Ajouter)** pour ajouter une catégorie d'URL personnalisée.

   Vérifiez que vous êtes dans **Explicit_Proxy_Device_Group**.
2. Spécifiez un **Type** de **URL List (Liste d'URL)**.
3. **Add (Ajoutez)** la liste des sites pour activer l'intégration d'Office 365.

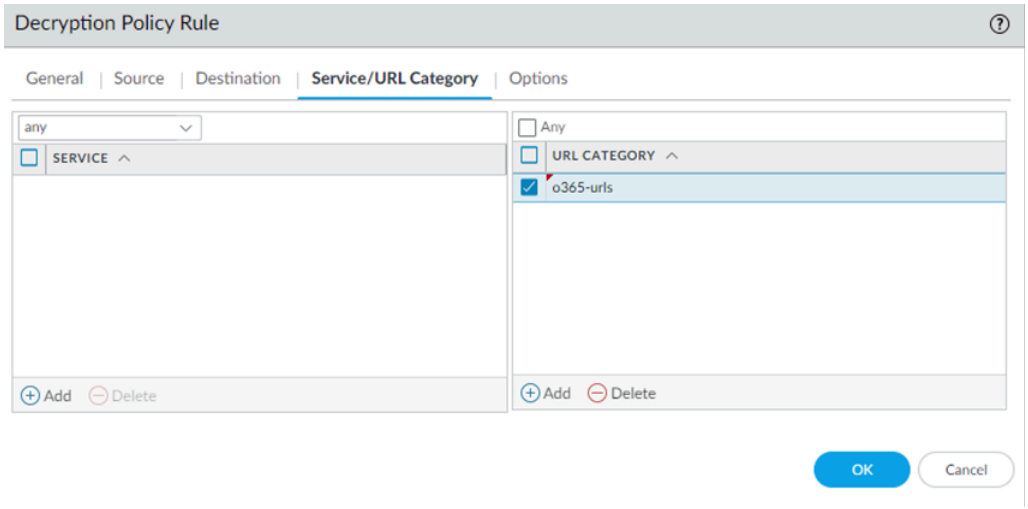
   Pour simplifier le chargement des URL, vous pouvez copier la liste des URL d'Office 365 à l'adresse https://saasedl.paloaltonetworks.com/feeds/m365/worldwide/any/all/url,

 ©2025 Palo Alto Networks, Inc.

enregistrer ces URL dans un fichier, et **Import (Importer)** le fichier dans la catégorie d'URL personnalisée.



4. Sélectionnez **Policies (Politiques)** > **Decryption (Décryptage)** > **Pre Rules (Pré-règles)**, puis cliquez sur **Add (Ajouter)** pour ajouter une règle de politique de décryptage.
5. Spécifiez l'icône **URL Category (Catégorie d'URL)** que vous avez créé.



6.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Ajoutez des politiques de décryptage pour les fonctionnalités de protection des données et de protection contre les menaces, notamment la prévention des pertes de données d'entreprise (DLP d'entreprise), WildFire, Prévention des menacesou Sécurité SaaS.

STEP 4 | Utilisez le Service d'hébergement EDL pour créer une liste dynamique externe.

STEP 5 |

Configurer l'intégration d'Office 365 basée sur une application avec le proxy explicite

Le proxy explicite ne prend pas en charge la version complète d'Office 365 basée sur le client (application), car Office 365 utilise des ports et des protocoles non web et des certificats épinglés, ce qui empêche l'utilisation du décryptage. Si vous avez besoin de sécuriser le trafic provenant des applications clientes d'Office 365, vous pouvez utiliser l'une des fonctionnalités Prisma Access suivantes pour ce faire :

- Déployez un déploiement d'Utilisateurs mobiles – GlobalProtect avec proxy explicite et utilisez les options tunnel divisé de GlobalProtect pour acheminer le trafic en provenance des applications Office 365 vers le tunnel GlobalProtect, tout en spécifiant que l'autre trafic Internet doit être envoyé vers le tunnel GlobalProtect, directement vers Internet ou vers un proxy explicite, en fonction de votre fichier PAC et des options d'inclusion et d'exclusion du tunnel GlobalProtect.
- Si votre organisation exige que le trafic lié à Internet passe par un proxy explicite, ou si votre réseau ne dispose pas d'un itinéraire par défaut, vous pouvez déployer un Déploiement de réseau à distance avec proxy expliciteDéploiement de réseau à distance avec proxy explicite. Dans ce déploiement, le proxy explicite vous fournit une liste d'adresses Anycast et monodiffusion, et vous configurez votre CPE pour acheminer le trafic via ces adresses vers le réseau distant et, à partir de là, vers le proxy explicite et vers Internet.

  Pour utiliser Office 365 avec ce type de déploiement, spécifiez des règles de fichier PAC pour contourner l'Office 365 non-web directement vers Internet.
- Si vous n'êtes pas en mesure de déployer GlobalProtect ou un réseau distant Prisma Access dans votre environnement, vous pouvez configurer le fichier PAC de proxy explicite pour contourner le trafic d'Office 365. Utilisez la Liste des URL à contourner.

Liste des URL permettant d'activer l'intégration d'Office 365 avec le proxy explicite Prisma Access

L'une des options que vous pouvez utiliser pour intégrer des applications Office 365 sans navigateur avec le proxy explicite consiste à spécifier les URL liées à Office 365 et à contourner ces URL dans le fichier PAC du proxy explicite. Obtenez la liste des URL à contourner par l'une des méthodes suivantes :

- Utilisez l'URL EDL du Service d'hébergement EDL de Palo Alto Networks pour les applications Microsoft 365.

  L'utilisation du service d'hébergement allège la charge opérationnelle liée à la sécurisation du trafic vers vos applications SaaS en utilisant une URL de flux comme source EDL. Lorsqu'un fournisseur SaaS ajoute un nouveau terminal à une application SaaS, l'URL de flux correspondante est mise à jour.

  Pour les URL de Microsoft 365 dans le monde entier, utilisez l'URL https://saasedl.paloaltonetworks.com/feeds/m365/worldwide/any/all/url. D'autres URL sont fournies pour IPv4 et IPv6, ainsi que pour des applications spécifiques à un pays et de gouvernements.

 ©2025 Palo Alto Networks, Inc.

- Récupérez la liste des adresses IP et des URL d'Office 365 fournies par Microsoft à l'adresse https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges. Microsoft fournit également un service web d'adresses IP et d'URL d'Office 365 à l'adresse https://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-ip-web-service.

Configurer le chaînage de proxy avec le proxy Blue Coat

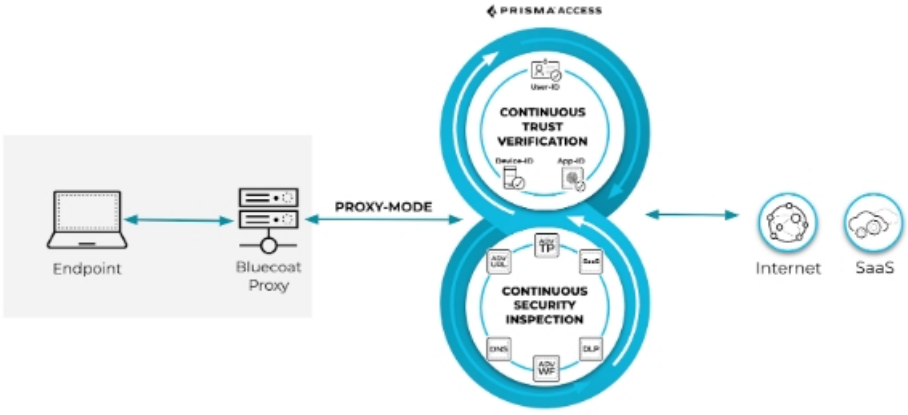
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Licence Prisma Access.

Le chaînage de proxy crée un chemin Internet à plusieurs sauts en mettant en cascade plusieurs serveurs proxys pour une couche de sécurité supplémentaire ou en raison de la conformité. Chaque serveur transmet votre trafic au suivant, atteignant finalement Internet. Cette technique utilise votre infrastructure réseau existante et permet de se connecter à un proxy en amont pour une communication HTTP et HTTPS sécurisée. L'intégration préserve les paramètres du navigateur de l'utilisateur tout en améliorant la sécurité et le contrôle.

Pourquoi les entreprises utilisent-elles la fonction de chaînage de proxy ? :

1. Confidentialité et anonymat améliorés en offrant une protection multicouche et en contournant les restrictions géographiques.
2. Sécurité et contrôle en filtrant les contenus malveillants, les spams et les tentatives de phishing en ajoutant une couche de sécurité supplémentaire à l'expérience de navigation de l'utilisateur.
3. Les entreprises peuvent utiliser le chaînage de proxy pour appliquer des règles de politique internes en limitant l'accès à certains sites Web ou services en fonction des rôles ou des emplacements des utilisateurs.
4. Au lieu de déployer un nouveau système, le chaînage de proxy vous permet d'utiliser votre infrastructure réseau existante en vous connectant à un serveur proxy en amont pour des tâches spécifiques. Il peut s'agir d'une solution rentable et efficace.

En savoir plus sur le fonctionnement du proxy explicite Prisma Access.



Voici le scénario dans lequel les clients souhaitent chaîner le trafic du proxy Blue Coat local vers le proxy explicite Prisma Access. Le proxy Blue Coat local authentifie les utilisateurs et transmet

 ©2025 Palo Alto Networks, Inc.

le nom d'utilisateur au proxy explicite Prisma Access en utilisant l'insertion de l'en-tête des utilisateurs authentifiés X (XAU) sur le proxy Blue Coat.

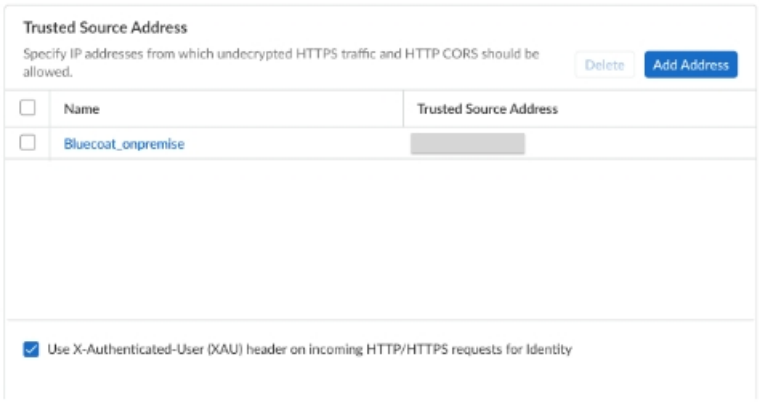
L'itinéraire statique et la NAT de destination pour les adresses IP du proxy explicite sont requis dans les réseaux sans itinéraire par défaut.

STEP 1 | Configurez Prisma Access.

1. Configurez un proxy explicite.
2. Ajoutez le proxy explicite Blue Coat en tant qu'adresse source fiable.
   1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Advanced Security Settings (Paramètres de sécurité avancés)** > **Add Address (Ajouter une adresse)**.
   2. Entrez l'adresse IP du proxy explicite Blue Coat.

      Vous pouvez ajouter des adresses IP ou des sous-réseaux.

   3. Sélectionnez **Use X-Authenticated-User (XAU) header on incoming HTTP/HTTPS requests for Identity (Utiliser l'en-tête des utilisateurs authentifiés X (XAU) sur les requêtes HTTP/HTTPS entrantes pour l'identité)**.

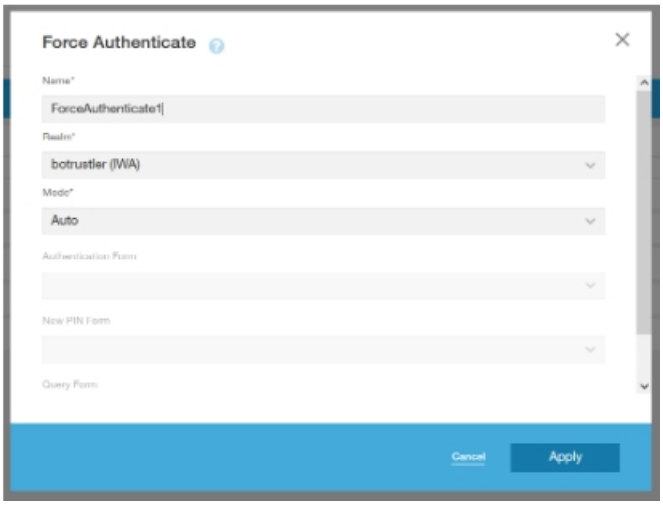


 ©2025 Palo Alto Networks, Inc.

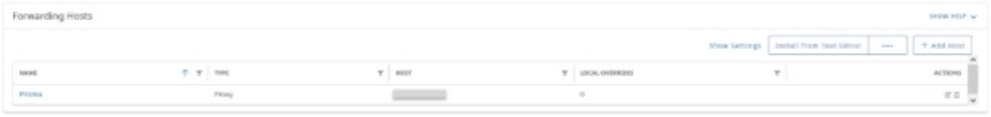
STEP 2 | Effectuez la configuration sur le proxy Blue Coat.

1. Appliquez l'authentification.



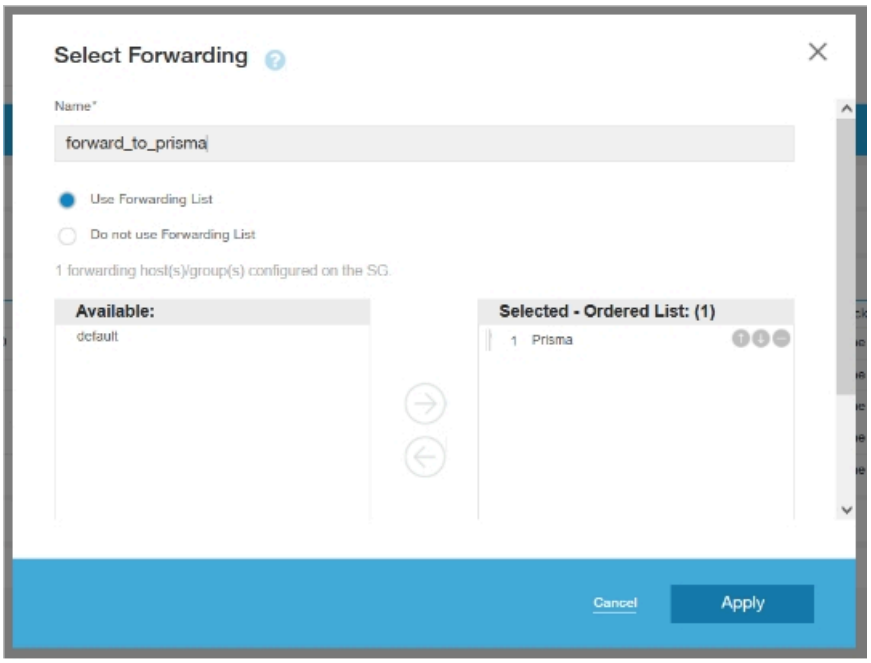


2. Configurez la couche de transfert.



1. Obtenez l'adresse IP du proxy explicite Prisma Access.
    1. Dans Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Infrastructure Settings (Paramètres d'infrastructure)**.
    2. Copiez le FQDN du proxy.

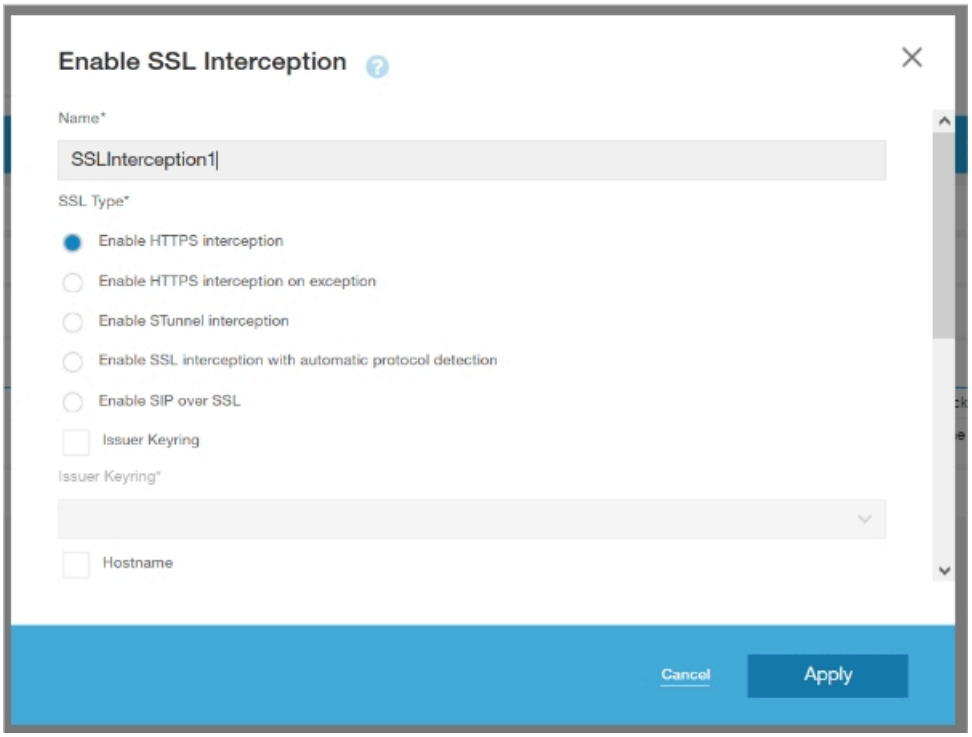
 ©2025 Palo Alto Networks, Inc.





2. Activez le déchiffrement HTTPS pour l'insertion de l'en-tête.

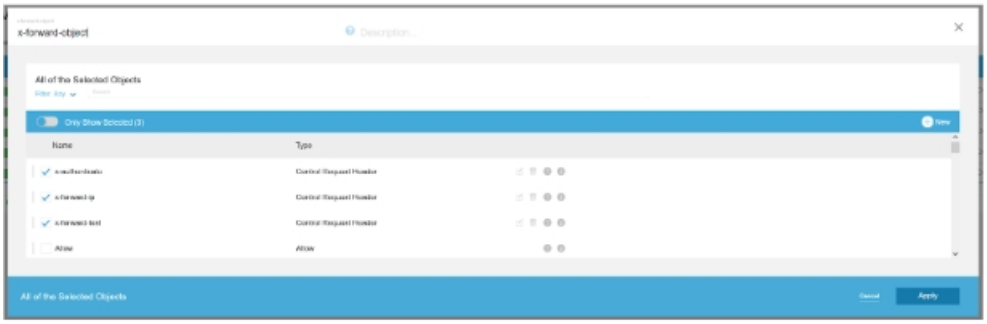
   Le déchiffrement est obligatoire pour l'insertion de l'en-tête.

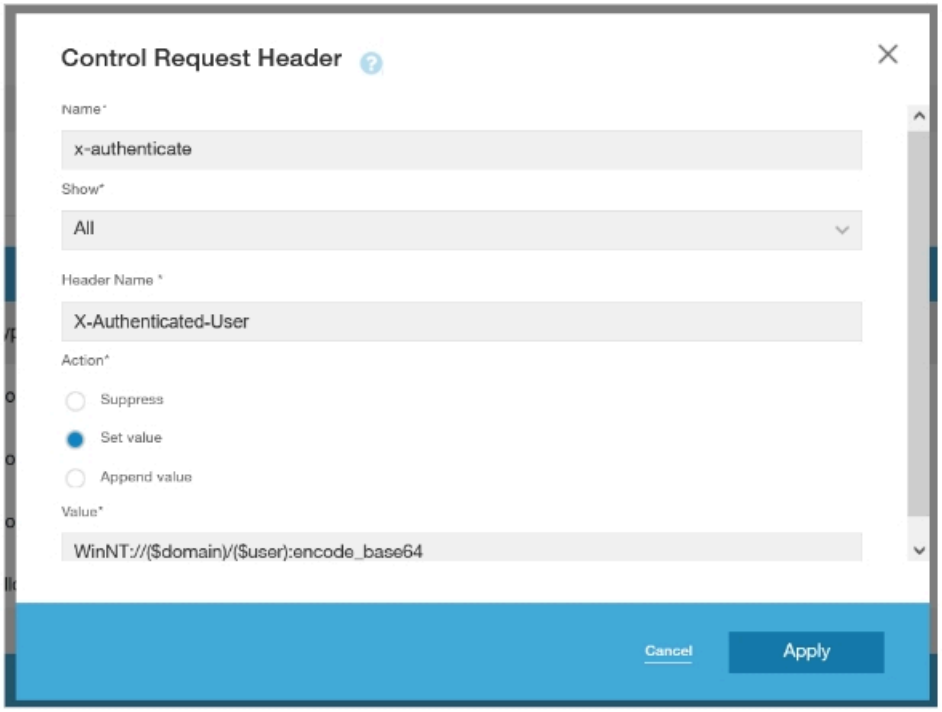


 ©2025 Palo Alto Networks, Inc.

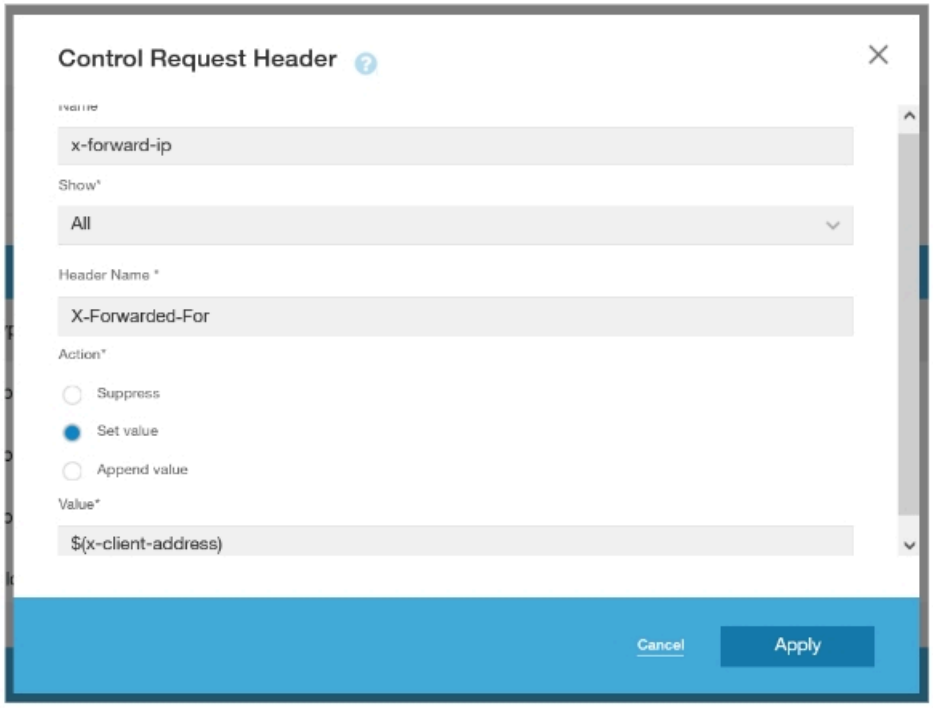


3. Configurez le transfert de l'en-tête.





 ©2025 Palo Alto Networks, Inc.



L'adresse IP du client reçue via l'en-tête XFF est simplement consignée et ne peut pas être exploitée pour la politique.

4. Définissez l'encodage de la valeur de l'en-tête sur base64 :

```
définissez l'action Encode_All_XFF set( request.x_header.X-
Authenticated-User, "$(user:encode_base64)" ) end define action
 x-authenticate set( request.x_header.X-Authenticated-User,
 "WinNT://($$domain)/($$user):encode_base64" ) end
```

STEP 3 | Vérifiez la configuration.

1. Dans Strata Cloud Manager, sélectionnez **Incidents and Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)**
2. Vérifiez les colonnes `X-Forwarded-For` et `Users (Utilisateurs)` pour vérifier que les informations de l'utilisateur et de l'adresse IP sont visibles sur Prisma Access.

STEP 4 | Considérez ces points :

1. Le proxy Blue Coat nécessite une authentification et un déchiffrement pour insérer les informations d'en-tête XAU.
2. La valeur de l'en-tête des utilisateurs authentifiés X doit être au format Base64.
3. Le proxy explicite Prisma Access peut voir l'identité de l'utilisateur pour le trafic déchiffré.

 ©2025 Palo Alto Networks, Inc.

Utiliser un proxy explicite avec GlobalProtect (ou un VPN tiers)

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

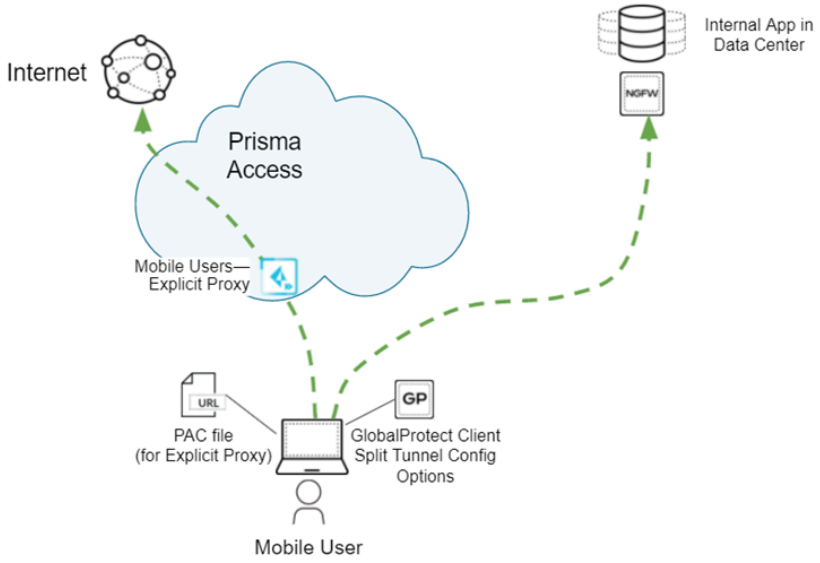
Vous pouvez combiner un proxy explicite avec GlobalProtect ou un VPN tiers :

- **Proxy explicite et GlobalProtect**
  - Utilisez GlobalProtect en mode segmentation du tunnel pour fournir un accès sécurisé aux applications privées uniquement.
  - Utilisez un proxy explicite pour sécuriser les applications publiques, y compris le trafic Internet et les applications SaaS externes.
- **Proxy explicite et VPN tiers**

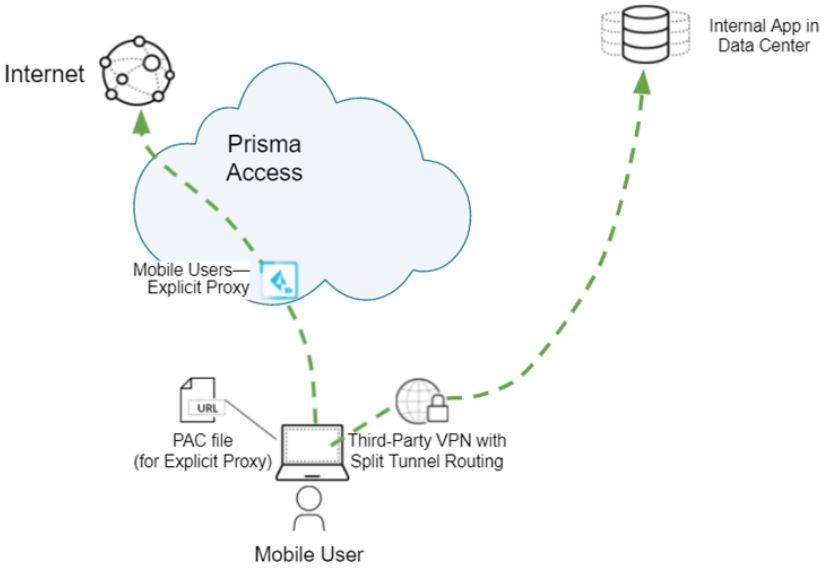
  Si vous utilisez un client VPN pour accéder au centre de données et aux applications privées, vous pouvez continuer à utiliser ce client pour sécuriser l'accès aux applications privées pendant que vous utilisez un proxy explicite et un fichier PAC pour sécuriser l'accès aux applications publiques. Vous pouvez déployer un proxy explicite dans un emplacement proche de vos utilisateurs mobiles, ce qui élimine le besoin d'amener le trafic vers votre centre de données pour la sécurité Web.

La figure suivante montre un déploiement utilisant une passerelle GlobalProtect avec un proxy explicite. GlobalProtect achemine le trafic à l'aide du client GlobalProtect vers le pare-feu nouvelle génération de Palo Alto Networks. Pour configurer ce déploiement, vous créez une configuration de segmentation du tunnel dans GlobalProtect, permettant de sécuriser les applications privées avec GlobalProtect et les applications publiques avec le proxy explicite. Une fois la configuration terminée, les utilisateurs mobiles se connectent aux applications privées du centre de données de votre organisation à l'aide de GlobalProtect et se connectent aux applications privées basées sur Internet à l'aide d'un proxy explicite.

 ©2025 Palo Alto Networks, Inc.



Si vous disposez d'un VPN tiers, vous pouvez l'utiliser pour vous connecter à des applications privées dans le centre de données, tout en sécurisant les applications publiques à l'aide d'un proxy explicite, comme illustré dans la figure suivante.



Mise en route :

- Comment cela fonctionne
- Proxy explicite – Directives
- Proxy explicite et GlobalProtect : Configurer cette fonctionnalité
- Proxy explicite avec des VPN tiers

 ©2025 Palo Alto Networks, Inc.

Exigences pour utiliser un proxy explicite avec GlobalProtect ou un VPN tiers

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Avant de commencer votre configuration, assurez-vous de suivre les exigences et recommandations requises pour déployer le proxy explicite avec GlobalProtect ou avec un VPN tiers :

- Pour utiliser le proxy explicite avec GlobalProtect, vous devez déployer GlobalProtect (soit un déploiement Utilisateurs mobiles—GlobalProtect, soit un déploiement GlobalProtect autonome qui utilise les passerelles et portails GlobalProtect).

  Vous configurez une configuration de tunnel fractionné dans GlobalProtect. Les exemples de cette section montrent que le trafic est divisé en fonction d'un domaine (URL) ou d'une application. Cependant, vous pouvez également diviser le trafic en fonction de la route d'accès.

  Vous pouvez également configurer des options DNS fractionnées dans GlobalProtect pour configurer les domaines résolus par les serveurs DNS attribués au VPN et les domaines résolus par les serveurs DNS locaux.
- Pour utiliser le proxy explicite avec un VPN tiers, vous devez déployer la solution VPN.
- Faites une liste des applications que vous souhaitez sécuriser avec les utilisateurs mobiles—déploiement GlobalProtect ou VPN tiers.

  Par exemple, si vous configurez le proxy explicite avec GlobalProtect, vous devez configurer GlobalProtect pour sécuriser tous les accès aux applications ou ressources privées, tout en configurant le fichier PAC proxy explicite pour sécuriser les applications publiques ou les applications SaaS. Dans les exemples de configuration de cette section, GlobalProtect résout les domaines internes et le proxy explicite résout les domaines externes.
- Configurez l'authentification pour le proxy explicite et GlobalProtect ou le VPN tiers.
  - Pour le proxy explicite, vous devez utiliser l'authentification SAML. Suivez les instructions de configuration SAML dans un déploiement de proxy explicite, y compris les URL pour utiliser pour la connexion SAML.
  - Pour les utilisateurs mobiles—déploiements GlobalProtect, si vous utilisez l'authentification SAML avec Okta comme fournisseur d'identité (IdP), consultez la procédure que vous utilisez pour configurer l'authentification SAML à l'aide d'Okta dans le Guide d'intégration Prisma Access (géré par Panorama).
  - Pour les déploiements GlobalProtect autonomes, vous pouvez configurer l'authentification SAML dans PAN-OS.
  - Pour un VPN tiers, reportez-vous à la documentation produit de ce VPN.

  Palo Alto Networks vous recommande d'utiliser le navigateur par défaut sur le point de terminaison de chaque utilisateur mobile pour l'authentification SAML afin que vous puissiez profiter de l'authentification unique (SSO) en modifiant la configuration du portail comme indiqué dans Configurer un proxy explicite.

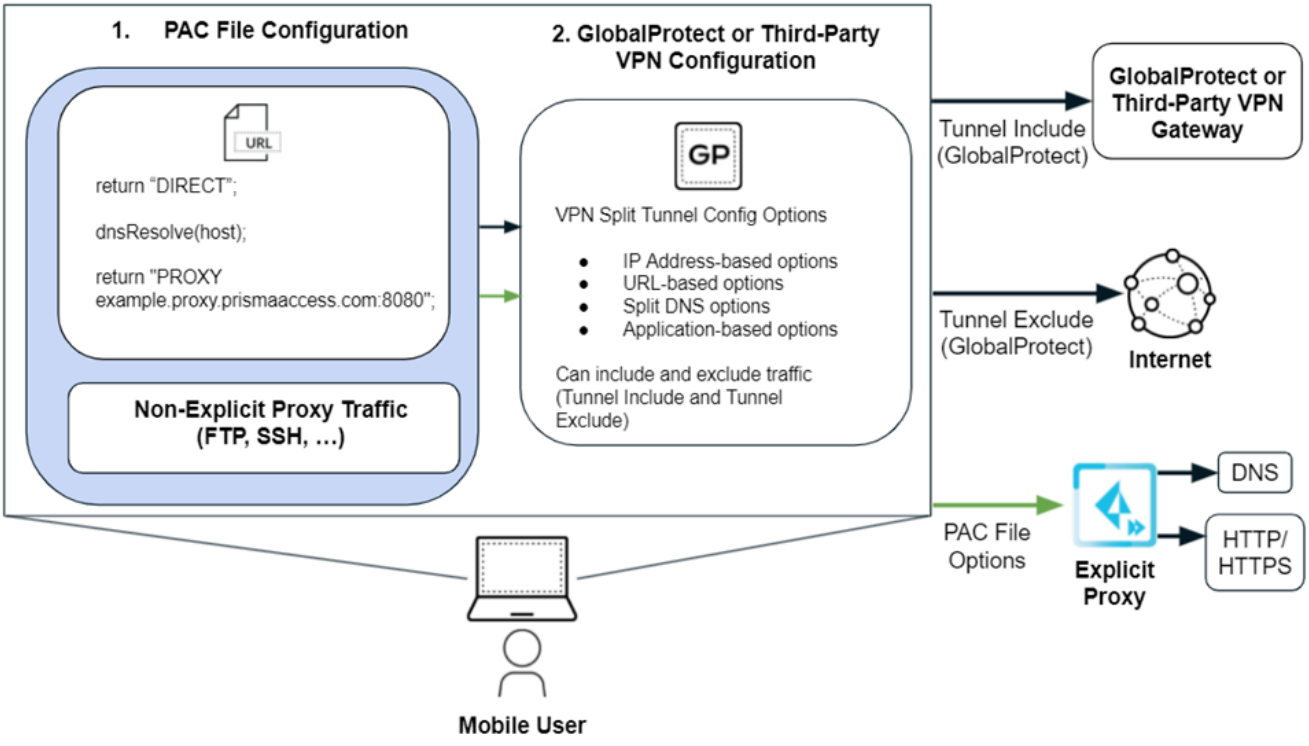
 ©2025 Palo Alto Networks, Inc.

- Vous devez vous assurer que les navigateurs utilisés par les utilisateurs mobiles respectent la configuration du fichier PAC.

Proxy explicite et GlobalProtect : Comment cela fonctionne

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Avant de décider quelles applications ou quel trafic vous devez protéger avec un proxy explicite et quelles applications vous devez protéger avec GlobalProtect ou un VPN tiers, vous devez comprendre comment GlobalProtect et Prisma Access prennent leurs décisions de transfert en fonction de la configuration du proxy explicite et du VPN. Les exemples de cette section supposent que vous avez déjà déployé un proxy explicite et GlobalProtect dans le réseau de votre entreprise et que vous avez configuré les options de segmentation de tunnel de GlobalProtect. La figure suivante illustre le processus.



Lorsqu'un utilisateur mobile demande une ressource ou une application privée ou basée sur Internet, la requête est évaluée par le fichier PAC de proxy explicite sur le terminal.

- Une fonction `return "DIRECT";` dans le fichier PAC fait que le trafic spécifié dans l'expression contourne le traitement du proxy explicite.

  Le proxy explicite vous fournit un exemple de fichier PAC qui utilise la fonction `return "DIRECT";` avec les adresses IP et les URL. Reportez-vous à la section Configurer votre

 ©2025 Palo Alto Networks, Inc.

fichier PAC de proxy explicite pour voir le contenu du fichier PAC et une description de son utilisation.

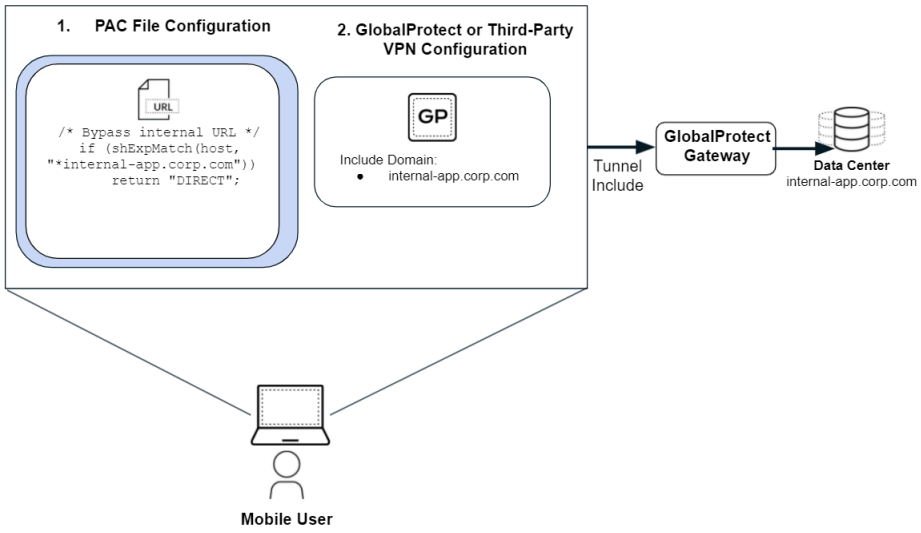
- Une fonction `dnsresolve(host)` dans le fichier PAC force le terminal à effectuer une requête DNS pour résoudre un nom d'hôte en une adresse IP. Cette requête suit ensuite la politique VPN (par exemple, segmentation de tunnel ou segmentation de DNS) pour le transfert de la requête DNS vers le serveur DNS de destination.

  Le fichier PAC fourni avec le proxy explicite utilise `dnsresolve(host)`, `return"DIRECT";`, et les adresses IP privées regroupées dans une expression. Si, après une recherche DNS, l'adresse IP renvoyée est incluse avec les adresses IP privées dans l'expression, le trafic associé à l'adresse IP privée contourne le traitement du proxy explicite.
- Le trafic spécifié dans le fichier PAC comme suit : `return"PROXY sitename:8080";` est transmis au proxy explicite.

Une fois que la requête Web est évaluée en fonction des conditions du fichier PAC, elle est envoyée à la configuration GlobalProtect ou à un VPN tiers sur le terminal pour traitement, et le trafic est évalué dans l'application GlobalProtect pour les options de configuration de segmentation de tunnel. Vous pouvez répartir le trafic en fonction du domaine (URL) ou de l'application ou du sous-réseau. Si vous avez configuré des options de segmentation de DNS dans GlobalProtect, le trafic est également évalué en fonction de ces options de DNS.

Une fois le trafic traité, il est ensuite envoyé à GlobalProtect, directement sur Internet, ou au proxy explicite, en fonction du fichier PAC et du traitement VPN.

La figure suivante illustre un utilisateur mobile qui tente d'accéder à une ressource privée à l'aide de l'URL **`internal-app.corp.com`**.



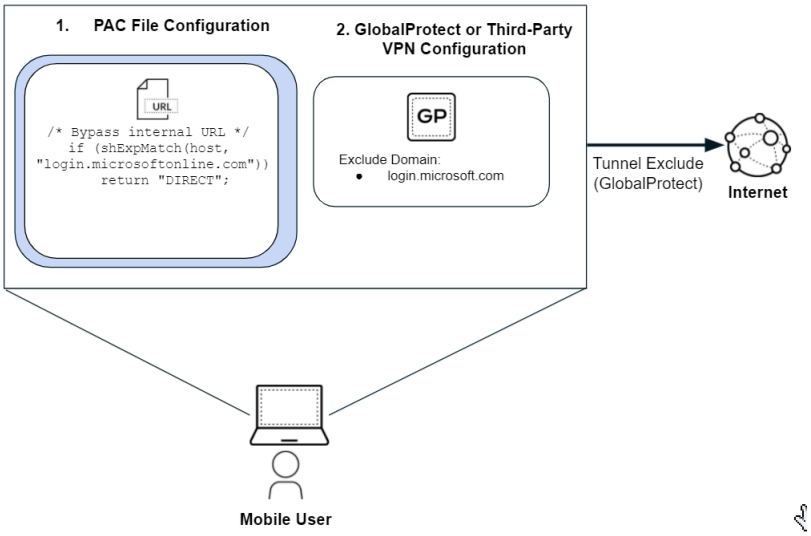
- Le fichier PAC est configuré de la manière suivante pour permettre à l'URL **`internal-app.corp.com`** de contourner le proxy explicite.

```
    /* Bypass internal URL */ if (shExpMatch(host, "*internal-
app.corp.com")) return "DIRECT";
```

 ©2025 Palo Alto Networks, Inc.

- Lorsque l'utilisateur mobile demande l'URL **internal-app.corp.com** à partir de son navigateur, celui-ci évalue les conditions dans le fichier PAC. Sur la base de cette évaluation, le navigateur ne transmet pas la requête au proxy et l'envoie directement à l'application GlobalProtect.
- GlobalProtect note que l'URL **internal-app.corp.com** est répertoriée dans **Include Domain (Inclure le domaine)** et l'envoie via le tunnel VPN.
- GlobalProtect envoie la requête à la ressource dans l'URL **internal-app.corp.com** en fonction des options de configuration de GlobalProtect.

Vous pouvez configurer certaines ressources, telles que les ressources de connexion, afin qu'elles n'utilisent ni le proxy explicite, ni GlobalProtect ou un VPN tiers pour le traitement. La figure suivante illustre un utilisateur qui se connecte à Microsoft Online en saisissant l'URL **login.microsoftonline.com** depuis son navigateur.



- Le fichier PAC est configuré de la manière suivante pour permettre à l'URL **internal-app.corp.com** de contourner le trafic du proxy explicite.

```
   /* Bypass internal URL */ if (shExpMatch(host,
"login.microsoftonline.com")) return "DIRECT";
```

- Lorsque l'utilisateur mobile demande l'URL **login.microsoftonline.com** depuis son navigateur, le fichier PAC évalue la requête à partir du fichier PAC dans le terminal de l'utilisateur mobile, puis l'envoie à la configuration VPN GlobalProtect (GlobalProtect dans ce cas) pour traitement.
- L'application GlobalProtect note que l'URL **login.microsoftonline.com** est répertoriée dans **Exclude Domain (Exclure le domaine)**.
- GlobalProtect contourne le VPN et envoie la requête directement sur Internet, en fonction des options de configuration de GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

Proxy explicite et GlobalProtect : Configurer cette fonctionnalité

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Pour que vos utilisateurs mobiles se connectent en toute sécurité, vous pouvez combiner un proxy explicite avec GlobalProtect ou un VPN tiers.

- Proxy explicite et GlobalProtect
  - Utilisez GlobalProtect en mode de segmentation de tunnel pour fournir un accès sécurisé aux applications privées uniquement.
  - Utilisez un proxy explicite pour sécuriser les applications publiques, y compris le trafic Internet et les applications SaaS externes.
- Proxy explicite et VPN tiers
  - Utilisez un client VPN pour accéder au centre de données et aux applications privées et pour sécuriser l'accès aux applications privées.
  - Utilisez un proxy explicite et un fichier PAC pour sécuriser l'accès aux applications publiques.

Avant de décider quelles applications ou quel trafic vous devez protéger avec un proxy explicite et avec GlobalProtect ou un VPN tiers, vous devez comprendre comment GlobalProtect et Prisma Access prennent leurs décisions de transfert en fonction de la configuration du proxy explicite et du VPN.

Lorsqu'un utilisateur mobile demande une ressource ou une application privée ou Internet, la requête est envoyée au fichier PAC du proxy explicite qui est installé sur le terminal.

- Le trafic qui est spécifié dans le fichier PAC comme return "DIRECT"; contourne le traitement du proxy explicite. Le DNS resolve (host) utilisé avec return "DIRECT"; permet le traitement du proxy explicite par passage IP spécifié.
- Le trafic qui est spécifié dans le fichier PAC comme return "PROXY sitename:8080"; est transféré à un proxy explicite.

Une fois le trafic traité, il est ensuite envoyé à GlobalProtect, directement sur Internet, ou à un proxy explicite, en fonction du fichier PAC et du traitement VPN.

Le fichier PAC est configuré de manière à permettre à « internal-app.corp.com » de contourner le proxy explicite. Lorsque l'utilisateur mobile demande l'URL « internal-app.corp.com » à partir de son navigateur, celui-ci évalue les conditions dans le fichier PAC. GlobalProtect note que l'URL « internal-app.corp.com » est répertoriée dans Include Domain (Inclure le domaine) et l'envoie via le tunnel VPN. GlobalProtect envoie la requête à la ressource dans l'URL « internal-app.corp.com » en fonction des options de configuration de GlobalProtect.

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

Proxy explicite et GlobalProtect : Configurer cette fonctionnalité (Strata Cloud Manager)

Pour mettre en œuvre GlobalProtect – Utilisateurs mobiles avec proxy explicite, suivez les étapes suivantes.

Ces étapes de configuration formulent les hypothèses suivantes sur votre environnement réseau ; si votre environnement réseau est différent, la configuration pourrait être différente :

- Les utilisateurs mobiles peuvent accéder et résoudre le nom d'hôte du portail GlobalProtect, les FQDN de la passerelle, l'URL du proxy explicite et l'URL du fichier PAC.

  Voici où trouver ces informations :

  - **FQDN de la passerelle GlobalProtect** et **Nom d'hôte du portail**

    # Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **Infrastructure** et modifiez les **Infrastructure Settings (Paramètres d'infrastructure)**.
  - **URL de proxy explicite** et **URL de fichier PAC**

    # Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Infrastructure** et modifiez les **Infrastructure Settings (Paramètres d'infrastructure)**.
- Les utilisateurs mobiles peuvent résoudre des domaines internes à partir de GlobalProtect.

STEP 1 | Décidez quelles applications vous souhaitez envoyer à GlobalProtect et quelles applications vous souhaitez envoyer au proxy explicite.

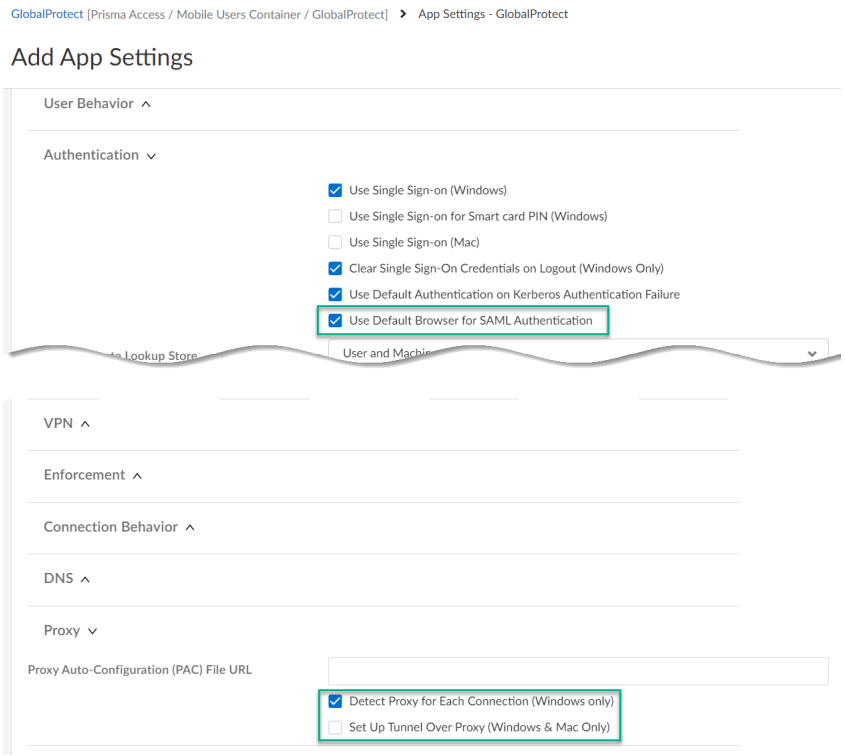
Les étapes suivantes dirigent les applications privées hébergées dans votre centre de données vers GlobalProtect et les requêtes vers les applications Internet et SaaS publiques vers le proxy explicite.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Modifiez les paramètres du portail GlobalProtect.

Accédez à **GlobalProtect** > **App Settings (Paramètres de l'application)** > **App Configuration (Configuration de l'application)** > **Advanced Settings (Paramètres avancés)**

1. Dans les paramètres du **Proxy** :
   - Cochez **Detect Proxy for Each Connection (Détecter le proxy pour chaque connexion)**
   - Décochez **Set Up Tunnel Over Proxy (Windows & Mac Only) (Définir le proxy du tunnel (Windows et Mac uniquement))**
2. Dans les paramètres **Authentication (Authentification)** :
   - Cochez **Use Default Browser for SAML Authentication (Utiliser le navigateur par défaut pour l'authentification SAML)**



STEP 3 | Créez une segmentation de tunnel dans GlobalProtect qui vous permet de diriger le trafic interne vers GlobalProtect.

Accédez à **GlobalProtect** > **Tunnel Settings (Paramètres de tunnel)** > **Split Tunneling (Segmentation du tunnel)**. Configurez une segmentation de tunnel basée sur le domaine (FQDN), les itinéraires d'accès ou les applications.

STEP 4 | Configurez le fichier PAC pour exclure les domaines que vous avez spécifiés pour la segmentation de tunnel GlobalProtect.

Pour télécharger le fichier PAC afin de pouvoir l'éditer, accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (proxy explicite)**

 ©2025 Palo Alto Networks, Inc.

> **Infrastructure** > **Infrastructure Settings (Paramètres d'infrastructure)** > **Proxy Auto Configuration (Configuration automatique du proxy).**.

L'exemple suivant montre un fichier PAC avec l'URL qui héberge des applications privées (internal-app.corp.com) contournant le proxy interne. Les paramètres dans le fichier PAC suivant sont tous des valeurs d'exemple :

- Le nom d'hôte du portail est `splittunnel.gpcloudservice.com`.
- Les passerelles d'utilisateur mobile sont contenues dans le FQDN à caractères génériques `*examplegateways.gw.gpcloudservice.com`.
- L'URL du fichier PAC est `https://pacfileurl.pac`.
- `internal-app.corp.com` héberge les applications privées qui sont protégées par les utilisateurs mobiles—GlobalProtect.
- Okta est utilisé pour l'authentification SAML.
- L'URL du proxy explicite est `example.proxy.prismaacess.com`.

```
function FindProxyForURL(url, host) { /* Bypass FTP */ if
 (url.substring(0,4) == "ftp:") return "DIRECT"; /* Bypass
 the Prisma Access Portal Hostname */ if (shExpMatch(host,
 "*.splittunnel.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access Gateway */ if (shExpMatch(host,
 "*examplegateways.gw.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access PAC File URL */ if (shExpMatch(host,
 "https://pacfileurl.pac")) return "DIRECT"; /* Bypass the URLs
 Being Sent to the GlobalProtect Portal */ if (shExpMatch(host,
 "*.internal-app.corp.com")) return "DIRECT"; /* Bypass ACS
 */ if (shExpMatch(host, "*.acs.prismaaccess.com")) return
 "DIRECT"; /* Forward to Prisma Access */ return "PROXY
 example.proxy.prismaaccess.com:8080"; }
```

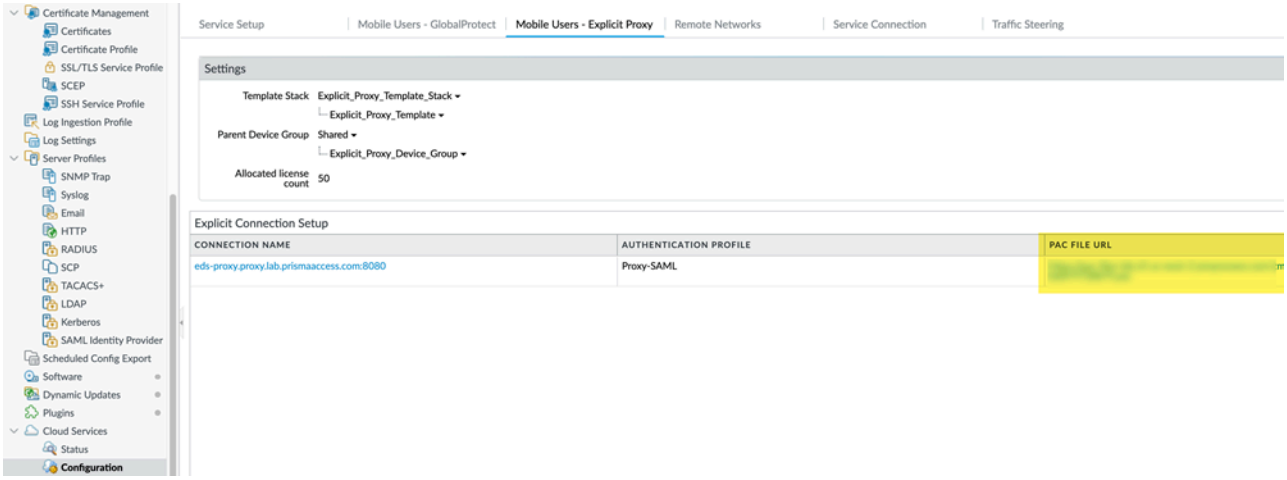
Proxy explicite et GlobalProtect : Configurer cette fonctionnalité (Panorama)

Pour mettre en œuvre GlobalProtect – Utilisateurs mobiles avec proxy explicite, suivez les étapes suivantes.

Ces étapes de configuration formulent les hypothèses suivantes sur votre environnement réseau ; si votre environnement réseau est différent, la configuration pourrait être différente :

 ©2025 Palo Alto Networks, Inc.

- Les utilisateurs mobiles peuvent atteindre et résoudre le nom d'hôte du portail GlobalProtect, les FQDN de la passerelle, l'URL du proxy explicite et l'URL du fichier PAC.
  - Pour rechercher les FQDN de la passerelle, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Mobile Users—GlobalProtect (Utilisateurs mobiles—GlobalProtect)** > **Gateways (Passerelles)**.
  - Pour trouver la **PAC File URL (URL du fichier PAC)**, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—Explicit Proxy (Utilisateurs mobiles – proxy explicite)** > **PAC File URL (URL du fichier PAC)**.



- Les utilisateurs mobiles peuvent résoudre des domaines internes à partir de GlobalProtect.

STEP 1 | Planifiez votre déploiement Utilisateurs mobiles – proxy explicite et votre déploiement GlobalProtect (soit votre déploiement Utilisateurs mobiles – GlobalProtect ou GlobalProtect autonome).

STEP 2 | Décidez quelles applications vous souhaitez envoyer à GlobalProtect et quelles applications vous souhaitez envoyer au proxy explicite.

Les étapes suivantes dirigent les applications privées hébergées dans votre centre de données vers GlobalProtect et les requêtes vers les applications Internet et SaaS publiques vers le proxy explicite.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Dans le Panorama qui gère Prisma Access, configurez les paramètres du portail GlobalProtect.

1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**.

   Assurez-vous que vous êtes dans le **Mobile_User_Template** de la liste déroulante **Template (Modèle)**.
2. Sélectionnez **GlobalProtect_Portal** pour modifier la configuration du portail Prisma Access.
3. Sélectionnez l'onglet **Agent** et sélectionnez la configuration **DEFAULT (PAR DÉFAUT)** ou **Add (Ajoutez)** une nouvelle.
4. Sélectionnez l'onglet **App (Applications)**.
5. Apportez les modifications suivantes à la configuration de l'application :
   - Dans **Detect Proxy for Each Connection (Détecter le proxy pour chaque connexion)**, sélectionnez **Yes (Oui)**.
   - Dans **Set Up Tunnel Over Proxy (Windows & Mac Only) (Définir le proxy du tunnel (Windows et Mac uniquement))**, sélectionnez **No (Non)**.
   - Dans **Use Default Browser for SAML Authentication (Utiliser le navigateur par défaut pour l'authentification SAML)**, sélectionnez **Yes (Oui)**.

STEP 4 | Créez une segmentation de tunnel dans GlobalProtect qui vous permet de diriger le trafic interne vers GlobalProtect.

L'exemple suivant utilise une segmentation de tunnel pour diriger le trafic en fonction du domaine (FQDN). Vous pouvez également configurer une segmentation de tunnel en fonction de l'itinéraire d'accès du trafic.

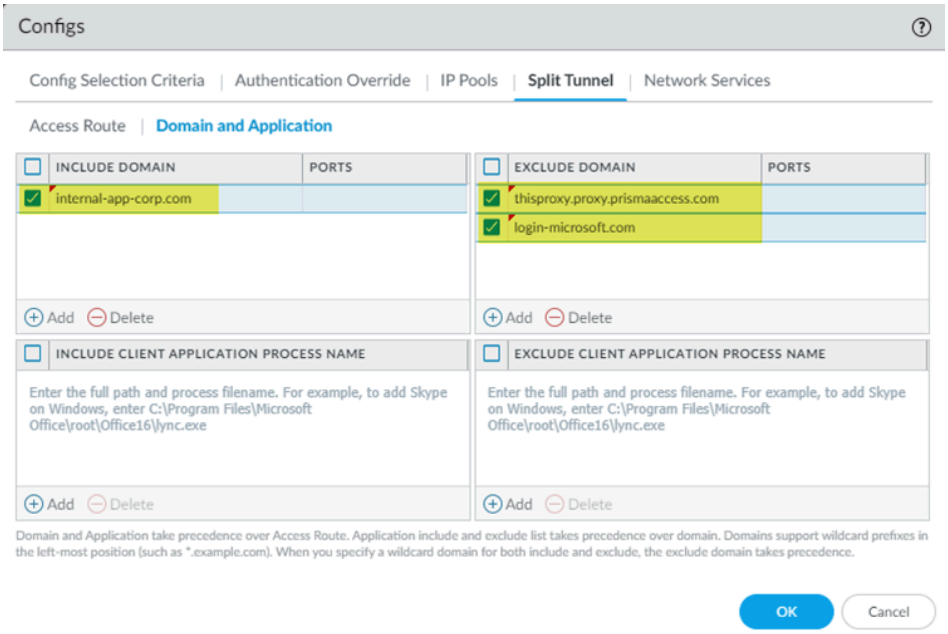
1. Pendant que vous êtes encore dans la configuration de l'agent GlobalProtect (**Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > **GlobalProtect External Gateway**

 ©2025 Palo Alto Networks, Inc.

(Passerelle externe GlobalProtect)), sélectionnez **Agent** > **Client Settings (Paramètres du client)**.

2. Sélectionnez la configuration **DEFAULT (PAR DÉFAUT)** ou **Add (Ajoutez)** une nouvelle.
3. Sélectionnez **Split Tunnel (Segmentation de tunnel)** > **Domain and Application (Domaine et application)**.
4. **Add (Ajoutez) Include Domain (Inclure le domaine)** et, éventuellement, les **Ports** à utiliser avec le domaine.

   Cet exemple utilise internal-app.corp.com comme URL que vous utilisez pour héberger des applications dans votre centre de données. Vous ajoutez cette URL et l'URL d'authentification SAML dans **Exclude Domain (Exclure le domaine)**.



5. Cliquez sur **OK** pour enregistrer vos modifications.
6. **Commit and Push (Validez et appliquez)** vos modifications.

STEP 5 | Configurez le fichier PAC pour exclure les domaines que vous avez saisis pour la segmentation de tunnel.

L'exemple suivant montre un fichier PAC avec l'URL qui héberge des applications privées (internal-app.corp.com) contournant le proxy interne. Les paramètres dans le fichier PAC suivant sont tous des valeurs d'exemple :

- Le nom d'hôte du portail est `splittunnel.gpcloudservice.com`.
- Les passerelles d'utilisateurs mobiles (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Mobile Users—GlobalProtect (Utilisateurs**

 ©2025 Palo Alto Networks, Inc.

mobiles – GlobalProtect) > **Gateways (Passerelles)**) sont contenues dans le FQDN à caractères génériques `*examplegateways.gw.gpcloudservice.com`.

- La **PAC File URL (URL du fichier PAC)** (**Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—Explicit Proxy (Utilisateurs mobiles : proxy explicite)** > **PAC File URL (URL du fichier PAC)**) est `https://pacfileurl.pac`.
- `internal-app.corp.com` héberge les applications privées protégées par Mobile Users—GlobalProtect (Utilisateurs mobiles – GlobalProtect).
- Okta est utilisé pour l'authentification SAML.
- L'URL de proxy explicite est `example.proxy.prismaacess.com`.

```
function FindProxyForURL(url, host) { /* Bypass FTP */ if
 (url.substring(0,4) == "ftp:") return "DIRECT"; /* Bypass
 the Prisma Access Portal Hostname */ if (shExpMatch(host,
 "*.splittunnel.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access Gateway */ if (shExpMatch(host,
 "*examplegateways.gw.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access PAC File URL */ if (shExpMatch(host,
 "https://pacfileurl.pac")) return "DIRECT"; /* Bypass the URLs
 Being Sent to the GlobalProtect Portal */ if (shExpMatch(host,
 "*.internal-app.corp.com")) return "DIRECT"; /* Bypass ACS
 */ if (shExpMatch(host, "*.acs.prismaaccess.com")) return
 "DIRECT"; /* Forward to Prisma Access */ return "PROXY
 example.proxy.prismaaccess.com:8080"; }
```

Proxy explicite avec des VPN tiers

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Pour utiliser des VPN tiers avec le proxy explicite, vous devez pouvoir effectuer les modifications suivantes dans votre réseau :

- Vous devez configurer votre VPN tiers pour effectuer une segmentation de tunnel afin de diriger le trafic Internet vers le proxy explicite.

  Pour toute assistance concernant la configuration de votre VPN tiers, contactez votre fournisseur de VPN tiers.
- Modifiez le fichier PAC pour que le proxy explicite contourne l'un des composants VPN suivants :
  - Toute adresse IP associée au VPN tiers
  - Toute URL de connexion requise pour le VPN tiers

 ©2025 Palo Alto Networks, Inc.

Dans l'exemple suivant, vous avez configuré le fichier PAC de sorte que le proxy explicite contourne les ressources internes à l'aide d'adresses IP privées, ainsi que les flux de trafic d'authentification.

```
++++++++++++++++ function FindProxyForURL(url, host) { if
 (isPlainHostName(host) || shExpMatch(host, "*.local")
 || isInNet(dnsResolve(host), "10.0.0.0", "255.0.0.0") ||
 isInNet(dnsResolve(host), "127.0.0.0", "255.255.255.0"))
 return "DIRECT"; /* Bypass SAML for AnyConnect Azure */
 if (shExpMatch(host, "login.microsoftonline.com")) return
 "DIRECT"; if (shExpMatch(host, "login.windows.net")) return
 "DIRECT"; if (shExpMatch(host, "login.microsoft.com"))
 return "DIRECT"; /* Forward to Prisma Access */ return "PROXY
 example.proxy.prismaaccess.com:8080"; }
```

Optimisation de l'adresse IP pour les utilisateurs de proxys explicites : déploiements de proxys

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) Si vous souhaitez utiliser cette fonctionnalité dans votre Prisma Access environnement, contactez votre équipe de compte pour en savoir plus.	• Prisma Access 5.2 • Plan de données Prisma Access 10.2.4 • Plug-in Panorama version 5.2.0

L'optimisation des adresses IP est un ensemble d'améliorations architecturales qui réduisent le nombre total d'adresses IP dans votre déploiement, simplifiant vos flux de travail de mise en liste d'autorisation tout en améliorant la résilience et en permettant une intégration plus rapide des locataires Prisma Access.

Adhérence de l'adresse IP

Grâce à l'adhérence des adresses IP, vous pouvez sécuriser les applis SaaS et les sites web qui nécessitent que les sessions utilisateur maintiennent la même adresse IP de sortie de Prisma Access tout au long de la session utilisateur.

Simplifier l'intégration des applications SaaS

L'ajout d'un emplacement Prisma Access ou la survenue d'un événement de mise à l'échelle sur un emplacement Prisma Access existant peut entraîner l'attribution de nouvelles adresses IP à vos déploiements de proxy explicite. Il est recommandé de récupérer les nouvelles adresses IP de sortie et de passerelle et de les ajouter à une liste d'autorisation des applications SaaS. L'optimisation des adresses IP réduit le nombre d'adresses IP que vous devez gérer dans les déploiements de grande envergure.

Dépannage

 ©2025 Palo Alto Networks, Inc.

Si vous souhaitez cibler des applications spécifiques pour l'optimisation des adresses IP, vous pouvez les ajouter à la catégorie d'URL ou à la liste dynamique externe (External Dynamic List, EDL). Une fois que vous avez configuré les objets spéciaux, seuls les domaines inclus dans ces objets bénéficieront de l'optimisation des adresses IP.

Panorama : configurez la catégorie d'URL comme suit : **PANW EP IP Affinity URL List (Liste des URL d'affinité IP PANW EP)** ou EDL comme **PANW EP IP Affinity List (Liste d'affinité IP PANW EP)**. Évitez les entrées à caractères génériques, exemple **.*** ou des domaines de premier niveau tels que **.com**.

Strata Cloud Manager : prend en charge la liste d'URL **PANW EP IP Affinity URL List (Liste des URL d'affinité IP PANW EP)**.

Résolution DNS pour les utilisateurs mobiles — Déploiements de proxys explicites

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Si vous souhaitez utiliser cette fonctionnalité dans votre Prisma Access environnement, contactez votre équipe de compte pour en savoir plus.	❑ Licence Prisma Access ❑ Prisma Access version 5.2.0

Prisma Access vous permet de spécifier les serveurs DNS pour résoudre à la fois les domaines internes à votre organisation et les domaines externes. Prisma Access utilise un proxy pour la requête DNS basée sur la configuration de vos serveurs DNS. Le proxy explicite prend en charge les fonctionnalités DNS suivantes :

- Utilisation d'un navigateur tiers avec le proxy explicite
- Utilisation d'un serveur DNS par région avec Prisma Access Browser

- *La configuration du proxy DNS pour le proxy explicite a priorité sur les paramètres internes des serveurs DNS définis sous **Prisma Access Setup (Configuration de Prisma Access)**.*
- *Après avoir activé le proxy DNS pour le proxy explicite, vous devez migrer la configuration DNS existante de **Prisma Access Setup (Configuration de Prisma Access)** > **Internal DNS Servers (Serveurs DNS internes)** vers **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Infrastructure Settings (Paramètres d'infrastructure)** > **DNS Proxy (Proxy DNS)***

Configurer les paramètres DNS

Pour configurer les paramètres du proxy DNS, procédez comme suit :

 ©2025 Palo Alto Networks, Inc.

1. Ajoutez une règle de serveur DNS du proxy explicite.
   1. Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Infrastructure Settings (Paramètres d'infrastructure)**.
   2. Cliquez sur l'icône de paramètres et accédez à **Client DNS (DNS client)**.
   3. **Add Region (Ajouter une région)** et donnez-lui un nom unique.
   4. Sélectionnez une région ou un emplacement ou sélectionnez **Worldwide (Universel)**.

      Si vous spécifiez plusieurs paramètres de proxy avec un mélange de paramètres Universels et théâtre, Prisma Access utilise les paramètres du groupe d'emplacements (un groupe d'emplacements plus petit que le théâtre), puis du théâtre, puis universel. Prisma Access évalue les règles de haut en bas dans la liste.
   5. Ajoutez l'adresse IP du serveur DNS.

2. Choisissez si vous souhaitez que Prisma Access effectue l'action **Resolve internal domains (Résoudre les domaines internes)**. Si c'est le cas, cliquez sur **Add (Ajouter)** pour ajouter une ou plusieurs **Internal Domain Resolve Rules (Règles de résolution de domaine interne)**.

3. Cliquez sur **Add (Ajouter)** et définissez les **Internal Domain Resolve Rules (Règles de résolution de domaine interne)**.

   *Actuellement, l'option **Internal Domain Resolve Rules (Règles de résolution de domaine interne)** est uniquement prise en charge pour Prisma Access Browser et le proxy d'agent.*
4. Ajoutez un **Name (Nom)** unique pour la règle et une adresse IP personnalisée sous **Primary DNS (DNS principal)** et **Secondary DNS (DNS secondaire)**.
5. Sélectionnez **Prisma Access Default (Prisma Access par défaut)** pour utiliser le serveur DNS Prisma Access par défaut pour résoudre les domaines internes. Si vous souhaitez que votre serveur DNS interne résolve uniquement les domaines que vous spécifiez, saisissez les domaines à résoudre dans la **Domain List (Liste de domaines)**.
6. Si vous disposez d'un serveur DNS **Custom (Personnalisé)** capable d'accéder à vos domaines internes, spécifiez les adresses IP du serveur **Primary DNS (DNS principal)** et du serveur **Secondary DNS (DNS secondaire)**.

7. Si vous souhaitez que votre serveur DNS interne résolve uniquement les domaines que vous spécifiez, saisissez les domaines à résoudre dans les **Domain Lists (Listes de domaines)**. Spécifiez un astérisque devant le domaine ; par exemple, *.acme.com. Cliquez sur **Save (Enregistrer)**.
8. Cliquez sur **Push Config (Transmettre la configuration)** pour enregistrer et transmettre vos modifications de configuration.

 ©2025 Palo Alto Networks, Inc.

Afficher des mappages de l'utilisateur à l'adresse IP ou à des groupes

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	• Licence Prisma Access

Prisma Access Insights vous permet d'afficher le mappage de l'utilisateur à l'adresse IP ou l'utilisateur à des groupes pour les utilisateurs mobiles en temps réel. Pour les réseaux distants et les connexions aux services, vous pouvez afficher les mappages de l'utilisateur aux groupes d'utilisateurs.

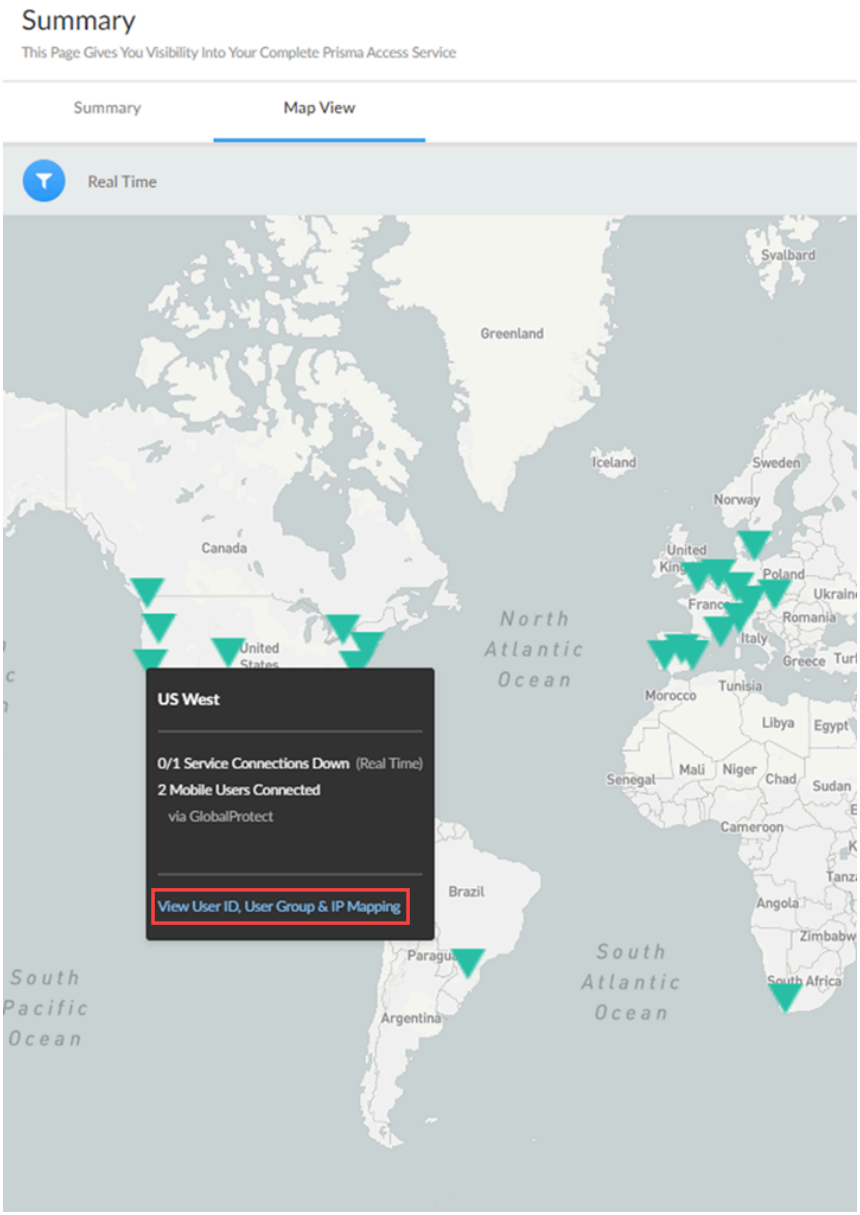
Les triangles inversés sur la carte sont codés par couleur pour indiquer l'état de l'emplacement de Prisma Access :

- Vert : Toutes les instances sont en place.
- Rouge : Toutes les instances sont inactives.
- Jaune : Les instances sont une combinaison de haut, bas et inconnu, et peuvent nécessiter votre attention.
- Gris : Toutes les instances sont inconnues.

STEP 1 | Dans le tableau de bord **Summary (Résumé)**, sélectionnez la **Map View (Vue carte)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Passez le curseur de votre souris sur un emplacement jusqu'à ce qu'une boîte de dialogue contextuelle apparaisse.



STEP 3 | Sélectionnez **View User ID, User Groups & IP Mapping (Afficher le mappage ID utilisateur, groupes d'utilisateurs et IP)** dans la boîte de dialogue. La boîte de dialogue **UserID and User Group Distribution Check (Vérification de la distribution de l'ID utilisateur et du groupe d'utilisateurs)** s'ouvre.

STEP 4 | Sélectionnez le **Prisma Access Location (Emplacement Prisma Access)** et le **Node Type (Type de nœud)**. Le **Prisma Access Location filter (Filtre emplacement Prisma Access)** n'est pas pris

 ©2025 Palo Alto Networks, Inc.

en considération lorsque le **Node Type (Type de nœud)** est **Mobile Users (GlobalProtect) (Utilisateurs mobiles (GlobalProtect))**.

Pour les réseaux distants et les connexions aux services, vous ne pouvez voir que les mappages ID utilisateur aux groupes d'utilisateurs.

1. Sélectionnez un **Prisma Access Location (Emplacement Prisma Access)**. Si l'emplacement Prisma Access que vous sélectionnez n'a pas de réseaux distants ou de connexions aux services associés, un message « No Data Available » (Aucune donnée disponible) s'affiche dans les champs **Remote Networks Site (Site de réseaux distants)** ou **Service Connections Site (Site de connexions aux services)**, selon le cas, et les boutons **Show User Groups (Afficher les groupes d'utilisateurs)** et **Export to CSV (Exporter au format CSV)** sont désactivés.
2. Dans **Node Type (Type de nœud)**, sélectionnez Réseaux distants ou Connexions aux services.
3. Dans le champ **Remote Networks Site (Site de réseaux distants)** ou **Service Connections Site (Site de connexions aux services)**, sélectionnez le site à partir duquel vous souhaitez récupérer les données.
4. Dans View (Affichage), sélectionnez si vous souhaitez voir à quels groupes d'utilisateurs appartient un ID utilisateur (User (Utilisateur)) ou quels utilisateurs font partie d'un groupe (Group (Groupe)) particulier associé au site.

   - Si vous sélectionnez **User (Utilisateur)**, saisissez le**User ID (ID utilisateur)** de l'utilisateur (par exemple, saas\testuser3) pour obtenir le mappage ID utilisateur aux groupes d'utilisateurs, puis sélectionnez **Show User Groups (Afficher les groupes d'utilisateurs**. Une liste de tous les groupes auxquels appartient l'ID utilisateur est affichée sous **User ID-IP Mappings (Mappages identifiant utilisateur-IP)**.

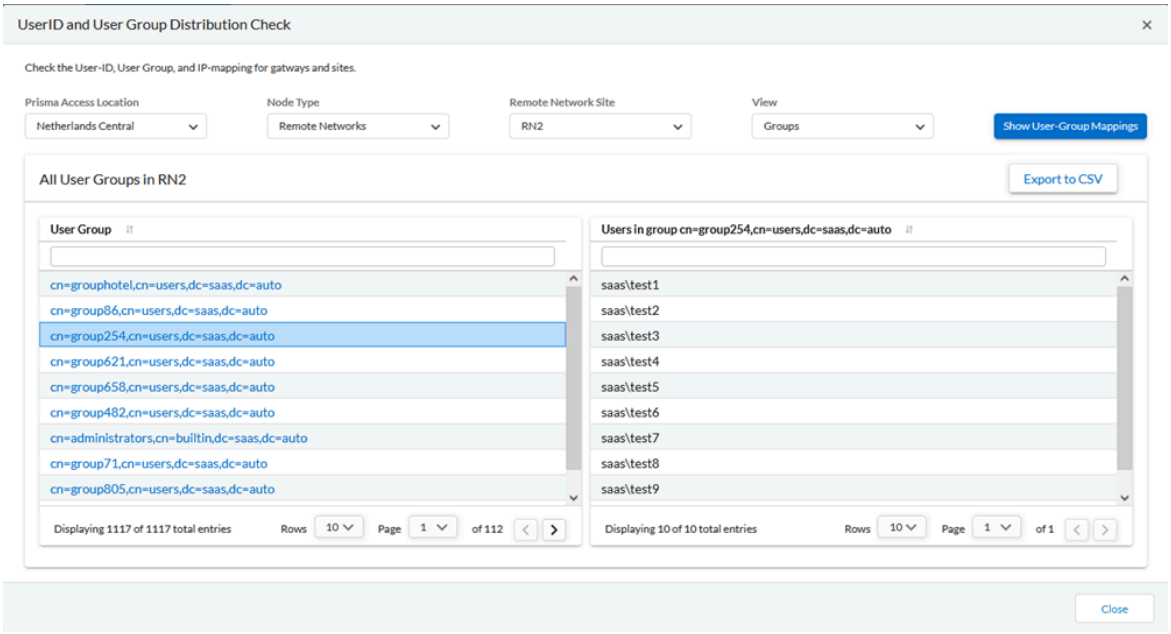
     Vous pouvez rechercher un groupe spécifique en tapant le nom du groupe ou une chaîne de caractères contenue dans le nom du groupe que vous souhaitez trouver en l'inscrivant dans la zone de texte **User Group (Groupe d'utilisateurs)**. Si vous recherchez un groupe qui n'existe pas, vous voyez une erreur disant : « No data is available » (Aucune donnée n'est disponible). Vous pouvez également trier la liste des groupes en basculant l'icône représentant les flèches en regard de **User Group (Groupe d'utilisateurs)**. Vous pouvez sélectionner le nombre d'entrées que vous souhaitez afficher, ainsi que faire défiler les pages en cliquant sur les flèches avant et arrière.

     Si vous sélectionnez **Groups (Groupes)**, la sélection **Show User-Group Mappings (Afficher les mappages utilisateur-groupes)** affiche tous les groupes disponibles dans le site sous **All User Groups in *<selected_site>*(Tous les groupes d'utilisateurs dans)**. Si vous sélectionnez un groupe, tous les utilisateurs appartenant au groupe sont affichés dans le volet de droite. Le bouton **Export to CSV (Exporter vers un fichier CSV)** devient activé, et vous pouvez exporter tous les utilisateurs appartenant à ce groupe dans un fichier CSV. Le fichier CSV exporté contient toutes les entrées du groupe, même si elles ne sont pas affichées dans l'interface utilisateur au moment de l'exportation.

     Vous pouvez rechercher un groupe spécifique en tapant le nom du groupe ou une chaîne de caractères contenue dans le nom du groupe que vous souhaitez trouver en l'inscrivant dans la zone de texte **User Group (Groupe d'utilisateurs)**. Si vous recherchez un groupe qui n'existe pas, vous voyez une erreur disant : « No data is available » (Aucune donnée n'est disponible). Vous pouvez également trier la liste des groupes en basculant l'icône représentant les flèches en regard de **User Group (Groupe d'utilisateurs)**. Vous pouvez

 ©2025 Palo Alto Networks, Inc.

sélectionner le nombre d'entrées que vous souhaitez afficher, ainsi que faire défiler les pages en sélectionnant les flèches avant et arrière.



Node Type (Type de nœud) : Utilisateurs mobiles (GlobalProtect)

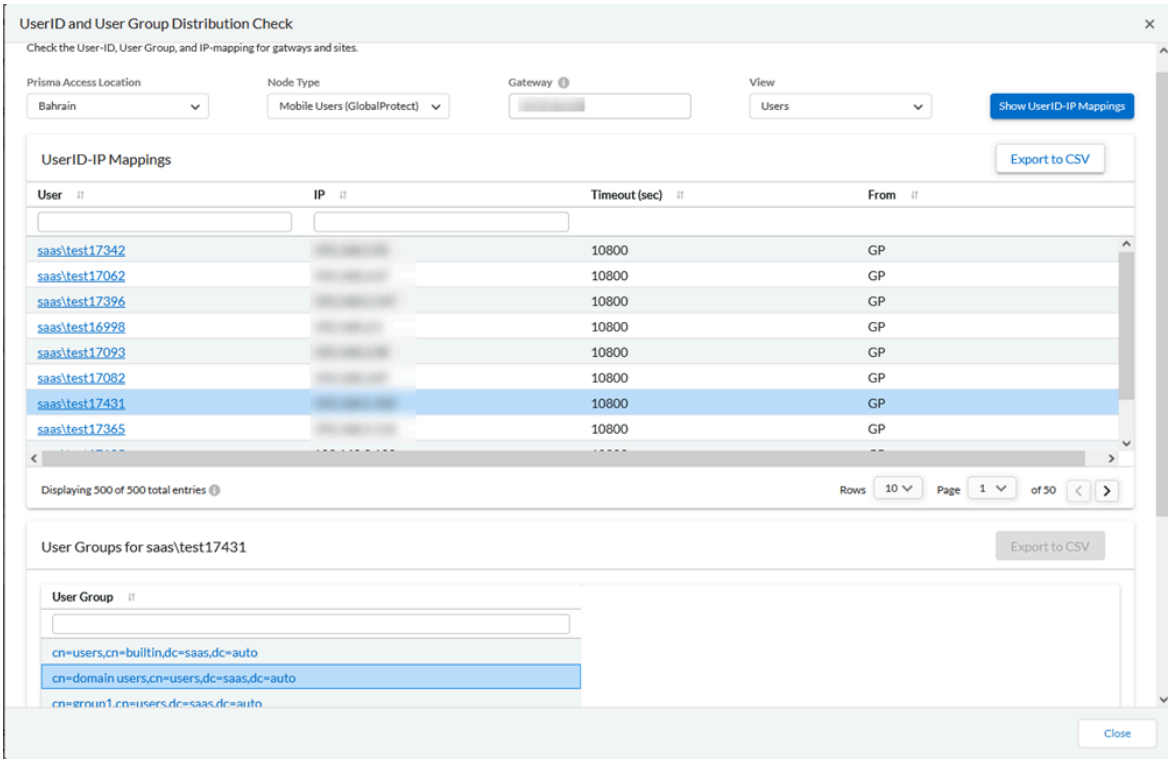
Vous pouvez voir le mappage ID utilisateur vers IP ainsi que le mappage ID utilisateur aux groupes d'utilisateurs. Le filtre **Prisma Access Location (Emplacement Prisma Access)** n'est pas pris en considération lorsque le **Node Type (Type de nœud)** sélectionné est **Mobile Users (GlobalProtect) (Utilisateurs mobiles (GlobalProtect))**. Prisma Access Insights utilise plutôt l'adresse IP de la passerelle GlobalProtect pour rechercher les données.

1. Saisissez une adresse de passerelle IP GlobalProtect dans la zone de texte **Gateway (Passerelle)**.
2. Sélectionnez si vous souhaitez **View (Afficher)** les données pour le mappage ID utilisateur vers IP utilisateur (**Users (Utilisateurs)**) ou les mappages ID utilisateur aux groupes d'utilisateurs (**Groups (Groupes)**) pour les utilisateurs connectés à votre passerelle GlobalProtect spécifiée.

   Si vous avez sélectionné **Users (Utilisateurs)**, sélectionnez **Show UserID-IP Mappings (Afficher les mappages ID utilisateur-IP)**. Un tableau du mappage ID utilisateur à son IP utilisateur est affiché avec le **Timeout (Délai d'expiration)**, qui vous montre combien de temps (en secondes) l'entrée ID utilisateur à IP utilisateur est valide. La sélection d'un utilisateur particulier affiche les groupes auxquels il appartient. La sélection d'un groupe affiche chaque utilisateur qui appartient à ce groupe. Elle active également le bouton **Export**

 ©2025 Palo Alto Networks, Inc.

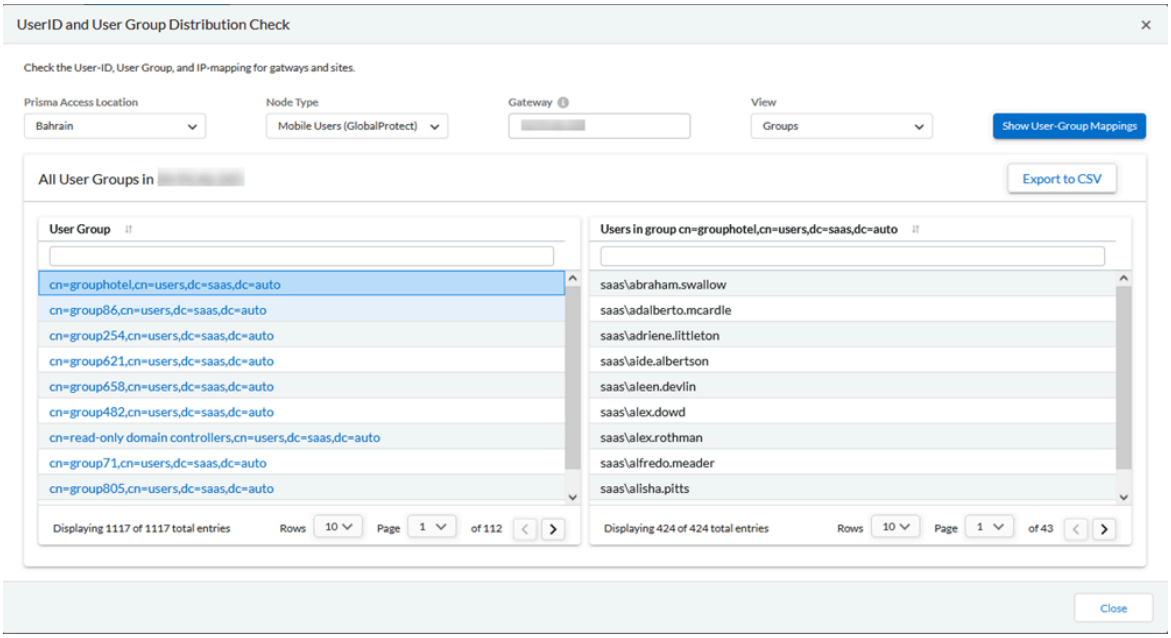
to CSV (Exporter vers un fichier CSV), qui vous permet d'exporter tous les utilisateurs de ce groupe indépendamment de toute vue filtrée affichée dans l'interface utilisateur.



Si vous avez sélectionné **Groups (Groupes)**, choisissez **Show User-Group Mappings (Afficher les mappages utilisateur-groupe)**. Une liste de tous les groupes d'utilisateurs appartenant à cette passerelle GlobalProtect apparaît sous **User Group (Groupe d'utilisateurs)**. La sélection d'un groupe d'utilisateurs affiche tous les utilisateurs appartenant à ce groupe dans le volet de droite. Elle active également le bouton **Export to**

 ©2025 Palo Alto Networks, Inc.

CSV (Exporter vers un fichier CSV), qui vous permet d'exporter tous les utilisateurs de ce groupe indépendamment de toute vue filtrée affichée dans l'interface utilisateur.



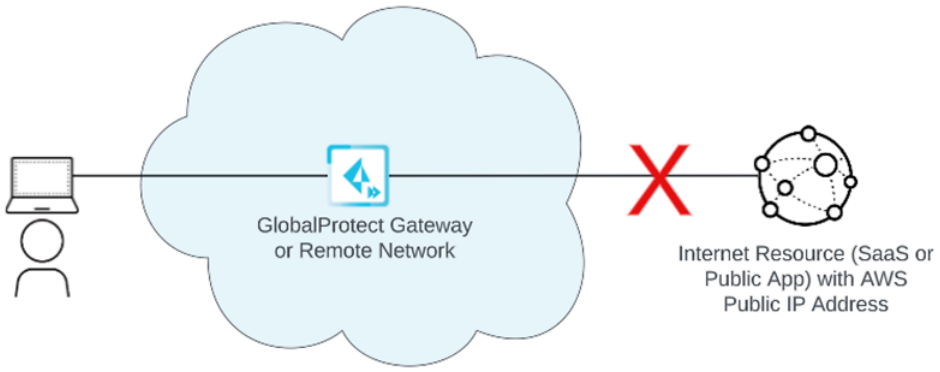
 ©2025 Palo Alto Networks, Inc.

Signaler les problèmes d'accès au site pour les utilisateurs mobiles

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Certains sites Web, tels que stubhub.com, ticketmaster.com ou dollartree.com, bloquent le trafic provenant de la plage d'adresses IP du cloud AWS. Lorsque les utilisateurs qui sont sécurisés par Prisma Access tentent d'accéder à ces sites Web, ils peuvent se voir refuser l'accès avec le message suivant sur le navigateur Web :

```
Accès refusé. Vous n'êtes pas autorisé à accéder à
 « http://www.dollartree.com/ » sur ce serveur. Référence
 #18.7f955b8.1509600370.44eb7c8
```



Pour signaler ce problème, entrez https://reportasite.gpcloudservice.com/ à partir d'un navigateur Web et fournissez l'URL du site Web inaccessible. Après 24 à 48 heures, retournez à https://reportasite.gpcloudservice.com/ et entrez la même URL pour voir son statut.

Palo Alto Networks vous fournit l'adresse IP utilisée par l'URL ; dans certains cas, vous devez ajouter cette adresse IP aux listes d'autorisation de votre organisation afin que ce trafic ne soit pas bloqué. Si vous avez des URL qui sont redirigées, ajoutez les adresses IP suivantes à vos listes d'autorisation :

- 65.154.226.160
- 154.59.126.110
- 66.232.36.110

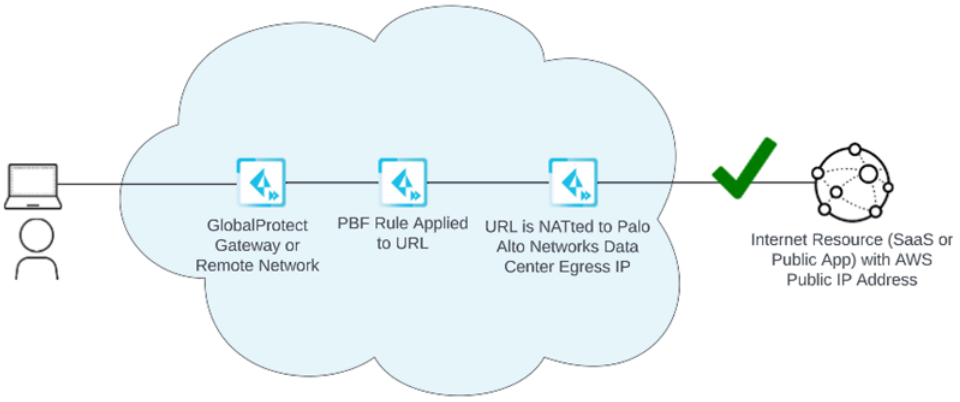
Prisma Access Processus de redirection d'URL

 ©2025 Palo Alto Networks, Inc.

Certains sites Web bloquent le trafic provenant d'une plage d'adresses IP cloud. Lorsque les utilisateurs qui sont sécurisés par Prisma Access tentent d'accéder à ces sites Web, ils peuvent se voir refuser l'accès. Afin de s'assurer que l'accès à ces sites Web est rétabli, Palo Alto Networks examine tous les sites signalés et, si un problème d'accès est détecté, catégorise le site et ajoute une politique de sortie qui attribue la traduction de l'adresse IP à une adresse accessible. Palo Alto Networks examine minutieusement les sites pour déterminer leur réputation et seuls les sites Web ayant une réputation irréprochable sont ajoutés à la règle de sortie, tandis que les autres sont rejetés, en utilisant ce processus :

1. Vous nous informez de l'URL avec des problèmes d'accès en utilisant https://reportasite.gpcloudservice.com/.
2. L'automatisation de l'ingénierie de la fiabilité du site (SRE) examine l'URL.
3. Si SRE détermine que l'URL est sûre, une règle de redirection basée sur des stratégies (PBF) est appliquée à l'URL et à son domaine parent.
4. Le trafic est acheminé via Prisma Access de la passerelle GlobalProtect ou du réseau distant vers un hub de traitement d'URL, où la règle PBF est appliquée au domaine, et du hub vers un centre de données de Palo Alto Networks.
5. Lorsque le trafic sort du centre de données, l'URL est la source NAT de l'adresse IP du centre de données.

À la suite de ces actions, le trafic à destination et en provenance des applications SaaS n'est pas abandonné, car l'adresse IP du centre de données a une bonne réputation.



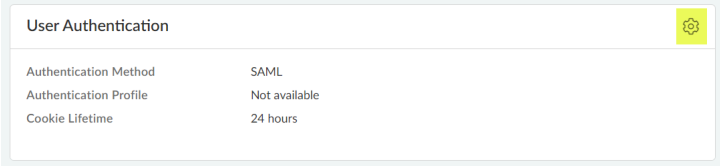
 ©2025 Palo Alto Networks, Inc.

Permettre aux utilisateurs mobiles de s'authentifier auprès de Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Vous pouvez authentifier les utilisateurs mobiles auprès de Prisma Access à l'aide de l'un des types d'authentification pris en charge. Suivez ces étapes pour configurer l'authentification pour les utilisateurs mobiles de GlobalProtect ou de proxy explicite.

STEP 1 | Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** et accédez à votre configuration de Utilisateurs mobiles : GlobalProtect ou de proxy explicite et **Set Up User Authentication (Configurez l'authentification utilisateur)**.



STEP 2 | Choisissez votre **Authentication Method (Méthode d'authentification)** parmi les types d'authentification pris en charge.

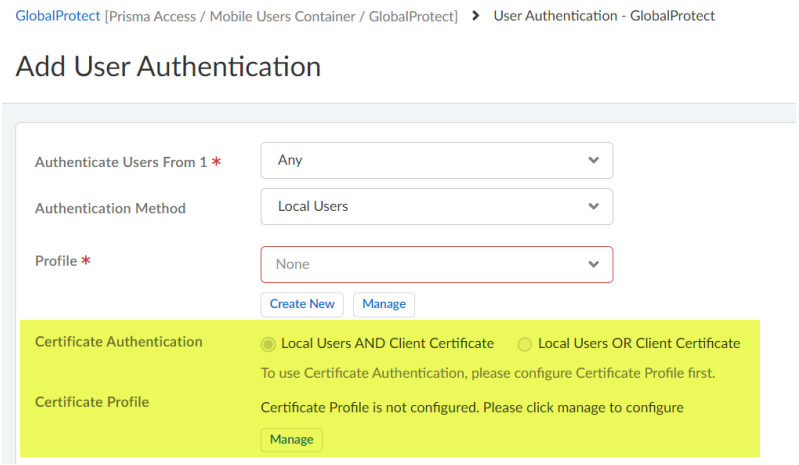
Si vous n'avez pas encore intégré Prisma Access à vos services d'authentification, voici comment.

STEP 3 | Choisissez le **Profile (Profil)** d'authentification que vous avez configuré pour permettre à Prisma Access de se connecter au service que vous souhaitez utiliser pour authentifier les utilisateurs.

- Spécifiez le **Profile (Profil)** d'authentification SAML si vous avez utilisé SAML à l'étape 2, ou créez un profil d'authentification SAML à utiliser avec Prisma Access.
- Spécifiez le **Profile (Profil)** d'authentification CIE si vous avez utilisé CIE à l'étape 2, ou créez un profil d'authentification CIE à utiliser avec Prisma Access.
- Spécifiez le **Profile (Profil)** d'authentification Kerberos si vous avez utilisé Kerberos à l'étape 2, ou créez un profil d'authentification Kerberos à utiliser avec Prisma Access.

©2025 Palo Alto Networks, Inc.

STEP 4 | Spécifiez les paramètres d'authentification du certificat :



- **Authentification du certificat**

  Pour une sécurité renforcée, utilisez un certificat (en plus de votre service d'authentification) pour obtenir des noms d'utilisateur et authentifier les utilisateurs dans Prisma Access. Pour authentifier les utilisateurs sur la base d'un certificat client, un des champs de certificat, tel que le champ Subject Name (Nom du sujet), doit identifier le nom d'utilisateur. Les utilisateurs mobiles qui s'authentifient au moyen de l'authentification par certificat client n'ont pas la possibilité de se déconnecter de l'application GlobalProtect.

  Avec Prisma Access, vous pouvez choisir d'exiger que les utilisateurs mobiles passent à la fois l'authentification par certificat et l'authentification basée sur le type d'authentification ou d'accorder l'accès aux utilisateurs mobiles à condition qu'ils aient passé une seule de ces vérifications.

- **Profil du certificat**

  Utilisez un profil de certificat facultatif pour vérifier les certificats que les utilisateurs mobiles présentent à Prisma Access avec une requête de connexion. Le profil de certificat spécifie le contenu des champs nom d'utilisateur et domaine utilisateur ; répertorie les certificats d'AC ; critères de blocage d'une session ; et offre des manières de déterminer l'état de révocation des certificats d'AC. Étant donné que le certificat fait partie de l'authentification de l'utilisateur mobile, vous devez pré-déployer les certificats utilisés dans les profils de certificat pour vos utilisateurs avant leur connexion initiale. Le profil de certificat spécifie quel champ de certificat contient le nom d'utilisateur (Subject ou Subject Alt). Si le profil de certificat indique Sujet dans le champ Nom d'utilisateur, le certificat présenté par le point de terminaison doit contenir un nom commun pour que le point de terminaison puisse se connecter. Si le profil de certificat indique Subject-Alt avec un Email (e-mail) ou un Principal Name (nom principal) pour le champ Username (nom d'utilisateur), le certificat doit contenir les champs correspondants, qui seront utilisés pour le nom d'utilisateur lorsque l'application GlobalProtect s'authentifie sur Prisma Access.

STEP 5 | Spécifiez une **Cookie Lifetime (Durée de vie de cookie)** pour le cookie qui stocke les informations d'authentification des utilisateurs.

Une fois que l'IdP a authentifié l'utilisateur, Prisma Access stocke l'état d'authentification de l'utilisateur dans le service de cache d'authentification (authentication cache service, ACS). La

 ©2025 Palo Alto Networks, Inc.

période de validité de l'authentification est basée sur la valeur **Cookie Lifetime (Durée de vie du cookie)** que vous spécifiez ici.

Pour éviter les problèmes empêchant les utilisateurs de télécharger des fichiers volumineux avant l'expiration de la durée de vie du cookie, ou l'expiration du cookie lorsque les utilisateurs accèdent à un seul site Web pendant une longue période, Palo Alto Networks vous recommande de configurer une durée de vie du cookie d'au moins un jour. Si les utilisateurs de proxy explicite rencontrent un problème d'expiration de la durée de vie des cookies, ils peuvent accéder à un autre site Web pour se réauthentifier auprès d'ACS et actualiser le cookie ACS.

Support et fonctionnalités d'authentification

Les services qui s'intègrent avec Prisma Access afin de fournir l'authentification, et les fonctionnalités à prendre en compte lorsque vous planifiez votre configuration d'authentification sont énumérés ci-après :

Appui à l'authentification :

- Moteur d'identité sur le cloud
- SAML
- TACACS+
- RADUIS
- LDAP
- Kerberos
- MFA
- Authentification de base de données locale

Caractéristiques de la fonctionnalité d'authentification :

- SSO
- Portail d'authentification
- Séquence d'authentification

Appui à l'authentification

Moteur d'identité sur le cloud	Vous déployez Cloud Identity Engine pour l'authentification des utilisateurs en configurant un fournisseur d'identité (identity provider, IdP) basé sur SAML 2.0, une chaîne de certificats et d'autorités de certification (certificate authority, CA) client ou les deux. Après avoir spécifié comment vous souhaitez authentifier vos utilisateurs, configurez votre profil d'authentification pour définir votre politique de sécurité d'authentification et configurez éventuellement la politique

 ©2025 Palo Alto Networks, Inc.

	d'authentification sur votre pare-feu ou Panorama.
SAML	Si vos utilisateurs accèdent à des services et à des applications qui se trouvent à l'extérieur de votre réseau, vous pouvez utiliser SAML pour intégrer Prisma Access à un fournisseur d'identité (identity provider, IdP) qui contrôle l'accès aux services et aux applications internes et externes. Single Sign-On (ouverture de session unique - SSO) SAML permet à un seul utilisateur d'accéder à plusieurs applications. Elle est utile dans les environnements où chaque utilisateur accède à de nombreuses applications et où l'authentification pour chacune d'entre elles entraverait la productivité de l'utilisateur. Dans ce cas, Single Sign-On (ouverture de session unique - SSO) SAML permet à une connexion d'accéder à plusieurs applications. Dans le même ordre idée, le service de déconnexion unique (SLO) en SAML permet de fermer une session accédant à plusieurs applications en se déconnectant d'une seule session. SSO fonctionne pour les utilisateurs mobiles qui accèdent aux applications via l'application GlobalProtect. De même que les utilisateurs des réseaux distants qui accèdent aux applications via le portail d'authentification. SLO est disponible pour les utilisateurs de l'application GlobalProtect. *Vous ne pouvez pas utiliser les profils d'authentification SAML pour des séquences d'authentification.*
TACACS+	Terminal Access Controller Access-Control System Plus (TACACS+) est une famille de protocoles permettant une authentification et une autorisation à partir d'un serveur centralisé. TACACS+ crypte les noms d'utilisateurs et mots de passe, assurant ainsi une meilleure sécurité que RADIUS, qui crypte uniquement les mots de passe. TACACS+ est aussi plus fiable car il utilise le protocole TCP, alors que RADIUS utilise le protocole UDP.

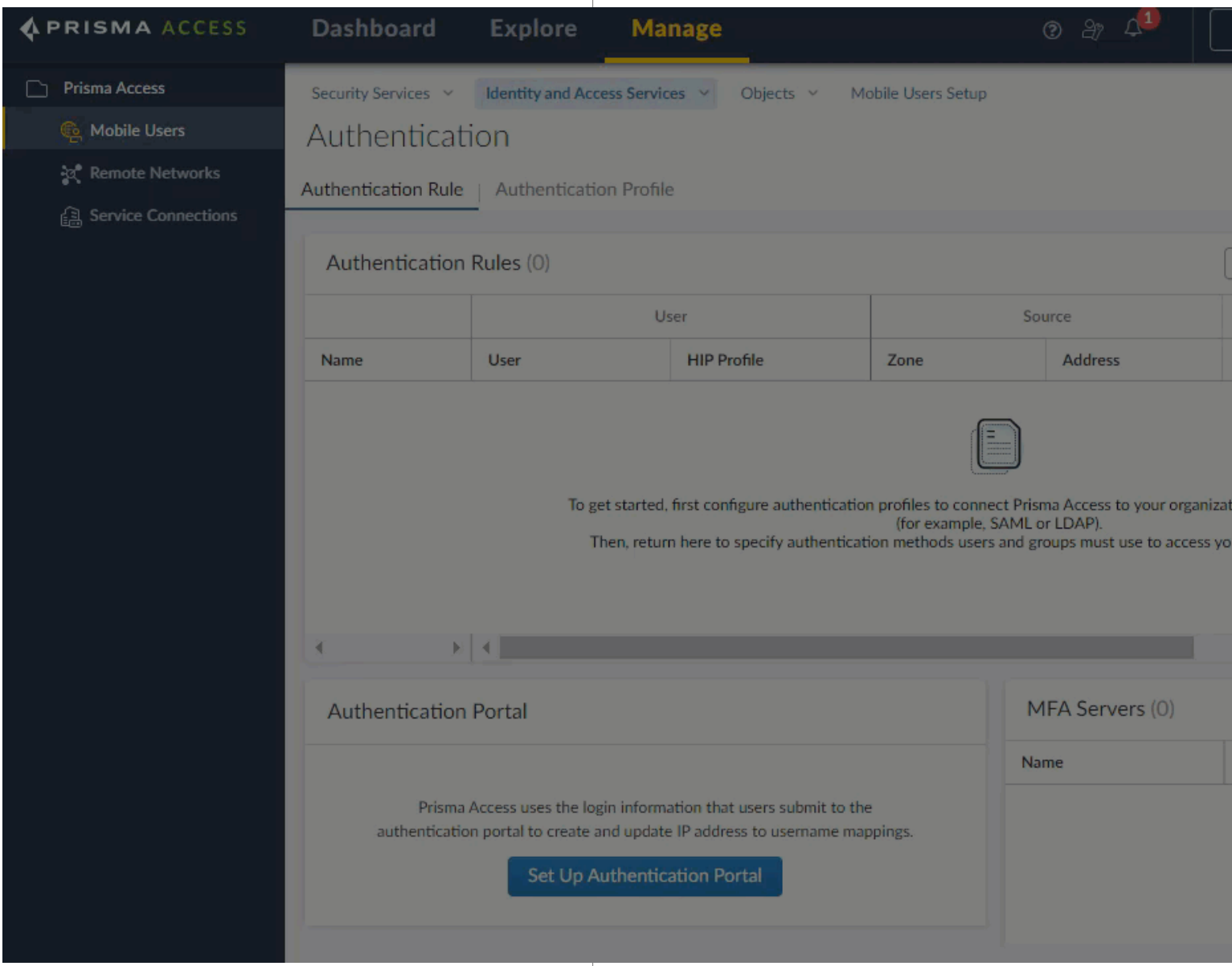
 ©2025 Palo Alto Networks, Inc.

RADIUS	Radius (Remote Authentication Dial-In User Service) est un protocole réseau bénéficiant d'un large support et fournissant une authentification et une autorisation centralisées. Vous pouvez également ajouter un serveur RADIUS à Prisma Access pour implémenter une authentification multi-facteurs.
LDAP	LDAP (Lightweight Directory Access Protocol) est un protocole standard d'accès aux répertoires d'informations. Vous pouvez utiliser LDAP pour authentifier les utilisateurs qui accèdent à des applications ou des services via le portail d'authentification.
Kerberos	Kerberos est un protocole d'authentification qui permet un échange sécurisé d'informations entre les parties en utilisant des clés uniques (appelées tickets) pour identifier les parties. Avec Kerberos, vous pouvez authentifier les utilisateurs qui accèdent aux applications via le portail d'authentification. Lorsque la SSO Kerberos est activée, l'utilisateur doit se connecter uniquement pour un premier accès au réseau (par exemple, une connexion à Microsoft Windows). À l'issue de cette première connexion, l'utilisateur peut accéder à n'importe quel service basé sur un navigateur dans le réseau sans avoir à se connecter à nouveau jusqu'à l'expiration de la session SSO. Pour utiliser Kerberos, vous devez d'abord avoir un compte Kerberos pour Prisma Access qui authentifiera les utilisateurs. Un compte permet de créer un keytab Kerberos qui est un fichier contenant le nom principal et le mot de passe haché du pare-feu ou de Panorama. Un keytab est indispensable au processus SSO. Kerberos SSO est disponible uniquement pour les services et les applications internes à votre environnement Kerberos. Lorsque la SSO est activée pour des services et applications externes, il est possible d'utiliser SAML.
MFA	L'authentification multi-facteurs (MFA) vous permet de mettre en œuvre plusieurs défis d'authentification de différents types (appelés *facteurs*) pour protéger vos services

 ©2025 Palo Alto Networks, Inc.

et applications les plus sensibles. Par exemple, vous pourriez souhaiter disposer d'une authentification plus forte pour les documents financiers clés que pour les moteurs de recherche.

Prisma Access dispose d'une liste intégrée des fournisseurs MFA pris en charge. Cette liste est automatiquement mise à jour au fur et à mesure que de nouveaux fournisseurs sont ajoutés :



Authentification de base de données locale	Créez une base de données qui s'exécute localement sur Prisma Access et contient des comptes d'utilisateurs (noms d'utilisateur et mots de passe ou mots de passe hachés)

 ©2025 Palo Alto Networks, Inc.

	et des groupes d'utilisateurs. Ce type d'authentification est utile pour créer des comptes d'utilisateurs qui réutilisent les informations d'identification des comptes Unix existants dans les cas où vous connaissez uniquement les mots de passe hachés, pas les mots de passe en texte brut. Pour les comptes utilisant des mots de passe en clair, vous pouvez également définir la complexité du mot de passe et les paramètres d'expiration. Cette méthode d'authentification est disponible pour les utilisateurs qui accèdent aux services et applications via le portail d'authentification ou l'application GlobalProtect.

Caractéristiques de la fonctionnalité d'authentification

SSO	Si vous utilisez SAML ou Kerberos, vous pouvez mettre en œuvre une Single Sign-On (ouverture de session unique - SSO), qui permet aux utilisateurs de ne s'authentifier qu'une seule fois pour accéder à plusieurs services et applications. SAML et Kerberos prennent en charge la SSO.
Portail d'authentification	Redirigez les requêtes web qui correspondent à une règle d'authentification vers une page de connexion Prisma Access où elles sont invitées à s'authentifier. Prisma Access utilise les informations que l'utilisateur soumet à ce portail d'authentification pour créer ou mettre à jour des mappages adresse IP/nom d'utilisateur. Ceci est particulièrement utile pour les réseaux distants, afin que vous continuiez à surveiller et à appliquer le trafic en fonction d'un utilisateur (ou d'un groupe). Lorsqu'un utilisateur lance un trafic web (HTTP ou HTTPS) correspondant à une règle d'authentification, Prisma Access invite l'utilisateur à s'authentifier via le portail d'authentification. Prisma Access crée ou met à jour le mappage nom d'utilisateur/adresse IP en fonction des informations que l'utilisateur soumet au portail. Cela vous permet de savoir exactement qui accède à vos applications et données les plus sensibles à partir d'un site réseau distant.

 ©2025 Palo Alto Networks, Inc.

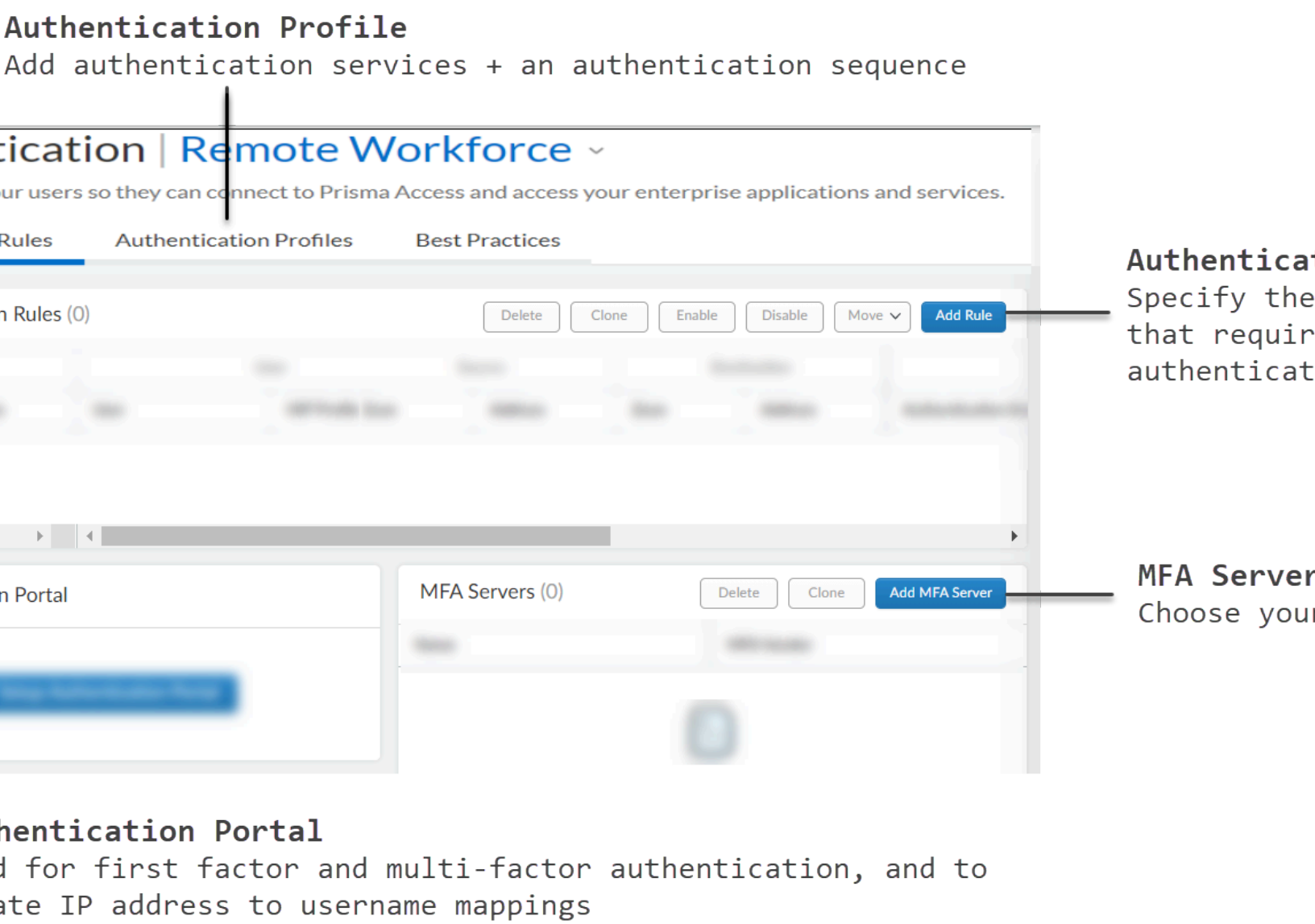
Séquence d'authentification	Si vous utilisez plusieurs types d'authentification à des fins différentes, vous pouvez définir une séquence d'authentification pour classer vos profils. Prisma Access vérifie chaque profil en fonction de votre classement jusqu'à ce qu'un authentifie l'utilisateur avec succès.

Configurer l'authentification

Pour configurer l'authentification avec Prisma Access, ajoutez d'abord votre ou vos services d'authentification à Prisma Access. Spécifiez ensuite le trafic pour lequel vous souhaitez exiger une authentification. Ces paramètres permettent d'ajouter d'autres fonctionnalités d'authentification, telles que MFA, des séquences d'authentification, ou d'activer Prisma Access pour créer et mettre à jour les mappages adresses IP à nom d'utilisateur.

Voici comment commencer—tous les paramètres dont vous avez besoin pour activer l'authentification avec Prisma Access se trouvent au même endroit : **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Authentication (Authentification)**. Sélectionnez la portée de la configuration **Prisma Access**.

 ©2025 Palo Alto Networks, Inc.



- **Règles d'authentification** C'est ici que vous spécifiez le trafic pour lequel vous souhaitez exiger une authentification

  La configuration d'une règle d'authentification inclut l'ajout d'un profil d'authentification à la règle. Lorsque Prisma Access détecte un trafic correspondant à une règle d'authentification, il applique les méthodes et paramètres d'authentification définis dans le profil d'authentification au trafic correspondant. Le profil est l'élément qui définit la manière dont les utilisateurs devront s'authentifier.

  1. Allez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Authentication (Authentification)** > **Authentication Rule (Règle d'authentification)** et **Add Authentication Rule (Ajouter une règle d'authentification)**. Sélectionnez la portée de la configuration **Prisma Access**.

©2025 Palo Alto Networks, Inc.

2. Définissez les utilisateurs, les services et les catégories d'URL qui nécessitent une authentification.
3. Attribuez la valeur **Authenticate (Authentifier)** à l'action de la règle et choisissez le **Profile (Profil)** qui définit la méthode d'authentification que vous souhaitez utiliser pour le trafic correspondant à cette règle.



- **Profil d'authentification** Ajoutez vos services d'authentification ici et définissez les paramètres d'authentification

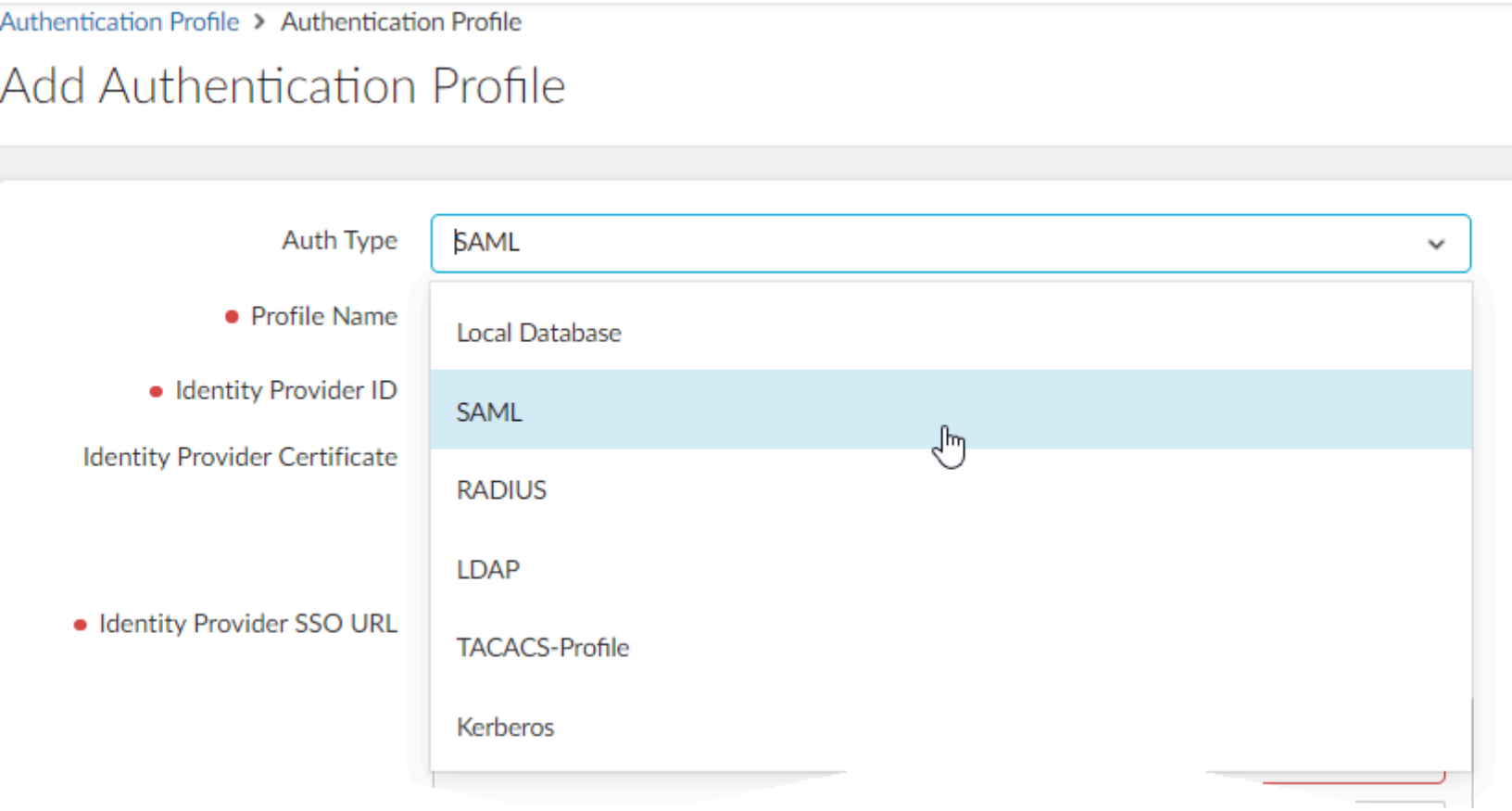
  Connectez Prisma Access aux services que vous souhaitez utiliser pour authentifier les utilisateurs—SAML, TACACS+, RADIUS, LDAP ou Kerberos—et définissez les paramètres

 ©2025 Palo Alto Networks, Inc.

d'authentification (par exemple, définissez une limite pour les tentatives de connexion infructueuses).

Si vous utilisez un service d'authentification sur site, vous devez d'abord créer une connexion aux services pour connecter le service d'authentification sur site à Prisma Access. Revenez ici par la suite pour configurer votre profil d'authentification.

Allez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Authentication (Authentification)** > **Authentication Profile (Profil d'authentification)** > **Add Profile (Ajouter un profil)** et commencez en paramétrant le profil **Auth Type (Type d'authentification)**. Sélectionnez la portée de la configuration **Prisma Access** :



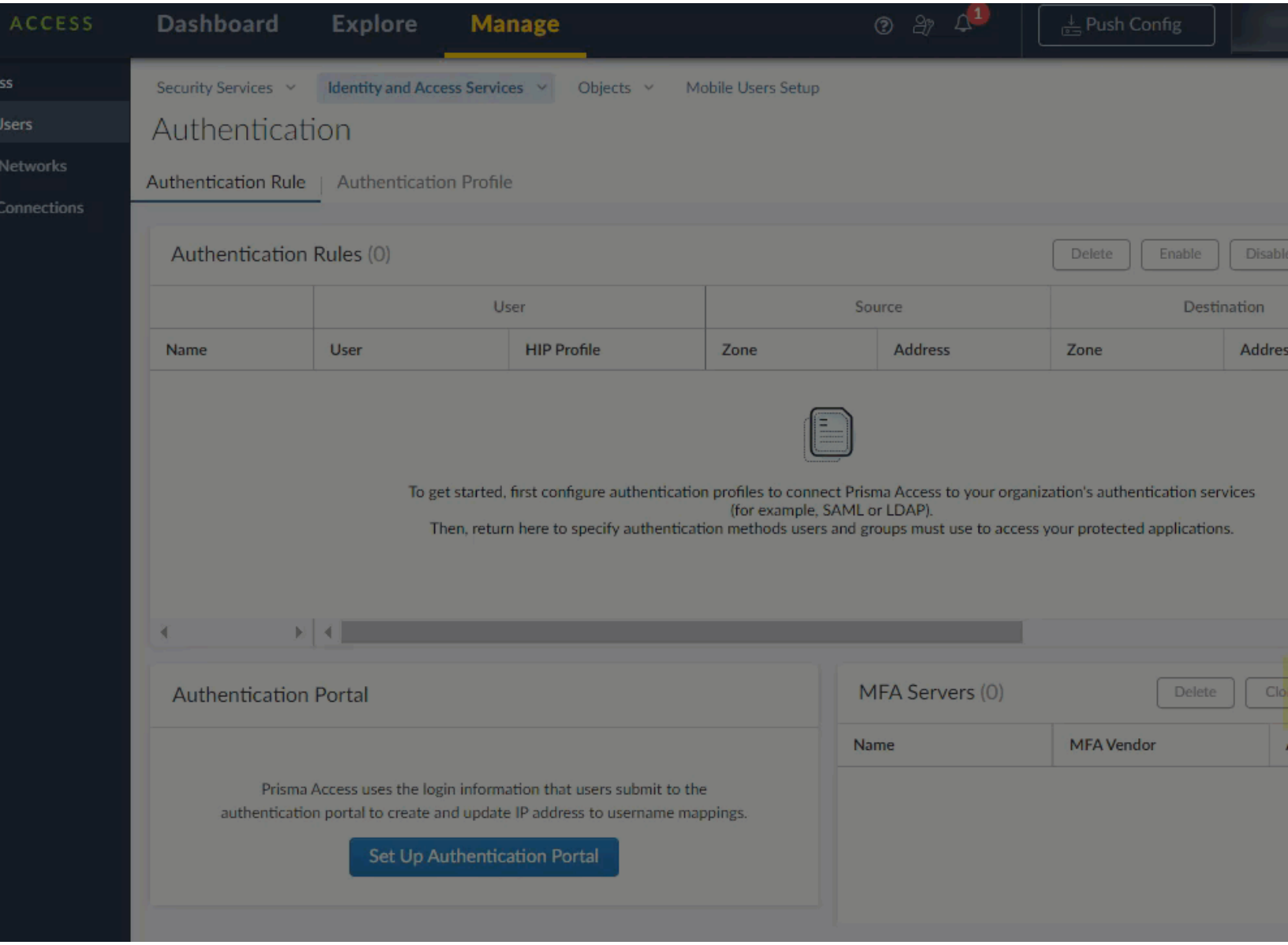
Vous serez invité à ajouter des détails sur le service d'authentification que vous avez choisi et qui activera Prisma Access pour vous connecter au service et lire les informations d'identification de l'utilisateur et les autorisations de rôle. Des paramètres supplémentaires pour personnaliser l'authentification sont fournis dans le profil et peuvent varier en fonction du type d'authentification que vous configurez.

- **Serveurs MFA** Spécifiez le fournisseur MFA que vous utilisez

  Pour utiliser plusieurs méthodes d'authentification des utilisateurs auprès d'applications sensibles, commencez par ajouter les fournisseurs MFA que vous souhaitez utiliser (**Add MFA**

 ©2025 Palo Alto Networks, Inc.

Server (Ajouter un serveur MFA)). Prisma Access fournit une liste de fournisseurs MFA parmi lesquels vous pouvez choisir.



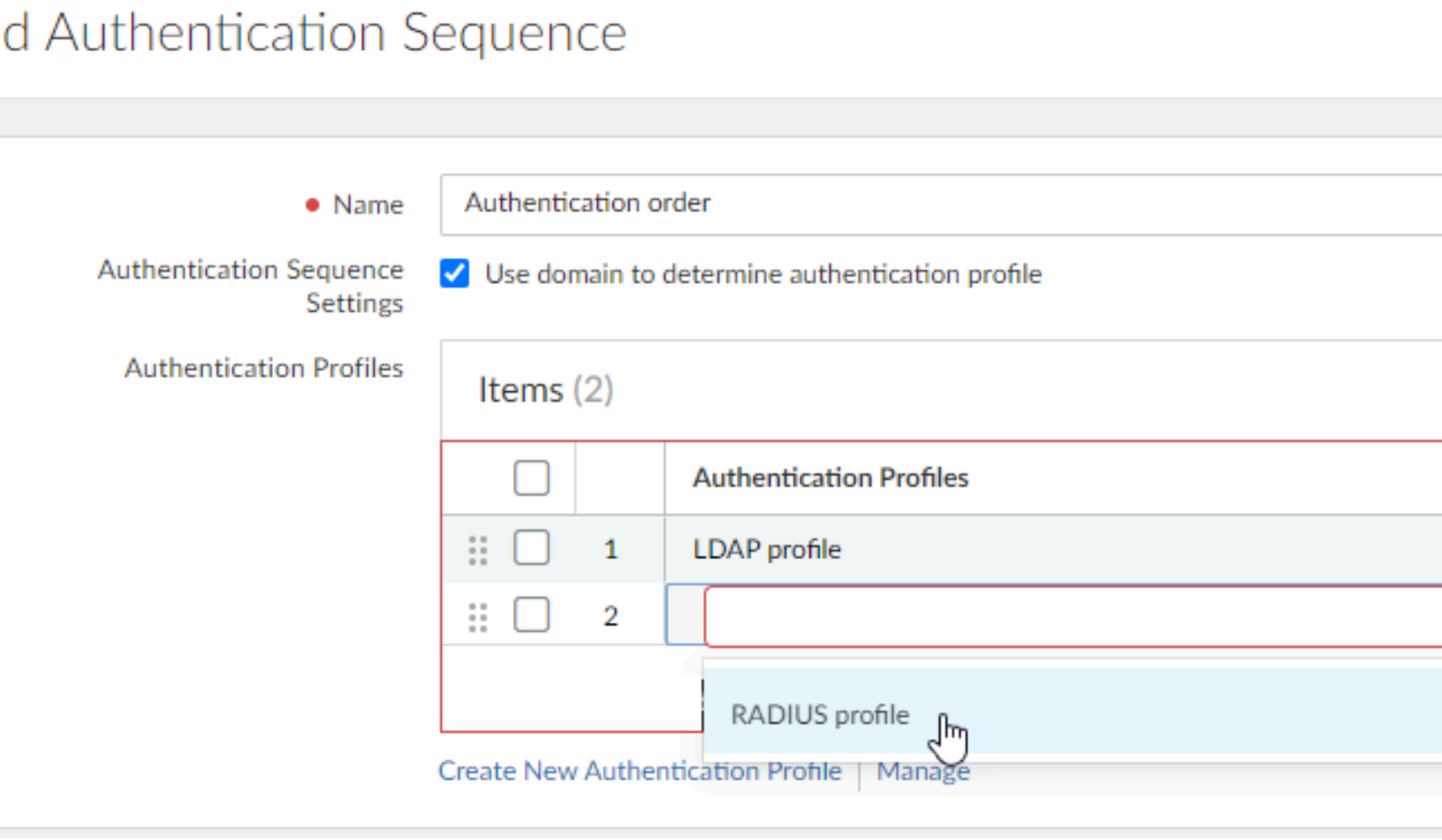
- **Portail d'authentification** Configurez le portail d'authentification (anciennement appelé *Portail captif*) pour les utilisateurs des sites réseau distants et activez Prisma Access pour créer des mappages adresse IP à nom d'utilisateurs

  Pour l'authentification à premier facteur (identifiant et mot de passe), les utilisateurs des sites réseau distants doivent s'authentifier via le portail d'authentification. Si l'authentification réussit, Prisma Access affiche une page de connexion MFA pour chaque facteur d'authentification supplémentaire requis. Prisma Access utilise les informations d'identification soumises par les utilisateurs pour créer et mettre à jour les mappages adresse IP à nom d'utilisateur. Cela signifie que vous saurez toujours qui, sur un site distant du réseau, accède au contenu Web et aux applications d'entreprise.

 ©2025 Palo Alto Networks, Inc.

- **Séquence d'authentification** Classez les profils d'authentification dans l'ordre dans lequel vous souhaitez que Prisma Access les essaie

  Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Authentication (Authentification)** > **Authentication Profile (Profil d'authentification)** > **Add Authentication Sequence (Ajouter séquence d'authentification)**. Sélectionnez la portée de configuration **Prisma Access**. Prisma Access vérifie chacun d'eux dans l'ordre jusqu'à ce que l'un d'eux authentifie l'utilisateur.



 ©2025 Palo Alto Networks, Inc.

Permettre aux utilisateurs mobiles d'accéder aux ressources de l'entreprise

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	• Licence Prisma Access

L'activation de Prisma Access pour l'accès Internet uniquement pour les utilisateurs ne nécessite aucune configuration de services réseau, car Prisma Access fournit un pool d'adresses IP par défaut et un serveur DNS cloud par défaut.

Cependant, si vous souhaitez que vos utilisateurs mobiles puissent accéder aux ressources internes de votre siège social, de vos centres de données ou de sites réseau distants sur lesquels vous avez intégré Prisma Access, vous devrez :

- ❑ définir les pools d'adresses IP que Prisma Access utilise pour attribuer des adresses IP à vos utilisateurs mobiles,
- ❑ configurer l'infrastructure de services de Prisma Access,
- ❑ et, pour permettre l'accès à votre siège social ou à vos centres de données, intégrer des connexions aux services.

Si vous souhaitez que vos utilisateurs mobiles se connectent à des sites de réseau distant, vous devez configurer au moins une connexion aux services, même si vous ne prévoyez pas d'utiliser la connexion pour fournir un accès à votre centre de données ou à vos sièges sociaux. Bien que toutes les branches soient entièrement maillées, les connexions des utilisateurs mobiles ne le sont pas. La création d'une connexion aux services établit l'architecture en étoile requise pour permettre au trafic des utilisateurs mobiles d'être acheminé vers vos réseaux de branche. Dans ce cas, vous pouvez configurer au minimum la connexion aux services comme suit :

- Lorsque vous intégrez la connexion aux services, utilisez un emplacement Prisma Access proche de vos utilisateurs mobiles.
- Lorsque vous configurez le tunnel IPSec principal de la connexion aux services, configurez les paramètres d'authentification d'homologue et de tunnel IPSec à l'aide de valeurs d'espace réservé.
- Lorsque vous activez le routage et la QoS pour la connexion aux services, ajoutez des sous-réseaux IP d'espace réservé.

  Parce que Prisma Access n'achemine aucun trafic via ce tunnel, assurez-vous simplement que le sous-réseau IP que vous utilisez n'entre pas en conflit ou ne chevauche pas d'autres sous-réseaux configurés connectés à Prisma Access.

STEP 1 | Accédez à **Manage (Gérer)** > **Mobile Users (Utilisateurs mobiles)** > **Mobile Users Setup (Configuration des utilisateurs mobiles)** et modifiez les **Infrastructure Settings (Paramètres d'infrastructure)** pour ajuster les paramètres du réseau pour les utilisateurs mobiles.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Vérifiez ou ajustez le **Client IP Pool (Pool d'adresses IP client)** que Prisma Access utilise pour attribuer des adresses IP aux utilisateurs mobiles.

- Par défaut, un pool d'adresses IP **Worldwide (Mondial)** est disponible pour tous les utilisateurs mobiles.
- Vous pouvez **Customize per region (Personnaliser par région)** pour utiliser une configuration de pools d'IP dédiée aux régions ou aux emplacements. Pour les régions ou les emplacements pour lesquels vous ne spécifiez pas de pool d'IP, Prisma Access utilise le pool d'IP mondial.

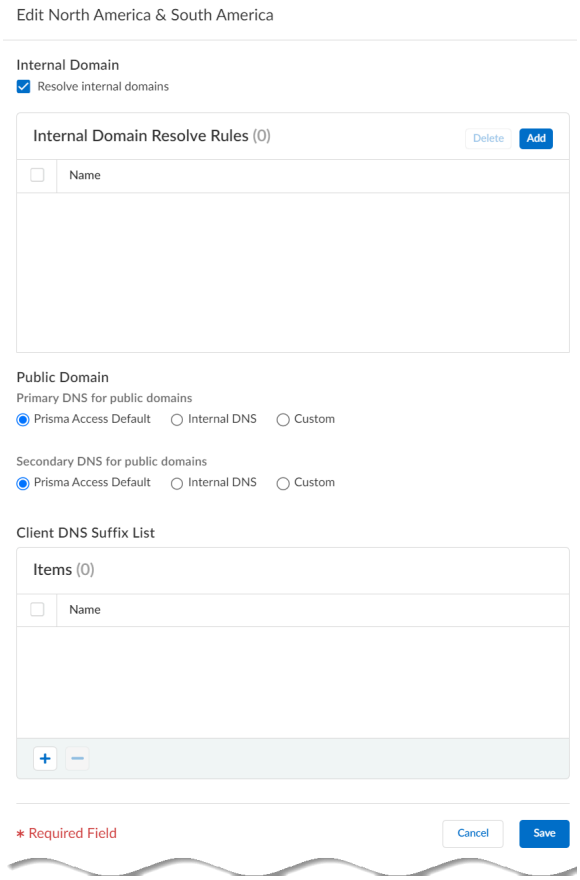
Les pools d'adresses IP que vous définissez doivent répondre aux exigences suivantes :

- Il est recommandé de définir des pools d'adresses IP conformes à la RFC 1918 pour éviter les conflits d'adresses IP.
- Assurez-vous que les pools d'adresses IP que vous définissez ne chevauchent pas d'autres adresses IP que vous utilisez en interne.
- Assurez-vous que les pools d'adresses IP que vous définissez ne chevauchent pas le pool d'adresses IP d'infrastructure que vous utilisez pour Prisma Access.
- Ne spécifiez aucun sous-réseau qui chevauche 169.254.0.0/16 et la plage de sous-réseaux 100.64.0.0/10, car Prisma Access réserve ces adresses IP et sous-réseaux à son usage interne.
- Assurez-vous de désigner un pool d'adresses IP qui permet une couverture suffisante pour tous les utilisateurs mobiles de votre organisation, en fonction des directives suivantes :
- Si vous prévoyez d'utiliser un pool d'adresses mondial déployé dans une ou deux régions, le pool d'adresses IP minimum requis est /23 (adresse IP 512).
- Si vous prévoyez d'utiliser un pool d'adresses mondial déployé dans trois régions ou plus, le pool d'adresses IP minimum requis est /19 (8 192 adresses IP), soit dans un pool d'adresses IP unique, soit réparti sur plusieurs pools.
- Si vous prévoyez de définir des pools d'adresses IP par région, la taille minimale du pool dans n'importe quelle région est /23 (512 adresses IP).
- Vous n'avez pas besoin d'attribuer un pool d'adresses IP dans les régions où vous ne prévoyez pas de déployer Prisma Access. Par exemple, sélectionnez les régions USA Est (Virginie du Nord), USA Est (Ohio) et USA Ouest (Californie du Nord) uniquement lorsque vous intégrez Prisma Access pour les utilisateurs, vous devez spécifier un pool d'adresses IP pour la région Amériques uniquement. Gardez toutefois à l'esprit que les utilisateurs d'autres régions ne pourront pas se connecter à Prisma Access.
- Si vous prévoyez de définir un mélange de pools mondiaux et régionaux, assurez-vous d'allouer au moins 512 adresses IP par région. Par exemple, pour un déploiement sur trois régions, vous pouvez spécifier 1 024 adresses dans la région Europe et 512 adresses dans le monde entier.
- Il est recommandé de désigner des pools d'adresses IP afin de disposer d'au moins une adresse IP pour chaque utilisateur mobile unique de votre organisation afin qu'ils puissent se connecter simultanément. Si vous désignez un pool d'adresses IP qui comporte un nombre d'adresses IP inférieur au nombre d'utilisateurs sous licence, Prisma Access affichera un message d'avertissement. Cependant, si vous disposez d'un pool d'adresses IP limité et que vous ne prévoyez pas que tous les utilisateurs se connectent simultanément, vous pouvez contourner le message et utiliser une taille de pool plus petite.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Ajoutez les paramètres de **Client DNS (DNS du client)** : vous pouvez utiliser la valeur par défaut **Worldwide (mondial)** ou personnaliser les paramètres en fonction de la région.

Sélectionnez la région pour laquelle vous souhaitez personnaliser les paramètres DNS :



Cochez l'option permettant d'utiliser ces paramètres DNS pour **Resolve internal domains (Résoudre les domaines internes)** et éventuellement **Use the internal DNS Server for resolving public domains too (Utiliser le serveur DNS interne pour résoudre également les domaines publics)**. Si vous ne sélectionnez pas cette option, Prisma Access utilise ses serveurs DNS cloud par défaut pour résoudre les requêtes de domaines publics.

Le proxy DNS dans Prisma Access envoie les requêtes aux serveurs DNS que vous spécifiez. L'adresse source dans la requête DNS est la première adresse IP du pool d'IP que vous attribuez à la région. Pour garantir que vos requêtes DNS peuvent atteindre les serveurs, vous devez vous assurer que vous autorisez le trafic provenant de toutes les adresses de votre pool d'adresses IP d'utilisateurs mobiles vers vos serveurs DNS.

STEP 4 | Si vous souhaitez que vos utilisateurs mobiles puissent accéder aux ressources de votre siège social, de vos réseaux de centres de données ou d'autres branches, vous devez configurer les Paramètres d'infrastructure de Prisma Access pour activer la dorsale du réseau.

Accéder à **Manage (Gérer)** > **Prisma Access** > **Prisma Access Setup (Configuration Prisma Access)**.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Pour permettre aux utilisateurs mobiles d'accéder aux ressources de votre siège social ou de vos centres de données, créez des connexions aux services pour connecter ces sites à Prisma Access.

Accédez à **Manage (Gérer)** > **Service Connections (Connexions aux services)** > **Service Connections Setup (Configuration des connexions aux services)**.

STEP 6 | Lorsque vous êtes prêt, **Push Config (Transmettez la configuration)** vers Prisma Access pour enregistrer vos paramètres d'utilisateurs mobiles.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Prisma Access Réseaux distants

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

À mesure que votre entreprise se développe et que vos bureaux sont répartis géographiquement, Prisma Access pour les réseaux vous permet d'intégrer rapidement vos sites réseau distants et de fournir une sécurité de premier ordre pour vos utilisateurs. Il offre une option pratique qui élimine la complexité de la configuration et de la gestion des périphériques à chaque emplacement distant. Le service offre un moyen efficace d'ajouter facilement de nouveaux emplacements de réseau distant et de minimiser les défis opérationnels liés à la garantie que les utilisateurs de ces emplacements sont toujours connectés et en sécurité, et il vous permet de gérer la politique de manière centralisée depuis Panorama pour une sécurité cohérente et rationalisée de vos emplacements de réseau distant.

Pour connecter vos emplacements réseau distants à Prisma Access, vous pouvez utiliser le pare-feu de nouvelle génération de Palo Alto Networks ou un périphérique tiers conforme à l'IPSec, y compris SD-WAN, qui peut établir un tunnel IPSec vers le service.

En plus de la connectivité des tunnels IPSec, Prisma SD-WAN vous permet d'utiliser un CloudBlade que vous intégrez en tant que réseau distant pour connecter le contrôleur Prisma SD-WAN et les périphériques ION avec Prisma Access.

Liste de contrôle de planification pour les réseaux distants

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Avant de commencer à intégrer les réseaux distants, veillez à ce que les éléments de configuration suivants soient prêts pour vous assurer d'être en mesure d'activer correctement le service et d'appliquer la politique pour les utilisateurs dans vos emplacements de réseaux distants :

- **Vous avez besoin d'accéder aux ressources d'entreprise ?**

  Si votre réseau distant nécessite un accès à l'infrastructure ou aux ressources de votre siège social ou d'un centre de données, créez une connexion aux services Prisma Access vers le site de l'entreprise. Si l'emplacement du réseau distant est autonome et n'a pas besoin d'accéder à l'infrastructure d'autres emplacements, cela ne sera pas nécessaire.

- **Prisma Access emplacements**

  Lorsque les utilisateurs de votre succursale se connectent à Prisma Access, l'emplacement Prisma Access que vous choisissez détermine la langue dans laquelle le contenu d'Internet est diffusé. Pour une expérience utilisateur optimale, sélectionnez la région et l'emplacement dans le même pays que votre succursale afin de garantir la meilleure expérience possible à vos utilisateurs. Si aucun emplacement n'est disponible dans le même pays que votre succursale, choisissez un emplacement qui utilise la même langue que la majorité des utilisateurs du site.

  Peu d'emplacements sont marqués comme **Local Zones (Zones locales)**. Ces emplacements offrent des emplacements de calcul Prisma Access proches des centres de population et d'industrie importants.

- **Sous-réseaux IP**

  Pour que Prisma Access achemine le trafic vers vos réseaux distants, vous devrez fournir des informations de routage pour les sous-réseaux que vous souhaitez sécuriser à l'aide de Prisma Access. Vous pouvez procéder de plusieurs façons. Vous pouvez soit définir un itinéraire statique vers chaque sous-réseau à l'emplacement du réseau distant, soit configurer BGP entre vos emplacements de connexions aux services et Prisma Access, ou utiliser une combinaison des deux méthodes. Si vous configurez les itinéraires statiques et activez BGP, les itinéraires statiques sont prioritaires. Bien qu'il puisse être pratique d'utiliser des itinéraires statiques si vous n'avez que quelques sous-réseaux sur vos emplacements de réseaux distants, dans un déploiement à grande échelle où vous avez des réseaux distants avec des sous-réseaux qui se chevauchent, BGP vous permettra une mise à l'échelle plus facile.

- **Modèle de bande passante agrégée** : la bande passante de vos emplacements de réseau distant est allouée à un niveau agrégé par emplacement de calcul. Chaque emplacement que vous intégrez comporte un emplacement de calcul correspondant pour lequel la bande passante

 ©2025 Palo Alto Networks, Inc.

est allouée. Vous devez allouer la bande passante par emplacement de calcul, plutôt que par emplacement. Cette méthode est dite *Modèle de bande passante agrégée*.

Le modèle de bande passante agrégée est disponible pour tous les nouveaux déploiements. Si vous disposez d'un déploiement existant qui alloue de la bande passante par emplacement, vous pouvez migrer de l'allocation de bande passante par emplacement à l'allocation de bande passante par emplacement de calcul.



Avant de migrer vers le modèle de bande passante agrégée, vous devez consulter Planifier votre migration vers le nouveau modèle.

Tous les emplacements que vous intégrez partagent la bande passante allouée à cet emplacement de calcul. Par exemple, vous devez intégrer quatre succursales en utilisant des réseaux distants dans les emplacements de Singapour, de Thaïlande et du Vietnam. Tous ces emplacements correspondent à l'emplacement de calcul de l'Asie du Sud-Est. Si vous allouez 200 Mbit/s de bande passante à l'emplacement de calcul Asie du Sud-Est, Prisma Access divise les 200 Mbit/s de bande passante entre les quatre succursales que vous avez intégrées à cet emplacement. Si vous ajoutez également un emplacement à Hong Kong, vous notez que Hong Kong correspond à l'emplacement de calcul de Hong Kong et que vous devrez ajouter de la bande passante à cet emplacement de calcul. Spécifiez une bande passante minimale de 50 Mbit/s par emplacement de calcul.

Prisma Access alloue dynamiquement la bande passante en fonction de la charge ou de la demande par emplacement. En utilisant l'exemple précédent où les quatre sites utilisent collectivement jusqu'à 200 Mbit/s, si un ou plusieurs sites n'utilisent pas autant de bande passante que les autres, Prisma Access fournit davantage de bande passante aux emplacements qui sont plus en demande de manière à garantir une utilisation plus efficace de la bande passante allouée. De plus, si l'un des sites tombe en panne, Prisma Access réalloue la bande passante et la répartit entre les autres sites toujours opérationnels dans cet emplacement de calcul.

Les emplacements marqués comme **Local Zones (Zones locales)** prennent en charge une bande passante maximale de 500 Mbit/s pour les réseaux distants. Pour prendre en charge une bande passante de 1 Gbit/s, contactez le support de Palo Alto Networks. Ces emplacements offrent des emplacements de calcul Prisma Access proches des centres de population et d'industrie importants. Cependant, ils présentent également certaines limitations. Pour ajouter une zone locale, contactez votre représentant Palo Alto Networks.

- Si vous rencontrez des problèmes pour accéder aux URL, signalez le problème du site web au support de Palo Alto Networks.
- **Directives de dimensionnement et considérations relatives à l'allocation de la bande passante**

  Lorsque vous calculez la quantité de bande passante nécessaire sur un site, prenez en compte que l'utilisation de la bande passante inclut à la fois le trafic de sortie et d'entrée pour la connexion au réseau distant (c'est-à-dire que la bande passante allouée représente la somme des entrées et des sorties) et que tous les emplacements que vous intégrez partagent la bande passante allouée pour cet emplacement de calcul. Pour vous aider à déterminer combien de bande passante un site spécifique nécessite, considérez la bande passante disponible auprès de votre ISP à chaque emplacement.

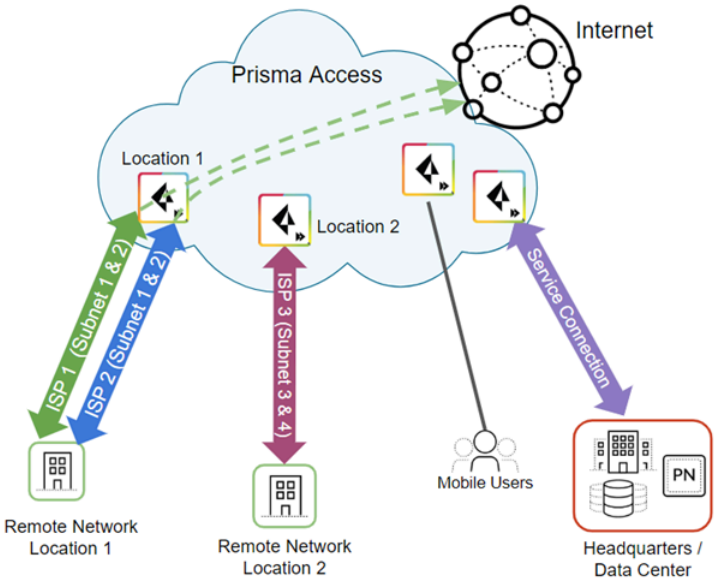
 ©2025 Palo Alto Networks, Inc.

Sous-réseaux qui se chevauchent

En règle générale, vous ne pouvez pas avoir de sous-réseaux qui se chevauchent dans une instance Prisma Access. C'est-à-dire que les sous-réseaux de tous les emplacements de réseau distant, vos connexions aux services et votre Prisma Access pour les utilisateurs mobiles, les pools d'adresses IP ne peuvent pas se chevaucher. Toutefois, il est impossible d'éviter les sous-réseaux qui se chevauchent dans certaines circonstances, par exemple, si vous avez acquis une société qui utilise des sous-réseaux qui se chevauchent avec vos sous-réseaux existants. Dans certains cas, vous pouvez configurer deux régions avec des sous-réseaux qui se chevauchent par conception, par exemple, si vous souhaitez créer un réseau d'invités distinct dans un magasin de détail avec des règles de politique différentes.

Prisma Access vous permet d'intégrer des emplacements de réseau distant avec des sous-réseaux qui se chevauchent, mais seul le flux de trafic Internet des succursales dont les sous-réseaux se chevauchent est pris en charge. Les succursales qui n'ont pas de sous-réseaux qui se chevauchent dans le même locataire bénéficient de toutes les fonctionnalités de Prisma Access. Pour plus de détails, reportez-vous au tableau de la figure suivante.

Traffic Flow	Supported?
Remote Network to Internet	Yes
Remote Network to Remote Network (Overlapping Subnets)	No
Remote Network to Remote Network (No Overlapping Subnets)	Yes
Remote Network to HQ (Overlapping Subnets)	No
Remote Network to HQ (No Overlapping Subnets)	Yes
HQ to Remote Network (Overlapping Subnets)	No
Mobile Users to and from Remote Network (Overlapping Subnets)	No
Mobile Users to and from Remote Network (No Overlapping Subnets)	Yes



Gardez toutefois à l'esprit que les sites dont les sous-réseaux se chevauchent présentent les limitations suivantes :

- Il n'y a pas de trafic réseau distant entrant à réseau distant. Les autres emplacements de réseau distant ne sauraient pas où acheminer le trafic, car plusieurs emplacements de réseau distant sont acheminés vers les mêmes sous-réseaux. Toutefois, les utilisateurs et les services de n'importe quel emplacement de réseau distant peuvent accéder aux ressources d'autres emplacements de réseau distant, à condition qu'il n'y ait pas de sous-réseaux qui se chevauchent sur le site, et que n'importe quel site puisse accéder à Internet via l'infrastructure Prisma Access.
- Le trafic provenant de vos connexions aux services ne peut pas accéder aux ressources de n'importe quel emplacement de réseau distant avec des sous-réseaux qui se chevauchent, car il ne saurait pas à quel emplacement de réseau distant il doit acheminer le trafic. Les emplacements de réseau distant ayant des sous-réseaux qui se chevauchent peuvent toutefois accéder aux ressources à partir des connexions aux services.

 ©2025 Palo Alto Networks, Inc.

- Les utilisateurs mobiles ne peuvent pas accéder aux ressources des emplacements de réseau distant dont les sous-réseaux se chevauchent, là encore en raison des limitations de routage entrant.

> *Si vous gérez Prisma Access à l'aide de Strata Cloud Manager, accédez à* ***Workflows (Flux de travail)*** *>* ***Prisma Access Setup (Configuration de Prisma Access)*** *>* ***Remote Networks (Réseaux distants)*** *>* ***Advanced Settings (Paramètres avancés)****. Modifiez les paramètres des* ***Overlapped Subnets (Sous-réseaux qui se chevauchent)*** *afin d'activer les sous-réseaux qui se chevauchent. Si vous utilisez Panorama pour gérer Prisma Access, accédez à* ***Panorama*** *>* ***Cloud Services*** *>* ***Configuration*** *>* ***Remote Networks (Réseaux distants)*** *et vérifiez les* ***Overlapped Subnets (Sous-réseaux qui se chevauchent)****.*

- **Nœuds de terminaison IPSec** : vous attribuez un *nœud de terminaison IPSec* au réseau distant pendant l'intégration. Vous pouvez spécifier un maximum de 500 sites de réseau distants (pour Prisma Access 5.0 et versions ultérieures) ou de 400 sites de réseau distants (pour les versions de Prisma Access antérieures à la version 5.0) par nœud de terminaison IPSec. Allouez plus de 500 Mbit/s à l'emplacement de calcul qui correspond au nœud de terminaison IPSec pour prendre en charge le nombre maximal de réseaux distants autorisés.

  Vous pouvez avoir un maximum de 200 nœuds de terminaison IPSec dans un emplacement de calcul. Chaque nœud de terminaison IPSec peut vous fournir une bande passante maximale de 1 000 Mbit/s. Si vous allouez plus de 1 000 Mbit/s de bande passante à un emplacement de calcul, Prisma Access vous fournit un nœud de terminaison IPSec supplémentaire.

  - **Nœuds de terminaison IPSec et mises à niveau à partir de versions antérieures à la version 3.2** : avant la version 3.2, un nœud de terminaison IPSec était alloué pour chaque 500 Mbit/s de bande passante alloués dans un emplacement de calcul. Si vous disposez d'un déploiement de réseau distant antérieur à la version 3.2 et que vous effectuez une mise à niveau vers une version 3.2.1 ou ultérieure, et si les emplacements de réseau distant ont plus de 500 Mbit/s alloués à leur emplacement de calcul correspondant, chaque réseau distant associé au nœud de terminaison IPSec peut prendre en charge jusqu'à 1 000 Mbit/s de bande passante. Après la mise à niveau vers la version 3.2 ou ultérieure, Prisma Access déploie un nœud de terminaison IPSec pour 1 000 Mbit/s de bande passante allouée. Pour les réseaux distants existants, Prisma Access peut augmenter la bande passante d'un réseau distant à l'aide d'un mécanisme de mise à l'échelle automatique qui se déclenche lorsque la consommation de bande passante sur le réseau distant nécessite une capacité supplémentaire. Consultez les Modifications du comportement par défaut dans les notes de version de Prisma Access (Panorama géré) pour plus de détails.

    Le mappage actuel du nœud de terminaison IPSec au réseau distant après la mise à niveau vers la version 3.2 est inchangé et le nombre de nœuds de terminaison IPSec reste le même. Les nœuds de terminaison IPSec ne sont ajoutés ou supprimés que lorsque vous augmentez ou diminuez la bande passante d'un emplacement de calcul existant ou lorsque vous intégrez de nouveaux emplacements de calcul pour des réseaux distants.

- **Connexion aux services** : si vos emplacements de réseau distant nécessitent l'accès à l'infrastructure de votre siège social pour authentifier les utilisateurs ou pour permettre l'accès à des ressources de réseau critiques, vous devez créer une connexion aux services afin que le siège social et les emplacements de réseau distant soient connectés. Si l'emplacement de réseau distant est autonome et n'a pas besoin d'accéder à l'infrastructure d'autres

 ©2025 Palo Alto Networks, Inc.

emplacements, vous n'avez pas besoin de configurer la connexion aux services (sauf si vos utilisateurs mobiles ont besoin d'un accès).

- **Modèle** : Prisma Access crée automatiquement une pile de modèles (Remote_Network_Template_Stack) et un modèle de niveau supérieur (Remote_Network_Template) pour Prisma Access pour les réseaux. Pour intégrer et configurer des réseaux distants, vous devrez soit configurer le modèle de niveau supérieur à partir de zéro, soit tirer parti de votre configuration existante, si vous exécutez déjà un pare-feu Palo Alto Networks sur site. Le modèle a besoin des paramètres pour établir le tunnel IPSec et la configuration Internet Key Exchange (échange de clés Internet - IKE) pour la négociation du protocole entre votre emplacement de réseau distant et Prisma Access pour les réseaux, des zones auxquelles vous pouvez faire référence dans la politique de sécurité et un profil de transfert des journaux afin que vous puissiez transférer les journaux à partir de Prisma Access pour les réseaux distants au Strata Logging Service.
- **Configurations de tunnel IPSec** : si vous disposez d'un modèle existant contenant des configurations de tunnel IPSec, de surveillance des tunnels et de profil crypto IPSec, vous pouvez ajouter ce modèle à la pile Remote_Network_Template_Stack pour simplifier le processus de création des tunnels IPSec. Sinon, vous pouvez modifier le modèle Remote_Network_Template qui est créé automatiquement et créer les configurations IPSec nécessaires pour établir le tunnel IPSec vers le site de l'entreprise. Prisma Access vous fournit également un ensemble de modèles IPSec prédéfinis pour certains périphériques réseau couramment utilisés, ainsi qu'un modèle générique pour tout périphérique qui n'est pas inclus dans les modèles prédéfinis. Veillez à suivre les recommandations du tunnel IPSec lors de la configuration du tunnel réseau distant.
- **Déterminer la méthode de routage (statique ou dynamique)** : pour que Prisma Access achemine le trafic vers vos réseaux distants, vous devez fournir des informations de routage pour les sous-réseaux que vous souhaitez sécuriser à l'aide de Prisma Access. Vous pouvez procéder de plusieurs façons. Vous pouvez soit définir un itinéraire statique vers chaque sous-réseau à l'emplacement du réseau distant, soit configurer BGP entre vos emplacements de connexions aux services et Prisma Access, ou utiliser une combinaison des deux méthodes. Si vous configurez les itinéraires statiques et activez BGP, les itinéraires statiques sont prioritaires. Bien qu'il puisse être pratique d'utiliser des itinéraires statiques si vous n'avez que quelques sous-réseaux sur vos emplacements de réseaux distants, dans un déploiement à grande échelle avec de nombreux réseaux distants avec des sous-réseaux qui se chevauchent, BGP vous permettra de mettre à l'échelle plus facilement.
- **Groupe de périphériques parent** : Prisma Access pour les réseaux vous oblige à spécifier un groupe de périphériques parent qui inclura votre politique de sécurité, vos profils de sécurité et d'autres objets de politique (comme les groupes d'applications et les objets, et les groupes d'adresses), ainsi que la politique d'authentification afin que Prisma Access pour les réseaux puisse appliquer de manière cohérente une politique pour le trafic acheminé via le tunnel IPSec vers Prisma Access pour les réseaux. Vous devrez définir des règles et des objets de politique sur Panorama ou utiliser un groupe de périphériques existant pour sécuriser les utilisateurs dans l'emplacement de réseau distant.

  Si vous utilisez un groupe de périphériques existant qui fait référence à des zones, veillez à ajouter le modèle correspondant qui définit les zones à la pile Remote_Network_Template_Stack. Cela vous permettra de terminer le mappage de zone lors de l'intégration et la configuration de réseaux distants.

 ©2025 Palo Alto Networks, Inc.

Allouer de la bande passante au réseau distant

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Les réseaux distants sont utilisés pour sécuriser les emplacements réseau distants, tels que les succursales, et les utilisateurs de ces succursales.

Les réseaux distants sont mesurés, ce qui signifie qu'une quantité spécifique de bande passante est allouée à l'emplacement de calcul et qu'un coût est associé à cette bande passante allouée.

Lorsque vous vous préparez à connecter des réseaux distants à Prisma Access, vous devez savoir combien de sites vous allez intégrer ainsi que les besoins en bande passante pour chacun.

Découvrez comment allouer la bande passante au réseau distant.

- Strata Cloud Manager
- Panorama

Allouer de la bande passante au réseau distant (Strata Cloud Manager)

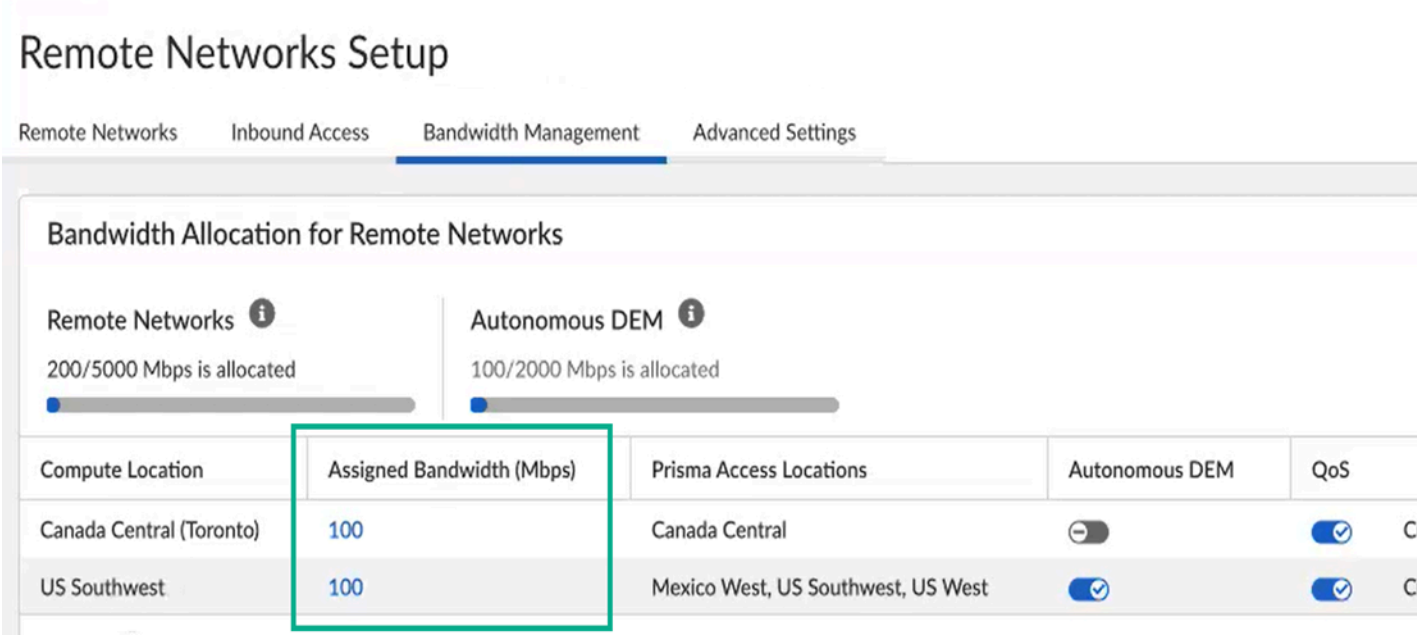
Au moins deux emplacements Prisma Access (souvent plus) géographiquement proches l'un de l'autre sont regroupés en *emplacements de calcul*. C'est le niveau auquel vous allouez de la bande passante, au lieu d'allouer de la bande passante à des emplacements Prisma Access individuels ou des sites réseau distants spécifiques. Cela signifie que Prisma Access peut allouer dynamiquement de la bande passante aux sites dans un emplacement de calcul en fonction de la charge ou de la demande.

Par exemple, vous devez intégrer quatre succursales en utilisant des réseaux distants dans les emplacements de Singapour, de Thaïlande et du Vietnam. Tous ces emplacements correspondent à l'emplacement de calcul de l'Asie du Sud-Est. Si vous allouez 200 Mbit/s de bande passante à l'emplacement de calcul Asie du Sud-Est, Prisma Access divise les 200 Mbit/s de bande passante entre les quatre succursales que vous avez intégrées à cet emplacement. Si vous ajoutez également un emplacement à Hong Kong, vous notez que Hong Kong correspond à l'emplacement de calcul de Hong Kong et que vous devrez ajouter de la bande passante à cet emplacement de calcul. Spécifiez une bande passante minimale de 50 Mbit/s par emplacement de calcul.

Prisma Access alloue dynamiquement la bande passante en fonction de la charge ou de la demande par emplacement. En utilisant l'exemple précédent où les quatre sites utilisent collectivement jusqu'à 200 Mbit/s, si un ou plusieurs sites n'utilisent pas autant de bande passante que les autres, Prisma Access fournit davantage de bande passante aux emplacements qui sont plus en demande de manière à garantir une utilisation plus efficace de la bande passante allouée. De plus, si l'un des sites tombe en panne, Prisma Access réalloue la bande passante et la répartit entre les autres sites toujours opérationnels dans cet emplacement de calcul.

 ©2025 Palo Alto Networks, Inc.

Pour commencer, rendez-vous dans **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Remote Networks (Réseaux distants)** > **Bandwidth Management (Gestion de la bande passante)**.



Lorsque vous allouez de la bande passante en fonction de l'emplacement, tenez toujours compte de la quantité de bande passante dont chaque site a besoin.

Pour vous aider à déterminer combien de bande passante un site spécifique nécessite, considérez la bande passante disponible auprès de votre ISP à chaque emplacement. Lors du calcul de la quantité de bande passante nécessaire sur un site, prenez en compte le fait que l'utilisation de la bande passante inclue à la fois le trafic sortant et entrant pour la connexion réseau distante.

L'accès entrant sécurisé pour les sites réseau distants et la qualité de service (Quality of Service, QOS) pour les réseaux distants ne sont pas pris en charge lorsque vous allouez de la bande passante entre les emplacements.

Allouer de la bande passante au réseau distant (Panorama)

Pour configurer un déploiement de réseau distant Prisma Access qui alloue de la bande passante par emplacement de calcul, suivez les étapes suivantes.

Si vous devez intégrer de nombreux réseaux distants (jusqu'à 1 000), vous pouvez intégrer un réseau distant en utilisant la procédure suivante, puis exporter la configuration du réseau distant dans un fichier CSV, ajouter les autres réseaux distants que vous souhaitez intégrer au fichier CSV et importer le fichier CSV pour enregistrer la configuration dans Prisma Access.

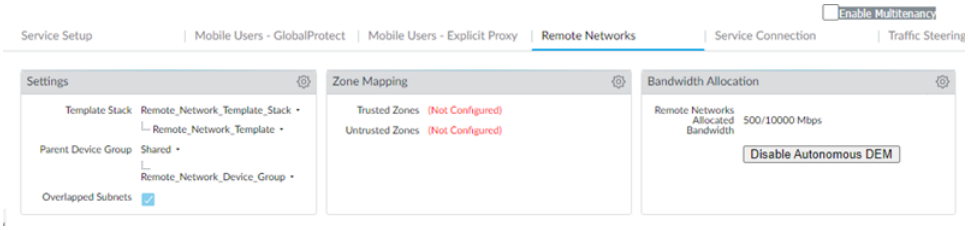
STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Allouez de la bande passante aux emplacements que vous souhaitez intégrer en cliquant sur l'icône d'engrenage dans la zone **Bandwidth Allocation (Allocation de bande passante)**.

Vous allouez de la bande passante à un niveau agrégé par emplacement de calcul. Pour plus d'informations, reportez-vous à la sectionPrisma Access Réseaux distants.

*Si vous avez supprimé Autonomous DEM en tant que licence complémentaire, ou si vous supprimez Autonomous DEM pour les réseaux distants de votre licence, sélectionnez **Disable Autonomous DEM (Désactiver Autonomous DEM)**. Si vous supprimez Autonomous DEM pour les réseaux distants et que vous ne le désactivez pas, vous recevrez un message d'erreur lors de la validation.*



Si vous avez un déploiement de réseaux distants existant qui intègre actuellement des réseaux distants par emplacement, une fenêtre contextuelle s'affiche et vous demande si vous souhaitez migrer vers le modèle de bande passante agrégée. Cliquez sur **Migrate (Migrer)** pour continuer ou sur **Cancel (Annuler)** pour annuler la migration.

*La migration vers le modèle de bande passante agrégée est permanente et non réversible. Avant de procéder à la migration, passez en revue la liste de contrôle pré-migration. Vous devez cliquer sur **Commit and Push (Valider et appliquer)** pour que vos modifications prennent effet.*

Les **Service IP Address (Adresse IP du service)** (le l'adresse IP publique utilisés du côté Prisma Access du tunnel IPSec pour la connexion au réseau distant) ne changent pas lorsque vous migrez votre déploiement vers le modèle de bande passante agrégée et aucune reconfiguration de votre tunnel IPSec n'est requise.

STEP 3 | Entrez la **Bandwidth Allocation (Allocation de bande passante)** que vous souhaitez pour chaque **Compute Location (Emplacement de calcul)** associé aux **Prisma Access Locations (Emplacements Prisma Access)** que vous souhaitez intégrer.

Pour vérifier la quantité de bande passante que vous avez saisie, sélectionnez la coche à côté de la quantité de bande passante. Pour annuler la quantité, sélectionnez **x**.

Spécifiez une bande passante minimale de 50 Mbit/s. La bande passante maximale correspond à la bande passante licenciée restante maximale.

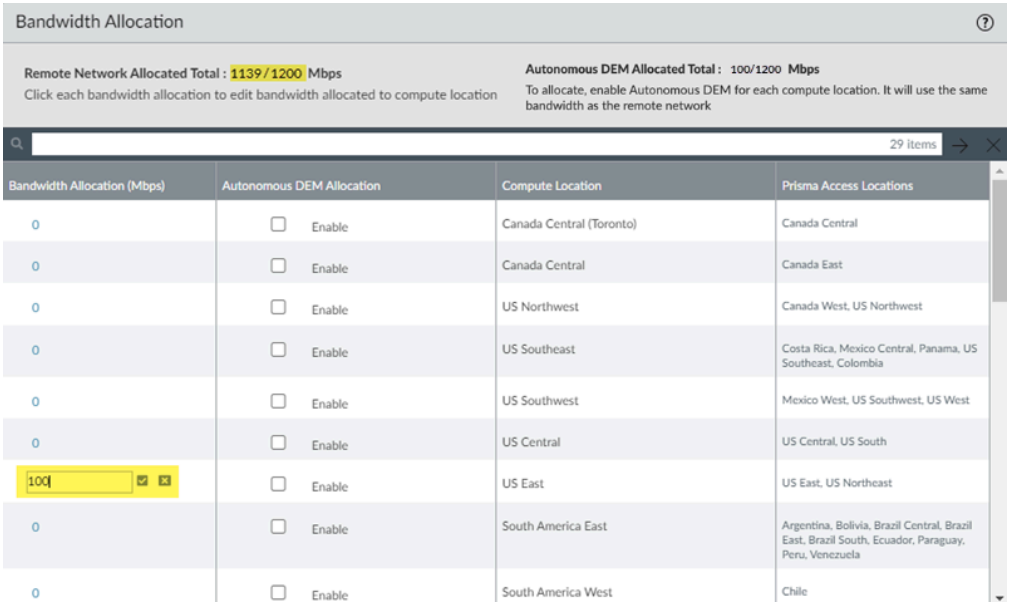
STEP 4 | (Facultatif, déploiements avec Autonomous DEM uniquement pour les licences de réseaux distants) Cliquez sur **Enable (Activer) Autonomous DEM Allocation (Allocation Autonomous DEM)** pour l'emplacement de calcul auquel vous avez alloué de la bande passante.

Si vous activez Autonomous DEM pour l'emplacement de calcul, la quantité de bande passante utilisée par la licence Autonomous DEM est la même que la quantité de bande passante que vous spécifiez pour l'emplacement de calcul. **Autonomous DEM Allocated Total (Total alloué à Autonomous DEM)** vous montre combien de bande passante est utilisée par Autonomous

 ©2025 Palo Alto Networks, Inc.

DEM ainsi que la quantité restante. Pour plus d'information, consultez le guide de Autonomous DEM.

STEP 5 | Attendez que la bande passante soit reflétée dans le champ **Allocated Total (Total alloué)** en haut de la page, puis cliquez sur **OK**.



STEP 6 | (Facultatif) Si vous souhaitez configurer votre réseau distant pour fournir un accès entrant sécurisé aux emplacements de réseau distant, cliquez sur l'onglet **Inbound Access Remote Networks (Réseaux distants à accès entrant)** et suivez le flux de travail pour configurer un accès entrant sécurisé pour un réseau distant.

STEP 7 | Cliquez sur l'option **Add (Ajouter)** un réseau distant et spécifiez un **Name (Nom)**.

Vous ne pouvez pas changer le nom de l'emplacement réseau distant après l'avoir saisi. Assurez-vous de connaître votre schéma d'affectation de nom pour vos réseaux distants avant de commencer l'intégration.

STEP 8 | (Facultatif, uniquement pour les déploiements BGP) Créez une configuration afin que votre connexion au réseau distant puisse utiliser jusqu'à quatre tunnels IPSec pour son trafic (**ECMP Load Balancing (Équilibrage de charge ECMP)**).

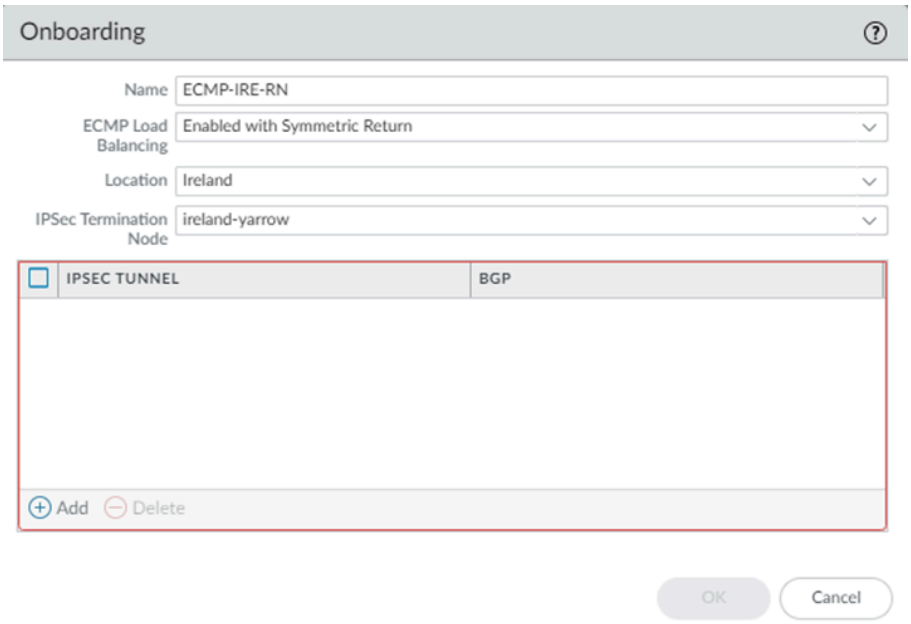
Les itinéraires statiques ne sont pas pris en charge (BGP requis), et, si vous avez configuré la QoS, vous ne pouvez pas changer le rapport d'allocation pour les liens ECMP. Si votre déploiement utilise un tunnel IPSec pour sa connexion au réseau distant ou utilise des itinéraires statiques, sélectionnez **None (Aucun)** pour **ECMP Load Balancing (Équilibrage de charge ECMP)** et passez à l'étape 11.

1. Sélectionnez l'une des options pour activer ou désactiver l'équilibrage de charge ECMP.
   - **None (Aucun)** : avec cette option, l'équilibrage de charge ECMP n'est pas utilisé (utilisez un seul tunnel de réseau distant pour cette connexion au réseau distant). C'est le seul choix que vous pouvez faire pour les itinéraires statiques ; BGP est requis pour l'équilibrage de charge ECMP.

 ©2025 Palo Alto Networks, Inc.

- **Enabled with Symmetric Return (Activé avec retour symétrique)** : spécifiez jusqu'à quatre tunnels IPSec pour cette connexion au réseau distant et forcez Prisma Access à utiliser le même lien pour le trafic de retour que celui utilisé pour envoyer le trafic.

  Sélectionnez cette option si vous avez un ou plusieurs tunnels de secours à utiliser uniquement si l'un des tunnels principaux n'est plus opérationnel. Si un lien échoue, Prisma Access utilise l'un des autres tunnels pour envoyer et recevoir le trafic de manière symétrique.



2. Vous devez cliquer sur **Add (Ajouter)** pour ajouter un tunnel IPSec pour la connexion au réseau distant et spécifier les valeurs suivantes :

   - **Enable (Activer)** : active BGP pour le tunnel IPSec.

     Cette sélection n'est pas configurable ; vous devez activer BGP pour configurer ECMP.

   - **Summarize Mobile User Routes before advertising (Résumer les itinéraires des utilisateurs mobiles avant de publier)** : réduit le nombre de publications de sous-réseaux IP d'utilisateurs mobiles sur le BGP vers votre équipement de locaux clients (CPE) en les résumant.

     Par défaut, Prisma Access publie les pools d'adresses IP des utilisateurs mobiles par blocs de sous-réseaux /24. Si vous les résumez, Prisma Access publie le pool en fonction du sous-réseau que vous avez spécifié. Par exemple, Prisma Access publie un pool d'adresses IP mobiles d'utilisateurs publics de 10.8.0.0/20 en utilisant le sous-réseau /20, plutôt que de diviser le pool en sous-réseaux de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, et ainsi de suite, avant de les publier. Le résumé de ces publicités peut réduire le nombre d'itinéraires stockés dans les tableaux de routage CPE. Par exemple, vous pouvez utiliser le résumé de pool d'adresses IP avec des

 ©2025 Palo Alto Networks, Inc.

passerelles VPN cloud (passerelles privées virtuelles [VGW] ou passerelles de transit [TGW]) qui peuvent accepter un nombre limité d'itinéraires.

Si vous activez la synthèse des itinéraires pour un emplacement qui utilise ECMP, vous devez activer la synthèse des itinéraires sur tous les liens vers cet emplacement, sinon vous recevrez un message d'erreur lors de la validation.

Prisma Access définit la chaîne de communauté pour les itinéraires d'utilisateurs mobiles agrégés à `0xFFFE:0xFFF0`.

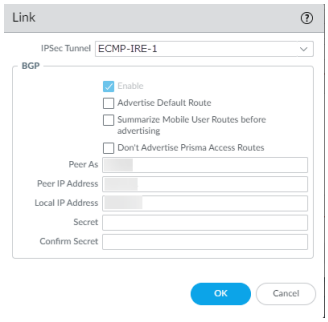
- **Advertise Default Route (Publier l'itinéraire par défaut)** : Prisma Access génère une publication d'itinéraire par défaut pour le réseau distant en utilisant eBGP.

  Assurez-vous que votre réseau n'a pas un autre itinéraire par défaut publié par BGP, sinon vous pourriez introduire des problèmes de routage dans votre réseau.

- **Don't Advertise Prisma Access Routes (Ne pas publier les itinéraires Prisma Access)** : empêche l'homologue BGP Prisma Access de transférer des itinéraires dans le réseau de votre organisation.

  Par défaut, Prisma Access publie toutes les informations de routage BGP, y compris les itinéraires locaux et tous les préfixes qu'il reçoit d'autres connexions aux services, de réseaux distants et de sous-réseaux d'utilisateurs mobiles. Cochez cette case pour empêcher Prisma Access d'envoyer des publications BGP, mais utilisez quand même les informations BGP qu'il reçoit pour apprendre les itinéraires d'autres voisins BGP.

  Puisque Prisma Access n'envoie pas de publications BGP si vous sélectionnez cette option, vous devez configurer des itinéraires statiques sur l'équipement local pour établir des itinéraires de retour vers Prisma Access.



- **Peer AS (AS homologue)** : spécifiez le système autonome (autonomous system, AS) auquel le pare-feu, le routeur virtuel ou le routeur BGP de votre réseau distant appartient.
- **Peer IP Address (Adresse IP de l'homologue)** : entrez l'adresse IP assignée comme identifiant de routeur du routeur eBGP sur le réseau distant pour lequel vous configurez cette connexion.
- **Local IP Address (Adresse IP locale)** (facultatif) : entrez une adresse que Prisma Access utilise comme adresse IP locale pour BGP. Spécifiez l'adresse IP à utiliser du côté Prisma Access du tunnel.

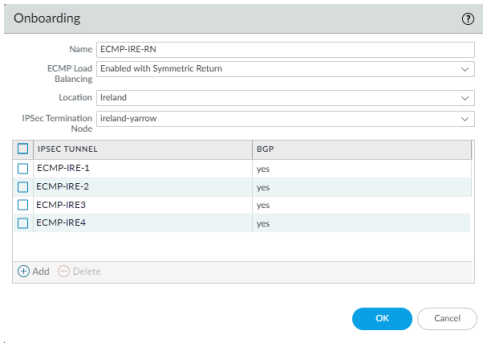
  La spécification d'une **Local Address (Adresse locale)** est utile lorsque le périphérique de l'autre côté de la connexion (tel qu'une passerelle virtuelle privée Amazon Web

 ©2025 Palo Alto Networks, Inc.

Service (AWS)) nécessite une adresse IP locale spécifique pour que l'appairage BGP réussisse. Assurez-vous que l'adresse que vous spécifiez ne soit pas en conflit ou ne chevauche pas les adresses IP dans le sous-réseau d'infrastructure ou les sous-réseaux du réseau distant.

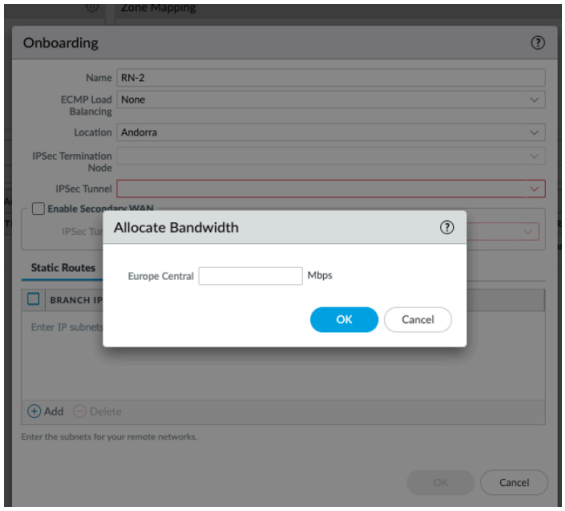
- **Secret (Phrase secrète)** et **Confirm Secret (Confirmer la phrase secrète)** (facultatif) : entrez et confirmez une phrase secrète pour authentifier les communications entre homologues BGP.

3. Répétez l'étape précédente pour ajouter jusqu'à quatre tunnels à utiliser avec la connexion au réseau distant.



STEP 9 | Sélectionnez le **Location (Emplacement)** dans lequel Prisma Access déploiera l'infrastructure nécessaire pour sécuriser votre emplacement réseau distant. Cette région devrait être géographiquement proche de votre emplacement de réseau distant.

Si vous n'avez pas encore alloué de bande passante pour l'emplacement de calcul auquel l'emplacement est associé, Prisma Access vous invite à entrer la bande passante pour cet emplacement de calcul.



STEP 10 | Sélectionnez le **IPSec Termination Node (Nœud de fin d'IPSec)** que vous souhaitez utiliser pour ce réseau distant.

Prisma Access utilise ce nœud pour associer des emplacements réseau distants à des emplacements de calcul.

 ©2025 Palo Alto Networks, Inc.

STEP 11 | (Routage statique ou déploiements à tunnel unique uniquement) Sélectionnez ou ajoutez une nouvelle configuration de **tunnel IPSec** pour accéder au pare-feu, au routeur ou au périphérique SD-WAN sur le site de l'entreprise :

- Sélectionnez l'un des modèles IPSec prédéfinis dans le modèle Remote_Network_Template ou, si vous avez ajouté un modèle à la pile Remote_Network_Template_Stack (ou modifié le modèle Remote_Network_Template prédéfini) qui inclut une configuration de tunnel IPSec, sélectionnez cet **IPSec Tunnel (Tunnel IPSec)** dans la liste déroulante. Notez que le tunnel que vous créez pour chaque connexion réseau distante connecte Prisma Access au périphérique compatible IPSec à chaque succursale.

  Utilisez les instructions suivantes lors de la configuration d'un tunnel IPSec :

  - Les adresses homologues dans la configuration IKE Gateway doivent être uniques pour chaque tunnel. Vous pouvez toutefois réutiliser certains des autres éléments de configuration courants, tels que les profils crypto.
  - Le tunnel IPSec que vous sélectionnez depuis un modèle doit utiliser l'échange automatique de clés et IPv4 uniquement.
  - Les noms de tunnel IPSec, de passerelle IKE et de profil crypto ne peuvent pas dépasser 31 caractères.
  - Si vous intégrez plusieurs réseaux distants au même emplacement avec des homologues IKE dynamiques, vous devez utiliser le même profil crypto IKE pour toutes les configurations de réseau distant.
- Pour créer une nouvelle configuration de tunnel IPSec, cliquez sur **New IPSec Tunnel (Nouveau tunnel IPSec)**, attribuez-lui un **Name (Nom)**, et configurez les paramètres IKE Gateway (Passerelle IKE), IPSec Crypto Profile (Profil crypto IPSec) et Tunnel Monitoring (Surveillance du tunnel).
  - Si le périphérique compatible IPSec de votre succursale utilise un VPN basé sur des politiques, sous l'onglet **Proxy IDs (ID proxy)**, vous devez cliquer sur **Add (Ajouter)** pour ajouter un ID proxy correspondant aux paramètres configurés sur votre périphérique IPSec local pour vous assurer que Prisma Access peut établir un tunnel IPSec avec votre périphérique local.
- Laissez l'option **Enable Replay Protection (Activer la protection contre la relecture** sélectionnée pour détecter et neutraliser les attaques par relecture.
- Sélectionnez **Copy TOS Header (Copier l'en-tête TOS)** pour copier le champ Type of Service (type de service - ToS) à partir de l'en-tête IP interne vers l'en-tête IP externe des paquets encapsulés afin de conserver les informations ToS d'origine.
- Pour activer la surveillance de tunnel pour la connexion de service, sélectionnez **Tunnel Monitor (Surveiller le tunnel**.
  - Saisissez l'adresse **IP de Destination**.

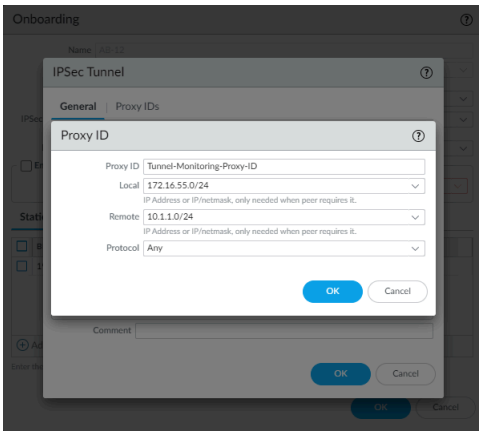
    Spécifiez une adresse IP à votre succursale à laquelle Prisma Access peut envoyer des requêtes ping ICMP pour la surveillance du tunnel IPSec. Assurez-vous que cette adresse

 ©2025 Palo Alto Networks, Inc.

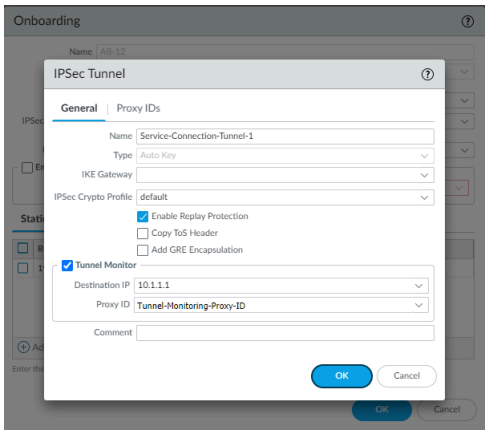
est accessible par ICMP depuis l'ensemble du sous-réseau de l'infrastructure Prisma Access.

- Si vous utilisez la surveillance de tunnel avec un périphérique homologue qui utilise plusieurs ID de proxy, spécifiez un **ID de proxy** ou ajoutez un **nouvel ID de proxy** qui autorise l'accès à partir du sous-réseau d'infrastructure à votre succursale.

  La figure suivante montre un ID proxy avec le sous-réseau d'infrastructure de service (172.16.55.0/24 dans cet exemple) comme sous-réseau IP **local** et le sous-réseau de l'emplacement de succursale (10.1.1.0/24 dans cet exemple) comme sous-réseau **distant**.



  La figure suivante montre l'ID proxy que vous avez créé appliqué à la configuration du moniteur de tunnel en le spécifiant dans le champ **Proxy ID (ID proxy)**.



Vous devez configurer un itinéraire statique sur votre CPE vers l'adresse IP du moniteur de tunnel pour que la surveillance du tunnel fonctionne. Pour trouver l'adresse IP de destination à utiliser pour la surveillance des tunnels entre votre succursale et Prisma Access, sélectionnez ***Panorama*** *>* ***Cloud Services*** *>* ***Status (État)*** *>* ***Network Details (Détails du réseau)****, cliquez sur le bouton d'option* ***Service Infrastructure (Infrastructure de service)*** *et recherchez la* ***Tunnel Monitor IP Address (Adresse IP de surveillance du tunnel)****.*

 ©2025 Palo Alto Networks, Inc.

STEP 12 | Si vous avez une liaison WAN secondaire à cet emplacement, sélectionnez **Enable Secondary WAN (Activer le WAN secondaire)**.

Veillez à créer un tunnel IPSec unique pour le WAN secondaire de chaque réseau distant ; Prisma Access ne prend pas en charge la réutilisation du même tunnel IPSec pour les WAN secondaires dans plusieurs réseaux distants.

La configuration d'un WAN secondaire n'est pas prise en charge dans les déploiements suivants :

- Si votre WAN secondaire est configuré en mode actif-actif avec le tunnel IPSec principal.
- Si l'équipement de vos locaux clients (CPE) est configuré dans une configuration ECMP (Equal Cost Multipath) avec le tunnel IPSec principal et secondaire.

Si vous utilisez des itinéraires statiques, le temps de basculement du tunnel est inférieur à 15 secondes à partir du moment de la détection, selon votre fournisseur WAN.

Si vous configurez le routage BGP et que vous avez activé la surveillance des tunnels, le temps d'attente par défaut le plus court pour déterminer qu'un index de paramètres de sécurité (SPI) est défaillant est le moniteur de tunnel, qui supprime toutes les routes vers un homologue lorsqu'il détecte une défaillance de tunnel pendant 15 secondes consécutives. De cette façon, le moniteur de tunnel détermine le comportement des routes BGP. Si vous ne configurez pas la surveillance du tunnel, la minuterie d'attente détermine la durée d'arrêt du tunnel avant de supprimer l'itinéraire. Prisma Access utilise la valeur d'attente BGP par défaut de 90 secondes comme défini par la RFC 4271, qui est le temps d'attente maximum avant que Prisma Access supprime un itinéraire pour un SPI inactif. Si le périphérique BGP homologue a un temps d'attente configuré plus court, le minuteur de maintien BGP utilise la valeur inférieure.

Lorsque le tunnel secondaire est installé avec succès, l'itinéraire secondaire a priorité jusqu'à ce que le tunnel primaire refonctionne. Si l'itinéraire principal et l'itinéraire secondaire sont tous deux opérationnels, l'itinéraire principal est prioritaire.

Si vous utilisez un homologue BGP différent pour la connexion secondaire (de secours), Prisma Access ne respecte pas les attributs du discriminateur multi-sortie (Multi-Exit Discriminator, MED) publiés par le CPE. Cette mise en garde s'applique si vous utilisez plusieurs homologues BGP sur des connexions réseau distantes ou des connexions de service.

STEP 13 | Activez le routage vers les sous-réseaux ou les adresses IP individuelles sur le site du réseau distant auquel vos utilisateurs auront besoin d'accéder.

Prisma Access utilise ces informations pour acheminer les requêtes vers le site approprié. Les réseaux de chaque site ne peuvent pas se chevaucher les uns avec les autres ni avec les pools d'adresses IP que vous avez désignés pour l'infrastructure de service ou pour le Prisma Access pour les pools d'adresses IP des utilisateurs. Vous pouvez configurer des **Static Routes (Itinéraires statiques)**, **BGP** ou une combinaison des deux.

- Pour configurer des **Static Routes (Itinéraires statiques)** :
  1. Dans l'onglet **Static Routes (Itinéraires statiques)**, cliquez sur **Add (Ajouter)** et saisissez l'adresse de sous-réseau (par exemple, 172.168.10.0/24) ou l'adresse IP individuelle d'une ressource, comme un serveur DNS (par exemple, 10.32.5.1/32) auquel vos utilisateurs distants auront besoin d'accéder.

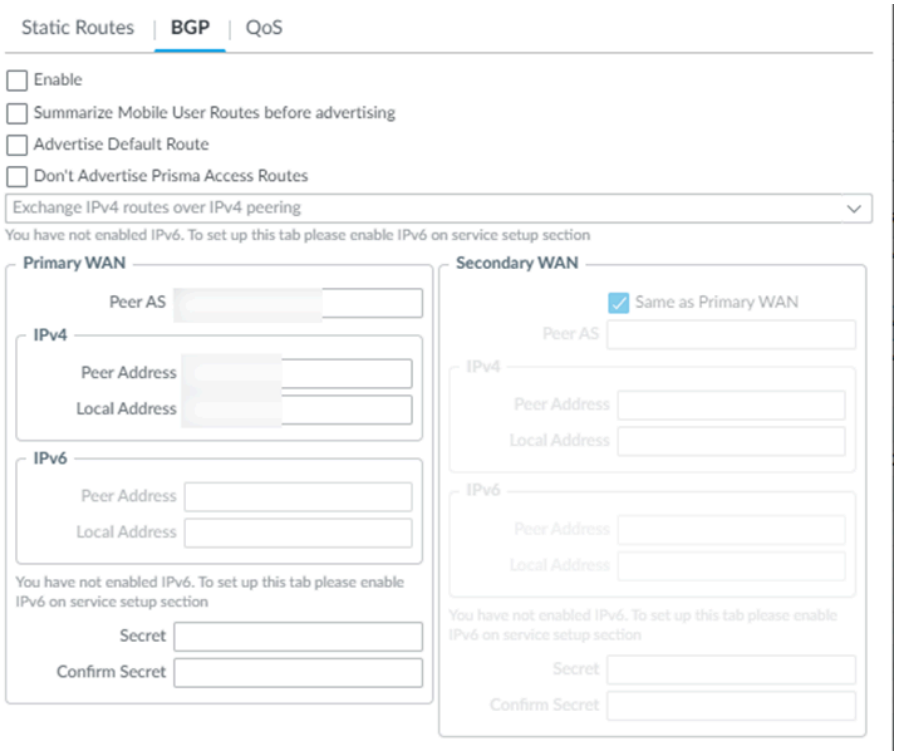
 ©2025 Palo Alto Networks, Inc.

2. Procédez de la même manière pour tous les sous-réseaux ou adresses IP auxquels Prisma Access aura besoin d'accéder à cet emplacement.



- Pour configurer **BGP** :

1. Sélectionnez l'onglet **BGP (BGP)**.
2. (Facultatif) Sélectionnez les choix relatifs à l'**ECMP Load Balancing (Équilibrage de charge ECMP)**. Reportez-vous l'étape 8.
3. Si vous sélectionnez l'option **Non (Aucun)** dans **ECMP Load Balancing (Équilibrage de charge ECMP)**, saisissez les choix BGP.



4. Pour activer BGP pour la connexion au réseau distant, sélectionnez **Enable (Activer)**.

   Lorsque vous activez BGP, Prisma Access définit la durée de vie (time to live, TTL) pour BGP externe (eBGP) à 8 pour tenir compte des éventuels sauts supplémentaires qui pourraient se produire entre l'infrastructure Prisma Access et l'équipement de vos locaux client (Customer Premises Equipment, CPE) qui termine la connexion eBGP.
5. Pour réduire le nombre de publications de sous-réseaux IP d'utilisateurs mobiles via BGP vers l'équipement de vos locaux client (Customer Premises Equipment, CPE) en les

 ©2025 Palo Alto Networks, Inc.

résumant, sélectionnez **Summarize Mobile User Routes before advertising (Résumer les itinéraires des utilisateurs mobiles avant de publier)**.

Par défaut, Prisma Access publie les pools d'adresses IP des utilisateurs mobiles par blocs de sous-réseaux /24. Si vous les résumez, Prisma Access publie le pool en fonction du sous-réseau que vous avez spécifié. Par exemple, Prisma Access publie un pool d'adresses IP mobiles d'utilisateurs publics de 10.8.0.0/20 en utilisant le sous-réseau /20, plutôt que de diviser le pool en sous-réseaux de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, et ainsi de suite, avant de les publier. Le résumé de ces publicités peut réduire le nombre d'itinéraires stockés dans les tableaux de routage CPE. Par exemple, vous pouvez utiliser le résumé de pool d'adresses IP avec des passerelles VPN cloud (passerelles privées virtuelles [VGW] ou passerelles de transit [TGW]) qui peuvent accepter un nombre limité d'itinéraires.

Prisma Access définit la chaîne de communauté pour les itinéraires d'utilisateurs mobiles agrégés à `0xFFFE:0xFFF0`.

6. Pour permettre à Prisma Access de publier un itinéraire par défaut pour le réseau distant en utilisant eBGP, sélectionnez **Advertise Default Route (Publier l'itinéraire par défaut)**.

   Si vous sélectionnez **Advertise Default Route (Publier l'itinéraire par défaut)**, assurez-vous que votre réseau n'a pas un autre itinéraire par défaut annoncé par BGP, sinon vous pourriez introduire des problèmes de routage dans votre réseau.

   Vous devez publier vos itinéraires par défaut avant de faire cette sélection pour les publier. De plus, assurez-vous que votre réseau n'a pas une autre itinéraire par défaut publié par BGP, sinon vous pourriez introduire des problèmes de routage dans votre réseau.

7. Pour empêcher l'homologue BGP sur le pare-feu Prisma Access de transférer des itinéraires dans le réseau de votre organisation, sélectionnez **Don't Advertise Prisma Access Routes (Ne pas publier les itinéraires Prisma Access)**.

   Par défaut, Prisma Access publie toutes les informations de routage BGP, y compris les itinéraires locaux et tous les préfixes qu'il reçoit d'autres connexions aux services, de réseaux distants et de sous-réseaux d'utilisateurs mobiles. Cochez cette case pour empêcher Prisma Access d'envoyer des publications BGP, mais utilisez quand même les informations BGP qu'il reçoit pour apprendre les itinéraires d'autres voisins BGP.

   Puisque Prisma Access n'envoie pas de publications BGP si vous sélectionnez cette option, vous devez configurer des itinéraires statiques sur l'équipement local pour établir des itinéraires de retour vers Prisma Access.

8. Entrez le **Peer AS (Homologue AS)**, qui est le système autonome (autonomous system, AS) auquel le pare-feu, le routeur virtuel ou le routeur BGP de votre réseau distant appartiennent.
9. Entrez l'adresse IP assignée comme identifiant de routeur du routeur eBGP sur le réseau distant pour lequel vous configurez cette connexion dans **Peer IP Address (Adresse IP de l'homologue)**.
10. (Facultatif) Entrez une adresse que Prisma Access utilise comme adresse IP locale pour BGP.

    La spécification d'une **Local Address (Adresse locale)** est utile lorsque le périphérique de l'autre côté de la connexion (tel qu'une passerelle virtuelle privée Amazon Web Service

 ©2025 Palo Alto Networks, Inc.

(AWS)) nécessite une adresse IP locale spécifique pour que l'appairage BGP réussisse. Assurez-vous que l'adresse que vous spécifiez ne soit pas en conflit ou ne chevauche pas les adresses IP dans le sous-réseau d'infrastructure ou les sous-réseaux du réseau distant.

*Vous devez configurer un itinéraire statique sur votre CPE vers la **Local Address (Adresse locale)** BGP.*

11. (Facultatif) Entrez et confirmez une phrase secrète pour authentifier les communications entre homologues BGP.
12. (Facultatif) Si vous avez configuré un **Secondary WAN (WAN secondaire)** et que vous devez changer la **Peer Address (Adresse de l'homologue)** ou la **Local Address (Adresse locale)** pour l'homologue BGP secondaire (de secours), désélectionnez **Same as Primary WAN (Identique au WAN principal)** et entrez une adresse IP d'homologue unique et, éventuellement, une adresse IP locale pour le WAN secondaire.

    Si vous utilisez la mise en réseau IPv6 dans votre déploiement de réseau distant, vous pouvez configurer des adresses **IPv6** ainsi que des adresses **IPv4**. Vous devez également activer la mise en réseau IPv6 globalement dans votre infrastructure Prisma Access avant de pouvoir utiliser l'adressage IPv6.

    Dans certains déploiements (par exemple, lors de l'utilisation de BGP pour établir un appairage avec une passerelle VPN AWS), l'homologue BGP pour le WAN principal et secondaire peut être différent. Dans ces scénarios, vous pouvez choisir de définir un homologue BGP différent pour le WAN secondaire.

    *Pour les déploiements BGP avec des WAN secondaires, Prisma Access définit à la fois le tunnel primaire et le tunnel secondaire dans un état **UP (Actif)**, mais suit le comportement normal de sauvegarde active BGP pour le trafic réseau. Prisma Access définit le tunnel principal comme actif, et envoie et reçoit du trafic uniquement par ce tunnel ; si le tunnel principal échoue, Prisma Access détecte l'échec en utilisant les règles BGP, définit le tunnel secondaire comme actif et utilise uniquement le tunnel secondaire pour envoyer et recevoir du trafic.*

STEP 14 | (Facultatif) Activez la **QoS** pour l'emplacement et spécifier un **QoS Profile (Profil QoS)**.

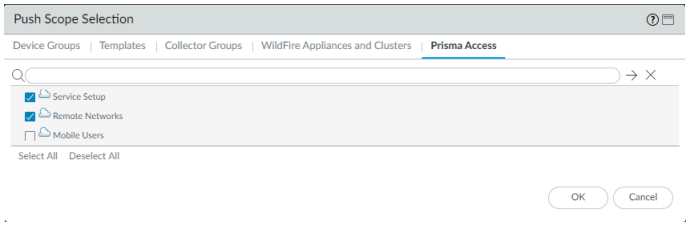
Vous spécifiez les options QoS et les paramètres globaux par emplacement de calcul dans les **Settings (Paramètres)**. Cependant, vous pouvez activer ou désactiver la QoS ou changer le profil QoS par emplacement ici.

STEP 15 | Validez les modifications apportées à la configuration dans Panorama et appliquez la configuration à Prisma Access pour les réseaux.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.
2. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**. Cliquez sur **Edit Selections (Modifier les sélections)** > **Prisma Access**, puis sélectionnez

 ©2025 Palo Alto Networks, Inc.

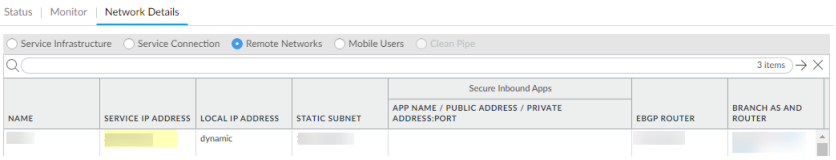
Prisma Access pour les réseaux et Prisma Access pour la configuration du service afin d'appliquer la configuration au service.



3. Cliquez sur **OK** et **Push (Appliquer)**.

STEP 16 | Configurez le périphérique compatible IPSec à l'emplacement du réseau distant pour configurer une connexion IPSec avec Prisma Access pour les réseaux.

1. Trouvez les **Service IP Address (Adresse IP du service)** pour cette connexion au réseau distant en sélectionnant **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)**, en cliquant sur le bouton d'option **Remote Networks (Réseaux distants)** et en consultant les champs **Service IP Address (Adresse IP du service)**. Prisma Access pour l'infrastructure des réseaux a attribué ce cette adresse IP pour la connexion au réseau distant Prisma Access et vous devez configurer cela comme l'adresse IP de l'homologue pour configurer le tunnel IPSec entre l'emplacement du réseau distant et Prisma Access pour les réseaux.



2. Vérifiez la **Local IP address (Adresse IP locale)** du périphérique à l'emplacement réseau distant sur la page **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Remote Networks (Réseaux distants)**. Si vous effectuez une NAT à l'emplacement du réseau distant, la **Local IP address (Adresse IP locale)** affiche l'adresse IP du périphérique après la NAT.

STEP 17 | Pour sécuriser le trafic à l'emplacement réseau distant, vous devez créer des règles de politique de sécurité.

1. Sélectionnez **Policies (Politiques)**.
2. Sélectionnez le **Device Group (Groupe de périphériques)** dans lequel vous souhaitez ajouter des règles de politique. Vous pouvez sélectionner le groupe Remote_Network_Device_Group ou le groupe de périphériques parent que vous avez sélectionné pour définir des politiques afin de sécuriser l'emplacement du réseau distant.
3. Créez des règles de politique de sécurité. Assurez-vous de ne pas définir de règles de politique de sécurité autorisant le trafic de n'importe quelle zone à n'importe quelle zone. Dans les règles de politique de sécurité, utilisez les zones que vous avez définies dans votre modèle.

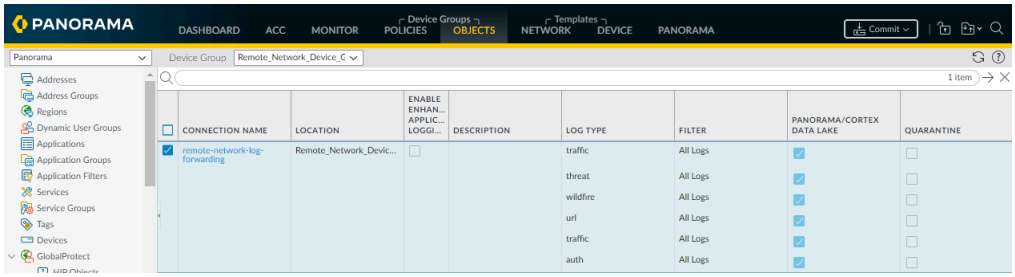
   Si un utilisateur de votre réseau se voit refuser l'accès à un site web, signalez les problèmes d'accès au site avant d'ouvrir un ticket auprès de Palo Alto Networks.

 ©2025 Palo Alto Networks, Inc.

STEP 18 | Activez la journalisation de Strata Logging Service. Vous devez créer et attacher un profil de transfert des journaux à chaque règle de politique pour laquelle vous souhaitez transférer les journaux.

1. Sélectionnez **Objects (Objets) > Log Forwarding (Transfert des journaux)**.
2. Sélectionnez le **Device Group (Groupe de périphériques)** dans lequel vous avez ajouté les règles de politique, par exemple, Remote_Network_Device_Group.
3. Cliquez sur **Add (Ajouter)** pour ajouter un profil de transfert des journaux. Dans la liste de correspondance du profil de transfert des journaux, cliquez sur **Add (Ajouter)** pour ajouter le **Log Type (Type de journal)** que vous souhaitez transférer.
4. Sélectionnez **Panorama/Strata Logging Service (Service de journalisation Panorama/Strata)** comme méthode de transfert pour permettre à Prisma Access de transférer les journaux à Strata Logging Service. Vous pourrez surveiller les journaux et générer des rapports depuis Panorama. Strata Logging Service offre une intégration transparente pour stocker les journaux sans les renvoyer à votre Panorama au siège social, et Panorama peut interroger Strata Logging Service selon le besoin.

   L'exemple suivant permet le transfert des journaux de trafic, de prévention des menaces, d'envois WildFire, de filtrage des URL, de filtrage des données et d'authentification sur Strata Logging Service.



5. Sélectionnez **Policies (Politiques) > Security (Sécurité)**, puis modifiez la règle de politique. Dans **Actions**, sélectionnez le profil de transfert des journaux que vous avez créé.

STEP 19 | Validez tous vos changements dans Panorama et appliquez les modifications apportées à la configuration à Prisma Access.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**.
2. Vous devez **Edit Selections (Modifier les sélections)** et, dans l'onglet **Prisma Access**, assurez-vous que l'option **Prisma Access for networks (Prisma Access pour réseaux)** est sélectionnée dans **Push Scope (Étendue de la transmission)**, puis cliquez sur **OK**.
3. **Commit and Push (Validez et appliquez)** vos modifications.

STEP 20 | Vérifiez l'état du réseau distant.

Pour plus d'informations, reportez-vous à la sectionVérifier si le réseau distant est connecté à Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Planifier votre migration vers le nouveau modèle

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

La bande passante pour les nouveaux déploiements Prisma Access de réseau distant sont alloués à un niveau agrégé par emplacement de calcul, également appelé *modèle de bande passante agrégée*. L'allocation de la bande passante au niveau de l'emplacement de calcul vous offre plus de flexibilité dans l'allocation de la bande passante de votre réseau distant sous licence, car Prisma Access alloue dynamiquement la bande passante pour chaque emplacement en fonction de la charge ou de la demande.

Si vous disposez d'un déploiement existant qui alloue la bande passante en fonction de l'emplacement Prisma Access, vous pouvez migrer vers le modèle de bande passante agrégée. Vous pouvez également migrer votre déploiement QoS de réseau distant. Lorsque vous migrez, tous les réseaux distants utilisent le modèle de bande passante agrégée.

Utilisez la liste de contrôle suivante pour planifier la migration vers le modèle de bande passante agrégée :

- ❑ Il convient de noter que les composants de réseau distant suivants restent inchangés après la migration :
  - Aucune modification n'a été apportée au plan de données. Le trafic continue à circuler dans le plan de données Prisma Access sans aucune modification de la configuration existante.
  - La migration n'a pas d'impact sur les tunnels existants.

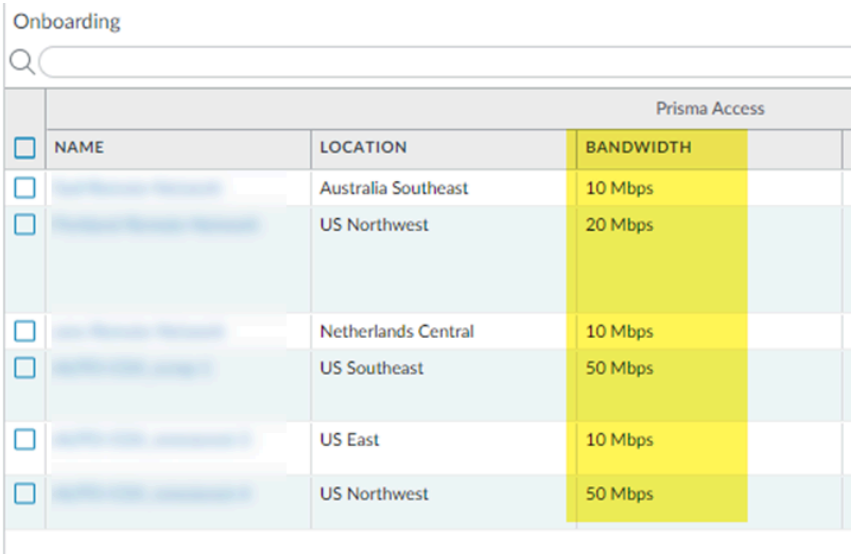
    Aucune reconfiguration des paramètres de votre tunnel IPSec n'est nécessaire. Les passerelles IKE, les configurations de tunnel IPSec et les profils crypto IKE et IPSec restent inchangés.
  - La **Service IP Address (Adresse IP du service)** (le les adresses IP publiques utilisées sur le côté Prisma Access du tunnel IPSec pour la connexion réseau distante) du réseau distant ne change pas pour chaque réseau distant lorsque vous migrez votre déploiement vers le modèle de bande passante agrégée.
- ❑ Prisma Access attribue des nœuds de terminaison IPSec et alloue la bande passante aux réseaux distants lors d'une migration vers le modèle de bande passante agrégée. Vous devez comprendre comment ce modèle fonctionne avant de migrer.

  *Si vous souhaitez réattribuer un réseau distant existant à un autre nœud de terminaison IPSec après la migration, Prisma Access attribue une autre **Service IP Address (Adresse IP du service)** au réseau distant après que vous ayez validé et transmis vos modifications. Dans ce cas, vous devrez reconfigurer votre CPE pour pointer vers la nouvelle adresse IP du tunnel de réseau distant.*

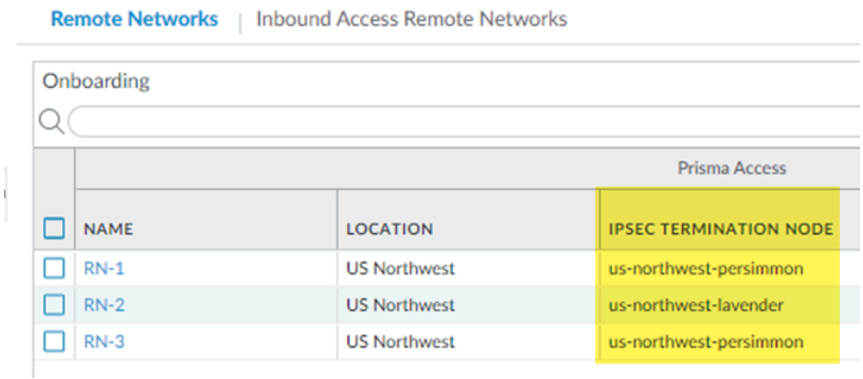
©2025 Palo Alto Networks, Inc.

- Si votre configuration n'est pas prise en charge, l'onglet Bandwidth Allocation (Allocation de bande passante) et la bannière de migration ne sont pas visibles. Les configurations suivantes ne sont pas prises en charge pour la migration vers le modèle de bande passante agrégée :
  - Un réseau distant avec une bande passante de **1000 Mbps (1 000 Mbit/s)**.
  - Une intégration Prisma SD-WAN CloudBlade avec Prisma Access d'une version antérieure à 3.0.
  - Une configuration réseau distante qui fournit un accès entrant sécurisé aux applications sur un site réseau distant antérieur à la version 2.1 Innovation.

  Si vous avez une QoS et que vous l'utilisez avec vos réseaux distants, veillez à suivre les directives de migration QoS avant d'effectuer la migration.
- Si vous n'êtes pas sûr du modèle utilisé par votre déploiement, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**.
  - Si un champ **Bandwidth (Bande passante)** se trouve dans la zone Réseaux distants, vous allouez de la bande passante en fonction de l'emplacement de Prisma Access, et vous pouvez migrer vers le modèle de bande passante agrégée.

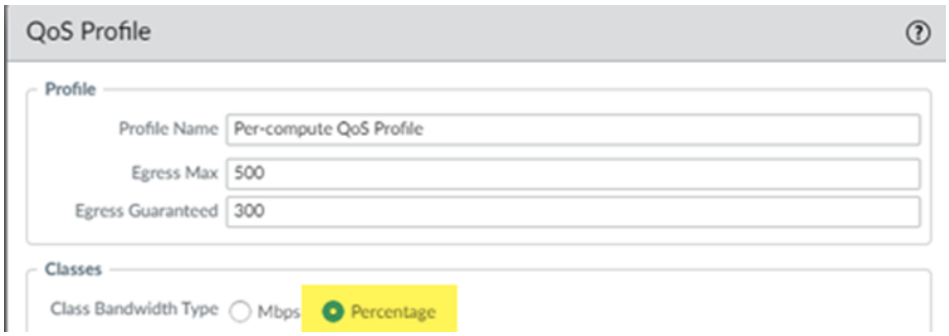


  - Si vous voyez un **IPSec Termination Node (Nœud de terminaison IPSec)**, vous avez déjà migré vers le modèle de bande passante agrégée.



 ©2025 Palo Alto Networks, Inc.

- Après avoir migré vers le modèle de bande passante agrégée, vous ne pouvez pas revenir à un déploiement qui alloue la bande passante en fonction de l'emplacement Prisma Access, car ce changement est permanent.
- Vous devez disposer d'un minimum de 50 Mbit/s de bande passante disponible pour migrer vers le modèle de bande passante agrégée.
- Si vous souhaitez mettre en œuvre la QoS après la migration, apprenez les différences concernant la configuration de la QoS pour un déploiement de bande passante agrégée.
  - Veillez à utiliser un **Class Bandwidth Type (Type de bande passante de classe)** de **Percentage (Pourcentage)** plutôt que de **Mbps (Mbit/s)** dans vos profils QoS. Prisma Access ne prend pas en charge les types de bande passante de **Mbps (Mbit/s)** dans les profils QoS pour les déploiements qui allouent la bande passante en fonction de l'emplacement de calcul.



  - Découvrez la manière de spécifier un rapport de bande passante garanti et de personnaliser la bande passante en fonction du site.

    Grâce à un rapport de bande passante garanti, vous pouvez allouer un pourcentage de la bande passante totale allouée dans l'emplacement de calcul. Prisma Access divise la bande passante garantie de manière égale par le nombre de nœuds de terminaison IPSec dans l'emplacement de calcul.

    La personnalisation de la bande passante en fonction du site vous permet d'appliquer un ratio d'allocation pour les sites et un seul nœud de terminaison IPSec et de spécifier des profils QoS par site dans les **Settings (Paramètres)** du réseau distant. Vous pouvez également spécifier un profil QoS durant de la configuration du réseau distant en sélectionnant le réseau distant et en spécifiant un profil QoS dans l'onglet **QoS**.
- Si vous avez configuré vos réseaux distants pour fournir un accès entrant sécurisé à vos emplacements réseau distant, toutes les fonctionnalités d'accès entrant existantes sont prises en charge, telles que l'activation d'une liaison WAN secondaire (**Enable Secondary WAN (Activer le WAN secondaire)**), les options BGP, QoS et source NAT. Aucun modification n'est apportée à la bande passante consommée par les adresses IP publiques allouées par Prisma Access (5 adresses IP prennent 150 Mbit/s de votre allocation de licence de réseau distant, et 10 adresses IP prennent 300 Mbit/s).

  Si vous devez configurer un accès entrant après la migration, utilisez la procédure d'accès entrant spécifique au modèle de bande passante agrégée.

 ©2025 Palo Alto Networks, Inc.

- Palo Alto Networks vous recommande de prendre note des paramètres existants de votre bande passante et du total sous licence de la bande passante avant de migrer.

  Bien que Prisma Access fait migrer votre bande passante pendant la migration ; vous devez prendre note de vos paramètres actuels comme une bonne pratique et apporter les ajustements nécessaires à la bande passante de l'emplacement de calcul après la migration.

  - Vérifiez les paramètres existants de votre bande passante en sélectionnant **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** et prenez note de la **Bandwidth (Bande passante)** existante qui est disponible pour chaque connexion de réseau distant.
  - Accédez à **Panorama** > **Licenses (Licences)** et vérifiez le total sous licence de votre bande passante en Mbit/s pour les réseaux distants. Ces informations sont incluses dans la section **Prisma Access Net Capacity (Capacité nette)** ou **GlobalProtect Cloud Service for Mobile Users (Service cloud GlobalProtect pour les utilisateurs mobiles)**, en fonction de votre type de licence.

Après la migration, prenez note des différences suivantes dans votre déploiement :

- Intégrez tous les nouveaux réseaux distants au moyen de la procédure d'intégration de réseau distant pour la bande passante agrégée.
- Lorsque vous consultez les statistiques d'utilisation de la bande passante, celles-ci sont affichées au niveau de chaque nœud de terminaison IPSec.

Allocation de bande passante pour un déploiement de bande passante agrégée migrée

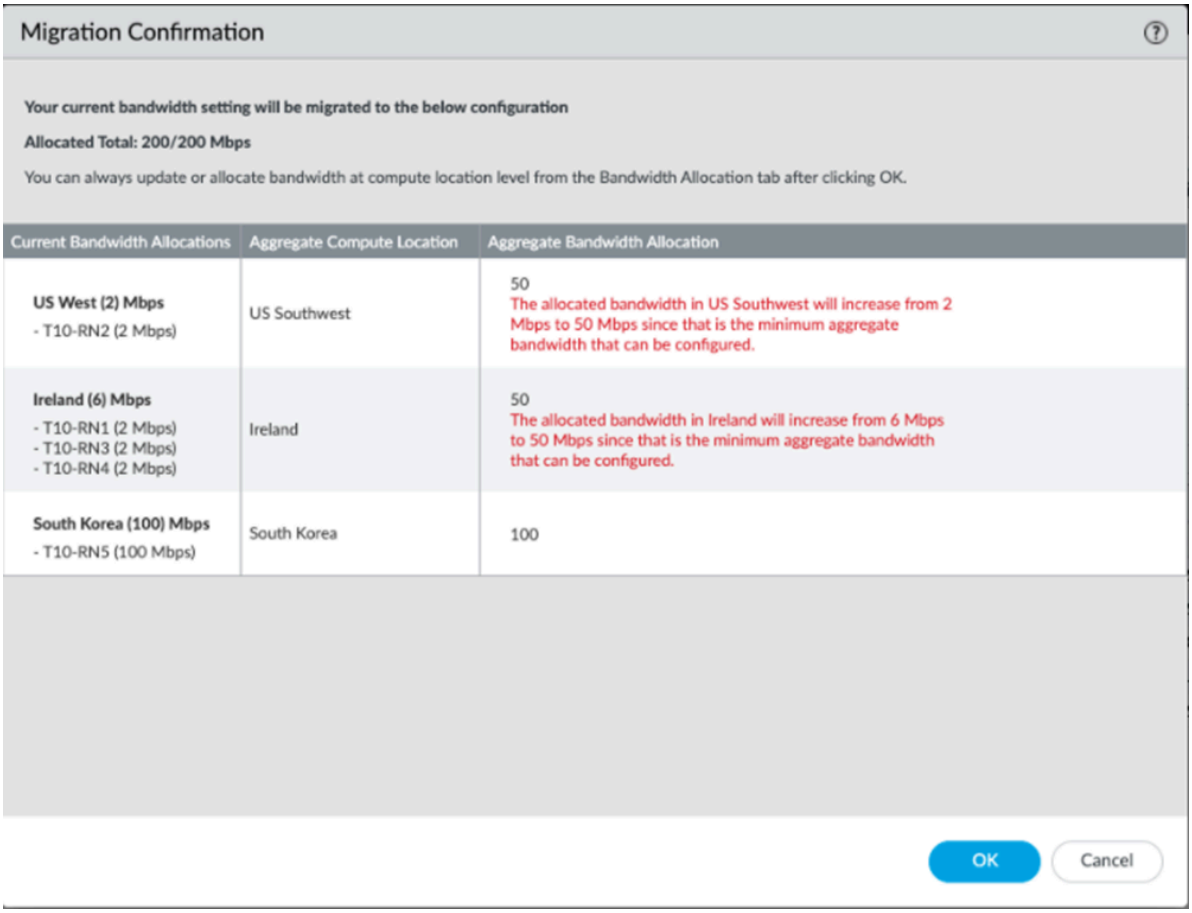
Si vous disposez d'un déploiement qui alloue de la bande passante en fonction de l'emplacement Prisma Access, Prisma Access apporte les modifications suivantes lors de votre migration vers le modèle de bande passante agrégée :

- Prisma Access additionne la bande passante de tous les emplacements d'un emplacement de calcul donné et alloue la bande passante additionnée à cet emplacement de calcul.

  Par exemple, vous avez trois emplacements (**Emplacement 1**, **Emplacement 2**et **Emplacement 3**) dans les régions du Mexique Ouest, des États-Unis Sud-Ouest et des États-Unis Ouest, et chaque emplacement existant dispose d'une bande passante de 50 Mbit/s. Étant donné que chaque emplacement se trouve dans l'emplacement de calcul des États-Unis Sud-Ouest, Prisma Access additionne la bande passante des trois emplacements et alloue 150 Mbit/s de bande passante à l'emplacement États-Unis Sud-Ouest.
- Si l'ensemble de l'emplacement ou tous les emplacements d'un emplacement de calcul ont une bande passante totale inférieure à 50 Mbit/s, Prisma Access augmentera la bande passante à

 ©2025 Palo Alto Networks, Inc.

50 Mbit/s pour cet emplacement de calcul. Prisma Access vous indique les emplacements qui nécessitent une augmentation de la bande passante pendant le processus de migration.



- Prisma Access utilise des nœuds de terminaison IPSec dans les déploiements de bande passante agrégée. Pendant la migration, Prisma Access fournit un nœud de terminaison IPSec par emplacement de calcul pour chaque 1 000 Mbit/s de bande passante allouée. Par exemple, si vous allouez 1 500 Mbit/s de bande passante dans un emplacement de calcul, Prisma Access fournit à cet emplacement deux nœuds de terminaison IPSec.

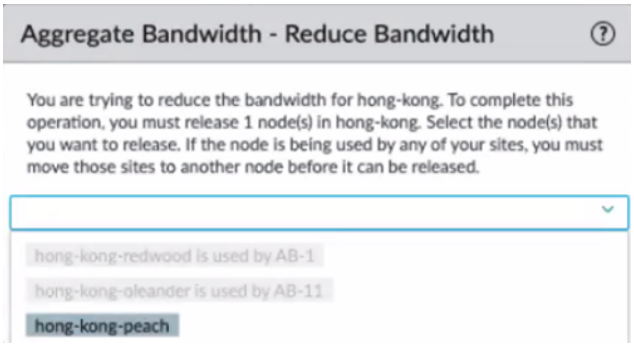
  Vous attribuez des nœuds de terminaison IPSec à un réseau distant lors de l'intégration du réseau distant. Dans une migration de bande passante agrégée, Prisma Access associe les nœuds de terminaison IPSec aux réseaux distants durant la migration. La liste suivante fournit des exemples d'association de nœuds de terminaison IPSec pour une migration :

  - Si vous disposez de quatre réseaux distants situés dans le même emplacement de calcul, et que ces emplacements ont chacun 50 Mbit/s de bande passante, Prisma Access alloue 200 Mbit/s de bande passante à cet emplacement de calcul, fournit un seul nœud de terminaison IPSec à cet emplacement de calcul et associe ce nœud de terminaison IPSec aux quatre réseaux distants.
  - Si vous disposez de trois réseaux distants dans le même emplacement de calcul ayant chacun 100 Mbit/s, Prisma Access alloue 300 Mbit/s de bande passante à cet emplacement de calcul, fournit un seul nœud de terminaison IPSec à cet emplacement de calcul et associe ce nœud de terminaison IPSec aux trois réseaux distants.

 ©2025 Palo Alto Networks, Inc.

- Si vous disposez de sept réseaux distants dans le même emplacement de calcul, avec deux réseaux distants de 500 Mbit/s et cinq réseaux distants de 100 Mbit/s chacun, Prisma Access alloue 1 500 Mbit/s de bande passante à cet emplacement de calcul. Étant donné que le total de bande passante alloué à cet emplacement de calcul est supérieur à 1 000 Mbit/s, Prisma Access alloue deux nœuds de terminaison IPSec et effectue les associations suivantes :
  - Les deux réseaux distants de 500 Mbit/s se voient attribuer un nœud de terminaison IPSec (un nœud pour chaque réseau distant de 1 000 Mbit/s).
  - Les cinq réseaux distants de 100 Mbit/s se voient attribuer un seul nœud de terminaison IPSec.

  Après la migration, vous pouvez modifier l'association de nœuds de terminaison IPSec pour augmenter la bande passante d'un emplacement. Par exemple, à partir d'un emplacement de calcul avec deux nœuds de terminaison IPSec, vous pouvez réaffecter un seul nœud de terminaison IPSec à un seul emplacement et réaffecter l'autre nœud de terminaison IPSec aux emplacements restants, ce qui fournit effectivement l'emplacement qui ne partage pas un nœud de terminaison IPSec avec plus de bande passante.
- Si vous réduisez suffisamment la bande passante, vous devrez peut-être libérer un nœud de terminaison IPSec. Par exemple, si vous réduisez la bande passante dans un emplacement de calcul de 1 500 Mbit/s à 800 Mbit/s, vous devez supprimer l'un des nœuds de terminaison IPSec existants. Si l'un de ces nœuds est utilisé par des emplacements existants, vous devez réaffecter le nœud de terminaison IPSec avant de supprimer le nœud de terminaison IPSec.



Directives relatives à la migration QoS

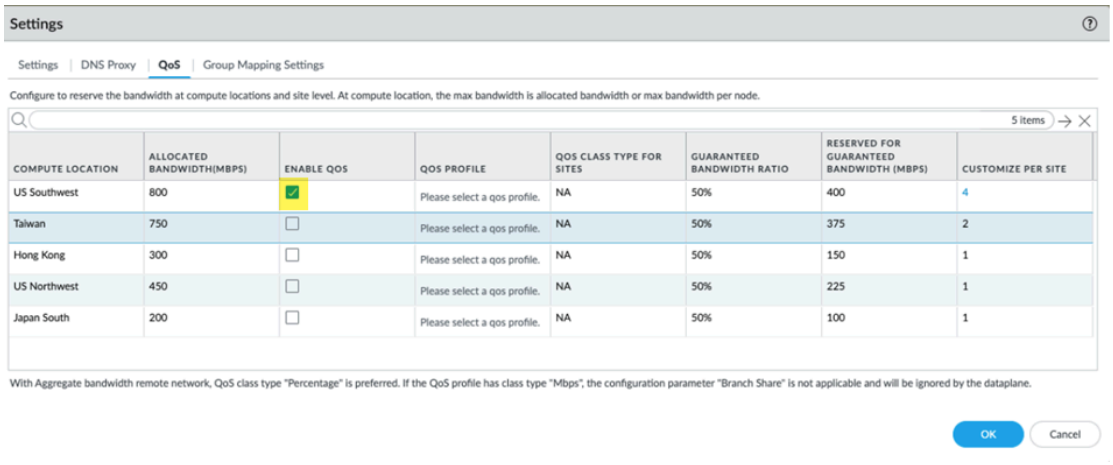
Si vous utilisez QoS avec votre déploiement Prisma Access réseau distant et que vous allouez la bande passante par emplacement, vous pouvez migrer vers un déploiement de bande passante agrégée tout en conservant vos politiques et profils QoS existants.

À l'aide du modèle de bande passante agrégée, vous allouez la bande passante à un niveau agrégé par emplacement de calcul, et Prisma Access alloue dynamiquement la bande passante en fonction de la charge ou de la demande par emplacement.

Après la migration, l'onglet **QoS** affiche la configuration QoS dans les paramètres du réseau distant (**Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** > **Settings (Paramètres)**). Tous les emplacements de calcul mappés à des emplacements pour lesquels la QoS est activée ont l'option **Enable QoS (Activer la QoS)** sélectionnée; tous les emplacements de calcul qui mappent des emplacements pour lesquels la QoS n'est pas activée ont l'option **Enable QoS (Activer la QoS)** désélectionnée.

 ©2025 Palo Alto Networks, Inc.

La capture d'écran suivante montre un exemple d'onglet QoS après la migration. La QoS est activée pour un réseau distant dans l'emplacement États-Unis Ouest, et n'est pas activée sur un autre emplacement. Étant donné que l'emplacement États-Unis Ouest correspond à l'emplacement de calcul États-Unis Sud-Ouest, l'onglet **QoS** indique que la QoS est activée pour l'emplacement de calcul États-Unis Sud-Ouest.

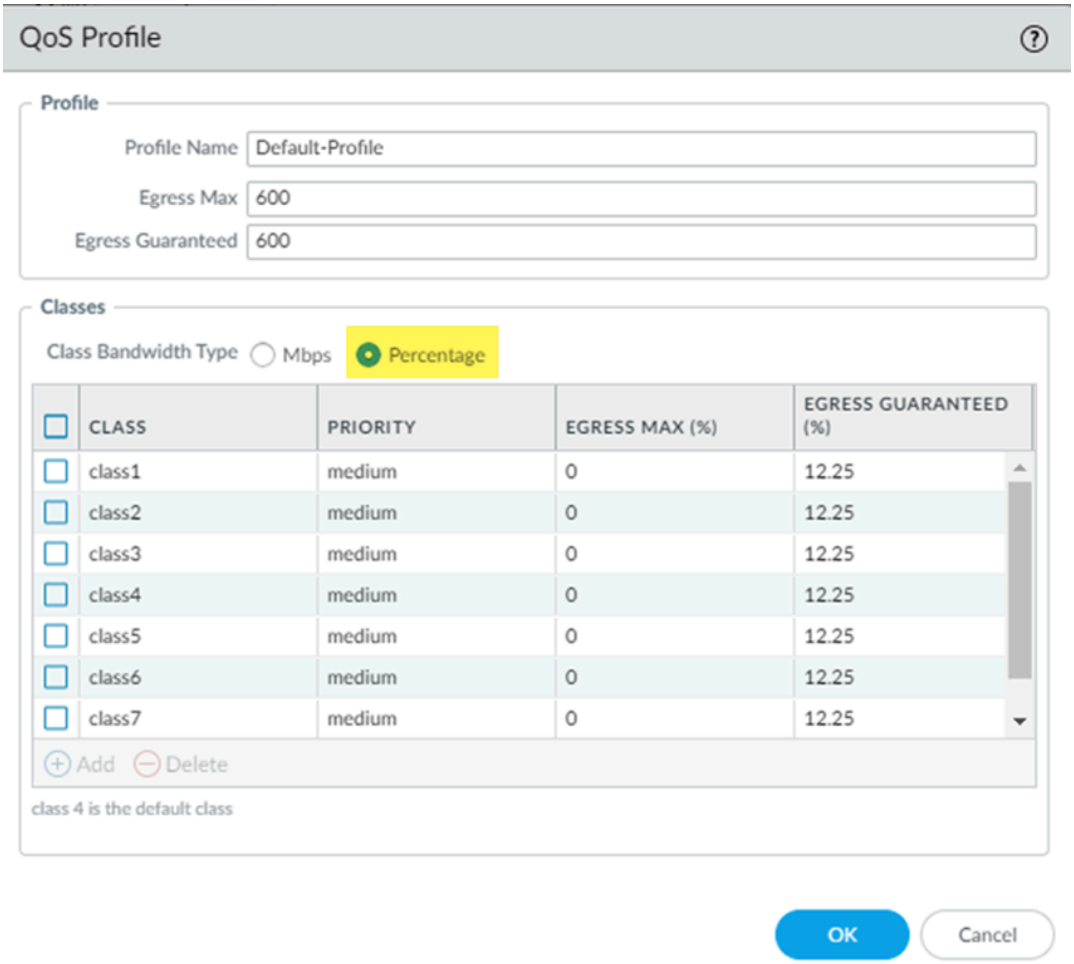


Palo Alto Networks formule les recommandations et les exigences suivantes pour la QoS dans un déploiement de bande passante agrégée.

- Étant donné que la bande passante est partagée pour tous les emplacements dans un seul emplacement de calcul, vous devez modifier le **Class Bandwidth Type (Type de bande passante de classe)** de **Mbps (Mbit/s)** à **Percentage (Pourcentage)**. La seule fois où un type de bande passante de **Mbps (Mbit/s)** est pris en charge lorsque vous disposez d'un déploiement existant

 ©2025 Palo Alto Networks, Inc.

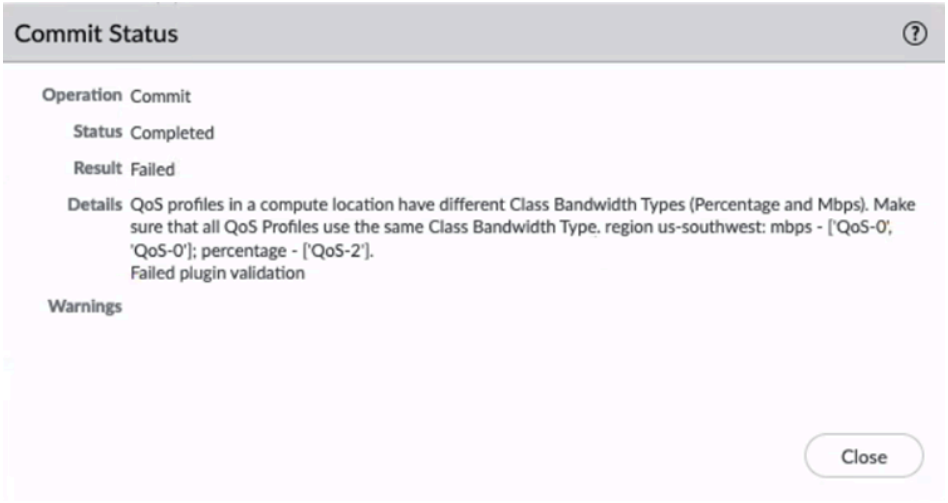
qui alloue la bande passante par emplacement, puis que vous migrez vers un déploiement de bande passante agrégée.



- Vous ne pouvez pas ajuster l'allocation de bande passante QoS en fonction des Mbit/s dans le profil ; pour les profils qui utilisent un type de bande passante de **Percentage (Pourcentage)**, vous pouvez modifier la bande passante QoS par emplacement en ajustant le rapport de bande passante garanti et en personnalisant le profil QoS par site.

 ©2025 Palo Alto Networks, Inc.

- Vous ne pouvez pas mélanger les types de bande passante dans un emplacement de calcul. Si vous le faites, vous recevez un message d'erreur lors de la validation.

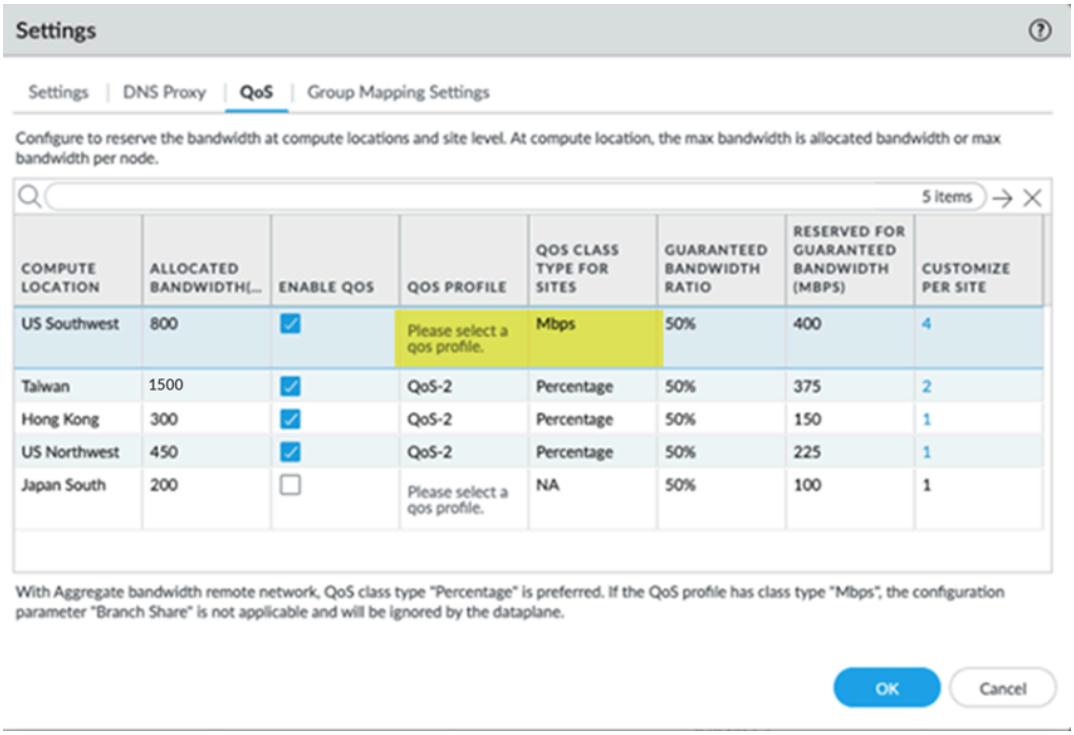


- Si vous ajoutez de nouveaux emplacements et qu'ils appartiennent à un nouvel emplacement de calcul, vous ne pourrez créer que des profils dotés d'un **Class Bandwidth Type (Type de bande passante de classe)** de **Percentage (Pourcentage)** dans le nouvel emplacement de calcul.
- Si vous conservez des profils QoS dotés d'un **Class Bandwidth Type (Type de bande passante de classe)** de **Mbps (Mbit/s)**, toute modification que vous apportez au rapport de bande passante garanti ou personnalisation que vous faites au profil QoS par site sera ignorée.
- Après la migration, tous les emplacements qui utilisent des profils QoS avec un **Class Bandwidth Type (Type de bande passante de classe)** de **Mbps (Mbit/s)** affichent un **QoS Class Type For Sites (Type de classe QoS pour les sites)** de **Mbps (Mbit/s)** pour leur emplacement de calcul correspondant dans l'onglet **QoS**. Les profils QoS ayant un **Class Bandwidth Type (Type de bande passante de classe)** de **Percentage (Pourcentage)** affichent un **QoS Class Type For Sites (Type de classe QoS pour les sites)** de **Percentage (Pourcentage)**.

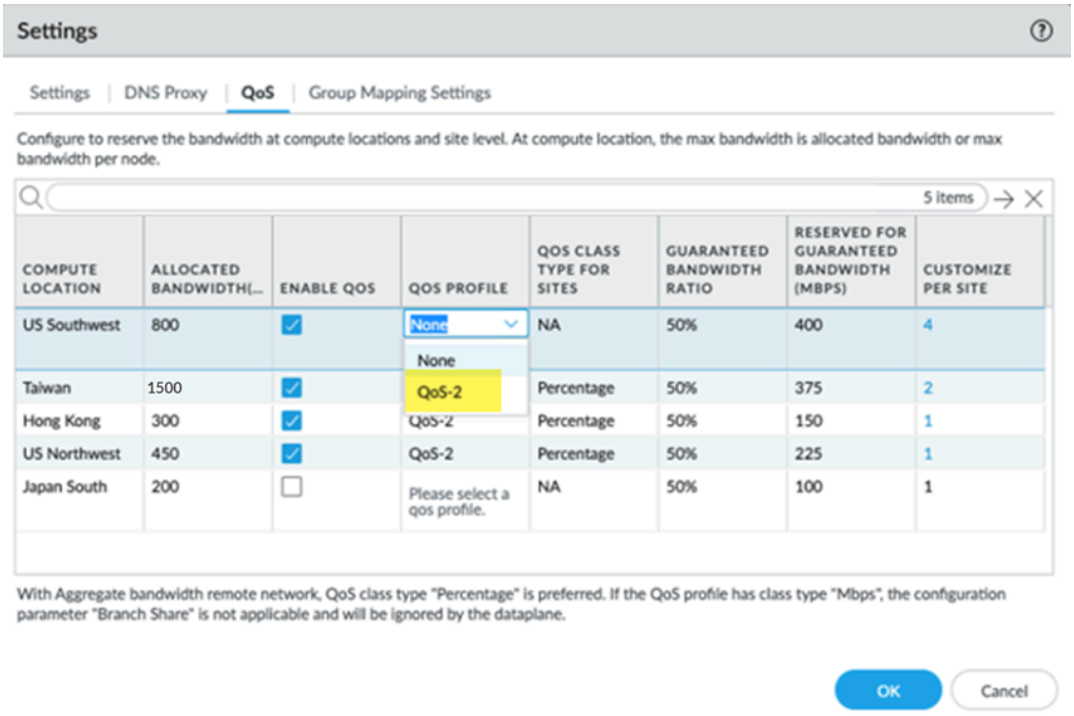
  En outre, vous ne pouvez pas sélectionner de profils QoS ayant un **Class Bandwidth Type (Type de bande passante de classe)** de **Mbps (Mbit/s)**. La capture d'écran suivante montre l'emplacement de calcul des États-Unis Sud-Ouest à l'aide d'un profil QoS doté d'un**Class**

 ©2025 Palo Alto Networks, Inc.

Bandwidth Type (Type de bande passante de classe) de **Mbps (Mbit/s)**. Ce choix n'est pas sélectionnable dans la liste déroulante de la zone **QoS Profile (Profil QoS)**.



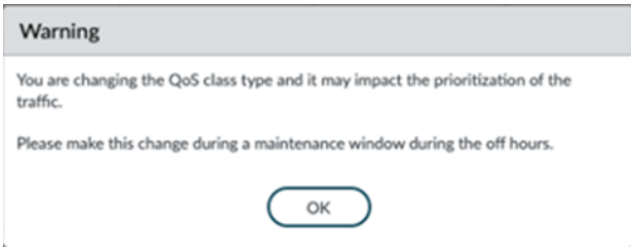
Toutefois, vous pouvez sélectionner un profil QoS qui utilise un **Class Bandwidth Type (Type de bande passante de classe)** de **Percentage (Pourcentage)** (QoS-2 dans cet exemple).



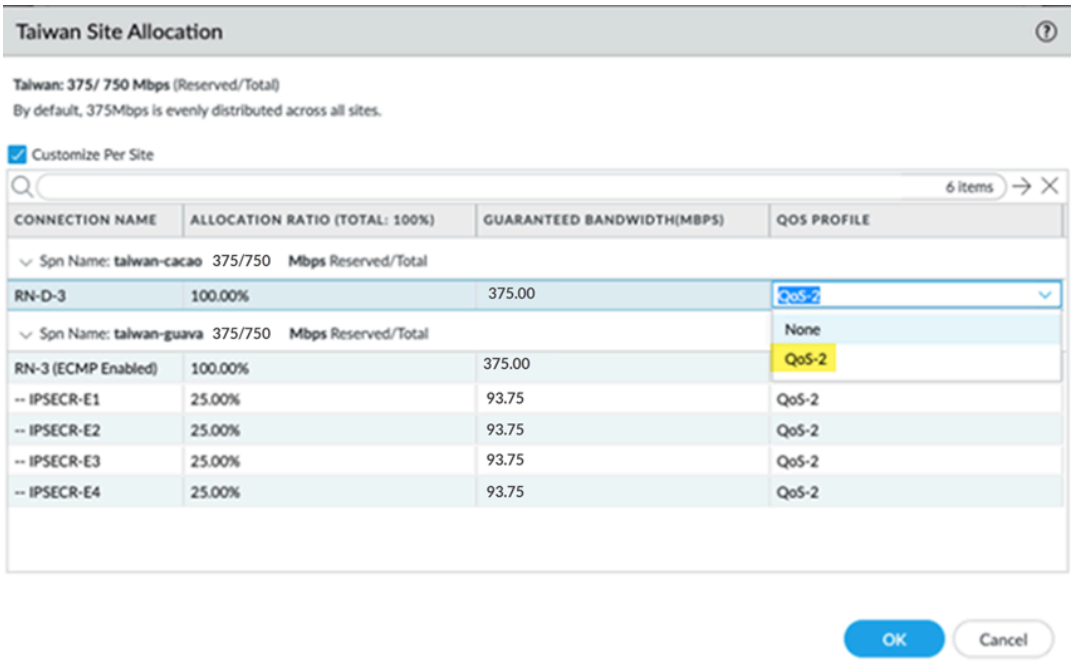
- Si vous changez le profil QoS d'un emplacement de calcul à partir d'un **Class Bandwidth Type (Type de bande passante de classe)** de **Mbps (Mbit/s)** en **Percentage (Pourcentage)**, vous

 ©2025 Palo Alto Networks, Inc.

devez effectuer le changement pendant une fenêtre de maintenance ou pendant les heures creuses. La modification du profil QoS peut modifier la hiérarchisation du trafic.



- Vous pouvez seulement sélectionner des profils QoS ayant un **Class Bandwidth Type (Type de bande passante de classe)** de **Percentage (Pourcentage)** lorsque vous personnalisez le profil QoS par site.



Migrer les paramètres de gestion de la bande passante

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Apprenez à migrer les paramètres de gestion de la bande passante.

Si vous avez un déploiement de réseau distant Prisma Access qui alloue la bande passante en fonction de l'emplacement, Prisma Access vous permet de rendre ce déploiement plus flexible et évolutif en migrant vers un déploiement qui alloue la bande passante en fonction de l'emplacement de calcul (le modèle de bande passante agrégée). Après avoir examiné la liste de contrôle de planification de la migration, suivez les étapes ci-dessous pour effectuer

 ©2025 Palo Alto Networks, Inc.

la migration vers le modèle de bande passante agrégée. Vous pouvez également migrer votre déploiement QoS de réseau distant. Lorsque vous migrez, tous les réseaux distants utilisent le modèle de bande passante agrégée.

Tenez compte des points suivants avant de migrer les paramètres de bande passante :

- Les composants de réseau distant suivants restent inchangés après la migration :
  - Le plan de données Prisma Access ne change pas.
  - Les tunnels existants ne sont pas affectés.
  - Les paramètres de tunnel IPSec ne sont pas reconfigurés.
  - Les passerelles IKE, les configurations de tunnel IPSec et les profils crypto IKE et IPSec restent inchangés.
  - La **Service IP Address (Adresse IP du service)** de réseau distant reste inchangée pour chacun des réseaux distants.
- Prisma Access attribue des nœuds de terminaison IPSec et alloue la bande passante aux réseaux distants lors d'une migration vers le modèle de bande passante agrégée.
- Si votre configuration n'est pas prise en charge, l'onglet Bandwidth Allocation (Allocation de bande passante) et la bannière de migration ne sont pas visibles.
- Si vous avez une QoS avec vos réseaux distants, veillez à suivre les directives de migration QoS avant d'effectuer la migration.
- Après avoir migré vers le modèle de bande passante agrégée, vous ne pouvez pas revenir à un déploiement qui alloue la bande passante en fonction de l'emplacement Prisma Access ; ce changement est permanent.
- Vous devez disposer d'un minimum de 50 Mbit/s de bande passante disponible pour migrer vers le modèle de bande passante agrégée.
- Si vous souhaitez mettre en œuvre la QoS après la migration, apprenez les différences concernant la configuration de la QoS pour un déploiement de bande passante agrégée.
- Une fois la migration effectuée, vous devez intégrer tous les nouveaux réseaux distants au moyen de la procédure d'intégration de réseau distant pour la bande passante agrégée.
- Une fois la migration effectuée, lorsque vous consultez les statistiques d'utilisation de la bande passante, celles-ci sont affichées au niveau de chaque nœud de terminaison IPSec.
- N'utilisez pas la CLI pour effectuer la migration ; utilisez uniquement l'interface utilisateur.
- Strata Cloud Manager
- Panorama

Migrer les paramètres de gestion de la bande passante (Strata Cloud Manager)

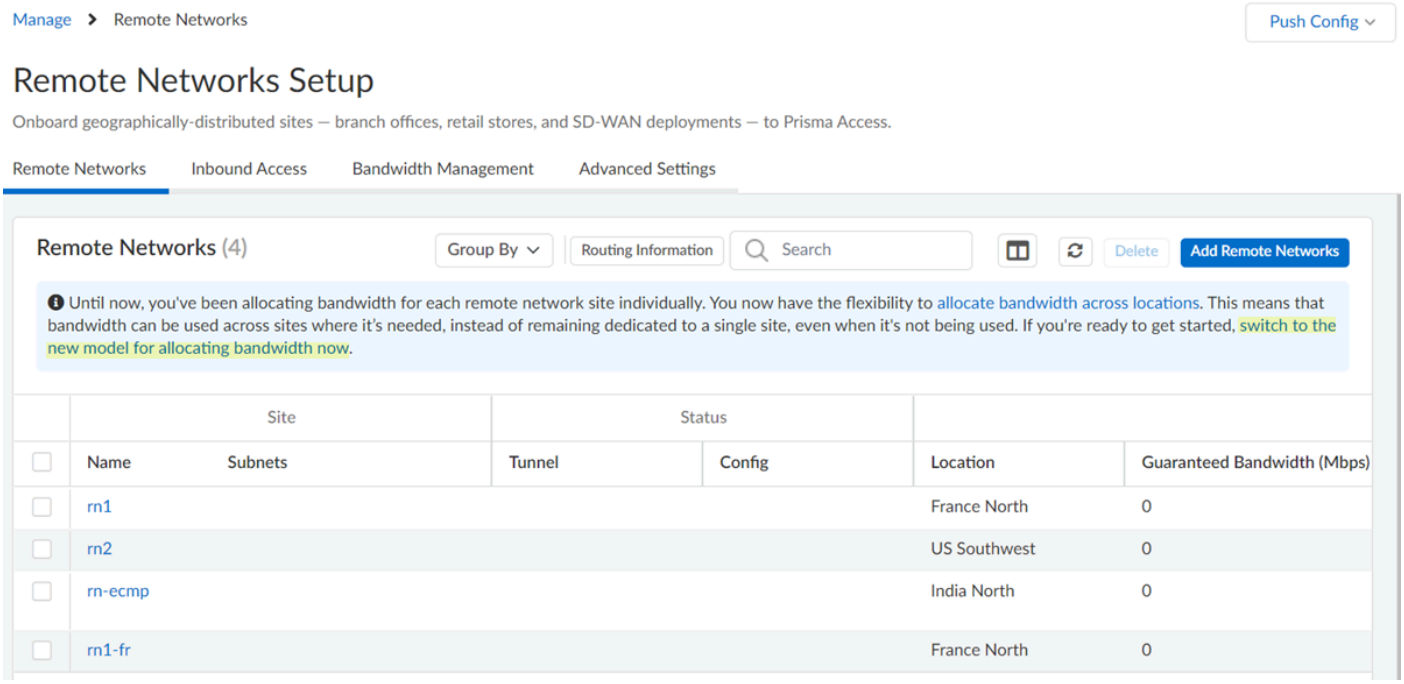
Si vous avez un déploiement de réseau distant Prisma Access qui alloue la bande passante en fonction de l'emplacement, Prisma Access vous permet de rendre ce déploiement plus flexible et évolutif en migrant vers un déploiement qui alloue la bande passante en fonction de l'emplacement de calcul (le modèle de bande passante agrégée). Après avoir examiné la liste de contrôle de planification de la migration, suivez les étapes ci-dessous pour effectuer la migration vers le modèle de bande passante agrégée.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Remote Networks (Réseaux distants)**.

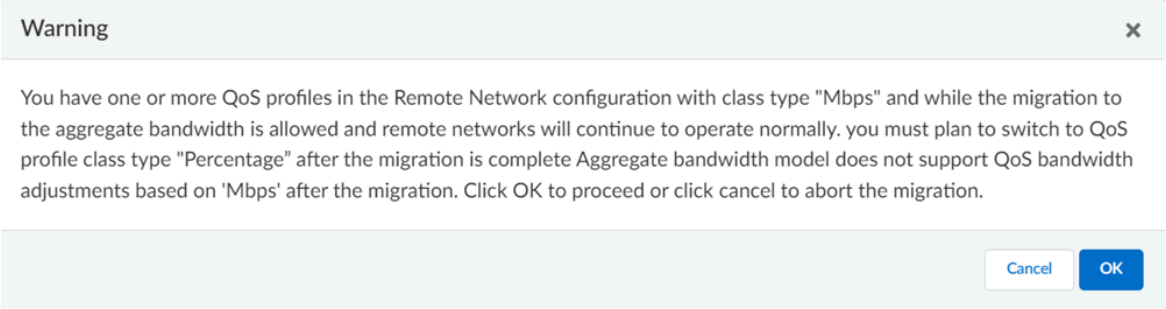
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Passez au nouveau modèle d'allocation de la bande passante.

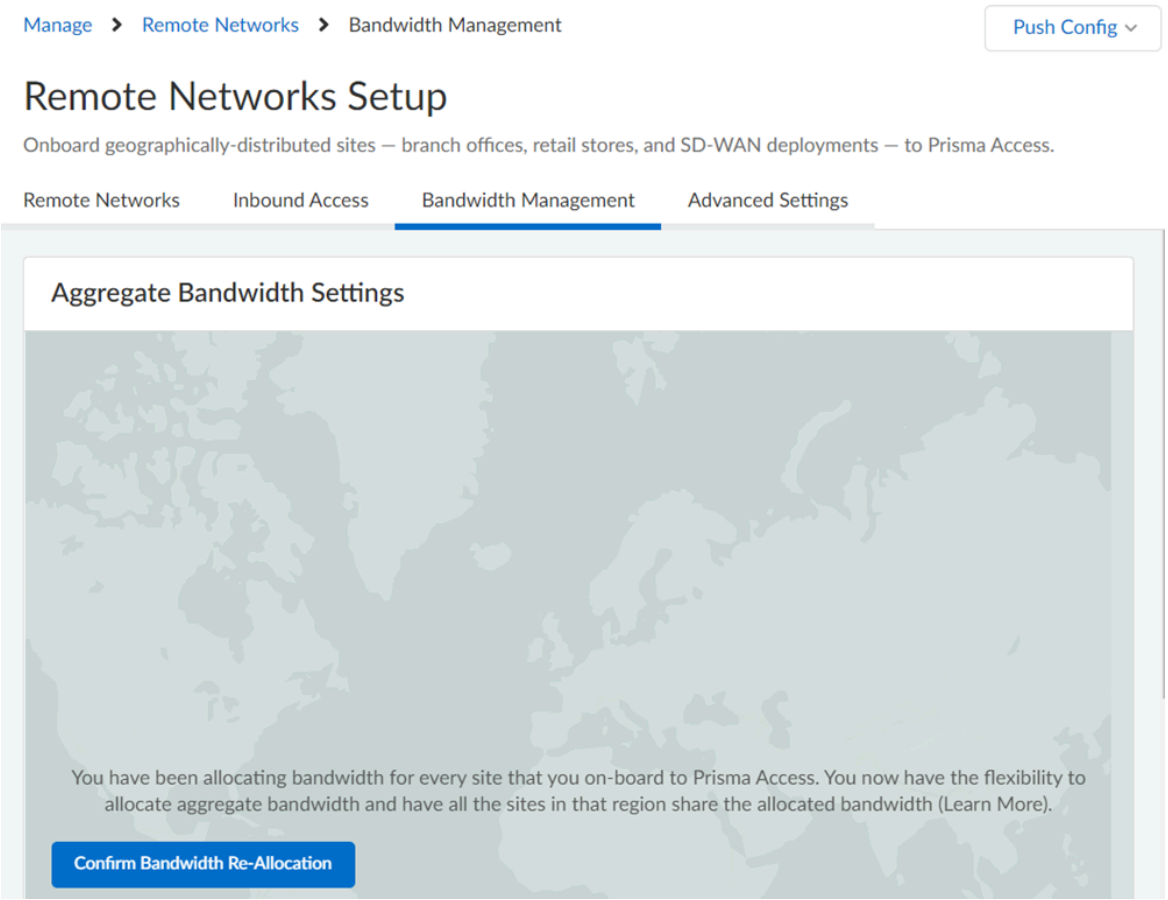


 ©2025 Palo Alto Networks, Inc.

- *Si vous disposez de profils QoS dont le **Class Bandwidth Type (Type de bande passante de classe)** est défini sur **Mbps (Mbit/s)**, Prisma Access vous avertit que vous devez prévoir de redéfinir le **Class Bandwidth Type (Type de bande passante de classe)** de ces profils sur **Percentage (Pourcentage)**.*



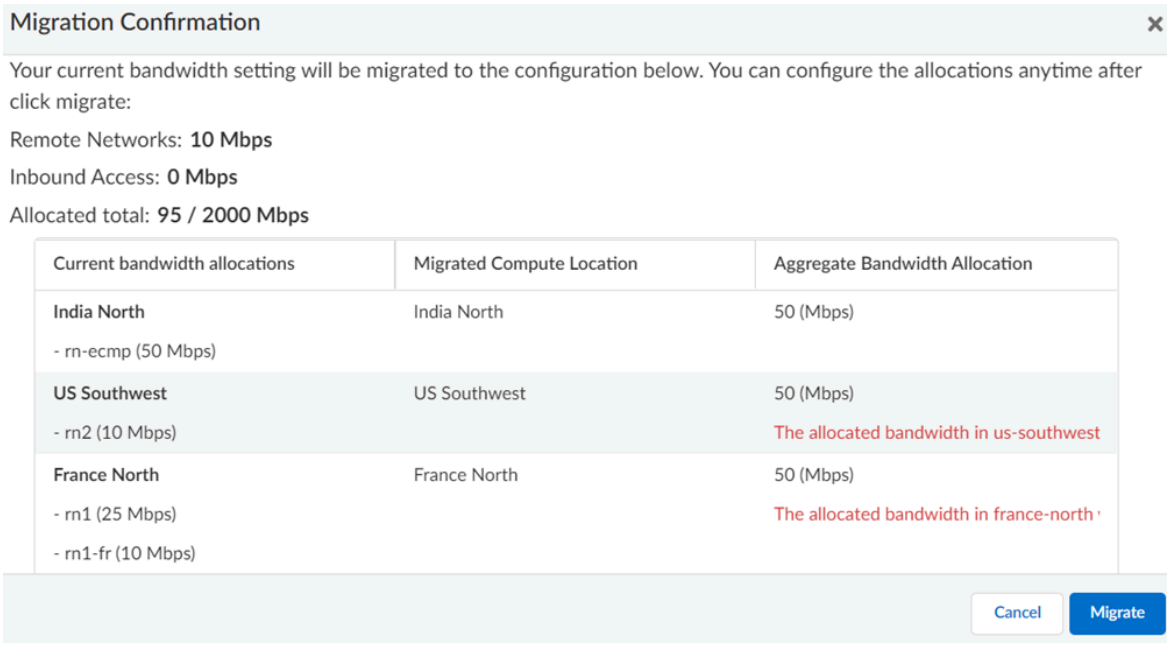
- *Vous pouvez également accéder à l'onglet **Bandwidth Management (Gestion de la bande passante)** et sélectionner **Confirm Bandwidth Re-Allocation (Confirmer la réallocation de la bande passante)**.*



 ©2025 Palo Alto Networks, Inc.

STEP 3 | Vérifiez les informations et sélectionnez **Migrate (Migrer)** dans la fenêtre contextuelle qui s'affiche.

Si l'ensemble de l'emplacement ou tous les emplacements d'un emplacement de calcul ont une bande passante totale inférieure à 50 Mbit/s, Prisma Access augmentera la bande passante à 50 Mbit/s pour cet emplacement de calcul. Prisma Access vous indique les emplacements qui nécessitent une augmentation de la bande passante pendant le processus de migration.



La migration vers le modèle de bande passante agrégée est permanente et ne peut pas être annulée. Avant d'effectuer la migration, passez en revue la liste de contrôle prémigration. Vous devez cliquer sur ***Commit and Push (Valider et appliquer)*** *pour que vos modifications prennent effet.*

Prisma Access migre la bande passante de réseau distant allouée vers le modèle de bande passante agrégée.

STEP 4 | **Commit and Push (Validez et appliquez)** vos modifications.

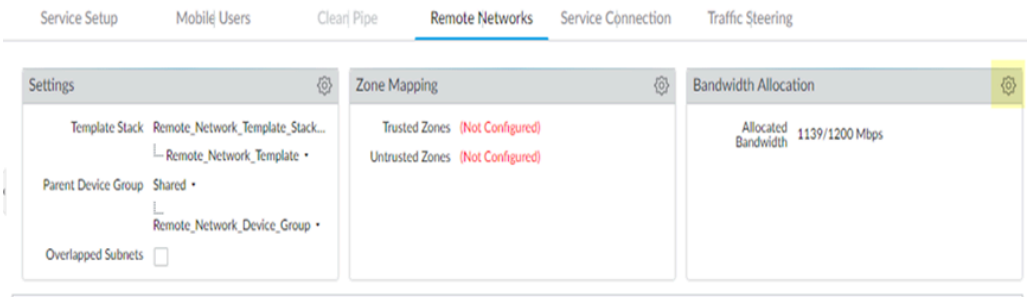
Migrer les paramètres de gestion de la bande passante (Panorama)

Si vous avez un déploiement de réseau distant Prisma Access qui alloue la bande passante en fonction de l'emplacement, Prisma Access vous permet de rendre ce déploiement plus flexible et évolutif en migrant vers un déploiement qui alloue la bande passante en fonction de l'emplacement de calcul (le modèle de bande passante agrégée). Après avoir examiné la liste de contrôle de planification de la migration, suivez les étapes ci-dessous pour effectuer la migration vers le modèle de bande passante agrégée.

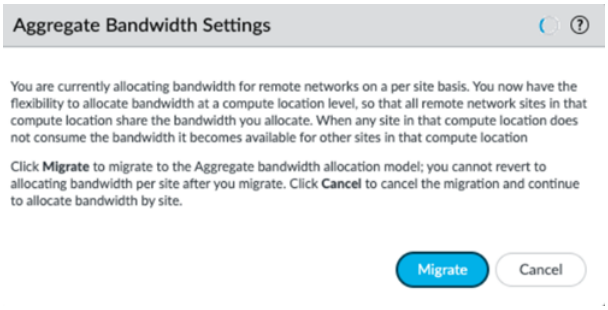
STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Pour modifier les paramètres, cliquez sur l'icône en forme d'engrenage dans la zone **Bandwidth Allocation (Allocation de bande passante)**.

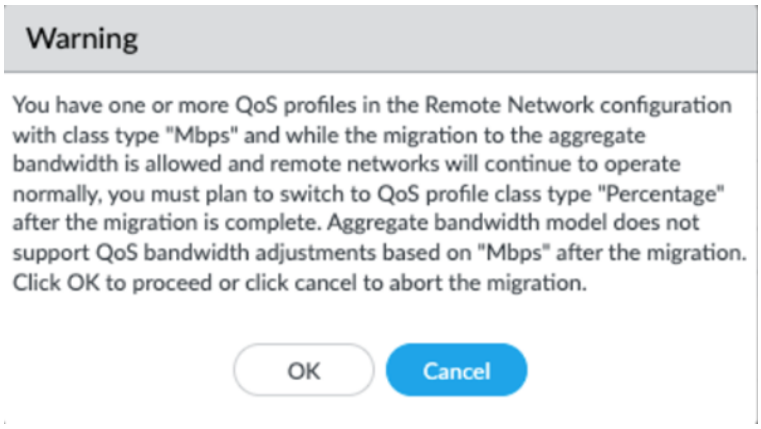


STEP 3 | Sélectionnez **Migrate (Migrer)** dans la fenêtre contextuelle qui s'affiche.



La migration vers le modèle de bande passante agrégée est permanente et ne peut pas être annulée. Avant d'effectuer la migration, passez en revue la liste de contrôle prémigration. Vous devez cliquer sur ***Commit and Push (Valider et appliquer)*** *pour que vos modifications prennent effet.*

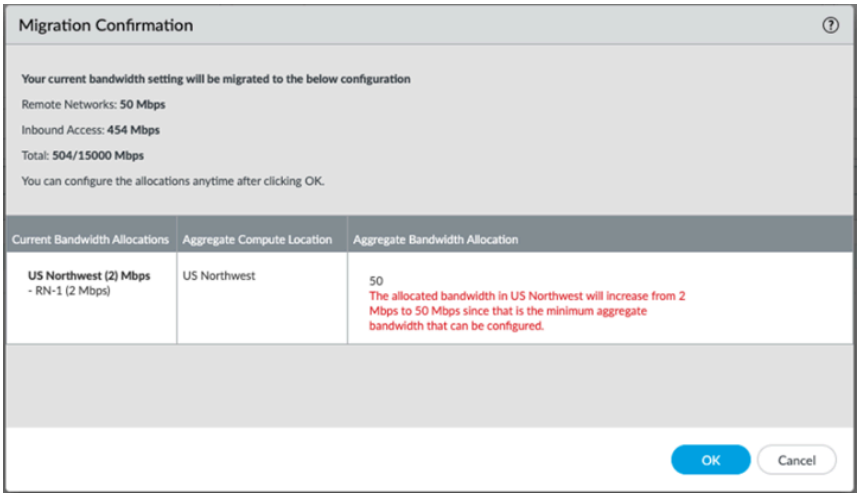
Si vous disposez de profils QoS dont le ***Class Bandwidth Type (Type de bande passante de classe)*** *est défini sur* ***Mbps (Mbit/s)****, Prisma Access vous avertit que vous devez prévoir de redéfinir le* ***Class Bandwidth Type (Type de bande passante de classe)*** *de ces profils sur* ***Percentage (Pourcentage)****.*



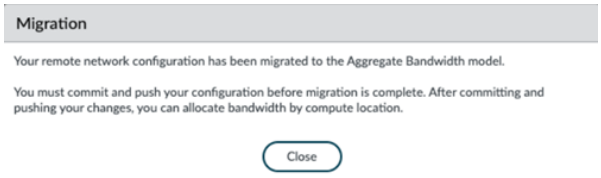
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Passez en revue les informations dans la fenêtre **Migration Confirmation (Confirmation de migration)**, puis cliquez sur **OK**.

Si l'ensemble de l'emplacement ou tous les emplacements d'un emplacement de calcul ont une bande passante totale inférieure à 50 Mbit/s, Prisma Access augmentera la bande passante à 50 Mbit/s pour cet emplacement de calcul. Prisma Access vous indique les emplacements qui nécessitent une augmentation de la bande passante pendant le processus de migration.



Prisma Access migre la bande passante de réseau distant allouée vers le modèle de bande passante agrégée et affiche une fenêtre de confirmation. Cliquez sur **Close (Fermer)** pour fermer la fenêtre.



STEP 5 | **Commit and Push (Validez et appliquez)** vos modifications.

 ©2025 Palo Alto Networks, Inc.

Intégrer un réseau distant

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Une fois que vous avez planifié votre réseau distant, vous pouvez commencer le processus de configuration. Celui-ci inclut l'intégration du réseau distant, la connexion du site du réseau distant à Prisma Access et l'activation du routage et de la QoS pour le réseau distant. Pour chaque réseau distant que vous souhaitez sécuriser à l'aide de Prisma Access pour les réseaux, vous pouvez transmettre la configuration de la politique requise à Prisma Access et intégrer chaque réseau distant afin de pouvoir commencer à envoyer du trafic depuis le site distant via le tunnel IPSec vers Prisma Access. Suivez l'une des procédures suivantes pour intégrer vos réseaux distants en fonction de votre type d'allocation de bande passante :

Apprenez à intégrer un réseau distant.

- Strata Cloud Manager
- Panorama

Intégrer un réseau distant (Strata Cloud Manager)

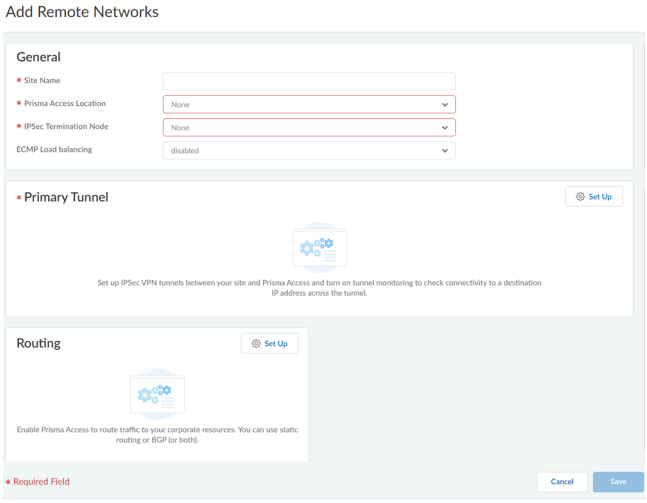
Voici comment ajouter un nouveau site de réseau distant à Prisma Access. Commencez par spécifier l'emplacement et à définir la quantité de bande passante à allouer à la connexion.

STEP 1 | Lancez Prisma Access (Managed by Strata Cloud Manager).

STEP 2 | Assurez-vous d'avoir alloué de la bande passante à l'emplacement où vous déploierez le réseau distant. Reportez-vous à la section Liste de contrôle de planification pour les réseaux distants.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Remote Networks (Réseaux distants)** > **Add Remote Networks (Ajouter des réseaux distants)**.



STEP 4 | Donnez au réseau distant un **Site Name (Nom de site)** descriptif.

STEP 5 | Sélectionnez la **Region (Région)** dans laquelle le site se trouve et cliquez sur Prisma Access **Location (Emplacement)** le plus proche.

STEP 6 | (Uniquement si vous prévoyez d'utiliser BGP pour le routage dynamique) Activez **ECMP Load Balancing (Équilibrage de charge ECMP)** afin que le site de réseau distant puisse utiliser jusqu'à quatre tunnels IPSec.

Le BGP est requis pour l'équilibrage de charge ECMP ; la QoS et les itinéraires statiques ne sont pas pris en charge.

Lorsque vous activez ECMP, la charge du trafic du réseau distant est équilibré sur les tunnels que vous configurez.

STEP 7 | Configurez les **Advanced Settings (Paramètres avancés)**.

- (Facultatif) Utilisez les **Static Entries (Entrées statiques)** pour résoudre les FQDN en adresses IP spécifiques.

  Cette fonctionnalité peut être utile si vous disposez de services Internet pour invités dans votre organisation et que vous souhaitez que vos invités utilisent les moteurs de recherche en toute sécurité, les empêchant de rechercher du contenu potentiellement inapproprié ou offensant qui pourrait être contraire à la politique de l'entreprise. Pour ce faire, saisissez un **Name (Nom)** unique pour la règle d'entrée statique, un **FQDN** et l'**Address (Adresse)** IP vers laquelle la demande FQDN doit être dirigée.



 ©2025 Palo Alto Networks, Inc.

- Si vous souhaitez que Prisma Access serve de proxy pour les requêtes DNS, configurez les valeurs de **UDP Queries Retries (Tentatives de requêtes UDP)** (**Interval (Intervalle) (sec)** pour réessayer la requête en secondes et le nombre de **Attempts (Tentatives)** de requête à effectuer.

STEP 8 | Connecter un site de réseau distant à Prisma Access, où vous créez un tunnel VPN IPSec pour connecter le site de réseau distant à Prisma Access.

STEP 9 | Configurez le routage statique.

1. Pour que les itinéraires statiques acheminent le trafic vers et depuis votre siège social ou centre de données, **Add (Ajoutez)** les sous-réseaux IP ou les adresses IP que vous voulez sécuriser au niveau de la succursale.

   Si vous apportez des modifications aux sous-réseaux IP de votre réseau de siège social ou de centre de données, vous devez mettre à jour les itinéraires statiques manuellement.

STEP 10 | Configurez le routage dynamique.

1. Pour que le routage dynamique annonce les sous-réseaux du siège social ou du centre de données, vous devez **Enable BGP for Dynamic Routing (Activer BGP pour le routage dynamique)**.
2. (Facultatif) Sélectionnez une valeur **MRAI Timer (Minuterie MRAI)**.

   Le routage BGP propose un minuteur que vous pouvez utiliser pour adapter la convergence du routage BGP dans votre réseau, appelé *Intervalle minimum d'annonce d'itinéraire (MRAI)*. MRAI agit pour limiter le débit des mises à jour par destination et les routeurs BGP attendent au moins le délai MRAI configuré avant d'envoyer une annonce pour le même préfixe. Un nombre plus petit vous donne un temps de convergence plus rapide mais crée plus d'annonces sur votre réseau. Un nombre plus élevé diminue le nombre d'annonces pouvant être envoyées, tout en ralentissant également la convergence de routage. Vous décidez du nombre à mettre dans votre réseau pour obtenir le meilleur équilibre entre une convergence de routage plus rapide et moins d'annonces.

   Configurez une plage MRAI comprise entre 1 et 600 secondes, avec une valeur par défaut de 30 secondes.
3. Pour réduire le nombre d'annonces de sous-réseaux IP d'utilisateurs mobiles via BGP vers votre équipement sur site client (CPE), spécifiez Prisma Access pour résumer les sous-réseaux avant de les annoncer en sélectionnant **Summarize Mobile User Routes before advertising (Résumer les itinéraires des utilisateurs mobiles avant de les annoncer)**.

   Par défaut, Prisma Access annonce les pools d'adresses IP des utilisateurs mobiles par blocs de sous-réseaux /24. Si vous les résumez, Prisma Access annonce le pool en fonction du sous-réseau que vous avez spécifié. Par exemple, Prisma Access annonce un pool d'adresses IP mobiles d'utilisateurs publics de 10.8.0.0/20 en utilisant le sous-réseau /20, plutôt que de diviser le pool en sous-réseaux de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, et ainsi de suite, avant de les annoncer. Le résumé de ces annonces peut réduire le nombre d'itinéraires stockés dans les tableaux de routage CPE. Par exemple, vous pouvez utiliser le résumé de pool d'adresses IP avec des passerelles VPN cloud

 ©2025 Palo Alto Networks, Inc.

(passerelles privées virtuelles [VGW] ou passerelles de transit [TGW]) qui peuvent accepter un nombre limité d'itinéraires.

4. (Facultatif) Pour que Prisma Access génère une annonce d'itinéraire par défaut pour le réseau distant à l'aide d'eBGP, sélectionnez **Advertise Default Route (Annoncer l'itinéraire par défaut)**. Assurez-vous que votre réseau n'a pas d'autre itinéraire par défaut annoncé par BGP, sinon vous pourriez introduire des problèmes de routage dans votre réseau.
5. (Facultatif) Si vous avez configuré un WAN secondaire et que vous devez modifier l'adresse de l'homologue BGP secondaire (de secours), sélectionnez **Use different BGP Peer for Secondary Tunnel (Utiliser un homologue BGP différent pour le tunnel secondaire)** et saisissez un homologue unique et, éventuellement, une adresse IP locale pour le WAN secondaire.
6. (Facultatif) Sélectionnez **Do Not Export Routes (Ne pas exporter les itinéraires)** pour empêcher Prisma Access de transférer les itinéraires vers le siège social ou le centre de données.

   Par défaut, Prisma Access annonce toutes les informations de routage BGP, y compris les itinéraires locaux et tous les préfixes qu'il reçoit d'autres connexions aux services, réseaux distants et sous-réseaux d'utilisateurs mobiles. Cochez cette case pour empêcher Prisma Access d'envoyer des annonces BGP, mais pour qu'il utilise toujours les informations BGP qu'il reçoit pour apprendre les itinéraires d'autres voisins BGP.

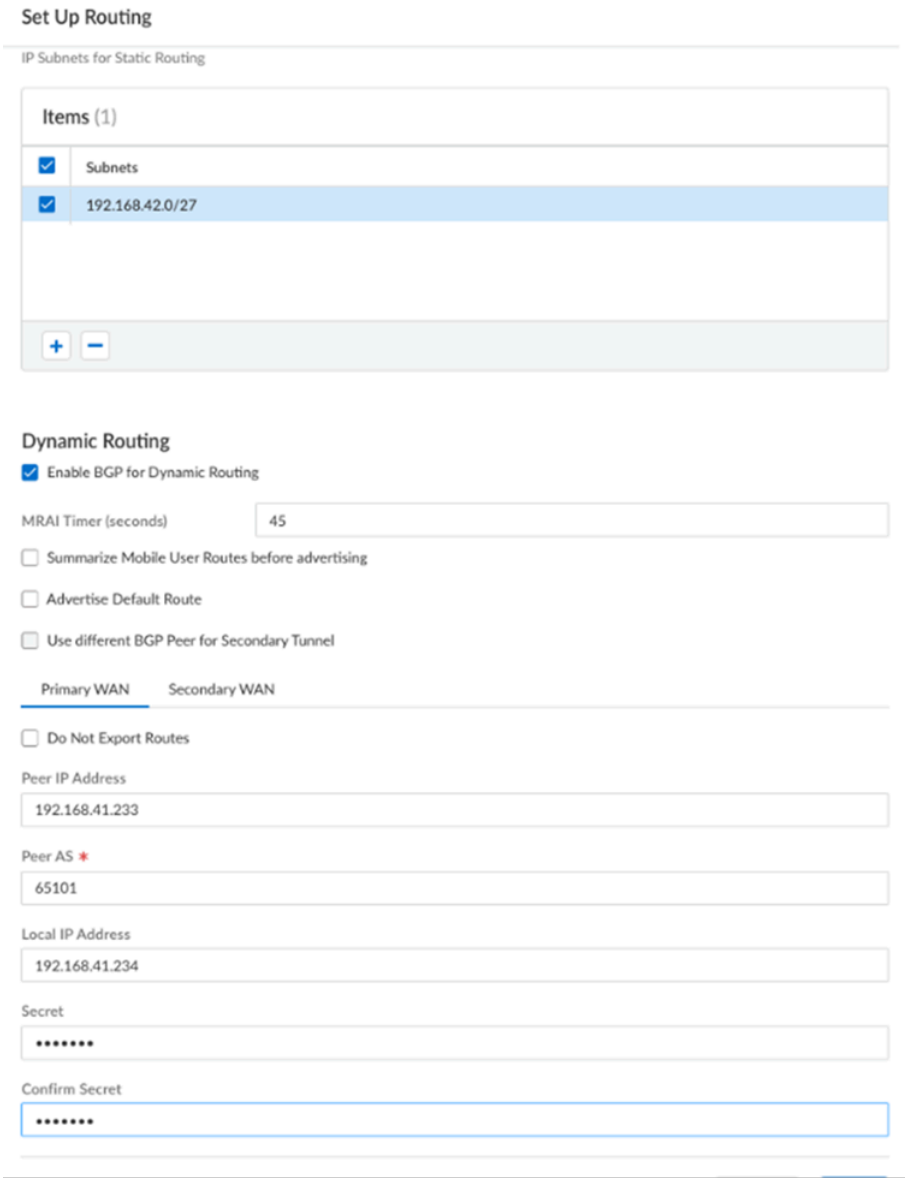
   Parce que Prisma Access n'envoie pas d'annonces BGP, si vous sélectionnez cette option, vous devez configurer des itinéraires statiques sur votre équipement sur site pour établir des itinéraires de retour vers Prisma Access.
7. Saisissez la **Peer IP Address (Adresse IP de l'homologue)** attribuée comme ID de routeur du routeur eBGP sur le réseau du siège social ou du centre de données.
8. Saisissez le **Peer AS (AS homologue)**, qui est le système autonome (AS) de votre réseau.

   Utilisez un numéro AS privé BGP conforme à la RFC 6996.
9. Saisissez la **Local IP Address (Adresse IP locale)** qui est utilisée par Prisma Access comme adresse IP locale pour BGP.

   Une adresse locale n'est requise que si votre périphérique de siège social ou de centre de données en a besoin pour que l'appairage BGP réussisse. Assurez-vous que l'adresse que vous spécifiez ne soit pas en conflit ou ne chevauche pas les adresses IP dans le sous-réseau d'infrastructure ou les sous-réseaux du réseau distant.
10. Saisissez un mot de passe **Secret (Phrase secrète)** pour authentifier les communications de l'homologue BGP.

 ©2025 Palo Alto Networks, Inc.

11. Sélectionnez **Confirm Secret (Confirmer la phrase secrète)**.



À partir de Prisma Access 5.2, vous pouvez intégrer un maximum de 25 000 réseaux distants et 50 000 passerelles IKE par locataire dans un déploiement Prisma Access. Pour prendre en compte cette amélioration, les modifications suivantes ont été apportées à l'interface web de Strata Cloud Manager :

- La pagination est ajoutée et vous pouvez choisir le nombre de lignes à afficher dans une page donnée.

- Le filtrage est activé pour les réseaux distants.

  Après avoir appliqué le filtrage, vous pouvez trier les résultats obtenus par nom.

 ©2025 Palo Alto Networks, Inc.

- Un nouveau champ **Group By (Grouper par)** est ajouté. Si vous sélectionnez un groupe par **Compute Location (Emplacement de calcul)**, tous les groupes s'affichent mais sont réduits et la taille de page que vous avez sélectionnée s'applique aux groupes. Si vous sélectionnez un emplacement de calcul pour le développer, les lignes s'affichent en fonction de la taille de page que vous avez sélectionnée.

- Lorsque les réseaux distants sont affichés dans une liste déroulante, l'interface web affiche les 500 premiers éléments. Vous pouvez rechercher le réseau distant souhaité dans la liste en tapant dans la zone de texte.

  En outre, le nombre total de réseaux distants s'affiche.

- Les pages supplémentaires suivantes ont une pagination appliquée :
  - Tunnels IPSec :
  - QoS :
  - Statistiques QoS :
  - **Troubleshooting—Remote Networks (Dépannage—Réseaux distants)** sous **External Dynamic Lists (Listes dynamiques externes)** :

Intégrer un réseau distant (Panorama)

Pour configurer un déploiement de réseau distant Prisma Access qui alloue de la bande passante par emplacement de calcul, suivez les étapes suivantes.

Si vous devez intégrer de nombreux réseaux distants (jusqu'à 1 000), vous pouvez intégrer un réseau distant en utilisant la procédure suivante, puis exporter la configuration du réseau distant dans un fichier CSV, ajouter les autres réseaux distants que vous souhaitez intégrer au fichier CSV et importer le fichier CSV pour enregistrer la configuration dans Prisma Access.

STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** et modifiez les paramètres en cliquant sur l'icône d'engrenage dans la zone **Settings (Paramètres)**.

1. Dans la section Modèles, **Add (Ajoutez)** tous les modèles contenant la configuration que vous souhaitez transmettre à Prisma Access pour les réseaux. Par exemple, si vous disposez de modèles existants contenant vos configurations de zone, votre tunnel IPSec, votre passerelle IKE ou vos paramètres de profil crypto, vous pouvez les ajouter à la pile de modèles Remote_Network_Template_Stack prédéfinie pour simplifier le processus d'intégration.

   Vous pouvez cliquer sur **Add (Ajouter)** pour ajouter plusieurs modèles à la pile, puis les classer par ordre approprié à l'aide des fonctions **Move Up (Déplacer vers le haut)** et **Move Down (Déplacer vers le bas)**. Ceci est important, car Panorama évalue la pile de

 ©2025 Palo Alto Networks, Inc.

haut en bas, en donnant la priorité aux paramètres des modèles plus haut dans la pile sur les mêmes paramètres spécifiés dans les modèles plus bas dans la pile. Notez que vous ne pouvez pas déplacer le modèle par défaut du haut de la pile.

Bien que vous puissiez utiliser le plug-in pour ajouter des modèles existants à la pile, il ne peut pas vous servir pour créer un nouveau modèle. Utilisez plutôt le flux de travail pour ajouter un nouveau modèle.

2. Sélectionnez le **Parent Device Group (Groupe de périphériques parent)** de Prisma Access pour les réseaux distants. Vous pouvez sélectionner un groupe de périphériques existant ou utiliser l'option **Shared (Partagé)**.

   Vous allez transférer toute la configuration, y compris la politique de sécurité, les profils de sécurité et d'autres objets de politique (tels que les groupes et objets d'applications et les groupes d'adresses), les objets et profils HIP et la politique d'authentification, qui est nécessaire pour Prisma Access pour les réseaux pour appliquer une politique cohérente à vos utilisateurs de réseau distants à l'aide de la hiérarchie de groupe de périphériques que vous spécifiez ici.

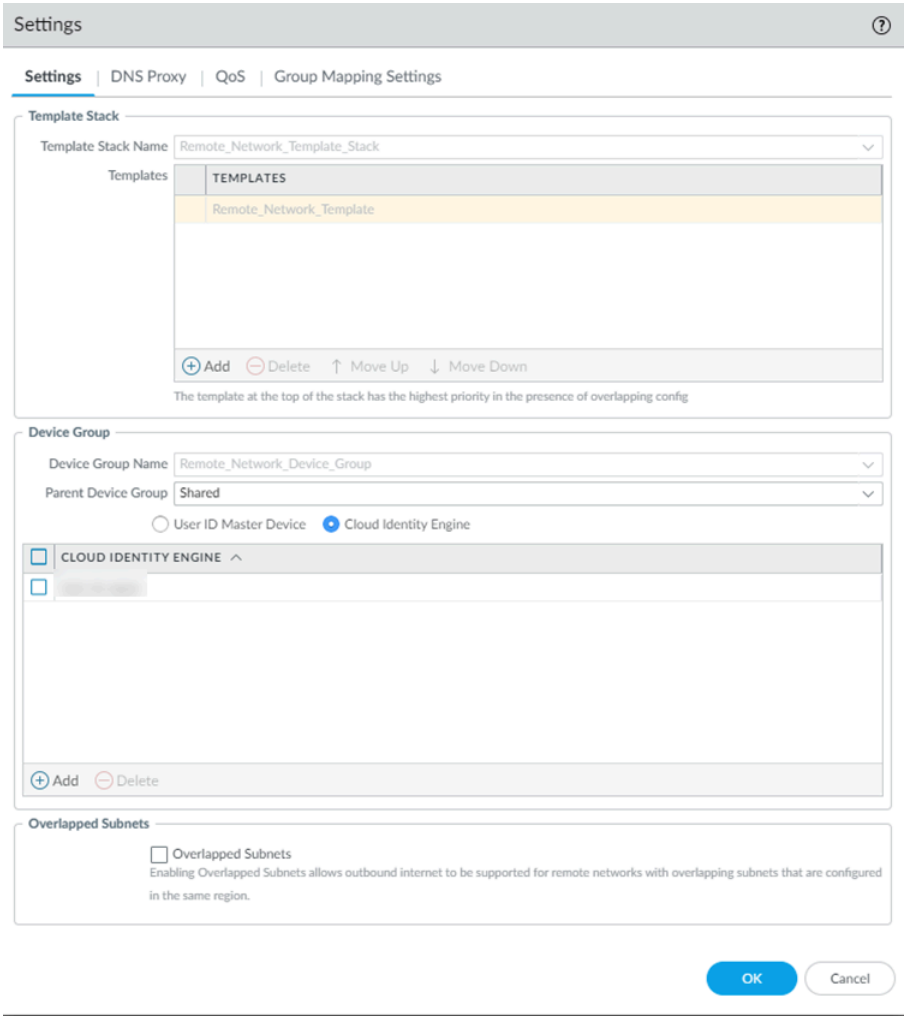
   Vous n'avez pas encore besoin de définir toutes les politiques que vous allez transférer au réseau distant. Configurez plutôt les paramètres d'intégration du site distant. Vous pouvez ensuite revenir en arrière et ajouter les modèles et les groupes de périphériques avec les configurations complètes pour transférer une politique cohérente à vos réseaux distants.

3. (Facultatif) Si vous avez configuré un pare-feu nouvelle génération en tant que périphérique principal ou ajouté un profil Cloud Identity Engine pour rendre les informations de l'utilisateur et du groupe sélectionnables dans les politiques de sécurité, sélectionnez **User-ID Master Device (Périphérique principal de User-ID)** ou **Cloud Identity Engine**; puis sélectionnez le profil du périphérique principal ou du Cloud Identity Engine que vous avez créé.

 ©2025 Palo Alto Networks, Inc.

4. Si vous devez configurer des réseaux distants comportant des sous-réseaux qui se chevauchent, cochez la case **Overlapped Subnets (Sous-réseaux qui se chevauchent)** pour activer l'accès Internet sortant pour ces emplacements.

   Bien que la configuration d'emplacements de réseau distants avec des sous-réseaux qui se chevauchent introduise certaines limitations, elle est acceptable dans certains cas (par exemple, si vous souhaitez ajouter un réseau pour les invités dans un magasin de détail).



STEP 2 | (Facultatif) Configurez les paramètres du **DNS Proxy (Proxy DNS)** pour votre réseau distant.

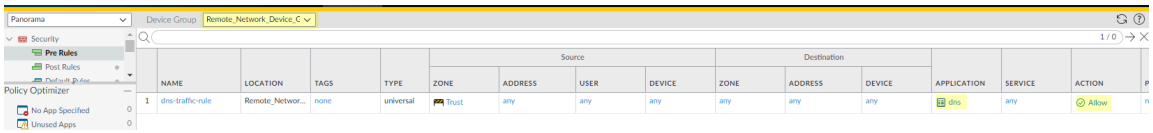
Prisma Access vous permet de spécifier des serveurs DNS pour résoudre à la fois les domaines internes à votre organisation et les domaines externes. Si vous ne spécifiez aucun paramètre, Prisma Access ne se procure pas les requêtes DNS pour les réseaux distants.

1. Dans le groupe de périphériques **Remote_Network_Device_Group**, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et cliquez sur **Add (Ajouter)** pour ajouter une règle de

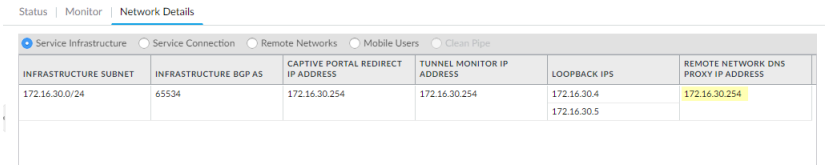
 ©2025 Palo Alto Networks, Inc.

politique de sécurité avec une **Application DNS** et une **Action Allow (Autoriser)** pour autoriser le trafic DNS.

Sans règle de politique de sécurité autorisant le trafic DNS, la résolution DNS ne se produit pas.



2. Si vous configurez Prisma Access pour servir de proxy pour les requêtes DNS de vos réseaux distants, mettez à jour les paramètres DNS sur tous les terminaux de ce réseau pour utiliser **Remote Network DNS Proxy IP Address (Adresse IP du proxy DNS du réseau distant)** de Prisma Access comme serveur DNS principal et utiliser votre serveur DNS comme serveur DNS secondaire. Vous pouvez obtenir cette adresse IP du proxy DNS dans **Panorama** > **Cloud Services** > **Statut (État)** > **Network Details (Détails du réseau)** > **Service Infrastructure (Infrastructure de service)**.



3. Cliquez sur **Add (Ajouter)** pour ajouter un ou plusieurs paramètres de **DNS Proxy (Proxy DNS)** en saisissant les valeurs suivantes :

   - Sélectionnez une **Region (Région)** dans la liste déroulante en haut de la fenêtre.

     Sélectionnez **Worldwide (Monde entier)** pour appliquer les paramètres DNS à l'échelle mondiale, sélectionnez un théâtre spécifique ou sélectionnez les paramètres par groupe d'emplacements (un groupe d'emplacements plus petit que le théâtre). Si vous ajoutez plusieurs paramètres, les paramètres du groupe d'emplacements sont utilisés en premier, puis les paramètres du théâtre, puis les paramètres du monde entier. Prisma Access évalue les règles de haut en bas dans la liste.
   - Cliquez sur **Add (Ajouter)** pour ajouter une ou plusieurs règles pour configurer les paramètres DNS des **Internal Domains (Domaines internes)**.
     - Saisissez un **Rule Name (Nom de règle)** unique pour la règle.
     - Si vous souhaitez que votre serveur DNS interne résolve uniquement les domaines que vous spécifiez, saisissez les domaines à résoudre dans la **Domain List (Liste de domaines)**. Spécifiez un astérisque devant le domaine ; par exemple, *.acme.com. Vous pouvez spécifier un maximum de 1 024 entrées de domaine.
     - Si vous disposez d'un **Custom DNS server (Serveur DNS personnalisé)** capable d'accéder à vos domaines internes, spécifiez les adresses IP du serveur **Primary DNS (DNS principal)** et du serveur **Secondary DNS (DNS secondaire)**, ou sélectionnez **Use Cloud Default (Utiliser la valeur par défaut du cloud)** pour utiliser la valeur par défaut du serveur DNS de Prisma Access.

 ©2025 Palo Alto Networks, Inc.

- Spécifiez les paramètres DNS pour les **Public Domains (Domaines publics)**.
  - **Use Cloud Default (Utiliser la valeur par défaut du cloud)** : utilisez la valeur par défaut du serveur DNS de Prisma Access.
  - **Same as Internal Domains (Même valeur que les domaines internes)** : utilisez le même serveur que vous utilisez pour résoudre les domaines internes. Lorsque vous sélectionnez cette option, le serveur DNS utilisé pour résoudre les domaines publics est le même que le serveur configuré pour la première règle dans la section **Internal Domains (Domaines internes)**.
  - **Custom DNS Server (Serveur DNS personnalisé)** : si vous disposez d'un serveur DNS capable d'accéder à vos domaines publics (externes), saisissez l'adresse du serveur DNS principal dans ce champ.

  (Facultatif) Vous pouvez **Add (Ajouter)** une **DNS Suffix List (Liste de suffixes DNS)** pour spécifier le suffixe que le client doit utiliser localement lorsqu'un nom d'hôte non qualifié est saisi et qu'il ne peut pas résoudre, par exemple, acme.local. Ne saisissez pas de caractère générique (*) avant le suffixe de domaine (par exemple, acme.com). Vous pouvez ajouter plusieurs suffixes.
- Si vous souhaitez que Prisma Access serve de proxy pour les requêtes DNS, configurez l'option Configurer les valeurs pour les utiliser dans les requêtes UDP (**Interval (Intervalle)** pour réessayer la requête en secondes et le nombre de **Attempts (Tentatives)** de requête à effectuer).

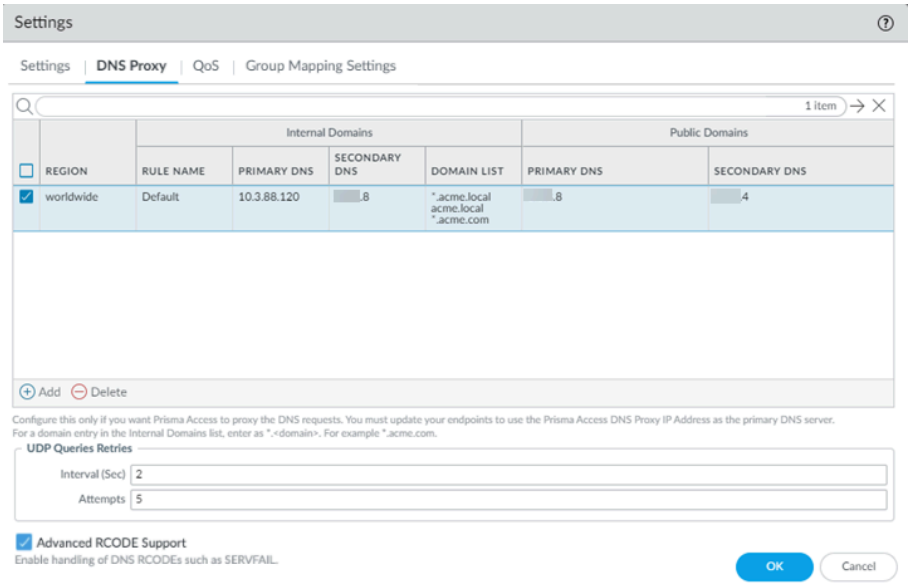
  Si vous souhaitez que Prisma Access serve de proxy pour les requêtes DNS de vos utilisateurs GlobalProtect, vous devez mettre à jour vos terminaux pour utiliser **Remote Network DNS Proxy IP Address (Adresse IP du proxy DNS du réseau distant)** comme serveur DNS principal (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Infrastructure (Infrastructure de service)**).

4. (Facultatif) Sélectionnez Support RCODE avancé pour autoriser le serveur DNS principal à basculer vers le serveur DNS secondaire en cas de réception d'un code de retour DNS RCODE 2 (SERVFAIL) et RCODE 5 (REFUSED).

   Un code de réponse DNS SERVFAIL fait référence à une erreur de communication avec le serveur DNS principal, et un code de réponse DNS REFUSED signifie que le serveur

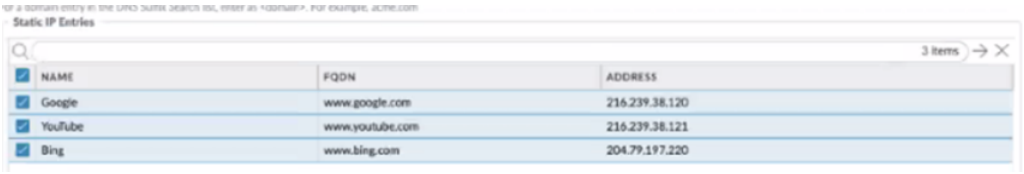
 ©2025 Palo Alto Networks, Inc.

DNS principal a refusé de fournir les informations demandées. Dans les deux cas, le service bascule vers le serveur DNS secondaire.



5. (Facultatif) Utilisez **Static IP Entries (Entrées IP statiques)** pour résoudre les FQDN en adresses IP spécifiques.

   Cette fonctionnalité peut être utile si vous disposez de services Internet pour invités dans votre organisation et que vous souhaitez que vos invités utilisent les moteurs de recherche en toute sécurité, les empêchant de rechercher du contenu potentiellement inapproprié ou offensant qui pourrait être contraire à la politique de l'entreprise. Pour ce faire, saisissez un **Name (Nom)** unique pour la règle d'entrée statique, un **FQDN** et l'**Address (Adresse)** IP vers laquelle la demande FQDN doit être dirigée.



STEP 3 | (Facultatif) Activez la **QoS** pour votre déploiement de réseau distant et spécifiez un **QoS Profile (Profil QoS)**, un **Guaranteed Bandwidth Ratio (Ratio de bande passante garantie)**, la quantité de bande passante **Reserved for Guaranteed Bandwidth (Mbps) (Réservée à la bande passante garantie (Mbit/s))** et, éventuellement, personnalisez les options du site par emplacement (**Personnaliser par site**).

Vous activez la QoS au niveau de l'emplacement de calcul ; toutefois, vous pouvez spécifier d'activer ou de désactiver la QoS selon le site et spécifier un profil QoS selon le site lorsque vous ajoutez votre réseau distant à une étape ultérieure. Avant de configurer la QoS, vous devez comprendre comment elle fonctionne pour les réseaux distants qui allouent la bande passante par emplacement de calcul, notamment en spécifiant la bande passante garantie et en personnalisant la bande passante par site.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | (Facultatif) Configurez **Group Mapping Settings (Paramètres de mappage de groupe)** pour que Prisma Access utilise le composant Synchronisation d'annuaire du Cloud Identity Engine pour récupérer les informations sur les utilisateurs et les groupes.

Vous devez configurer Cloud Identity Engine pour récupérer les informations sur les utilisateurs et les groupes à partir de votre Active Directory (AD) avant d'activer le mappage de groupe dans Prisma Access à l'aide des **Group Mapping Settings (Paramètres de mappage de groupe)**.

STEP 5 | Créez de nouvelles zones dans l'un des modèles de la pile (**Network (Réseau) > Zones> Add (Ajouter)**) ou mappez les zones référencées dans les modèles existants que vous avez ajoutés à la pile comme étant approuvées ou non approuvées. Sur Panorama, les règles de politique sont définies dans des groupes de périphériques et les zones sont définies dans des modèles. Par conséquent, vous devez vous assurer d'ajouter les modèles qui font référence aux zones incluses dans vos règles de politique à la pile de modèles.

Sur un pare-feu nouvelle génération Palo Alto Networks®, la politique de sécurité est appliquée entre les zones, qui correspondent aux interfaces physiques ou virtuelles sur le pare-feu. Mais comme Prisma Access pour les réseaux ne dispose que de deux zones, approuvée et non approuvée, vous devez mapper les zones avec du trafic lié à Internet (y compris vos applications SaaS approuvées) comme non approuvées et toutes les zones internes comme approuvées.

1. (Facultatif) Modifiez les paramètres de mappage de zone .

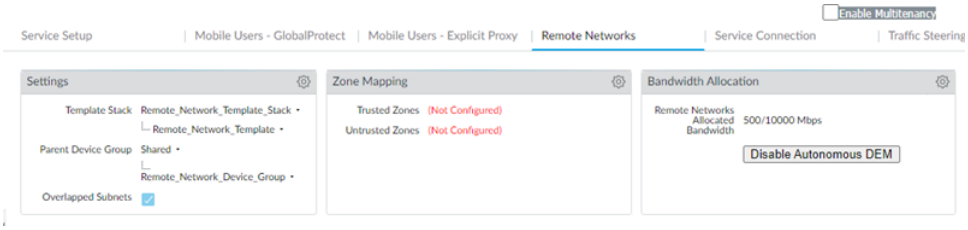
   Par défaut, toutes les zones de la pile de modèles de Prisma Access pour les réseau sont classées comme des zones non approuvées. Si vous n'avez pas encore défini de zones ou si les modèles dans Remote_Network_Template_Stack n'ont pas de configurations de zone, vous pouvez revenir et les ajouter lorsque vous transmettez la politique à Prisma Access pour les réseaux.
2. Pour chaque zone que vous souhaitez désigner comme approuvée, sélectionnez-la et cliquez sur **Add (Ajouter)** pour la déplacer vers la liste des **Trusted Zones (Zones approuvées)**.
3. Cliquez sur **OK** pour enregistrer les mappages.

 ©2025 Palo Alto Networks, Inc.

STEP 6 | Allouez de la bande passante aux emplacements que vous souhaitez intégrer en cliquant sur l'icône d'engrenage dans la zone **Bandwidth Allocation (Allocation de bande passante)**.

Vous allouez de la bande passante à un niveau agrégé par emplacement de calcul. Pour plus d'informations, reportez-vous à la sectionPrisma Access Réseaux distants.

*Si vous avez supprimé le Autonomous DEM en tant que licence complémentaire, ou si vous supprimez Autonomous DEM pour les réseaux distants de votre licence, sélectionnez **Disable Autonomous DEM (Désactiver Autonomous DEM)**. Si vous supprimez Autonomous DEM pour les réseaux distants et que vous ne le désactivez pas, vous recevrez un message d'erreur lors de la validation.*



Si vous avez un déploiement de réseaux distants existant qui intègre actuellement des réseaux distants par emplacement, une fenêtre contextuelle s'affiche et vous demande si vous souhaitez migrer vers le modèle de bande passante agrégée. Cliquez sur **Migrate (Migrer)** pour continuer ou sur **Cancel (Annuler)** pour annuler la migration.

*La migration vers le modèle de bande passante agrégée est permanente et non réversible. Avant de procéder à la migration, passez en revue la liste de contrôle de pré-migration. Vous devez cliquer sur **Commit and Push (Valider et appliquer)** pour que vos modifications prennent effet.*

Les **Service IP Address (Adresse IP du service)** (le les adresses IP publiques utilisés du côté Prisma Access du tunnel IPSec pour la connexion au réseau distant) ne changent pas lorsque vous migrez votre déploiement vers le modèle de bande passante agrégée et aucune reconfiguration de votre tunnel IPSec n'est requise.

STEP 7 | Entrez la **Bandwidth Allocation (Allocation de bande passante)** que vous souhaitez pour chaque **Compute Location (Emplacement de calcul)** associé aux **Prisma Access Locations (Emplacements Prisma Access)** que vous souhaitez intégrer.

Pour vérifier la quantité de bande passante que vous avez saisie, sélectionnez la coche à côté de la quantité de bande passante. Pour annuler la quantité, sélectionnez **x**.

Spécifiez une bande passante minimale de 50 Mbit/s. La bande passante maximale correspond à la bande passante licenciée restante maximale.

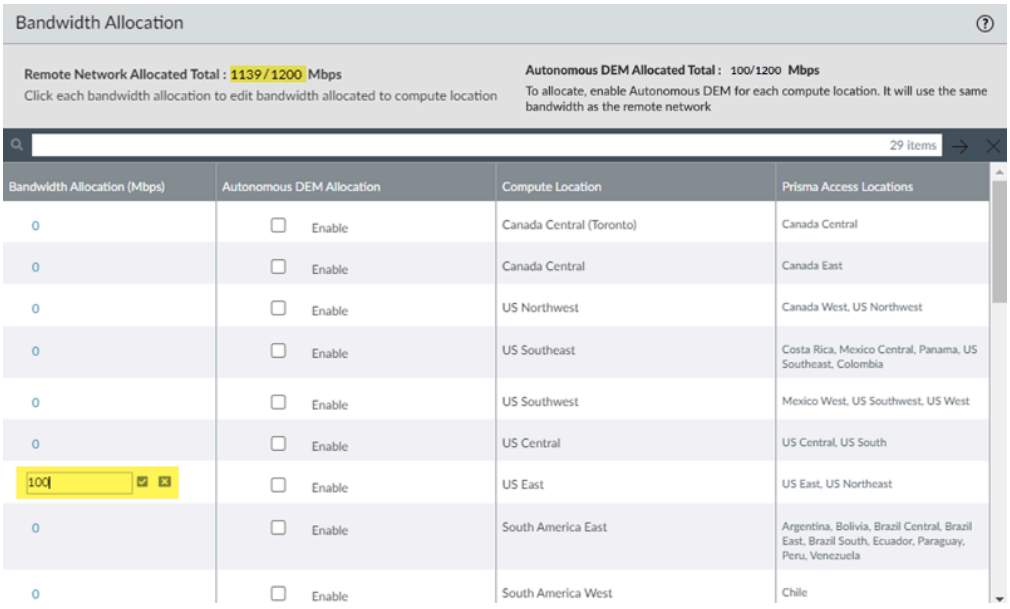
STEP 8 | (Facultatif, déploiements avec Autonomous DEM uniquement pour les licences de réseaux distants) Cliquez sur **Enable (Activer)** l'**Autonomous DEM Allocation (Allocation de l'Autonomous DEM)** pour l'emplacement de calcul auquel vous avez alloué de la bande passante.

Si vous activez Autonomous DEM pour l'emplacement de calcul, la quantité de bande passante utilisée par la licence Autonomous DEM est la même que la quantité de bande passante que vous spécifiez pour l'emplacement de calcul. L'**Autonomous DEM Allocated Total (Total alloué**

 ©2025 Palo Alto Networks, Inc.

à Autonomous DEM) vous montre combien de bande passante est utilisée par Autonomous DEM ainsi que la quantité restante. Pour plus d'information, consultez l'Autonomous DEM guide (guide de l'Autonomous DEM).

STEP 9 | Attendez que la bande passante soit reflétée dans le champ **Allocated Total (Total alloué)** en haut de la page, puis cliquez sur **OK**.



STEP 10 | (Facultatif) Si vous souhaitez configurer votre réseau distant pour fournir un accès entrant sécurisé aux emplacements de réseau distant, cliquez sur l'onglet **Inbound Access Remote Networks (Réseaux distants à accès entrant)** et suivez le flux de travail pour configurer un accès entrant sécurisé pour un réseau distant.

STEP 11 | Cliquez sur l'option **Add (Ajouter)** pour ajouter un réseau distant et spécifiez un **Name (Nom)**.

Vous ne pouvez pas changer le nom de l'emplacement réseau distant après l'avoir saisi. Assurez-vous de connaître votre schéma d'affectation de nom pour vos réseaux distants avant de commencer l'intégration.

STEP 12 | (Facultatif, uniquement pour les déploiements BGP) Créez une configuration afin que votre connexion au réseau distant puisse utiliser jusqu'à quatre tunnels IPSec pour son trafic (**ECMP Load Balancing (Équilibrage de charge ECMP**).

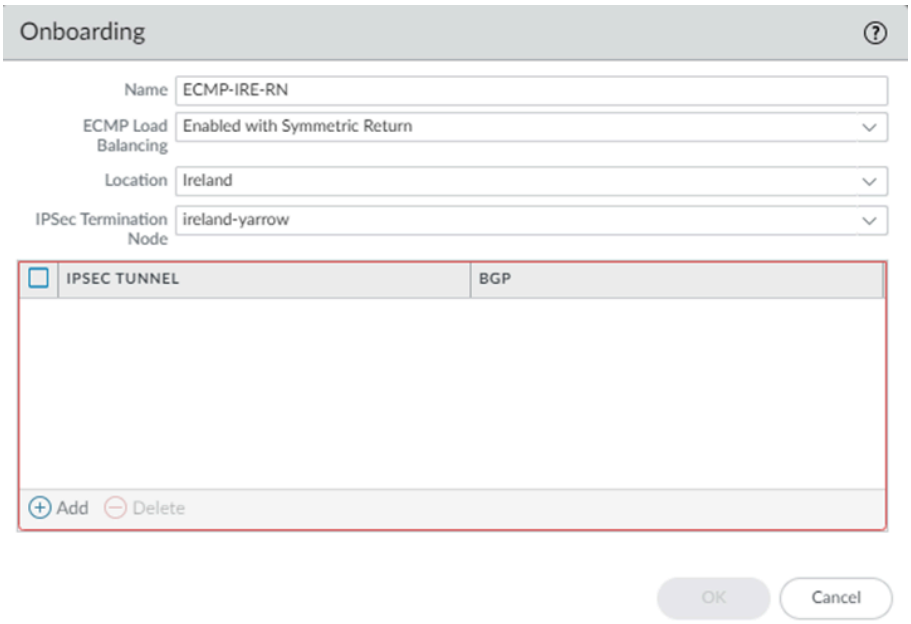
Les itinéraires statiques ne sont pas pris en charge (BGP requis), et, si vous avez configuré la QoS, vous ne pouvez pas changer le rapport d'allocation pour les liens ECMP. Si votre déploiement utilise un tunnel IPSec pour sa connexion au réseau distant ou utilise des itinéraires statiques, sélectionnez **None (Aucun)** pour **ECMP Load Balancing (Équilibrage de charge ECMP)** et passez à l'étape 15.

1. Sélectionnez l'une des options pour activer ou désactiver l'équilibrage de charge ECMP.
   - **None (Aucun)** : avec cette option, l'équilibrage de charge ECMP n'est pas utilisé (utilisez un seul tunnel de réseau distant pour cette connexion au réseau distant). C'est le seul choix que vous pouvez faire pour les itinéraires statiques ; BGP est requis pour l'équilibrage de charge ECMP.

 ©2025 Palo Alto Networks, Inc.

- **Enabled with Symmetric Return (Activé avec retour symétrique)** : spécifiez jusqu'à quatre tunnels IPSec pour cette connexion au réseau distant et forcez Prisma Access à utiliser le même lien pour le trafic de retour que celui utilisé pour envoyer le trafic.

  Sélectionnez cette option si vous avez un ou plusieurs tunnels de secours à utiliser uniquement si l'un des tunnels principaux n'est plus opérationnel. Si un lien échoue, Prisma Access utilise l'un des autres tunnels pour envoyer et recevoir le trafic de manière symétrique.



2. Vous devez cliquer sur **Add (Ajouter)** pour ajouter un tunnel IPSec pour la connexion au réseau distant et spécifier les valeurs suivantes :

   - **Enable (Activer)** : active BGP pour le tunnel IPSec.

     Cette sélection n'est pas configurable ; vous devez activer BGP pour configurer ECMP.

   - **Summarize Mobile User Routes before advertising (Résumer les itinéraires des utilisateurs mobiles avant de annoncer)** : réduit le nombre d'annonces de sous-réseaux IP d'utilisateurs mobiles sur le BGP vers votre équipement de locaux clients (CPE) en les résumant.

     Par défaut, Prisma Access annonce les pools d'adresses IP des utilisateurs mobiles par blocs de sous-réseaux /24. Si vous les résumez, Prisma Access annonce le pool en fonction du sous-réseau que vous avez spécifié. Par exemple, Prisma Access annonce un pool d'adresses IP mobiles d'utilisateurs publics de 10.8.0.0/20 en utilisant le sous-réseau /20, plutôt que de diviser le pool en sous-réseaux de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, et ainsi de suite, avant de les annoncer. Le résumé de ces annonces peut réduire le nombre d'itinéraires stockés dans les tableaux de routage CPE. Par exemple, vous pouvez utiliser le résumé de pool d'adresses IP avec des passerelles

 ©2025 Palo Alto Networks, Inc.

VPN cloud (passerelles privées virtuelles [VGW] ou passerelles de transit [TGW]) qui peuvent accepter un nombre limité d'itinéraires.

Si vous activez la synthèse des itinéraires pour un emplacement qui utilise ECMP, vous devez activer la synthèse des itinéraires sur tous les liens vers cet emplacement, sinon vous recevrez un message d'erreur lors de la validation.

Prisma Access définit la chaîne de communauté pour les itinéraires d'utilisateurs mobiles agrégés à `0xFFFE:0xFFF0`.

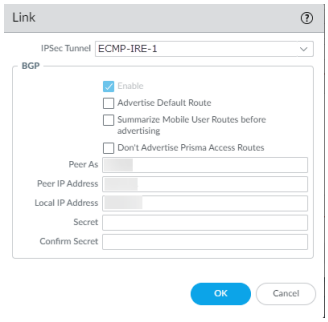
- **Advertise Default Route (Annoncer l'itinéraire par défaut)** : Prisma Access génère une annonce d'itinéraire par défaut pour le réseau distant en utilisant eBGP.

  Assurez-vous que votre réseau n'a pas d'autre itinéraire par défaut annoncé par BGP, sinon vous pourriez introduire des problèmes de routage dans votre réseau.

- **Don't Advertise Prisma Access Routes (Ne pas annoncer les itinéraires Prisma Access)** : empêche l'homologue BGP Prisma Access de transférer des itinéraires dans le réseau de votre organisation.

  Par défaut, Prisma Access annonce toutes les informations de routage BGP, y compris les itinéraires locaux et tous les préfixes qu'il reçoit d'autres connexions aux services, réseaux distants et sous-réseaux d'utilisateurs mobiles. Cochez cette case pour empêcher Prisma Access d'envoyer des annonces BGP, mais pour qu'il utilise toujours les informations BGP qu'il reçoit pour apprendre les itinéraires d'autres voisins BGP.

  Puisque Prisma Access n'envoie pas d'annonces BGP si vous sélectionnez cette option, vous devez configurer des itinéraires statiques sur l'équipement local pour établir des itinéraires de retour vers Prisma Access.



- (Facultatif) Sélectionnez une valeur de minuterie **MRAI**.

  Le routage BGP propose un minuteur que vous pouvez utiliser pour adapter la convergence du routage BGP dans votre réseau, appelé *Intervalle minimum d'annonce d'itinéraire (MRAI)*. MRAI agit pour limiter le débit des mises à jour par destination et les routeurs BGP attendent au moins le délai MRAI configuré avant d'envoyer une annonce pour le même préfixe. Un nombre plus petit vous donne un temps de convergence plus rapide mais crée plus d'annonces sur votre réseau. Un nombre plus élevé diminue le nombre d'annonces pouvant être envoyées, tout en ralentissant également la convergence de routage. Vous décidez du nombre à mettre dans votre

 ©2025 Palo Alto Networks, Inc.

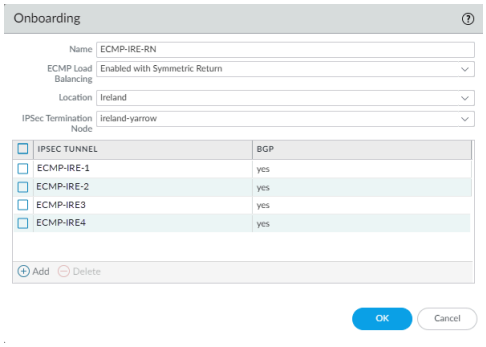
réseau pour obtenir le meilleur équilibre entre une convergence de routage plus rapide et moins d'annonces.

Configurez une plage MRAI comprise entre 1 et 600 secondes, avec une valeur par défaut de 30 secondes.

- **Peer AS (AS homologue)** : spécifiez le système autonome (AS) auquel le pare-feu, le routeur virtuel ou le routeur BGP de votre réseau distant appartient.
- **Peer IP Address (Adresse IP de l'homologue)** : entrez l'adresse IP assignée comme identifiant de routeur du routeur eBGP sur le réseau distant pour lequel vous configurez cette connexion.
- **Local IP Address (Adresse IP locale)** (Facultatif) : saisissez une adresse utilisée par Prisma Access comme adresse IP locale pour BGP. Spécifiez l'adresse IP à utiliser du côté Prisma Access du tunnel.

  La spécification d'une **Local Address (Adresse locale)** est utile lorsque le périphérique de l'autre côté de la connexion (tel qu'une passerelle virtuelle privée Amazon Web Service (AWS)) nécessite une adresse IP locale spécifique pour que l'appairage BGP réussisse. Assurez-vous que l'adresse que vous spécifiez ne soit pas en conflit ou ne chevauche pas les adresses IP dans le sous-réseau d'infrastructure ou les sous-réseaux du réseau distant.
- **Secret (Phrase secrète)** et **Confirm Secret (Confirmer la phrase secrète)** (facultatif) : entrez et confirmez une phrase secrète pour authentifier les communications entre homologues BGP.

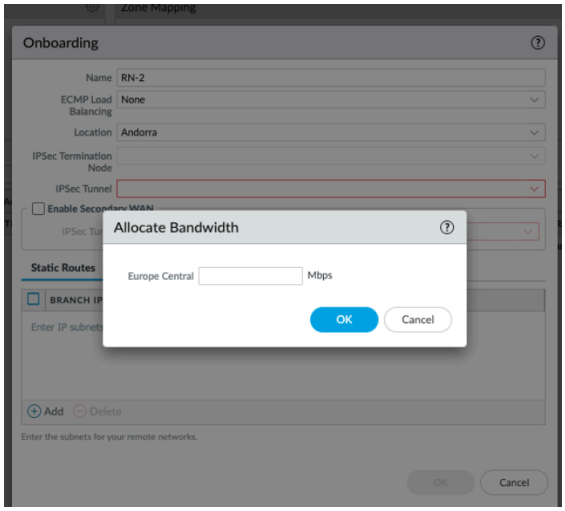
3. Répétez l'étape précédente pour ajouter jusqu'à quatre tunnels à utiliser avec la connexion au réseau distant.



 ©2025 Palo Alto Networks, Inc.

STEP 13 | Sélectionnez le **Location (Emplacement)** dans lequel Prisma Access déploiera l'infrastructure nécessaire pour sécuriser votre emplacement réseau distant. Cette région devrait être géographiquement proche de votre emplacement de réseau distant.

Si vous n'avez pas encore alloué de bande passante pour l'emplacement de calcul auquel l'emplacement est associé, Prisma Access vous invite à entrer la bande passante pour cet emplacement de calcul.



Les emplacements dotés de deux astérisques sont des **Local Zones (Zones locales)**. Ces emplacements placent les services de calcul, de stockage, de base de données et d'infrastructure à proximité de grands centres de population et d'industrie; cependant, ils présentent également certaines limites. Pour ajouter une zone locale, contactez votre représentant Palo Alto Networks.

STEP 14 | Sélectionnez le **IPSec Termination Node (Nœud de fin d'IPSec)** que vous souhaitez utiliser pour ce réseau distant.

Prisma Access utilise ce nœud pour associer des emplacements réseau distants à des emplacements de calcul.

STEP 15 | (Routage statique ou déploiements à tunnel unique uniquement) Sélectionnez ou ajoutez une nouvelle configuration de **tunnel IPSec** pour accéder au pare-feu, au routeur ou au périphérique SD-WAN sur le site de l'entreprise :

- Sélectionnez l'un des modèles IPSec prédéfinis dans le modèle Remote_Network_Template ou, si vous avez ajouté un modèle à la pile Remote_Network_Template_Stack (ou modifié le modèle Remote_Network_Template prédéfini) qui inclut une configuration de tunnel IPSec, sélectionnez cet **IPSec Tunnel (Tunnel IPSec)** dans la liste déroulante. Notez que le tunnel que vous créez pour chaque connexion réseau distante connecte Prisma Access au périphérique compatible IPSec à chaque succursale.

  Utilisez les instructions suivantes lors de la configuration d'un tunnel IPSec :

  - Les adresses homologues dans la configuration IKE Gateway doivent être uniques pour chaque tunnel. Vous pouvez toutefois réutiliser certains des autres éléments de configuration courants, tels que les profils crypto.
  - Le tunnel IPSec que vous sélectionnez depuis un modèle doit utiliser l'échange automatique de clés et IPv4 uniquement.

 ©2025 Palo Alto Networks, Inc.

    - Les noms de tunnel IPSec, de passerelle IKE et de profil crypto ne peuvent pas dépasser 31 caractères.
    - Si vous intégrez plusieurs réseaux distants au même emplacement avec des homologues IKE dynamiques, vous devez utiliser le même profil crypto IKE pour toutes les configurations de réseau distant.
- Pour créer une nouvelle configuration de tunnel IPSec, cliquez sur **New IPSec Tunnel (Nouveau tunnel IPSec)**, attribuez-lui un **Name (Nom)**, et configurez les paramètres IKE Gateway (Passerelle IKE), IPSec Crypto Profile (Profil crypto IPSec) et Tunnel Monitoring (Surveillance du tunnel).
    - Si le périphérique compatible IPSec de votre succursale utilise un VPN basé sur des politiques, sous l'onglet **Proxy IDs (ID proxy)**, vous devez cliquer sur **Add (Ajouter)** pour ajouter un ID proxy correspondant aux paramètres configurés sur votre périphérique IPSec local pour vous assurer que Prisma Access peut établir un tunnel IPSec avec votre périphérique local.
- Laissez l'option **Enable Replay Protection (Activer la protection contre la relecture** sélectionnée pour détecter et neutraliser les attaques par relecture.
- Sélectionnez **Copy TOS Header (Copier l'en-tête TOS)** pour copier le champ Type of Service (type de service - ToS) à partir de l'en-tête IP interne vers l'en-tête IP externe des paquets encapsulés afin de conserver les informations ToS d'origine.
- Pour activer la surveillance de tunnel pour la connexion de service, sélectionnez **Tunnel Monitor (Surveiller le tunnel**.
    - Saisissez l'adresse **IP de Destination**.

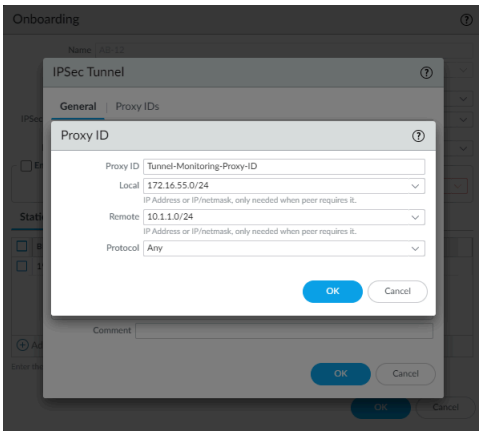
      Spécifiez une adresse IP à votre succursale à laquelle Prisma Access peut envoyer des requêtes ping ICMP pour la surveillance du tunnel IPSec. Assurez-vous que cette adresse

 ©2025 Palo Alto Networks, Inc.

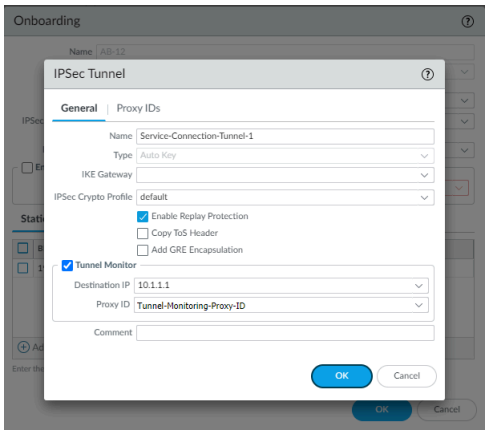
est accessible par ICMP depuis l'ensemble du sous-réseau de l'infrastructure Prisma Access.

- Si vous utilisez la surveillance de tunnel avec un périphérique homologue qui utilise plusieurs ID de proxy, spécifiez un **ID de proxy** ou ajoutez un **nouvel ID de proxy** qui autorise l'accès à partir du sous-réseau d'infrastructure à votre succursale.

  La figure suivante montre un ID proxy avec le sous-réseau d'infrastructure de service (172.16.55.0/24 dans cet exemple) comme sous-réseau IP **local** et le sous-réseau de l'emplacement de succursale (10.1.1.0/24 dans cet exemple) comme sous-réseau **distant**.



  La figure suivante montre l'ID proxy que vous avez créé appliqué à la configuration du moniteur de tunnel en le spécifiant dans le champ **Proxy ID (ID proxy)**.



Vous devez configurer un itinéraire statique sur votre CPE vers l'adresse IP du moniteur de tunnel pour que la surveillance du tunnel fonctionne. Pour trouver l'adresse IP de destination à utiliser pour la surveillance des tunnels entre votre succursale et Prisma Access, sélectionnez ***Panorama*** *>* ***Cloud Services*** *>* ***Status (État)*** *>* ***Network Details (Détails du réseau)****, cliquez sur le bouton radio* ***Service Infrastructure (Infrastructure de service)*** *et recherchez la* ***Tunnel Monitor IP Address (Adresse IP de surveillance du tunnel)****.*

 ©2025 Palo Alto Networks, Inc.

STEP 16 | Si vous avez une liaison WAN secondaire à cet emplacement, sélectionnez **Enable Secondary WAN (Activer le WAN secondaire)**.

Veillez à créer un tunnel IPSec unique pour le WAN secondaire de chaque réseau distant ; Prisma Access ne prend pas en charge la réutilisation du même tunnel IPSec pour les WAN secondaires dans plusieurs réseaux distants.

La configuration d'un WAN secondaire n'est pas prise en charge dans les déploiements suivants :

- Si votre WAN secondaire est configuré en mode actif-actif avec le tunnel IPSec principal.
- Si l'équipement de vos locaux clients (CPE) est configuré dans une configuration ECMP (Equal Cost Multipath) avec le tunnel IPSec principal et secondaire.

Si vous utilisez des itinéraires statiques, le temps de basculement du tunnel est inférieur à 15 secondes à partir du moment de la détection, selon votre fournisseur WAN.

Si vous configurez le routage BGP et que vous avez activé la surveillance des tunnels, le temps d'attente par défaut le plus court pour déterminer qu'un index de paramètres de sécurité (SPI) est défaillant est le moniteur de tunnel, qui supprime toutes les routes vers un homologue lorsqu'il détecte une défaillance de tunnel pendant 15 secondes consécutives. De cette façon, le moniteur de tunnel détermine le comportement des routes BGP. Si vous ne configurez pas la surveillance du tunnel, la minuterie d'attente détermine la durée d'arrêt du tunnel avant de supprimer l'itinéraire. Prisma Access utilise la valeur d'attente BGP par défaut de 90 secondes comme défini par la RFC 4271, qui est le temps d'attente maximum avant que Prisma Access supprime un itinéraire pour un SPI inactif. Si le périphérique BGP homologue a un temps d'attente configuré plus court, le minuteur de maintien BGP utilise la valeur inférieure.

Lorsque le tunnel secondaire est installé avec succès, l'itinéraire secondaire a priorité jusqu'à ce que le tunnel primaire refonctionne. Si l'itinéraire principal et l'itinéraire secondaire sont tous deux opérationnels, l'itinéraire principal est prioritaire.

Si vous utilisez un homologue BGP différent pour la connexion secondaire (de secours), Prisma Access ne respecte pas les attributs du discriminateur multi-sortie (Multi-Exit Discriminator, MED) annoncés par le CPE. Cette mise en garde s'applique si vous utilisez plusieurs homologues BGP sur des connexions réseau distantes ou des connexions de service.

STEP 17 | Activez le routage vers les sous-réseaux ou les adresses IP individuelles sur le site du réseau distant auquel vos utilisateurs auront besoin d'accéder.

Prisma Access utilise ces informations pour acheminer les requêtes vers le site approprié. Les réseaux de chaque site ne peuvent pas se chevaucher les uns avec les autres ni avec les pools d'adresses IP que vous avez désignés pour l'infrastructure de service ou pour le Prisma Access pour les pools d'adresses IP des utilisateurs. Vous pouvez configurer des **Static Routes (Itinéraires statiques)**, **BGP** ou une combinaison des deux.

- Pour configurer des **Static Routes (Itinéraires statiques)** :
  1. Dans l'onglet **Static Routes (Itinéraires statiques)**, cliquez sur **Add (Ajouter)** et saisissez l'adresse de sous-réseau (par exemple, 172.168.10.0/24) ou l'adresse IP individuelle d'une ressource, comme un serveur DNS (par exemple, 10.32.5.1/32) auquel vos utilisateurs distants auront besoin d'accéder.

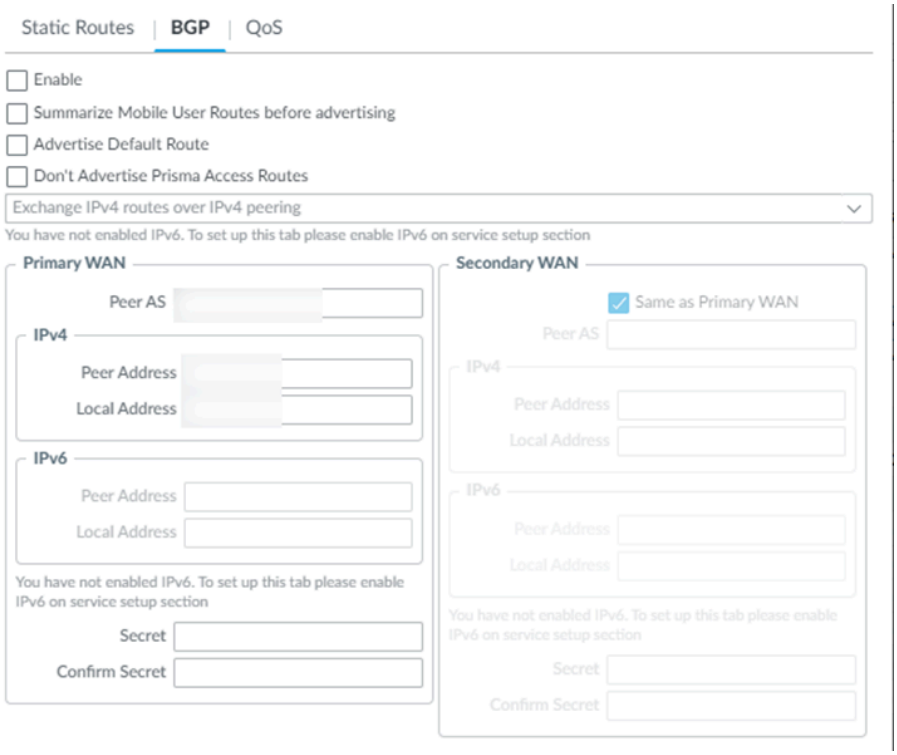
 ©2025 Palo Alto Networks, Inc.

2. Procédez de la même manière pour tous les sous-réseaux ou adresses IP auxquels Prisma Access aura besoin d'accéder à cet emplacement.



- Pour configurer **BGP** :

1. Sélectionnez l'onglet **BGP (BGP)**.
2. (Facultatif) Sélectionnez les choix relatifs à l'**ECMP Load Balancing (Équilibrage de charge ECMP)**. Reportez-vous l'étape 12.
3. Si vous sélectionnez l'option **None (Aucun)** dans **ECMP Load Balancing (Équilibrage de charge ECMP)**, saisissez les choix BGP.



4. Pour activer BGP pour la connexion au réseau distant, sélectionnez **Enable (Activer)**.

   Lorsque vous activez BGP, Prisma Access définit la durée de vie (time to live, TTL) pour BGP externe (eBGP) à 8 pour tenir compte des éventuels sauts supplémentaires qui pourraient se produire entre l'infrastructure Prisma Access et votre équipement de locaux clients (CPE) qui termine la connexion eBGP.
5. Pour réduire le nombre d'annonces de sous-réseaux IP d'utilisateurs mobiles via BGP vers votre équipement de locaux clients (CPE) en les résumant, sélectionnez **Summarize**

 ©2025 Palo Alto Networks, Inc.

Mobile User Routes before advertising (Résumer les itinéraires des utilisateurs mobiles avant de annoncer).

Par défaut, Prisma Access annonce les pools d'adresses IP des utilisateurs mobiles par blocs de sous-réseaux /24. Si vous les résumez, Prisma Access annonce le pool en fonction du sous-réseau que vous avez spécifié. Par exemple, Prisma Access annonce un pool d'adresses IP mobiles d'utilisateurs publics de 10.8.0.0/20 en utilisant le sous-réseau /20, plutôt que de diviser le pool en sous-réseaux de 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, et ainsi de suite, avant de les annoncer. Le résumé de ces annonces peut réduire le nombre d'itinéraires stockés dans les tableaux de routage CPE. Par exemple, vous pouvez utiliser le résumé de pool d'adresses IP avec des passerelles VPN cloud (passerelles privées virtuelles [VGW] ou passerelles de transit [TGW]) qui peuvent accepter un nombre limité d'itinéraires.

Prisma Access définit la chaîne de communauté pour les itinéraires d'utilisateurs mobiles agrégés à `0xFFFE:0xFFF0`.

6. Pour permettre à Prisma Access d'annoncer un itinéraire par défaut pour le réseau distant en utilisant eBGP, sélectionnez **Advertise Default Route (Annoncer l'itinéraire par défaut)**.

   Si vous sélectionnez **Advertise Default Route (Annoncer l'itinéraire par défaut)**, assurez-vous que votre réseau n'a pas un autre itinéraire par défaut annoncé par BGP, sinon vous pourriez introduire des problèmes de routage dans votre réseau.

   Vous devez publier vos itinéraires par défaut avant de faire cette sélection pour les annoncer. De plus, assurez-vous que votre réseau n'a pas une autre itinéraire par défaut annoncé par BGP, sinon vous pourriez introduire des problèmes de routage dans votre réseau.

7. Pour empêcher l'homologue BGP sur le pare-feu Prisma Access de transférer des itinéraires dans le réseau de votre organisation, sélectionnez **Don't Advertise Prisma Access Routes (Ne pas annoncer les itinéraires Prisma Access)**.

   Par défaut, Prisma Access annonce toutes les informations de routage BGP, y compris les itinéraires locaux et tous les préfixes qu'il reçoit d'autres connexions aux services, réseaux distants et sous-réseaux d'utilisateurs mobiles. Cochez cette case pour

 ©2025 Palo Alto Networks, Inc.

empêcher Prisma Access d'envoyer des annonces BGP, mais pour qu'il utilise toujours les informations BGP qu'il reçoit pour apprendre les itinéraires d'autres voisins BGP.

Puisque Prisma Access n'envoie pas d'annonces BGP si vous sélectionnez cette option, vous devez configurer des itinéraires statiques sur l'équipement local pour établir des itinéraires de retour vers Prisma Access.

8. Entrez le **Peer AS (Homologue AS)**, qui est le système autonome (autonomous system, AS) auquel le pare-feu, le routeur virtuel ou le routeur BGP de votre réseau distant appartiennent.
9. Entrez l'adresse IP assignée comme identifiant de routeur du routeur eBGP sur le réseau distant pour lequel vous configurez cette connexion dans **Peer IP Address (Adresse IP de l'homologue)**.
10. (Facultatif) Entrez une adresse que Prisma Access utilise comme adresse IP locale pour BGP.

    La spécification d'une **Local Address (Adresse locale)** est utile lorsque le périphérique de l'autre côté de la connexion (tel qu'une passerelle virtuelle privée Amazon Web Service (AWS)) nécessite une adresse IP locale spécifique pour que l'appairage BGP réussisse. Assurez-vous que l'adresse que vous spécifiez ne soit pas en conflit ou ne chevauche pas les adresses IP dans le sous-réseau d'infrastructure ou les sous-réseaux du réseau distant.

    *Vous devez configurer un itinéraire statique sur votre CPE vers la **Local address (Adresse locale)** BGP.*
11. (Facultatif) Entrez et confirmez une phrase secrète pour authentifier les communications entre homologues BGP.
12. (Facultatif) Si vous avez configuré un **Secondary WAN (WAN secondaire)** et que vous devez changer la **Peer Address (Adresse de l'homologue)** ou la **Local Address (Adresse locale)** pour l'homologue BGP secondaire (de secours), désélectionnez **Same as Primary WAN (Identique au WAN principal)** et entrez une adresse IP d'homologue unique et, éventuellement, une adresse IP locale pour le WAN secondaire.

    Si vous utilisez la mise en réseau IPv6 dans votre déploiement de réseau distant, vous pouvez configurer des adresses **IPv6** ainsi que des adresses **IPv4**. Vous devez également activer la mise en réseau IPv6 globalement dans votre infrastructure Prisma Access avant de pouvoir utiliser l'adressage IPv6.

    Dans certains déploiements (par exemple, lors de l'utilisation de BGP pour établir un appairage avec une passerelle VPN AWS), l'homologue BGP pour le WAN principal et secondaire peut être différent. Dans ces scénarios, vous pouvez choisir de définir un homologue BGP différent pour le WAN secondaire.

    *Pour les déploiements BGP avec des WAN secondaires, Prisma Access définit à la fois le tunnel primaire et le tunnel secondaire dans un état **UP (Actif)**, mais suit le comportement normal de sauvegarde active BGP pour le trafic réseau. Prisma Access définit le tunnel principal comme actif, et envoie et reçoit du trafic uniquement par ce tunnel ; si le tunnel principal échoue, Prisma Access détecte l'échec en utilisant les règles BGP, définit le tunnel secondaire comme actif et utilise uniquement le tunnel secondaire pour envoyer et recevoir du trafic.*

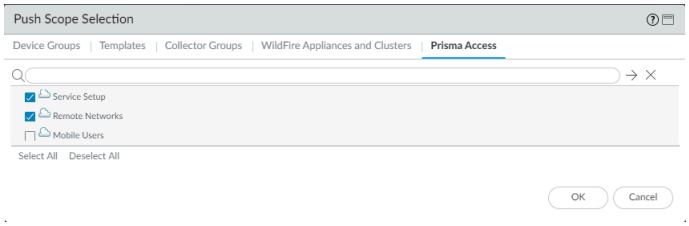
 ©2025 Palo Alto Networks, Inc.

STEP 18 | (Facultatif) Activez la **QoS** pour l'emplacement et spécifier un **QoS Profile (Profil QoS)**.

Vous spécifiez les options QoS et les paramètres globaux par emplacement de calcul dans les **Settings (Paramètres)**. Cependant, vous pouvez activer ou désactiver la QoS ou changer le profil QoS par emplacement ici.

STEP 19 | Validez les modifications apportées à la configuration dans Panorama et appliquez la configuration à Prisma Access pour les réseaux.

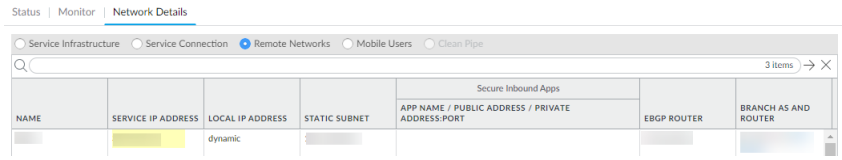
1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.
2. Cliquez sur **Commit (Valider)** > **Commit and Push (Valider et transmettre)**. Cliquez sur **Edit Selections (Modifier les sélections)** > **Prisma Access**, puis sélectionnez Prisma Access pour les réseaux et Prisma Access pour la configuration du service afin d'appliquer la configuration au service.



3. Cliquez sur **OK** et **Push (Appliquer)**.

STEP 20 | Configurez le périphérique compatible avec IPSec à l'emplacement du réseau distant pour configurer une connexion IPSec avec Prisma Access pour les réseaux.

1. Trouvez les **Service IP Address (Adresse IP du service)** pour cette connexion au réseau distant en sélectionnant **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)**, en cliquant sur le bouton radio **Remote Networks (Réseaux distants)** et en consultant les champs **Service IP Address (Adresse IP du service)**. Prisma Access pour l'infrastructure des réseaux a attribué ce cette adresse IP pour la connexion au réseau distant Prisma Access et vous devez configurer cela comme l'adresse IP de l'homologue pour configurer le tunnel IPSec entre l'emplacement du réseau distant et Prisma Access pour les réseaux.



2. Vérifiez la **Local IP address (Adresse IP locale)** du périphérique à l'emplacement réseau distant sur la page **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Remote Networks (Réseaux distants)**. Si vous effectuez une NAT à l'emplacement du réseau distant, la **Local IP address (Adresse IP locale)** affiche l'adresse IP du périphérique après la NAT.

STEP 21 | Pour sécuriser le trafic à l'emplacement réseau distant, vous devez créer des règles de politique de sécurité.

1. Sélectionnez **Policies (Politiques)**.
2. Sélectionnez le **Device Group (Groupe de périphériques)** dans lequel vous souhaitez ajouter des règles de politique. Vous pouvez sélectionner le groupe Remote_Network_Device_Group ou le groupe de périphériques parent que vous avez

 ©2025 Palo Alto Networks, Inc.

sélectionné pour définir des politiques afin de sécuriser l'emplacement du réseau à distance.

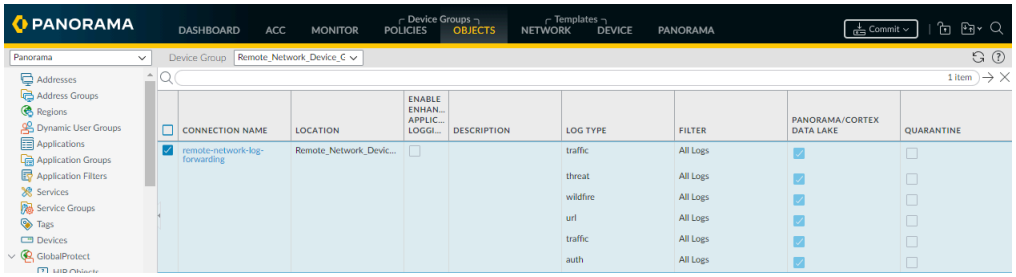
3. Créez des règles de politique de sécurité. Assurez-vous de ne pas définir de règles de politique de sécurité autorisant le trafic de n'importe quelle zone à n'importe quelle zone. Dans les règles de politique de sécurité, utilisez les zones que vous avez définies dans votre modèle.

   Si un utilisateur de votre réseau se voit refuser l'accès à un site web, signalez les problèmes d'accès au site avant d'ouvrir un ticket auprès de Palo Alto Networks.

STEP 22 | Activez la journalisation de Strata Logging Service. Vous devez créer et attacher un profil de transfert des journaux à chaque règle de politique pour laquelle vous souhaitez transférer les journaux.

1. Sélectionnez **Objects (Objets) > Log Forwarding (Transfert des journaux)**.
2. Sélectionnez le **Device Group (Groupe de périphériques)** dans lequel vous avez ajouté les règles de politique, par exemple, Remote_Network_Device_Group.
3. Cliquez sur **Add (Ajouter)** pour ajouter un profil de transfert des journaux. Dans la liste de correspondance du profil de transfert des journaux, cliquez sur **Add (Ajouter)** pour ajouter le **Log Type (Type de journal)** que vous souhaitez transférer.
4. Sélectionnez **Panorama/Strata Logging Service (Service de journalisation Panorama/Strata)** comme méthode de transfert pour permettre à Prisma Access de transférer les journaux à Strata Logging Service. Vous pourrez surveiller les journaux et générer des rapports depuis Panorama. Strata Logging Service offre une intégration transparente pour stocker les journaux sans les renvoyer à votre Panorama au siège social, et Panorama peut interroger Strata Logging Service selon le besoin.

   L'exemple suivant permet le transfert des journaux de trafic, de prévention des menaces, d'envois WildFire, de filtrage des URL, de filtrage des données et d'authentification sur Strata Logging Service.



5. Sélectionnez **Policies (Politiques) > Security (Sécurité)**, puis modifiez la règle de politique. Dans **Actions**, sélectionnez le profil de transfert des journaux que vous avez créé.

STEP 23 | Validez tous vos changements dans Panorama et appliquez les modifications apportées à la configuration à Prisma Access.

1. Cliquez sur **Commit (Valider)** > **Commit and Push (Valider et transmettre)**.
2. Vous devez **Edit Selections (Modifier les sélections)** et, dans l'onglet **Prisma Access**, assurez-vous que l'option **Prisma Access for networks (Prisma Access pour les réseaux)** est sélectionnée dans **Push Scope (Étendue de la transmission)**, puis cliquez sur **OK**.
3. **Commit and Push (Validez et appliquez)** vos modifications.

 ©2025 Palo Alto Networks, Inc.

STEP 24 | Vérifiez l'état du réseau distant.

Voir Vérifier l'état de la connexion du réseau distant pour plus de détails.

 ©2025 Palo Alto Networks, Inc.

Connecter un site de réseau distant à Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access

Configurez des tunnels VPN IPSec pour connecter vos sites de réseaux distants à Prisma Access. Vous devez créer un tunnel IPSec à partir de votre périphérique IPSec de branche vers Prisma Access.

Le premier tunnel que vous créez est le tunnel principal pour le site de réseau distant. Vous pouvez ensuite répéter ce flux de travail pour éventuellement configurer un tunnel secondaire. Lorsque les deux tunnels sont opérationnels, le tunnel principal est prioritaire sur le tunnel secondaire. Si le tunnel principal d'un site de réseau distant tombe en panne, le réseau distant revient au tunnel secondaire jusqu'à ce que le tunnel principal fonctionne de nouveau.

En fonction du périphérique IPSec que vous utilisez pour établir le tunnel sur le site de réseau distant, Prisma Access fournit des paramètres de sécurité IKE et IPSec intégrés et recommandés. Vous pouvez utiliser les paramètres recommandés pour démarrer rapidement ou les personnaliser selon les besoins de votre environnement.

- Ajouter des tunnels VPN IPSec principaux et secondaires
- Plus d'options IKE
- Plus d'options IPSec

Ajouter des tunnels VPN IPSec principaux et secondaires

STEP 1 | Lancez Prisma Access.

STEP 2 | Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Remote Networks (Réseaux distants)** > **Add Remote Networks (Ajouter des réseaux distants** et cliquez sur **Set Up (Configurer)** pour configurer le tunnel principal. Si vous avez déjà configuré un tunnel principal, vous pouvez continuer ici pour ajouter également un tunnel secondaire.

1. Donnez au tunnel un **nom**descriptif.
2. Sélectionnez **Branch Device Type (Type de périphérique de branche)** pour le périphérique IPSec sur le site de réseau distant que vous utilisez pour établir le tunnel Prisma Access.
3. Pour l'**adresse IP du périphérique de branche**, choisissez d'utiliser soit une adresse **IP statique** qui identifie le terminal du tunnel, soit une adresse IP **dynamique**.

   Si vous définissez **Branch Device IP Address (Adresse IP du périphérique de branche)** sur **Dynamic (Dynamique)**, vous devez également ajouter l'ID IKE du site de réseau distant (**IKE Local Identification (Identification locale IKE)**) ou pour Prisma Access (**IKE**

 ©2025 Palo Alto Networks, Inc.

Peer Identification (Identification d'homologue IKE)) pour permettre aux homologues IPSec de s'authentifier.

Étant donné que vous ne disposez pas des valeurs à utiliser pour l'ID IKE Prisma Access (**IKE Peer Identification (Identification d'homologue IKE)**) tant que le réseau distant n'est pas entièrement déployé, vous souhaiterez généralement définir l'ID IKE pour le site de réseau distant (**IKE Local Identification (Identification locale IKE)**) plutôt que l'ID IKE de Prisma Access.

STEP 3 | **Activer la surveillance des tunnels**.

Entrez une adresse **Destination IP (IP de destination)** de surveillance du tunnel sur le réseau distant pour que Prisma Access puisse l'utiliser pour déterminer si le tunnel est actif et, si votre périphérique IPSec de branche utilise un VPN basé sur des politiques, entrez le **Proxy ID (ID de proxy)** associé.

L'adresse IP de surveillance du tunnel que vous saisissez est automatiquement ajoutée à la liste des sous-réseaux de succursale.

STEP 4 | **Enregistrez** les paramètres du tunnel.

Pour continuer :

- Configurez et personnalisez les paramètres crypto avancés pour IKE et IPSec. Consultez Plus d'options IKE et Plus d'options IPSec.
- Activer le routage pour votre réseau distant.

Plus d'options IKE

En fonction du type de périphérique IPSec que vous avez sélectionné, Prisma Access fournit un ensemble recommandé de chiffrements et une durée de vie de clé pour le processus d'échange de clés IKE de la phase 1 entre le périphérique de site de réseau distant et Prisma Access. Vous pouvez utiliser les paramètres recommandés ou personnaliser les paramètres en fonction de vos besoins.

- Sélectionnez une **IKE Protocol Version (Version du protocole IKE)** pour votre périphérique de branche et Prisma Access à utiliser pour la négociation IKE.

  Si vous sélectionnez **IKEv1 Only Mode (Mode IKEv1 uniquement)**, Prisma Access ne peut utiliser que le protocole IKEv1 pour la négociation. Si vous sélectionnez **IKEv2 Only Mode (Mode IKEv2 uniquement)**, Prisma Access ne peut utiliser que le protocole IKEv2 pour la négociation. Si vous sélectionnez **IKEv2 Preferred Mode (Mode IKEv2 préféré)**, Prisma Access utilise le protocole IKEv2 uniquement si votre périphérique IPSec de branche prend également en charge IKEv2. Si votre périphérique IPSec de branche ne prend pas en charge IKEv2, Prisma Access revient à l'utilisation du protocole IKEv1.

 ©2025 Palo Alto Networks, Inc.

- Ajoutez un **profil crypto IKEv1** pour personnaliser les paramètres de chiffrement IKE qui définissent les algorithmes de chiffrement et d'authentification utilisés pour le processus d'échange de clés dans la phase 1 du protocole IKE.

  Prisma Access utilise automatiquement un profil crypto IKE par défaut basé sur le **Branch Device Type (Type de périphérique de branche)** utilisé pour établir ce tunnel.

  - **Chiffrement** : spécifiez l'algorithme de chiffrement utilisé dans la négociation IKE SA.

    Prisma Access prend en charge les algorithmes de chiffrement suivants : 3DES (168 bits), AES-128-CBC (128 bits), AES-192-CBC (192 bits), AES-256-CBC (256 bits) et DES (56 bits). Vous pouvez également sélectionner null (aucun chiffrement).
  - **Authentification** : spécifiez l'algorithme d'authentification utilisé dans la négociation IKE SA.

    Prisma Access prend en charge les algorithmes d'authentification suivants : sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits) et md5 (128 bits). Vous pouvez également sélectionner null (pas d'authentification).
  - **Groupe DH** : spécifiez les groupes Diffie-Hellman (DH) utilisés pour générer des clés symétriques pour IKE dans la négociation IKE SA. L'algorithme Diffie-Hellman utilise la clé privée d'une partie et la clé publique de l'autre pour créer un secret partagé, qui est une clé cryptée partagée par les deux homologues du tunnel PN.

    Prisma Access prend en charge les groupes DH suivants : Groupe 1 (768 bits), Groupe 2 (1 024 bits par défaut), Groupe 5 (1 536 bits), Groupe 14 (2 048 bits), Groupe 19 (groupe de courbes elliptiques 256 bits) et Groupe 20 (groupe de courbes elliptiques 384 bits). Pour obtenir la sécurité la plus forte, sélectionnez le groupe avec le nombre le plus élevé.
  - **Durée de vie** : spécifiez l'unité et la durée de validité de la clé de la phase 1 du protocole IKE (8 heures par défaut). Pour IKEv1, la Security Association (association de sécurité - SA) ne fait pas l'objet d'un changement de clef avant l'expiration de la durée de vie de la clé. Le changement de clef de la phase 1 du protocole IKEv1 se déclenche uniquement lorsque la SA expire. Pour IKEv2, la SA doit être faire l'objet d'un changement de clef avant l'expiration de la durée de vie de la clé. Si la SA ne fait pas l'objet d'un changement de clef à l'expiration, elle doit commencer une nouvelle clé de phase 1.
  - **IKEv2 Authentication Multiple (Multiple d'authentification IKEv2)** : spécifiez la valeur multipliée par la durée de vie de la clé pour déterminer le nombre d'authentifications (plage de 0 à 50 ; valeur par défaut 0). Le nombre d'authentifications est le nombre de fois où le nœud de traitement de sécurité peut effectuer un renouvellement de clé SA IKE IKEv2 avant de devoir recommencer la réauthentification IKEv2. La valeur par défaut de 0 désactive la fonction de réauthentification.

- Activez **IKE Passive Mode (Mode IKE passif)** afin que Prisma Access ne réponde qu'aux connexions IKE et ne les lance pas.

- **IKE NAT Traversal** est activé par défaut.

  Cela signifie que l'encapsulation UDP est utilisée sur les protocoles IKE et UDP, ce qui leur permet de passer par des périphériques Network Address Translation (traduction d'adresse réseau - NAT) situés entre les points de terminaison du tunnel VPN IPSec.

 ©2025 Palo Alto Networks, Inc.

Plus d'options IPSec

En fonction du type de périphérique IPSec que vous avez sélectionné, Prisma Access fournit un ensemble recommandé de paramètres de protocole IPSec et de durée de vie de la clé pour sécuriser les données dans le tunnel IPSec entre votre périphérique de branche et Prisma Access dans la phase 2 du protocole IKE pour la Security Association (association de sécurité - SA). Vous pouvez utiliser les paramètres recommandés ou personnaliser les paramètres en fonction de vos besoins.

- Personnalisez le **profil crypto IPSec** pour définir comment les données sont sécurisées dans le tunnel lorsque Auto Key IKE génère automatiquement des clés pour les SA IKE pendant la phase 2 du protocole IKE.

  Prisma Access configure automatiquement un profil crypto IPSec par défaut en fonction du fournisseur du **Branch Device Type (Type de périphérique de branche)**. Vous pouvez utiliser le profil par défaut ou créer un profil personnalisé.

  - **Protocole IPSec** : sécurisez les données qui traversent le tunnel VPN. **ESP** : le protocole ESP (Encapsulating Security Payload/Encapsulation sécurisée de la charge utile) crypte les données, authentifie la source et vérifie l'intégrité des données. **AH** : le protocole AH (Authentication Header/En-tête d'authentification) authentifie la source et vérifie l'intégrité des données.

    Si vous utilisez **ESP** comme protocole IPSec, spécifiez également l'algorithme **de chiffrement** utilisé dans la négociation SA IPSec.

    Prisma Access prend en charge les algorithmes de chiffrement suivants : aes-256-gcm (256 bits), aes-256-cbc (256 bits), aes-192-cbc (192 bits), aes-128-gcm (128 bits), aes-128-cbc (128 bits), 3des (168 bits) et des (56 bits). Vous pouvez également sélectionner null (aucun chiffrement).

- **Authentification** : spécifiez l'algorithme d'authentification utilisé dans la négociation SA IPSec.

  Prisma Access prend en charge les algorithmes d'authentification suivants : sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits) et md5 (128 bits). Si le protocole IPSec est ESP, vous pouvez également sélectionner none (aucune authentification).

- **Groupe DH** : spécifiez les groupes Diffie-Hellman (DH) pour IKE dans la négociation de la Security Association (association de sécurité - SA) IPSec.

  Prisma Access prend en charge les groupes DH suivants : Groupe 1 (768 bits), Groupe 2 (1 024 bits par défaut), Groupe 5 (1 536 bits), Groupe 14 (2 048 bits), Groupe 19 (groupe de courbes elliptiques 256 bits) et Groupe 20 (groupe de courbes elliptiques 384 bits). Pour obtenir la sécurité la plus forte, sélectionnez le groupe avec le nombre le plus élevé. Si vous ne souhaitez pas renouveler la clé créée par Prisma Access pendant la phase 1 du protocole IKE, sélectionnez **no-pfs** (pas de confidentialité persistante parfaite). Si vous sélectionnez cette option, Prisma Access réutilise la clé actuelle pour la négociation IPSec SA.

- **Durée de vie** : spécifiez l'unité et la durée de validité de la clé négociée (une heure par défaut).

- **Taille réelle** : spécifiez l'unité et la quantité de données que la clé peut utiliser pour le chiffrement.

 ©2025 Palo Alto Networks, Inc.

Activer le routage pour votre réseau distant

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access

Pour que Prisma Access achemine le trafic vers vos réseaux distants, vous devez fournir des informations de routage pour les sous-réseaux que vous souhaitez sécuriser à l'aide de Prisma Access. Vous pouvez le faire de plusieurs façons. Vous pouvez soit définir un itinéraire statique vers chaque sous-réseau sur le site du réseau distant, soit configurer BGP entre vos emplacements de connexion aux services et Prisma Access ou utiliser une combinaison des deux méthodes.

Si vous configurez les itinéraires statiques et activez BGP, les itinéraires statiques sont prioritaires. Bien qu'il puisse être pratique d'utiliser des itinéraires statiques si vous n'avez que quelques sous-réseaux sur vos emplacements de réseaux distants, dans un déploiement à grande échelle avec de nombreux réseaux distants avec des sous-réseaux qui se chevauchent, BGP vous permettra de mettre à l'échelle plus facilement.

- **Itinéraires statiques** : pour activer des itinéraires statiques vers et depuis votre site distant vers Prisma Access, identifiez les sous-réseaux ou les adresses IP individuelles du site distant que vous souhaitez que Prisma Access sécurise (pour le trafic entrant et sortant). Les sous-réseaux de chaque site ne doivent pas se chevaucher, avec les pools d'adresses IP que vous avez désignés pour Prisma Access pour les utilisateurs, ou avec le sous-réseau d'infrastructure.
- **BGP** : si vous souhaitez activer BGP pour acheminer dynamiquement le trafic vers et depuis votre réseau distant, vous devez fournir les informations BGP pour le routeur eBGP de votre branche :
  - **Numéro de système autonome (AS, Autonomous System) de routeur de branche** : l'AS auquel appartient le routeur eBGP sur le réseau distant. C'est ce qu'on appelle le **Peer AS (AS homologue)**.
  - **ID du routeur** : l'adresse IP attribuée comme ID de routeur du routeur eBGP sur le réseau distant. C'est ce qu'on appelle la **Peer Address (Adresse de l'homologue)**.

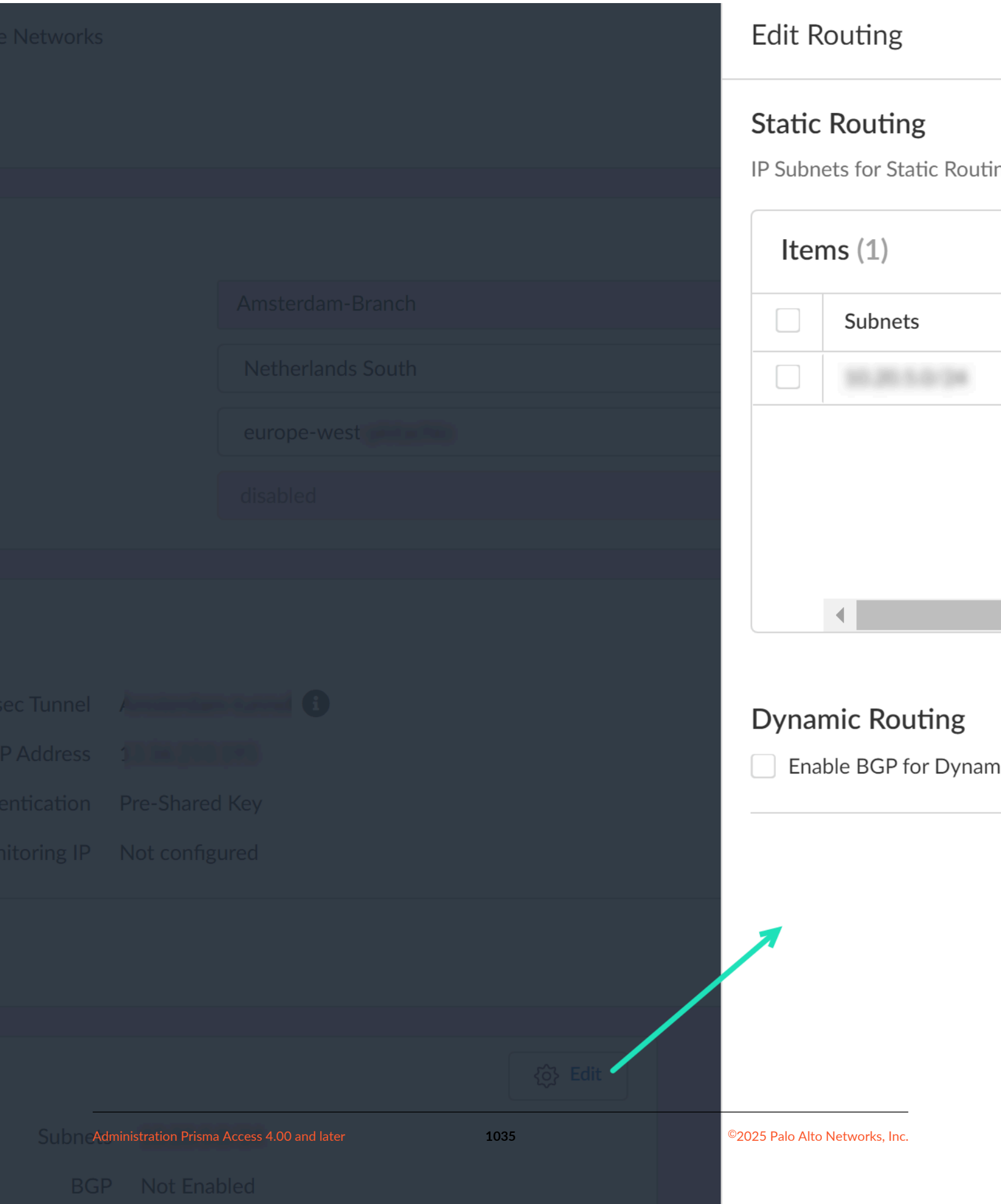
  Si vous configurez à la fois des itinéraires statiques et le routage BGP, les itinéraires statiques sont prioritaires.

Voici comment configurer les paramètres de routage de votre site de réseau distant.

 ©2025 Palo Alto Networks, Inc.

- Pour ajouter ou modifier les paramètres de routage, accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Remote Networks (Réseaux distants)** et ajoutez ou modifiez un site de réseau distant.

 ©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

- Configurez des itinéraires statiques.

  Si vous utilisez des itinéraires statiques pour acheminer le trafic vers et depuis votre branche, **Add (Ajoutez)** les sous-réseaux IP ou les adresses IP que vous voulez sécuriser au niveau de la branche. Notez que si vous apportez des modifications aux sous-réseaux IP de votre branche, vous devez mettre à jour manuellement les itinéraires statiques.

- Configurez le routage dynamique.

  Pour utiliser le routage dynamique afin de publier vos sous-réseaux de branches, procédez comme suit : **Enable BGP for Dynamic Routing (Activez BGP pour le routage dynamique)**, puis configurez les paramètres suivants :

  - **Do Not Export Routes (Ne pas exporter les itinéraires)** : empêchez Prisma Access de transférer des itinéraires vers votre réseau distant.

    Par défaut, Prisma Access publie toutes les informations de routage BGP, y compris les itinéraires locaux et tous les préfixes qu'il reçoit d'autres connexions aux services, réseaux distants et sous-réseaux d'utilisateurs mobiles. Cochez cette case pour empêcher Prisma Access d'envoyer des annonces BGP, mais pour qu'il utilise toujours les informations BGP qu'il reçoit pour apprendre les itinéraires d'autres voisins BGP.

    Parce que Prisma Access n'envoie pas d'annonces BGP, si vous sélectionnez cette option, vous devez configurer des itinéraires statiques sur votre équipement sur site pour établir des itinéraires de retour vers Prisma Access.

  - **Peer IP Address (Adresse IP de l'homologue)** : saisissez l'adresse IP de l'homologue attribuée comme ID de routeur du routeur eBGP sur le réseau distant.
  - **Peer AS (AS homologue)** : saisissez l'AS homologue, qui est le système autonome (AS) de votre réseau.

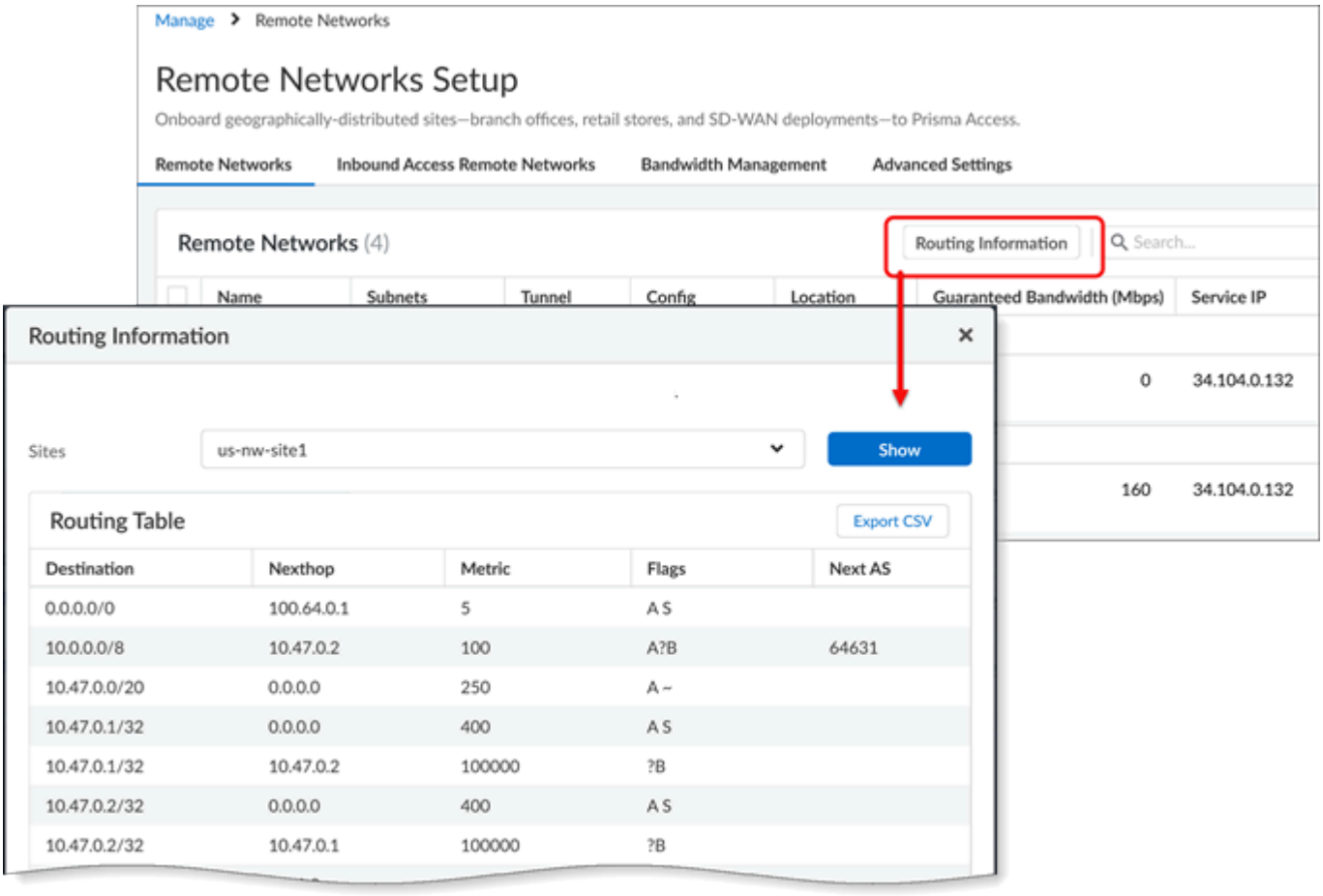
    Vous devez utiliser un numéro AS privé BGP conforme à la RFC 6996.
  - **Local IP Address (Adresse IP locale)** : saisissez l'adresse IP que Prisma Access utilise comme adresse IP locale pour BGP.

    Une adresse locale n'est requise que si votre périphérique de site distant en a besoin pour que l'appairage BGP réussisse. Assurez-vous que l'adresse que vous spécifiez ne soit pas en conflit ou ne chevauche pas les adresses IP dans le sous-réseau d'infrastructure ou les sous-réseaux du réseau distant.
  - **Secret** : saisissez un mot de passe secret pour authentifier les communications de l'homologue BGP, puis **Confirm Secret (Confirmez le secret)**.

Résoudre les problèmes de connexion au site

À des fins de dépannage, vous pouvez désormais afficher la table de routage d'un site de réseau distant ou d'un site de connexion aux services. Trouvez le bouton **Routing Information (Informations de routage)** sur le tableau de bord des réseaux distants ou de la connexion aux services.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

Intégrer plusieurs réseaux distants

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• Licence Prisma Access

Pour simplifier le processus d'intégration et de configuration des réseaux distants, vous avez la possibilité d'intégrer au moins un réseau distant, puis d'exporter ces paramètres dans un fichier texte CSV (valeur séparée par une virgule). Le fichier CSV inclut les valeurs des paramètres de tunnel IPSec et de passerelle IKE pour le réseau que vous avez sélectionné pour l'exportation, et vous pouvez ensuite modifier ces paramètres et les rendre uniques pour chaque nouveau réseau que vous souhaitez intégrer. Vous pouvez modifier le fichier CSV pour inclure 100 nouveaux réseaux distants, puis réimporter le fichier CSV pour accélérer le processus d'intégration de nouveaux emplacements de réseaux distants.

Le fichier CSV n'inclut pas de clés ou de mots de passe, tels que le secret partagé BGP, la clé prépartagée IKE, l'ID de proxy, le profil crypto IKE, le profil crypto IPSec. Par conséquent, l'ensemble des clés et mots de passe requis pour les paramètres du tunnel IPSec et de la passerelle IKE sont hérités du réseau que vous sélectionnez lors du lancement de l'importation de fichiers CSV.

Lorsque vous utilisez ce processus d'importation en bloc, vous devez attendre que Prisma Access déploie l'infrastructure nécessaire pour sécuriser ces sites.

STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** (dans la section Intégration).

STEP 2 | Sélectionnez un emplacement, puis cliquez sur **Export (Exporter)** pour exporter la configuration d'un réseau distant que vous avez précédemment intégré.

Si vous n'avez pas encore ajouté d'emplacements, vous devez **Add (Ajouter)** un emplacement, puis télécharger sa configuration. Vous devez sélectionner un réseau distant et cliquer sur **Export (Exporter)**. Un fichier CSV contenant les paramètres est téléchargé sur votre ordinateur.

STEP 3 | (Déploiements qui allouent la bande passante en fonction de l'emplacement de calcul uniquement) Vérifiez que vous avez alloué de la bande passante pour les emplacements à intégrer.

Chaque emplacement que vous intégrez comporte un emplacement de calcul correspondant pour lequel la bande passante est allouée.

1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** et cliquez sur l'engrenage dans la zone **Bandwidth Allocation (Allocation de bande passante)**.
2. Contrôlez le champ **Bandwidth Allocation (Allocation de bande passante)** dans le tableau qui s'affiche.

   Le tableau de cette zone indique le mappage de l'emplacement de calcul à l'emplacement de Prisma Access. Une bande passante doit être allouée pour les emplacements de calcul associés aux emplacements que vous souhaitez intégrer. Par exemple, pour intégrer

 ©2025 Palo Alto Networks, Inc.

l'emplacement Japon Centre, vérifiez que vous avez alloué de la bande passante à l'emplacement de calcul Asie Nord-Est.

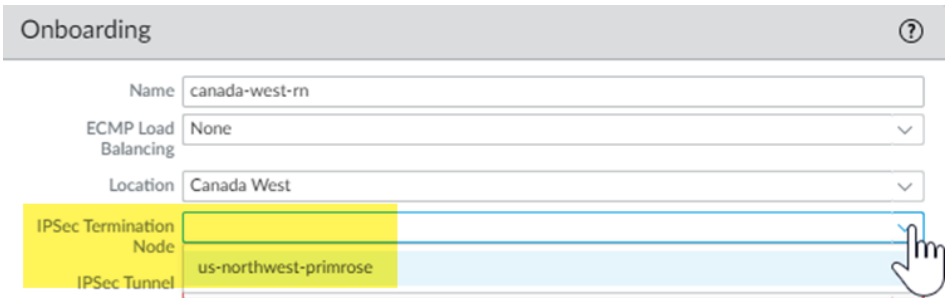
3. Si vous n'avez pas encore alloué de bande passante aux emplacements de calcul associés aux emplacements que vous souhaitez intégrer, ajoutez-la maintenant.

STEP 4 | (Déploiements qui allouent de la bande passante en fonction de l'emplacement de calcul uniquement) Recherchez le **IPSec Termination Node (Nœud de terminaison IPSec)** associé à ou aux emplacements que vous souhaitez intégrer.

Attribuez un *Nœud de terminaison IPSec* au réseau distant pendant l'intégration et saisissez cette valeur dans la colonne **spn_name** du fichier CSV. Chaque nœud de terminaison IPSec peut fournir jusqu'à 1 000 Mbit/s de bande passante.

Pour trouver le nœud de terminaison IPSec, effectuez l'une des actions suivantes :

- Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**, cliquez sur **Add (Ajouter)** pour ajouter un réseau distant et sélectionnez l'emplacement que vous souhaitez intégrer, puis notez les choix de nœud de terminaison IPSec dans la zone d'intégration.



- Ouvrez une session d'interface de ligne de commande (CLI) avec le Panorama qui gère Prisma Access et saisissez la commande `show plugins cloud_services remote-networks agg-bandwidth region` *compute-location-name* où *compute-location-name* désigne l'emplacement de calcul associé à l'emplacement que vous souhaitez intégrer. Le nœud de terminaison IPSec s'affiche dans le champ`spn-name-list`.

STEP 5 | Modifiez le fichier CSV pour ajouter une configuration pour les réseaux distants.

Reportez-vous à Champs du tableau des réseaux distants pour une description des champs et des valeurs possibles dans ce fichier.

Vous devez renommer le ou les réseaux répertoriés dans le fichier exporté. Si le fichier comporte des noms en double, l'importation échouera.

STEP 6 | Cliquez sur **Import (Importer)** pour importer le fichier CSV.

La configuration du fichier s'affiche à l'écran. Le réseau distant que vous avez sélectionné pour importer le fichier servira de configuration de modèle, et les réseaux distants répertoriés dans le fichier hériteront de là les clés et toutes les valeurs manquantes qui n'ont pas besoin d'être uniques.

STEP 7 | Validez et appliquez les modifications.

1. **Commit (Validez)** > **Commit and Push (Validez et appliquez)** vos modifications.
2. Cliquez sur **OK** et **Push (Appliquer)**.

 ©2025 Palo Alto Networks, Inc.

Champs du tableau des réseaux distants

Le tableau suivant fournit une description des champs du tableau des réseaux distants. Les champs marqués comme **Y** dans la ligne **Obligatoire** sont obligatoires et les champs marqués comme **N** sont facultatifs.

Champ	Description	Obligatoire (O/N)
Nom	Nom du réseau distant.	Y
Bande passante	(Déploiements qui allouent de la bande passante en fonction de l'emplacement uniquement) La bande passante allouée au réseau distant. Les valeurs acceptables sont les suivantes : • 2 Mbit/s • 5 Mbit/s • 10 Mbit/s • 20 Mbit/s • 25 Mbit/s • 50 Mbit/s • 100 Mbit/s • 150 Mbit/s • 300 Mbit/s • 500 Mbit/s • 1 000 Mbit/s *L'option de bande passante de 1 000 Mbit/s est en mode prévisualisation. Le débit pendant la prévisualisation est fourni dans la mesure du possible et les performances réelles varient en fonction de la composition du trafic.*	Y
région	Emplacement du réseau distant. Saisissez les emplacements exactement tels qu'ils sont dans ce document (par exemple, **US West (États-Unis Ouest)**ou **Japan South (Japon Sud)**.	Y
subnets	Sous-réseaux à itinéraire statique du côté LAN du réseau distant. Séparez plusieurs sous-réseaux par des virgules.	N

©2025 Palo Alto Networks, Inc.

Champ	Description	Obligatoire (O/N)
bgp_peer_as	Numéro de système autonome (ASN) BGP du périphérique homologue du réseau distant.	N
bgp_peer_address	Adresse de l'homologue BGP du périphérique homologue du réseau distant.	N
tunnel_name	Nom de la configuration du tunnel IPSec. Une valeur unique est requise.	Y
gateway_name	Nom de la configuration de la passerelle IKE. Une valeur unique est requise.	Y
peer_ip_address	Adresse IP du périphérique homologue Prisma Access.	N
local_id_type	Type d'ID IKE que Prisma Access présente au périphérique homologue. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats configurés.	N
local_id_value	Valeur de l'ID IKE que Prisma Access présente au périphérique homologue. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats configurés.	N
peer_id_type	Valeur de l'ID IKE que l'homologue présente à Prisma Access. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats homologues.	N
peer_id_value	Valeur de l'ID IKE que Prisma Access présente au périphérique homologue. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats homologues.	N
monitor_ip	Adresse IP de surveillance du tunnel qui sera utilisée par le cloud pour déterminer que le tunnel IPSec est opérationnel et que le réseau homologue est accessible.	N

 ©2025 Palo Alto Networks, Inc.

Champ	Description	Obligatoire (O/N)
	Vous ne pouvez pas exporter une valeur d'ID de proxy pour le moniteur de tunnel.	
proxy_ids	ID de proxy configurés pour l'homologue. Laissez ce champ vide pour les VPN basés sur des itinéraires. Spécifiez l'ID de proxy dans le format de configuration CSV suivant : [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	N
sec_wan_enabled	Spécifie si vous activez ou non un tunnel IPSec secondaire. Les valeurs acceptables sont `yes (oui)` et `no (non)`.	N
sec_tunnel_name	Nom de la configuration du tunnel IPSec secondaire. Une valeur unique est requise si vous spécifiez un tunnel secondaire.	N
sec_gateway_name	Nom de la configuration de la passerelle IKE secondaire. Une valeur unique est requise si vous spécifiez un tunnel secondaire.	N
sec_peer_ip_address	L'adresse IP du périphérique homologue Prisma Access pour le tunnel IPSec secondaire.	N
sec_local_id_type	Type de l'ID IKE présenté par Prisma Access au périphérique homologue du tunnel IPSec secondaire. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats configurés.	N
sec_local_id_value	Valeur de l'ID IKE présenté par Prisma Access au périphérique homologue du tunnel IPSec secondaire. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats configurés.	N
sec_peer_id_type	Valeur de l'ID IKE présenté par l'homologue à Prisma Access pour le tunnel IPSec secondaire. Si	N

 ©2025 Palo Alto Networks, Inc.

Champ	Description	Obligatoire (O/N)
	vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats homologues.	
sec_peer_id_value	Valeur de l'ID IKE présenté par Prisma Access au périphérique homologue du tunnel IPSec secondaire. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats homologues.	N
sec_monitor_ip	Adresse IP de surveillance du tunnel qui sera utilisée par le cloud pour le tunnel IPSec secondaire afin de déterminer que le tunnel IPSec est opérationnel et que le réseau homologue est accessible. *Vous ne pouvez pas exporter une valeur d'ID de proxy pour le moniteur de tunnel.*	N
sec_proxy_ids	ID de proxy configurés pour l'homologue du tunnel IPSec secondaire. Laissez ce champ vide pour les VPN basés sur des itinéraires. Spécifiez l'ID de proxy dans le format de configuration CSV suivant : [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	N
ecmp_link_1_tunnel_name	(Déploiements ECMP uniquement) Nom de la configuration du tunnel IPSec pour le tunnel ECMP 1. Une valeur unique est requise.	
ecmp_link_1_gateway_name	(Déploiements ECMP uniquement) Nom de la configuration de la passerelle IKE pour le tunnel ECMP 1. Une valeur unique est requise.	
ecmp_link_1_peer_ip_address	(Déploiements ECMP uniquement) Adresse IP du dispositif homologue Prisma Access pour le tunnel ECMP 1.	

 ©2025 Palo Alto Networks, Inc.

Champ	Description	Obligatoire (O/N)
ecmp_link_1_local_id_type	(Déploiements ECMP uniquement) Type d'ID IKE présenté par Prisma Access au périphérique homologue pour le tunnel ECMP 1. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats configurés.	
ecmp_link_1_local_id_value	(Déploiements ECMP uniquement) Valeur de l'ID IKE présenté par Prisma Access au périphérique homologue pour le tunnel ECMP 1. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats configurés.	
ecmp_link_1_peer_id_type	(Déploiements ECMP uniquement) Valeur de l'ID IKE que l'homologue présente à Prisma Access pour le tunnel ECMP 1. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats homologues.	
ecmp_link_1_peer_id_value	(Déploiements ECMP uniquement) Valeur de l'ID IKE présenté par Prisma Access au périphérique homologue pour le tunnel ECMP 1. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats homologues.	
ecmp_link_1_monitor_ip	(Déploiements ECMP uniquement) Adresse IP de surveillance du tunnel que le cloud utilisera pour déterminer que le tunnel IPSec est opérationnel et que le réseau homologue est accessible pour le tunnel ECMP 1. *Vous ne pouvez pas exporter une valeur d'ID de proxy pour le moniteur de tunnel.*	
ecmp_link_1_proxy_ids	(Déploiements ECMP uniquement) ID de proxy configurés pour l'homologue du tunnel ECMP 1. Laissez ce champ vide pour les VPN basés sur des itinéraires. Spécifiez l'ID de proxy dans le format de configuration CSV suivant :	

 ©2025 Palo Alto Networks, Inc.

Champ	Description	Obligatoire (O/N)
	[{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	
ecmp_link_1_bgp_peer_as	(Déploiements ECMP uniquement) Numéro de système autonome (ASN) BGP du périphérique homologue du réseau distant pour le tunnel ECMP 1.	
ecmp_link_1_bgp_peer_address	(Déploiements ECMP uniquement) Adresse de l'homologue BGP du périphérique d'homologue réseau distant pour le tunnel ECMP 1.	
ecmp_link_2_tunnel_name	(Déploiements ECMP uniquement) Nom de la configuration du tunnel IPSec pour le tunnel ECMP 2. Une valeur unique est requise.	
ecmp_link_2_gateway_name	(Déploiements ECMP uniquement) Nom de la configuration de la passerelle IKE pour le tunnel ECMP 2. Une valeur unique est requise.	
ecmp_link_2_peer_ip_address	(Déploiements ECMP uniquement) Adresse IP du périphérique homologue Prisma Access pour le tunnel ECMP 2.	
ecmp_link_2_local_id_type	(Déploiements ECMP uniquement) Type d'ID IKE présenté par Prisma Access au périphérique homologue pour le tunnel ECMP 2. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats configurés.	
ecmp_link_2_local_id_value	(Déploiements ECMP uniquement) Valeur de l'ID IKE présenté par Prisma Access au périphérique homologue pour le tunnel ECMP 2. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats configurés.	
ecmp_link_2_peer_id_type	(Déploiements ECMP uniquement) Valeur de l'ID IKE que l'homologue présente à Prisma Access pour le tunnel ECMP 2. Si vous utilisez	

 ©2025 Palo Alto Networks, Inc.

Champ	Description	Obligatoire (O/N)
	des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats homologues.	
ecmp_link_2_peer_id_value	(Déploiements ECMP uniquement) Valeur de l'ID IKE présenté par Prisma Access au périphérique homologue pour le tunnel ECMP 2. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats homologues.	
ecmp_link_2_monitor_ip	(Déploiements ECMP uniquement) Adresse IP de surveillance du tunnel que le cloud utilisera pour déterminer que le tunnel IPSec est opérationnel et que le réseau homologue est accessible pour le tunnel ECMP 2. *Vous ne pouvez pas exporter une valeur d'ID de proxy pour le moniteur de tunnel.*	
ecmp_link_2_proxy_ids	(Déploiements ECMP uniquement) ID de proxy configurés pour l'homologue du tunnel ECMP 2. Laissez ce champ vide pour les VPN basés sur des itinéraires. Spécifiez l'ID de proxy dans le format de configuration CSV suivant : [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	
ecmp_link_2_bgp_peer_as	(Déploiements ECMP uniquement) Numéro de système autonome (ASN) BGP du périphérique homologue du réseau distant pour le tunnel ECMP 2.	
ecmp_link_2_bgp_peer_address	(Déploiements ECMP uniquement) Adresse de l'homologue BGP du périphérique d'homologue réseau distant pour le tunnel ECMP 2.	

 ©2025 Palo Alto Networks, Inc.

Champ	Description	Obligatoire (O/N)
ecmp_link_3_tunnel_name	(Déploiements ECMP uniquement) Nom de la configuration du tunnel IPSec pour le tunnel ECMP 3. Une valeur unique est requise.	
ecmp_link_3_gateway_name	(Déploiements ECMP uniquement) Nom de la configuration de la passerelle IKE pour le tunnel ECMP 3. Une valeur unique est requise.	
ecmp_link_3_peer_ip_address	(Déploiements ECMP uniquement) Adresse IP du périphérique homologue Prisma Access pour le tunnel ECMP 3.	
ecmp_link_3_local_id_type	(Déploiements ECMP uniquement) Type d'ID IKE présenté par Prisma Access au périphérique homologue pour le tunnel ECMP 3. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats configurés.	
ecmp_link_3_local_id_value	(Déploiements ECMP uniquement) Valeur de l'ID IKE présenté par Prisma Access au périphérique homologue pour le tunnel ECMP 3. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats configurés.	
ecmp_link_3_peer_id_type	(Déploiements ECMP uniquement) Valeur de l'ID IKE que l'homologue présente à Prisma Access pour le tunnel ECMP 3. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats homologues.	
ecmp_link_3_peer_id_value	(Déploiements ECMP uniquement) Valeur de l'ID IKE présenté par Prisma Access au périphérique homologue pour le tunnel ECMP 3. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats homologues.	
ecmp_link_3_monitor_ip	(Déploiements ECMP uniquement) Adresse IP de surveillance du tunnel que le cloud utilisera pour déterminer que le tunnel IPSec est opérationnel	

 ©2025 Palo Alto Networks, Inc.

Champ	Description	Obligatoire (O/N)
	et que le réseau homologue est accessible pour le tunnel ECMP 3. *Vous ne pouvez pas exporter une valeur d'ID de proxy pour le moniteur de tunnel.*	
ecmp_link_3_proxy_ids	(Déploiements ECMP uniquement) ID de proxy configurés pour l'homologue du tunnel ECMP 3. Laissez ce champ vide pour les VPN basés sur des itinéraires. Spécifiez l'ID de proxy dans le format de configuration CSV suivant : [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	
ecmp_link_3_bgp_peer_as	(Déploiements ECMP uniquement) Numéro de système autonome (ASN) BGP du périphérique homologue du réseau distant pour le tunnel ECMP 3.	
ecmp_link_3_bgp_peer_address	(Déploiements ECMP uniquement) Adresse de l'homologue BGP du périphérique d'homologue réseau distant pour le tunnel ECMP 3.	
ecmp_link_4_tunnel_name	(Déploiements ECMP uniquement) Nom de la configuration du tunnel IPSec pour le tunnel ECMP 4. Une valeur unique est requise.	
ecmp_link_4_gateway_name	(Déploiements ECMP uniquement) Nom de la configuration de la passerelle IKE pour le tunnel ECMP 4. Une valeur unique est requise.	
ecmp_link_4_peer_ip_address	(Déploiements ECMP uniquement) Adresse IP du périphérique homologue Prisma Access pour le tunnel ECMP 4.	
ecmp_link_4_local_id_type	(Déploiements ECMP uniquement) Type d'ID IKE présenté par Prisma Access au périphérique homologue pour le tunnel ECMP 4. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types	

 ©2025 Palo Alto Networks, Inc.

Champ	Description	Obligatoire (O/N)
	importés spécifiés feront référence aux valeurs des certificats configurés.	
ecmp_link_4_local_id_value	(Déploiements ECMP uniquement) Valeur de l'ID IKE présenté par Prisma Access au périphérique homologue pour le tunnel ECMP 4. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats configurés.	
ecmp_link_4_peer_id_type	(Déploiements ECMP uniquement) Valeur de l'ID IKE que l'homologue présente à Prisma Access pour le tunnel ECMP 4. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats homologues.	
ecmp_link_4_peer_id_value	(Déploiements ECMP uniquement) Valeur de l'ID IKE présenté par Prisma Access au périphérique homologue pour le tunnel ECMP 4. Si vous utilisez des certificats dans le réseau distant vers lequel vous importez ce fichier, tous les types importés spécifiés feront référence aux valeurs des certificats homologues.	
ecmp_link_4_monitor_ip	(Déploiements ECMP uniquement) Adresse IP de surveillance du tunnel que le cloud utilisera pour déterminer que le tunnel IPSec est opérationnel et que le réseau homologue est accessible pour le tunnel ECMP 4. *Vous ne pouvez pas exporter une valeur d'ID de proxy pour le moniteur de tunnel.*	
ecmp_link_4_proxy_ids	(Déploiements ECMP uniquement) ID de proxy configurés pour l'homologue du tunnel ECMP 4. Laissez ce champ vide pour les VPN basés sur des itinéraires. Spécifiez l'ID de proxy dans le format de configuration CSV suivant : [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*",	

 ©2025 Palo Alto Networks, Inc.

Champ	Description	Obligatoire (O/N)
	"remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	
ecmp_link_4_bgp_peer_as	(Déploiements ECMP uniquement) Numéro de système autonome (ASN) BGP du périphérique homologue du réseau distant pour le tunnel ECMP 4.	
ecmp_link_4_bgp_peer_address	(Déploiements ECMP uniquement) Adresse de l'homologue BGP du périphérique d'homologue réseau distant pour le tunnel ECMP 4.	
spn-name	(Déploiements qui allouent de la bande passante en fonction de l'emplacement de calcul uniquement) Nom du nœud de terminaison IPSec. Ce champ est obligatoire pour les déploiements qui allouent de la bande passante en fonction de l'emplacement de calcul.	

 ©2025 Palo Alto Networks, Inc.

Vérifier si le réseau distant est connecté à Prisma Access

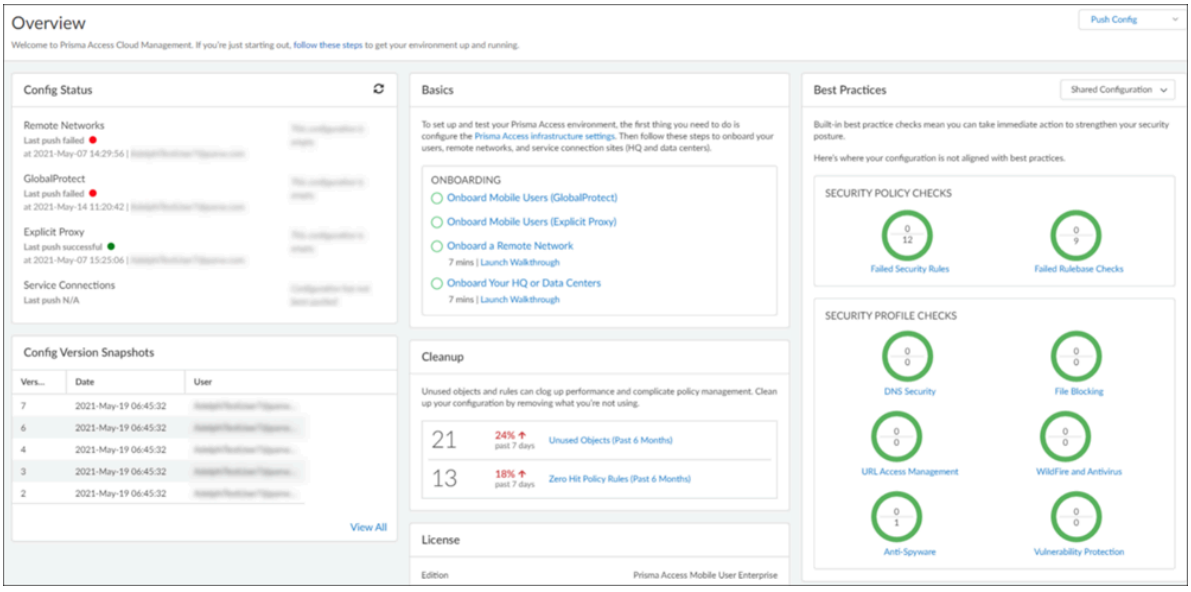
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Après avoir configuré le périphérique VPN IPSec sur le réseau distant, vérifiez l'état du tunnel. Lorsque vous vérifiez l'état des réseaux distants, n'oubliez pas ce qui suit :

- Vérifiez l'état du tunnel IPSec vers votre réseau distant.
- La dernière étape lors de la vérification des réseaux distants consiste à examiner les journaux et à s'assurer que le trafic circule via Prisma Access. S'il y a des erreurs ou des avertissements, consultez les journaux système dans Prisma Access et les journaux locaux sur le périphérique réseau distant. Résolvez toutes les erreurs ou tous les avertissements avant de procéder à la configuration.
- Continuez à ajouter des réseaux distants au besoin.
- Strata Cloud Manager
- Panorama

Vérifier si le réseau distant est connecté à Prisma Access (Strata Cloud Manager)

Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)**, modifiez la**Configuration Scope (Portée de la configuration)** en **Prisma Access** et sélectionnez **Prisma Access Sync Status (État de la synchronisation de Prisma Access)** > **Remote Networks (Réseaux distants)**.



 ©2025 Palo Alto Networks, Inc.

Vérifier si le réseau distant est connecté à Prisma Access (Panorama)

STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Status (État)**pour vérifier que les connexions aux réseaux distants ont été déployées avec succès.

La zone **Deployment Status (État du déploiement)** vous permet d'afficher la progression des tâches d'intégration et de déploiement avant qu'elles ne soient terminées, ainsi que de voir plus d'informations sur l'état des tâches terminées.

STEP 2 | Pour afficher une carte indiquant les emplacements des réseaux distants dans les régions que vous avez sélectionnées, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Monitor (Surveiller)** et cliquez sur l'onglet **Remote Networks (Réseaux distants)**.

STEP 3 | Sélectionnez une région pour obtenir plus de détails sur cette région.

STEP 4 | Cliquez sur les onglets sous la carte pour voir des statistiques supplémentaires sur le réseau distant.

Onglet **Status (État)** :

- **Location (Emplacement)** : emplacement où votre réseau distant est déployé.
- **Remote Peer (Homologue distant)** : homologue auquel le réseau distant dispose d'une connexion tunnel IPSec.
- **IPSec Termination Node (Nœud de terminaison IPSec)** : nœud de terminaison IPSec associé au réseau distant. Ce champ s'affiche uniquement si vous allouez la bande passante par emplacement de calcul.
- **ECMP** :indique si vous avez activé **EMCP Load Balancing (Équilibrage de charge ECMP)** sur cette connexion au réseau distant.
- **Config Status (État de la configuration)** : état de votre dernière transmission de configuration au service. Si vous avez effectué une modification localement et que vous n'avez pas encore transmis la configuration au cloud, l'état indique **Out of sync (Désynchronisé)**. Passez la souris sur l'indicateur d'état pour obtenir des informations plus détaillées. Après avoir validé et transmis la configuration vers Prisma Access, l'état de configuration passe à **In sync (Synchronisé)**.
- **BGP Status (État BGP)** : affiche des informations sur l'état BGP entre le pare-feu ou le routeur à l'emplacement de réseau distant et Prisma Access. Bien que vous puissiez voir temporairement l'état passer par les différents états BGP (**Idle (Inactif)**, **Active (Actif)**, **Open send (Envoi ouvert)**, **Open pend (Attente ouverte)**, **Open confirm (Confirmation ouverte)**, le plus souvent, l'état BGP indique :
  - **Connect (Connecter)** : le routeur à l'emplacement de réseau distant tente d'établir la relation de l'homologue BGP avec Prisma Access.
  - **Established (Établi)** : la relation de l'homologue BGP a été établie.

    Ce champ indiquera également si la connexion BGP est dans un état d'erreur :
  - **Warning (Avertissement)** : il n'y a pas eu de mise à jour de l'état BGP depuis plus de huit minutes. Cela peut indiquer une panne du pare-feu.

 ©2025 Palo Alto Networks, Inc.

- **Error (Erreur)** : l'état BGP est inconnu.
- **Tunnel Status (État du tunnel)** :état de fonctionnement de la connexion entre Prisma Access et le réseau distant.

Onglet **Statistics (Statistiques)** :

- **Location (Emplacement)** : emplacement où votre réseau distant est déployé.
- **Remote Peer (Homologue distant)** : emplacement de l'entreprise vers lequel ce réseau distant configure un tunnel IPSec.
- **Ingress Bandwidth (Mbps) (Bande passante d'entrée (Mbit/s))** : bande passante de l'emplacement de réseau distant à Prisma Access.

  Pour les champs Ingress Bandwidth (Bande passante d'entrée), Ingress Peak Bandwidth (Bande passante maximale d'entrée), Egress Bandwidth (Bande passante de sortie) et Egress Peak Bandwidth (Bande passante maximale de sortie), lorsque la consommation de bande passante sur un réseau distant dépasse 80 % de la bande passante allouée, les nombres s'affichent en rouge.
- **Ingress Peak Bandwidth (Mbps) (Bande passante maximale d'entrée (Mbit/s))**: charge maximale de l'emplacement de réseau distant vers le service cloud.
- **Egress Bandwidth (Mbps) (Bande passante de sortie (Mbit/s))** : bande passante de Prisma Access vers l'emplacement de réseau distant.
- **Egress Peak Bandwidth (Mbps) (Bande passante maximale de sortie (Mbit/s))** : charge maximale de Prisma Access vers l'emplacement de réseau distant.

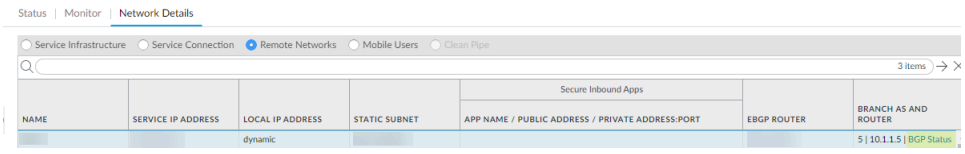
Pour trouver des statistiques sur les emplacements de la région, sélectionnez **Bandwidth Usage (Utilisation de la bande passante)**.

Sélectionnez la coche correspondant à un emplacement pour voir l'utilisation détaillée de la bande passante. Pour les déploiements qui allouent la bande passante par emplacement de calcul, sélectionnez un nœud de terminaison IPSec pour afficher les statistiques de ce nœud. Prisma Access utilise la norme du 95e percentile pour collecter des statistiques, qui suivent la bande passante à l'utilisation maximale et ignorent les 5 % supérieurs des pics d'utilisation et des grandes rafales.

Vérifier l'état BGP de la connexion à distance

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

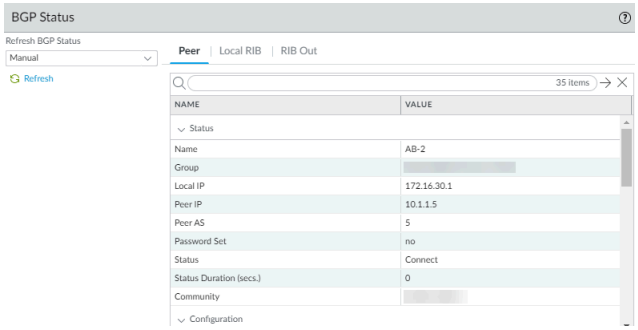
Si vous avez configuré BGP, vous pouvez vérifier son état en sélectionnant **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Remote Networks (Réseaux distants)** > **BGP Status (État BGP)**.



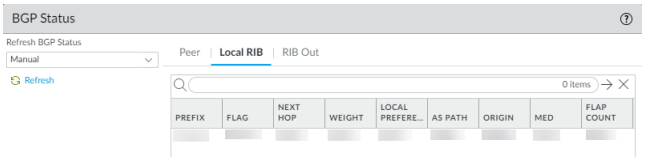
 ©2025 Palo Alto Networks, Inc.

La boîte de dialogue BGP Status (État BGP) s'affiche. Ce tableau fournit les informations suivantes :

- **Peer (Homologue)** : informations de routage pour l'homologue BGP, y compris l'état, le nombre total d'itinéraires, la configuration, les statistiques et les compteurs d'exécution. Le nombre total d'itinéraires s'affiche dans la zone **bgpAfiIpv4-unicast Counters (Compteurs bgpAfiIpv4-unicast)**, dans les champs **Incoming Total (Total entrant)** et **Outgoing Total (Total sortant)**.



- **Local RIB (RIB locale)** : informations de routage reçues de différents homologues et stockées dans la base d'informations de routage (RIB).



- **RIB Out (Sortie de RIB)** : informations de routage que Prisma Access publie auprès de ses homologues par le biais de messages de mise à jour BGP. Reportez-vous à la section Comment BGP annonce les pools d'adresses IP des utilisateurs mobiles pour les connexions aux services et les connexions au réseau distant pour obtenir un exemple de ce tableau et pour plus d'informations sur la façon dont BGP utilise le pool d'adresses IP que vous créez pour les utilisateurs mobiles.

 ©2025 Palo Alto Networks, Inc.

Configurer un réseau distant et une connexion aux services connectés via un lien WAN

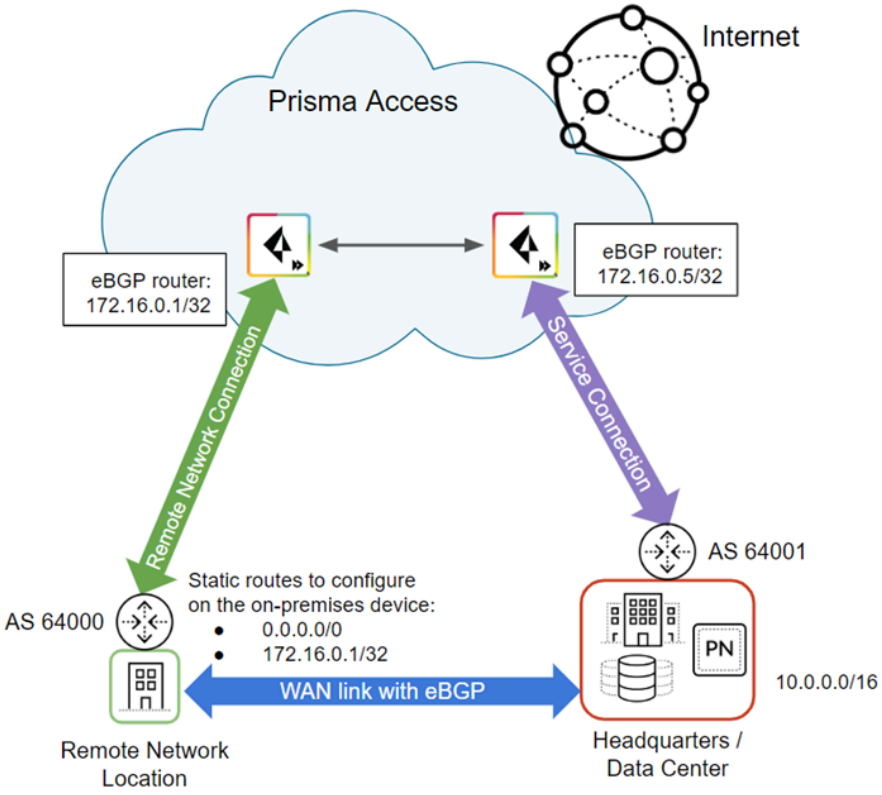
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Si vous avez un déploiement où un ou plusieurs emplacements réseau distants et un siège ou un centre de données avec une connexion aux services sont directement connectés via un lien WAN, pour garantir un routage optimal (avec eBGP), vous devez effectuer les actions suivantes :

- Ajoutez un itinéraire statique à l'adresse du routeur eBGP. En plus de l'itinéraire par défaut qui envoie tout le trafic à Prisma Access, vous devez ajouter un itinéraire statique localement sur le périphérique ou le routeur compatible IPSec sur le ou les réseaux distants.
- Filtrez les itinéraires publiés à partir du périphérique ou du routeur compatible IPSec au siège vers les homologues eBGP situés à d'autres emplacements directement connectés. Il est recommandé de configurer le routeur BGP au siège pour qu'il ne publie que les itinéraires que vous souhaitez autoriser sur le lien WAN. Vous vous assurez que le routeur eBGP au siège ne publie pas les itinéraires à partir desquels il apprend de Prisma Access vers d'autres emplacements de réseau distants sécurisés par Prisma Access. Dans cet exemple, le routeur eBGP du siège publie uniquement les itinéraires que les employés de la succursale devront connecter aux serveurs (sous-réseaux) du siège.

L'illustration suivante montre une entreprise de vente au détail avec deux chemins d'accès aux serveurs à l'emplacement du siège. L'un est un lien WAN qui fournit une connectivité directe aux employés accédant aux serveurs du siège, et l'autre chemin sécurise le trafic généré par d'autres utilisateurs à cet emplacement. Par exemple, le trafic généré par les clients qui accèdent au site Web du détaillant via le Wi-Fi ou qui utilisent le kiosque de la succursale pour vérifier les stocks. Ce trafic est envoyé via le tunnel vers le réseau distant, puis vers le siège.

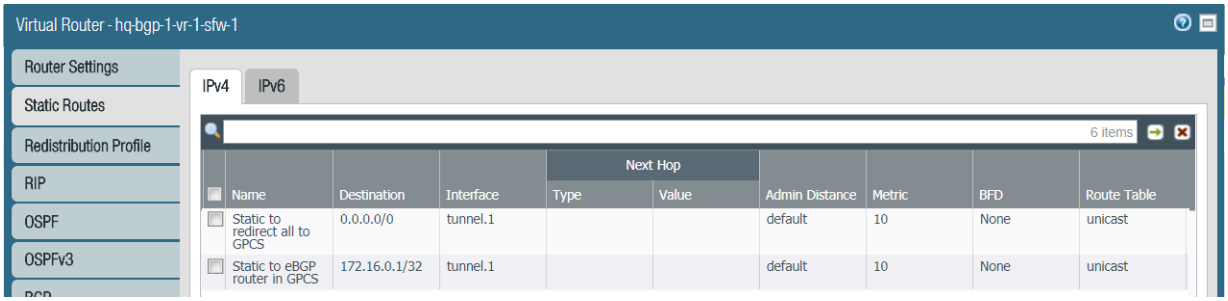
 ©2025 Palo Alto Networks, Inc.



Pour configurer cette configuration, créez une connexion au réseau distant et créez une connexion aux services pour intégrer le réseau distant et les emplacements du siège. Les détails ci-dessous montrent comment configurer la configuration du routeur à chaque emplacement pour assurer un routage optimal :

STEP 1 | Ajoutez les itinéraires statiques sur votre routeur ou votre périphérique IPSec local à l'emplacement du réseau distant.

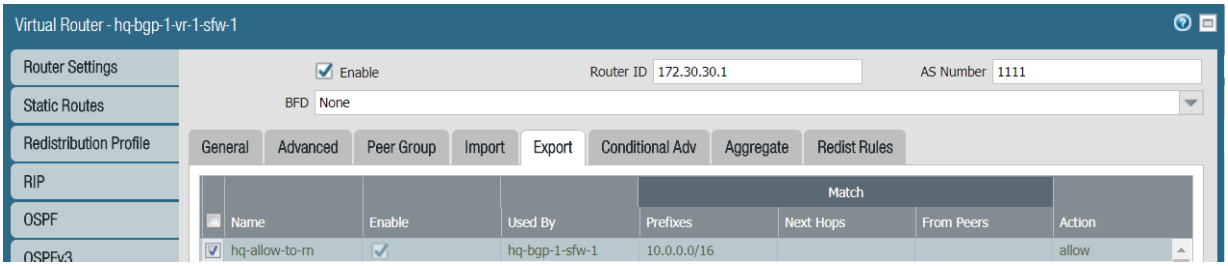
Si vous disposez d'un pare-feu Palo Alto Networks à la périphérie du lien WAN, sur **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** > **Static Routes (Itinéraires statiques)**, cliquez sur **Add (Ajouter)** pour ajouter les itinéraires statiques :



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configurez les itinéraires que vous souhaitez publier sur un autre emplacement directement connecté via le lien WAN.

Dans cet exemple, vous devez configurer l'itinéraire sur l'emplacement au siège. Si vous disposez d'un pare-feu Palo Alto Networks local à la périphérie du lien WAN, vous pouvez configurer la redistribution des itinéraires et les itinéraires BGP sur lesquels exporter sur **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** > **BGP**.



 ©2025 Palo Alto Networks, Inc.

QoS pour les réseaux distants

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version : 3.0 Préféré

Nouveaux Prisma Access déploiements de bande passante embarquée pour les réseaux distants par emplacement de calcul. Pour utiliser la QoS avec des réseaux distants, vous devez activer ou désactiver la QoS et spécifier la bande passante garantie au niveau de l'emplacement de calcul. Toutefois, vous pouvez toujours personnaliser la QoS et la bande passante garantie à un niveau par emplacement en personnalisant la bande passante par site.

Prisma Access divise la bande passante de l'emplacement de calcul à l'aide de *Nœuds de terminaison IPSec*. Chaque nœud de terminaison IPSec peut vous fournir une bande passante maximale de 1 000 Mbit/s. Si vous allouez plus de 1 000 Mbit/s de bande passante à un emplacement de calcul, Prisma Access vous fournit des nœuds de terminaison IPSec supplémentaires.

- Strata Cloud Manager
- Panorama

QoS pour les réseaux distants (Strata Cloud Manager)

Utilisez la QoS pour hiérarchiser le trafic critique dans vos réseaux distants et pour définir des bandes passantes maximales et garanties pour les sites de réseaux distants dans un emplacement de calcul.

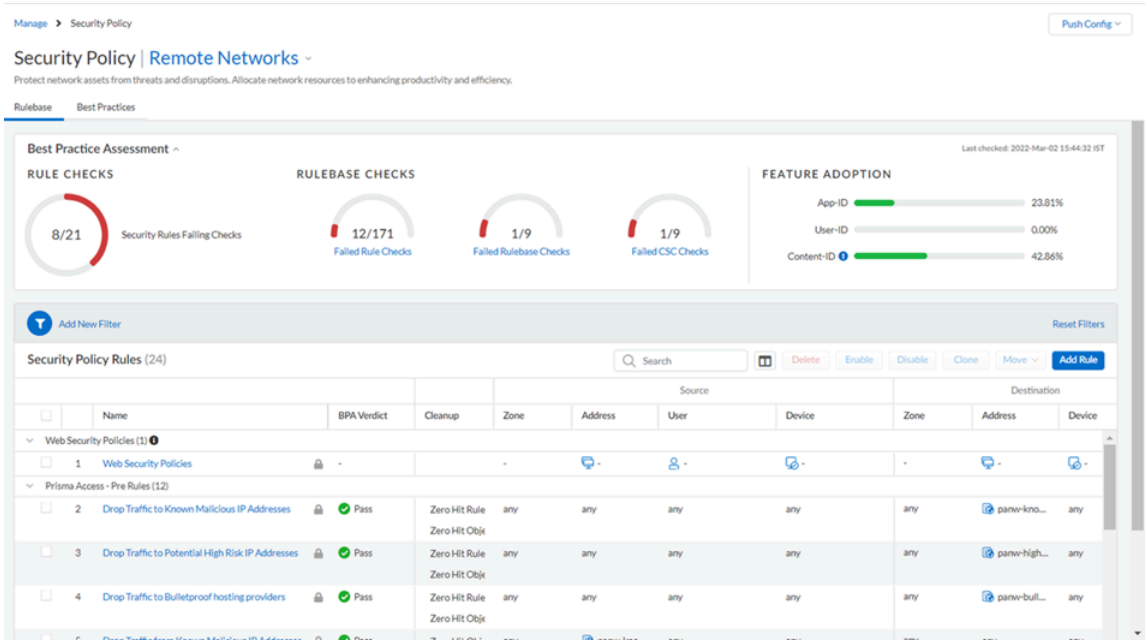
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Marquez le trafic pour lequel vous souhaitez recevoir un traitement QoS.

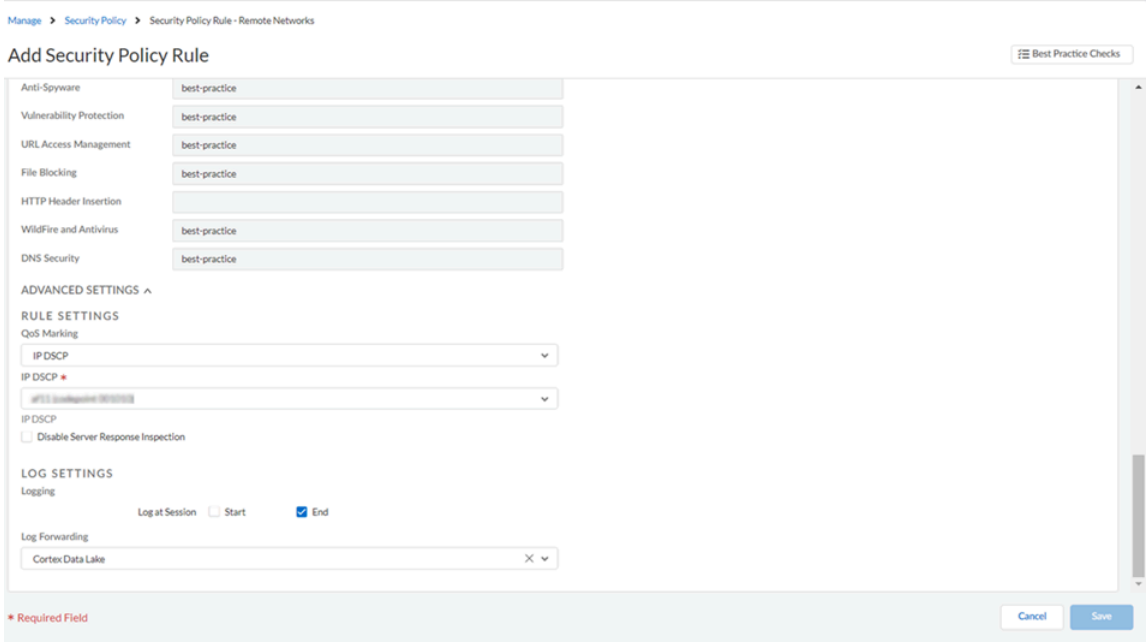
1. Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)**.

   Assurez-vous que vous créez la politique pour les réseaux distants.

2. Cliquez sur **Add Rule (Ajouter une règle)**.



3. Marquez le trafic entrant en attribuant une valeur DSCP dans **Advanced Settings (Paramètres avancés)** et enregistrez la politique.

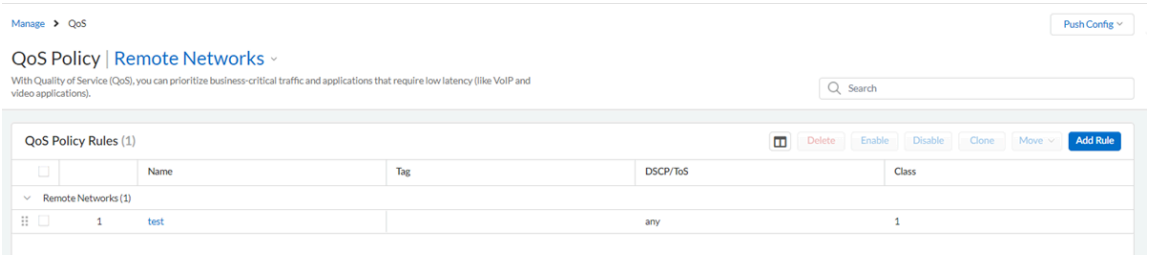


 ©2025 Palo Alto Networks, Inc.

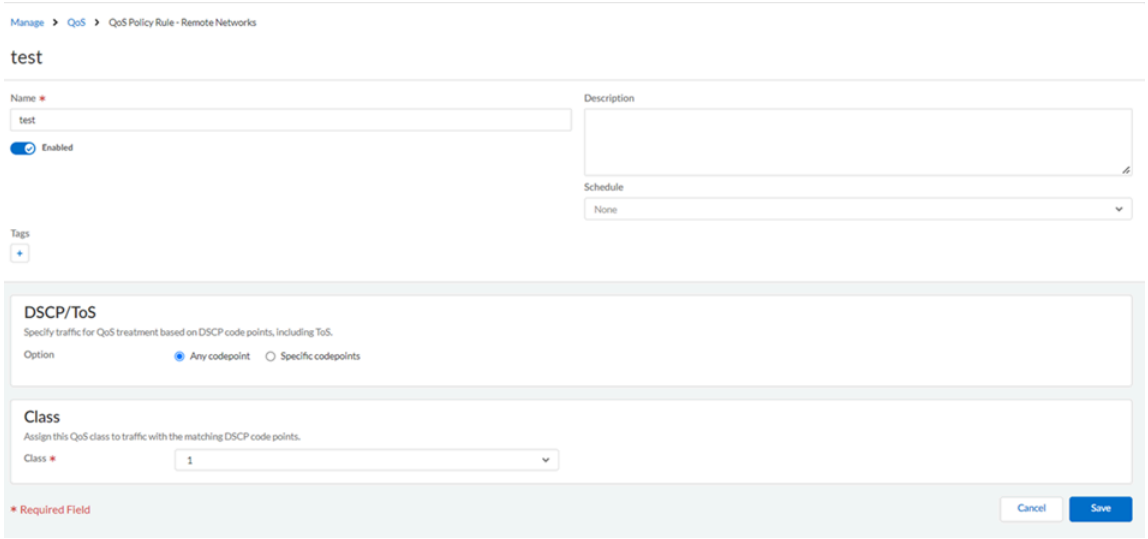
STEP 2 | Ajoutez une ou plusieurs règles de politique QoS.

Vous utilisez des politiques QoS pour lier le marquage DSCP à l'une des huit classes disponibles. Vous allez définir le traitement qu'une classe QoS reçoit dans les étapes suivantes. La classe QoS détermine la priorité et la bande passante du trafic correspondant à la règle de politique QoS.

1. Sélectionnez **Monitor (Surveiller)** > **Network Services (Services réseau)** > **QoS**.
2. Cliquez sur **Add Rule (Ajouter une règle)**.



3. Entrez des valeurs et enregistrez la politique.



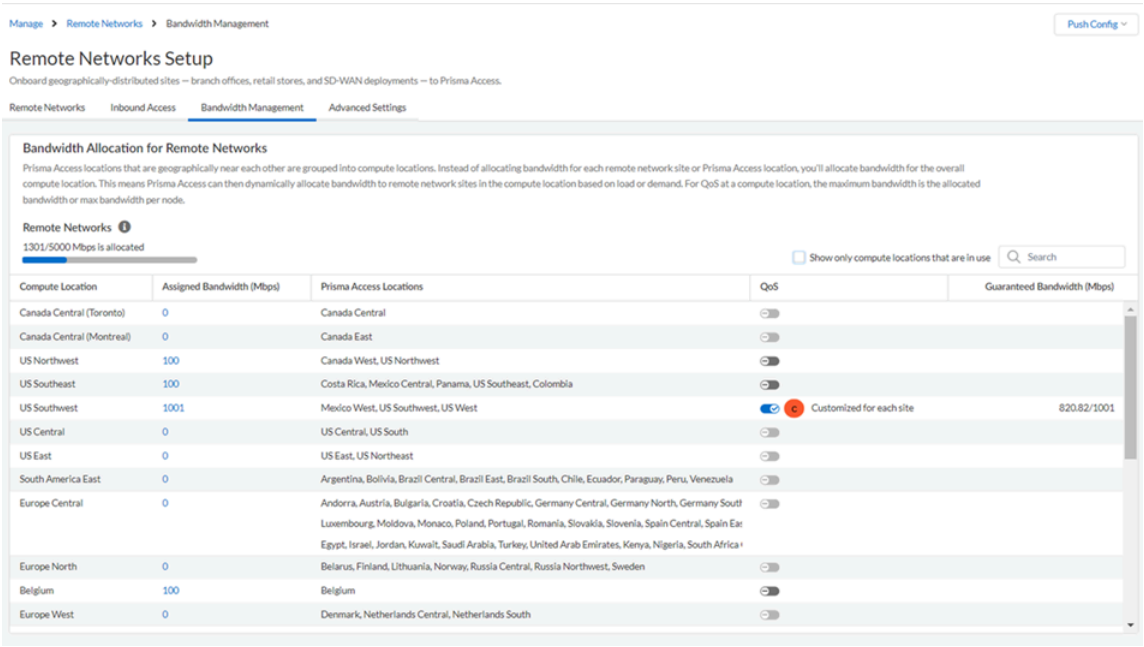
 ©2025 Palo Alto Networks, Inc.

STEP 3 | Activez la QoS pour vos emplacements de réseaux distants.

1. Sélectionnez **Manage (Gérer)** > **Service Setup (Configuration du service)** > **Remote Networks (Réseaux distants)** > **Bandwidth Management (Gestion de la bande passante)**.
2. Déterminez les emplacements Prisma Access où vous souhaitez déployer la QoS. Trouvez ensuite l'emplacement de calcul qui correspond à chaque emplacement Prisma Access.

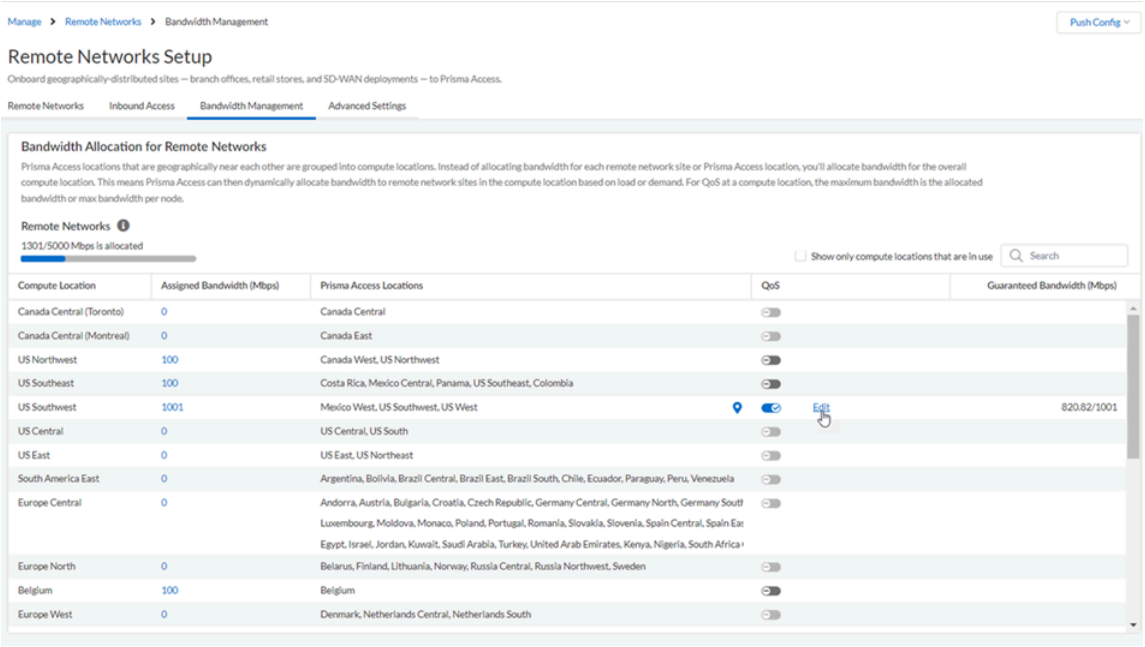
   Chaque emplacement Prisma Access est la bande passante allouée à partir de son emplacement de calcul, et vous devez connaître le nom de l'emplacement de calcul pour les emplacements où vous souhaitez allouer la QoS.
3. Activez la QoS au niveau d'un emplacement de calcul dans la colonne **QoS**.

   Quels que soient les paramètres que vous entrez, ils s'appliquent à tous les emplacements qui correspondent à cet emplacement de calcul.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Cliquez sur **Edit (Modifier)** pour modifier les paramètres QoS de l'emplacement de calcul.



1. Sélectionnez le rapport de bande passante garantie, qui est un rapport basé sur l'ensemble de la bande passante allouée pour l'emplacement de calcul.

   Par exemple, si vous avez alloué une bande passante de 1 001 Mbit/s pour l'emplacement de calcul du sud-ouest des États-Unis et que vous entrez un **Guaranteed Bandwidth Ratio (Rapport de bande passante garantie)** de 82 %, la bande passante garantie pour cet emplacement de calcul est de 820,82 Mbit/s.

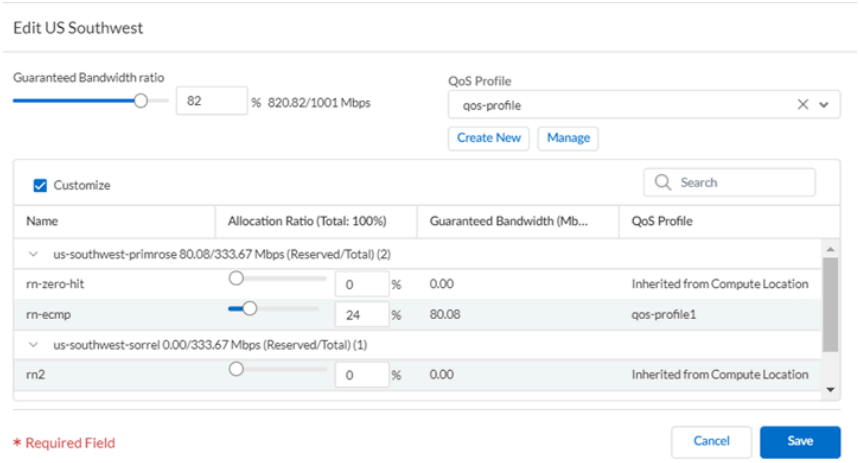
   Par défaut, chaque réseau distant reçoit un pourcentage égal au nombre de connexions. Par exemple, avec 4 connexions dans un emplacement de calcul et une bande passante totale garantie de 820,82 Mbit/s, chaque emplacement reçoit 25 % de cette bande passante, soit 205,2 Mbit/s.

   Si la licence ADEM alimentée par AIOps est activée, la licence est activée automatiquement pour tous les emplacements de calcul.
2. Cliquez sur **Create New (Créer nouveau)** pour créer un profil QoS ou sur **Manage (Gérer)** pour gérer un profil QoS existant.

   Vous utilisez des profils QoS pour façonner le trafic au point de sortie.
3. (Facultatif) Personnalisez les paramètres QoS pour les sites de réseaux distants dans un emplacement de calcul. Si vous avez plusieurs réseaux distants par emplacement de calcul et que vous souhaitez modifier le rapport de bande passante ou le profil QoS de

 ©2025 Palo Alto Networks, Inc.

chaque réseau distant, sélectionnez **Customize (Personnaliser)** et modifiez le rapport d'allocation de bande passante, le profil QoS ou les deux.



*Si vous sélectionnez **Customize (Personnaliser)**, puis intégrez des réseaux distants supplémentaires dans le même nœud de terminaison IPSec, les sites nouvellement intégrés reçoivent un rapport d'allocation de 0 et vous devez rééquilibrer manuellement le rapport d'allocation entre les sites existants et le site nouvellement intégré.*

STEP 5 | Cliquez sur **Save (Enregistrer)** pour enregistrer les modifications.

STEP 6 | Cliquez sur **Push (Appliquer)** pour appliquer les configurations.

QoS pour les réseaux distants (Panorama)

Configurez la qualité de service dans Prisma Access en effectuant la tâche suivante.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Ajoutez une ou plusieurs règles de politique de sécurité pour les réseaux distants et les utilisateurs mobiles afin de marquer le trafic entrant pour la QoS.

Vous utilisez ces politiques pour faire correspondre un flux de trafic et lui attribuer une valeur DSCP sélectionnée.

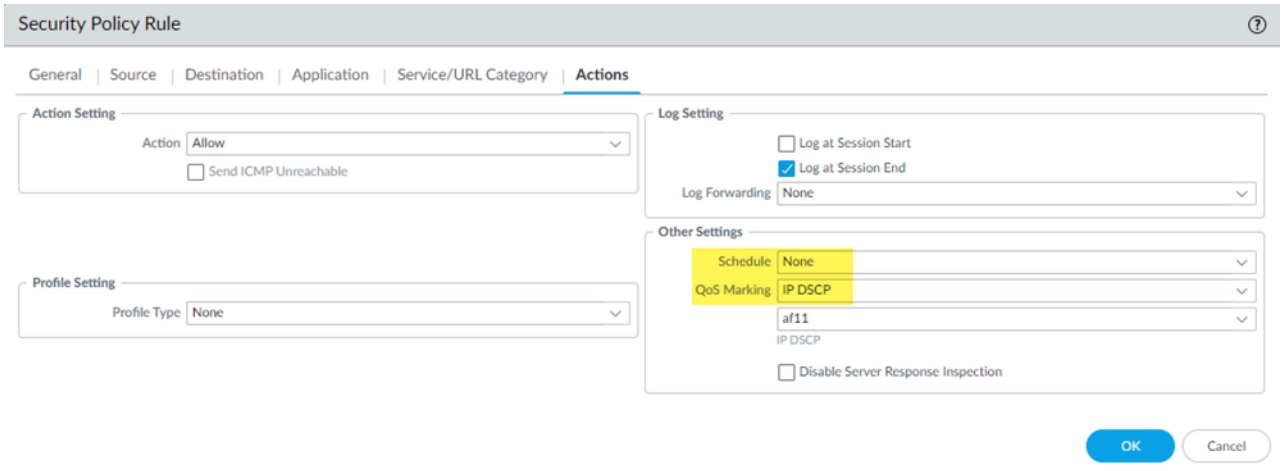
1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Pré-règles)**.

   Vous pouvez également sélectionner **Policies (Politiques)** > **Security (Sécurité)** > **Post Rules (Post-règles)** pour ajouter une règle au bas de l'ordre des règles qui est évaluée après une pré-règle.

   *Assurez-vous de sélectionner le bon **Device Group (Groupe de périphériques)**. Pour créer une règle de sécurité pour un réseau distant, sélectionnez le groupe de périphériques pour le réseau distant (par exemple, **Remote_Network_Device_Group**). Pour les utilisateurs mobiles, sélectionnez le groupe de périphériques pour les utilisateurs mobiles (par exemple, **Mobile_User_Device_Group**).*
2. Cliquez sur **Add (Ajouter)** pour ajouter une règle de politique de sécurité.
3. Donnez un **Name (Nom)** à la règle.
4. Définissez les critères de correspondance des champs source ou de destination du paquet.

   Reportez-vous à la section Créer une règle de politique de sécurité pour plus de détails.
5. Cliquez sur **Actions**, puis sélectionnez un **QoS Marking (Marquage QoS)** pour **IP DSCP** ou **IP Precedence (Priorité IP)**.
6. Entrez la valeur QoS sous forme binaire ou sélectionnez-la dans la liste déroulante.

   La capture d'écran suivante montre une règle de politique de sécurité qui correspond au trafic marqué d'une valeur **IP DSCP** de **af11**.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Ajoutez une ou plusieurs règles de politique QoS.

Vous utilisez des politiques QoS pour lier le marquage DSCP à l'une des huit classes disponibles. Vous utiliserez ces classes ultérieurement lorsque vous créerez un ou plusieurs profils QoS.

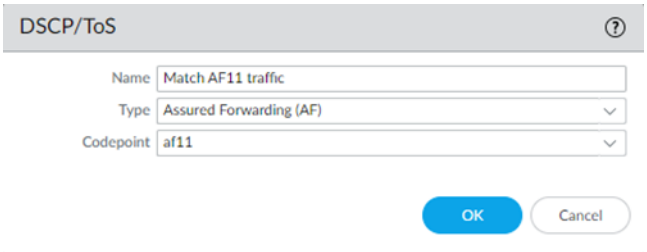
1. Sélectionnez **Policies (Politiques)** > **QoS** > **Pre Rules (Pré-règles)**.

   Vous pouvez également utiliser les post-règles (**Policies (Politiques)** > **QoS** > **Post Rules (Post-règles)**) pour ajouter une règle au bas de l'ordre des règles qui est évaluée après une pré-règle.

   Les connexions aux services ne prennent pas en charge les post-règles QoS. Utilisez les pré-règles uniquement avec les connexions aux services.

   Assurez-vous de sélectionner le bon **Device Group (Groupe de périphériques)** pour la connexion aux services (par exemple, **Service_Conn_Device_Group**) ou à une connexion au réseau distant (par exemple, **Remote_Network_Device_Group**). Si une règle d'un groupe de périphériques partagés a défini des valeurs autres que celles des zones de paramètres **General (Général)**, **DSCP/ToS** et **Other (Autre)**, Prisma Access n'applique pas la règle sur la connexion au réseau distant et aux services.
2. Cliquez sur **Add (Ajouter)** pour ajouter une règle de politique QoS.
3. Cliquez sur **General (Général)** et entrez un nom pour la règle de politique.
4. Cliquez sur l'onglet **DSCP/ToS**, puis cliquez sur **Codepoints (Points de code)** et **Add (Ajouter)** pour ajouter un ou plusieurs nouveaux points de code.

   Pour les déploiements Clean Pipe, vous pouvez spécifier des paramètres QoS supplémentaires dans la politique, tels que la source, la destination ou l'application.
5. Spécifiez un **Name (Nom)** pour la règle DSCP/ToS, puis sélectionnez un **Type** et un **Codepoint (Point de code)**.



   Vous pouvez également conserver la valeur par défaut (**Any (Indifférent)**) pour permettre à la politique de s'adapter au trafic, quelle que soit la valeur DSCP (Differentiated

 ©2025 Palo Alto Networks, Inc.

Services Code Point) ou la priorité IP/le type de service (Type of Service, ToS) défini pour le trafic.

6. Cliquez sur l'onglet **Other Settings (Autres paramètres)**, puis choisissez la **Class (Classe)** de la QoS à attribuer à la règle.

   Vous définissez les caractéristiques de classe dans le profil QoS.

7. Cliquez sur **OK**.



STEP 3 | Créez un ou plusieurs profils QoS pour façonner le trafic QoS à la sortie des connexions aux services et des connexions au réseau distant.

Vous utilisez des profils pour façonner le trafic au point de sortie en définissant des classes QoS et en leur attribuant une bande passante. Vous devez sélectionner un profil QoS existant ou créer un nouveau profil QoS lorsque vous activez la QoS pour Prisma Access.

1. Sélectionnez le bon modèle de profil que vous souhaitez créer (**Remote_Network_Template** ou **Service_Conn_Template**). Ensuite, sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **QoS Profile (Profil QoS)** et
2. cliquez sur **Add (Ajouter)** pour ajouter un profil.
3. Saisissez un **Name (Nom)** de profil.
4. Définissez les limites de bande passante globale de la règle de profil QoS :
   - Entrez une **Egress Max (Sortie max)** qui représente le débit maximal (en Mbit/s) du trafic quittant la connexion aux services ou la connexion au réseau distant.
     - Pour les connexions aux services, spécifiez un nombre allant jusqu'à 1 Gbit/s (1 000 Mbit/s).

       N'entrez pas un nombre supérieur à 1 Gbit/s. Prisma Access calcule la bande passante de connexion aux services par tunnel IPSec de connexion aux services et non de manière cumulative sur plusieurs tunnels.
   - Pour les connexions au réseau distant, entrez la valeur **0**.
   - Entrez une valeur de bande passante **Egress Guaranteed (Sortie garantie)** qui correspond à la bande passante garantie pour ce profil (en Mbit/s).
     - Pour les connexions aux services, entrez une bande passante **Egress Guaranteed (Sortie garantie)** qui correspond à la bande passante garantie pour ce profil (en Mbit/s).

       L'acheminement du trafic dépassant la valeur de Egress Guaranteed (Sortie garantie) se fait dans la mesure du possible et n'est pas garanti. La bande

 ©2025 Palo Alto Networks, Inc.

passante qui est garantie, mais qui n'est pas utilisée demeure disponible pour l'acheminement de l'ensemble du trafic.

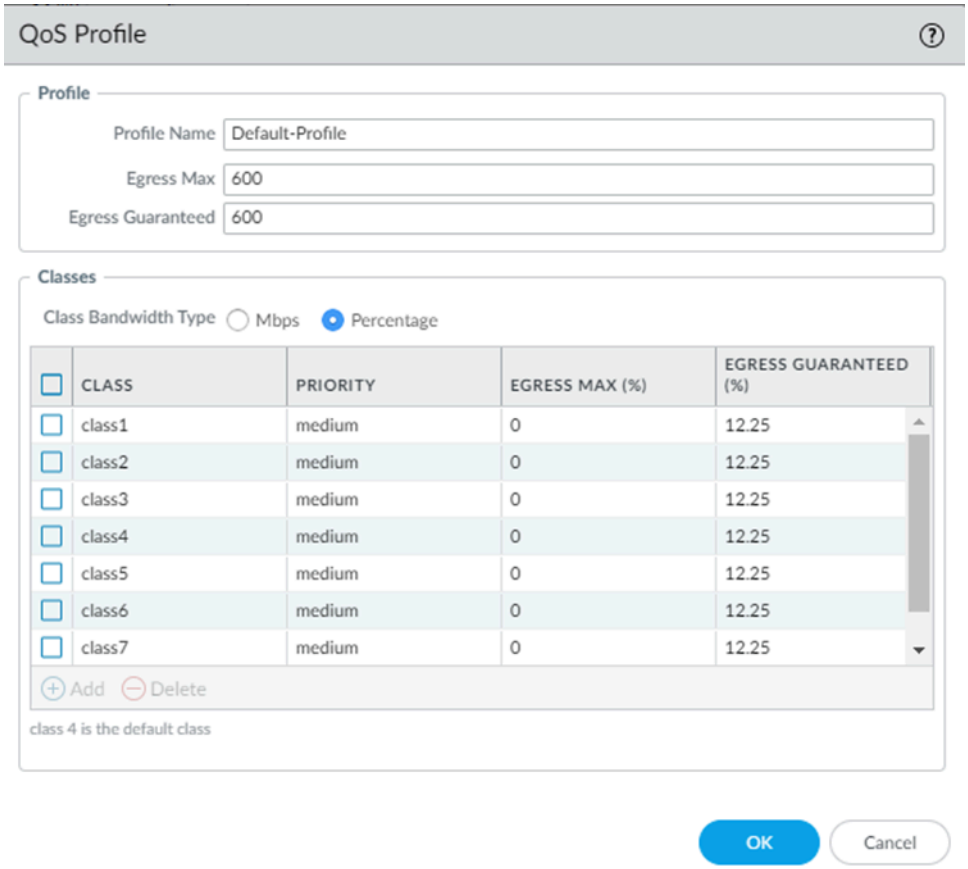
- Pour les connexions au réseau distant, entrez la valeur **0**.

5. Dans la section Classes, cliquez sur **Add (Ajouter)** pour ajouter une ou plusieurs classes et spécifiez comment marquer jusqu'à huit classes QoS individuelles.
   - Pour les profils QoS utilisés par des réseaux distants qui allouent de la bande passante en fonction de l'emplacement de calcul, modifiez le **Class Bandwidth Type (Type de bande passante de classe)** sur **Percentage (Pourcentage)** et entrez des pourcentages pour les valeurs **Egress Max (Sortie max)** et **Egress Guaranteed (Sortie garantie)** que vous entrez dans cette zone.
   - Pour les profils QoS utilisés par les connexions aux services ou par les réseaux distants qui allouent la bande passante par emplacement, spécifiez le type de **Mbps (Mbit/s)**.
   - Sélectionnez la **Priority (Priorité)** de la classe (**real-time (temps réel)**, **high (élevée)**, **medium (moyenne)** ou **low (basse)**).
   - Entrez la valeur **Egress Max (Sortie max)** pour le trafic attribué à chaque classe QoS que vous créez.
     - Pour les réseaux distants qui allouent de la bande passante en fonction de l'emplacement de calcul, entrez **0**.
     - Pour les profils QoS basés sur la bande passante (utilisés par les connexions aux services ou les réseaux distants qui allouent la bande passante par emplacement), entrez une valeur en Mbit/s. La valeur Egress Max (Sortie max) d'une classe QoS doit être inférieure ou égale à la valeur Egress Max (Sortie max) du profil QoS.
   - Entrez le pourcentage de **Egress Guaranteed (Sortie garantie)** ou la bande passante en Mbit/s pour chaque classe QoS. Pour les profils QoS pour les réseaux distants, entrez un pourcentage.

     La bande passante garantie attribuée à une classe n'est pas réservée à cette classe ; la bande passante qui n'est pas utilisée demeure disponible pour l'acheminement de tout trafic. Lorsqu'une classe de trafic dépasse la bande passante de sortie garantie, Prisma Access gère ce trafic dans la mesure du possible.

 ©2025 Palo Alto Networks, Inc.

- Entrez un **Class Bandwidth Type (Type de bande passante de classe)** pour le profil.



6. Cliquez sur **OK**.

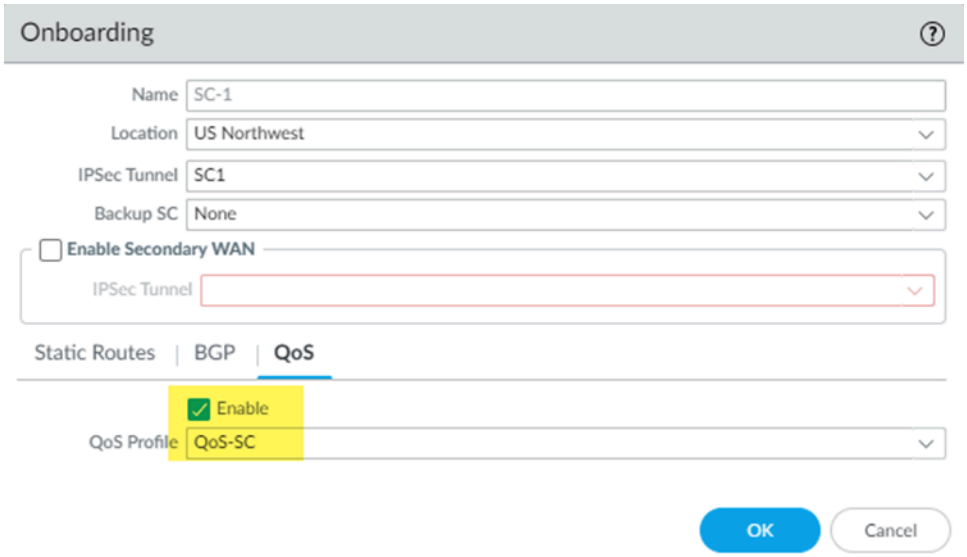
STEP 4 | (Connexions aux services uniquement) Activez la QoS pour la connexion aux services et appliquez le profil QoS à la connexion.

1. Activez la QoS en sélectionnant **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)**, en sélectionnant **Connection Name (Nom de connexion)**, en cliquant sur l'onglet **QoS**, puis cliquez sur **Enable (Activer)** pour activer la QoS.

   Si vous allouez la bande passante de votre réseau distant par Prisma Access Réseaux distants plutôt que par emplacement de calcul, configurez la QoS de la même manière que vous effectuez les connexions de service. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**, sélectionnez l'hypertexte pour le **Nom (Name)** d'une connexion au réseau distant, cliquez sur l'onglet **QoS** et sur **Enable (Activer)** pour activer la QoS. Si vous allouez la bande passante en fonction de l'emplacement de calcul (méthode par défaut), passez à l'étape 5 pour configurer la QoS pour les réseaux distants.

 ©2025 Palo Alto Networks, Inc.

2. Sélectionnez un profil QoS et cliquez sur **OK**.



STEP 5 | (Déploiements de réseaux distants qui allouent la bande passante en fonction de l'emplacement de calcul uniquement) Activez la QoS pour vos emplacements de réseaux distants.

1. Déterminez les emplacements Prisma Access où vous souhaitez déployer la QoS. Recherchez ensuite l'emplacement de calcul qui correspond à chaque emplacement.

   Chaque emplacement reçoit de la bande passante allouée à partir de son emplacement de calcul, et vous devez connaître le nom de l'emplacement de calcul pour les emplacements où vous souhaitez allouer la QoS. Pour obtenir la liste des mappages d'emplacement à emplacement de calcul, consultez Prisma Access emplacementsou sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** > **Aggregate Bandwidth (Bande passante agrégée)** et cliquez sur l'icône d'engrenage. Les mappages s'affichent dans les colonnes **Compute Location (Emplacement de calcul)** et **Prisma Access Location (Emplacement Prisma Access)**.
2. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** > **Settings (Paramètres)**, cliquez sur l'icône d'engrenage pour modifier les paramètres, puis sélectionnez **QoS**.
3. Cliquez sur **Enable QoS (Activer la QoS)** au niveau de l'emplacement de calcul.

   Quels que soient les paramètres que vous entrez, ils s'appliquent à tous les emplacements qui correspondent à cet emplacement de calcul.

 ©2025 Palo Alto Networks, Inc.

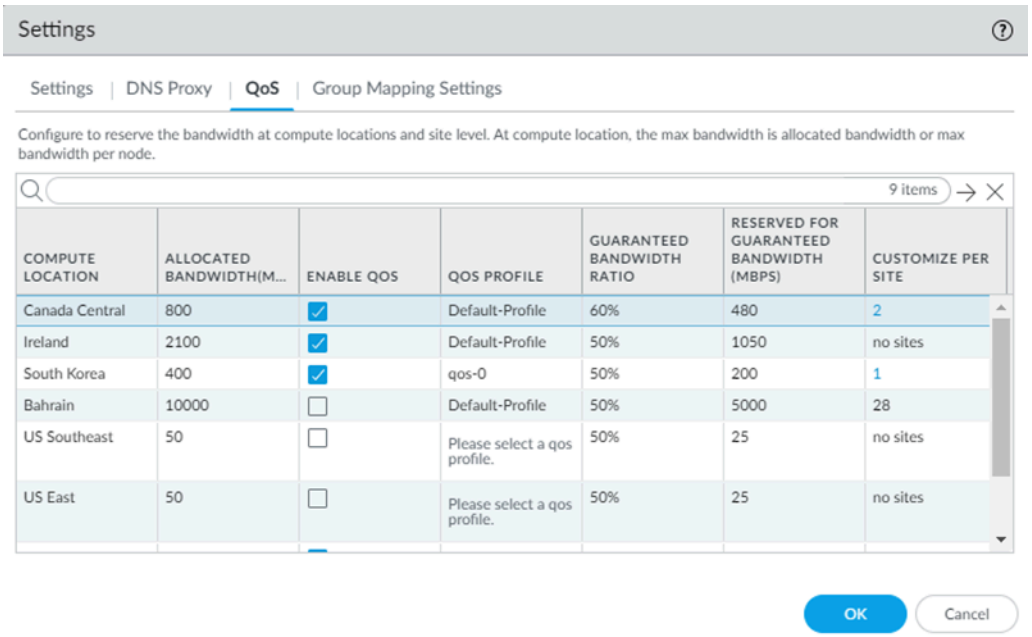
4. Entrez **QoS Profile (Profil QoS)**, **Guaranteed Bandwidth Ratio (Rapport de bande passante garantie)**et **Reserved for Guaranteed Bandwidth (Mbps) (Réservée pour la bande passante garantie (Mbit/s))**.

   - Entrez le **QoS Profile (Profil QoS)** à utiliser avec cet emplacement de calcul.

     Si vous souhaitez utiliser des profils QoS différents pour chaque réseau distant, utilisez **Customize Per Site (Personnaliser par site)** comme décrit dans une étape ultérieure.
   - Entrez le rapport de bande passante garantie, qui est un rapport basé sur l'ensemble de la bande passante allouée pour l'emplacement de calcul.

     Par exemple, si vous avez alloué une bande passante de 800 Mbit/s pour l'emplacement de calcul du centre du Canada et que vous entrez un **Guaranteed Bandwidth Ratio (Rapport de bande passante garantie)** de **60% (60 %)**, la bande passante garantie pour cet emplacement de calcul est de 480 Mbit/s.
   - Entrez la quantité de bande passante **Reserved for Guaranteed Bandwidth (Mbps) (Réservée pour la bande passante garantie (Mbit/s))** pour le profil QoS et l'emplacement de calcul que vous avez sélectionnés.

   La capture d'écran suivante montre la QoS activée pour les emplacements de calcul du centre du Canada, de l'Irlande et de la Corée du Sud.



5. (Facultatif) Si vous disposez de plusieurs connexions au réseau distant par emplacement de calcul et que vous souhaitez modifier le rapport de bande passante ou le profil QoS pour chaque emplacement, intégrez vos emplacements de réseaux distants.

 ©2025 Palo Alto Networks, Inc.

Ensuite, sélectionnez **Customize Per Site (Personnaliser par site)** et modifiez le rapport d'allocation de bande passante, le profil QoS ou les deux.

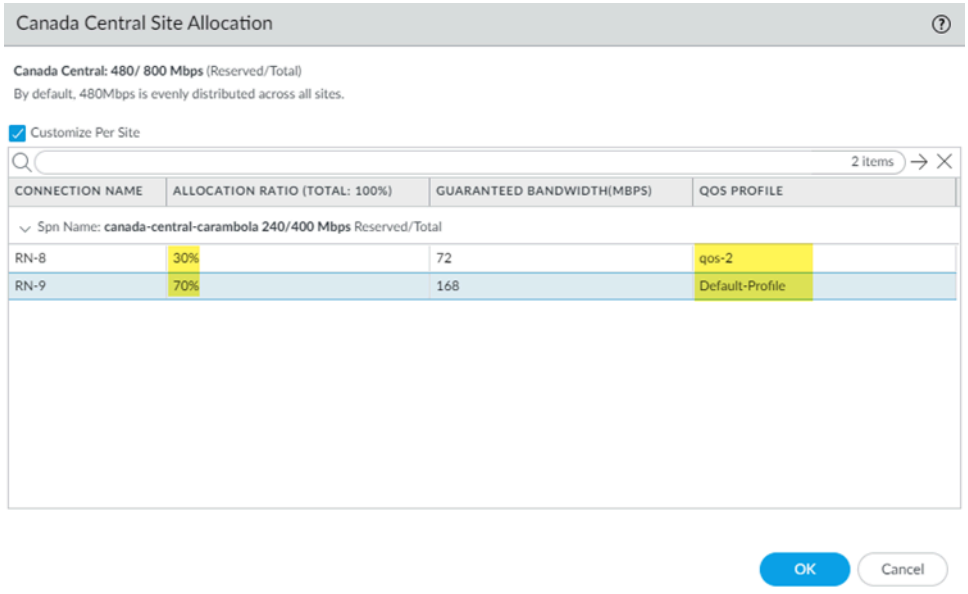
- Pour personnaliser la bande passante garantie, cliquez sur le nombre dans la zone **Customize Per Site (Personnaliser par site)**, sélectionnez **Customize Per Site (Personnaliser par site)** et modifiez le **Allocation Ratio (Rapport d'allocation)**.

  Par défaut, chaque connexion distante reçoit un pourcentage égal au nombre de connexions. Par exemple, avec 4 connexions dans un emplacement de calcul et une bande passante totale garantie de 100 Mbit/s, chaque emplacement reçoit 25 % de cette bande passante, soit 25 Mbit/s.

  *Si vous sélectionnez **Customize Per Site (Personnaliser par site)**, puis intégrez des réseaux distants supplémentaires dans le même nœud de terminaison IPSec, les sites nouvellement intégrés reçoivent un rapport d'allocation de **0** et vous devez rééquilibrer manuellement le rapport d'allocation entre les sites existants et le site nouvellement intégré.*

  *Si vous ne cliquez pas sur **Customize Per Site (Personnaliser par site)**, le pourcentage de bande passante se rééquilibre automatiquement lorsque vous ajoutez des réseaux distants. Par exemple, si vous n'avez pas sélectionné **Customize Per Site (Personnaliser par site)** et avez quatre réseaux distants intégrés, chacun de ces réseaux distants a un rapport d'allocation de 25 %. Si vous ajoutez un cinquième réseau distant, les cinq sites se rééquilibrent et reçoivent une bande passante garantie de 20 %.*

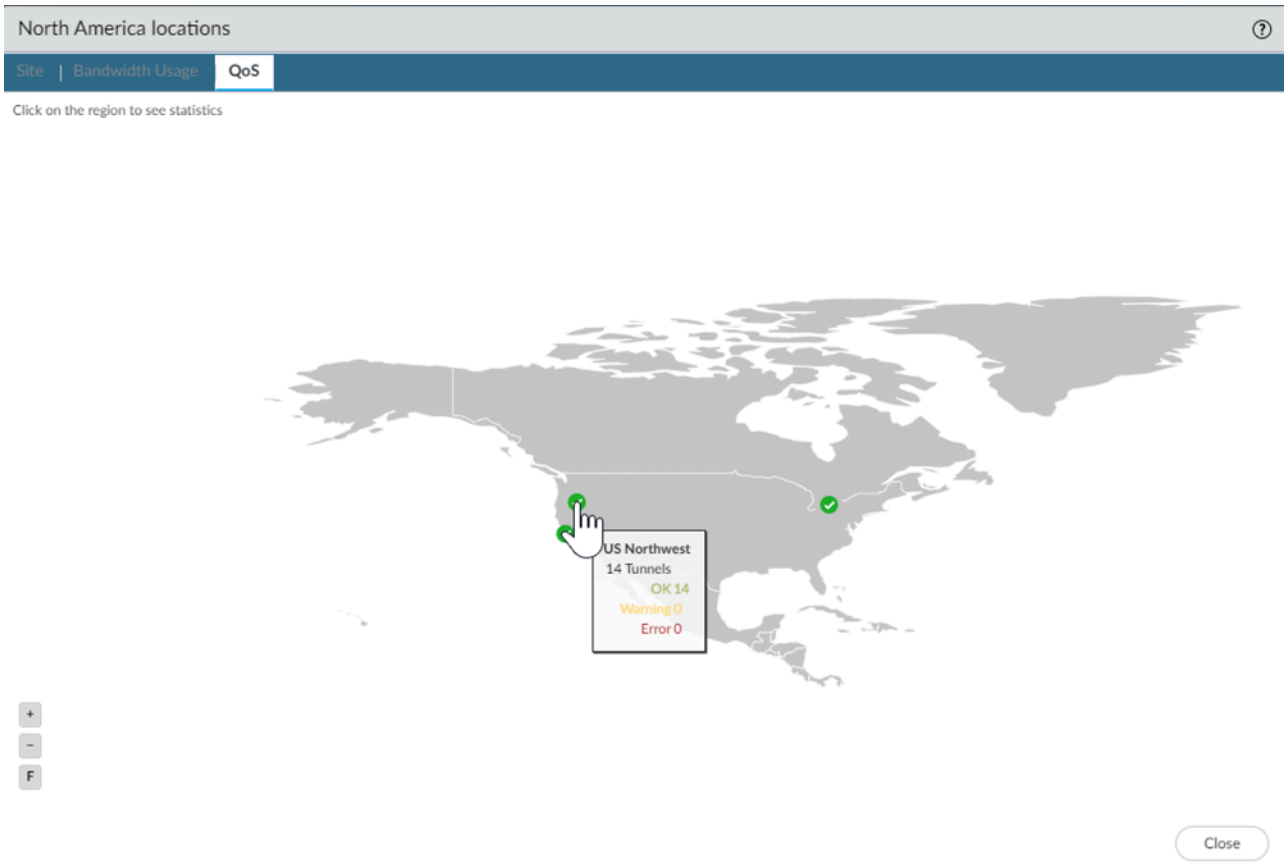
- Si vous souhaitez spécifier un profil QoS au niveau d'un réseau distant, sélectionnez un autre **QoS Profile (Profil QoS)** pour le réseau distant.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | Vérifiez l'état de la QoS.

- Pour les réseaux distants, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Monitor (Surveiller)** > **Remote Networks (Réseaux distants)**, sélectionnez une région sur la carte, sélectionnez **QoS**, puis sélectionnez un emplacement.

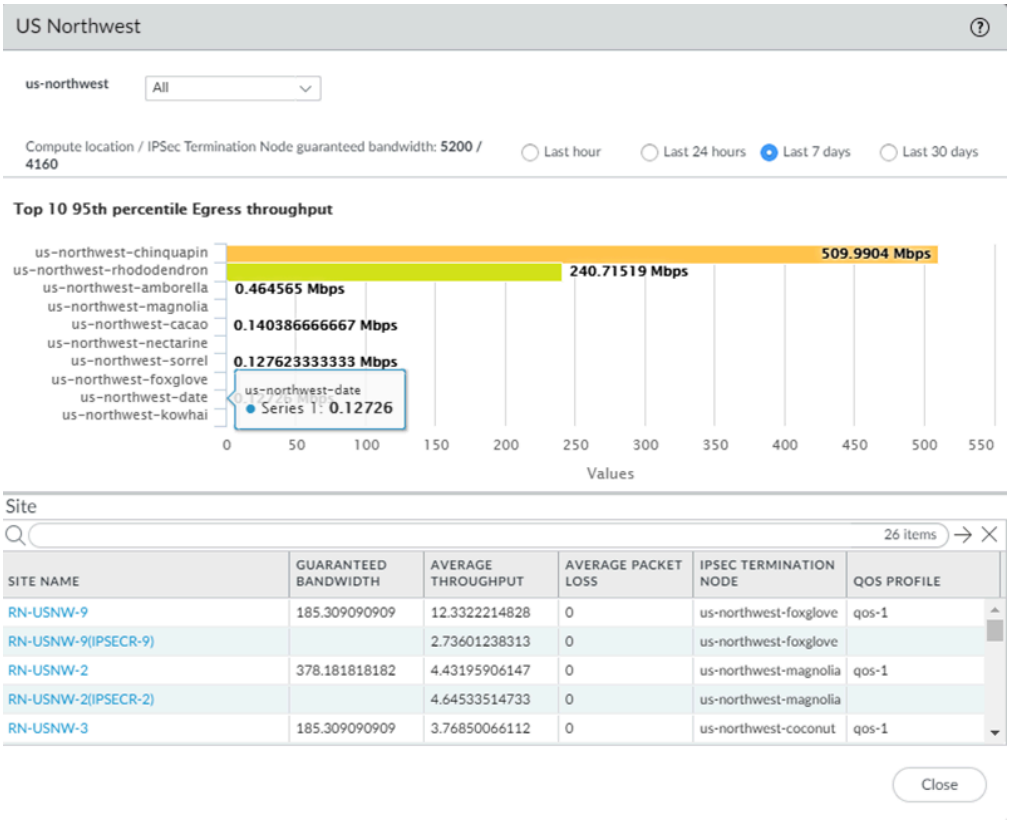


Les statistiques du réseau distant s'affichent pour les 10 nœuds de terminaison IPSec qui ont le débit le plus élevé. Prisma Access utilise la norme du 95e centile pour collecter

 ©2025 Palo Alto Networks, Inc.

des statistiques, qui suit la bande passante lors des pics d'utilisation et ignore les 5 % supérieurs des pics d'utilisation et des grandes rafales.

Sélectionnez la plage horaire (**Last hour (Dernière heure)**, **Last 24 hours (Dernières 24 heures)**, **Last 7 days (7 derniers jours)**ou **Last 30 days (30 derniers jours)**) pour afficher les statistiques de cette période.

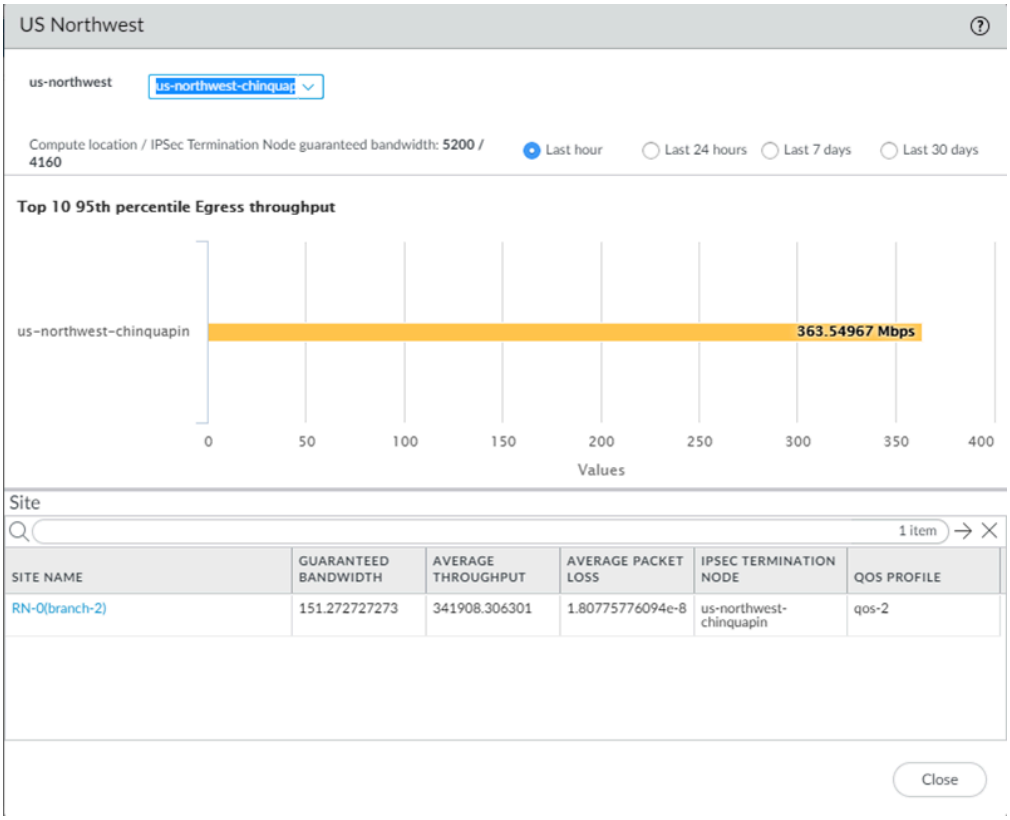


Les réseaux distants avec l'utilisation de la bande passante de sortie la plus élevée s'affichent dans la zone **Site**, ainsi que les statistiques des emplacements de réseaux distants pour les valeurs **Guaranteed Bandwidth (Bande passante garantie)**, **Average Throughput (Débit moyen)**, **Average Packet Loss (Perte moyenne de paquets)**, **IPSec Termination Node (Nœud de terminaison IPSec)** et **QoS Profile (Profil QoS)** utilisées par le réseau distant. Vous pouvez également cliquer sur **Search (Rechercher)** pour rechercher un lieu.

Pour afficher les réseaux distants associés à un nœud de terminaison IPSec spécifique, modifiez la liste déroulante en haut de la page de **All (Tout)** à un nœud

 ©2025 Palo Alto Networks, Inc.

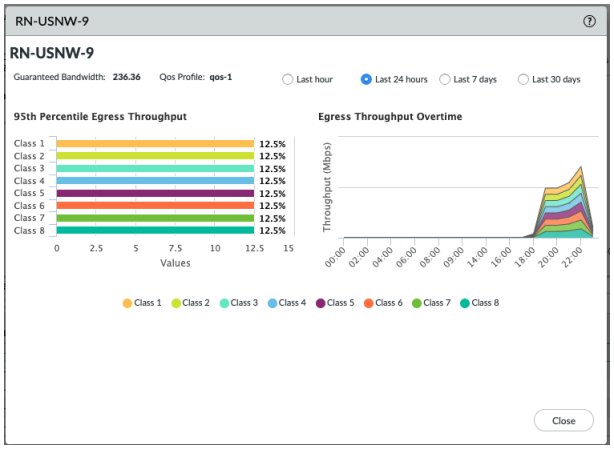
de terminaison IPSec spécifique pour afficher les statistiques de ce nœud de terminaison IPSec et les réseaux distants de ce site.



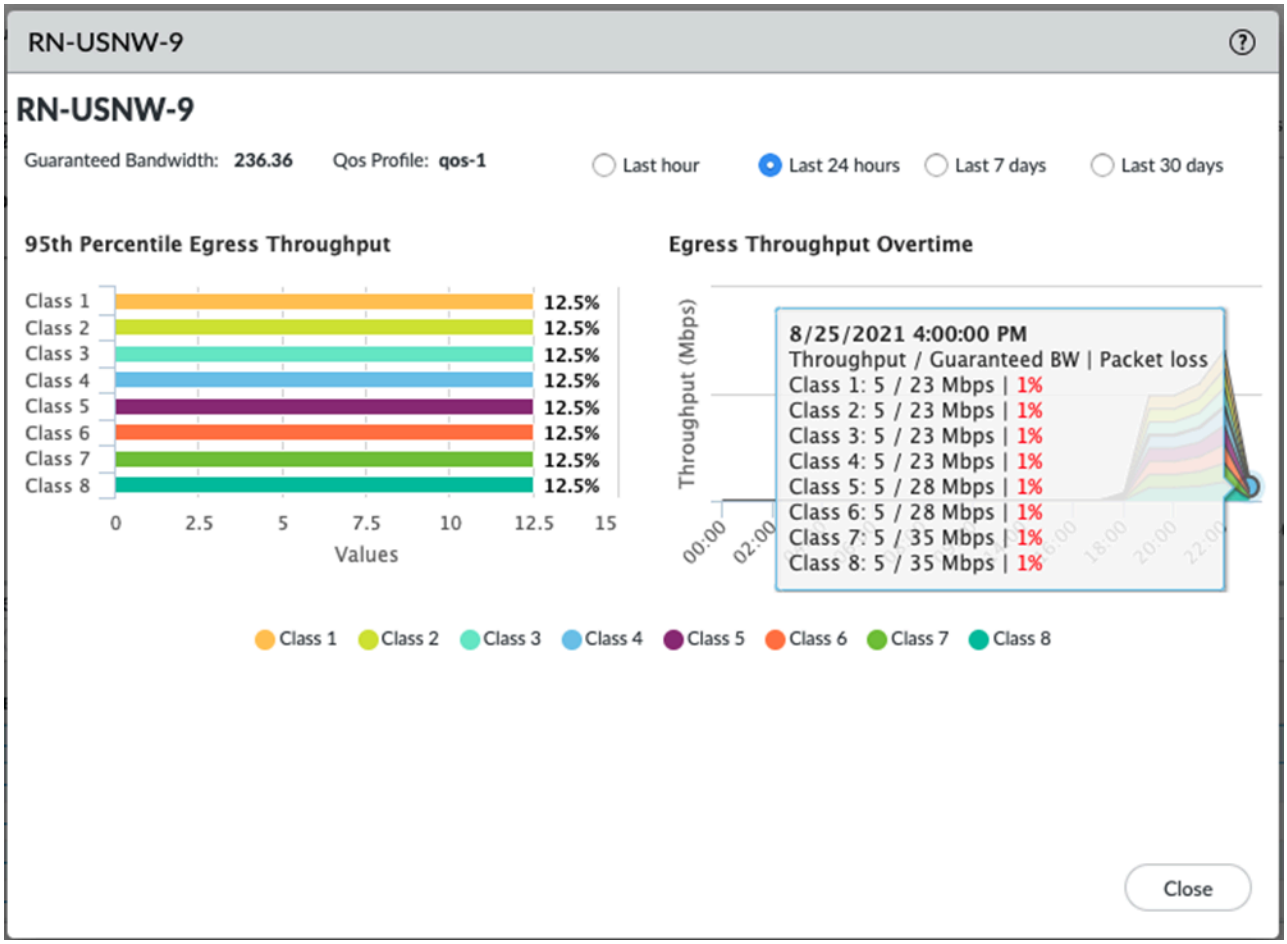
Pour afficher le trafic spécifique d'un site trié par classe QoS, cliquez sur le **Site Name (Nom du site)**. La bande passante garantie, le débit de sortie et le débit dans le temps

 ©2025 Palo Alto Networks, Inc.

s'affichent pour le site du réseau distant. Vous pouvez également trier ces informations sur la dernière heure, les dernières 24 heures, les 7 derniers jours ou les 30 derniers jours.



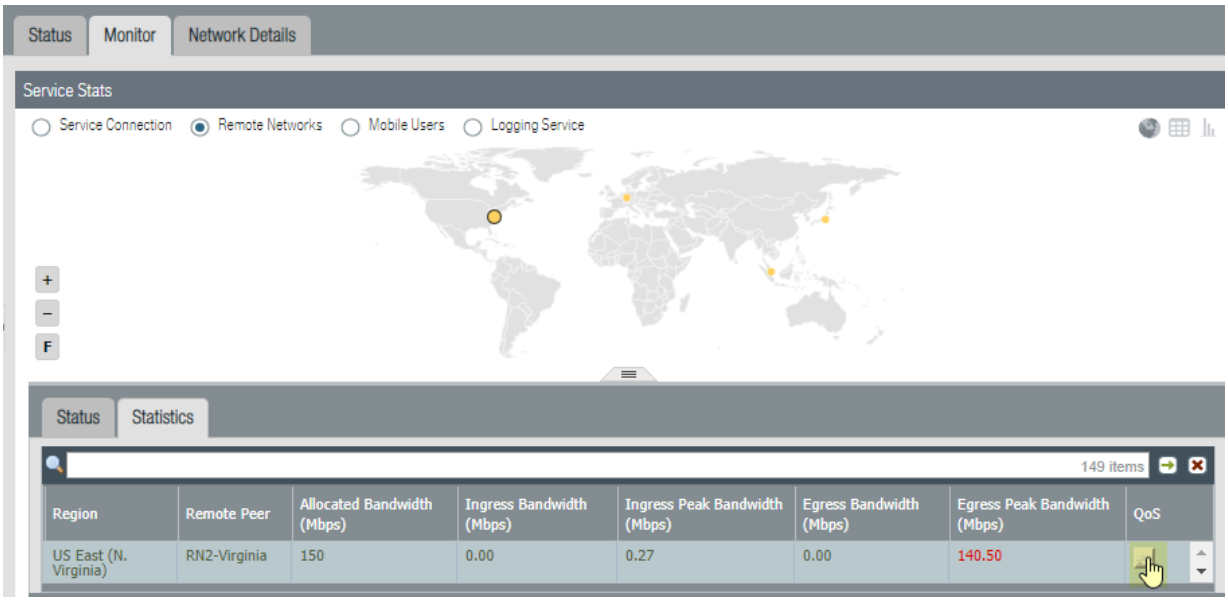
Passez la souris sur le graphique à droite pour obtenir des informations détaillées pour une période de temps spécifique.



- Pour les connexions aux services, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Monitor (Surveiller)** > **Service Connection (Connexion aux services)**, sélectionnez une région, puis cliquez sur **Monitor (Surveiller)** et **Statistics (Statistiques)**.

Cliquez sur **QoS** pour afficher une page avec des statistiques QoS.

 ©2025 Palo Alto Networks, Inc.

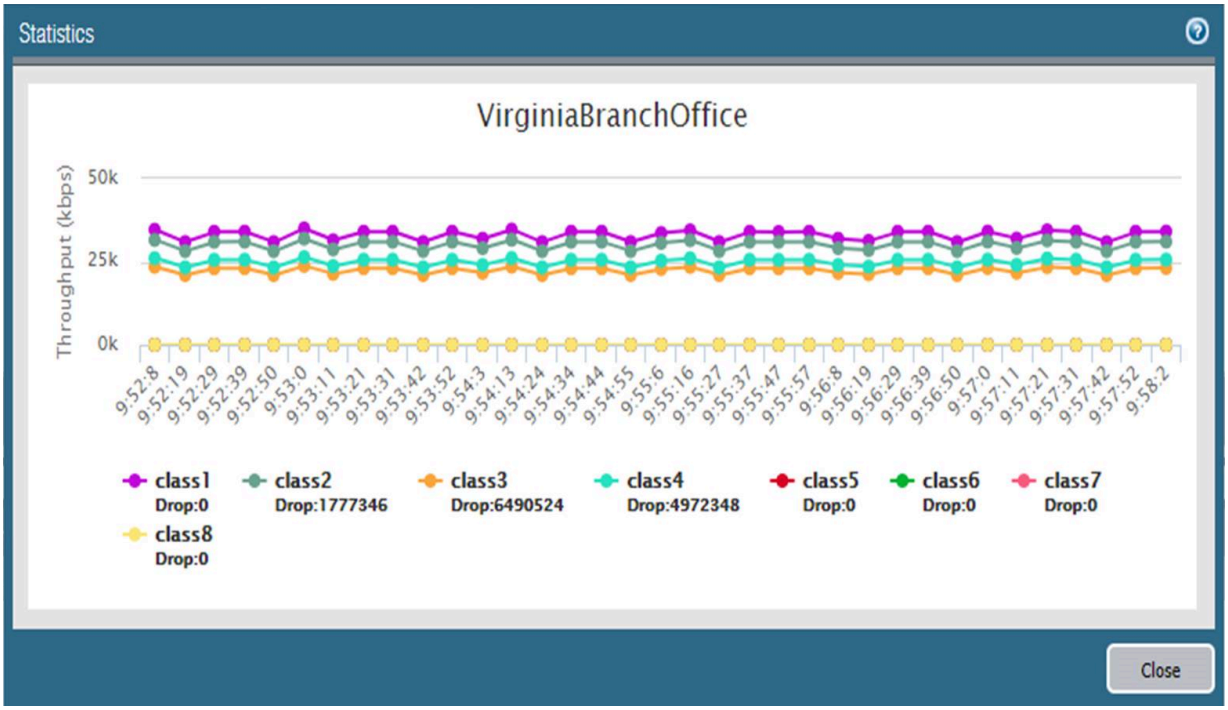


Cette page affiche un graphique avec des statistiques QoS en temps réel et historiques, y compris le nombre de paquets abandonnés par classe. Ce graphique s'affiche uniquement pour les connexions aux services ou les connexions de réseau distant pour lesquelles la QoS est

 ©2025 Palo Alto Networks, Inc.

activée, affiche les cinq dernières minutes de l'activité réseau de la connexion et s'actualise toutes les 10 secondes.

La figure suivante montre le trafic transmis pour les classes 1, 2, 3 et 4. Les données sous la figure montrent le nombre de paquets abandonnés en fonction de la configuration QoS pour les classes 2, 3 et 4.



Modifier la bande passante garantie

Modifier la bande passante garantie

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Si vous disposez de plusieurs emplacements réseau distants associés à un nœud de terminaison IPSec, vous pouvez modifier la bande passante garantie pour chaque site. Dans l'exemple suivant, vous souhaitez que l'emplacement Est du Canada reçoive plus de bande passante que l'emplacement centre du Canada. Pour ce faire, procédez comme suit.

STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** > **Settings (Paramètres)**.

STEP 2 | Cliquez sur l'engrenage pour modifier les paramètres et sélectionnez **QoS**.

STEP 3 | Cliquez sur **Enable QoS (Activer la QoS)**, attribuez un **QoS Profile (Profil QoS)** (**Default-Profile (Profil par défaut)** dans cet exemple) et un **Guaranteed Bandwidth Ratio (Rapport de bande passante garantie)** à l'emplacement de calcul du centre du Canada.

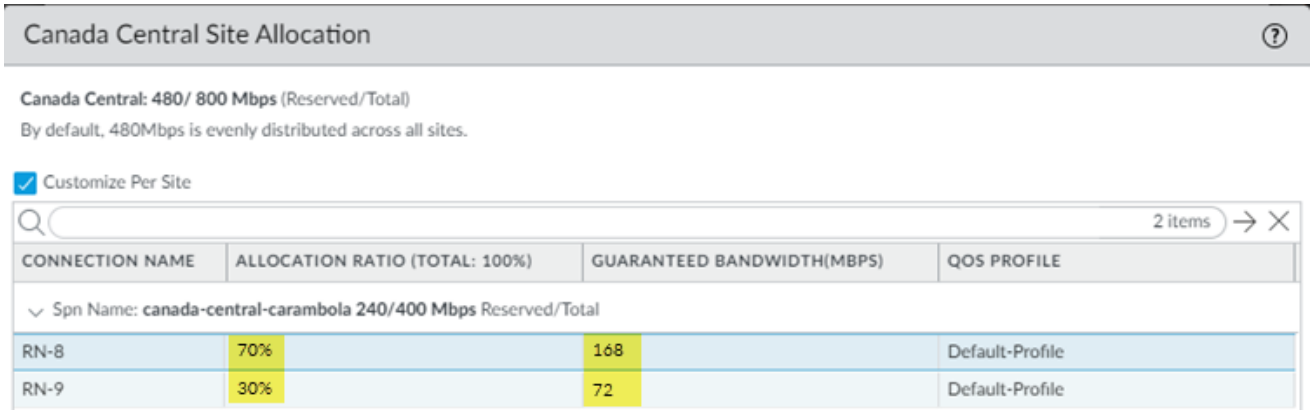
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Sélectionnez **Customize Per Site (Personnaliser par site)**, activez **Customize Per Site (Personnaliser par site)**, puis appliquez un **Allocation Ratio (Rapport d'allocation)** de la bande

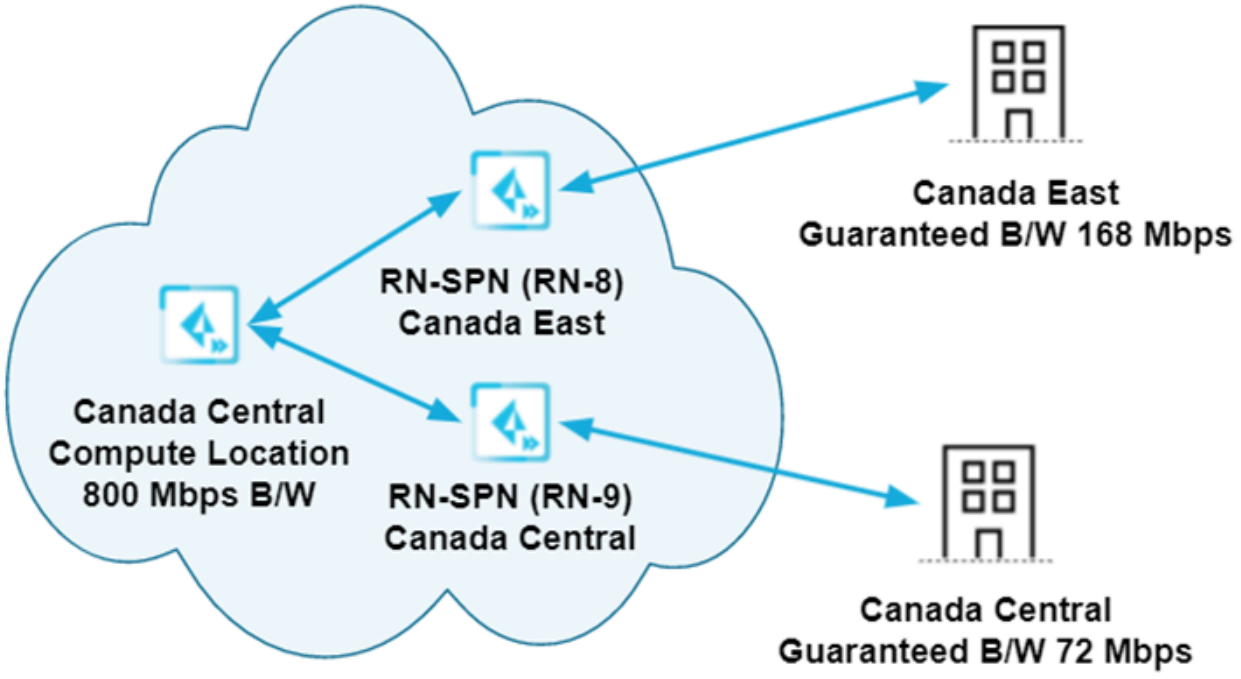
 ©2025 Palo Alto Networks, Inc.

passante plus élevé pour le réseau distant RN-8 (pour l'emplacement Est du Canada) que pour le réseau distant RN-9 (pour l'emplacement du centre Canada).

L'exemple suivant montre un **Allocation Ratio (Rapport d'allocation)** de 70 % pour RN-8 et de 30 % pour RN-9. La **Guaranteed Bandwidth (Mbps) (Bande passante garantie (Mbit/s))** change en conséquence, en affichant les nouvelles quantités de bande passante garantie.



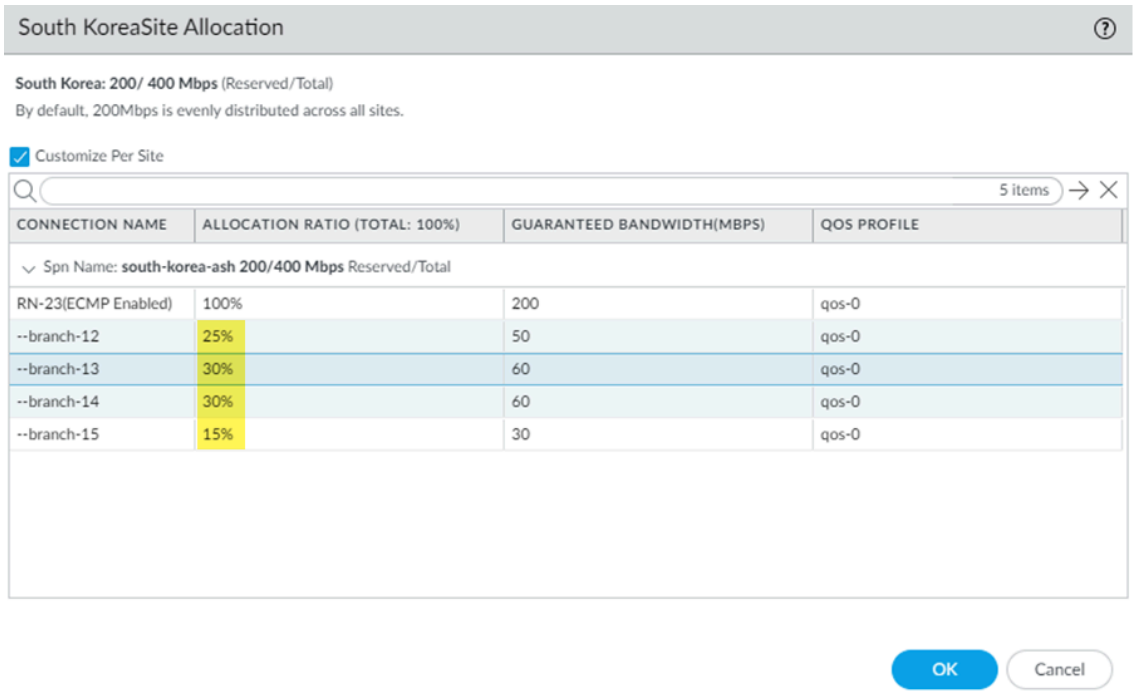
Une fois terminée, votre configuration dispose de l'allocation de bande passante garantie suivante pour les deux sites.



Vous pouvez également attribuer différents profils QoS par emplacement réseau distant. Pour attribuer différents profils, activez l'option **Customize Per Site (Personnaliser par site)** et sélectionnez différents profils QoS pour chaque emplacement réseau distant.

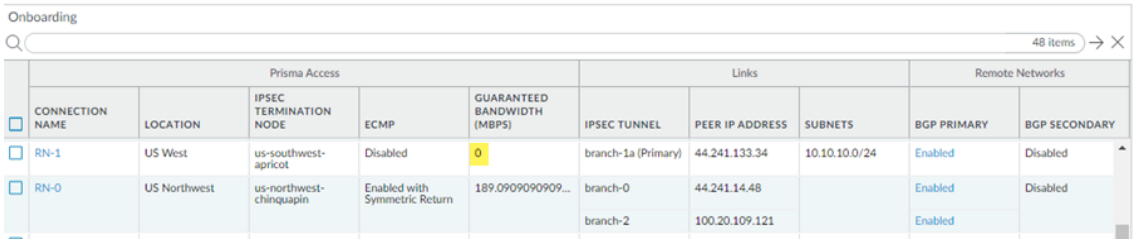
Si vous disposez d'un réseau distant sur lequel ECMP est activé pour utiliser plusieurs tunnels IPSec pour un seul réseau distant, vous pouvez modifier l'option **Allocation Ratio (Rapport d'allocation)** pour les tunnels IPSec que vous utilisez pour cet emplacement réseau distant.

 ©2025 Palo Alto Networks, Inc.



STEP 5 | Enregistrez et validez vos modifications.

Les valeurs de bande passante garantie s'affichent dans la zone **Panorama** > **Cloud Services** > **Status (État)** > **Monitor (Surveiller)** > **Remote Networks (Réseaux distants)** de la zone **Guaranteed Mbps (Mbit/s) garantis)**. Si vous n'avez pas spécifié de bande passante, elle s'affiche comme 0.



 ©2025 Palo Alto Networks, Inc.

Réseaux distants : haute performance

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access *Ceci est une version à disponibilité limitée. Pour activer cette fonctionnalité, contactez votre représentant de compte Palo Alto Networks.*

Avec l'évolution de votre activité et la distribution géographique de vos bureaux, les réseaux distants Prisma Access vous permettent d'intégrer rapidement vos sites de succursales et d'offrir une sécurité optimale à vos utilisateurs. Pour intégrer un site de succursale avec une bande passante élevée, Prisma Access vous fournit un *réseau distant hautes performances*.

Pour intégrer un réseau distant hautes performances, vous spécifiez l'emplacement du site de la succursale et Prisma Access sélectionne l'emplacement le plus proche du site. Vous pouvez éventuellement configurer un emplacement secondaire (de sauvegarde) vers le site pour la redondance et la résilience. Le réseau distant hautes performances utilise une adresse IP de service unique pour chaque tranche de bande passante de 3 Gbits/s, ce qui supprime la complexité de la configuration et de la gestion de plusieurs périphériques IPSec à chaque emplacement distant.

Un emplacement secondaire n'est pas pris en charge pour les déploiements Prisma Access (Managed by Panorama).

Après avoir planifié votre réseau distant hautes performances, vous pouvez commencer le processus de configuration, qui comprend l'intégration du réseau distant hautes performances au Prisma Access et l'activation de la QoS et du routage.

Capacités et lignes directrices des réseaux distants hautes performances

Un réseau distant hautes performances vous offre les capacités de base suivantes :

- Jusqu'à 3 Gbits/s de bande passante agrégée par nœud dans une région de calcul
- Jusqu'à 2 Gbits/s de bande passante par tunnel de réseau distant depuis un site distant
- Jusqu'à 500 succursales distantes par adresse IP de service avec Prisma SD-WAN et déploiements étendus (tiers) de CPE

Lors de la configuration d'un réseau distant hautes performances pour un site de succursale, tenez compte des lignes directrices et des différences suivantes entre les sites et les réseaux distants :

- Emplacements**Prisma Access**—Réseaux distants hautes performances prennent en charge un sous-ensemble d'emplacements Prisma Access.

©2025 Palo Alto Networks, Inc.

- **Qualité de service (QoS)**—Pour les sites de succursale, Prisma Access prend en charge la QoS au niveau de chaque site, et le profil QoS que vous sélectionnez s'applique à l'ensemble du site.
- **Débit d'information validé (CIR)**—Pour sécuriser et valider la quantité de bande passante utilisée par site, spécifiez un CIR. S'il existe plusieurs réseaux distants qui partagent la bande passante dans un emplacement de calcul, le réseau distant hautes performances reçoit au moins la bande passante spécifiée dans le CIR lorsqu'il y a litige avec d'autres sites dans cet emplacement de calcul.
- **Nœuds de terminaison IPSec**—Contrairement aux réseaux distants, vous ne devez pas sélectionner un nœud de terminaison IPSec lors de l'intégration pour les déploiements Prisma Access (Managed by Strata Cloud Manager). Prisma Access équilibre automatiquement la charge des connexions réseau distantes pour maximiser l'allocation de bande passante aux sites.

  Vous devez encore sélectionner un nœud de terminaison IPSec pour les réseaux distants embarqués depuis Panorama.
- **Redondance des tunnels et des emplacements de calcul et tunnels maximum par site**—Un réseau distant hautes performances vous permet de configurer à la fois l'emplacement et la redondance IPSec.
  - Redondance des emplacements (spécifiant un emplacement **Primary (Principal)** dans un emplacement de calcul et spécifiant un emplacement **Secondary (Secondaire)** dans un emplacement de calcul séparé).

    La configuration d'un emplacement secondaire est facultative, et l'emplacement secondaire doit se trouver dans un emplacement de calcul différent de l'emplacement principal.
  - Redondance de tunnel IPSec (spécifiant les tunnels comme **Active/Active (Actif/Actif)** ou **Active/Passive (Actif/Passif)**).

  Ce tableau vous fournit le nombre minimum et maximum d'emplacements par tunnel.

Type de déploiement d'emplacement	Type de déploiement de tunnel	Nombre minimum de tunnels	Nombre maximum de tunnels
Principal uniquement	Actif/Passif	1	2
Principal uniquement	Actif/Actif	2	4
Principal et secondaire	Actif/Passif	2	4
Principal et secondaire	Actif/Actif	4	8

- **Allocation d'adresses IP de service en fonction du type de déploiement**—Le nombre d'adresses IP de service que vous recevez dépend de la configuration de vos réseaux distants hautes performances dans un seul emplacement ou de leur configuration à l'aide de deux emplacements différents dans un déploiement principal et secondaire.
  - Si vous avez configuré votre réseau distant hautes performances dans un seul emplacement sans emplacement secondaire, Prisma Access vous fournit une adresse IP de service unique.

 ©2025 Palo Alto Networks, Inc.

- Si vous configurez la redondance de l'emplacement de calcul dans une configuration principale et secondaire, Prisma Access vous fournit deux adresses IP de service (une pour la configuration principale et une pour la configuration secondaire).

Si vous configurez des tunnels IPSec dans une configuration Active/Passive, Prisma Access vous fournit une adresse IP de service unique pour les deux tunnels (la même qu'une configuration réseau distant Prisma Access standard).

- **Allocation d'adresse IP de service basée sur la bande passante** —Prisma Access vous fournit une adresse IP ou nom de domaine complet unique pour chaque 3 Gbits/s de bande passante dans un emplacement de calcul.
- **Bande passante par emplacement de calcul**–Vous allouez la bande passante par emplacement de calcul de la même façon que pour un réseau distant standard. Vous pouvez planifier et allouer la bande passante avant de commencer la configuration ou lors de la création de réseau distant hautes performances.
- **Prise en charge IPv6**—IPv6 n'est pas pris en charge pour les déploiements de réseaux distants hautes performances.

Utilisez l'une des procédures suivantes pour intégrer vos réseaux distants en fonction de votre type d'allocation de bande passante :

- Prisma Access (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Panorama)

Strata Cloud Manager

Voici comment ajouter un réseau distant hautes performances à l'aide de Strata Cloud Manager.

STEP 1 | Depuis Strata Cloud Manager, allez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Branch Sites (Sites des succursales)**.

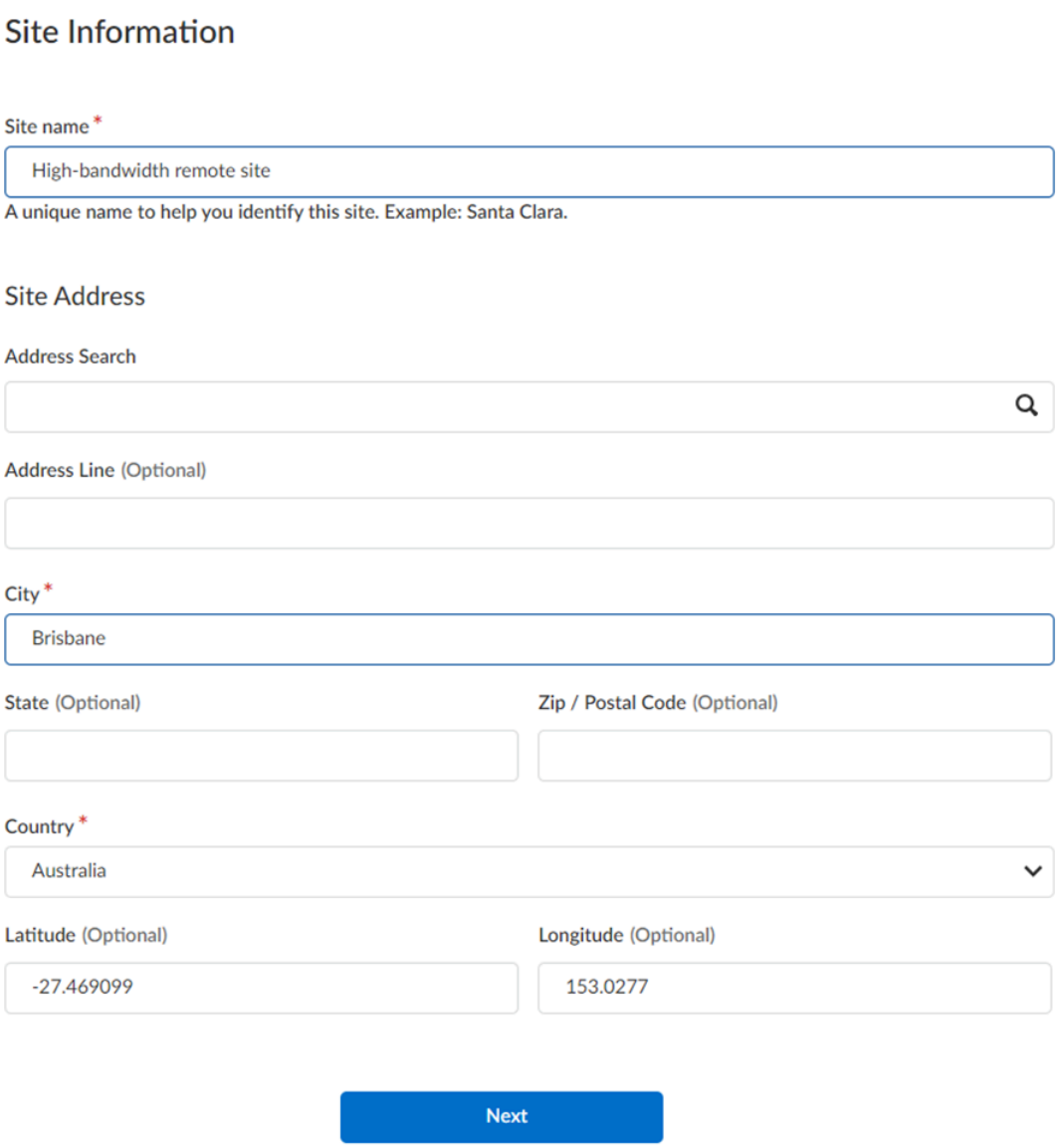
Ce choix indique que le tunnel que vous créez pour les sites des succursales est terminé par votre CPE (un pare-feu de la nouvelle génération de Palo Alto Networks ou un CPE tiers).

STEP 2 | **Add Site (Ajouter un site)** et donner au réseau distant un **Site Name (Nom de site)** descriptif.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Sélectionnez **City (Ville)** et **Country (Pays)** sur le site.

Pour des recherches plus précises, ajoutez une adresse.



STEP 4 | Cliquez sur **Next (Suivant)**.

STEP 5 | Entrez le **QoS CIR (Committed Information Rate) (QoS CIR (Taux d'informations validé))** en Mbps.

Si vous avez plusieurs réseaux distants qui partagent la bande passante dans un emplacement de calcul, et s'il existe un conflit de bande passante avec d'autres sites dans cet emplacement de calcul, le réseau distant hautes performances reçoit au moins la bande passante spécifiée dans le CIR.

Si vous configurez des sites principaux et secondaires, vous spécifiez des régions de calcul différentes et la région secondaire reçoit 20 % du CIR. Par exemple, si vous configurez un CIR

 ©2025 Palo Alto Networks, Inc.

de 100 Mbit/s pour un site, Prisma Access fournit au site principal un CIR de 100 Mbit/s et au site secondaire un CIR de 20 Mbit/s.

Si le CIR est de 500 Mbit/s et si toute la bande passante restante dans l'emplacement de calcul est utilisée par d'autres sites, Prisma Access supprime toute bande passante supérieure à 500 Mbit/s. Toutefois, si d'autres sites n'utilisent pas de bande passante, la bande passante du réseau distant hautes performances peut dépasser 500 Mbit/s jusqu'à la bande passante allouée dans l'emplacement de calcul.

Entrez un CIR minimum de 1 Mbit/s et un maximum de 2 000 Mbit/s. Ne dépassez pas la bande passante spécifiée pour la région de calcul.

STEP 6 | Sélectionnez un **Primary Prisma Access Location (Emplacement d'accès principal à Prisma)**.

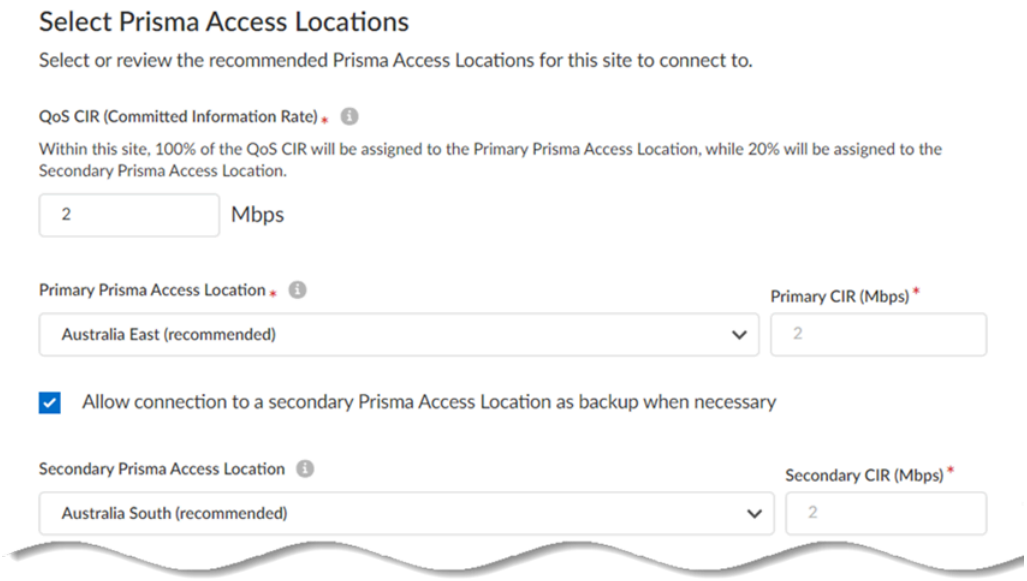
Si plusieurs emplacements sont **Recommended (Recommandés)** dans la liste ; sélectionnez l'emplacement qui convient le mieux à votre déploiement.

STEP 7 | (Facultatif) Pour créer un site secondaire (de sauvegarde), sélectionnez **Allow connection to a secondary Prisma Access Location as backup when necessary (Autoriser la connexion à un emplacement d'accès Prisma secondaire en tant que sauvegarde si nécessaire)** puis sélectionnez un **Secondary Prisma Access Location (Emplacement d'accès secondaire à Prisma)**.

Si vous sélectionnez ce choix, Prisma Access préremplit le ou les meilleurs emplacements secondaires qui se trouvent dans un emplacement de calcul différent de l'emplacement

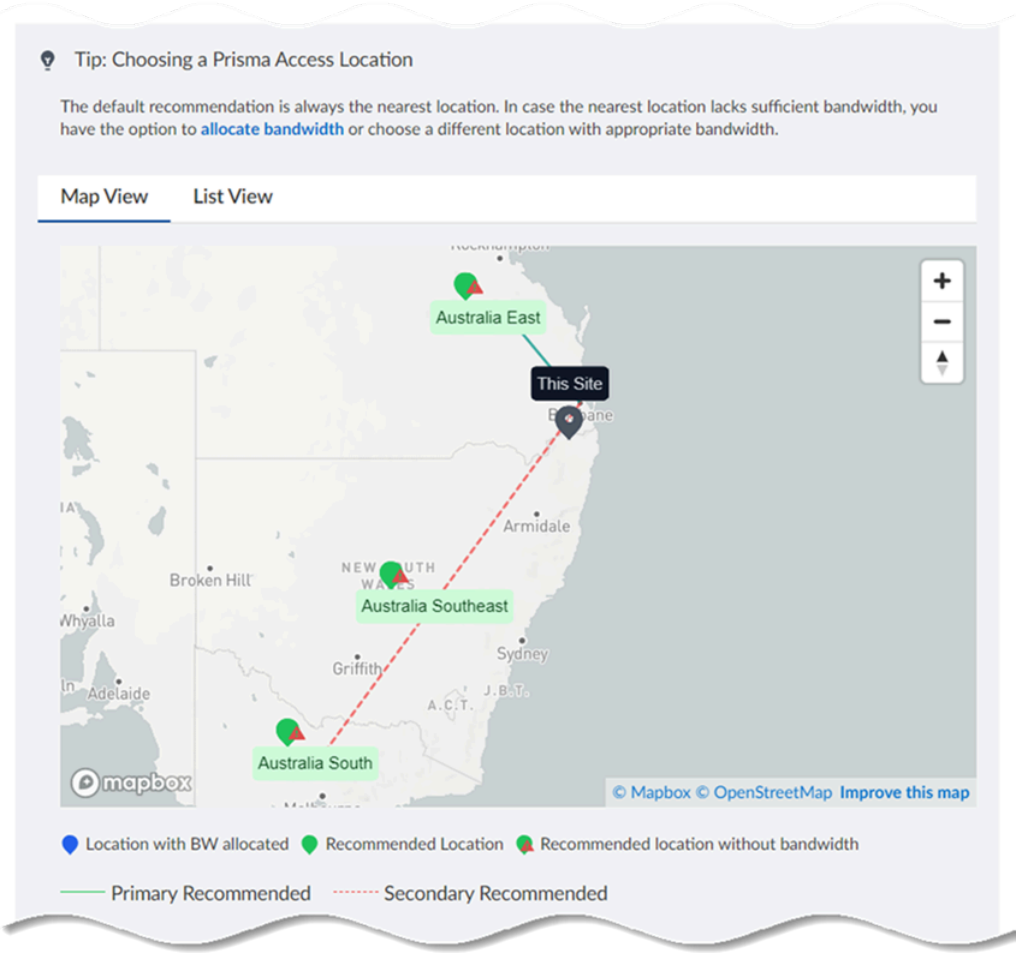
 ©2025 Palo Alto Networks, Inc.

principal. Si plusieurs emplacements sont **Recommended (Recommandés)** ; sélectionnez l'emplacement qui convient le mieux à votre déploiement.



Prisma Access vous fournit une carte avec des suggestions d'emplacements pour vous aider à en choisir un.

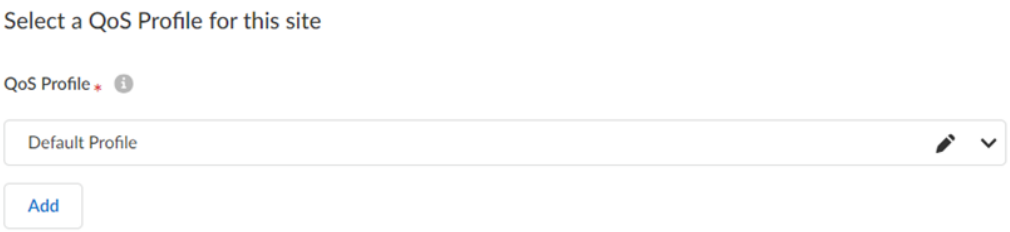
 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | Sélectionnez un **QoS Profile (Profil QoS)** à utiliser pour ce site.

Les réseaux distants hautes performances utilisent un seul profil QoS.

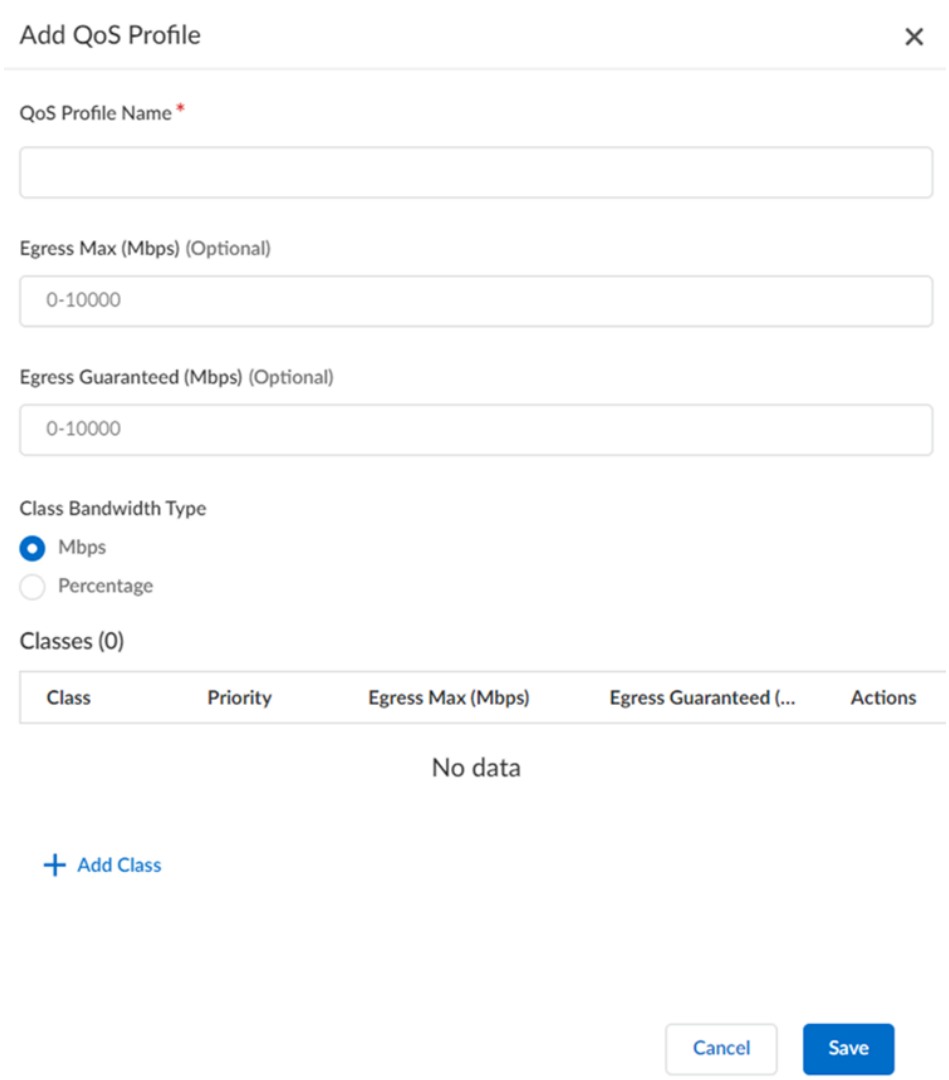


Si vous n'avez pas encore créé de profil QoS, **Add (Ajouter)** un profil QoS, en spécifiant les valeurs suivantes :

- Entrez un **QoS Profile Name (Nom de profil QoS)** unique.
- (Facultatif) Entrez un **Egress Max (Mbps) (Sortie maximale (Mbit/s))** qui représente le débit maximal en Mbit/s pour le trafic quittant la connexion aux services ou la connexion réseau distante.
- (Facultatif) Entrez une valeur **Egress Guaranteed (Mbps) (Sortie garantie (Mbit/s))** qui représente la bande passante garantie pour ce profil en Mbit/s.
- Entrez un **Class Bandwidth Type (Type de bande passante de classe)** de **Percentage (Pourcentage)** ou **Mbps (Mbit/s)**.

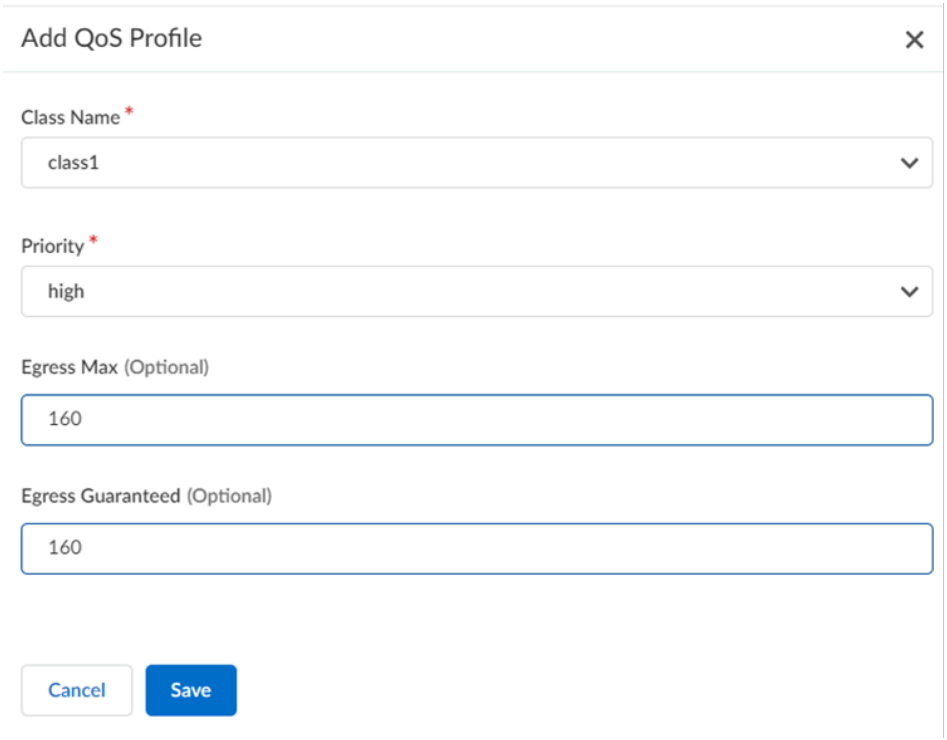
  QoS pour les réseaux distants hautes performances n'utilise pas un rapport de bande passante garanti.

 ©2025 Palo Alto Networks, Inc.



- Dans la section Classes, **Add Class (Ajouter une classe)** et spécifiez comment traiter jusqu'à huit classes QoS individuelles.
  - Entrez une **Class Name (Nom de la classe)**.
  - Sélectionnez la **Priority (Priorité)** pour la classe (soit **real-time (temps réel)**, **high (élevée)**, **medium (moyenne)**, ou **low (basse)**).
  - Entrez une **Egress Max (Sortie Max)** qui représente le débit maximal (en Mbit/s) du trafic quittant la connexion aux services ou la connexion réseau distante.
  - Entrez une valeur **Egress Guaranteed (Sortie garantie)** qui représente la bande passante garantie pour ce profil (en Mbit/s).
- Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

 ©2025 Palo Alto Networks, Inc.

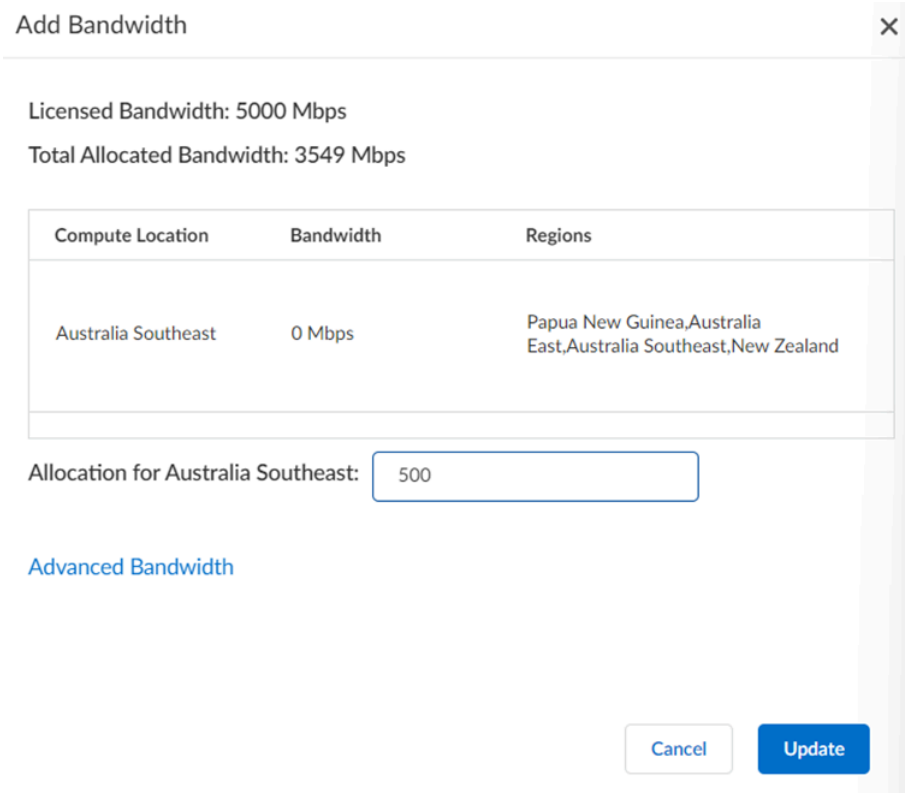


STEP 9 | Si vous n'avez pas encore alloué de bande passante, Prisma Access vous invite à **allocate (allouer)** de la bande passante pour l'emplacement de calcul associé à l'emplacement que vous avez sélectionné. Spécifiez une bande passante minimale de 50 Mbit/s par emplacement de calcul.



 ©2025 Palo Alto Networks, Inc.

STEP 10 | Allouez de la bande passante aux emplacements que vous avez sélectionnés si vous ne l'avez pas déjà fait ; puis, sélectionnez **Update (Mettre à jour)** pour enregistrer vos modifications.



STEP 11 | Cliquez sur **Next (Suivant)**.

STEP 12 | Définissez **Tunnel & Circuit Settings (Paramètres du tunnel et du circuit)**.

1. Sélectionnez un **Tunnel Mode (Mode Tunnel)** : **Active/Active (Actif/Actif)** ou **Active/Passive (Actif/Passif)**.

   Le mode tunnel spécifie le nombre de circuits de votre ISP que vous souhaitez utiliser pour le réseau distant hautes performances.

   - Si vous sélectionnez **Active/Active (Actif/Actif)**, Prisma Access utilise quatre circuits ISP pour créer deux ou quatre tunnels actifs.
   - Si vous sélectionnez **Active/Passive (Actif/Passif)**, Prisma Access utilise deux circuits ISP pour créer deux tunnels actifs. Si le tunnel actif tombe en panne, le tunnel passif devient actif.

2. Sélectionnez le nombre de **Internet Circuits (Circuits Internet)** à utiliser.

   Prisma Access attribue des tunnels en fonction du nombre de circuits que vous spécifiez ici, et si votre déploiement est Actif/Actif ou Actif/Passif, comme indiqué dans le tableau suivant.

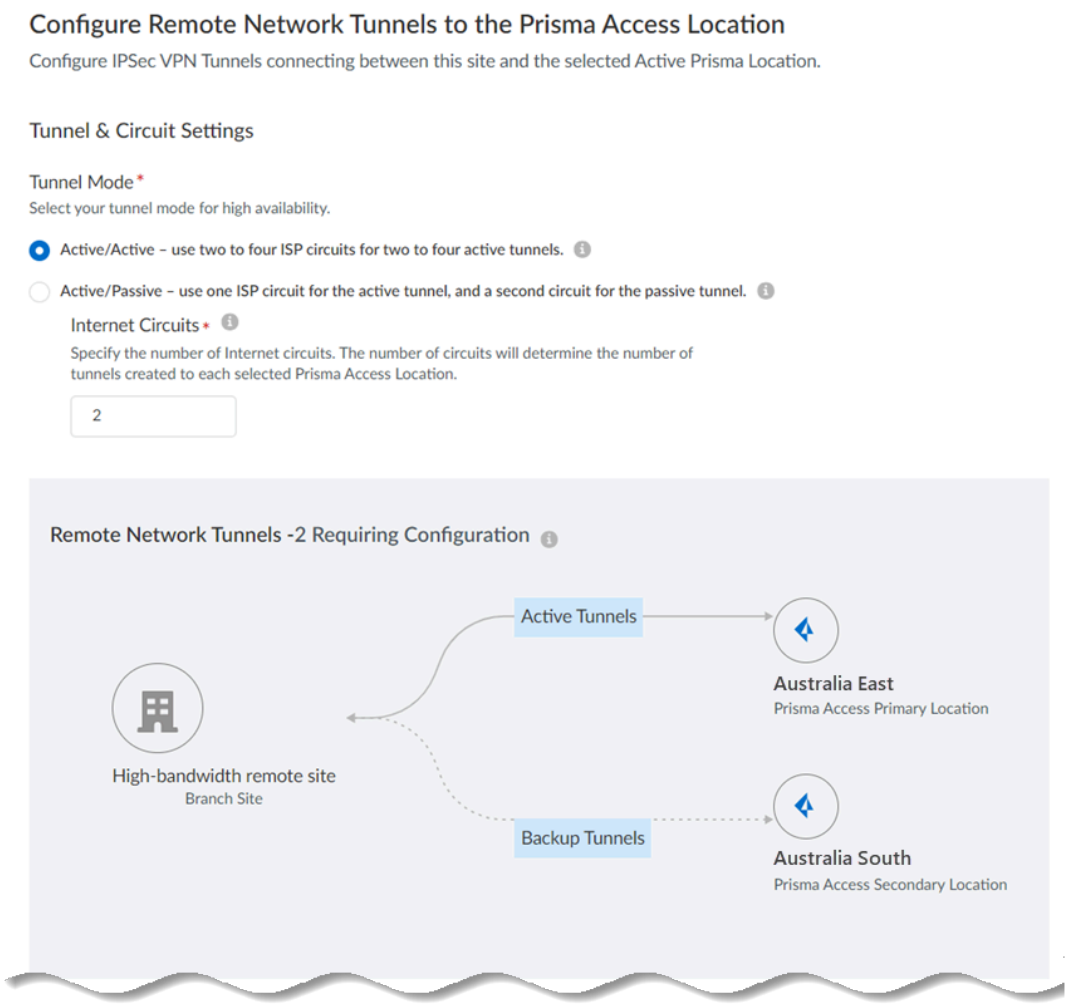
Nombre de circuits	Type de déploiement	Nombre de tunnels
1	Actif/Passif	1 (un pour le tunnel actif).

 ©2025 Palo Alto Networks, Inc.

Nombre de circuits	Type de déploiement	Nombre de tunnels
2	Actif/actif	2 (un pour chaque tunnel actif). Si vous sélectionnez des emplacements principaux et secondaires, Prisma Access crée un tunnel actif pour l'emplacement principal et un tunnel actif pour l'emplacement secondaire.
2	Actif/Passif	2 (un pour chaque tunnel actif). Si vous sélectionnez des emplacements principaux et secondaires, Prisma Access crée un tunnel actif et passif pour l'emplacement principal et un tunnel actif et passif pour l'emplacement secondaire. Si le tunnel actif tombe en panne, Prisma Access utilise la même adresse IP de service ou FQDN pour le tunnel passif qui devient actif.
4	Actif/actif	4 (un pour chaque tunnel actif). Si vous sélectionnez des emplacements principaux et secondaires, Prisma Access crée deux tunnels actifs

 ©2025 Palo Alto Networks, Inc.

Nombre de circuits	Type de déploiement	Nombre de tunnels
		pour l'emplacement principal et deux tunnels actifs pour l'emplacement secondaire.



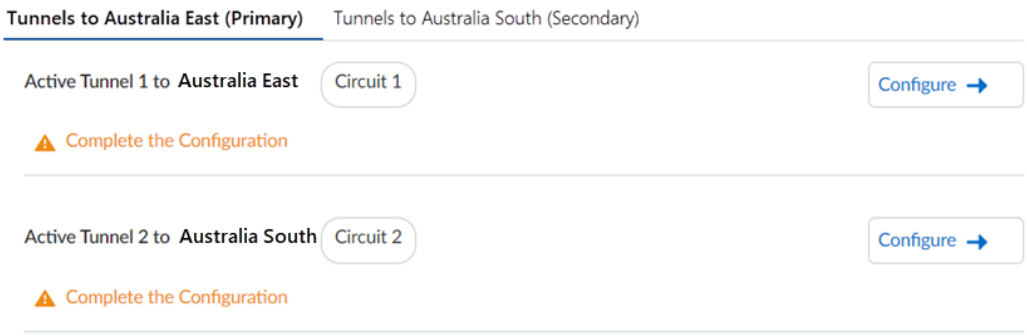
3. (Facultatif) **Configure (Configurer)** vos paramètres de votre tunnel IPSec.

   Prisma Access vous fournit les paramètres de tunnel IPSec par défaut. Ces paramètres déterminent les paramètres de chiffrement IPSec et IKE pour le tunnel réseau distant. Si

 ©2025 Palo Alto Networks, Inc.

vous souhaitez les modifier, sélectionnez l'icône **Primary Tunnel (Tunnel primaire)** et **Edit (Éditer)** vos paramètres.

Si vous spécifiez un emplacement secondaire, Prisma Access remplit automatiquement les valeurs du tunnel primaire vers le tunnel secondaire ; pour modifier le tunnel secondaire, sélectionnez-le et **Edit (Éditer)** les paramètres.



Prenez note de ces paramètres ; vous devez faire correspondre les paramètres du CPE qui termine le tunnel IPSec sur votre site.

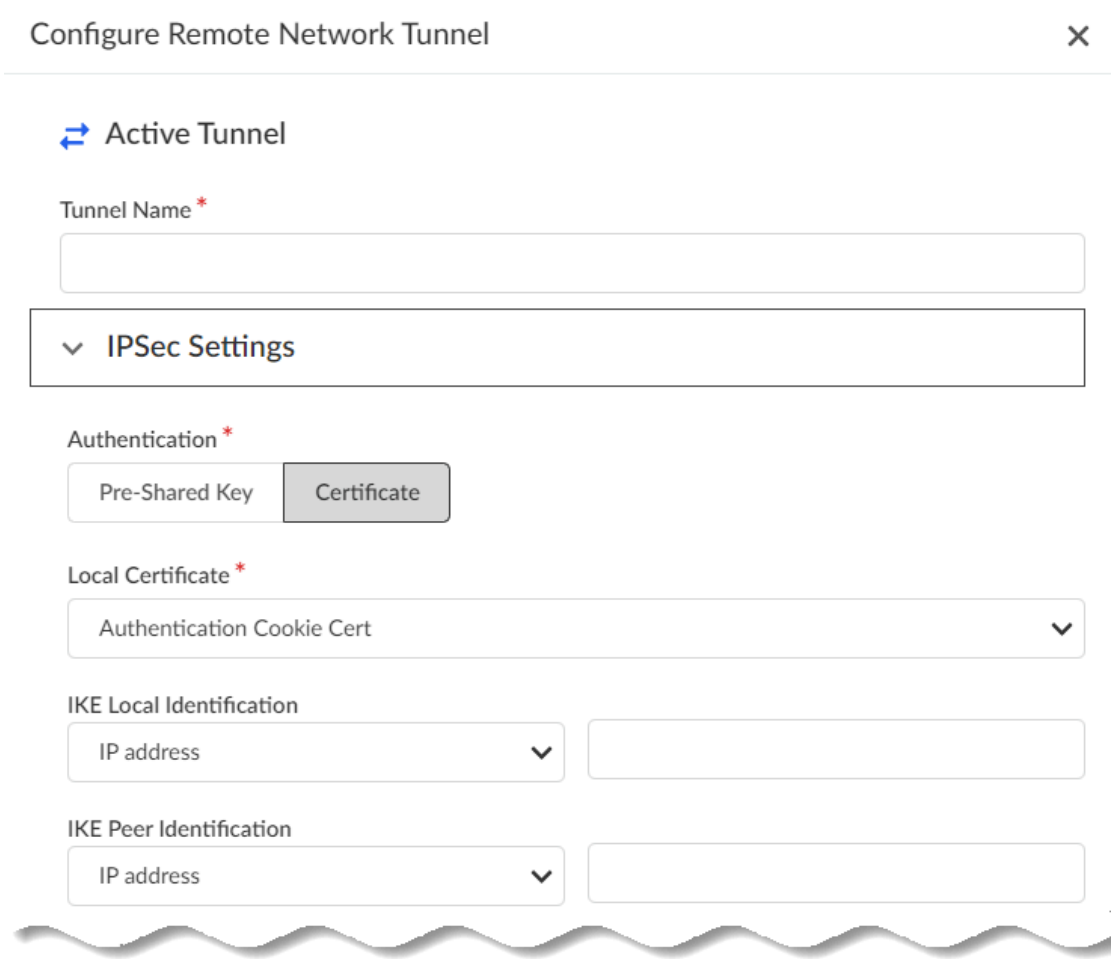
- Donnez au tunnel actif un **Tunnel Name (Nom de tunnel)** unique.
- Spécifiez **IPSec Settings (Paramètres IPSec)**.
  - Spécifiez un type **Authentication (Authentification)** (soit **Pre-Shared Key (Clé pré-partagée)** ou **Certificate (Certificat)**).

    Si vous spécifiez une**Pre-Shared Key (Clé pré-partagée)**, entrez et confirmez la **Pre-Shared Key (Clé pré-partagée)**.

    Si vous spécifiez un **Certificate (Certificat)**, entrez le **Local Certificate (Certificat local)** à utiliser. Ce certificat doit déjà exister dans Strata Cloud Manager.
  - Spécifiez le **IKE Local Identification (Identification locale IKE)** (soit **IP Address (Adresse IP)**, **Distinguished Name (Subject) (Nom distinctif (sujet))**, **User FQDN (email address) (FQDN de l'utilisateur (adresse e-mail))**, ou **FQDN (hostname) (FQDN (nom d'hôte))**.
  - Spécifiez le **IKE Peer Identification (Identification de l'homologue IKE)** (soit **IP Address (Adresse IP)**, **Distinguished Name (Subject) (Nom distinctif (Sujet))**,

 ©2025 Palo Alto Networks, Inc.

User FQDN (email address) (FQDN de l'utilisateur (adresse e-mail)), ou **FQDN (hostname) (FQDN (nom d'hôte))).**

- 

- Précisez le type de Vérification de l'ID de l'homologue) :
  - **Exact (Exact)**—assure que le paramètre local et la charge utile ID IKE de l'homologue correspondent parfaitement.
  - **Wildcard (Caractère générique)** : permet à l'identification de l'homologue de correspondre tant que chaque caractère situé avant le caractère générique (*) correspond. Il n'est pas nécessaire que les caractères après le caractère générique correspondent.
- (Facultatif) **Permit peer identification and certificate payload identification mismatch (Autoriser une non-correspondance de l'identification de l'homologue et de l'identification de la charge utile du certificat)** pour autoriser une SA IKE réussie

 ©2025 Palo Alto Networks, Inc.

même si l'identification de l'homologue ne correspond pas à l'identification de l'homologue dans le certificat.

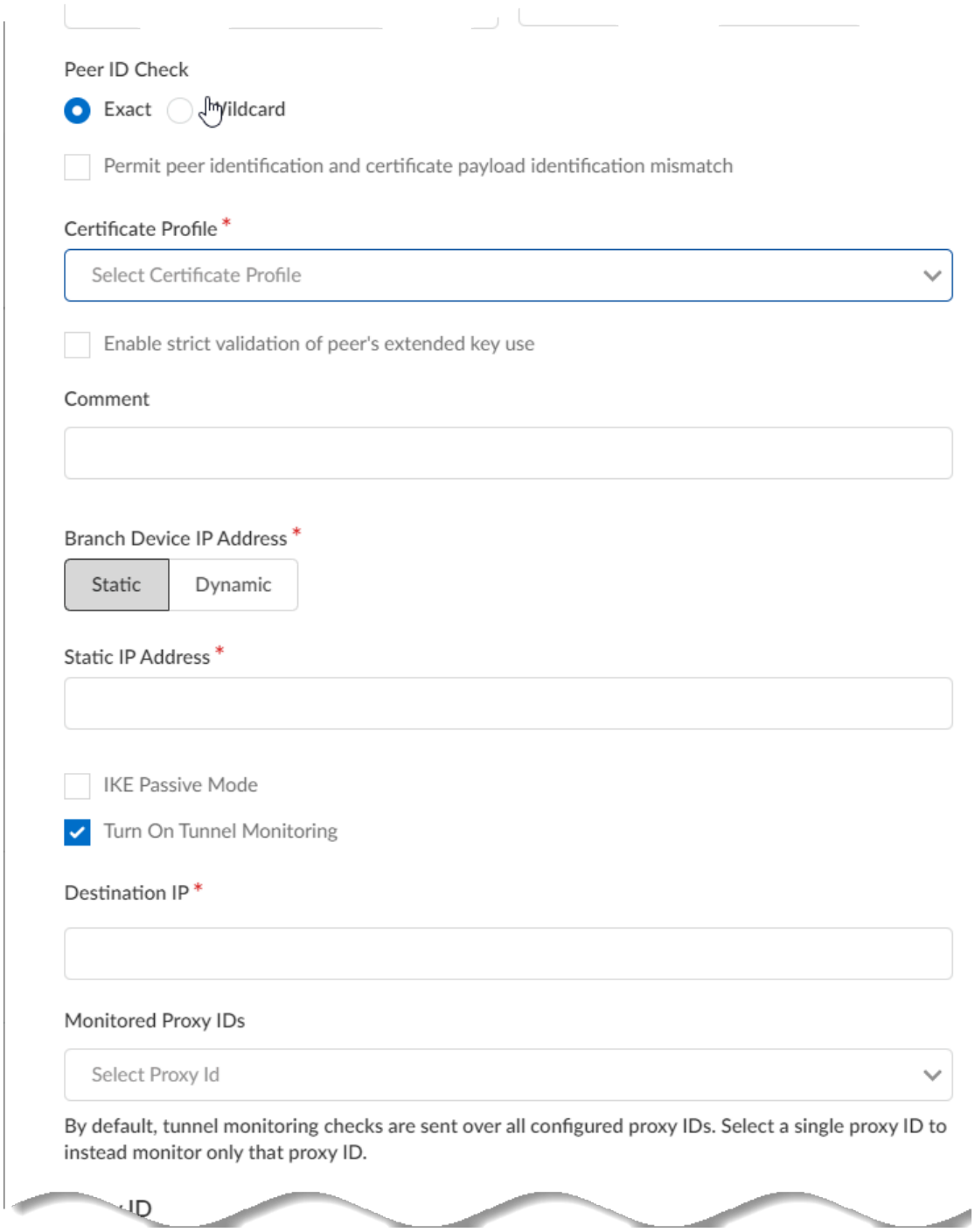
- Choisissez un **Certificate Profile (Profil de certificat)**. Un profil de certificat contient des informations sur comment authentifier la passerelle homologue.
- (Facultatif) **Enable strict validation of peer's extended key use (Activer la validation stricte de l'utilisation de la clé étendue de l'homologue)** pour contrôler strictement l'utilisation de la clé.
- Sélectionnez **Branch Device IP Address (Adresse IP du périphérique de branche)** (**Static (Statique)** ou **Dynamic (Dynamique)**).
  - Si vous sélectionnez **Static (Statique)**, entrez **Static IP Address (Adresse IP statique)** à utiliser pour le tunnel IPSec.
  - Spécifiez **Dynamic (Dynamique)** pour obtenir automatiquement l'adresse IP.
- (Facultatif, Recommandé) Activer **IKE Passive Mode (Mode passif IKE)** pour que Prisma Access réponde aux connexions IKE, mais sans les initier.

  Bien que cela ne soit pas obligatoire, le **IKE Passive Mode (Mode passif IKE)** est le paramètre recommandé.
- (Facultatif) **Turn on Tunnel Monitoring (Activer la surveillance des tunnels)**.

  Entrez une adresse **Destination IP (IP de destination)** de surveillance du tunnel sur le réseau distant pour que Prisma Access détermine si le tunnel est actif et, si votre

 ©2025 Palo Alto Networks, Inc.

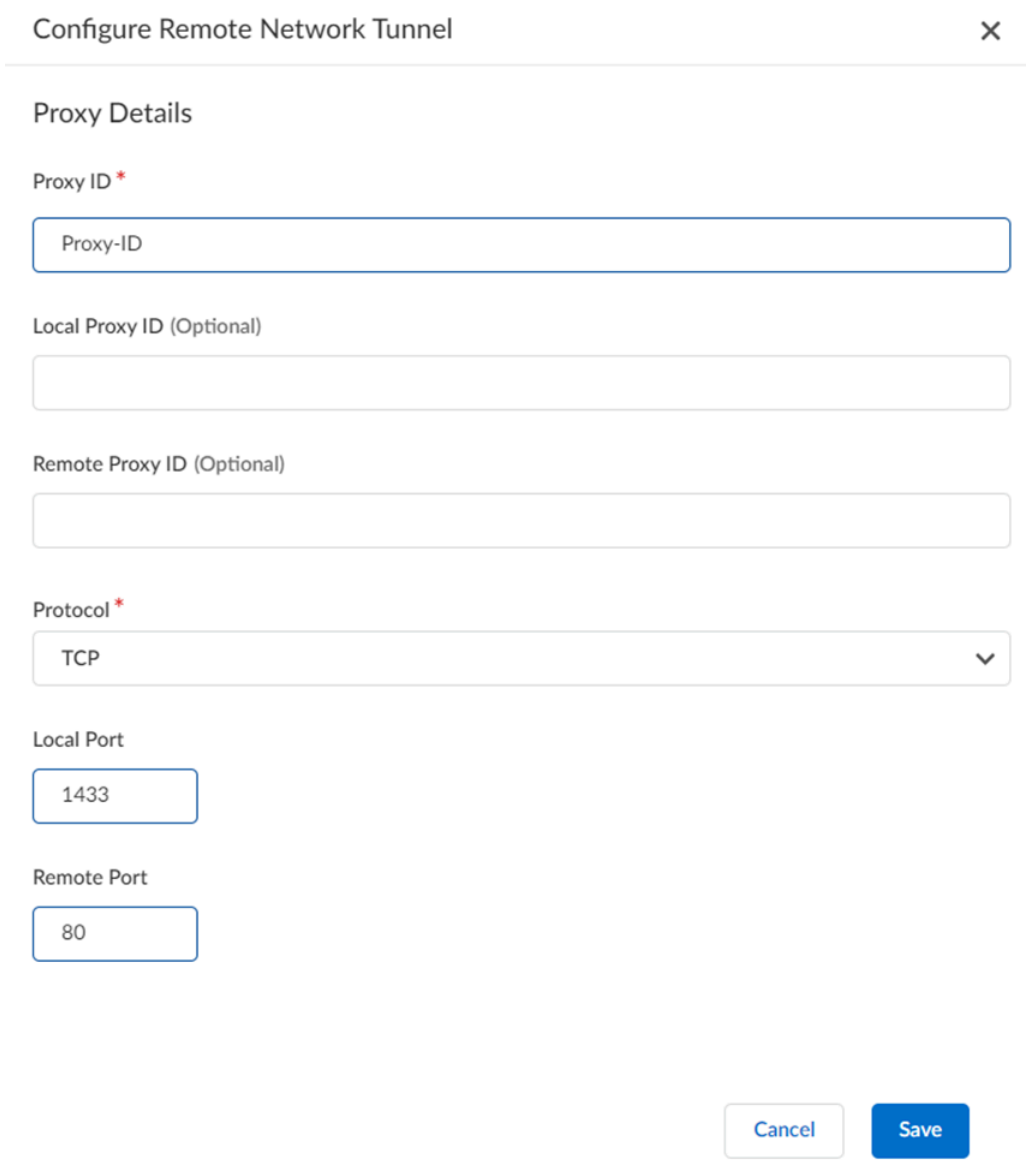
périphérique IPSec de succursale utilise un VPN basé sur des stratégies, entrez le **Proxy ID (ID de proxy)** associé comme le **Monitored Proxy ID (UD de proxy surveillé)**.

- 

- (Facultatif) Si vous avez besoin d'un ID de proxy :
  - **Add Proxy ID (Ajouter un ID de proxy)** et entrez le **Proxy ID (ID de proxy)**.
  - Si vous le souhaitez, entrez le **Local Proxy ID (ID de proxy local)** et **Remote Proxy ID (ID du proxy distant)**.
  - Entrez le **Protocol (Protocole)** à utiliser pour l'ID du proxy. Entrez un **Number (Nombre)**, **TCP** ou **UDP**.

 ©2025 Palo Alto Networks, Inc.

- Spécifiez un **Local Port (Port local)** et **Remote Port (Port distant)** pour TCP ou UDP, ou spécifiez un
- **Save (Enregistrer)** vos modifications.



- Spécifiez des **IKE Advanced Options (Options avancées IKE)**.
  - Sélectionnez une **IKE Protocol Version (Version du protocole IKE)**.
  - Sélectionnez un **IKEv1 Crypto Profile (Profil crypto IKEv1)**.

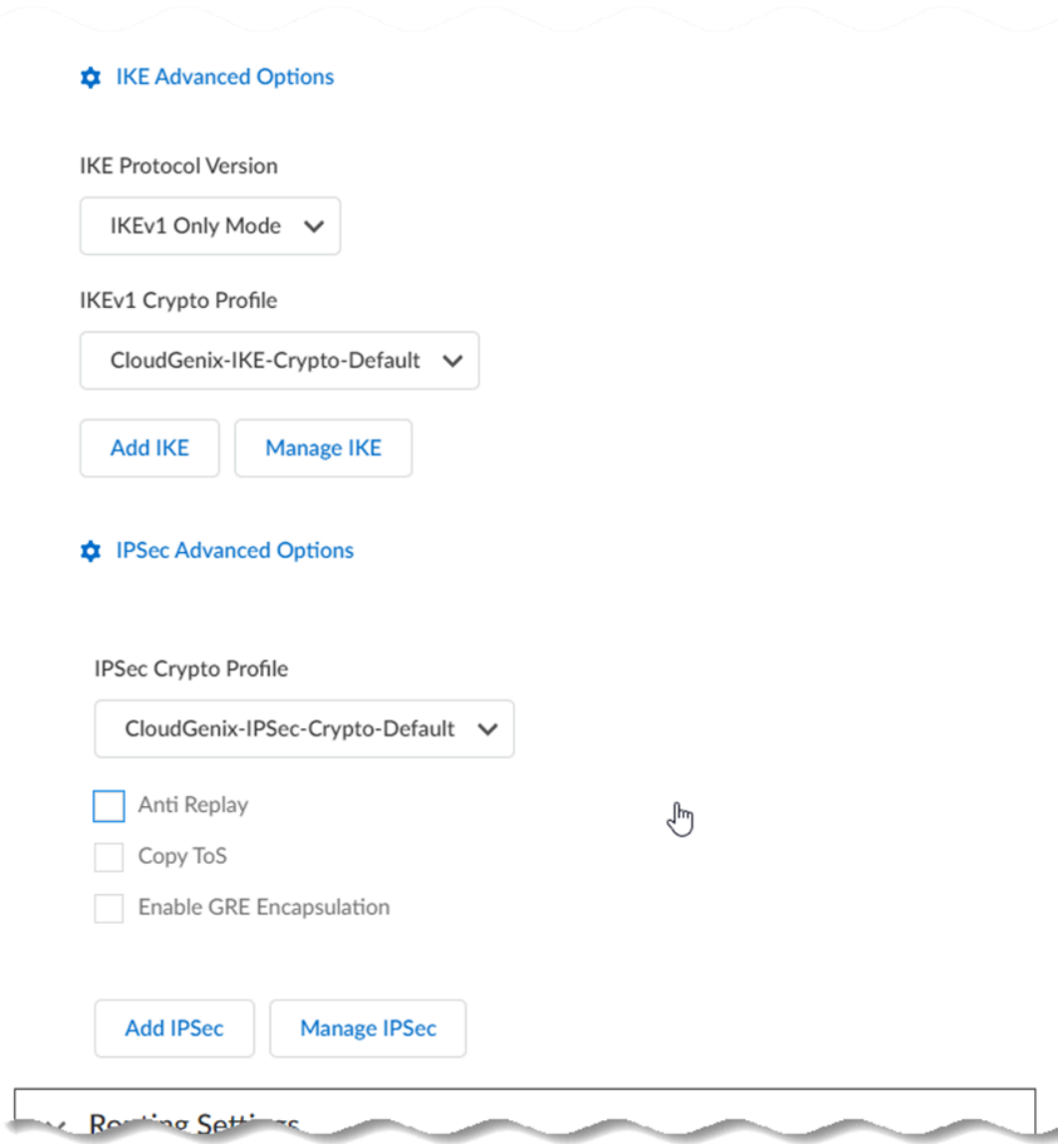
    Pour ajouter un profil crypto, **Add IKE (Ajouter IKE)**. Pour gérer un profil IKE existant, **Manage IKE (Gérer IKE)** et sélectionnez le profil à modifier.
  - Sélectionnez un **IKEv2 CRypto Profile (Profil crypto IKEv2)**.

    Pour ajouter un profil crypto, **Add IKE (Ajouter IKE)**. Pour gérer un profil IKE existant, **Manage IKE (Gérer IKE)** et sélectionnez le profil à modifier.
- Spécifiez **IPSec Advanced Options (Options avancées IPSec)**.

 ©2025 Palo Alto Networks, Inc.

- Sélectionnez un **IPSec Crypto Profile (Profil crypto IPSec)**.

  Pour ajouter un profil crypto, **Add IPSec (Ajouter IPSec)**. Pour gérer un profil IPSec existant, **Manage IPSec (Gérer IPSec)** et sélectionnez le profil à modifier.

- 

- Choisissez vos **Routing Settings (Paramètres de routage)**.
  - Sélectionnez le **Routing Type (Type de routage)** (soit **Static (Statique)** ou **Dynamic (Dynamique)**).

    Si vous sélectionnez **Static (Statique)**, **Add (Ajouter)** les sous-réseaux IP ou les adresses IP que vous souhaitez sécuriser sur le site.

    Si vous sélectionnez **Dynamic (Dynamique)** :

    - Entrez le **Peer AS (AS homologue)** (le système autonome (AS) pour votre réseau).

      Utilisez un numéro AS privé BGP conforme à la RFC 6996.

 ©2025 Palo Alto Networks, Inc.

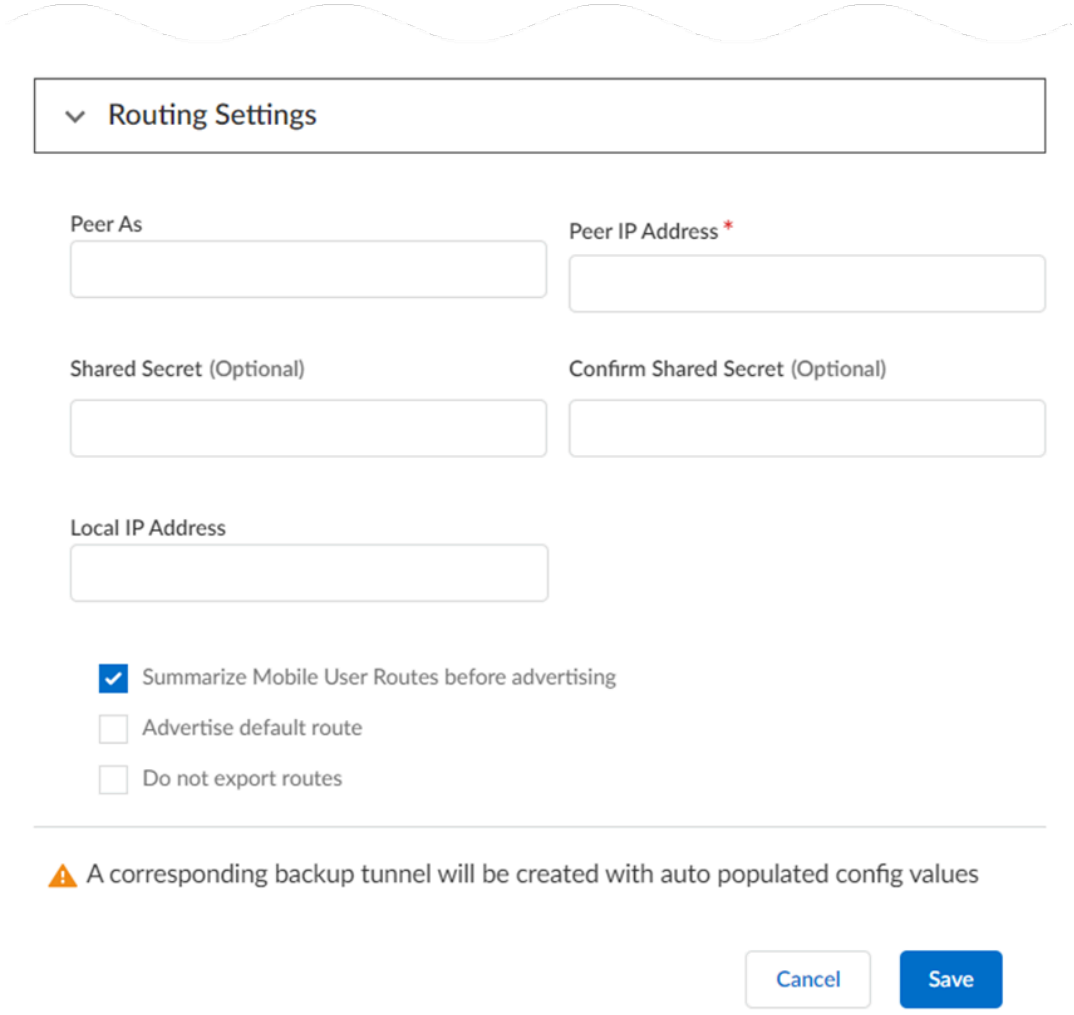
- Entrez la **Peer IP Address (Adresse IP de l'homologue)** attribuée en tant qu'ID de routeur du routeur eBGP sur le réseau du siège social ou du centre de données.
- (Facultatif) Entrez un mot de passe **Shared Secret (Secret partagé)** pour authentifier les communications BGP des homologues.
- Entrez la **Local IP Address (Adresse IP locale)** que Prisma Access utilise comme adresse IP locale pour BGP.
- (Facultatif) Sélectionnez **Summarize Mobile User Routes before advertising (Résumer les itinéraires des utilisateurs mobiles avant de faire de la publicité)** pour réduire le nombre de publicités de sous-réseau IP d'utilisateur mobile via BGP sur l'équipement des locaux de votre client (CPE) en demandant à Prisma Access de résumer les sous-réseaux avant d'en faire la publicité.
- (Facultatif) Sélectionnez **Advertise Default Route (Annoncer l'itinéraire par défaut)** pour que Prisma Access crée une publicité d'itinéraire par défaut pour le réseau distant utilisant eBGP. Assurez-vous que votre réseau ne dispose

 ©2025 Palo Alto Networks, Inc.

pas d'une autre itinéraire par défaut annoncé par BGP, sinon vous risquez d'introduire des problèmes de routage dans votre réseau.

- (Facultatif) Sélectionnez **Don't Export Routes (Ne pas exporter d'itinéraires)** pour empêcher Prisma Access de transférer des itinéraires dans le siège social ou le centre de données.

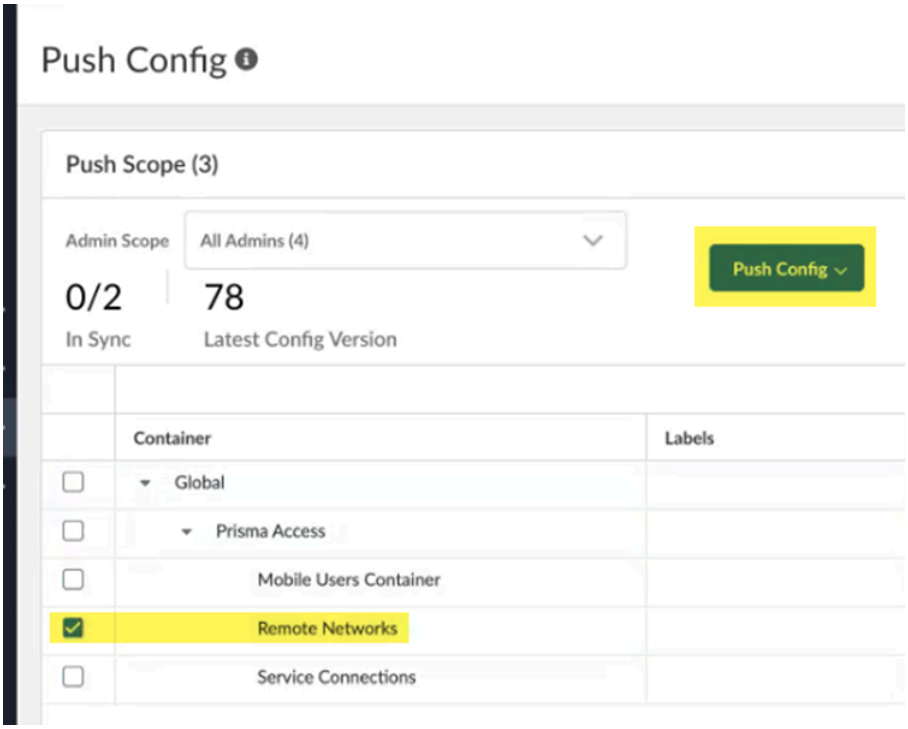
4. **Save (Enregistrer)** les modifications de votre tunnel IPSec.



STEP 13 | **Save & Exit (Enregistrer et quitter)**.

 ©2025 Palo Alto Networks, Inc.

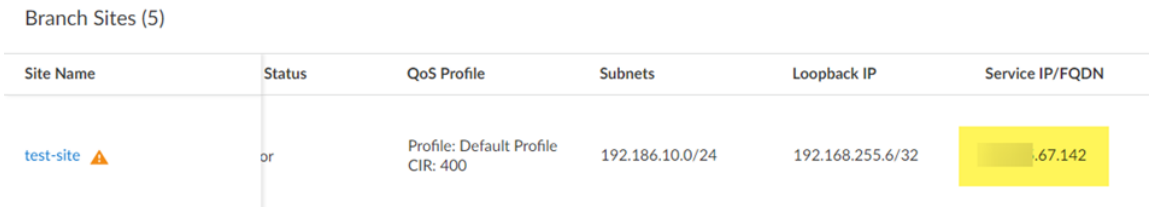
STEP 14 | **Push Configuration (Transmettre la configuration)** pour enregistrer vos modifications de configuration, assurez-vous de sélectionner **Remote Networks (Réseaux distants)** dans la **Push Scope (Étendue de la transmission)**.



STEP 15 | Trouvez **Service IP address (Adresse IP du service)** que vous spécifiez sur votre CPE.

Lorsque vous configurez le réseau distant, utilisez l'adresse IP du service comme adresse IP d'homologue sur votre CPE pour mettre fin au tunnel IPSec.

1. Allez à **Workflows (Flux de travail)** > **Prisma SASE Setup (Configuration de Prisma SASE)** > **Branch Site Management (Gestion de site de succursale)** > **Extended CPE Site (Site CPE étendu)**.
2. Trouvez l'adresse **Service IP/FQDN (Service IP/FQDN)**.



Panorama

Les étapes de configuration d'un réseau distant hautes performances sont les mêmes que celles de l'intégration d'un réseau distant standard dans Prisma Access (Managed by Panorama), y compris le choix d'un **IPSec Termination Node (Nœud de terminaison IPSec)** lors de l'intégration.

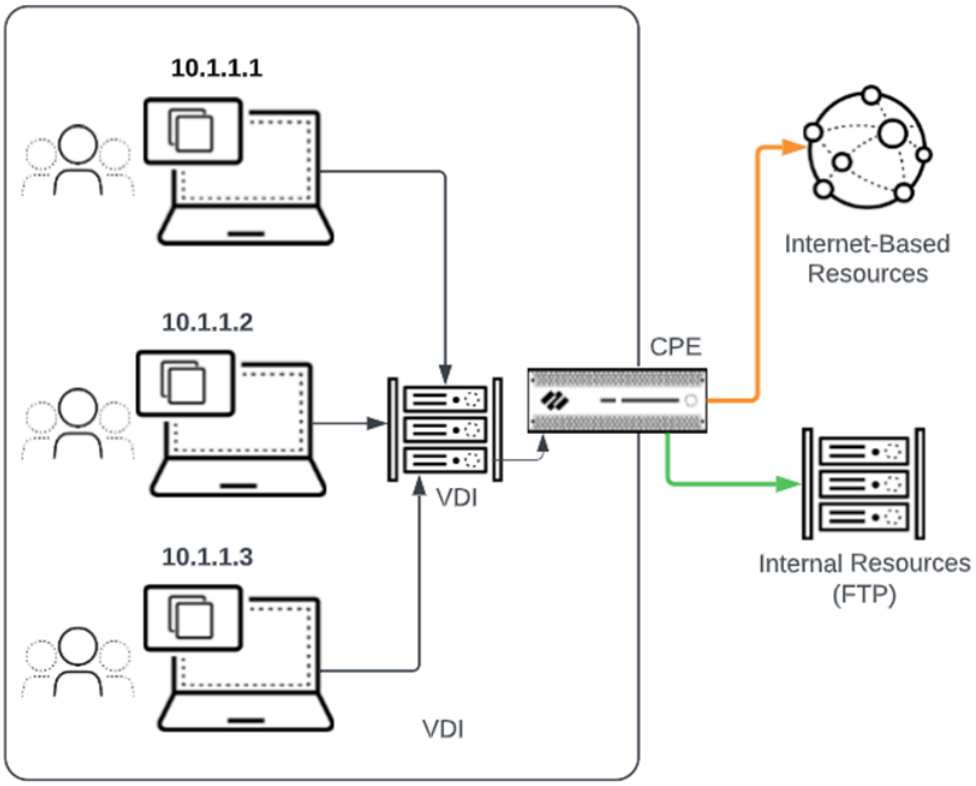
 ©2025 Palo Alto Networks, Inc.

Intégration d'une VDI de bureau partagé à Prisma Access à l'aide d'un serveur de terminaux

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access

L'infrastructure de bureau virtuel (VDI) est une technologie qui utilise des machines virtuelles (Virtual Machine – VM) pour provisionner et gérer des bureaux virtuels. La VDI déploie des environnements de bureau à l'aide d'un serveur géré et les déploie pour les utilisateurs finaux sur demande. Les utilisateurs finaux accèdent aux ressources dont ils ont besoin, comme les applications et ressources publiques basées sur Internet ou les applications et ressources privées disponibles à partir d'une connexion FTP, à partir des bureaux VDI provisionnés.

Il est possible de mettre en œuvre une topologie VDI l'aide de bureaux partagés ou dédiés. Si les bureaux sont partagés, plusieurs utilisateurs utilisent la même adresse IP ; ce sont alors les ports qui permettent de les différencier.



Si votre déploiement VDI utilise une mise en œuvre de bureaux partagés, Prisma Access offre une solution qui permet aux utilisateurs finaux d'accéder en toute sécurité aux ressources Internet et FTP à l'aide d'une connexion unique, tout en protégeant les utilisateurs VDI et les ressources

 ©2025 Palo Alto Networks, Inc.

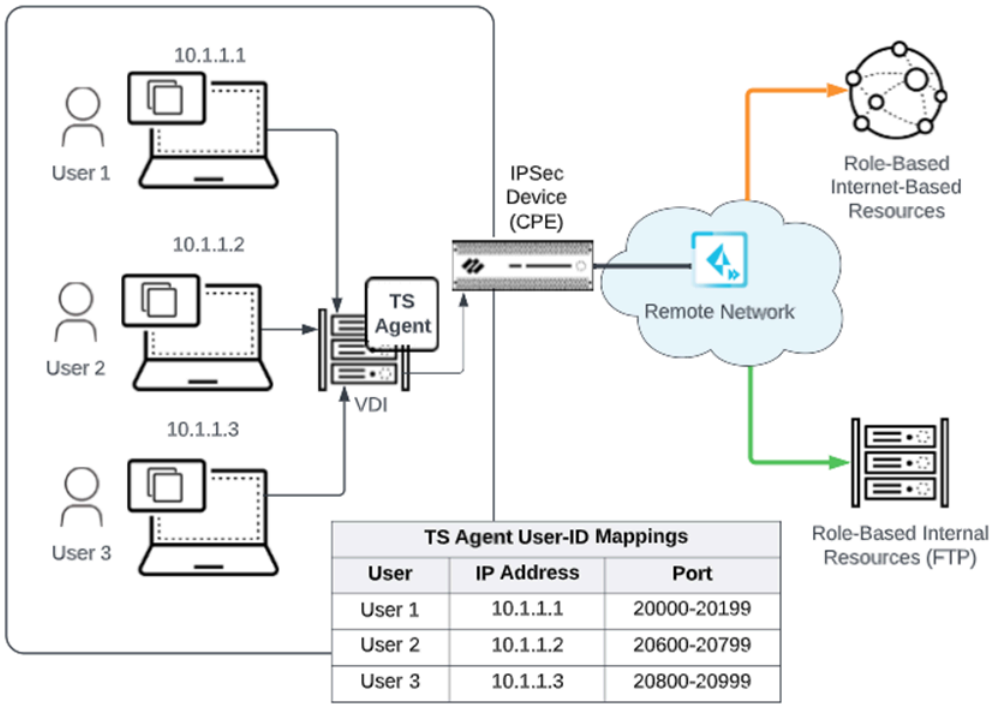
internes et externes de votre organisation. Cette solution utilise l'agent TS Palo Alto Networks que vous pouvez installer sur les serveurs VDI.

L'agent TS est un logiciel User-ID installé pour résoudre le problème lié à l'identification des mappages entre les noms d'utilisateur et les adresses IP lorsque plusieurs utilisateurs partagent la même adresse IP. Une fois l'agent TS installé, tous les utilisateurs connectés sont surveillés et un ensemble spécifique de ports est attribué à chaque utilisateur. Quand Prisma Access reçoit le trafic réseau VDI de la VDI, il identifie l'utilisateur en fonction de son port source. Ce déploiement vous fournit une solution basée sur le cloud qui permet aux administrateurs de créer des règles de politique de sécurité pour que les utilisateurs finaux VDI puissent contrôler leur accès à Internet et aux sites internes.

Si votre réseau dispose d'un itinéraire par défaut, vous pouvez intégrer un ou plusieurs réseaux distants et mettre en œuvre l'agent TS pour protéger facilement et simplement les utilisateurs et les ressources de votre organisation.

Dans ce déploiement :

- Vous spécifiez une plage de ports sur l'agent TS pour identifier des utilisateurs spécifiques sur les serveurs de terminaux Windows. L'agent TS informe Prisma Access des plages de ports allouées afin que Prisma Access puisse appliquer la politique en fonction des utilisateurs et des groupes d'utilisateurs.
- Le réseau distant applique la sécurité et le contrôle d'accès pour les ressources FTP et Internet.



Vous ne pouvez pas redistribuer les informations de mappage d'utilisateur collectées à partir d'un agent TS.

Pour intégrer une VDI à l'aide de l'agent TS et d'un réseau distant Prisma Access dans Cloud Managed Prisma Access, procédez comme suit.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Installez et configurez l'agent TS Palo Alto Networks sur les serveurs VDI.

Afin de mapper tous vos utilisateurs, vous devez installer l'agent TS sur tous les serveurs de terminaux auxquels vos utilisateurs se connectent.

1. Sur les serveurs Windows VDI, installez et configurez l'agent Terminal Server (TS) Palo Alto Networks.
2. Définissez la plage de ports que l'agent TS alloue aux utilisateurs finaux.

   Vérifiez le nombre d'échelles pris en charge pour l'agent TS dans la matrice de compatibilité.
3. (Facultatif) S'il existe plusieurs serveurs VDI, configurez un agent TS sur chaque serveur.

STEP 2 | Intégrez un réseau distant et connectez-le au site de succursale VDI dans Cloud Managed Prisma Access (si vous ne l'avez pas déjà fait).

STEP 3 | Configurez les options sur le périphérique IPSec (CPE) de la succursale pour permettre au réseau distant de communiquer avec la VDI.

- Configurez les paramètres crypto IPSec et IKE pour le tunnel IPSec qui correspondent aux paramètres que vous avez configurés dans Prisma Access.
- Utilisez l'adresse **Service IP (Adresse IP de service)** (**Manage (Gérer)** > **Remote Networks (Réseaux distants)** > **Service IP (Adresse IP de service)**) comme côté Prisma Access du tunnel IPSec pour le réseau distant.
- Configurez un itinéraire sur le périphérique IPSec pour autoriser le trafic VDI vers le tunnel du réseau distant.
- Configurez un itinéraire sur le périphérique IPSec pour autoriser le trafic du réseau distant vers l'agent TS via le tunnel.
- Si nécessaire, configurez une politique de sécurité sur le périphérique IPSec pour autoriser le passage du trafic par le tunnel.

STEP 4 | Configurez l'agent TS pour autoriser le mappage d'utilisateur dans le réseau distant.

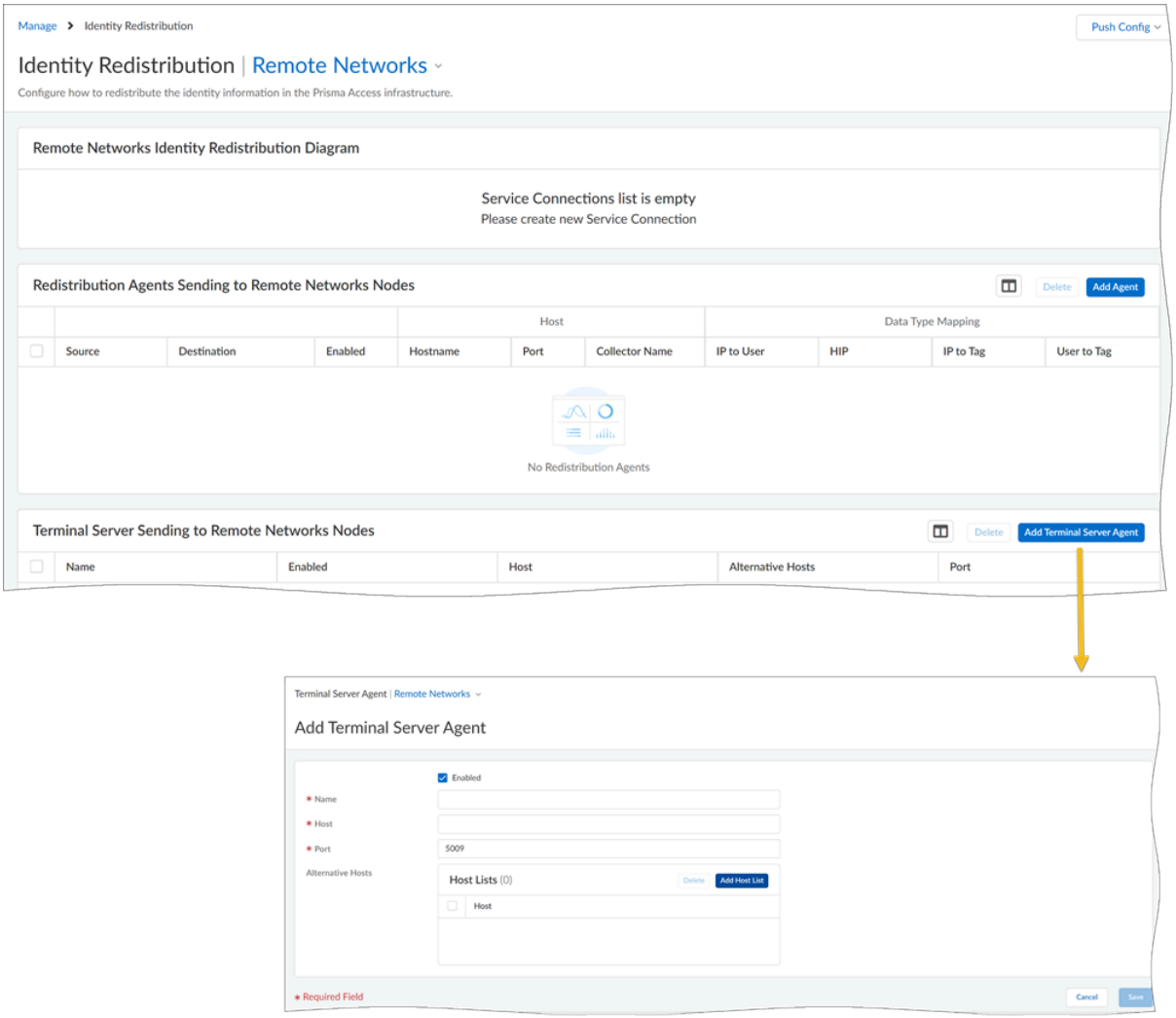
Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Identity Redistribution (Redistribution d'identité)**, définissez le paramètre **Configuration Scope (Portée de la configuration)** sur **Remote Networks (Réseaux distants)**, puis sélectionnez **Add Terminal Server Agent (Ajouter un agent Terminal Server)**.

- Vérifiez que l'agent est **Enabled (Activé)**.
- Entrez un **Name (nom)** pour l'agent TS.
- Saisissez l'adresse IP de **Host (l'hôte)** Windows sur lequel l'agent TS est installé.
- Saisissez le numéro de **Port (Port)** sur lequel l'agent écoutera les requêtes de mappage d'utilisateur.

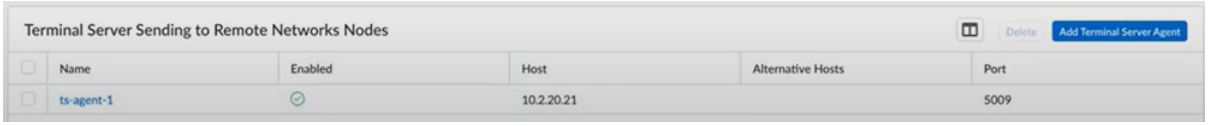
  Le port est défini sur 5009 par défaut.

 ©2025 Palo Alto Networks, Inc.

- Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.



Dans l'exemple suivant, un agent est configuré avec l'adresse d'hôte 10.2.20.21 et le port 5009.

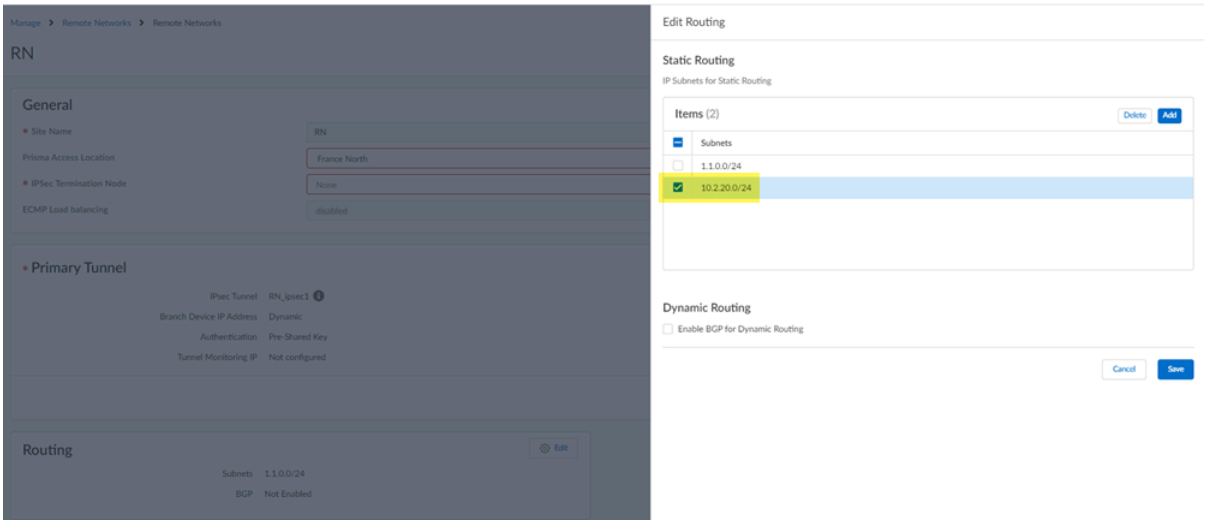


 ©2025 Palo Alto Networks, Inc.

STEP 5 | Autorisez le routage entre la VDI et le réseau distant Prisma Access.

1. Accédez à **Manage (Gérer)** > **Service Setup (Configuration du service)** > **Remote Networks (Réseaux distants)** > ***remote-network-name*** > **Routing (Routage)**, puis sélectionnez **Add (Ajouter)** pour ajouter un itinéraire vers le sous-réseau VDI.

   L'ajout de ce sous-réseau permet à l'agent TS de communiquer avec le réseau distant. Dans la capture d'écran d'exemple suivante, le sous-réseau VDI est 10.2.20.0/24.



2. Accédez à **Manage (Gérer)** > **Configuration** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)**, définissez la portée sur **Remote Networks (Réseaux distants)** et ajoutez une règle de politique de sécurité (**Add Rule (Ajouter une règle)**) pour autoriser le trafic entre le sous-réseau VDI et le réseau distant.

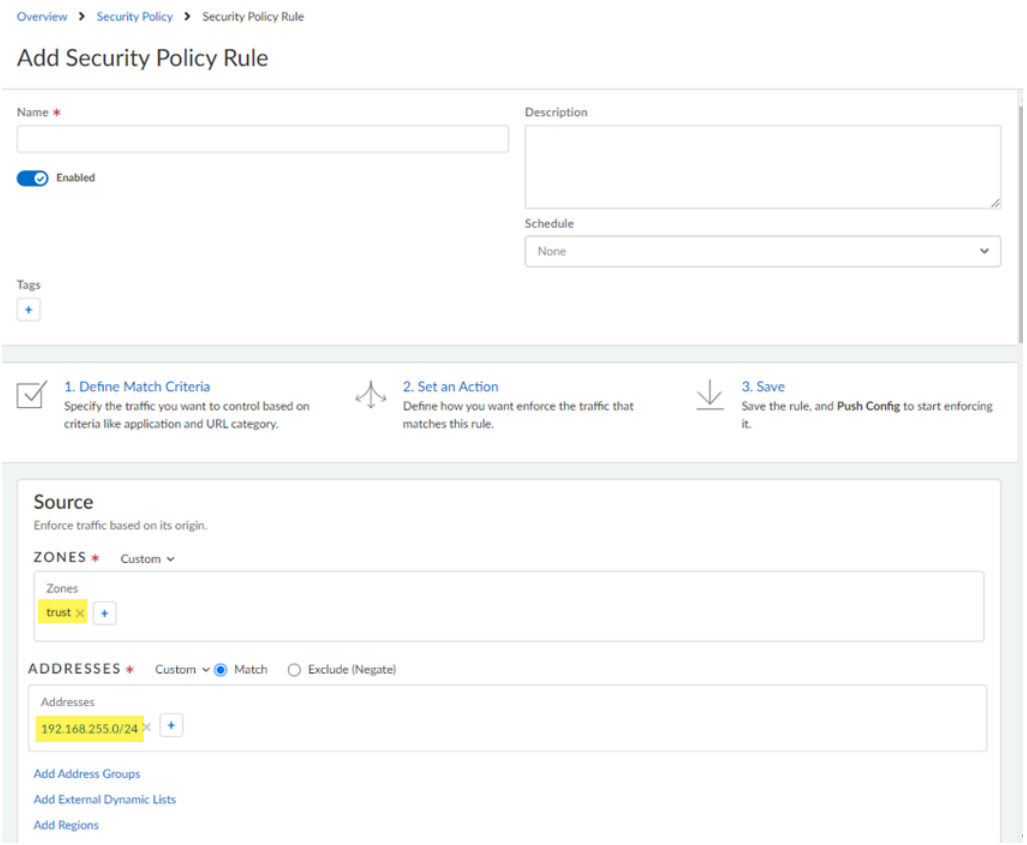
   Les utilisateurs de réseaux distants qui se connectent à Prisma Access à partir de la VDI se voient attribuer une adresse IP à partir du sous-réseau d'infrastructure Prisma Access et vous devez autoriser le routage entre le sous-réseau d'infrastructure et le sous-réseau VDI.

   - Vérifiez que la règle est **Enabled (Activée)**.
   - **Source** : définissez les paramètres suivants.
     - **Zones** : définissez ce paramètre sur **Trust (Approuvée)**.
     - **Addresses (Adresses)** : créez un objet d'adresse pour le sous-réseau d'infrastructure (**Manage (Gérer)** > **Shared (Partagé)** > **Infrastructure**

 ©2025 Palo Alto Networks, Inc.

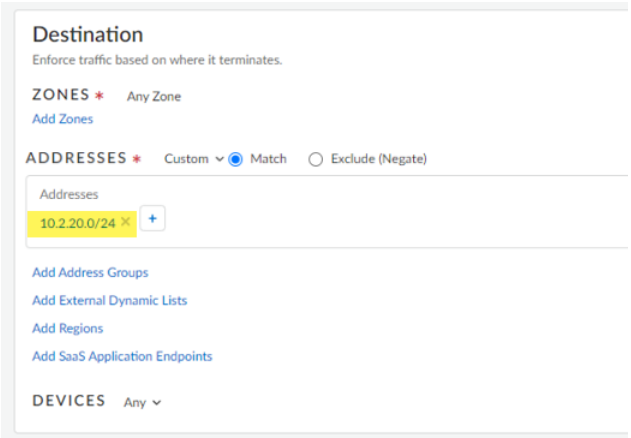
Settings (Paramètres d'infrastructure) > **Infrastructure Subnet (Sous-réseau d'infrastructure)**) et ajoutez l'objet d'adresse ici.

Il est préférable d'utiliser un objet d'adresse plutôt que d'entrer le sous-réseau d'infrastructure réel, car si le sous-réseau change, vous pouvez modifier l'objet d'adresse et cette modification est appliquée à toutes les configurations où l'objet d'adresse est utilisé.



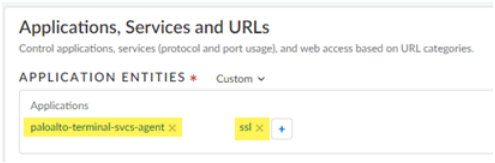
- **Destination** : ajoutez l'hôte VDI qui exécute l'agent TS aux **Addresses (Adresses)**.

  Si vous avez configuré l'agent TS sur plusieurs hôtes VDI, ajoutez-les tous ici.



 ©2025 Palo Alto Networks, Inc.

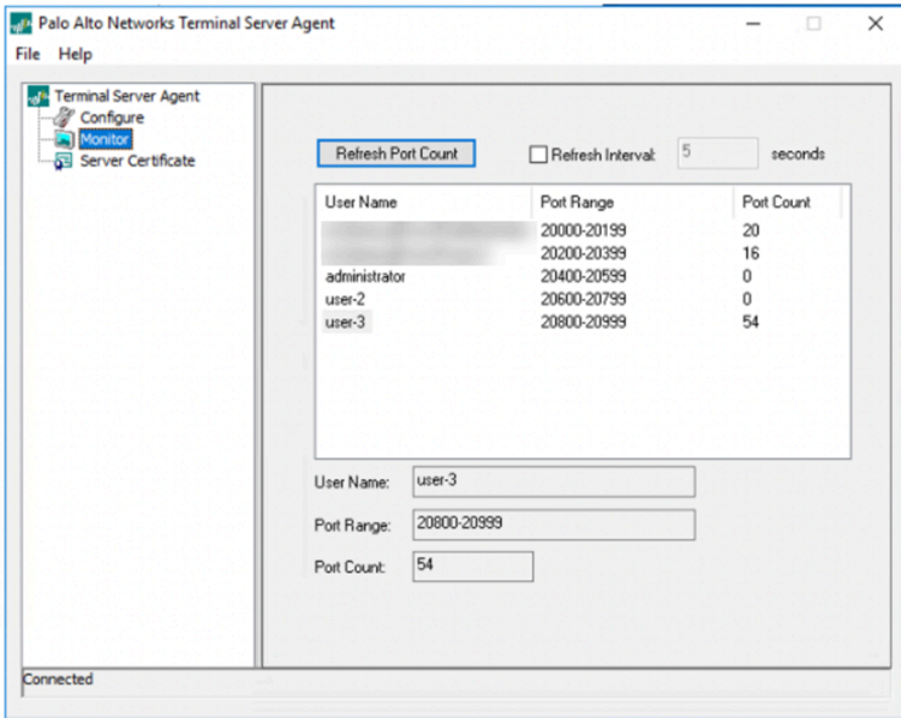
- **Applications, Services and URLs (Applications, services et URL)** : ajoutez **paloalto-terminal-svcs-agent** aux **Application Entities (Entités d'application)**.



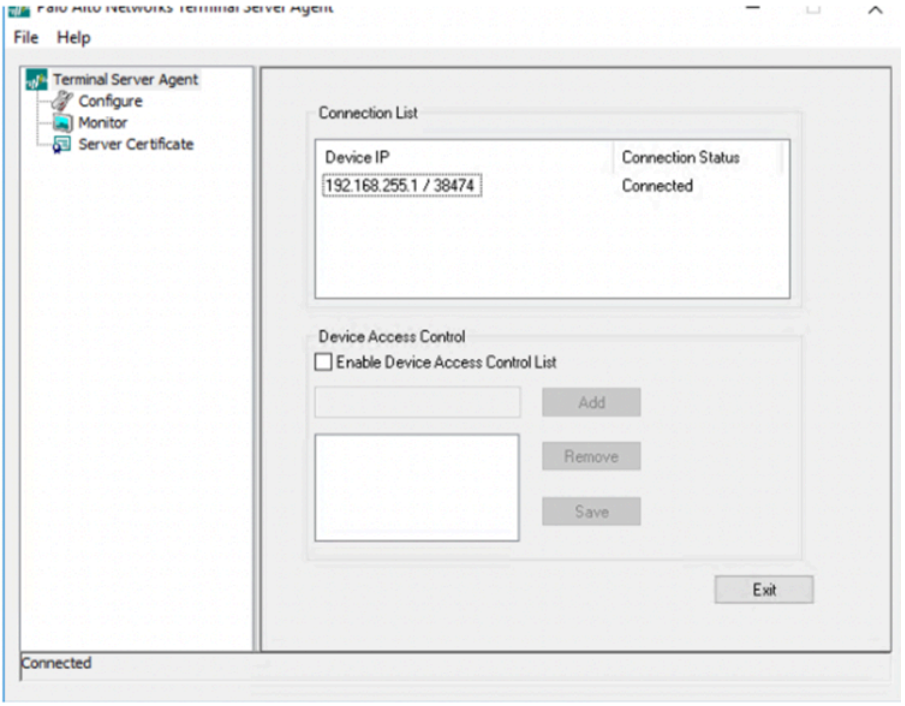
 ©2025 Palo Alto Networks, Inc.

STEP 6 | Vérifiez que la mise en œuvre fonctionne correctement.

1. Dans l'agent TS, utilisez l'option **Monitor (Surveiller)** pour surveiller son état et vérifiez que l'agent TS reflète le bon mappage entre le nom d'utilisateur et le port.

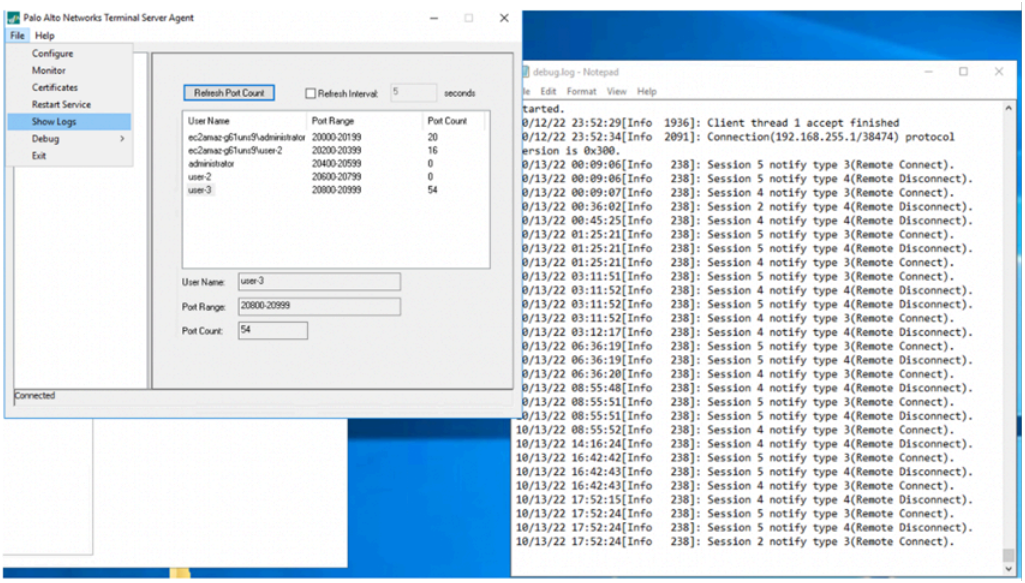


2. Vérifiez que l'adresse IP du réseau distant est connectée à l'agent TS.

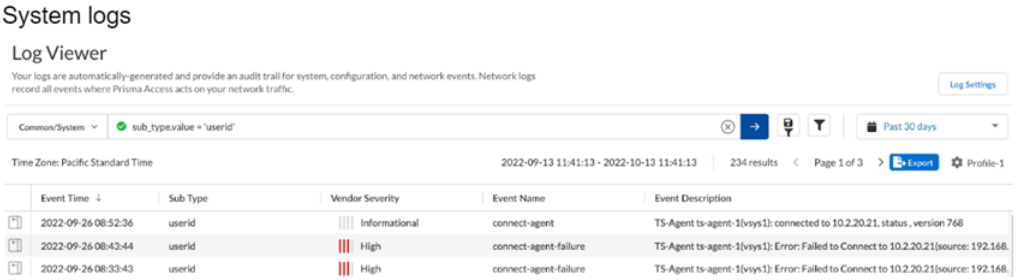


3. Accédez à **File (Fichier)** > **Show Logs (Afficher les journaux)** et consultez les messages de journal de l'agent TS.

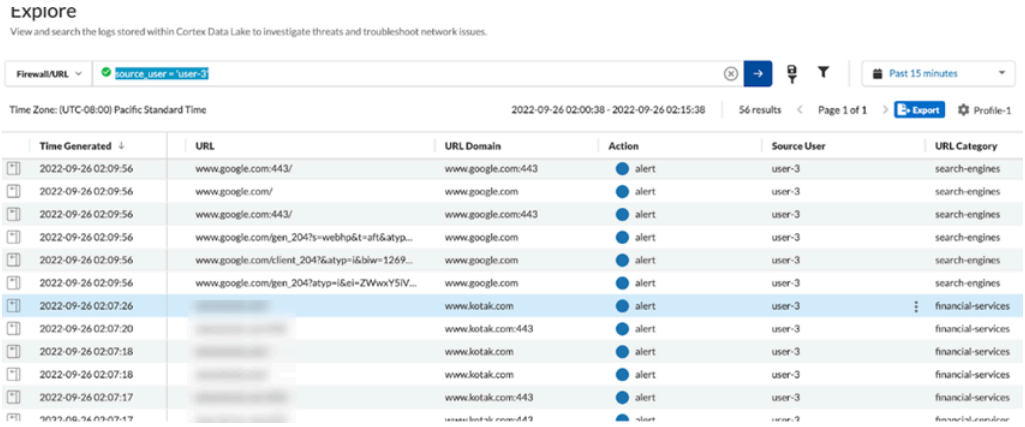
 ©2025 Palo Alto Networks, Inc.



4. Dans Prisma Access (Managed by Strata Cloud Manager), accédez à **Activity (Activité)** > **Log Viewer (Visionneuse de journaux)** > **Common/System (Commun/Système)** et vérifiez que les réseaux distants peuvent se connecter à l'agent TS.



5. Accédez à **Activity (Activité)** > **Log Viewer (Visionneuse de journaux)** > **Firewall/URL (Pare-feu/URL)** et vérifiez que les réseaux distants sont en mesure d'appliquer des politiques basées sur l'identité.



 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Surveillance et visibilité de Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Licence ADEM Observability requise pour l'accès à Autonomous DEM.

Prisma Access fournit les fonctionnalités suivantes pour vous permettre d'obtenir un aperçu de votre activité de sécurité et de surveiller votre déploiement. Ces fonctionnalités offrent une visibilité sur le trafic réseau et utilisateur via des journaux, des notifications d'alerte sur les réseaux distants, les connexions aux services, les utilisateurs mobiles et vos entités sous licence, ainsi que des tableaux de bord interactifs. Vous profitez ainsi d'une vue complète des données sur les applications, les menaces, les utilisateurs et les abonnements de sécurité à l'œuvre sur votre réseau. Vous pouvez également surveiller Prisma Access dans Strata Cloud Manager.

- Journaux Prisma Access

  Vos journaux sont automatiquement générés et fournissent une piste d'audit pour les événements système, de configuration et de réseau. Les journaux de réseau enregistrent tous les événements au cours desquels Prisma Access agit sur votre trafic réseau. Par exemple, des entrées sont enregistrées lorsque Prisma Access bloque le trafic en raison d'une règle de sécurité, accorde un accès à un utilisateur sur la base d'une règle d'authentification ou façonne le trafic conformément à une règle QoS. Vous pouvez consulter les journaux Prisma Access dans Strata Cloud Manager et les interfaces de gestion Panorama.
- Prisma Access Tableaux de bord et rapports Activité

  La fonctionnalité Activity (Activité) vous offre une vue complète de ce qui se passe sur votre réseau, depuis vos données de journal jusqu'aux résultats clés que vous pouvez utiliser pour mettre à jour les politiques de façon ciblée et combler les lacunes en matière de sécurité de l'entreprise et de productivité des utilisateurs.
- Surveiller Prisma Access dans Strata Cloud Manager
- Obtenez une visibilité complète sur l'ensemble de votre trafic réseau et sur les produits et abonnements que vous gérez à l'aide des sections Monitor (Surveiller) et Workflows (Flux de travail) de Strata Cloud Manager.
- Prisma Access et Autonomous DEM

  Autonomous DEM fournit une visibilité et des informations natives de bout en bout sur tout le trafic utilisateur dans votre SASE (Strata Cloud Manager). La fonctionnalité Autonomous DEM étant nativement intégrée à l'application GlobalProtect et à Prisma Access, vous n'avez pas besoin de déployer des appareils ou des agents supplémentaires. Vous pouvez rapidement isoler la source des problèmes d'expérience numérique et simplifier la correction.

- Centre de commande de Strata Cloud Manager

  Le centre de commande est un résumé visuel et interactif des périphériques IoT, des utilisateurs, des hôtes et du trafic sur votre réseau. S'appuyant sur les données de vos abonnements ADEM et de sécurité en mode cloud, le centre de commande révèle d'importantes informations sur les menaces, l'expérience utilisateur et la sécurité des données sur votre réseau.

  Le centre de commande vous permet d'interagir avec les données et de visualiser les relations entre les événements sur le réseau. Ainsi, vous pouvez identifier les anomalies ou trouver des améliorations à apporter à votre sécurité réseau.

 ©2025 Palo Alto Networks, Inc.

Journaux Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Un journal est un fichier horodaté généré automatiquement qui fournit une piste d'audit pour des événements systèmes ou des événements de trafic réseau surveillé par Prisma Access. Les entrées de journal contiennent des artefacts, qui sont des propriétés, des activités ou des comportements associés avec l'événement journalisé, tels que le type d'application ou l'adresse IP d'un pirate. Chaque type de journal enregistre des informations sur un type d'événement distinct. Par exemple, Prisma Access peut générer un journal des menaces pour enregistrer le trafic correspondant à une signature de logiciel espion, de vulnérabilité ou de virus. Prisma Access (Managed by Strata Cloud Manager) fournit des journaux de réseau (tels que le trafic, les menaces, les URL, les fichiers, la correspondance HIP), des journaux des terminaux et des journaux communs (système et configuration). Vous pouvez afficher les détails de chaque entrée de journal et, pour les journaux des menaces, vous pouvez consulter les détails des menaces et voir s'il existe des remplacements des menaces en place.

- Strata Cloud Manager
- Panorama

Journaux Prisma Access (Strata Cloud Manager)

Si vous utilisez **Strata Cloud Manager**, accédez à **Incidents & Alerts (incidents et alertes)** > **Log Viewer (Visionneuse de journaux)**.

Prisma Access (Managed by Strata Cloud Manager) fournit des journaux de réseau (trafic, menace, URL, fichier, correspondance HIP) et des journaux communs (système et configuration).

Vous pouvez afficher les détails de chaque entrée de journal. Pour les journaux des menaces, vous pouvez également examiner les détails des menaces et voir si des remplacements de menaces sont en place. En savoir plus.

Journaux Prisma Access (Panorama)

Vous pouvez également consulter les journaux Prisma Access dans l'interface Prisma Access (Managed by Panorama). L'infrastructure Prisma Access transmet tous les journaux à Strata Logging Service. Prisma Access récupère les résultats de journal depuis Strata Logging Service à l'aide du plug-in Cloud Services et fournit une vue agrégée des journaux du trafic des réseaux distants et des utilisateurs mobiles. Quelle que soit l'interface de gestion que vous utilisez pour Prisma Access (Panorama ou Strata Cloud Manager), vous pouvez afficher vos journaux dans Prisma Access (Managed by Strata Cloud Manager) sous **Activity (Activité)** > **Logs (Journaux)** > **Log Viewer (Visionneuse de journaux)**.

 ©2025 Palo Alto Networks, Inc.

En plus des journaux de l'infrastructure du service cloud Prisma Access, vous pouvez afficher les journaux directement à partir de l'appareil Panorama qui gère Prisma Access. Pour afficher les journaux, accédez à **Monitor (Surveiller) > Logs (Journaux)**. En savoir plus.

 ©2025 Palo Alto Networks, Inc.

Journaux externes et autres données

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Vous avez peut-être déjà l'habitude de consulter et d'interagir avec les journaux Prisma Access qui sont stockés dans le Strata Logging Service de **Activity (Activité)** > **Logs (Journaux)**. Mais, saviez-vous que Prisma Access prend également en charge l'ingestion de journaux et d'autres données provenant de diverses sources externes tierces lorsque vous avez un lac de données de licence Cortex XDR Pro per TB ? Une fois que vous êtes prêt, vous pouvez utiliser l'application Strata Logging Service sur la plateforme pour afficher les journaux et configurer le transfert des journaux. Les fournisseurs pris en charge comprennent :

• Activer le collecteur d'événements Windows	• Corelight Zeek	• PAN IoT Security
• Amazon S3	• ElasticSearch Filebeat	• PingFederate
• Apache Kafka	• Forcepoint DLP	• PingOne for Enterprise
• AWS	• Fortinet Fortigate	• Prisma Cloud
• AWS CloudTrail et Amazon CloudWatch	• Google Cloud Platform	• Prisma Cloud Compute
• Azure Event Hub	• Google Kubernetes Engine	• Proofpoint Targeted Attack Protection
• Azure Network Watcher	• Google Workspace	• ServiceNow CMDB
• BeyondTrust Privilege Management Cloud	• Microsoft Azure	• Windows DCHP à l'aide d'Elasticsearch Filebeat
• Check Point FW1/VPN1	• Microsoft Office 365	• Workday
• Cisco ASA	• Okta	• Pare-feu cloud Zscaler

Vous pouvez utiliser les journaux ingérés à partir de sources tierces comme seule source de données ou, vous pouvez utiliser ces journaux conjointement avec les journaux de Palo Alto Networks Prisma Access et des sources de données supplémentaires.

Avec Palo Alto Networks, réduisez votre charge opérationnelle et simplifiez radicalement vos opérations SOC en collectant, intégrant et normalisant les données de toutes les sources de données : réseau, terminaux et cloud. Obtenez une vue unifiée et des informations exploitables sur l'utilisation des applications, les modèles de trafic, les menaces et les incidents dans votre entreprise.

 ©2025 Palo Alto Networks, Inc.

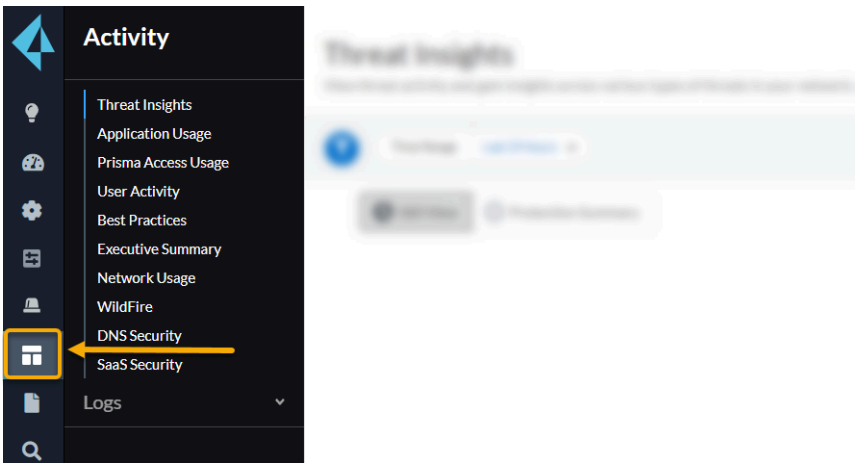
Prisma Access Tableaux de bord et rapports Activité

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	❑ Licence Prisma Access ❑ Revoir les licences et autres exigences pour les tableaux de bord et les rapports d'activité

L'activité identifie les principaux résultats que vous pouvez utiliser pour éclairer les mises à jour de vos politiques, et combler les lacunes en matière de sécurité de l'entreprise et de productivité des utilisateurs. L'activité vous fournit :

- Des tableaux de bord interactifs dans lesquels vous pouvez examiner les données des applications, des menaces, des utilisateurs et des abonnements de sécurité à l'œuvre sur votre réseau ;
- des rapports que vous pouvez partager hors ligne et pour lesquels vous pouvez planifier des mises à jour régulières ;
- la Visionneuse de journaux, qui fournit une piste d'audit pour les événements du système, de configuration et de réseau. Vous pouvez passer des tableaux de bord à la Visionneuse de journaux pour obtenir plus de contexte et explorer les données ;
- la fonction Rechercher d'artefacts de sécurité, qui vous permet d'effectuer des recherches sur des artefacts d'éléments tels qu'un hachage de fichier, une URL, un domaine ou une adresse IP (IPv4 ou IPv6) pour interagir avec les données de cet artefact uniquement. Les résultats de la recherche incluent l'historique de l'artefact, les renseignements sur les menaces concernant l'artefact et les résultats d'analyses tierces de l'artefact.

Les utilisateurs Prisma Access (Managed by Strata Cloud Manager) et Panorama Managed Prisma Access peuvent utiliser **Activity (Activité)** dans l'application Prisma Access (Managed by Strata Cloud Manager). Pour commencer, lancez Prisma Access (Managed by Strata Cloud Manager) et cliquez sur l'onglet **Activity (Activité)** dans le volet de navigation de gauche.



 ©2025 Palo Alto Networks, Inc.

L’outil Informations est pris en charge dans le cadre de la certification FedRAMP High « In Process » de Prisma SASE. L’outil Activité est pris en charge dans le cadre de la certification FedRAMP High « In Process » de Prisma SASE.

- Premiers pas avec l’activité

 ©2025 Palo Alto Networks, Inc.

Afficher et surveiller Prisma Access dans Strata Cloud Manager

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Il s'agit d'une fonctionnalité Prisma Access Insights.

Le centre de commande de Strata Cloud Manager de Palo Alto Networks est une plateforme de sécurité réseau alimentée par l'IA. Avec Strata Cloud Manager et le centre de commande Strata Cloud Manager, vous pouvez facilement gérer votre infrastructure de sécurité réseau Palo Alto Networks à partir d'une interface utilisateur unique et rationalisée.

Vous pouvez obtenir une visibilité complète sur l'ensemble de votre trafic réseau et sur les produits et abonnements que vous gérez à l'aide des Activity Insights (Informations sur l'activité) et des sections Monitor (Surveiller) et Workflows (Flux de travail) du centre de commande.

- **View and Monitor Applications (Afficher et surveiller les applications)** : accédez à **Activity Insights (Informations sur l'activité)** > **Applications** pour obtenir des informations sur les applications que vous utilisez.
- **View and Monitor App Acceleration (Afficher et surveiller l'accélération des applications)** : l'accélération des applications s'attaque aux causes des mauvaises performances des applications et agit en temps réel pour les atténuer, améliorant ainsi l'expérience utilisateur pour les utilisateurs de Prisma Access GlobalProtect et de réseaux distants. Accédez à **Activity Insights (Informations sur l'activité)** > **Applications** pour afficher des détails sur toutes les applications accélérées.
- **View Mobile Users (Afficher les utilisateurs mobiles)** – **All Users (Tous les utilisateurs)** fournit un aperçu de tous les utilisateurs connectés aux solutions de sécurité de Palo Alto Networks, y compris le pare-feu nouvelle génération (NGFW) et Prisma Access. Vous pouvez facilement déterminer l'état de la connexion d'un utilisateur au NGFW ou à Prisma Access, que ce soit sur un site de succursale, une connexion aux services ou un emplacement distant. Accédez à **Activity Insights (Informations sur l'activité)** > **Insights (Informations)** > **Users (Utilisateurs)** pour afficher des informations sur les **utilisateurs de l'agent** Prisma Access, les **utilisateurs proxy sans agent**, les **utilisateurs de bureau** et les **autres utilisateurs**.
- **View and Monitor Branch Sites (Afficher et surveiller les sites des succursales)** : accédez à **Monitor (Surveiller)** > **Branch Sites (Sites des succursales)** > **Prisma Access** pour afficher l'état et la connectivité de vos réseaux distants et l'utilisation de tous vos réseaux distants déployés dans différents emplacements Prisma Access. Cette section indique en temps réel l'état de la connectivité et les détails de la consommation de la bande passante ainsi que d'autres détails du déploiement. Les utilisateurs mobiles, les succursales et les points de vente se connectent à des réseaux distants. Vous pouvez également consulter l'état des tunnels configurés dans vos réseaux distants et chez vos utilisateurs mobiles.
- **View and Monitor Data Centers (Afficher et surveiller les centres de données)** : accédez à **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **Service Connections (Connexions**

 ©2025 Palo Alto Networks, Inc.

aux services) pour afficher les données agrégées des connexions aux services ainsi que des informations sur les connexions aux services individuelles.

Accédez à **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **ZTNA Connectors (Connecteurs ZTNA)** pour afficher l'intégrité et l'état d'un groupe de connecteurs ZTNA et de connecteurs ZTNA individuels.

- Accédez à **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **ZTNA Access Objects (Objets d'accès ZTNA)** pour obtenir une visibilité sur les objets d'accès de connecteur ZTNA.
- **View and Monitor Network Services (Afficher et surveiller les services réseau)** : accédez à **Monitor (Surveiller)** > **Network Services (Services réseau)** > **GlobalProtect Authentication (Authentification GlobalProtect)** pour afficher les performances des services réseau courants qui affectent l'expérience utilisateur lors de l'accès aux applications. Les services réseau incluent le signalement des authentifications GlobalProtect réussies et infructueuses. Cette mesure permet d'évaluer la capacité des utilisateurs mobiles à se connecter à Prisma Access. Accédez à **Monitor (Surveiller)** > **Network Services (Services réseau)** > **DNS** pour afficher les demandes de proxy DNS et les réponses transmises aux serveurs au cours de l'intervalle de temps spécifié.
- **View and Monitor Subscription Usage (Afficher et surveiller l'utilisation de l'abonnement)** : sélectionnez **Monitor (Surveiller)** > **Subscription Usage (Utilisation de l'abonnement)** pour afficher des détails sur les **Prisma Access Base Subscriptions (Abonnements Prisma Access de base)**, y compris le nombre de licences que vous avez consommées jusqu'à présent.
- **View and Monitor Prisma Access Locations (Afficher et surveiller les emplacements Prisma Access)** : accédez à **Monitor (Surveiller)** > **Prisma Access Locations (Emplacements Prisma Access)** pour voir un aperçu de l'intégrité de tous vos emplacements Prisma Access pour vos réseaux distants et utilisateurs mobiles. Vous pouvez sélectionner un intervalle de temps pour consulter l'état des emplacements Prisma Access et la connectivité Strata Logging Service pendant cette période, afficher un tableau qui répertorie tous les emplacements Prisma Access et sélectionner un emplacement Prisma Access individuel à l'aide de son nom pour afficher ses détails.
- **View Prisma Access Upgrades (Afficher les mises à niveau de Prisma Access)** : sélectionnez **Workflows (Flux de travail)** > **Software Upgrades (Mises à niveau logicielles)** > **Prisma Access** pour afficher des informations sur le processus de mise à niveau de Prisma Access.
- **View and Monitor Third-Party Device-IDs (Afficher et surveiller les Device-ID tiers)** : accédez à **Monitor (Surveiller)** > **Devices (Périphériques)** > **IOT** pour obtenir des informations sur vos périphériques IoT, comme le nombre de périphériques IoT connectés au cours des 30 dernières minutes, tous les périphériques IoT connectés au cours de l'intervalle de temps sélectionné et des détails sur tous les périphériques IoT connectés.
- **View and Monitor Remote Browser Isolation (Afficher et surveiller l'isolation de navigateur à distance)** : sélectionnez **Monitor (Surveiller)** > **Users (Utilisateurs)** pour obtenir une visibilité sur votre déploiement RBI et afficher des mesures telles que le nombre d'utilisateurs RBI actifs, les tendances, l'état de la connectivité, l'état de l'emplacement RBI, les mesures du trafic et la consommation des licences.

 ©2025 Palo Alto Networks, Inc.

Premiers pas avec la surveillance de Prisma Access dans Strata Cloud Manager

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Il s'agit d'une fonctionnalité de Prisma Access Insights.

Prisma Access vous offre un moyen de surveiller en permanence votre environnement Prisma Access dans Strata Cloud Manager Command Center. Plusieurs tableaux de bord vous offrent des vues spécifiques de vos différents déploiements, de vos alertes et de l'infrastructure Prisma Access. Lorsqu'un événement ou un état requiert votre attention, Prisma Access vous envoie des notifications d'alerte pour vous permettre d'identifier rapidement les problèmes que vous pouvez résoudre. Il vous donne également la visibilité sur les correctifs sur lesquels l'équipe Prisma Access travaille. Vous pouvez filtrer les données que vous souhaitez afficher en sélectionnant ou en définissant un intervalle de temps et afficher les informations de référence dans les pages Monitor (Surveillance) avec une licence Autonomous DEM.

Filtre de sélection d'intervalle de temps

Le filtre de sélection **Time Range (Intervalle de temps)** s'affiche en haut des tableaux de bord où vous souhaitez filtrer les informations par intervalle de temps.

L'heure est localisée, vous pouvez donc filtrer en fonction de l'heure locale de votre région. Les données sont récupérées toutes les minutes, mais les points de données affichés dans la plupart des histogrammes varient en fonction du **Time Range (Intervalle de temps)** sélectionné.

Pour votre commodité, Prisma Access vous permet de choisir le **Time Range (Intervalle de temps)** parmi quelques intervalles prédéfinis ou de configurer votre propre intervalle de temps (date et heure) :

- **15 dernières minutes**

  1 point de données toutes les 3 minutes pour un total de 5 points de données.
- **Dernière heure**

  1 point de données toutes les 3 minutes pour un total de 20 points de données.
- **3 dernières heures**

  1 point de données toutes les 3 minutes pour un total de 60 points de données.
- **24 dernières heures**

  1 point de données toutes les 5 minutes pour un total de 288 points de données.
- **7 derniers jours**

  1 point de données toutes les 30 minutes, pour un total de 336 points de données.
- **30 derniers jours**

  1 point de données toutes les 3 heures, pour un total de 180 points de données.

 ©2025 Palo Alto Networks, Inc.

- **Personnalisé**

  Vous pouvez définir un intervalle de temps personnalisé (par exemple, la date et l'heure commencent à 17 h 00 le 1er juin et se terminent à 16 h 00 le 2 juin) en plus des sélections de **Time Range (Intervalle de temps)** préremplies disponibles dans le filtre.

  Pour définir une heure de début, sélectionnez d'abord la date dans le calendrier, puis sélectionnez l'heure sous **Start (Début)**. **Apply (Appliquez)** l'heure de début, puis définissez l'heure de fin en sélectionnant une date de fin dans le calendrier et une heure sous **End (Fin)**.

  Une fois que vous avez défini un intervalle de temps personnalisé, celui-ci est enregistré et appliqué à tous les widgets d'Insights qui utilisent le filtre d'intervalle de temps pour afficher des données au lieu de données en temps réel.

  Vous pouvez choisir parmi des sélections de **Time Range (Intervalle de temps)** préremplies pour les intervalles de temps personnalisés :

  - **15 dernières minutes**

    1 point de données toutes les 3 minutes pour un total de 5 points de données.
  - **Dernière heure**

    1 point de données toutes les 3 minutes pour un total de 20 points de données.
  - **3 dernières heures**

    1 point de données toutes les 3 minutes pour un total de 60 points de données.
  - **24 dernières heures**

    1 point de données toutes les 5 minutes pour un total de 288 points de données.
  - **48 dernières heures**

    1 point de données toutes les 30 minutes pour un total de 96 points de données.
  - **7 derniers jours**

    1 point de données toutes les 30 minutes pour un total de 336 points de données.
  - **30 derniers jours**

    1 point de données toutes les 3 heures pour un total de 240 points de données.

Références dans les widgets

Si vous avez acheté la licence AI-Powered ADEM, vous voyez une bande de données de référence sur les widgets de tendances dans les pages Monitor (Surveillance) suivantes : Users (Utilisateurs), Branch Sites (Branches), Data Centers (Centres de données) et Network Services (Services réseau). Les widgets affichent la référence en arrière-plan sur les lignes de tendance. Cela vous permet de voir en un coup d'œil si vos données ont franchi les limites supérieure ou inférieure de la référence.

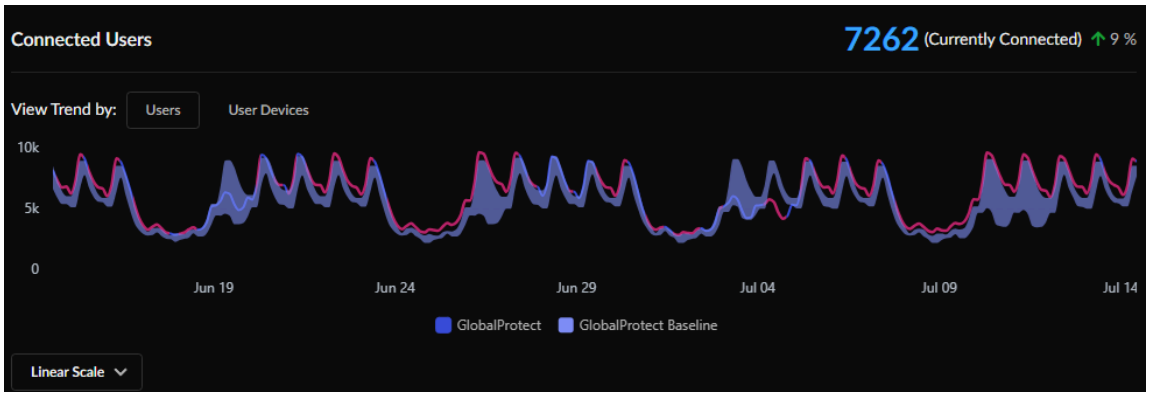
Les données de référence sont calculées en tailles d'emplacement de 1 heure et prennent en compte les données des 28 derniers jours de ces emplacements d'une heure pour un tunnel, un site, un emplacement Prisma Access ou un nombre d'utilisateurs GlobalProtect particulier. Par exemple, la référence de 13 h 00 à 14 h 00 le mardi est calculée à partir de l'intervalle de temps de 13 h 00 à 14 h 00 des quatre mardis précédents. La limite inférieure est le 10e centile des données historiques collectées, et la limite supérieure est son 90e centile. Cela vous permet de voir les tendances en matière de bande passante, de nombre d'utilisateurs, de

 ©2025 Palo Alto Networks, Inc.

nombre d'authentifications et de requêtes et de réponses de proxy DNS. Étant donné que les données de référence sont extraites des données historiques des 28 derniers jours, les locataires nouvellement intégrés devront être opérationnels et riches en données pendant 28 jours pour que la référence soit calculée correctement. Si vos données datent de moins de 28 jours, vous pouvez constater des anomalies.

Lorsque les valeurs de la ligne de tendance du widget s'écartent des limites supérieure ou inférieure de la référence, la ligne de tendance pour cette période s'affiche en rouge dans l'interface Web.

L'exemple suivant montre la référence GlobalProtect à partir du widget **Connected User (Utilisateur connecté)** de la page Users (Utilisateurs).



Afficher et surveiller les applications

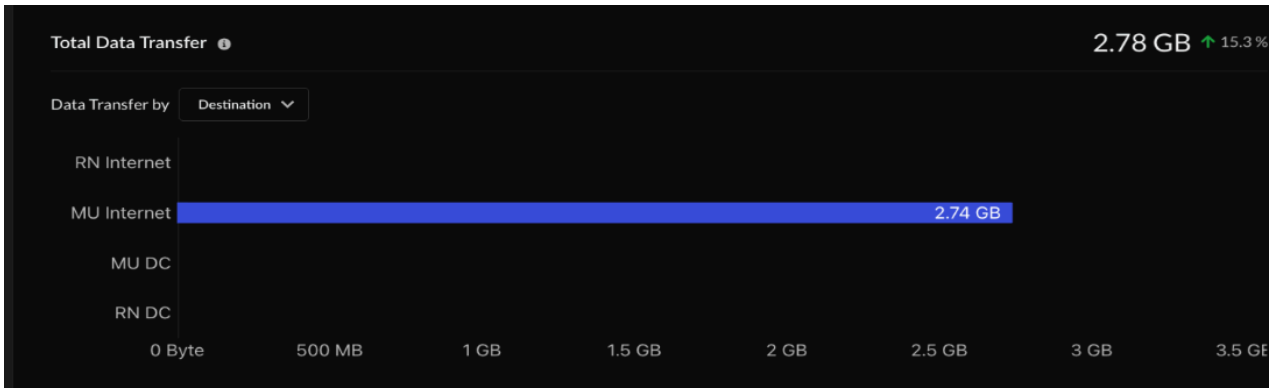
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Il s'agit d'une fonctionnalité Prisma Access Insights.

Utilisez le centre de commande de Strata Cloud Manager pour surveiller les applications Prisma Access de votre réseau, les utilisateurs qui utilisent l'application et leur impact potentiel sur la sécurité. Accédez à **Insights** > **Applications** pour obtenir une visibilité sur les applications Prisma Access ainsi que des informations sur les menaces, les utilisateurs, le transfert de données, les scores de risque et l'expérience utilisateur des applications.

Transfert de données total

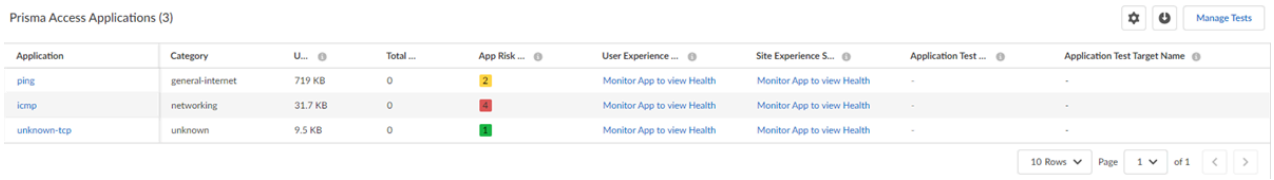
Total Data Transfer (Transfert de données total) vous montre le transfert de données total sur les pare-feu Prisma Access pendant l'intervalle de temps sélectionné. Utilisez la liste déroulante **Add Filter (Ajouter un filtre)** pour d'autres options de filtrage. Dans l'exemple, vous voyez le transfert de données par **Application Category (Catégorie d'application)**, qui affiche les principales applications et le transfert de données total pour ces applications. Vous pouvez également afficher le transfert de données total par **Destination**.

 ©2025 Palo Alto Networks, Inc.



Applications Prisma Access

Utilisez ce widget pour voir quelles applications sont surveillées avec des tests synthétiques exécutés sur elles. Le tableau affiche également leur score d'expérience, qui vous donne l'état de chaque application. Cliquez sur le bouton **Manage Tests (Gérer les tests)** afin d'afficher tous les tests synthétiques configurés pour toutes vos applications dans le tableau Application Test (Tests d'application).



Colonne	Description
Application	ID d'application de l'application surveillée.
Catégorie	Type d'application.
Usage	Trafic total dans l'infrastructure Prisma Access détectée pour l'application spécifique.
Nombre total de menaces	Nombre total de menaces rencontrées par l'application.
Score de risque de l'application	Données sur les menaces pour cette application spécifique. 1 est le risque le plus faible et 5 est le risque le plus élevé.
Expérience utilisateur	Scores d'expérience d'application collectés par Autonomous DEM. Il est agrégé pour tous les utilisateurs surveillés pour cette application.
Score de l'expérience du site	Score d'expérience d'application pour ce site de succursale spécifique.

 ©2025 Palo Alto Networks, Inc.

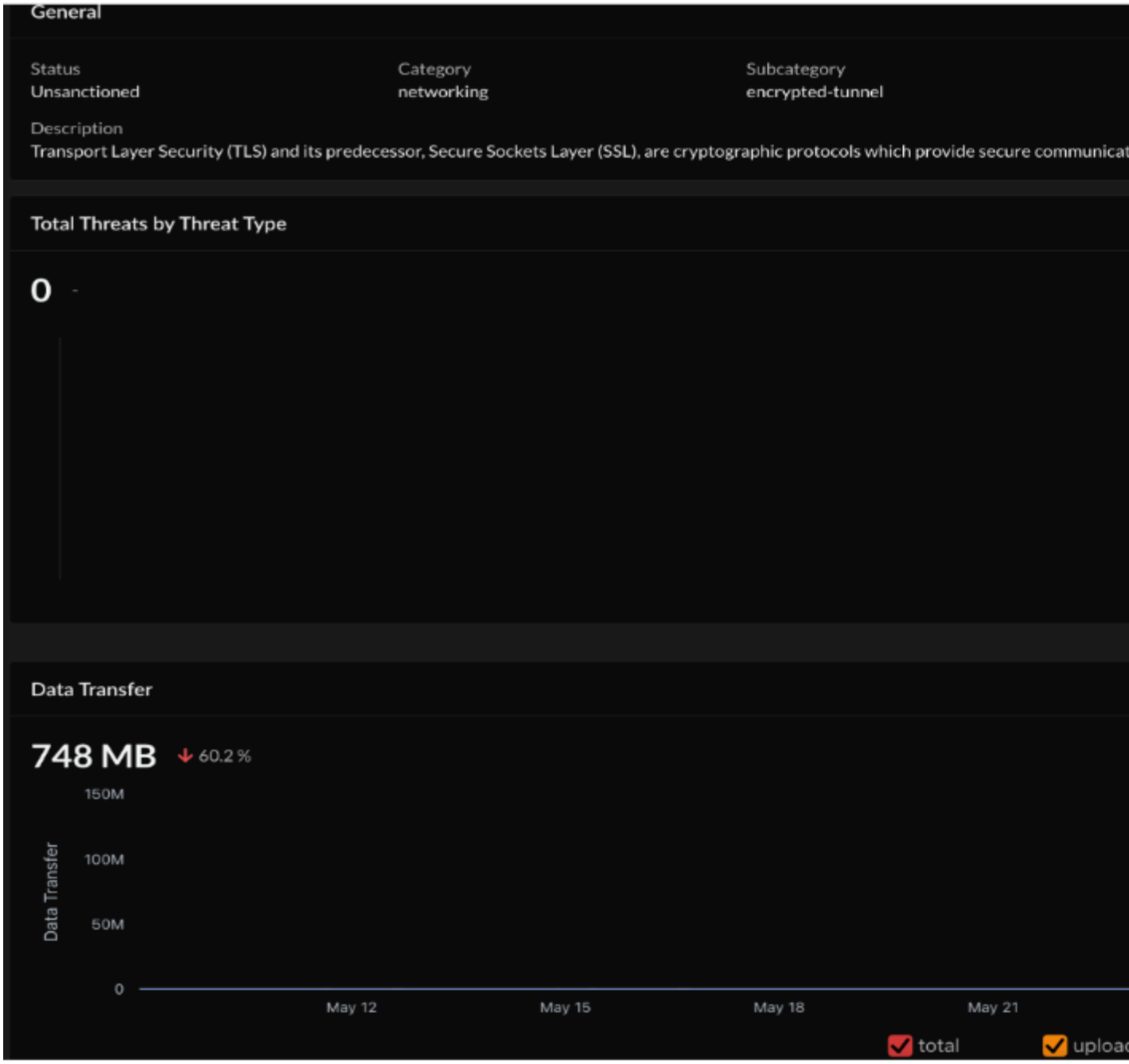
Colonne	Description
Nom du test d'application	Nom du test configuré par l'utilisateur pour cette application.
Nom de la cible de test d'application	Adresse IP du FQDN sur lequel les tests synthétiques sont ciblés à partir de différents terminaux.

Détails de l'application

Sélectionnez n'importe quelle application pour afficher ses détails **General (Généraux)**, tels que l'état, la catégorie, la sous-catégorie, les ports, la technologie et le score de risque.

- **Total Threats by Threat Type (Nombre total de menaces par type de menace)** : menaces actuelles pour l'application.
- **Total Users (Nombre total d'utilisateurs)** : nombre total d'utilisateurs accédant à cette application au cours de l'intervalle de temps spécifié.
- **Data Transfer (Transfert de données)** : consultez les données qui ont été chargées ou téléchargées pour cette application.

©2025 Palo Alto Networks, Inc.



Afficher et surveiller l'accélération des applications

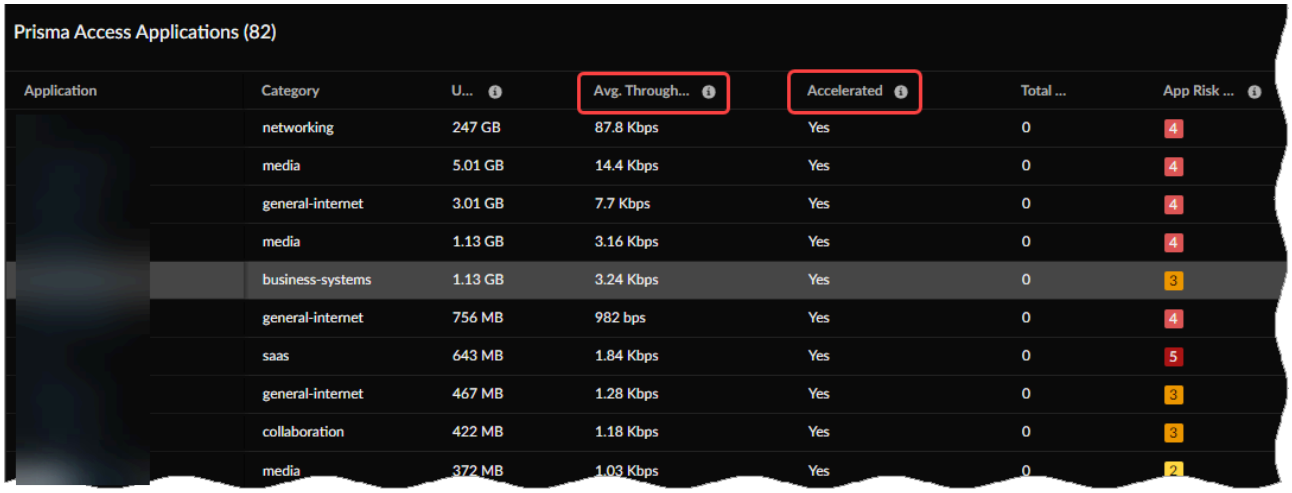
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

©2025 Palo Alto Networks, Inc.

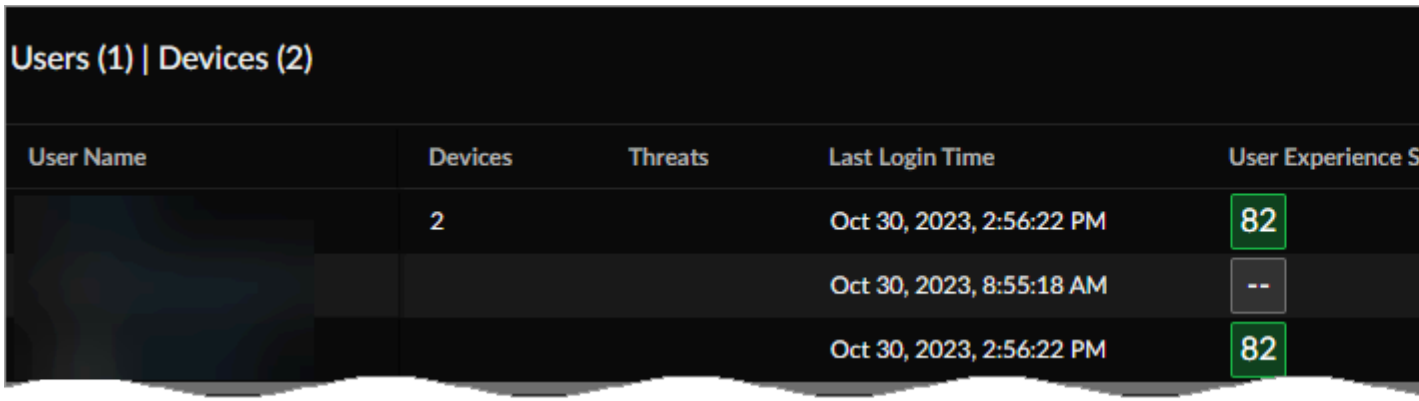
L'accélération des applications s'attaque aux causes des performances médiocres des applications et agit en temps réel pour les atténuer, améliorant ainsi l'expérience utilisateur pour les utilisateurs de GlobalProtect Prisma Access et de réseaux distants.

Lorsque vos utilisateurs accèdent à des applications, les performances des applications peuvent être médiocres en raison d'une diminution du débit, qui peut être causée par une connectivité sans fil dégradée, l'encombrement du réseau et d'autres facteurs. Ces problèmes de réseautage peuvent nuire à l'expérience des employés et réduire leur productivité. L'accélération des applications permet de comprendre en toute sécurité les capacités du périphérique, les capacités du réseau et le contexte de l'application afin d'optimiser le débit et s'ajuste en temps réel pour tenir compte de l'évolution des conditions du réseau.

Dans le centre de commande deStrata Cloud Manager, accédez à **Insights** > **Applications** pour afficher des détails sur les applications qui ont été accélérées dans votre environnement. Le tableau Applications Prisma Access comprend la colonne Avg. Throughout (Débit moyen), qui s'affiche uniquement si le trafic de votre utilisateur est accéléré, et la colonne Accelerated (Accélérée), qui indique qu'une partie ou la totalité du trafic de votre application a été accélérée.



Accédez à **Insights** > **Users (Utilisateurs)** pour afficher des informations sur les utilisateurs de l'accélération des applications dans votre environnement. Vos utilisateurs pour lesquels l'accélération des applications est activée dans leurs environnements disposent du tableau Users | Devices (Utilisateurs | Périphériques), qui affiche la colonne Traffic Accelerated (Trafic accéléré). Cette colonne indique qu'une partie ou la totalité du trafic des applications des utilisateurs a été accélérée.



 ©2025 Palo Alto Networks, Inc.

L'ADEM (Autonomous DEM alimenté par l'IA) s'intègre à l'accélération des applications et vous fournit des mesures telles que le nombre d'applications qui ont été accélérées et l'amélioration globale des performances obtenue. Accédez à **SASE Health (État SASE)** > **Experience (Expérience)** pour voir ADEM performance metrics (Indicateurs de performance ADEM) dans les onglets **Accelerated Applications (Applications accélérées)** et **Monitored Applications (Applications surveillées)**.

Afficher les utilisateurs mobiles

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma® Access (géré par Strata Cloud Manager)	• Licence Prisma Access • Licence ADEM alimentée par l'IA

Reportez-vous aux informations sur l'activité : utilisateurs pour une vue d'ensemble de tous les utilisateurs et hôtes connectés aux solutions de sécurité Prisma Access de Palo Alto Networks. Vous pouvez facilement déterminer l'état de connexion d'un utilisateur ou d'un hôte à Prisma Access, que ce soit sur un site de succursale, une connexion aux services ou un emplacement distant. Affichez :

- Le nombre total d'utilisateurs uniques actuellement connectés aux solutions de sécurité de Palo Alto Networks et aux utilisateurs connectés à Prisma Access.
- Le nombre d'utilisateurs connectés pendant un certain intervalle de temps, subdivisé selon les utilisateurs connectés via Prisma Access.
- Les utilisateurs basés sur des agents connectés via Prisma Access.
- Les utilisateurs de proxy explicite basés sur un agent ou sur un navigateur connectés à Prisma Access.
- Les utilisateurs connectés via les Prisma Access Browsers.
- Une liste d'utilisateurs de périphériques non gérés accédant à Prisma Access.
- Une liste d'utilisateurs se connectant depuis des sites de succursales à Prisma Access.
- Une liste d'utilisateurs connectant leurs centres de données en utilisant des connexions aux services spécifiques.

Afficher et surveiller IPv6 pour les utilisateurs mobiles

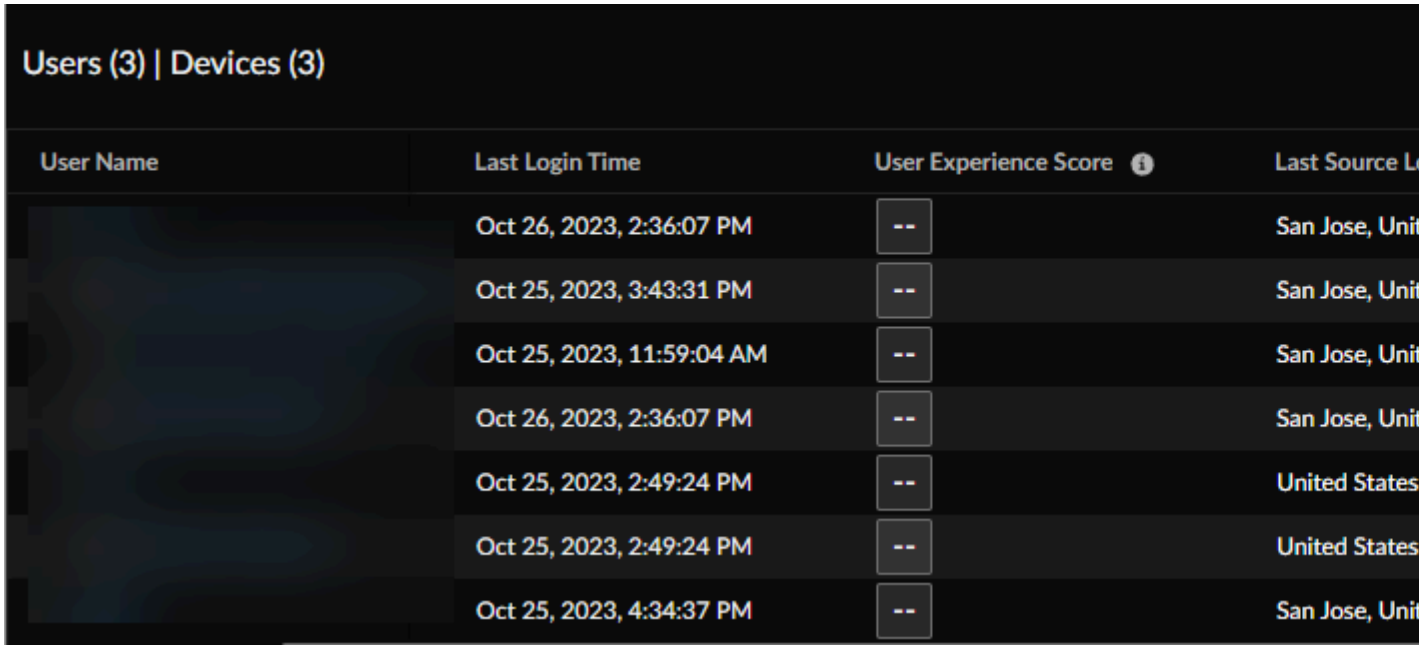
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Innovation Prisma Access 5.0 ❑ Licence Prisma Access

Si vous utilisez la mise en réseau IPv6 dans votre déploiement Utilisateurs mobiles – GlobalProtect, vous pouvez configurer Prisma Access pour utiliser des adresses IPv6 dans votre

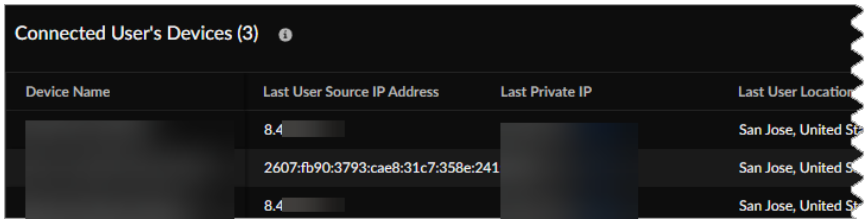
 ©2025 Palo Alto Networks, Inc.

réseau d'utilisateurs mobiles. Vous devez également activer la mise en réseau IPv6 globalement dans votre infrastructure Prisma Access avant de pouvoir utiliser l'adressage IPv6.

Avec IPv6 dans votre déploiement GlobalProtect, le tableau Users | Devices (Utilisateurs | Périphériques) affiche une adresse IPv4 ou IPv6 dans la colonne Source IP Address (Adresse IP source).

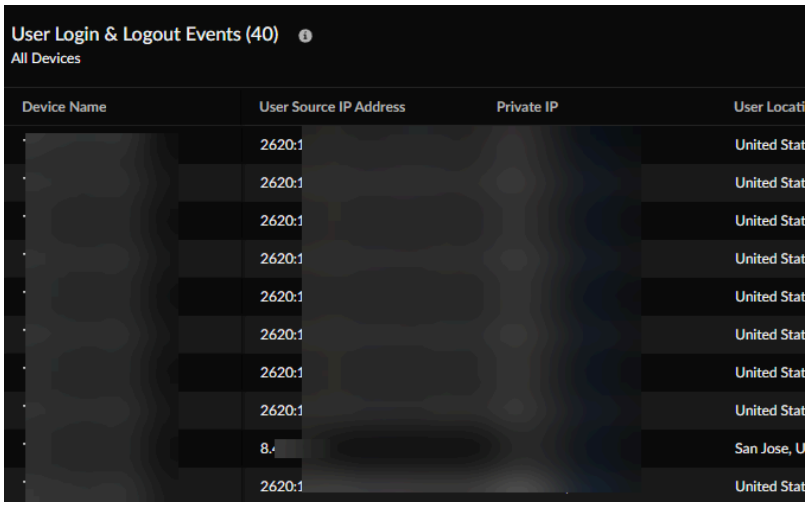


Sélectionnez n'importe quel utilisateur connecté pour afficher des informations sur la tendance de ses périphériques. Le tableau Connected User's Devices (Périphériques utilisateur connectés) affiche des données sur les périui d'un utilisateur, y compris l'adresse IP source du dernier utilisateur et la dernière adresse IP privée, qui peuvent toutes deux inclure des adresses IPv4 et IPv6 pour une seule entrée de périphérique.



Vous pouvez afficher les informations d'adresse IPv6 dans le tableau User Login & Logout Events (Événements de connexion et de déconnexion de l'utilisateur). Les colonnes User Source IP Address (Adresse IP source de l'utilisateur) et Private IP Address (Adresse IP privée) affichent une adresse IPv4 ou IPv6.

 ©2025 Palo Alto Networks, Inc.



Afficher et surveiller les sites des succursales

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ adem-aiops-valeur

Sélectionnez**Monitor (Surveiller)** > **Branch Sites (Sites de succursales)** > **Prisma Access** pour afficher l'état et la connectivité de vos réseaux distants et l'utilisation de tous vos réseaux distants déployés dans différents emplacements Prisma Access. Il indique en temps réel l'état de la connectivité et les détails de la consommation de la bande passante, ainsi que d'autres détails du déploiement. Vous pouvez également afficher l'état des tunnels configurés dans vos réseaux distants.

Reportez-vous aux réseaux distants Prisma Access pour plus d'informations sur la planification de vos réseaux distants, l'allocation de bande passante des réseaux distants et l'intégration des réseaux distants. Pour afficher vos sites de succursales, accédez à **Monitor (Surveiller)** > **Branch Sites (Sites de succursales)** > **Prisma Access**.

Sites par statut

Consultez les sites de vos réseaux distants en fonction de leur état en accédant à **Sites by Status (Sites par état)**. Vous pouvez voir combien de sites sont **Up (Actif)**, **Down (Inactif)**, **Inactive (Inactif)**ou **Not Available (Non disponible)**, et combien de sites ont un **Warning (Avertissement)** pendant le **Time Range (Intervalle de temps)** sélectionné.



 ©2025 Palo Alto Networks, Inc.

Consommation de bande passante

La **Bandwidth Consumption (Consommation de bande passante)** indique la bande passante maximale la plus élevée consommée dans une région de calcul sur toutes les régions de calcul du locataire dans le modèle d'allocation de bande passante agrégée. La bande passante maximale la plus élevée consommée par un site sur tous les sites est indiquée pour le modèle d'allocation de bande passante par site. Les valeurs maximales sont calculées pour la durée du filtre temporel sélectionné.

Sélectionnez **View Consumption by Compute Region (Afficher la consommation par région de calcul)** pour afficher les valeurs de consommation et les graphiques de tendance pour toutes les régions de calcul et leurs nœuds de fin IPSec configurés.

Afficher la consommation par régions de calcul

Accédez à **Monitor (Surveiller)** > **Branch Sites (Sites de succursales)** > **Prisma Access**. Lorsque vous utilisez le modèle d'allocation de bande passante agrégée, sélectionnez **View Consumption by Compute Regions (Afficher la consommation par régions de calcul)** dans le widget **Bandwidth Consumption (Consommation de bande passante)** pour voir la consommation de bande passante et les tendances pour vos régions.

La page **Compute Regions (Régions de calcul)** affiche les données de consommation de bande passante pendant le **Time Range (Intervalle de temps)** que vous sélectionnez. Vous pouvez afficher un tableau avec la **Average Bandwidth (Bande passante moyenne)**, la **Median Bandwidth (Bande passante médiane)** et la **Peak Bandwidth (Bande passante maximale)** de vos régions de calcul.

Le graphique **Bandwidth Consumption Trend by Compute Region (Tendance de consommation de bande passante par région de calcul)** affiche des données sur votre région de calcul. Filtrez les données pour affiner les informations que vous souhaitez afficher.

- Sélectionnez **Cumulative (Ingress + Egress) (Cumulée (Entrée + Sortie))**, **Ingress (Entrée)**, **Egress (Sortie)** ou **Ingress vs. Egress (Entrée versus Sortie)** à partir de la liste déroulante.
- Affichez la tendance de consommation de bande passante **Peak (Maximale)**, **Median (Médiane)** ou **Average (Moyenne)** pendant l'intervalle de temps sélectionné. Le paramètre par défaut est la consommation **Peak (Maximale)** de bande passante.
- **Log Scale (Échelle des journaux)** ou **Linear Scale (Échelle linéaire)**.
- **Compute Region (Région de calcul)** : sélectionnez une ou plusieurs régions à afficher.

Le graphique **IPSec Termination Node Utilization (Utilisation des nœuds de fin IPSec)** vous permet d'afficher la consommation de bande passante des nœuds de fin IPSec configurés dans une région de calcul spécifique. Filtrez les données pour affiner les informations que vous souhaitez afficher :

- Sélectionnez la région de calcul pour laquelle vous souhaitez afficher les données.
- Sélectionnez le site spécifique de la région de calcul que vous souhaitez voir.

 ©2025 Palo Alto Networks, Inc.

- Choisissez **Node Aggregate (Agrégation de nœuds)** ou **Breakdown by Sites (Répartition par sites)** pour afficher la tendance de consommation de bande passante pour les sites qui se terminent au nœud de fin IPSec sélectionné.
- Affichez la consommation **Peak (Maximale)**, **Average (Moyenne)**ou **Median (Médiane)**.
- Affichez **Log Scale (Échelle des journaux)** ou **Linear Scale (Échelle linéaire)**.



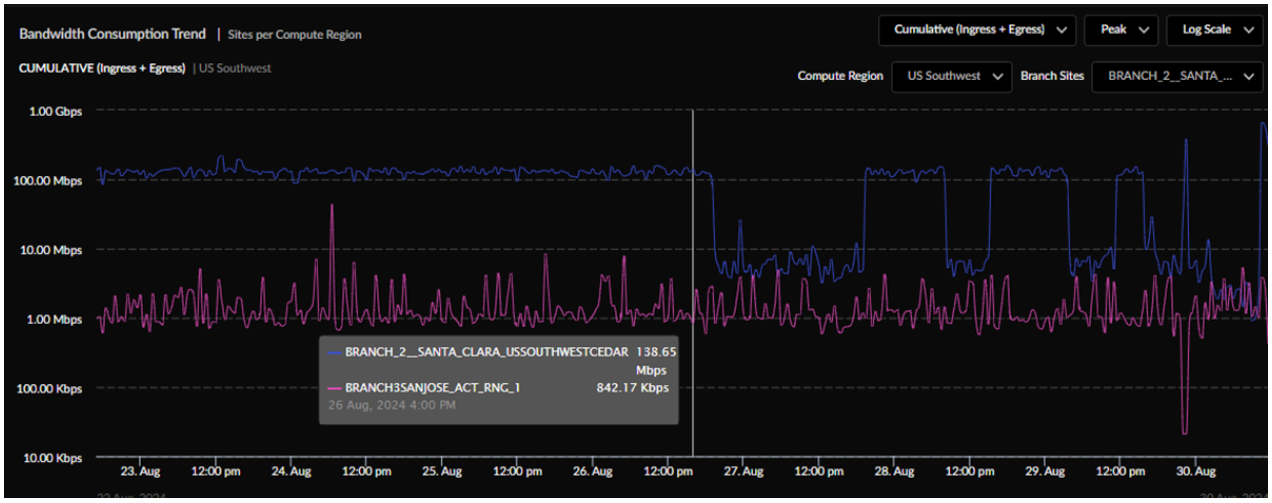
Tendance de consommation de la bande passante

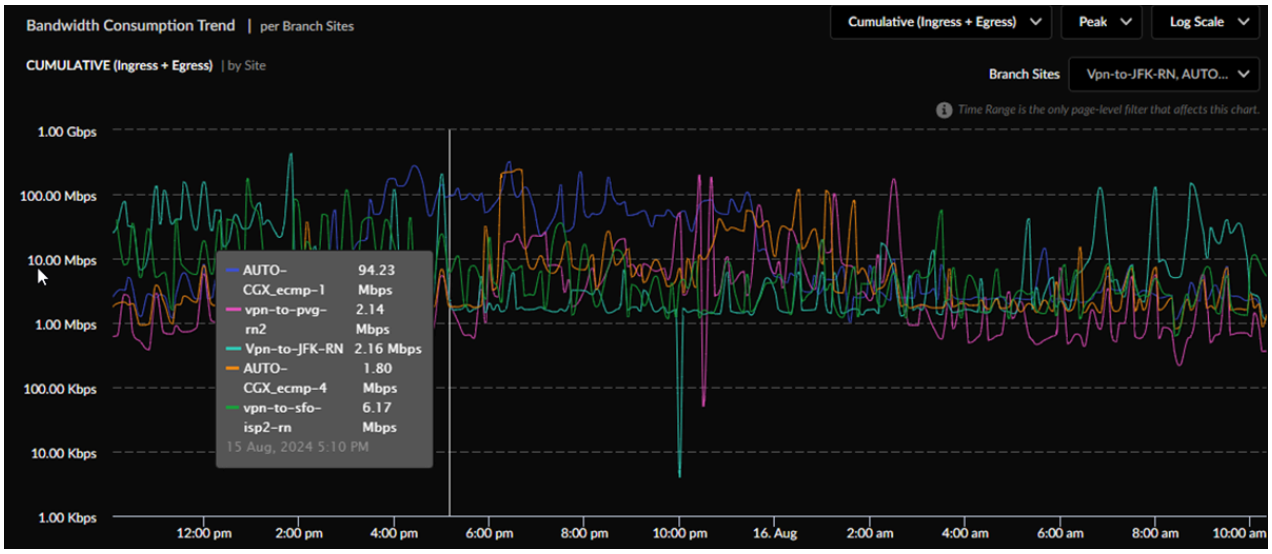
Sur la page principale **Branch Sites (Sites de succursales)**, vous pouvez afficher vos **Bandwidth Consumption Trend Sites per Compute Region (Sites de tendance de consommation de bande passante par région de calcul)** pour toutes les régions de calcul lorsque vous utilisez le modèle d'allocation de bande passante agrégée ou la **Bandwidth Consumption Trend per Branch Sites (Tendance de consommation de bande passante par sites de succursales)** lorsque vous utilisez le **Per-Site Bandwidth Allocation Model (Modèle d'allocation de bande passante par site)**. Pour le modèle d'allocation de bande passante agrégée, vous pouvez sélectionner une région de calcul, puis sélectionner les sites de cette région de calcul dont la tendance de consommation de bande passante vous intéresse. Filtrez les données pour affiner les informations que vous souhaitez

 ©2025 Palo Alto Networks, Inc.

afficher, et vous pouvez survoler le graphique avec la souris pour afficher la consommation de bande passante des sites à ce moment-là :

- La vue par défaut affiche la consommation de bande passante **Cumulative (Ingress + Egress) (Cumulée (Entrée + Sortie))**. Les autres options sont **Ingress (Entrée)**, **Egress (Sortie)** ou **Ingress vs. Egress (Entrée + Sortie)**.
- Affichez la tendance de consommation de bande passante **Peak (Maximale)**, **Median (Médiane)** ou **Average (Moyenne)** pendant l'intervalle de temps sélectionné. Le paramètre par défaut est la consommation **Peak (Maximale)** de bande passante.
- **Log Scale (Échelle des journaux)** ou **Linear Scale (Échelle linéaire)**.
- **Compute Region (Région de calcul)** : affichez les régions de calcul avec une répartition des sites se terminant dans la région lorsque le locataire utilise le modèle d'allocation de bande passante agrégée. Pour chaque région de calcul, sélectionnez les sites se terminant dans la région de calcul pour afficher leur tendance de consommation de bande passante.
- **Branch Sites (Sites de succursales)** : sélectionnez au moins 1 site et au maximum 10 sites pour afficher leurs lignes de tendance sur le graphique pendant l'intervalle de temps sélectionné.





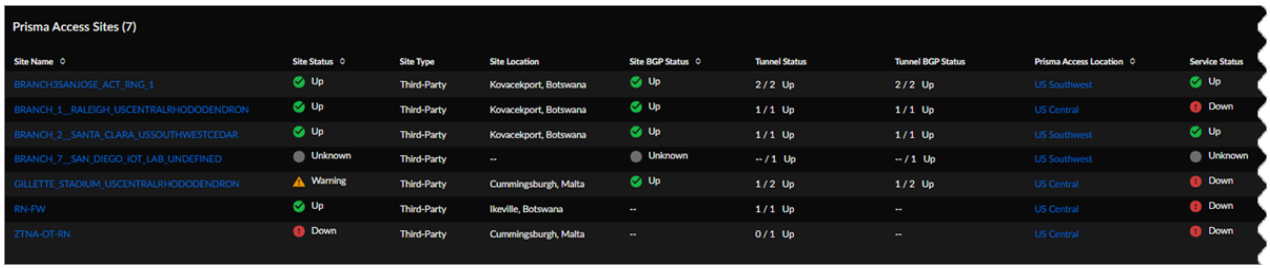
 ©2025 Palo Alto Networks, Inc.

Sites Prisma Access

Le tableau **Prisma Access Sites (Sites Prisma Access)** répertorie vos sites distants Prisma Access et les informations.

- **Site Name (Nom du site)** : nom unique du site Prisma Access.
- **Site Status (État du site)**—**Up (Actif)**, **Down (Inactif)**, **Warning (Avertissement)**ou **Unknown (Inconnu)**.
- **Site Type (Type de site)** : tiers.
- **Site Location (Emplacement du site)** : emplacement du site Prisma Access.
- **Site BGP Status (État BGP du site)** : indique si l'état BGP du site est **Up (Actif)**, **Down (Inactif)**ou **Unknown (Inconnu)**.
- **Tunnel Status (État du tunnel)** : le nombre de tunnels du site et le nombre de ces tunnels qui sont opérationnels.
- **Tunnel BGP Status (État BGP du tunnel)** : l'état BGP de chaque tunnel.
- **Prisma Access Location (Emplacement Prisma Access)** : emplacement de ce site Prisma Access. Sélectionnez un emplacement pour afficher les détails de ses Prisma Access Locations (Emplacements Prisma Access).
- **Service Status (État du service)** : ce champ indique l'état de l'instance ou du pare-feu auquel le site est connecté. L'état peut être **Up (Actif)**, **Down (Inactif)**ou **Unknown (Inconnu)**.
- **Compute Location (Emplacement de calcul)** : tous les emplacements Prisma Access sont mappés à un emplacement ou à une région de calcul de traitement de sécurité en fonction des performances et de la latence optimisées. Au moins deux emplacements Prisma Access (souvent plus) géographiquement proches l'un de l'autre sont regroupés dans un seul emplacement de calcul.
- **Aggregated Bandwidth Allocated (Bande passante agrégée allouée)** : bande passante agrégée allouée pour le site pendant l'intervalle de temps sélectionné. Cette colonne apparaît uniquement si vous avez utilisé le modèle de bande passante agrégée.
- **Peak Burst Bandwidth Consumed (Bande passante maximale consommée en rafale)** : valeur maximale cumulée obtenue en combinant les valeurs d'entrée et de sortie pour ce site pendant l'intervalle de temps sélectionné.
- **Avg Bandwidth Consumed (Bande passante moyenne consommée)** : valeur moyenne cumulée obtenue en combinant les valeurs d'entrée et de sortie pour ce site pendant l'intervalle de temps sélectionné.
- **Disconnections (Déconnexions)** : nombre de déconnexions survenues sur ce site pendant l'intervalle de temps sélectionné.
- **Disconnections Duration (Durée des déconnexions)** : durée totale, en secondes, pendant laquelle le site a été déconnecté pendant l'intervalle de temps sélectionné.

 ©2025 Palo Alto Networks, Inc.



Visibilité des sites de succursales à haute performance

Les succursales à haute performance (RN-HP) ont des attributs différents des succursales héritées et les deux coexisteront dans votre locataire. Les sites de succursales à haute performance de Prisma Access présentent les avantages suivants :

- L'architecture aborde les gains d'efficacité en séparant les fonctions de traitement réseau des fonctions de traitement de sécurité. Un périphérique ION doté d'une grande capacité de traitement de paquets met fin à plusieurs connexions de succursales avec une capacité allant jusqu'à 5 Gbit/s et distribue le traitement de sécurité aux SPN.
- Vous pouvez utiliser une seule adresse IP ou un seul FQDN pour terminer plusieurs succursales de la région vers un seul nœud de traitement réseau (NPN).
- Vous n'avez plus besoin de surveiller et de gérer la terminaison des sites de succursales vers les nœuds de fin IPSec. Les SPN appropriés effectuent l'inspection du trafic des succursales et le NPN effectue l'équilibrage de la charge.
- Vous pouvez atteindre une véritable haute disponibilité en étant en mesure de spécifier différentes régions pour la redondance.

Vous pouvez afficher à la fois les succursales à haute performance et héritées de votre environnement. Dans Strata Cloud Manager, accédez à **Monitor (Surveiller)** > **Branch Sites (Sites de succursales)** > **Prisma Access**et, dans le tableau **Prisma Access Sites (Sites Prisma Access)**, sélectionnez un site de succursale.

Détails du site Prisma Access

Sélectionnez n'importe quel **Site Name (Nom de site)** Prisma Access pour afficher son **Site Status (État de site)**, où vous pouvez voir sa **Connectivity (Connectivité)** et son**BGP Status (État BGP)** (**Up (Actif)**, **Down (Inactif)**, **Inactive (Inactif)**ou **Not Available (Non disponible**). Affichez la **Peak Consumption (Consommation maximale)** de bande passante pour l'intervalle de temps sélectionné.

Vous pouvez afficher les informations **Cumulative (Ingress + Egress) (Cumulée (Entrée + Sortie)** dans le graphique **Bandwidth Consumption Trend (Tendance de la consommation de bande passante)**.

- Utilisez la liste déroulante pour afficher le graphique de consommation de bande passante par **Ingress (Entrée)**, **Egress (Sortie)**, **Ingress vs. Egress (Entrée versus Sortie)**, ou **Cumulative (Ingress + Egress) (Cumulée (Entrée + Sortie))**.

- Affichez les métriques du graphique de tendance de consommation de bande passante par valeur **Maximale (Peak)** (par défaut), **Average (Moyenne)** ou **Median (Médiane)** pour le site de la succursale.

 ©2025 Palo Alto Networks, Inc.

Visibilité de la table d'itinéraires

Pour vous aider à relever les défis d'accessibilité, nous offrons une visibilité sur la table d'itinéraires de chaque site réseau distant. Vous pouvez effectuer une recherche dans la table d'itinéraires pour une adresse IP de destination afin de déterminer s'il existe un itinéraire disponible pour atteindre la destination souhaitée. Grâce à ces informations, vous pouvez rechercher d'autres causes potentielles de défaillance. Ces connaissances vous permettent de concentrer vos efforts sur la résolution de tous les problèmes susceptibles d'affecter l'accessibilité.

Sélectionnez **View Routing Table (Afficher la table d'itinéraires)** pour voir la **Routing Table (Table d'itinéraires)**de cette succursale, qui contient des itinéraires IP pour les destinations disponibles dans la succursale à partir de Prisma Access.

- Utilisez la barre de recherche pour sélectionner la destination ou rechercher l'itinéraire.
- Utilisez la liste déroulante pour filtrer par **Flag (Indicateur)**.

La table d'itinéraires affiche :

- **#** : numéro d'itinéraire.
- **Destination** : adresse IP et sous-réseau du réseau accessible.
- **Next Hop (Saut suivant)** : adresse IP de la passerelle au saut suivant vers le réseau de destination. Un saut suivant de 0.0.0.0 indique l'itinéraire par défaut.
- **Metric (Métrique)** : métrique pour l'itinéraire déterminé par le protocole de routage.
- **Flag (Indicateur)** : informations pour cet itinéraire, comme suit :
- - **A B** : actif et appris via BGP.
  - **A C** : actif et connecté. Destination : réseau.
  - **A H** : actif et connecté. Destination : hôte uniquement.
  - **A R** : actif et appris via RIP.
  - **O1** : OSPF externe de type 1.
  - **O2** : OSPF externe de type 2.
  - **Oi** : OSPF intra-zone.
  - **Oo** : OSPF interzone.
  - **S** : inactif et statique.
  - **A S** : actif et statique.

Tunnels

Affichez les tunnels et les données des tunnels pour ce site.

- **Tunnel Name (Nom du tunnel)** : nom unique du tunnel.
- **Prisma Access Location (Emplacement Prisma Access)** : emplacement Prisma Access pour ce réseau distant.
- **Tunnel Status (État du tunnel)** :**Up (Actif)**, **Down (En panne)**, **Init (Initialisation)** ou **Unavailable (Indisponible)**.

 ©2025 Palo Alto Networks, Inc.

- **Tunnel BGP Status (État du tunnel BGP) :Up (Actif)**, **Down (Inactif)** ou **Unknown (Inconnu)**.
- **Tunnel Monitoring (Surveillance du tunnel)** : si vous avez activé **Tunnel Monitoring (Surveillance du tunnel)**, cette colonne indique si elle est **Up (Active)** ou **Down (Inactive)**. Si vous ne l'avez pas activé, cette colonne indique **Not Configured (Non configurée)**.
- **Average Throughput (Débit moyen)** : bande passante moyenne du tunnel pour l'intervalle de temps sélectionné, en tenant compte des paramètres **Ingress (Entrée)**, **Egress (Sortie)**, **Ingress Vs. Egress (Entrée versus Sortie)**, ou de la valeur **Cumulative (Ingress + Egress) (Cumulée (Entrée + Sortie))** que vous avez sélectionnée.
- **Peak Throughput (Débit maximal)** : la bande passante maximale du tunnel pour l'intervalle de temps sélectionné, en tenant compte des paramètres **Ingress (Entrée)**, **Egress (Sortie)**, **Ingress vs. Egress (Entrée versus Sortie)**, ou **Cumulative (Ingress + Egress) (Cumulée (Entrée + Sortie))**.
- **Source IP Address (Adresse IP source)**: adresse IP source.
- **Destination Endpoint Address (Adresse du terminal de destination)** : adresse IP ou FQDN pour Prisma Access afin de déterminer si le tunnel est actif.
- **Disconnections (Déconnexions)** : nombre de déconnexions pendant l'intervalle de temps sélectionné.
- **Disconnections Duration (Durée des déconnexions)** : durée, en secondes, pendant laquelle le tunnel est déconnecté pendant l'intervalle de temps sélectionné.

Sélectionnez un **Tunnel Name (Nom de tunnel)** pour voir son **Tunnel Status (État de tunnel)**, sa **Bandwidth Consumption Trend (Tendance de consommation de bande passante)** et d'autres détails du tunnel.

Tendances du tunnel

Avec **Tunnel Monitoring (Surveillance des tunnels)** activée, vous pouvez sélectionner un certain nombre de tunnels et afficher leur **Round-Trip Time (Temps aller-retour)** médian. Si vous ne spécifiez pas un ensemble de tunnels, par défaut, le RTT médian est calculé pour les 10 tunnels avec le RTT observé le plus élevé.

La **Aggregated Tunnel Connectivity (Connectivité des tunnels agrégés)** vous indique le nombre total de tunnels connectés pour l'intervalle de temps sélectionné. Passez la souris sur l'un des graphiques pour voir le nombre de connexions à un moment précis.

Les **Commits Pushed (Validations transmises)** indiquent combien de validations ont été transmises pendant le **Time range (Intervalle de temps)** sélectionné et quand la **Last Push Commit (Dernière validation transmise)** a eu lieu.

État du site

Le **Site Status (État du site)** indique la disponibilité du site pendant l'intervalle de temps sélectionné. **Le vert** signifie que le site était actif pendant cette période, **le rouge** signifie que le site était inactif et **le gris** signifie qu'aucune donnée n'était disponible pendant la période indiquée.

 ©2025 Palo Alto Networks, Inc.

Afficher et surveiller les centres de données

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Connexions aux services

Une connexion de service, également connue sous le nom de nœud d'accès d'entreprise (CAN), permet aux utilisateurs mobiles et aux utilisateurs de réseaux distants d'accéder à des applications et des ressources privées et permet à vos utilisateurs mobiles et à vos réseaux distants de communiquer entre eux. Palo Alto Networks recommande de toujours créer une connexion aux services dans votre déploiement Prisma Access. Toutes les connexions aux services permettent d'accéder aux ressources de votre siège ou de votre centre de données, et permettent aux réseaux distants et aux utilisateurs mobiles de communiquer entre eux.

Le nombre de connexions de service que vous recevez dépend de votre licence Prisma Access. Reportez-vous aux connexions aux services Prisma Access pour des détails sur les connexions aux services et comment les configurer.

Dans Strata Cloud Manager, sélectionnez **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **Service Connections (Connexions aux services)**pour avoir une visibilité sur vos connexions aux services.

Connecteurs ZTNA

Le connecteur Zero Trust Network Access (ZTNA) vous permet de connecter Prisma Access aux applications privées de votre organisation. Le connecteur ZTNA offre aux utilisateurs mobiles et aux utilisateurs des sites de succursales un accès à vos applications privées via un tunnel sécurisé automatisé. Le connecteur ZTNA configure automatiquement les tunnels, vous n'avez donc pas à configurer manuellement les tunnels IPSec et le routage vers les centres de données ou les emplacements du siège, les emplacements de cloud public et les réseaux partenaires où se trouvent vos applications privées.

Dans Strata Cloud Manager, sélectionnez **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **ZTNA Connectors (Connecteurs ZTNA)** pour avoir une visibilité sur vos connecteurs ZTNA.

Afficher et surveiller les connexions aux services

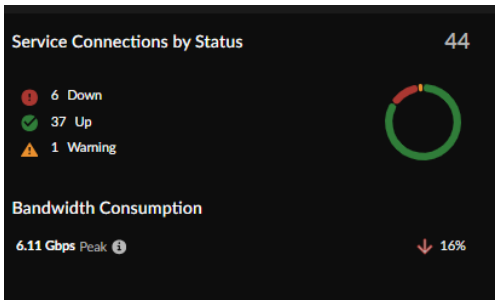
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

 ©2025 Palo Alto Networks, Inc.

Consultez les données agrégées sur les connexions aux services ainsi que les informations sur les connexions aux services individuelles. Les connexions aux services sont utilisées à la fois par les utilisateurs mobiles et les réseaux distants. Outre l'accès aux ressources de l'entreprise, les connexions de service permettent à vos utilisateurs mobiles de se rendre dans les succursales. Vous pouvez afficher vos connexions aux services dans Strata Cloud Manager pour voir l'état de la connexion aux services, les tendances de consommation de bande passante, les données et tendances du tunnel, ainsi que des informations sur l'état global de la connexion aux services. Sélectionnez **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **Service Connections (Connexions aux services)** pour commencer.

Connexions de service par état

Vous pouvez afficher l'état de toutes vos connexions aux services. Le graphique à code couleur vous montre une répartition du nombre de connexions aux services en activité, inactif ou nécessitant une attention particulière. Vous pouvez consulter une synopsis de la bande passante consommée par vos connexions aux services au cours des 30 derniers jours.



La **Bandwidth Consumption (Consommation de bande passante)** indique la bande passante maximale la plus élevée consommée par un site sur tous les sites pour le modèle d'allocation de bande passante par site. Les valeurs maximales sont calculées pour la durée du filtre temporel sélectionné.

Tendance de consommation de la bande passante

Affichez la **Bandwidth Consumption Trend per Service Connection (Tendance de consommation de bande passante par connexion aux services)**. La tendance montre la consommation de bande passante de chacune de vos connexions aux services, ainsi que leurs utilisations moyennes et maximales.

- La vue par défaut affiche la consommation de bande passante **Cumulative (Ingress + Egress) (Cumulée (Entrée + Sortie))**. Les autres options sont **Ingress (Entrée)**, **Egress (Sortie)** ou **Ingress vs. Egress (Entrée versus Sortie)**.
- Affichez la tendance de consommation de bande passante **Peak (Maximale)**, **Median (Médiane)** ou **Average (Moyenne)** pendant l'intervalle de temps sélectionné. Le paramètre par défaut est la consommation **Peak (Maximale)** de bande passante.
- **Log Scale (Échelle des journaux)** ou **Linear Scale (Échelle linéaire)**.
- Sélectionnez 1 à 10 **Service Connections (Connexions aux services)** pour afficher leurs lignes de tendance sur le graphique pendant l'intervalle de temps sélectionné. Passez la souris sur le graphique pour obtenir des informations sur chacune des connexions aux services que vous avez sélectionnées.

 ©2025 Palo Alto Networks, Inc.

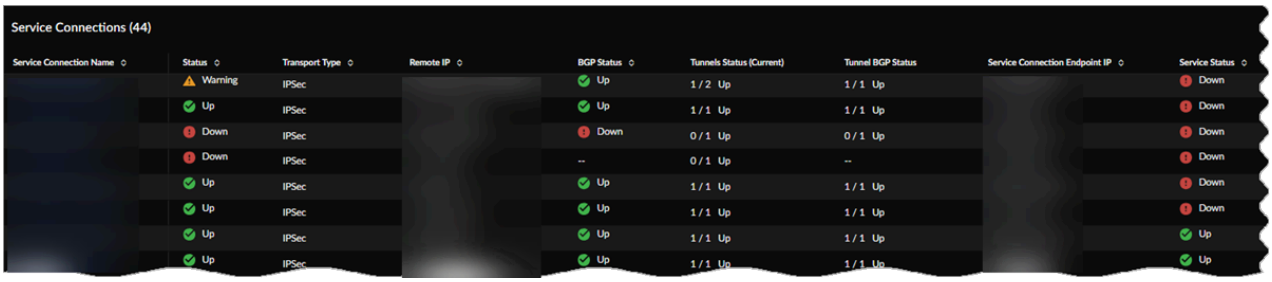


Tableau Service Connections (Connexions aux services)

Le tableau **Service Connections (Connexions aux services)** affiche des données sur vos connexions aux services, telles que l'état, l'adresse IP distante, l'état BGP, l'état actuel du tunnel et d'autres données. Sélectionnez un **Service Connection Name (Nom de connexion aux services)** pour obtenir des détails sur cette connexion aux services.

- **Service Connection Name (Nom de connexion aux services)** : nom unique de la connexion aux services.
- **Status (État)** : **Up (Actif)**, **Down (Inactif)**, **Warning (Avertissement)** ou **Unknown (Inconnu)**.
- **Transport Type (Type de transport)** : IPSec.
- **Remote IP (Adresse IP distante)** : adresse IP distante.
- **BGP Status (État BGP)** : indique si l'état BGP du site est **Up (Actif)**, **Down (Inactif)**ou **Unknown (Inconnu)**.
- **Tunnels Status (Current) (État des tunnels (actuel))** : nombre de tunnels du site et nombre de ces tunnels qui sont actifs.
- **Tunnel BGP Status (État BGP du tunnel)** : l'état BGP de chaque tunnel.
- **Service Connection Endpoint IP (IP du terminal de connexion aux services)** : adresse IP du terminal de connexion aux services.
- **Service Status (État du service)** : ce champ indique l'état de l'instance ou du pare-feu auquel le site est connecté. L'état peut être **Up (Actif)**, **Down (Inactif)**ou **Unknown (Inconnu)**.
- **Prisma Access Location (Emplacement Prisma Access)** : emplacement Prisma Access de la connexion aux services.
- **Average Bandwidth Consumption (Consommation moyenne de bande passante)** : consommation moyenne de bande passante en Kbit/s.
- **Consommation maximale de bande passante** : consommation maximale de bande passante en Kbit/s.

 ©2025 Palo Alto Networks, Inc.



Détails des connexions aux services

Sélectionnez n'importe quelle **Service Connection Name** (Nom de connexion aux services) pour afficher ses détails. Affichez son **Service Connection Status (État de connexion aux services)**, **Bandwidth Consumed (Bande passante consommée)** au cours des 30 derniers jours. Le graphique **Bandwidth Consumption Trend (Tendance de consommation de bande passante)** affiche la consommation de bande passante de chacune de vos connexions aux services pendant l'intervalle de temps sélectionné.

État du site

Sélectionnez n'importe quel **Service Connection Name (Nom de connexion aux services)** pour afficher son **Site Status (État du site)**, où vous pouvez voir sa **Connectivity (Connectivité)** et son **BGP Status (État BGP)** (**Up (Actif)**, **Down (Inactif)**, **Inactive (Inactif)**ou **Not Available (Non disponible)**). Affichez la **Peak Consumption (Consommation maximale)** de bande passante pour l'intervalle de temps sélectionné.

Visibilité de la table d'itinéraires

Pour vous aider à relever les défis d'accessibilité, nous offrons une visibilité sur la table d'itinéraires de chaque connexion aux services. Vous pouvez effectuer une recherche dans la table d'itinéraires pour une adresse IP de destination afin de déterminer s'il existe un itinéraire disponible pour atteindre la destination souhaitée. Grâce à ces informations, vous pouvez recevoir des conseils de votre infrastructure Prisma Access pour étudier d'autres causes potentielles de défaillance. Ces connaissances vous permettent de concentrer vos efforts sur la résolution de tout problème affectant l'accessibilité.

Sélectionnez **View Routing Table (Afficher la table d'itinéraires)** pour voir la **Routing Table (Table d'itinéraires)**de cette succursale, qui contient des itinéraires IP pour les destinations disponibles dans la succursale à partir de Prisma Access.

- Utilisez la barre de recherche pour sélectionner la destination ou rechercher l'itinéraire.
- Utilisez la liste déroulante pour filtrer par **Flag (Indicateur)**.

La table de routage affiche :

- **#** : numéro d'itinéraire
- **Destination** : adresse IP et sous-réseau du réseau accessible.
- **Next Hop (Saut suivant)** : adresse IP de la passerelle au saut suivant vers le réseau de destination. Un saut suivant de 0.0.0.0 indique l'itinéraire par défaut.
- **Metric (Métrique)** : métrique pour l'itinéraire déterminé par le protocole de routage.
- **Flag (Indicateur)** : informations pour cet itinéraire, comme suit :
- • **A B** : actif et appris via BGP.

 ©2025 Palo Alto Networks, Inc.

- **A C** : actif et connecté. Destination : réseau.
- **A H** : actif et connecté. Destination : hôte uniquement.
- **A R** : actif et appris via RIP.
- **O1** : OSPF externe de type 1.
- **O2** : OSPF externe de type 2.
- **Oi** : OSPF intra-zone.
- **Oo** : OSPF interzone.
- **S** : inactif et statique.
- **A S** : actif et statique.

Tendance de consommation de la bande passante

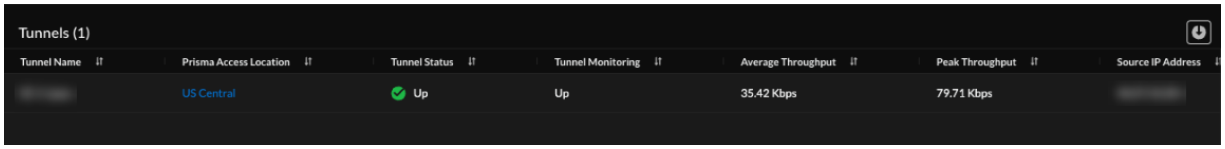
La **Bandwidth Consumption Trend (Tendance de consommation de bande passante)** affiche les informations **Cumulative (Ingress + Egress) (Cumulée (Entrée + Sortie))** par défaut.

- Utilisez la liste déroulante pour afficher le graphique de consommation de bande passante par **Ingress (Entrée)**, **Egress (Sortie)**, **Ingress vs. Egress (Entrée versus Sortie)**, ou **Cumulative (Ingress + Egress) (Cumulée (Entrée + Sortie))**.

- Affichez les métriques du graphique de tendance de consommation de bande passante par valeur **Maximale (Peak)** (par défaut), **Average (Moyenne)** ou **Median (Médiane)** pour le site de la succursale.

Tunnels

Découvrez combien de **Tunnels** il existe pour cette connexion aux services et affichez les détails de chaque tunnel. Pour télécharger les données des **Tunnels**, sélectionnez l'icône Download (Télécharger).



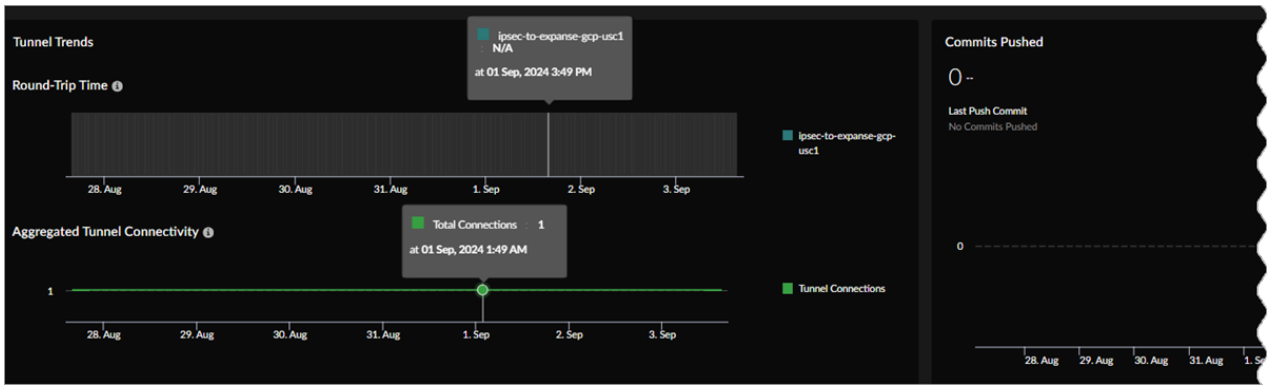
Tendances du tunnel

Vous pouvez sélectionner un certain nombre de tunnels et afficher leur **Round-Trip Time (Temps aller-retour)** médian. Si vous ne spécifiez pas d'ensemble de tunnels, le RTT médian est calculé pour les 10 tunnels avec le RTT observé le plus élevé.

La **Aggregated Tunnel Connectivity (Connectivité des tunnels agrégés)** vous indique le nombre total de tunnels connectés pour l'intervalle de temps sélectionné. Passez la souris sur l'un des graphiques pour voir le nombre de connexions à un moment précis.

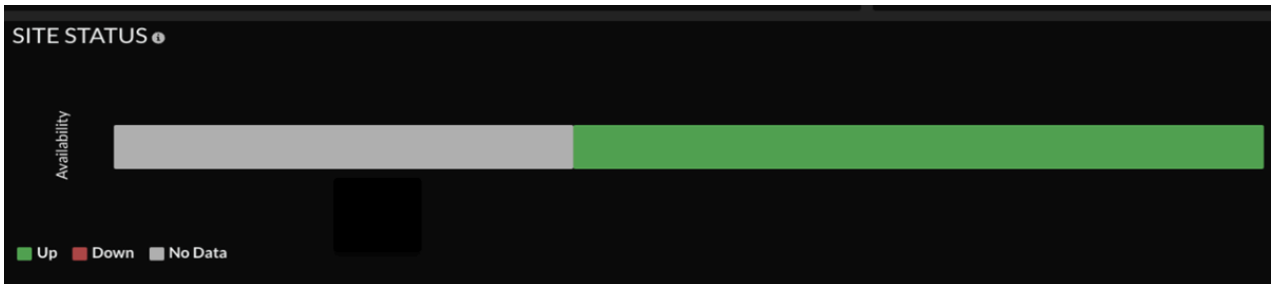
Les **Commits Pushed (Validations transmises)** indiquent combien de validations ont été transmises pendant le **Time range (Intervalle de temps)** sélectionnée et quand la **Last Push Commit (Dernière validation transmise)** a eu lieu.

 ©2025 Palo Alto Networks, Inc.



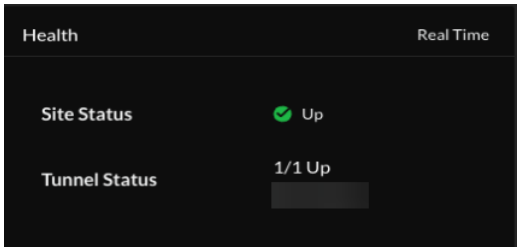
État du site

Le **Site Status (État du site)** indique la disponibilité du site pendant l'intervalle de temps sélectionné. Le vert signifie que le site était actif pendant cette période, le rouge signifie que le site était inactif et le gris signifie qu'aucune donnée n'était disponible pendant la période indiquée.



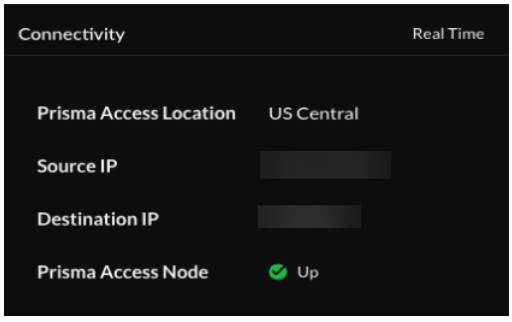
Santé

Health (État) vous montre le **Site Status (État du site)**, ainsi que le nom et l'état de chaque tunnel du site.



Connectivité

La **Connectivity (Connectivité)** montre l'emplacement Prisma Access auquel le site est connecté, ses adresses IP source et de destination, ainsi que l'état du nœud Prisma Access.



 ©2025 Palo Alto Networks, Inc.

Consommation

La **Consumption (Consommation)** affiche les détails de la consommation de bande passante.

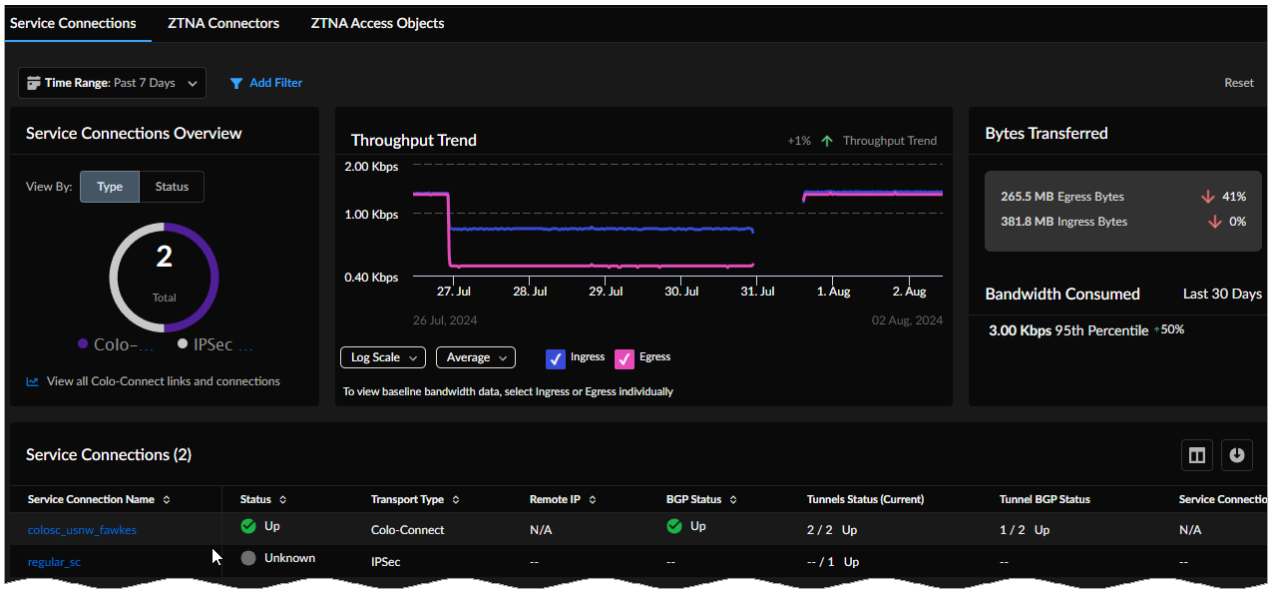


Afficher et surveiller Colo-Connect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	Licence Prisma Access

Prisma Access Colo-Connect exploite la technologie d'interconnexion GCP native du cloud pour fournir des connexions aux services à large bande passante à vos applications privées. Colo-Connect coexiste avec les connexions aux services basées sur le tunnel IPSec existantes. Ainsi, si vous devez fournir un accès privé aux applications à des centres de données plus petits qui ne nécessitent pas un débit de bande passante élevé, vous pouvez également utiliser des connexions aux services pour ces centres de données. Obtenez une visibilité sur votre déploiement Colo-Connect en affichant des mesures telles que le nombre de liens Colo-Connect et leur état, les tendances de débit et les détails individuels des tunnels, des connexions et des liens. En affichant les données sur vos connexions aux services Colo-Connect, vous pouvez obtenir une vue d'ensemble de l'état et de la connectivité de votre déploiement.

Accédez à **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **Service Connections (Connexions aux services)** pour afficher et surveiller votre connectivité privée au cloud hybride et aux centres de données locaux via des interconnexions cloud.



Vue d'ensemble des connexions de service

La **Service Connections Overview (Vue d'ensemble des connexions de service)** affiche le nombre de connexions de service par **Type** de transport.

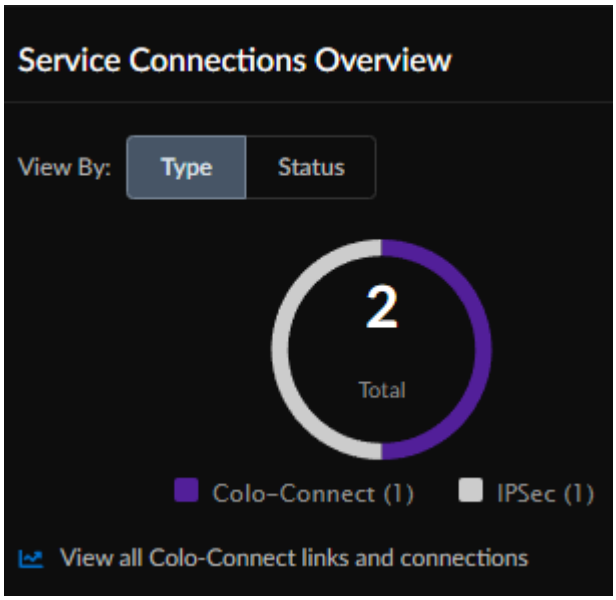
Vous pouvez voir une agrégation des transports connectés par **Type** ou par leur **Status (État)** de disponibilité.

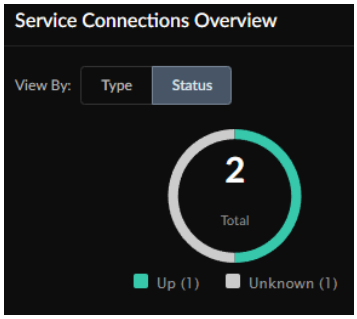
 ©2025 Palo Alto Networks, Inc.

- **IPSec**
- **Colo-Connect**

Vous pouvez afficher le type de transport du tunnel par état : **Up (Actif)**, **Down (Inactif)**, **Degraded (Dégradé)** ou **Unknown (Inconnu)**.

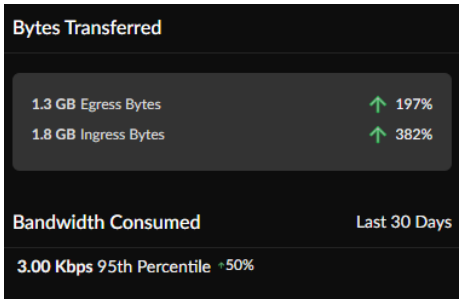
Sélectionnez **View all Colo-Connect links and connections (Afficher tous les liens et connexions Colo-Connect)** pour afficher la page des détails de Colo-Connect.





Vue d'ensemble des connexions aux services : Octets transférés et bande passante consommée

Les **Bytes Transferred (Octets transférés)** affichent une agrégation des octets entrants et sortants consommés, ainsi que la différence de consommation par rapport à l'intervalle de temps que vous avez sélectionné précédemment. La **Bandwidth Consumed (Bande passante consommée)** indique le 95e percentile de la bande passante consommée au cours des 30 derniers jours.

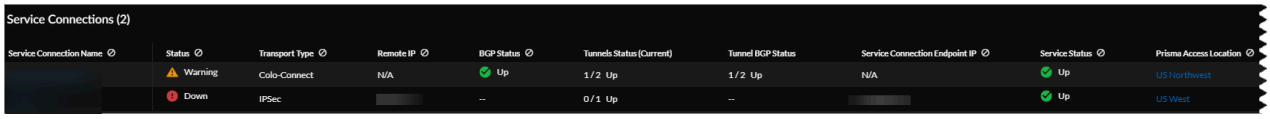


 ©2025 Palo Alto Networks, Inc.

Connexions aux services

Le tableau **Service Connections (Connexions aux services** affiche les détails suivants pour chaque connexion aux services indiquée :

- **Service Connection Name (Nom de connexion aux services)**: nom de la connexion au service Colo-Connect ou IPSec. Sélectionnez un **Service Connection Name (Nom de connexion aux services)** pour accéder à sa page de détails.
- **Status (État)** : actif, inactif, dégradé ou inconnu.
- **Transport Type (Type de transport)** : Colo-Connect ou IPSec.
- **Remote IP (IP distante)** : IP de destination.
- **BGP Status (État BGP)** : actif, inactif ou avertissement si certains tunnels BGP sont actifs et d'autres sont inactifs.
- **Tunnel Status (Current) (État du tunnel (actuel))** : état actuel du tunnel.
- **Tunnel BGP Status (État du tunnel BGP)** : nombre de tunnels par état BGP (actif, inactif ou avertissement).
- **Service Connection Endpoint (IP de terminal de connexion aux services)** : l'adresse IP du nœud Prisma Access.
- **Service Status (État du service)** : l'état du service est déterminé par la connexion aux services active ou par l'état du ou des clusters du centre de données (plus d'un cluster) (actif, inactif ou avertissement).
- **Prisma Access Location (Emplacement Prisma Access)** : sélectionnez un **Prisma Access Location (Emplacement Prisma Access)**.
- **Average Bandwidth Consumption (Consommation moyenne de bande passante)** : consommation moyenne de bande passante pour le site pendant l'intervalle de temps sélectionné.
- **Peak Bandwidth Consumption (Consommation maximale de bande passante)** : consommation maximale de bande passante pour le site pendant l'intervalle de temps sélectionné.



Détails des connexions aux services

Dans le tableau **Service Connections (Connexions aux services)** sur la page principale, sélectionnez une **Service Connection (Connexion aux services)** avec son **Type** de transport Colo-Connect pour accéder à sa page de détails.

 ©2025 Palo Alto Networks, Inc.



État de connexion aux services, Colo-Connect et sessions simultanées

- Consultez le **Access Location (Emplacement d'accès)** de la connexion de service et l'état des **GRE Tunnels (Tunnels GRE)** (actif, inactif ou avertissement).
- Affichez le nombre total de liens et de connexions **Colo-Connect**.
- Les **Concurrent Sessions (Sessions simultanées)** indiquent le nombre de sessions en cours et le nombre total de sessions au cours des 30 derniers jours.

Tendance du débit

La **Throughput Trend (Tendance de débit)** affiche le trafic de débit entrant et sortant consommé par cette connexion aux services pendant l'intervalle de temps sélectionné.

Octets transférés et bande passante consommée

Les **Bytes Transferred (Octets transférés)** affichent une agrégation des octets entrants et sortants consommés par cette connexion aux services, ainsi que la différence de consommation par rapport à l'intervalle de temps sélectionné. La **Bandwidth Consumed (Bande passante consommée)** indique le 95e percentile de la bande passante consommée par la connexion aux services au cours des 30 derniers jours.

Tunnels GRE

Affichez les détails sur les tunnels de cette connexion aux services :

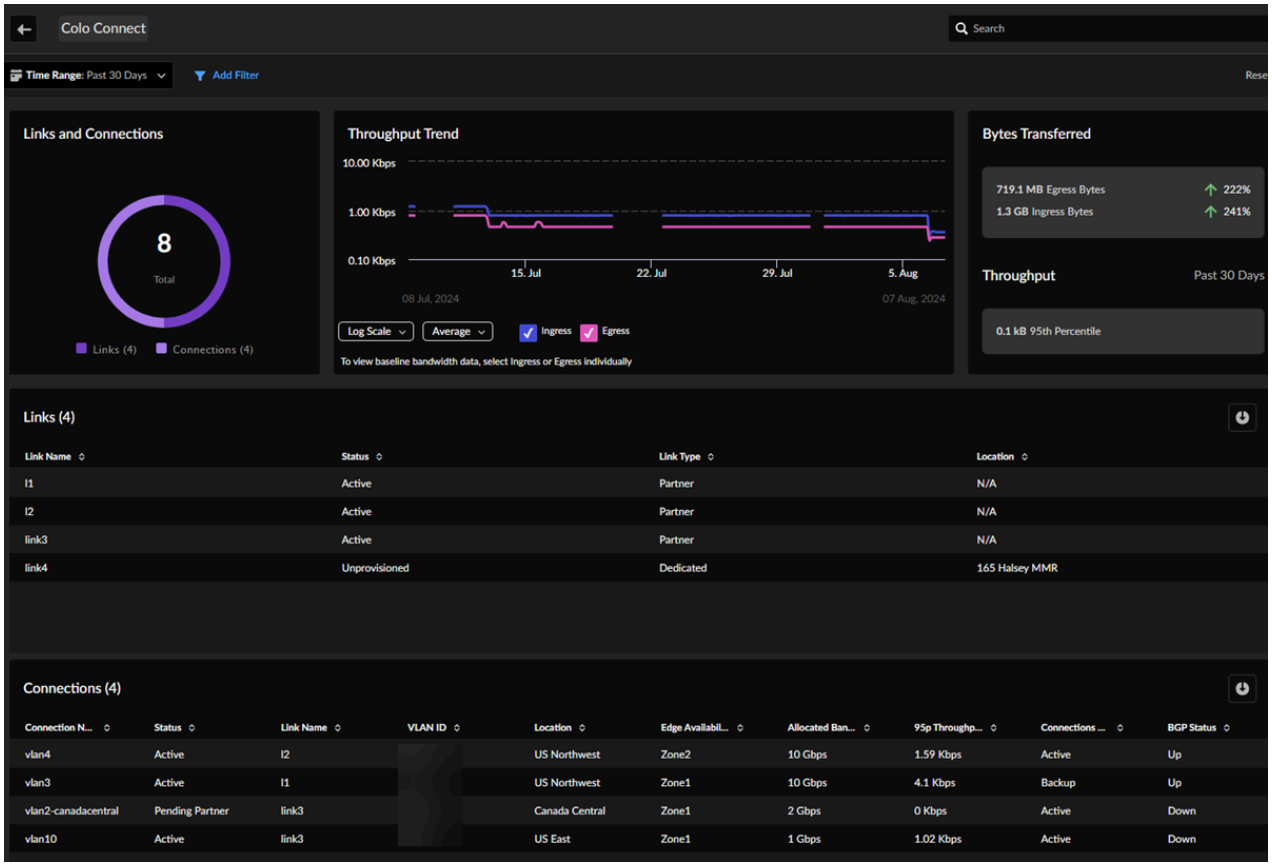
- **Tunnel Name (Nom du tunnel)** : nom unique du tunnel.
- **Tunnel Status (État du tunnel)** : actif, inactif ou inconnu.
- **Connection Name (Nom de connexion)** : nom unique de la connexion.
- **Tunnel State (État du tunnel)**: état de la connexion (actif ou de secours).
- **Remote IP (IP distante)** : adresse IP de destination.
- **Source IP (IP source)** : adresse IP du périphérique local.
- **95% Throughput (95 % de débit)** : 95e percentile de la bande passante consommée au cours des 30 derniers jours.
- **Peak Throughput (Débit maximal)** : débit maximal pendant l'intervalle de temps sélectionné.
- **BGP Status (État BGP)** : actif, inactif, dégradé ou inconnu.
- **BGP Local IP (IP locale BGP)** : IP locale BGP.

 ©2025 Palo Alto Networks, Inc.

- **Disconnections (Déconnexions)** : nombre de déconnexions subies par ce tunnel.
- **Disconnections Duration (Durée des déconnexions)** : durée des déconnexions.
- **Ingress Bytes (Octets entrants)** : nombre d'octets entrants consommés pendant l'intervalle de temps sélectionné.
- **Egress Bytes (Octets sortants)** : nombre d'octets sortants consommés pendant l'intervalle de temps sélectionné.
- **Ingress Packet Count (Nombre de paquets entrants)** : nombre de paquets entrants.
- **Egress Packet Count (Nombre de paquets sortants)** : nombre de paquets sortants.

Détails Colo Connect

Depuis la page principale **Service Connections (Connexions aux services)**, sélectionnez **View all Colo-Connect links and connections (Afficher tous les liens et connexions Colo-Connect)** dans le widget **Service Connections Overview (Vue d'ensemble des connexions aux services)** pour ouvrir la page des détails de **Colo-Connect**. Les widgets sur cette page affichent vos informations actuelles (actuelles définies comme les 20 dernières minutes).



Liens et connexions

Le graphique circulaire montre le nombre total de liens et de connexions Colo-Connect actuels.

Liens

Le tableau affiche les détails de vos liens Colo-Connect actuels.

- **Link Name (Nom du lien)** : nom du lien Colo-Connect unique.

 ©2025 Palo Alto Networks, Inc.

- **Status (État)** : actif ou en cours de maintenance.
- **Link Type (Type de lien)** :partenaire ou dédié.
- **Location (Emplacement)** : emplacement Prisma Access.

Connexions

Affichez les détails de chacun de vos liens Colo-Connect actuels. Passez la souris sur les connexions pour voir les informations sur l'état affiché.

- **Connection Name (Nom de connexion)** nom de connexion Colo-Connect unique.
- **Status (État)** : actif, partenaire en attente, disparu.
- **Link Name (Nom du lien)** : nom du lien de la connexion.
- **VLAN ID (VLAN ID)** : ID VLAN de la connexion.
- **Location (Emplacement)** : emplacement Prisma Access.
- **Edge Availability Zone (Zone de disponibilité Edge)** : Zone1 ou Zone2.
- **Allocated Bandwidth (Bande passante allouée)** : 1 Gbit/s, 2 Gbit/s, 5 Gbit/s, 10 Gbit/s ou 20 Gbit/s.
- **95 Throughput (95 % de débit)** : 95e percentile de la bande passante consommée.
- **Connection State (État de connexion)** : actif ou de secours.
- **BGP Status (État BGP)** : actif ou inactif.

Afficher et surveiller les connecteurs ZTNA

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Il s'agit d'une fonctionnalité Prisma Access Insights.

Le connecteur ZTNA (Zero Trust Network Access) simplifie l'accès aux applications privées pour toutes vos applications. La VM du connecteur ZTNA de votre environnement forme automatiquement des tunnels entre vos applications privées et Prisma Access. Affichez un résumé de tous les connecteurs ZTNA configurés, y compris **Application Targets (Cibles de l'application)** associé au connecteur, sa bande passante moyenne et médiane, et le **Status (État)** (vers le haut, partiellement vers le haut ou vers le bas). Sélectionnez **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **ZTNA Connectors (Connecteurs ZTNA)** dans Strata Cloud Manager pour voir les performances de vos connecteurs ZTNA et de vos groupes de connecteurs.

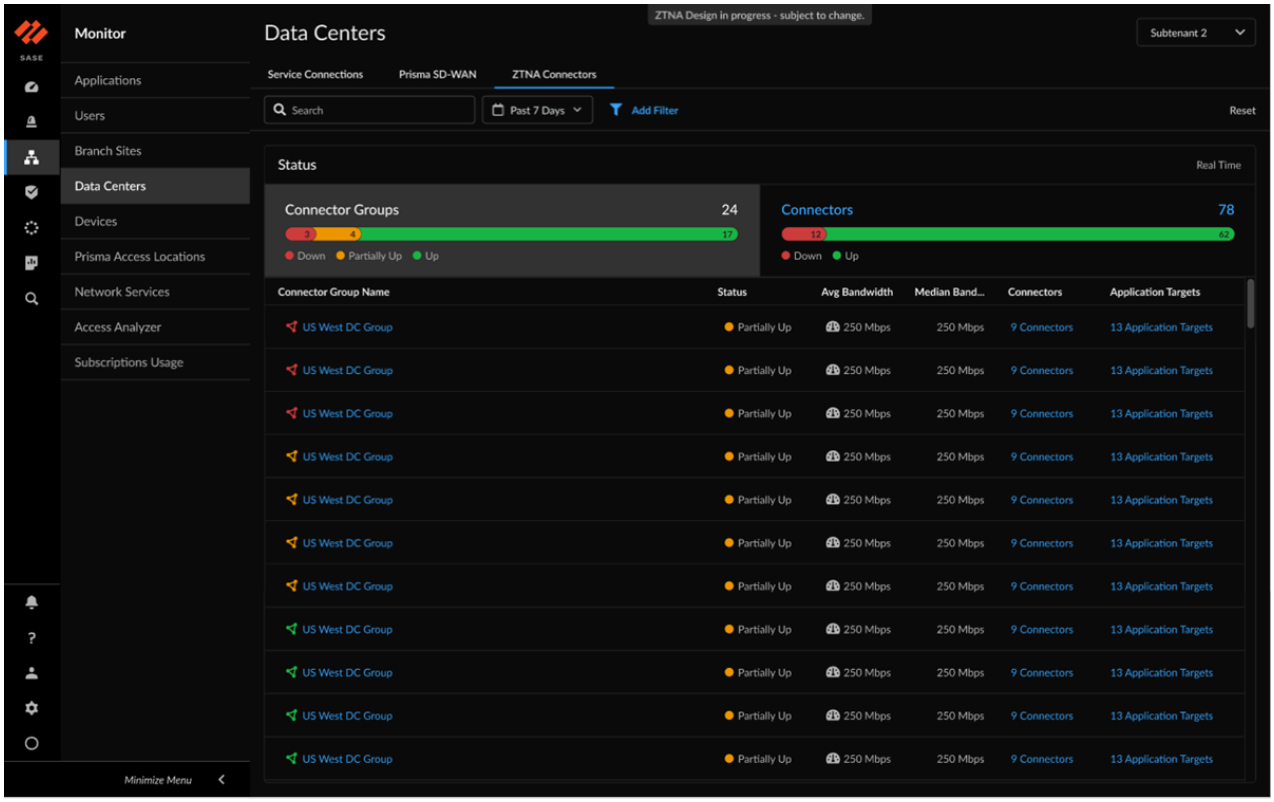
État des groupes de connecteurs ZTNA

Les connecteurs de chaque groupe déterminent le **Status (État)** du groupe de connecteurs.

- Si tous les **Connectors (Connecteurs)** dans un **Groupe de connecteurs (Connector Group)** sont activés, le **Status (État)** est **Actif** (vert).
- Si tous les **Connectors (Connecteurs)** sont inactifs, l'état est **Down (Inactif)** (rouge).
- Si certains connecteurs sont actifs et d'autres inactifs, le **Status (État)** est **Partiellement actif** (orange).

 ©2025 Palo Alto Networks, Inc.

- Les connecteurs désactivés apparaissent en gris.



État des connecteurs ZTNA

Affichez un résumé de tous les connecteurs configurés, y compris les cibles d'application associées au connecteur et le **Status (État)**.

Sélectionnez n'importe quel **Connector Name (Nom du connecteur)** pour afficher des détails sur les groupes de connecteurs associés et les cibles d'application associées à chaque connecteur.

Afficher et surveiller les objets d'accès au connecteur ZTNA

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Obtenez de la visibilité sur vos applications privées qui ont été ajoutées via les objets d'accès du connecteur ZTNA en consultant des données telles que le nombre d'applications ajoutées par FQDN, sous-réseaux IP et caractères génériques, l'état de connectivité de chaque objet d'accès, ainsi que les groupes de connecteurs et les connecteurs associés à chaque objet d'accès. En affichant ces informations, vous pouvez obtenir une vue d'ensemble de l'état et de la connectivité de votre déploiement.

Les applications privées dans les centres de données se connectent à Prisma Access via les machines virtuelles (VM) de votre connecteur. Vous pouvez ajouter des applications basées sur ces objets d'accès : FQDN, caractères génériques FQDN ou sous-réseaux IP.

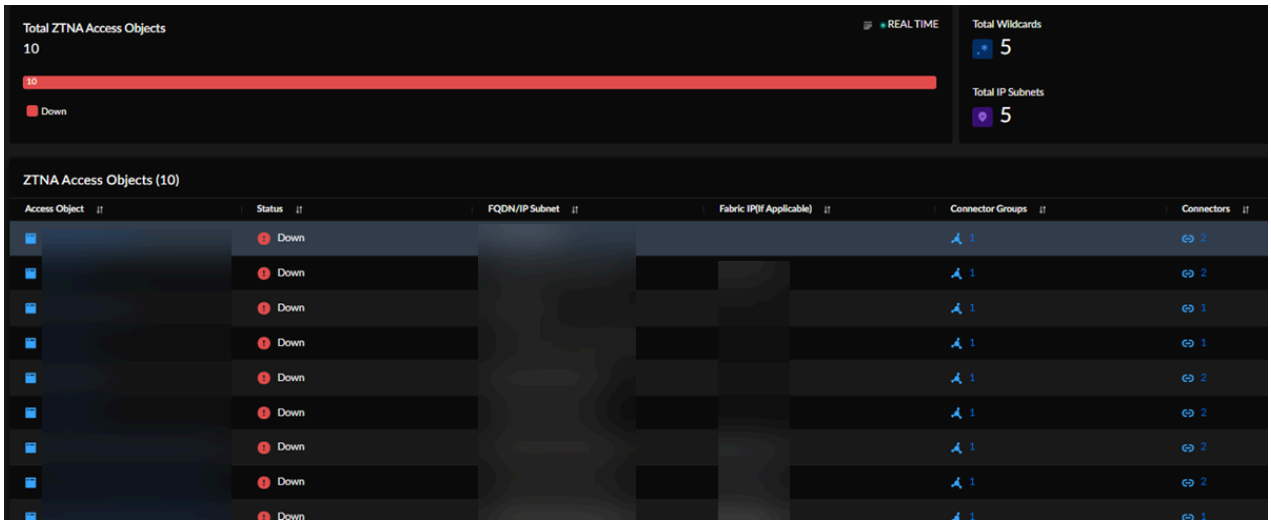
 ©2025 Palo Alto Networks, Inc.

- **FQDN** : Prisma Access résout les FQDN des applications que vous intégrez au connecteur ZTNA aux adresses IP du bloc d'adresses IP de l'application.
- **Wildcards (Caractères génériques)** : pour les applications basées sur des caractères génériques, créez un groupe de connecteurs basé sur un FQDN, puis spécifiez le caractère générique à utiliser (par exemple, *.example.com) pour la cible de l'application. Lorsque les utilisateurs accèdent à des sites qui correspondent au caractère générique, ces applications sont automatiquement intégrées pour l'accès depuis le connecteur ZTNA pour vos utilisateurs mobiles et vos utilisateurs de réseaux distants.
- **IP Subnets (Sous-réseaux IP)** : créez un groupe de connecteurs basé sur un sous-réseau IP, puis saisissez le sous-réseau IP à utiliser pour la cible de l'application.

Dans Strata Cloud Manager, accédez à **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **ZTNA Access Objects (Objets d'accès ZTNA)** pour obtenir une visibilité sur vos objets d'accès du connecteur ZTNA.

Tous les objets d'accès

Affichez **Total ZTNA Access Objects (Nombre total des objets d'accès ZTNA)** pour consulter des informations sur tous vos objets d'accès du connecteur ZTNA (FQDN, caractères génériques et sous-réseaux IP) en temps réel. Le nombre dans **Total ZTNA Access Objects (Nombre total des objets d'accès ZTNA)** et le tableau **ZTNA Access Objects (Objets d'accès ZTNA)** doit correspondre, représentant le nombre d'applications FQDN, d'applications de sous-réseau et d'applications de caractères génériques découvertes.



- Affichez un graphique de **Total ZTNA Access Objects (Nombre total des objets d'accès ZTNA)** dans votre environnement par état, ce qui signifie que les tunnels sécurisés automatisés pour l'objet d'accès sont actifs, partiellement actifs, inactifs ou désactivés. Si l'état est inactif, le connecteur associé à cet objet d'accès ne peut pas atteindre votre application.
  - **Up (Actif)** : tous les tunnels sont actifs.
  - **Partially Up (Partiellement actif)** : certains tunnels sont actifs et d'autres sont inactifs ou désactivés.
  - **Down (Inactif)** : tous les tunnels sont inactifs.

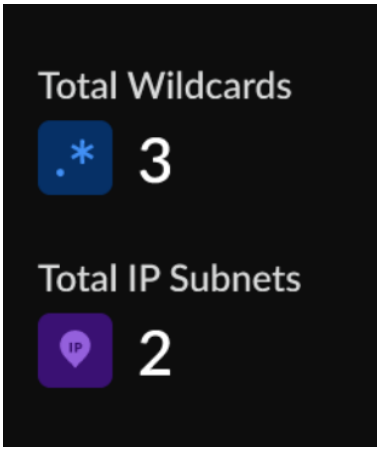
 ©2025 Palo Alto Networks, Inc.

- **Disabled (Désactivé)** : tous les tunnels sont désactivés.

  Sélectionnez un carré de couleur d'état dans le widget **Total ZTNA Access Objects (Nombre total des objets d'accès ZTNA)** pour trier les objets d'accès par état dans le tableau **ZTNA Access Objects (Objets d'accès ZTNA).**

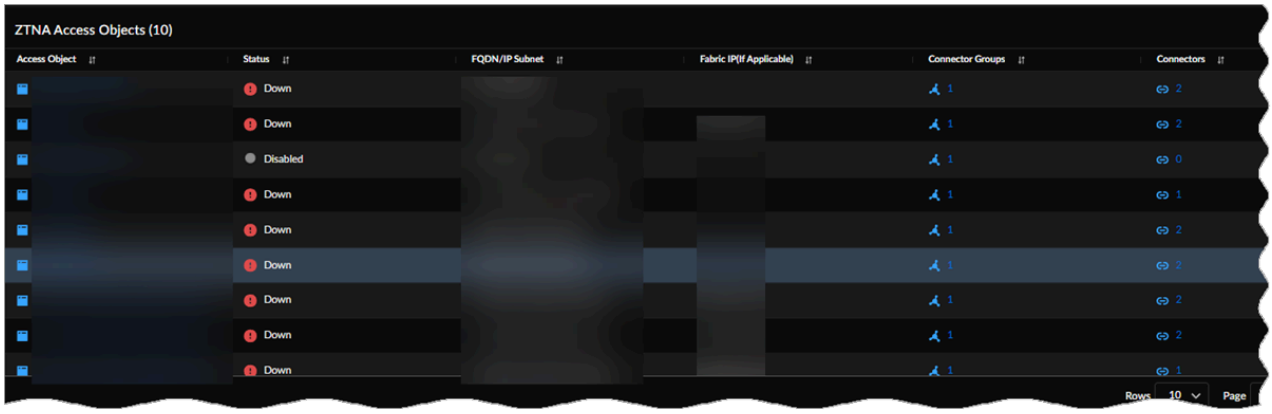


- **Total Wildcards and Total IP Subnets (Tous les caractères génériques et tous les sous-réseaux IP)** résument combien de sous-réseaux IP et de règles de caractères génériques vous avez intégrés. Il s'agit du nombre de règles de caractères génériques que vous avez créées, qui est un total différent du nombre d'applications découvertes à la suite de la création de ces règles.



 ©2025 Palo Alto Networks, Inc.

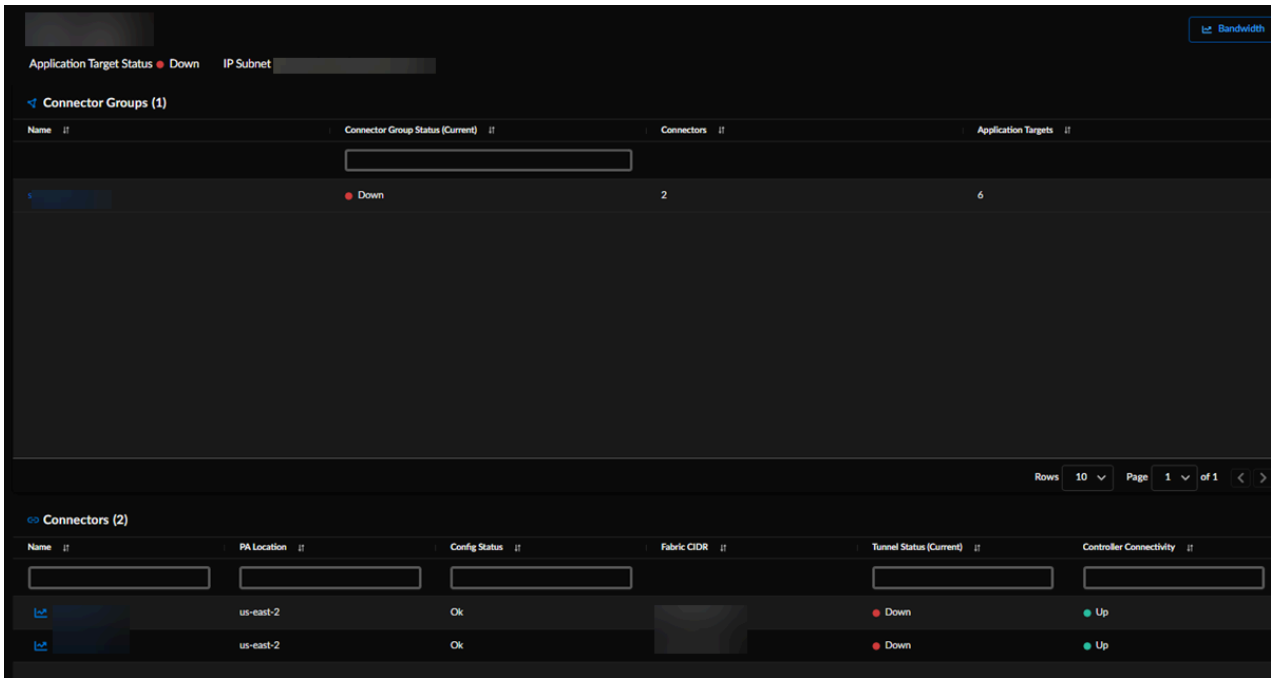
- Les **ZTNA Access Objects (Objets d'accès ZTNA)** fournissent des informations sur tous vos objets d'accès.
  - **Access Object (Objet d'accès)** : sélectionnez un objet d'accès spécifique pour voir ses détails.
  - **Status (État)** : le tunnel sécurisé automatisé pour l'objet d'accès est actif, partiellement actif, inactif ou désactivé.
  - **FQDN/IP Subnet (FQDN/Sous-réseau IP)** : FQDN ou sous-réseau IP utilisé pour ajouter cet objet d'accès.
  - **Fabric IP (If Applicable) (IP d'infrastructure (le cas échéant))** : IP d'infrastructure associée à cet objet d'accès.
  - **Connector Groups (Groupes de connecteurs)** : les groupes de connecteurs sont des regroupements logiques de connecteurs et d'applications. Affichez les groupes de connecteurs associés à un objet d'accès.
  - **Connectors (Connecteurs)** : les connecteurs représentent les machines virtuelles (VM) fonctionnant dans vos centres de données qui se connectent à Prisma Access. Affichez les connecteurs associés à un objet d'accès.



Sélectionnez un **Access Object (Objet d'accès)** pour voir ses détails.

- **Connector Groups (Groupes de connecteurs)** : découvrez combien de groupes de connecteurs sont associés à cet objet d'accès. Sélectionnez un groupe de connecteurs pour afficher des informations sur ses connexions aux services.
- **Connector Group Status (Current) (État du groupe de connecteurs (actuel))** : actif, partiellement actif, inactif ou désactivé.
- **Connectors (Connecteurs)** : nombre de connecteurs dans ce groupe de connecteurs.
- **Cibles d'application (Application Targets)** : nombre de cibles d'application dans ce groupe de connecteurs.
- **Bandwidth (Bande passante)** : sélectionnez le bouton **Bandwidth (Bande passante)** pour afficher les informations de bande passante pour cet objet d'accès.

 ©2025 Palo Alto Networks, Inc.



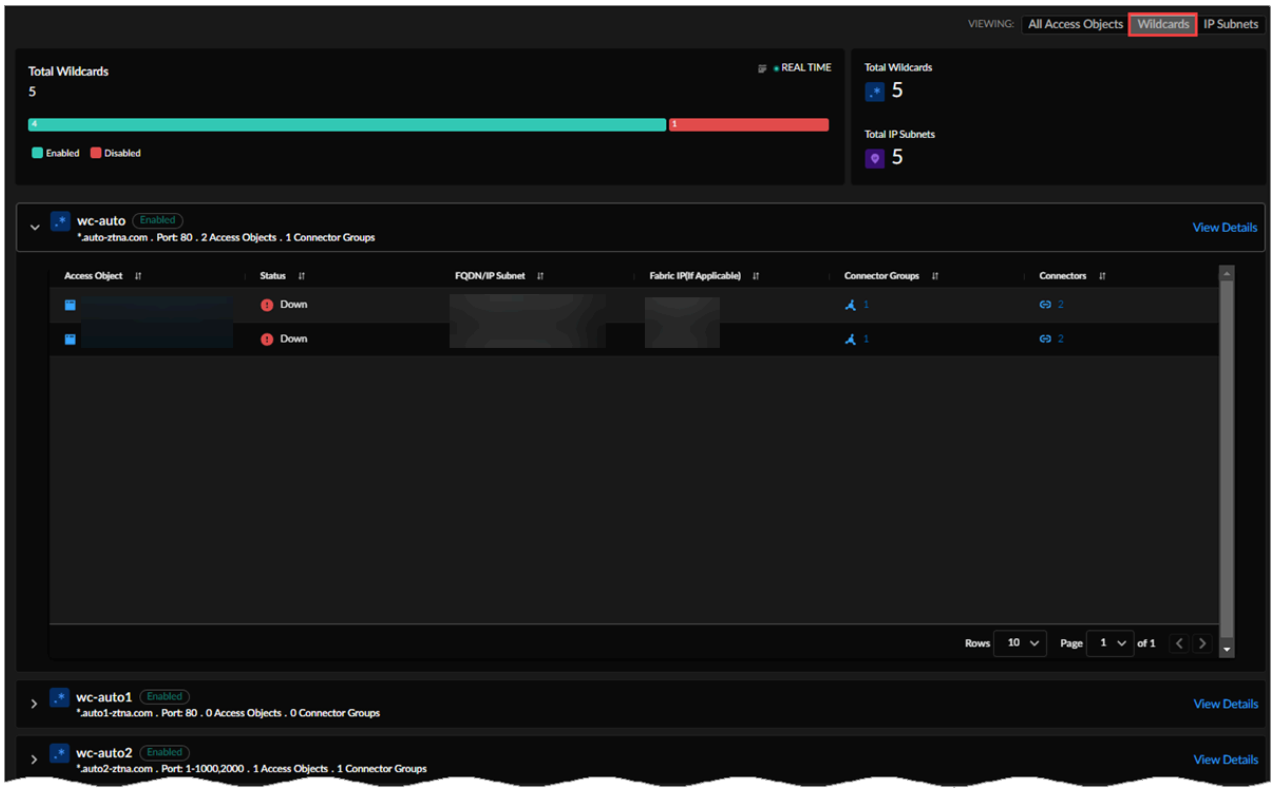
Sélectionnez l'un des **Connectors (Connecteurs)** d'un objet d'accès pour voir ses détails.

- **PA (Prisma Access) Location (Emplacement PA (Prisma Access))** : emplacement Prisma Access associé à chaque connecteur.
- **Config status (État de la configuration)** : l'état de la configuration du connecteur est OK ou Error (Erreur). Si l'état est Error (Erreur), le connecteur ZTNA n'a pas terminé l'intégration.
- **Fabric CIDR (CIDR d'infrastructure)** : CIDR d'infrastructure associé à ce connecteur.
- **Tunnel Status (Current) (État du tunnel (actuel))** : état du tunnel sécurisé automatisé pour ce connecteur.
- **Controller Connectivity (Connectivité du contrôleur)** : actif, partiellement actif, actif ou désactivé.

Caractères génériques

Sélectionnez des **Wildcards (Caractères génériques)** pour voir vos objets d'accès de caractères génériques. Affichez **Total Wildcards (Tous les caractères génériques)** par état et le nombre de **Total Wildcards (Tous les caractères génériques)** et **Total IP Subnets (Tous les sous-réseaux IP)**.

 ©2025 Palo Alto Networks, Inc.



Sélectionnez la flèche à côté d'un caractère générique ou sélectionnez **View Details (Afficher les détails)** pour obtenir des informations sur les objets d'accès qui composent ce caractère générique.

- **Access Object (Objet d'accès)** : sélectionnez un objet d'accès spécifique pour voir ses détails.
- **Status (État)** : le tunnel sécurisé automatisé pour l'objet d'accès est actif, partiellement actif, inactif ou désactivé.
- **FQDN/IP Subnet (FQDN/Sous-réseau IP)** : FQDN ou sous-réseau IP utilisé pour ajouter cet objet d'accès.
- **Fabric IP (If Applicable) (IP d'infrastructure (le cas échéant))** : IP d'infrastructure associée à cet objet d'accès.
- **Connector Groups (Groupes de connecteurs)** : les groupes de connecteurs sont des regroupements logiques de connecteurs et d'applications. Affichez les groupes de connecteurs associés à un objet d'accès.
- **Connectors (Connecteurs)** : les connecteurs représentent les machines virtuelles (VM) fonctionnant dans vos centres de données qui se connectent à Prisma Access. Affichez les connecteurs associés à un objet d'accès.



Sélectionnez un **Access Object (Objet d'accès)** pour voir ses détails.

 ©2025 Palo Alto Networks, Inc.

- **Connector Groups (Groupes de connecteurs)** : découvrez combien de groupes de connecteurs sont associés à cet objet d'accès. Sélectionnez un groupe de connecteurs pour afficher des informations sur ses connexions aux services.
- **Connector Group Status (Current) (État du groupe de connecteurs (actuel))** : actif, partiellement actif, inactif ou désactivé.
- **Connectors (Connecteurs)** : nombre de connecteurs dans ce groupe de connecteurs.
- **Cibles d'application (Application Targets)** : nombre de cibles d'application dans ce groupe de connecteurs.
- **Bandwidth (Bande passante)** : sélectionnez le bouton **Bandwidth (Bande passante)** pour afficher les informations de bande passante pour cet objet d'accès.

Sélectionnez les **Connector Groups (Groupes de connecteurs)** ou les **Connectors (Connecteurs)** pour voir les groupes de connecteurs ou les connecteurs uniques associés aux objets d'accès dans le caractère générique.

Sous-réseaux IP

Sélectionnez les **IP Subnets (Sous-réseaux IP)** pour voir votre total d'objets d'accès aux sous-réseaux IP. Un objet d'accès de sous-réseau IP consiste en un regroupement de plusieurs applications différentes.

Affichez le **Total IP Subnets (Total des sous-réseaux IP)** dans votre environnement par état (Actif, Partiellement actif, Inactif ou Désactivé).

Les**IP Subnet ZTNA Access Objects (Objets d'accès ZTNA de sous-réseau IP)** fournissent des informations sur tous vos objets d'accès.

- - **Access Object (Objet d'accès)** : sélectionnez un objet d'accès spécifique pour voir ses détails.
  - **Status (État)** : actif, partiellement actif, inactif ou désactivé.
  - **IP Subnet (Sous-réseau IP)** : sous-réseau IP utilisé pour ajouter cet objet d'accès.
  - **Connector Groups (Groupes de connecteurs)** : les groupes de connecteurs sont des regroupements logiques de connecteurs et d'applications. Affichez les groupes de connecteurs associés à un objet d'accès.
  - **Connectors (Connecteurs)** : les connecteurs représentent les machines virtuelles (VM) fonctionnant dans vos centres de données qui se connectent à Prisma Access. Affichez les connecteurs associés à un objet d'accès.



 ©2025 Palo Alto Networks, Inc.

Sélectionnez un **Access Object (Objet d'accès)** pour voir ses détails.

- **Connector Groups (Groupes de connecteurs)** : découvrez combien de groupes de connecteurs sont associés à cet objet d'accès. Sélectionnez un groupe de connecteurs pour afficher des informations sur ses connexions aux services.
- **Connector Group Status (Current) (État du groupe de connecteurs (actuel))** : actif, partiellement actif, inactif ou désactivé.
- **Connectors (Connecteurs)** : nombre de connecteurs dans ce groupe de connecteurs.
- **Cibles d'application (Application Targets)** : nombre de cibles d'application dans ce groupe de connecteurs.
- **Bandwidth (Bande passante)** : sélectionnez le bouton **Bandwidth (Bande passante)** pour afficher les informations de bande passante pour cet objet d'accès.

Sélectionnez des **Connector Groups (Groupes de connecteurs)** ou des **Connectors (Connecteurs)** pour voir les groupes de connecteurs ou les connecteurs uniques associés aux objets d'accès dans le sous-réseau IP.

Afficher et surveiller les services réseau

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Il s'agit d'une fonctionnalité Prisma Access Insights.

Vous pouvez les performances des services réseau courants qui affectent votre expérience utilisateur pour l'accès aux applications. Les services réseau incluent le signalement du nombre de réussites et d'échecs de l'authentification GlobalProtect comme mesure de la capacité des utilisateurs mobiles à se connecter à Prisma Access et l'affichage des requêtes de proxy DNS et des réponses transmises aux serveurs au cours d'un intervalle de temps que vous spécifiez.

Authentification GlobalProtect

Accédez à **Monitor (Surveiller)** > **Network Services (Services réseau)** > **GlobalProtect Authentication (Authentification GlobalProtect)** dans Strata Cloud Manager pour voir les réussites et les échecs de l'authentification GlobalProtect qui affectent votre environnement.

- Définissez le filtre **Time Range (Intervalle de temps)** pour examiner les données des services réseau pour cet intervalle de temps.
- Spécifiez un **Prisma Access Location (Emplacement Prisma Access)** pour afficher sa réussite d'authentification, le nombre total d'échecs et les échecs de délai d'expiration dans l'intervalle de temps sélectionné.

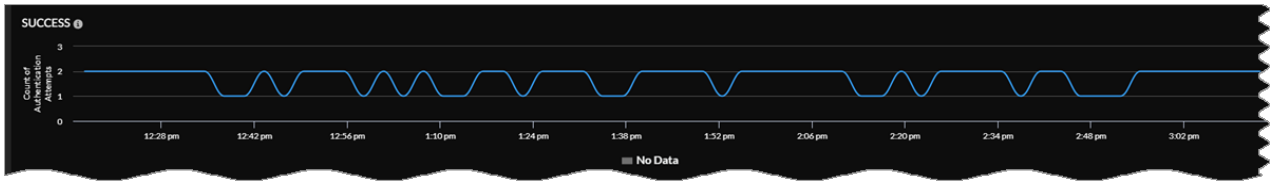
Les données représentent le nombre d'utilisateurs mobiles à un moment donné qui tentent de s'authentifier auprès d'un portail GlobalProtect, qui envoie ensuite les informations d'identification des utilisateurs mobiles pour vérification à un serveur Active Directory (AD) local, ce qui entraîne la réussite ou l'échec de l'authentification. Si vous constatez un grand nombre d'échecs d'authentification, vous pouvez les corréler avec un événement réseau qui indique un problème avec un certain emplacement ou un serveur d'authentification local qui

 ©2025 Palo Alto Networks, Inc.

était inactif. Les données de ces graphiques fournissent des informations de résolution des problèmes aux administrateurs réseau qui résolvent les problèmes de réseau. Vous pouvez afficher le nombre de réussites ou d'échecs d'authentification pour les utilisateurs mobiles sur les portails et les passerelles GlobalProtect, utiliser ces données pour en savoir plus sur les modèles de réussites ou d'échecs d'authentification au fil du temps et établir des plages de nombres qui peuvent être normales ou anormales dans votre déploiement Prisma Access. Par exemple, des nombres anormaux peuvent indiquer l'incapacité des utilisateurs existants à se connecter à Prisma Access en raison de problèmes de disponibilité avec les portails GlobalProtect ou de serveurs d'authentification lents. Ou encore, les nombres anormaux peuvent représenter un grand nombre d'utilisateurs intégrés au réseau du client en une seule fois.

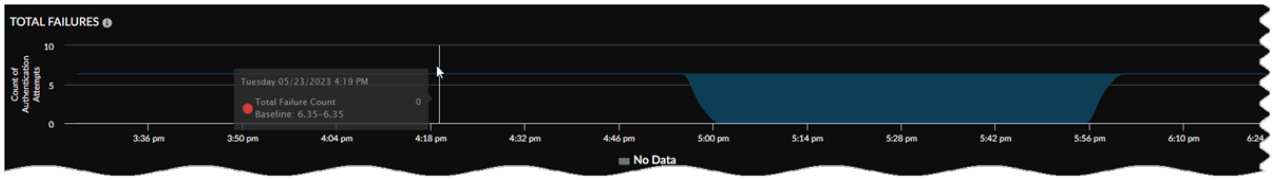
Réussite d'authentification GlobalProtect

Affichez des précisions relatives au nombre de réussites d'authentification pour GlobalProtect pour différents emplacements. Passez votre curseur sur n'importe quel point du graphique pour voir les détails sur le nombre d'utilisateurs pour les authentifications réussies à différents emplacements de localisation Prisma Access affichés à un moment donné.



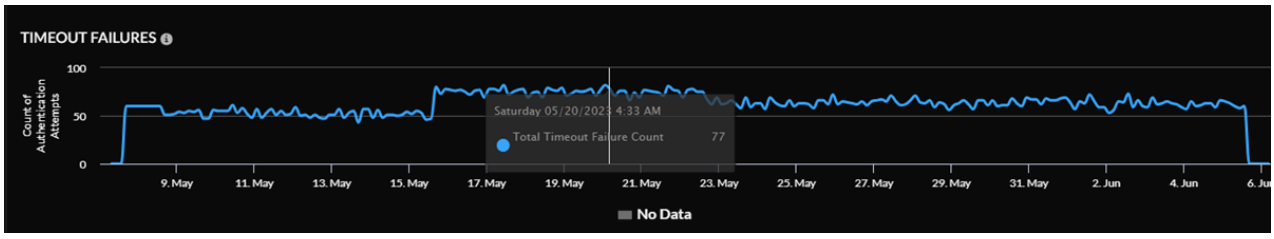
Nombre total d'échecs d'authentification GlobalProtect

Affichez des précisions relatives au nombre d'échecs d'authentification pour GlobalProtect pour différents emplacements. Passez votre curseur sur n'importe quel point du graphique pour voir les détails sur le nombre d'utilisateurs pour les échecs d'authentification à différents emplacements de localisation Prisma Access, tels que US East (Est des États-Unis) et Canada East (Est du Canada), à un moment donné.



Échecs du délai d'expiration de l'authentification GlobalProtect

Affichez des précisions relatives au nombre d'échecs d'authentification pour GlobalProtect pour différents emplacements. Passez votre curseur sur n'importe quel point du graphique pour voir les détails sur le nombre d'utilisateurs pour les échecs d'authentification à différents emplacements de localisation Prisma Access, tels que US East (Est des États-Unis) et Canada East (Est du Canada), à un moment donné.



 ©2025 Palo Alto Networks, Inc.

DNS

Accédez à **Monitor (Surveiller)** > **Network Services (Services réseau)** > **GlobalProtect Authentication (Authentification GlobalProtect)** dans Strata Cloud Manager pour afficher les requêtes de proxy DNS et les réponses transmises aux serveurs au cours d'un intervalle de temps que vous spécifiez.

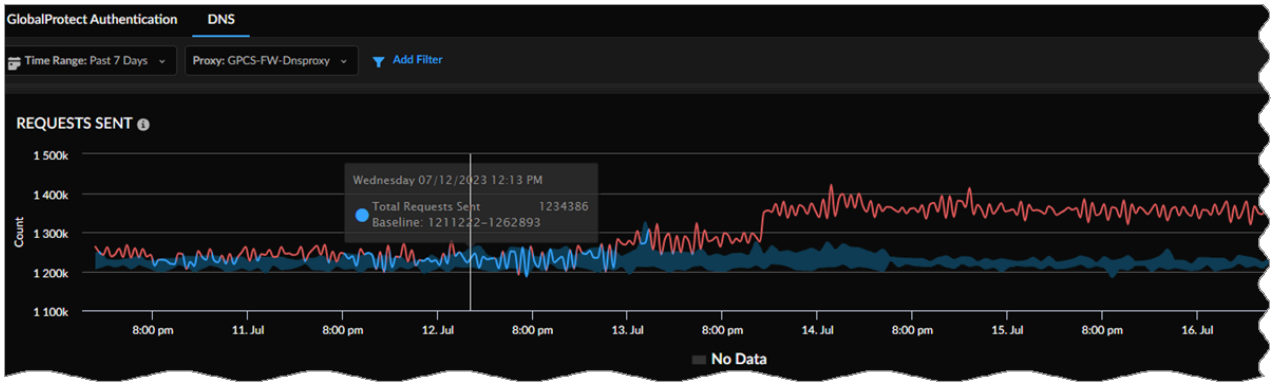
Les filtres que vous pouvez utiliser sont les suivants :

- **Plage horaire**
- **Noms de proxy DNS**

Les valeurs du filtre proxy DNS sont liées aux 30 derniers jours et sont automatiquement sélectionnées lors du chargement (c'est-à-dire que s'il n'y a pas de données Proxy explicites, les filtres Proxy explicites n'existent pas). Passez la souris sur le graphique pour voir les détails de toutes les **Requests Sent (Requêtes envoyées)** et **Requests Received (Requêtes reçues)** aux serveurs proxy DNS à un moment donné.

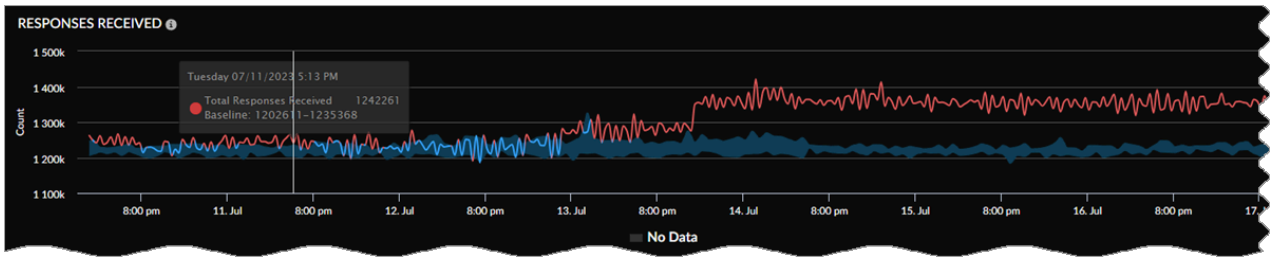
Requêtes envoyées

Affichez les demandes et requêtes réseau transmises aux serveurs sur l'intervalle de temps que vous spécifiez. Passez votre curseur sur n'importe quel point du graphique pour voir des informations sur les requêtes envoyées aux serveurs proxy DNS à ce moment-là. Si vous avez sélectionné un nom de proxy sur lequel filtrer, vous voyez les données de ce proxy.



Réponses reçues

Affichez le nombre total de réponses reçues par les locataires pendant l'intervalle de temps que vous spécifiez. Passez votre curseur sur n'importe quel point du graphique pour voir des informations sur les réponses reçues à ce moment-là. Si vous avez sélectionné un nom de proxy sur lequel filtrer, vous voyez les données de ce proxy.



 ©2025 Palo Alto Networks, Inc.

Afficher et surveiller les services réseau : Authentification GlobalProtect

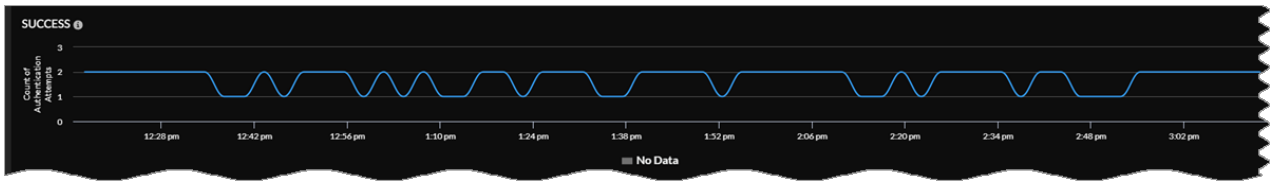
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Il s'agit d'une fonctionnalité Prisma Access Insights.

Les services réseau incluent la notification pour le nombre de succès et d'échecs liés à l'authentification GlobalProtect. Cette mesure permet d'évaluer la capacité des utilisateurs mobiles à se connecter à Prisma Access. Sélectionnez **Monitor (Surveiller)** > **Network Services (Services réseau)** > **GlobalProtect Authentication (Authentification GlobalProtect)** dans Strata Cloud Manager pour commencer.

- Définissez le filtre **Time Range (Intervalle de temps)** pour examiner les données des services réseau pour cet intervalle de temps.
- Spécifiez un **Prisma Access Location (Emplacement Prisma Access)** pour afficher sa réussite d'authentification, le nombre total d'échecs et les échecs de délai d'expiration dans l'intervalle de temps sélectionné.

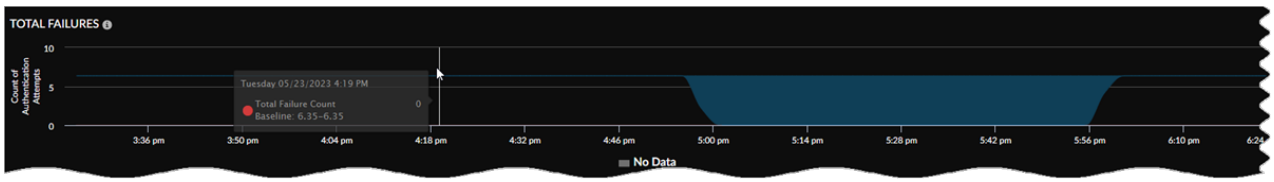
Réussite d'authentification GlobalProtect

Affichez des précisions relatives au nombre de réussites d'authentification pour GlobalProtect pour différents emplacements. Passez votre curseur sur n'importe quel point du graphique pour voir les détails sur le nombre d'utilisateurs pour les authentifications réussies à différents emplacements de localisation Prisma Access affichés à un moment donné.



Nombre total d'échecs d'authentification GlobalProtect

Affichez des précisions relatives au nombre d'échecs d'authentification pour GlobalProtect pour différents emplacements. Passez votre curseur sur n'importe quel point du graphique pour voir les détails sur le nombre d'utilisateurs pour les échecs d'authentification à différents emplacements de localisation Prisma Access, tels que US East (Est des États-Unis) et Canada East (Est du Canada), à un moment donné.

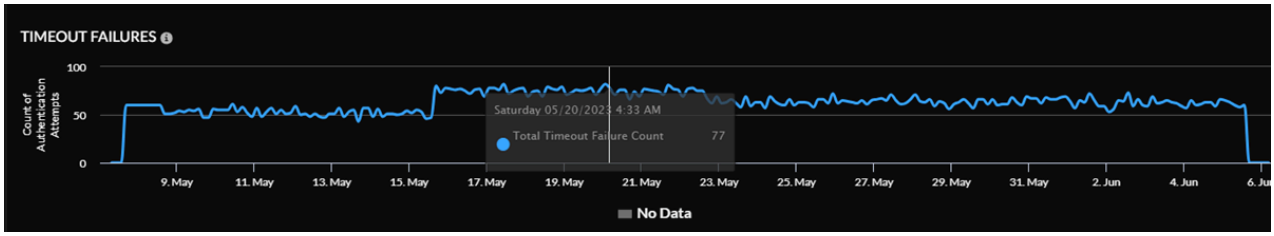


Échecs du délai d'expiration de l'authentification GlobalProtect

Affichez des précisions relatives au nombre d'échecs d'authentification pour GlobalProtect pour différents emplacements. Passez votre curseur sur n'importe quel point du graphique pour voir les détails sur le nombre d'utilisateurs pour les échecs d'authentification à différents emplacements

 ©2025 Palo Alto Networks, Inc.

de localisation Prisma Access, tels que US East (Est des États-Unis) et Canada East (Est du Canada), à un moment donné.



Afficher et surveiller les services réseau : DNS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ C'est une fonctionnalité Prisma Access Insights.

Services de réseau : DNS (Network Services: DNS) affiche les requêtes et réponses proxy DNS transmises aux serveurs pendant un intervalle de temps que vous spécifiez.

Filtres que vous pouvez utiliser :

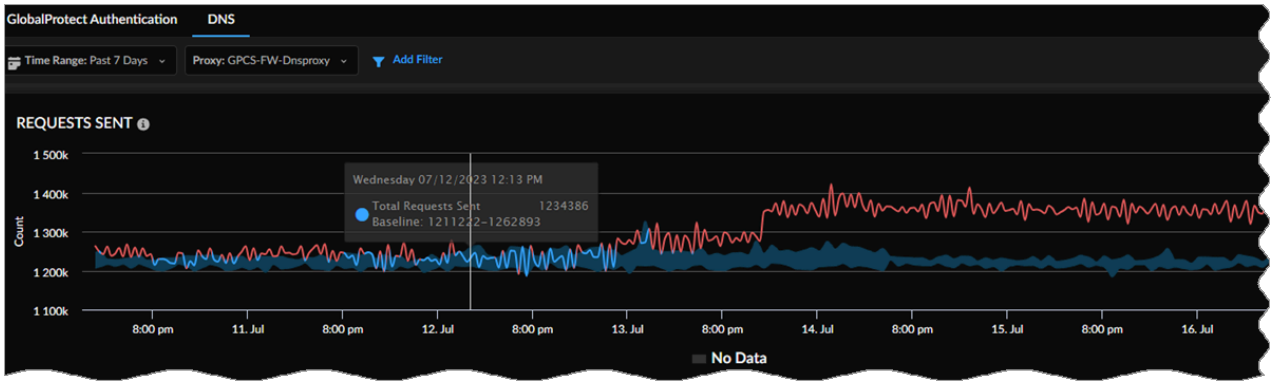
- **Plage horaire**
- **Noms de proxy DNS**

Les valeurs du filtre proxy DNS sont liées aux 30 derniers jours et sont automatiquement sélectionnées lors du chargement (c'est-à-dire que s'il n'y a pas de données Proxy explicites, les filtres Proxy explicites n'existent pas).

Passez la souris sur le graphique pour voir les détails de toutes les **Requests Sent (Requêtes envoyées)** et **Requests Received (Requêtes reçues)** aux serveurs proxy DNS à un moment donné.

Requêtes envoyées

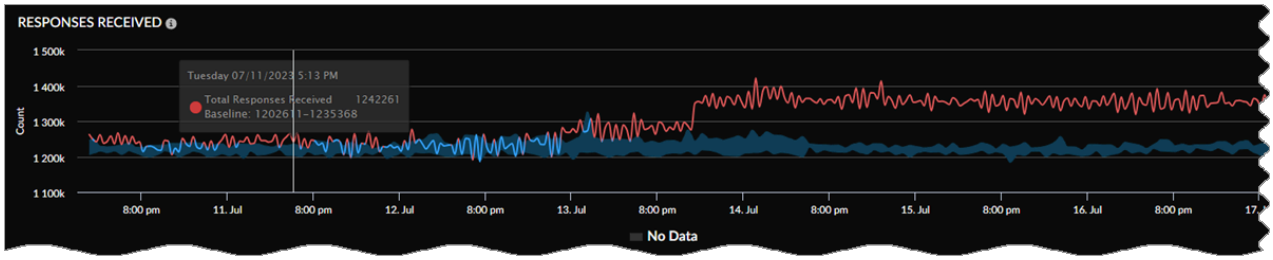
Affichez les demandes et requêtes réseau transmises aux serveurs sur l'intervalle de temps que vous spécifiez. Passez votre curseur sur n'importe quel point du graphique pour voir des informations sur les requêtes envoyées aux serveurs proxy DNS à ce moment-là. Si vous avez sélectionné un nom de proxy sur lequel filtrer, vous voyez les données de ce proxy.



 ©2025 Palo Alto Networks, Inc.

Réponses reçues

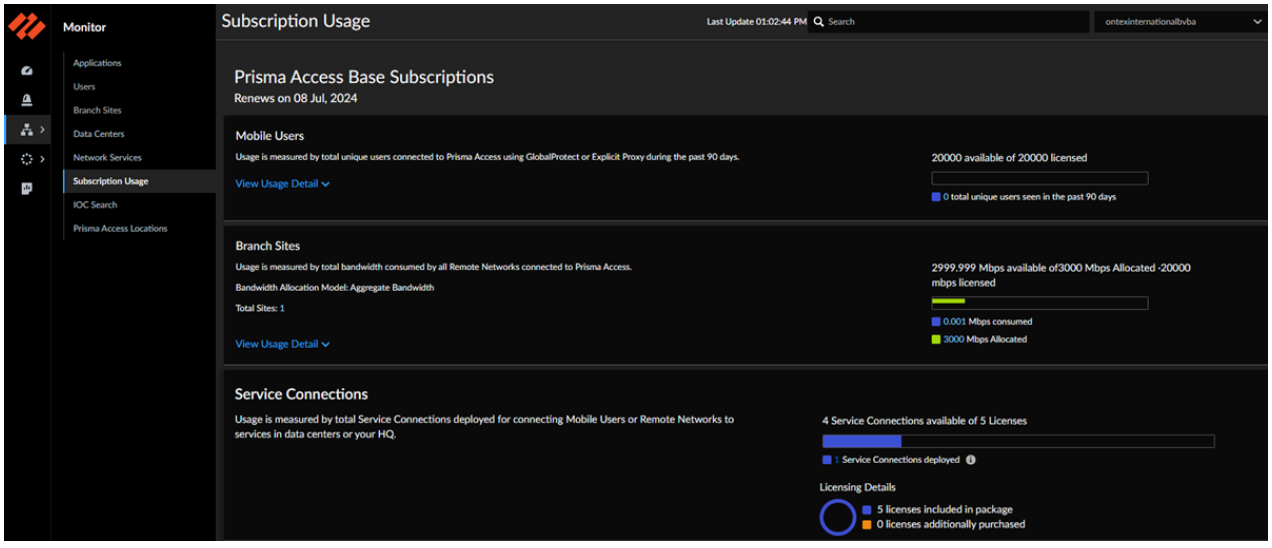
Affichez le nombre total de réponses reçues par les locataires pendant l'intervalle de temps que vous spécifiez. Passez votre curseur sur n'importe quel point du graphique pour voir des informations sur les réponses reçues à ce moment-là. Si vous avez sélectionné un nom de proxy sur lequel filtrer, vous voyez les données de ce proxy.



Afficher l'utilisation de l'abonnement

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Sélectionnez **Monitor (Surveiller)** > **Subscription usage (Utilisation de l'abonnement)** pour afficher les détails de vos **Prisma Access Base Subscriptions (Abonnements de base Prisma Access)**, y compris le nombre de licences que vous avez consommées jusqu'à présent.

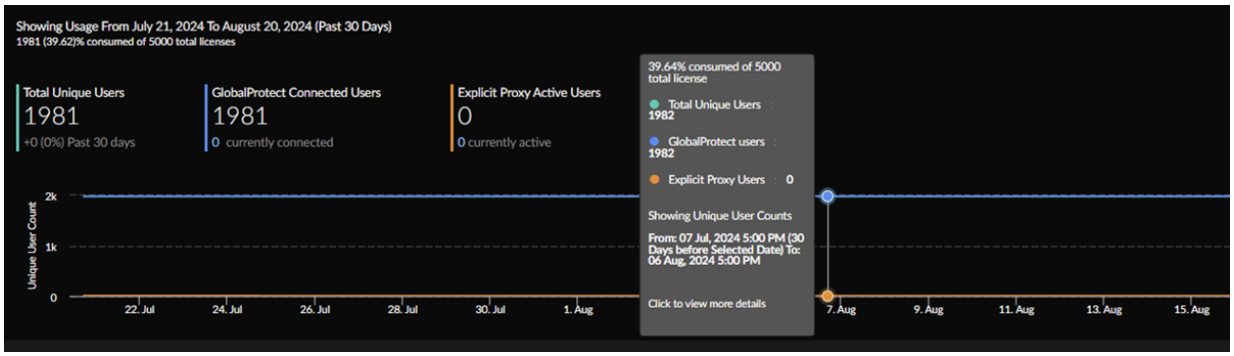


- **Mobile Users (Utilisateurs mobiles)** : affichez le nombre de licences de **Mobile Users (Utilisateurs mobiles)** que vous avez consommées jusqu'à présent. Le widget affiche le nombre total de licences utilisées par les utilisateurs mobiles uniques connectés à Prisma Access au cours des 30 derniers jours, car l'utilisation des licences est basée sur les données de connexion à Prisma Access des 30 derniers jours. Un utilisateur qui s'est connecté à Prisma Access au

 ©2025 Palo Alto Networks, Inc.

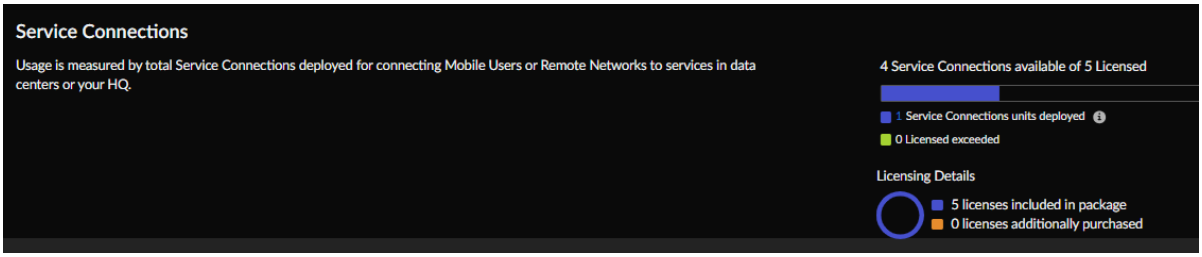
moins une fois au cours des 30 derniers jours contribue à l'utilisation d'une licence d'Utilisateur mobile.

Sélectionnez **View Usage Detail (Afficher les détails d'utilisation)** pour voir les détails sur l'utilisation de la licence au cours des 30 derniers jours. Vous pouvez afficher le nombre total d'utilisateurs uniques au cours des 30 derniers jours, le nombre total d'utilisateurs connectés à GlobalProtect et le nombre total d'utilisateurs actifs de proxy explicite. Passez la souris sur le graphique pour voir les licences consommées à ce moment-là.



- **Branch Sites (Sites de succursales)** : consultez l'utilisation totale de la bande passante par tous les réseaux distants connectés à Prisma Access. Affichez la quantité de bande passante que vous avez allouée et celle que vous avez utilisée, en Mbits/s. Vous voyez l'utilisation de la bande passante totale utilisée par tous les réseaux distants connectés à Prisma Access.

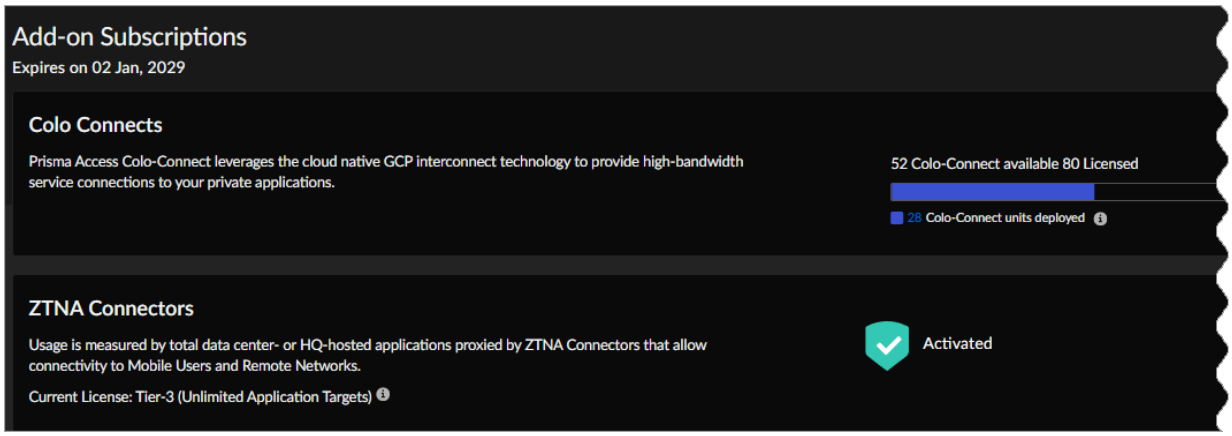
  Sélectionnez **View Usage Detail (Afficher les détails d'utilisation)** pour voir votre consommation de bande passante sous licence par régions de calcul ou sites de succursales en fonction de votre modèle d'allocation de bande passante. Dans chaque cas, une valeur de consommation de bande passante maximale quotidienne est indiquée pour chacun des 30 jours considérés pour le calcul de la licence. Vous pouvez filtrer la vue graphique en sélectionnant des régions de calcul ou des sites de succursales. Trois lignes sont tracées par région de calcul ou par site dans le graphique, indiquant les valeurs de consommation maximale quotidiennes, la bande passante allouée à la région de calcul ou au site et la valeur du 95e percentile obtenue à partir des pics quotidiens.
- **Service Connections (Connexions aux services)** : découvrez combien de **Service Connections (Connexions aux services)** vous avez consommées jusqu'à présent.



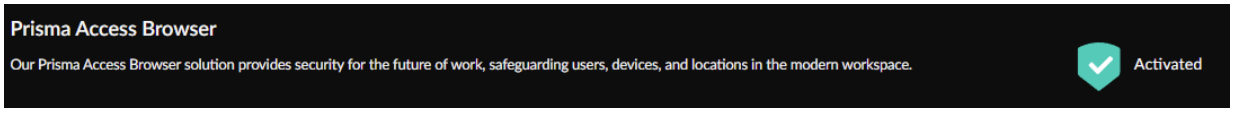
Consultez la section **Add-On Subscriptions (Abonnements complémentaires)** sur cette page pour voir les licences supplémentaires que vous avez achetées. Vous pouvez voir le nombre total de licences achetées ainsi que le nombre de licences non utilisées jusqu'à présent. Les images suivantes décrivent certaines des licences supplémentaires que vous pouvez acheter.

 ©2025 Palo Alto Networks, Inc.

- **Colo-Connects** : Prisma Access Colo-Connect exploite la technologie GCP native du cloud pour fournir des connexions aux services à large bande passante à vos applications privées.



- **Prisma Access Browser** : le navigateur d'entreprise Prisma Access Secure (Prisma Access Browser) est la seule solution qui sécurise les périphériques gérés et non gérés via un navigateur d'entreprise intégré nativement qui étend la protection aux périphériques non gérés. Prisma Access Browser protège les applications et les données professionnelles en plaçant la sécurité dans le navigateur. Votre abonnement au Prisma Access Browser apparaît dans les **Add-on Subscriptions (Abonnements complémentaires)** ou **Prisma Access Base Subscriptions (Abonnements de base Prisma Access)**.
  - **Prisma Access Base Subscriptions (Abonnements de base Prisma Access)** : le locataire dispose d'une licence autonome Prisma Access Browser.
  - **Add-on Subscriptions (Abonnements complémentaires)** : lorsque vous avez acheté la licence Prisma Access Browser pour tous les utilisateurs mobiles, l'abonnement Prisma Access Browser est **Activated (Activé)**.



Afficher et surveiller les emplacements Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Il s'agit d'une fonctionnalité Prisma Access Insights.

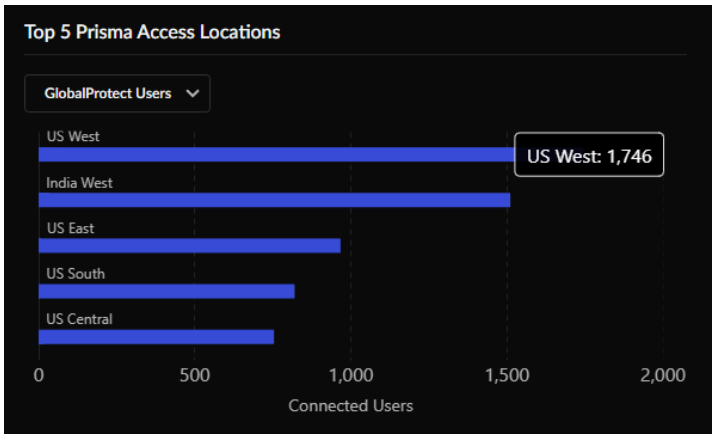
Sélectionnez **Monitor (Surveiller)** > **Prisma Access Locations (Emplacements Prisma Access)** pour avoir une vue d'ensemble de l'état de tous vos emplacements Prisma Access pour vos réseaux distants et vos utilisateurs mobiles.

Top 5 des emplacements Prisma Access

Les barres affichent des données sur le top 5 des emplacements Prisma Access des réseaux distants, des connexions aux services, des utilisateurs mobiles GlobalProtect ou des utilisateurs

 ©2025 Palo Alto Networks, Inc.

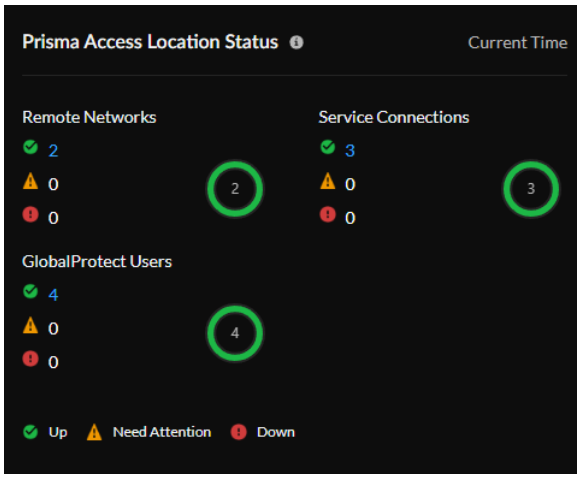
mobiles Proxy explicite (sélectionnés dans la liste déroulante), en fonction de la bande passante totale consommée au cours de l'intervalle de temps sélectionné. Passez la souris sur n'importe quelle barre pour voir combien d'utilisateurs se trouvent à cet emplacement particulier.



État de l'emplacement Prisma Access

En fonction de votre licence, ce widget indique le nombre de sites de réseau distant connectés, de sites de connexion aux services, d'utilisateurs GlobalProtect uniques et d'utilisateurs de proxy explicite uniques connectés à Prisma Access. Le code couleur du widget est basé sur le nombre de réseaux distants, de connexions aux services, d'utilisateurs GlobalProtect et d'utilisateurs de proxy explicite dont l'état est le suivant :

- **Connected (Connecté)** (vert) : tous les emplacements Prisma Access sont connectés.
- **Disconnected (Déconnecté)** (rouge) : tous les emplacements Prisma Access sont déconnectés.
- **Partially Connected (Partiellement connecté)** (orange) : un ou plusieurs emplacements Prisma Access sont déconnectés.



Strata Logging Service Connectivité

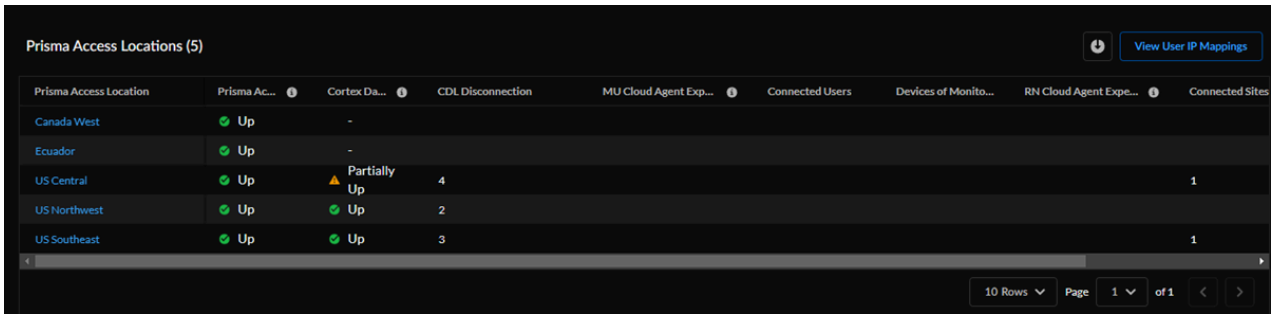
Strata Logging Service Connectivity (Connectivité) vous donne une visibilité sur l'état de la connectivité Strata Logging Service de toutes vos instances Prisma Access pour la région Strata Logging Service que vous avez sélectionnée lors de l'activation de votre licence Prisma Access. Il vous aide à déterminer si les pare-feu se sont déconnectés de Strata Logging Service et vous n'obtenez plus les journaux du pare-feu. Chaque locataire ne peut se connecter qu'à

 ©2025 Palo Alto Networks, Inc.

un seul Strata Logging Service dans la région de son choix. Prisma Access interroge la base de données Strata Logging Service toutes les 5 minutes pour vérifier la connectivité entre les nœuds (utilisateurs mobiles, réseaux distants et connexions aux services) et la base de données Strata Logging Service.

État des emplacements Prisma Access

Consultez l'état des **Prisma Access Locations (Emplacements Prisma Access)** en temps réel. Au sein d'un emplacement spécifique, si un utilisateur se connecte à partir de plusieurs hôtes, il est compté comme un seul utilisateur, mais si un utilisateur se connecte à partir de deux emplacements Prisma Access différents en se déconnectant de l'un et en se connectant à partir d'un autre dans le laps de temps, l'utilisateur est compté comme deux utilisateurs. Sélectionnez un emplacement pour afficher les détails, tels que la bande passante consommée, l'état, la connectivité Strata Logging Service, et les mappages d'ID utilisateur et de groupe.



Afficher et surveiller les Device-ID tiers

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

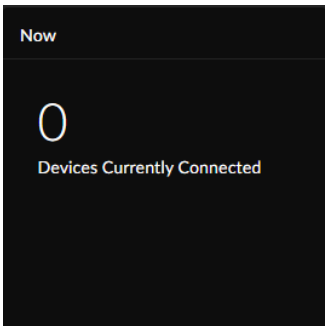
Vous pouvez utiliser Cloud Identity Engine avec Prisma Access pour appliquer des informations provenant de sources de détection IoT tierces afin de simplifier l'identification et la correction des failles de sécurité pour les périphériques de votre réseau. Reportez-vous à Configurer le Device-ID tiers dans Prisma Access pour plus de détails sur l'installation et la configuration.

Accédez à **Monitor (Surveiller)** > **Devices (Périphériques)** > **IOT** pour obtenir des informations sur vos périphériques IoT, telles que le nombre de périphériques IoT connectés au cours des 30 dernières minutes, tous les périphériques IoT connectés pendant l'intervalle de temps sélectionné et des détails sur tous les périphériques IoT connectés.

Appareils actuellement connectés

Affichez le nombre de périphériques connectés, le cas échéant, au cours des 30 dernières minutes. **Now (Maintenant)** affiche toujours le **Périphériques actuellement connectés** seulement dans les 30 dernières minutes.

 ©2025 Palo Alto Networks, Inc.

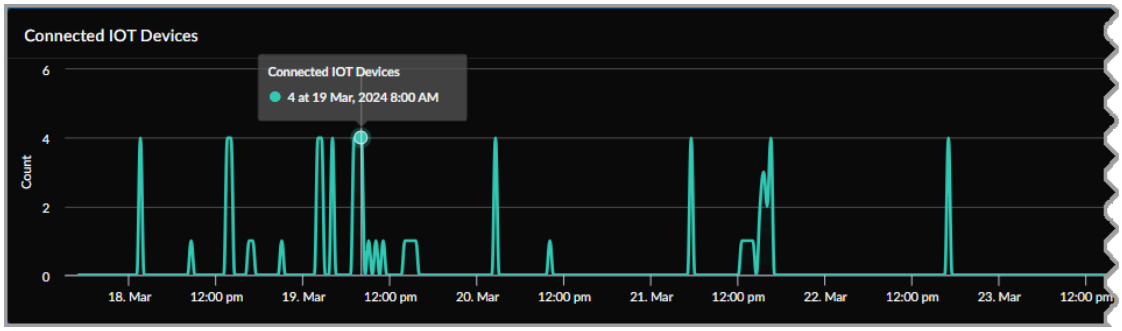


Périphériques IoT connectés

Connected IoT Devices (Périphériques IoT connectés) affiche le nombre de périphériques connectés filtrés par **Time Range (Intervalle de temps)**. Personnalisez les données affichées en sélectionnant d'autres options de filtrage dans la liste déroulante **Add Filters (Ajouter des filtres)**.

- **Category (Catégorie)** : catégorie à laquelle appartient ce périphérique.
- **Mac Address (Adresse MAC)** : adresse MAC du périphérique.
- **Profile (Profil)** : profil du périphérique.
- **Vendor (Fournisseur)** : fournisseur du périphérique.
- **Source IP (Adresse IP)** : adresse IP du périphérique.
- **Prisma Access Location (Emplacement Prisma Access)** : emplacement Prisma Access du périphérique.
- **Branch Site (Site de succursale)**: site de succursale sur lequel se trouve le périphérique.

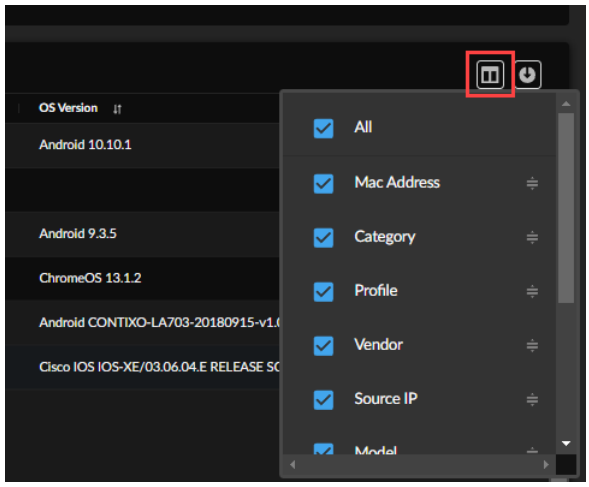
Passez la souris sur un point du graphique pour voir le nombre d'utilisateurs à un moment donné. Connaître les tendances des utilisateurs sur une période donnée peut vous aider à surveiller l'utilisation et à enquêter sur les modèles inhabituels.



Appareils IoT

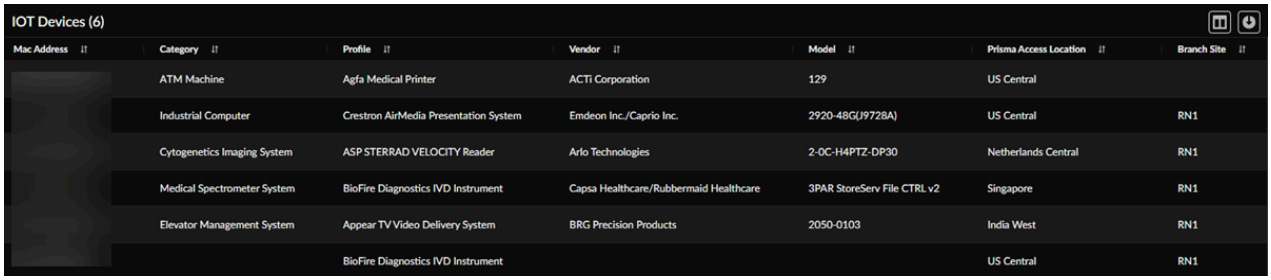
Affichez le nombre de périphériques IoT connectés au cours de la **Time Range (Intervalle de temps)**. Utilisez la liste déroulante des colonnes pour sélectionner ou désélectionner les colonnes qui apparaissent dans le tableau.

 ©2025 Palo Alto Networks, Inc.



- **Mac Address (Adresse MAC)** : adresse MAC du périphérique.
- **Category (Catégorie)** : catégorie à laquelle appartient ce périphérique.
- **Profile (Profil)** : profil du périphérique.
- **Vendor (Fournisseur)** : fournisseur du périphérique.
- **Source IP (Adresse IP source)** : adresse IP du périphérique.
- **Modèle (Modèle)** : modèle du périphérique.
- **OS Version (Version du système d'exploitation)** : version du système d'exploitation.
- **OS Family (Famille de systèmes d'exploitation)** : famille de systèmes d'exploitation à laquelle appartient le périphérique.
- **Prisma Access Location (Emplacement d'accès Prisma)** : emplacement Prisma Access utilisé.
- **Branch Site (Site de succursale)** : site de succursale sur lequel se trouve le périphérique.

Le tableau suivant IOT Devices (Périphériques IOT) présente une sélection de colonnes personnalisée. Pour afficher toutes les colonnes du tableau, sélectionnez toutes les options dans la liste déroulante.



Afficher et surveiller l'isolation de navigateur à distance

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Innovation Prisma Access 5.0

 ©2025 Palo Alto Networks, Inc.

Vous pouvez utiliser Strata Cloud Manager pour obtenir une visibilité complète sur le trafic de votre réseau et pour l'isolation de navigateur à distance (RBI) en utilisant les sections Monitor (Surveiller) et Workflows (Flux de travail) de Strata Cloud Manager. Obtenez de la visibilité sur votre déploiement RBI en consultant des indicateurs tels que le nombre d'utilisateurs RBI actifs, les tendances, l'état de la connectivité, l'état de l'emplacement RBI, les mesures de trafic et la consommation de licences. En affichant les données sur vos utilisateurs, vous pouvez obtenir une vue d'ensemble de l'état et de la connectivité de votre déploiement.

RBI redirige l'activité de navigation Internet des utilisateurs vers un environnement isolé hébergé par un fournisseur RBI. Le site Web est rendu pour les utilisateurs, qui peuvent consulter les ressources dont ils ont besoin, sans accéder directement à des sites inconnus ou risqués depuis leurs périphériques et leur réseau. Prisma Access s'intègre facilement avec les fournisseurs RBI pour ce type de redirection de navigateur.

 ©2025 Palo Alto Networks, Inc.

Prisma Access et Autonomous DEM

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Strata Cloud Manager Managed Prisma Access • Panorama Managed Prisma Access	❑ Licence Prisma Access ❑ Licence Autonomous DEM

Lancez-vous avec Autonomous DEM dans Prisma Access pour surveiller en permanence l'expérience numérique de l'ensemble des utilisateurs, applications et sites distants de votre environnement SASE. Tant que vous disposez des licences correspondantes, vous pouvez activer Autonomous DEM pour vos utilisateurs mobiles GlobalProtect qui se connectent à Prisma Access.

- Fiche de référence : ADEM avec Prisma Access
- Premiers pas avec Autonomous DEM
- Surveiller le trafic des utilisateurs et les applications avec Autonomous DEM

©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Prisma Access Politique basée sur l'utilisateur

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • Cloud Identity Engine	• Licence Prisma Access

Prisma Access nécessite que vous configuriez le mappage nom d'utilisateur/adresse IP pour appliquer de manière cohérente la stratégie basée sur l'utilisateur pour les utilisateurs mobiles et les utilisateurs situés sur des emplacements réseau distants. De plus, vous devez configurer mappage du nom d'utilisateur au groupe d'utilisateurs si vous souhaitez appliquer une stratégie basée sur l'appartenance à un groupe.

Pour sélectionner les groupes dans une liste déroulante lorsque vous créez et configurez des stratégies dans Panorama, vous pouvez également configurer Panorama pour obtenir la liste des groupes d'utilisateurs récupérée à partir du mappage de nom d'utilisateur à groupe d'utilisateurs.

Les sections suivantes fournissent une vue d'ensemble et les étapes à suivre pour configurer et implémenter l'ID utilisateur et utiliser Cloud Identity Engine pour obtenir le mappage de l'adresse IP vers le nom d'utilisateur et du nom d'utilisateur vers le groupe d'utilisateurs Prisma Access.

Configurer la stratégie basée sur l'utilisateur pour Prisma Access

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

Politique axée sur l'utilisateur Prisma Access (Strata Cloud Manager)

Après avoir intégré Cloud Identity Engine avec Prisma Access, vous devez confirmer que Prisma Access est connecté à Cloud Identity Engine et avec lequel il partage des informations de répertoire Prisma Access.

- Vérifiez que vous pouvez afficher vos répertoires dans Prisma Access.

  Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Cloud Identity Engine**.

- Vérifiez que vous pouvez ajouter des utilisateurs et des groupes à une règle de politique.

  Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Decryption (Décryptage)**.

  Dans une règle de politique de sécurité ou de décryptage, vérifiez que la liste déroulante **Users (Utilisateurs)** affiche vos entrées d'utilisateur et de groupe Active Directory. Vous pouvez maintenant commencer à ajouter ces utilisateurs et groupes à vos règles de politique de sécurité et de décryptage.

Une fois que vous avez vérifié que Cloud Identity Engine est correctement connecté, vous pouvez commencer à exécuter les rapports d'activité des utilisateurs pour obtenir une meilleure visibilité sur le comportement de votre base d'utilisateurs.

 ©2025 Palo Alto Networks, Inc.

Politique axée sur l'utilisateur Prisma Access (Panorama)

Cette section décrit les étapes à suivre pour configurer User-ID pour Prisma Access.

STEP 1 | Configurez le mappage nom d'utilisateur/adresse IP pour vos utilisateurs mobiles et les utilisateurs sur des emplacements de réseaux distants.

- Pour les déploiements d'utilisateurs mobiles GlobalProtect, l'agent GlobalProtect dans Prisma Access effectue automatiquement le mappage User-ID.
- Pour les utilisateurs de réseaux distants, configurez User-ID pour les déploiements de réseaux distants pour mapper les adresses IP aux ID utilisateur.

STEP 2 | Configurez le mappage nom d'utilisateur-groupe d'utilisateurs pour vos utilisateurs mobiles et les utilisateurs sur des emplacements de réseaux distants.

Pour les utilisateurs mobiles GlobalProtect, proxys explicites et les déploiements de réseaux distants, configurez le composant Directory Sync (Synchronisation du répertoire) de Cloud Identity Engine pour récupérer des informations sur les utilisateurs et les groupes à partir de votre Active Directory (AD). Ensuite, configurez **Group Mapping Settings (Paramètres de mappage de groupe)** dans vos utilisateurs mobiles GlobalProtect ou vos déploiements de réseaux distants.

Vous pouvez également activer le mappage nom d'utilisateur-groupe d'utilisateurs pour les utilisateurs mobiles et les utilisateurs sur des réseaux distants à l'aide d'un profil du serveur LDAP.



Nous vous recommandons d'utiliser une liste d'inclusion de groupe dans le profil du serveur LDAP, afin que vous puissiez spécifier les groupes que vous souhaitez récupérer, au lieu de récupérer toutes les informations de groupe.

STEP 3 | Autorisez Panorama à utiliser le mappage nom d'utilisateur-groupe d'utilisateurs dans les politiques de sécurité en effectuant l'une des actions suivantes :

- Configurez le composant Directory Sync (Synchronisation du répertoire) de Cloud Identity Engine pour récupérer des informations sur les utilisateurs et les groupes à partir de votre Active Directory (AD). Ensuite, configurez **Group Mapping Settings (Paramètres de mappage de groupe)** dans vos utilisateurs mobiles GlobalProtect, vos utilisateurs mobiles—proxy explicite ou votre déploiement de réseaux distants.
- Configurez la politique basée sur les groupes en précisant le nom unique (DN) complet du groupe.

STEP 4 | Redistribuez les informations HIP vers Panorama.

 ©2025 Palo Alto Networks, Inc.

Intégrer le Cloud Identity Engine à Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

- Strata Cloud Manager
- Panorama

Intégrer le Cloud Identity Engine à Prisma Access (Strata Cloud Manager)

Le Cloud Identity Engine (synchronisation d'annuaire) donne à Prisma Access un accès en lecture seule à vos informations Active Directory afin que vous puissiez facilement configurer et gérer des politiques de sécurité et de décryptage pour les utilisateurs et les groupes.

Le Moteur d'identité sur le cloud fonctionne avec Active Directory et Azure Active Directory sur site.

Pour configurer le Cloud Identity Engine avec Prisma Access, commencez par vous rendre sur le concentrateur pour activer le Cloud Identity Engine et l'ajouter à Prisma Access. Ensuite, accédez à Prisma Access pour vérifier que Prisma Access est capable d'accéder aux données d'annuaire.

 ©2025 Palo Alto Networks, Inc.



STEP 1 | Activer le Moteur d'identité sur le cloud

Le Moteur d'identité sur le cloud peut partager des informations Active Directory avec n'importe quelle application prise en charge sur le concentrateur. Il est gratuit et ne nécessite pas de code d'authentification pour commencer. La configuration du Moteur d'identité sur le cloud comprend l'activation de l'appli Moteur d'identité sur le cloud sur le concentrateur, la configuration de l'agent Moteur d'identité sur le cloud pour rassembler les mappages Active Directory et la configuration de l'authentification mutuelle entre l'identité et l'agent.

Veillez à déployer l'instance du Cloud Identity Engine dans la région où vous avez déployé Prisma Access et Strata Logging Service.

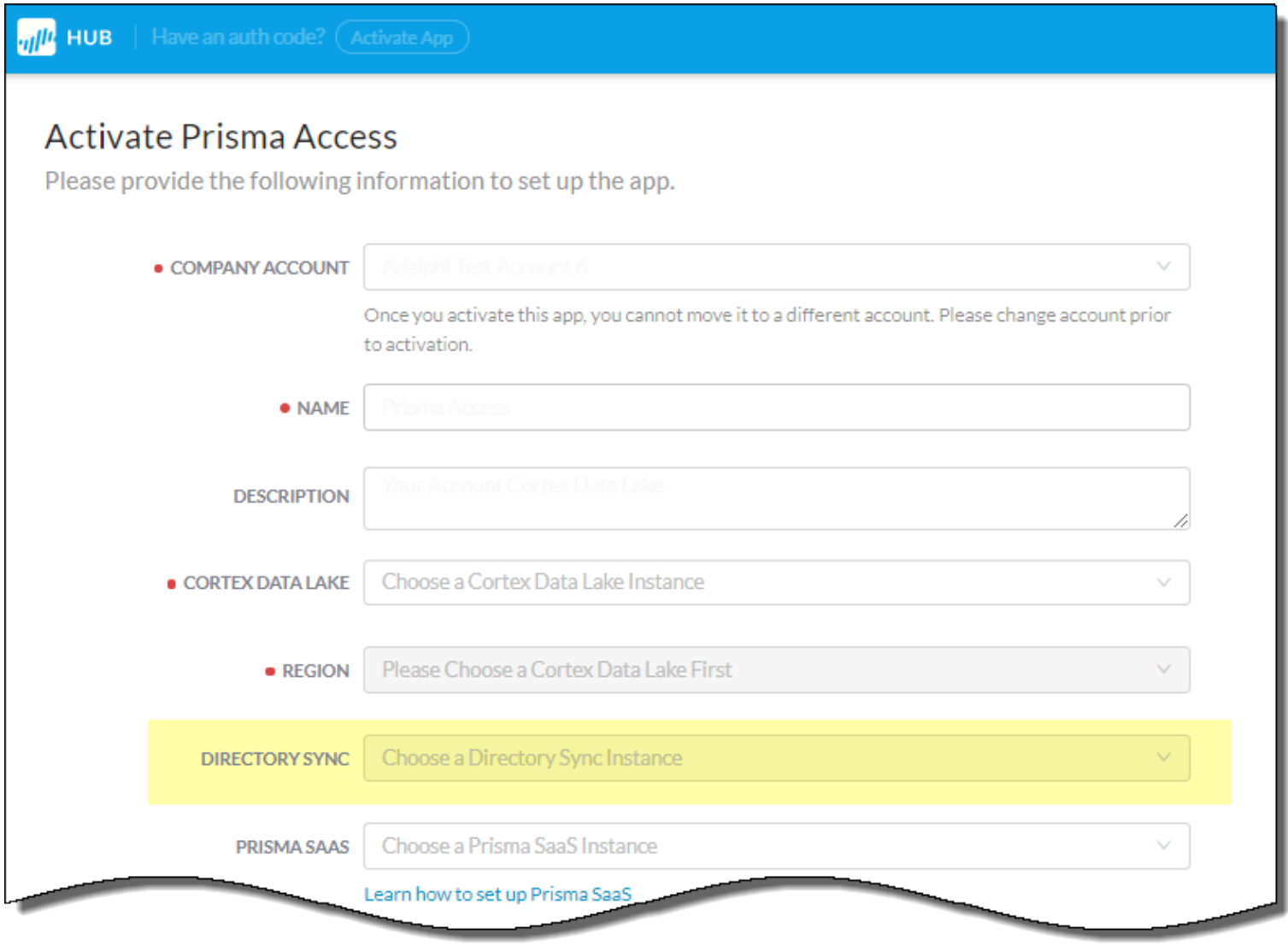
STEP 2 | Activez le Cloud Identity Engine pour Prisma Access.

Vous pouvez associer Prisma Access au Cloud Identity Engine lors de la première activation de Prisma Access ou à tout moment après :

- **Pendant l'activation de Prisma Access :** Lorsque vous activez Cloud Managed Prisma Access pour la première fois, vous pouvez choisir une instance du Cloud Identity Engine

 ©2025 Palo Alto Networks, Inc.

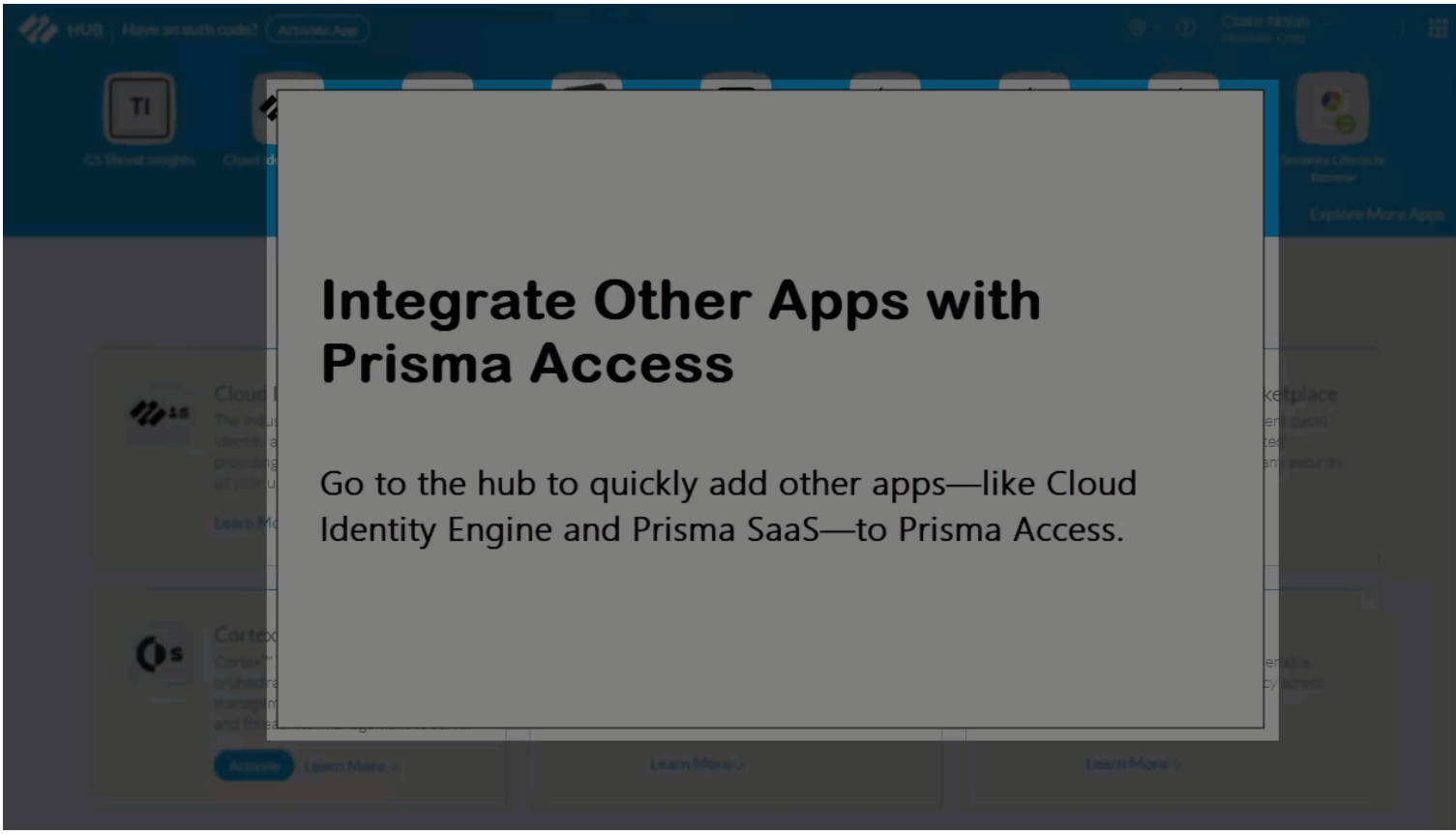
pour Prisma Access. Veillez à sélectionner une instance déployée dans la même région que Prisma Access.



- **Après l'activation de Prisma Access :** Pour activer le Cloud Identity Engine pour une instance Prisma Access existante, connectez-vous au concentrateur. Dans le menu déroulant Paramètres du concentrateur (voir l'engrenage dans la barre de menu supérieure), sélectionnez **Manage Apps (Gérer les applis)**. Recherchez l'instance Prisma Access que vous

 ©2025 Palo Alto Networks, Inc.

souhaitez mettre à jour, puis sélectionnez l'instance du Cloud Identity Engine que Prisma Access doit utiliser.



STEP 3 | Vérifiez que Prisma Access est connecté au Cloud Identity Engine.

Intégrer le Cloud Identity Engine à Prisma Access (Panorama)

Prisma Access récupère les informations sur les utilisateurs et les groupes à partir de l'annuaire cloud ou du service Active Directory (AD) de votre organisation pour appliquer une politique basée sur les utilisateurs et les groupes. Prisma Access peut éventuellement récupérer les signaux de risque basés sur le comportement des utilisateurs auprès de certains fournisseurs d'annuaires cloud, tels qu'Azure Active Directory, pour appliquer des actions de sécurité automatisées. Vous pouvez simplifier la récupération des informations sur les utilisateurs et les groupes en utilisant le Cloud Identity Engine.

En plus de simplifier la récupération des informations sur les utilisateurs et les groupes, l'intégration du Cloud Identity Engine à Prisma Access peut libérer la bande passante et réduire la charge sur votre annuaire cloud ou AD.

Vous pouvez utiliser le Cloud Identity Engine pour récupérer des informations sur les utilisateurs et les groupes pour Prisma Access pour les utilisateurs mobiles, les réseaux distants ou les deux en procédant comme suit.

L'intégration du Cloud Identity Engine à Prisma Access présente les restrictions de mise en œuvre suivantes :

 ©2025 Palo Alto Networks, Inc.

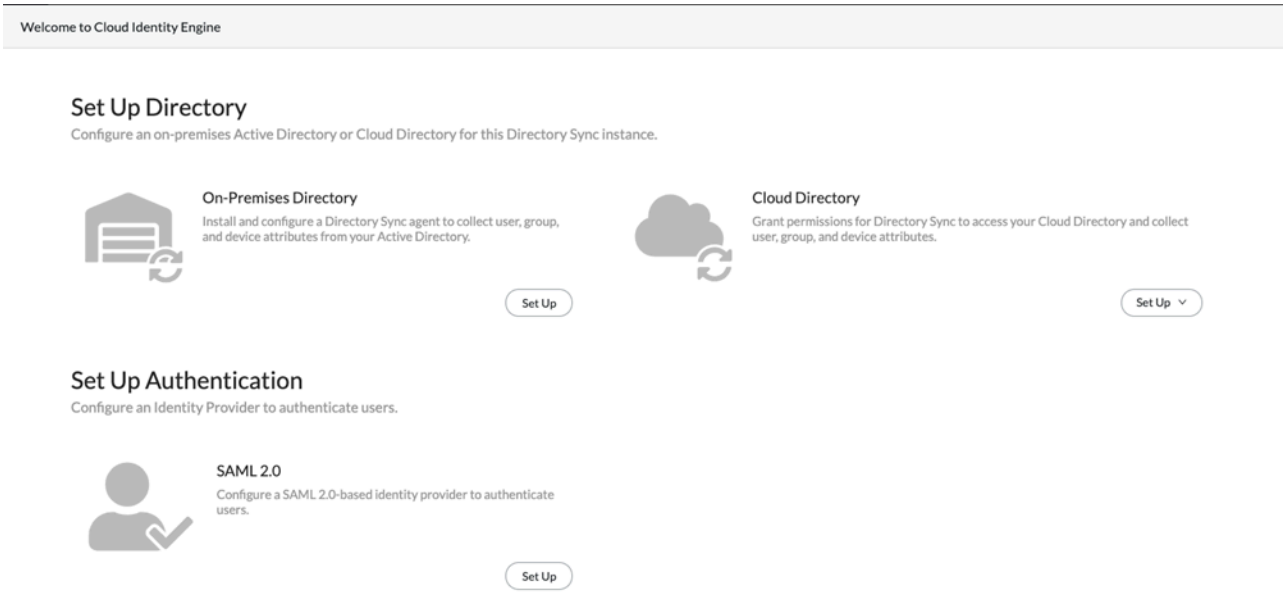
- Assurez-vous que les groupes que vous utilisez avec le Cloud Identity Engine ne contiennent aucun des caractères spéciaux suivants, car Prisma Access ne prend pas en charge l'utilisation de ces caractères spéciaux dans les groupes et les opérations de validation échoueront :
  - " (guillemet double)
  - ' (apostrophe)
  - < (signe inférieur à)
  - > (signe supérieur à)
  - & (esperluette)
- Si vous associez le Cloud Identity Engine à Prisma Access, vos noms d'utilisateur doivent utiliser le format NetBIOS qui inclut le domaine. Vous pouvez spécifier des noms d'utilisateur au format e-mail (*username***@***domain*), au format **`NetBIOS\sAMAccountName`** ou au format nom d'utilisateur principal (UPN) (*username***@***domain*.com).
- Saisissez les noms de groupe au format **distinguishedName** (par exemple, **`CN=Users,CN=Builtin,DC=Example,DC=com`**).
- Le Cloud Identity Engine n'applique aucun paramètre que vous spécifiez dans la liste d'inclusion de groupe (**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres du mappage de groupe)** > **Group Include List (Liste d'inclusion de groupe)**) ; à la place, il récupère les informations sur les utilisateurs et les groupes à partir de l'ensemble de votre configuration, y compris les groupes utilisés dans tous les modèles et groupes d'appareils.

STEP 1 | Créez une instance du Cloud Identity Engine pour Prisma Access et notez le nom de l'instance.

Lorsque vous activez le Cloud Identity Engine, il crée une instance. Vous utiliserez le nom de l'instance lorsque vous associerez le Cloud Identity Engine à Prisma Access dans une prochaine étape. Si vous devez éventuellement créer une instance distincte pour Prisma Access, créez-la et notez son nom.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configurez le Cloud Identity Engine pour qu'il récupère vos données d'annuaire.



STEP 3 | (Déploiements avec Active Directory sur site uniquement) Si vous utilisez un service Active Directory sur site, installez et configurez Cloud Identity Agent pour qu'il communique avec le service AD sur site et configurez l'authentification mutuelle entre le service Cloud Identity Engine et l'agent.

STEP 4 | Activez le Cloud Identity Engine sur Prisma Access

1. Sur le Panorama qui gère Prisma Access, sélectionnez l'onglet des paramètres du mappage nom d'utilisateur-groupe d'utilisateurs.
   - Pour un déploiement Utilisateurs mobiles – GlobalProtect, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—GlobalProtect (Utilisateurs mobiles – GlobalProtect)**, sélectionnez l'icône en forme d'engrenage pour modifier les paramètres, puis choisissez **Group Mapping Settings (Paramètres du mappage de groupe)**.
   - Pour un déploiement Utilisateurs mobiles – Proxy explicite, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—Explicit Proxy (Utilisateurs mobiles – Proxy explicite)**, sélectionnez l'icône en forme d'engrenage pour modifier les paramètres, puis choisissez **Group Mapping Settings (Paramètres du mappage de groupe)**.
   - Pour un déploiement de réseau à distance, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**, sélectionnez l'icône en forme d'engrenage pour modifier les paramètres, puis choisissez **Group Mapping Settings (Paramètres du mappage de groupe)**.
2. Sélectionnez **Enable Directory Sync Integration (Activer l'intégration de la synchronisation d'annuaire)** pour activer le Cloud Identity Engine sur Prisma Access.

 ©2025 Palo Alto Networks, Inc.

3. Saisissez les informations suivantes :
   - Saisissez le **Primary Username (Nom d'utilisateur principal)**. Ce champ est obligatoire.

     L'attribut **Primary Username (Nom d'utilisateur principal)** détermine le format utilisé dans les journaux et les rapports. Si l'attribut du nom d'utilisateur principal est **userPrincipalName** (UPN), toutes les entrées de journal et de rapport affichent l'utilisateur source dans ce format. De nombreux déploiements utilisent un format UPN, **sAMAccountName**ou **mail (e-mail)**. Si votre organisation utilise un autre attribut, vous pouvez le spécifier ici pour garantir la cohérence dans les journaux et les rapports créés au sein de votre organisation.

     Si vous configurez un annuaire Azure AD ou Okta comme fournisseur d'identité (IdP) dans le Cloud Identity Engine, définissez le **Primary Username (Nom d'utilisateur principal)** sur **userPrincipalName**. Prisma Access prend en charge l'attribut userPrincipalName (UPN) utilisé avec les annuaires Azure AD et Okta.
   - (Facultatif) Saisissez l'attribut **E-Mail** (tel que **mail (e-mail)**).
   - (Facultatif) Si vous utilisez d'autres attributs de nom pour l'utilisateur, saisissez-les. Vous pouvez saisir jusqu'à trois autres noms d'utilisateur (**Alternate User Name 1 (Autre nom d'utilisateur 1)**, **Alternate User Name 2 (Autre nom d'utilisateur 2)** et **Alternate User Name 3 (Autre nom d'utilisateur 3)**).
4. Cliquez sur **OK** lorsque vous avez terminé.

STEP 5 | Validez et appliquez (**Commit (Valider)** > **Commit and Push (Valider et appliquer)**) les modifications.

 ©2025 Palo Alto Networks, Inc.

Récupérer les mappages de groupe User-ID pour Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Cloud Identity Engine	• Licence Prisma Access

Après avoir configuré le mappage User-ID dans Prisma Access, vous devez être en mesure de récupérer les informations username-to-user group actuelles pour les utilisateurs mobiles et les utilisateurs sur des réseaux distants. Lors de la configuration le mappage de groupe dans Cloud Identity Engine effectue le mappage username-to-user group, ces groupes d'utilisateurs ne sont pas sélectionnables dans les règles de stratégie de sécurité. Vous pouvez remplir les groupes pour leur permettre d'être sélectionnés dans les listes déroulantes des règles de stratégie de sécurité en configurant un pare-feu de la nouvelle génération en tant que périphérique principal ou en configurant Cloud Identity Engine pour le faire.

- Moteur d'identité sur le cloud
- Périphérique principal
- Entrées de Distinguished Name (nom unique - DN) détaillées

Moteur d'identité sur le cloud

En plus d'utiliser Cloud Identity Engine pour récupérer les informations sur l'utilisateur et le groupe, vous pouvez utiliser Cloud Identity Engine pour renseigner les noms de groupe d'utilisateurs dans les règles de stratégie de sécurité. Cette intégration élimine le besoin de configurer un pare-feu de nouvelle génération sur site ou de la série VM en tant que périphérique principal à cette fin ; cependant, les périphériques principaux sont toujours pris en charge.

Vous pouvez également utiliser Cloud Identity Engine pour renseigner les noms de groupe dans les déploiements à plusieurs locataires gérés par Panorama, ce qui n'est pas possible lors de l'utilisation d'un périphérique principal.

Pour permettre au Cloud Identity Engine de renseigner les noms de groupe dans les règles de stratégie de sécurité, procédez comme suit.

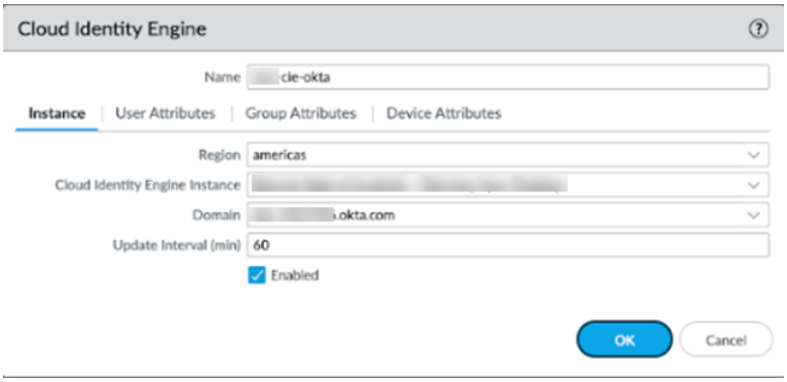
STEP 1 | Dans le Cloud Identity Engine, activez le Cloud Identity Engine et ajoutez un répertoire sur site ou basé sur le cloud, si vous ne l'avez pas déjà fait.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configurez le Cloud Identity Engine en tant que source de mappage.

1. Depuis Panorama qui gère Prisma Access, sélectionnez **Panorama** > **User Identification (Identification de l'utilisateur)** > **Cloud Identity Engine** et **Add (Ajouter)** un profil.
2. Pour l'**Instance**, spécifiez les paramètres suivants :
   - **Region (Région)**—Sélectionnez le point de terminaison régional pour votre locataire.

     La région que vous sélectionnez doit correspondre à la région que vous sélectionnez lorsque vous avez activé votre locataire Cloud Identity Engine.
   - **Cloud Identity Engine Instance (Instance Cloud Identity Engine)**—Sélectionnez l'instance Cloud Identity Engine à associer au profil.
   - **Domain (Domaine)**—Sélectionnez le domaine qui contient les répertoires que vous souhaitez utiliser.
   - **Update Interval (min) (Intervalle de mise à jour (min))**—Entrez le nombre de minutes pendant lesquelles vous souhaitez que Panorama attende entre les mises à jour de l'application Cloud Identity Engine vers Panorama (également appelé intervalle d'actualisation). La valeur par défaut est de 60 minutes et la plage est de 5 à 1440.
3. Vérifiez que le profil est **Enabled (activé)**.

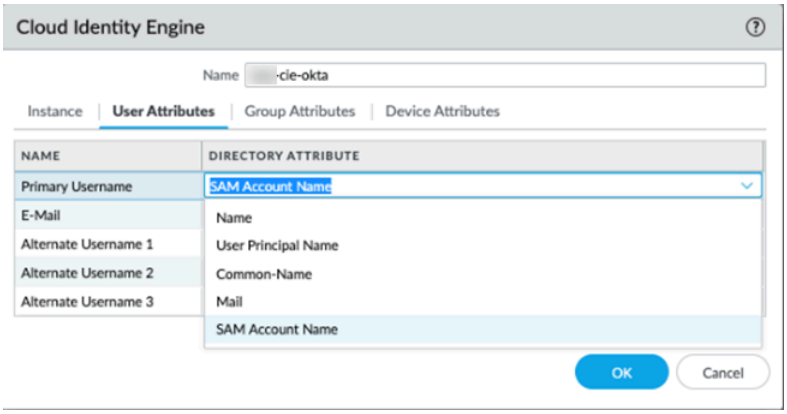


4. Pour les **User Attributes (attributs utilisateur)**, sélectionnez le format du **Primary Username (nom d'utilisateur principal)**. Vous pouvez éventuellement sélectionner les formats d'e-mail et un autre nom d'utilisateur. Vous pouvez configurer jusqu'à trois

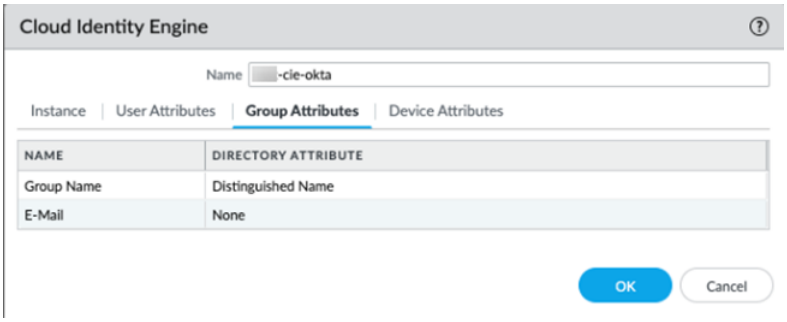
 ©2025 Palo Alto Networks, Inc.

formats de nom d'utilisateur alternatifs si vos utilisateurs se connectent en utilisant plusieurs formats de nom d'utilisateur.

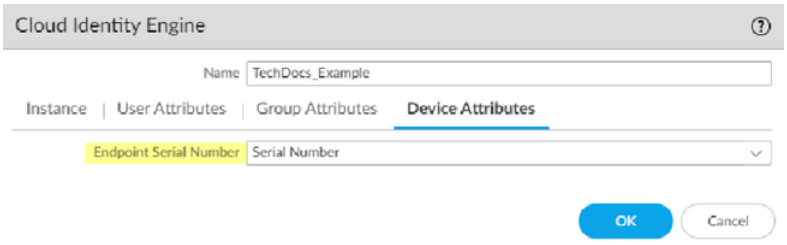
Lorsque vous affichez des utilisateurs dans des règles de stratégie de sécurité, le nom d'utilisateur s'affiche dans le format de nom d'utilisateur principal que vous sélectionnez ici.



5. Pour les **Groupe Attributes (attributs de groupe)**, sélectionnez le format du **Group Name (nom de groupe)**.



6. Laissez les **Device Attributes (Attributs du périphérique)** sur**None (Aucun)**.

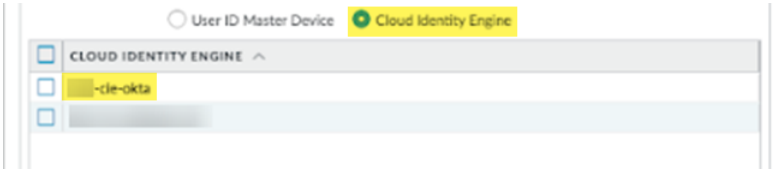


7. Cliquez sur **OK** puis sur **Commit and Push (Valider et appliquer)** vos modifications.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Associez votre profil à votre configuration Prisma Access.

1. Accédez aux paramètres du déploiement que vous ajoutez.
   - Pour un déploiement Utilisateurs mobiles–GlobalProtect, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—GlobalProtect (Utilisateurs mobiles—GlobalProtect)** et cliquez sur l'engrenage pour modifier les **Settings (Paramètres)**.
   - Pour un déploiement Utilisateurs mobiles–Proxy explicite, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users–Explicit Proxy (Utilisateurs mobiles–Proxy explicite)** et cliquez sur l'engrenage pour modifier les **Settings (Paramètres)**.
   - Pour un déploiement Utilisateurs mobiles–Réseaux distants, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobiles Users–Remote Networks (Utilisateurs mobiles–Réseaux distants)** et cliquez sur l'engrenage pour modifier les **Settings (Paramètres)**.
2. Sélectionnez **Cloud Identity Engine**.
3. Sélectionnez le profil Cloud Identity Engine que vous avez créé.



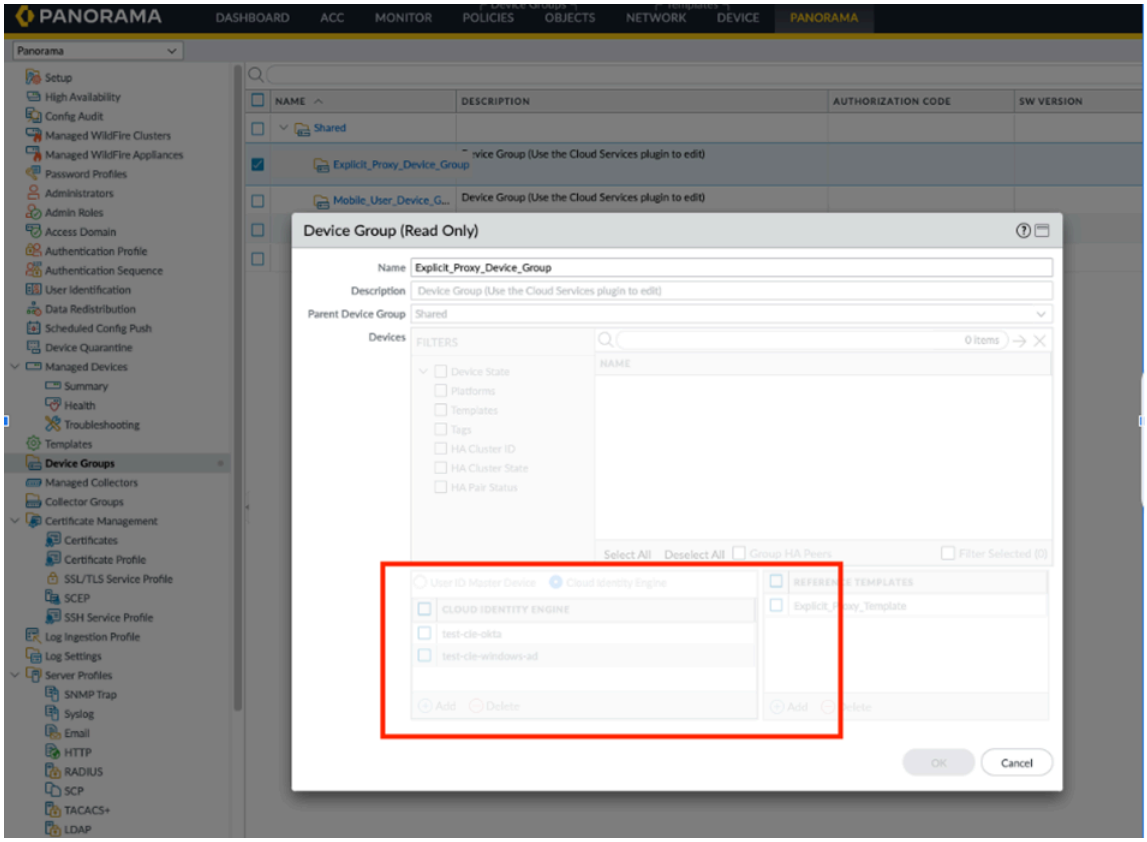
STEP 4 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Vérifiez si Prisma Access dispose des informations de mappage de Cloud Identity Engine.

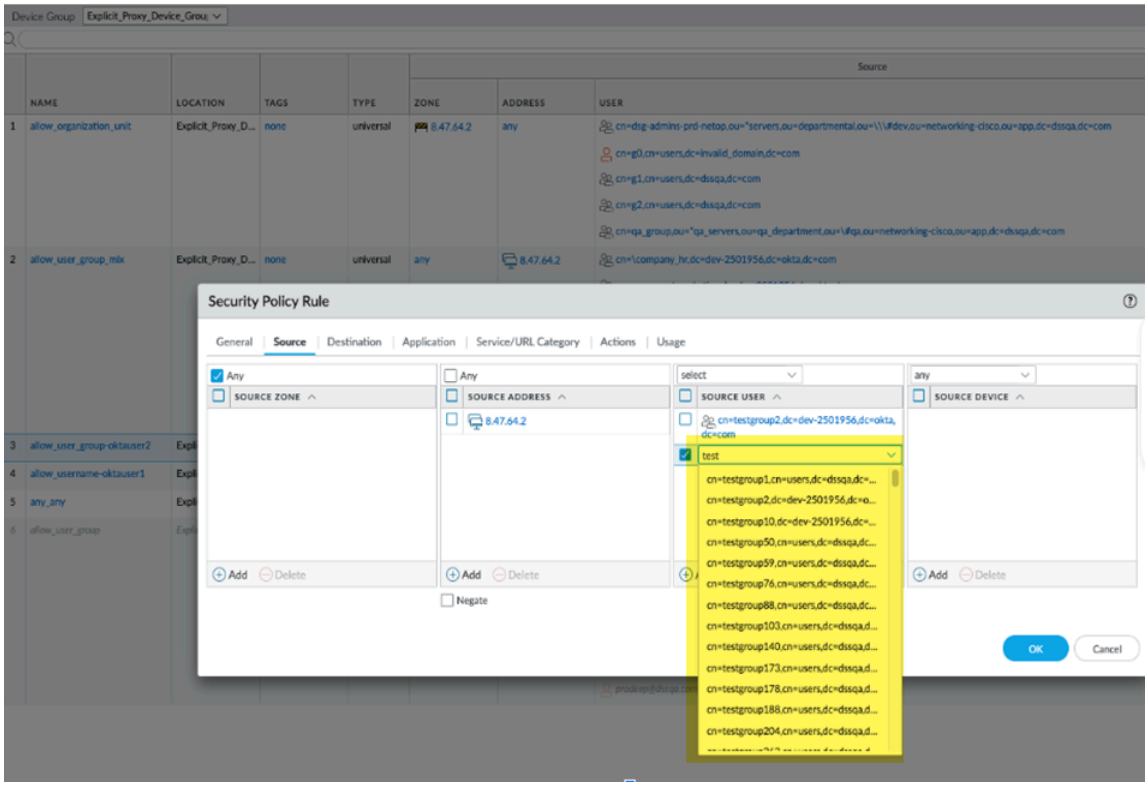
1. Sélectionnez **Panorama** > **Device Groups (Groupes de périphériques)** > ***<template-name>*** où *<template-name>* est le modèle du déploiement que vous configurez, et vérifiez si le profil de Cloud Identity Engine est attaché au groupe de périphériques.

   L'exemple suivant montre que le groupe de périphériques est correctement attaché à Explicit_Proxy_Device_Group.



2. Sélectionnez **Objects (Objets)** > **Security (Sécurité)** > **Pre-Rules (Pré-règles)**, **Add (Ajouter)** une règle de stratégie de sécurité et vérifiez si les groupes sont renseignés dans la zone utilisateur.

 ©2025 Palo Alto Networks, Inc.



Périphérique principal

Lors de la configuration le mappage de groupe dans Cloud Identity Engine effectue le mappage username-to-user group, ces noms d'utilisateur et groupes d'utilisateurs ne sont pas renseignés selon les stratégies de sécurité. Pour simplifier la création ou la modification de stratégies basées sur l'utilisateur et le groupe, vous pouvez utiliser un périphérique principal pour ajouter les noms de groupe aux listes déroulantes dans les règles des stratégies de sécurité. Vous devez désigner un pare-feu comme périphérique principal pour chaque groupe de périphériques. Une fois que vous avez ajouté un périphérique principal, le groupe de périphériques hérite de toutes les stratégies définies sur le périphérique principal ; pour cette raison, il doit s'agir d'un périphérique autonome et dédié à utiliser pour ce groupe de périphériques.

Pour permettre la sélection de noms de groupe dans les listes déroulantes des stratégies de sécurité, Palo Alto Networks vous recommande de désigner un **Master Device (Périphérique principal)** pour chaque groupe de périphériques. Vous pouvez configurer un pare-feu local ou un pare-feu de série VM en tant que périphérique principal.

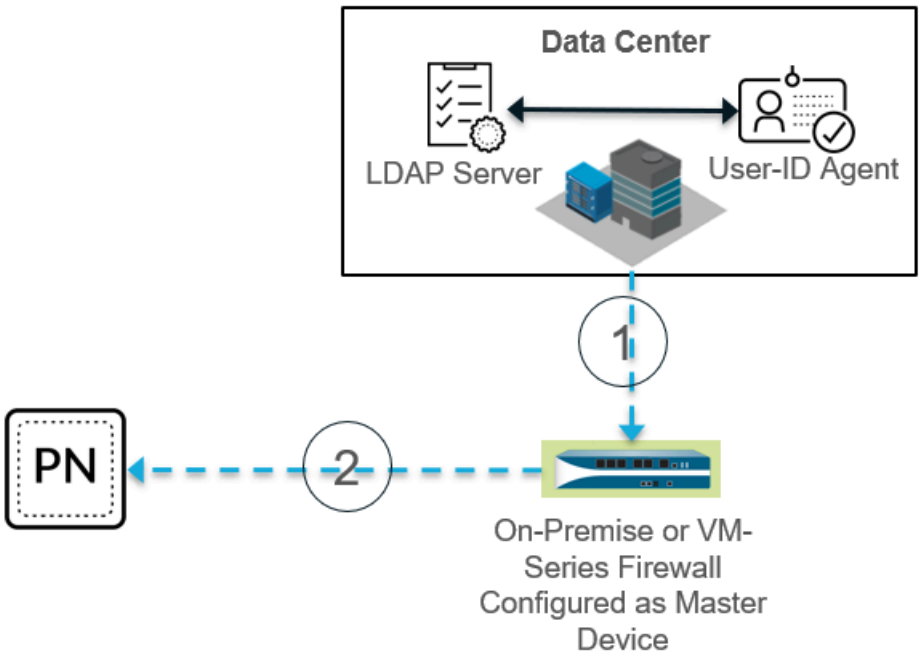
La figure suivante illustre un déploiement User-ID dans lequel l'administrateur a configuré un périphérique local comme **Master Device (Périphérique principal)**. Les légendes de la figure illustrent le processus.

1. Un pare-feu de la nouvelle génération local ou de série VM que l'administrateur a configuré comme périphérique principal récupère le dernier mappage username-to-user group à partir du serveur LDAP et de l'agent User-ID dans le centre de données.

 ©2025 Palo Alto Networks, Inc.

2. Panorama obtient le mappage username-to-user group à partir du périphérique principal.

   Panorama utilise ce mappage uniquement dans le but de remplir les noms de groupe dans les listes déroulantes des stratégies de sécurité, simplifiant ainsi la création de stratégies basées sur les groupes.



Configurer un pare-feu local ou de série VM comme périphérique principal

Utilisez la procédure suivante pour configurer un pare-feu local ou de série VM comme périphérique principal.

Vous ne pouvez utiliser qu'un seul périphérique principal par groupe de périphériques ; si vous devez configurer un périphérique principal pour différents groupes de périphériques, vous devez créer un périphérique principal distinct pour chaque groupe de périphériques.

STEP 1 | Assurez-vous que le périphérique que vous souhaitez utiliser comme périphérique principal est géré par le même Panorama qui gère Prisma Access.

Vous pouvez vérifier vos périphériques gérés sous **Panorama** > **Managed Devices (Périphériques gérés)**.

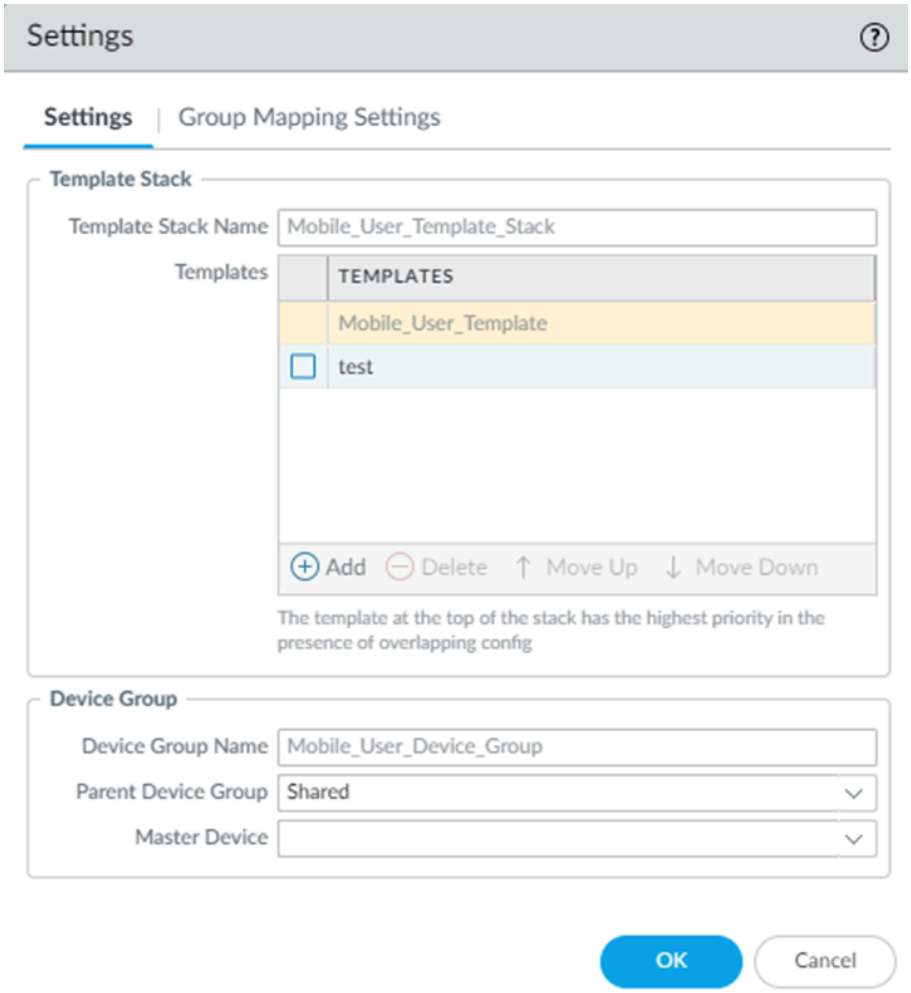
STEP 2 | Ajoutez le périphérique principal à votre Prisma Access déploiement utilisateur mobile ou réseau distant.

- Pour un déploiement Utilisateurs mobiles–GlobalProtect, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—GlobalProtect (Utilisateurs mobiles—GlobalProtect)**, cliquez sur l'icône d'engrenage dans **Settings (Paramètres)** et sélectionnez

 ©2025 Palo Alto Networks, Inc.

le pare-feu local que vous souhaitez spécifier comme**Master Device (Périphérique principal)**.

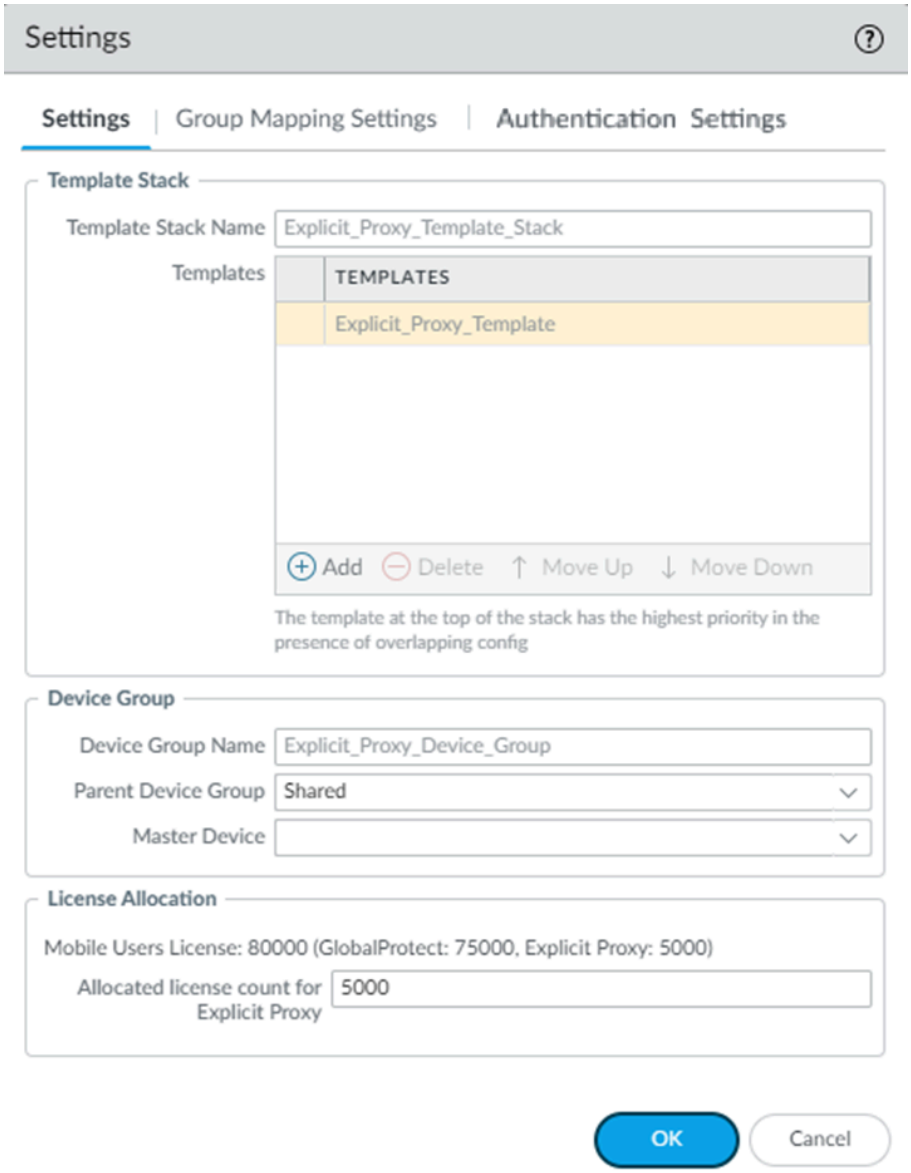
*Si vous utilisez l'option par défaut **Device Group Name (Nom du groupe de périphériques)** (**Mobile_User_Device_Group** dans ce cas) et **Parent Device Group (Groupe de périphériques parent)** (**Shared (Partagé)** dans ce cas), tous les périphériques qui ne sont pas associés à un autre groupe de périphériques s'affichent dans les choix déroulants. Si vous avez associé le périphérique principal à un autre groupe de périphériques, sélectionnez le **Parent Device Group (Groupe de périphériques parent)** associé à ce groupe de périphériques pour qu'il s'affiche dans la liste déroulante.*



- Pour un déploiement Utilisateurs mobiles–Proxy explicite, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users–Explicit Proxy (Utilisateurs mobiles–Proxy**

 ©2025 Palo Alto Networks, Inc.

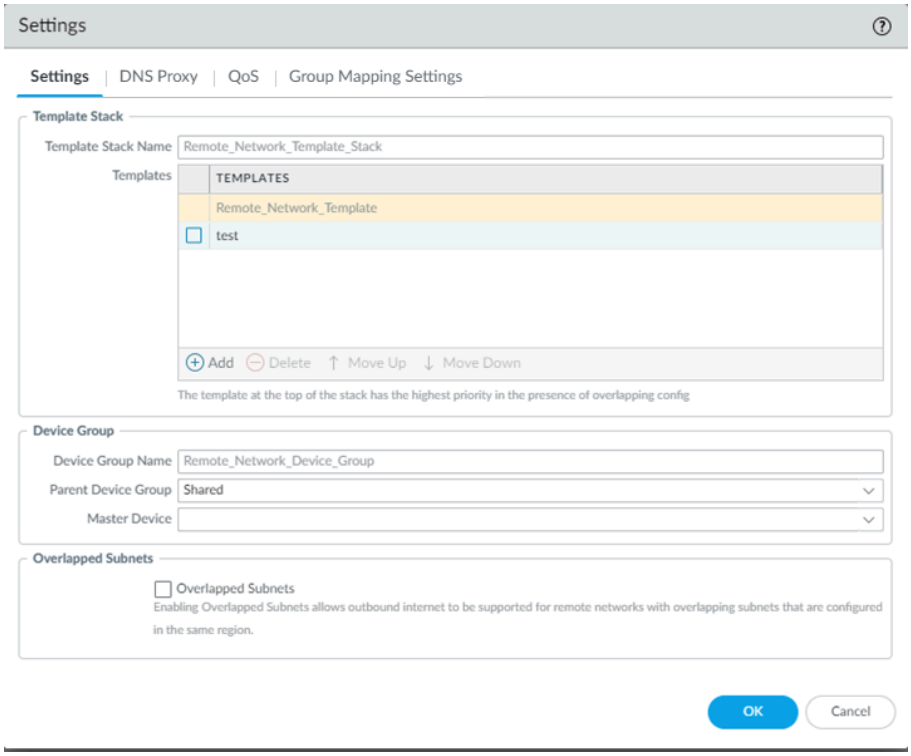
explicite), cliquez sur l'icône d'engrenage dans **Settings (Paramètres)**, puis sélectionnez l'icône **Master Device (Périphérique principal)** que vous avez créée.



- Pour les déploiements de réseau distants, le groupe de périphériques avec une connexion réseau distante, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote**

 ©2025 Palo Alto Networks, Inc.

Networks (Réseaux distants), cliquez sur l'icône d'engrenage dans **Settings (Paramètres)**, puis sélectionnez le **Master Device (Périphérique principal)** que vous avez créé.



*Prisma Access remplit automatiquement le mappage username-to-user group pour le groupe de périphériques associé au périphérique principal uniquement. Pour cet exemple, le remplissage automatique ne se produirait que dans le groupe de périphériques **Remote_Network_Device_Group** et ne serait pas renseigné dans d'autres groupes de périphériques.*

STEP 3 | Cliquez sur **OK**.

Entrées de Distinguished Name (nom unique - DN) détaillées

Si vous n'avez pas configuré de pare-feu nouvelle génération en tant que périphérique principal ou configuré un Cloud Identity Engine pour renseigner les utilisateurs et les groupes dans les règles de politique de sécurité, vous pouvez utiliser des entrées de Distinguished Name (nom unique - DN) détaillées dans Panorama. Prisma Access utilise les entrées DN pour évaluer les politiques basées sur l'User-ID que vous avez configurées dans Panorama.

Par exemple, pour un utilisateur nommé **Bob Alice** qui travaille dans le service informatique et qui se trouve au premier étage, une politique de sécurité correspondante peut contenir `cn=first_floor, ou=it_staff, dc=dev, dc=example, dc=com` si la politique doit être appliquée à tout le personnel informatique du premier étage, ou `cn=Bob Alice, ou=it_staff, dc=dev, dc=example, dc=com` si la politique ne doit s'appliquer qu'à Bob Alice.

 ©2025 Palo Alto Networks, Inc.

Redistribution d'identité

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Pour que vous puissiez appliquer votre politique de sécurité de manière cohérente, Prisma Access partage les données d'identité que GlobalProtect découvre localement sur l'ensemble de votre environnement Prisma Access. Prisma Access peut également partager des données d'identité avec des périphériques sur site sur des sites de réseau distants ou des sites de connexion aux services (siège et centres de données).

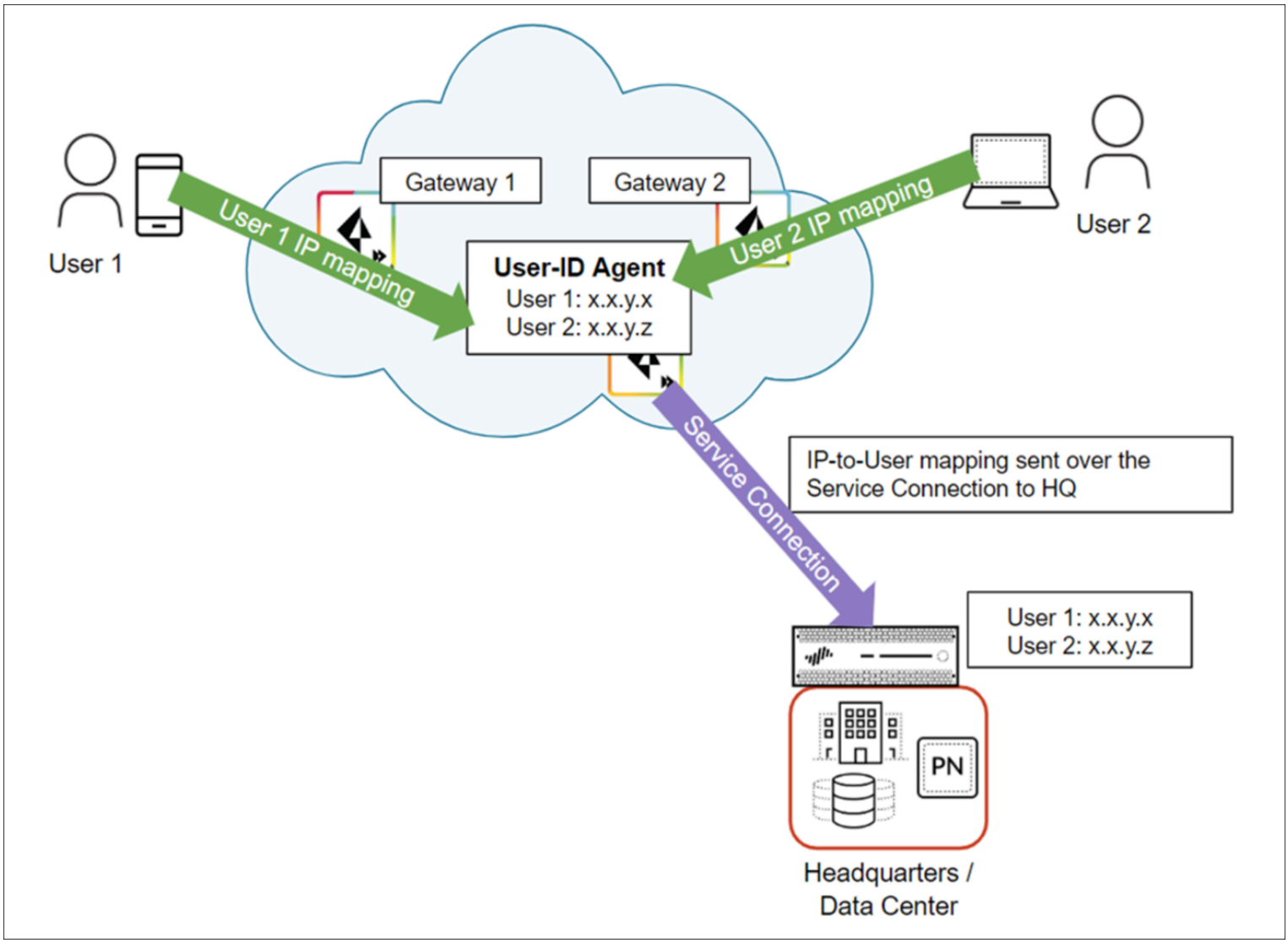
Lorsque les utilisateurs mobiles accèdent à une ressource sur un réseau distant ou au siège/centre de données sécurisé par un périphérique avec des politiques basées sur l'utilisateur, vous devez redistribuer les données d'identité des utilisateurs mobiles Prisma Access et des utilisateurs sur les réseaux distants vers ce périphérique sur site.

Lors de la connexion des utilisateurs à Prisma Access, Prisma Access recueille les données d'identité de l'utilisateur et les stocke.

L'exemple suivant montre deux utilisateurs mobiles qui ont un mappage nom d'utilisateur/adresse IP dans Prisma Access. Prisma Access redistribue ensuite ce mappage par le biais d'une connexion aux services vers les périphériques sur site qui sécurisent le siège/centre de données.

Prisma Access (Managed by Strata Cloud Manager) permet automatiquement aux connexions aux services de fonctionner comme des agents de redistribution d'identité (également appelés agents User-ID).

 ©2025 Palo Alto Networks, Inc.



- Strata Cloud Manager
- Panorama

Redistribution d'identité (Strata Cloud Manager)

Pour que vous puissiez appliquer votre politique de sécurité de manière cohérente, Prisma Access partage les données d'identité que GlobalProtect découvre localement sur l'ensemble de votre Prisma Access environnement. Prisma Access peut également partager des données d'identité avec des périphériques sur site sur des sites de réseau distants ou des sites de connexion aux services (siège et centres de données).

Pour Prisma Access (Managed by Strata Cloud Manager), nous avons activé certaines redistributions de données d'identité par défaut, et pour ce qui reste, nous avons permis à la configuration d'activer la redistribution très simple (sélectionnez simplement une case à cocher pour sélectionner les données que vous souhaitez partager).

Depuis le tableau de bord Identity Distribution (Distribution d'identité), vous pouvez voir comment les données d'identité sont partagées et gérer la redistribution des données (**Manage**

 ©2025 Palo Alto Networks, Inc.

(Gérer) > Configuration > NGFW and Prisma Access (NGFW et Prisma Access) > Identity Services (Services d'identité).

Les données d'identité que vous pouvez redistribuer incluent :

- données HIP
- mappages d'adresses IP vers les étiquettes
- mappages d'utilisateurs vers les adresses IP
- mappages utilisateur vers étiquette
- Périphériques en quarantaine

Commencez à redistribuer les identités :

- Configurer la redistribution d'identité
- Identification et mise en quarantaine des périphériques compromis

Configurer la redistribution d'identité

Configurer la redistribution d'identité

1. Confirmer la configuration de votre connexion aux services

   Si vous n'avez pas encore configuré de connexion de service pour votre siège social ou vos centres de données, vous pouvez commencer par configurer une connexion de service. Une connexion aux services est nécessaire pour que Prisma Access partage les données d'identité sur votre environnement ; Prisma Access active automatiquement les connexions aux services pour qu'elles fonctionnent comme des agents de redistribution. Un site de connexion aux services nouvellement créé est prêt à être utilisé en tant qu'agent de redistribution lorsque vous constatez qu'une adresse d'agent User-ID lui a été attribuée (Prisma Access le fait automatiquement, et cela ne prendra que quelques minutes).

   ***Gestion de la redistribution des User-ID**—Parfois, des contrôles granulaires sont nécessaires pour la redistribution de l'User-ID dans les déploiements Prisma Access à particulièrement grande échelle. La gestion de la redistribution de l'User-ID vous permet de désactiver manuellement le comportement de redistribution d'identité par défaut pour certaines connexions aux services en retirant la coche dans la colonne **User ID (User ID)**, puis sélectionnez les connexions aux services spécifiques à utiliser pour la redistribution de l'identité. Il n'est pas nécessaire de le faire pour la plupart des configurations. Contactez le support de Palo Alto Networks pour activer cette fonctionnalité.*

   Allez à **Manage (Gérer) > Configuration > NGFW and Prisma Access (NGFW et Prisma Access) > Identity Services (Services d'identité) > Identity Redistribution (Redistribution d'identité)** et définissez la portée de la configuration sur **Service Connections (Connexions aux services)** pour vérifier les détails de la connexion aux services Agent User-ID.

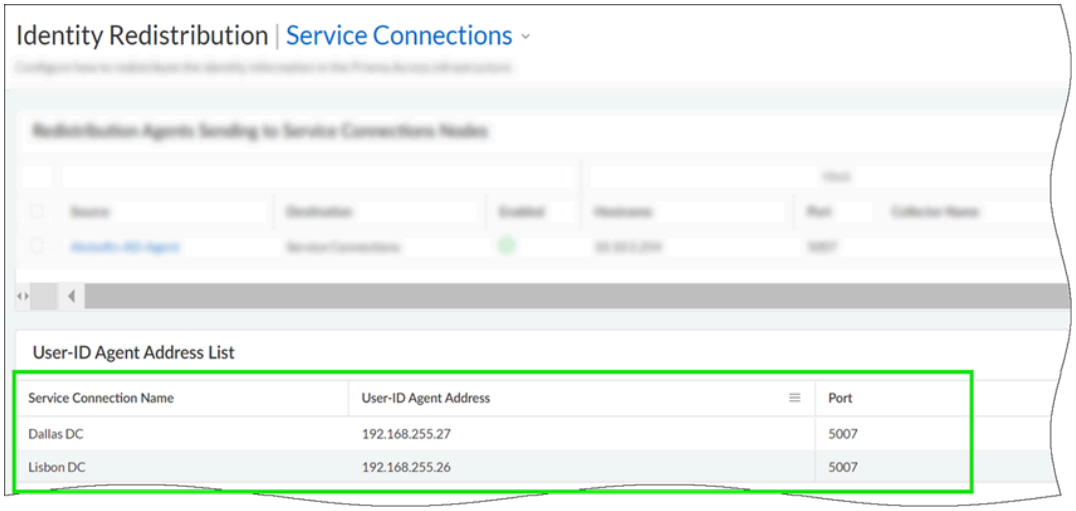
 ©2025 Palo Alto Networks, Inc.

- Envoyez des données d'identité depuis Prisma Access vers Périphériques sur site

  Les informations de l'Agent User-ID de la connexion aux services sont tout ce dont vous avez besoin pour configurer Prisma Access afin de distribuer les données d'identité aux périphériques locaux.

  Allez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Identity Redistribution (Redistribution d'identité)** et définissez la portée de la configuration sur **Service Connections (Connexions aux services)** pour obtenir les détails de la connexion aux services Agent User-ID.

  Utilisez ces détails pour configurer Prisma Access en tant que agent de redistribution de données sur Panorama ou un pare-feu de nouvelle génération de Palo Alto Networks.



- Envoyez des données d'identité à partir des périphériques sur site vers Prisma Access.

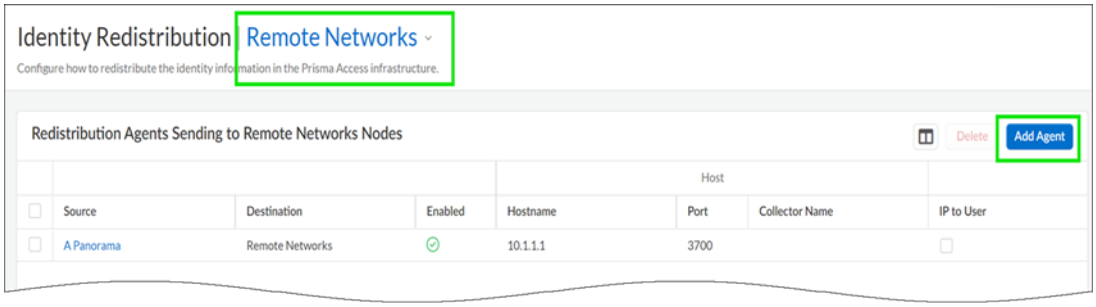
  Ajoutez des périphériques sur site à Prisma Access en tant qu'agents de redistribution ; les périphériques que vous ajoutez pourront distribuer des données d'identité à Prisma Access.

  - **À partir des périphériques situés sur des sites réseau distants :**

    Accédez au tableau de bord **Identity Redistribution (Redistribution des identités)**, définissez la porté de la configuration sur des **Remote Networks (Réseaux distants)** et **Add Agent (Ajouter un agent)**. En plus de spécifier les détails de l'hôte, sélectionnez le type de données

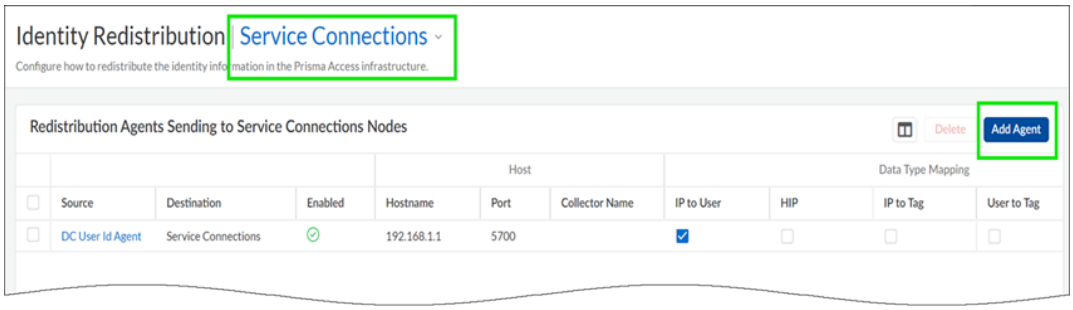
 ©2025 Palo Alto Networks, Inc.

que le périphérique partage avec Prisma Access. Les paramètres facultatifs incluent le nom et une clé pré-partagée pour le périphérique.



- **À partir des périphériques situés sur les sites de raccordement au service :**

  Accédez au tableau de bord de **Identity Redistribution (Redistribution d'identité)**, définissez la portée de la configuration sur **Service Connections (Connexions de service)** et **Add Agent (Ajouter un agent)**. En plus de spécifier les détails de l'hôte, sélectionnez le type de données que le périphérique partage avec Prisma Access. Les paramètres facultatifs incluent le nom et une clé pré-partagée pour le périphérique.



- Configurer l'agent Terminal Server pour le mappage d'utilisateurs.

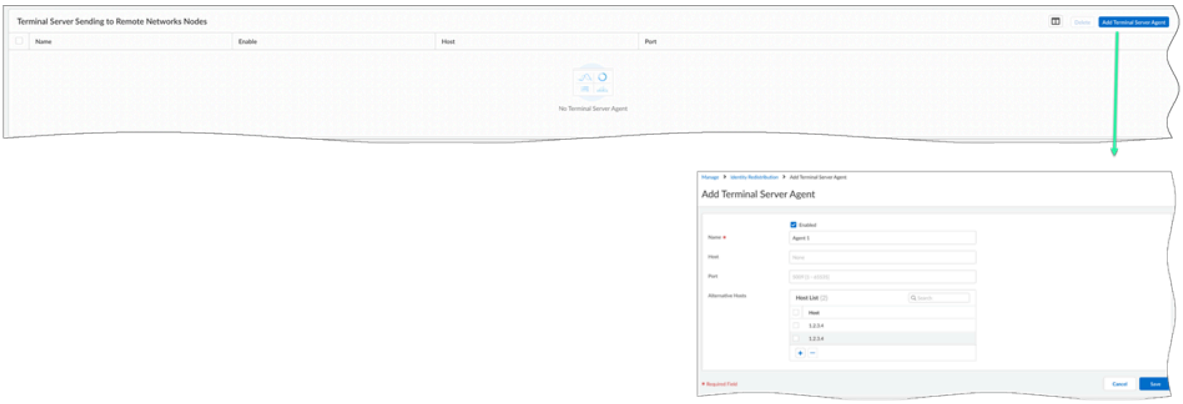
  L'agent Terminal Server (TS) alloue une plage de ports à chaque utilisateur pour identifier des utilisateurs spécifiques sur les serveurs de terminaux Windows. L'agent TS informe Prisma Access des plages de ports allouées, afin que Prisma Access puisse appliquer la politique en fonction des utilisateurs et des groupes d'utilisateurs.

  Dans le tableau de bord **Identity Redistribution (Redistribution d'identité)**, définissez la portée de la configuration sur **Remote Networks (Réseaux distants)**et **Ajoutez l'agent Terminal Server**

 ©2025 Palo Alto Networks, Inc.

(Add Terminal Server Agent) sous **Terminal Server Sending to Remote Networks Nodes (Envoi du serveur Terminal Server aux nœuds de réseaux distants)**.

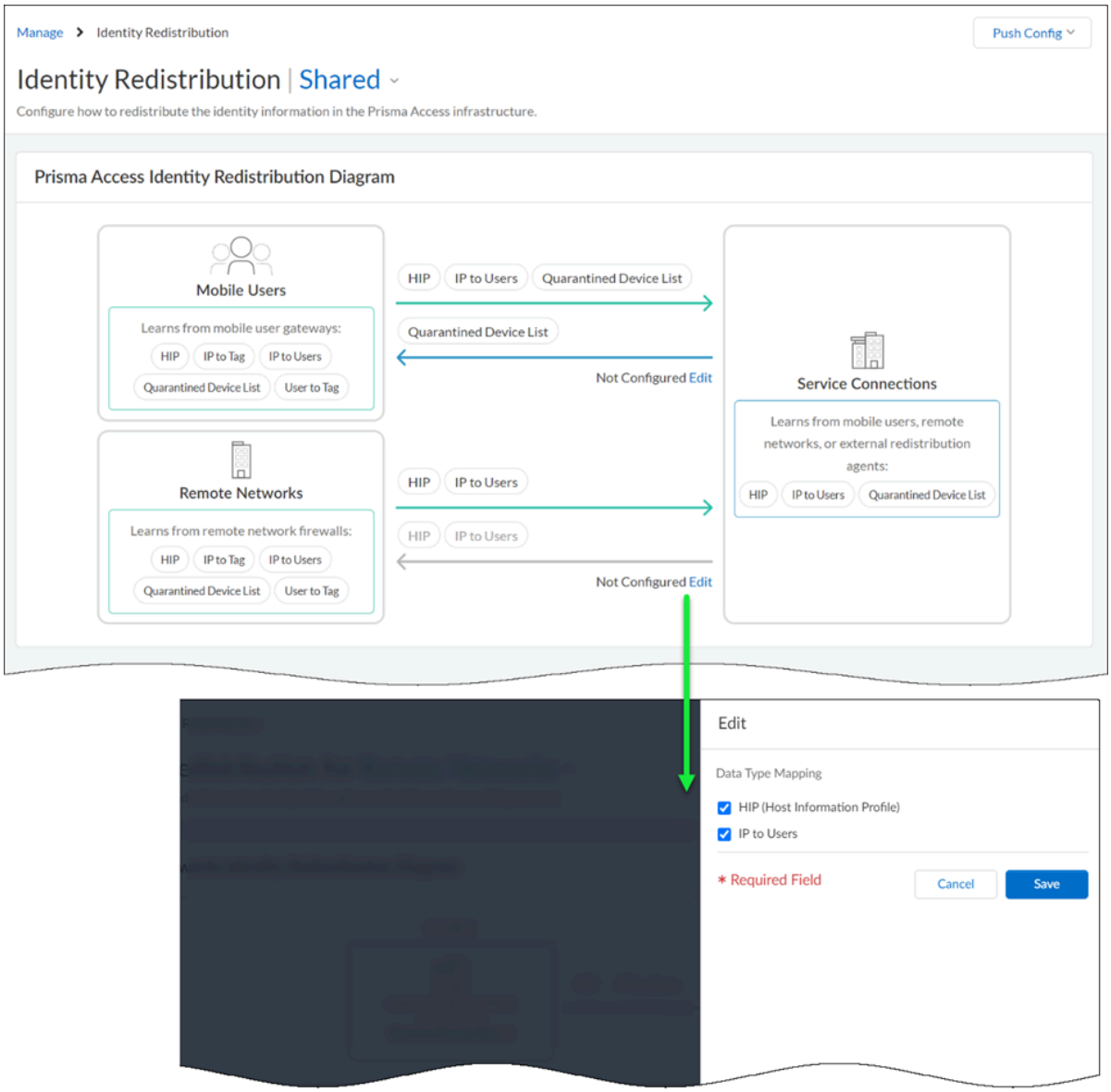
- Par défaut, la configuration est **Enabled (Activée)**.
- Entrez un **Name (nom)** pour l'agent TS.
- Saisissez l'adresse IP du **Host (Hôte)** Windows sur lequel l'agent TS est installé.
- Saisissez le numéro de **Port (Port)** sur lequel l'agent écoutera les requêtes de mappage d'utilisateur. Le port est défini sur 5009 par défaut.
- Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.



 ©2025 Palo Alto Networks, Inc.

- Distribuez les données d'identité dans votre environnement Prisma Access.

  Dans le tableau de bord **Identity Redistribution (Redistribution d'identité)**, **Edit (Modifier)** le diagramme pour spécifier les données d'identité que vous souhaitez collecter à partir de chaque source et partager sur Prisma Access.



- Pour activer vos modifications, envoyez la configuration à Prisma Access.

Redistribution d'identité (Panorama)

Après avoir configuré l'ID utilisateur, vous appliquez systématiquement la stratégie basée sur l'utilisateur pour tous les utilisateurs mobiles et les utilisateurs situés sur des sites réseau distants en redistribuant l'IP address-to-username mapping à partir de Prisma Access à tous les pare-feu de la nouvelle génération qui sécurisent l'accès aux ressources du réseau. Utilisez l'une des méthodes suivantes pour redistribuer l'IP address-to-username mapping aux utilisateurs mobiles

 ©2025 Palo Alto Networks, Inc.

et aux utilisateurs des réseaux distants à partir d'un pare-feu de nouvelle génération sur site et vice versa :

- Redistribuer les informations d'identification de l'utilisateur de Prisma Access vers un pare-feu local
- Redistribuer les informations d'identification de l'utilisateur d'un pare-feu local vers Prisma Access

Redistribuer les informations d'identification de l'utilisateur à partir de Prisma Access vers un pare-feu sur site

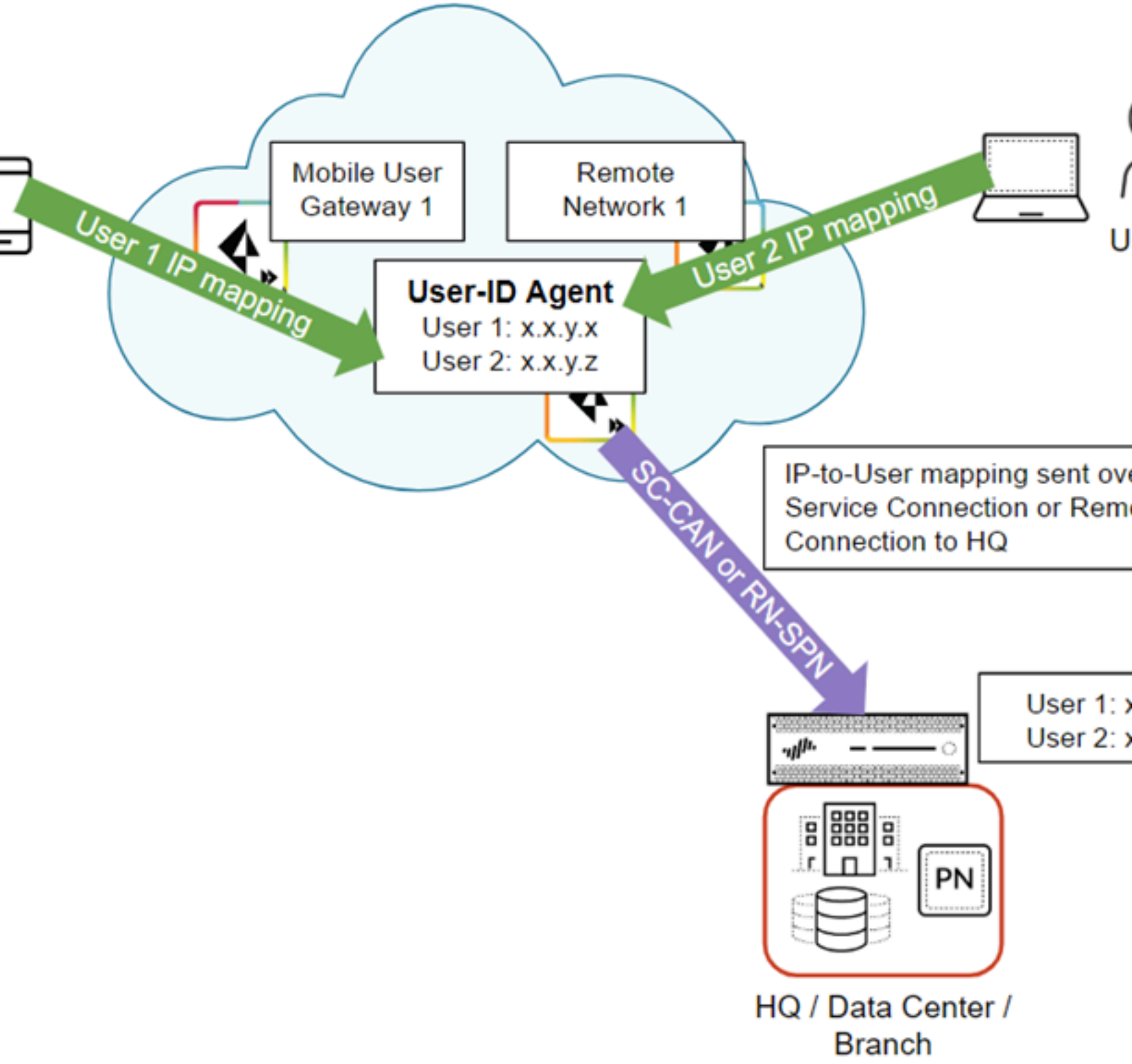
Redistribuer les informations d'identification de l'utilisateur à partir de Prisma Access vers un pare-feu sur site.

Dans les cas où les utilisateurs mobiles doivent accéder à une ressource sur un emplacement réseau distant ou au siège social/centre de données et que la ressource est sécurisée par un pare-feu de la nouvelle génération sur site avec des stratégies basées sur l'utilisateur, vous devez redistribuer l'IP address-to-username mapping à partir des Prisma Access utilisateurs mobiles et des utilisateurs de réseaux distants vers le pare-feu sur site. Lorsque l'utilisateur se connecte à Prisma Access, il collecte ce user-to-IP address mapping et le stocke.

La figure suivante montre deux utilisateurs mobiles qui ont un IP address-to-username mapping dans Prisma Access. Prisma Access redistribue ensuite ce mappage via une connexion aux services (SC-CAN) ou une connexion réseau distant (RN-SPN) au pare-feu local qui sécurise le siège social/centre de données.

Prisma Access utilise la connexion aux services ou la connexion réseau distante comme tunnel IPSec qui sert de chemin sous-jacent au réseau de couche 3. Vous pouvez utiliser n'importe quel chemin d'itinéraire sur un tunnel IPSec approuvé pour les destinations adressées de manière privée afin de redistribuer ce mappage.

 ©2025 Palo Alto Networks, Inc.



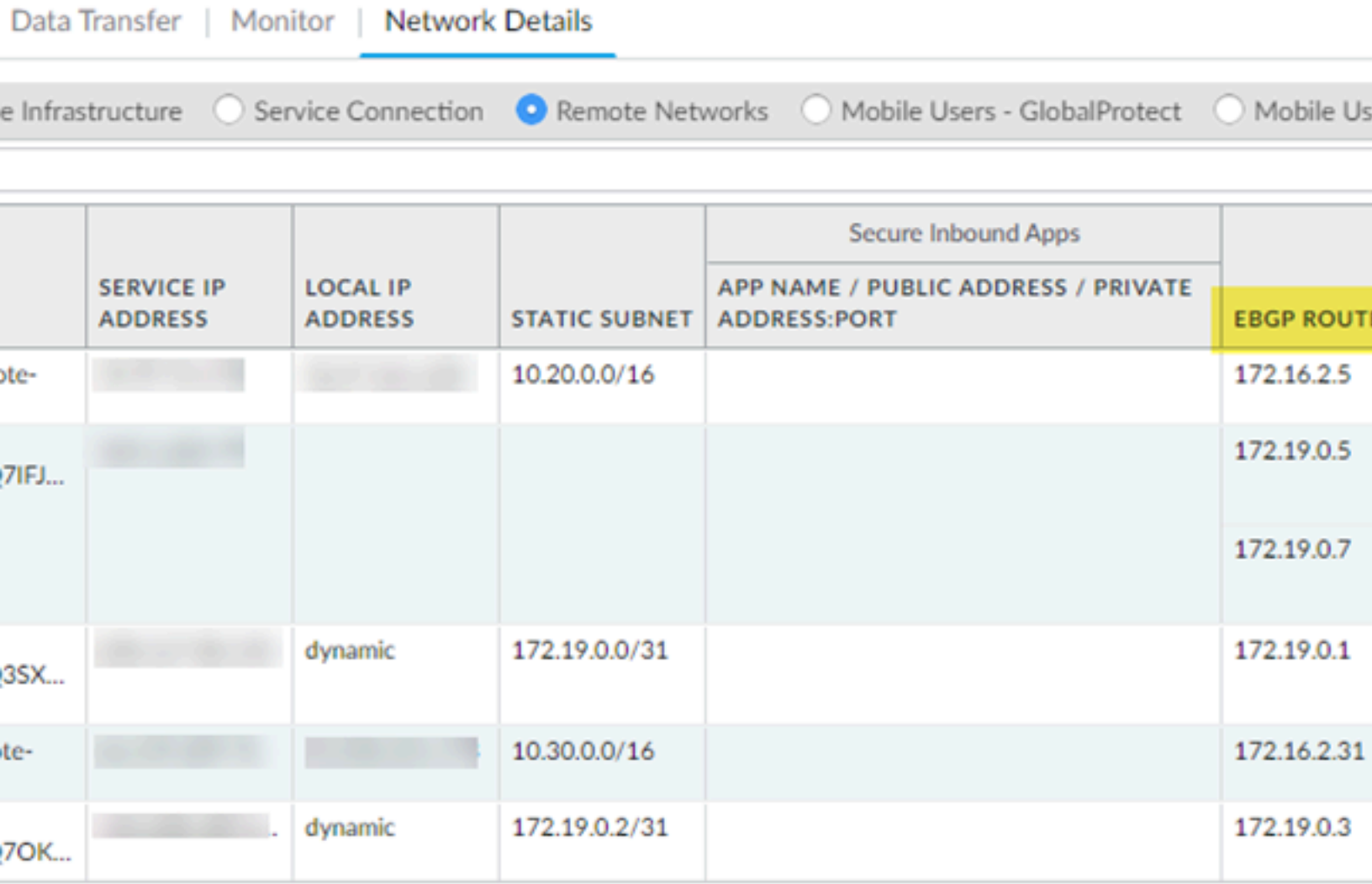
Pour redistribuer les mappages d'ID utilisateur à partir de Prisma Access vers un pare-feu sur site, procédez comme suit.

 ©2025 Palo Alto Networks, Inc.

Assurez-vous de n'appliquer aucun décryptage SSL sur aucune connexion qui redistribue l'identité de l'utilisateur au pare-feu local (SC-CAN ou RN-SPN), y compris tous les pare-feu qui se trouvent dans le chemin de redistribution. Vous pouvez également appliquer une exclusion de décryptage *au trafic de redistribution.*

STEP 1 | Notez l'adresse IP à utiliser lorsque vous configurez l'agent de redistribution des données.

- Pour les connexions réseau à distance, recherchez l'adresse **EBGP Router (Routeur EBGP)** (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails réseau)** > **Remote Networks (Réseaux distants)** > **EBGP Router (Routeur EBGP)**).



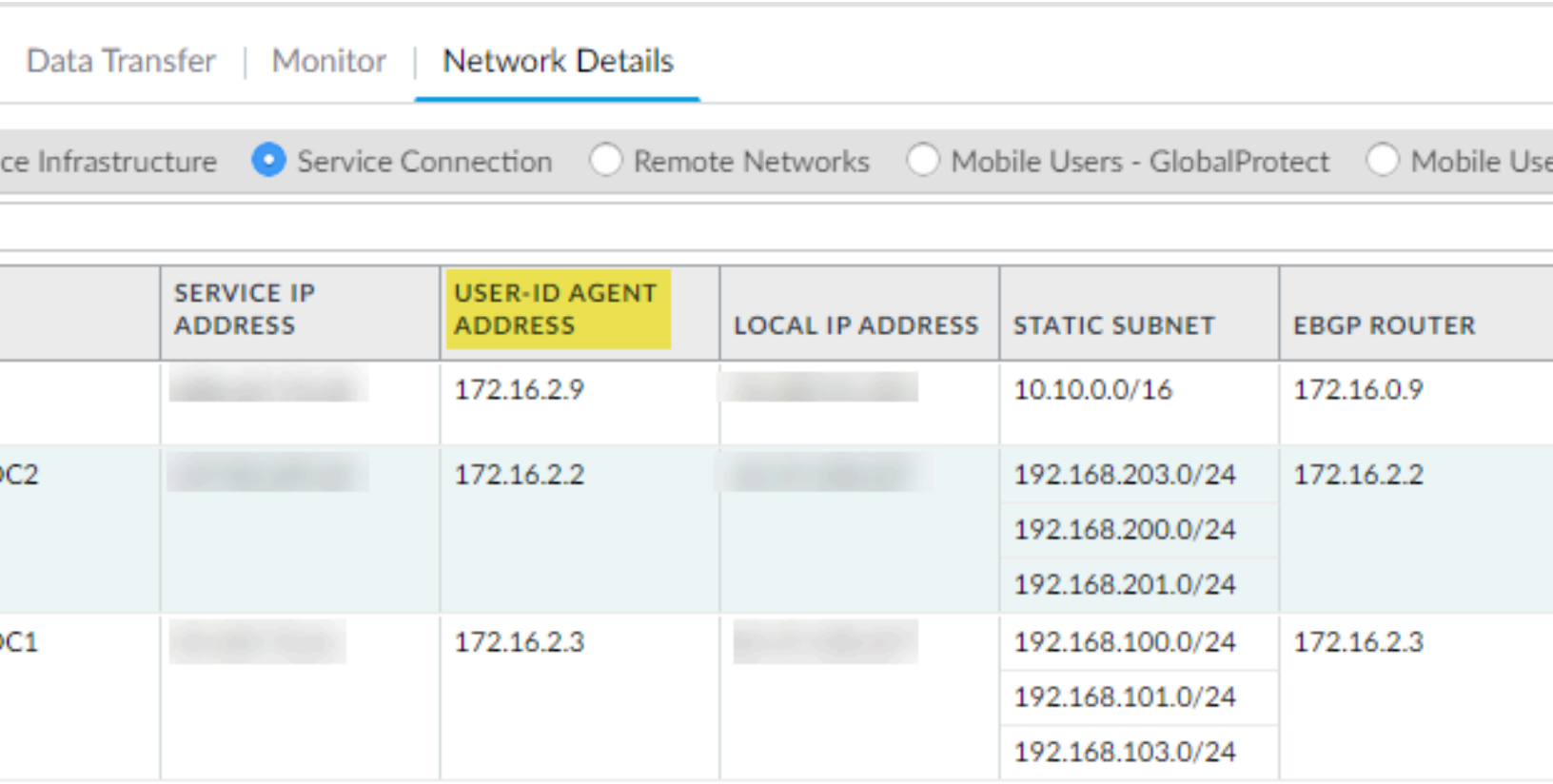
- Pour les connexions aux services, recherchez **User-ID Agent Address (Adresse de l'agent User-ID)** (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **User-ID Agent Address (Adresse de l'agent User-ID)**).

  Si vous n'avez pas encore configuré de connexion aux services pour votre siège social ou vos centres de données, commencez par configurer une connexion aux services. Prisma Access utilise des connexions aux services pour partager des données d'identité dans votre environnement ; Prisma Access permet automatiquement aux connexions

 ©2025 Palo Alto Networks, Inc.

aux services de fonctionner comme agents de redistribution. Le site de connexion aux services nouvellement créé sera prêt à être utilisé comme agent de redistribution lorsque vous verrez qu'une adresse d'agent User-ID lui a été attribuée (Prisma Access le fait automatiquement, et cela ne prendra que quelques minutes).

Gestion de la redistribution de User-ID— *Parfois, des contrôles précis sont nécessaires pour la redistribution des User-ID dans les déploiements Prisma Access à particulièrement grande échelle. La gestion de la redistribution de l'User-ID vous permet de désactiver manuellement le comportement de redistribution d'identité par défaut pour certaines connexions aux services en retirant la coche dans la colonne **User ID (User ID)**, puis sélectionnez les connexions aux services spécifiques à utiliser pour la redistribution de l'identité. Il n'est pas nécessaire de le faire pour la plupart des configurations. Contactez le support de Palo Alto Networks pour activer cette fonctionnalité.*

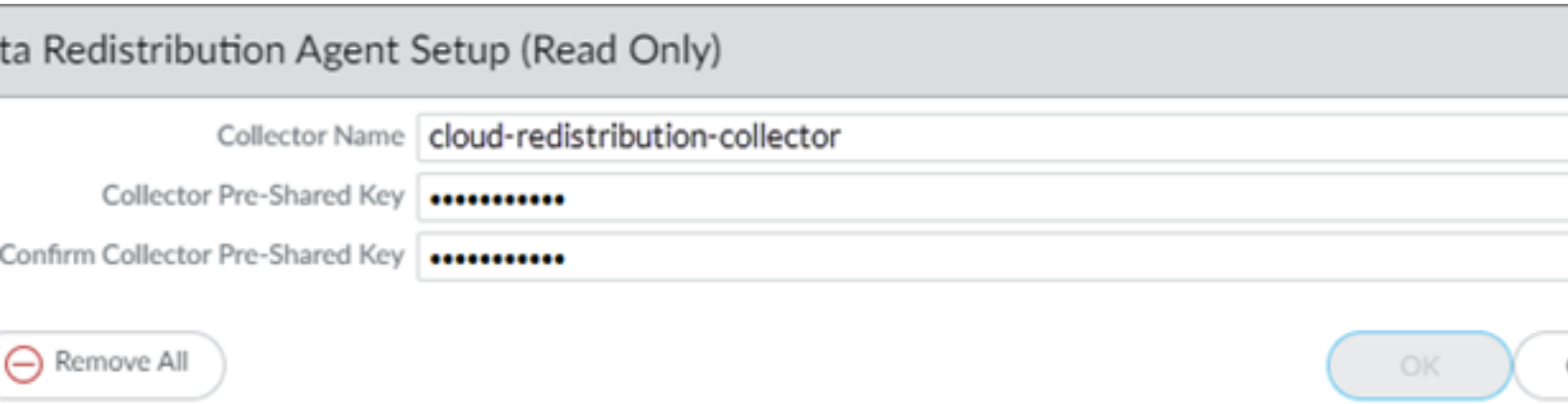


 ©2025 Palo Alto Networks, Inc.

STEP 2 | Configurez Prisma Access en tant qu'agent User-ID qui redistribue les informations de mappage des utilisateurs.

1. Dans le Panorama qui gère Prisma Access, sélectionnez **Device (Périphérique)** > **Data Redistribution (Redistribution des données)** > **Collector Settings (Paramètres du collecteur)**.

   Pour configurer le collecteur sur une connexion aux services, sélectionnez **Service_Conn_Template** ; pour configurer le collecteur sur une connexion réseau distante, sélectionnez **Remote_Network_Template.**
2. Cliquez sur l'engrenage pour modifier les paramètres.
3. Fournissez un **Collector Name (Nom de collecteur)** et une **Collector Pre-Shared Key (Clé pré-partagée de collecteur)** pour identifier Prisma Access en tant qu'agent User-ID.
4. Cliquez sur **OK** pour enregistrer vos modifications.

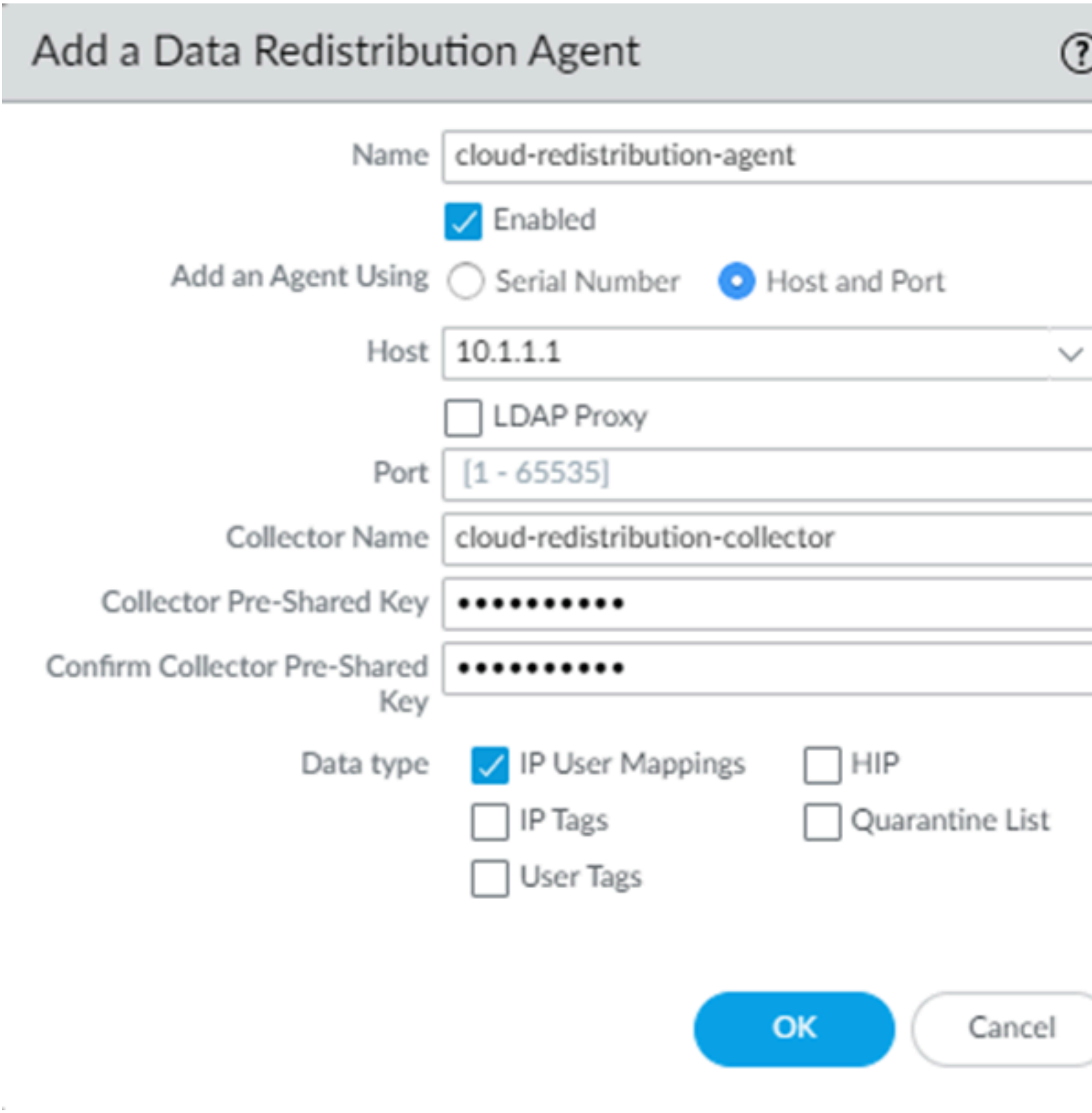


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configurez le pare-feu sur site pour collecter le mappage d'ID utilisateur à partir de Prisma Access.

1. À partir du pare-feu local, sélectionnez **Device (Périphérique)** > **Data Redistribution (Redistribution de données)** > **Agents (Agents)**.
2. **Add (Ajouter)** un agent User-ID et donnez-lui un **Name (Nom)**.
3. Sélectionnez **Host and Port (Hôte et port)**.
4. Saisissez **User-ID Agent Address (Adresse de l'agent User-ID)** (pour une connexion aux services) ou **EBGP Router Address (Adresse du routeur EBGP)** (pour une connexion réseau distante) à partir de Prisma Access dans le champ **Host (Hôte)**.
5. Saisissez le **Collector Name (Nom du collecteur)** et la **Collector Pre-Shared Key (Clé pré-partagée du collecteur)** pour le collecteur Prisma Access que vous avez créé plus tôt dans la procédure.
6. Sélectionnez **IP User Mappings (Mappages d'utilisateur IP)**.
7. Cliquez sur **OK**.
8. Répétez ces étapes pour chaque connexion aux services ou connexion réseau distante pour laquelle vous souhaitez redistribuer les mappages.

 ©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

Redistribuer les informations d'identification de l'utilisateur d'un pare-feu local vers Prisma Access

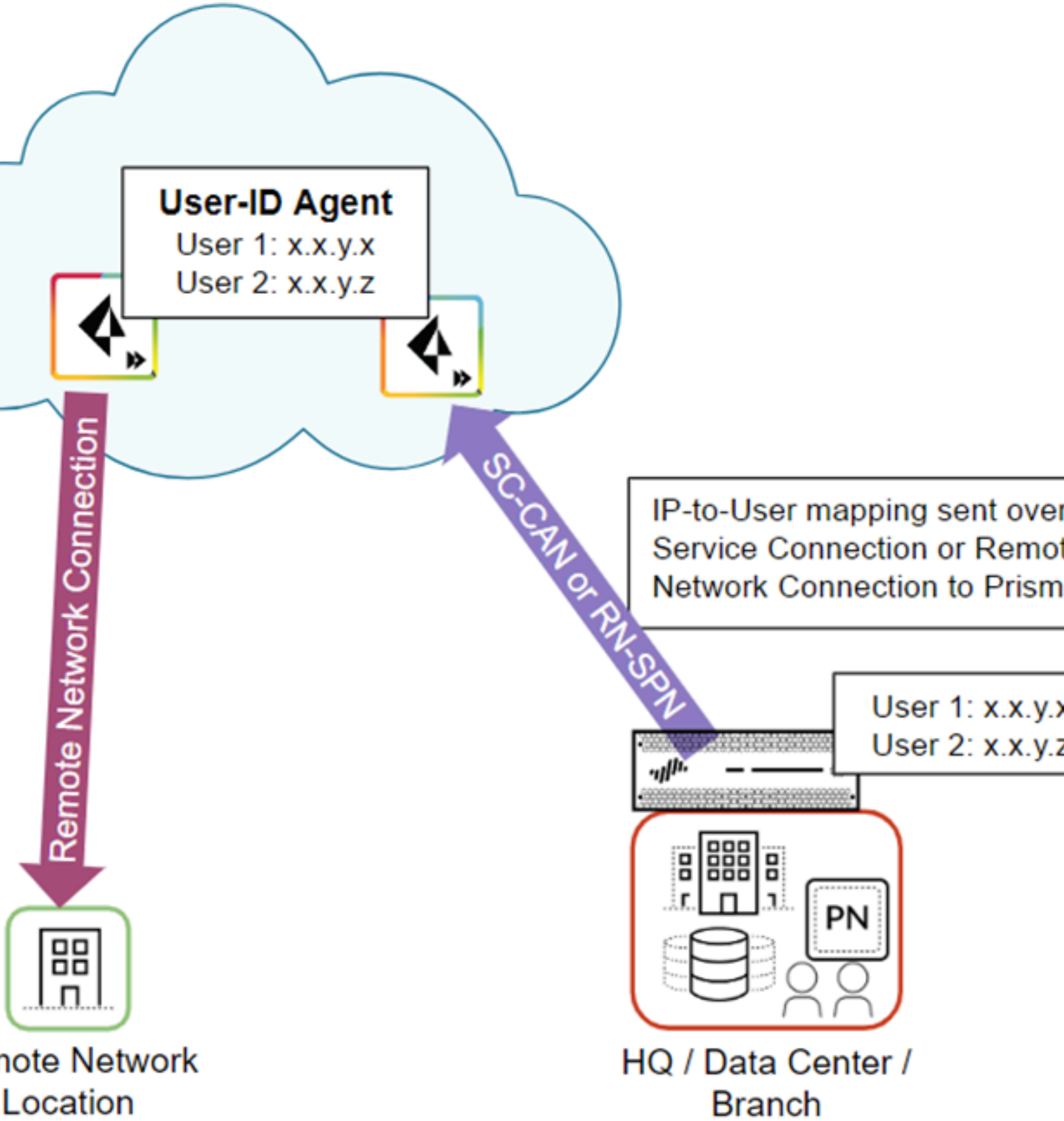
Redistribuer les informations d'identification de l'utilisateur d'un pare-feu local vers Prisma Access.

Dans les cas où les utilisateurs se trouvent dans une succursale ou un siège social sécurisé par un pare-feu de la nouvelle génération sur site avec des stratégies basées sur les utilisateurs, et qu'ils doivent accéder aux ressources d'une autre succursale que vous avez sécurisée avec Prisma Access, vous devez redistribuer les IP address-to-user name mappings du pare-feu local vers Prisma Access.

La figure suivante montre un siège social/centre de données avec un pare-feu de la nouvelle génération sur site avec IP address-to-username mapping existant. Prisma Access se connecte au pare-feu avec une connexion aux services (SC-CAN) ou une connexion réseau distante (RN-SPN), et le pare-feu local redistribue le mappage vers Prisma Access.

La figure suivante montre une Prisma Access connexion aux services ou une connexion réseau distante utilisée pour redistribuer le mappage. Vous pouvez utiliser n'importe quel chemin d'itinéraire sur un tunnel IPSec approuvé pour les destinations adressées de manière privée afin de redistribuer ce mappage.

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

Pour redistribuer les mappages d'ID utilisateur d'un pare-feu local vers Prisma Access, procédez comme suit.

STEP 1 | Configurez le pare-feu sur site pour qu'il redistribue les informations d'ID utilisateur à Prisma Access.

1. À partir du pare-feu local, sélectionnez **Device (Périphérique)** > **Data Redistribution (Redistribution des données)** > **Collector Settings (Paramètres du collecteur)**.
2. Cliquez sur l'engrenage pour modifier les paramètres.
3. Fournissez un **Collector Name (Nom de collecteur)** et une **Collector Pre-Shared Key (Clé pré-partagée de collecteur)** pour identifier le pare-feu local en tant qu'agent User-ID.
4. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 2 | Configurez Prisma Access pour collecter le mappage d'ID utilisateur à partir du pare-feu local.

1. Dans le Panorama qui gère Prisma Access, sélectionnez **Device (Périphérique)** > **Data Redistribution (Redistribution des données)** > **Agents (Agents)**.

   Assurez-vous d'avoir sélectionné le **Service_Conn_Template** (pour les connexions aux services) ou le **Remote_Network_Template** (pour les connexions réseau à distance) dans la liste déroulante **Templates (Modèles)** en haut de la page.
2. **Add (Ajouter)** un agent User-ID et donnez-lui un **Name (Nom)**.
3. Sélectionnez **Host and Port (Hôte et port)**.
4. Saisissez l'adresse IP de l'interface MGT ou de la route de service que le pare-feu utilise pour envoyer les mappages utilisateur dans le champ **Host (Hôte)**.

   Pour l'interface MGT, vous pouvez saisir un nom d'hôte au lieu de l'adresse IP.
5. Saisissez le **Collector Name (Nom du collecteur)** et **Collector Pre-Shared Key (Clé pré-partagée du collecteur)**, en utilisant les valeurs du collecteur que vous avez utilisé pour le pare-feu local à l'étape 1.
6. Sélectionnez **IP User Mappings (Mappages d'utilisateur IP)**.
7. Cliquez sur **OK**.

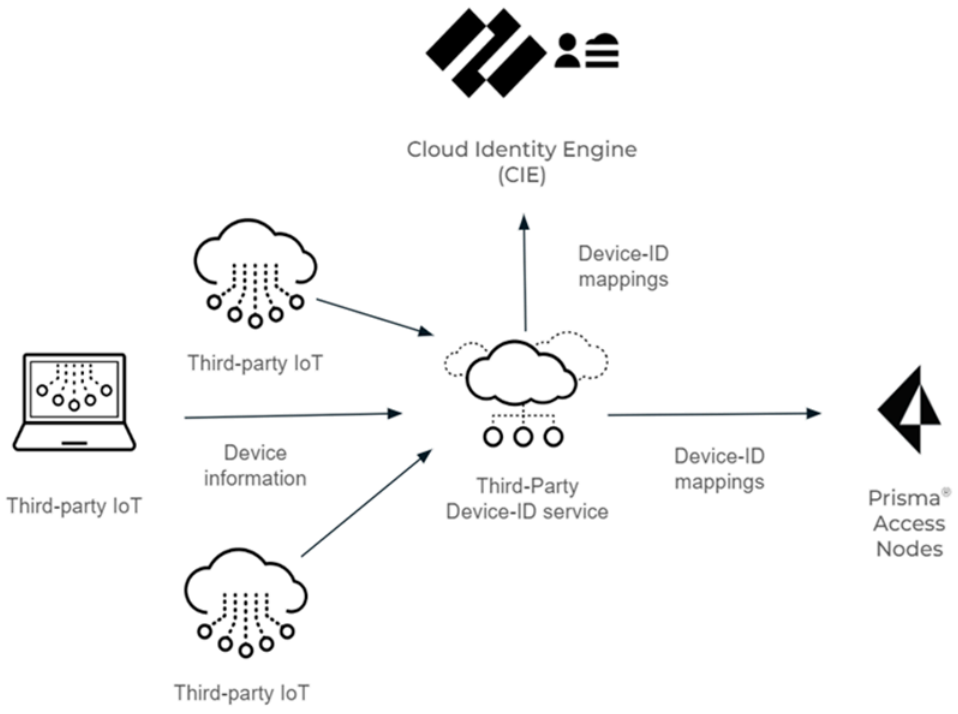
 ©2025 Palo Alto Networks, Inc.

Configurer Third-Party Device-ID dans Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) Si vous souhaitez utiliser cette fonctionnalité dans votre Prisma Access environnement, contactez votre équipe de compte pour en savoir plus.	❑ Licence Prisma Access avec la fonctionnalité Cloud Identity Engine activée

Vous pouvez utiliser Cloud Identity Engine avec Prisma Access pour appliquer des informations provenant de sources de détection IoT tierces afin de simplifier l'identification et la correction des failles de sécurité pour les périphériques de votre réseau. Après avoir configuré Third-Party Device-ID dans Cloud Identity Engine à l'aide d'une API, vous pouvez configurer un objet de périphérique et une règle de politique de sécurité dans Prisma Access pour obtenir et utiliser des informations provenant de solutions de visibilité IoT tierces via Cloud Identity Engine pour la visibilité et le contrôle des périphériques.

Dans la figure suivante, le service Third-Party Device-ID reçoit les informations sur le périphérique des solutions IoT tierces, qu'il transmet ensuite sous forme de mappages d'adresse IP à périphérique à Cloud Identity Engine et aux nœuds de traitement de sécurité (SPN) Prisma Access.



 ©2025 Palo Alto Networks, Inc.

- Strata Cloud Manager
- Panorama

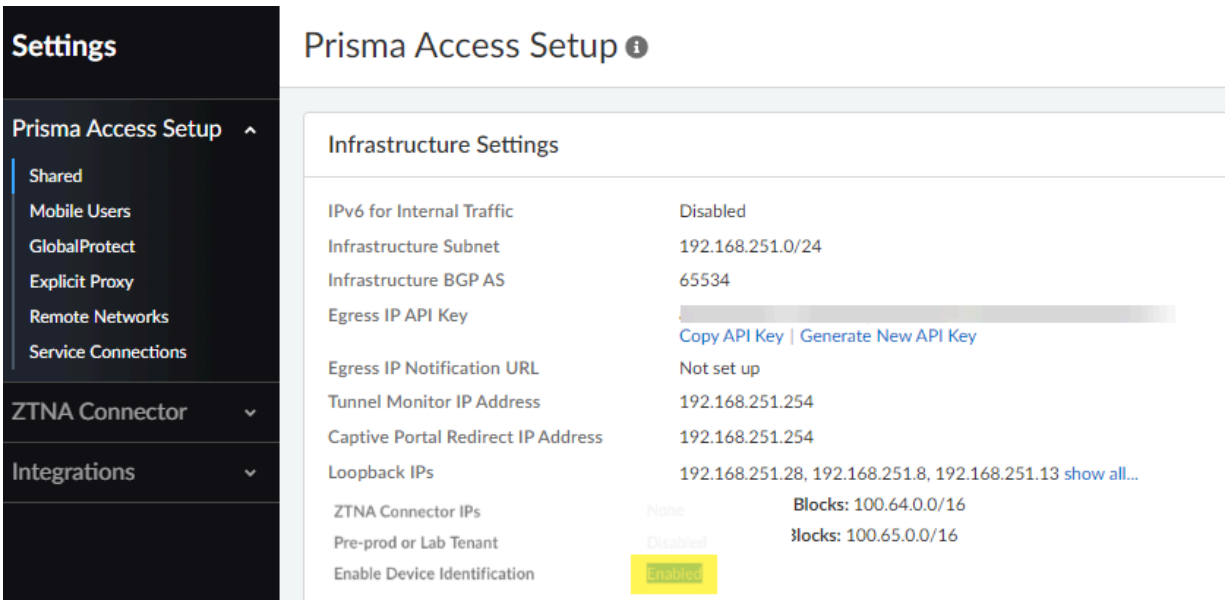
Configurer Third-Party Device-ID dans Prisma Access (Strata Cloud Manager)

Pour configurer un Third-Party Device-ID, effectuez la tâche suivante.

STEP 1 | Activez le Third-Party Device-ID dans Cloud Identity Engine.

Cette procédure comprend le téléchargement d'un certificat signé et son utilisation avec une API pour communiquer avec le fournisseur IoT tiers et télécharger des informations d'ID de périphérique à partir de celui-ci.

STEP 2 | Activez Third-Party Device-ID dans Prisma Access en vous accédant à **Settings (Paramètres)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Shared (Partagé)** ou **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access**et définissez **Enable Device Identification (Activer l'identification du périphérique)** sur **Enabled (Activée)**.



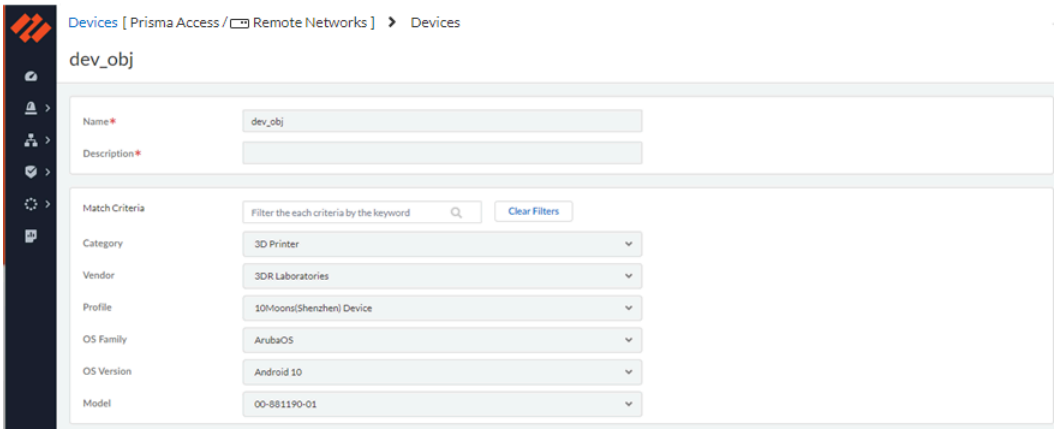
STEP 3 | Configurez un objet de périphérique et entrez les attributs du périphérique. Cliquez sur **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)**, définissez la portée de la configuration sur **Remote Networks (Réseaux distants)**, et sélectionnez **Objects (Objets)** > **Devices (Périphériques)** et **Add Devices (Ajouter des**

 ©2025 Palo Alto Networks, Inc.

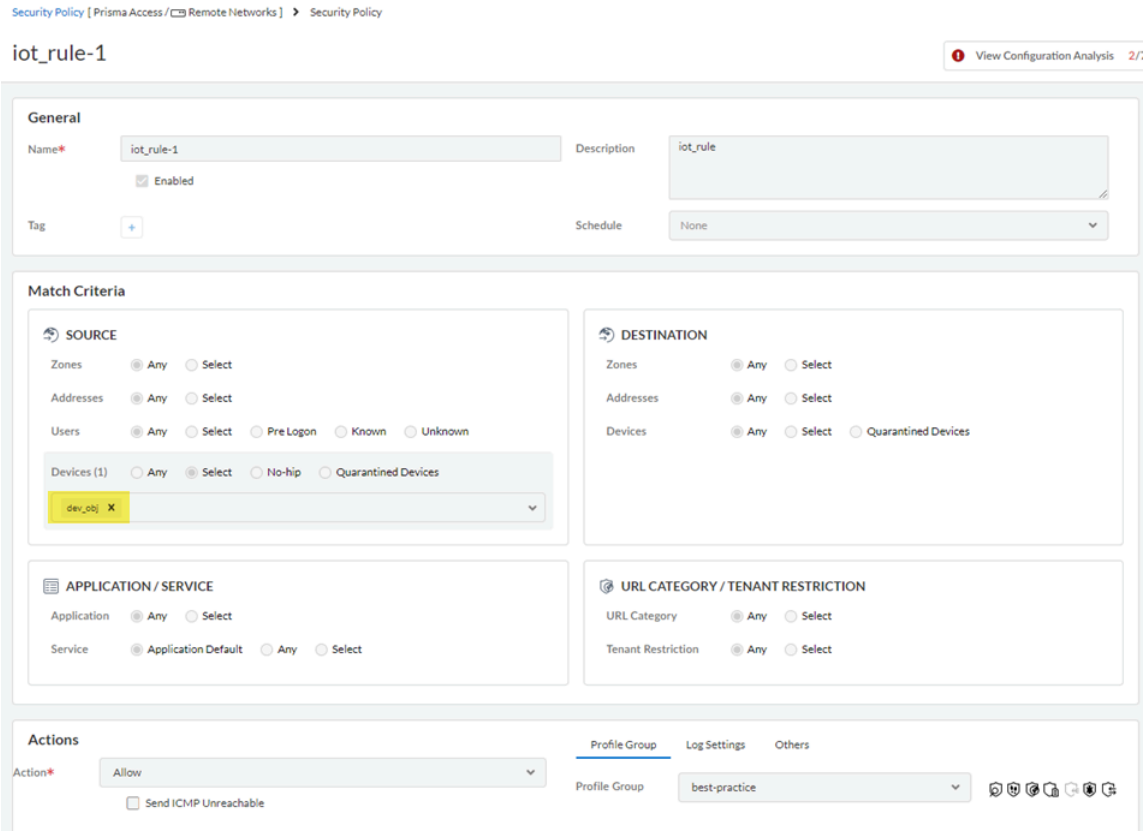
périphériques). Assurez-vous que vous êtes dans le groupe de périphériques de réseaux distants.

1. Ajoutez un objet de périphérique qui correspond aux attributs des objets tiers.

   La zone **Mappings (Mappages)** de Cloud Identity Engine affiche les attributs des périphériques tiers. Vous pouvez utiliser tous les attributs récupérés à partir de là.



STEP 4 | Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)**, définissez la portée de la configuration sur **Remote Networks (Réseaux distants)**, et sélectionnez **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** et cliquez sur **Add (Ajouter)** pour ajouter une politique de sécurité, en ajoutant les objets de périphérique que vous avez créés dans la zone **Devices (Périphériques)**.

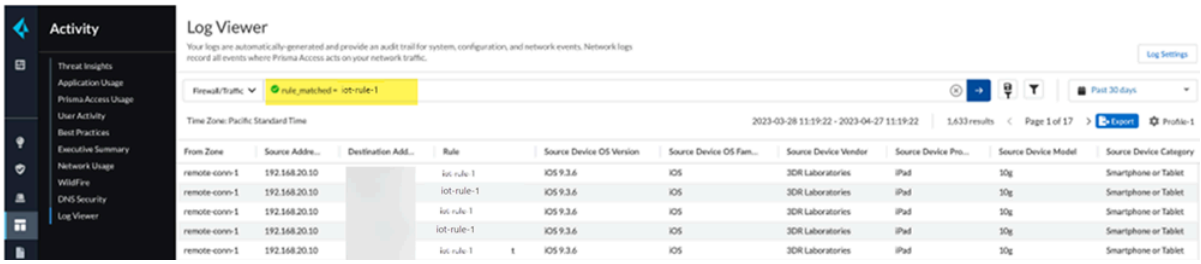


 ©2025 Palo Alto Networks, Inc.

STEP 5 | Cliquez sur **Push Config (Transmettre la configuration)** pour enregistrer vos modifications dans la configuration Prisma Access, en vous assurant de sélectionner **Remote Networks (Réseaux distants)** dans l'étendue de la transmission.

STEP 6 | Vérifiez que Prisma Access reçoit les journaux d'ID de périphérique en accédant à **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)**, en sélectionnant **Firewall/Traffic (Pare-feu/trafic)** et en recherchant le trafic sous la règle que vous avez créée en entrant `rule_matched = rulename` où *rulename* est la règle de politique de sécurité que vous avez créée pour les périphériques IoT tiers.

Les mappages de l'ID de périphérique à l'adresse IP s'affichent dans les journaux.



Configurer Third-Party Device-ID dans Prisma Access (Panorama)

Pour configurer un Third-Party Device-ID, effectuez la tâche suivante.

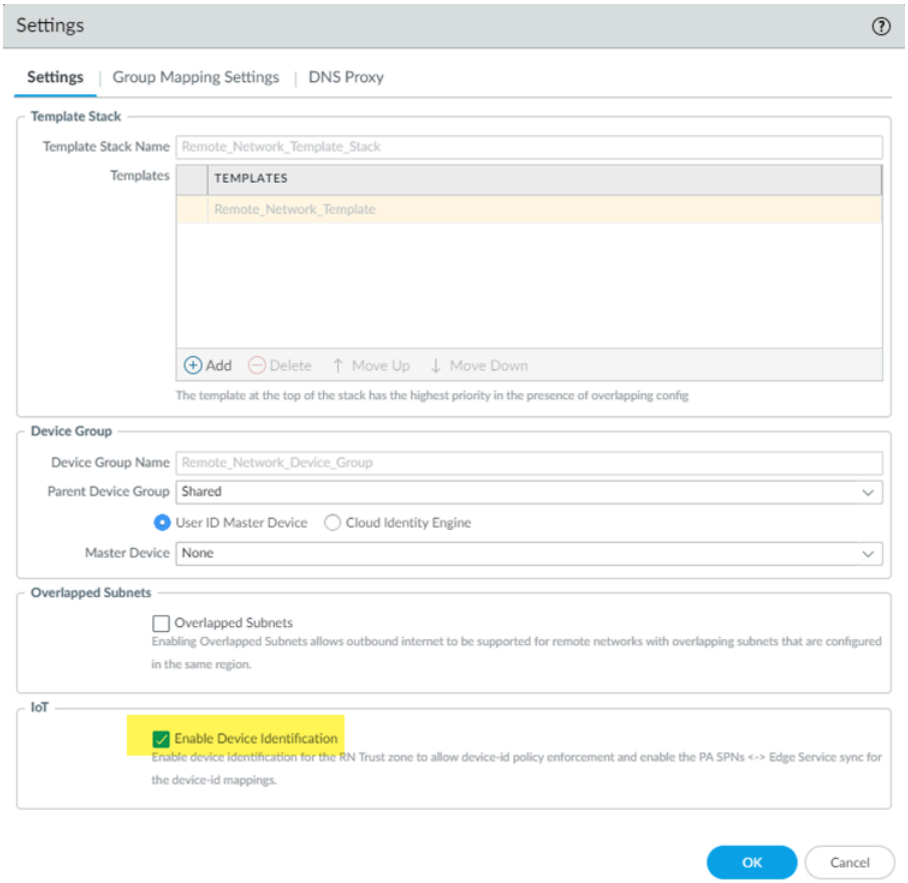
STEP 1 | Activez le Third-Party Device-ID dans Cloud Identity Engine.

Cette procédure comprend le téléchargement d'un certificat signé et son utilisation avec une API pour communiquer avec le fournisseur IoT tiers et télécharger des informations d'ID de périphérique à partir de celui-ci.

STEP 2 | Activez Third-Party Device-ID dans Prisma Access en accédant à **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** > **Settings (Paramètres)**, en cliquant

 ©2025 Palo Alto Networks, Inc.

sur l'engrenage pour modifier les **Settings (Paramètres)**, et en sélectionnant **Enable Device Identification (Activer l'identification du périphérique)**.



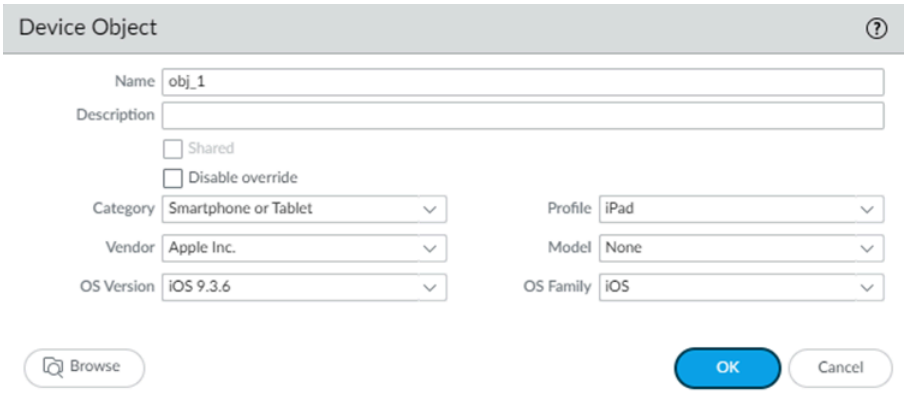
 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configurez un objet de périphérique et entrez les attributs du périphérique.

1. Accédez à **Objects (Objets)** > **Devices (Périphériques)** et cliquez sur **Add (Ajouter)** pour ajouter un objet de périphérique qui correspond à tous les attributs d'ID du périphérique.

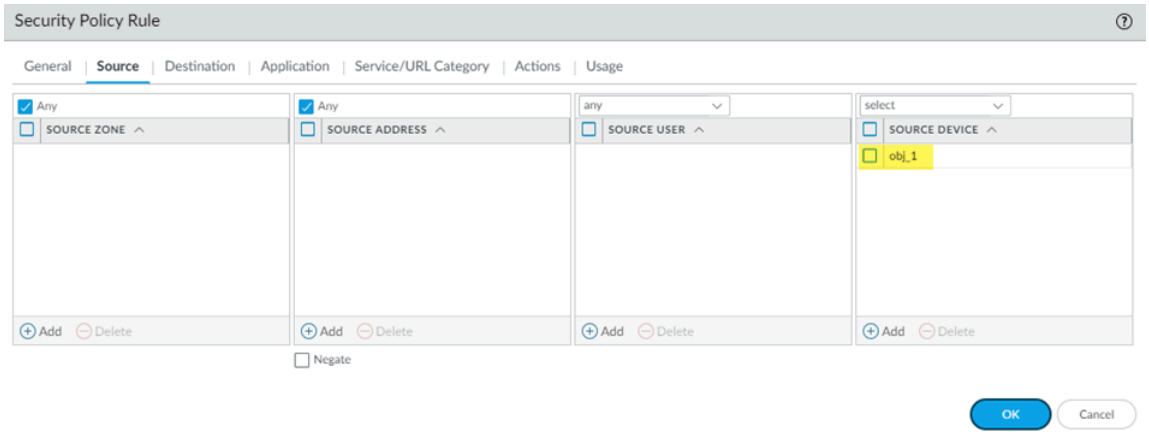
   Assurez-vous que vous êtes dans le groupe **Remote_Network_Device_Group** ou dans le groupe de périphériques **Shared (Partagés)**.
2. Cliquez sur **Add (Ajouter)** pour ajouter un objet de périphérique qui correspond aux attributs des objets tiers.

   *La zone **Mappings (Mappages)** de Cloud Identity Engine affiche les attributs des périphériques tiers. Vous pouvez utiliser tous les attributs récupérés à partir de là.*



STEP 4 | Accédez à **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Pré-règles)** et cliquez sur **Add (Ajouter)** une politique de sécurité, en ajoutant les objets de périphérique que vous avez créés dans les zones **Devices (Périphériques)** comme **Source Device (Périphérique source)**.

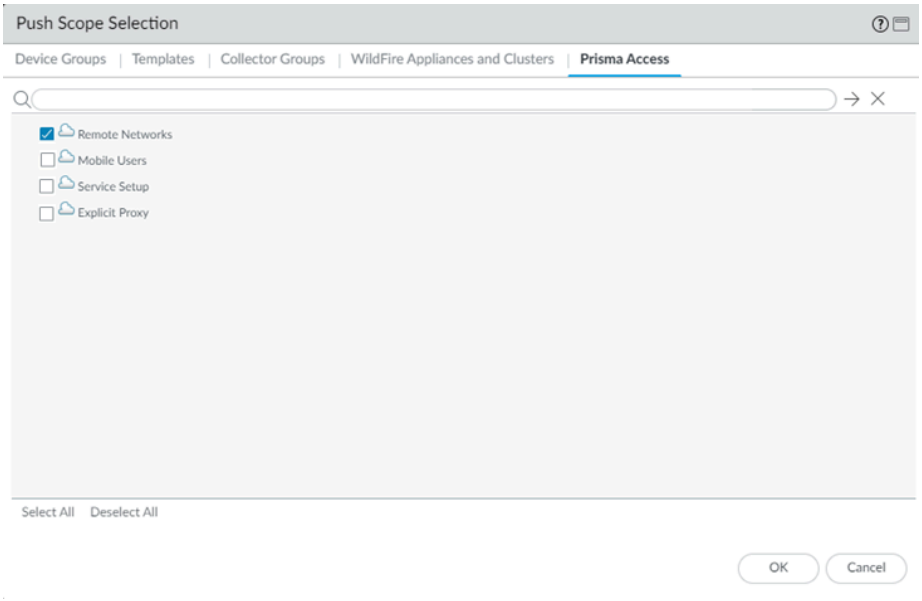
Assurez-vous que vous êtes dans le groupe **Remote_Network_Device_Group** ou dans le groupe de périphériques **Shared (Partagés)**.



 ©2025 Palo Alto Networks, Inc.

STEP 5 | Validez et appliquez vos modifications, en vous assurant que **Remote Networks (Réseaux distants)** est sélectionné dans **Push Scope (Étendue de la transmission)**.

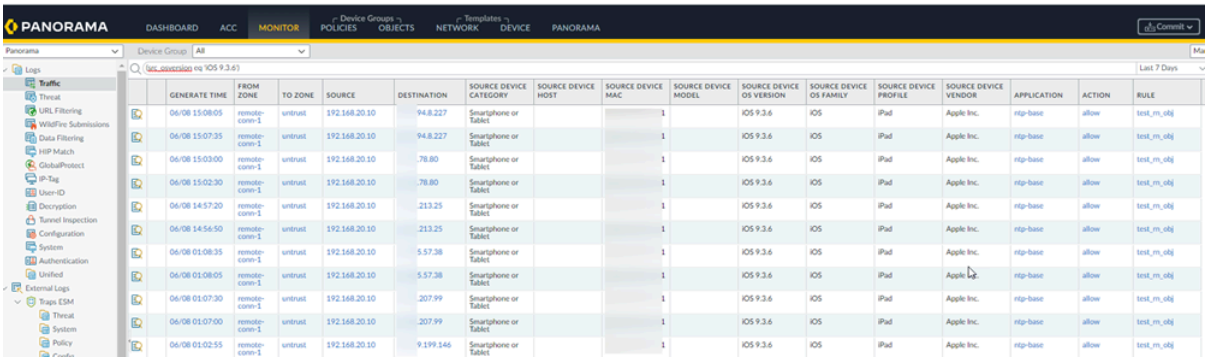
1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**.
2. Cliquez sur **Edit Selections (Modifier les sélections)** et, dans l'onglet **Prisma Access**, assurez-vous que **Remote Networks (Réseaux distants)** est sélectionné dans **Push Scope (Étendue de la transmission)**, puis cliquez sur **OK**.



3. Cliquez sur **Commit and Push (Valider et appliquer)**.

STEP 6 | Vérifiez que Prisma Access reçoit les journaux d'ID de périphérique en accédant à **Monitor (Surveiller)** > **Logs (Journaux)**, et en recherchant les journaux **Traffic (Trafic)** pour le trafic sous la règle que vous avez créée en entrant `rule_matched = rulename`, où *rulename* est la règle de politique de sécurité que vous avez créée pour les périphériques IoT tiers.

Les mappages de l'ID de périphérique à l'adresse IP s'affichent dans les journaux.



 ©2025 Palo Alto Networks, Inc.

API d'identification de périphériques tiers

Une fois que vous avez intégré le service d'identification des périphériques tiers à l'aide de l'interface utilisateur de Cloud Identity Engine, vous pouvez utiliser ces API pour gérer les *verdicts*, ou les mappages d'adresses IP aux périphériques, détectés sur votre réseau et stockés dans le service d'identification des périphériques tiers. Ces mappages indiquent à Prisma Access quels attributs appartiennent à un périphérique avec une adresse IP particulière afin que vous puissiez définir une politique de sécurité ciblant les périphériques avec des attributs spécifiques.

Ces API n'accèdent pas directement aux données stockées dans votre locataire Cloud Identity Engine. Au lieu de cela, les API interagissent avec les mappages d'adresses IP vers des périphériques dans le service d'ID de périphériques tiers, qui partage ces mappages avec Cloud Identity Engine.

Les API d'identification de périphériques tiers utilisent un certificat, une clé API et une URL de base pour les requêtes d'API. Pour authentifier les requêtes d'API d'identification de périphériques tiers, vous devez utiliser le certificat signé et le jeton d'API que vous avez obtenus lors de l'intégration dans l'interface utilisateur de Cloud Identity Engine.

Lorsque vous disposez d'un certificat et d'une clé d'API, vous pouvez effectuer des requêtes auprès du service d'identification de périphériques tiers. Fournissez le certificat avec sa clé publique, la clé d'API et l'URL de base dans chaque requête. Exemple :

```
curl --cert onida1.crt --key onida.key "https://device-identity-
broker-beta.service-edge.panservicetest.com/:443/api/v1/token/
{apiKey}/verdicts"
```


- Mettre à jour les verdicts
- Supprimer tous les verdicts
- Verdicts de requête
- Interroger les verdicts par adresse IP
- Statistiques du Verdict de requête

Mettre à jour les verdicts

Ajoute, modifie ou supprime des mappages d'adresse IP à périphérique.

Synopsis

URI	`/api/v1/token/{apiKey}/verdicts:update`
Méthode HTTP	POST

Description

Le Device-ID tiers ingère des données provenant de sources de détection IoT tierces dans votre réseau et crée des mappages d'adresse IP à périphérique que Prisma Access peut utiliser pour

 ©2025 Palo Alto Networks, Inc.

appliquer les règles de politique de sécurité spécifiques au périphérique. Utilisez cette API pour ajouter un nouveau mappage, modifier un mappage existant ou supprimer un mappage.

Vous ajoutez ou modifiez un mappage à l'aide du champ `Mettre à jour`, et vous supprimez un mappage à l'aide du champ `Supprimer`.

Si le mappage existe déjà, `Mettre à jour` remplace les attributs de périphérique existants par les attributs spécifiés dans le corps de la requête. Si le mappage n'existe pas, Mettre à jour crée le nouveau mappage.

Cette API ne prend pas en charge les mises à jour partielles. Si vous souhaitez mettre à jour des attributs spécifiques d'un mappage, vous devez également saisir à nouveau les valeurs précédentes pour les attributs que vous ne souhaitez pas mettre à jour. Laisser les attributs vides effacera les valeurs existantes.

Vous pouvez mettre à jour ou supprimer jusqu'à 10 000 mappages à la fois. La requête est atomique : une réponse de réussite signifie que le système a tout traité, et une réponse de défaillance signifie que le système n'a rien traité.

Champs

Champ	Description
Mettre à jour	Objet JSON qui fournit les attributs d'un mappage d'adresse IP à périphérique que vous souhaitez mettre à jour ou créer. Doit avoir une adresse IP et au moins un autre attribut renseigné.
Supprimer	Objet JSON qui spécifie l'adresse IP du mappage à supprimer.

Par exemple :

```
{ "update": [ { "ip": "string", "serialNo": "string", "mac":
 "string", "category": "string", "vendor": "string", "model":
 "string", "os": "string", "osFamily": "string", "hostname":
 "string", "profile": "string", } ], "delete": [ { ip: "string" } ] }
```

Réponse de réussite

En cas de réussite, le code de réponse HTTP est 200. De plus, la réponse contient un objet JSON avec le champ suivant :

Champ	Description
`updateTime`	Horodatage unix qui représente le moment où la requête réussit.

Par exemple :

```
{ "updateTime": unix-timestamp }
```

 ©2025 Palo Alto Networks, Inc.

Réponse d'erreur

En cas d'erreur, le code de réponse HTTP est l'un des suivants :

Code de réponse	Description
400	Requête non valide. La requête était incomplète ou déformée d'une certaine manière. Corrigez la requête avant de réessayer.
401	Jeton non autorisé. Essayez de régénérer votre jeton API. Si cela ne fonctionne pas, contactez le support.
409	Conflit. La requête n'a pas pu être traitée, car une autre tâche de mise à jour ou de suppression est en cours. Réessayez une fois que l'autre tâche est terminée.
429	Trop de requêtes. La requête n'a pas pu être traitée, car le système a émis trop de requêtes dans un laps de temps précis. Ne dépassez pas plus d'une requête par seconde. Attendez et réessayez.

En outre, le corps de réponse contient les champs suivants :

Champ	Description
Code	Code d'erreur.
Message	Message d'erreur.

Mettre à jour un objet

Contient les informations nécessaires pour mettre à jour les mappages d'adresses IP aux périphériques. Cet objet JSON comporte les champs suivants :

Champ	Description
ip (adresse IP)	Adresse IP du périphérique.
updateTime	Horodatage Unix qui indique la date et l'heure de la dernière mise à jour du mapp
catégorie	Type de périphérique. Exemple : Imprimante
Constructeur	Fournisseur de périphérique. Exemple : Société SHARP
model	Modèle de périphérique. Exemple : MX-6070N
os	Système d'exploitation du périphérique. Exemple : ThreadX 5

 ©2025 Palo Alto Networks, Inc.

osFamily	Famille à laquelle appartient le système d'exploitation du périphérique. Exemple
profile	Profil du périphérique. Exemple : Imprimante Sharp

Supprimer tous les verdicts

Supprime tous les mappages d'adresse IP à périphérique du service Third-Party Device-ID.

Synopsis

URI	/api/v1/token/{apiKey}/verdicts:all
Méthode HTTP	DELETE

Description

Demande au service Third-Party Device-ID de supprimer tous les mappages d'adresse IP à périphérique dans le service Third-Party Device-ID. Une réponse réussie signifie que le service a supprimé tous les mappages. Une réponse d'erreur signifie que le service ne pouvait supprimer aucun mappage.

Réponse réussie

En cas de succès, le code de réponse HTTP est 200. Le corps de réponse est vide.

Réponse d'erreur

En cas d'erreur, le code de réponse HTTP est l'un des suivants :

Code de réponse	Description
401	Jeton non autorisé. Essayez de régénérer votre jeton API. Si cela ne fonctionne pas, contactez le support.
409	Conflit. Le système n'a pas pu traiter la requête, car il y a une autre mise à jour ou suppression de tâche en cours. Réessayez une fois que l'autre tâche est terminée.
429	Trop de requêtes. Le système ne pouvait pas traiter la requête, car il avait émis trop de requêtes dans un laps de temps précis. Ne dépassez pas plus d'une requête par seconde. Attendez et réessayez.

En outre, le corps de réponse contient les champs suivants :

Champ	Description
Code	Le code d'erreur.

 ©2025 Palo Alto Networks, Inc.

Champ	Description
Message	Le message d'erreur.

Verdicts de requête

Récupère les IP address-to-device mappings dans le service d'identification de périphériques tiers.

Synopsis

URI	/api/v1/token/{apiKey}/verdicts? bookmark={STRING}&pageLen={INTEGER}
Méthode HTTP	GET

Description

Renvoie soit tous les mappages, soit un sous-ensemble.

Pour renvoyer tous les mappages, envoyez la requête une seule fois sans aucun paramètre. Prenez note de la valeur `nextBookmark` dans la réponse. Envoyez une autre requête en utilisant cette valeur pour `signet` ajouté à l'URI. L'appelant répétera la requête jusqu'à ce que le `nombre` soit vide dans la réponse, indiquant qu'il a renvoyé tous les mappages.

Pour renvoyer un sous-ensemble de mappages, spécifiez le nombre de mappages que vous souhaitez récupérer à l'aide de `pageLen`, jusqu'à 10000.

Paramètres

Cette API accepte ces paramètres :

Paramètre	Description
signet	(Facultatif) Utilisé après la première requête pour renvoyer tous les mappages.
pageLen	(Facultatif) Le nombre de mappages à récupérer. La plage est comprise entre 1 et 10000. Si elle n'est pas spécifiée, la valeur par défaut est 10000.

Réponse de réussite

En cas de succès, le code de réponse HTTP est 200. De plus, la réponse contient un objet JSON avec les champs suivants :

Champ	Description

 ©2025 Palo Alto Networks, Inc.

nextBookmark	La valeur que vous utilisez dans le paramètre signet pour effectuer des requêtes ce que tous les mappages soient renvoyés.
nombre	Entier représentant le nombre de mappages renvoyés dans la réponse.
verdicts	Objet contenant les mappages spécifiés dans la requête.

Par exemple :

```
{ "nextBookmark": CkcKVxdWVuY2USAggEEjFqCHN, "count": 1, "verdicts" :
 [ { "ip": "10.10.10.10", "updateTime": 1623974506, "mac":
 "0a:d4:5f:e9:96:10", "category": "Smartphone or Tablet", "vendor":
 "Apple Inc.", "model": "iPad2", "os": "iOS 9.3.6", "osFamily":
 "iOS", "profile": "iPad" } ] } }
```

Réponse d'erreur

En cas d'erreur, le code de réponse HTTP est l'un des suivants :

Code de réponse	Description
400	Demande non valide. La requête était incomplète ou déformée d'une certaine ma Vous devez corriger la requête avant de réessayer.
401	Jeton non autorisé.
429	Trop de requêtes. La requête n'a pas pu être traitée parce qu'un trop grand nomb ont été émises dans un laps de temps précis. Il n'est pas permis de faire plus d'un seconde. Veuillez patienter et réessayer.

En outre, le corps de réponse contient les champs suivants :

Champ	Description
code	Le code d'erreur.
message	Le message d'erreur.

verdicts Objet

L'objet renvoyé lorsque vous interrogez avec succès un mappage d'adresse IP à périphérique. Cet objet contient les informations suivantes :

Champ	Description

©2025 Palo Alto Networks, Inc.

ip (adresse IP)	Adresse IP du périphérique.
updateTime	Horodatage Unix qui indique la date et l'heure de la dernière mise à jour du mapp
catégorie	Type de périphérique. Exemple : Imprimante
Constructeur	Fournisseur de périphérique. Exemple : Société SHARP
model	Modèle de périphérique. Exemple : MX-6070N
os	Système d'exploitation du périphérique. Exemple : ThreadX 5
osFamily	Famille à laquelle appartient le système d'exploitation du périphérique. Exemple
profile	Profil du périphérique. Exemple : Imprimante Sharp

Interroger les verdicts par adresse IP

Récupère les IP address-to-device mappings en fonction de l'adresse IP.

Synopsis

URI	/api/v1/token/{apiKey}/verdicts?ip={STRING}
Méthode HTTP	GET

Description

Utilise les adresses IP pour renvoyer les mappages de périphériques correspondants. Vous pouvez récupérer plusieurs mappages en fournissant une liste d'un maximum de 10 adresses IP, séparées par des virgules, ajoutées à l'URI.

Si le service ne trouve pas de mappage associé à une adresse IP, il ne renverra pas de mappage pour cette adresse IP.

Réponse de réussite

En cas de succès, le code de réponse HTTP est 200. De plus, la réponse contient un objet JSON avec les champs suivants :

Champ	Description
nombre	Entier représentant le nombre de mappages renvoyés dans la réponse.
verdicts	Objet contenant les mappages spécifiés dans la requête.

Par exemple :

 ©2025 Palo Alto Networks, Inc.

```
{ "count": 1, "verdicts" : [ { "ip": "10.10.10.10", "updateTime":
 1623974506, "mac": "0a:d4:5f:e9:96:10", "category": "Smartphone
 or Tablet", "vendor": "Apple Inc.", "model": "iPad2", "os": "iOS
 9.3.6", "osFamily": "iOS", "profile": "iPad" } ] } }
```


Réponse d'erreur

En cas d'erreur, le code de réponse HTTP est l'un des suivants :

Code de réponse	Description
400	Demande non valide. La requête était incomplète ou déformée d'une certaine ma Corrigez la requête avant de réessayer.
401	Jeton non autorisé.
429	Trop de requêtes. Le système n'a pas pu traiter la requête, car il a émis trop de re laps de temps précis. Ne dépassez pas plus d'une requête par seconde. Attendez

En outre, le corps de réponse contient les champs suivants :

Champ	Description
code	Le code d'erreur.
message	Le message d'erreur.

Statistiques du Verdict de requête

Récupère des statistiques sur le service d'identification de périphériques tiers.

Synopsis

URI	/api/v1/token/{apiKey}/verdicts:statistics
Méthode HTTP	GET

Réponse de réussite

En cas de succès, le code de réponse HTTP est 200. De plus, la réponse contient un objet JSON avec les champs suivants :

Champ	Description
verdicts	Objet qui contient des statistiques sur les IP address-to-mappings de votre locata champs suivants :

 ©2025 Palo Alto Networks, Inc.

	• totalCount - Le nombre total d'IP address-to-device mappings du locataire. • totalUpdate - Le nombre d'IP address-to-service mappings qui ont été mis à jo création. • totalDelete - Le nombre d'IP address-to-device mappings qui ont été supprim création de votre locataire.
requestRcvd	Objet qui contient le nombre de fois que le locataire a reçu chaque type de dema • update - Le nombre de demandes Mettre à jour les verdicts reçues. • deleteAll - Le nombre de demandes Supprimer tous les verdicts reçues. • query - Le nombre de demandes Verdicts de requête et Interroger les verdicts reçues. • Statistics - Le nombre de demandes Statistiques du Verdict de requête reçues

Par exemple :

```
{ "verdicts: { "totalCount": 1, "totalUpdate": 0, "totalDelete":
 0, }, "requestRcvd": { "update": 1, "deleteAll": 0, "query": 0,
 "statistics": 1 } }
```

Réponse d'erreur

En cas d'erreur, le code de réponse HTTP est l'un des suivants :

Code de réponse	Description
401	Jeton non autorisé.
429	Trop de requêtes. La requête n'a pas pu être traitée parce qu'un trop grand nomb ont été émises dans un laps de temps précis. Il n'est pas permis de faire plus d'un seconde. Veuillez patienter et réessayer.

En outre, le corps de réponse contient les champs suivants :

Champ	Description
code	Le code d'erreur.
message	Le message d'erreur.

 ©2025 Palo Alto Networks, Inc.

Multilocation Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Pour plus d'informations sur la gestion de plusieurs locataires dans Prisma Access (Managed by Strata Cloud Manager), consultez Prisma SASE.	❑ Licence Prisma Access

Cette section fournit uniquement des informations sur la gestion de plusieurs locataires dans Prisma Access (Panorama). Pour plus d'informations sur la gestion de plusieurs locataires dans Prisma Access (Managed by Strata Cloud Manager), consultez Prisma SASE.

Pour vous permettre de créer et de gérer plusieurs instances Prisma Access, Prisma Access offre la multilocation, qui vous permet de créer jusqu'à 200 instances (locataires) sur un seul appareil Panorama (ou 2 appareils en mode haute disponibilité [High Availability – HA]), chaque locataire disposant de ses propres modèles et piles de modèles, groupes d'appareils et domaines d'accès.

Les déploiements non multilocataires existants ou futurs ne sont pas concernés par la multilocation et continueront de fonctionner normalement. Nous vous recommandons d'activer la multilocation uniquement si votre organisation doit gérer plusieurs locataires dans Prisma Access.

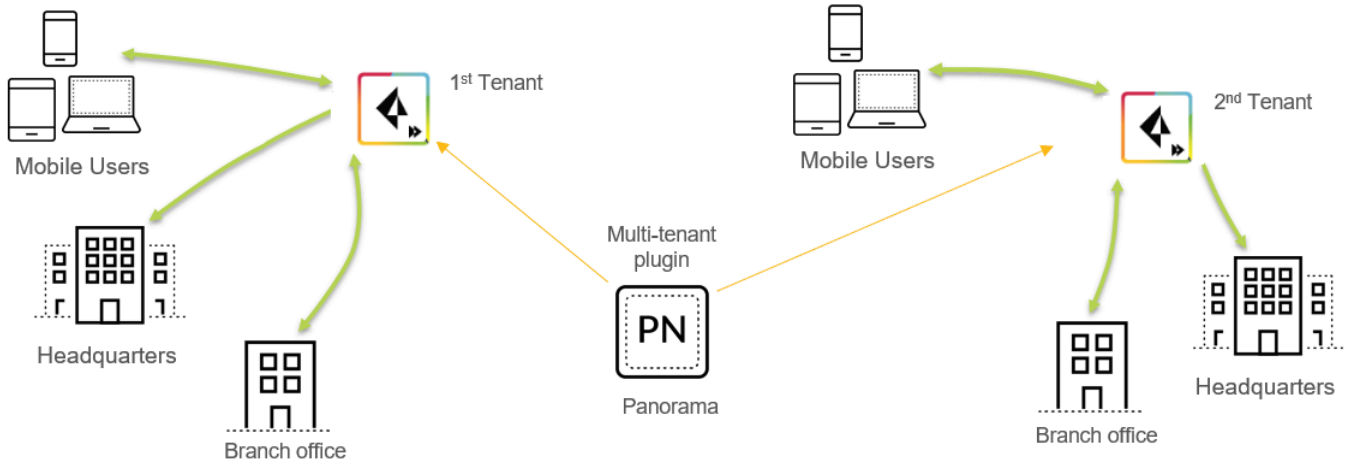
Cette section fournit uniquement les tâches que vous devez effectuer pour configurer des locataires pour les déploiements de réseaux distants, d'utilisateurs mobiles ou d'une combinaison des deux. Pour configurer le service Clean Pipe, consultez la section Prisma Access pour Clean Pipe.

Présentation de la configuration multilocataire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Pour plus d'informations sur la gestion de plusieurs locataires dans Prisma Access (Managed by Strata Cloud Manager), consultez Prisma SASE.	❑ Licence Prisma Access

L'activation du multilocataire vous permet d'héberger plusieurs instances Prisma Access sur un seul appareil Panorama. Chaque instance est connue sous le nom de *Locataire*.

Les locataires Prisma Access disposent de leurs propres instances Prisma Access dédiées et elles ne sont pas partagées entre les locataires.



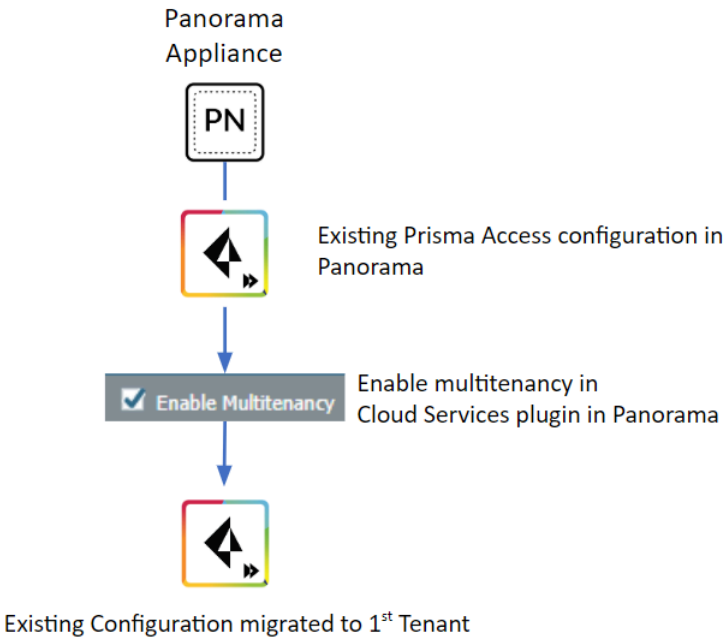
Utilisez le flux de travail suivant pour configurer la possibilité de gérer plusieurs locataires dans un seul appareil Panorama :

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Activez le multilocataire. Si vous disposez d'une instance Prisma Access, l'activation du multilocataire migre automatiquement votre configuration Prisma Access existante vers le premier locataire.

Donnez un nom au premier locataire (migré) et spécifiez un domaine d'accès. Prisma Access migre les modèles, les piles de modèles et les groupes de périphériques associés à la configuration existante et les associe au domaine d'accès que vous créez.

Une fois que vous avez migré votre configuration initiale, l'utilisateur administratif dans Panorama devient un super utilisateur avec la capacité de créer et de gérer tous les locataires Prisma Access.



STEP 2 | Ensuite, ajoutez des locataires à Prisma Access.

Pour déployer plusieurs locataires, assurez-vous de disposer des minimums de licence suivants :

*Pour déterminer le type de licence Prisma Access que vous avez de Panorama, sélectionnez **Panorama** > **Licenses (Licences)**.*

- Si vous avez une licence **Business**, **Business Premium**, **Passerelle Internet sécurisée (SIG) avec accès au réseau Zero Trust (ZTNA)**, ou **Entreprise**, utilisez les minimums suivants à titre indicatif :

  Prisma Access pour les réseaux et **Prisma Access pour les utilisateurs** :

  Si vous disposez d'une édition **Local (Locale)**, vous devez avoir une quantité minimale de 200 unités pour chaque locataire, et tous les locataires seront locaux.

  Si vous disposez d'une édition **Worldwide (Monde entier)**, vous devez avoir une quantité minimale de 1 000 unités pour créer un locataire **Worldwide (Monde entier)**. Si vous attribuez entre 200 et 999 unités à un locataire, Prisma Access crée un locataire **Local** ;

 ©2025 Palo Alto Networks, Inc.

si vous attribuez 1 000 unités ou plus à un locataire, Prisma Access crée un locataire **Worldwide (Monde entier)**.

Les *unités* correspondent à la bande passante en Mbit/s pour Prisma Access pour les réseaux distants et le nombre d'utilisateurs mobiles pour Prisma Access pour les utilisateurs.

- Si votre type de licence commence par **GlobalProtect Cloud Service (Service cloud GlobalProtect)**, utilisez les minimums suivants à titre indicatif :

  Prisma Access pour les réseaux : vous devez disposer d'un minimum de 200 Mbit/s dans votre licence pour chaque locataire.

  Prisma Access pour les utilisateurs : vous devez disposer d'un minimum de 200 utilisateurs mobiles disponibles dans votre licence pour chaque locataire.

  Dans les deux types de configurations Prisma Access, vous pouvez ajouter des licences supplémentaires (au-delà de ces minimums) de l'un ou l'autre type. Vous pouvez augmenter ou diminuer la bande passante ou l'allocation des utilisateurs mobiles pour n'importe quel locataire après l'intégration, à condition de conserver l'allocation minimale requise par locataire et de ne pas dépasser la capacité globale sous licence.

Vous pouvez configurer une configuration multilocataire pour les réseaux distants uniquement, les utilisateurs mobiles uniquement, ou les deux. Vous pouvez attribuer des licences en fonction de chaque locataire lorsque vous activez le multilocataire.

Si vous disposez d'une licence pour les réseaux distants et les utilisateurs mobiles, vous pouvez configurer un locataire individuel ayant seulement des utilisateurs mobiles ou des réseaux distants. Par exemple, si votre déploiement Prisma Access a une licence d'édition **Worldwide (Monde entier)** pour les utilisateurs mobiles et les réseaux distants, vous pouvez configurer un locataire pour les utilisateurs mobiles uniquement, à condition de spécifier un minimum de 1 000 utilisateurs mobiles pour le locataire.

Pour chaque locataire que vous créez après le premier, Prisma Access crée automatiquement des modèles, des piles de modèles et des groupes de périphériques pour chaque locataire et les associe au domaine d'accès que vous créez. Prisma Access crée cet environnement pour vous permettre de créer un utilisateur administrateur au niveau du locataireà l'aide d'un rôle d'administrateur basé sur les groupes de périphériques et les modèles du locataire, puis de créer un utilisateur administrateur basé sur ce rôle. De cette façon, vous créez un utilisateur

 ©2025 Palo Alto Networks, Inc.

administrateur disposant d'un accès à un seul locataire sans autoriser cet utilisateur à accéder aux autres locataires gérés par l'appareil Panorama.

Prisma Access crée des piles de modèles, des modèles et des groupes de périphériques en appliquant la convention de dénomination suivante :

- Une pile de modèles de connexion aux services portant le nom **sc-stk-***tenant* (locataire) où *tenant* (locataire) est le nom du locataire.
- Un modèle de connexion aux services portant le nom **sc-tpl-***tenant* (locataire).
- Un groupe de périphériques de connexion aux services portant le nom **sc-dg-***tenant* (locataire).
- Une pile de modèles d'utilisateurs mobiles portant le nom **mu-stk-***tenant* (locataire).
- Un modèle d'utilisateur mobile portant le nom **mu-tpl-***tenant* (locataire).
- Un groupe de périphériques d'utilisateurs mobiles portant le nom **mu-dg-***tenant* (locataire).
- Une pile de modèles de réseau distant portant le nom **rn-stk-***tenant* (locataire).
- Un modèle de réseau distant portant le nom **rn-tpl-***tenant* (locataire).
- Un groupe de périphériques de réseau distant portant le nom **rn-dg-***tenant* (locataire).
- Une pile de modèles de proxy explicite portant le nom **ep-stk-***tenant* (locataire).
- Un modèle de proxy explicite portant le nom **ep-tpl-***tenant* (locataire).
- Un groupe de périphériques de proxy explicite portant le nom **ep-dg-***tenant* (locataire).
- Une pile de modèles Clean Pipe portant le nom **cp-stk-***tenant* (locataire).
- Un modèle Clean Pipe portant le nom **cp-tpl-***tenant* (locataire).
- Un groupe de périphériques Clean Pipe portant le nom **cp-dg-***tenant* (locataire).

Des piles de modèles, des modèles et des groupes de périphériques sont créés pour tous les types de Prisma Access, même ceux pour lesquels vous ne disposez peut-être pas de licence. Par exemple, si vous achetez une licence pour des réseaux distants, Prisma Access crée automatiquement des piles de modèles, des modèles et des groupes de périphériques pour les réseaux distants, les utilisateurs mobiles et Clean Pipe.

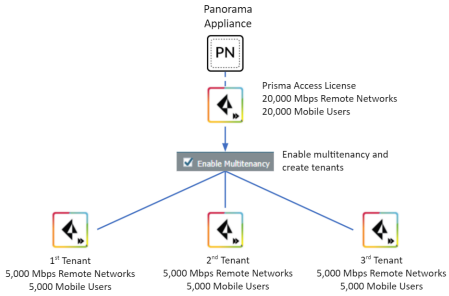
Si vous ajoutez des modèles personnalisés, ceux-ci ne peuvent pas avoir la priorité sur les modèles créés par Prisma Access.

Vous allouez les ressources de la licence de réseaux distants et d'utilisateurs mobiles pour chaque locataire en fonction de la licence associée au plug-in Cloud Services dans Panorama.

La figure suivante montre un exemple de déploiement Prisma Access utilisant une licence avec un pool de bande passante de 20 000 Mbit/s pour les réseaux distants et 20 000 utilisateurs mobiles. L'administrateur a alloué une bande passante de 5 000 Mbit/s pour les réseaux distants et 5 000 utilisateurs mobiles pour la configuration existante. Une fois que l'administrateur a activé le multilocataire, l'allocation de licence a été migrée avec toutes les autres configurations vers le premier locataire. L'administrateur a ensuite créé des locataires supplémentaires, chacun avec un pool de bande passante de 5 000 Mbit/s pour les réseaux distants et 5 000 utilisateurs mobiles pour chaque locataire. Prisma Access alloue les ressources de licence à partir de l'allocation globale de la licence. Une fois cette configuration

 ©2025 Palo Alto Networks, Inc.

terminée, la licence dispose d'une bande passante de 5 000 Mbit/s pour les réseaux distants et de 5 000 utilisateurs mobiles.



 ©2025 Palo Alto Networks, Inc.

Planifier votre déploiement multilocataire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Pour plus d'informations sur la gestion de plusieurs locataires dans Prisma Access (Managed by Strata Cloud Manager), consultez Prisma SASE.	• Licence Prisma Access

Avant d'activer le multilocataire, de migrer le premier locataire et d'en créer d'autres, assurez-vous de disposer de toutes les informations et ressources nécessaires pour ce faire en effectuant les tâches suivantes :

- ❑ Si vous migrez un déploiement monolocataire existant vers un déploiement multilocataire, sachez que les fonctionnalités Prisma Access suivantes ne sont pas prises en charge. Consultez la matrice de compatibilité Palo Alto Networks pour obtenir la liste des fonctionnalités non prises en charge.
- ❑ Si vous n'avez pas de configuration Prisma Access existante, vous devez **Enable Multitenancy (Activer le multilocataire)** et ajouter vos locataires; puis configurer les locataires après les avoir créés. Pour plus d'informations, reportez-vous à la section Créer un tout nouveau déploiement multilocataire.
- ❑ Notez l'allocation de votre licence pour les réseaux distants et les utilisateurs mobiles.

  Ouvrez votre licence (**Panorama** > **Licenses (Licences)**) et recherchez le **Total Mbps (Total Mbit/s)** (pool de bande passante pour les réseaux distants) de Prisma Access pour les réseaux distants et **User Limit (Limite d'utilisateurs)** (nombre total d'utilisateurs sous licence) pour les utilisateurs mobiles.

  Lorsque vous créez des locataires, vous attribuez des ressources pour les réseaux distants et les utilisateurs mobiles à partir de cette allocation de licence. Si vous utilisez la totalité de Mbps sous licence minimum requis pour les réseaux distants ou les utilisateurs mobiles, vous ne pourrez pas créer de locataires supplémentaires.

  Vous devez également noter l'allocation de bande passante et d'utilisateurs mobiles de votre configuration existante. Après avoir migré votre configuration vers le premier locataire, contrôlez ces valeurs pour vous assurer que le premier locataire a migré correctement.
- ❑ Dressez une liste des noms que vous utiliserez pour identifier chaque locataire.

  Lorsque vous créez des noms de locataire, évitez d'utiliser des noms comme Locataire-1, Locataire-2, Locataire-3, etc. Les journaux système réservent un petit nombre de caractères au nom du locataire dans la sortie du journal et, si les locataires ont des noms similaires, il peut être difficile d'associer le locataire aux journaux. Nous recommandons d'utiliser un nom unique et court pour les locataires (par exemple, Acme ou Hooli).

 ©2025 Palo Alto Networks, Inc.

- Dressez une liste des utilisateurs administratifs que vous allez créer et attribuer à chaque locataire, et notez le nombre maximum d'utilisateurs administratifs qui peuvent être connectés simultanément.

  Lorsque des utilisateurs administratifs effectuent des opérations multilocataires normales comme des changements de configuration et des opérations de validation, nous recommandons d'avoir un maximum de 12 utilisateurs administratifs connectés simultanément à Panorama.

  Un utilisateur administratif capable de gérer plusieurs locataires peut provisionner jusqu'à 200 locataires en même temps par une seule opération de validation.
- Veillez à disposer de ressources de licence suffisantes pour activer plusieurs locataires.

  L'attribution de licence minimale pour chaque locataire est de 200 Mbit/s par réseau distant ou 200 utilisateurs mobiles. Vous pouvez également créer un locataire ayant uniquement des réseaux distants ou des utilisateurs mobiles, et configurer des locataires selon des configurations différentes sur le même Panorama. Par exemple, vous pouvez créer un locataire ayant uniquement des réseaux distants, un locataire ayant uniquement des utilisateurs mobiles, ou un locataire ayant des utilisateurs mobiles et des réseaux distants, à condition que chaque locataire respecte l'allocation de licence minimale et que les licences concernées soient activées et associées au Panorama dans lequel vous configurez les locataires.
- Lors de la configuration d'un locataire en mode multilocataire, créez un nom unique pour chaque tunnel IPSec et passerelle IKE pour les connexions aux services et les connexions réseau distantes, et essayez d'utiliser un nom qui ne sera pas dupliqué par un autre locataire. Bien que les fonctionnalités n'en seront pas affectées, vous ne pouvez pas supprimer un tunnel IPSec ou une passerelle IKE si un autre locataire utilise un tunnel ou une passerelle portant le même nom.

  Cette mise en garde s'applique à tous les objets, y compris les profils QoS (vous ne pouvez pas supprimer les objets avec des noms en double dans un déploiement multilocataire si l'un des objets est référencé par un autre locataire).
- Les journaux système ne peuvent pas être consultés par les utilisateurs monolocataires, seulement par les super utilisateurs. Vous pouvez toutefois trier les journaux par locataire.
- Lorsqu'un utilisateur mobile se connecte à un seul locataire Prisma Access, il consomme une unité de licence. Si un utilisateur se connecte à des locataires supplémentaires dans le cadre d'un seul déploiement multilocataire, il consomme une unité de licence pour chaque locataire auquel il est connecté. Par exemple, si un seul utilisateur est connecté à cinq locataires, l'utilisateur consomme cinq unités de licence d'utilisateur mobile au total.
- Lorsque vous utilisez la fonctionnalité multilocataire et que vous êtes connecté en tant qu'utilisateur administratif au niveau du locataire, l'ouverture du gestionnaire des tâches Panorama (en cliquant sur **Tasks (Tâches)** au bas de l'interface web de Panorama) affiche toutes les tâches pour tous les locataires, y compris les tâches effectuées au niveau du super utilisateur (administrateur).
- Certaines fonctionnalités de Prisma Access ne sont pas prises en charge pour une utilisation multilocataire. Consultez les Fonctionnalités de multilocataire non prises en charge dans la matrice de compatibilité Palo Alto Networks pour en savoir plus.

 ©2025 Palo Alto Networks, Inc.

- Si vous sauvegardez une configuration Panorama, puis que vous rétablissez une configuration antérieure enregistrée, Panorama ne peut pas rétablir la configuration que vous avez enregistrée si vous effectuez les actions suivantes dans l'ordre suivant :

  1. Sauvegarder une configuration Panorama
  2. Supprimer un locataire.
  3. Restaurer la configuration.

  Si vous supprimez un locataire, vous ne pouvez pas utiliser une sauvegarde antérieure que vous avez enregistrée avant de supprimer le locataire. Cependant, vous pouvez utiliser toutes les sauvegardes que vous faites après la suppression du locataire.

 ©2025 Palo Alto Networks, Inc.

Créer un tout nouveau déploiement multilocataire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Pour plus d'informations sur la gestion de plusieurs locataires dans Prisma Access (Managed by Strata Cloud Manager), consultez Prisma SASE.	❑ Licence Prisma Access

Si vous souhaitez créer un déploiement multilocataire et que vous ne disposez pas d'une configuration Prisma Access, vous pouvez cliquer sur **Enable Multitenancy (Activer la multilocation)** et ajouter vos locataires. Configurez ensuite les locataires après les avoir créés.

Si vous disposez d'un déploiement à locataire unique existant et que vous souhaitez migrer vers un déploiement multilocataire, utilisez le flux de travail pour activer la multilocation et migrer le premier locataire.

Lorsque vous créez le premier locataire sans configuration existante, assurez-vous des différences et des instructions suivantes à suivre :

- Puisqu'il n'y a pas de configuration à déplacer, Prisma Access crée des modèles, des piles de modèles et des groupes de périphériques pour chaque locataire et les associe au domaine d'accès que vous créez lors de la création du locataire. Consultez Présentation de la configuration multilocataire pour connaître la convention de dénomination que Prisma Access utilise.
- Si vous le souhaitez, après avoir créé le domaine d'accès au niveau du locataire, vous pouvez créer un utilisateur administrateur qui permet l'administration d'un seul locataire en associant un administrateur au domaine d'accès.
- Si vous disposez de modèles ou de groupes de périphériques existants (par exemple, des modèles d'un périphérique local géré par Panorama qui doivent également être utilisés par Prisma Access), assurez-vous d'ajouter ces groupes de périphériques et ces domaines de modèles à la zone **Access Domain (Domaine d'accès)** lorsque vous le créez et le configurez. Si vous n'ajoutez pas de groupes de périphériques et de modèles au domaine d'accès, vous ne pouvez pas les afficher ou les sélectionner lorsque vous configurez les composants Prisma Access dans le plug-in Cloud Services.

©2025 Palo Alto Networks, Inc.

Activer le multilocataire et migrer le premier locataire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Pour plus d'informations sur la gestion de plusieurs locataires dans Prisma Access (Managed by Strata Cloud Manager), reportez-vous à la page Prisma SASE.	❑ Licence Prisma Access

Utilisez le flux de travail suivant pour activer le multilocataire et migrer votre configuration existante vers le premier locataire que vous créez. Si vous n'avez aucune configuration existante, vous pouvez activer le multilocataire et ajouter vos locataires, puis les configurer.

Lorsque vous activez le multilocataire, Prisma Access migre les composants suivants de votre configuration :

- Toutes les informations de connexion au service et d'intégration du tunnel de réseau distant, y compris la configuration du tunnel.
- Les informations d'intégration pour les utilisateurs mobiles existants.
- Les informations de Strata Logging Service.
- La configuration de Autonomous DEM (ADEM) existante.
- Les modèles, les piles de modèles et les groupes d'appareils pour les connexions aux services, les réseaux distants et les utilisateurs mobiles.

Vous devez spécifier le nombre d'utilisateurs (pour un déploiement d'utilisateurs mobiles), la bande passante (pour un déploiement de réseaux distants) et le Autonomous DEM (ADEM) à allouer pour chaque déploiement (si vous avez acheté une licence ADEM).

En raison de ces modifications de groupe d'appareils, vous créez un domaine d'accès et ajoutez les groupes d'appareils, les modèles et les piles de modèles migrés, comme indiqué dans le flux de travail suivant.

Si vous n'avez pas de configuration Prisma Access existante et que vous créez un tout nouveau déploiement multilocataire, n'utilisez pas ce flux de travail ; à la place, suivez les étapes de la section Ajouter des locataires à Prisma Access pour créer le premier locataire.

 ©2025 Palo Alto Networks, Inc.

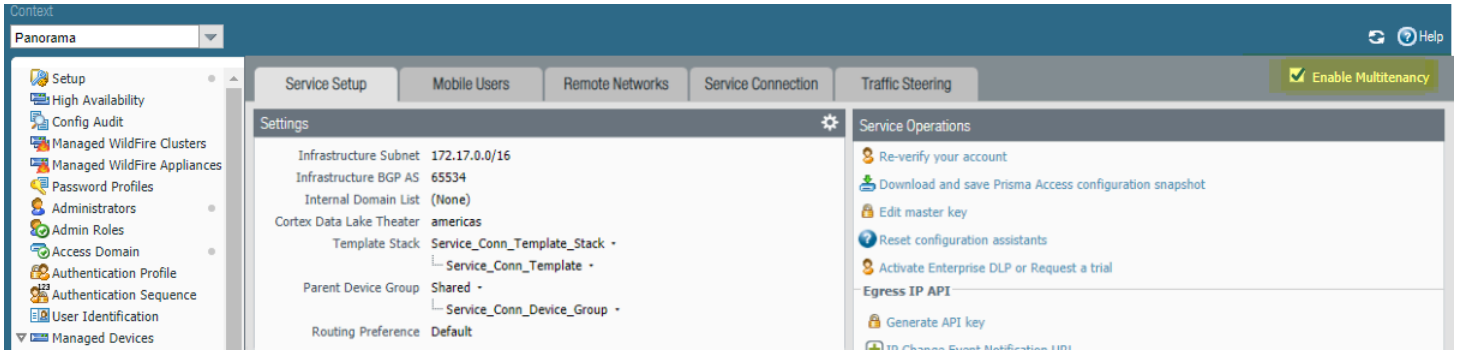
STEP 1 | Déterminez le nombre d'unités sous licence que vous souhaitez allouer à ce déploiement.

Pendant que Prisma Access migre votre configuration vers le premier locataire, vous devez spécifier :

- La **Bandwidth (Bande passante)** à allouer au déploiement des utilisateurs distants du locataire (le cas échéant).
- Les **Users (Utilisateurs)** à allouer au déploiement des utilisateurs mobiles du locataire (le cas échéant).
- Le nombre d'unités ADEM à allouer aux usages mobiles et aux réseaux distants (le cas échéant).

STEP 2 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration**.

STEP 3 | Sélectionnez **Enable Multitenancy (Activer le multilocataire)** (situé en haut à droite de la page).



Après avoir activé le multilocataire, Panorama affiche une notification vous informant que la configuration Prisma Access existante est déplacée vers le premier locataire.

Une fois que vous avez activé le multilocataire, votre déploiement devient définitivement un déploiement multilocataire et vous ne pouvez pas revenir au mode locataire unique.

STEP 4 | Cliquez sur **OK** pour migrer la configuration existante vers le premier locataire.

La page **Tenants (Locataires)** s'affiche et des graphiques circulaires au centre de la fenêtre s'affichent.

- Si vous disposez d'une licence de réseaux distants ou d'utilisateurs mobiles, la quantité disponible de bande passante de réseau distant sous licence et d'utilisateurs mobiles s'affiche.
- (Déploiements de réseaux distants et d'utilisateurs mobiles uniquement) Si vous avez acheté une licence Autonomous DEM, le nombre d'unités disponibles pour les utilisations ADEM s'affiche.
- Si vous disposez d'un déploiement Clean Pipe, la quantité de bande passante pour le locataire s'affiche.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Choisissez le type de déploiement que vous souhaitez utiliser pour le locataire.

- Pour un déploiement de réseaux distants ou d'utilisateurs mobiles, ou pour configurer les deux types de déploiements pour un locataire, sélectionnez **Remote Networks/Mobile Users (Réseaux distants/Utilisateurs mobiles)**.
- Pour un déploiement de Clean Pipe, sélectionnez **Clean Pipe**.

  Cette section décrit uniquement comment configurer les locataires pour les types de déploiements réseaux distants, utilisateurs mobiles ou réseaux distants et utilisateurs mobiles. Pour configurer le service Clean Pipe, reportez-vous à la section Prisma Access pour Clean Pipe.

 ©2025 Palo Alto Networks, Inc.

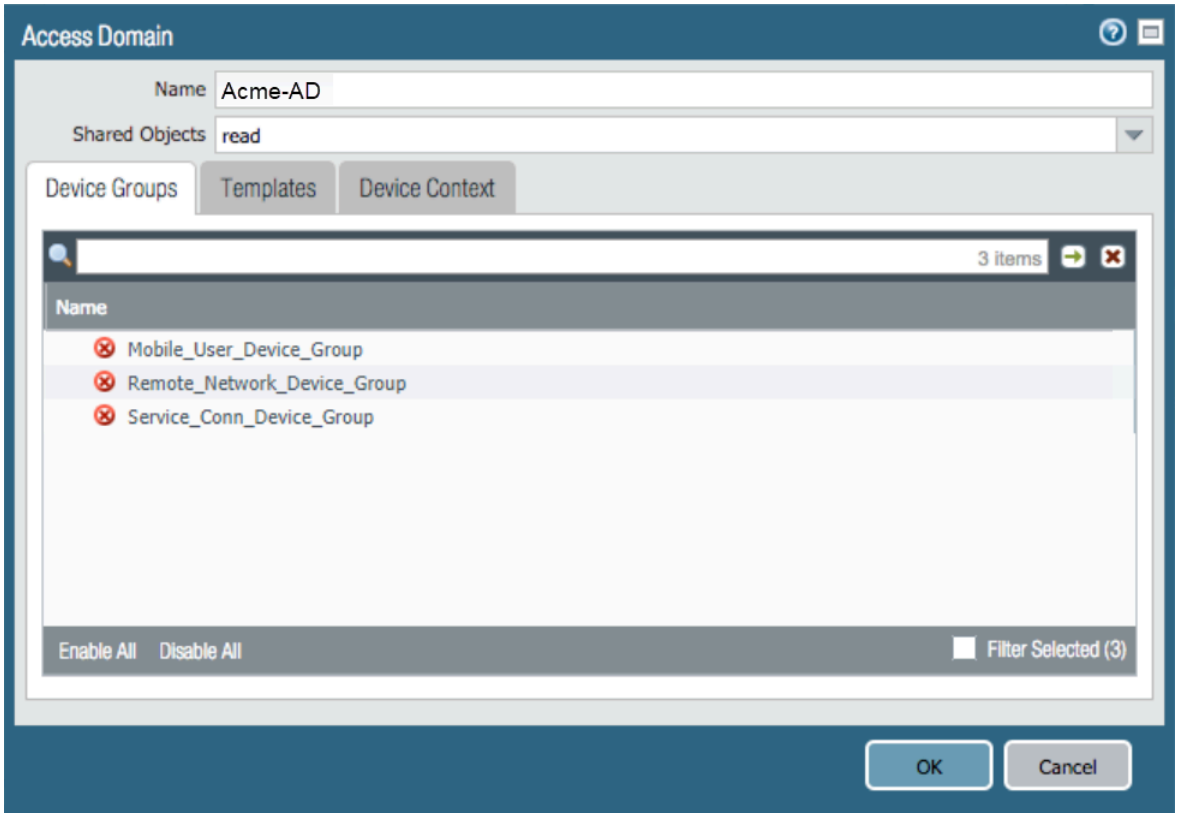
STEP 6 | Migrez la configuration existante vers le premier locataire.

Le nom du premier sous-locataire migré est automatiquement renseigné à partir du locataire que vous migrez et ne peut pas être modifié.

1. Créez un **Access Domain (Domaine d'accès)** en cliquant sur la flèche vers le bas et en sélectionnant **New Access Domain (Nouveau domaine d'accès)**.
2. Saisissez un **Name (Nom)** pour le domaine d'accès et cliquez sur **OK**.

   Prisma Access ajoute les **Device Groups (Groupes d'appareils)** **Mobile_User_Device_Group**, **Remote_Network_Device_Group** et **Service_Conn_Device_Group** au nouveau domaine d'accès.

   N'associez pas les groupes d'appareils et les modèles par défaut à d'autres sous-locataires que le premier sous-locataire migré.

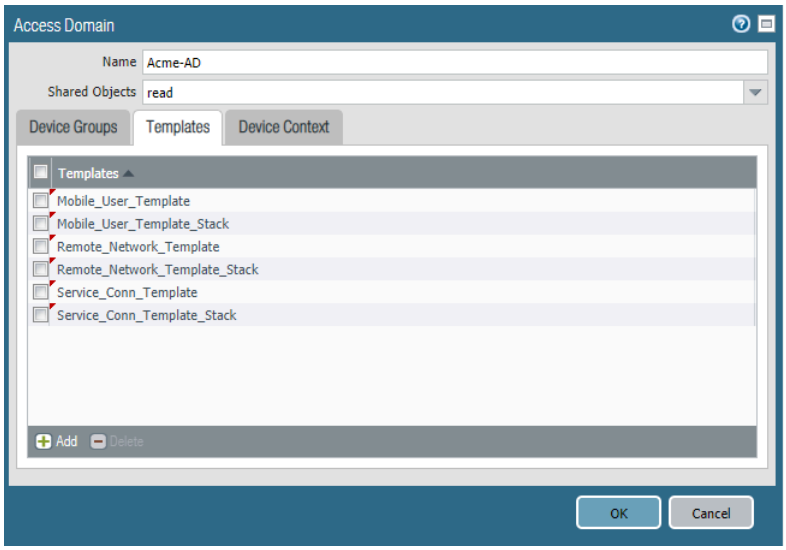


3. (Facultatif) Cliquez sur **Templates (Modèles)** pour vérifier que Prisma Access a ajouté les modèles et les piles de modèles suivants :
   - **Explicit_Proxy_Template**
   - **Explicit_Proxy_Template_Stack**
   - **Mobile_User_Template**
   - **Mobile_User_Template_Stack**
   - **Remote_Network_Template**
   - **Remote_Network_Template_Stack**
   - **Service_Conn_Template**

 ©2025 Palo Alto Networks, Inc.

- **Service_Conn_Template_Stack**

  Il s'agit des piles de modèles et des modèles par défaut pour un déploiement Prisma Access standard ; si vous avez ajouté d'autres modèles, assurez-vous que Prisma Access les a ajoutés.



4. (Facultatif) Si vous avez d'autres modèles associés à cette configuration, sélectionnez-les.
5. Cliquez sur **OK** pour fermer la page **Access Domain (Domaine d'accès)** et revenir à la page **Tenants (Locataires)**.

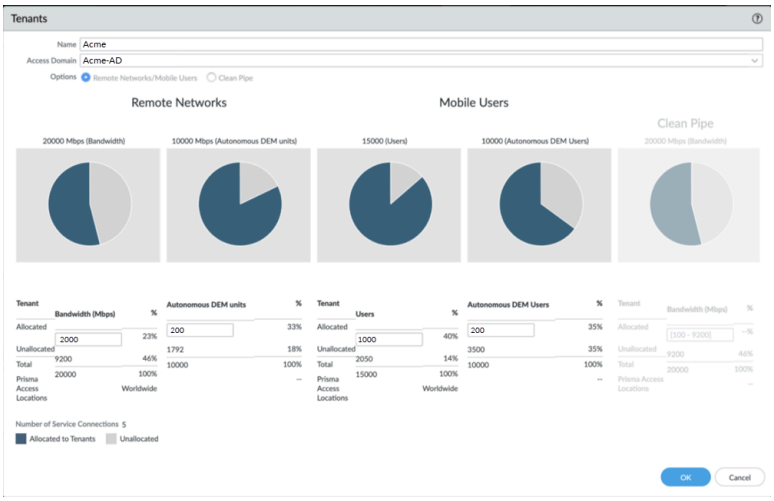
STEP 7 | Saisissez les valeurs de **Bandwidth (Mbps) (Bande passante (Mbit/s))** pour les réseaux distants, de **Users (Utilisateurs)** pour les utilisateurs mobiles et le nombre d'**Autonomous**

 ©2025 Palo Alto Networks, Inc.

DEM Users (Utilisateurs de Autonomous DEM) que vous souhaitez allouer pour chaque type de déploiement.

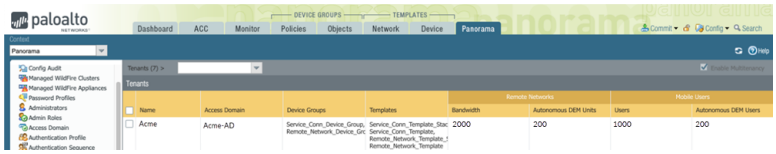
Utilisez les directives suivantes lors de l'allocation d'unités ADEM à un locataire :

- Le nombre d'unités ADEM que vous pouvez allouer aux utilisateurs mobiles et aux réseaux distants ne peut être qu'égal ou inférieur à la licence de base.
- Le nombre minimum d'unités que vous pouvez allouer est de 200.
- Après avoir alloué les unités ADEM à un locataire, vous pouvez modifier ou supprimer ces unités.
- Si vous n'avez pas acheté de licence ADEM pour votre type de déploiement (utilisateurs mobiles ou réseaux distants), ce choix est grisé.



STEP 8 | Cliquez sur **OK**.

La page **Panorama** > **Cloud Services** > **Configuration** affiche le premier locataire migré avec succès et une liste déroulante **Tenants (Locataires)** est ajoutée au-dessus de la zone **Tenants (Locataires)**.



STEP 9 | Assurez-vous que tous les modèles et groupes d'appareils ont été renseignés sur le locataire.

1. Sélectionnez le locataire dans la liste déroulante.
2. Accédez à **Panorama** > **Cloud Services** > **Configuration**.
3. Sélectionnez **Service Setup (Configuration du service)**.
4. Pour modifier les **Settings (Paramètres)**, cliquez sur l'engrenage.
5. Assurez-vous que la pile de modèles, le modèle et le groupe d'appareils corrects (Service_Conn_Template_Stack, Service_Conn_Template et Service_Conn_Device_Group, respectivement) ont été renseignés dans les paramètres.
6. Accédez aux autres onglets pour lesquels vous disposez d'une configuration existante (par exemple, **Mobile Users—GlobalProtect (Utilisateurs mobiles — GlobalProtect)**,

 ©2025 Palo Alto Networks, Inc.

Mobile Users—Explicit Proxy (Utilisateurs mobiles — Proxy explicite), **Remote Networks (Réseaux distants)** ou **Service Connection (connexion aux services)**), cliquez sur l'engrenage pour modifier les **Settings (Paramètres)** et assurez-vous que la pile de modèles, le modèle et le groupe d'appareils corrects ont été renseignés dans les paramètres.

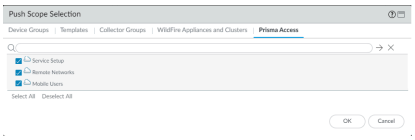
STEP 10 | Validez vos modifications localement dans Panorama (**Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.

STEP 11 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**pour enregistrer vos modifications localement sur le Panorama qui gère Prisma Access.

Si vous n'effectuez pas de validation locale, les composants Prisma Access ne s'affichent pas dans l'étendue de la transmission lorsque vous validez et transmettez vos modifications.

STEP 12 | Validez et transmettez vos modifications pour les rendre actives dans Prisma Access.

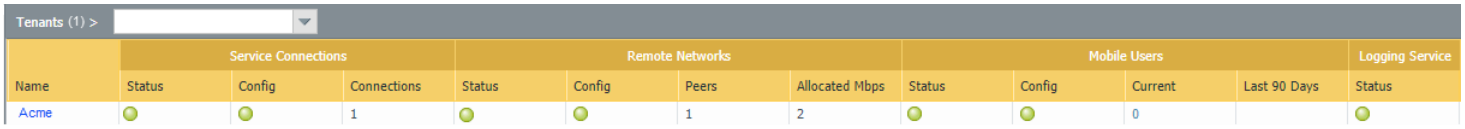
1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
2. Sélectionnez **Prisma Access**, puis sélectionnez le locataire que vous avez créé, **Service Setup (Configuration du service)**, **Remote Networks (Réseaux distants)** et **Mobile Users (Utilisateurs mobiles)**.



3. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.
4. **Commit (Validez)** et **Push (Transmettez)** vos modifications.

STEP 13 | Sélectionnez **Panorama** > **Cloud Services** > **Status (État)**.

La page d'état affiche l'état de tous les locataires. Étant donné que vous n'avez créé qu'un seul locataire, ce locataire est le seul qui s'affiche. Si vous sélectionnez ce locataire dans la liste déroulante, vous affichez un état détaillé de ce locataire.



La sélection d'un locataire dans la liste déroulante vous renvoie à la page Status (État) de ce locataire.

STEP 14 | Continuez à ajouter plus de locataires à Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Ajouter des locataires à Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Pour en savoir plus sur la gestion de plusieurs locataires dans Prisma Access (Managed by Strata Cloud Manager), consultez Prisma SASE.	❑ Licence Prisma Access

Après avoir migré les informations existantes en tant que premier locataire, vous pouvez créer et configurer des locataires supplémentaires. Pour chaque locataire que vous créez après le premier, Prisma Access crée un domaine d'accès distinct avec son propre ensemble de piles de modèles et de modèles, et ses propres groupes de domaines.

Utilisez ce flux de travail pour ajouter plus de locataires à Prisma Access.

Si vous créez un tout nouveau déploiement multilocataire, utilisez ce workflow pour ajouter le premier locataire ainsi que des locataires supplémentaires. Pour plus d'informations, reportez-vous à la section Créer un tout nouveau déploiement multilocataire.

STEP 1 | Connectez-vous à Panorama en tant que super utilisateur.

STEP 2 | Ajoutez et configurez le locataire.

1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration**, puis **Add (Ajouter)** pour ajouter un nouveau locataire.

   Veillez à sélectionner **Remote Networks/Mobile Users (Réseaux distants / Utilisateurs mobiles)** ; pour créer et configurer un déploiement Clean Pipe, consultez Prisma Access pour Clean Pipe.
2. Donnez un **Name (Nom)** descriptif au locataire.
3. Sélectionnez **Add (Ajouter)** pour ajouter un nouvel **Access Domain (Domaine d'accès)**, donnez-lui un nom descriptif dans **Name (Nom)**, puis cliquez sur **OK** pour revenir à la fenêtre **Tenants (Locataires)**.

   Une fois que vous avez cliqué sur **OK**, Prisma Access crée automatiquement des modèles, des piles de modèles et des groupes de périphériques et les associe au domaine d'accès que vous créez.

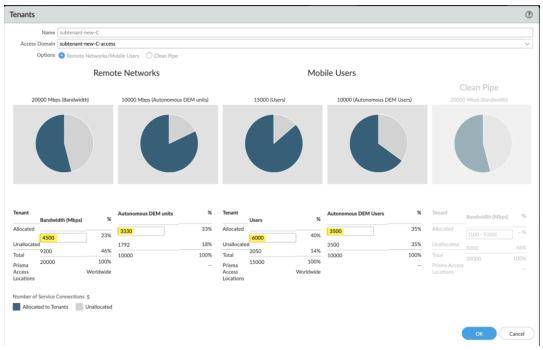
STEP 3 | Dans **Bandwidth (Mbps) (Bande passante (Mbit/s))**, indiquez la quantité de bande passante à allouer aux **Remote Networks (Réseaux distants)**. Dans **Users (Utilisateurs)**, indiquez le nombre d'utilisateurs à allouer aux **Mobile Users (Utilisateurs mobiles)**.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | (Déploiements avec Autonomous DEM uniquement) Si vous avez acheté une licence Autonomous DEM (ADEM), sélectionnez le nombre d'unités à allouer à ADEM.

Utilisez les lignes directrices suivantes lors de l'allocation d'unités ADEM à un locataire :

- Le nombre d'unités ADEM que vous pouvez allouer aux utilisateurs mobiles et aux réseaux distants doit être égal ou inférieur à la licence de base.
- Vous devez allouer au minimum 200 unités.
- Après avoir attribué des unités ADEM à un locataire, vous pouvez modifier ou supprimer ces unités.
- Si vous n'avez pas acheté de licence ADEM pour votre type de déploiement (utilisateurs mobiles ou réseaux distants), ce choix est grisé.

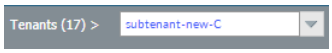


STEP 5 | Cliquez sur **OK** pour créer le premier locataire.

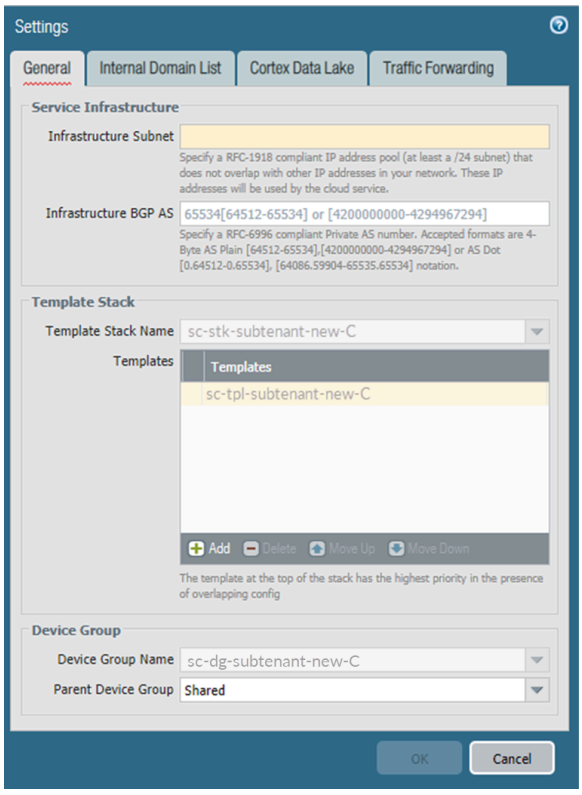
 ©2025 Palo Alto Networks, Inc.

STEP 6 | Vérifiez que Prisma Access a appliqué les paramètres de service de pile de modèles, de modèle et de groupe de périphériques aux paramètres de connexion aux services du locataire que vous venez de créer.

1. Sélectionnez le client que vous avez créé dans la liste déroulante **Tenant (Locataire)**.



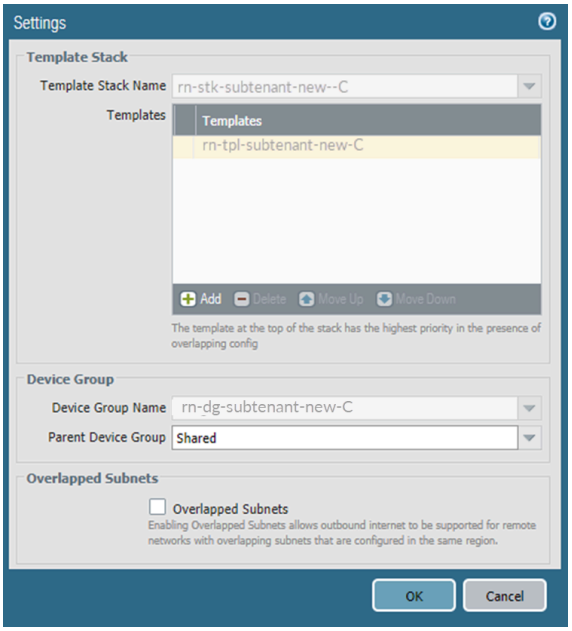
2. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)**.
3. Cliquez sur l'icône d'engrenage à droite de la zone **Settings (Paramètres)** pour modifier les paramètres.
4. Vérifiez que Prisma Access a associé la pile de modèles (**sc-stk-***tenant* (locataire)), le modèle (**sc-tpl-***tenant* (locataire)) et le groupe de périphériques (**sc-dg-***tenant* (locataire)) à vos paramètres de connexion aux services.
5. Veillez à ce que le **Parent Device Group (Groupe de périphériques parent)** soit défini sur **Shared (Partagé)**, puis cliquez sur **OK**.



 ©2025 Palo Alto Networks, Inc.

STEP 7 | Vérifiez que Prisma Access a appliqué la pile de modèles, le modèle et le groupe de périphériques aux paramètres de réseau distant.

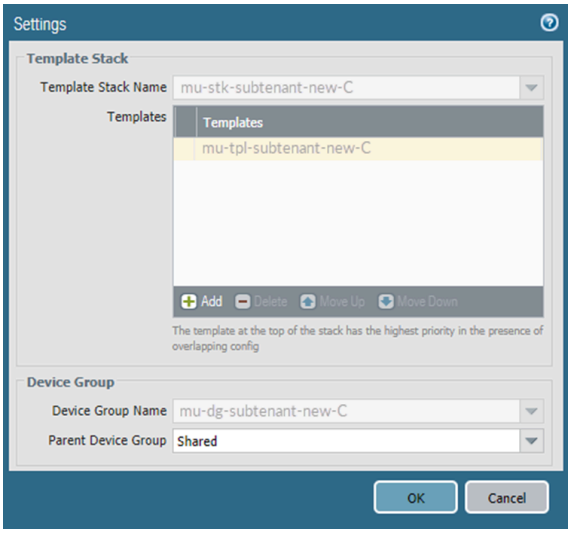
1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** et cliquez sur l'icône d'engrenage à droite de la zone **Settings (Paramètres)** pour modifier les paramètres.
2. Vérifiez que Prisma Access a associé la pile de modèles (**rn-stk-***tenant* (locataire)), le modèle (**rn-tpl-***tenant* (locataire)) et le groupe de périphériques (**rn-dg-***tenant* (locataire)) aux paramètres de réseau distant.
3. Veillez à ce que le **Parent Device Group (Groupe de périphériques parent)** soit défini sur **Shared (Partagé)**, puis cliquez sur **OK**.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | Vérifiez que Prisma Access a appliqué la pile de modèles, le modèle et le groupe de périphériques aux paramètres d'utilisateur mobile.

1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users (Utilisateurs mobiles)** et cliquez sur l'icône d'engrenage à droite de la zone **Settings (Paramètres)** pour modifier les paramètres.
2. Vérifiez que Prisma Access a associé la pile de modèles (**mu-stk-***tenant* (locataire)), le modèle (**mu-tpl-***tenant* (locataire)) et le groupe de périphériques (**mu-dg-***tenant* (locataire)) aux paramètres de réseau distant.
3. Veillez à ce que le **Parent Device Group (Groupe de périphériques parent)** soit défini sur **Shared (Partagé)**, puis cliquez sur **OK**.



STEP 9 | Validez vos modifications localement sur Panorama (**Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.

STEP 10 | (Déploiements d'utilisateurs mobiles uniquement) – Ajoutez un sous-réseau d'infrastructure, puis validez et transmettez vos modifications pour les rendre actives dans Prisma Access.

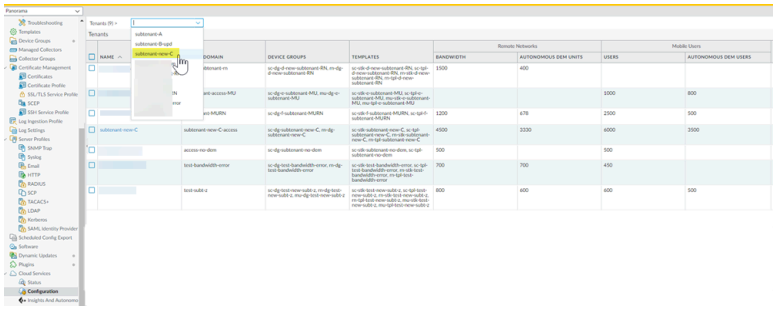
Ces étapes sont nécessaires pour que les modifications apportées aux utilisateurs mobiles prennent effet.

1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)**, cliquez sur l'icône d'engrenage pour modifier les paramètres, puis configurez un sous-réseau d'infrastructure.
2. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et transmettre)**, **Edit Selections (Modifier les sélections)** dans l'étendue de la transmission et veillez à ce que **Mobile Users (Utilisateurs mobiles)** soit sélectionné.
3. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.
4. Sélectionnez **Commit (Valider)** et **Push (Pousser)** pour valider et transmettre les modifications.

 ©2025 Palo Alto Networks, Inc.

STEP 11 | Sélectionnez le nouveau locataire que vous avez créé en sélectionnant **Panorama** > **Cloud Services** > **Configuration** > ***tenant-name*** **(nom du locataire)** et continuez la configuration du locataire.

1. Configurez l'infrastructure de service.
2. Créez une connexion aux services pour autoriser l'accès aux applications privées.
3. Intégrez et configurez des réseaux distants si vous disposez d'une licence pour les réseaux distants.
4. Configurez GlobalProtect pour Prisma Access (Managed by Panorama) si vous disposez d'une licence pour les utilisateurs distants.



 ©2025 Palo Alto Networks, Inc.

Supprimer un locataire

Supprimez un locataire dans un déploiement Prisma Access (Managed by Panorama) en suivant les étapes suivantes.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Pour plus d'informations sur la gestion de plusieurs locataires dans Prisma Access (Managed by Strata Cloud Manager), consultez Prisma SASE.	❑ Licence Prisma Access

- *Bien que vous puissiez supprimer tous les locataires dans un déploiement multilocataire, vous ne pouvez pas supprimer la configuration Prisma Access au niveau administrateur où vous ajoutez ou supprimez des locataires.*
- *Lorsque vous supprimez un locataire, Prisma Access supprime le modèle et le groupe de périphériques pour lesquels vous disposez d'une licence, mais ne supprime pas l'ensemble sans licence. Par exemple, si vous avez un Prisma Access pour les utilisateurs sous licence et si vous supprimez un locataire, Prisma Access supprime les piles de modèles, les modèles et les groupes de périphériques liés à l'utilisateur mobile, mais ne supprime pas l'ensemble qu'il a créé pour les périphériques sans licence Prisma Access pour les réseaux. Vous pouvez supprimer manuellement ces ensembles de modèles et de groupes de périphériques inutilisés après avoir supprimé le locataire.*

STEP 1 | À partir du Panorama qui gère Prisma Access, sélectionnez **Panorama** > **Cloud Services** > **Configuration**.

STEP 2 | Sélectionnez le locataire et supprimez toute la configuration qui lui est associée.

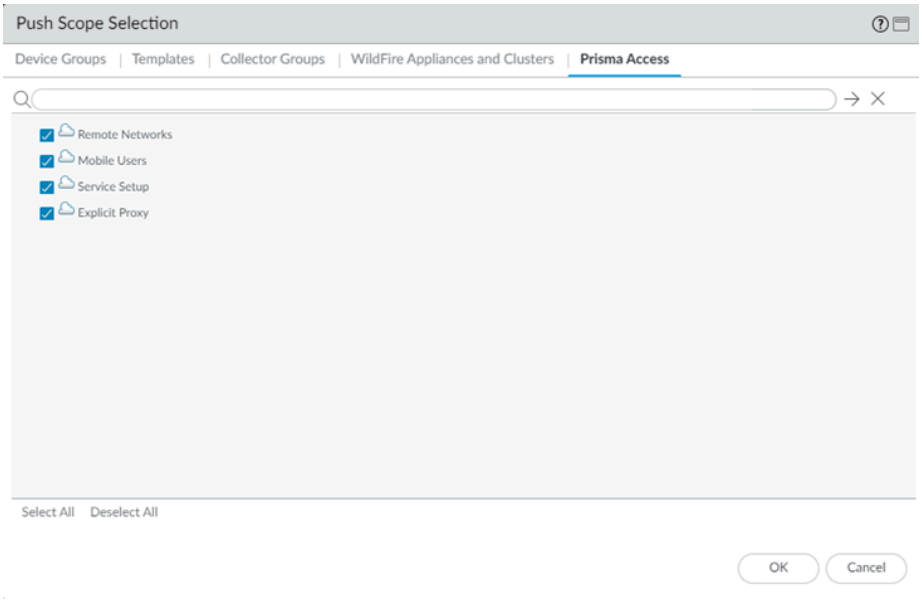
Effectuez cette étape en tant que meilleure pratique pour vous assurer que toute la configuration est supprimée du locataire, y compris toute configuration de connexion aux services, d'utilisateur mobile, de réseau distant ou de Clean Pipe.

STEP 3 | Validez et appliquez vos modifications apportées à Prisma Access.

1. Sélectionnez **Commit (valider)** > **Push to Devices (Appliquer aux périphériques)**.
2. Cliquez sur **Edit Selections (Modifier les sélections)** et assurez-vous que tous les composants que vous avez supprimés (y compris les réseaux distants, les utilisateurs

 ©2025 Palo Alto Networks, Inc.

mobiles, la configuration du service, le proxy explicite et Clean Pipe, selon votre déploiement) sont sélectionnés.



3. Cliquez sur **Push (Transmettre)**.

STEP 4 | Sélectionnez un ou plusieurs locataires, puis appuyez sur **Delete (Supprimer)** pour les supprimer.

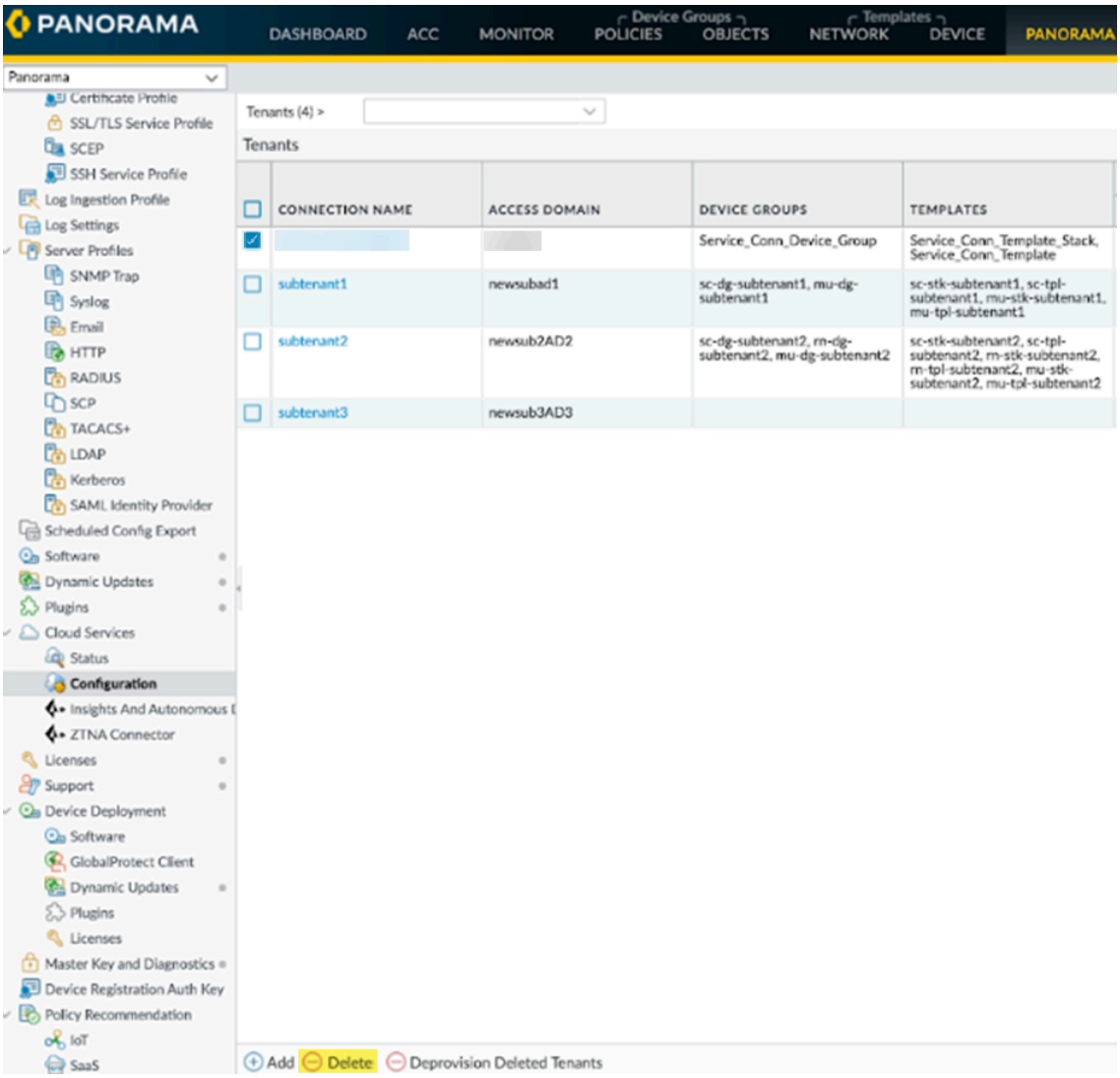
La suppression d'un locataire supprime le locataire de Panorama, mais ne supprime pas le locataire de l'infrastructure Prisma Access. Pour supprimer un locataire et le

 ©2025 Palo Alto Networks, Inc.

retirer de l'infrastructure, supprimez-le, effectuez une validation locale, puis annulez son provisionnement comme indiqué dans les étapes suivantes.

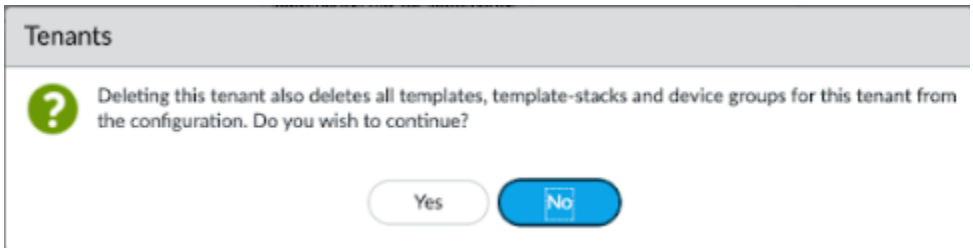
Si vous supprimez le locataire, mais ne le déprovisionnez pas, vous pouvez toujours le récupérer en contactant le support de Palo Alto Networks.

Si vos Panoramas sont configurés dans une configuration HA, effectuez uniquement les opérations de suppression et de déprovisionnement du Panorama actif dans une paire HA.



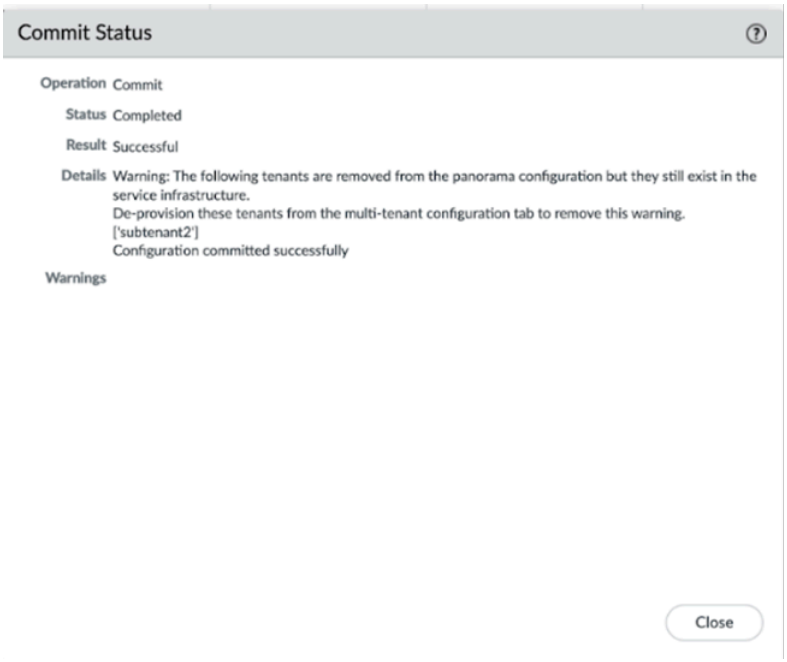
Une fenêtre contextuelle s'affiche, confirmant le processus de suppression du locataire. Cliquez sur **Yes (Oui)** pour continuer ou sur **No (Non)** pour annuler la suppression.

 ©2025 Palo Alto Networks, Inc.



STEP 5 | Validez vos modifications localement dans Panorama en sélectionnant **Commit (Valider)** > **Commit to Panorama (Valider dans Panorama)** et cliquez sur **Commit (Valider)** pour valider vos modifications.

Après la validation locale, les locataires sont marqués pour suppression et sont supprimés de la liste des locataires, mais ne sont pas supprimés de l'infrastructure Prisma Access. Une fenêtre contextuelle s'affiche indiquant les locataires supprimés.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | (Facultatif) Pour supprimer complètement les locataires de l'infrastructure Prisma Access, cliquez sur **Deprovision Deleted Tenants (Déprovisionner les locataires supprimés)**.

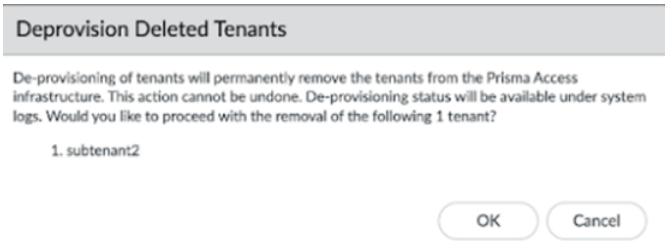
Déprovisionnement d'un locataire :

- Le supprime de votre configuration et de l'infrastructure Prisma Access, et vous ne pouvez pas le récupérer.
- Récupère la licence qui a été attribuée au locataire.



Un message de confirmation s'affiche avec les noms des locataires qui seraient déprovisionnés. Cliquez sur **OK** pour continuer le déprovisionnement du locataire ou sur **Cancel (Annuler)** pour annuler l'opération.

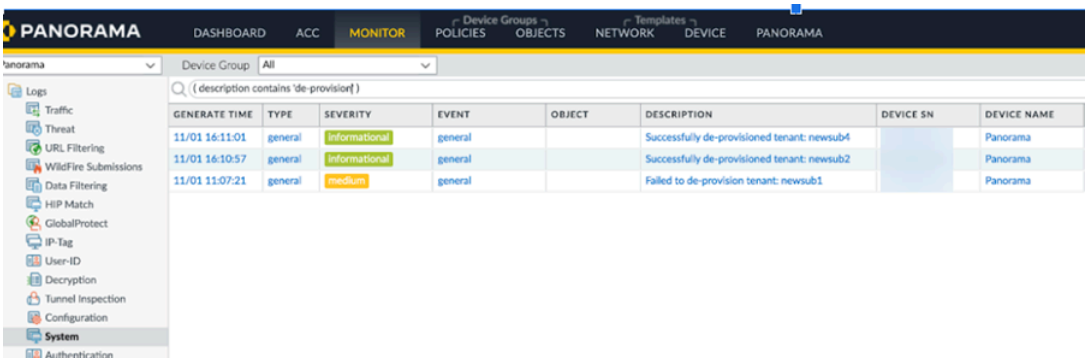
Lorsque vous annulez l'approvisionnement d'un locataire, vous supprimez complètement le locataire et toutes les ressources qui lui sont allouées, et vous récupérez les licences qui ont été allouées à ces locataires. Le locataire ne peut pas être récupéré.



Si aucun locataire ne doit être déprovisionné, le message suivant s'affiche.



STEP 7 | (Facultatif) Vérifiez l'état de l'opération de déprovisionnement en accédant à **Monitor (Surveiller)** > **Logs (Journaux)** > **System (Système)**. L'opération de déprovisionnement et le nom du locataire sont affichés dans les journaux.



 ©2025 Palo Alto Networks, Inc.

Créer un utilisateur administrateur au niveau du locataire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Pour plus d'informations sur la gestion de plusieurs locataires dans Prisma Access (Managed by Strata Cloud Manager), reportez-vous à la page Prisma SASE.	❑ Licence Prisma Access

Vous devez créer un utilisateur administrateur pour chaque locataire. De cette façon, un administrateur au niveau du locataire peut afficher et apporter des modifications à la configuration de son locataire, mais n'a pas accès aux autres locataires. Pour créer un utilisateur administrateur pour un locataire spécifique, effectuez la tâche suivante. Pour plus d'informations sur le contrôle d'accès basé sur les rôles (RBAC) pour les utilisateurs administrateur au niveau du locataire, consultez Contrôler l'accès basé sur les rôles pour les utilisateurs administrateur au niveau du locataire.

*Les utilisateurs qui gèrent des locataires uniques ne peuvent pas voir les journaux système, car l'option **Monitor (Surveiller)** > **Logs (Journaux)** > **System (Système)** n'est pas disponible. Cette limitation s'applique à tous les administrateurs qui ont un rôle administrateur **Device Group and Template (Groupe de périphériques et modèle)**. Seuls les super utilisateurs peuvent afficher les journaux système en mode multilocation.*

 ©2025 Palo Alto Networks, Inc.

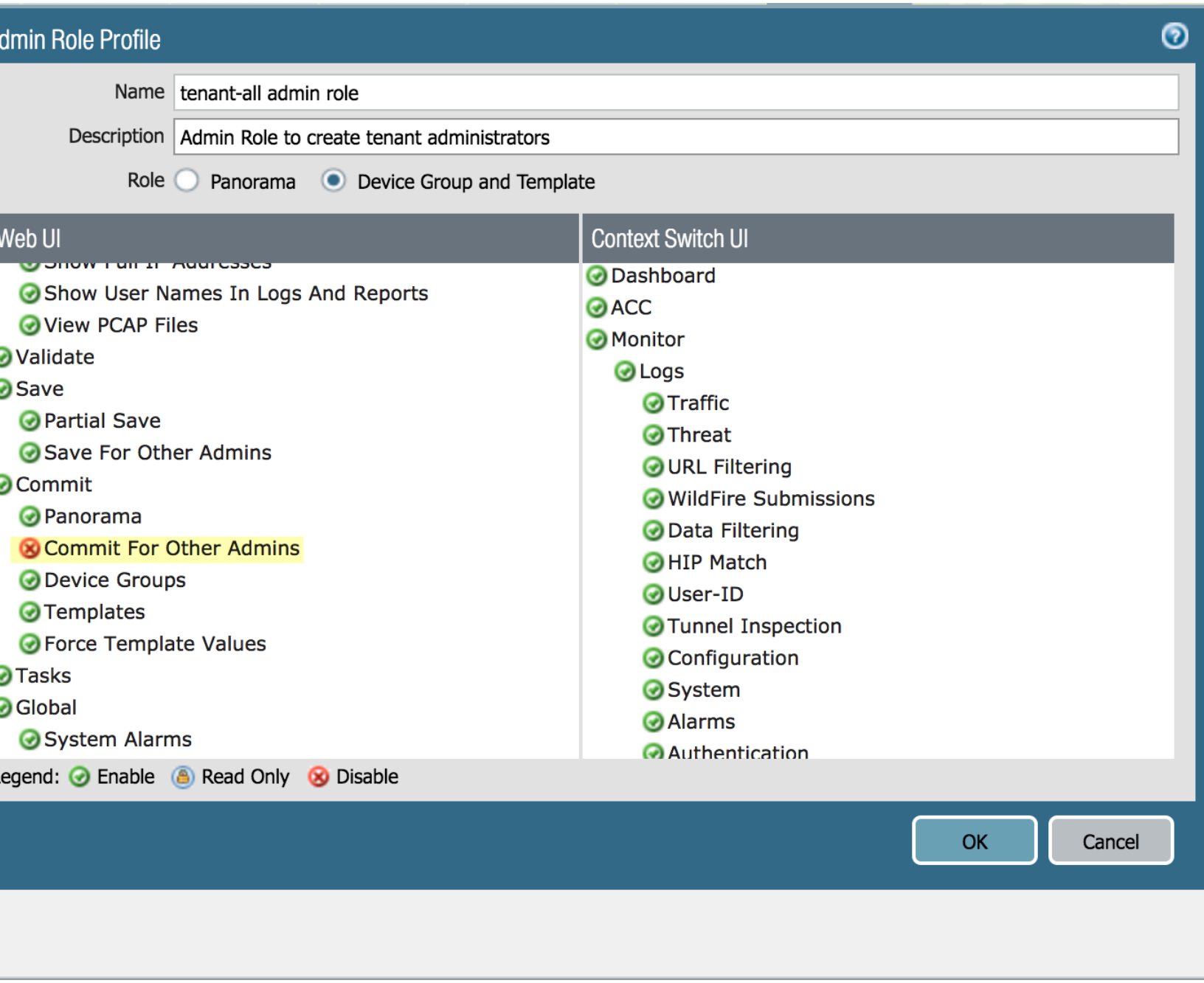
STEP 1 | Créez un rôle administrateur avec un type **Device Group and Template (Groupe de périphériques et modèle)**.

1. Sélectionnez **Panorama** > **Admin Roles (Rôles administrateur)**.
2. Cliquez sur **Add (Ajouter)** pour ajouter un profil de rôle administrateur avec un **Role (Rôle) Device Group and Template (Groupe de périphériques et modèle)**.
3. Cliquez sur **OK**.

Vous pouvez créer un seul profil de rôle administrateur et le partager entre plusieurs locataires. Toutefois, vous devez créer un administrateur distinct pour chaque locataire.

*Bien que vous adaptiez le rôle administrateur aux besoins de votre organisation, nous vous recommandons de désélectionner **Commit for Other Admins (Valider pour les autres administrateurs)**. La désélection de cette option permet à un utilisateur au niveau du locataire de valider uniquement les modifications qu'il a apportées et l'empêche de valider involontairement d'autres modifications que d'autres utilisateurs administrateur au niveau du locataire ont effectuées et qui ne sont pas encore validées.*

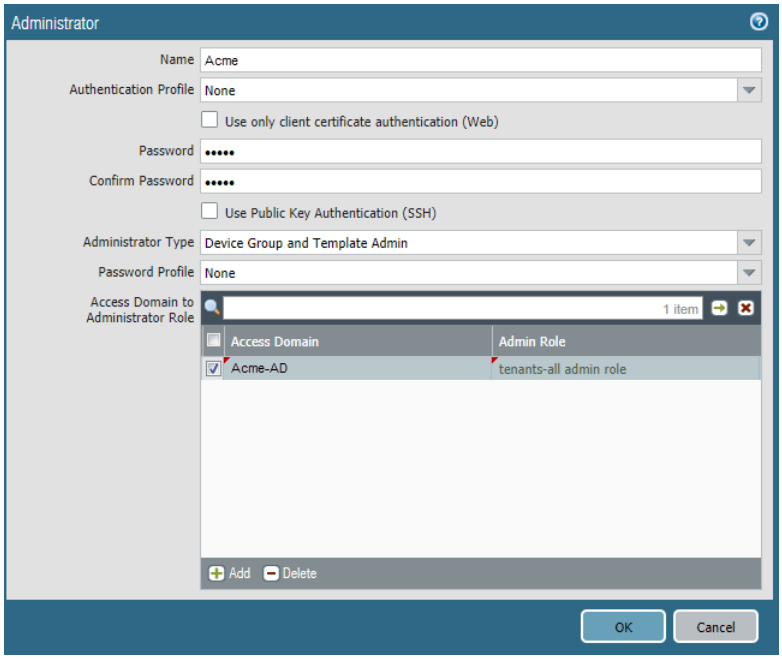
 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Créez et configurez un administrateur pour le locataire.

1. Sélectionnez **Panorama** > **(Administrateurs)**.
2. Cliquez sur **Add (Ajouter)** pour ajouter un administrateur.
3. Saisissez et confirmez un **Password (Mot de passe)** pour le nouvel administrateur.
4. Spécifiez un **Administrator Type (Type d'administrateur) Device Group and Template Admin (Administrateur du groupe de périphériques et du modèle)**.
5. Spécifiez la valeur **Access Domain (Domaine d'accès)** qui est associée aux groupes de périphériques de ce locataire.
6. Spécifiez la zone **Admin Role (Rôle administrateur)** que vous avez créée à l'étape 1 pour le locataire.



STEP 3 | Cliquez sur **OK**.

STEP 4 | Répétez les étapes 2 et 3 pour ajouter des utilisateurs supplémentaires afin de gérer vos locataires selon les besoins.

STEP 5 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

 ©2025 Palo Alto Networks, Inc.

Contrôler l'accès basé sur les rôles pour les utilisateurs administrateur au niveau du locataire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Pour en savoir plus sur la gestion de plusieurs locataires dans Prisma Access (Managed by Strata Cloud Manager), consultez Prisma SASE.	❑ Licence Prisma Access

Si vous gérez un déploiement multilocataire, vous pouvez utiliser le contrôle d'accès basé sur les rôles (RBAC) pour créer des utilisateurs administrateur au niveau du locataire.

Pour modifier l'accès au niveau RBAC pour les utilisateurs administrateur au niveau du locataire dans Panorama, vous devez créer un utilisateur administrateur au niveau du locataire et utiliser un profil de rôle administrateur avec un **Role (Rôle)** de **Device Group and Template (Groupe de périphériques et modèle)**, puis cliquez sur **Enable (Activer)**, **Disable (Désactiver)**, ou donnez un accès **Read Only (Lecture seule)** aux zones du **Web UI (Interface utilisateur Web)** Panorama. Utilisez cette méthode pour gérer l'accès à tous les composants Panorama pour les utilisateurs au niveau du locataire, à l'exception de l'accès au plug-in Cloud Services dans lequel vous gérez Prisma Access.

Si vous souhaitez empêcher un utilisateur au niveau du locataire de configurer les composants Prisma Access dans Panorama, vous ne pouvez pas utiliser les rôles administrateur. Pour interdire aux utilisateurs de configurer Prisma Access, vous devez empêcher l'utilisateur d'accéder au plug-in Cloud Services, ce qui l'empêche également de le consulter. À l'aide de cette méthode, vous pouvez créer un utilisateur administratif pour un professionnel de la sécurité qui est autorisé à apporter des modifications aux politiques de sécurité et à envoyer ces modifications à Panorama, mais qui ne peut pas afficher ou apporter des modifications à la configuration de Prisma Access.

Vous pouvez activer ou désactiver l'accès au plug-in Cloud Services pour un utilisateur, mais vous ne pouvez pas lui accorder un accès en lecture seule. Si un utilisateur a accès à l'affichage du plug-in Cloud Services, il peut également apporter des modifications de configuration à ses composants, notamment Prisma Access.

Le tableau suivant présente des exemples de rôles administrateur au niveau du locataire et les étapes à suivre pour créer ces rôles.

Exemple de configuration au niveau du locataire	Tâche de configuration
Créez un utilisateur axé sur le réseautage qui : • Peut modifier les configurations des plug-ins • Peut valider sur Panorama	Créez un utilisateur administrateur au niveau du locataire, en activant les autorisations **Save (Enregistrer)** et **Commit (Valider)** dans **Admin Role Profile (Profil de rôle administrateur)**, et en désactivant ou activant le mode **Read Only (Lecture seule)** de toutes les autorisations que vous ne souhaitez pas

 ©2025 Palo Alto Networks, Inc.

Exemple de configuration au niveau du locataire	Tâche de configuration
• Peut transmettre la configuration à Prisma Access	que l'utilisateur administrateur au niveau du locataire possède.
Créez un utilisateur axé sur la sécurité qui : • Peut afficher et modifier les politiques de sécurité • Peut valider sur Panorama • Ne peut pas voir ou apporter des modifications au plug-in Cloud Services • Ne peut pas transmettre la configuration à Prisma Access (nécessite que le super utilisateur transmette la configuration)	Pour empêcher un utilisateur administrateur au niveau du locataire d'afficher ou d'accéder au plug-in, supprimez l'accès au plug-in pour un administrateur au niveau du locataire. Pour toutes les autres autorisations liées à Panorama, modifiez les autorisations du rôle administrateur pour l'utilisateur.
Créez un utilisateur hybride qui : • Dispose d'un accès en lecture seule au plug-in Cloud Services • Dispose d'un accès en lecture-écriture à la politique de sécurité • Ne peut pas transmettre la configuration à Prisma Access (nécessite que le super utilisateur transmette la configuration)	Cette configuration n'est pas possible. Vous ne pouvez pas activer le mode Lecture seule du plug-in Cloud Services. Vous pouvez uniquement fournir l'accès aux utilisateurs administrateur pour qu'ils puissent l'afficher et l'utiliser pour apporter des modifications de configuration, ou leur interdire de l'afficher.

Supprimer l'accès au plug-in pour un utilisateur administrateur de niveau locataire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Pour plus d'informations sur la gestion de plusieurs locataires dans Prisma Access (Managed by Strata Cloud Manager), consultez Prisma SASE.	☐ Licence Prisma Access

Dans les configurations multilocataires normales, vous utilisez des domaines d'accès Ajouter des locataires à Prisma Access et associez chaque domaine d'accès à un locataire. Pour empêcher un utilisateur administratif de niveau locataire d'afficher ou d'apporter des modifications de configuration à Prisma Access, vous créez un domaine d'accès, mais vous ne l'associez pas à un locataire.

 ©2025 Palo Alto Networks, Inc.

Étant donné que vous avez associé le domaine d'accès aux groupes de périphériques et aux piles de modèles pour le locataire, l'utilisateur administratif de niveau locataire dispose d'un accès RBAC au niveau du locataire et ne peut effectuer la configuration que pour ce locataire. Étant donné que vous n'avez pas associé le domaine d'accès à un locataire dans Prisma Access, le domaine d'accès ne peut pas afficher le plug-in Cloud Services, qui permet d'accéder à Prisma Access. De cette façon, vous créez un utilisateur qui peut effectuer des tâches de configuration au niveau du locataire sans pouvoir accéder, afficher ou apporter des modifications de configuration à Prisma Access.

Pour supprimer Prisma Access pour un utilisateur de niveau administratif, effectuez la tâche suivante.

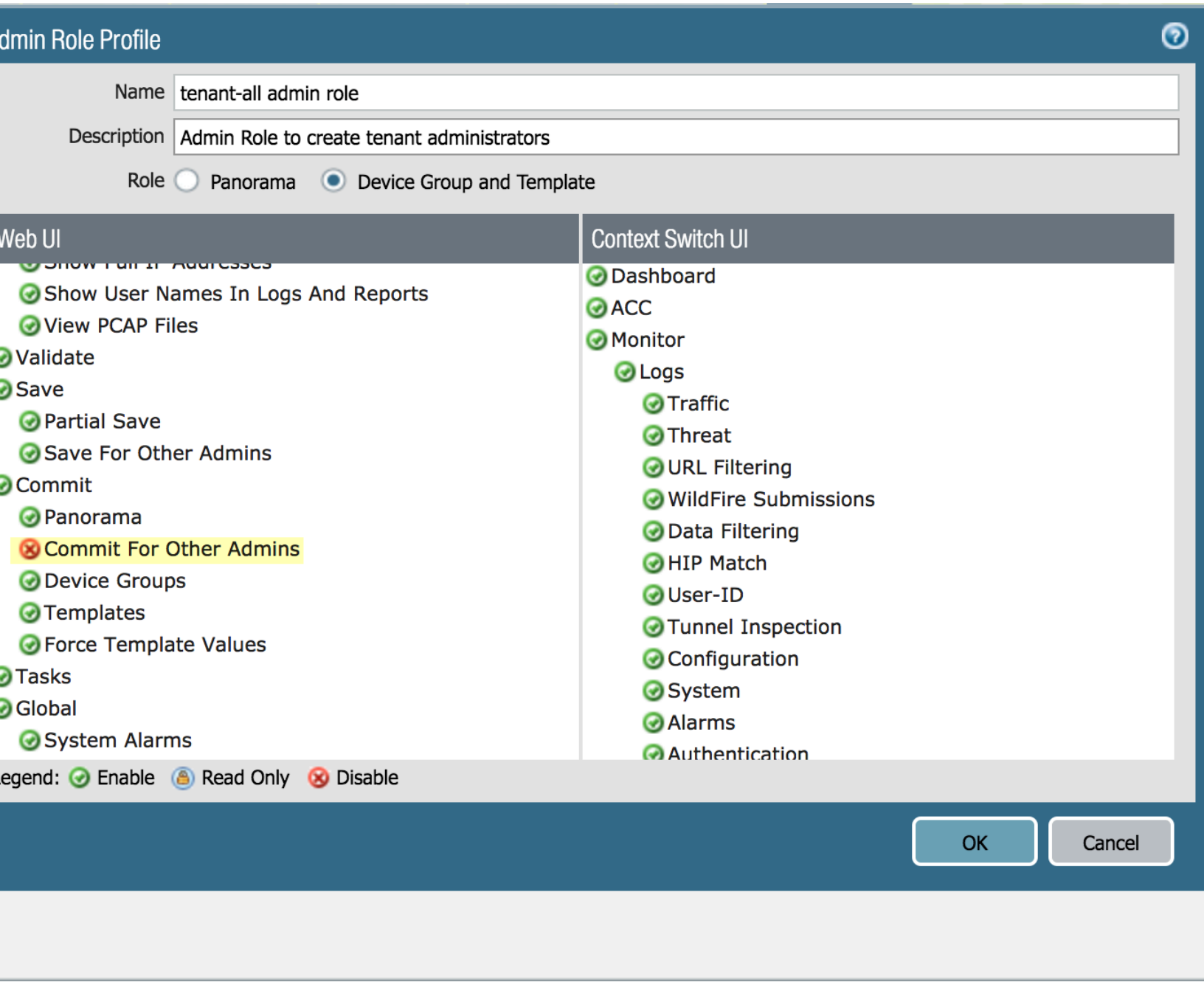
Cette tâche suppose que vous avez des Ajouter des locataires à Prisma Access *modèles, piles de modèles et groupes de périphériques pour le locataire ; vous les associerez à l'utilisateur administratif de niveau locataire.*

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Créez un rôle administratif avec un type de **Device Group and Template (Groupe de périphériques et modèle)**.

1. Sélectionnez **Panorama** > **Admin Roles (Rôles d'administrateur)**.
2. **Add (Ajouter)** un profil de rôle d'administrateur avec un **Role (Rôle)** de **Device group and Template (Groupe de périphériques et modèle)**.
3. Cliquez sur **OK**.

   Vous pouvez créer un profil de rôle d'administrateur unique et le partager entre plusieurs locataires.

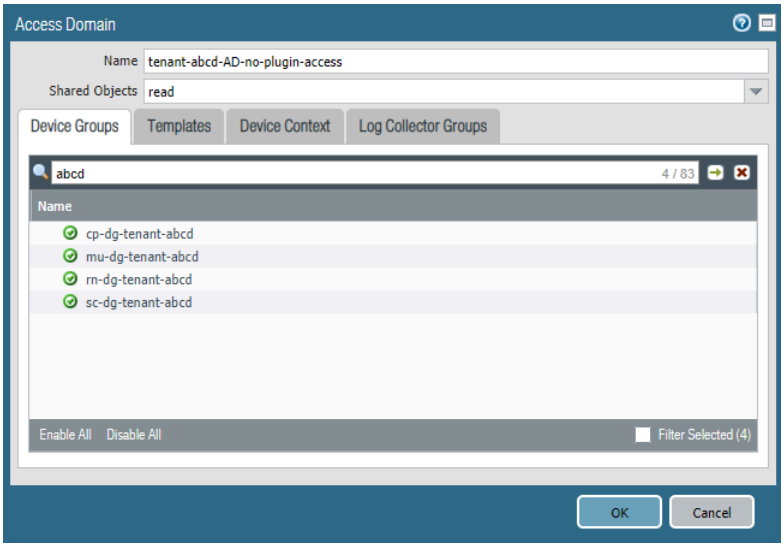


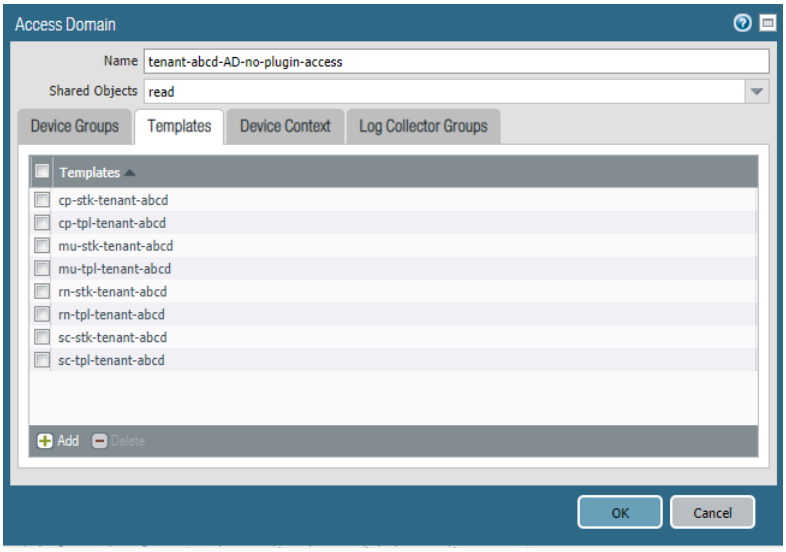
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Sélectionnez **Panorama** > **Access domain (Domaine d'accès)** et **Add (Ajouter)** un Domaine d'accès.

STEP 3 | Spécifiez les **Device Groups (Groupes de périphériques)** et **Templates (Modèles)** associés au locataire.

*Si vous avez créé des groupes de périphériques qui sont des enfants ou des petits-enfants d'autres groupes de périphériques sous le groupe de périphériques parent **Shared (Partagé)**, sélectionnez uniquement le groupe de périphériques au niveau hiérarchique le plus bas (enfant ou petit-enfant) ; ne sélectionnez pas le parent, sinon vous aurez des erreurs lors de la validation.*



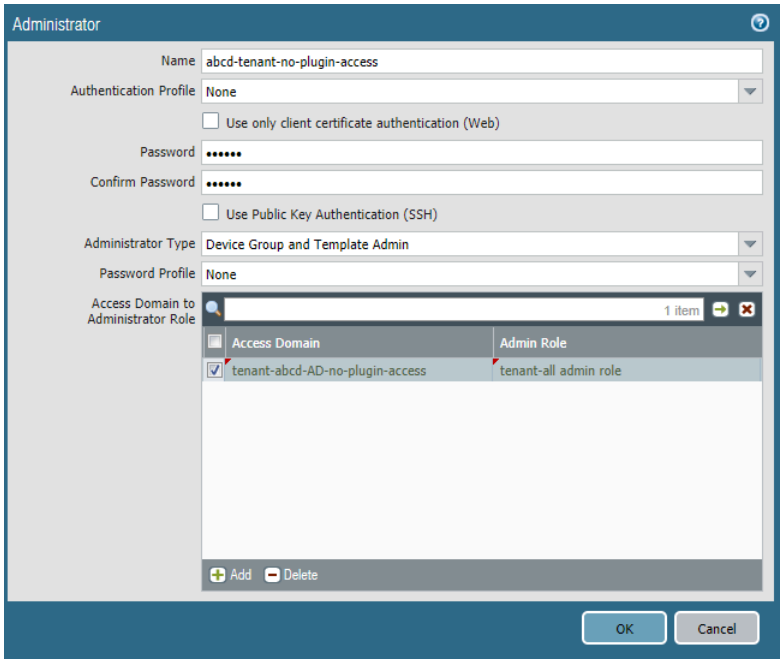


 ©2025 Palo Alto Networks, Inc.

STEP 4 | Créez et configurez un Administrateur pour l'utilisateur administratif au niveau du locataire, en spécifiant le domaine d'accès que vous venez de créer.

1. Sélectionnez **Panorama** > **(Administrateurs)**.
2. **Add (Ajouter)** un administrateur.
3. Saisissez et confirmez un **Password (Mot de passe)** pour le nouvel administrateur.
4. Spécifiez un **Administrator Type (Type d'administrateur)** du **Device Group and Template Admin (Administrateur de groupe de périphériques et modèle)**.
5. Spécifiez le **Access Domain (Domaine d'accès)** qui est associé aux groupes de périphériques de ce locataire.
6. Spécifiez le **Admin Role (Rôle d'administrateur)** que vous avez créé à l'étape 1 pour le locataire.

   Lorsque vous terminez cet exemple, le **abcd-tenant-no-plugin-access** L'utilisateur administratif disposera d'autorisations basées sur ce que vous avez défini dans le profil de rôle d'administrateur, mais ne pourra pas afficher ou configurer le plug-in Cloud Services (y compris Prisma Access). Notez toutefois qu'ils ne pourront pas appliquer les modifications qu'ils apportent au cloud.



STEP 5 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** et **Commit (Validez)** vos changements.

 ©2025 Palo Alto Networks, Inc.

Trier les journaux par ID de groupe de périphériques dans un déploiement multilocataire

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Pour plus d'informations sur la gestion de plusieurs locataires dans Prisma Access (Managed by Strata Cloud Manager), consultez Prisma SASE.	❑ Licence Prisma Access

Pour trier manuellement les journaux par locataire dans Panorama, sélectionnez **Monitor (Surveiller)** > **Logs (Journaux)** et choisissez l'icône **Device groupe (Groupe de périphériques)** associée à ce locataire pour afficher les journaux de ce groupe de périphériques. Toutefois, si vous transférez vos journaux vers un périphérique externe, vous devrez peut-être trier ces journaux au niveau du locataire. Pour ce faire, recherchez l'ID du groupe de périphériques associé au groupe de périphériques dans les journaux et utilisez le mappage de cet ID de groupe à groupe de périphériques pour associer les journaux à un locataire.

Quatre champs sont associés au groupe de périphériques dans les journaux : **Hiérarchie DG de niveau 1**, **Hiérarchie DG de niveau 2**, **Hiérarchie DG de niveau 3**et **Hiérarchie DG de niveau 4**. Ces champs affichent les ID de groupe de périphériques dans leur hiérarchie. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure.

Hiérarchie DG de niveau 1 fait référence au premier niveau de groupe de périphériques de la hiérarchie. Si vous avez ajouté des groupes de périphériques enfants ou petits-enfants, les champs **Hiérarchie DG de niveau 2** à **Hiérarchie DG de niveau 4** affichent la hiérarchie entre le groupe enfant et le groupe arrière-petit-enfant, respectivement.

Pour rechercher des journaux par locataire, effectuez la tâche suivante.

STEP 1 | Recherchez les ID de groupe de périphériques associés au groupe de périphériques.

- Pour trouver ces informations à l'aide d'une commande CLI, connectez-vous à Panorama en tant que super utilisateur (utilisateur de niveau administrateur), entrez la commande `show readonly` en mode de configuration, et affichez les valeurs dans l'en-tête **device-group**. Les ID des groupes de périphériques s'affichent sous le nom du groupe de périphériques. L'exemple suivant montre que l'ID de périphérique pour le groupe de périphériques **acme-sc** est **20**.

  Notez que ces groupes de périphériques se trouvent au premier niveau de la hiérarchie (**Hiérarchie DG de niveau 1**) ; vous utiliserez ces informations lors de l'étape suivante.

```
admin# show readonly ... device-group { acme-sc { id 20; } acme-
rn { id 39; } acme-mu { id 40; } hooli-rn { id 56; } hooli-sc
 { id 57; } hooli-mu {
```

 ©2025 Palo Alto Networks, Inc.

- Pour utiliser une requête d'API, entrez la commande API suivante :

```
/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>
```

Pour plus d'informations sur l'utilisation des API avec les journaux, consultez Retrieve logs (API) (Récupérer les journaux [API]).

STEP 2 | Utilisez le mappage de l'ID de groupe de périphériques pour associer les journaux à un locataire.

STEP 3 | **Add (Ajouter)** les paramètres de la fonctionnalité **Forwarding (Transfert)** qui sélectionnent les journaux que vous souhaitez transférer.

 ©2025 Palo Alto Networks, Inc.

Prisma Access dans un environnement FedRAMP

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Versions du plug-in Cloud Services 3.2.1-h94+, 4.0.0-h88+, 4.1.0-h58+, 5.0.0-h31+

Le programme fédéral de gestion des risques et des autorisations (FedRAMP) est un programme gouvernemental américain qui fournit une approche standardisée de l'évaluation de la sécurité, de l'autorisation et de la surveillance continue des produits et services cloud pour les utilisateurs gouvernementaux. Palo Alto Networks a démontré sa conformité au programme FedRAMP modéré pour Prisma Access (Managed by Panorama). Lisez les rubriques suivantes pour en savoir plus sur la configuration de Prisma Access afin de garantir la conformité au FedRAMP modéré.

Pour les services basés sur le cloud tels que Prisma Access, le gouvernement des États-Unis exige un niveau d'assurance spécifique, appelé *modéré*, dans lequel la perte de confidentialité, d'intégrité et de disponibilité aurait une incidence négative grave sur les opérations, les actifs ou les individus d'une agence. Les effets indésirables graves pourraient inclure des dommages opérationnels importants aux actifs de l'agence, des pertes financières ou des préjudices individuels qui ne constituent pas une perte de vie ou une perte physique.

Prisma Access est conforme aux exigences du programme FedRAMP modéré et a obtenu une autorisation d'exploitation (ATO) du gouvernement fédéral. Pour garantir la conformité au programme FedRAMP modéré, vous devez installer et configurer Prisma Access selon les exigences et les directives énumérées dans les rubriques suivantes.

Exigences FedRAMP de Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Versions du plug-in Cloud Services 3.2.1-h94+, 4.0.0-h88+, 4.1.0-h58+, 5.0.0-h31+

FedRAMP est le programme utilisé par le gouvernement des États-Unis qui fournit une approche standard en matière de conformité pour les offres de services cloud (CSO). Pour vous assurer que votre Prisma Access (Managed by Panorama) Access est conforme au niveau modéré FedRAMP, suivez ces directives et exigences lors de l'installation, de l'activation, de la configuration initiale et de la configuration Prisma Access.

Conditions préalables à l'installation et à l'activation du produit

Pour vous assurer que votre déploiement Prisma Access reste conforme, veillez à suivre ces exigences relatives à l'installation et à l'activation du produit.

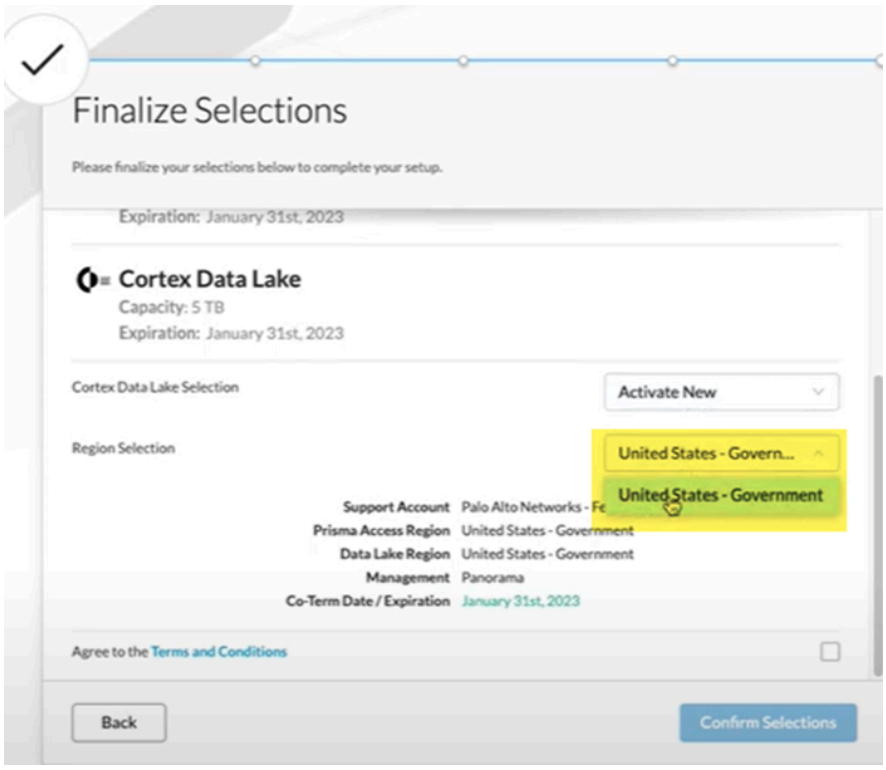
- **Conditions préalables à l'installation :**
  - **Type de déploiement (nouveau ou existant)** : les nouveaux déploiements Prisma Access sont pris en charge dans un environnement FedRAMP modéré. Les mises à niveau à partir d'un déploiement Prisma Access existant vers un déploiement Prisma Access FedRAMP modéré ne sont pas prises en charge.
  - **SKU requis** : lorsque vous achetez Prisma Access pour un déploiement FedRAMP modéré, Prisma Access exige des SKU spécifiques à l'environnement FedRAMP. Travaillez avec votre représentant ou partenaire Palo Alto Networks agréé pour vous assurer d'acheter les bons SKU pour votre déploiement FedRAMP modéré.
  - Utilisez uniquement les versions Panorama, les versions GlobalProtect et les versions du plug-in Cloud Services répertoriées dans Versions requises de Panorama, du plug-in et du plan de données PAN-OS.
  - **Liste d'autorisation des adresses IP publiques Strata Logging Service** : le bloc d'adresses IP utilisé par la région fédérale de Strata Logging Service est 34.67.50.64/28. Si votre entreprise utilise des listes d'autorisation, veillez à ajouter ces adresses IP à vos listes d'autorisation pour vous assurer que Strata Logging Service puisse recevoir les journaux de Prisma Access.
  - **Modifications apportées aux URL de l'API** : lorsque vous exécutez le script d'API pour récupérer les adresses IP publiques utilisées par Prisma Access, modifiez l'URL de l'API de **`https://api.gpcloudservice.com/GetPrismaAccessIP/v2`** en **`https://api.fed.prismaaccess.com/GetPrismaAccessIP/v2`**.

    Si votre appareil Panorama utilise un serveur proxy (**Panorama** > **Setup (Configuration)** > **Service** > **Proxy Server (Serveur proxy)**) ou si vous utilisez le décryptage proxy de transfert SSL avec Prisma Access, assurez-vous d'ajouter l'URL api.fed.prismaaccess.com à votre liste d'autorisation sur le proxy ou le serveur proxy.

 ©2025 Palo Alto Networks, Inc.

- **Changement de nom du portail GlobalProtect** : le nom d'hôte du portail par défaut pour un déploiement Prisma Access GlobalProtect pour les utilisateurs mobiles FedRAMP est différent d'un déploiement non FedRAMP. Le nom du portail est *<portal-name>*.fed.prismaaccess.com. au lieu de *<portal-name>*.gpcloudservice.com.
- **Exigences en matière de support** : Prisma Access FedRAMP modéré nécessite les services d'assistance du gouvernement américain de Palo Alto Networks, qui incluent une assistance 24h/24 et 7j/7 pour le personnel américain sur le sol américain.

- **Conditions d'activation** : lorsque vous activez et installez votre déploiement Prisma Access, les tâches d'activation et d'installation sont similaires à celles d'un déploiement non FedRAMP. Cependant, vous devez sélectionner une région **Strata Logging Service** du **United States—Government (Gouvernement des États-Unis)** lors de l'activation du produit.



Versions requises de Panorama, du plug-in et du plan de données PAN-OS

Pour veiller à ce que Prisma Access reste conforme aux exigences de FedRAMP modéré, vérifiez que votre déploiement Prisma Access (Managed by Panorama) utilise les versions suivantes de Panorama, du plug-in Cloud Services et de GlobalProtect.

Composant	Version requise
Version Panorama PAN-OS	PAN-OS version 10.2.8-h3 ou une version ultérieure du correctif 10.2.8 PAN-OS version 10.2.9-h1 ou une version ultérieure du correctif 10.2.9

 ©2025 Palo Alto Networks, Inc.

Composant	Version requise
	L'activation des normes de traitement et des critères communs (FIPS-CC) sur le Panorama qui gère Prisma Access est la bonne pratique recommandée alignée sur les contrôles FedRAMP. L'activation de la prise en charge de FIPS-CC sur Panorama nécessite l'accès à l'outil de récupération après maintenance (MRT). *Pour simplifier le processus d'installation et d'activation, vous pouvez sélectionner un Panorama existant que vous avez déjà configuré en mode FIPS, si vous avez enregistré Panorama, installé les licences et activé la licence de support sur le portail de support client (CSP). Si vous avez ajouté le numéro de série de Panorama au même compte CSP sur lequel vous souhaitez déployer Prisma Access, vous pouvez sélectionner le numéro de série de cet appareil Panorama lors de l'installation.* Vous ne pouvez pas utiliser un Panorama qui a été utilisé pour gérer un autre déploiement Prisma Access ou Strata Logging Service.
Version du plug-in Cloud Services	• 3.2.1-h94+ • 4.0.0-h88+ • 4.1.0-h58+ • 5.0.0-h31
Version de GlobalProtect	5.1.4+ et 6.0.7+ La version 5.1.4 est certifiée FIPS et constitue la version par défaut à utiliser pour les déploiements basés sur le gouvernement fédéral. Si vous modifiez la version GlobalProtect par défaut de 5.1.4, vous ne pouvez pas sélectionner la version 5.1.4 à partir de l'interface utilisateur Panorama et vous devrez ouvrir une demande d'assistance auprès du support technique de Palo Alto Networks pour la rajouter.

 ©2025 Palo Alto Networks, Inc.

Emplacements FedRAMP pris en charge par Prisma Access

Les emplacements suivants sont autorisés à être utilisés avec Prisma Access dans un environnement FedRAMP modéré, qui inclut la prise en charge d'emplacements dans la zone continentale des États-Unis (CONUS) et en dehors de la zone continentale des États-Unis (OCONUS) :

- Australie Sud-Est
- Belgique
- Sud du Brésil
- Est du Canada
- Finlande
- Allemagne Centre
- Ouest de l'Inde
- Japon Centre
- Japon Sud
- Pays-Bas Centre
- Singapour
- Suisse
- Taïwan
- Royaume-Uni
- États-Unis Centre
- États-Unis Est
- États-Unis Nord-Ouest
- États-Unis Sud-Est
- États-Unis Sud-Ouest

Fonctionnalités prises en charge et non prises en charge dans un déploiement Prisma Access FedRAMP

La prise en charge IPv6 pour l'accès aux applications privées est prise en charge dans un environnement Prisma Access FedRAMP modéré.

Les applications et fonctionnalités suivantes ne sont pas prises en charge pour une utilisation dans un environnement Prisma Access modéré FedRAMP :

- Prisma Access Informations
- DEM autonome
- Proxy explicite
- Prisma Access pour Clean Pipe
- Enterprise DLP
- IoT Security

 ©2025 Palo Alto Networks, Inc.

- Assistance SaaS Security Inline – Visibilité

 ©2025 Palo Alto Networks, Inc.

Configurer Prisma Access dans un environnement FedRAMP

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Versions du plug-in Cloud Services 3.2.1-h94+, 4.0.0-h88+, 4.1.0-h58+, 5.0.0-h31+

Une fois les exigences remplies, terminez la configuration du déploiement Prisma Access pour un environnement FedRAMP modéré en procédant comme suit.

Avant de commencer, notez les exigences et les directives spécifiques à un déploiement Prisma Access FedRAMP, y compris la configuration de l'appareil Panorama en mode FIPS-CC et les versions spécifiques requises pour Panorama, le plug-in Cloud Services et GlobalProtect.

STEP 1 | Assurez-vous que vous disposez d'un compte du portail du support client (CSP) que vous pouvez dédier exclusivement à vos déploiements FedRAMP.

Vous ne pouvez pas avoir de déploiements FedRAMP et non FedRAMP dans un seul compte CSP. Pour cette raison, Palo Alto Networks vous recommande de créer un nouveau compte CSP à utiliser uniquement pour les comptes FedRAMP.

STEP 2 | Préparez votre appareil Panorama pour l'utiliser dans l'environnement Prisma Access FedRAMP.

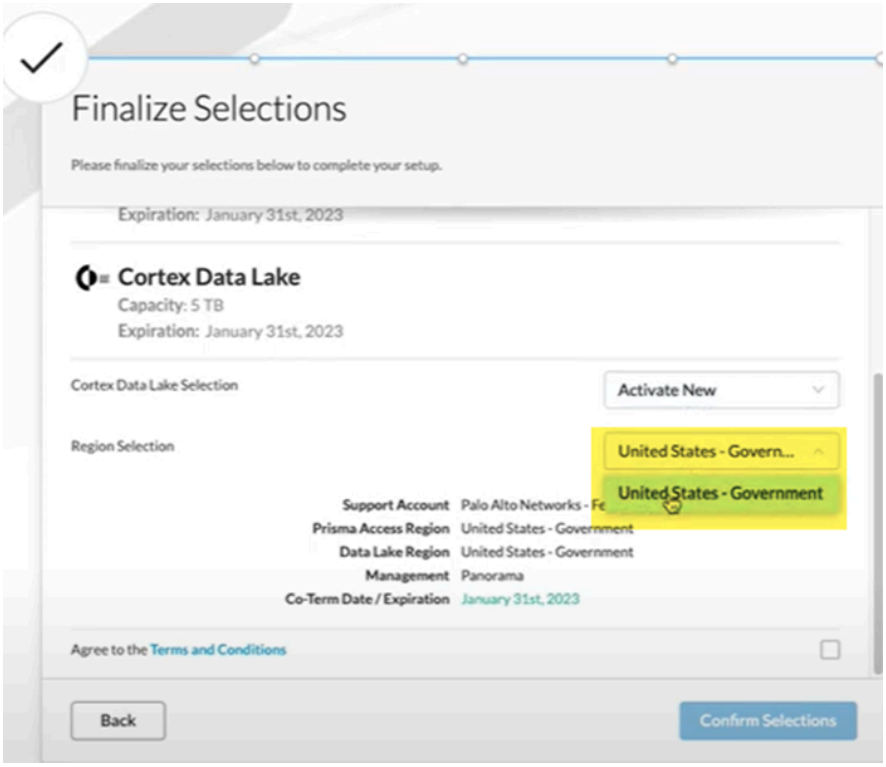
1. Installez l'appareil Panorama (un appareil M-Series ou un appareil virtuel).
2. (Facultatif, recommandé) Activez la prise en charge de la norme FIPS-CC (Federal Information Processing Standard and Common Criteria) sur l'appareil Panorama.

   L'activation de la prise en charge de FIPS nécessite l'accès au Maintenance Recovery Tool (Outil de récupération après maintenance, MRT).
3. Mettez à niveau votre version Panorama vers la version répertoriée dans Versions requises de Panorama, du plug-in et du plan de données PAN-OS.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Identifiez vos exigences de licence, puis activez et installez les composants de licence Prisma Access.

Sélectionnez une région **Strata Logging Service (Service de journalisation Strata)** des **United States—Government (États-Unis – Gouvernement)** lors de l'activation du produit.



STEP 4 | Ajoutez les URL, adresses IP et ports suivants à une liste autorisée sur tout appareil de sécurité que vous utilisez avec l'appareil Panorama qui gère Prisma Access.

De plus, si votre appareil Panorama utilise un serveur proxy (**Panorama** > **Setup (Configuration)** > **Service** > **Proxy Server (Serveur proxy)**) ou si vous utilisez un proxy de transfert SSL avec Prisma Access, assurez-vous d'ajouter les URL, adresses IP et ports suivants à une liste autorisée sur le proxy ou le serveur proxy.

- api.gpcloudservice.com (pour Prisma Access)
- api.paloaltonetworks.com (pour Prisma Access)
- api.fed.prismaaccess.com (pour Prisma Access)
- apitrusted.paloaltonetworks.com (pour Prisma Access)
- Les FQDN et les ports requis pour le service de journalisation Strata
- 34.67.50.64/28

  Le bloc d'adresse IP utilisé par la région fédérale Strata Logging Service est 34.67.50.64/28. Ajoutez ces adresses IP à votre liste autorisée afin que Strata Logging Service puisse recevoir les journaux de Prisma Access.
- Les ports utilisés par Panorama.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Ouvrez un dossier dans le portail du support client (CSP) pour que Palo Alto Networks autorise la liste des ports source et de destination pour Strata Logging Service.

Pour utiliser Strata Logging Service dans un environnement Prisma Access, vous devez créer un cas pour que Palo Alto Networks puisse autoriser la liste des ports source et de destination en interne.

STEP 6 | Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire** et entrez **`wildfire.gov.paloaltonetworks.com`**.

Les déploiements FedRAMP nécessitent que vous utilisiez le cloud WildFire du gouvernement américain.

STEP 7 | Intégrez les utilisateurs mobiles et sécurisez-les avec GlobalProtect, si nécessaire pour votre déploiement.

Nous vous recommandons d'utiliser l'authentification locale comme première étape pour vérifier que le service est configuré et que vos utilisateurs ont accès à Internet. Vous pourrez ensuite passer à l'utilisation de vos méthodes d'authentification d'entreprise.

1. Configurez les utilisateurs mobiles GlobalProtect.
2. Configurez des zones pour les utilisateurs mobiles.
    1. Créez deux zones dans le modèle Utilisateur mobile. Par exemple, les utilisateurs mobiles et Internet.
    2. Mappez les zones. Mappez n'importe quelle zone qui n'est pas celle des utilisateurs connectés à Prisma Access, du siège social ou des succursales sur Non approuvé.

        Sous **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users (Utilisateurs mobiles)**, mappez Internet sur Non approuvé ; Utilisateurs mobiles sur Approuvé.
3. Configurez les politiques de sécurité pour le groupe de périphériques.

    Pour créer une politique de sécurité autorisant le trafic vers Internet, sélectionnez le Mobile_User_Device_Group **Policies (Politiques)** > **Security (Sécurité)** > **Prerules (Pré-règles)** > **Add (Ajouter)** pour ajouter une règle. Par exemple : Les utilisateurs mobiles vers Internet.
4. Validez et appliquez vos modifications pour commencer à utiliser le service.
    1. Cliquez sur **Commit (Valider)** localement sur Panorama.
    2. Cliquez sur **Commit and Push (Valider et appliquer)** sur Prisma Access.
    3. Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Monitor (Surveiller)** > **Mobile Users (Utilisateurs mobiles)** pour afficher le **Status (État)** et vérifier que vous pouvez envoyer un ping au FQDN du portail.
5. Validez ce Prisma Access sécurise le trafic Internet pour les utilisateurs mobiles.
    1. Téléchargez et installez l'application GlobalProtect.
    2. Utilisez l'application pour vous connecter au portail en tant qu'utilisateur mobile (utilisateur local).
    3. Parcourez quelques sites Web sur Internet et vérifiez les journaux du trafic sur Panorama.

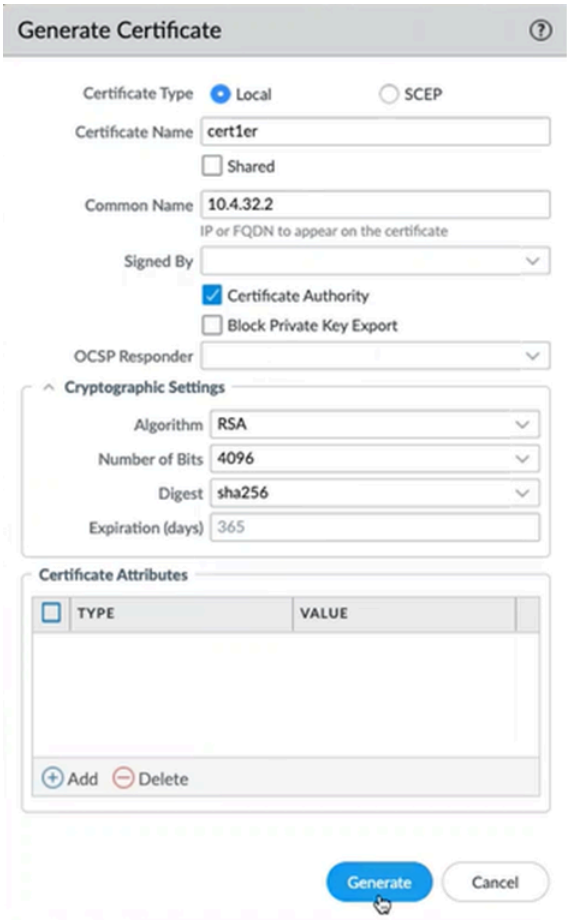
 ©2025 Palo Alto Networks, Inc.

STEP 8 | (Déploiements d'utilisateurs mobiles GlobalProtect uniquement) Créez un certificat de remplacement d'authentification dans votre déploiement Utilisateurs mobiles — GlobalProtect qui répond aux exigences d'un Panorama exécuté en mode FIPS et appliquez ce certificat à votre déploiement.

Générez un nouveau certificat, car le certificat par défaut pour les utilisateurs mobiles GlobalProtect, **Authentication Cookie CA (Cookie d'authentification CA)**) ne répond pas aux exigences minimales de la suite de chiffrement pour un Panorama exécuté en mode FIPS-CC.

1. À partir du Panorama qui gère Prisma Access, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.

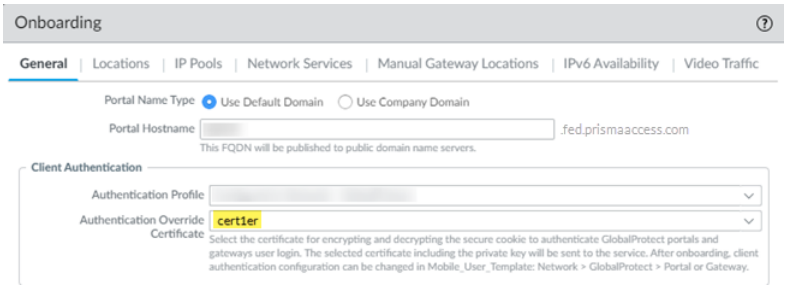
   Assurez-vous que vous êtes dans le **Mobile_User_Template**.
2. Générez un certificat qui répond aux exigences minimales de la suite de chiffrement pour un Panorama en mode FIPS-CC.



3. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—GlobalProtect (Utilisateurs mobiles GlobalProtect)**, sélectionnez le **Hostname (Nom d'hôte)** et, dans la zone **Client Authentication (Authentification client)**, sélectionnez le

 ©2025 Palo Alto Networks, Inc.

Authentication Override Certificate (Certificat de remplacement d'authentification) que vous avez créé.



Si vous avez déjà créé votre configuration d'utilisateurs mobiles GlobalProtect, cette zone est grisée. Pour modifier le certificat de remplacement d'authentification, sélectionnez ***Network (Réseau)*** *>* ***GlobalProtect*** *>* ***Portals (Portails)*** *>* ***<portal-config>*** *>* ***Agent*** *>* ***DEFAULT (Par défaut)*** *>* ***Authentication (Authentification)*** *et sélectionnez ce certificat sous le* ***Certificate to Encrypt/Decrypt Cookie (Certificat pour chiffrer/déchiffrer le cookie)****.*

STEP 9 | Activer l'infrastructure de service et les connexions aux services qui permettent la communication entre les éléments Prisma Access.

1. Planifiez l'activation de l'infrastructure de service et des connexions aux services.
2. Activez l'infrastructure de service.
3. Créez une connexion aux services pour permettre l'accès à vos ressources d'entreprise.

   Si vous n'avez pas besoin d'accéder à vos ressources d'entreprise, vous devez tout de même créer une connexion aux services pour permettre l'accès entre les utilisateurs mobiles et les réseaux distants.

STEP 10 | Planifiez, créez et configurez des connexions réseau à distance.

1. Ajoutez un ou plusieurs réseaux distants à Prisma Access.

   Vous pouvez intégrer un emplacement, puis ajouter des emplacements supplémentaires à l'aide de la fonction d'importation en bloc.
2. Créez une règle de politique de sécurité pour autoriser le trafic des réseaux distants vers le siège social (par exemple : de « approuvé » à « approuvé »).
3. Validez la connectivité entre la connexion aux services, la connexion au réseau distant et les utilisateurs mobiles.

STEP 11 | Récupérez les adresses IP publiques et privées Prisma Access.

Vous ajoutez ces adresses à une liste autorisée sur le réseau de votre organisation pour limiter l'accès entrant à votre réseau d'entreprise et à vos applications.

Si vous disposez d'un déploiement d'utilisateurs mobiles GlobalProtect, vous pouvez utiliser l'interface utilisateur Prisma Access au lieu de cette API pour gérer l'allocation d'adresses IP publiques et confirmer que les adresses IP ont été ajoutées à vos listes autorisées avant que Prisma Access publie les adresses IP. De cette façon, Prisma Access provisionne uniquement les adresses IP que vous avez autorisées dans la liste.

 ©2025 Palo Alto Networks, Inc.

STEP 12 | (Facultatif) Modifiez la méthode d'authentification de l'authentification locale à la méthode d'authentification de votre organisation.

Utilisez l'une des méthodes suivantes pour configurer l'authentification SAML pour les utilisateurs mobiles :

- Configurer l'authentification SAML Azure AD pour les déploiements d'utilisateurs mobiles

  Configurez uniquement les parties GlobalProtect de cette configuration et omettez la configuration du proxy explicite.
- Configurer l'authentification SAML à l'aide d'Okta comme IdP pour les utilisateurs mobiles
- Configurer ADFS comme fournisseur SAML pour les utilisateurs mobiles

Bien que vous puissiez utiliser Cloud Identity Engine pour récupérer des informations sur les utilisateurs et les groupes à l'aide de Cloud Identity Engine après avoir configuré l'authentification, vous ne pouvez pas authentifier les utilisateurs à l'aide de Cloud Identity Engine uniquement.

STEP 13 | (Facultatif) Transférez les journaux de Strata Logging Service vers un récepteur Syslog externe en configurant l'application de transfert des journaux.

 ©2025 Palo Alto Networks, Inc.

Déploiements Prisma Access avancés

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Certains déploiements de routage et de mise en réseaux Prisma Access nécessitent une compréhension approfondie de la topologie et des périphériques de routage de votre organisation, ainsi qu'une compréhension du fonctionnement du routage Prisma Access. Découvrez ces déploiements avancés et la manière de les configurer dans cette section.

Déploiements avancés applicables aux connexions aux services, aux utilisateurs mobiles et aux réseaux distants :

- Ajouter un nouvel emplacement de calcul pour un emplacement Prisma Access déployé
- Prise en charge de l'IPv6
- Résolution DNS pour les utilisateurs mobiles – Déploiements GlobalProtect et de réseaux distants
- Comment BGP annonce les pools d'adresses IP des utilisateurs mobiles pour les connexions aux services et les connexions au réseau distant
- Prise en charge du proxy pour Prisma Access et Strata Logging Service
- Bloquer les connexions entrantes en provenance de pays spécifiques
- Sécuriser le trafic Internet depuis AWS WorkSpace
- Prisma Access pour les réseaux sans itinéraire par défaut

Déploiements avancés des connexions aux services :

- Redondance multicloud des connexions aux services
- Utiliser la redirection du trafic pour transférer le trafic lié à Internet aux connexions aux services
- Routage pour le trafic de connexion aux services
- Préserver le mappage de User-ID et Device-ID pour les connexions aux services avec NAT source

Déploiements avancés d'utilisateurs mobiles –GlobalProtect :

- Configurer plusieurs portails dans Prisma Access
- Prise en charge de l'enregistrement DNS dynamique pour le dépannage et les mises à jour à distance

- Prise en charge de l'enregistrement DNS dynamique pour les utilisateurs mobiles – GlobalProtect
- Identification et mise en quarantaine des périphériques compromis dans un déploiement GlobalProtect Prisma Access
- Trafic de l'entonnoir IPv6 chez les utilisateurs mobiles : déploiements GlobalProtect
- Redistribuer les informations HIP avec Prisma Access
- Voir les rapports HIP
- Prise en charge de l'encodage Gzip dans un VPN sans client
- Réplication du trafic dans Prisma Access

Déploiements avancés de réseaux distants :

- Fournir un accès sécurisé entrant aux emplacements réseau distants
- Créer un réseau à large bande passante pour un site distant

 ©2025 Palo Alto Networks, Inc.

Ajouter un nouvel emplacement de calcul pour un emplacement Prisma Access déployé

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Pour optimiser les performances et améliorer la latence, Prisma Access peut introduire de nouveaux emplacements de calcul pour les emplacements que vous avez déjà déployés dans le cadre d'une mise à niveau du plug-in. Lorsque vous mettez à niveau le plug-in, le mappage existant entre les emplacements de calcul et les emplacements ne change pas, mais vous pouvez profiter du nouvel emplacement de calcul. Si vous changez l'emplacement de calcul, Prisma Access modifie les adresses IP de la passerelle et du portail (pour les utilisateurs mobiles) et les adresses IP de service (pour les réseaux distants) pour les emplacements auxquels le nouvel emplacement de calcul est associé. Si vous utilisez des listes d'autorisation dans votre réseau permettre aux utilisateurs d'accéder à des ressources Internet telles que des applications SaaS ou des applications partenaires accessibles au public, vous devez ajouter ces nouvelles adresses IP aux listes d'autorisation.

Pour passer à un nouvel emplacement de calcul lorsqu'il devient disponible, procédez comme suit.

Étant donné que la suppression et l'ajout de l'emplacement existant et la modification des listes d'autorisation (pour les utilisateurs mobiles) ou de l'adresse IP du tunnel IPSec homologue (pour les déploiements de réseaux distants) prendront un certain temps, Palo Alto Networks vous recommande d'effectuer le changement d'emplacement de calcul pendant une fenêtre de maintenance ou pendant les heures creuses.

Pour réduire le temps d'interruption pour les déploiements d'utilisateurs mobiles, utilisez l'API pour allouer au préalable les nouvelles adresses IP de passerelle et de portail d'utilisateur mobile avant d'effectuer ces étapes.

STEP 1 | Ajoutez de la bande passante pour les nouveaux emplacements de calcul de réseaux distants.

1. (Déploiements de réseaux distants qui allouent la bande passante de réseau distant en fonction de l'emplacement de calcul uniquement) Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**.
2. Cliquez sur l'icône en forme d'engrenage dans la zone **Bandwidth Allocation (Allocation de bande passante)** et ajoutez **Bandwidth Allocation (Mbps) (Allocation de bande passante (Mbit/s))** pour le nouvel emplacement de calcul.
3. Attendez que la bande passante soit reflétée dans le champ Allocated Total (Total alloué) en haut de la page, puis cliquez sur **OK**.

STEP 2 | (Déploiements d'utilisateurs mobiles uniquement) Récupérez les nouvelles adresses IP de passerelle et de portail à l'aide du script API et ajoutez-les aux listes d'autorisation.

STEP 3 | Supprimez l'emplacement de connexion aux services, de connexion aux réseaux distants ou d'utilisateur mobile associé au nouvel emplacement de calcul.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Validez et appliquez les modifications.

STEP 5 | Rajoutez les emplacements que vous venez de supprimer.

STEP 6 | Validez et appliquez les modifications.

STEP 7 | (Déploiements de réseaux distants et de connexions aux services uniquement) Modifiez votre CPE pour qu'il pointe vers les nouvelles adresses IP du tunnel IPSec pour la connexion aux réseaux distants ou la connexion aux services.

Pour les connexions aux réseaux distants, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Remote Networks (Réseaux distants)**, notez la **Service IP Address (Adresse IP de service)** et configurez la nouvelle **Service IP Address (Adresse IP de service)** pour l'utiliser comme adresse homologue pour le tunnel IPSec des réseaux distants sur votre CPE.

Pour les connexions aux services, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)**, notez la **Service IP Address (Adresse IP de service)** et configurez la nouvelle **Service IP Address (Adresse IP de service)** pour l'utiliser comme adresse IP homologue pour le tunnel IPSec des connexions aux services sur votre CPE.

STEP 8 | Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Remote Networks (Réseaux distants)**, notez la **Service IP Address (Adresse IP de service)** et configurez la nouvelle **Service IP Address (Adresse IP de service)** pour l'utiliser comme adresse homologue pour le tunnel IPSec des réseaux distants sur votre CPE.

Lorsque vous supprimez et rajoutez une connexion à un réseau distant, l'adresse IP du tunnel IPSec du côté de Prisma Access change.

STEP 9 | (Déploiements d'utilisateurs mobiles uniquement) Après qu'un emplacement a été remappé, récupérez le nouveau FQDN de passerelle et ajoutez-le à la configuration d'authentification de votre fournisseur SAML.

Si un emplacement d'utilisateur mobile est remappé, le FQDN de passerelle peut changer après la mise à niveau de l'infrastructure qui a entraîné le remappage, ce qui pourrait causer des problèmes avec l'authentification SAML. Pour trouver le nom de la passerelle :

- Dans Prisma Access (Managed by Strata Cloud Manager), sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **GlobalProtect Setup (Configuration de GlobalProtect)** > **Infrastructure** > **Infrastructure Settings (Paramètres d'infrastructure)**, cliquez sur l'icône en forme d'engrenage pour afficher les paramètres d'infrastructure, puis copiez la passerelle renommée dans la zone Gateway FQDNs (FQDN de passerelle).
- Dans Prisma Access (Managed by Panorama), sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Mobile Users—GlobalProtect (Utilisateurs mobiles – GlobalProtect)** et copiez la passerelle renommée dans la zone Gateways (Passerelles).

 ©2025 Palo Alto Networks, Inc.

Prise en charge de l'IPv6

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access 2.2 Préféré et versions ultérieures ❑ L'accès IPv6 natif aux applications publiques et privées nécessite les versions minimales suivantes : • Prisma Access (Managed by Strata Cloud Manager) : Version de juin 2024 • Prisma Access (Managed by Panorama) : Prisma Access 5.1.1 pour les nouveaux déploiements uniquement. Tous les autres déploiements (y compris les déploiements Prisma Access (Managed by Panorama) existants) prennent uniquement en charge l'accès aux applications privées.

Si votre organisation utilise l'adressage IPv6, Prisma Access vous permet d'accéder aux applications internes (privées) qui se trouvent derrière des adresses IPv6. Selon la version de Prisma Access, vous pouvez accéder soit aux applications privées (internes) utilisant l'IPv6, soit à la fois aux applications internes et publiques (externes) pour GlobalProtect et les réseaux distants.

Pour l'accès aux applications externes, la fonctionnalité IPv6 n'est pas activée par défaut sur certains composants Prisma Access. Avant d'activer l'IPv6 natif pour l'accès aux applications publiques, contactez l'équipe de compte Palo Alto Networks et ouvrez un ticket TAC pour lancer le processus d'activation.

Un avantage de la prise en charge de l'IPv6 natif réside dans la possibilité pour les utilisateurs mobiles sur IPv6 uniquement et les terminaux à double pile de se connecter à Prisma Access par l'intermédiaire de connexions IPv6 via GlobalProtect. Un autre avantage est la possibilité pour GlobalProtect et les réseaux distants d'accéder à Internet et aux applications SaaS publiques sur Internet lorsque les destinations Internet nécessitent des connexions IPv6.

L'IPv6 offre un espace d'adressage nettement plus grand que l'IPv4, permettant un nombre presque illimité d'adresses IP uniques. D'un autre côté, la double pile est une approche transitoire qui permet aux réseaux et aux périphériques de fonctionner en utilisant simultanément l'IPv4 et l'IPv6. La prise en charge de l'IPv6 natif rend Prisma Access compatible avec les connexions IPv6 et double pile pour faciliter le processus de migration de l'IPv4 vers l'IPv6, assurer la rétrocompatibilité et optimiser votre parcours vers le cloud et les réseaux compatibles IPv6.

Vous configurez l'IPv6 dans les composants réseau Prisma Access suivants :

- Activez l'IPv6 et spécifiez un sous-réseau IPv6 dans votre sous-réseau d'infrastructure pour établir une infrastructure réseau IPv6 afin de permettre la communication entre les réseaux

 ©2025 Palo Alto Networks, Inc.

distants (emplacements de succursale), les utilisateurs mobiles et les connexions aux services (emplacements de centre de données ou du siège).

Pour de meilleurs résultats, fournissez votre propre pool d'adresses IPv6 (publiques ou privées) avec une longueur de préfixe de /64, par exemple 3005:10:209:55::/64.

- Pour un déploiement Utilisateurs mobiles – GlobalProtect, spécifiez si la mise en réseau IPv6 doit être utilisée pour les emplacements de calcul associés aux emplacements d'utilisateurs mobiles.

  Vous pouvez spécifier des pools d'adresses IP pour les utilisateurs mobiles IPv6 et des adresses de serveurs DNS IPv6 selon vos besoins.

  Pour de meilleurs résultats, fournissez votre propre pool d'adresses IPv6 (publiques ou privées) avec une longueur de préfixe de /64, par exemple 3001:192:168:32::/64, appliqué à un niveau mondial.

  Prisma Access attribue un pool d'un sous-réseau /80 à chaque région de calcul et un pool d'un sous-réseau /112 à chaque emplacement (passerelle). Étant donné que chaque connexion GlobalProtect utilise une adresse IP du pool, cette allocation permet d'attribuer plus de 65 000 adresses IPv6 disponibles (/128) aux terminaux des utilisateurs par emplacement.
- Pour les connexions aux services et les connexions aux réseaux distants, vous pouvez spécifier un adressage IPv6 pour le type de routage utilisé par la connexion (itinéraires statiques ou BGP).
  - Pour les itinéraires statiques, spécifiez une adresse IPv6 pour les sous-réseaux qu'ils utilisent.
  - Pour les itinéraires BGP, spécifiez une **Peer Address (Adresse de l'homologue)** et une **Local Address (Adresse locale)** IPv6.

    Vous pouvez également spécifier la méthode de transport utilisée pour l'échange d'informations d'appairage BGP. Vous pouvez choisir d'utiliser l'IPv4 pour l'échange de toutes les informations d'appairage BGP (y compris IPv4 et IPv6), d'utiliser l'IPv6 pour l'échange de toutes les informations d'appairage BGP, ou d'utiliser l'IPv4 pour l'échange d'informations d'appairage BGP IPv4 et l'IPv6 pour l'échange des informations d'appairage BGP IPv6.

    Pour de meilleurs résultats, fournissez votre propre pool d'adresses IPv6 (publiques ou privées) avec une longueur de préfixe maximale de /64, par exemple 2005:10:209:79::/64.
- Pour les réseaux distants, vous pouvez ajouter des adresses IPv6 pour les serveurs DNS.

  Pour de meilleurs résultats, fournissez votre propre pool d'adresses IPv6 (publiques ou privées) avec une longueur de préfixe maximale de /64, par exemple 2001:10:209:65::/64.

  Chaque succursale doit utiliser un sous-réseau unique /112 (longueur maximale), ce qui permet plus de 65 000 hôtes uniques.

 ©2025 Palo Alto Networks, Inc.

- *Les adresses IPv6 que vous fournissez ne doivent pas chevaucher l'espace d'adressage IPv6 public BYOIP Prisma Access.*
- *Le pool d'adresses IP, les sous-réseaux de succursale (réseau distant), les sous-réseaux d'entreprise (connexion aux services) et le sous-réseau d'infrastructure ne doivent pas se chevaucher (ils doivent être mutuellement exclusifs).*

Les emplacements de calcul suivants ne prennent pas en charge l'IPv6 :

- Corée du Sud
- Asie Nord-Est
- Amérique du Sud Est
- Bahreïn
- Afrique du Sud Ouest
- Europe Nord (Stockholm)
- Moyen-Orient Centre (EAU)

Les emplacements suivants ne prennent pas en charge l'IPv6 :

- Tous les emplacements de zone locale
- Canada Ouest
- Afrique du Sud Centre

Les déploiements suivants ne prennent pas en charge l'adressage IPv6 :

- Réseaux distants : haute performance
- Optimisation IP

  Les déploiements de l'optimisation IP ne prennent pas en charge l'IPv6 pour l'accès aux applications publiques (externes) ; l'accès aux applications privées est pris en charge. Pour activer l'IPv6 pour votre nouveau déploiement Prisma Access, contactez l'équipe de compte Palo Alto Networks, qui ouvrira un dossier TAC pour répondre à la demande.
- Déploiements Clean Pipe
- Redirection du trafic (utilisation de règles de redirection du trafic pour rediriger le trafic Internet à l'aide d'une connexion aux services)
- Itinéraires sortants pour le service pour les connexions aux services et les connexions à des réseaux distants

  Prisma Access ne publie pas les itinéraires par défaut IPv6.

Présentation de la prise en charge de l'IPv6 natif

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Licence Prisma Access version 2.2 Préférée et ultérieure

 ©2025 Palo Alto Networks, Inc.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ L'accès IPv6 natif aux applications publiques et privées nécessite les versions minimales suivantes : • Prisma Access (Managed by Strata Cloud Manager) : version de juin 2024 • Prisma Access (Managed by Panorama) : Prisma Access 5.1.1 pour les nouveaux déploiements uniquement. Tous les autres déploiements (y compris les déploiements Prisma Access (Managed by Panorama) existants) prennent uniquement en charge l'accès aux applications privées.

Prisma Access étend la prise en charge de l'IPv6 au-delà de l'accès aux applications privées pour prendre en charge l'IPv6 pour GlobalProtect ainsi que les réseaux distants nativement.

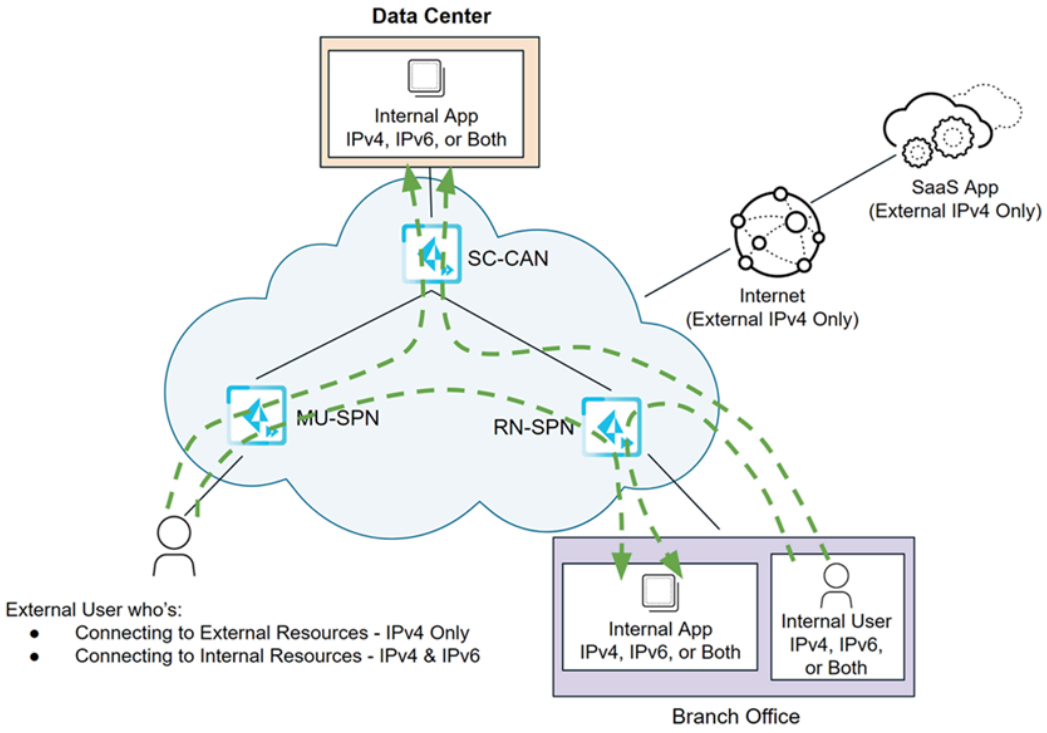
Un avantage de la prise en charge de l'IPv6 natif réside dans la possibilité pour les utilisateurs mobiles sur IPv6 uniquement et les terminaux à double pile de se connecter à des connexions Prisma Access sur IPv6 à via GlobalProtect. Un autre avantage est la possibilité pour GlobalProtect et les réseaux distants d'accéder à Internet et aux applications SaaS publiques sur Internet lorsque les destinations Internet nécessitent des connexions IPv6.

IPv6 offre un espace d'adresses nettement plus grand sur IPv4, permettant un nombre presque illimité d'adresses IP uniques. En même temps, la double pile est une approche transitoire qui permet aux réseaux et aux périphériques de fonctionner en utilisant simultanément IPv4 et IPv6. La prise en charge de l'IPv6 natif rend Prisma Access compatible avec les connexions IPv6 et double pile pour faciliter le processus de migration d'IPv4 vers IPv6, assurer la rétrocompatibilité et optimiser votre parcours vers le cloud et les réseaux compatibles IPv6.

Support des applications privées

Certains déploiements Prisma Access prennent en charge les connexions IPv6 aux applications internes « privées ». Prisma Access se connecte aux centres de données (Connexions aux services) et aux bureaux des succursales (Réseaux distants) en utilisant une sous-couche, dans laquelle le trafic IPv6 est acheminé par un tunnel IPv4.

 ©2025 Palo Alto Networks, Inc.



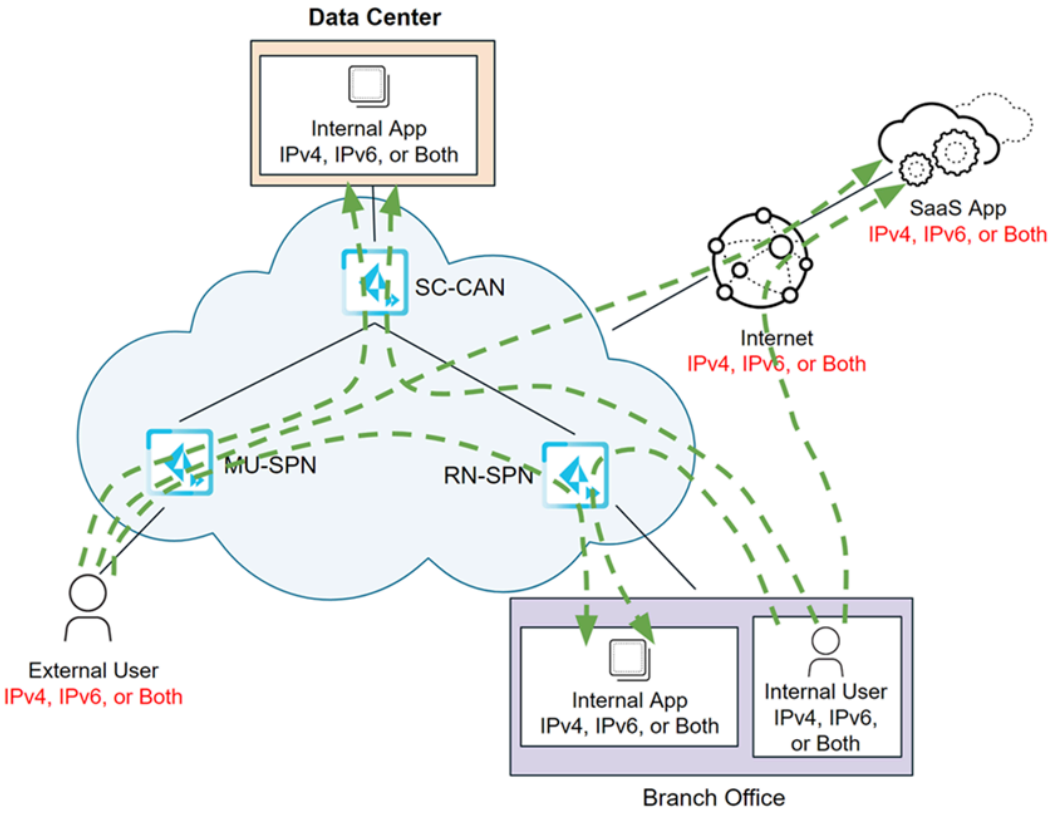
IPv6 natif dans Prisma Access

Prisma Access

- Connexions entrantes IPv4/IPv6 à double pile à Prisma Access
- Connexions sortantes IPv4/IPv6 à double pile à Internet et aux applications SaaS via Internet

Désormais, les utilisateurs peuvent se connecter à internet et aux applications SaaS « publiques » via internet à l'aide de l'IPv6.

 ©2025 Palo Alto Networks, Inc.



Les utilisateurs externes (utilisateurs mobiles) doivent être sur l'une des versions GlobalProtect suivantes prises en charge pour que l'IPv6 natif fonctionne :

- *5.2.13-c418 (Win/Mac)*
- *6.0.7-c378 (Win/Mac)*
- *6.0.7-c20 (Linux)*
- *6.1.2 (Win/Mac/Linux)*
- *6.2.0-c89 (Win/Mac)*

Le tableau suivant montre la connectivité prise en charge avec les déploiements de Prisma Access sur IPv4 et IPv6. Une coche indique que cette connectivité est prise en charge, et un tiret qu'elle ne l'est pas.

 ©2025 Palo Alto Networks, Inc.

IPv6 Not Enabled

Mobile User IP Version	GlobalProtect IP Version	Internet Destination Gateway ➞ Internet		Private App Access Service Connection ➞ Internet		GlobalProtect Tunnel	NAT Gateway ➞ Internet
		IPv4	IPv6	IPv4	IPv6	ESP	IPv4 ➞ IPv4
IPv4	IPv4	✓	—	✓	—	IPv4	NAT44
Dual Stack	Dual Stack	✓	✓ Sinkhole	✓	✓	IPv4	NAT44
IPv6	—	—	—	—	—	—	—

IPv6 Enabled

Mobile User IP Version	GlobalProtect IP Version	Internet Destination Gateway ➞ Internet		Private App Access Service Connection ➞ Internet		GlobalProtect Tunnel	NAT Gateway ➞ Internet	
		IPv4	IPv6	IPv4	IPv6	ESP	IPv6 ➞ IPv4	IPv6 ➞ IPv6
IPv4	IPv4	✓	—	✓	—	IPv4	NAT64	NPTv6
Dual Stack	Dual Stack	✓	✓	✓	✓	IPv6	NAT64	NPTv6
IPv6	Dual Stack	✓ (DNS64 & NAT64 Req'd)	✓	✓ (Custom DNS64 + NAT64)	✓	IPv6	NAT64	NPTv6

Suivez ces flux de travail pour activer IPv6 dans votre configuration.

- ❑ Activer et configurer le réseau IPv6 et les pools IP dans votre infrastructure Prisma Access
- ❑ Activer la mise en réseau IPv6 pour les utilisateurs mobiles – Déploiement de GlobalProtect
- ❑ Activer la mise en réseau IPv6 pour les connexions aux services
- ❑ Activer la mise en réseau IPv6 pour les réseaux distants

Activer et configurer la mise en réseau IPv6 et les pools d'adresses IP dans votre infrastructure Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access 2.2 préférée et versions ultérieures

 ©2025 Palo Alto Networks, Inc.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
	❑ L'accès IPv6 natif aux applications publiques et privées nécessite les versions minimales suivantes : • Prisma Access (Managed by Strata Cloud Manager) : Version de juin 2024 • Prisma Access (Managed by Panorama) : Prisma Access 5.1.1 pour les nouveaux déploiements uniquement. Tous les autres déploiements (y compris les déploiements Prisma Access (Managed by Panorama) existants) prennent uniquement en charge l'accès aux applications privées.

Pour tout déploiement Prisma Access, vous devez activer IPv6 globalement et spécifier un sous-réseau IPv6 dans votre sous-réseau d'infrastructure pour que Prisma Access puisse établir une infrastructure réseau IPv6 entre vos emplacements de réseaux distants, vos utilisateurs mobiles et vos connexions aux services. Pour ce faire, procédez comme suit.

- Strata Cloud Manager
- Panorama

Activer et configurer la mise en réseau IPv6 et les pools d'adresses IP dans votre infrastructure Prisma Access (Strata Cloud Manager)

STEP 1 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** et sélectionnez l'icône d'engrenage pour modifier les paramètres.

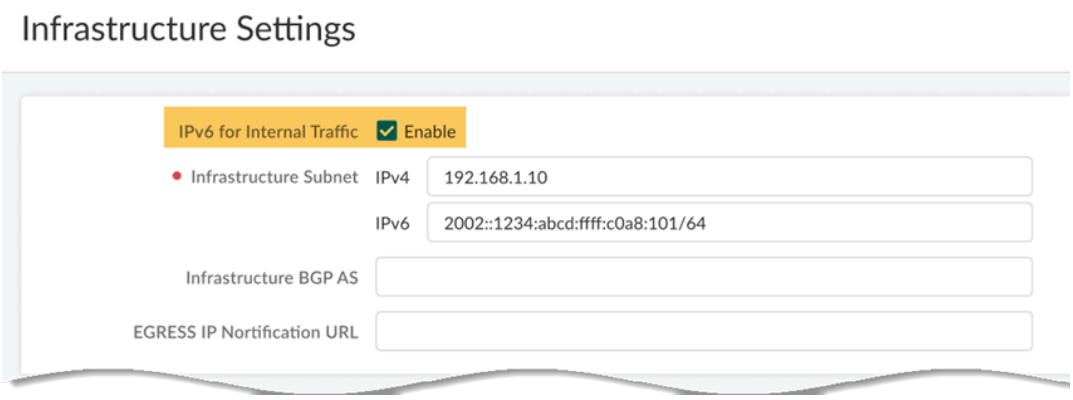
STEP 2 | Cochez la case **Enable (Activer)** pour activer IPv6 pour le trafic interne.

L'activation ou la désactivation d'IPv6 entraîne une brève interruption du trafic (jusqu'à 120 secondes) pendant que le plan de données se prépare à accepter ou à rejeter les itinéraires IPv6 sur la zone principale Prisma Access. Palo Alto Networks vous recommande de

 ©2025 Palo Alto Networks, Inc.

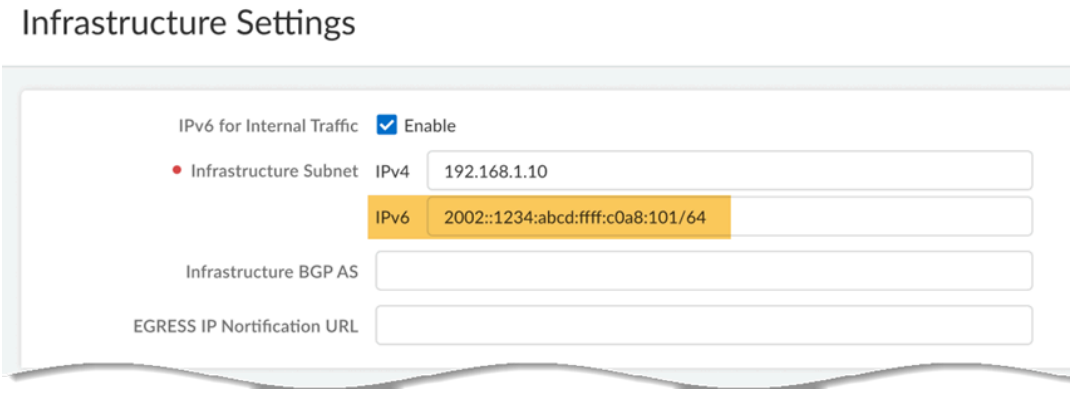
valider ce changement de configuration pendant une fenêtre de maintenance ou pendant les heures creuses.

Si vous devez supprimer IPv6, supprimez toute la configuration (y compris pour les utilisateurs mobiles, le réseau distant et les connexions aux services, le cas échéant) avant de décocher la case ***Enable IPv6 (Activer IPv6)*** *pour le trafic interne.*



STEP 3 | Spécifiez un sous-réseau d'infrastructure **IPv6** et une **Infrastructure BGP AS**.

- Spécifiez un sous-réseau minimum de /96.
- Vous devez également entrer un sous-réseau IPv4. Prisma Access nécessite des sous-réseaux IPv4 et IPv6 dans son infrastructure réseau pour utiliser IPv6. Pour plus d'informations, reportez-vous à la sectionGestion de l'infrastructure Prisma Access.
- Palo Alto Networks vous recommande d'utiliser des adresses IPv4 et IPv6 privées (et non publiques).
- N'utilisez pas d'adresses locales de liaison IPv6 (fe80::/10).



STEP 4 | Entrez l'**Infrastructure BGP AS** que vous souhaitez utiliser dans l'infrastructure Prisma Access.

Si vous souhaitez utiliser le routage dynamique pour activer Prisma Access afin de découvrir dynamiquement les itinéraires vers les ressources sur vos réseaux distants et les emplacements de votre siège/centre de données, spécifiez le numéro du système autonome (AS). Si vous ne fournissez pas de numéro AS, le numéro AS par défaut 65534 sera utilisé.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Si ce n'est pas déjà fait, envisagez d'ajouter des serveurs DNS internes pour permettre à Prisma Access de résoudre vos domaines internes pour accéder à des services, tels que LDAP et le serveur DNS, sur votre réseau d'entreprise.

Pour plus d'informations, reportez-vous à la sectionGestion de l'infrastructure Prisma Access.

STEP 6 | (Déploiements d'utilisateurs mobiles uniquement) Ajouter des pools d'adresses IP IPv6 pour votre déploiement d'utilisateurs mobiles GlobalProtect.

Un déploiement d'utilisateurs mobiles GlobalProtect nécessite des pools d'adresses IP. Les pools d'adresses IP IPv4 et IPv6 sont requis pour activer la fonctionnalité IPv6. Appliquez des adresses IPv4 au niveau régional ou mondial. Appliquez des adresses IPv6 à un niveau mondial. Spécifiez un sous-réseau minimum de /80.

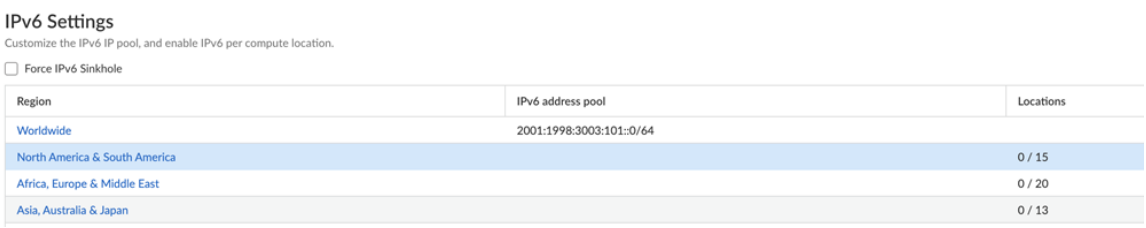
Prisma Access subdivise les adresses IPv6 mondiales à l'aide de la méthode suivante :

- Prisma Access attribue à chaque emplacement (passerelle) un pool à partir d'un sous-réseau /112. Étant donné que chaque connexion GlobalProtect utilise une adresse IP du pool, cette allocation permet d'attribuer plus de 65 000 adresses IPv6 disponibles aux terminaux des utilisateurs par emplacement.

  Si vous rencontrez un événement de mise à l'échelle automatique (si un grand nombre d'utilisateurs se connectent à un seul emplacement Prisma Access), Prisma Access peut ajouter un autre emplacement avec un autre sous-réseau /112.
- Lorsque vous activez un emplacement pour utiliser IPv6, Prisma Access attribue un pool d'adresses IPv6 à la région à laquelle l'emplacement appartient et divise le pool entre le nombre total de régions pour lesquelles IPv6 est activé.

N'utilisez pas d'adresses de liaison locale (fe80::/10) dans un pool d'adresses IP.

1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** et sélectionnez l'icône d'engrenage pour modifier les paramètres d'infrastructure.
2. Dans la section Client IP Pools (Pools d'adresses IP client), sélectionnez une **Region (Région)** ou cliquez sur **Add IP Portal (Ajouter un portail IP)**.
3. Entrez dans un **IPv6 Address Pool (Pool d'adresses IPv6)**.
   - Vous devez saisir les adresses IP IPv4 et IPv6 pour les utilisateurs mobiles. Prisma Access nécessite des adresses IPv4 et IPv6 pour prendre en charge son infrastructure interne lors de l'utilisation d'IPv6.
   - Entrez un sous-réseau IPv6 minimum de /80.
   - Prisma Access subdivise chaque sous-réseau par région.



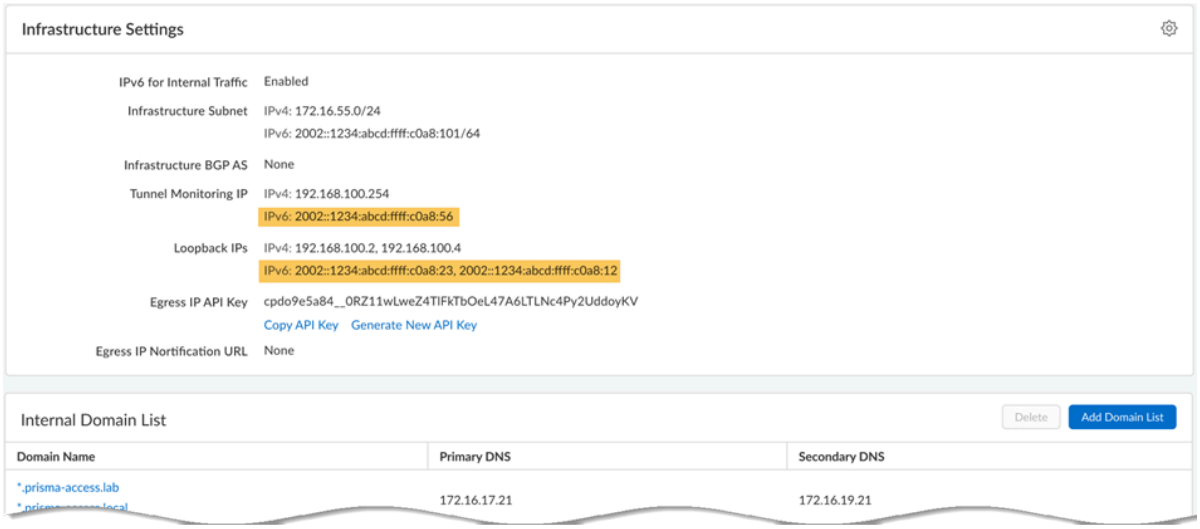
 ©2025 Palo Alto Networks, Inc.

STEP 7 | Cliquez sur **Save (Enregistrer)** et sur **Push Config (Transmettre la configuration)**.

STEP 8 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** et notez les adresses IPv6 suivantes dans vos paramètres d'infrastructure :

- Option **Captive Portal Redirect IP Addresses (Adresses IP de redirection du portail captif)**—Utilisée avec le mappage d'adresses User-ID basé sur le portail d'authentification
- Option **Tunnel Monitor IP Address (Adresse IP de surveillance du tunnel)**—Utilisée pour la surveillance du tunnel

Puisque les utilisateurs mobiles de GlobalProtect ont besoin d'une adresse IPv4 pour les tunnels VPN, les adresses de bouclage, dont les adresses IP sont extraites du sous-réseau d'infrastructure, utilisent toujours des adresses IPv4.



Activer et configurer la mise en réseau IPv6 et les pools d'adresses IP dans votre infrastructure Prisma Access (Panorama)

STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** et cliquez sur l'icône engrenage pour modifier les paramètres.

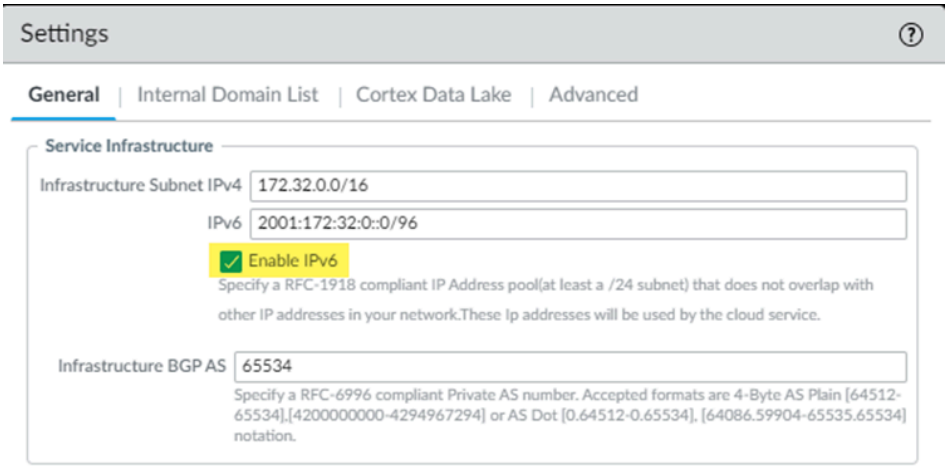
STEP 2 | Sur l'onglet **General (Général)**, sélectionnez **Enable IPv6 (Activer IPv6)**.

L'activation ou la désactivation d'IPv6 entraîne une brève interruption du trafic (jusqu'à 120 secondes) pendant que le plan de données se prépare à accepter ou à rejeter les itinéraires IPv6 sur la zone principale Prisma Access. Palo Alto Networks vous recommande de

 ©2025 Palo Alto Networks, Inc.

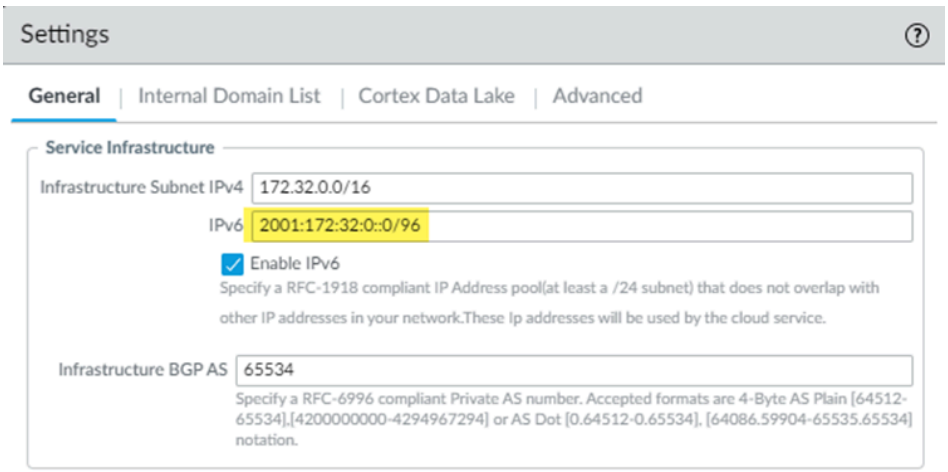
valider ce changement de configuration pendant une fenêtre de maintenance ou pendant les heures creuses.

Si vous devez supprimer IPv6, supprimez toute la configuration (y compris pour les utilisateurs mobiles, le réseau distant et les connexions aux services, le cas échéant) avant de décocher la case ***Enable IPv6 (Activer IPv6)****.*



STEP 3 | Spécifiez un sous-réseau d'infrastructure **IPv6** et une **Infrastructure BGP AS**.

- Spécifiez un sous-réseau minimum de /96.
- Vous devez également entrer un sous-réseau IPv4. Prisma Access nécessite des sous-réseaux IPv4 et IPv6 dans son infrastructure réseau pour utiliser IPv6. Pour plus d'informations, reportez-vous à la sectionConfigurer l'infrastructure de service Prisma Access (Panorama).
- Palo Alto Networks vous recommande d'utiliser des adresses IPv4 et IPv6 privées (et non publiques).
- N'utilisez pas d'adresses locales de liaison IPv6 (fe80::/10).



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Entrez l'**Infrastructure BGP AS** que vous souhaitez utiliser dans l'infrastructure Prisma Access.

Si vous souhaitez utiliser le routage dynamique pour activer Prisma Access afin de découvrir dynamiquement les itinéraires vers les ressources sur vos réseaux distants et les emplacements de votre siège/centre de données, spécifiez le numéro du système autonome (AS). Si vous ne fournissez pas de numéro AS, le numéro AS par défaut 65534 sera utilisé.

STEP 5 | Si vous n'avez pas encore terminé la configuration du service, entrez les paramètres **Internal Domain List (Liste de domaines internes)**, **Strata Logging Service (Service de journalisation Strata** et **Advanced (Avancés)**.

Pour plus d'informations, reportez-vous à la sectionConfigurer l'infrastructure de service Prisma Access (Panorama).

STEP 6 | (Déploiements d'utilisateurs mobiles uniquement) Ajouter des pools d'adresses IP IPv6 pour votre déploiement d'utilisateurs mobiles GlobalProtect.

Un déploiement d'utilisateurs mobiles GlobalProtect nécessite des pools d'adresses IP. Les pools d'adresses IP IPv4 et IPv6 sont requis pour activer la fonctionnalité IPv6. Appliquez des adresses IPv4 au niveau régional ou mondial. Appliquez des adresses IPv6 à un niveau mondial. Spécifiez un sous-réseau minimum de /80.

Prisma Access subdivise les adresses IPv6 mondiales à l'aide de la méthode suivante :

- Prisma Access attribue à chaque emplacement (passerelle) un pool à partir d'un sous-réseau /112. Étant donné que chaque connexion GlobalProtect utilise une adresse IP du

 ©2025 Palo Alto Networks, Inc.

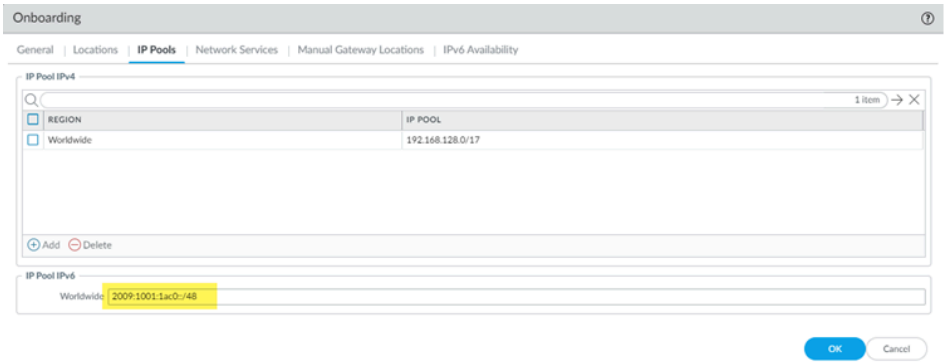
pool, cette allocation permet d'attribuer plus de 65 000 adresses IPv6 disponibles aux terminaux des utilisateurs par emplacement.

Si vous rencontrez un événement de mise à l'échelle automatique (si un grand nombre d'utilisateurs se connectent à un seul emplacement Prisma Access), Prisma Access peut ajouter un autre emplacement avec un autre sous-réseau /112.

- Lorsque vous activez un emplacement pour utiliser IPv6, Prisma Access attribue un pool d'adresses IPv6 à la région à laquelle l'emplacement appartient et divise le pool entre le nombre total de régions pour lesquelles IPv6 est activé.

N'utilisez pas d'adresses de liaison locale (fe80::/10) dans un pool d'adresses IP.

1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users—GlobalProtect (Utilisateurs mobiles — GlobalProtect)**.
2. Dans la section Onboarding (Intégration), sélectionnez le **Hostname (Nom d'hôte)** du portail ou sélectionnez **Configure (Configurer)**.
3. Sélectionnez l'onglet **IP Pools (Pools d'adresses IP)**.
4. Entrez un **IP Pool IPv6 (Pool d'adresses IP IPv6)**.
   - Vous devez saisir les adresses IP IPv4 et IPv6 pour les utilisateurs mobiles. Prisma Access nécessite des adresses IPv4 et IPv6 pour prendre en charge son infrastructure interne lors de l'utilisation d'IPv6.
   - Entrez un sous-réseau IPv6 minimum de /80.
   - Prisma Access subdivise chaque sous-réseau par région.



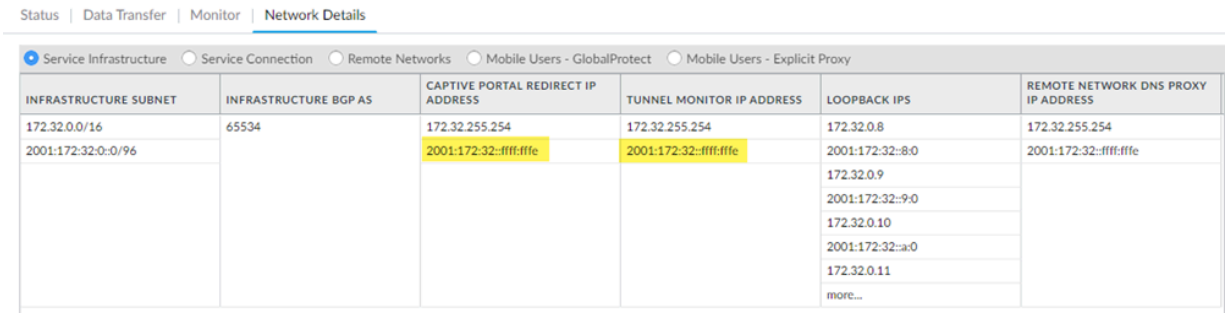
STEP 7 | **Commit and Push (Validez et appliquez)** vos modifications.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Infrastructure (Infrastructure du service)** et notez les adresses IPv6 suivantes :

- Option **Captive Portal Redirect IP Addresses (Adresses IP de redirection du portail captif)**—Utilisée avec le mappage d'adresses User-ID basé sur le portail d'authentification
- Option **Tunnel Monitor IP Address (Adresse IP de surveillance du tunnel)**—Utilisée pour la surveillance du tunnel

Puisque les utilisateurs mobiles de GlobalProtect ont besoin d'une adresse IPv4 pour les tunnels VPN, les adresses de bouclage, dont les adresses IP sont extraites du sous-réseau d'infrastructure, utilisent toujours des adresses IPv4.



Activer la mise en réseau IPv6 pour les utilisateurs mobiles – Déploiement de GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access 2.2 préférée et versions ultérieures ❑ L'accès IPv6 natif aux applications publiques et privées nécessite les versions minimales suivantes : • Prisma Access (Managed by Strata Cloud Manager) : publication en juin 2024 • Prisma Access (Managed by Panorama) : Prisma Access 5.1.1 pour les nouveaux déploiements uniquement. Tous les autres déploiements (y compris les déploiements Prisma Access (Managed by Panorama) existants) prennent uniquement en charge l'accès aux applications privées.

En plus de spécifier les pools d'adresses IP des utilisateurs mobiles, vous devez configurer la **IPv6 Availability (Disponibilité IPv6)** pour vos utilisateurs mobiles – déploiements GlobalProtect. Si votre réseau utilise des serveurs DNS IPv6 pour résoudre des domaines internes, vous pouvez

 ©2025 Palo Alto Networks, Inc.

également spécifier des adresses IPv6 pour les serveurs DNS principaux et secondaires, comme indiqué dans la section suivante.

- Strata Cloud Manager
- Panorama

Activer la mise en réseau IPv6 pour les utilisateurs mobiles – Déploiement de GlobalProtect (Strata Cloud Manager)

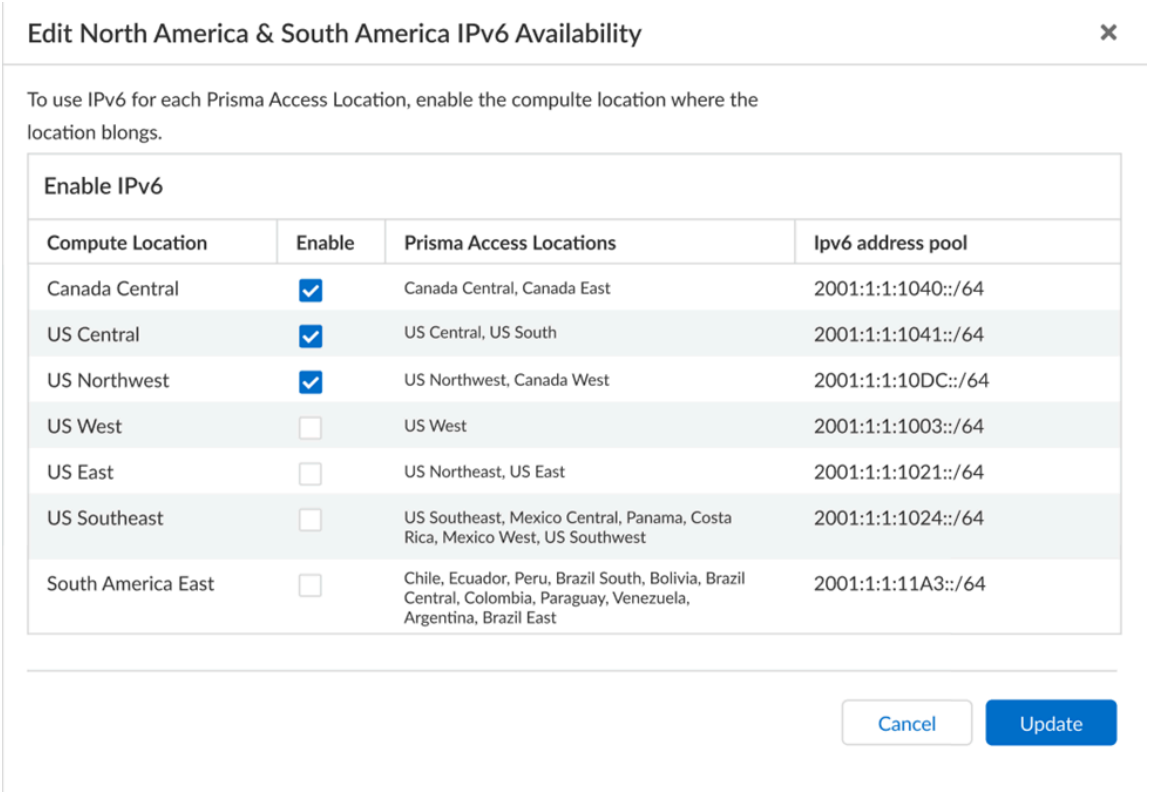
En plus de spécifier les pools d'adresses IP des utilisateurs mobiles, vous devez configurer la **IPv6 Availability (Disponibilité IPv6)** pour vos utilisateurs mobiles – déploiements GlobalProtect. Si votre réseau utilise des serveurs DNS IPv6 pour résoudre des domaines internes, vous pouvez également spécifier des adresses IPv6 pour les serveurs DNS principaux et secondaires, comme indiqué dans la section suivante.

STEP 1 | Planifiez si vous souhaitez déployer IPv6 sur l'ensemble de votre déploiement Prisma Access, ou seulement pour un certain nombre d'emplacements de calcul.

STEP 2 | Configurez la disponibilité d'IPv6 pour les régions où vous souhaitez déployer IPv6.

1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** et sélectionnez l'icône d'engrenage pour modifier les **Infrastructure Settings (Paramètres d'infrastructure)**.
2. Dans la section **IPv6 Settings (Paramètres IPv6)**, choisissez les emplacements pour lesquels vous souhaitez **Enable (Activer)** IPv6.

   Tous les emplacements sont associés à un emplacement de calcul. Si IPv6 n'est pas activé pour les emplacements dans un emplacement de calcul, laissez cet emplacement de calcul désélectionné.



 ©2025 Palo Alto Networks, Inc.

STEP 3 | (Facultatif) Si vos serveurs DNS internes sont accessibles par des adresses IPv6, sélectionnez **Add Region (Ajouter une région)** dans la section **Client DNS (DNS client)**, cochez la case pour **Resolve Internal Domains (Résoudre les domaines internes)**, **Add (Ajoutez)** une règle ou spécifiez la règle par défaut, et spécifiez les adresses IPv6 de serveurs DNS **Custom (Personnalisés)** pour le serveur **Primary DNS (DNS principal)** et le serveur **Secondary DNS (DNS secondaire)**.

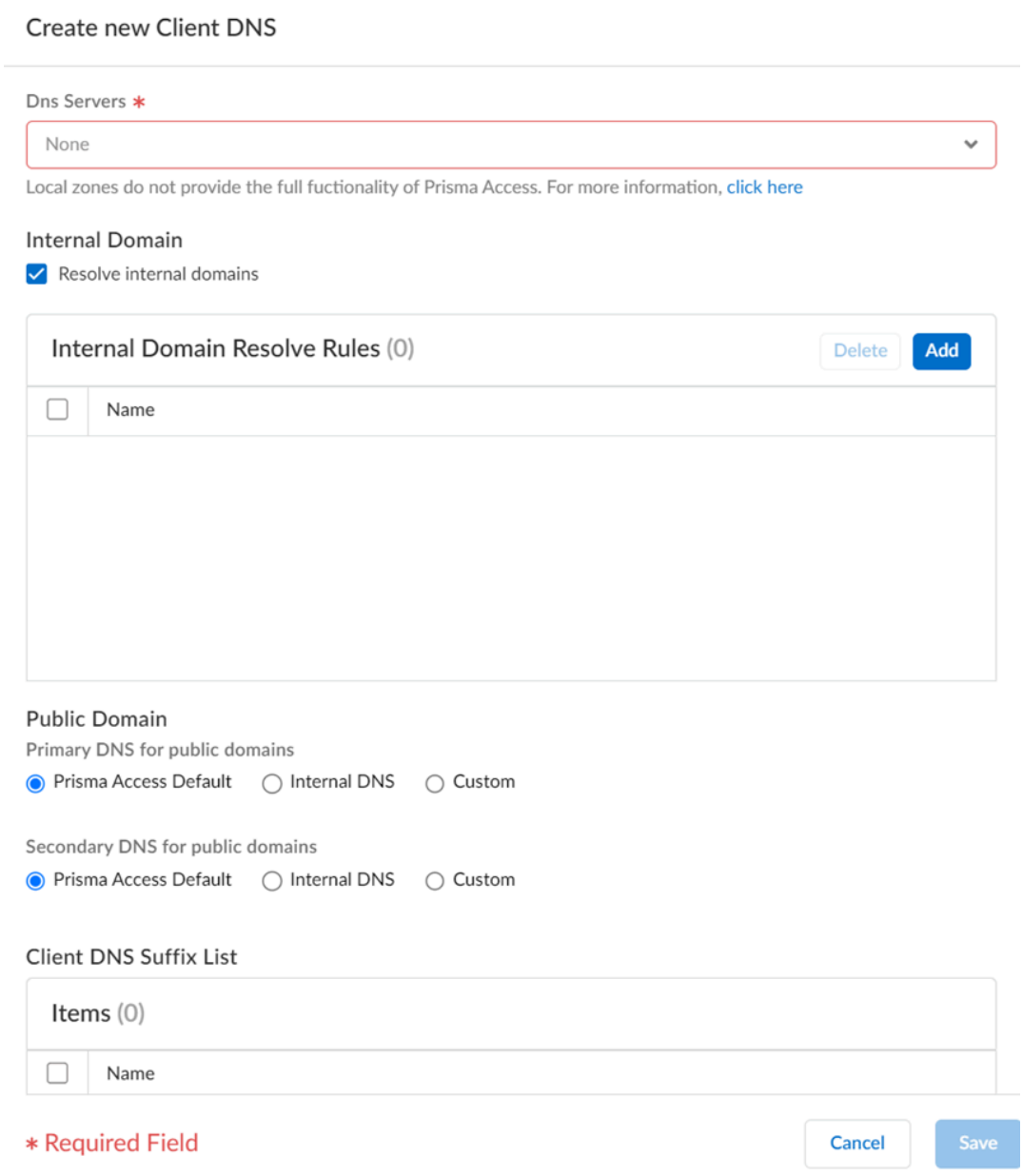
Si vous saisissez des adresses IPv6 pour les serveurs DNS, vous devez également avoir des adresses IPv6 dans votre pool d'adresses IP des utilisateurs mobiles.

Vous pouvez saisir n'importe quelle combinaison d'adresses IPv4 ou IPv6 pour les serveurs DNS principaux et secondaires. Si vous saisissez une adresse IPv6 pour le serveur DNS principal et une adresse IPv4 pour le serveur DNS secondaire, et qu'une requête DNS est reçue d'un emplacement de calcul qui n'a pas la **IPv6 Availability**

 ©2025 Palo Alto Networks, Inc.

(Disponibilité IPv6) activée, Prisma Access utilise le serveur DNS secondaire, car il utilise une adresse IPv4.

Les adresses IPv4 utilisent des enregistrements A, tandis que les adresses IPv6 utilisent des enregistrements AAAA. Certains serveurs DNS peuvent effectuer des recherches DNS AAAA sur un transport IPv4 ; par conséquent, vous n'aurez peut-être pas besoin d'un serveur avec une adresse IP IPv6.



STEP 4 | (Facultatif) Si vous n'avez pas encore terminé la configuration des utilisateurs mobiles, terminez-la maintenant. Reportez-vous à la section Configurez les utilisateurs mobiles GlobalProtect pour plus de détails.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | **Push Config (Transmettez la configuration)** pour déployer vos modifications sur votre réseau.

Activer la mise en réseau IPv6 pour les utilisateurs mobiles – Déploiement de GlobalProtect (Panorama)

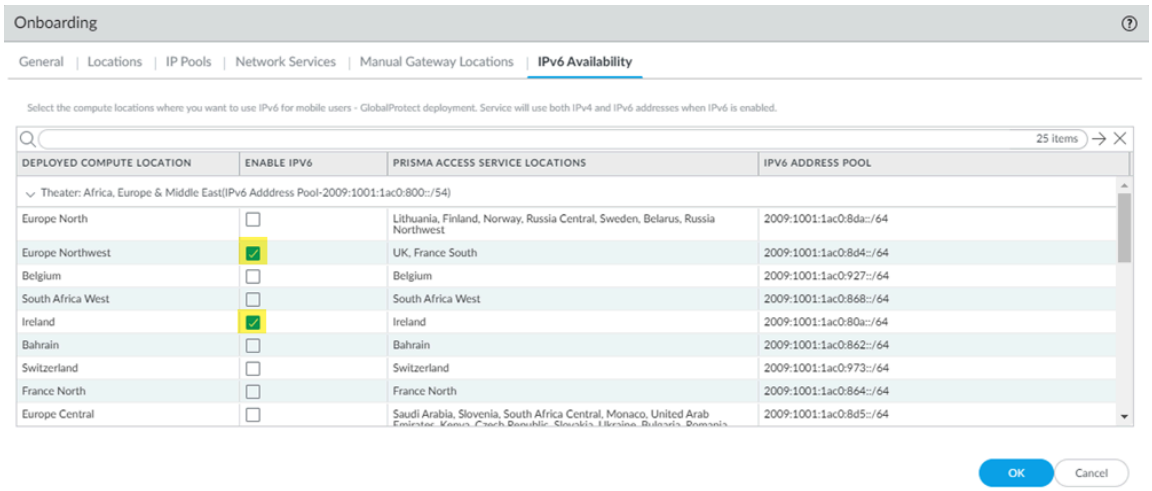
En plus de spécifier les pools d'adresses IP des utilisateurs mobiles, vous devez configurer la **IPv6 Availability (Disponibilité IPv6)** pour vos utilisateurs mobiles – déploiements GlobalProtect. Si votre réseau utilise des serveurs DNS IPv6 pour résoudre des domaines internes, vous pouvez également spécifier des adresses IPv6 pour les serveurs DNS principaux et secondaires, comme indiqué dans la section suivante.

STEP 1 | Planifiez si vous souhaitez déployer IPv6 sur l'ensemble de votre déploiement <ph keyref="pa"/>, ou seulement pour un certain nombre d'emplacements de calcul.

STEP 2 | Configurez la disponibilité d'IPv6 pour les régions où vous souhaitez déployer IPv6.

1. Dans l'onglet **IPv6 Availability (Disponibilité IPv6)**, **Enable IPv6 (Activez IPv6)** pour les emplacements pour lesquels vous souhaitez activer IPv6.

   Tous les emplacements sont associés à un emplacement de calcul. Si IPv6 n'est pas activé pour les emplacements dans un emplacement de calcul, laissez cet emplacement de calcul désélectionné.



STEP 3 | (Facultatif) Si vos serveurs DNS internes sont accessibles par des adresses IPv6, cliquez sur l'onglet **Network Services (Services réseau)**, **Add (Ajoutez)** une règle ou spécifiez la règle par défaut, et spécifiez les adresses IPv6 de **Custom DNS Server (serveurs DNS personnalisés)** pour le serveur **Primary DNS (DNS principal)** et le serveur **Secondary DNS (DNS secondaire)**.

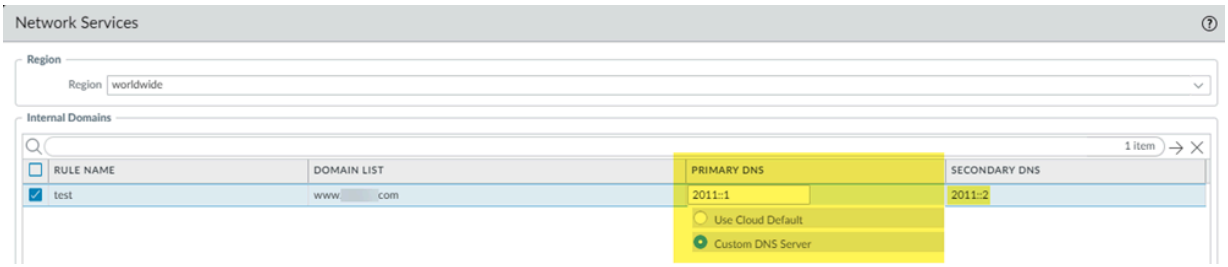
Si vous saisissez des adresses IPv6 pour les serveurs DNS, vous devez également avoir des adresses IPv6 dans votre pool d'adresses IP des utilisateurs mobiles.

Vous pouvez saisir n'importe quelle combinaison d'adresses IPv4 ou IPv6 pour les serveurs DNS principaux et secondaires. Si vous saisissez une adresse IPv6 pour le serveur DNS principal et une adresse IPv4 pour le serveur DNS secondaire, et qu'une requête DNS est reçue d'un emplacement de calcul qui n'a pas la **IPv6 Availability**

 ©2025 Palo Alto Networks, Inc.

(Disponibilité IPv6) activée, <ph keyref="pa"/> utilise le serveur DNS secondaire, car il utilise une adresse IPv4.

Les adresses IPv4 utilisent des enregistrements A, tandis que les adresses IPv6 utilisent des enregistrements AAAA. Certains serveurs DNS peuvent effectuer des recherches DNS AAAA sur un transport IPv4 ; par conséquent, vous n'aurez peut-être pas besoin d'un serveur avec une adresse IP IPv6.



STEP 4 | (Facultatif) Si vous n'avez pas encore terminé la configuration des utilisateurs mobiles, terminez-la maintenant. Reportez-vous à la section Configurez les utilisateurs mobiles GlobalProtect pour plus de détails.

STEP 5 | **Commit and Push (Validez et appliquez)** vos modifications.

Activer la mise en réseau IPv6 pour les connexions aux services

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access 2.2 préférée et versions ultérieures ❑ L'accès IPv6 natif aux applications publiques et privées nécessite les versions minimales suivantes : • Prisma Access (Managed by Strata Cloud Manager) : publication en juin 2024 • Prisma Access (Managed by Panorama) : Prisma Access 5.1.1 pour les nouveaux déploiements uniquement. Tous les autres déploiements (y compris les déploiements Prisma Access (Managed by Panorama) existants) prennent uniquement en charge l'accès aux applications privées.

Pour les connexions aux services, vous pouvez utiliser les sous-réseaux IPv6 pour le routage statique ou BGP. Pour le routage BGP, vous pouvez saisir des adresses de l'homologue IPv6 et spécifier les options de routage IPv4 et IPv6.

 ©2025 Palo Alto Networks, Inc.

Pour configurer la mise en réseau IPv6 pour les connexions aux services, effectuez la tâche suivante.

- Prisma Access (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Panorama)

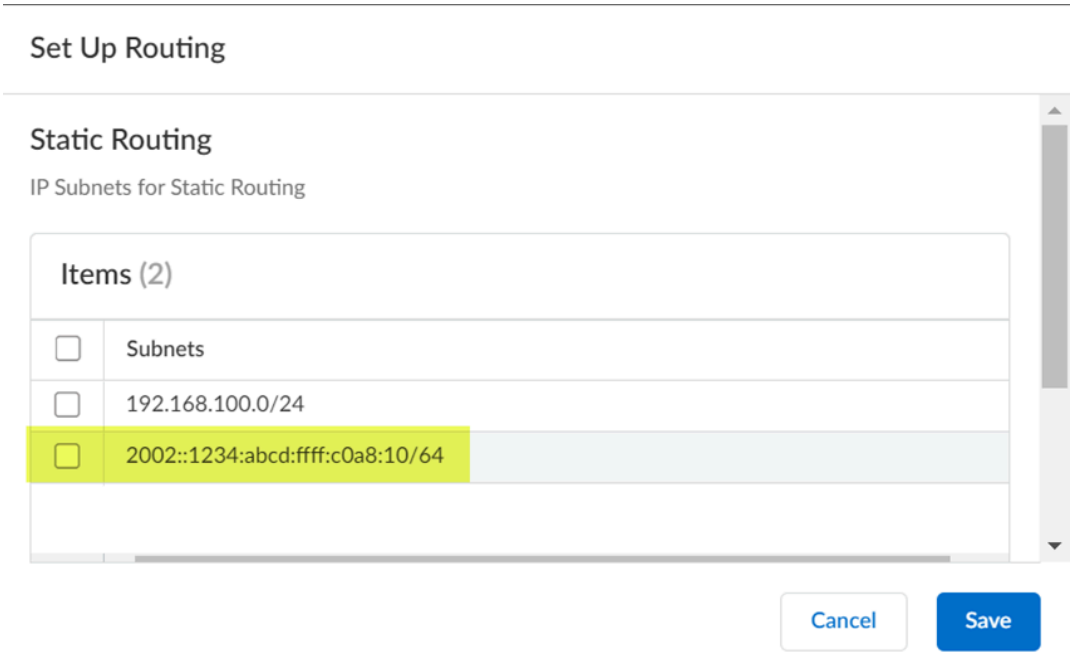
Activer la mise en réseau IPv6 pour les connexions aux services (Strata Cloud Manager)

STEP 1 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connections (Connexions aux services)** et **Add Service Connection (Ajouter une connexion aux services)**.

STEP 2 | Ajoutez une nouvelle connexion aux services ou sélectionnez une connexion aux services existante pour la modifier.

STEP 3 | Configurez le routage IPv6 pour la connexion aux services.

1. (Déploiements de routage statique uniquement) Saisissez un ou plusieurs **Corporate Subnets (Sous-réseaux d'entreprise)** dans l'onglet **Static Routes (Itinéraires statiques)**.



2. (Déploiements de routage BGP uniquement) Spécifiez la méthode d'échange des itinéraires BGP IPv4 et IPv6 ; ensuite, saisissez une **Peer Address (Adresse de l'homologue)** et une **Local Address (Adresse locale)** IPv6.
   - Pour utiliser une seule session BGP IPv4 pour échanger des informations d'appairage BGP IPv4 et IPv6, sélectionnez **Exchange both IPv4 and IPv6 routes over IPv4 peering (Échanger des itinéraires IPv4 et IPv6 via l'appairage IPv4)**.
   - Pour utiliser une session BGP IPv4 pour échanger des informations d'appairage BGP IPv4 et une session IPv6 pour échanger des informations d'appairage BGP IPv6, sélectionnez **Exchange IPv4 routes over IPv4 peering and IPv6 routes over IPv6**

 ©2025 Palo Alto Networks, Inc.

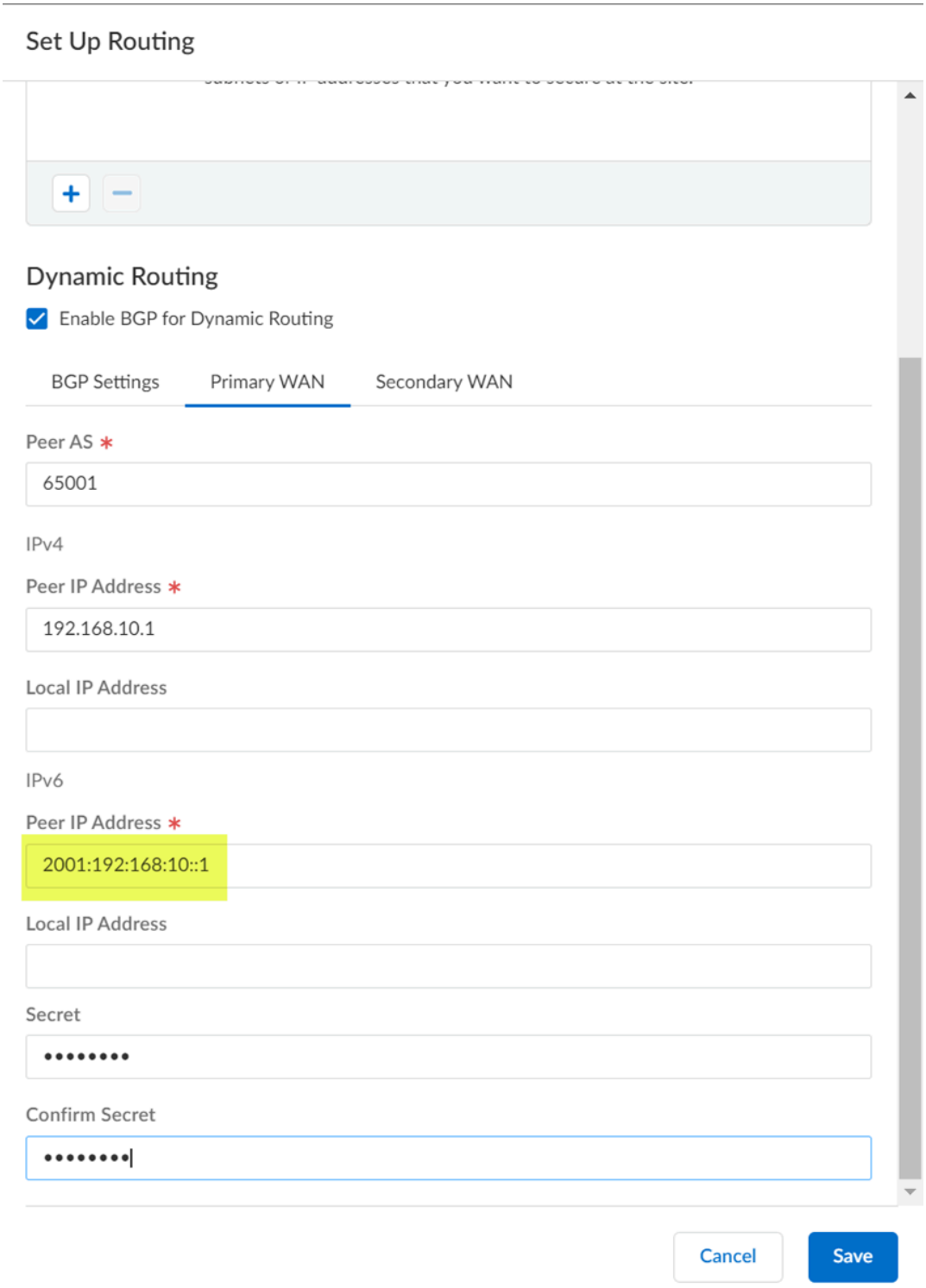
peering (Échanger des itinéraires IPv4 via l'appairage IPv4 et des itinéraires IPv6 via l'appairage IPv6).

- Pour utiliser une seule session BGP IPv6 pour échanger des informations d'appairage BGP IPv6, sélectionnez **Exchange IPv6 routes over IPv6 peering (Échanger des itinéraires IPv6 via l'appairage IPv6)**.

3. Si votre WAN secondaire utilise une adresse de l'homologue ou une adresse locale différente, désélectionnez **Same as Primary WAN (Identique au WAN principal)** et

 ©2025 Palo Alto Networks, Inc.

saisissez la **Peer Address (Adresse de l'homologue)** et la **Local Address (Adresse locale)** IPv6 pour le WAN secondaire.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Si vous n'avez pas encore terminé la configuration de votre connexion aux services, terminez-la maintenant. Reportez-vous à la section Configurer une connexion aux services dans Prisma Access pour plus de détails.

> *L'accès Internet IPv6 pour les connexions aux services est rendu possible par une connexion sous-jacente, dans laquelle le trafic IPv6 transite par un tunnel IPv4.*

STEP 5 | **Push Config (Transmettez la configuration)** pour déployer vos modifications sur votre réseau.

STEP 6 | Si vous n'avez pas encore terminé la configuration des utilisateurs mobiles, terminez-la maintenant.

Activer la mise en réseau IPv6 pour les connexions aux services (Panorama)

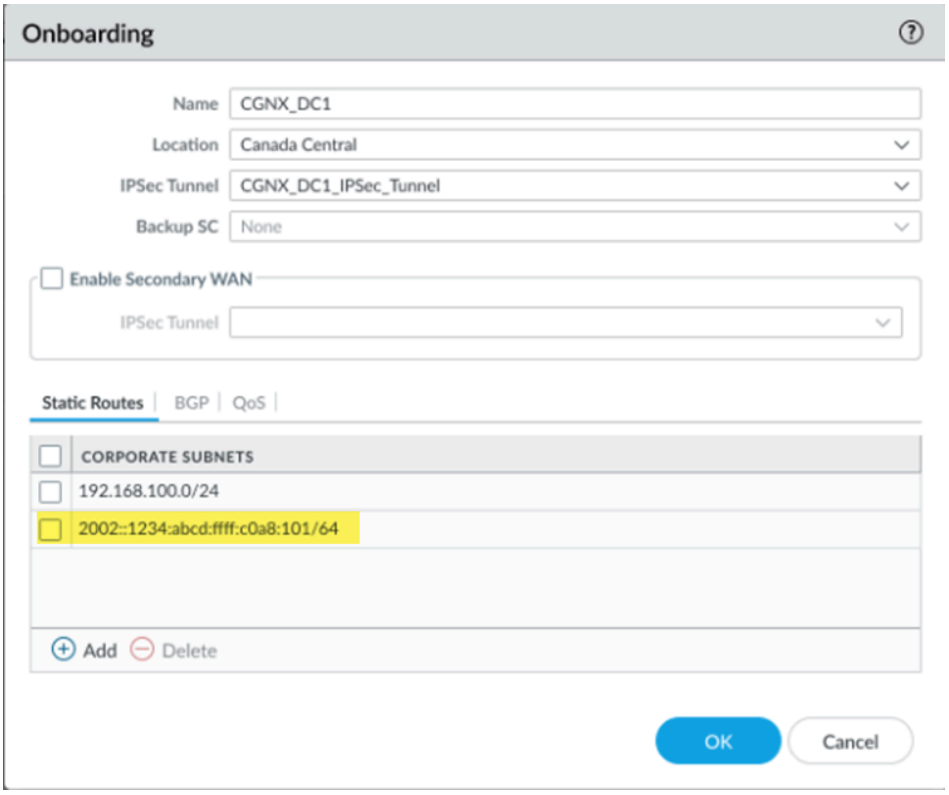
STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Connection (connexion aux services)**.

STEP 2 | **Add (Ajoutez)** une nouvelle connexion aux services ou sélectionnez une connexion aux services existante pour la modifier.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configurez le routage IPv6 pour la connexion aux services.

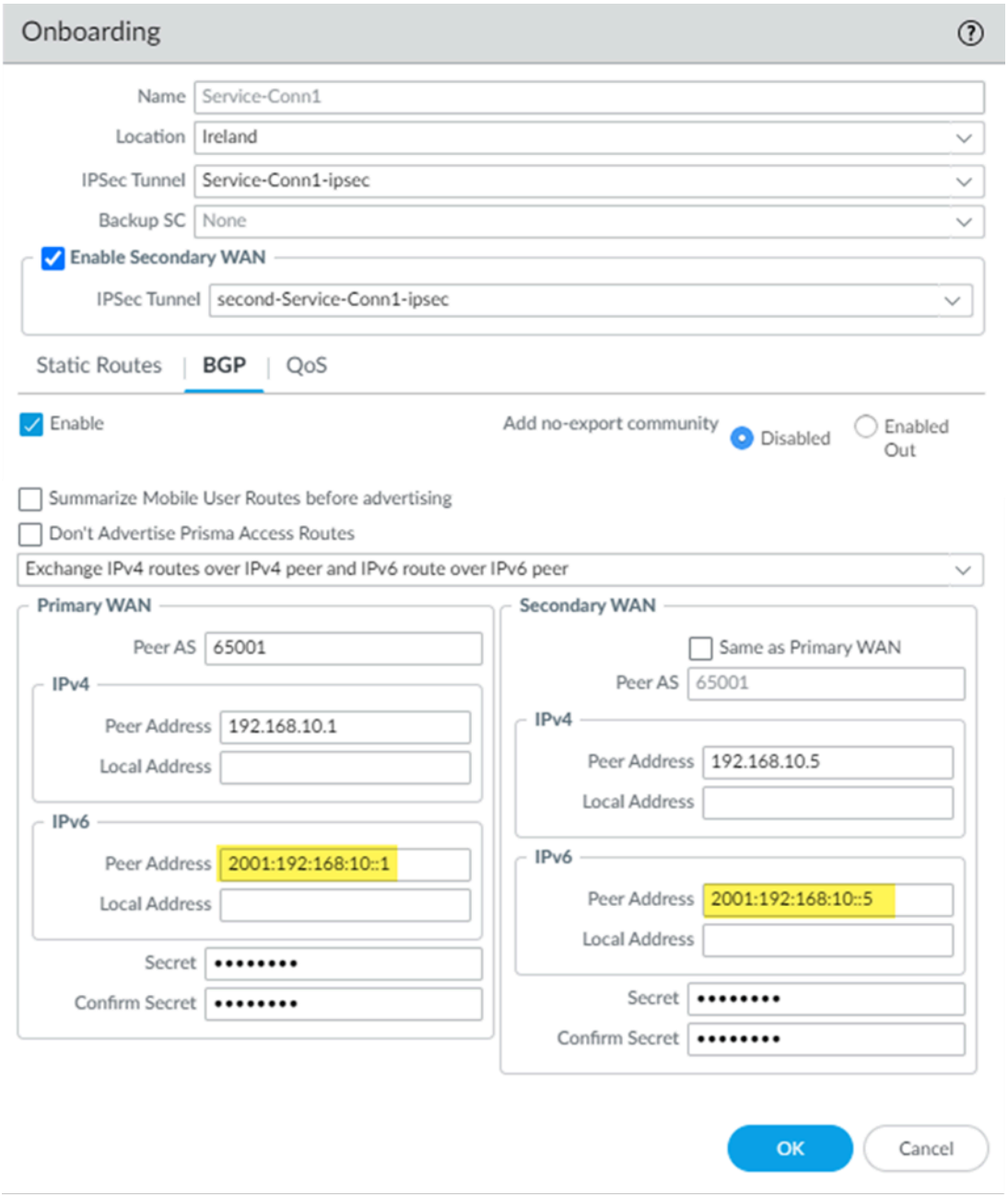
1. (Déploiements de routage statique uniquement) Saisissez un ou plusieurs **Corporate Subnets (Sous-réseaux d'entreprise)** dans l'onglet **Static Routes (Itinéraires statiques)**.



2. (Déploiements de routage BGP uniquement) Spécifiez la méthode d'échange des itinéraires BGP IPv4 et IPv6 ; ensuite, saisissez une **Peer Address (Adresse de l'homologue)** et une **Local Address (Adresse locale)** IPv6.
   - Pour utiliser une seule session BGP IPv4 pour échanger des informations d'appairage BGP IPv4 et IPv6, sélectionnez **Exchange both IPv4 and IPv6 routes over IPv4 peering (Échanger des itinéraires IPv4 et IPv6 via l'appairage IPv4)**.
   - Pour utiliser une session BGP IPv4 pour échanger des informations d'appairage BGP IPv4 et une session IPv6 pour échanger des informations d'appairage BGP IPv6, sélectionnez **Exchange IPv4 routes over IPv4 peering and IPv6 routes over IPv6 peering (Échanger des itinéraires IPv4 via l'appairage IPv4 et des itinéraires IPv6 via l'appairage IPv6)**.
   - Pour utiliser une seule session BGP IPv6 pour échanger des informations d'appairage BGP IPv6, sélectionnez **Exchange IPv6 routes over IPv6 peering (Échanger des itinéraires IPv6 via l'appairage IPv6)**.
3. Si votre WAN secondaire utilise une adresse de l'homologue ou une adresse locale différente, désélectionnez **Same as Primary WAN (Identique au WAN principal)** et

 ©2025 Palo Alto Networks, Inc.

saisissez la **Peer Address (Adresse de l'homologue)** et la **Local Address (Adresse locale)** IPv6 pour le WAN secondaire.



STEP 4 | Si vous n'avez pas encore terminé la configuration de votre connexion aux services, terminez-la maintenant. Reportez-vous à la section Configurer une connexion aux services dans Prisma Access pour plus de détails.

STEP 5 | **Commit and Push (Validez et appliquez)** vos modifications.

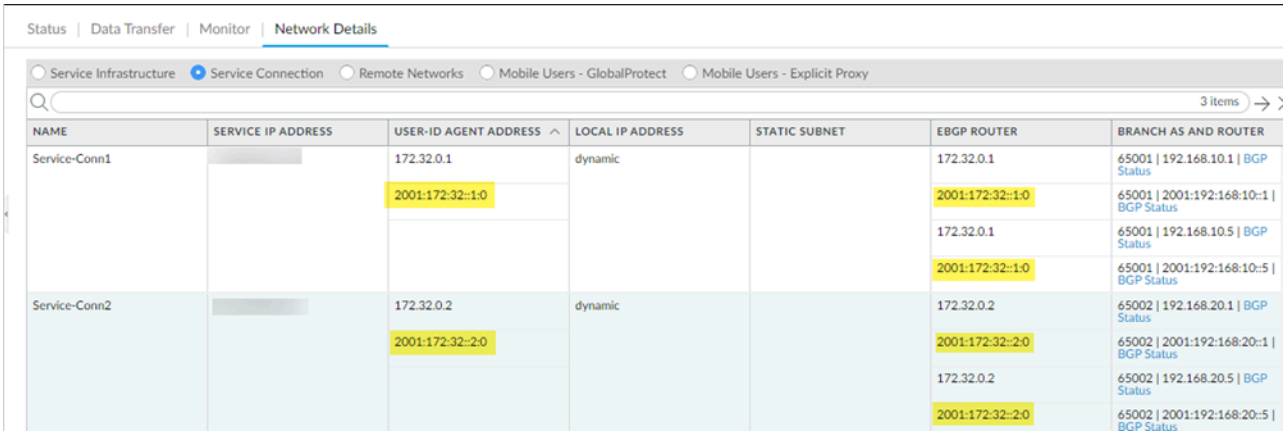
©2025 Palo Alto Networks, Inc.

STEP 6 | Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (connexion aux services)** et notez la **User-ID Agent Address (Adresse de l'agent User-ID)** IPv6 et l'adresse IPv6 du **EBGP Router (Routeur EBGP)**.

Après avoir validé vos modifications, vous disposerez d'une **User-ID Agent Address (Adresse de l'agent User-ID)** IPv6 (utilisée pour la récupération et distribution de User-ID) et d'adresses de **EBGP Router (Routeur EBGP)** pour les connexions aux services.

Étant donné que le tunnel IPSec utilisé pour la connexion aux services utilise l'adressage IPv4, la **Service IP Address (Adresse IP du service)** est une adresse IPv4.

L'accès Internet IPv6 pour les connexions aux services est rendu possible par une connexion sous-jacente, dans laquelle le trafic IPv6 transite par un tunnel IPv4.



STEP 7 | Si vous n'avez pas encore terminé la configuration des utilisateurs mobiles, terminez-la maintenant.

Activer la mise en réseau IPv6 pour les réseaux distants

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access 2.2 préférée et versions ultérieures ❑ L'accès IPv6 natif aux applications publiques et privées nécessite les versions minimales suivantes : • Prisma Access (Managed by Strata Cloud Manager) : publication en juin 2024 • Prisma Access (Managed by Panorama) : Prisma Access 5.1.1 pour les nouveaux déploiements uniquement. Tous les autres déploiements (y compris les déploiements Prisma Access (Managed by Panorama) existants) prennent uniquement en charge l'accès aux applications privées.

 ©2025 Palo Alto Networks, Inc.

Pour les connexions à un réseau distant, vous pouvez utiliser des sous-réseaux IPv6 pour les itinéraires statiques. Pour le routage BGP, vous pouvez saisir des adresses de l'homologue IPv6 et spécifier que BGP utilise uniquement le routage IPv6 ou le routage IPv4 et IPv6.

Pour configurer la mise en réseau IPv6 pour les connexions à un réseau distant, effectuez la tâche suivante.

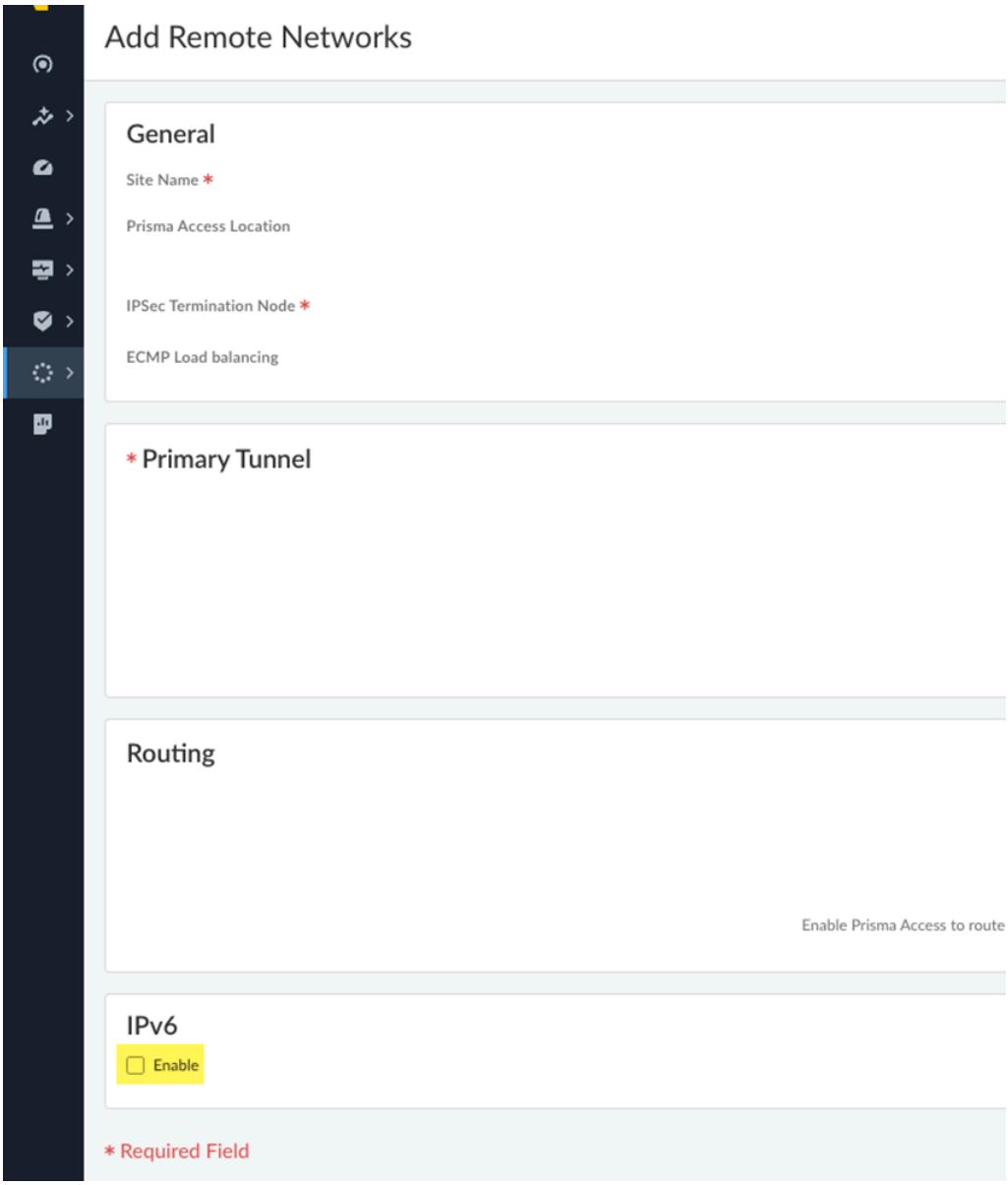
- Prisma Access (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Panorama)

Activer la mise en réseau IPv6 pour les réseaux distants (Strata Cloud Manager)

STEP 1 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Remote Networks (Réseaux distants)**et **Add Remote Networks (Ajouter des réseaux distants)**.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | **Enable (Activez)** IPv6.

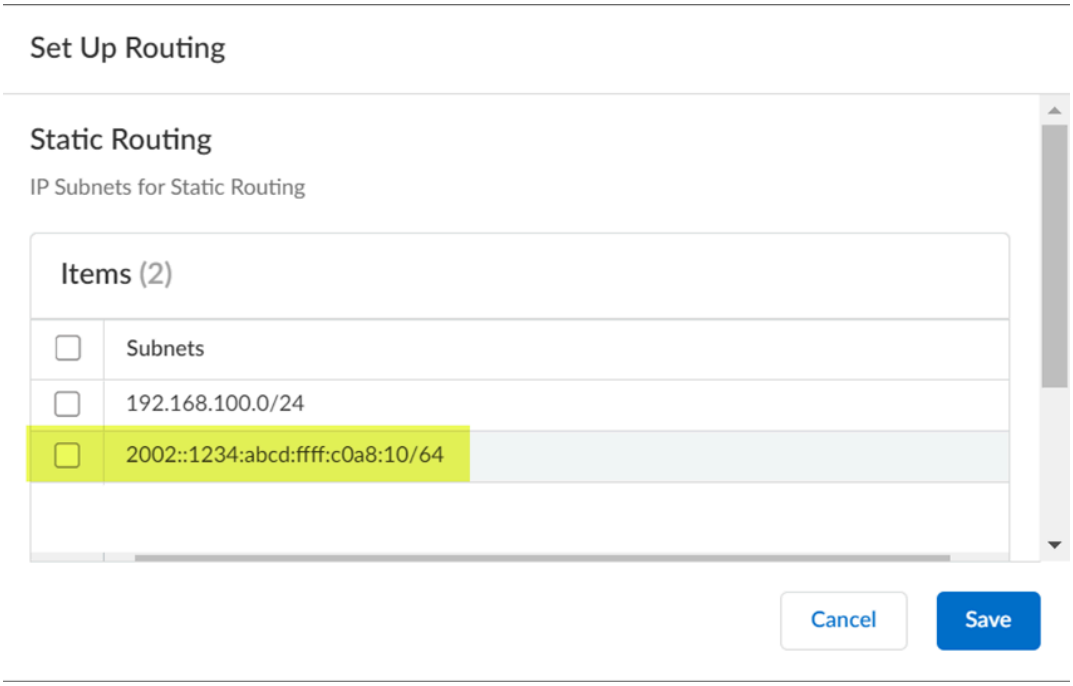


STEP 3 | Ajoutez une nouvelle connexion à un réseau distant ou sélectionnez une connexion à un réseau distant existante pour la modifier.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Configurez le routage IPv6 pour votre réseau distant.

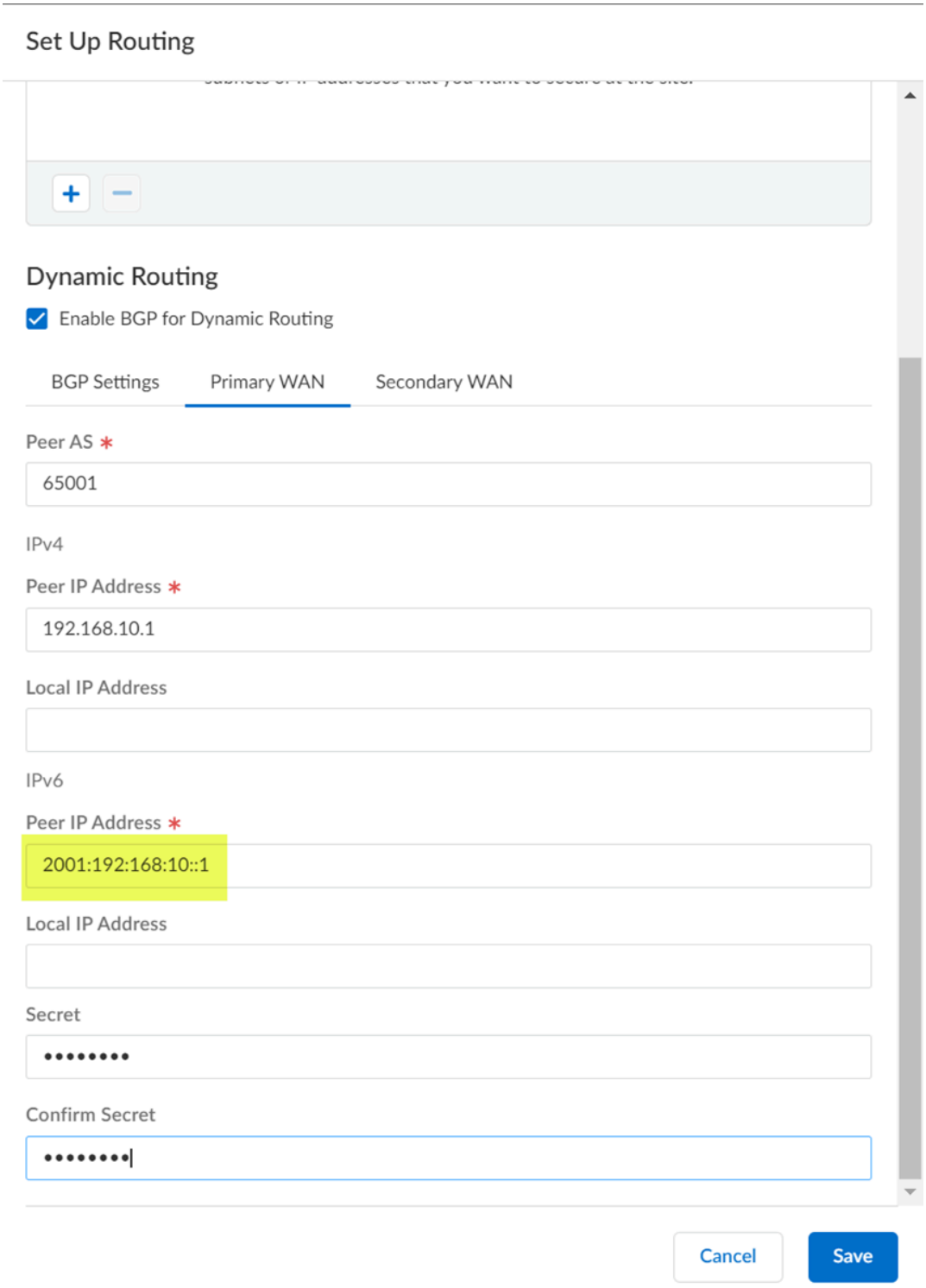
1. (Déploiements de routage statique uniquement) Saisissez un ou plusieurs **Corporate Subnets (Sous-réseaux d'entreprise)** dans l'onglet **Static Routes (Itinéraires statiques)**.



2. (Déploiements de routage BGP uniquement) Spécifiez la méthode d'échange des itinéraires BGP IPv4 et IPv6 ; ensuite, saisissez une **Peer Address (Adresse de l'homologue)** et une **Local Address (Adresse locale)** IPv6.
   - Pour utiliser une seule session BGP IPv4 pour échanger des informations d'appairage BGP IPv4 et IPv6, sélectionnez **Exchange both IPv4 and IPv6 routes over IPv4 peering (Échanger des itinéraires IPv4 et IPv6 via l'appairage IPv4)**.
   - Pour utiliser une session BGP IPv4 pour échanger des informations d'appairage BGP IPv4 et une session IPv6 pour échanger des informations d'appairage BGP IPv6, sélectionnez **Exchange IPv4 routes over IPv4 peering and IPv6 routes over IPv6 peering (Échanger des itinéraires IPv4 via l'appairage IPv4 et des itinéraires IPv6 via l'appairage IPv6)**.
   - Pour utiliser une seule session BGP IPv6 pour échanger des informations d'appairage BGP IPv6, sélectionnez **Exchange IPv6 routes over IPv6 peering (Échanger des itinéraires IPv6 via l'appairage IPv6)**.
3. Si votre WAN secondaire utilise une adresse de l'homologue ou une adresse locale différente, désélectionnez **Same as Primary WAN (Identique au WAN principal)** et

 ©2025 Palo Alto Networks, Inc.

saisissez la **Peer Address (Adresse de l'homologue)** et la **Local Address (Adresse locale)** IPv6 pour le WAN secondaire.



STEP 5 | (Facultatif) Si vos serveurs DNS internes sont accessibles par des adresses IPv6, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Remote Networks (Réseaux distants)** > **Advanced Settings (Paramètres avancés)** cherchez

 ©2025 Palo Alto Networks, Inc.

DNS Proxy (Proxy DNS), **Add (Ajoutez)** une règle ou spécifiez la règle par défaut, puis spécifiez les adresses IPv6 de **Custom DNS Server (Serveur DNS personnalisé)** pour le serveur **Primary DNS (DNS principal)** et le serveur **Secondary DNS (DNS secondaire)**.

Prisma Access vous permet de spécifier les serveurs DNS pour résoudre à la fois les domaines internes à votre organisation et les domaines externes. Si vous ne spécifiez aucun paramètre, Prisma Access ne se procure pas les requêtes DNS pour les réseaux distants. Vous devez également sélectionner une **Region (Région)**.

Vous pouvez saisir n'importe quelle combinaison d'adresses IPv4 ou IPv6 pour les serveurs DNS principaux et secondaires.

- *Les adresses IPv4 utilisent des enregistrements A, tandis que les adresses IPv6 utilisent des enregistrements AAAA. Certains serveurs DNS peuvent effectuer des recherches DNS AAAA sur un transport IPv4 ; par conséquent, vous n'aurez peut-être pas besoin d'un serveur avec une adresse IP IPv6.*

STEP 6 | Si vous n'avez pas encore terminé la configuration de la connexion à un réseau distant, terminez-la maintenant.

L'accès Internet IPv6 pour les connexions à des réseaux distants est rendu possible par une connexion sous-jacente, dans laquelle le trafic IPv6 transite par un tunnel IPv4.

STEP 7 | **Push Config (Transmettez la configuration)** pour déployer vos modifications sur votre réseau.

Activer la mise en réseau IPv6 pour les réseaux distants (Panorama)

STEP 1 | (Facultatif) Saisissez les adresses IPv6 dans la configuration de proxy de votre serveur DNS personnalisé.

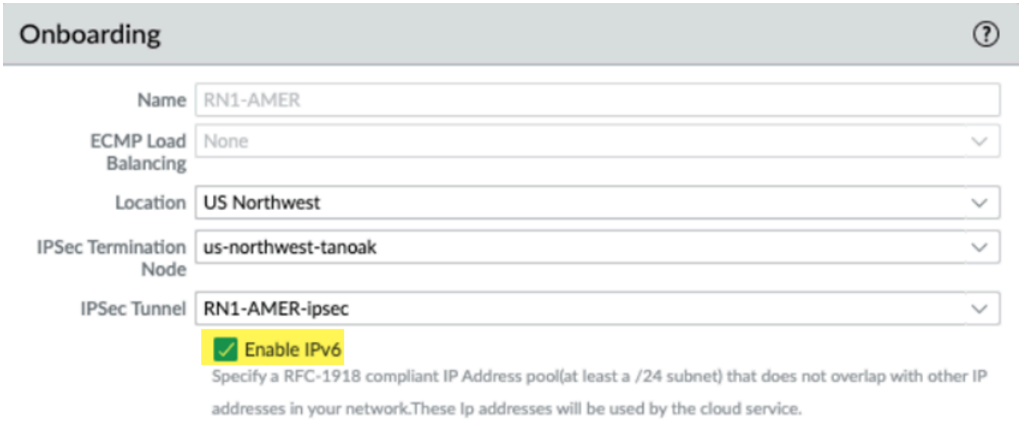
1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** et modifiez les paramètres en cliquant sur l'icône d'engrenage dans la zone **Settings (Paramètres)**.
2. Dans la zone **DNS Proxy (Proxy DNS)**, saisissez les adresses IPv6 de **Custom DNS Server (Serveur DNS personnalisé)** pour vos paramètres de proxy DNS.

STEP 2 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**.

STEP 3 | **Add (Ajoutez)** une nouvelle connexion à un réseau distant ou sélectionnez une connexion à un réseau distant existante pour la modifier.

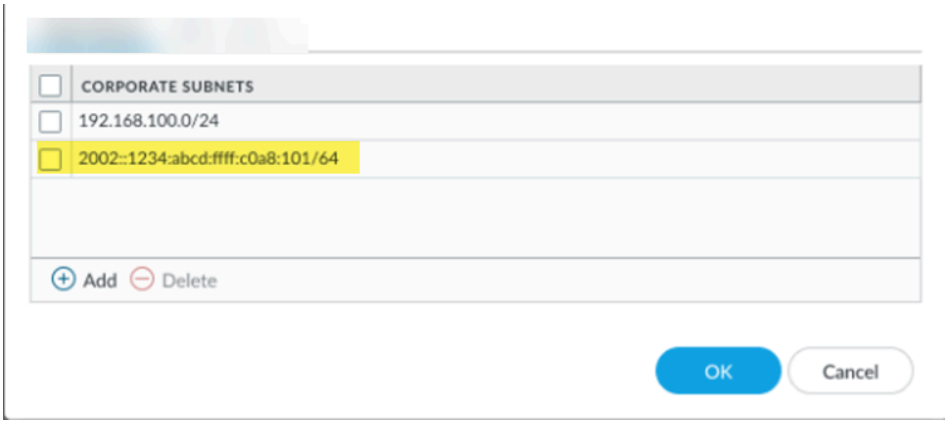
 ©2025 Palo Alto Networks, Inc.

STEP 4 | **Enable IPv6 (Activez IPv6).**



STEP 5 | Configurez le routage IPv6 pour votre réseau distant.

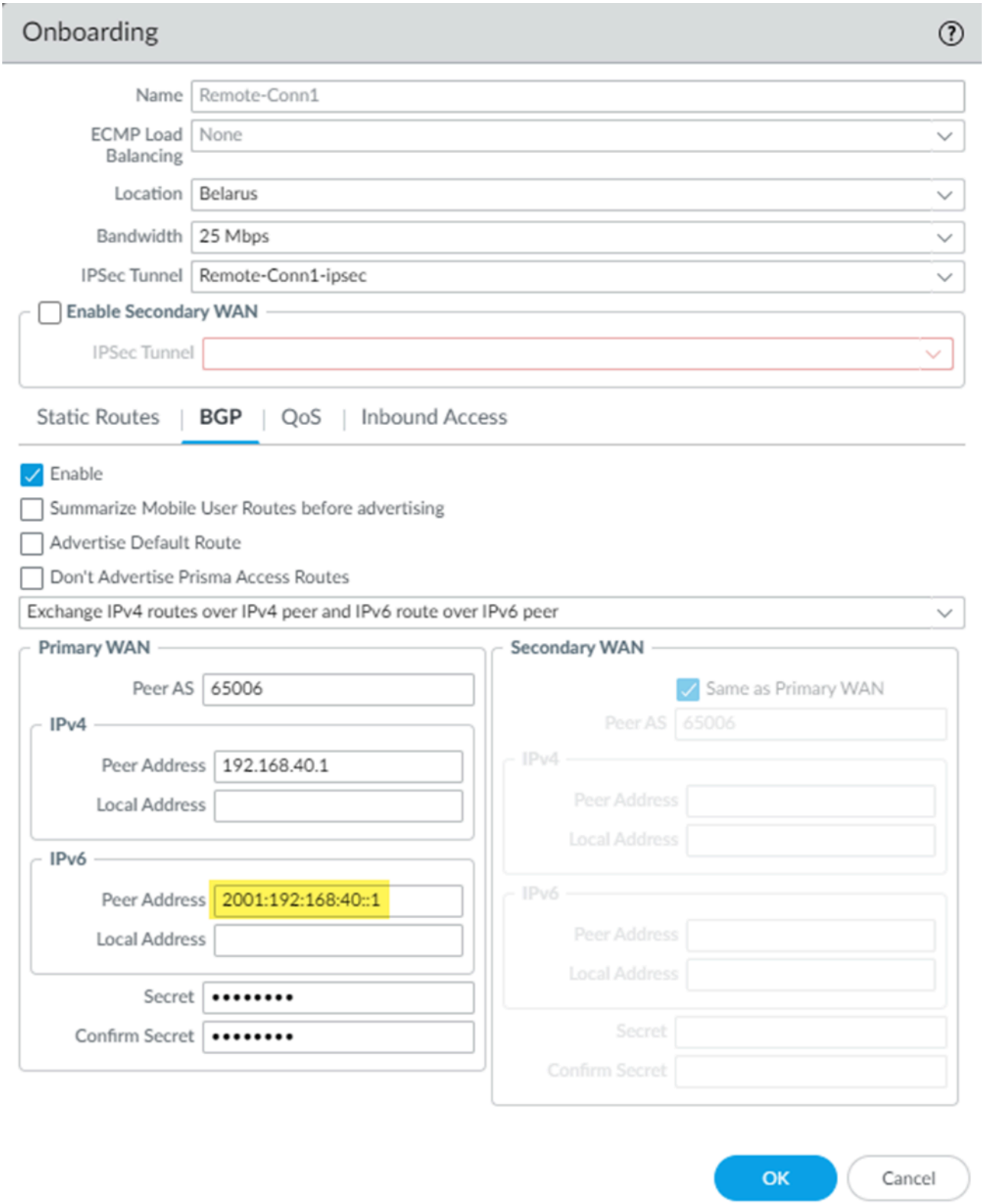
1. (Déploiements de routage statique uniquement) Saisissez un ou plusieurs **Corporate Subnets (Sous-réseaux d'entreprise)** dans l'onglet **Static Routes (Itinéraires statiques)**.



2. (Déploiements de routage BGP uniquement) Spécifiez la méthode d'échange des itinéraires BGP IPv4 et IPv6 ; ensuite, saisissez une **Peer Address (Adresse de l'homologue)** et une **Local Address (Adresse locale)** IPv6.
   - Pour utiliser une seule session BGP IPv4 pour échanger des informations d'appairage BGP IPv4 et IPv6, sélectionnez **Exchange both IPv4 and IPv6 routes over IPv4 peering (Échanger des itinéraires IPv4 et IPv6 via l'appairage IPv4)**.
   - Pour utiliser une session BGP IPv4 pour échanger des informations d'appairage BGP IPv4 et une session IPv6 pour échanger des informations d'appairage BGP IPv6, sélectionnez **Exchange IPv4 routes over IPv4 peering and IPv6 routes over IPv6 peering (Échanger des itinéraires IPv4 via l'appairage IPv4 et des itinéraires IPv6 via l'appairage IPv6)**.
   - Pour utiliser une seule session BGP IPv6 pour échanger des informations d'appairage BGP IPv6, sélectionnez **Exchange IPv6 routes over IPv6 peering (Échanger des itinéraires IPv6 via l'appairage IPv6)**.
3. Si votre WAN secondaire utilise une adresse de l'homologue ou une adresse locale différente, désélectionnez **Same as Primary WAN (Identique au WAN principal)** et

 ©2025 Palo Alto Networks, Inc.

saisissez la **Peer Address (Adresse de l'homologue)** et la **Local Address (Adresse locale)** IPv6 pour le WAN secondaire.



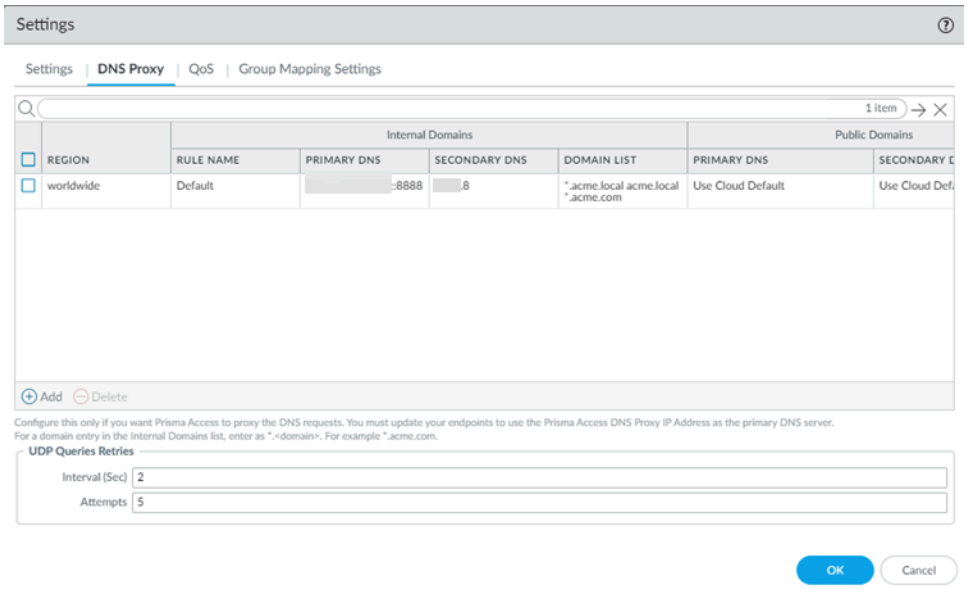
 ©2025 Palo Alto Networks, Inc.

STEP 6 | (Facultatif) Si vos serveurs DNS internes sont accessibles par des adresses IPv6, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Network (Réseau distant)** > **Settings (Paramètres)**, cliquez sur l'icône d'engrenage pour modifier les paramètres, sélectionnez l'onglet **DNS Proxy (Proxy DNS)**, **Add (Ajoutez)** une règle ou spécifiez la règle par défaut, puis spécifiez les adresses IPv6 de **Custom DNS Server (Serveur DNS personnalisé)** pour le serveur **Primary DNS (DNS principal)** et le serveur **Secondary DNS (DNS secondaire)**.

Prisma Access vous permet de spécifier les serveurs DNS pour résoudre à la fois les domaines internes à votre organisation et les domaines externes. Si vous ne spécifiez aucun paramètre, Prisma Access ne se procure pas les requêtes DNS pour les réseaux distants. Vous devez également sélectionner une **Region (Région)**.

Vous pouvez saisir n'importe quelle combinaison d'adresses IPv4 ou IPv6 pour les serveurs DNS principaux et secondaires.

Les adresses IPv4 utilisent des enregistrements A, tandis que les adresses IPv6 utilisent des enregistrements AAAA. Certains serveurs DNS peuvent effectuer des recherches DNS AAAA sur un transport IPv4 ; par conséquent, vous n'aurez peut-être pas besoin d'un serveur avec une adresse IP IPv6.



STEP 7 | Si vous n'avez pas encore terminé la configuration de la connexion à un réseau distant, terminez-la maintenant.

STEP 8 | **Commit and Push (Validez et appliquez)** vos modifications.

 ©2025 Palo Alto Networks, Inc.

STEP 9 | Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Remote Networks (Réseaux distants)** et notez les adresses du **EBGP Router (Routeur EBGP)**.

Après avoir validé vos modifications, vous disposerez d'un **EBGP Router (Routeur EBGP)** d'adresses IPv6 pour les connexions aux services.

Étant donné que le tunnel IPSec utilisé pour la connexion à un réseau distant utilise l'adressage IPv4, la **Service IP Address (Adresse IP du service)** reste une adresse IPv4.

L'accès Internet IPv6 pour les connexions à des réseaux distants est rendu possible par une connexion sous-jacente, dans laquelle le trafic IPv6 transite par un tunnel IPv4.

 ©2025 Palo Alto Networks, Inc.

Résolution DNS pour les utilisateurs mobiles – Déploiements GlobalProtect et de réseaux distants

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access 2.2 préférée et versions ultérieures ❑ L'accès IPv6 natif aux applications publiques et privées nécessite les versions minimales suivantes : • Prisma Access (Managed by Strata Cloud Manager) : Version de juin 2024 • Prisma Access (Managed by Panorama) : Prisma Access 5.1.1 pour les nouveaux déploiements uniquement. Tous les autres déploiements (y compris les déploiements Prisma Access (Managed by Panorama) existants) prennent uniquement en charge l'accès aux applications privées.

Prisma Access vous permet de spécifier les serveurs DNS pour résoudre à la fois les domaines internes à votre organisation et les domaines externes. Prisma Access utilise un proxy pour la requête DNS basée sur la configuration de vos serveurs DNS. Le tableau suivant présente les méthodes de résolution DNS prises en charge pour les domaines internes et externes et indique quand Prisma Access utilise un proxy pour les requêtes DNS.

Méthode de résolution DNS interne	Méthode de résolution DNS externe	Prisma Access utilise un proxy pour la requête DNS (Oui/Non)
Règle unique, serveur DNS configuré pour les domaines internes	Cloud par défaut (Google Public DNS64 pour IPv6)	Oui
Règle unique, serveur DNS configuré pour les domaines internes	Identique aux domaines internes	Non
Règle unique, serveur DNS configuré pour les domaines internes	Serveur DNS personnalisé (Google Public DNS64 pour IPv6)	Oui
Règle unique, cloud par défaut défini pour un domaine	Cloud par défaut (Google Public DNS64 pour IPv6)	Oui

 ©2025 Palo Alto Networks, Inc.

Méthode de résolution DNS interne	Méthode de résolution DNS externe	Prisma Access utilise un proxy pour la requête DNS (Oui/Non)
Règle unique, cloud par défaut défini pour un domaine	Identique aux domaines internes (Google Public DNS64 pour IPv6)	Oui
Règle unique, cloud par défaut défini pour le domaine	Serveur DNS personnalisé (Google Public DNS64 pour IPv6)	Oui
Plusieurs règles, serveur DNS configuré pour les domaines internes	Cloud par défaut (Google Public DNS64 pour IPv6)	Oui
Plusieurs règles, serveur DNS configuré pour les domaines internes	Identique aux domaines internes	Oui
Plusieurs règles, serveur DNS configuré pour les domaines internes	Serveur DNS personnalisé (Google Public DNS64 pour IPv6)	Oui
Aucune configuration	Serveur DNS personnalisé (Google Public DNS64 pour IPv6)	Oui
Aucune configuration	Cloud par défaut (pour IPv6, primaire = Google Public DNS64, secondaire = cloud par défaut)	Non
Aucune configuration	Aucune configuration	Non
Aucune résolution DNS spécifiée (la configuration par défaut est présente, qui utilise le cloud par défaut)	Aucune résolution DNS spécifiée	Non
Connecteur ZTNA (*quelle que soit la méthode de résolution DNS*)	S. O.	Oui
Après avoir activé le connecteur ZTNA, Prisma Access utilise un proxy pour toutes les requêtes DNS à l'aide des règles DNS configurées pour les réseaux distants et les utilisateurs mobiles - GlobalProtect.		

L'adresse IP source de la requête DNS dépend du fait que Prisma Access utilise ou non un proxy pour la requête DNS.

 ©2025 Palo Alto Networks, Inc.

- Lorsque Prisma Access n'utilise pas de proxy pour les requêtes DNS, l'adresse IP source de la requête DNS change en adresse IP du périphérique qui a demandé la recherche DNS. Cette adresse IP source vous permet d'appliquer des politiques DNS basées sur l'adresse IP source ou d'identifier les terminaux qui communiquent avec des domaines malveillants. Ce comportement s'applique aussi bien aux utilisateurs mobiles qu'aux déploiements de réseaux distants.
- Lorsque Prisma Access utilise un proxy pour les requêtes DNS, l'adresse IP source de la requête DNS change vers les adresses suivantes :
  - **Déploiements d'utilisateurs mobiles** : l'adresse IP source de la requête DNS est une adresse IP extraite du pool d'adresses IP de l'utilisateur mobile pour les requêtes internes et l'adresse IP de la passerelle de l'emplacement de l'utilisateur mobile pour les requêtes externes.
  - **Déploiements de réseaux distants** : l'adresse IP source de la requête DNS est l'adresse **EBGP Router Address (Adresse du routeur EBGP)** pour les requêtes internes et l'adresse IP du service de la connexion au réseau distant pour les requêtes externes.

Les directives et restrictions suivantes s'appliquent à l'utilisation de la résolution DNS avec Prisma Access :

- Le nombre maximal de requêtes DNS TCP simultanées en attente (**Max Pending Requests (Requêtes maximales en attente)**) prises en charge par Prisma Access est de 64.
- Pour les requêtes UDP, le proxy DNS envoie une autre requête s'il n'a pas reçu de réponse dans les 2 secondes et réessaye 5 fois maximum avant d'essayer le serveur DNS suivant.
- Prisma Access met en cache les entrées DNS avec une valeur de durée de vie (TTL) de 300 secondes. Les réponses EDNS sont également mises en cache.

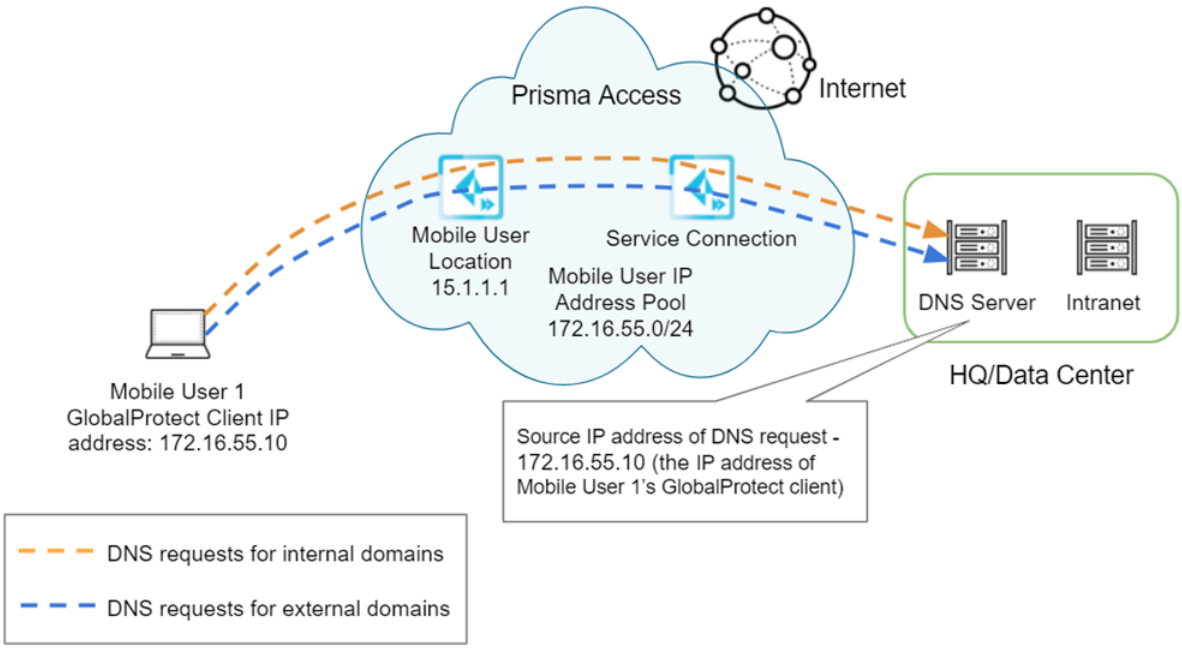
Résolution DNS pour les déploiements d'utilisateurs mobiles GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Panorama	• Licence Prisma Access

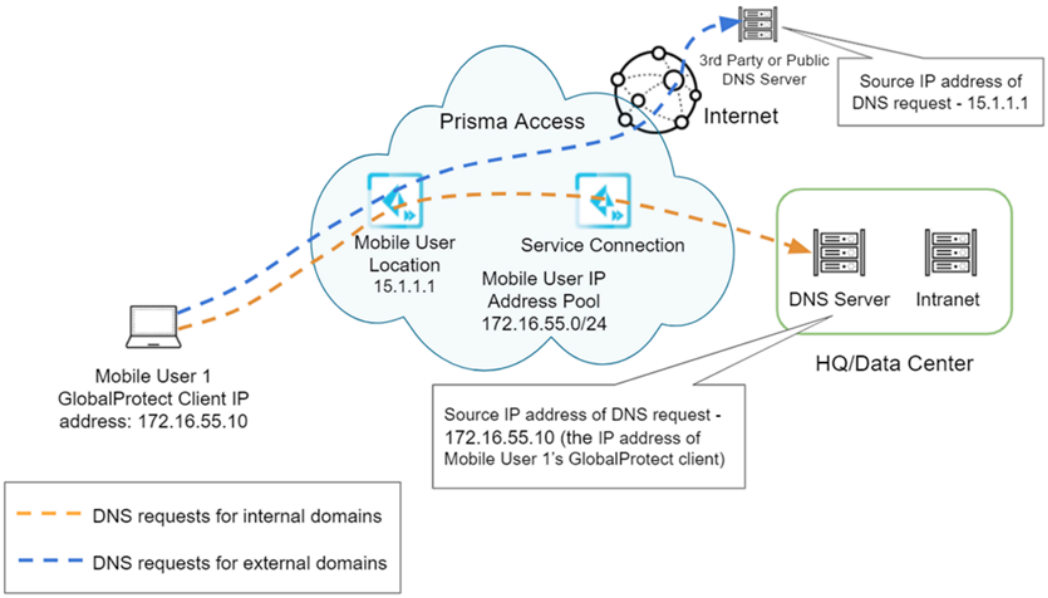
La section suivante fournit des exemples de la façon dont Prisma Access traite l'adresse IP source des requêtes DNS après avoir configuré la résolution DNS pour les utilisateurs mobiles et pour les réseaux distants.

La figure suivante illustre un déploiement dans lequel vous avez affecté un serveur DNS interne pour résoudre les domaines internes et externes. Dans ce cas, Prisma Access n'utilise pas de proxy pour les requêtes DNS et la requête DNS provient de l'adresse IP du client GlobalProtect de l'utilisateur mobile 1. Le client GlobalProtect attribue cette adresse IP à l'utilisateur mobile et elle est extraite de l'adresse IP de la passerelle de l'emplacement de l'utilisateur mobile.

 ©2025 Palo Alto Networks, Inc.

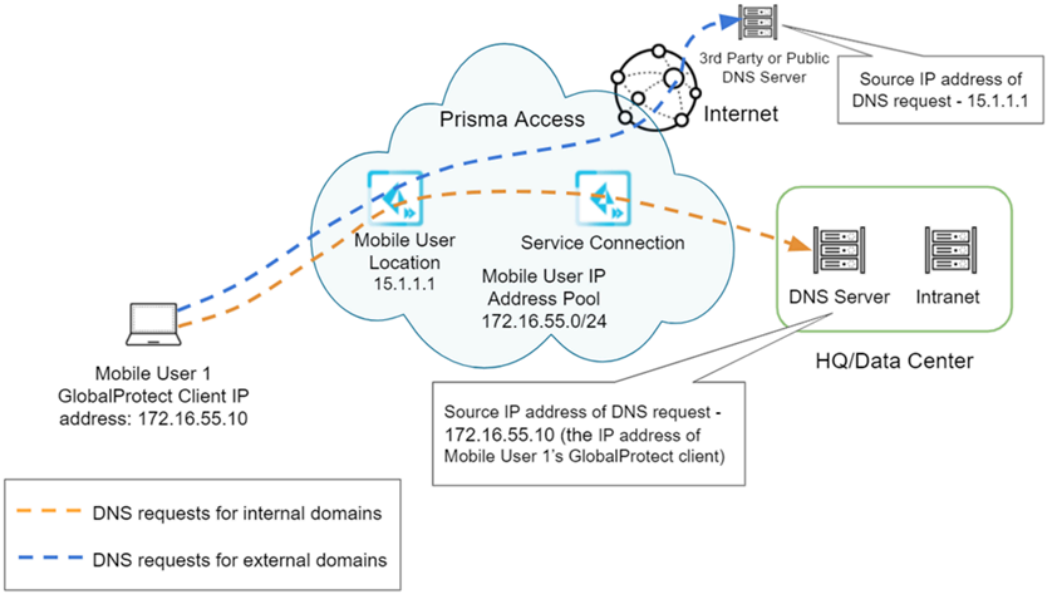


La figure suivante montre les requêtes DNS pour les domaines internes résolues par le serveur DNS dans le siège social ou le centre de données, tandis que les requêtes pour les domaines externes sont résolues par le serveur DNS cloud par défaut de Prisma Access. Dans ce cas, Prisma Access utilise un proxy pour les requêtes pour la requête externe, et l'adresse IP source est l'adresse IP de la passerelle Prisma Access (15.1.1.1 dans cet exemple), tandis que l'adresse IP source interne reste l'adresse IP du client GlobalProtect de l'utilisateur mobile 1.



La figure suivante montre l'organisation utilisant un serveur DNS tiers ou public accessible via Internet pour les requêtes vers des domaines externes. Prisma Access utilise un proxy également pour ces requêtes.

 ©2025 Palo Alto Networks, Inc.



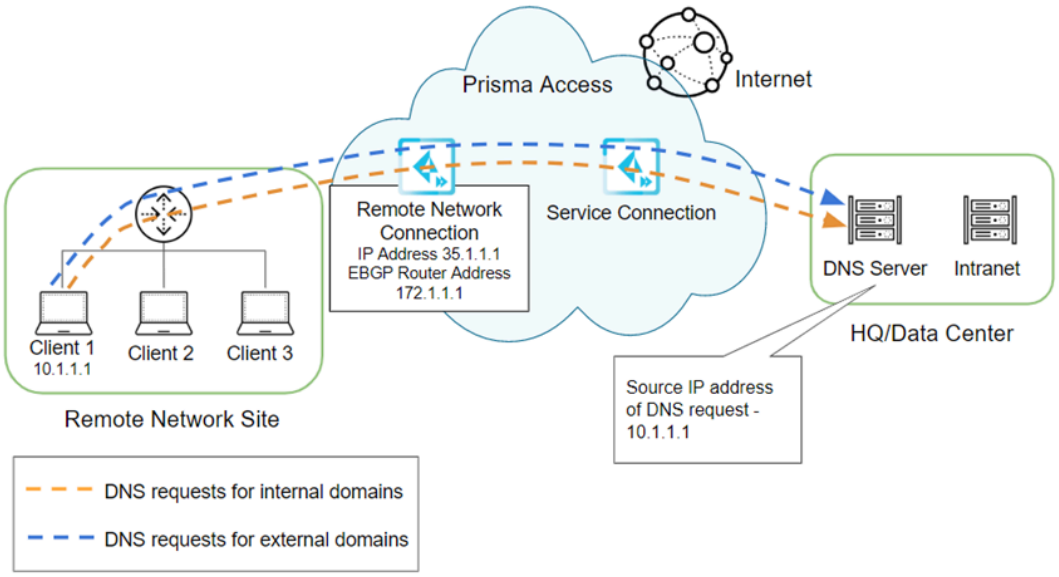
Résolution DNS pour les réseaux distants

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Panorama	• Licence Prisma Access

Si vous disposez déjà d'un déploiement de réseaux distants, vous pouvez continuer à utiliser les méthodes de résolution DNS que vous avez déjà mises en place, ou vous pouvez utiliser un proxy pour la requête DNS avec Prisma Access. L'utilisation de proxys pour les requêtes DNS vous permet d'envoyer des requêtes DNS pour les domaines publics à un serveur et d'envoyer des requêtes DNS pour les domaines internes à un autre serveur.

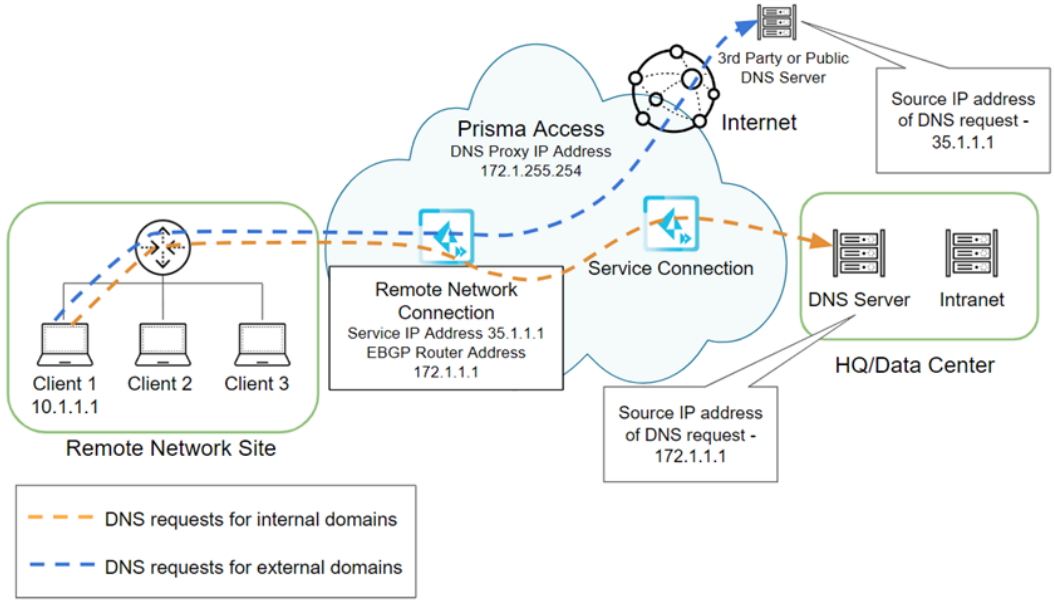
La figure suivante montre une requête DNS adressée à un déploiement où un serveur DNS interne est utilisé pour traiter les requêtes des domaines internes et externes. L'adresse IP du réseau distant est 35.1.1.1 et l'adresse IP **EBGP Router (Routeur EBGP)** est 172.1.1.1. Dans ce cas, Prisma Access n'utilise pas de proxy pour les requêtes et, si le serveur DNS interne n'utilise pas NAT, l'IP source de la requête DNS est 10.1.1.1 (l'adresse IP du périphérique du client 1 sur le site de réseau distant).

 ©2025 Palo Alto Networks, Inc.



Si Prisma Access utilise un proxy pour la requête DNS, les adresses IP sources des requêtes DNS avec proxy sont modifiées en **EBGP Router Address (Adresse du routeur EBGP)** pour les requêtes internes et en adresse IP du service, de la connexion au réseau distant pour les requêtes externes, comme illustré dans la figure suivante.

*Lorsque vous configurez l'adresse DNS de votre réseau à utiliser pour les requêtes externes Prisma Access avec proxy, spécifiez l'adresse **Remote Network DNS Proxy IP Address (Adresse IP du proxy DNS du réseau distant)** (**Panorama** > **Cloud Services** > **Status (État)** > **Service Infrastructure (Infrastructure du service)** > **Remote Network DNS Proxy IP Address (Adresse IP du proxy DNS du réseau distant)**). Dans l'exemple suivant, vous spécifieriez 172.1.255.254 dans votre réseau pour le serveur DNS.*



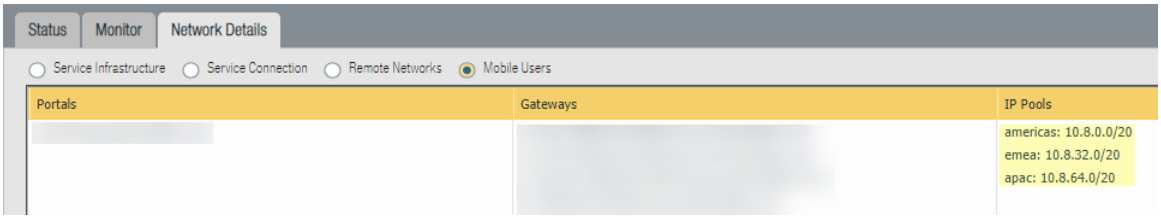
 ©2025 Palo Alto Networks, Inc.

Comment BGP annonce les pools d'adresses IP des utilisateurs mobiles pour les connexions aux services et les connexions au réseau distant

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Panorama	• Licence Prisma Access

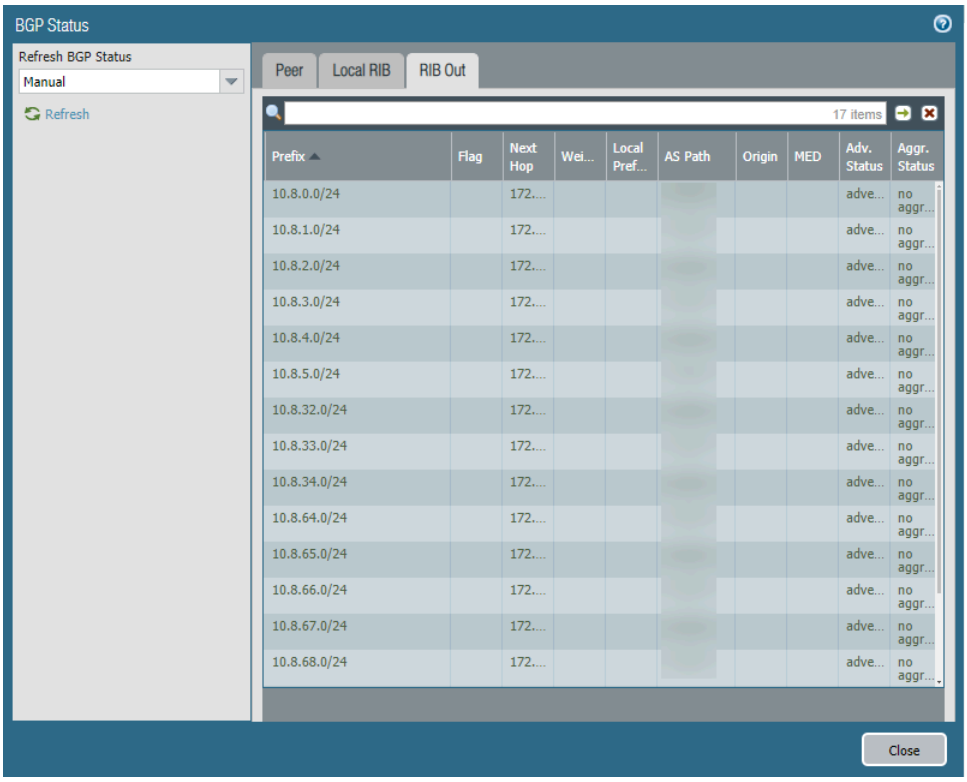
Si vous activez BGP pour les connexions aux services ou les connexions au réseau distant, après avoir Configurer les utilisateurs mobiles GlobalProtect (Panorama), Prisma Access alloue les pools d'adresses IP d'utilisateurs mobiles que vous avez spécifiés à l'aide de blocs d'adresses de classe C (/24). BGP annonce donc les sous-réseaux d'utilisateurs mobiles alloués par blocs de /24, plutôt que l'ensemble des pools associés à cette région. Quand Prisma Access ajoute un sous-réseau /24 pour une passerelle Prisma Access, il envoie automatiquement une annonce BGP. Au fur et à mesure que des sous-réseaux sont ajoutés et supprimés, Prisma Access met à jour automatiquement ses annonces BGP. Cette méthode d'allocation offre plus de flexibilité lors de l'annonce des itinéraires BGP, en particulier si vous avez configuré un pool **Worldwide (Mondial)** au lieu d'allouer des pools par région. La division du pool d'adresses IP en sous-réseaux plus petits permet d'ajouter, de supprimer ou de supprimer le même sous-réseau, puis de le réutiliser dans différentes régions lorsque l'espace d'adresses alloué est épuisé.

La capture d'écran suivante, issue de **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Mobile Users—GlobalProtect (Utilisateurs mobiles – GlobalProtect)**, affiche trois pools d'adresses IP /20 pour les utilisateurs mobiles divisés par région.



Le tableau **RIB Out (Sortie RIB)**, de **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **Show BGP Status (Afficher l'état BGP)** (dans la zone **Branch AS and Router (AS de branche et routeur)**), affiche le pool d'adresses des utilisateurs mobiles divisé en blocs de /24 sous-réseaux pour les annonces d'itinéraire BGP. Notez que l'ensemble des sous-réseaux /20 ne sont pas annoncés.

©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

Prise en charge du proxy pour Prisma Access et Strata Logging Service

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Panorama	• Licence Prisma Access

Si vous déployez un serveur proxy entre Panorama, l'Prisma Access infrastructure et Strata Logging Service, reportez-vous au tableau suivant pour plus de détails sur le comportement attendu :

Fonctionnalité	Prise en charge via un serveur proxy qui n'effectue pas de décryptage SSL	Prise en charge via un serveur proxy qui effectue le décryptage SSL
Intégration initiale à Strata Logging Service avec vérification de l'état de révocation du certificat à l'aide d'OCSP	Pris en charge	Seuls les proxys de transfert sont pris en charge ; tout proxy utilisant le décryptage SSL n'est pas pris en charge.
Requêtes Panorama à Strata Logging Service pour les rapports et les journaux	Si le serveur proxy est l'itinéraire par défaut sur Panorama, vous ne pouvez pas afficher les données sur les pages ACC et **Monitor (Surveiller)** > **Logs (Journaux)**. Vous pouvez afficher les données sur les pages ACC et **Monitor (Surveiller)** > **Logs (Journaux)** si Panorama dispose d'un itinéraire alternatif vers le Strata Logging Service et vous pouvez contourner le serveur proxy.	

©2025 Palo Alto Networks, Inc.

Bloquer les connexions entrantes en provenance de pays spécifiques

Prisma Access vous permet de créer des règles de politique de sécurité pour bloquer les tentatives de connexion pour le réseau distant, les utilisateurs mobiles — GlobalProtect et les utilisateurs mobiles — proxy explicite provenant des pays que vous spécifiez. Prisma Access bloque les connexions entrantes des pays que vous spécifiez en fonction des informations d'emplacement géographique de l'adresse IP source du client.

Pour bloquer les connexions entrantes en provenance de ces pays, complétez la tâche suivante.

STEP 1 | Créez une pré-règle de politique de sécurité en utilisant l'un des noms de règles spécifiques :

Assurez-vous de configurer cette règle en tant que pré-règle.

- Pour bloquer un pays pour les utilisateurs mobiles — déploiements GlobalProtect, créez une règle nommée **Mobile_User_EMBG_Source_Countries**.
- Pour bloquer un pays pour les utilisateurs mobiles — déploiements de proxy explicite, créez une règle nommée **Explicit_Proxy_EMBG_Source_Countries**.
- Pour bloquer un pays pour les déploiements de réseau distant, créez une règle nommée **Remote_Network_EMBG_Source_Countries**.

STEP 2 | Ajoutez une **Tag (Étiquette)** pour la règle nommée **PA_predefined_embargo_rule**.

STEP 3 | Ajoutez un ou plusieurs pays à bloquer dans la **Source**.

STEP 4 | Spécifiez une **Action** de **Drop (Blocage)**.

 ©2025 Palo Alto Networks, Inc.

Sécuriser le trafic Internet depuis AWS WorkSpace

Les organisations doivent repenser leur approche pour sécuriser leurs travailleurs à distance, leurs sous-traitants, le personnel hospitalier et les utilisateurs de centres d'appels qui accèdent à Internet via des machines virtuelles Amazon WorkSpace basées sur le cloud. Ces utilisateurs doivent pouvoir accéder à Internet de manière sécurisée et rester protégés contre les menaces basées sur Internet, tandis que l'organisation maintient une visibilité complète sur le trafic Internet généré par ces machines virtuelles hébergées dans le cloud.

Les modèles de mise en réseau traditionnels conçus pour les travailleurs et les ressources à distance ne sont plus suffisants dans l'économie complexe et innovante d'aujourd'hui, où la main-d'œuvre, les données et les applications cloud deviennent de plus en plus distribuées. Les organisations ont besoin de la flexibilité et de l'évolutivité des services cloud, mais ces services nécessitent des solutions de sécurité cloud conçues pour répondre à leurs besoins uniques.

En savoir plus sur Prisma SASE et AWS WorkSpace.

En utilisant Palo Alto Networks Strata Cloud Manager, vous pouvez fournir un accès sécurisé à Internet pour AWS WorkSpace en utilisant les méthodes suivantes :

- Configurer d'un fichier PAC sur les clients AWS WorkSpace
- Configurer un tunnel de site à site entre AWS et Prisma Access

Configurer d'un fichier PAC sur les clients AWS WorkSpace

L'une des méthodes de sécurisation du trafic Internet à partir d'Amazon WorkSpaces consiste à utiliser un fichier de configuration automatique de proxy (Proxy Auto-Configuration, PAC). Un fichier PAC est un code JavaScript qui indique à un navigateur web comment se connecter à un serveur proxy. Les environnements d'entreprise utilisent des fichiers PAC pour contrôler le trafic web et appliquer des règles de politique de sécurité. Un serveur web stocke généralement le fichier PAC et le navigateur web télécharge le fichier PAC au démarrage.

STEP 1 | Si vous ne l'avez pas déjà fait, configurez le proxy explicite Prisma SASE.

Vous pouvez héberger un fichier PAC dans Prisma SASE ou sur le serveur web. Vérifiez que le serveur PAC est accessible à partir des clients WorkSpace en accédant à l'URL du fichier PAC à l'aide d'un navigateur web.

STEP 2 | Personnalisez le fichier PAC du proxy explicite Prisma SASE pour mettre à jour le FQDN et définir des exclusions.

1. Dans Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Explicit Proxy (Proxy explicite)** > **Forwarding Rules (Règles de transfert)** .
2. Modifiez le fichier PAC en fonction des directives relatives aux fichiers PAC.

STEP 3 | Téléchargez les certificats racine du proxy explicite Prisma SASE à installer sur AWS WorkSpace.

STEP 4 | Installez le certificat sur le client AWS WorkSpace pour appliquer des règles de politique basées sur l'utilisateur, l'inspection du trafic et la création de rapports.

Cela permettra au client WorkSpace de communiquer avec le proxy explicite SASE Prisma.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Configurez le fichier PAC sur AWS WorkSpace.

La façon dont vous procédez dépend du navigateur que vous utilisez.

- Google Chrome :
  1. Ouvrez Chrome.
  2. Sélectionnez les trois points dans le coin supérieur droit de la fenêtre.
  3. Sélectionnez **Settings (Paramètres)**.
  4. Sélectionnez **Advanced (Avancé)**.
  5. Sous **System (Système)**, sélectionnez **Open proxy settings (Ouvrir les paramètres du proxy)**.
  6. Dans la fenêtre Local Area Network (LAN) Settings (Paramètres du réseau local (LAN)), sélectionnez **Use automatic configuration script (Utiliser un script de configuration automatique)**.
  7. Dans le champ **Address (Adresse)**, entrez l'URL de votre fichier PAC.
  8. Sélectionnez **OK** pour enregistrer vos modifications.
- Firefox :
  1. Ouvrez Firefox.
  2. Sélectionnez les trois lignes dans le coin supérieur droit de la fenêtre.
  3. Sélectionnez **Options**.
  4. Sélectionnez **Advanced (Avancé)**.
  5. Dans **Network (Réseau)**, sélectionnez **Settings (Paramètres)**.
  6. Dans la fenêtre **Connection Settings (Paramètres de connexion)**, sélectionnez **Automatic proxy configuration URL (URL de configuration automatique du proxy)**.
  7. Dans le champ **URL**, entrez l'URL de votre fichier PAC.
  8. Sélectionnez **OK** pour enregistrer vos modifications.

Une fois que vous avez appliqué le fichier PAC, Chrome et Firefox l'utilisent pour déterminer le serveur proxy à utiliser pour chaque site web.

STEP 6 | Redémarrez le navigateur AWS WorkSpace.

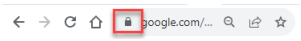
Après le redémarrage du navigateur WorkSpace, il récupère le nouveau fichier PAC et commence à acheminer le trafic via le proxy SASE Prisma.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Testez et vérifiez le flux de trafic.

Une fois que vous avez configuré les clients WorkSpace de manière à ce qu'ils utilisent le proxy explicite SASE Prisma, vous pouvez tester le flux de trafic en validant le certificat dans le navigateur et en consultant les journaux sur Prisma Access.

1. Si vous utilisez Google Chrome, sélectionnez le cadenas dans la barre d'adresse.



   1. Sélectionnez **Connection is secure (La connexion est sécurisée)**.
   2. Sélectionnez **Certificate is valid (Le certificat est valide)**.
   3. Vérifiez que les détails du certificat qui s'affichent dans la fenêtre contextuelle sont corrects.
2. Si vous utilisez Safari, sélectionnez l'icône du cadenas dans la barre d'adresse.
   1. Sélectionnez **Connection secure (Connexion sécurisée)**.
   2. Sélectionnez **More information (Plus d'informations)**.
   3. Sélectionnez **View Certificate (Afficher le certificat)**.
   4. Vérifiez que les détails du certificat qui s'affichent dans la fenêtre contextuelle sont corrects.

Configurer un tunnel de site à site entre AWS et Prisma Access

Au fur et à mesure que votre entreprise se développe et que plusieurs clients AWS WorkSpace sont en cours d'exécution, les réseaux distants Prisma Access vous permettent d'intégrer rapidement votre WorkSpace et de fournir une sécurité de pointe à vos utilisateurs. Ils offrent une option pratique qui simplifie la configuration et la gestion de WorkSpace.

Les organisations peuvent intégrer les utilisateurs d'AWS WorkSpace à Prisma Access en établissant un tunnel IPSec entre AWS et Prisma Access.

L'avantage de l'utilisation d'un réseau distant est qu'il sécurise le trafic Internet sortant pour les utilisateurs qui se connectent via Prisma Access pour accéder à Internet.

STEP 1 | Configurez un cloud privé virtuel (Virtual Private Cloud, VPC) pour votre Amazon WorkSpace ou utilisez le VPC existant pour votre Amazon WorkSpace.

STEP 2 | Rattachez la passerelle de transit AWS au VPC pour configurer le tunnel IPSec de site à site entre AWS et Prisma Access.

STEP 3 | Configurez le VPN IPSec entre la passerelle de transit AWS et le réseau distant Prisma Access.

STEP 4 | Sur le réseau distant Prisma Access, vous pouvez définir des règles de sécurité pour restreindre le trafic Internet afin de protéger les utilisateurs d'AWS WorkSpace.

 ©2025 Palo Alto Networks, Inc.

Prisma Access pour les réseaux sans itinéraire par défaut

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access	❑ Licence Prisma Access

Qu'est-ce qu'un réseau sans itinéraire par défaut ?

Un réseau sans itinéraire par défaut est un réseau qui n'a aucun itinéraire par défaut configuré. Lorsqu'un réseau n'a pas d'itinéraire par défaut configuré, il abandonne les paquets destinés à des destinations inconnues. Les entreprises utilisent souvent les réseaux sans itinéraire par défaut pour restreindre l'accès de leurs utilisateurs. Si un périphérique sur un réseau sans itinéraire par défaut doit accéder à une certaine destination (adresse IP ou sous-réseau), l'administrateur devra configurer manuellement un itinéraire pour cette destination. Les entreprises ont également besoin d'un accès Internet restreint et sécurisé pour les utilisateurs, les serveurs et les périphériques sur un réseau de succursales sans itinéraire par défaut.

Il existe plusieurs raisons pour lesquelles quelqu'un pourrait vouloir configurer un réseau sans itinéraire par défaut :

- Améliorer la sécurité en bloquant le trafic malveillant et DDoS sortant vers des destinations aléatoires à partir de terminaux compromis sur le réseau, ce qui protège contre les attaques par déni de service et d'autres trafics malveillants.
- Améliorer les performances des périphériques de routage en réduisant le nombre d'itinéraires à traiter.
- Mettre en œuvre des politiques de routage qui répondent aux besoins spécifiques des utilisateurs en configurant des itinéraires spécifiques pour des destinations spécifiques.

Considérations relatives aux réseaux sans itinéraire par défaut

Lorsqu'elles sécurisent le trafic Internet à partir d'un réseau sans défaut, les entreprises doivent clairement évaluer les utilisateurs, les terminaux, les serveurs et les périphériques du réseau de succursales qui pourraient communiquer avec Internet.

Dans les succursales sans itinéraire par défaut, il peut exister des périphériques avec divers systèmes d'exploitation différents, des terminaux multi-utilisateurs ou partagés tels que des VDI et des périphériques sans tête tels que des serveurs et des périphériques IoT. Le trafic Internet de tous ces périphériques exige une sécurité. Il est essentiel de disposer d'une solution qui couvre tous ces cas d'utilisation, qui offre une flexibilité avec différentes méthodes de connectivité et qui offre une plateforme unifiée pour sécuriser un accès cohérent à Internet, quel que soit le type de périphérique.

Recommandations de déploiement pour sécuriser l'accès à Internet pour les réseaux sans itinéraire par défaut

Si vous n'avez pas de réseau sans itinéraire par défaut, voici notre recommandation pour sécuriser le trafic Internet :

 ©2025 Palo Alto Networks, Inc.

Périphériques	Recommandation
Windows, macOS	Agent GlobalProtect en mode proxy
ChromeOS, VDI	Fichiers PAC sans agent
iOS, Android	Fichiers PAC sans agent
Linux	Fichiers PAC sans agent
Serveurs	Fichiers PAC sans agent
Périphériques IoT (proxy conscient)	Fichiers PAC sans agent
Périphériques IoT (proxy non conscient)	Réseaux distants (IPSec)

Considérations clés

Lors du déploiement de GlobalProtect dans un réseau sans itinéraire par défaut, tenez compte des points suivants :

- Ajoutez un itinéraire sur le périphérique de périmètre pour acheminer le trafic Internet de l'utilisateur vers l'adresse IP de proxy explicite de Prisma Access.
- Hébergez le fichier PAC en interne pour transmettre l'URL de l'IdP et l'URL du portail Prisma Access vers le proxy explicite pour autoriser GlobalProtect à se connecter au portail et à l'IdP.
- Ajoutez des enregistrements DNS internes pour résoudre le FQDN du proxy explicite, du fichier PAC et du portail Prisma Access si le serveur DNS du réseau sans itinéraire par défaut est incapable de résoudre les FQDN externes.
- Configurez DNAT pour l'adresse IP du proxy explicite de Prisma Access et l'adresse IP du portail Prisma Access en adresse IP du proxy explicite réelle et adresse IP du portail.

Pour les déploiements basés sur PAC, il n'est pas nécessaire de transférer l'URL du portail Prisma Access vers un proxy explicite et l'exclure des paramètres d'authentification dans les paramètres de proxy explicite de Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Prisma Access Déploiements avancés de connexion aux services

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Panorama	• Licence Prisma Access

Les sections suivantes vous montrent les déploiements avancés disponibles pour Prisma Access Connexions aux services :

- Redondance multicloud des connexions aux services
- Utiliser la redirection du trafic pour transférer le trafic lié à Internet aux connexions aux services
- Routage pour le trafic de connexion aux services
- Créer un réseau à large bande passante à l'aide de plusieurs connexions aux services

Redondance multicloud des connexions aux services

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

La redondance multicloud de connexion aux services est prise en charge à partir de Prisma Access 3.1 Innovation.

Si vous utilisez Prisma Access Connexions aux services pour fournir aux utilisateurs mobiles et aux utilisateurs de sites distants un accès aux ressources et applications internes d'un siège social ou d'un centre de données, vous pouvez garantir un accès plus résilient à ces ressources en créant des connexions aux services actives et de sauvegarde dans différents fournisseurs de cloud. Vous pouvez spécifier ces connexions aux services actives et de sauvegarde au même emplacement ou à différents emplacements dans différentes régions géographiques, ce qui vous permet d'accéder aux ressources via des connexions aux services même lorsqu'un fournisseur de cloud ou une région devient indisponible.

Vous spécifiez les connexions aux services actives et de sauvegarde dans un *site*. Un site est un centre de données client ou un siège social (local ou dans le cloud public) où se terminent une ou plusieurs connexions aux services. Après avoir créé des connexions aux services, créez un site, ajoutez des connexions aux services à ce site, puis spécifiez les connexions aux services que vous avez ajoutées comme actives ou de sauvegarde.

Si une panne régionale ou d'un fournisseur de cloud entraîne la panne d'une connexion aux services active sur un site, Prisma Access redirige le trafic à l'aide de ces règles, ce qui permet à vos utilisateurs mobiles de continuer à accéder aux ressources de ce siège social ou de ce centre de données :

 ©2025 Palo Alto Networks, Inc.

- S'il existe une seule connexion aux services active sur un site, Prisma Access sélectionne la connexion aux services de sauvegarde sur ce site pour acheminer le trafic.
- S'il existe plusieurs connexions aux services actives sur un site, Prisma Access sélectionne une autre des connexions aux services actives pour acheminer le trafic, et la connexion aux services de secours est uniquement utilisée pour acheminer le trafic lorsque toutes les connexions aux services actives sont interrompues.

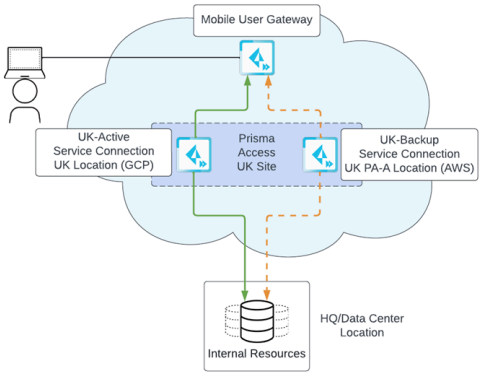
Pour utiliser un site qui utilise des emplacements actifs et de sauvegarde dans le même pays, vous intégrez des connexions aux services à l'aide d'emplacements préférés et alternatifs dans le pays, puis créez un site et ajoutez ces emplacements du pays au site.

Prisma Access vous fournit également des messages d'état concernant les connexions aux services que vous avez intégrées sur un site (par exemple, si toutes les connexions aux services d'un site sont déployées dans une seule région).

Les exemples suivants montrent comment vous pouvez tirer parti de la création de sites et de l'ajout de connexions aux services à ceux-ci :

- **Différents fournisseurs de cloud dans la même région géographique**—Si vous êtes une organisation (comme une banque) qui exige que vos données soient accessibles dans un pays spécifique, vous pouvez sélectionner un emplacement préféré dans ce pays et un emplacement alternatif dans ce même pays. L'exemple suivant montre une organisation au Royaume-Uni qui intègre ses connexions aux services au Royaume-Uni pour respecter les réglementations en matière de localisation des données. Dans ce cas, l'administrateur de l'organisation intègre deux connexions aux services au Royaume-Uni, UK-Active dans l'emplacement du Royaume-Uni et UK-Backup dans l'emplacement PA-A du Royaume-Uni. L'emplacement au Royaume-Uni est hébergé par le fournisseur de cloud préféré (GCP) au Royaume-Uni, et l'emplacement PA-A au Royaume-Uni est hébergé par le fournisseur de cloud alternatif (AWS) dans ce pays. La liste des emplacements dans le pays indique le fournisseur de cloud préféré et alternatif pour un pays. L'administrateur crée ensuite un site et désigne UK-Active comme emplacement actif et UK-Backup comme emplacement de sauvegarde sur ce site.

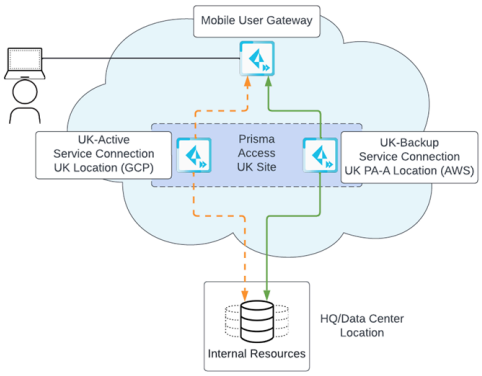
  En fonctionnement normal, les utilisateurs mobiles accèdent aux ressources internes du siège social ou du centre de données à l'aide de la connexion aux services UK-Active.



  Si une panne de GCP affecte la connexion aux services UK-Active, Prisma Access bascule vers la connexion aux services UK-Backup, qui est hébergée sur AWS. De cette façon, Prisma Access permet aux utilisateurs mobiles d'accéder aux ressources du centre de données ou du

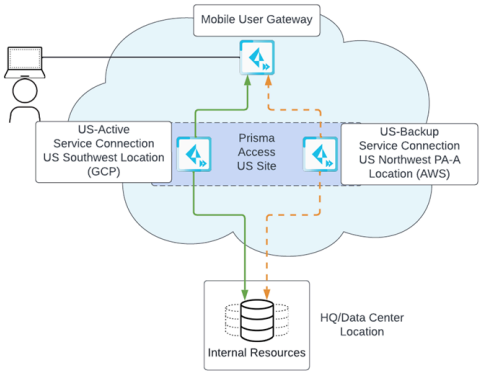
 ©2025 Palo Alto Networks, Inc.

siège social, même en cas de panne du fournisseur de cloud. Le diagramme suivant montre le flux de trafic.



- **Différentes régions géographiques**—Si vous souhaitez garantir la redondance en cas de panne régionale, vous pouvez spécifier deux ou davantage de connexions aux services dans différents emplacements de calcul ainsi que différents fournisseurs de cloud, qui vous fournissent un accès de secours en cas de panne dans une région géographique. Dans le diagramme suivant, l'administrateur a intégré des connexions aux services à partir d'emplacements aux États-Unis (US-Active dans l'emplacement du Sud-Ouest des États-Unis et US-Backup dans l'emplacement du Nord-Ouest des États-Unis PA-A) et a créé un site faisant de US-Active la connexion aux services active sur le site et de US-Backup la connexion de sauvegarde.

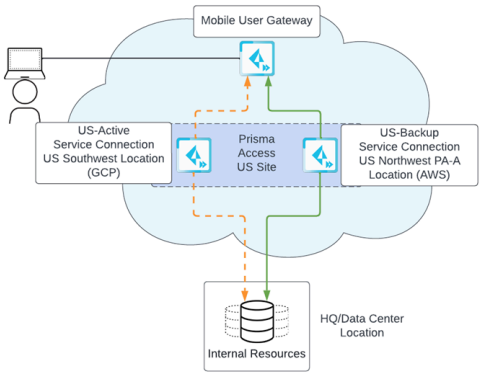
  Étant donné que vous avez intégré des connexions aux services qui se trouvent dans différents emplacements de calcul ainsi que chez différents fournisseurs de cloud, vous avez configuré un site qui vous offre une redondance géographique et de fournisseur de cloud.



  Si l'emplacement US-Active tombe en panne (en raison d'une panne d'un fournisseur de cloud ou d'une panne régionale), la connexion aux services bascule vers l'emplacement US-Backup,

 ©2025 Palo Alto Networks, Inc.

qui utilise un fournisseur de cloud et un emplacement de calcul différents de la connexion aux services US-Active, comme illustré dans le diagramme suivant.

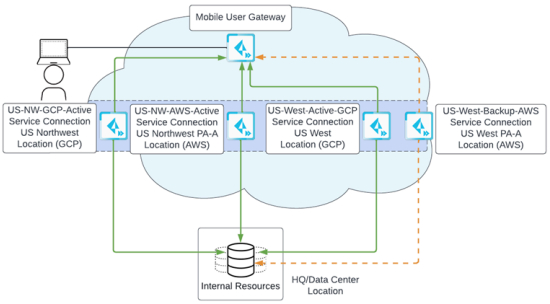


- **Connexion à large bande passante utilisant plusieurs connexions aux services**—Si vous avez besoin d'une connexion à large bande passante vers vos ressources internes, vous pouvez créer un site avec plusieurs connexions actives. Le diagramme suivant montre quatre sites en cours d'intégration, avec un mélange de fournisseurs de cloud GCP et AWS utilisés :
  - US-NW-GCP-Active, utilisant l'emplacement Nord-Ouest des États-Unis (GCP)
  - US-NW-AWS-Active, utilisant l'emplacement Nord-Ouest des États-Unis PA-A (AWS)
  - US-West-Active-GCP, utilisant l'emplacement Ouest des États-Unis (GCP)
  - US-West-Backup-AWS, utilisant l'emplacement Ouest des États-Unis PA-A (AWS)

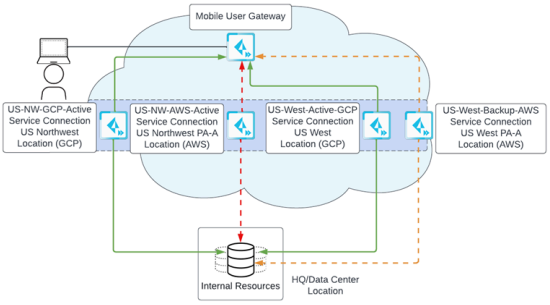
  Sur le site, trois des connexions aux services sont désignées comme connexions aux services actives, une quatrième connexion aux services étant désignée comme connexion de secours. Désigner trois connexions aux services comme actives vous donne effectivement trois fois

 ©2025 Palo Alto Networks, Inc.

plus de bande passante pour vos ressources internes par rapport à une seule connexion aux services.

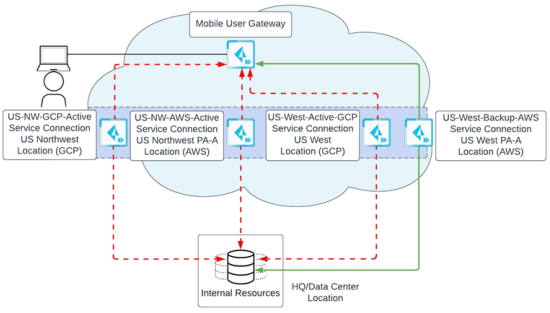


Si l'une des connexions aux services actives tombe en panne, la connexion de secours n'est pas utilisée ; à la place, Prisma Access détourne le trafic vers les connexions aux services actives restantes qui sont en service, comme indiqué dans le diagramme suivant.



Si toutes les connexions aux services actives sont interrompues, la connexion aux services de secours est alors utilisée et devient la connexion active.

Si vous configurez plusieurs connexions aux services en tant que connexions aux services de sauvegarde, Prisma Access met toutes les connexions aux services de sauvegarde en service et la charge partage le trafic de connexion aux services.



Utilisez les instructions suivantes lors de la configuration de connexions aux services de fournisseurs de cloud redondantes :

 ©2025 Palo Alto Networks, Inc.

- Vous pouvez ajouter des connexions aux services en utilisant des emplacements préférés ou alternatifs sur un site.

  Palo Alto Networks vous recommande fortement d'utiliser le fournisseur cloud préféré comme connexion aux services active sur un site.
- Toutes les connexions aux services d'un site doivent pointer vers la même ressource dans le même siège social ou centre de données. Vous ne pouvez pas avoir de connexions aux services dans un site pointant vers différentes ressources dans différents emplacements.
- Vous devez sélectionner au moins une connexion aux services active sur un site ; toutefois, vous pouvez également avoir plusieurs connexions aux services actives sur un seul site. La configuration de site suivante est valide :
  - Centre des États-Unis (active)
  - Centre des États-Unis PA-A (sauvegarde)
  - Est des États-Unis (active)
  - Est des États-Unis PA-A (sauvegarde)
- Si vous avez plusieurs connexions aux services actives sur un site et qu'une connexion aux services active tombe en panne, le trafic est détourné vers l'autre connexion aux services active (c'est-à-dire que la connexion aux services de secours n'est pas utilisée tant que l'une des connexions aux services actives est active).
- Utilisez les instructions suivantes pour le routage des connexions aux services statiques et dynamiques :
  - Si vous utilisez le routage statique pour les connexions aux services, assurez-vous que les sous-réseaux que vous spécifiez pour les connexions aux services pointent vers les mêmes sous-réseaux.

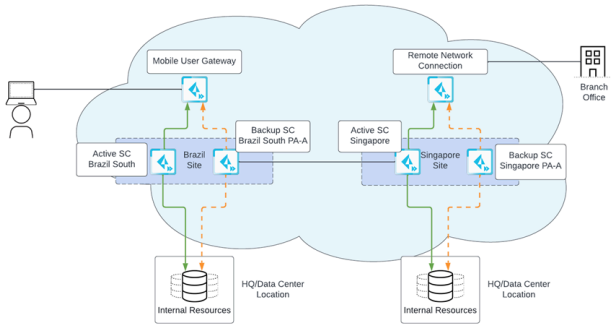
    Par exemple, si vous disposez d'un site qui utilise 192.168.41.0/24, 192.168.44.0/24 et 192.168.47.0/24 comme sous-réseaux pour les connexions aux services actives, assurez-vous de spécifier les mêmes sous-réseaux pour les connexions aux services de sauvegarde.
  - Si vous utilisez un routage dynamique (BGP) pour les connexions aux services, assurez-vous que toutes les connexions aux services annoncent les mêmes préfixes au même centre de données ou siège social.
- Prisma Access utilise les valeurs du discriminateur de sorties multiples BGP (MED) pour distinguer les connexions aux services actives et de sauvegarde sur un site, comme indiqué dans le tableau suivant. Notez que les valeurs MED pour les connexions aux services actives changent selon que vous avez ou non activé un tunnel IPSec secondaire pour la connexion aux services active. Prisma Access annonce ces valeurs MED au CPE (homologue BGP).

Connection Type (Type de connexion)	Valeur MED
Connexions aux service IPSec actives sur un site	
Connexion aux services active, aucun tunnel IPSec secondaire configuré	0
Connexion aux services active, tunnel IPSec secondaire configuré, tunnel principal	100

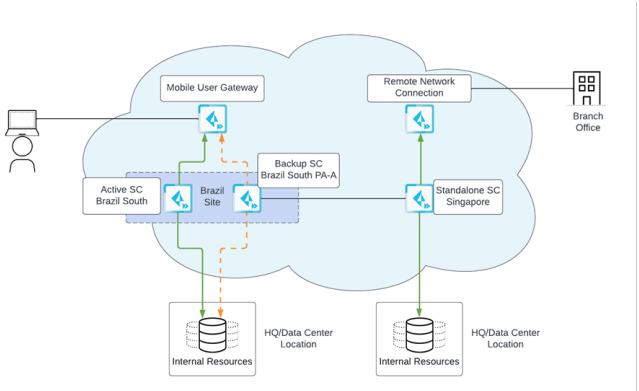
 ©2025 Palo Alto Networks, Inc.

Connection Type (Type de connexion)	Valeur MED
Connexion aux services active, tunnel IPSec secondaire configuré, tunnel secondaire	200
Connexions aux service IPSec de sauvegarde sur un site	
Connexion aux services de sauvegarde, tunnel principal (indépendamment du fait qu'un tunnel IPSec secondaire soit configuré ou non)	500
Connexion aux services de sauvegarde, tunnel IPSec secondaire configuré, tunnel secondaire	600

- Vous pouvez ajouter plusieurs sites dans un seul Prisma Access déploiement, comme indiqué dans le diagramme suivant.



- Vous pouvez toujours utiliser une connexion aux services unique et autonome pour accéder aux ressources internes. Vous pouvez également combiner des connexions aux services autonomes avec des connexions aux services actives et de sauvegarde, comme illustré dans le diagramme suivant.



- La redondance multicloud des connexions aux services n'est pas prise en charge lors de l'utilisation du routage Hot Potato pour les connexions aux services.
- N'utilisez pas l'interface CLI pour intégrer et configurer les connexions aux services. Si vous avez besoin d'utiliser CLI pour intégrer des connexions aux services, contactez votre équipe Palo Alto Networks.

 ©2025 Palo Alto Networks, Inc.

Configurer et activer la redondance des fournisseurs de cloud des connexions aux services

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Pour configurer plusieurs connexions aux services pour les fournisseurs de cloud, procédez comme suit.

STEP 1 | (Déploiements Prisma Access existants uniquement) Si vous avez mis à niveau votre plug-in vers une version qui prend en charge la redondance des fournisseurs de cloud, effectuez une opération **Commit and Push (Valider et appliquer)** après avoir mis à niveau vers le plug-in pris en charge.

La redondance multicloud des connexions aux services est prise en charge à partir de Prisma Access version 3.1 préférée et innovation. Après avoir mis à niveau le plug-in Cloud Services, vous devez effectuer une opération **Commit and Push (Valider et appliquer)** pour que les modifications de redondance du cloud apparaissent dans l'interface utilisateur.

Si vous avez un nouveau déploiement (et non une mise à niveau), ignorez cette étape.

 ©2025 Palo Alto Networks, Inc.

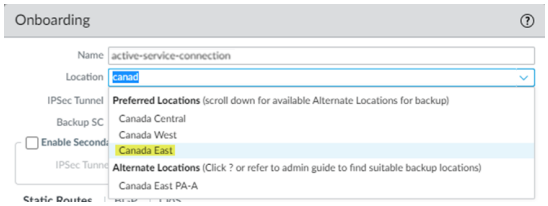
STEP 2 | Créez les connexions aux services à utiliser comme connexions aux services actives et de secours dans un site.

Après avoir créé des emplacements préférés et alternatifs, et validé et appliqué vos modifications, vous ne pouvez plus modifier ces emplacements. Par exemple, vous ne pouvez pas remplacer l'emplacement préférés de l'Est du Canada par l'emplacement de l'Est du Canada PA-A et vous ne pouvez pas remplacer l'emplacement alternatif de l'Est du Canada PA-A par l'emplacement de l'Est du Canada.

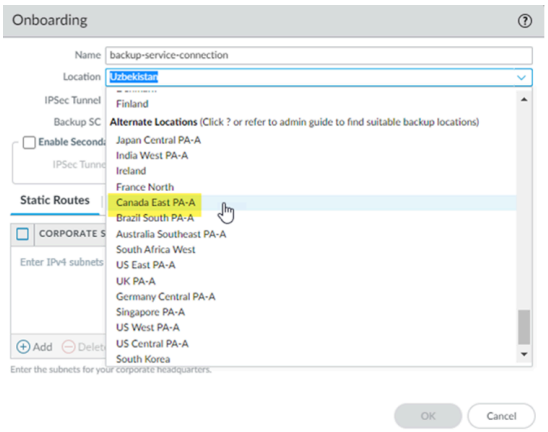
1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Connection (Connexion aux services)**.
2. Cliquez sur **Add (Ajouter)** pour ajouter une connexion aux services que vous désignerez comme connexion aux services active dans un site.

   Choisissez parmi la liste des emplacements préférés ou alternatifs.

   *Pour rechercher un emplacement, commencez à taper le nom du **Location (Emplacement)**.*



3. Cliquez sur **Add (Ajouter)** pour ajouter une connexion aux services que vous désignerez comme connexion aux services de secours dans un site.



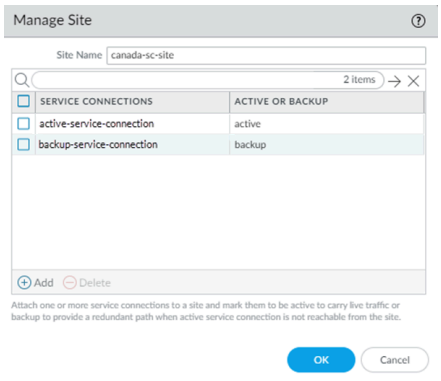
4. (Facultatif) Continuez à intégrer des connexions aux services à désigner comme sites actifs et de secours, au besoin.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Créez un site. Ensuite, désignez les connexions aux services que vous avez ajoutées comme connexions aux services actives ou de secours dans le site.

1. Dans **Manage Sites (Gérer les sites)**, cliquez sur **Add (Ajouter)** pour ajouter un nouveau site.
2. Vous devez également **Add (Ajouter)** les connexions aux services que vous avez intégrées.
3. Désignez les emplacements de service que vous avez ajoutés comme **Active (Actifs)** et **Backup (De secours)** dans le site.

   Vous pouvez créer plusieurs sites actifs et de secours. Spécifiez au moins un site comme site actif.
4. Cliquez sur **OK**.
5. (Facultatif) Continuez à ajouter des sites pour vos connexions aux services actives et de secours, au besoin.



STEP 4 | **Commit and Push (Validez et appliquez)** vos modifications.

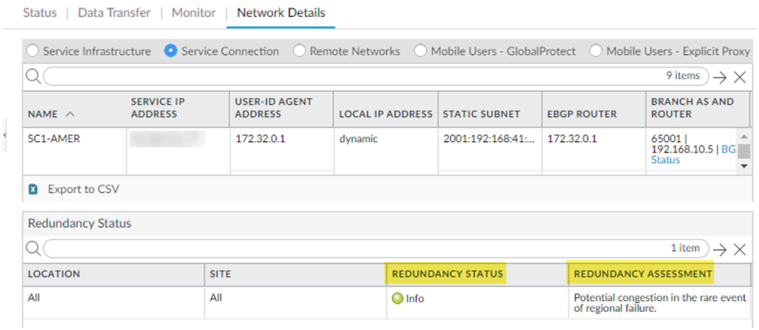
STEP 5 | Vérifiez l'état de vos sites.

1. Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **Redondance Status (État de la redondance)**.
2. Vérifiez les informations dans les champs **Redundancy Status (État de la redondance)** et **Redundancy Assessment (Évaluation de la redondance)**. L'état de la redondance vous indique l'état des sites que vous déployez et l'évaluation de la redondance vous fournit plus de détails sur les connexions aux services déployées dans le site.

État de la redondance	Évaluation de la redondance
info	Vos connexions aux services peuvent être congestionnées en cas de panne régionale.
Avertissement	Toutes les connexions aux services sont déployées dans une seule région. Veuillez envisager de les déployer dans des emplacements voisins. Ce message vous informe que toutes vos connexions aux services sont déployées dans une seule région.

 ©2025 Palo Alto Networks, Inc.

État de la redondance	Évaluation de la redondance
Attention	Toutes les connexions aux services se connectant au site sont déployées dans une seule région. Veuillez envisager de les déployer dans des emplacements voisins. Ce message vous informe que toutes les connexions aux services se connectant à un site sont déployées dans une seule région.



Prise en charge des emplacements de redondance des fournisseurs de cloud actifs et de sauvegarde dans le pays

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Panorama	• Licence Prisma Access

Si vous souhaitez configurer un déploiement où les emplacements actifs et de sauvegarde se trouvent dans le même pays, sélectionnez dans cette liste des emplacements privilégiés et alternatifs dans le pays.

Emplacements privilégiés	Emplacements alternatifs
Australie Sud-Est	Australie Sud-Est PA-A
Bahreïn PA-A	Bahreïn
Sud du Brésil	Sud du Brésil PA-A
Est du Canada	Est du Canada PA-A
Nord de la France PA-A	Nord de la France
Allemagne Centre	Allemagne Centre PA-A
Ouest de l’Inde	Ouest de l’Inde PA-A

 ©2025 Palo Alto Networks, Inc.

Emplacements privilégiés	Emplacements alternatifs
Irlande PA-A	Irlande
Japon Centre	Japon Centre PA-A
Singapour	Singapour PA-A
Afrique du Sud Ouest PA-A	Afrique du Sud Ouest
Corée du Sud PA-A	Corée du Sud
Royaume-Uni	Royaume-Uni PA-A
Émirats arabes unis PA-A	Émirats arabes unis
États-Unis Centre	États-Unis Centre PA-A
États-Unis Est	États-Unis Est PA-A
États-Unis Nord-Ouest	États-Unis Nord-Ouest PA-A
États-Unis Ouest	États-Unis Ouest PA-A

Utiliser la redirection du trafic pour transférer le trafic lié à Internet aux connexions aux services

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ La possibilité d'envoyer la liste de révocation de certificat (CRL) et le protocole de vérification des certificats en ligne (OCSP) directement à Internet nécessite une version minimale de Prisma Access de 5.1.1.

Prisma Access vous permet de créer des règles de redirection du trafic pour spécifier des cibles pour le trafic lié à Internet des utilisateurs mobiles et des connexions aux réseaux distants. Vous pouvez spécifier le trafic à rediriger vers une connexion aux services avant l'envoi vers Internet, ou vous pouvez spécifier le trafic à sortir directement vers Internet. Cette fonctionnalité est connue sous le nom de *Redirection du trafic*.

Vous pouvez également configurer Prisma Access pour qu'il accepte un itinéraire par défaut de votre CPE vers Prisma Access afin que Prisma Access transfère le trafic des utilisateurs mobiles lié à Internet vers la meilleure connexion au service de votre déploiement.

 ©2025 Palo Alto Networks, Inc.

Itinéraires par défaut avec redirection du trafic Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Utilisez la fonctionnalité d'itinéraire par défaut dans Prisma Access pour accepter les itinéraires par défaut publiés par votre CPE vers les connexions aux services. Vous pouvez utiliser BGP ou des itinéraires statiques pour publier l'itinéraire par défaut. Prisma Access utilise BGP pour publier ces routes sur plusieurs connexions aux services, ce qui permet à Prisma Access de diriger le trafic des utilisateurs mobiles via la meilleure connexion aux services pour un emplacement donné de l'utilisateur mobile. Pour permettre aux connexions aux services d'accepter les itinéraires par défaut, spécifiez **Accept Default Route over Service Connections (Accepter l'itinéraire par défaut via les connexions aux services)** lorsque vous Configurer la redirection du trafic dans Prisma Access.

Après avoir activé les itinéraires par défaut, votre trafic Internet sera dirigé vers les connexions aux services au lieu de sortir des emplacements des utilisateurs mobiles. Cette fonctionnalité peut être utile si vous souhaitez rediriger le trafic Internet vers le centre de données. Par exemple, si vous avez une pile de sécurité tierce dans votre centre de données et que vous souhaitez que la pile effectue un filtrage ou une inspection supplémentaires.

Utilisez les directives suivantes lors de la mise en œuvre des itinéraires par défaut :

- Les itinéraires par défaut s'appliquent uniquement aux déploiements d'utilisateurs mobiles. Les connexions au réseau distant fonctionnent normalement sans changement lorsque vous activez les itinéraires par défaut.
- Vous n'avez pas besoin de spécifier les connexions aux services cibles ou les règles de redirection du trafic lorsque vous autorisez les itinéraires par défaut, bien qu'elles soient prises en charge pour une utilisation avec les itinéraires par défaut.
- Lorsque vous spécifiez le paramètre **Accept Default Route over Service Connections (Accepter l'itinéraire par défaut via les connexions aux services)**, toutes les connexions aux services Prisma Access, à l'exception des connexions aux service dédiées, acceptent les itinéraires par défaut et utiliseront les itinéraires dans les décisions de redirection du trafic.
- Avant d'activer ce paramètre, assurez-vous que vos centres de données envoient des itinéraires par défaut. Sinon, le routage via les connexions aux services échouera.
- Palo Alto Networks recommande que tous les centres de données publient un itinéraire par défaut. Lorsque Prisma Access reçoit les itinéraires, il peut alors sélectionner la meilleure connexion aux services à utiliser pour l'emplacement du réseau distant.
- Lorsque vous configurez des connexions aux services, utilisez soit uniquement des itinéraires statiques, soit uniquement BGP pour les connexions. Palo Alto Networks ne recommande pas de mélanger les connexions aux services qui utilisent BGP et les itinéraires statiques lors de l'utilisation d'itinéraires par défaut.
- (Pour les déploiements Prisma Access (Managed by Panorama) uniquement) L'utilisation d'itinéraires par défaut est prise en charge avec les déploiements multilocataires.

 ©2025 Palo Alto Networks, Inc.

- Prisma Access ne transfère pas le trafic d'authentification SAML du VPN sans client, du portail ou de la passerelle à un fournisseur d'identité public (IdP) en utilisant l'itinéraire par défaut.

Pour plus d'informations et des exemples de mise en œuvre d'itinéraires par défaut avec la redirection du trafic, consultez Exemple d'itinéraires par défaut avec redirection du trafic, Exemple d'itinéraires par défaut avec redirection du trafic directement vers Internet et Exemple d'itinéraires par défaut avec redirection du trafic et connexion aux services dédiée.

Redirection du trafic dans Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Dans les déploiements de Prisma Access standard, une connexion de service donne accès à des ressources réseau internes, telles que des services d'authentification et des applications privées dans votre siège ou votre centre de données. Les connexions de service traitent le trafic interne, où aucun accès Internet n'est requis. Dans certains cas, vous pouvez rediriger le trafic lié à Internet vers le centre de données. La redirection du trafic vous permet de rediriger le trafic des utilisateurs mobiles ou du réseau distant vers une connexion de service avant d'être envoyé vers Internet.

Vous pouvez utiliser la redirection du trafic avec des déploiements d'utilisateurs mobiles, des déploiements de réseau distant ou une combinaison des deux. Utilisez la redirection du trafic pour rediriger le trafic réseau lié à Internet en fonction de nombreux critères, y compris les adresses IP, les utilisateurs, les URL, les catégories d'URL personnalisées, le type de service (HTTP ou HTTPS), l'identifiant utilisateur, les groupes d'adresses dynamiques (DAG), les groupes d'utilisateurs dynamiques (DUG) et les listes dynamiques externes (EDL) basées sur IP.

Il existe deux types d'action pris en charge avec la redirection du trafic :

- **Forward to the target (Transférer vers la cible)** – Utilisez les critères des règles de redirection du trafic pour transférer le trafic lié à Internet via une cible que vous créez qui utilise une ou plusieurs connexions de service.
- **Forward to the internet (Transférer vers Internet)** — Utilisez les critères des règles de redirection du trafic pour transférer directement le trafic de sa source (emplacement de l'utilisateur mobile ou connexion réseau distante) vers Internet, sans être transféré vers une connexion de service.

Si vous transférez vers une cible, vous pouvez choisir de créer deux types de groupes cibles : dédiés et non dédiés.

- Une connexion de service qui est utilisée uniquement pour le trafic lié à la redirection du trafic est une *connexion de service dédiée*. Pour définir une connexion de service à utiliser en tant que connexion de service dédiée, sélectionnez **Dedicated for Traffic Steering Only (Dédié à la direction du trafic uniquement)** lorsque vous Configurer la redirection du trafic dans Prisma

 ©2025 Palo Alto Networks, Inc.

Access dans Panorama. Sélectionnez **Dedicated for PBF Only (Dédié pour PBF uniquement)** lorsque vous configurez une règle de redirection du trafic dans Strata Cloud Manager.

Vous pouvez configurer une connexion de service dédiée si vous utilisez une pile de sécurité tierce qui se trouve en dehors du réseau interne de votre organisation pour traiter le trafic avant qu'il ne soit envoyé à une application SaaS publique ou à Internet. Étant donné que la pile de sécurité ne fait pas partie du réseau de votre organisation, cette connexion de service ne doit pas traiter le trafic réseau interne.

- Une connexion de service qui est utilisée pour la redirection du trafic et pour le trafic standard lié à la connexion de service (comme le trafic allant à un serveur d'authentification dans le centre de données) est une *connexion de service non dédiée*.

La définition d'une connexion de service en tant que connexion de service dédiée entraîne les modifications suivantes dans votre déploiement :

- (Réservé aux déploiements Prisma Access (Managed by Strata Cloud Manager)) Les connexions de service appliquent le NAT source au trafic transféré. L'adresse IP source est l'adresse **EBGP Router (Routeur EBGP)** de la connexion de service, qui est tirée du sous-réseau Infrastructure.
- La zone pour toutes les connexions de service associées à cette cible passe de Trust à Untrust. Vérifiez votre mappage de zone et votre Configurer le mappage de zone et les politiques de sécurité pour les connexions dédiées à la redirection du trafic pour vous assurer que votre réseau reflète ce changement.
- Les connexions de service configurées en tant que connexions de service dédiées ne participent pas au routage BGP, que ce soit en interne ou en externe.
- (Réservé aux déploiements Prisma Access (Managed by Panorama)) Si votre connexion de service dédiée utilise BGP, l'état BGP apparaît comme **Not Enabled (Non activé)** lorsque vous ouvrez la page d'état (**Panorama** > **Cloud Services** > **Status (État)** > **Monitor (Surveiller)** > **Service Connection (Connexion de service)**), sélectionnez une région, puis sélectionnez l'onglet Status (État). Pour vérifier l'état BGP d'une connexion de service, consultez la page de configuration des connexions de service (**Panorama** > **Cloud Services** > **Configuration** > **Service Connection (Connexion de service)**).
- (Réservé aux déploiements Prisma Access (Managed by Panorama)) Par défaut, les connexions de service appliquent le NAT source au trafic transféré. L'adresse IP source est la **User-ID Agent Address (Adresse User-ID)** de la connexion de service (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion de service)** > **User-ID Agent Address (Adresse User-ID)**), qui est tirée du sous-réseau Infrastructure (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Infrastructure (Infrastructure du service)**).

  (Réservé aux déploiements Prisma Access (Managed by Panorama)) Vous pouvez désactiver le NAT source et utiliser les adresses IP source de votre organisation pour la connexion de service dédiée ; pour ce faire, sélectionnez **Disable Source NAT for Dedicated SC (Désactiver le NAT source pour SC dédié)** lorsque vous cliquez sur **Add (Ajouter)** pour ajouter une cible dans la section **Target Service Connections for Traffic Steering (Connexions de service cible pour la redirection du trafic)**.

 ©2025 Palo Alto Networks, Inc.

Exigences relatives à la redirection du trafic

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Avant de mettre en œuvre la redirection du trafic dans votre déploiement Prisma Access, assurez-vous que votre environnement réseau respecte l'infrastructure minimale suivante :

- Prisma Access doit être en mesure de se connecter au CPE compatible IPSec (comme un routeur ou un périphérique SD-WAN) que votre organisation utilise pour mettre fin à la connexion de service, et l'adresse IP du périphérique doit être accessible à partir de Prisma Access.

  Vous créez une connexion de service à l'aide de profils cryptographiques standard IPSec et IKE entre l'emplacement de la pile et Prisma Access. Vous pouvez utiliser des itinéraires statiques, BGP ou une combinaison des deux lorsque vous configurez une connexion de service et utilisez la redirection du trafic. Si vous utilisez des itinéraires par défaut avec la redirection du trafic, Palo Alto Networks recommande d'utiliser uniquement BGP ou uniquement des itinéraires statiques. Si vous utilisez une redirection statique, spécifiez l'adresse IP publique utilisée par le CPE de l'organisation en tant que **Peer Address (Adresse du pair)** lorsque vous créez une passerelle IKE.
- Prisma Access peut ne pas correspondre aux premiers paquets d'une URL d'une catégorie d'URL dans une règle de redirection du trafic, ce qui signifie que les premiers paquets d'une session réseau (par exemple, un établissement de liaison TCP) peuvent ne pas correspondre à la règle. Palo Alto Networks recommande, pour les URL que vous utilisez dans les règles de redirection du trafic, de créer une règle de politique de sécurité pour les autoriser à traverser la zone non approuvée afin que l'établissement de la liaison puisse se terminer lorsqu'une nouvelle session commence.
- Si vous utilisez cette configuration avec une pile de sécurité, l'emplacement de la pile doit être accessible à partir de la connexion de service par une configuration de tunnel IPSec standard.

Utilisez les instructions suivantes lors de la configuration de la redirection du trafic :

- Vous pouvez spécifier jusqu'à 1 000 URL (agrégées) dans une configuration de redirection du trafic, y compris les URL standard et génériques (*.exemple.com) dans des catégories d'URL personnalisées.

  Ce nombre inclut à la fois les URL saisies manuellement, les URL génériques et les URL saisies dans une catégorie d'URL personnalisée.
- Prisma Access ajoute un astérisque aux URL dans les catégories d'URL personnalisées, si vous utilisez cette catégorie dans une règle de redirection du trafic. Si vous utilisez les mêmes politiques de catégorie d'URL pour la redirection du trafic et d'autres règles de politique de sécurité, ces modifications s'appliquent à la fois aux règles de redirection du trafic et aux autres règles de politique de sécurité.

  Si vous avez des catégories d'URL personnalisées qui ne sont pas utilisées dans les règles de redirection du trafic, Prisma Access ne modifie pas les URL de ces catégories.

 ©2025 Palo Alto Networks, Inc.

- Utilisez toutes les URL en minuscules lorsque vous entrez des URL dans une règle de transfert de trafic et lorsque vous ajoutez des URL dans une catégorie d'URL personnalisée.
- Vous pouvez configurer un maximum de 100 règles de transfert de trafic.
- Si vous avez configuré des tunnels principal et de secours, la redirection du trafic à l'aide des règles de redirection du trafic ne fonctionnera pas après un basculement du tunnel principal (actif) vers le tunnel de secours. Itinéraires par défaut avec redirection du trafic Prisma Access fonctionne dans un scénario de basculement avec des tunnels principaux et de secours.

Exemple d'itinéraires par défaut avec redirection du trafic

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

L'exemple suivant montre un déploiement Prisma Access des composants suivants :

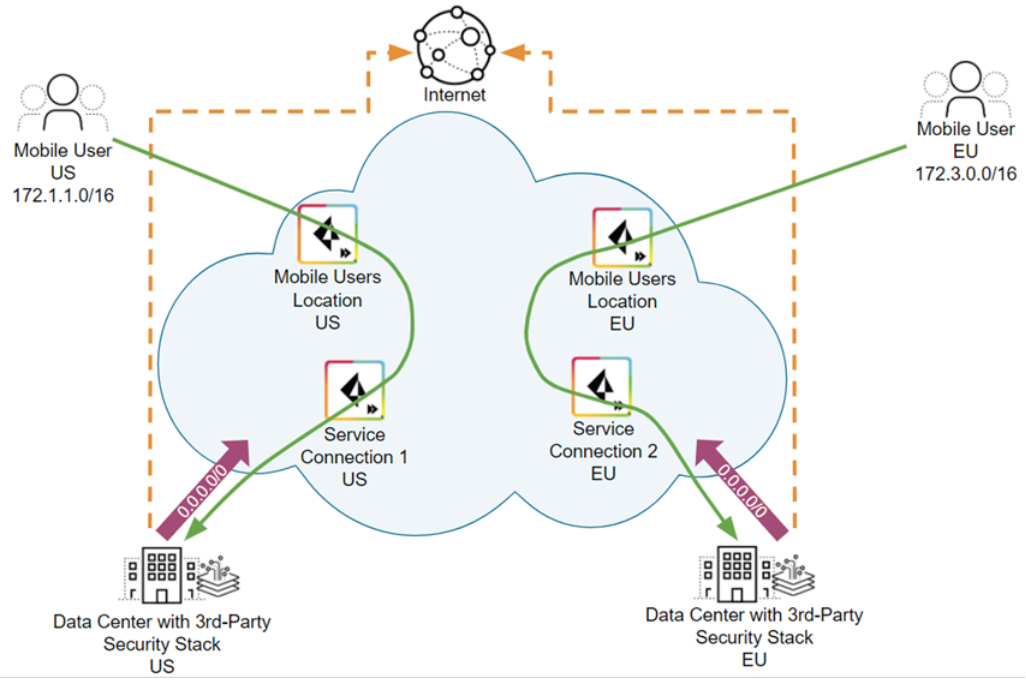
- Deux emplacements d'utilisateurs mobiles Prisma Access ; l'un aux États-Unis (US) et l'autre en Europe (UE).
- Deux connexions aux services Prisma Access ; une aux États-Unis et une dans l'UE, avec les deux centres de données envoyant des itinéraires par défaut aux connexions aux services (l'option **Accept Default Route over Service Connections (Accepter l'itinéraire par défaut via les connexions aux services)** est activée).
- Deux centres de données ; un aux États-Unis et un dans l'UE.

  Chaque centre de données dispose d'une pile de sécurité tierce. Pour cette raison, vous souhaitez que tout le trafic sortant vers Internet passe par le centre de données avant de sortir vers Internet.

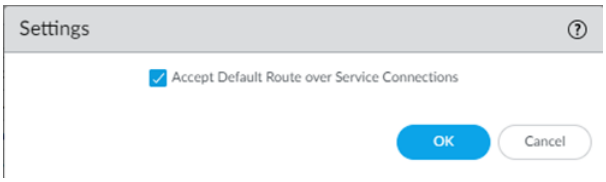
Lorsqu'un utilisateur mobile envoie du trafic de centre de données, Prisma Access vérifie ses tables de routage, détermine la connexion aux services la plus proche et transfère le trafic à cette connexion aux services. Dans l'exemple suivant, Prisma Access envoie le trafic des centres de données des utilisateurs mobiles aux États-Unis vers la connexion aux services et le trafic des utilisateurs mobiles de l'UE vers la connexion aux services 2.

*N'utilisez pas les connexions aux services **Dedicated for Traffic Steering Only (Dédiées à la redirection du trafic uniquement)** avec des itinéraires par défaut. Les connexions aux services dédiées ne participent pas au routage BGP, donc elles ne peuvent pas recevoir d'annonces BGP du siège ou du centre de données.*

 ©2025 Palo Alto Networks, Inc.



Pour activer les itinéraires par défaut, sélectionnez **Accept Default Route over Service Connections (Accepter l'itinéraire par défaut via les connexions aux services)** lorsque vous configurez les paramètres de redirection du trafic. Après avoir configuré ce paramètre, puis validé et appliqué vos modifications, Prisma Access envoie le trafic sortant vers Internet via les connexions aux services.

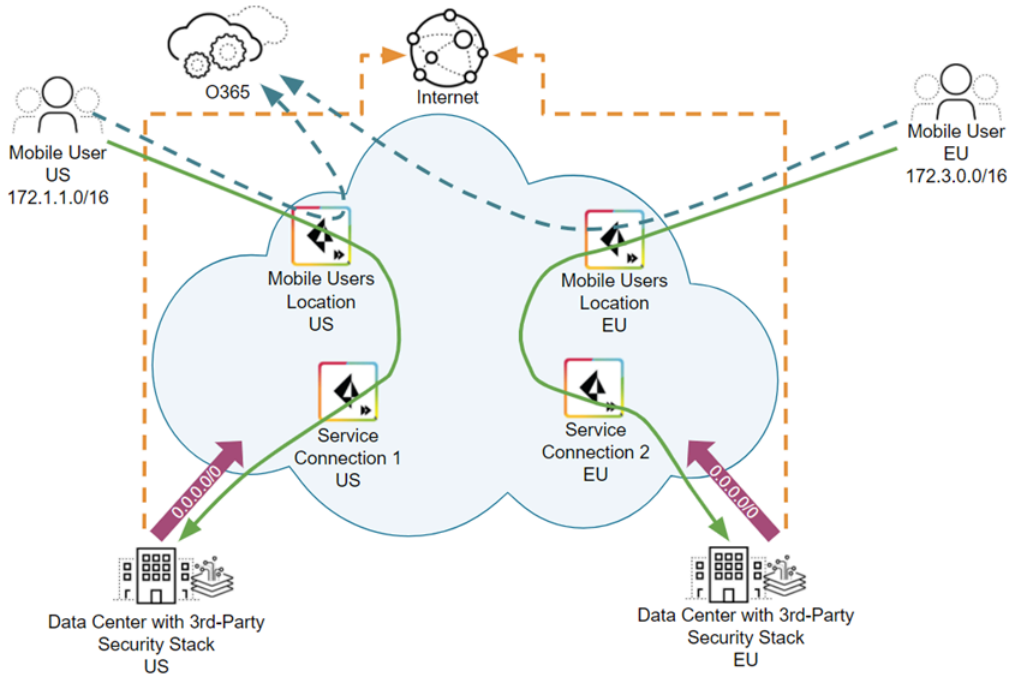


Exemple d'itinéraires par défaut avec redirection du trafic directement vers Internet

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

L'exemple suivant vous montre comment utiliser un contrôle plus granulaire pour le trafic lié aux applications SaaS externes. Dans ce cas, vous souhaitez envoyer le trafic Office 365 vers la sortie directement depuis l'emplacement de l'utilisateur mobile, au lieu de l'envoyer au centre de données pour un traitement supplémentaire. Utilisez la gestion du trafic avec les itinéraires par défaut pour cette configuration.

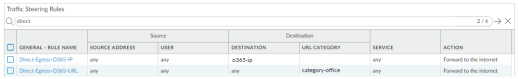
 ©2025 Palo Alto Networks, Inc.



Pour autoriser Prisma Access à router le trafic Office 365 directement vers Internet, effectuez les actions suivantes :

- Créez une EDL (**Object (Objet)** > **External Dynamic Lists (Listes dynamiques externes)**) avec des adresses IP qui correspondent aux adresses Office 365.
- Créez une catégorie d'URL personnalisée (**Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)**) avec des URL qui correspondent à l'URL Office 365.
- Créez Configurer la redirection du trafic dans Prisma Access et spécifiez l'EDL et la catégorie d'URL que vous avez créées comme critères de correspondance de destination avec une **Action Forward to the internet (Transférer vers Internet)**.

Cette configuration envoie le trafic Office 365 directement sur Internet, tandis que les autres trafics à destination d'Internet sont envoyés au centre de données pour un traitement supplémentaire avant de sortir vers Internet.



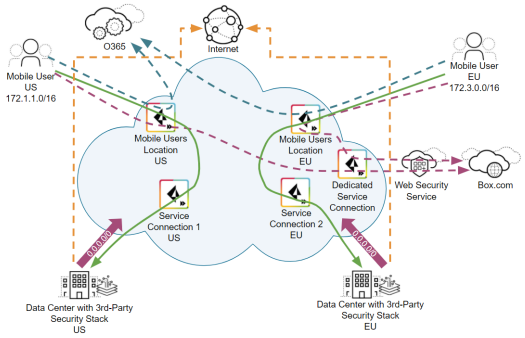
Exemple d'itinéraires par défaut avec redirection du trafic et connexion aux services dédiée

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	☐ Licence Prisma Access

Dans cet exemple, en plus de la configuration précédente, vous disposez d'un service de sécurité Internet tiers et vous souhaitez envoyer du trafic à partir de box.com pour qu'il soit traité par le service de sécurité avant de sortir vers Internet. Vous ne souhaitez pas envoyer d'autre

 ©2025 Palo Alto Networks, Inc.

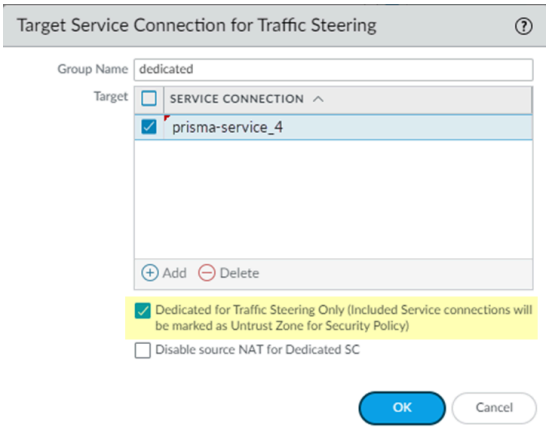
trafic Internet au service de sécurité. Pour cette raison, vous créez une connexion aux services dédiée pour le trafic box.com. Une fois votre configuration terminée, Prisma Access envoie le trafic de destination *.box.com vers la pile.



Pour activer ce déploiement, vous devez effectuer les actions suivantes dans l'onglet Traffic Steering (Redirection du trafic) :

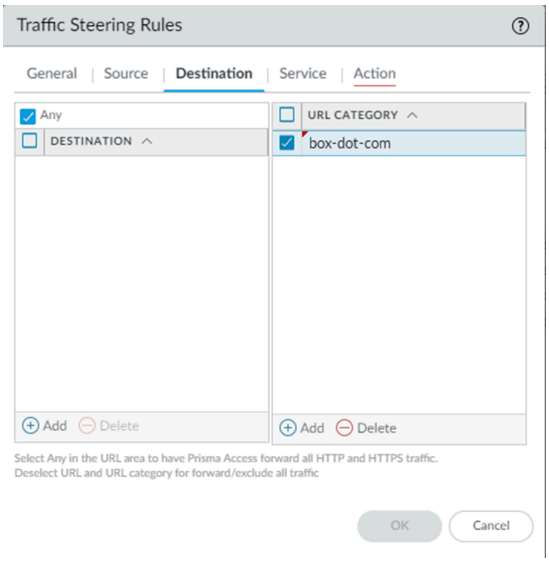
- Créez un groupe de connexions aux services cible qui attribue une ou plusieurs connexions aux services à la cible, puis sélectionnez **Dedicated for Traffic Steering Only (Dédiée à la redirection du trafic uniquement)**, ce qui rend la ou les connexions aux services cibles dédiées.

Si vous créez une cible avec plusieurs connexions aux services, Prisma Access choisit la meilleure connexion aux services pour transférer le trafic Internet.

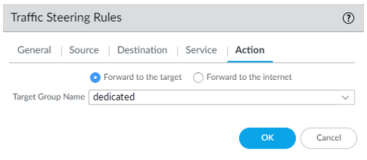


 ©2025 Palo Alto Networks, Inc.

- Créez une règle de redirection du trafic qui redirige le trafic vers l'URL. La capture d'écran suivante montre que la destination du trafic se voit attribuer une catégorie d'URL personnalisée contenant l'URL *.box.com.



- Créez une **Action** dans la règle de redirection du trafic **Forward to the target (Transférer vers la cible)** et spécifiez le nom du groupe cible que vous avez créé (**dedicated (dédié)** dans ce cas).



Lignes directrices sur les règles de redirection du trafic Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Panorama	• Licence Prisma Access

La redirection du trafic peut traiter une grande variété de configurations possibles ; cependant, il est important de comprendre comment Prisma Access traite les règles, afin de pouvoir créer des règles faciles à maintenir et à gérer. Pour créer les règles les mieux adaptées à votre déploiement, suivez ces instructions :

- Prisma Access évalue les règles dans l'ordre dans lequel vous les créez (de haut en bas). Spécifiez les règles plus spécifiques en haut et les règles plus générales en bas.
- Créez plusieurs règles avec moins de critères de correspondance, au lieu de créer moins de règles avec plusieurs types de critères. La création de règles plus simples accélère la création de règles et facilite leur modification.
- Étant donné que vous ne pouvez pas déplacer une règle vers le haut ou vers le bas dans une liste après l'avoir créée, planifiez soigneusement l'ordre de vos règles avant de les créer.
- Les règles qui spécifient **Any (Toute)** adresse source et tout utilisateur, **Any (Toute)** destination source et catégorie d'URL, ainsi que **Any (Tout)** service ne sont pas prises en charge. Utilisez

 ©2025 Palo Alto Networks, Inc.

des règles plus spécifiques ; par exemple, spécifiez une règle avec **Any (Tout)** trafic source ou de destination et un service **service-http** et **service-https**.

- Si vous souhaitez spécifier des règles pour les utilisateurs dans le champ **Source User (Utilisateur source)**, assurez-vous que Prisma Access peut distinguer les utilisateurs si le même nom d'utilisateur est partagé entre les utilisateurs qui s'authentifient localement et ceux qui s'authentifient via LDAP en authentifiant les utilisateurs LDAP au format `domaine/nom d'utilisateur` et en authentifiant les utilisateurs locaux au format `nom d'utilisateur` (sans le nom de domaine).
- Si vous avez configuré un pare-feu nouvelle génération sur site en tant que périphérique maître, vous pouvez renseigner automatiquement les informations d'utilisateur et de groupe pour les groupes de périphériques d'utilisateurs mobiles dans les règles de redirection du trafic et de politique de sécurité en sélectionnant **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users (Utilisateurs mobiles)**, en cliquant sur l'icône d'engrenage pour modifier les paramètres et en sélectionnant le **Master Device (Périphérique maître)** dans la section Device Group (Groupe de périphériques). Bien que cela renseigne le périphérique maître dans chaque groupe de périphériques, cela renseigne uniquement les informations d'utilisateur et de groupe pour les utilisateurs mobiles dans les règles de politique de sécurité.
- Si une EDL (type Liste IP) est utilisée dans une règle de redirection du trafic et que l'URL source de l'EDL est mise à jour vers une URL qui n'est pas accessible, Prisma Access peut continuer à utiliser la liste IP mise en cache de l'URL précédente.
- Prisma Access contourne la redirection du trafic pour les règles avec un type de service HTTP ou HTTPS si vous utilisez une politique de contrôle prioritaire sur l'application pour les ports TCP 80 et 443.

  De plus, la redirection du trafic ne fonctionne pas pour les URL des catégories d'URL référencées dans la règle de redirection du trafic si vous avez configuré une politique de contrôle prioritaire sur l'application pour les ports TCP 80 ou 443.
- Vous pouvez spécifier des adresses IP de destination et des catégories d'URL dans la même règle. Si vous le faites, Prisma Access utilise un OU logique pour traiter les critères de destination dans la règle, mais traite les URL et le trafic de catégorie d'URL en fonction des ports TCP 80 et 8080 pour HTTP et du port TCP 443 pour HTTPS.

  Pour une règle avec des adresses IP et des catégories d'URL, le trafic correspond à la règle si l'adresse IP ou la catégorie d'URL correspond, mais traite le trafic de catégorie d'URL en fonction des ports 80, 443 et 8080 uniquement. Palo Alto Networks ne recommande pas de créer une règle de ce type ; créez plutôt des règles plus simples.

Par exemple, vous souhaitez appliquer les règles suivantes à votre trafic réseau :

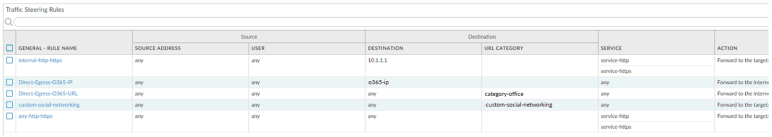
- Vous disposez d'un serveur HTTP interne avec une adresse IP de 10.1.1.1 dans le centre de données et vous souhaitez diriger le trafic HTTP et HTTPS interne vers ce serveur. L'adresse IP du serveur est 10.1.1.1.

  Le trafic vers ce serveur ne doit pas passer par Internet et doit être traité en interne. Par conséquent, choisissez une cible non dédiée pour ce trafic, car ce type de cible traite à la fois le trafic interne et celui lié à Internet.
- Vous souhaitez que le trafic office365.com soit acheminé directement vers Internet.
- Vous souhaitez que le trafic provenant de *.exemple.com ou tout trafic défini dans une catégorie d'URL personnalisée de **custom-social-networking** soit acheminé vers une connexion dédiée.

 ©2025 Palo Alto Networks, Inc.

- Vous souhaitez que tout autre trafic HTTP et HTTPS utilise la même cible de connexion de service non dédiée que celle utilisée pour le serveur HTTP interne.

Pour cet exemple, créez les règles de la plus spécifique à la moins spécifique, comme indiqué dans la capture d'écran suivante. N'ajoutez pas d'abord la règle qui autorise tout le trafic HTTP et HTTPS, sinon Prisma Access redirigerait tout le trafic HTTP et HTTPS vers la connexion non dédiée sans évaluer aucune des autres règles.



Configurer le mappage de zone et les politiques de sécurité pour les connexions dédiées à la redirection du trafic

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Si vous créez une cible qui utilise une connexion aux services dédiée, la zone de la connexion aux services dédiée passe de **Trust (Approuvée)** à **Untrust (Non approuvée)** (les cibles de connexion aux services non dédiée ne changent pas de zone). Puisque vous ne pouvez pas créer de zones ou configurer le mappage de zones pour les connexions aux services, vous apportez plutôt des modifications au mappage des zones et à la politique de sécurité pour les connexions aux services dédiées aux utilisateurs mobiles et aux groupes de périphériques. Procédez comme suit pour configurer le mappage de zone pour les connexions dédiées.

Ces étapes montrent un exemple de configuration. Vous pouvez personnaliser cet exemple en fonction de votre déploiement.

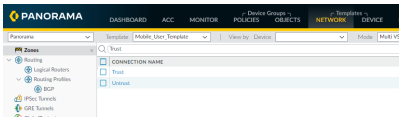
STEP 1 | Sélectionnez **Network (Réseau)** > **Zones**.

STEP 2 | Sélectionnez le bon **Template (Modèle)** dans la liste déroulante (**Mobile_User_Template** pour les utilisateurs mobiles ou **Remote_Network_Template** pour les réseaux distants).

Si vous disposez d'un utilisateur mobile et d'un déploiement de réseaux distants, vous devez effectuer ces étapes deux fois : une fois dans le modèle **Mobile_User_Template** et une fois dans le modèle **Remote_Network_Template**.

STEP 3 | Cliquez sur **Add (Ajouter)** pour ajouter deux zones pour vos zones approuvées et non approuvées.

Cet exemple crée deux zones appelées **Trust (Approuvée)** et **Untrust (Non approuvée)**.



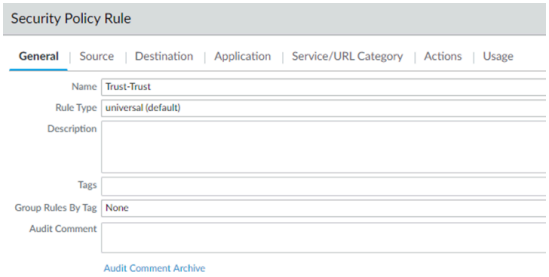
 ©2025 Palo Alto Networks, Inc.

STEP 4 | Créez des politiques par défaut pour les zones que vous avez créées.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Post Rules (Post-règles)**.
2. Sélectionnez le bon **Device Group (Groupe de périphériques)** dans la liste déroulante (**Mobile_User_Device_Group** pour les réseaux distants ou **Remote_Network_Device_Group** pour les utilisateurs mobiles).

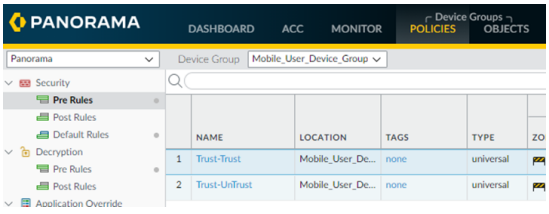
   Si vous disposez d'un utilisateur mobile et d'un déploiement de réseaux distants, vous devez effectuer ces étapes deux fois : une fois dans le modèle **Mobile_User_Device_Group** et une fois dans le modèle **Remote_Network_Device_Group**.
3. Cliquez sur **Add (Ajouter)** pour ajouter une politique par défaut à utiliser pour le trafic d'une zone approuvée à une zone non approuvée.

   Cette politique permet au trafic **Any (Indifférent)** de passer pour tous les trafics suivants : **Source**, **User (Utilisateur)**, **Destination**, **Application** et **Service/URL Category (Catégorie de service/URL)**.



4. Cliquez sur **Add (Ajouter)** pour ajouter une politique par défaut à utiliser pour le trafic d'une zone approuvée à une zone non approuvée, en utilisant les mêmes paramètres que ceux que vous avez utilisés pour la politique approuvée-non approuvée.

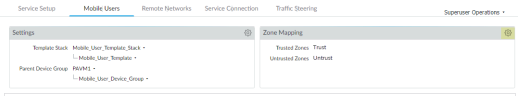
   Une fois l'opération terminée, vous disposez de deux politiques de sécurité, l'une pour le trafic d'une zone approuvée-approuvée et l'autre pour le trafic d'une zone approuvée-non approuvée.



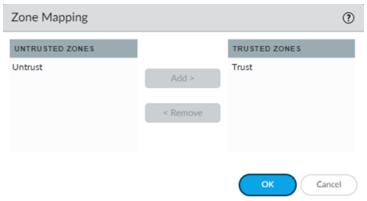
 ©2025 Palo Alto Networks, Inc.

STEP 5 | Définissez le mappage de zone pour les réseaux distants, les utilisateurs mobiles ou les deux, selon les besoins de votre déploiement.

1. Définissez le mappage de zone pour les réseaux distants, les utilisateurs mobiles ou les deux.
   - Pour les utilisateurs mobiles, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Mobile Users (Utilisateurs mobiles)**.
   - Pour les réseaux distants, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**.
2. Cliquez sur l'icône d'engrenage à côté de **Zone Mapping (Mappage des zones)** pour modifier les paramètres.



3. Définissez la zone **Zone Mapping (Mappage des zones)** pour votre déploiement, en déplaçant la zone de trafic approuvé vers **Trusted Zones (Zones approuvées)** et la zone pour le trafic non approuvé vers **Untrusted Zones (Zones non approuvées)**. Ensuite, cliquez sur **OK**.



Configurer la redirection du trafic dans Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ La possibilité d'envoyer la liste de révocation de certificats (CRL) et le protocole de vérification des certificats en ligne (OCSP) directement à Internet nécessite une version minimale de Prisma Access de 5.1.1.

La redirection du trafic vous permet de configurer l'accès pour créer des règles de redirection du trafic afin de spécifier des cibles pour le trafic sortant vers Internet des utilisateurs mobiles et des connexions au réseau distant. Vous pouvez spécifier le trafic à rediriger vers une connexion aux services avant l'envoi vers Internet, ou vous pouvez spécifier le trafic à sortir directement vers Internet. Configurez la redirection du trafic pour votre déploiement Prisma Access en procédant comme suit.

- Strata Cloud Manager
- Panorama

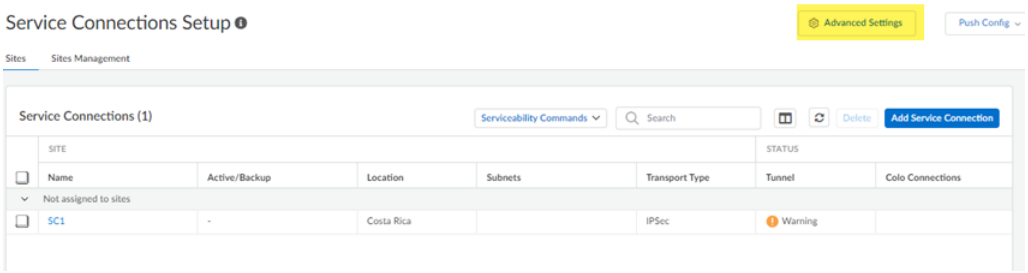
 ©2025 Palo Alto Networks, Inc.

Configurer la redirection du trafic dans Prisma Access (Strata Cloud Manager)

Dans les déploiements Prisma Access, une connexion aux services donne accès à des ressources réseau internes, telles que des services d'authentification et des applications privées dans votre siège ou votre centre de données. Les connexions de service traitent le trafic interne, où aucun accès Internet n'est requis. Dans certains cas, vous pouvez rediriger le trafic lié à Internet vers le centre de données. La redirection du trafic vous permet de rediriger le trafic des utilisateurs mobiles ou du réseau distant vers une connexion de service avant d'être envoyé vers Internet. Configurez la redirection du trafic pour votre déploiement Prisma Access en procédant comme suit.

STEP 1 | Intégrez vos connexions aux services, utilisateurs mobiles et réseaux distants, selon votre déploiement.

STEP 2 | Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Service Connections (Connexions aux services)** > **Advanced Settings (Paramètres avancés)**.



STEP 3 | Configurez la règle **Traffic Steering (Redirection du trafic)**.

1. (Facultatif, déploiements pour utilisateurs mobiles uniquement) Autorisez Prisma Access à accepter et installer l'itinéraire par défaut publié sur une ou plusieurs connexions aux services à partir du CPE en cliquant sur l'icône d'engrenage pour ouvrir les paramètres et en sélectionnant **Accept Default Route over Service Connections (Accepter l'itinéraire par défaut sur les connexions aux services)**.

   Les itinéraires par défaut ont des directives que vous devez suivre lorsque vous les utilisez. Par exemple, les itinéraires par défaut sont pris en charge pour les déploiements d'utilisateurs mobiles uniquement et n'ont aucun effet sur les déploiements de réseaux distants. Assurez-vous de consulter ces directives avant de mettre en œuvre des itinéraires par défaut avec la redirection du trafic.

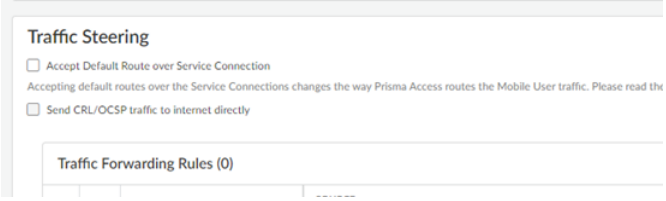
STEP 4 | (Facultatif) Autorisez Prisma Access à envoyer le trafic de la liste de révocation de certificats (CRL) et du protocole de vérification des certificats en ligne (OCSP) directement vers Internet

 ©2025 Palo Alto Networks, Inc.

en sélectionnant **Send CRL/OCSP traffic to internet directly (Envoyer le trafic CRL/OCSP directement vers Internet)**.

Sélectionnez ce choix si vous avez un serveur OCSP ou CRP dans l'Internet public et que vous souhaitez envoyer ce trafic directement vers Internet en utilisant la zone non approuvée. Si vous ne sélectionnez pas ce choix, Prisma Access envoie ce trafic à la connexion aux services.

*Assurez-vous d'avoir mis à niveau votre déploiement Prisma Access vers une version minimale de 5.1.1 avant de sélectionner **Send CRL/OCSP traffic to internet directly (Envoyer le trafic CRL/OCSP directement vers Internet)**.*



STEP 5 | Créez des règles pour la cible que vous avez créée et appliquez-les à la cible.

1. Cliquez sur **Add Rule (Ajouter une règle)**.
2. Saisissez un **Name (Nom)** unique pour la règle.
3. Sous la zone **Source** :
   - Spécifiez la liste des utilisateurs à mettre en correspondance.

     Vous pouvez cliquer sur **Match Any User (Faire correspondre n'importe quel utilisateur)**, **Match Pre-logon (Faire correspondre une préouverture de session)**, **Match known-user (Faire correspondre l'utilisateur connu)**, **Match unknown (Faire correspondre un utilisateur inconnu)** ou **Add Users (Ajouter des utilisateurs)**, puis sélectionnez l'utilisateur ou les utilisateurs à faire correspondre.
   - Sélectionnez **Source Address Entities (Entités d'adresse source)**. Vous pouvez sélectionner un ou plusieurs des objets suivants :
     - Une adresse IP
     - Un groupe d'adresses
     - Une liste dynamique externe (EDL) avec des adresses IP ou des URL
4. Dans la zone **Destination**, spécifiez l'une des options suivantes **Destination Address Entities (Entités d'adresse de destination)** ou sélectionnez **Any (Indifférent)** pour que le trafic soit traité par les règles dans le champ URL Category (Catégorie d'URL) :
   - Une adresse IP
   - Un groupe d'adresses
   - Une liste dynamique externe (EDL) avec des adresses IP ou des URL
5. Spécifiez une **URL Category (Catégorie d'URL)**.

   Si vous créez une catégorie d'URL personnalisée, entrez les URL en minuscules. La redirection du trafic prend en charge les URL personnalisées et les catégories d'URL

 ©2025 Palo Alto Networks, Inc.

prédéfinies. Vous pouvez utiliser des caractères génériques avec les URL dans les catégories d'URL. Les formats de caractères génériques suivants sont pris en charge :

- *.exemple.com
- *.fqdn.exemple.com

Les formats suivants ne sont pas pris en charge :

- *
- *.*
- *exemple.com
- exemple.com/ (les barres obliques de fin dans les URL ne sont pas prises en charge dans les catégories d'URL utilisées avec la redirection du trafic)
- exemple.com/path (seuls les noms de domaine sont pris en charge)
- *fqdn.exemple.com
- fqdn.exemple.*

Utilisez les directives suivantes lors de la configuration des options de destination :

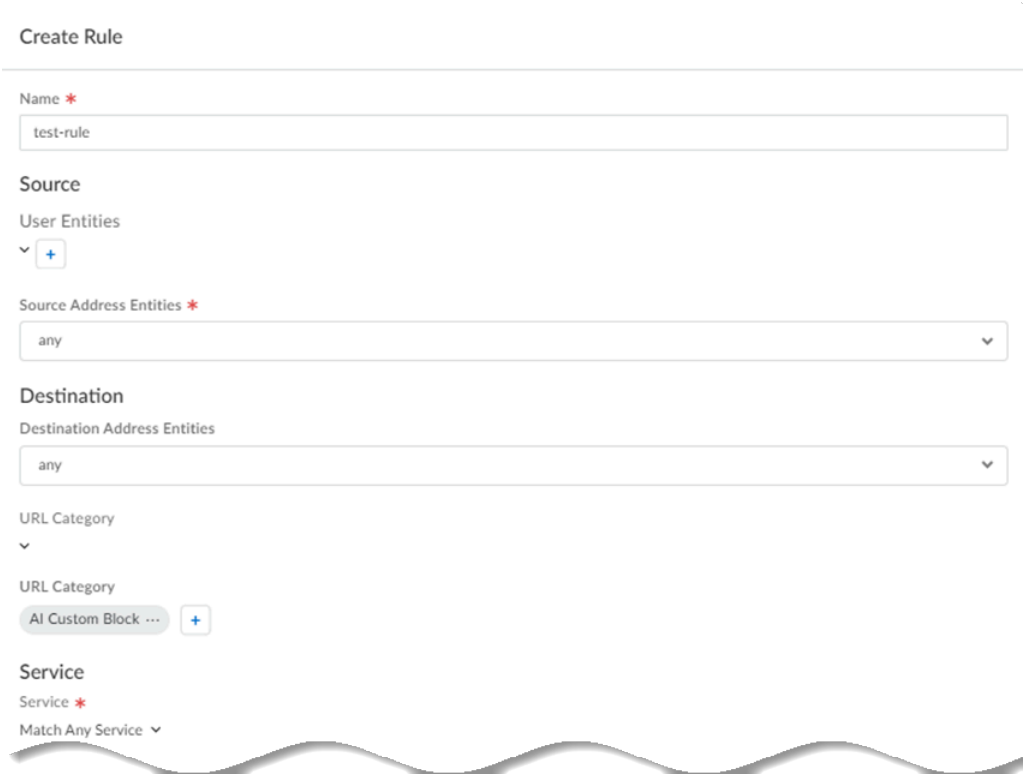
- Si vous spécifiez une catégorie d'URL, Prisma Access correspond uniquement au trafic HTTP et HTTPS, même lorsque le service est défini sur **Any (Indifférent)**.
- Ne créez pas de catégorie d'URL personnalisée avec le type **Catégorie Match (Faire correspondre une catégorie)**.

Ne créez pas de catégorie d'URL personnalisée avec le nom **Custom_URL_Category_TFR**.

6. Spécifiez un type **Service** et sélectionnez **Add Service (Ajouter un service)**.

   Spécifiez **service-http** pour transférer le trafic HTTP et spécifiez **service-https** pour spécifier le trafic HTTPS. Sélectionnez **Match Any Service (Faire correspondre n'importe quel service)** pour transférer le trafic de n'importe quel type de service.

 ©2025 Palo Alto Networks, Inc.



7. Créez un groupe de connexions aux services et spécifiez une **Action**.
   1. Sélectionnez **Create New (Créer nouveau)** ou **Manage (Gérer)** pour gérer un groupe et lui donner un **Name (Nom)**.
   2. Spécifiez la **Service Connection (Connexion aux services)** ou des connexions aux services à utiliser avec la cible.

      Palo Alto Networks ne recommande pas d'utiliser plusieurs connexions aux services (dédiées ou non) dans un groupe de connexions aux services cible référencé dans une règle de redirection du trafic. En outre, une connexion aux services donnée ne peut exister que dans une seule cible et vous ne pouvez pas ajouter une seule connexion aux services à deux cibles différentes.
   3. (Facultatif) Vous pouvez utiliser une connexion aux services dédiée pour rediriger le trafic vers une pile de sécurité ou un cloud tiers qui n'est pas dans vos locaux et n'a pas besoin de participer au routage. Pour définir une connexion aux services à utiliser en tant que connexion aux services dédiée, sélectionnez **Dedicated for Traffic Steering Only (Dédiée à la redirection du trafic uniquement)**.

      Les connexions aux services dédiées changent de zone et sont marquées comme zone non approuvée pour les règles de politique de sécurité.

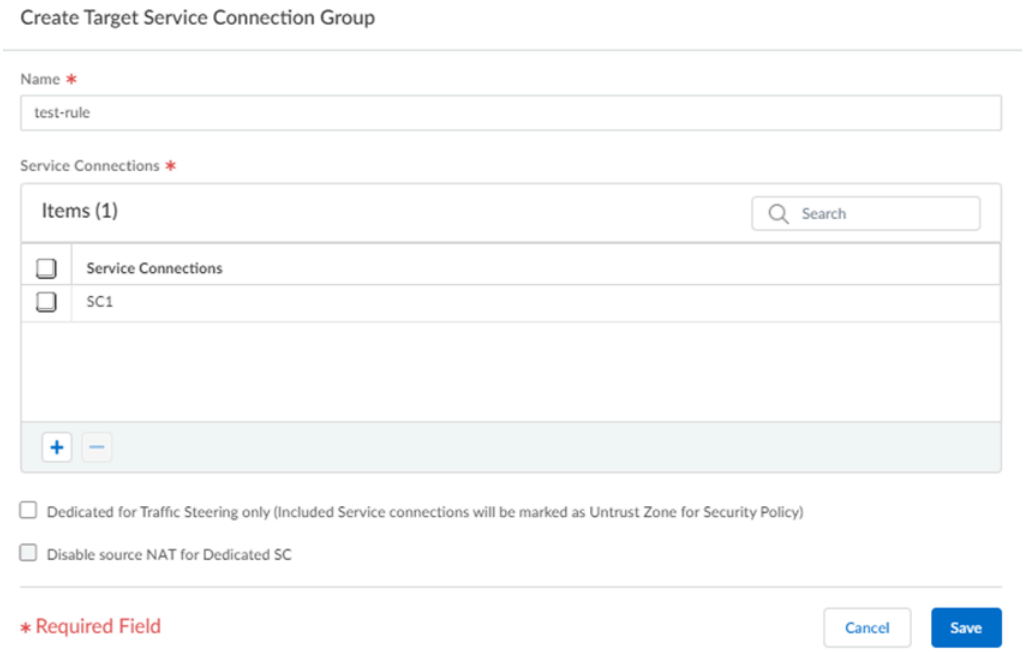
      Désélectionnez **Dedicated for Traffic Steering Only (Dédiée à la redirection du trafic uniquement)** si vous envoyez à la fois du trafic normal lié à la connexion aux services

 ©2025 Palo Alto Networks, Inc.

et du trafic de redirection du trafic via la connexion aux services. Avec ce choix, la zone pour la connexion aux services reste comme approuvée.

4. Désactivez la NAT source pour les connexions aux services dédiées en sélectionnant **Disable Source NAT for Dedicated SC (Désactiver la NAT source pour le SC dédié)**. La NAT source est activée par défaut (la case est décochée).

   Si vous désactivez la NAT source, Prisma Access utilise les adresses IP source de votre organisation pour la connexion aux services dédié. Si vous activez la NAT source, Prisma Access utilise l'adresse **EBGP Router (Routeur EBGP)** de la connexion aux services (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **EBGP Router (Routeur EBGP)**) comme adresse IP source, même après la sortie du trafic de la connexion aux services dédiée.
5. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.



8. Transférez le trafic vers la cible de connexion aux services spécifiée, ou envoyez le trafic directement vers Internet sans passer par la connexion aux services.
   - Pour que Prisma Access transfère le trafic vers une cible de connexion aux services, sélectionnez **Forward to the target (Transférer vers la cible)**, puis sélectionnez le **Target Service Connection Group (Groupe cible de connexions aux services)**.

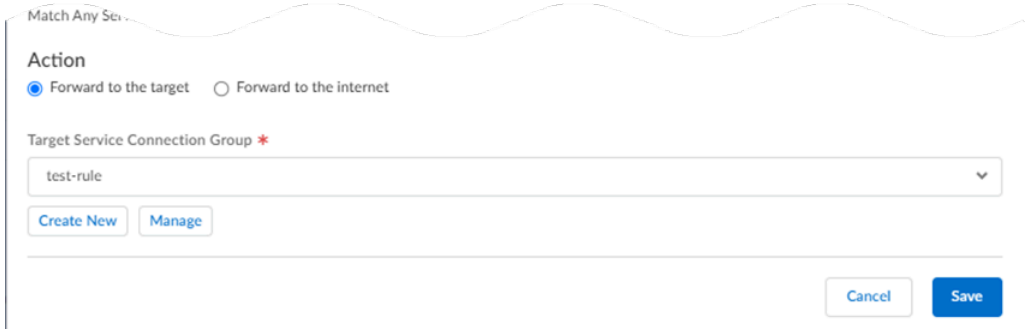
     Spécifiez ce choix si vous devez envoyer du trafic à votre environnement existant ou hérité en raison des limitations de la liste d'autorisation des applications SaaS, ou

 ©2025 Palo Alto Networks, Inc.

si vous souhaitez créer un flux de trafic pour rediriger le trafic Internet spécifié vers votre réseau local.

- Pour que Prisma Access transfère le trafic directement vers Internet sans l'envoyer au préalable à une connexion aux services, sélectionnez **Forward to the internet (Transférer vers Internet)**.

  Spécifiez ce choix si vous envoyez un itinéraire par défaut à Prisma Access et si vous souhaitez rediriger une partie du trafic directement vers Internet.



STEP 6 | Cliquez sur **Push Config (Transmettre la configuration)** pour enregistrer vos modifications.

Configurer la redirection du trafic dans Prisma Access (Panorama)

STEP 1 | Intégrez vos connexions aux services, utilisateurs mobiles et réseaux distants, selon votre déploiement.

STEP 2 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Traffic Steering (Redirection du trafic)**.

STEP 3 | (Facultatif, déploiements pour utilisateurs mobiles uniquement) Autorisez Prisma Access à accepter et installer l'itinéraire par défaut publié sur une ou plusieurs connexions aux services à partir du CPE en cliquant sur l'icône d'engrenage pour ouvrir les paramètres et en sélectionnant **Accept Default Route over Service Connections (Accepter l'itinéraire par défaut sur les connexions aux services)**.

Les itinéraires par défaut ont des directives que vous devez suivre lorsque vous les utilisez. Par exemple, les itinéraires par défaut sont pris en charge pour les déploiements d'utilisateurs mobiles uniquement et n'ont aucun effet sur les déploiements de réseaux distants. Assurez-vous de consulter ces directives avant de mettre en œuvre des itinéraires par défaut avec la redirection du trafic.

STEP 4 | (Facultatif) Autorisez Prisma Access à envoyer le trafic de la liste de révocation de certificats (CRL) et du protocole de vérification des certificats en ligne (OCSP) directement vers Internet

 ©2025 Palo Alto Networks, Inc.

en sélectionnant **Send CRL/OCSP traffic to internet directly (Envoyer le trafic CRL/OCSP directement vers Internet)**.

Sélectionnez ce choix si vous avez un serveur OCSP ou CRP dans l'Internet public et que vous souhaitez envoyer ce trafic directement vers Internet en utilisant la zone non approuvée. Si vous ne sélectionnez pas ce choix, Prisma Access envoie ce trafic à la connexion aux services.

*Assurez-vous d'avoir mis à niveau votre déploiement Prisma Access vers une version minimale de 5.1.1 avant de sélectionner **Send CRL/OCSP traffic to internet directly (Envoyer le trafic CRL/OCSP directement vers Internet)**.*



STEP 5 | (Facultatif) Créez un groupe cible et attribuez-lui une connexion aux services.

1. Dans la zone **Target Service Connections for Traffic Steering (Connexions aux services cibles pour la redirection du trafic)**, cliquez sur **Add (Ajouter)** pour ajouter un groupe et donnez-lui un **Group Name (Nom de groupe)**.
2. Cliquez sur **Add (Ajouter)** pour ajouter une **Target (Cible)** pour le trafic, en spécifiant la **Service Connection (Connexion aux services)** à utiliser avec la cible, puis cliquez sur **OK**.

   Palo Alto Networks ne recommande pas d'utiliser plusieurs connexions aux services (dédiées ou non) dans un groupe de connexions aux services cibles qui est référencé dans une règle de redirection du trafic. En outre, une connexion aux services donnée ne peut exister que dans une seule cible et vous ne pouvez pas ajouter une seule connexion aux services à deux cibles différentes.
3. Choisissez de faire ou non des connexions aux services associées à cette cible une connexion aux services dédiée.

   - Vous pouvez utiliser une connexion aux services dédiée pour rediriger le trafic vers une pile de sécurité ou un cloud tiers qui n'est pas dans vos locaux et n'a pas besoin de participer au routage. Pour définir une connexion aux services à utiliser en tant que connexion aux services dédiée, sélectionnez **Dedicated for Traffic Steering Only (Dédiée à la redirection du trafic uniquement)**.

     Les connexions aux services dédiées changent de zone.

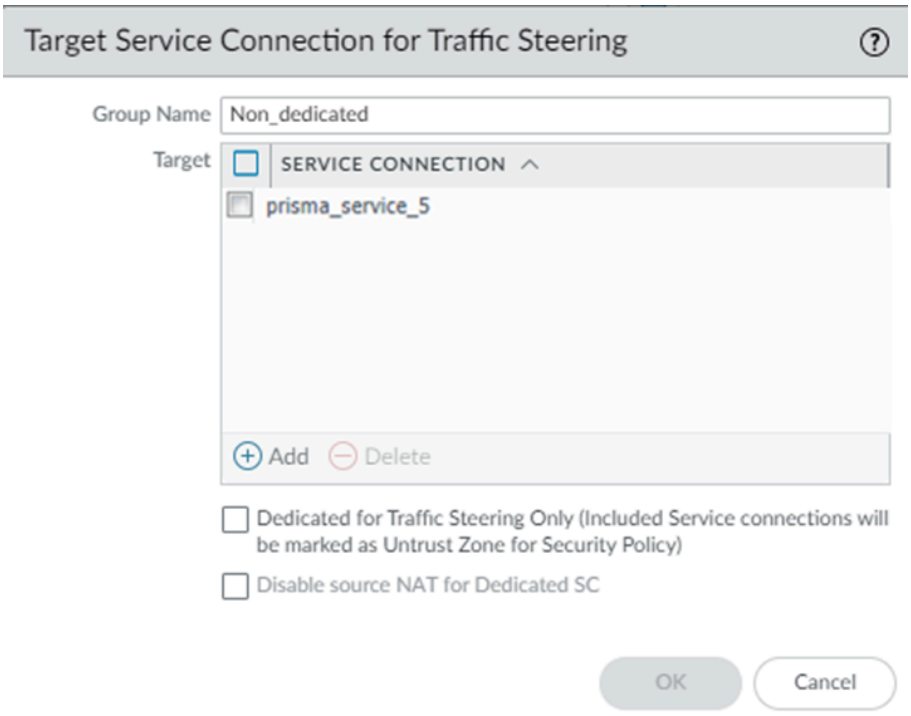
   - Désélectionnez **Dedicated for Traffic Steering Only (Dédiée à la redirection du trafic uniquement)** si vous envoyez à la fois du trafic normal lié à la connexion aux services et du trafic de redirection du trafic via la connexion aux services. Avec ce choix, la zone pour la connexion aux services reste comme approuvée.

 ©2025 Palo Alto Networks, Inc.

4. Choisissez d'activer ou de désactiver la NAT source.

   Pour désactiver la NAT source pour les connexions aux services dédiées, sélectionnez **Disable Source NAT for Dedicated SC (Désactiver la NAT source pour le SC dédié)**. La NAT source est activée par défaut (la case est décochée).

   Si vous désactivez la NAT source, Prisma Access utilise les adresses IP source de votre organisation pour la connexion aux services dédié. Si vous activez la NAT source, Prisma Access utilise l'adresse **EBGP Router (Routeur EBGP)** de la connexion aux services (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **EBGP Router (Routeur EBGP)**) comme adresse IP source, même après la sortie du trafic de la connexion aux services dédiée.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | Créez des règles pour la cible que vous avez créée et appliquez-les à la cible.

1. Dans la zone **Traffic Steering Rules (Règles de redirection du trafic)**, cliquez sur **Add (Ajouter)** pour ajouter une règle de redirection du trafic.
2. Dans l'onglet **General (Général)**, cliquez sur **Name (Nommer)** pour nommer la règle de redirection du trafic.
3. Dans l'onglet **Source**, spécifiez des règles pour le trafic source.
   - Dans le champ **Source Address (Adresse source)**, spécifiez un ou plusieurs des objets suivants, ou sélectionnez **All (Tout)** pour que le trafic de toute source se dirige vers cette cible :
     - Une adresse IP
     - Un objet d'adresse que vous avez créé dans Panorama (**Objects (Objets)** > **Addresses (Adresses)**)
     - Un Dynamic Address Group (groupe d'adresses dynamiques, DAG)
     - Une liste dynamique externe (EDL) utilisant des adresses IP ou URL
   - Dans le champ **Source User (Utilisateur source)**, spécifiez des règles pour le trafic utilisateur source. Vous pouvez spécifier les informations utilisateur suivantes :
     - Utilisateurs

       Entrez les utilisateurs dans le format *domaine/utilisateur* ou *utilisateur@domaine*.
     - Groupes d'utilisateurs

       Utilisez des noms uniques (DN) complets lorsque vous entrez des groupes d'utilisateurs.
     - Utilisateurs configurés sur Panorama (**Device (Périphérique)** > **Local User Database (Base de données locale d'utilisateurs)** > **Users (Utilisateurs)**)
     - Groupes d'utilisateurs configurés sur Panorama (**Device (Périphérique)** > **Local User Database (Base de données locale d'utilisateurs)** > **User Groups (Groupes d'utilisateurs)**)

   Si vous utilisez des objets d'adresse, des DAG, des EDL, des utilisateurs ou des groupes d'utilisateurs, spécifiez-les comme **Shared (Partagés)** pour les partager avec tous les

 ©2025 Palo Alto Networks, Inc.

groupes de périphériques dans Prisma Access. En outre, n'entrez pas 0.0.0.0/0 dans les objets d'adresse, les DAG ou les EDL ; entrez plutôt 0.0.0.0/0 directement dans la règle.

Prisma Access remplit automatiquement les utilisateurs du groupe de périphériques des utilisateurs mobiles uniquement.

4. Dans l'onglet **Destination**, spécifiez les valeurs suivantes :

   - Dans la zone **Destination**, spécifiez l'un des critères suivants ou sélectionnez **All (Tout)** pour que le trafic soit traité selon les règles dans le champ **URL Category (Catégorie URL)** :
     - Une adresse IP ou un préfixe
     - Un objet d'adresse que vous avez créé dans Panorama (**Objects (Objets)** > **Addresses (Adresses)**)
     - Un Dynamic Address Group (groupe d'adresses dynamiques, DAG)
     - Une liste dynamique externe (EDL) basée sur l'adresse IP

     N'entrez pas 0.0.0.0/0 dans les objets d'adresse, les DAG ou les EDL ; entrez plutôt 0.0.0.0/0 directement dans la règle.

     Laissez **Any (Indifférent)** sélectionné pour passer tout le trafic à traiter par les règles dans la zone **URL Category (Catégorie URL)**. Si vous spécifiez des règles dans les zones **Destination** et **URL Category (Catégorie d'URL)**, Prisma Access traite d'abord les règles de la catégorie **Destination**.
   - Dans le champ **URL Category (Catégorie d'URL)**, saisissez une catégorie d'URL personnalisée (**Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)**) Lorsque vous créez une catégorie d'URL personnalisée, saisissez les URL en minuscules. La redirection du trafic prend en charge les URL personnalisées et les catégories d'URL prédéfinies.

     Vous pouvez utiliser des caractères génériques avec les URL dans les catégories d'URL. Les formats de caractères génériques suivants sont pris en charge :
     - *.exemple.com

 ©2025 Palo Alto Networks, Inc.

- *.fqdn.exemple.com

Les formats suivants ne sont pas pris en charge :

- *
- *.*
- *exemple.com
- exemple.com/ (les barres obliques de fin dans les URL ne sont pas prises en charge dans les catégories d'URL utilisées avec la redirection du trafic)
- exemple.com/*path* (seuls les noms de domaine sont pris en charge)
- *fqdn.exemple.com
- fqdn.exemple.*

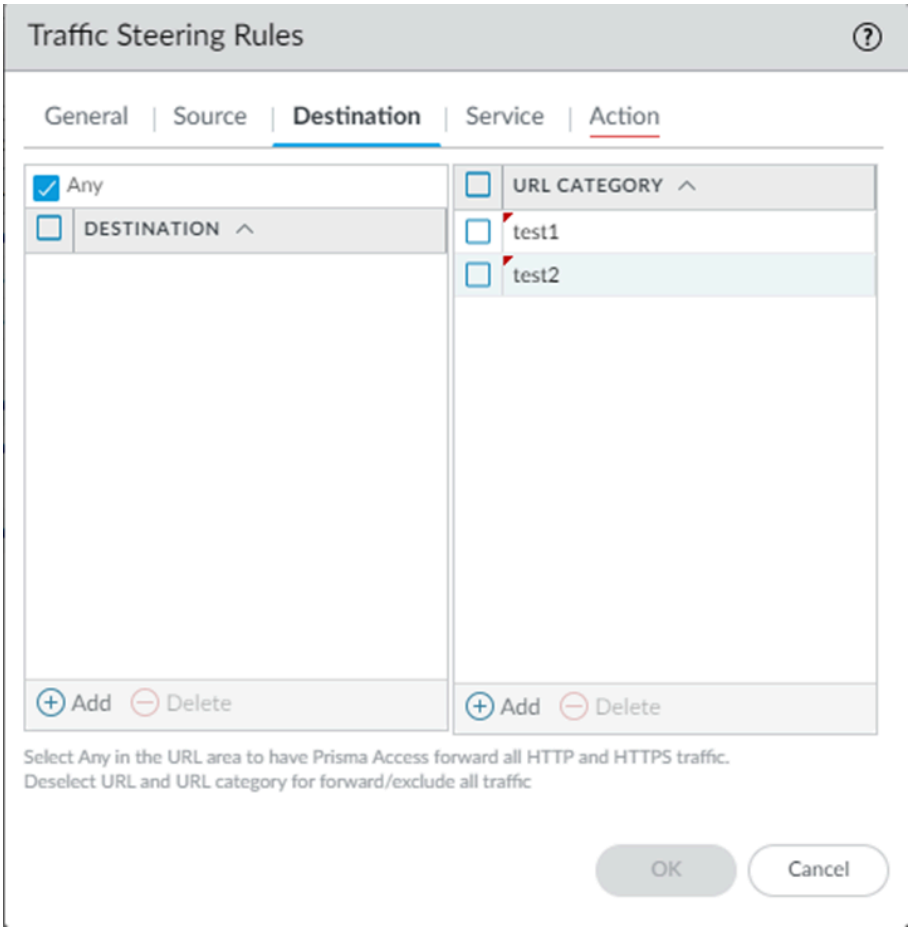
Les URL des catégories d'URL personnalisées utilisent la même correspondance de modèles d'URL que celle utilisée par les pare-feu nouvelle génération.

Utilisez les directives suivantes lors de la configuration des options de destination :

- Si vous spécifiez une catégorie d'URL, Prisma Access correspond uniquement au trafic HTTP et HTTPS, même lorsque le service est défini sur Any (Indifférent).
- Ne créez pas de catégorie d'URL personnalisée avec un type de **Category Match (Correspondance de catégorie)**.
- Ne créez pas de catégorie d'URL personnalisée avec le nom **Custom_URL_Category_TFR**, car, pour les déploiements qui sont migrés de Prisma Access 1.7 vers 2.0, les URL saisies dans la zone URL de la version 1.7 sont déplacées

 ©2025 Palo Alto Networks, Inc.

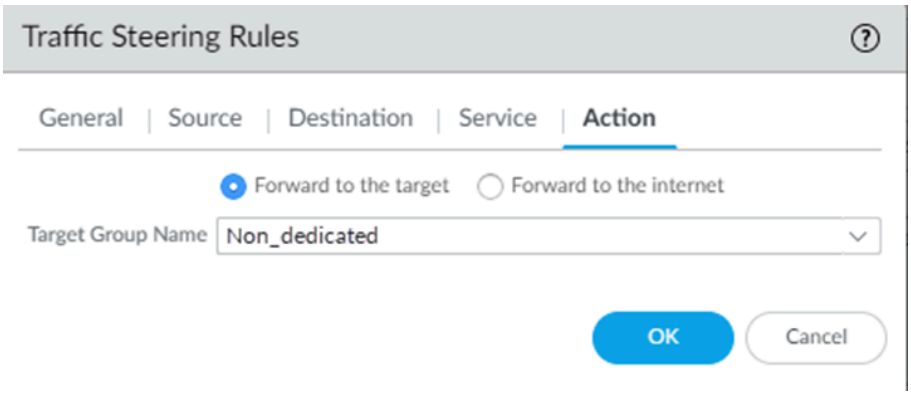
vers une catégorie d'URL personnalisée nommée **Custom_URL_Category_TFR***number*, où *number* est un nombre ajouté à la catégorie d'URL personnalisée.



5. Dans l'onglet **Service**, spécifiez un type de service.

   Spécifiez **service-http** pour transférer le trafic HTTP et spécifiez **service-https** pour spécifier le trafic HTTPS. Sélectionnez **Any (Indifférent)** pour transférer le trafic de tout type de service.
6. Dans l'onglet **Action**, sélectionnez le **Target Group Name (Nom du groupe cible)** que vous souhaitez appliquer à la règle de redirection du trafic.
7. Transférez le trafic vers la cible de connexion aux services spécifiée, ou envoyez le trafic directement vers Internet sans passer par la connexion aux services.
   - Pour que Prisma Access transfère le trafic vers une cible de connexion aux services, sélectionnez **Forward to the target (Transférer vers la cible)**, puis sélectionnez le **Target Group Name (Nom du groupe cible)**.
   - Pour que Prisma Access transfère le trafic directement vers Internet sans l'envoyer au préalable à une connexion aux services, sélectionnez **Forward to the internet (Transférer vers Internet)**.

 ©2025 Palo Alto Networks, Inc.



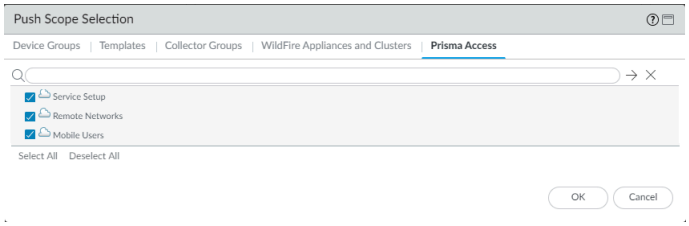
8. Cliquez sur **OK** pour enregistrer vos modifications.

STEP 7 | Facultatif Spécifiez des règles supplémentaires de redirection du trafic.

Prisma Access traite plusieurs règles dans l'ordre où vous les créez (de haut en bas).

STEP 8 | Validez et appliquez vos modifications pour les rendre actives dans Prisma Access.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
2. Sélectionnez **Prisma Access**, puis **Service Setup (Configuration du service)**, **Remote Networks (Réseaux distants)** et **Mobile Users (Utilisateurs mobiles)**.



3. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.
4. Cliquez sur **Commit (Valider)** et **Push (Appliquer)** pour valider et appliquer vos modifications.

Routage pour le trafic de connexion aux services

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Prisma Access utilise BGP pour le routage dynamique et utilise la sélection de chemin BGP pour installer des itinéraires dans la table de routage. Quand Prisma Access achemine le trafic vers votre siège social ou votre centre de données à l'aide de connexions aux services, il utilise des méthodes de routage qui dirigent ce trafic efficacement. Prisma Access utilise un modèle de routage par défaut conçu pour s'adapter à la majorité des déploiements réseau ; cependant, tous les réseaux des organisations ne sont pas identiques. Pour s'adapter à une plus large gamme

 ©2025 Palo Alto Networks, Inc.

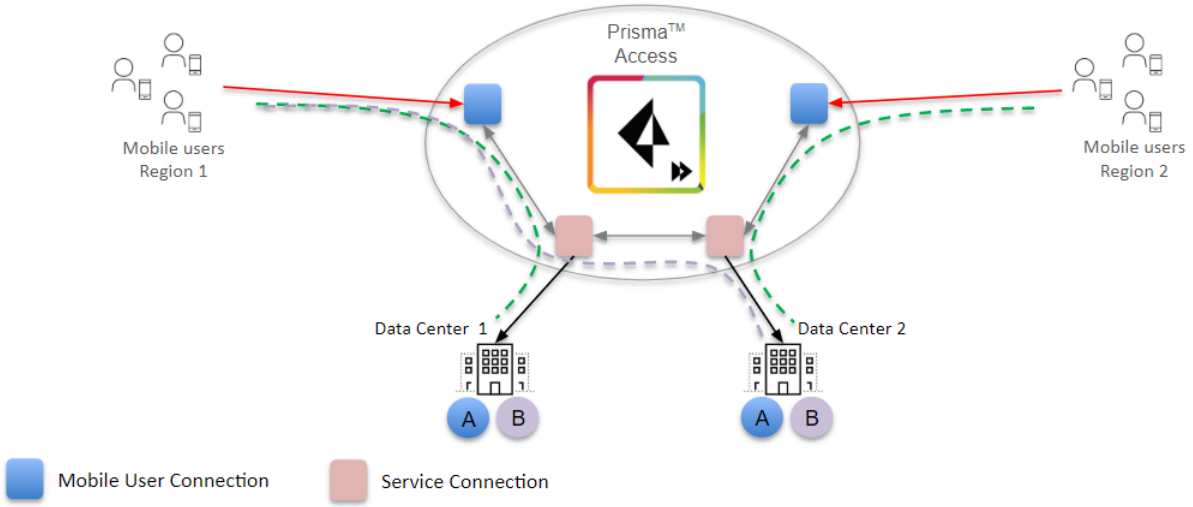
de déploiements, Prisma Access vous permet de choisir un autre mode pour le routage de la connexion aux services.

Changer la méthode de routage de connexion aux services Prisma Access nécessite une compréhension approfondie de la topologie et des périphériques de routage de votre organisation, ainsi qu'une compréhension de la manière dont Prisma Access fonctionne comme décrit dans cette section. Lisez attentivement cette section avant de modifier la méthode de routage par défaut.

Prisma Access prend en charge le routage statique et le routage dynamique à l'aide de BGP pour les connexions aux services et les connexions réseau distantes. Lorsque vous utilisez le routage BGP pour vos connexions, le réseau de votre organisation apprend les informations BGP à partir de Prisma Access.

Avant de décider quel routage de connexion aux services utiliser, vous devez comprendre comment Prisma Access achemine le trafic entre les utilisateurs mobiles, les réseaux distants et les connexions aux services, car le routage utilisé par le trafic des utilisateurs mobiles et le trafic du réseau distant entre les connexions aux services est différent.

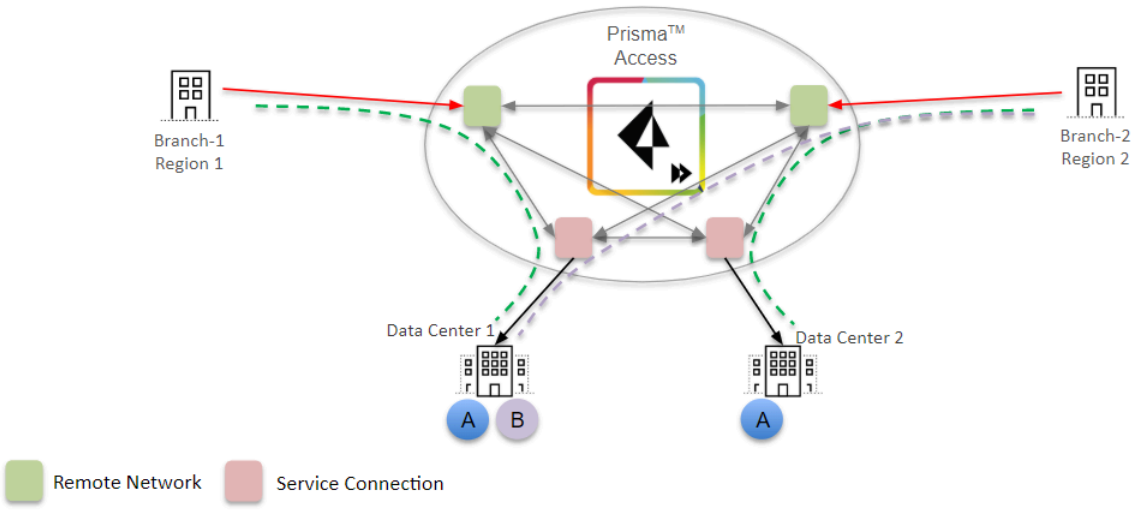
Routage de connexion aux services utilisateur mobile—La connexion utilisateur mobile forme un tunnel IPSec avec la connexion aux services la plus proche. Prisma Access utilise iBGP pour le routage interne et eBGP pour établir un peering avec l'équipement local du client au centre de données. Dans le diagramme suivant, les utilisateurs mobiles des régions 1 et 2 sont acheminés vers les connexions aux services respectives dans leur région. Les utilisateurs mobiles de la région 1 accèdent aux applications **A** et **B** situées dans le centre de données 1. Si le réseau de votre organisation utilise le routage BGP pour les connexions aux services et qu'une de ces connexions rencontre un échec avec l'ISP au centre de données 1, Prisma Access détecte l'échec et achemine le trafic des applications **A** et **B** vers le centre de données 2 après la convergence BGP, assurant ainsi la redondance des centres de données de votre réseau.



 ©2025 Palo Alto Networks, Inc.

Prisma Access utilise le minutage suivant avec le BGP lorsqu'il détecte un échec : Si vous configurez le routage BGP et que vous avez activé la surveillance des tunnels, le temps d'attente par défaut le plus court pour déterminer qu'un index de paramètres de sécurité (SPI) est défaillant est le moniteur de tunnel, qui supprime toutes les routes vers un homologue lorsqu'il détecte une défaillance de tunnel pendant 15 secondes consécutives. De cette façon, le moniteur de tunnel détermine le comportement des routes BGP. Si vous ne configurez pas la surveillance des tunnels, la minuterie d'attente détermine la durée d'arrêt du tunnel avant la suppression de l'itinéraire. Prisma Access utilise la valeur d'attente BGP par défaut de 90 secondes qui a été définie dans la RFC 4271. Il s'agit du temps d'attente maximal avant que Prisma Access ne supprime un itinéraire pour un SPI inactif. Si le périphérique BGP homologue a un temps d'attente configuré plus court, le minuteur de maintien BGP utilise la valeur inférieure. Lorsque le tunnel secondaire est installé avec succès, l'itinéraire secondaire a priorité jusqu'à ce que le tunnel primaire refonctionne. Si l'itinéraire principal et l'itinéraire secondaire sont tous deux opérationnels, l'itinéraire principal est prioritaire.

Routage entre réseau distant et connexion aux services : Prisma Access crée un réseau maillé complet avec d'autres réseaux distants et connexions aux services. Comme pour les utilisateurs mobiles, Prisma Access utilise l'iBGP pour le routage interne et l'eBGP pour l'appairage avec l'équipement des locaux d'abonné afin d'échanger des itinéraires. Si un utilisateur de la succursale 1 accède à l'application **A** à partir du centre de données 1 dans le centre de données de votre organisation et que le lien entre la succursale 1 et le centre de données 1 tombe en panne, Prisma Access achemine le trafic de l'application **A** vers le centre de données 2 après la convergence BGP.



Lorsque vous avez compris le routage de la connexion aux services Prisma Access et sa relation avec votre réseau, vous pouvez choisir l'un des modes de routage suivants pour les connexions aux services :

- Routage par défaut—il s'agit du modèle de routage par défaut que Prisma Access utilise.

  Utilisez ce mode de routage si vous souhaitez que Prisma Access utilise les meilleurs mécanismes de sélection de chemin BGP sans ajuster aucun des attributs BGP. Dans ce mode, Prisma Access honorera tout attribut annoncé par l'équipement local du client (CPE).

 ©2025 Palo Alto Networks, Inc.

- Routage Hot Potato—Prisma Access transmet le trafic aussi rapidement que possible au réseau de votre organisation.

  Utilisez cette méthode de routage si vous souhaitez que le réseau de votre organisation effectue la majorité des décisions de routage.

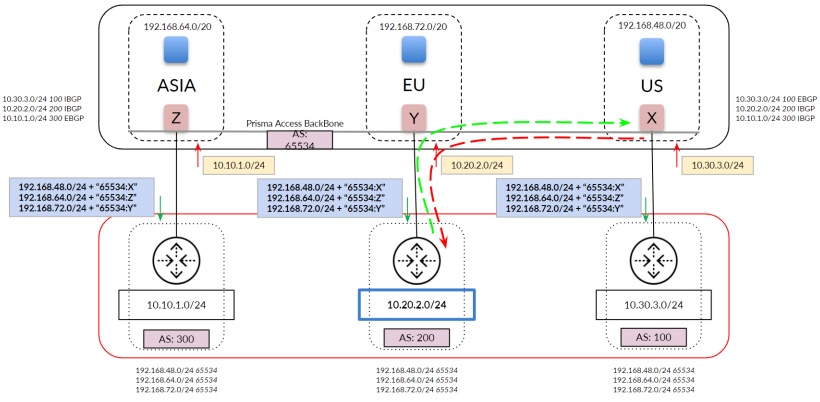
Prisma Access Routage par défaut

La figure suivante montre un exemple de routage Prisma Access du trafic de connexion aux services en mode de routage par défaut. Le réseau de l'organisation dispose de trois réseaux distincts dans trois centres de données et ne dispose pas d'une dorsale reliant les réseaux. En mode de routage par défaut, les pools d'utilisateurs mobiles sont annoncés de manière égale sur les trois réseaux, comme indiqué au bas de la figure.

Notez que, lorsque Prisma Access annonce les itinéraires des utilisateurs mobiles, il divise les sous-réseaux en blocs d'adresses de classe C /24 avant de les annoncer ; ainsi, il annonce les sous-réseaux utilisateurs mobiles /20 en morceaux de /24 au fur et à mesure que les préfixes sont consommés par les passerelles.

Prenez note de la façon dont Prisma Access utilise les annonces d'itinéraire BGP :

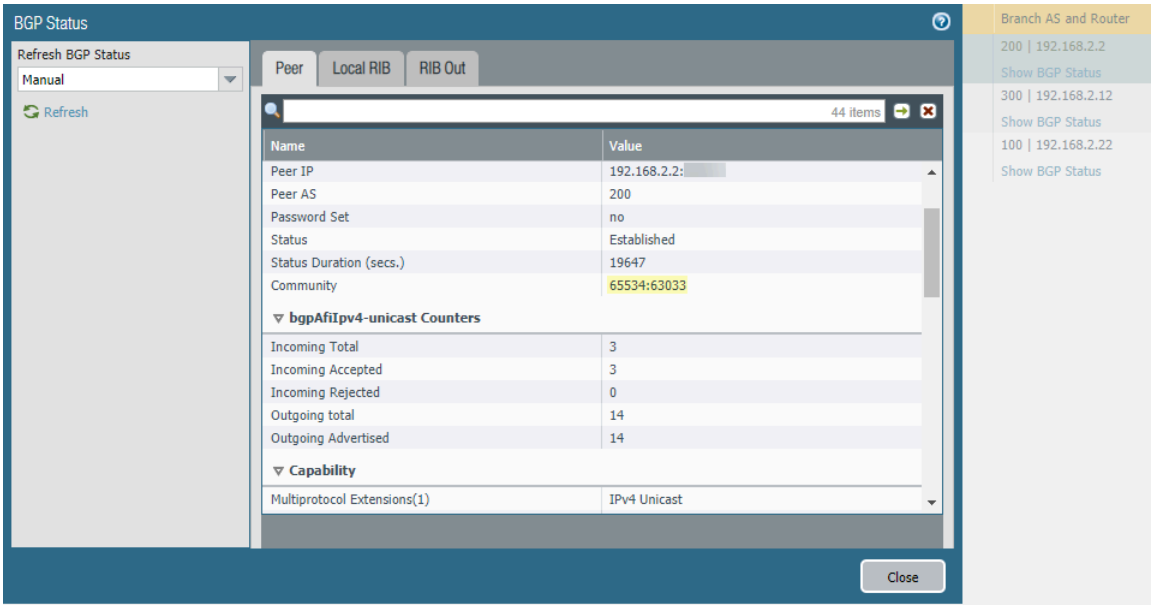
- Prisma Access n'ajuste pas les attributs BGP par défaut pour les itinéraires annoncés par les utilisateurs mobiles (Prisma Access ajoute son numéro AS aux annonces d'itinéraire).
- Prisma Access annonce les itinéraires des utilisateurs mobiles dans des blocs de /24 sous-réseaux et ajoute des valeurs de communauté BGP dans les itinéraires qu'il annonce via la connexion aux services. La figure suivante montre un déploiement d'utilisateur mobile avec trois connexions aux services et trois blocs d'adresses IP différents spécifiés pour le pool d'adresses IP d'utilisateur mobile : `192.168.64.0/20` pour la région **Asia, Australia & Japan (Asie, Australie et Japon)**, `192.168.72.0/20` pour la région **Africa, Europe & Middle East (Afrique, Europe et Moyen-Orient)** et `192.168.48.0/20` pour la région **North America & South America (Amérique du Nord et Amérique du Sud)**. Prisma Access divise ces itinéraires en blocs de /24 et les annonce avec un numéro AS de **65534**, mais ajoute également les valeurs de la communauté BGP aux annonces (**Z** pour l'Asie, **Y** pour l'UE et **X** pour les États-Unis). Ces itinéraires sont indiqués au milieu de la figure. De cette façon, vous pouvez différencier les connexions aux services dans votre réseau, même si Prisma Access leur attribue le même numéro AS.



Vous pouvez afficher la chaîne de communauté en sélectionnant **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails réseau)** > **Service Connection (Connexion aux services)**

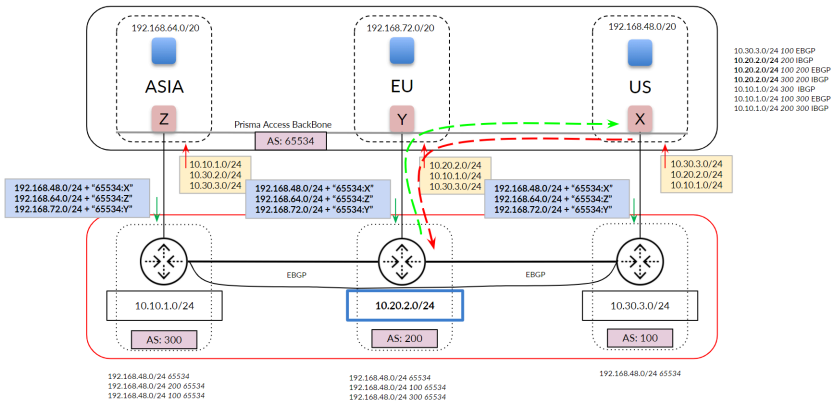
 ©2025 Palo Alto Networks, Inc.

> **Show BGP Status (Afficher le statut BGP)** et recherchez le champ **Community (Communauté)** dans l'onglet **Peer (Pair)**.



La figure suivante montre un réseau plus courant avec une dorsale eBGP entièrement maillée. La figure montre les itinéraires que Prisma Access a appris du réseau de votre organisation en haut à droite. Notez les itinéraires supplémentaires que Prisma Access a appris via le Prisma Access backbone (iBGP) et le backbone de votre organisation (eBGP).

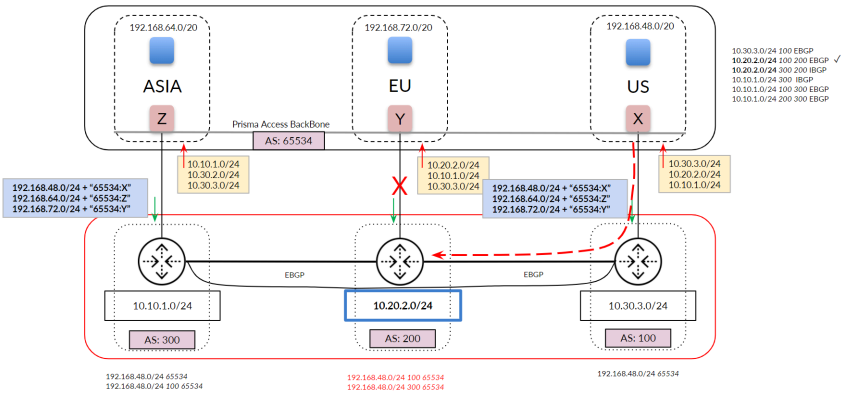
Pour le trafic entre les utilisateurs mobiles de la région **North America & South America (Amérique du Nord et Amérique du Sud)** (États-Unis dans le diagramme) et le centre de données de la région **Africa, Europe & Middle East (Afrique, Europe et Moyen-Orient)** de votre organisation (UE dans le diagramme), Prisma Access choisit le chemin via la connexion aux services de l'UE car il préfère les itinéraires avec un itinéraire AS-PATH plus court.



Dans les déploiements avec un backbone eBGP entièrement maillé, une asymétrie peut survenir lorsque Prisma Access ne peut pas atteindre un centre de données particulier en raison d'une défaillance ISP/CPE au centre de données du client. La figure suivante montre ce qui pourrait se produire en cas de coupure du lien vers la connexion aux services de l'UE. Votre réseau détecte la défaillance de la liaison et crée une nouvelle table d'itinéraire pour AS 200. Le trafic de la connexion aux services américaine vers AS 200 utilise le chemin via AS 100 car l'itinéraire eBGP pour votre backbone entre AS 200 et AS 100 est préférée à l'itinéraire iBGP entre les connexions

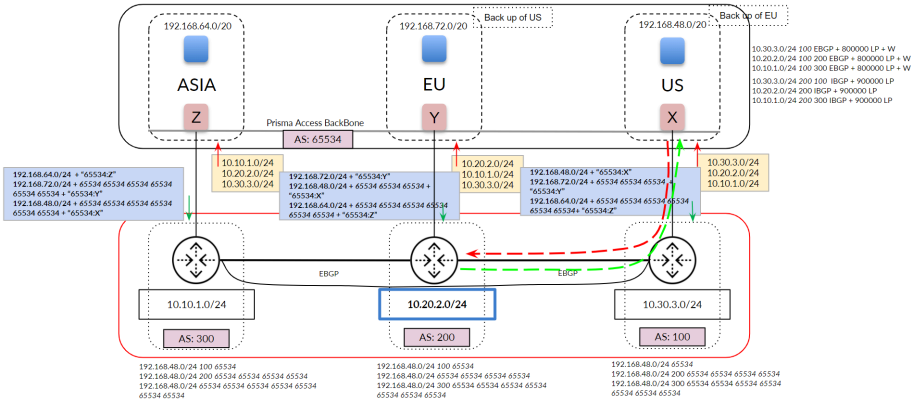
 ©2025 Palo Alto Networks, Inc.

aux services UE et États-Unis. Cependant, le trafic de retour n'est pas garanti via le même chemin, car le CPE local peut choisir l'un ou l'autre chemin (affiché en rouge) pour renvoyer le trafic.



Les exemples précédents montrent un réseau dont les itinéraires n'ont pas été agrégés (c'est-à-dire que vous n'avez pas effectué de résumé de route avant d'envoyer les annonces d'itinéraire BGP à Prisma Access). L'exemple suivant montre un réseau qui résume ses itinéraires vers 10.0.0.0/8 avant de les envoyer à Prisma Access. Si vous sélectionnez le routage par défaut, cette configuration peut entraîner des problèmes de routage asymétrique, car Prisma Access ne peut pas déterminer le chemin de retour correct à partir des itinéraires résumés.

Si votre déploiement Prisma Access possède des réseaux distants, Palo Alto Networks ne recommande pas l'utilisation du résumé d'itinéraire sur les connexions aux services. Le résumé d'itinéraire sur les connexions aux services est destiné uniquement aux déploiements d'utilisateurs mobiles.



Si vous utilisez l'agrégation d'itinéraires pour les utilisateurs mobiles, nous vous recommandons vivement d'activer le routage hot potato au lieu du routage par défaut, où Prisma Access transfère le trafic le plus rapidement possible vers le réseau de votre organisation ; en outre, nous vous recommandons de sélectionner un **Backup SC (SC de sauvegarde)** comme décrit dans la section suivante pour chaque connexion aux services afin d'avoir un comportement de routage déterministe.

Prisma Access Routage hot potato

Lorsque vous sélectionnez **Hot Potato Routing (Routage Hot Potato)**, Prisma Access fait sortir le trafic lié aux connexions aux services/centres de données de son réseau interne le plus rapidement possible.

 ©2025 Palo Alto Networks, Inc.

Avec un routage hot potato, Prisma Access ajoute le chemin AS (AS-PATH) au préfixe BGP des annonces envoyées depuis les passerelles. Cet ajout est effectué lorsque les préfixes sont annoncés en dehors de la connexion aux services au CPE sur site de votre organisation. Prisma Access ajoute les AS-PATH afin que votre CPE donne la bonne préférence aux tunnels principal et secondaire, de sorte que si le tunnel principal tombe en panne, votre CPE choisit le tunnel secondaire comme tunnel de secours.

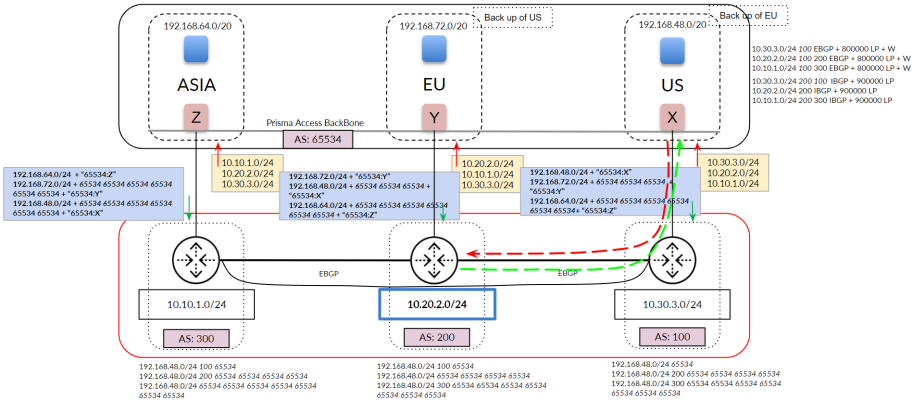
Si vous avez spécifié une adresse IP différente pour l'homologue BGP secondaire (de secours), Prisma Access ajoute plus de préfixes en fonction du type de tunnel, comme indiqué dans le tableau suivant.

Type de préfixe	Type de tunnel de connexion aux services	Nombre de préfixes As-Path	Nombre total d'AS-PATH observés sur le CPE
Préfixes de passerelle de la connexion aux services principale	Tunnel principal ou secondaire avec la même adresse IP de l'homologue BGP	0	1
Préfixes de passerelle de la connexion aux services de secours	Tunnel principal ou secondaire avec la même adresse IP de l'homologue BGP	3	4
Préfixes de passerelle de toutes les autres connexions aux services	Tunnel principal ou secondaire avec la même adresse IP de l'homologue BGP	6	7
Préfixes de passerelle de la connexion aux services principale	Tunnel secondaire avec une adresse IP de l'homologue BGP différente	1	2
Préfixes de passerelle de la connexion aux services de secours	Tunnel secondaire avec une adresse IP de l'homologue BGP différente	4	5
Préfixes de passerelle de toutes les autres connexions aux services	Tunnel secondaire avec une adresse IP de l'homologue BGP différente	7	8

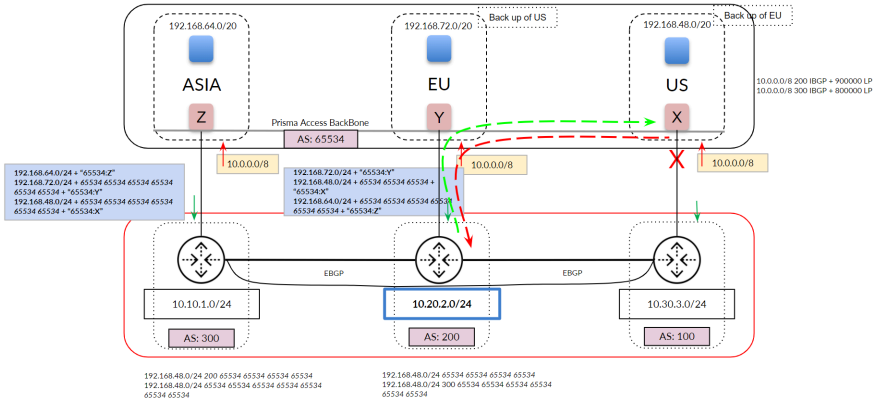
En mode de routage hot potato, Prisma Access vous permet de spécifier une connexion aux services de secours lors de l'intégration. La spécification d'une **Backup SC (SC de secours)** informe Prisma Access qu'il doit utiliser cette connexion aux services comme connexion de secours en cas de défaillance d'une liaison de connexion aux services.

 ©2025 Palo Alto Networks, Inc.

La figure suivante illustre une configuration de routage hot potato pour le trafic entre la connexion aux services US et AS 200, avec la connexion aux services de l'UE configurée comme **Backup SC (SC de secours)** de la connexion US. En utilisant le routage hot potato, Prisma Access envoie le trafic depuis son chemin de sortie le plus proche via la connexion aux services US. Le trafic de retour emprunte le même chemin via AS100, car ce chemin possède un AS-PATH plus court vers le pool d'utilisateurs mobiles aux États-Unis. Prisma Access ajoute l'AS-PATH à ses annonces de préfixe selon que le tunnel est un tunnel principal, un tunnel de secours ou qu'il n'est pas utilisé pour le tunnel principal ou de secours.

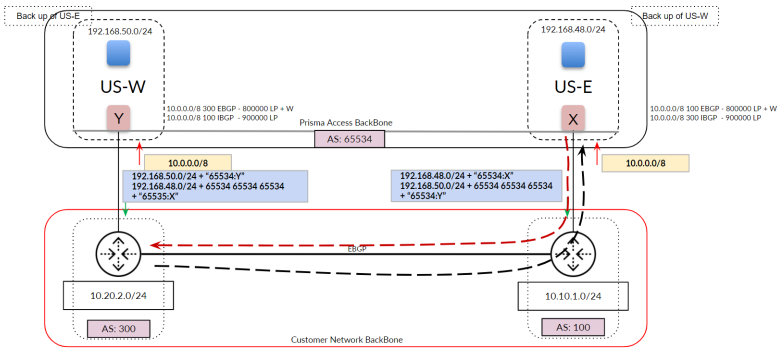


Étant donné que vous avez configuré une connexion aux services de secours, si le lien vers la connexion aux services US tombe en panne, le routage hot potato envoie le trafic en utilisant son itinéraire le plus court via la connexion aux services de l'UE. Ce scénario de routage s'applique également aux réseaux qui utilisent l'agrégation d'itinéraires.



Vous pouvez également utiliser des connexions aux services de secours pour plusieurs connexions aux services dans une seule région. La figure suivante montre un déploiement Prisma Access avec deux connexions aux services dans la région Amérique du Nord. Dans ce cas, vous spécifiez une **Backup SC (SC de secours)** US-E pour la connexion aux services US-W, et vice versa, pour garantir un routage symétrique.

 ©2025 Palo Alto Networks, Inc.



Configurer les préférences de routage

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

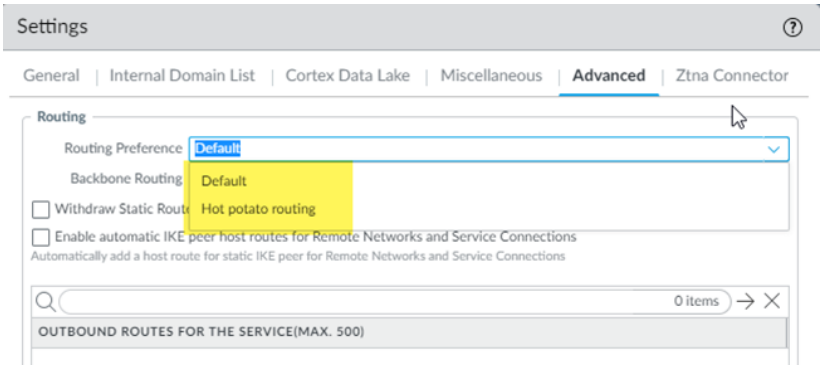
Pour activer les préférences de routage, procédez comme suit.

Pour configurer ces préférences de routage, vous devez utiliser le routage BGP et non le routage statique pour vos connexions aux services.

STEP 1 | Configurez votre connexion aux services.

STEP 2 | (Facultatif) Sélectionnez l'itinéraire à utiliser pour vos connexions aux services.

1. À partir du Panorama qui gère Prisma Access, accédez à **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** et cliquez sur l'engrenage pour modifier les **Settings (Paramètres)**.
2. Dans les paramètres **Advanced (Avancé)**, sélectionnez votre **Routing Preference (Préférence de routage)** (**Default (Par défaut)** ou **Hot potato**).



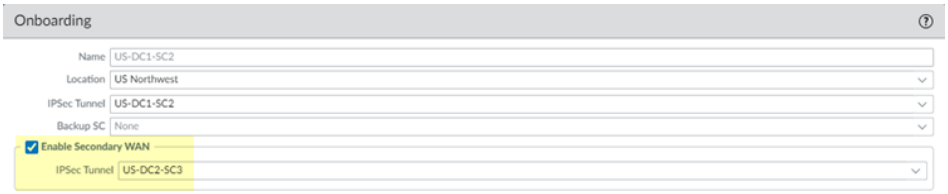
STEP 3 | (Facultatif, déploiements de routage hot potato uniquement) Pour spécifier une connexion aux services préférée à utiliser en cas de défaillance d'un lien, configurez un **Backup SC (SC de secours)** lorsque vous configurez une connexion aux services.

Vous pouvez sélectionner n'importe quelle connexion de service que vous avez déjà ajoutée. Prisma Access utilise le **Backup SC** que vous sélectionnez comme connexion de service préférée en cas d'échec de liaison. La sélection d'une connexion aux services de secours peut

 ©2025 Palo Alto Networks, Inc.

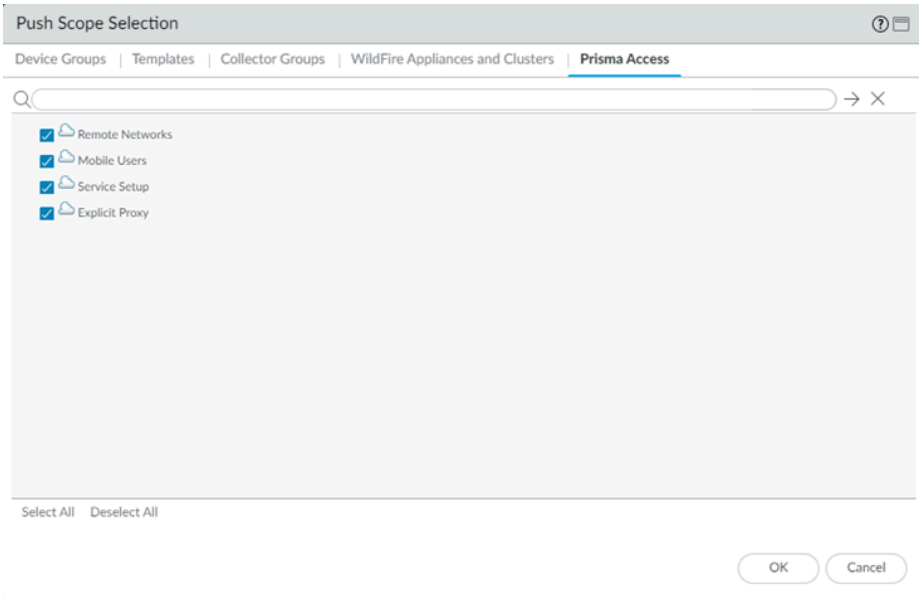
éviter les problèmes de routage asymétrique si vous avez intégré plus de deux connexions aux services. Ce choix est disponible en mode de routage hot potato uniquement.

1. Accédez à **Panorama** > **Cloud Service** > **Configuration** > **Service Connection (Connexion aux services)**
2. Sélectionnez la connexion aux services à configurer, ou cliquez sur **Add (Ajouter)** pour en ajouter un nouveau.
3. Sélectionnez une connexion aux services à utiliser comme sauvegarde préférée (**Backup SC (SC de secours)**).



STEP 4 | Validez vos modifications dans Panorama et transmettez les modifications de configuration à Prisma Access.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**.
2. Cliquez sur **Edit Selections (Modifier les sélections)** et, dans l'onglet Prisma Access, assurez-vous que l'option **Service Setup (Configuration du service)** est sélectionnée dans **Push Scope (Étendue de la transmission)**, puis cliquez sur **OK**.

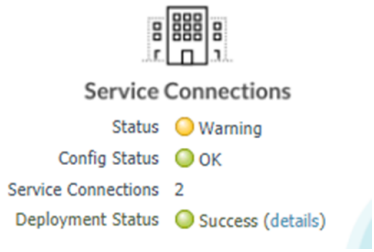


3. Cliquez sur **Commit and Push (Valider et appliquer)**.

 ©2025 Palo Alto Networks, Inc.

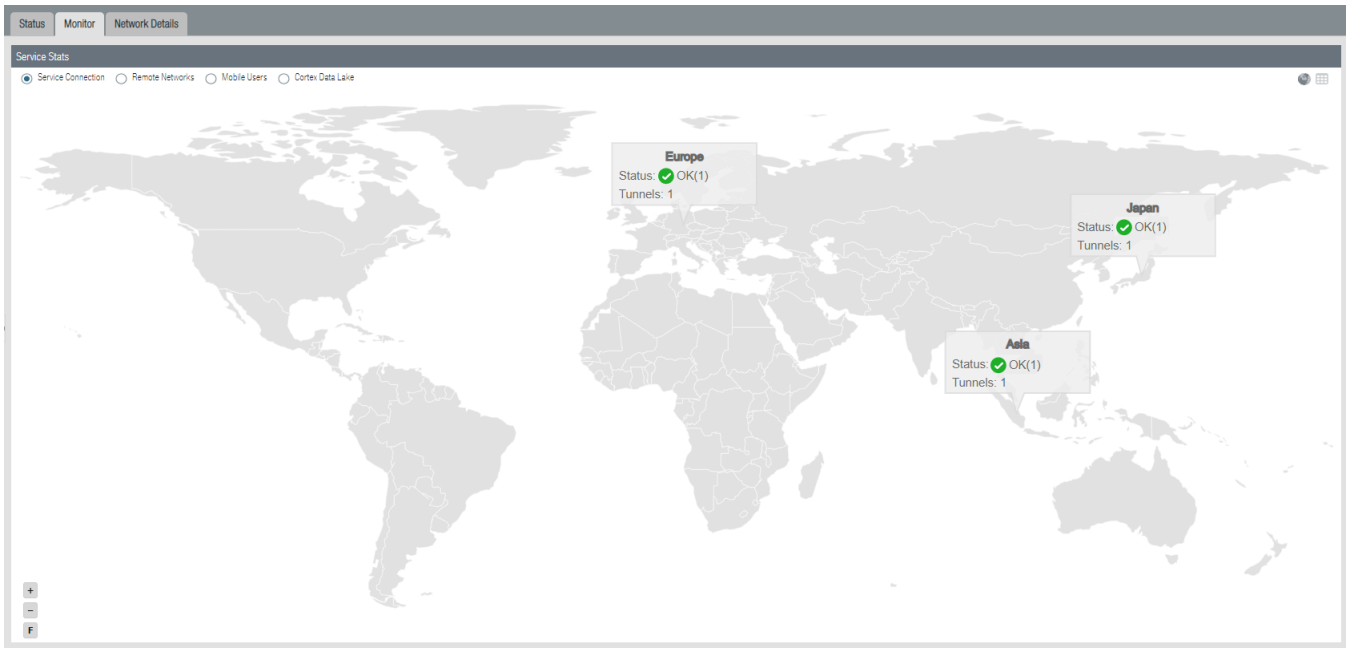
STEP 5 | Vérifiez que votre connexion aux services est active en sélectionnant **Panorama > Cloud Services > Status (État) > Status (État)** et en vérifiant que son état est **OK**.

La zone **Deployment Status (État du déploiement)** vous permet d'afficher la progression des tâches d'intégration et de déploiement avant qu'elles ne soient terminées, ainsi que de voir plus d'informations sur l'état des tâches terminées.



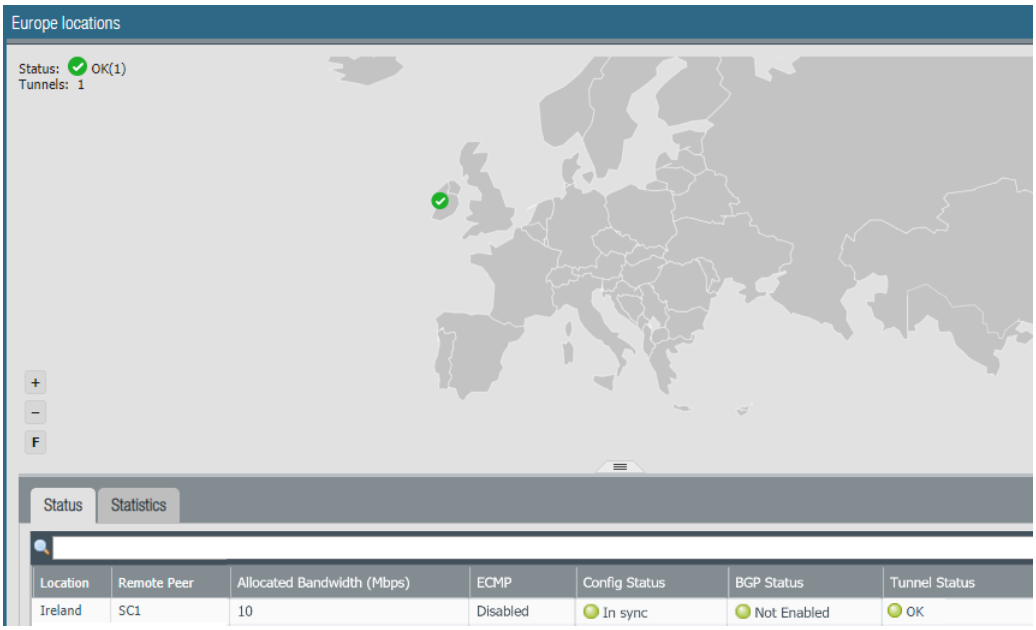
Si l'état n'est pas **OK**, passez la souris sur l'icône d'état pour afficher les erreurs.

Pour afficher une représentation graphique de la connexion aux services avec les détails de l'état, sélectionnez **Service Connection (Connexion aux services)** sur l'onglet **Monitor (Surveiller)**.



Sélectionnez une région pour obtenir plus de détails sur cette région.

 ©2025 Palo Alto Networks, Inc.



Cliquez sur les onglets sous la carte pour afficher des informations supplémentaires sur les connexions aux services.

Onglet **Statut (État)** :

- **Location (Emplacement)** : l'emplacement où votre connexion aux services est déployée.
- **Remote Peer (Homologue à distance)** : l'emplacement de l'entreprise vers laquelle cette infrastructure de service configure un tunnel IPSec.
- **Allocated Bandwidth (Bande passante allouée)** : le nombre de connexions aux services que vous avez allouées multiplié par 300 Mbit/s.

  Ce nombre ne reflète pas la bande passante de connexion aux services disponible.

  Bien que chaque connexion aux services fournisse un débit d'environ 1 Gbit/s, le débit réel dépend de plusieurs facteurs, notamment :

  - *Répartition du trafic (par exemple, taille de trame)*
  - *Latence et perte de paquets entre la connexion aux services et l'emplacement du siège social ou du centre de données*
  - *Limites de performance des fournisseurs de services*
  - *Limites de performance du périphérique de résiliation du client*
  - *Autres trafics du centre de données des clients*
- **ECMP** : si vous avez configuré le chemin d'accès multiple à coût égal (Equal Cost Multipath; ECMP) pour cette connexion aux services. Puisque l'ECMP n'est pas utilisé pour les connexions aux services, cet état est **Disabled (Désactivé)**.

 ©2025 Palo Alto Networks, Inc.

- **Config Status (État de la configuration)** : l'état de votre dernière transmission de configuration au service. Si la configuration locale et la configuration dans le cloud correspondent, l'état de la configuration est **In sync (En synchronisation)**. Si vous avez effectué une modification localement et que vous n'avez pas encore appliqué la configuration au cloud, l'état peut être affiché comme **Out of sync (Désynchronisé)**. Passez la souris sur l'indicateur d'état pour obtenir des informations plus détaillées. Après avoir validé et appliqué la configuration pour Prisma Access, l'état de configuration passe à **In sync (En synchronisation)**.
- **BGP Status (État BGP)** : affiche des informations sur l'état BGP entre le pare-feu ou le routeur à l'emplacement de votre entreprise/siège social et Prisma Access où la connexion aux services est établie. Bien que vous puissiez voir temporairement l'état passer par les différents états BGP (**Idle (Inactif)**, **Active (Actif)**, **Open send (Envoi ouvert)**, **Open pend (Attente ouverte)**, **Open confirm (Confirmation ouverte)**, le plus souvent, l'état BGP indique :
  - **Connect (Connecter)** : le routeur de votre centre de données/siège social tente d'établir la relation de l'homologue BGP avec Prisma Access.
  - **Established (Établi)** : la relation de l'homologue BGP a été établie.

  Ce champ indiquera également si la connexion BGP est dans un état d'erreur :
  - **Warning (Avertissement)** : il n'y a pas eu de mise à jour de l'état BGP depuis plus de huit minutes. Cela peut indiquer une panne du pare-feu.
  - **Error (Erreur)** : l'état BGP est inconnu.
- **Tunnel Status (État du tunnel)** : l'état de fonctionnement de la connexion entre Prisma Access et votre connexion aux services.

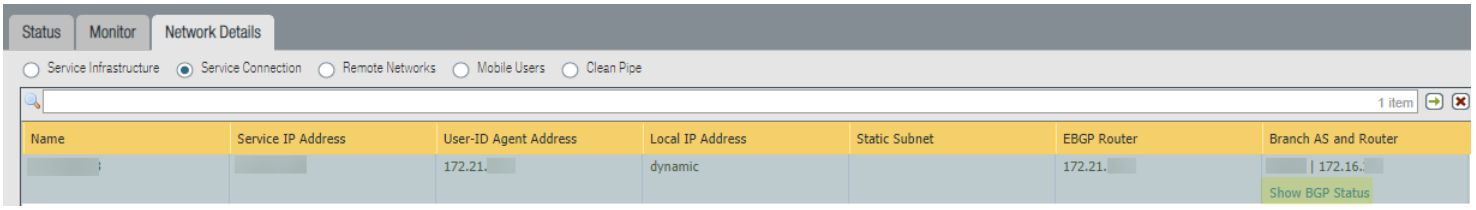
Onglet **Statistics (Statistiques)** :

- **Location (Emplacement)** : l'emplacement où votre connexion aux services est déployée.
- **Remote Peer (Homologue à distance)** : emplacement de l'entreprise auquel la connexion aux services configure un tunnel IPSec.
- **Ingress Bandwidth (Mbps) (Bande passante d'entrée (Mbit/s))** : la bande passante entre l'emplacement du siège social/du centre de données et Prisma Access.
- **Ingress Peak Bandwidth (Mbps) (Bande passante maximale d'entrée (Mbit/s))** : la charge maximale depuis l'emplacement du siège/centre de données vers le service cloud.
- **Egress Bandwidth (Mbps) (Bande passante de sortie (Mbit/s))** : la bande passante de Prisma Access dans l'emplacement du siège social/du centre de données.
- **Egress Peak Bandwidth (Mbps) (Bande passante maximale de sortie (Mbit/s))** : la charge de maximale de Prisma Access dans l'emplacement du siège social/du centre de données.
- **QoS** : sélectionnez ce bouton pour afficher un graphique qui affiche des statistiques de QoS en temps réel et historiques, y compris le nombre de paquets abandonnés par classe.

 ©2025 Palo Alto Networks, Inc.

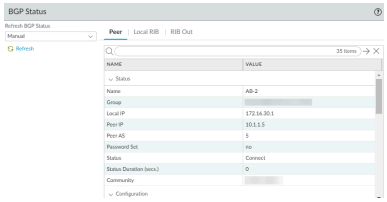
Ce graphique s'affiche uniquement pour les connexions aux services ou les connexions au réseau distant pour lesquelles la QoS est activée.

Si vous avez configuré BGP, vous pouvez vérifier son état en sélectionnant **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **Show BGP Status (Afficher l'état BGP)**.



La boîte de dialogue BGP Status (État BGP) s'affiche. Ce tableau fournit les informations suivantes :

- **Peer (Homologue)** : informations de routage pour l'homologue BGP, y compris l'état, le nombre total d'itinéraires, la configuration, les statistiques et les compteurs d'exécution. Le nombre total d'itinéraires s'affiche dans la région **bgpAfiIpv4-unicast Counters (Compteurs bgpAfiIpv4-unicast)**, dans les champs **Incoming Total (Total entrant)** et **Outgoing Total (Total sortant)**.



- **Local RIB (RIB locale)** : les itinéraires BGP que Prisma Access utilise localement. Prisma Access sélectionne ces informations dans le tableau BGP RIB-In, qui stocke les informations envoyées par les périphériques réseau voisins, applique les politiques d'importation BGP locales et les décisions de routage, et stocke les informations RIB locales dans la base d'informations de routage (Routing Information Base, RIB).

  Notez que seules les 256 premières entrées sont affichées. Pour afficher des entrées supplémentaires, entrez un sous-réseau ou une adresse IP dans le champ Filter (Filtre), puis cliquez sur Apply Filter (Appliquer le filtre) pour afficher un sous-ensemble des entrées de routage jusqu'à un maximum de 256.



- **RIB Out (Sortie de RIB)** : informations de routage que Prisma Access publie auprès de ses homologues par le biais de messages de mise à jour BGP.

Créer un réseau à large bande passante à l'aide de plusieurs connexions aux services

Si vous disposez d'un siège social ou d'un centre de données qui nécessite une bande passante de connexion aux services supplémentaire, vous pouvez configurer plusieurs connexions aux services à cet emplacement.

 ©2025 Palo Alto Networks, Inc.

Chaque connexion aux services Prisma Access n'est pas limitée à la bande passante, mais Palo Alto Networks s'attend à ce que chaque connexion aux services puisse fournir un débit d'environ 1 Gbit/s. Bien que cette bande passante soit généralement suffisante pour accéder aux ressources internes d'un siège social ou d'un centre de données, il se peut que vous ayez un déploiement qui nécessite une bande passante supplémentaire. Par exemple, si vous hébergez une application SaaS interne ou privée dans un centre de données.

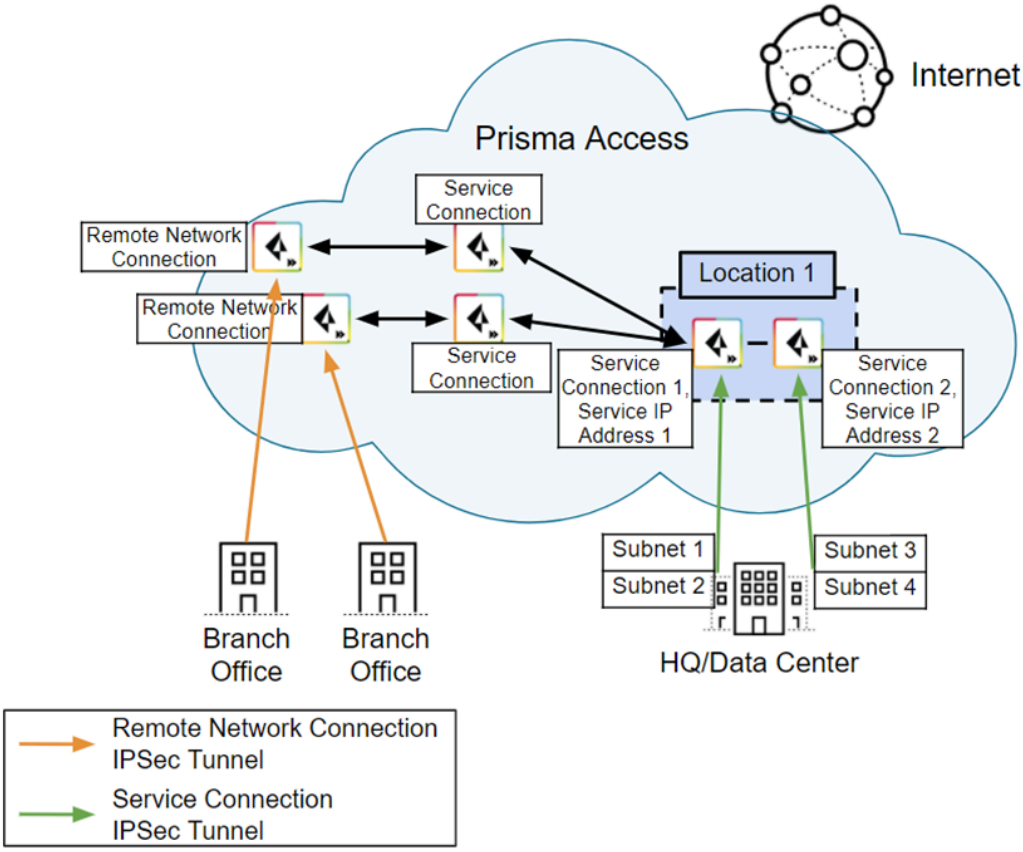
Pour créer une connexion aux services à large bande passante à un siège social ou à un site de centre de données, vous intégrez le site à l'aide de plusieurs connexions aux services au même emplacement Prisma Access.

Puisque Prisma Access ne limite pas le nombre maximal de connexions aux services que vous pouvez intégrer à un seul siège social ou à un seul emplacement de réseau distant de centre de données, Palo Alto Networks recommande de ne pas utiliser plus de quatre connexions aux services dans un déploiement à large bande passante. Si vous avez besoin de plus de bande passante pour accéder aux applications internes, utilisez le connecteur ZTNA *ou* Colo-Connect *au lieu de plusieurs connexions aux services.*

Le diagramme suivant montre un déploiement de réseau distant Prisma Access avec un siège social ou un site de centre de données disposant de deux connexions aux services à partir du même emplacement Prisma Access, fournissant effectivement 2 Gbit/s de bande passante entre le site et l'emplacement Prisma Access.

Outre les connexions aux services déployées pour l'accès à large bande passante, le diagramme montre un autre ensemble de connexions aux services. Ces connexions aux services fournissent des fonctions de routage normales pour Prisma Access (dans ce diagramme, elles fournissent un accès de routage interne entre les connexions au réseau distant et les connexions aux services à large bande passante). Palo Alto Networks recommande, lorsque vous déployez une connexion à large bande passante, de réserver les connexions aux services pour fournir l'accès à la ressource dans le siège social ou l'emplacement du centre de données uniquement, et de déployer des connexions aux services supplémentaires à utiliser pour le routage interne entre les réseaux distants, les utilisateurs mobiles et les ressources du centre de données.

 ©2025 Palo Alto Networks, Inc.



Chaque connexion aux services est active et possède sa propre adresse **Service IP Address (Adresse IP du service)** . Utilisez cette adresse pour terminer le tunnel IPSec pour chaque connexion aux services.

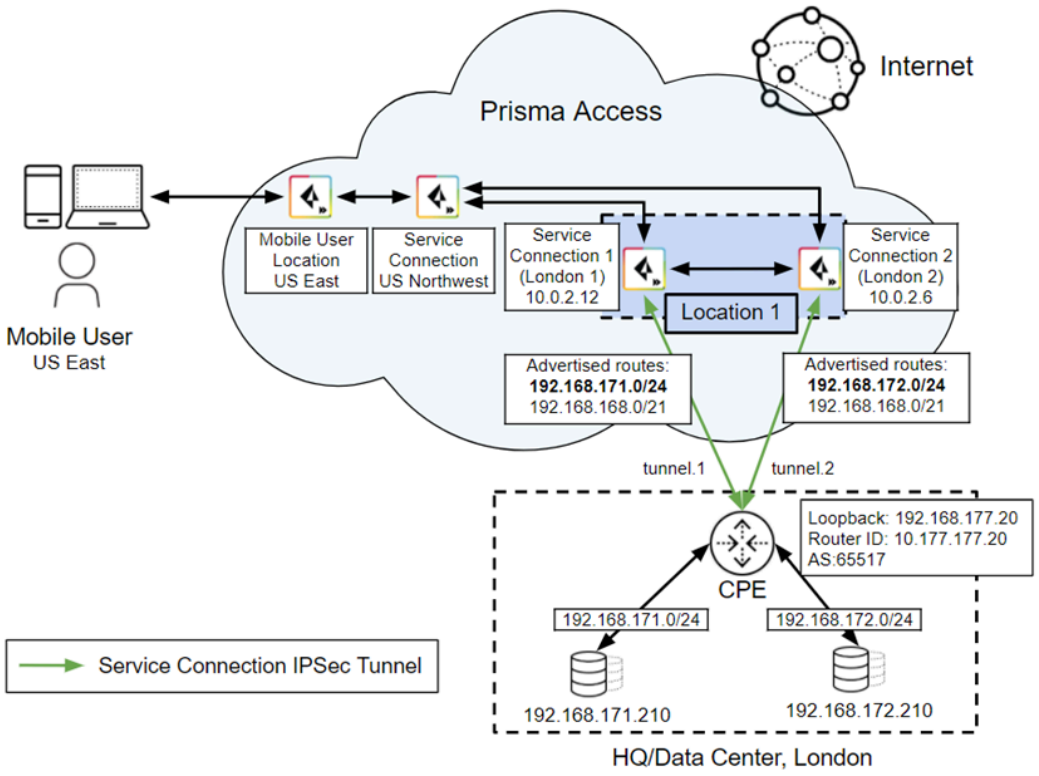
Créer une connexion à large bande passante vers un siège social ou un centre de données

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Pour configurer plusieurs connexions aux services à un seul siège social ou centre de données, procédez comme suit.

Les étapes de cette section utilisent un exemple de déploiement comme indiqué dans le diagramme suivant. Dans cet exemple, le siège social de Londres se connecte à deux connexions aux services différentes (London 1 et London 2) à l'aide de deux tunnels IPSec différents qui se terminent sur deux interfaces d'équipement sur site client (CPE) différentes (tunnel.1 et tunnel.2).

 ©2025 Palo Alto Networks, Inc.



Cet exemple et les étapes de cette section utilisent un pare-feu nouvelle génération pour mettre fin aux connexions aux services sur le CPE. Toutefois, vous pouvez utiliser n'importe quel CPE prenant en charge le routage symétrique et le routage PBF ou basé sur des politiques comme le CPE.

Utilisez ces étapes à titre indicatif. Chaque cas d'utilisation peut nécessiter une conception et une planification supplémentaires qui dépassent le cadre de ce document.

STEP 1 | Avant de déployer plusieurs connexions aux services à partir d'un seul emplacement Prisma Access sur un site unique, assurez-vous que votre réseau possède les prérequis suivants :

- Vous devez diviser les sous-réseaux dans l'emplacement du siège social ou du centre de données et publier un sous-réseau unique sur chaque connexion aux services.
- Votre équipement sur site client (CPE) doit prendre en charge et vous devez pouvoir configurer les fonctionnalités réseau suivantes :
  - Policy-Based Forwarding (transfert basé sur une politique - PBF) ou routage basé sur une politique : votre CPE doit pouvoir choisir de manière sélective un chemin spécifique pour une adresse IP source locale et un sous-réseau spécifiques.
  - Retour symétrique : vous devez pouvoir configurer votre CPE pour garantir des flux de trafic symétriques vers et depuis une adresse IP et un sous-réseau spécifiques, et configurer un retour symétrique pour les tunnels de basculement si l'un des tunnels tombe en panne.

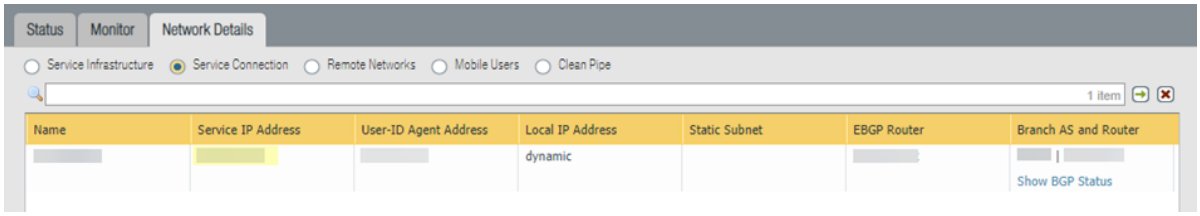
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Créez les connexions aux services et établissez la connectivité pour les tunnels IPSec utilisés pour les connexions aux services.

1. Sur le Panorama qui gère Prisma Access, configurez une connexion aux services, y compris la création d'une nouvelle configuration du tunnel IPSec, d'une passerelle IKE, d'un profil crypto IPSec et des paramètres de surveillance du tunnel.

   Prisma Access propose des modèles IPSec prédéfinis que vous pouvez utiliser pour simplifier le processus de création de tunnels IPSec.

2. Recherchez l'adresse IP à utiliser comme côté distant du tunnel IPSec de votre CPE sur Prisma Access en sélectionnant **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)**, en cliquant sur le bouton radio **Service Connection (Connexion aux services)** et en notant **l'adresse IP du service et l'adresse** pour le site.



3. Sur votre CPE, créez un tunnel IPSec vers les connexions aux services.

   1. Vérifiez que les tunnels IKE et IPSec utilisent les mêmes profils crypto pour l'authentification et le chiffrement entre les homologues.
   2. Utilisez **Service IP Address (Adresse IP du service)** comme homologue adresse IP pour le tunnel.

   Si vous utilisez un pare-feu nouvelle génération comme CPE, sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** et créez deux tunnels pour les connexions aux services (**tunnel.1** et **tunnnel.2** dans la capture d'écran suivante).



STEP 3 | Créez des paramètres de routeur virtuel pour le CPE.

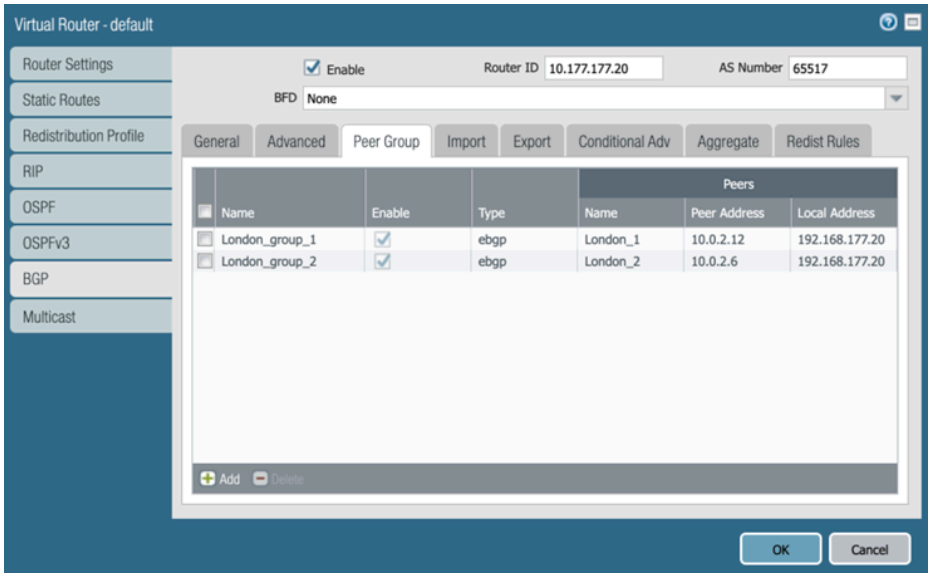
Vous créez des instances de routage BGP qui publient un sous-réseau sur un tunnel et l'autre sous-réseau sur un autre tunnel, ce qui garantit l'équilibrage de la charge sur les deux tunnels actifs.

Si vous utilisez un pare-feu nouvelle génération comme CPE, sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, cliquez sur **Add (Ajouter)** pour ajouter les paramètres du

 ©2025 Palo Alto Networks, Inc.

routeur virtuel, puis sur **Add (Ajouter)** pour ajouter un **BGP Peer Group (Groupe d'homologues BGP)** pour chaque tunnel, en spécifiant les paramètres suivants :

- Spécifiez un **Router ID (ID de routeur)** et un **AS Number (Numéro AS)** du routeur CPE (10.177.177.20 et 65517, respectivement, dans cet exemple).
- Spécifiez l'adresse du **EBGP Router (Routeur EBGP)** des connexions aux services (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **EBGP Router (Routeur EBGP)**) comme **Peer Address (Adresse d'homologue)** pour les connexions aux services (10.0.2.12 pour la connexion aux services 1 et 10.0.2.6 pour la connexion aux services 2 dans cet exemple).
- Pour la zone **Local Address (Adresse locale)**, vous pouvez spécifier l'adresse de bouclage du CPE (192.168.177.20 dans cet exemple).



STEP 4 | Créez un sous-réseau résumé pour les adresses IP utilisées pour les deux tunnels.

Fournir un sous-réseau résumé garantit la redondance. Lorsque les deux tunnels sont opérationnels, le trafic utilise les itinéraires les plus spécifiques pour atteindre sa destination ; par exemple, 192.168.171.0/24 utilise le tunnel.1 pour atteindre sa destination. L'ajout d'un sous-réseau résumé qui couvre tous les sous-réseaux publiés (192.168.168.0/21 dans cet exemple) garantit que le trafic de 192.168.171.0/24 est accessible depuis le tunnel.2 si le tunnel.1 tombe en panne et que le trafic de 192.168.172.0/24 est accessible depuis le tunnel.1 si le tunnel.2 tombe en panne.

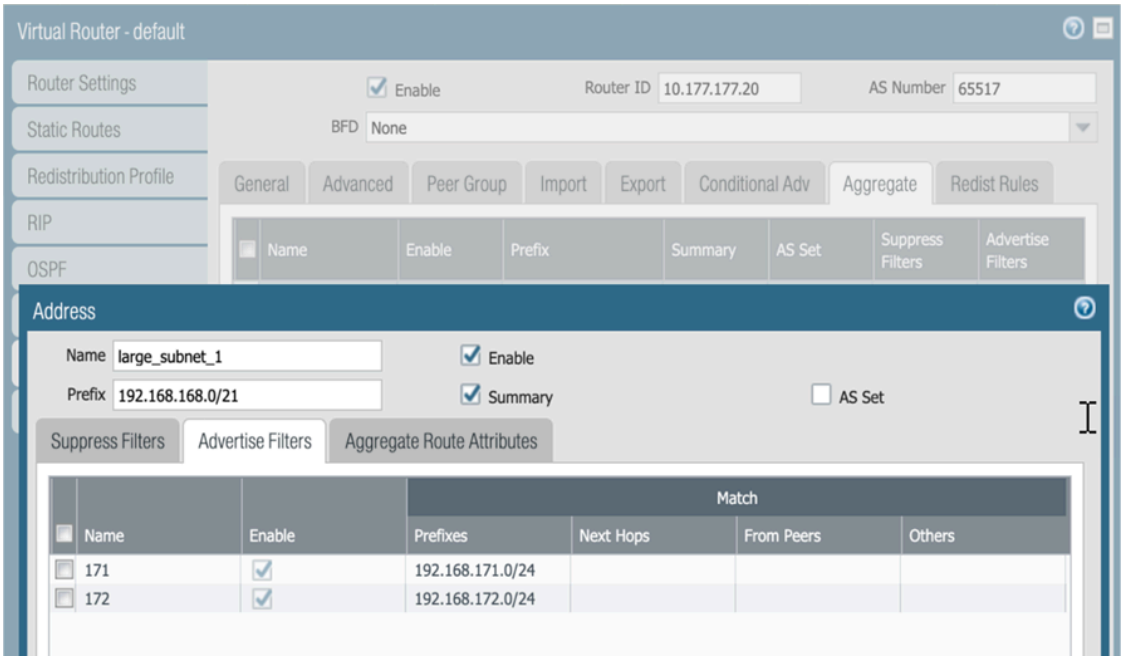
Si vous utilisez un pare-feu nouvelle génération comme CPE, procédez comme suit.

1. Continuez à modifier le profil du routeur virtuel et cliquez sur **Add (Ajouter)** pour ajouter des paramètres d'agrégation d'itinéraires (**Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** > **BGP** > **Aggregate (Agréger)**).

 ©2025 Palo Alto Networks, Inc.

2. Saisissez les sous-réseaux résumés pour les sous-réseaux que vous publiez pour les connexions aux services.

   Dans cet exemple, entrez un **Prefix (Préfixe)** de **192.168.168.0/21**, qui résume les deux sous-réseaux du centre de données.

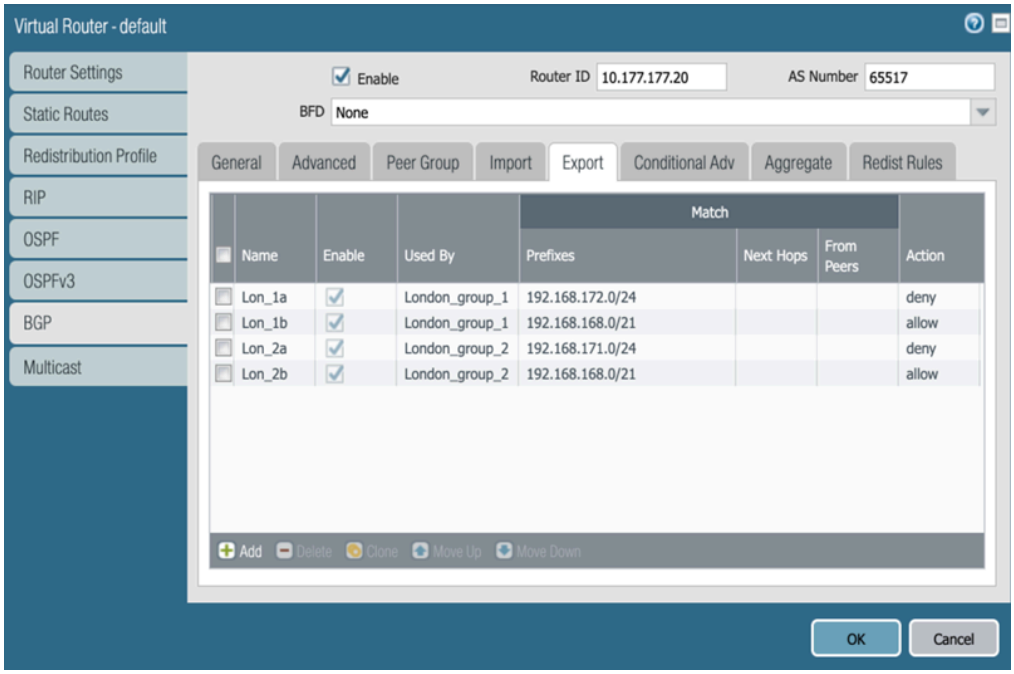


3. Saisissez les paramètres **Export (Exportation)** pour garantir que les tunnels publient les sous-réseaux corrects.

   Dans cet exemple, vous spécifiez une **Action** de **deny (déni)** et **allow (autorisation)** pour les sous-réseaux afin que le premier sous-réseau (192.168.171.0/24) soit accessible

 ©2025 Palo Alto Networks, Inc.

depuis le tunnel.1 et que le deuxième sous-réseau (192.168.172.0/24) soit accessible depuis le tunnel.2.



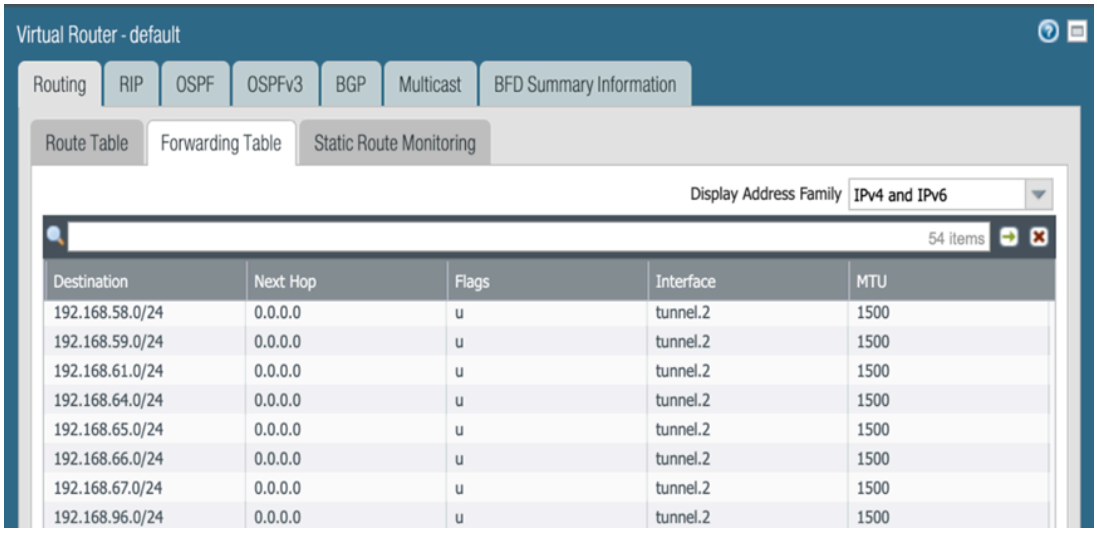
STEP 5 | (Déploiements avec plus de deux connexions aux services uniquement) Si vous avez besoin de plus de deux connexions aux services pour connecter les utilisateurs à des ressources privées pour une bande passante supérieure à 2 Gbit/s, ajoutez des préfixes AS-PATH pour les itinéraires exportés afin que les connexions aux services utilisent le routage symétrique vers et depuis le centre de données en cas de basculement. Pour plus d'informations, reportez-vous à la sectionConfigurer plus de deux connexions aux services à un siège ou à un centre de données.

STEP 6 | Pour garantir un retour symétrique (pour garantir que le trafic provenant de 192.168.171.0/24 utilise toujours le tunnel.1 et que le trafic provenant de 192.168.172.0 utilise toujours le tunnel.2), entrez des règles de routage basées sur PBF ou des politiques.

Par défaut, BGP installe des itinéraires dans la table de routage pour toutes les destinations différentes, quel que soit le tunnel préféré. La capture d'écran suivante montre que BGP

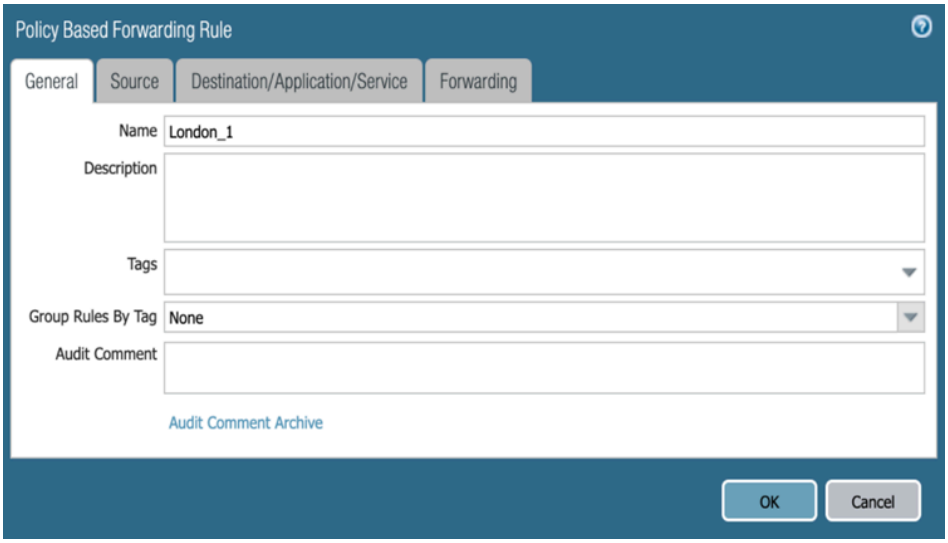
 ©2025 Palo Alto Networks, Inc.

annonce toutes les destinations du sous-réseau 192.168.168.0/21 pour tunnel.2, ce qui peut entraîner un routage asymétrique pour le trafic provenant de 192.168.171.0/24.



Pour garantir un routage symétrique, configurez un ensemble de règles de transfert basées sur PBF ou sur un itinéraire. Si vous utilisez un pare-feu nouvelle génération comme CPE, procédez comme suit.

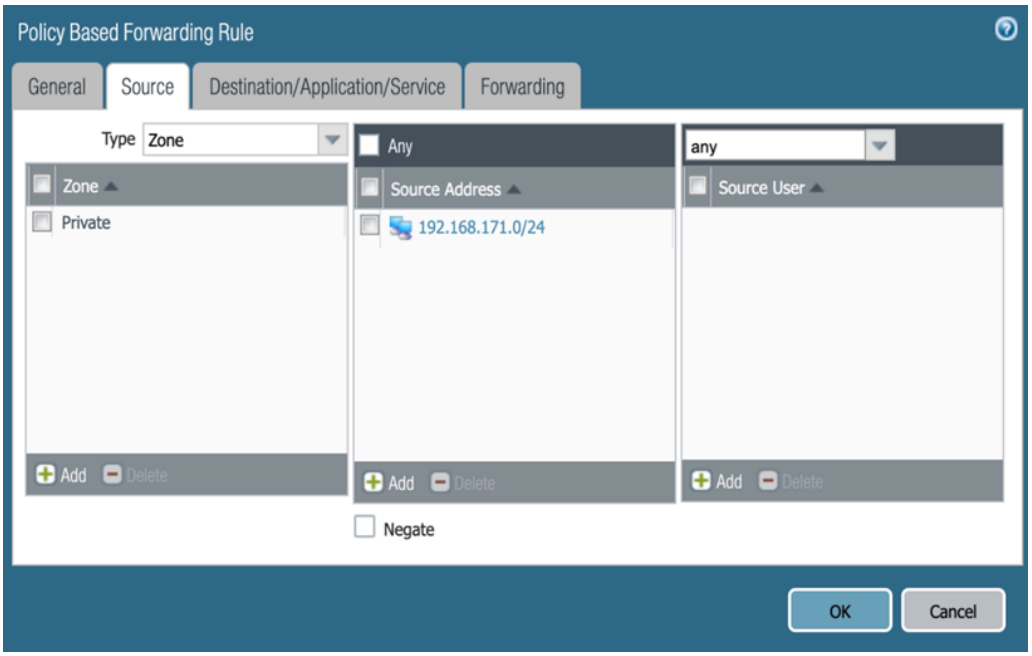
1. Sélectionnez **Policies (Politiques)** > **Policy Based Forwarding (Transfert basé sur une politique)**, puis **Add (Ajoutez)** une règle de politique PBF.



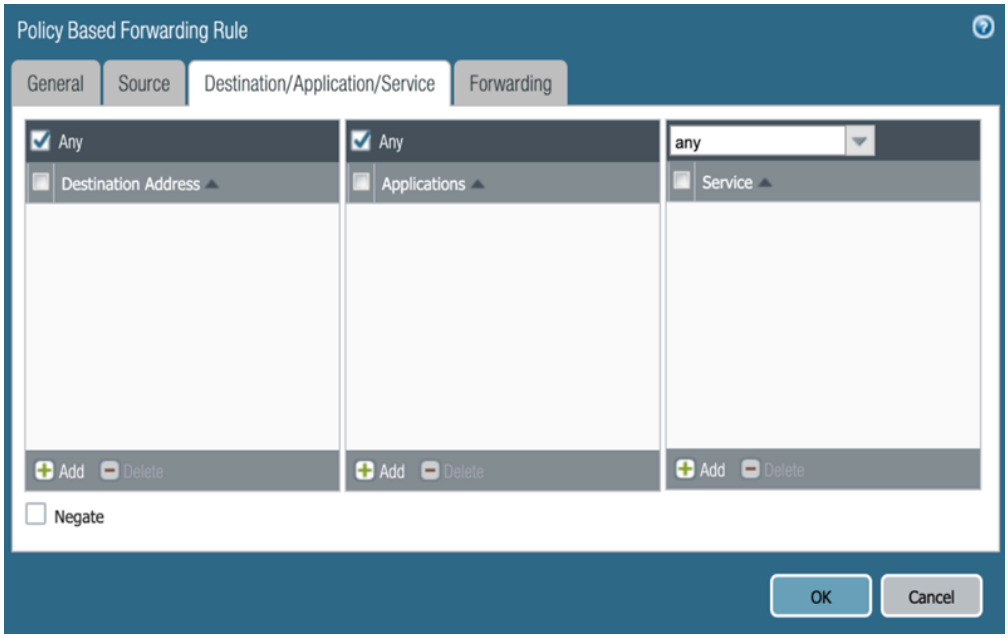
2. Sélectionnez **Source** et **Add (Ajouter)** pour ajouter une **Source Address (Adresse source)** à utiliser pour le PBF.

   Dans ce cas, vous souhaitez créer un PBF pour tunnel.1, vous entrez donc le sous-réseau 192.168.171.0/24.

 ©2025 Palo Alto Networks, Inc.



3. Sélectionnez **Destination/Application/Service** et sélectionnez une adresse de destination **Any (Indifférente)** et une application **Any (Indifférente)**.

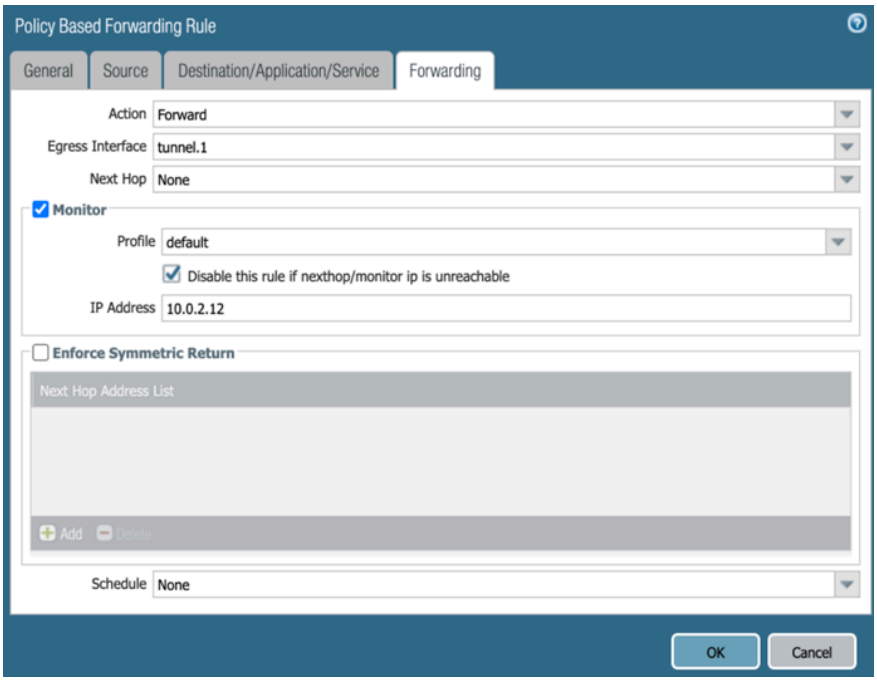


4. Sélectionnez **Forwarding (Transfert)** et spécifiez les paramètres suivants, puis cliquez sur **OK** :
   - Sélectionnez une **Action Forward (Transfert)**.
   - Sélectionnez une **Egress Interface (Interface de sortie)** du tunnel vers lequel vous souhaitez transférer le sous-réseau IP (**tunnel.1** dans ce cas).
   - Sélectionnez **Monitor (Surveiller)** et sélectionnez les profils de surveillance suivants :
     - Sélectionnez un **Profile (Profil) default (par défaut)**.

 ©2025 Palo Alto Networks, Inc.

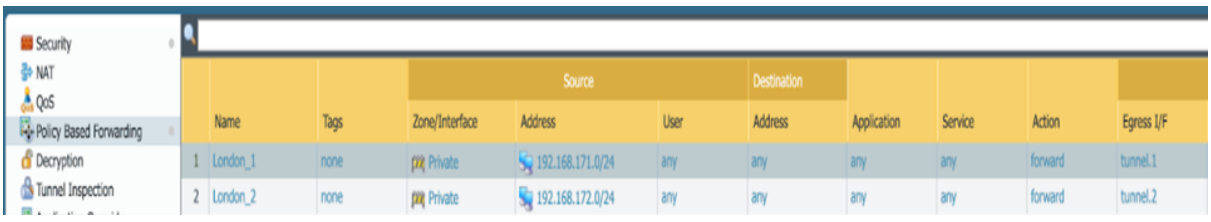
- Sélectionnez **Disable this rule if nexthop/monitor ip is unreachable (Désactiver cette règle si l'adresse IP de surveillance/le saut suivant est inaccessible)**.
- Spécifiez une **IP Address (Adresse IP)** de l'adresse du **EBGP Router (Routeur EBGP)** de la connexion aux services (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **EBGP Router (Routeur EBGP)**).

L'activation de la surveillance et la sélection de l'adresse du routeur EBGP de la connexion aux services garantissent que, si le tunnel.1 tombe en panne, le pare-feu désactive la politique PBF et achemine le trafic sur le tunnel qui est toujours actif (tunnel.2).



5. Répétez l'étape 6, en remplaçant l'adresse du **EBGP Router (Routeur EBGP)** de la connexion aux services 1 par l'adresse du **EBGP Router (Routeur EBGP)** de la connexion aux services 2 et le sous-réseau du tunnel.1 par le sous-réseau du tunnel.2.

   Une fois terminé, vous disposez de deux politiques PBF, une pour tunnel.1 et une pour tunnel.2.

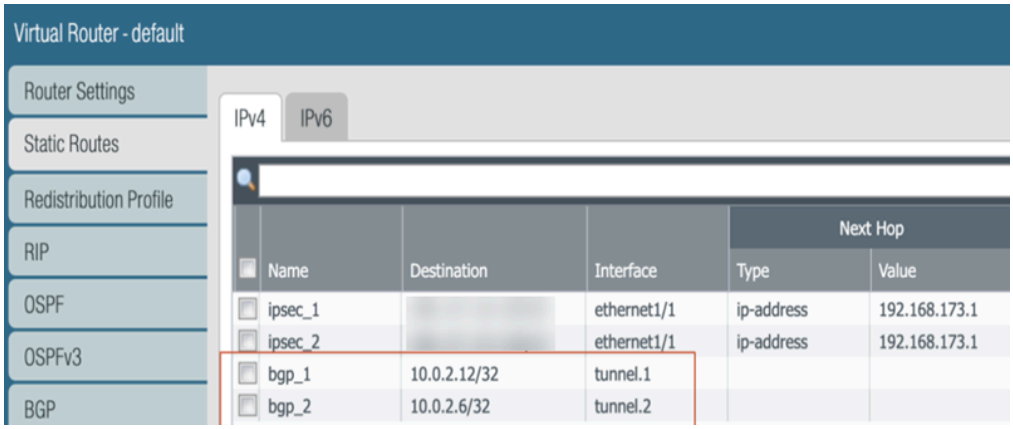


STEP 7 | Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** > **Static Routes (Itinéraires statiques)** et attribuez l'adresse du **EBGP Router (Routeur EBGP)** de la connexion

 ©2025 Palo Alto Networks, Inc.

aux services 1 à la zone **Interface** du **tunnel.1**. Attribuez ensuite l'adresse du **EBGP Router (Routeur EBGP)** de la connexion aux services 2 à la zone **Interface** du **tunnel.2**

La saisie d'itinéraires statiques spécifiques pour chacune des adresses BGP du routeur garantit que la surveillance du tunnel fonctionne correctement, car l'adresse IP du routeur EBGP de la connexion aux services 1 est accessible uniquement par le tunnel.1 et l'adresse IP du routeur EBGP de la connexion aux services 2 est accessible uniquement par le tunnel.2.



Configurer plus de deux connexions aux services à un siège ou à un centre de données

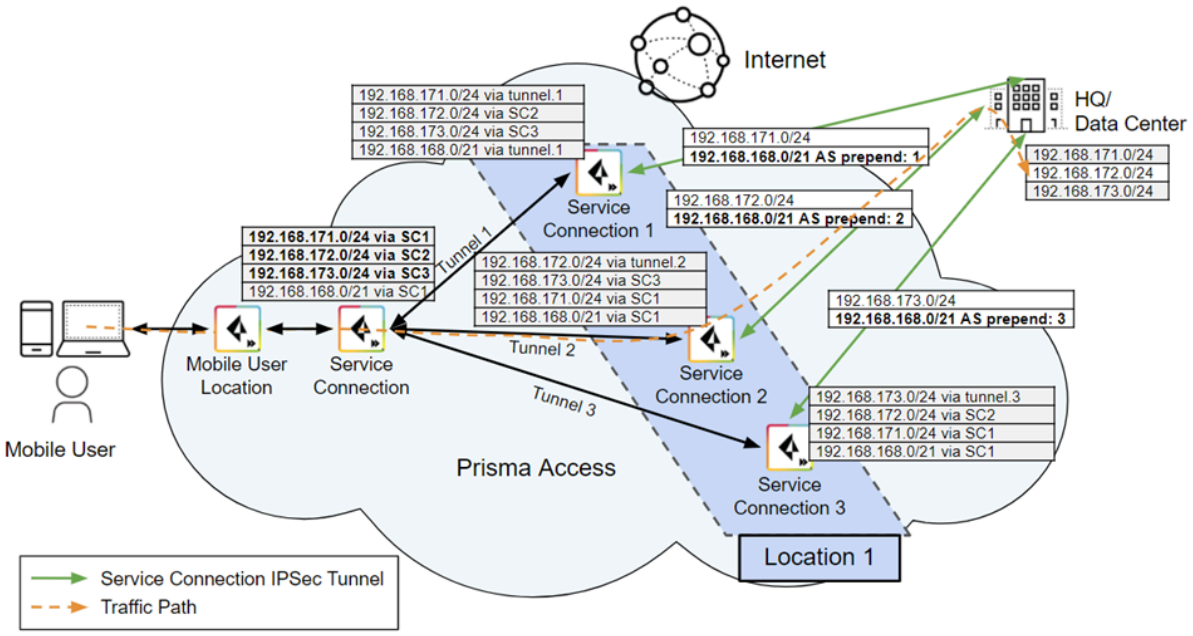
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Lorsque vous utilisez deux tunnels pour une connexion aux services à large bande passante, il ne reste qu'un seul chemin de trafic disponible en cas de défaillance d'un tunnel, ce qui simplifie la configuration d'un chemin de basculement. Si vous utilisez plus de deux connexions pour une connexion à large bande passante, vous devez effectuer une configuration supplémentaire pour garantir un comportement cohérent pour les basculements de tunnel.

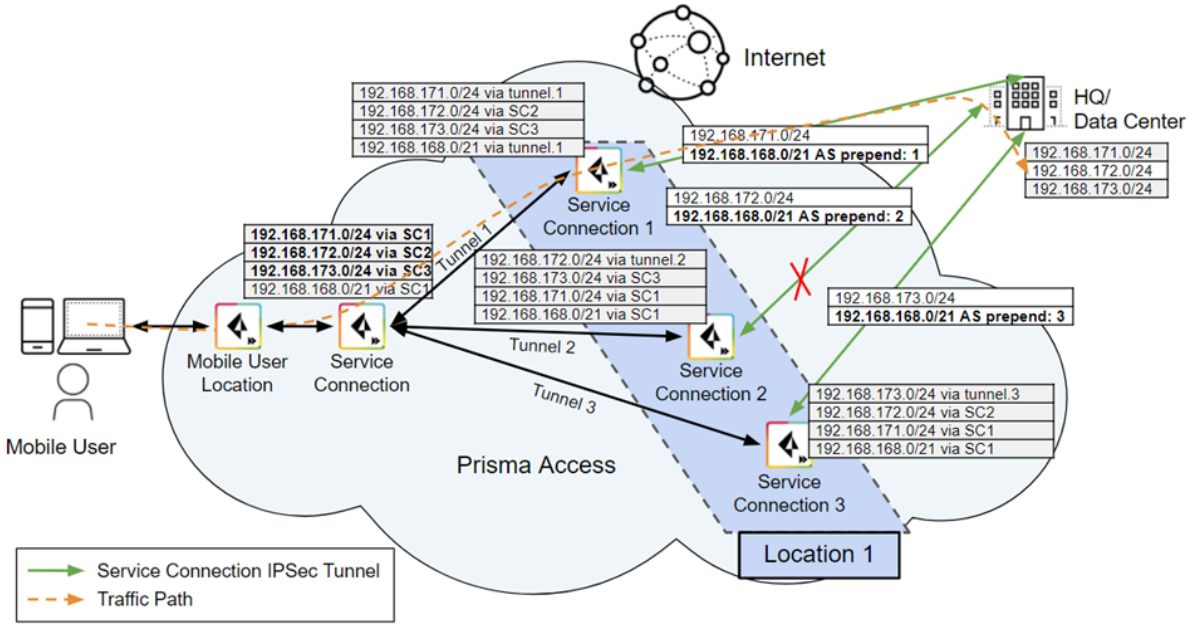
Étant donné que vous utilisez un sous-réseau résumé pour le basculement du tunnel, vous devez indiquer explicitement le tunnel de connexion aux services à utiliser en cas de basculement. Étant donné que le routage BGP choisit le plus petit nombre de chemins AS en tant qu'itinéraire, vous pouvez préfixer des chemins AS à des itinéraires pour que BGP privilégie un tunnel en cas de basculement.

L'exemple suivant montre les tables de routage d'une connexion aux services à large bande passante à l'aide de trois connexions aux services. Si les trois tunnels sont actifs, Prisma Access utilise les itinéraires les plus spécifiques pour atteindre les sous-réseaux à l'emplacement du siège social ou du centre de données. Étant donné que l'utilisateur accède à une ressource dans le sous-réseau 192.168.172.0/24, la connexion aux services la plus proche de l'utilisateur mobile vérifie sa table de routage et sélectionne le tunnel 2 comme chemin d'accès à la ressource du centre de données.

 ©2025 Palo Alto Networks, Inc.



Si le tunnel 2 tombe en panne, l'itinéraire le plus spécifique vers la ressource dans le sous-réseau 192.168.172.0/24 n'est pas disponible. Par conséquent, la connexion aux services la plus proche de l'utilisateur utilise le sous-réseau résumé 192.168.168.0/21. Vous n'avez configuré qu'un seul préfixe de chemin AS pour la connexion aux services 1. De ce fait, Prisma Access choisit le tunnel 1 comme chemin de basculement, car il comporte moins de préfixes de chemins AS.

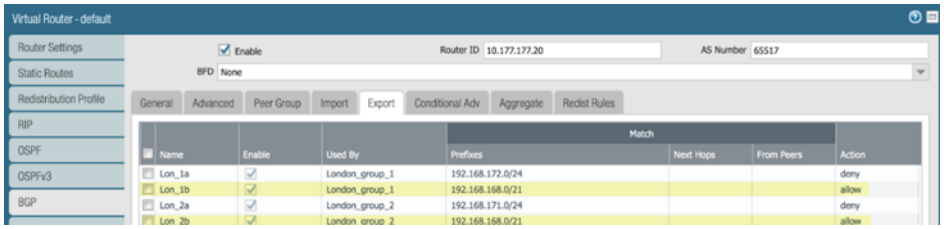


Si vous utilisez un pare-feu nouvelle génération en tant que CPE, effectuez la tâche suivante pour ajouter des préfixes à des itinéraires.

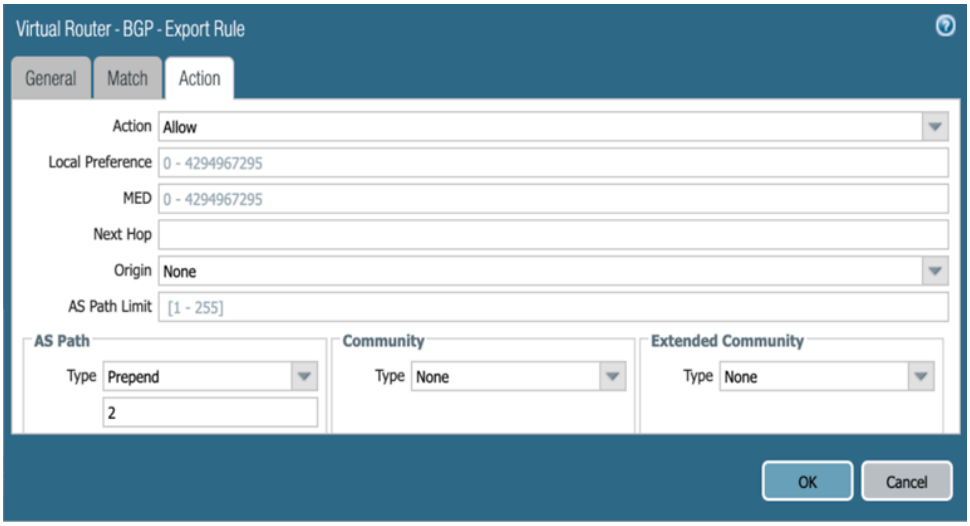
STEP 1 | Sélectionnez les profils d'exportation du routeur virtuel BGP (**Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** > **BGP** > **Export (Exporter)**).

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Modifiez la règle d'exportation que vous avez créée lorsque vous avez configuré les connexions aux services qui présente l'**Action Allow (Autoriser)**.



STEP 3 | Dans la zone AS Path (Chemin AS), ajoutez un **Prepend (Préfixe)**, puis entrez le nombre de préfixes de chemin AS à ajouter (**2** dans cet exemple).



STEP 4 | Répétez les étapes 2 et 3 pour chaque règle d'exportation présentant l'**Action Allow (Autoriser)**, en ajoutant des préfixes de chemin AS pour correspondre aux scénarios de basculement que vous avez planifiés pour votre déploiement.

Dans les exemples utilisés dans cette section, vous allez ajouter le préfixe de chemin AS 1 pour le tunnel vers l'emplacement du centre de données pour la connexion aux services 1 (tunnel.1), le préfixe de chemin AS 2 pour le tunnel utilisé pour la connexion aux services 2 (tunnel.2) et le préfixe de chemin AS 3 pour le tunnel utilisé pour la connexion aux services 3 (tunnel.3).

Une fois ceci terminé, cet exemple utilise les tunnels suivants en cas de basculement :

- En cas de panne du tunnel.2 ou tunnel.3, le trafic du sous-réseau correspondant bascule vers tunnel.1, dont le chemin AS annoncé est le plus court.
- Si tunnel.1 tombe en panne, le trafic de son sous-réseau (192.168.171.0/24) bascule vers tunnel.2, dont le chemin AS annoncé est le plus court.

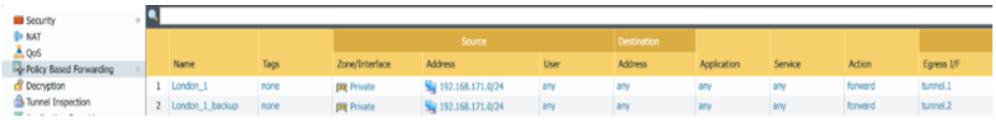
STEP 5 | Ajoutez des PBF de secours ou des politiques de routage basées sur des politiques pour garantir un trafic de retour symétrique en cas de défaillance d'un tunnel.

Alors que les préfixes de chemin AS garantissent que le trafic de Prisma Access au centre de données utilise un tunnel spécifique, en cas de basculement, vous devez également assurer un chemin de retour symétrique pour le trafic du centre de données vers Prisma Access. Pour garantir un retour symétrique, utilisez des politiques de routage PBF ou basées sur des

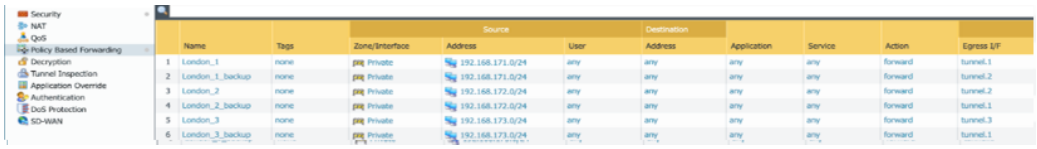
 ©2025 Palo Alto Networks, Inc.

politiques qui reflètent les scénarios de basculement que vous avez créés pour le trafic depuis Prisma Access vers le centre de données.

Dans cet exemple, pour le trafic du tunnel.1 dont l'adresse IP source est 192.168.171.0/24, vous créez une politique PBF de secours qui force le trafic de retour à utiliser tunnel.2 en cas de basculement. La première règle PBF est désactivée si l'adresse IP de surveillance du tunnel n'est pas accessible. Lorsque ce basculement se produit, le CPE (dans cet exemple, un pare-feu nouvelle génération) évalue la règle suivante dans la liste.



Vous ajoutez ensuite d'autres règles PBF pour correspondre aux scénarios de basculement que vous avez créés pour le trafic depuis Prisma Access vers le centre de données.



Préserver le mappage de User-ID et Device-ID pour les connexions aux services avec NAT source

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Pare-feu nouvelle génération (NGFW) exécutant une version minimale de PAN-OS 11.2 ❑ Cette fonctionnalité utilise l'encapsulation Geneve. Veillez à ce que tous les pare-feu en aval, en plus des NGFW exécutant PAN-OS 11.2 ou une version ultérieure, soient capables de décapsuler l'encapsulation Geneve. Cette fonctionnalité n'est pas prise en charge avec l'accès à privilèges dynamiques.

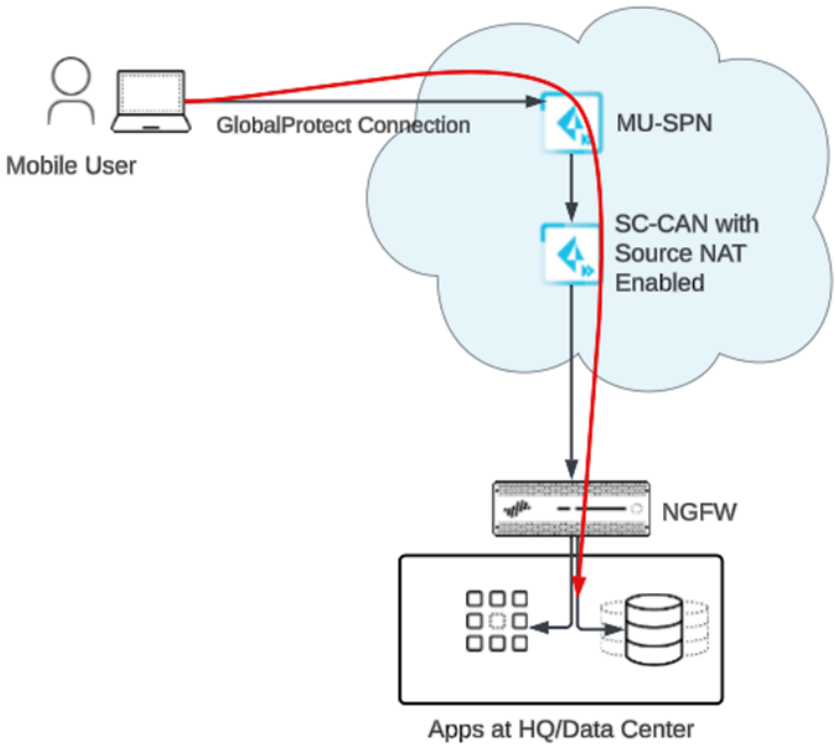
Vous utilisez des connexions aux services, également appelées nœuds d'accès de connexion aux services d'entreprise (SC-CAN), dans Prisma Access pour sécuriser les applications privées. Pour limiter l'accès aux applications en fonction du User-ID ou du Device-ID, vous pouvez déployer un pare-feu nouvelle génération (NGFW) dans le centre de données ou le siège social dans lequel se trouvent les applications privées. Ensuite, configurez les règles de politique sur le NGFW en fonction du mappage du User-ID, du Device-ID ou des deux.

Pour utiliser ces règles, le NGFW doit recevoir le mappage du User-ID ou du Device-ID du SC-CAN. Cependant, si les utilisateurs se connectent à Prisma Access à l'aide de GlobalProtect et que le SC-CAN a l'option **Data Traffic source NAT (NAT de source du trafic de données)** activée,

 ©2025 Palo Alto Networks, Inc.

le NGFW ne peut pas obtenir ce mappage. Si la **Data Traffic source NAT (NAT de source du trafic de données)** est activée sur le SC-CAN, elle exécute la NAT sur le pool d'adresses IP de l'utilisateur mobile et n'annonce pas ces adresses IP dans le centre de données ou le siège social.

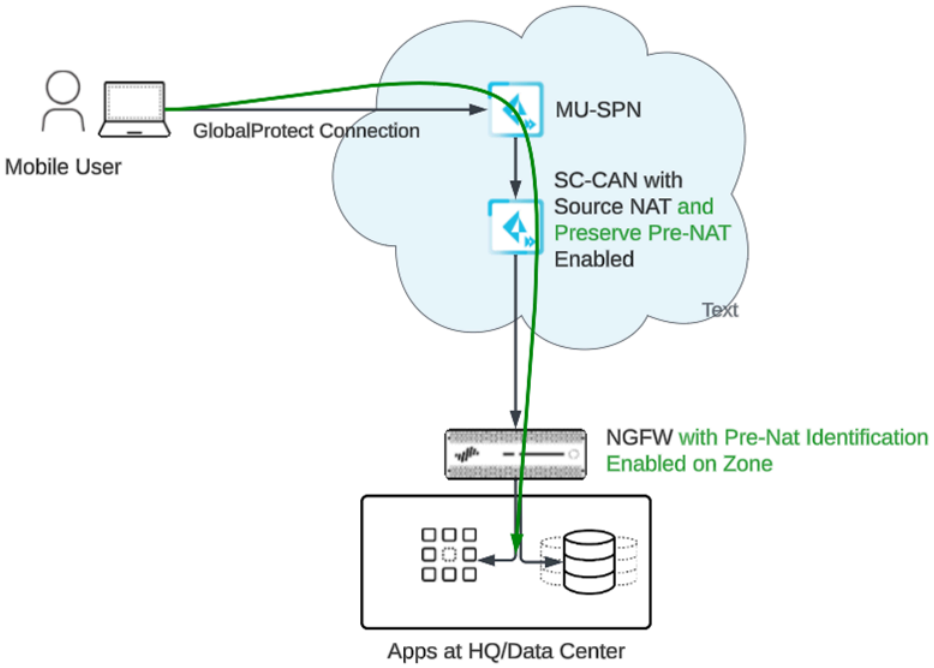
Dans ce cas, le NGFW ne peut pas récupérer le User-ID ou le Device-ID des utilisateurs GlobalProtect, ce qui signifie que vous ne pouvez pas appliquer une politique basée sur le User-ID ou le Device-ID.



Pour vous assurer que votre réseau distribue le mappage du User-ID ou du Device-ID au siège social ou au centre de données, effectuez la procédure répertoriée dans l'une des sections suivantes, ce qui permet au NGFW d'appliquer des règles de politique de sécurité en fonction du mappage du User-ID qu'il apprend auprès de GlobalProtect.

Un NGFW avec une version PAN-OS minimale de 11.2 est requis. La connexion aux services n'a pas besoin de se terminer sur le NGFW et peut se terminer sur un autre périphérique compatible IPSec, à condition que le NGFW soit en aval de l'endroit où la connexion aux services se termine.

 ©2025 Palo Alto Networks, Inc.



- Strata Cloud Manager
- Panorama

Préserver le mappage des identifiants utilisateur et de périphérique pour les connexions aux services avec NAT source (Strata Cloud Manager)

Pour que Prisma Access distribue les mappages des identifiants utilisateur des utilisateurs GlobalProtect vers un NGFW au siège social ou au centre de données Prisma Access (Managed by Strata Cloud Manager), effectuez les étapes suivantes.

Cette procédure suppose que vous disposez de la configuration réseau suivante :

- Vous avez activé **Data Traffic source NAT (NAT source de trafic de données)** sur la connexion aux services.
- Vous avez déployé un NGFW au siège ou dans le centre de données où se trouvent les applications privées.
- Vous avez appliqué des règles de politique de sécurité pour Prisma Access sur le NGFW en fonction des zones que vous avez créées dans le NGFW.

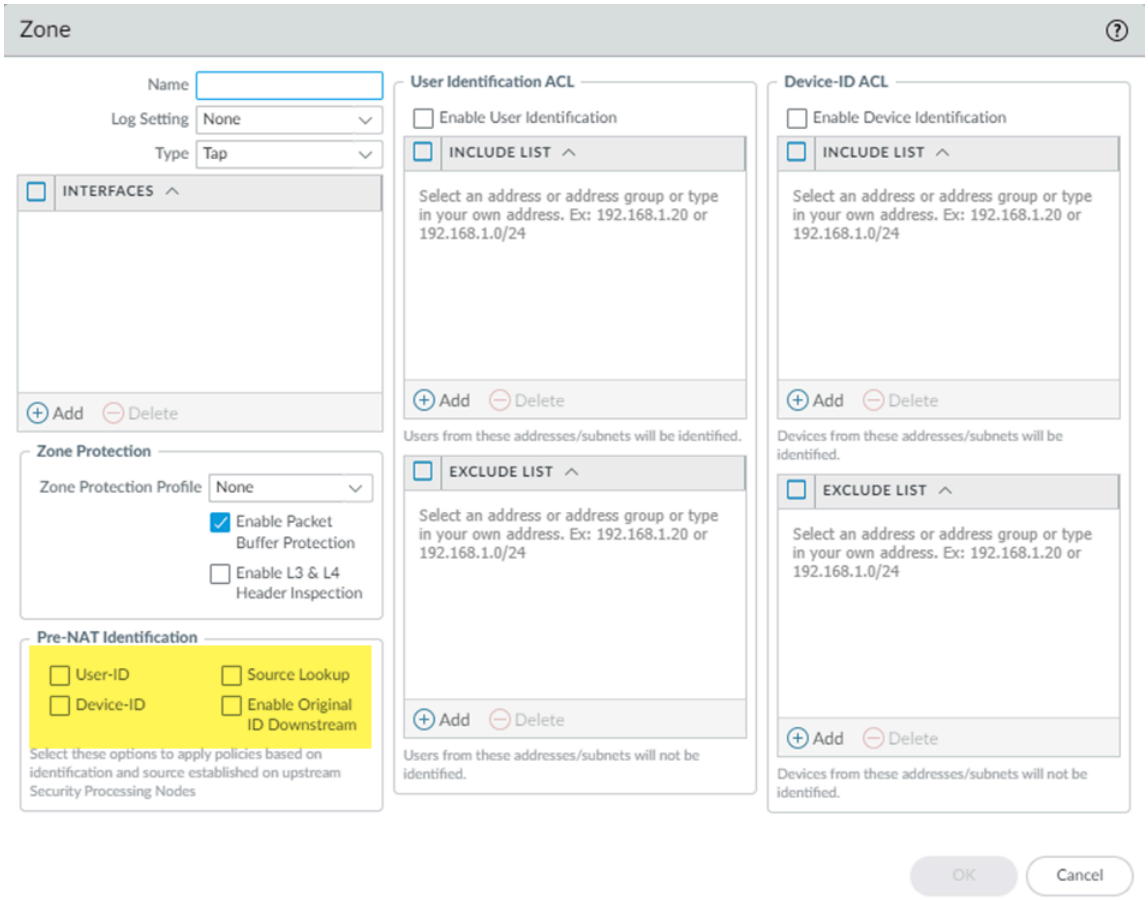
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Saisissez les paramètres d'identification pré-NAT sur le NGFW.

1. Connectez-vous au NGFW, ou au SCM ou au Panorama qui gère le NGFW, et accédez à **Network (Réseau)** > **Zones**.
2. **Add (Ajoutez)** une zone ou sélectionnez une zone existante.
3. Sélectionnez un ou plusieurs paramètres **Pre-NAT Identification (Identification pré-NAT)** :
   - **User-ID** : préserve le mappage du User-ID de l'utilisateur mobile utilisé avant la NAT des adresses IP. Activez cette option si vous utilisez des identifiants d'utilisateur dans les règles de politique de sécurité.
   - **Device-ID** : préserve le mappage du Device-ID de l'utilisateur mobile utilisé avant la NAT des adresses IP. Activez cette option si vous utilisez l'ID du périphérique dans les règles de politique de sécurité.
   - **Source Lookup (Recherche de source)** : vous permet de faire correspondre l'adresse IP source d'origine reçue de GlobalProtect. Si vous utilisez la recherche de source dans les politiques QoS ou de transfert basé sur des politiques (PBF), la comparaison d'IP source est basée sur l'adresse IP source pré-NAT. Par exemple, si vous aviez une politique de sécurité qui autorisait une adresse IP source de 1.1.1.1 et une adresse IP de destination de Any (tout), 1.1.1.1 est comparé à l'adresse IP source pré-NAT dans l'en-tête du paquet.
   - **Enable Original ID Downstream (Activer l'ID d'origine en aval)** : si vous avez deux NGFW consécutifs, spécifiez cette option pour que le premier NGFW envoie les informations pré-NAT au deuxième NGFW après que le premier NGFW a inspecté le

 ©2025 Palo Alto Networks, Inc.

trafic et lui a appliqué des politiques. Il s'agit de la configuration par défaut sur les SC-CAN.



4. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

STEP 2 | Créez une session d'interface en ligne de commande (CLI) avec NGFW et saisissez la commande suivante en mode de configuration :

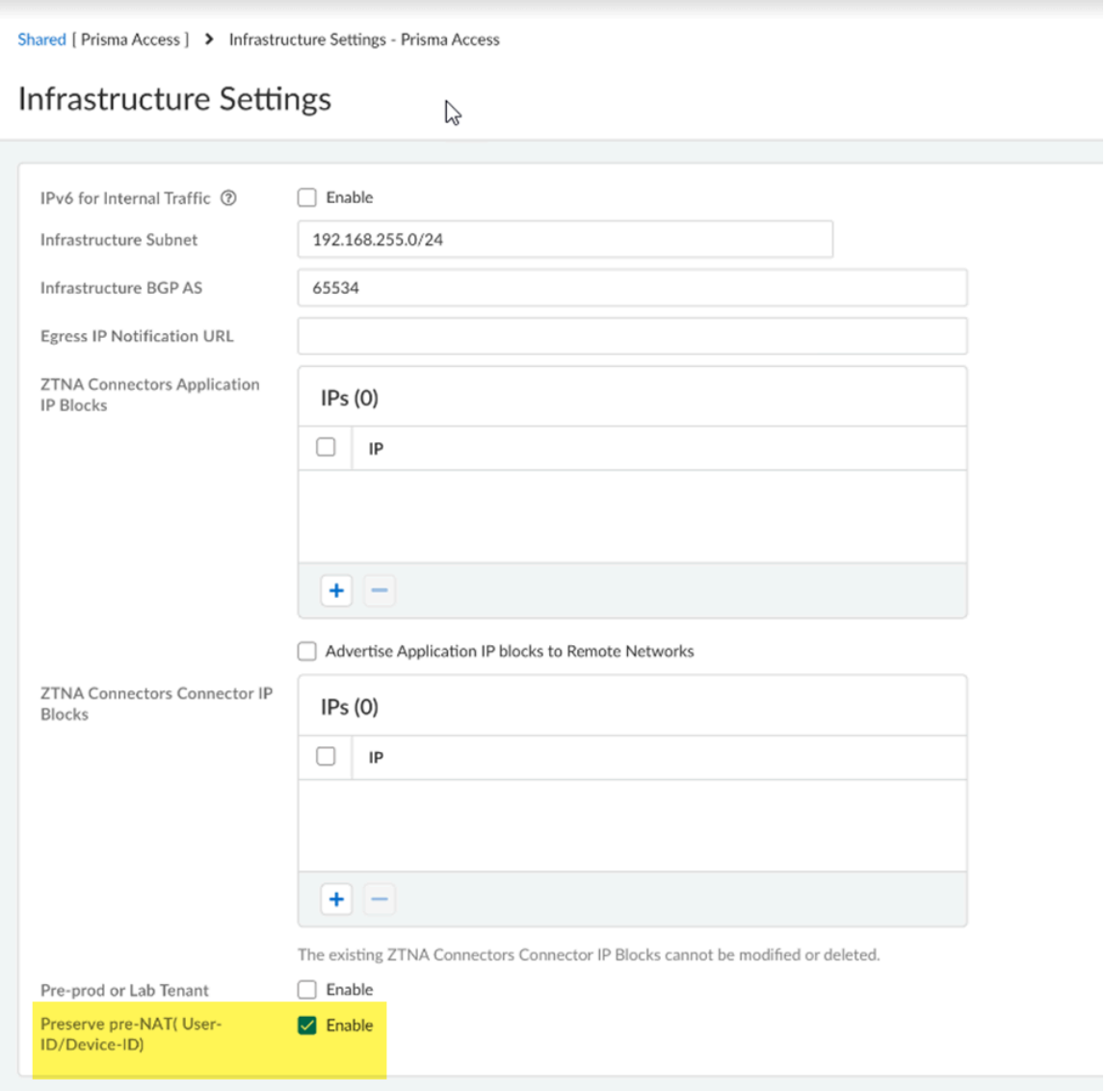
```
set deviceconfig setting preserve-prenat-feature yes
```

Si vous devez désactiver cette fonctionnalité à l'avenir, saisissez `set deviceconfig setting preserve-prenat-feature no`.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Activez les paramètres pré-NAT dans Strata Cloud Manager.

1. Accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Infrastructure Settings (Paramètres d'infrastructure)**.
2. **Enable (Activer) Preserve pre-NAT (User-ID/Device-ID) (Préserver pré-NAT(User-ID/Device-ID)**.



3. Cliquez sur **Push Config (Transmettre la configuration)** pour enregistrer vos modifications.

Préserver le mappage des identifiants utilisateur et de périphérique pour les connexions aux services avec NAT source (Panorama)

Pour que Prisma Access distribue les mappages des identifiants utilisateur des utilisateurs GlobalProtect vers un NGFW au siège social ou au centre de données Prisma Access (Managed by Panorama), effectuez les étapes suivantes.

Cette procédure suppose que vous disposez de la configuration réseau suivante :

 ©2025 Palo Alto Networks, Inc.

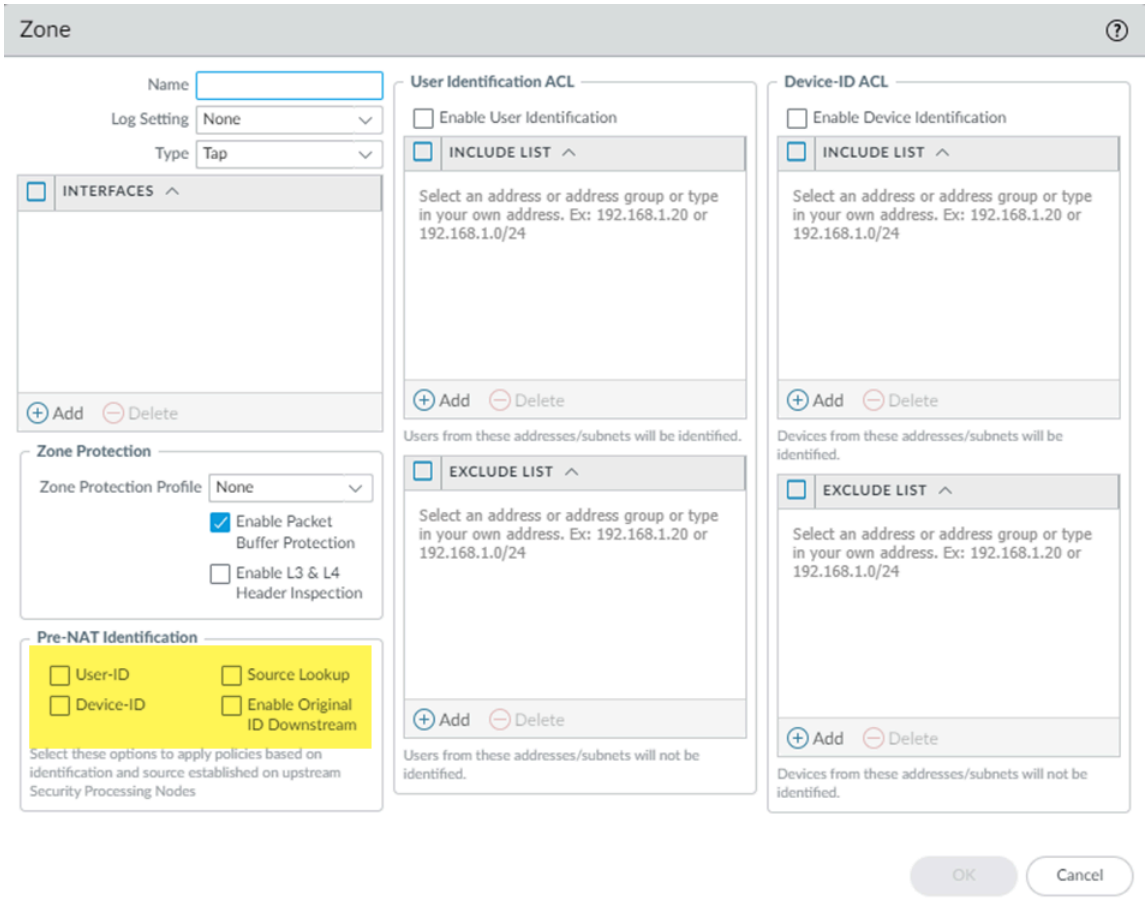
- Vous avez activé **Data Traffic source NAT (NAT source de trafic de données)** sur la connexion aux services.
- Vous avez déployé un NGFW au siège ou dans le centre de données où se trouvent les applications privées.
- Vous avez appliqué des règles de politique de sécurité pour Prisma Access sur le NGFW en fonction des zones que vous avez créées dans le NGFW.

STEP 1 | Saisissez les paramètres d'identification pré-NAT sur le NGFW.

1. Connectez-vous au NGFW, ou au SCM ou au Panorama qui gère le NGFW, et accédez à **Network (Réseau)** > **Zones**.
2. **Add (Ajoutez)** une zone ou sélectionnez une zone existante.
3. Sélectionnez un ou plusieurs paramètres **Pre-NAT Identification (Identification pré-NAT)** :
   - **User-ID** : préserve le mappage du User-ID de l'utilisateur mobile utilisé avant la NAT des adresses IP. Activez cette option si vous utilisez des identifiants d'utilisateur dans les règles de politique de sécurité.
   - **Device-ID** : préserve le mappage du Device-ID de l'utilisateur mobile utilisé avant la NAT des adresses IP. Activez cette option si vous utilisez l'ID du périphérique dans les règles de politique de sécurité.
   - **Source Lookup (Recherche de source)** : vous permet de faire correspondre l'adresse IP source d'origine reçue de GlobalProtect. Si vous utilisez la recherche de source dans les politiques QoS ou de transfert basé sur des politiques (PBF), la comparaison d'IP source est basée sur l'adresse IP source pré-NAT. Par exemple, si vous aviez une politique de sécurité qui autorisait une adresse IP source de 1.1.1.1 et une adresse IP de destination de Any (tout), 1.1.1.1 est comparé à l'adresse IP source pré-NAT dans l'en-tête du paquet.
   - **Enable Original ID Downstream (Activer l'ID d'origine en aval)** : si vous avez deux NGFW consécutifs, spécifiez cette option pour que le premier NGFW envoie les informations pré-NAT au deuxième NGFW après que le premier NGFW a inspecté le

 ©2025 Palo Alto Networks, Inc.

trafic et lui a appliqué des politiques. Il s'agit de la configuration par défaut sur les SC-CAN.



4. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

STEP 2 | Créez une session d'interface en ligne de commande (CLI) avec NGFW et saisissez la commande suivante en mode de configuration :

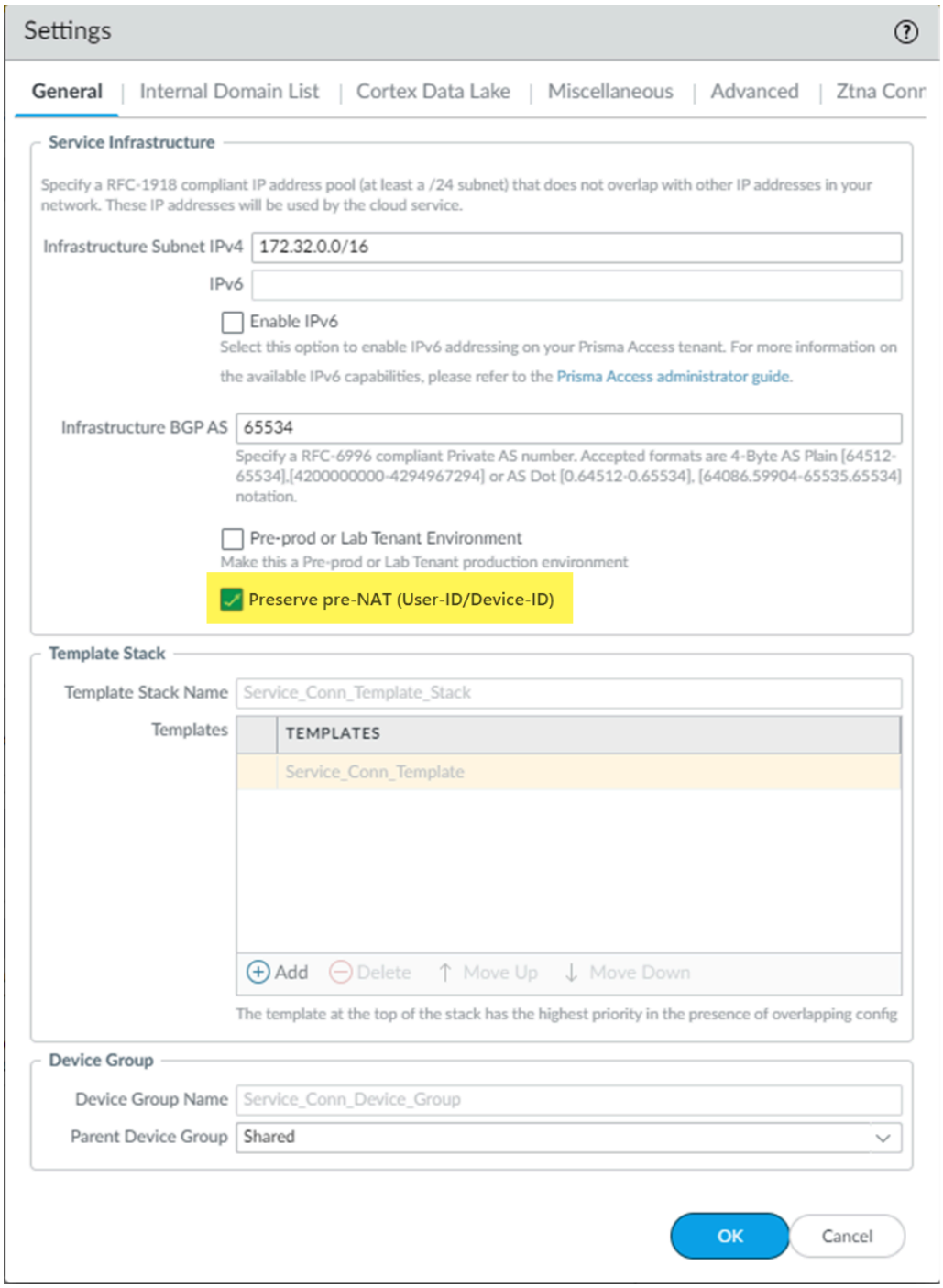
```
set deviceconfig setting preserve-prenat-feature yes
```

Si vous devez désactiver cette fonctionnalité à l'avenir, saisissez `set deviceconfig setting preserve-prenat-feature no`.

©2025 Palo Alto Networks, Inc.

STEP 3 | À partir de Panorama qui gère Prisma Access, activez les paramètres pré-NAT.

1. Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** et cliquez sur l'engrenage pour modifier les **Settings (Paramètres)**.
2. Sélectionnez **Preserve pre-NAT (User-ID/Device-ID) (Préserver pré-NAT(User-ID/Device-ID)**.



3. **Commit and Push (Validez et appliquez)** vos modifications.

 ©2025 Palo Alto Networks, Inc.

Déploiements Utilisateurs mobiles – GlobalProtect avancés dans Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Les sections suivantes présentent les déploiements avancés disponibles dans un déploiement Utilisateurs mobiles – GlobalProtect :

- Prise en charge de l'enregistrement DNS dynamique pour les utilisateurs mobiles – GlobalProtect
- Identification et mise en quarantaine des périphériques compromis dans un déploiement GlobalProtect Prisma Access
- Trafic de l'entonnoir IPv6 chez les utilisateurs mobiles : déploiements GlobalProtect
- Redistribuer les informations HIP avec Prisma Access
- Voir les rapports HIP
- Prise en charge de l'encodage Gzip dans un VPN sans client
- Réplication du trafic dans Prisma Access

Configurer plusieurs portails dans Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Version minimale requise du client GlobalProtect : 6.1 (Windows et macOS uniquement)

Vous pouvez configurer deux portails basés sur des numéros de port dans le même locataire Prisma Access, chaque portail prenant en charge une méthode d'authentification différente. Activez cette fonctionnalité pour migrer les utilisateurs mobiles d'une méthode d'authentification à une autre sans créer de locataire Prisma Access. Cette configuration offre une plus grande flexibilité d'authentification en vous permettant de déplacer progressivement les utilisateurs vers l'authentification basée sur le cloud, sans qu'il soit nécessaire de disposer d'une instance Prisma Access distincte.

Prisma Access avec plusieurs portails GlobalProtect utilise un numéro de port différent pour chaque portail au sein du même locataire. Configurez le premier portail GlobalProtect à l'aide du port standard 443. Lorsque vous activez la fonctionnalité de portails multiples, Prisma Access configure un deuxième portail GlobalProtect à l'aide d'un autre port 8443 et autorise les connexions au second portail à l'aide du même FQDN que le premier. La fonctionnalité de portails multiples ne prend en charge que deux portails par FQDN.

 ©2025 Palo Alto Networks, Inc.

Lorsqu'un utilisateur se connecte au portail à l'aide du port 443, le trafic est envoyé au premier portail d'authentification sans modification de l'adresse IP. Ce flux n'a pas changé par rapport aux configurations sans la fonctionnalité de portails multiples GlobalProtect. Lorsqu'un utilisateur se connecte à l'aide du port 8443, le trafic atteint une règle NAT de destination. Cela conduit l'utilisateur au deuxième portail d'authentification à une adresse IP différente. Après s'être authentifié sur l'un des portails, l'utilisateur est redirigé vers la passerelle avec le cookie de remplacement d'authentification. Cette fonctionnalité dépend des paramètres des cookies de remplacement d'authentification et est activée pour les portails et les passerelles.

Le tableau suivant décrit la prise en charge de plusieurs portails GlobalProtect avec des combinaisons de méthodes d'authentification et de certificats utilisant l'authentification héritée (telle que RADIUS ou LDAP) sur le portail principal et l'authentification cloud (telle que SAML ou SAML avec CAS) sur le portail secondaire.

Authentification de l'utilisateur du portail principal	Authentification de l'utilisateur du portail secondaire	Options de méthode de connexion
Héritage, pas de certificat	Cloud, pas de certificat	Connexion utilisateur (permanente, à la demande)
Héritage, <auth profile selection> ET certificat client Note : Le profil de certificat doit être identique.	Cloud, <auth profile selection> ET certificat client Note : Le profil de certificat doit être identique.	Connexion utilisateur (permanente, à la demande) Préouverture de session (toujours active, à la demande)
Héritage, pas de certificat	Cloud, <auth profile selection> OU certificat client	Connexion utilisateur (permanente, à la demande)
Héritage, <auth profile selection> OU certificat client Les configurations de plusieurs portails ne prennent pas en charge les clients utilisant uniquement un certificat client pour l'authentification	Cloud, pas de certificat	Connexion utilisateur (permanente, à la demande) Préouverture de session (toujours active, à la demande), en cas de certificat
Héritage, <auth profile selection> OU certificat client Les configurations de plusieurs portails ne prennent pas en charge les clients utilisant uniquement un certificat client pour l'authentification	Cloud, <auth profile selection> OU certificat client Les configurations de plusieurs portails ne prennent pas en charge les clients utilisant uniquement un certificat client pour l'authentification	Connexion utilisateur (permanente, à la demande) Préouverture de session (toujours active, à la demande), en cas de certificat

©2025 Palo Alto Networks, Inc.

Avant de configurer plusieurs portails, assurez-vous des éléments suivants :

- Les deux portails ont les mêmes profils de certificat ou n'ont aucun profil de certificat
- La liste d'autorisation associée aux profils d'authentification doit être la même
- Lorsque vous acceptez un cookie pour le remplacement de l'authentification sur le portail, assurez-vous que la durée de vie du cookie est la même sur le portail et sur la passerelle
- Les configurations de plusieurs portails ne prennent pas en charge l'utilisation uniquement de l'authentification basée sur un certificat client

> Le VPN sans client *n'est pas pris en charge pour une utilisation sur le portail secondaire dans un déploiement à plusieurs portails. Cependant, le VPN sans client fonctionne sur le portail principal avec votre méthode d'authentification existante.*

- Strata Cloud Manager
- Panorama

Configurer plusieurs portails dans Prisma Access (Strata Cloud Manager)

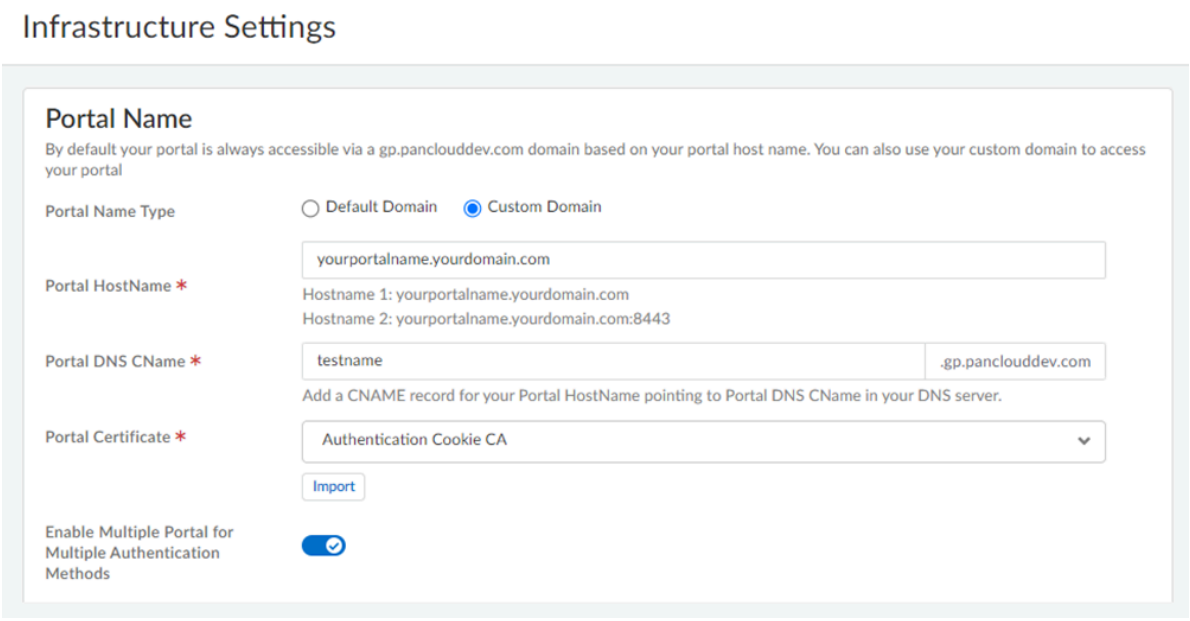
STEP 1 | Contactez le support de Palo Alto Networks pour activer cette fonctionnalité.

STEP 2 | Configurez un utilisateur mobile et sa méthode d'authentification.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Activez plusieurs portails pour la même passerelle.

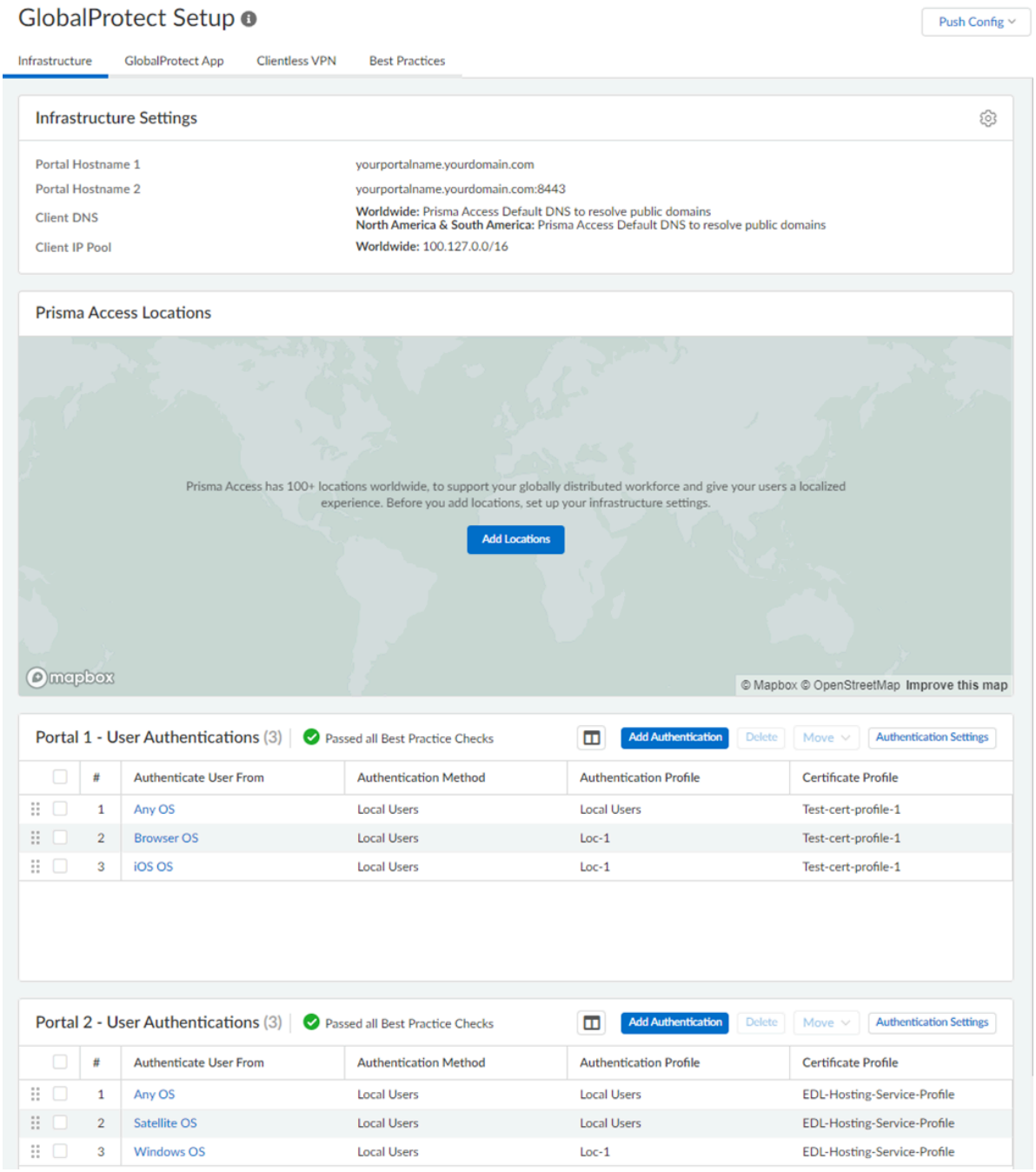
1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **GlobalProtect Setup (Configuration de GlobalProtect)** > **Infrastructure**.
2. Modifiez les **Infrastructure Settings (Paramètres d'infrastructure)**.
3. Cliquez sur **Enable Multiple Portal for Multiple Authentication Methods (Activer plusieurs portails pour plusieurs méthodes d'authentification)**.



Le nouveau portail apparaît pour le port 8443 pour le même locataire. Ce portail hérite des paramètres de configuration du port d'origine, soit le port 443.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Modifiez les configurations du portail pour mettre à jour les paramètres d'authentification.

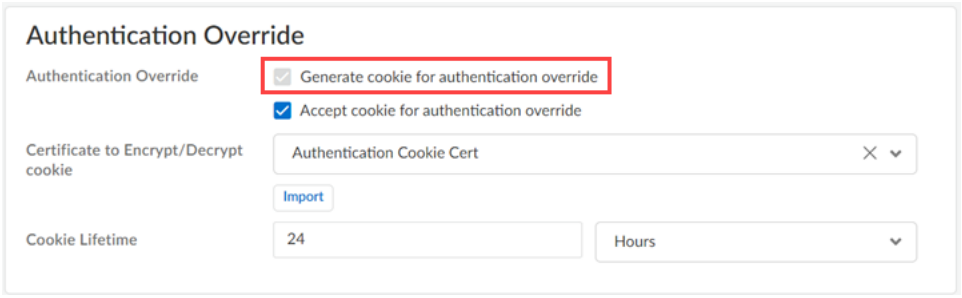


Vous pouvez modifier uniquement les **Authentication Settings (Paramètres d'authentification)** et le **Certificate Profile (Profil de certificat)** du portail.

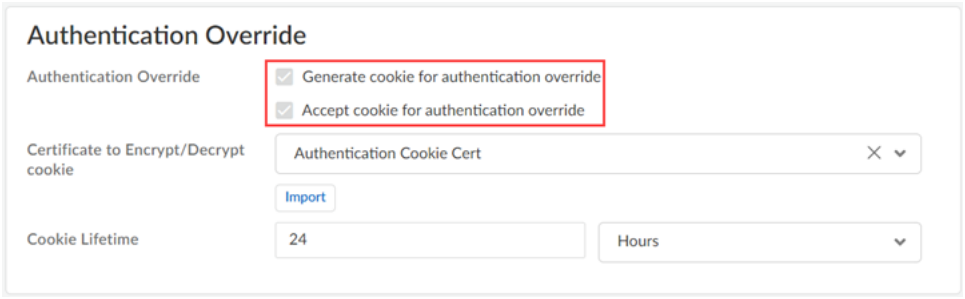
Si vous utilisez une authentification basée sur des certificats dans les deux portails, assurez-vous que les deux portails utilisent le même profil de certificat client pour l'authentification.

Cette fonctionnalité permet aux paramètres de remplacement d'authentification de générer des cookies pour les deux portails dans les paramètres de l'application GlobalProtect.

 ©2025 Palo Alto Networks, Inc.



Cette fonctionnalité permet aux paramètres de remplacement d'authentification de générer et d'accepter des cookies pour les deux portails dans les paramètres du tunnel.



STEP 5 | Enregistrez toutes vos modifications et cliquez sur **Push (Appliquer)** pour appliquer les modifications apportées à la configuration à Prisma Access.

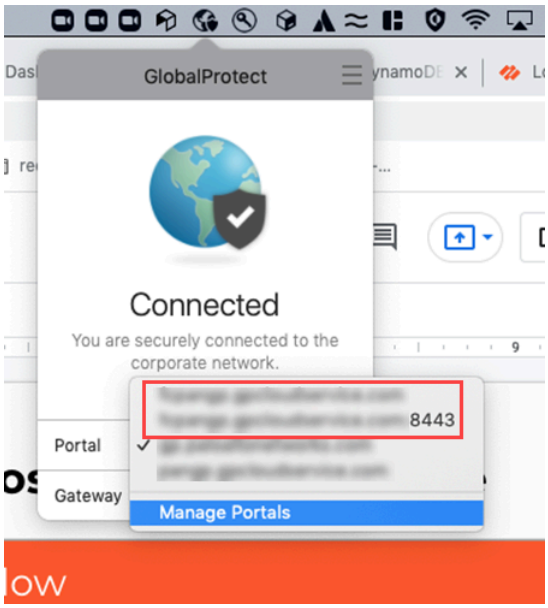
STEP 6 | Ajoutez les portails manuellement ou à l'aide d'un logiciel de gestion des terminaux dans l'application GlobalProtect.

 ©2025 Palo Alto Networks, Inc.

STEP 7 | Vérifiez si vous pouvez vous connecter aux deux portails avec des profils d'authentification différents pour la passerelle.

1. Connectez-vous à votre machine Windows.
2. Connectez-vous aux portails de votre application GlobalProtect.

   Lorsque vous modifiez la connexion entre des portails de différentes méthodes d'authentification, authentifiez la connexion utilisateur.



Si le cookie d'authentification expire lorsque vous vous connectez au portail 8443 et que vous basculez vers la passerelle manuelle, GlobalProtect se connecte à la ***Best Available Gateway (Meilleure passerelle disponible)****.*

Si votre application GlobalProtect utilise des configurations de portail en cache, le repli sur portail ne fonctionne pas.

Si vous utilisez l'authentification basée sur SAML pour le portail secondaire, saisissez les valeurs comme suit lors de l'intégration :

- ***Single sign on URL (URL d'ouverture de session unique)*** *: Entrez* ***`https://Portal-FQDN:443/SAML20/SP/ACS`***

  Portal-FQDN (FQDN du portail) est le FQDN du portail Prisma Access

  Utilisez le portail ***`443`*** *même si vous avez configuré le portail secondaire (8443).*
- ***Audience URI (SP Entity ID) (URI d'audience (ID d'entité SP))*** *: Entrez* ***`https://Portal-FQDN:443/SAML20/SP`***

Configurer plusieurs portails dans Prisma Access (Panorama)

STEP 1 | Contactez votre représentant de compte Palo Alto Networks pour activer cette fonctionnalité.

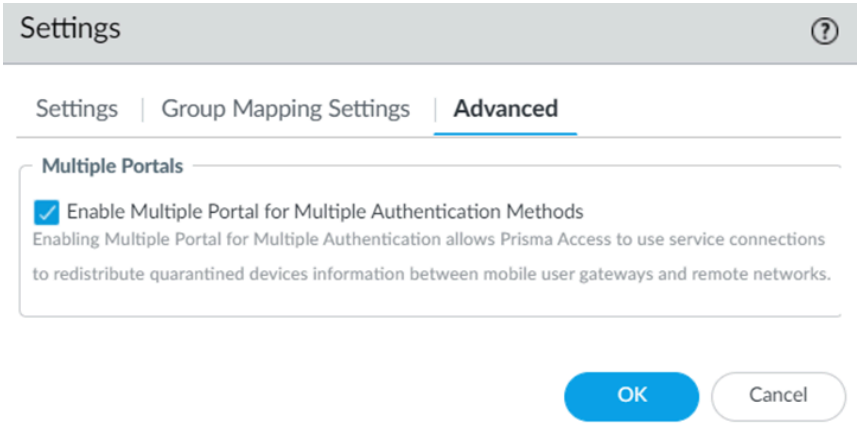
 ©2025 Palo Alto Networks, Inc.

Lors de la configuration de plusieurs portails GlobalProtect avec la redirection du trafic, ne configurez pas ***Accept Default Routes over Service Connections (Accepter les routes par défaut sur les connexions aux services)*** *(****Panorama*** *>* ***Cloud Services*** *>* ***Configuration*** *>* ***Traffic Steering (Redirection du trafic)*** *>* ***Settings (Paramètres)*** *>* ***Accept Default Routes over Service Connections (Accepter les routes par défaut sur les connexions aux services)****). Si vous le faites, les utilisateurs mobiles ne peuvent pas se connecter au portail secondaire.*

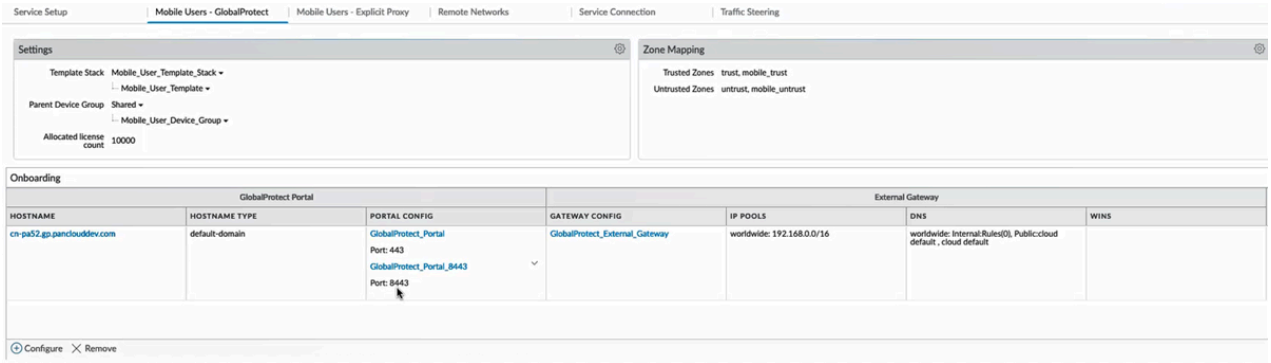
STEP 2 | Configurez un utilisateur mobile et sa méthode d'authentification.

STEP 3 | Sélectionnez **Cloud Services** > **Configuration** > **Mobile Users—GlobalProtect (Utilisateurs mobiles — GlobalProtect)** > **Settings (Paramètres)** > **Advanced (Avancé)**.

STEP 4 | Cliquez sur **Enable Multiple Portal for Multiple Authentication Methods (Activer plusieurs portails pour plusieurs méthodes d'authentification)**.



Le nouveau portail apparaît pour le port 8443 pour le même locataire. Ce portail hérite des paramètres de configuration du port d'origine, soit le port 443.



 ©2025 Palo Alto Networks, Inc.

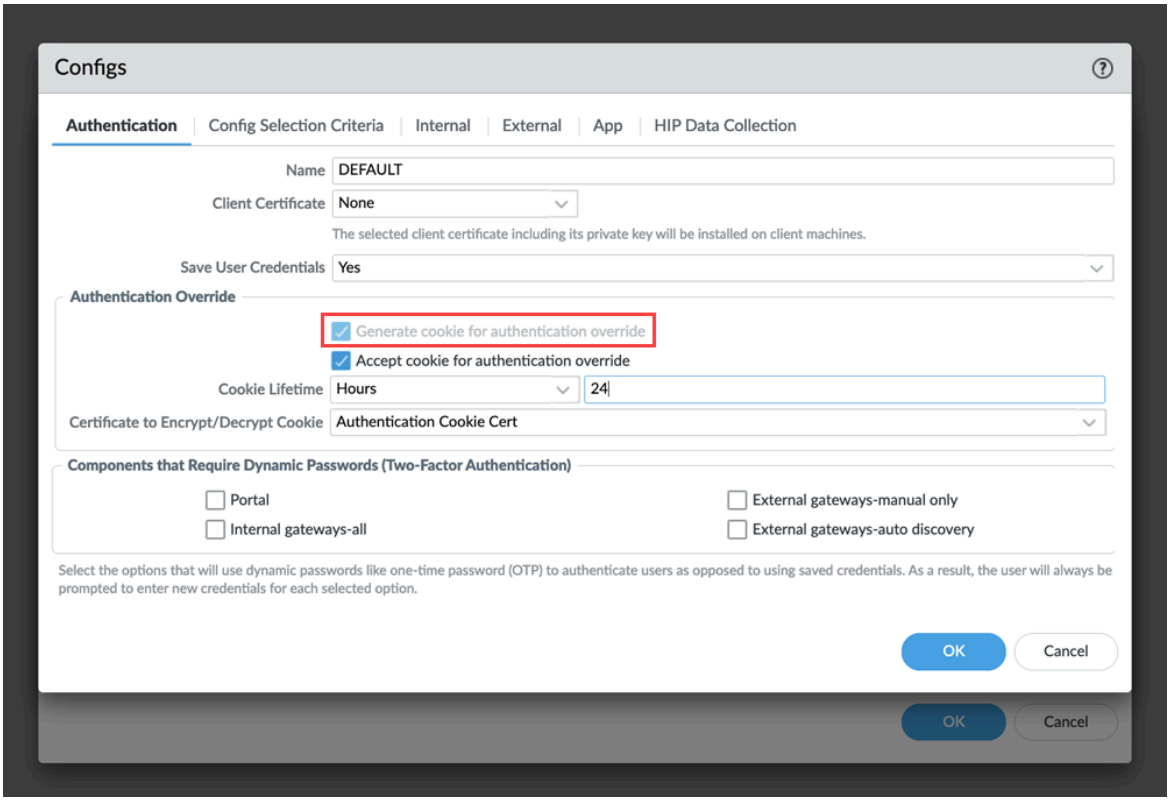
STEP 5 | Modifiez les configurations du portail pour mettre à jour les paramètres d'authentification.

1. Cliquez sur le lien hypertexte du portail ou sélectionnez **Panorama** > **Templates (Modèles)** > **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** et cliquez sur le lien hypertexte du portail.
2. Dans la section **Authentication (Authentification)**, cliquez sur **Add (Ajouter)** pour ajouter une **Client Authentication (Authentification du client)** avec un **Authentication Profile (Profil d'authentification)** différent.

Vous ne pouvez modifier que les paramètres de la **Client Authentication (Authentification du client)** et du **Certificate Profile (Profil de certificat)**.

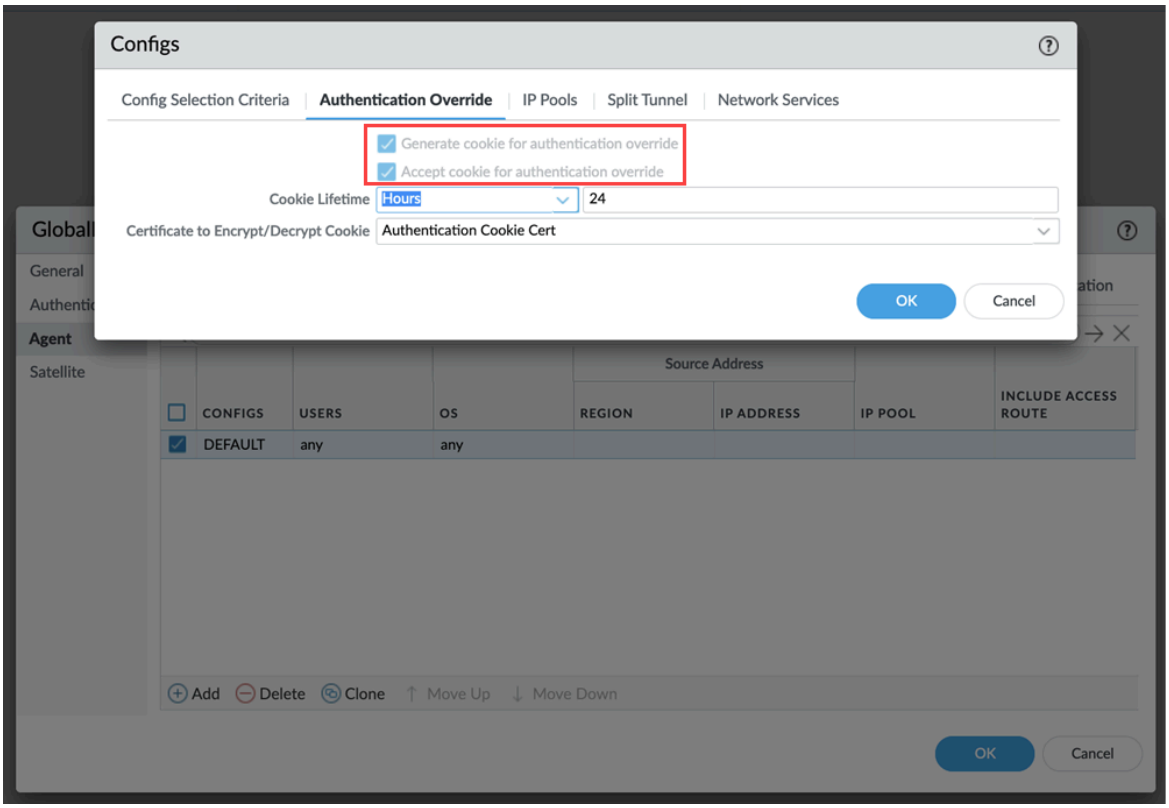
Si vous utilisez l'authentification basée sur des certificats dans les deux portails, assurez-vous que la passerelle n'a pas d'authentification basée sur des certificats.

Cette fonctionnalité permet aux paramètres de remplacement d'authentification de générer des cookies pour les deux portails dans les paramètres de l'application GlobalProtect.



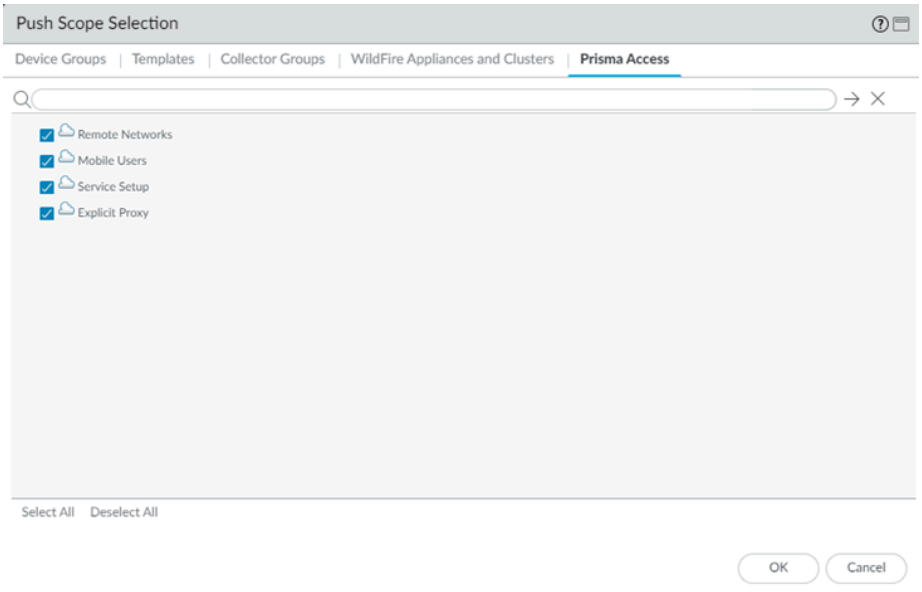
Cette fonctionnalité permet aux paramètres de remplacement d'authentification de générer et d'accepter des cookies pour les deux portails dans les paramètres du tunnel.

 ©2025 Palo Alto Networks, Inc.



STEP 6 | Validez toutes les modifications dans Panorama et appliquez les modifications de configuration sur Prisma Access.

1. Cliquez sur **Commit (Valider)** > **Commit and Push (Valider et transmettre)**.
2. Cliquez sur **Edit Selections (Modifier les sections)** pour modifier les sections et, dans l'onglet **Prisma Access**, assurez-vous que l'option **Mobile Users (Utilisateurs mobiles)** est sélectionnée dans la**Push Scope (Étendue de la transmission)**, puis cliquez sur **OK**.



3. Cliquez sur **Commit and Push (Valider et appliquer)**.

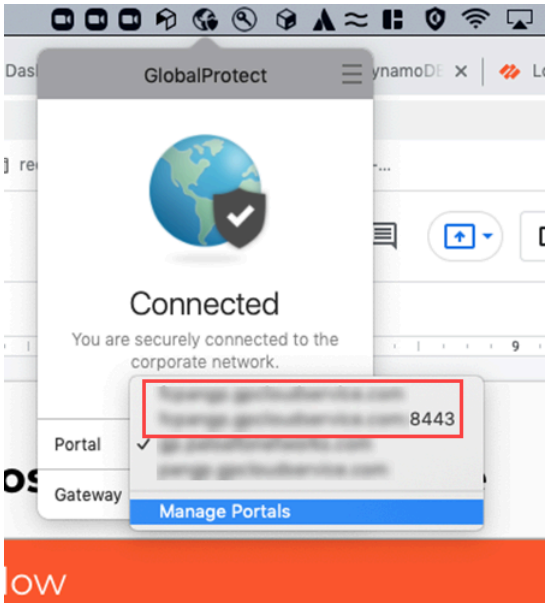
 ©2025 Palo Alto Networks, Inc.

STEP 7 | Ajoutez les portails manuellement ou à l'aide d'un logiciel de gestion des terminaux dans l'application GlobalProtect.

STEP 8 | Vérifiez si vous pouvez vous connecter aux deux portails avec des profils d'authentification différents pour la passerelle.

1. Connectez-vous à votre machine Windows.
2. Connectez-vous aux portails de votre application GlobalProtect.

   Lorsque vous modifiez la connexion entre des portails de différentes méthodes d'authentification, authentifiez la connexion utilisateur.



   Si le cookie d'authentification expire lorsque vous vous connectez au portail 8443 et que vous basculez vers la passerelle manuelle, GlobalProtect se connecte à la ***Best Available Gateway (Meilleure passerelle disponible)****.*

   Si votre application GlobalProtect utilise des configurations de portail en cache, le repli sur portail ne fonctionne pas.

3. Consultez les journaux des deux portails dans **Monitor (Surveiller)** > **Logs (Journaux)** > **GlobalProtect** pour voir les informations sur le portail et l'authentification.

Si vous utilisez l'authentification basée sur SAML pour le portail secondaire, saisissez les valeurs comme suit lors de l'intégration :

- ***Single sign on URL (URL d'ouverture de session unique)*** *: Entrez* ***`https://Portal-FQDN:443/SAML20/SP/ACS`***

  Portal-FQDN (FQDN du portail) est le FQDN du portail Prisma Access

  Utilisez le portail ***443*** *même si vous avez configuré le portail secondaire (8443).*

- ***Audience URI (SP Entity ID) (URI d'audience (ID d'entité SP))*** *: Entrez* ***`https://Portal-FQDN:443/SAML20/SP`***

 ©2025 Palo Alto Networks, Inc.

Prise en charge de l'enregistrement DNS dynamique pour le dépannage et les mises à jour à distance

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access, y compris les utilisateurs mobiles GlobalProtect ❑ Version de Prisma Access minimale requise : 5.1 Innovation (version minimale du plan de données PAN-OS 11.2 requise)

Lorsqu'un utilisateur mobile se connecte à distance à Prisma Access à l'aide de l'agent GlobalProtect, la passerelle GlobalProtect attribue à l'utilisateur une adresse IP et un FQDN du terminal. Cependant, Prisma Access ne met pas à jour les serveurs DNS de votre entreprise avec ces informations. Puisque les serveurs DNS ne disposent pas de l'adresse IP et des informations de FQDN attribuées à l'utilisateur mobile, votre administrateur informatique et les applications de votre réseau ne peuvent pas identifier et mettre à jour les terminaux à distance avec le FQDN.

À l'aide de l'enregistrement DNS dynamique, vous pouvez intégrer Prisma Access avec les fournisseurs de gestion des adresses IP (IPAM) pour créer dynamiquement des enregistrements A et PTR dans les serveurs DNS à l'aide de nsupdate, offrant ainsi les avantages suivants :

- Intégration directe avec les principaux fournisseurs IPAM tels qu'InfoBlox, BlueCat et Windows.
- Les mises à jour DDNS sont effectuées à l'aide de la signature de transaction (TSIG) ou de Kerberos comme protocole d'authentification, ce qui garantit des mises à jour sécurisées de la base de données DNS.
- Les mises à jour DDNS en temps réel sont effectuées à partir de Prisma Access au serveur DNS à l'aide d'appels nsupdate groupés basés sur les événements de connexion et de déconnexion GlobalProtect. Ces mises à jour utilisent un service DDNS sur le nœud de traitement de la sécurité des utilisateurs mobiles (MU-SPN).

Après avoir configuré cette solution, vous pouvez effectuer les actions suivantes :

- Vous pouvez utiliser des outils logiciels tels que Microsoft Endpoint Configuration Manager (MECM) pour envoyer des mises à jour logicielles aux terminaux GlobalProtect.
- Le personnel informatique et le personnel du service d'assistance peuvent connecter et gérer le terminal GlobalProtect à l'aide du FQDN du périphérique.
- Vous pouvez mettre en place des applications client (telles que des applications bancaires) qui s'appuient sur des recherches inversées DNS pour autoriser l'accès à partir de terminaux GlobalProtect approuvés.

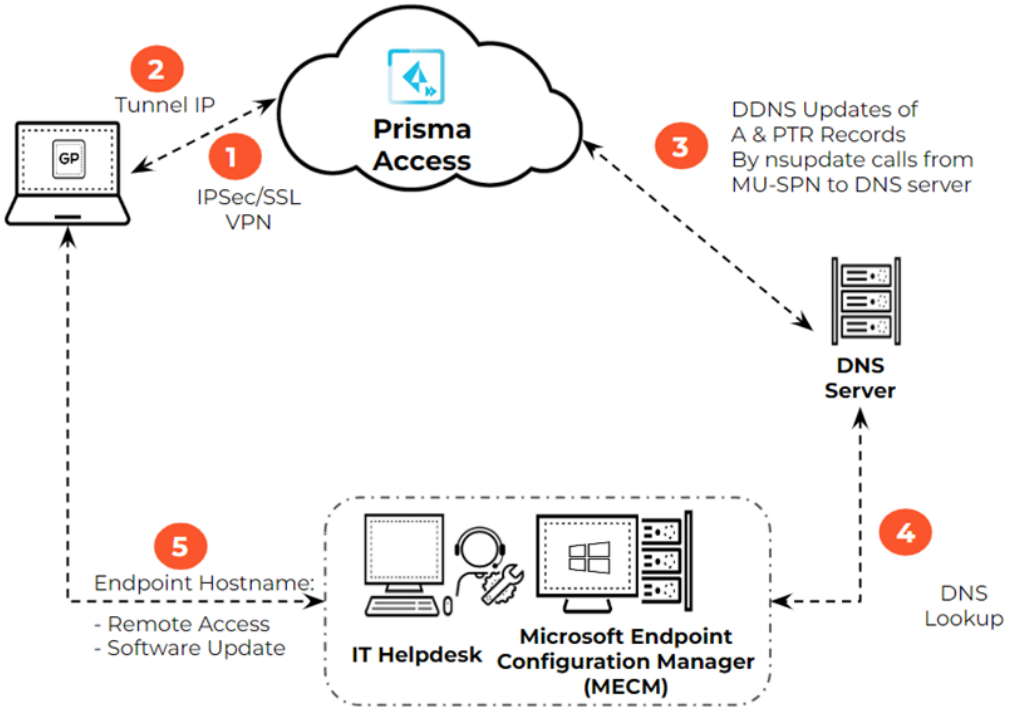
Cette solution DDNS n'est pas compatible avec la solution de prise en charge de l'enregistrement DNS dynamique pour les utilisateurs mobiles GlobalProtect qui utilise Strata Logging Service pour envoyer les mises à jour DDNS au serveur. Si vous avez mis en place la solution existante utilisant Strata Logging Service et que vous la déployez, Prisma Access utilise cette solution et désactive la solution existante à l'aide de Strata Logging Service.

 ©2025 Palo Alto Networks, Inc.

Cas d'utilisation de la prise en charge de l'enregistrement DNS dynamique

Le diagramme suivant illustre un cas d'utilisation typique de la solution DDNS Prisma Access. Dans cet exemple, vous souhaitez mettre à jour les terminaux GlobalProtect à l'aide de MECM ou souhaitez que le service d'assistance informatique puisse se connecter au terminal GlobalProtect à distance pour le dépannage.

1. GlobalProtect établit un tunnel SSL entre le terminal GlobalProtect et la passerelle Prisma Access.
2. GlobalProtect envoie le nom d'hôte, le nom de domaine et les informations d'adresse IP du tunnel de l'appareil de l'utilisateur mobile via le tunnel vers la passerelle sur site ou Prisma Access.
3. Prisma Access fournit des mises à jour DDNS des enregistrements A et PTR à l'aide de nsupdate au serveur DNS. Prisma Access fournit ces mises à jour sécurisées en temps réel lorsqu'il traite les événements de connexion et de déconnexion.
4. L'administrateur informatique ou un logiciel d'entreprise utilise ces enregistrements par le biais d'une recherche DNS ou RDNS et résout le nom du terminal ou l'adresse IP.
5. L'administrateur informatique ou le logiciel de gestion des terminaux utilise ces informations pour gérer le terminal ou envoyer des mises à jour logicielles.



Exigences en matière de connectivité réseau

Avant de mettre en œuvre cette solution, assurez-vous que votre réseau dispose des exigences suivantes :

©2025 Palo Alto Networks, Inc.

- Vous avez ajouté des itinéraires pour assurer la connectivité au serveur DNS à partir du MU-SPN et des connexions aux services Prisma Access.

  Pour ce faire, ajoutez des itinéraires à partir du sous-réseau d'infrastructure Prisma Access, que vous pouvez trouver dans **Workflows (Flux de travail)** > > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Infrastructure Subnet (Sous-réseau d'infrastructure)** et le pool d'adresses IP des utilisateurs mobiles GlobalProtect, que vous pouvez trouver dans **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **Client IP Pool (Pool d'adresses IP client)**.
- Vous avez établi la connectivité en créant une connexion aux services entre Prisma Access et le périphérique de terminaison IPSec (par exemple, un pare-feu ou un routeur nouvelle génération) qui dispose d'une connectivité au serveur DNS.
- Vous vous êtes assuré que votre serveur DNS est accessible via le tunnel IPSec de connexion aux services.
- Vous avez vérifié que les commandes nsupdate envoyées à partir des nœuds de traitement de sécurité (SPN) des utilisateurs mobiles GlobalProtect Prisma Access sont autorisées et peuvent atteindre le serveur DNS.

  Les étapes à suivre pour obtenir cette connectivité diffèrent en fonction de l'emplacement et du type de serveur DNS utilisé. Par exemple :

  - Si le serveur DNS se trouve dans le centre de données, vous pouvez configurer la connectivité à l'aide de tunnels IPSec à partir du SPN des utilisateurs mobiles GlobalProtect vers les connexions aux services, puis à partir de la connexion aux services vers le routeur de passerelle (par exemple, un pare-feu nouvelle génération configuré en tant que machine virtuelle) derrière lequel le serveur DNS existe.
  - Si le serveur DNS se trouve dans le cloud, vous pouvez obtenir la connectivité au serveur DNS à partir du SPN des utilisateurs mobiles GlobalProtect à l'aide des règles de politique de sécurité appropriées.
- Vous avez configuré des zones de recherche directe et inverse sur les serveurs DNS.
- Vous avez mis en place un serveur DNS Infoblox, Bluecat ou Windows qui prend en charge nsupdate.
- Si vous conservez individuellement les autorisations pour les zones, assurez-vous d'avoir créé des règles de politique de sécurité pour autoriser nsupdates à partir de périphériques disposant de la clé TSIG ou Kerberos correcte.

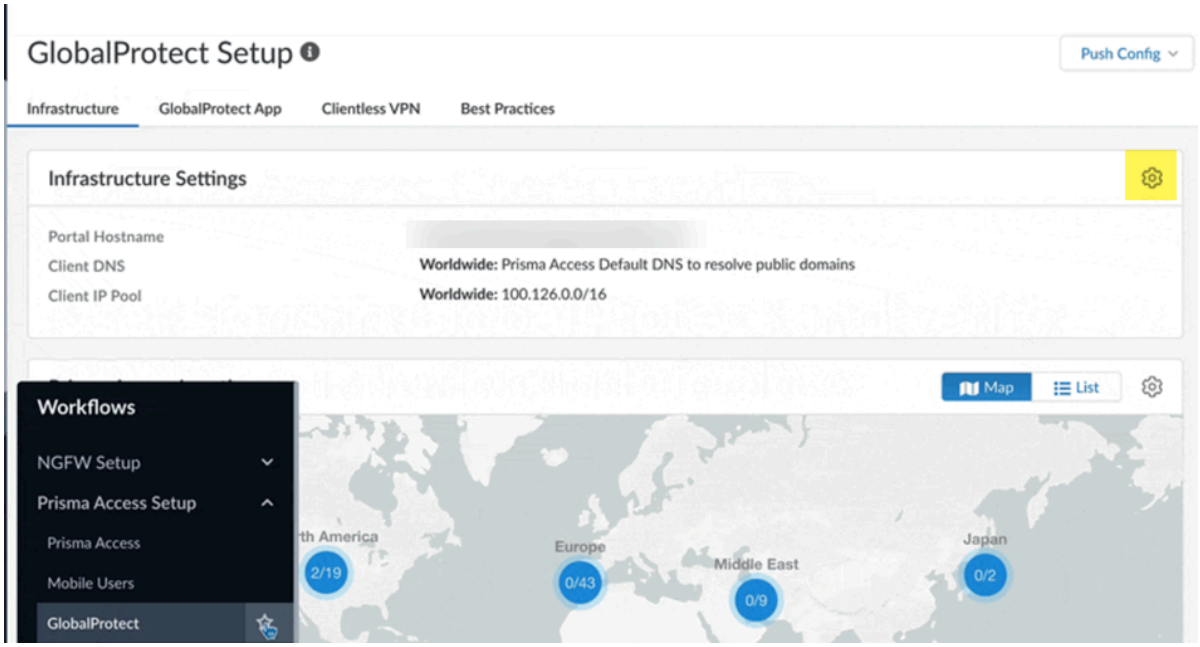
Pour configurer cette solution, utilisez l'une des procédures suivantes, en fonction de votre type de déploiement.

- Gestion du cloud
- Panorama

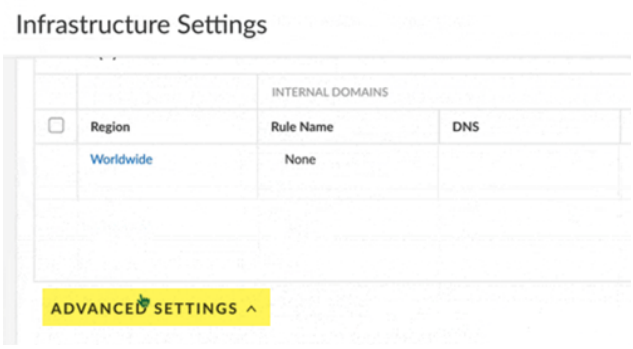
Configurer les mises à jour DNS dynamiques pour Prisma Access (Managed by Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Depuis Strata Cloud Manager, accédez à **Workflows (Flux de travail)** > **GlobalProtect** et cliquez sur l'engrenage pour modifier les **Infrastructure Settings (Paramètres d'infrastructure)**.



STEP 2 | Sélectionnez **Paramètres avancés**.



STEP 3 | Configurez les paramètres **Dynamic DNS Support (Support DNS dynamique)**.

1. Sélectionnez **Dynamic DNS Support for GlobalProtect (Support DNS dynamique pour GlobalProtect)**.
2. Sélectionnez le **Domain Type (Type de domaine)**.
   - **Fallback Domain (Domaine de repli)** : le domaine utilisé pour les événements nsupdate revient au domaine que vous spécifiez dans la zone **Fallback Domain (Domaine de repli)**. Utilisez cette option si les clients GlobalProtect ne sont joints à

 ©2025 Palo Alto Networks, Inc.

aucun domaine ou s'ils sont joints au même domaine que celui utilisé par le service DDNS pour mettre à jour les enregistrements sur le serveur DNS.

Si vous sélectionnez **Fallback Domain (Domaine de repli)** et que les utilisateurs qui ne sont pas connectés à un domaine se connectent à GlobalProtect, leurs informations sont ajoutées sous la zone de domaine de repli créée sur le serveur DNS.

Si les clients GlobalProtect qui se connectent à GlobalProtect appartiennent à un domaine inattendu qui n'est pas configuré sur le serveur DNS, nsupdate peut échouer. Dans ce cas, sélectionnez **Override Domain (Remplacer le domaine)** pour remplacer le domaine inconnu par le domaine connu du serveur DNS.

- **Override Domain (Remplacer le domaine)** : Prisma Access utilise uniquement le domaine que vous spécifiez pour mettre à jour le serveur DNS et remplace tous les autres domaines. Si des clients GlobalProtect se connectent à un autre domaine, le service DDNS utilise le domaine que vous spécifiez ici pour mettre à jour les enregistrements DNS A et PTR.

3. Sélectionnez le domaine utilisé pour mettre à jour les enregistrements PTR pour les domaines de repli ou de remplacement dans le champ **Fallback Domain (Domaine de repli)**.
4. Sélectionnez l'adresse **DNS Server IP (IP du serveur DNS)**.
5. Sélectionnez le **Server Type (Type de serveur)** (soit **TSIG** ou **Kerberos**).
6. (Déploiements TSIG uniquement) Sélectionnez la **TSIG Key (Clé TSIG)** à utiliser avec TSIG.

   Assurez-vous que le fichier TSIG est dans le bon format et que son type de fichier est .key.

   Si vous choisissez un type d'authentification Kerberos, chargez une clé d'authentification par le biais d'un fichier .key contenant le fichier keytab Kerberos non codé récupéré à partir du serveur DNS.

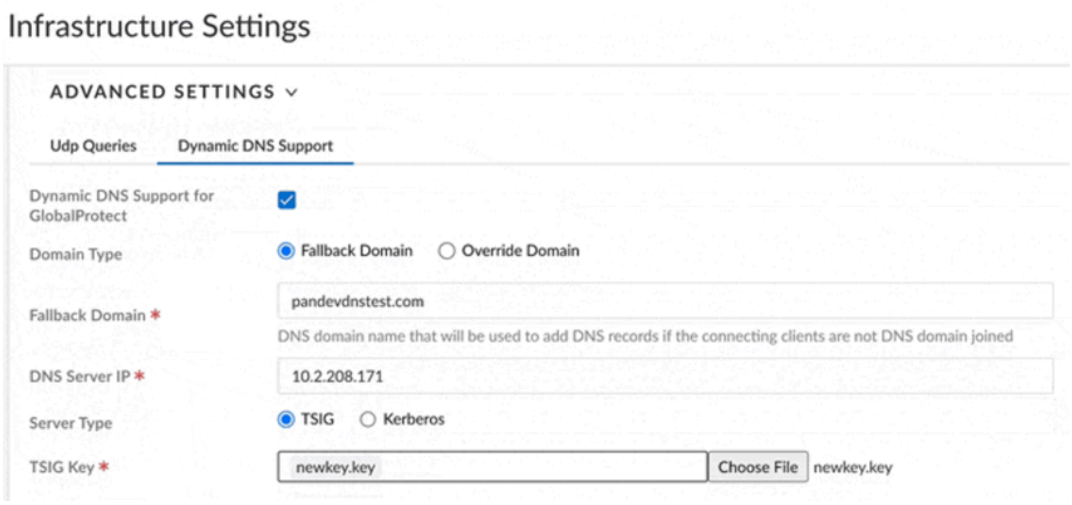
   Le fichier TSIG doit être au format suivant :

```
key "ddns-gp" { algorithm hmac-sha256; secret
 "aBCDEFGhiJklMNO89PQR+8stUVWX+YZAbcdeFgHI5J="; };
```

 ©2025 Palo Alto Networks, Inc.

7. (Déploiements Kerberos uniquement) Spécifiez les options Kerberos à utiliser.
   - Entrez l'adresse IP du **Kerberos Domain Controller (Contrôleur de domaine Kerberos)**.
   - Entrez l'adresse IP du **Kerberos Admin Server (Serveur d'administration Kerberos)**.
   - Entrez le **Kerberos User Name (Nom d'utilisateur Kerberos)**.
   - Entrez la **Kerberos Key (Clé Kerberos)** (le keytab) à utiliser.

     Assurez-vous que la clé Kerberos est au bon format.



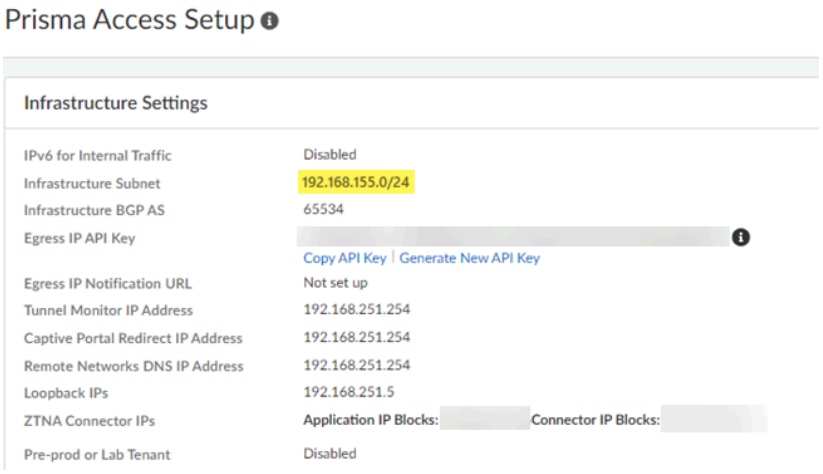
STEP 4 | Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

 ©2025 Palo Alto Networks, Inc.

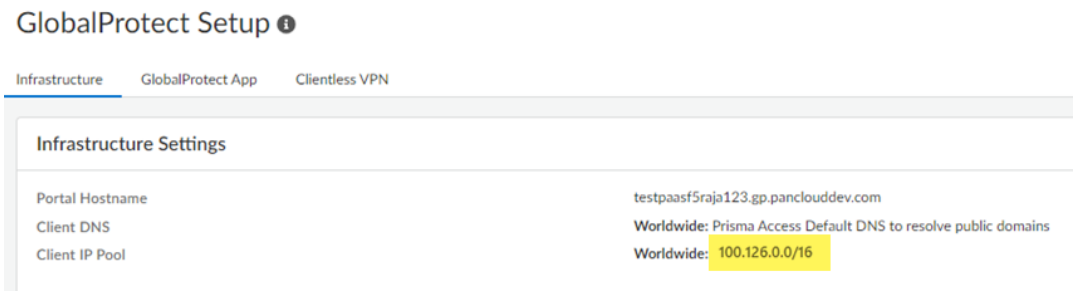
STEP 5 | Configurez des zones de recherche directe et inversée sur votre serveur DNS.

Reportez-vous à la documentation de votre fournisseur IPAM pour configurer ces zones. Pour cette étape, vous devez entrer le **Infrastructure Subnet (Sous-réseau d'infrastructure)** et le **Client IP Pool (Pool d'adresses IP du client)** de Prisma Access.

- Pour trouver le sous-réseau d'infrastructure, accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** et prenez note de l'**Infrastructure Subnet (Sous-réseau d'infrastructure)**.



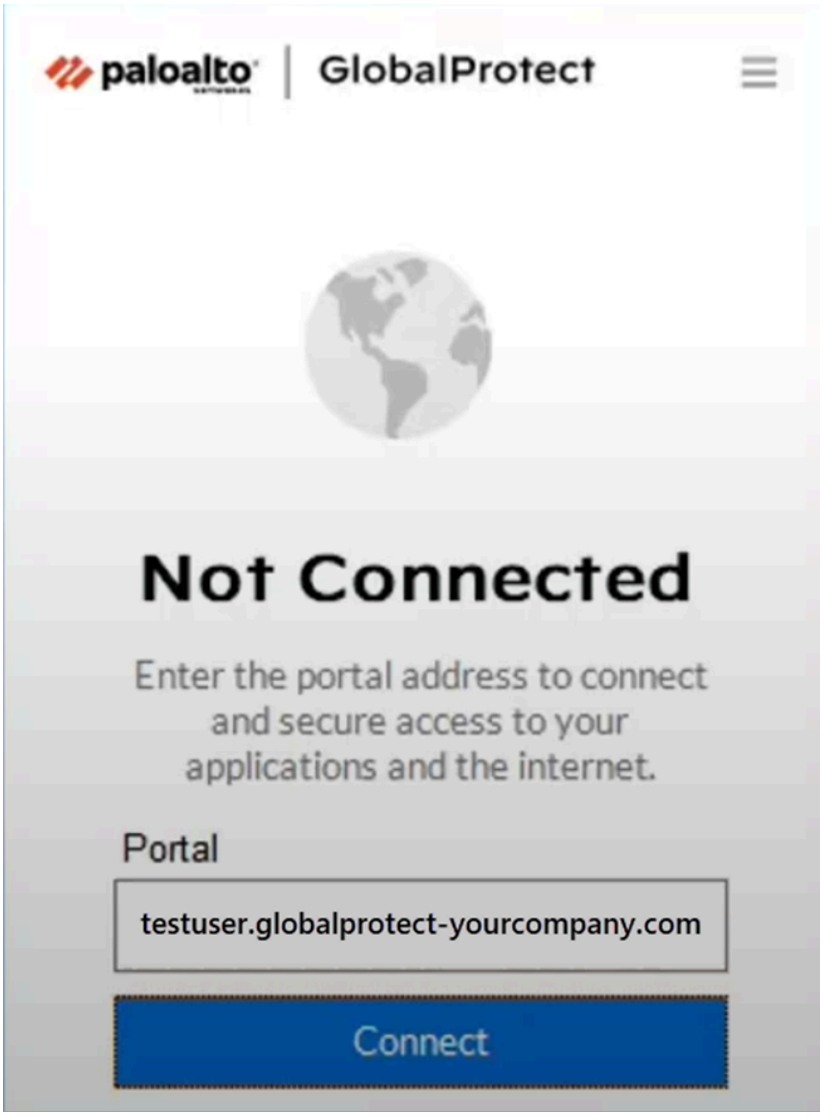
- Pour trouver le pool d'adresses IP des utilisateurs mobiles GlobalProtect, accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** et prenez note du **Client IP Pool (Pool d'adresses IP du client)**.



 ©2025 Palo Alto Networks, Inc.

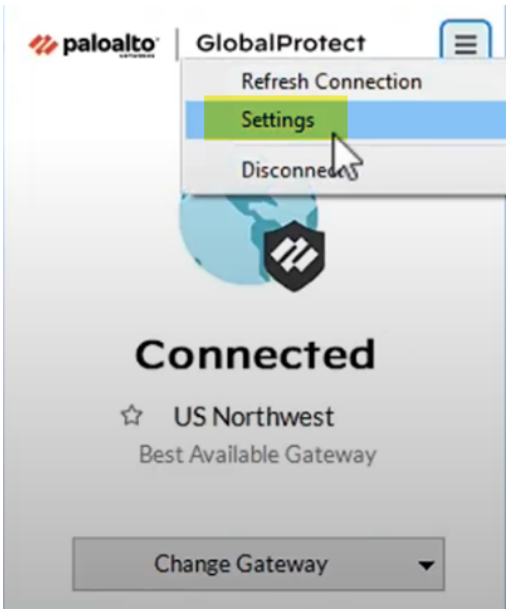
STEP 6 | Vérifiez que les enregistrements DNS sont mis à jour sur le serveur DNS IPAM.

1. Ouvrez une machine client et connectez-vous à une passerelle GlobalProtect Prisma Access.

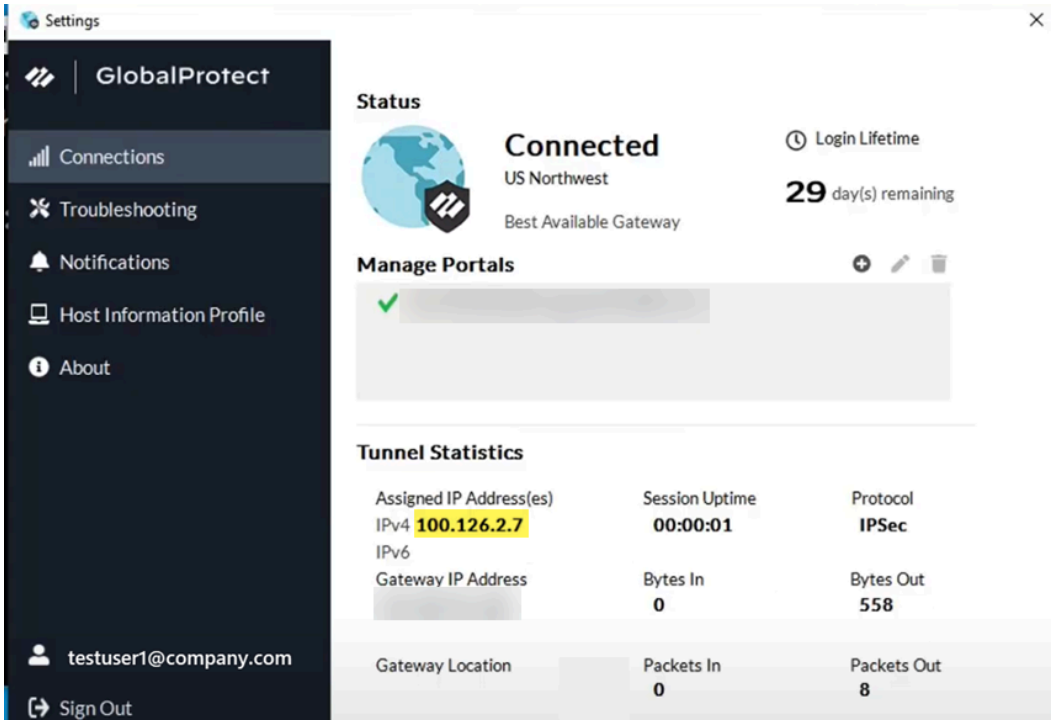


2. Sélectionnez **Settings (Paramètres)** GlobalProtect et vérifiez l'adresse IP GlobalProtect que Prisma Access a attribuée à l'utilisateur.

 ©2025 Palo Alto Networks, Inc.

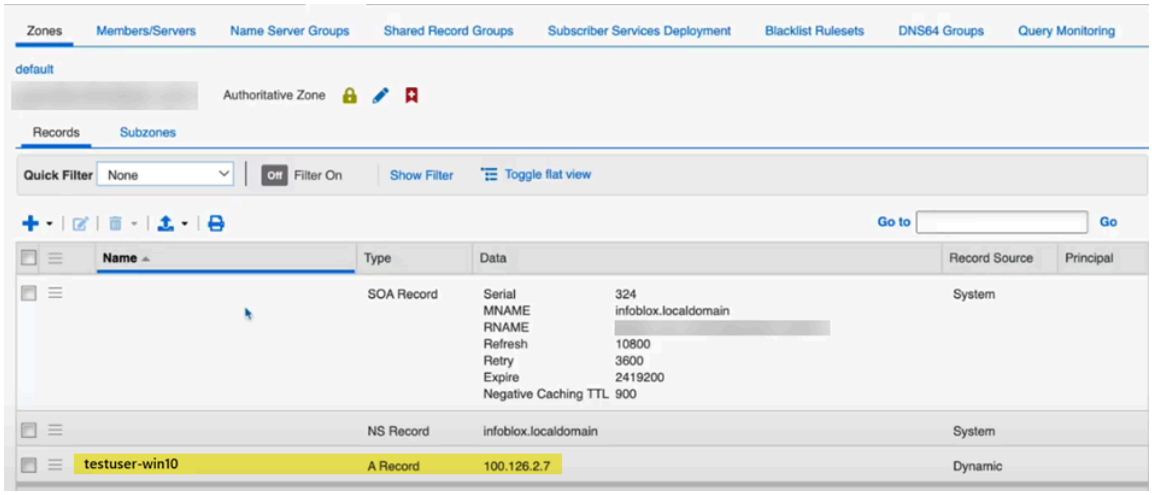


Les **Assigned IP Address(es) (Adresse(s) IP(s) attribuée(s))** (100.126.2.7) indiquent que l'adresse IP provient du pool d'adresses IP GlobalProtect (100.126.0.0/16).

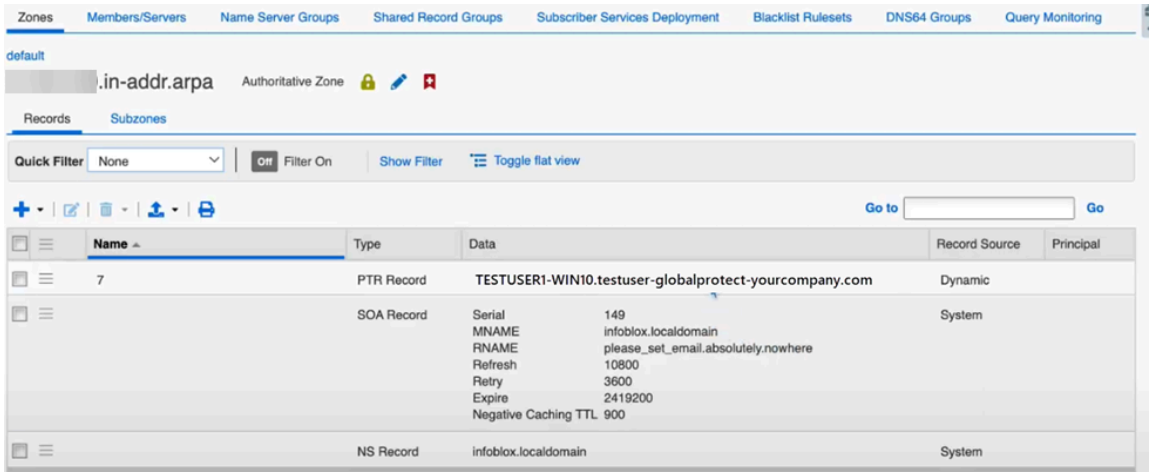


3. À partir du serveur DNS IPAM, affichez l'enregistrement de l'utilisateur.
   Dans cet exemple, l'utilisateur est nommé `testuser1-win10`.

 ©2025 Palo Alto Networks, Inc.



La recherche inversée DNS affiche également le nom d'utilisateur dans l'enregistrement PTR.



4. Déconnectez l'utilisateur de GlobalProtect et vérifiez les enregistrements pour vous assurer que le serveur DNS a supprimé les enregistrements de l'utilisateur.

Configurer les mises à jour DNS dynamiques pour Prisma Access (Managed by Panorama)

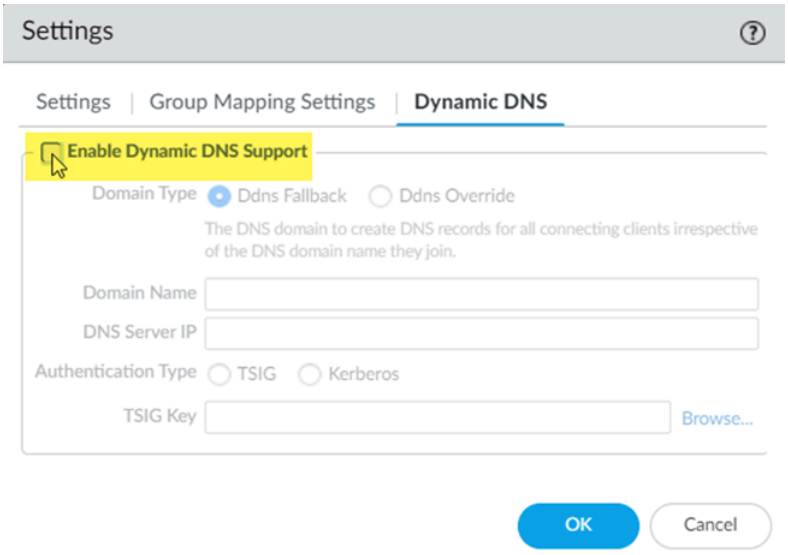
Pour configurer les mises à jour DNS dynamiques pour Prisma Access (Managed by Panorama), suivez ces étapes.

STEP 1 | Depuis Panorama, accédez à **Cloud Services** > **Configuration** > **Mobile Users—GlobalProtect (Utilisateurs mobiles — GlobalProtect)** et cliquez sur l'engrenage pour modifier les **Settings (Paramètres)**.

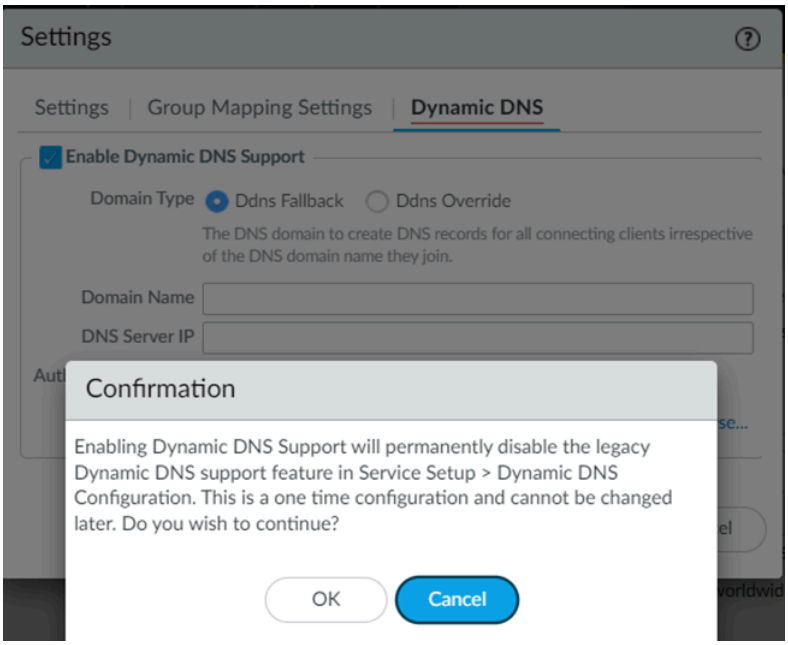
STEP 2 | Sélectionnez **Dynamic DNS (DNS dynamique)**.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Cliquez sur **Enable Dynamic DNS Support (Activer le support DNS dynamique)**.



STEP 4 | Vous êtes informé que, si le support DNS dynamique hérité est activé, l'activation du support mis à jour désactive définitivement le support hérité. Cliquez sur **OK** pour continuer.



STEP 5 | Configurez les paramètres **Dynamic DNS (DNS dynamique)**.

1. Sélectionnez **Enable Dynamic DNS Support (Activer le support DNS dynamique)**.
2. Sélectionnez le **Domain Type (Type de domaine)**.
   - **Ddns Fallback (Repli DDNS)** : le domaine utilisé pour les événements nsupdate revient au domaine que vous spécifiez dans la zone **Domain Name (Nom du domaine)**. Utilisez cette option si les clients GlobalProtect ne sont joints à aucun domaine ou s'ils

 ©2025 Palo Alto Networks, Inc.

sont joints au même domaine que celui utilisé par le service DDNS pour mettre à jour les enregistrements sur le serveur DNS.

Si vous sélectionnez **Ddns Fallback (Repli DDNS)** et que les utilisateurs qui ne sont pas connectés à un domaine se connectent à GlobalProtect, leurs informations sont ajoutées sous la zone de repli DDNS créée sur le serveur DNS.

Si les clients GlobalProtect qui se connectent à GlobalProtect appartiennent à un domaine inattendu qui n'est pas configuré sur le serveur DNS, nsupdate peut échouer. Dans ce cas, sélectionnez **DDNS Override (Remplacement DDNS)** pour remplacer le domaine inconnu par le domaine connu du serveur DNS.

- **Ddns Override (Remplacement DDNS)** : Prisma Access utilise uniquement le domaine que vous spécifiez pour mettre à jour le serveur DNS et remplace tous les autres domaines. Si des clients GlobalProtect se connectent à un autre domaine, le service DDNS utilise le domaine que vous spécifiez ici pour mettre à jour les enregistrements DNS A et PTR.

3. Sélectionnez le domaine utilisé pour mettre à jour les enregistrements PTR pour les replis ou les noms de domaines dans le champ **Domain Name (Nom de domaine)**.
4. Sélectionnez l'adresse **DNS Server IP (IP du serveur DNS)**.
5. Sélectionnez le **Authentication Type (Type d'authentification)** (soit **TSIG** ou **Kerberos**).
6. (Déploiements TSIG uniquement) Sélectionnez la **TSIG Key (Clé TSIG)** à utiliser avec TSIG.

   Assurez-vous que le fichier TSIG est au bon format et qu'il présente le type de fichier .key.

   - Si vous exécutez un déploiement géré par Panorama avec une version de plug-in 5.2.0 ou supérieure et que vous choisissez un type d'authentification Kerberos, chargez une clé d'authentification par le biais d'un fichier .key contenant la chaîne encodée en base64 de la clé Kerberos récupérée à partir du serveur DNS, par exemple : `"ABCDEFGHIJKLMNOPQRSTUV5WXYZOUy5DT00ADUFabcDluaXN0cmF0b3IAAAABAAAAAAEAE`
   - Si vous exécutez un déploiement géré par Panorama avec une version de plug-in inférieure à 5.1.0 et que vous choisissez un type d'authentification Kerberos, chargez une clé d'authentification via un fichier .key contenant le fichier keytab Kerberos non codé récupéré à partir du serveur DNS.

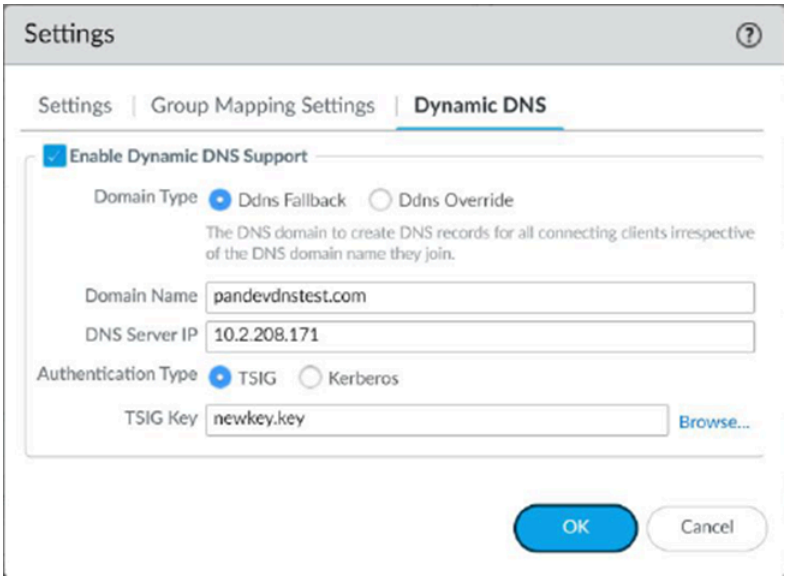
   Le fichier TSIG doit être au format suivant :

```
key "ddns-gp" { algorithm hmac-sha256; secret
 "aBCDEFGhiJklMNO89PQR+8stUVWX+YZAbcdeFgHI5J="; };
```

 ©2025 Palo Alto Networks, Inc.

7. (Déploiements Kerberos uniquement) Spécifiez les options Kerberos à utiliser.
   - Entrez l'adresse IP du **Kerberos Domain Controller (Contrôleur de domaine Kerberos)**.
   - Entrez l'adresse IP du **Kerberos Admin Server (Serveur d'administration Kerberos)**.
   - Entrez le **Kerberos User Name (Nom d'utilisateur Kerberos)**.
   - Entrez la **Kerberos Key (Clé Kerberos)** (le keytab) à utiliser.

     Utilisez l'encodage en base64 sur la clé Kerberos avant de la télécharger.



STEP 6 | Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

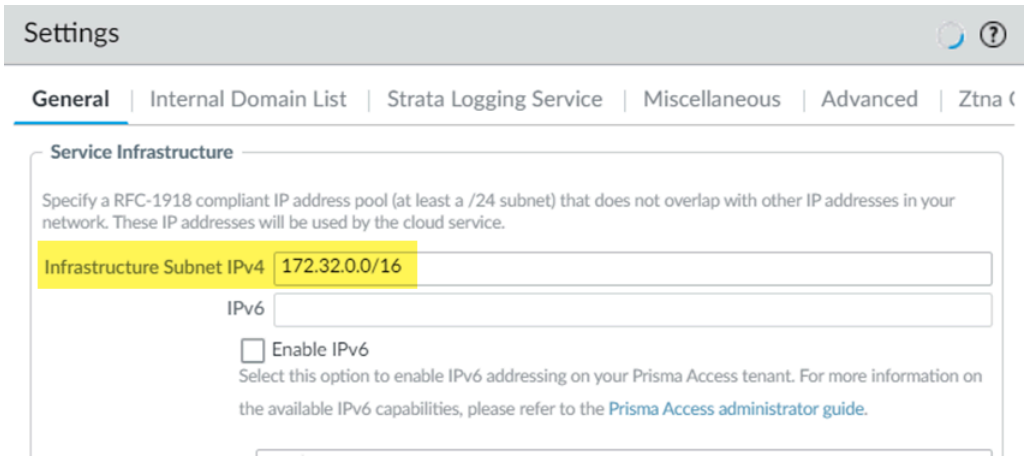
STEP 7 | Configurez des zones de recherche directe et inversée sur votre serveur DNS.

Reportez-vous à la documentation de votre fournisseur IPAM pour configurer ces zones. Pour cette étape, vous devez entrer le **Infrastructure Subnet (Sous-réseau d'infrastructure)** et le **Client IP Pool (Pool d'adresses IP du client)** de Prisma Access.

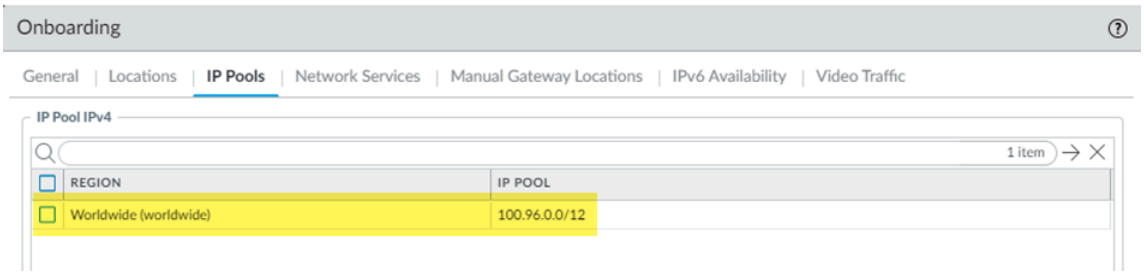
- Pour trouver le sous-réseau d'infrastructure, accédez à **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)**, cliquez sur l'engrenage pour

 ©2025 Palo Alto Networks, Inc.

modifier les **Settings (Paramètres)** et prenez note de l'**Infrastructure Subnet IPv4 (Sous-réseau d'infrastructure IPv4)**.



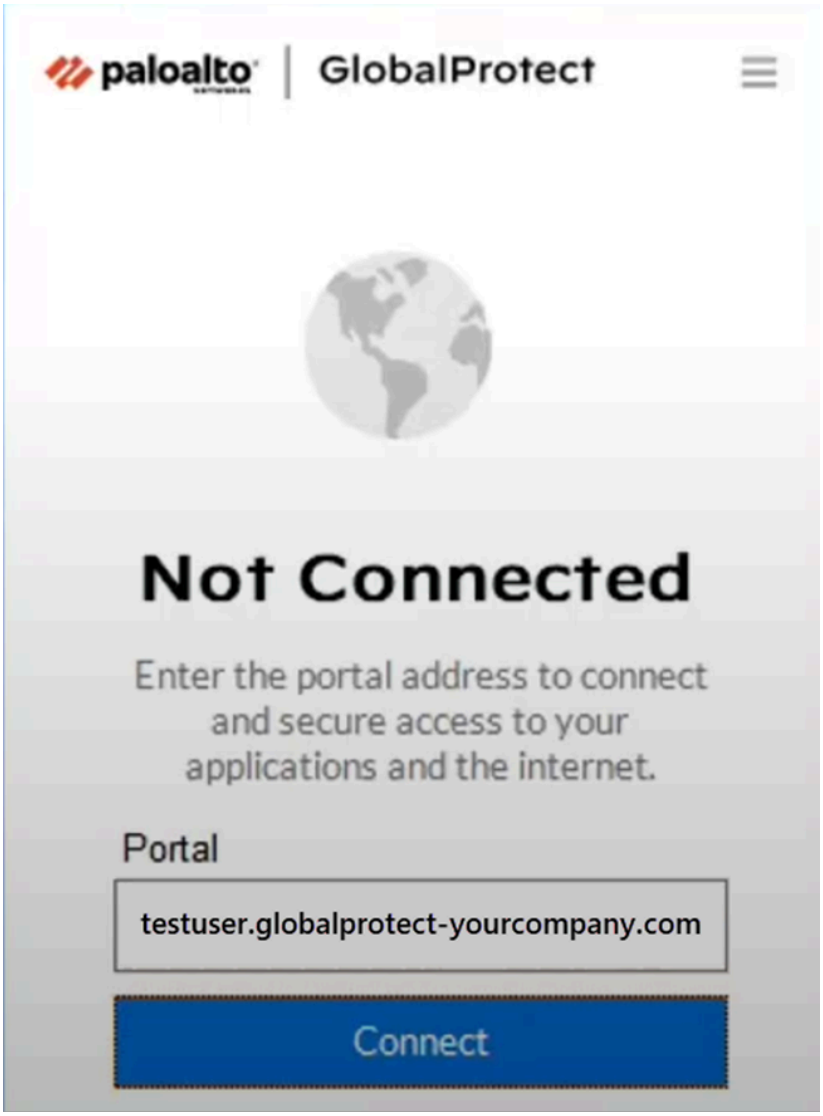
- Pour trouver le pool d'adresses IP des utilisateurs mobiles GlobalProtect, accédez à **Panorama** > **Cloud Services** > **Mobile Users—GlobalProtect (Utilisateurs mobiles — GlobalProtect)**, sélectionnez le **Hostname (Nom d'hôte)**, sélectionnez **IP Pools (Pools d'adresses IP)** et prenez note de l'**IP Pool IPv4 (Pool d'adresses IP IPv4)**.



 ©2025 Palo Alto Networks, Inc.

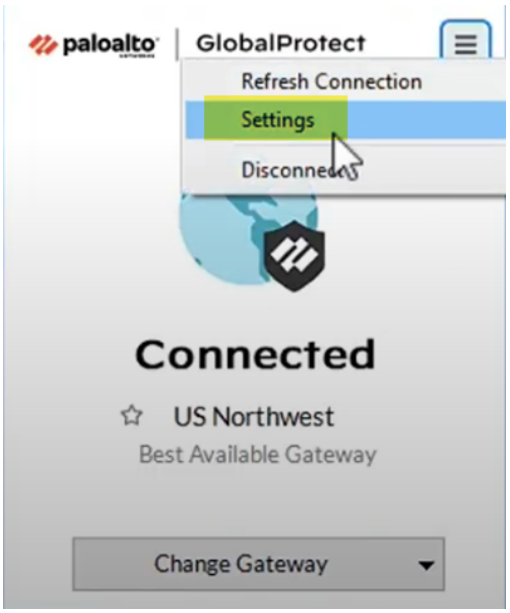
STEP 8 | Vérifiez que les enregistrements DNS sont mis à jour sur le serveur DNS IPAM.

1. Ouvrez une machine client et connectez-vous à une passerelle GlobalProtect Prisma Access.

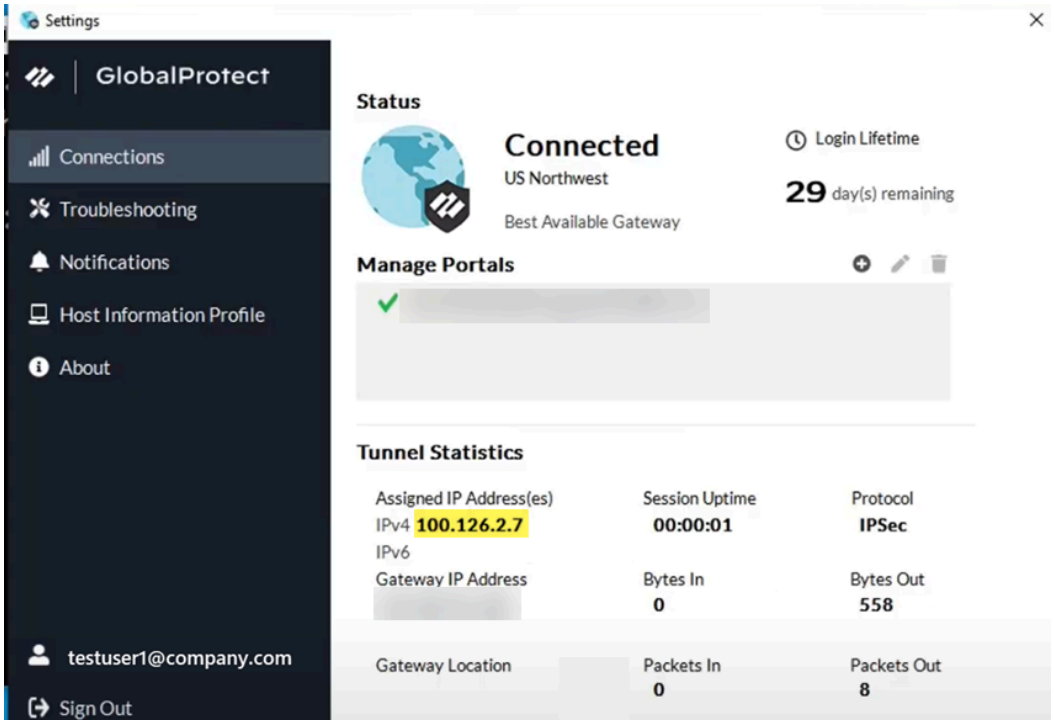


2. Sélectionnez **Settings (Paramètres)** GlobalProtect et vérifiez l'adresse IP GlobalProtect que Prisma Access a attribuée à l'utilisateur.

 ©2025 Palo Alto Networks, Inc.

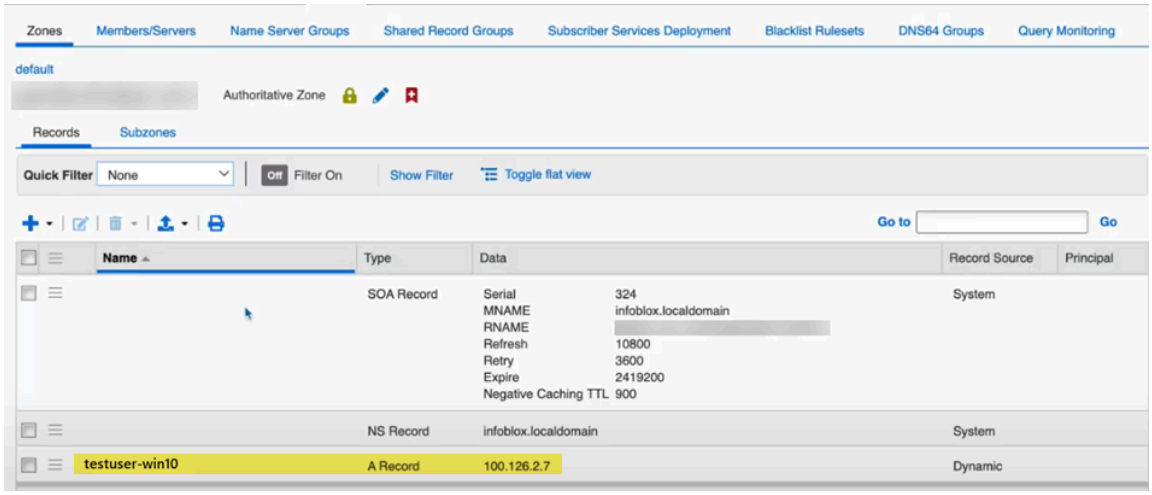


Les **Assigned IP Address(es) (Adresse(s) IP(s) attribuée(s))** (100.126.2.7) indiquent que l'adresse IP provient du pool d'adresses IP GlobalProtect (100.126.0.0/16).

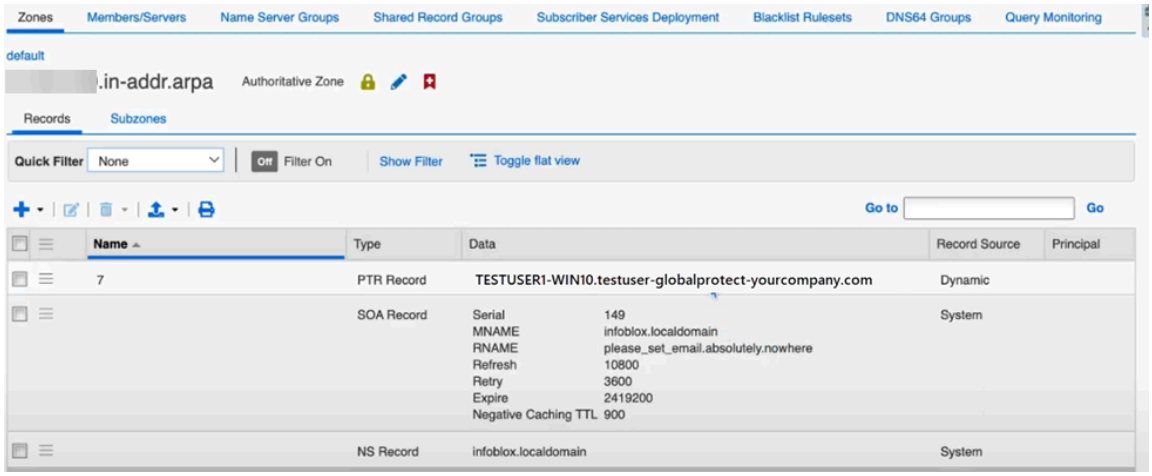


3. À partir du serveur DNS IPAM, affichez l'enregistrement de l'utilisateur.
   Dans cet exemple, l'utilisateur est nommé `testuser1-win10`.

 ©2025 Palo Alto Networks, Inc.



La recherche inversée DNS affiche également le nom d'utilisateur dans l'enregistrement PTR.



4. Déconnectez l'utilisateur de GlobalProtect et vérifiez les enregistrements pour vous assurer que le serveur DNS a supprimé les enregistrements de l'utilisateur.

Prise en charge de l'enregistrement DNS dynamique pour les utilisateurs mobiles – GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Pare-feu nouvelle génération gérés par Panorama avec une licence Strata Logging Service et un plug-in Cloud Services	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version : 3.1.1 préférée ou Innovation ❑ Pris en charge sur les Panoramas exécutant les versions 10.2 et ultérieures (non pris en charge sur les Panoramas exécutant la version 10.1)

 ©2025 Palo Alto Networks, Inc.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
	❑ Vos terminaux clients doivent être joints à un domaine.

Cette fonctionnalité est disponible pour les déploiements Prisma Access commençant par Prisma Access (Managed by Panorama) 3.1.1.

Cette fonctionnalité n'est pas disponible pour les déploiements Prisma Access (Managed by Strata Cloud Manager).

Lorsqu'un utilisateur mobile se connecte à distance à Prisma Access en utilisant GlobalProtect, les serveurs DNS de votre entreprise ne sont pas mis à jour avec l'adresse IP attribuée par la passerelle GlobalProtect. Avant d'activer le DNS dynamique (DDNS), il n'existe aucun mappage des adresses IP du tunnel avec le nom du terminal, qui sont enregistrées sous forme d'enregistrements d'adresse et de pointeur (A et PTR). Par conséquent, votre administrateur informatique ou votre logiciel de gestion des utilisateurs ne peut pas mapper le nom du terminal distant à l'adresse IP.

Après avoir activé la fonction DDNS sur Prisma Access, le plug-in Cloud Services Prisma Access vérifie les événements GlobalProtect dans Strata Logging Service toutes les 15 minutes pour capturer le nom d'hôte du terminal, le nom de domaine et l'adresse IP du tunnel. Il crée dynamiquement des enregistrements A et PTR dans le serveur DNS à l'aide de NSUPDATE.

Flux de travail du DNS dynamique pour les utilisateurs mobiles – GlobalProtect

Après avoir activé DDNS et lorsqu'un utilisateur mobile se connecte avec l'application GlobalProtect :

Lisez les sections suivantes pour avoir un aperçu du fonctionnement du DDNS, des directives et des exigences, et de son activation.

1. GlobalProtect établit un tunnel SSL entre le terminal GlobalProtect et une passerelle sur site ou Prisma Access.
2. GlobalProtect envoie le nom d'hôte, le nom de domaine et les informations d'adresse IP du tunnel du périphérique de l'utilisateur mobile via le tunnel vers la passerelle sur site ou Prisma Access.
3. La passerelle sur site ou Prisma Access transmet ces informations sous forme d'événements GlobalProtect à Strata Logging Service.
4. Le plug-in Cloud Services Prisma Access sonde Strata Logging Service toutes les 15 minutes pour mettre à jour le serveur DNS.

   Si le plug-in ne reçoit pas les événements GlobalProtect de Strata Logging Service, il réessaye la requête cinq fois maximum. Si les requêtes de nouvelle tentative n'ont pas abouti, le plug-in réessaye l'opération toutes les 15 minutes, quatre fois maximum. Par conséquent, le plug-in peut recevoir des mises à jour pendant un intervalle de temps d'une heure.

   Si vous souhaitez des mises à jour plus fréquentes, vous pouvez entrer la commande `debug plugins cloud_services set-gp-ddns-interval` pour modifier l'intervalle de mise à jour à cinq minutes. L'enregistrement A n'est pas tenu de mettre à jour l'intervalle de temps. Si vous modifiez l'intervalle à cinq minutes, le plug-in Cloud Services peut mettre à jour un maximum de 15 000 enregistrements avec une latence réseau de 50 ms et peut recevoir des mises à jour pendant un intervalle de temps de 20 minutes.

 ©2025 Palo Alto Networks, Inc.

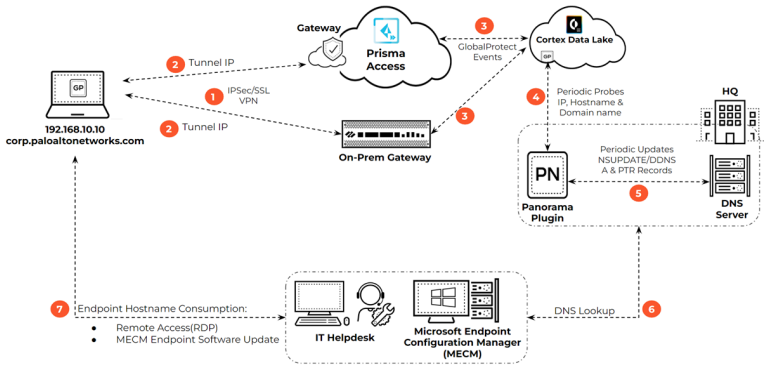
- *Aucune **Commit (Validation)** n'est requise après avoir modifié l'intervalle de temps à l'aide de la commande.*
- *Ces chiffres proviennent d'un environnement contrôlé et les conditions de fonctionnement réelles peuvent affecter ces chiffres.*

5. Après avoir reçu les mises à jour de Strata Logging Service, le plug-in Cloud Services regroupe les enregistrements A et PTR sous la forme NSUPDATE et met à jour le serveur DNS principal toutes les 15 minutes.

   Si vous avez modifié l'intervalle de temps à cinq minutes à l'aide de la commande `debug plugins cloud_services set-gp-ddns-interval`, le plug-in met à jour le serveur DNS toutes les cinq minutes.

   Si le plug-in ne parvient pas à mettre à jour le serveur DNS via NSUPDATE, le plug-in réessaye l'opération de mise à jour cinq fois maximum. Si les mises à jour n'ont pas réussi, le plug-in réessaye l'opération de mise à jour toutes les 15 minutes, ou toutes les cinq minutes si vous avez modifié l'intervalle à cinq minutes, quatre fois maximum. Par conséquent, le plug-in essaie de mettre à jour les événements enregistrés pendant une heure maximum (si vous utilisez un intervalle de 15 minutes) ou 20 minutes (si vous utilisez un intervalle de cinq minutes), après quoi il redémarre.
6. Une fois que les enregistrements A et PTR des utilisateurs mobiles GlobalProtect sont disponibles sur le serveur DNS, un administrateur informatique ou un logiciel d'entreprise utilise ces enregistrements via une recherche DNS ou RDNS et résout le nom du terminal ou l'adresse IP.
7. L'administrateur informatique ou le logiciel de gestion des terminaux utilise ces informations pour gérer le terminal ou envoyer des mises à jour logicielles.

La figure suivante illustre ce flux de travail.



*Pour afficher les journaux d'échec de connexion, sélectionnez **Dashboard (Tableau de bord)** > **System Logs (Journaux système)** ou **Monitor (Surveiller)** > **Logs (Journaux)** > **System (Système)** pour **Mobile_User_Device_Group**.*

Directives et exigences relatives au DNS dynamique

Avant d'activer le DDNS, assurez-vous que votre déploiement et votre serveur DNS répondent aux directives et exigences suivantes :

- Vos terminaux clients doivent être joints à un domaine.

 ©2025 Palo Alto Networks, Inc.

- Mettez à jour votre client GlobalProtect vers les versions d'application GlobalProtect suivantes en fonction de votre système d'exploitation :
  - Windows : 5.2.11 ou version ultérieure
  - Mac : 5.2.11 ou version ultérieure
  - Linux : 5.3.3 ou version ultérieure
- Activez Strata Logging Service si vous utilisez une passerelle sur site autre que Prisma Access.
- Un serveur DNS Infoblox avec une version minimale de 8.6.1 ou ultérieure prenant en charge les mises à jour DDNS via NSUPDATE est requis.
- Les déploiements Prisma Access multilocataires ne prennent pas en charge le DDNS.
- Enregistrez la clé d'authentification de votre serveur DNS au format base64 avec une extension de fichier .key. Vous pouvez télécharger la clé uniquement dans ce format dans Prisma Access.
- Activez NTP sur votre serveur DNS et assurez-vous qu'il est identique à celui de Prisma Access.
- Créez des zones dans Infoblox pour les adresses PTR inversées et les adresses A transférées.

Vous pouvez déployer le DNS dynamique dans un déploiement autonome avec des pare-feu nouvelle génération ainsi qu'avec Prisma Access. Pour les pare-feu, toutes les conditions préalables de cette section s'appliquent et vous devez également disposer d'une licence Strata Logging Service valide et utiliser le plug-in Cloud Services dans Panorama *pour la journalisation.*

Activer le DDNS pour les déploiements d'utilisateurs mobiles GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Pour mettre à jour votre serveur DNS avec les enregistrements A et PTR de vos utilisateurs mobiles GlobalProtect, procédez comme suit.

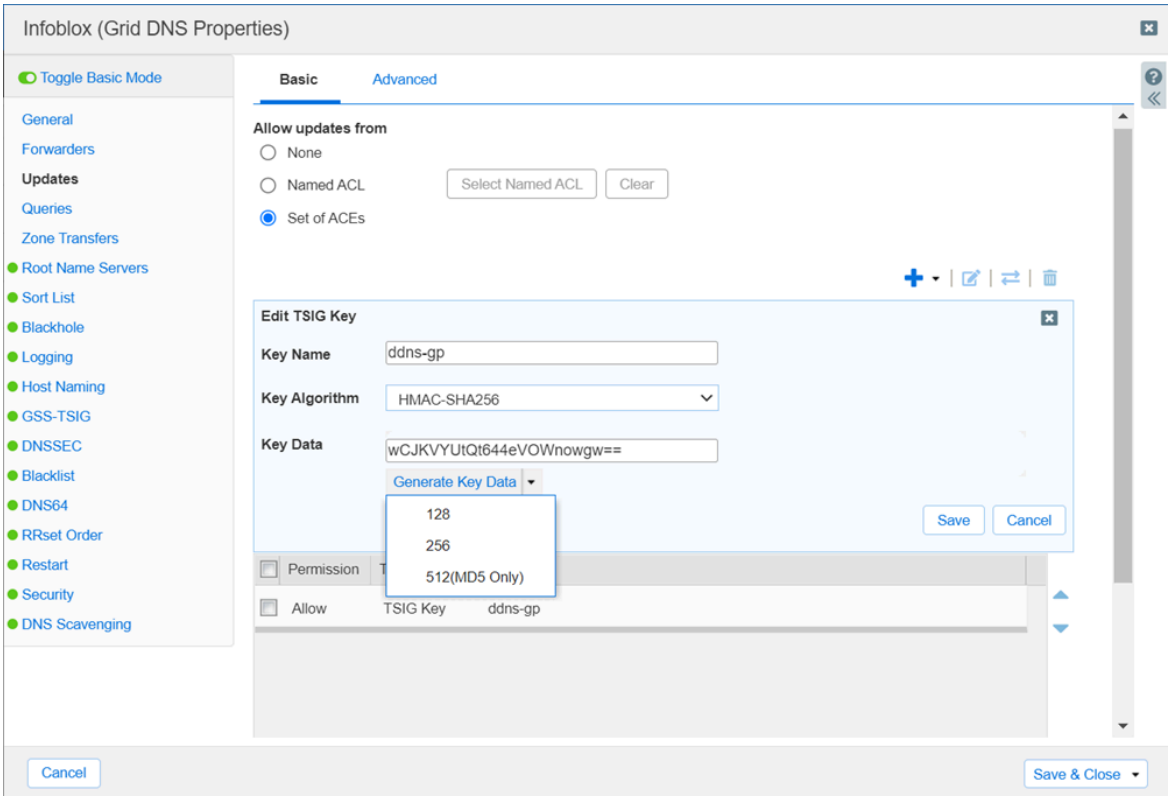
 ©2025 Palo Alto Networks, Inc.

STEP 1 | Créez une clé d'authentification dans votre serveur DNS.

Cet exemple utilise Infoblox en tant que serveur DNS.

1. Connectez-vous à votre serveur DNS.
2. Sélectionnez **Data Management (Gestion des données)** > **DNS** > **Grid DNS Properties (Propriétés DNS de la grille)** > **Updates (Mises à jour)**.
3. Autorisez les mises à jour à partir de **Set of ACEs (Ensemble d'ACE)**.
4. Ajoutez une **TSIG Key (Clé TSIG)** après avoir rempli les détails.

   - *Sélectionnez l'algorithme de la clé **256**.*
   - *Cliquez sur **Generate Key Data (Générer les données de la clé)** pour créer une nouvelle clé. Sélectionnez les données de la clé **256**.*



5. Copiez les données de la clé dans un fichier au format suivant et enregistrez le fichier avec l'extension .key.

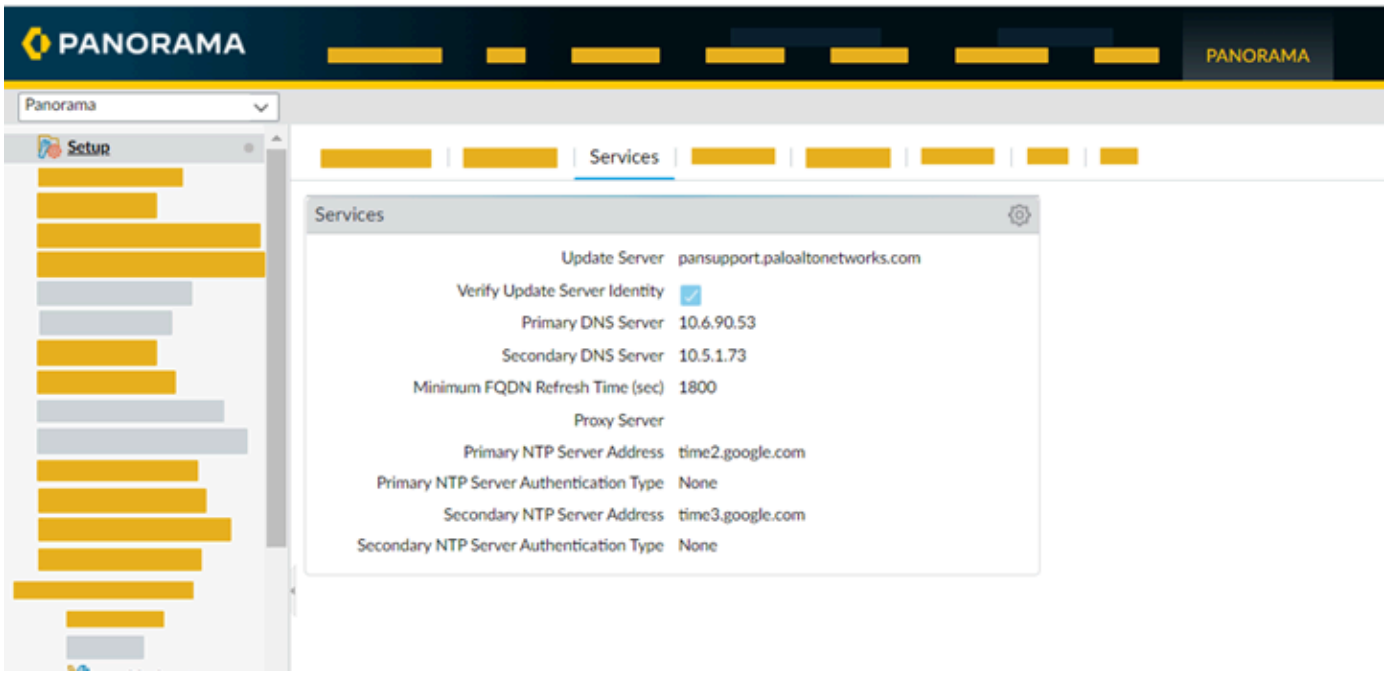
```
key "ddns-gp" { algorithm hmac-sha256; secret
 "wCJKVYUtQt644eVOWnowgw==";  };
```

Téléchargez cette clé sur Cloud Prisma Access Services dans une étape ultérieure.

 ©2025 Palo Alto Networks, Inc.

STEP 2 | Dans votre déploiement Prisma Access, spécifiez votre serveur DNS comme serveur DNS principal.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Services**.
2. Cliquez sur **Edit (Éditer)** pour éditer les paramètres et mettez à jour les détails du serveur DNS principal.

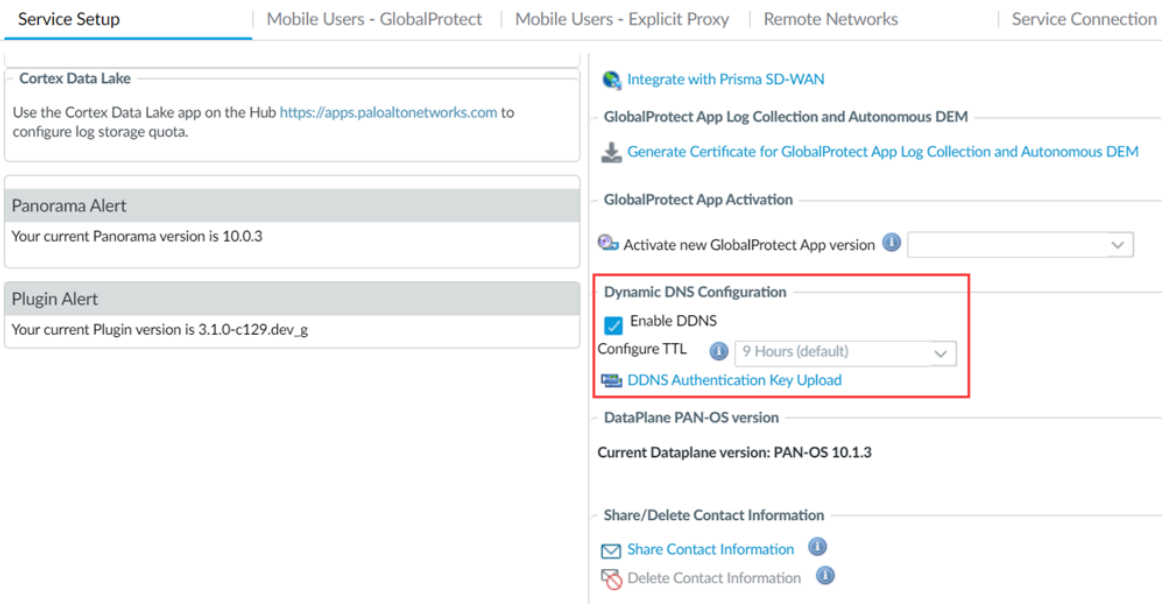


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Configurez les paramètres DDNS.

1. Sélectionnez **Panorama** > **Cloud Services (Services Cloud)** > **Configuration** > **Service Setup (Configuration du service)**.
2. Sélectionnez **Service Operations (Opérations du service)** > **Dynamic DNS Configuration (Configuration du DNS dynamique)** et **Enable DDNS (Activer le DDNS)**.
3. (Facultatif) Cliquez sur **Configure TTL (Configurer la durée de vie)**, qui est la valeur de durée de vie (TTL), à la fréquence à laquelle vous souhaitez que Prisma Access actualise le FDQN dans son cache.

   La valeur est définie sur 9 heures par défaut.



4. Téléchargez la clé d'authentification DDNS que vous avez créée à l'étape 1 depuis votre serveur DNS.

STEP 4 | **Commit to Panorama (Validez sur Panorama)**.

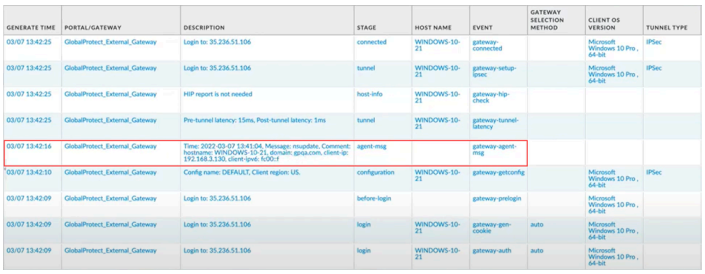
Vérifier la configuration DNS dynamique

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Panorama	• Licence Prisma Access

Une fois que vous avez activé DDNS, surveillez les journaux et résolvez les problèmes en vérifiant les composants Prisma Access suivants.

Sélectionnez **Monitor (Surveiller)** > **Logs (Journaux)** > **GlobalProtect**. Le message de l'agent de passerelle contient le nom d'hôte, le nom de domaine et l'adresse IP du tunnel. GlobalProtect envoie le message de l'agent uniquement si le terminal fait partie d'un domaine ou d'un AD.

 ©2025 Palo Alto Networks, Inc.



GENERATE TIME	PORTAL/GATEWAY	DESCRIPTION	STAGE	HOST NAME	EVENT	GATEWAY SELECTION METHOD	CLIENT OS VERSION	TUNNEL TYPE
03/07 13:42:25	GlobalProtect_External_Gateway	Login to: 35.236.51.106	connected	WINDOWS-10-21	gateway-connected		Microsoft Windows 10 Pro , 64-bit	IPSec
03/07 13:42:25	GlobalProtect_External_Gateway	Login to: 35.236.51.106	tunnel	WINDOWS-10-21	gateway-setup-ipsec		Microsoft Windows 10 Pro , 64-bit	IPSec
03/07 13:42:25	GlobalProtect_External_Gateway	HIP report is not needed	host-info	WINDOWS-10-21	gateway-hip-check			
03/07 13:42:25	GlobalProtect_External_Gateway	Pre-tunnel latency: 15ms, Post-tunnel latency: 1ms	tunnel	WINDOWS-10-21	gateway-tunnel-latency			
03/07 13:42:16	GlobalProtect_External_Gateway	Time: 2022-03-07 13:41:04, Message: msupdate, Comment: hostname: WINDOWS-10-21, domain: gpqa.com, client-ip: 192.168.3.130, client-ipv6: fc00:f	agent-msg		gateway-agent-msg			
03/07 13:42:10	GlobalProtect_External_Gateway	Config name: DEFAULT, Client region: US.	configuration	WINDOWS-10-21	gateway-getconfig		Microsoft Windows 10 Pro , 64-bit	IPSec
03/07 13:42:09	GlobalProtect_External_Gateway	Login to: 35.236.51.106	before-login		gateway-prelogin		Microsoft Windows 10 Pro , 64-bit	
03/07 13:42:09	GlobalProtect_External_Gateway	Login to: 35.236.51.106	login	WINDOWS-10-21	gateway-gen-cookie	auto	Microsoft Windows 10 Pro , 64-bit	
03/07 13:42:09	GlobalProtect_External_Gateway	Login to: 35.236.51.106	login	WINDOWS-10-21	gateway-auth	auto	Microsoft Windows 10 Pro , 64-bit	

Vérifiez la commande `gp_ddns_support.log` dans la CLI de Panorama pour afficher d'autres journaux DDNS.

Identification et mise en quarantaine des périphériques compromis dans un déploiement GlobalProtect Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access

Prisma Access vous permet d'identifier et de mettre en quarantaine les périphériques compromis qui sont connectés à l'application GlobalProtect. Pour ce faire, vous pouvez ajouter manuellement ou automatiquement des périphériques à une liste de quarantaine. Après avoir mis le périphérique en quarantaine, vous pouvez empêcher le périphérique mis en quarantaine d'accéder au réseau pour garantir une politique cohérente.

Chaque emplacement d'utilisateur mobile Prisma Access envoie et reçoit ses informations de quarantaine entre le Panorama qui gère Prisma Access et sa connexion aux services la plus proche. Si vous disposez de pare-feu ou de passerelles nouvelle génération, vous devez demander à la connexion aux services de redistribuer les informations de la liste de quarantaine vers et depuis Panorama et les pare-feu ou passerelles sur site. Vous devez également redistribuer les informations de la liste de quarantaine de Panorama vers la connexion aux services afin de garantir une application cohérente des politiques pour tous les emplacements d'utilisateurs mobiles (passerelles) dans Prisma Access.

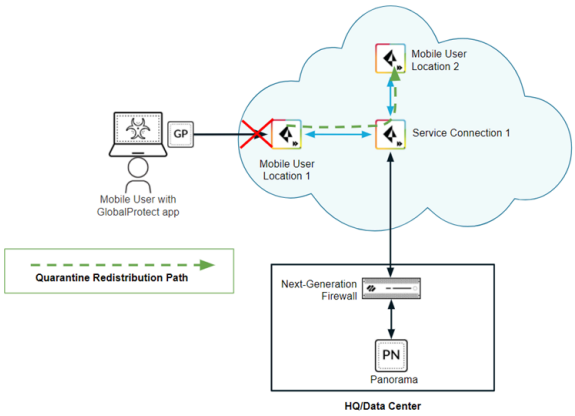
Cas d'utilisation pour la redistribution de la liste de quarantaine

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access

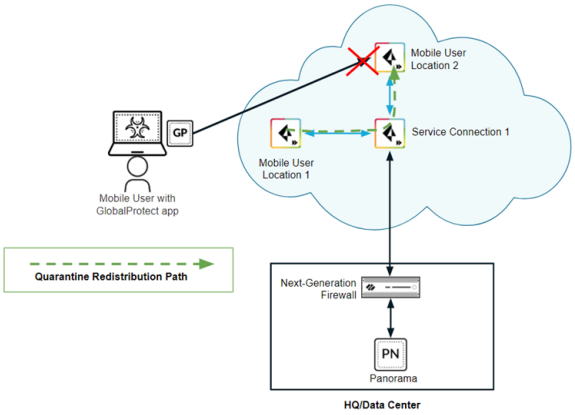
La section suivante décrit certains déploiements Prisma Access courants, où la redistribution de la liste de quarantaine est utile pour l'application cohérente des politiques pour les périphériques compromis.

 ©2025 Palo Alto Networks, Inc.

- **Redistribution de la liste de quarantaine entre les emplacements d'utilisateurs mobiles connectés à la même connexion aux services** : dans l'exemple suivant, un utilisateur mobile GlobalProtect connecté à l'emplacement d'utilisateur mobile 1 est compromis et est mis en quarantaine automatiquement. Prisma Access bloque ou restreint le périphérique mis en quarantaine conformément à la politique.



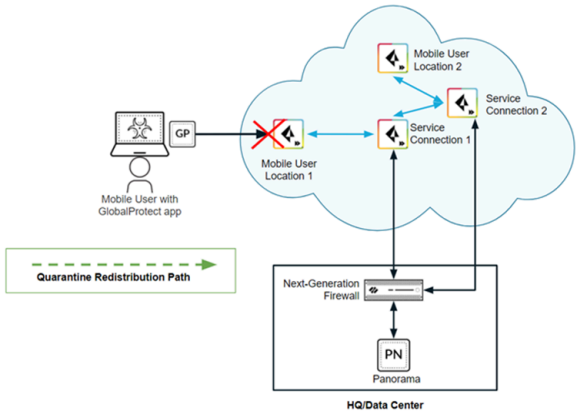
Une connexion aux services (connexion aux services 1 dans cet exemple) redistribue les informations de la liste de quarantaine entre tous les emplacements d'utilisateurs mobiles auxquels elle est connectée. Étant donné que l'emplacement d'utilisateur mobile 2 reçoit les informations de la liste de quarantaine redistribuées via la connexion aux services 1, la tentative de connexion de l'utilisateur mobile GlobalProtect à l'emplacement d'utilisateur mobile 2 est également bloquée.



- **Redistribution de la liste de quarantaine entre les emplacements d'utilisateurs mobiles connectés à différentes connexions aux services** : dans l'exemple suivant, il existe deux emplacements d'utilisateurs mobiles, mais ils se connectent à deux connexions aux services différentes. Un utilisateur GlobalProtect a tenté de se connecter à l'emplacement d'utilisateur

 ©2025 Palo Alto Networks, Inc.

mobile 1. L'emplacement d'utilisateur mobile 1 détecte le terminal utilisateur GlobalProtect comme compromis et le met en quarantaine.

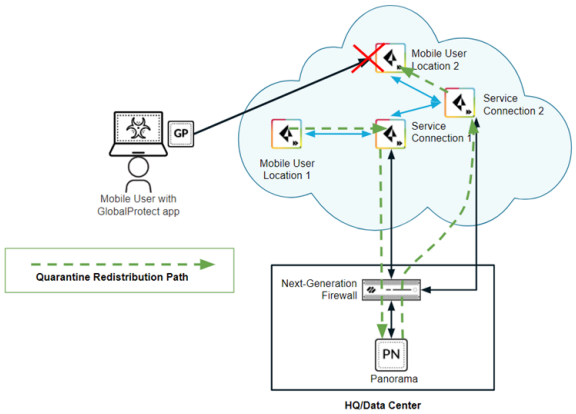


Pour redistribuer les informations de la liste de quarantaine de l'emplacement d'utilisateur mobile 1 vers l'emplacement d'utilisateur mobile 2, effectuez les actions suivantes :

- Redistribuez les informations de la liste de quarantaine de la connexion aux services 1 à Panorama.
- Redistribuez les informations de la liste de quarantaine de Panorama vers la connexion aux services 2.

Avec cette configuration, lorsque l'utilisateur GlobalProtect se connecte à l'emplacement d'utilisateur mobile 1 et est mis en quarantaine, les informations de la liste de quarantaine sont redistribuées de l'emplacement d'utilisateur mobile 1 à l'emplacement d'utilisateur mobile 2 et toutes les tentatives de connexion à l'emplacement d'utilisateur mobile 2 sont bloquées.

Cette configuration est également valide si l'utilisateur GlobalProtect se connecte à l'emplacement d'utilisateur mobile 2 et est mis en quarantaine ; les informations de la liste de quarantaine sont redistribuées de l'emplacement d'utilisateur mobile 2 vers l'emplacement d'utilisateur mobile 1.



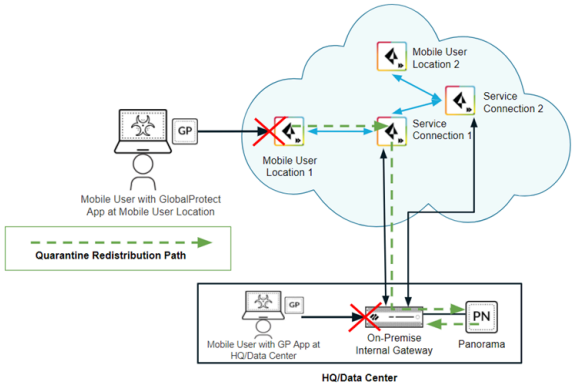
- **Redistribution de la liste de quarantaine entre Prisma Access et un pare-feu ou une passerelle nouvelle génération** : sans l'exemple suivant, un utilisateur GlobalProtect a tenté de se connecter à l'emplacement d'utilisateur mobile 1. L'emplacement d'utilisateur mobile 1 détecte le terminal utilisateur GlobalProtect comme compromis et le met en quarantaine. L'utilisateur mobile se rend ensuite au siège de l'entreprise et tente de se connecter à nouveau. Le siège

 ©2025 Palo Alto Networks, Inc.

social est protégé par un pare-feu nouvelle génération configuré comme une passerelle GlobalProtect utilisant la détection d'hôte interne.

L'emplacement d'utilisateur mobile 1 redistribue les informations de la liste de quarantaine à Panorama via la connexion au service 1, et Panorama redistribue les informations de la liste de quarantaine à la passerelle interne locale. Lorsque l'utilisateur tente de se connecter à partir du siège social, GlobalProtect détecte que la passerelle locale est configurée comme passerelle interne et se connecte à la passerelle sans tunnel.

Étant donné que les informations de la liste de quarantaine ont été redistribuées à la passerelle locale, l'utilisateur est bloqué au niveau de la passerelle en fonction des politiques utilisateur configurées.



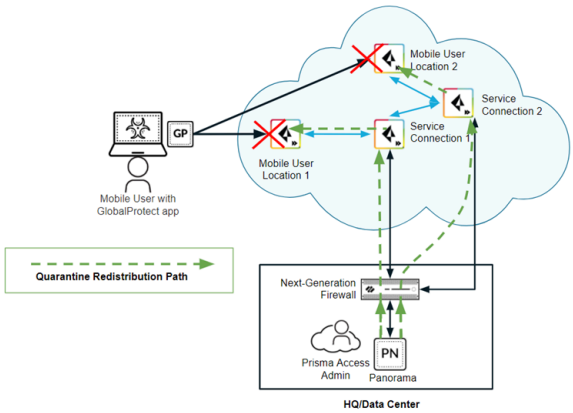
Si vous utilisez un pare-feu ou une passerelle nouvelle génération avec Prisma Access, vous devez configurer Panorama pour redistribuer les informations de la liste de quarantaine au pare-feu ou à la passerelle, à toutes les connexions aux services et à Panorama.

- **L'administrateur met manuellement en quarantaine l'utilisateur mobile sur Panorama** : dans cet exemple, l'administrateur Prisma Access a ajouté manuellement un utilisateur mobile à la liste de quarantaine sur l'appareil Panorama qui gère Prisma Access. L'administrateur a configuré une redistribution entre Panorama, le pare-feu nouvelle génération et les connexions aux services. Panorama redistribue les informations mises à jour de la liste de quarantaine au pare-feu et aux connexions aux services. Les connexions aux services redistribuent ensuite les informations de la liste de quarantaine aux emplacements d'utilisateurs mobiles.

  L'utilisateur mobile a été connecté à l'emplacement d'utilisateur mobile 1. Une fois que l'emplacement d'utilisateur mobile 1 reçoit les informations de la liste de quarantaine mises à jour, l'utilisateur est déconnecté. Si l'utilisateur tente de se connecter à l'emplacement

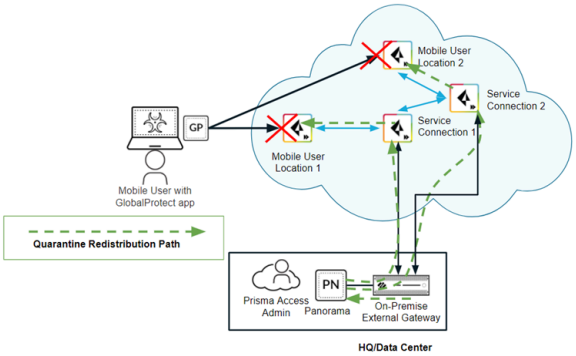
 ©2025 Palo Alto Networks, Inc.

d'utilisateur mobile 2, la connexion est bloquée et l'utilisateur mobile reçoit une notification de quarantaine.



- **L'utilisateur mobile est mis en quarantaine automatiquement ou manuellement au niveau de la passerelle locale** : dans cet exemple, il existe un pare-feu nouvelle génération qui a été configuré comme passerelle externe au siège social ou au centre de données. L'administrateur a mis manuellement en quarantaine un utilisateur mobile au niveau de la passerelle externe. La passerelle externe redistribue les informations de la liste de quarantaine de la passerelle externe vers Panorama.

  Une fois que Panorama a reçu les informations mises à jour de la liste de quarantaine de la passerelle externe, il redistribue ces informations aux connexions aux services 1 et 2, qui les redistribuent ensuite aux emplacements d'utilisateurs mobiles 1 et 2. Si un utilisateur mobile tente de se connecter à l'emplacement d'utilisateur mobile 1 ou 2, Prisma Access bloque la connexion et l'utilisateur reçoit une notification de quarantaine.



Configurer la redistribution de la liste de quarantaine dans Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access

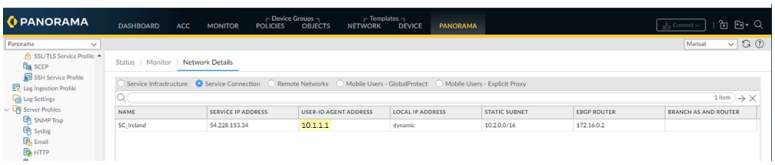
©2025 Palo Alto Networks, Inc.

Pour redistribuer les informations de quarantaine vers et depuis les connexions aux services, le Panorama qui gère Prisma Access, et les pare-feu nouvelle génération, complétez les étapes suivantes.

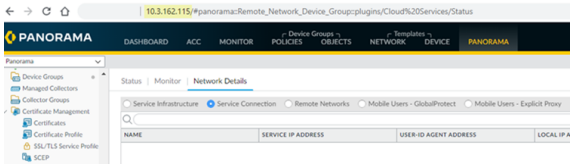
STEP 1 | Assurez-vous que l'adresse IP de gestion de Panorama peut communiquer avec l'adresse de l'agent User-ID pour toutes les connexions aux services pour lesquelles vous souhaitez redistribuer les informations de liste de quarantaine.

La communication entre l'adresse de l'agent User-ID de la connexion aux services et l'adresse IP de gestion de Panorama est nécessaire pour Prisma Access afin de pouvoir envoyer et recevoir des informations sur la liste de quarantaine entre Panorama et les connexions aux services.

- Pour trouver la **User-ID Agent Address (Adresse de l'agent User-ID)**, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **User-ID Agent Address (Adresse de l'agent User-ID)**



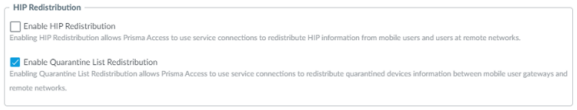
- Pour trouver l'adresse IP de gestion du Panorama qui gère Prisma Access, notez l'adresse IP qui s'affiche dans le navigateur Web lorsque vous accédez à Panorama.



STEP 2 | Autorisez Prisma Access à redistribuer les informations de la liste de quarantaine.

1. Dan Panorama, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)**.
2. Cliquez sur l'engrenage pour modifier les paramètres.
3. Dans l'onglet **Advanced (Avancé)**, sélectionnez **Enable Quarantine List Redistribution (Activer la redistribution de la liste de quarantaine)**.

   Activez la redistribution de la liste de quarantaine permet à Prisma Access de redistribuer les informations de la liste de quarantaine reçues d'un ou plusieurs emplacements d'utilisateurs mobiles (passerelles) aux connexions aux services.

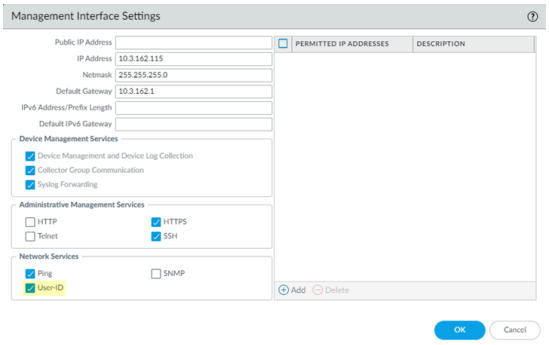


STEP 3 | Cliquez sur **Commit (Valider)** et **Push (Appliquer)** pour valider et appliquer vos modifications.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Configurez Panorama pour recevoir des informations sur la liste de quarantaine de Prisma Access en configurant les paramètres de l'interface de gestion.

1. Dans le Panorama qui gère Prisma Access, sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces**.
2. Sélectionnez l'interface **Management (Gestion)**.
3. Sélectionnez **User-ID (ID utilisateur)**.



STEP 5 | Configurez un agent de redistribution des données qui redistribue les informations de la liste de quarantaine des connexions aux services vers Panorama.

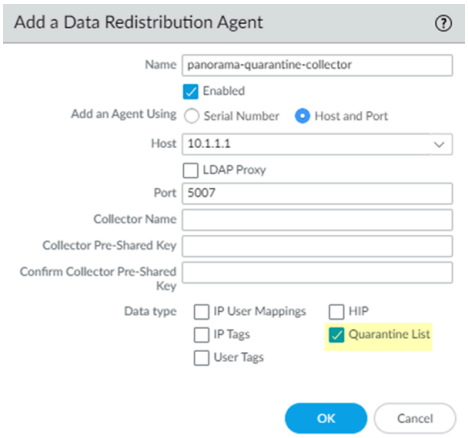
1. Depuis le Panorama qui gère Prisma Access, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)**.
2. Prenez note de **User-ID Agent Address (Adresse de l'agent User-ID)** (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **User-ID Agent Address (Adresse de l'agent User-ID)**) pour chaque connexion aux services.
3. Sélectionnez **Panorama** > **Data Redistribution (Redistribution des données)** > **Agents**.
4. Cliquez sur **Add (Ajouter)** pour ajouter un agent de redistribution des données, donnez-lui un **Name (Nom)** et sélectionnez **Enabled (Activé)**.
5. Entrez la valeur **User-ID Agent Address (Adresse de l'agent User-ID)** de la connexion aux services comme **Host (Hôte)** et 5007 comme **Port**.

   Assurez-vous que votre réseau ne bloque pas l'accès à ce port entre Panorama et Prisma Access.
6. (Facultatif) Si vous avez configuré cette connexion aux services comme Collecteur (**Device (Périphérique)** > **Data Redistribution (Redistribution des données)** > **Collector**

 ©2025 Palo Alto Networks, Inc.

Settings (Paramètres du collecteur)), saisissez le **Collector Name (Nom du collecteur)** et la **Collector Pre-Shared Key (Clé pré-partagée du collecteur)**

7. Sélectionnez la **Quarantine List (Liste de quarantaine)**. Puis, cliquez sur **OK**.



8. Répétez l'étape 5 pour toutes les connexions aux services dans votre déploiement Prisma Access.

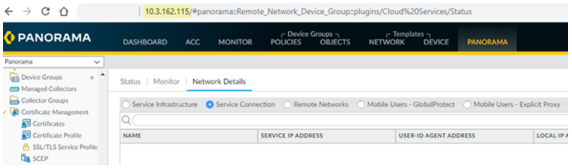
STEP 6 | Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** pour enregistrer vos modifications localement sur le Panorama qui gère Prisma Access.

 ©2025 Palo Alto Networks, Inc.

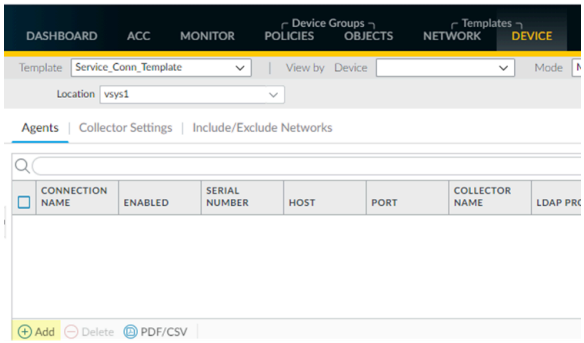
STEP 7 | Configurez un agent de redistribution des données qui redistribue les informations de la liste de quarantaine de Panorama vers les connexions aux services.

1. Trouvez l'adresse IP de gestion du Panorama qui gère Prisma Access.

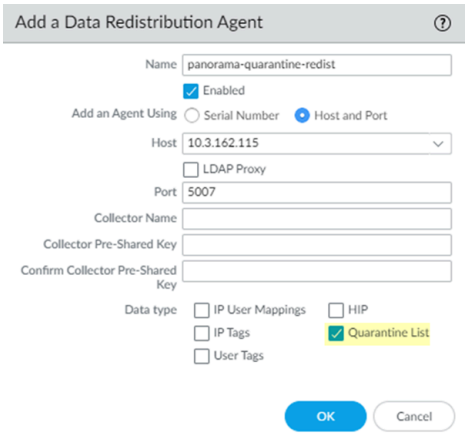
   Cette adresse s'affiche dans la barre d'adresse du navigateur Web lorsque vous accédez à Panorama.



2. Assurez-vous que vous êtes dans le modèle **Service_Conn_Template**, puis sélectionnez **Device (Périphérique)** > **Data Redistribution (Redistribution des données)** > **Agents**.



3. Cliquez sur **Add (Ajouter)** pour ajouter un agent de redistribution des données, donnez-lui un **Name (Nom)** et sélectionnez **Enabled (Activé)**.
4. Entrez l'adresse IP de gestion de l'appareil Panorama comme **Host (Hôte)** et 5007 comme **Port**.



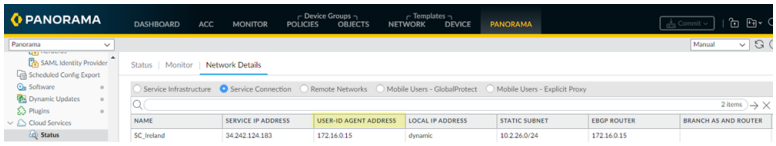
5. Sélectionnez la **Quarantine List (Liste de quarantaine)**. Puis, cliquez sur **OK**.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Configurez un agent de redistribution des données qui redistribue les informations de la liste de quarantaine des connexions aux services vers les passerelles des utilisateurs mobiles.

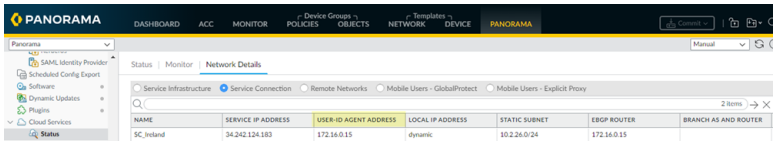
1. Depuis le Panorama qui gère Prisma Access, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)**.
2. Prenez note de la valeur **User-ID Agent Address (Adresse de l'agent User-ID)** de la connexion aux services à partir de laquelle vous souhaitez redistribuer les informations de la liste de quarantaine.

   Puisque toutes les connexions aux services ont les mêmes informations de liste de quarantaine redistribuée, choisissez n'importe quelle connexion aux services. Vous pouvez également configurer plus d'une connexion aux services.



3. Assurez-vous d'être dans le modèle **Mobile_User_Template**, puis sélectionnez **Device (Périphérique)** > **Data Redistribution (Redistribution des données)** > **Agents**.
4. Cliquez sur **Add (Ajouter)** pour ajouter un agent de redistribution des données, donnez-lui un **Name (Nom)** et sélectionnez **Enabled (Activé)**.
5. Entrez la valeur **User-ID Agent Address (Adresse de l'agent User-ID)** de la connexion aux services comme Host (Hôte) et **5007** comme Port.

   Assurez-vous que votre réseau ne bloque pas l'accès à ce port entre Panorama et Prisma Access.
6. (Facultatif) Si vous avez configuré cette connexion aux services comme Collecteur (**Device (Périphérique)** > **Data Redistribution (Redistribution des données)** > **Collector Settings (Paramètres du collecteur)**), saisissez le **Collector Name (Nom du collecteur)** et la **Collector Pre-Shared Key (Clé pré-partagée du collecteur)**.
7. Sélectionnez la **Quarantine List (Liste de quarantaine)**. Puis, cliquez sur **OK**.



8. **Commit and Push (Validez et appliquez)** vos modifications.

STEP 9 | Consultez les informations de votre liste de quarantaine en sélectionnant **Panorama** > **Device Quarantine (Quarantaine des périphériques)**.

Consultez les informations sur les périphériques mis en quarantaine dans le guide de l'administrateur GlobalProtect pour plus de détails.

 ©2025 Palo Alto Networks, Inc.

Trafic de l'entonnoir IPv6 chez les utilisateurs mobiles : déploiements GlobalProtect

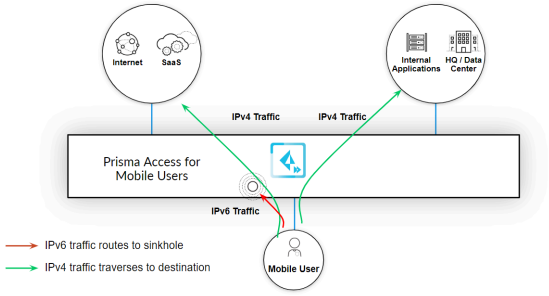
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Dans un terminal à double pile capable de traiter à la fois le trafic IPv4 et IPv6, l'application GlobalProtect envoie le trafic IPv4 des utilisateurs mobiles à protéger via le tunnel VPN GlobalProtect vers Prisma Access. Cependant, le trafic IPv6 des utilisateurs mobiles n'est pas envoyé à Prisma Access par défaut et est envoyé à la carte réseau locale sur le terminal à la place. Pour réduire la surface d'attaque pour les menaces basées sur IPv6, Palo Alto Networks recommande de configurer Prisma Access pour mettre en entonnoir le trafic IPv6. Parce que les terminaux peuvent automatiquement revenir à une adresse IPv4, vous pouvez offrir une expérience utilisateur sécurisée et ininterrompue pour le trafic des utilisateurs mobiles vers Internet.

L'itinéraire IPv6 par défaut a la priorité sur les autres itinéraires. Cependant, si des itinéraires IPv6 plus spécifiques existent via l'interface réseau physique ou si vous spécifiez l'adresse source IPv6 de l'interface physique, ce type de trafic sera envoyé à la carte réseau locale.

De plus, Palo Alto Networks recommande de configurer GlobalProtect pour désactiver complètement le trafic réseau sur la carte réseau locale. Si vous disposez d'un déploiement hybride de Prisma Access avec des pare-feu locaux nouvelle génération configurés en tant que passerelles GlobalProtect, vous pouvez configurer la fonctionnalité de l'entonnoir IPv6 sur la passerelle GlobalProtect sur site.

Vous pouvez configurer Prisma Access pour qu'il mette en entonnoir le trafic IPv6 des utilisateurs mobiles. Lorsque vous activez cette fonctionnalité, Prisma Access attribue une adresse IPv6 au terminal de connexion en plus d'une adresse IPv4 ; ensuite, il achemine le trafic IPv6 vers Prisma Access et le supprime à l'aide d'une politique de sécurité intégrée, comme le montre la figure ci-dessous.



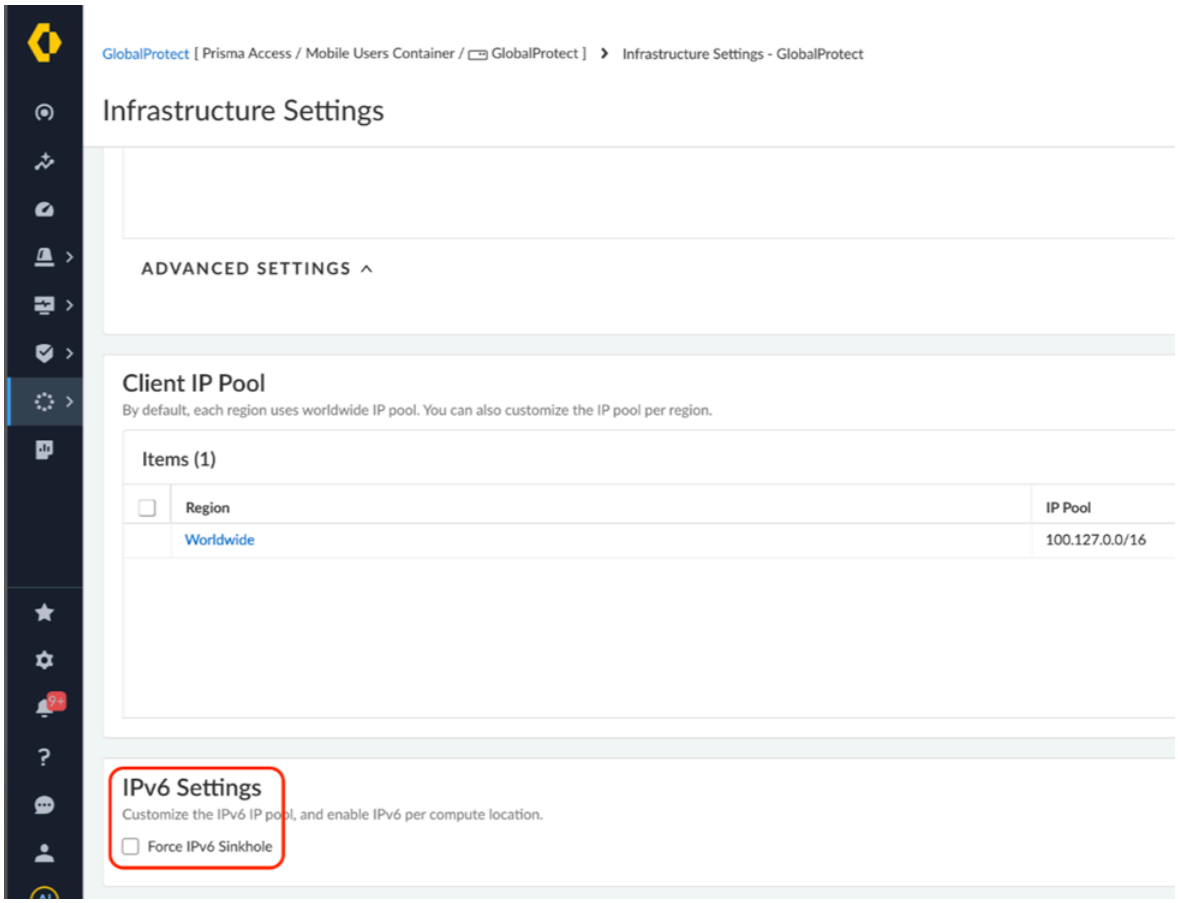
Pour configurer Prisma Access afin qu'il mette en entonnoir le trafic IPv6 des utilisateurs mobiles, suivez les étapes suivantes.

 ©2025 Palo Alto Networks, Inc.

- Déploiements de Prisma Access (Managed by Strata Cloud Manager) :

  Allez à **Workflows** > **Configuration de Prisma Access** > **Utilisateurs mobiles** > **Configuration de GlobalProtect** > **Paramètres avancés**et sélectionnez **Forcer l'entonnoir IPv6**.

  Prisma Access utilise fc00:0:0:0:0:0:0:0/64 comme adresse d'entonnoir.



- Déploiements de Prisma Access (Managed by Panorama) :

  1. Ouvrez une session CLI sécurisée avec des privilèges d'administrateur, en utilisant la même adresse IP que celle que vous utilisez pour vous connecter au Panorama qui gère Prisma Access.
  2. Entrez `configurer` pour entrer en mode de configuration.
  3. Entrez la commande **`set plugins cloud_services mobile-users ipv6 yes`**.

     Si vous devez désactiver cette commande à l'avenir, entrez **`set plugins cloud_services mobile-users ipv6 no`**.
  4. Entrez **`Commit (Valider)`** pour enregistrer vos modifications localement.
  5. Entrez **`Exit (Quitter)`** pour quitter le mode de configuration.
  6. Entrez **`commit-all shared-policy include-template yes device-group Mobile_User_Device_Group`** pour valider vos modifications et les rendre actives dans Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Configurer GlobalProtect pour désactiver l'accès direct au réseau local

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Pris en charge sur tous les terminaux GlobalProtect macOS et Windows. Pris en charge sur les terminaux Linux à partir de la version 6.0.0 de l'application GlobalProtect.

Pour vous assurer que tout le trafic des utilisateurs mobiles est envoyé à Prisma Access, vous pouvez complètement désactiver les connexions sortantes, y compris le trafic du sous-réseau local, afin qu'il ne soit pas envoyé à l'adaptateur local. Vous pouvez désactiver toutes les connexions sortantes vers l'adaptateur local en apportant des modifications à la configuration de la passerelle GlobalProtect.

Vous pouvez effectuer ces étapes sur Panorama ou sur un pare-feu sur site qui a été configuré en tant que passerelle GlobalProtect.

*Activez le paramètre **No direct access to local network (Aucun accès direct au réseau local)** pour réduire les risques dans les réseaux non approuvés tels que les points d'accès Wi-Fi malveillants.*

STEP 1 | Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)**.

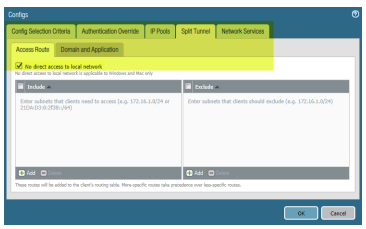
STEP 2 | Sélectionnez une passerelle GlobalProtect existante ou ajoutez-en une nouvelle en cliquant sur **Add (Ajouter)**.

STEP 3 | Sélectionnez **Agent** > **Client Settings (Paramètres du client)**.

STEP 4 | Sélectionnez la configuration **DEFAULT (PAR DÉFAUT)** ou ajoutez-en une nouvelle en cliquant sur **Add (Ajouter)**.

STEP 5 | Sélectionnez **Split Tunnel (Tunnel fractionné)**, puis sélectionnez **No direct access to local network (Aucun accès direct au réseau local)**.

La désactivation de l'accès au réseau local empêche tout le trafic, y compris le trafic IPv4 et IPv6, d'être envoyé à l'adaptateur local. En outre, vous ne pourrez pas accéder aux ressources de votre sous-réseau local, telles que les imprimantes. Le trafic de tunnel divisé en fonction de l'itinéraire d'accès, du domaine de destination et de l'application fonctionne toujours comme prévu.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | (Déploiements Panorama et Prisma Access uniquement) Validez vos modifications localement pour les rendre actives dans Panorama.

1. Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**.
2. Assurez-vous que votre modification fait partie de la **Commit Scope (Étendue de la validation)**.
3. Cliquez sur **OK** pour enregistrer les modifications dans l'étendue de l'application.
4. **Commit (Validez)** vos modifications.

STEP 7 | Vous devez **Commit (Valider)** et **Push (Appliquer)** vos modifications pour les rendre actives dans Prisma Access.

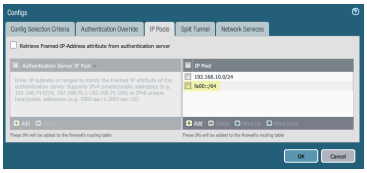
Configurer un entonnoir IPv6 sur la passerelle locale

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Si vous avez un déploiement hybride qui utilise des pare-feu de la nouvelle génération configurés comme passerelles avec Prisma Access, effectuez la tâche suivante sur la passerelle sur site pour supprimer le trafic IPv6.

STEP 1 | Ajoutez des pools IPv6 à votre configuration d'agent GlobalProtect.

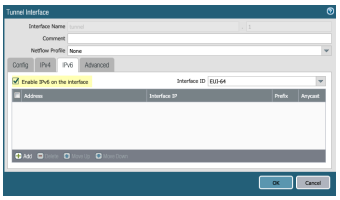
1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)**.
2. Sélectionnez une passerelle GlobalProtect existante ou ajoutez-en une nouvelle en cliquant sur **Add (Ajouter)**.
3. Sélectionnez **Agent** > **Client Settings (Paramètres du client)**.
4. Sélectionnez la configuration de l'agent à modifier ou à **Add (Ajouter)**.
5. Sélectionnez **IP Pools (Pools IP)** ; puis **Add (Ajouter)** un pool IPv6 à affecter à l'adaptateur réseau virtuel sur les terminaux qui se connectent à la passerelle GlobalProtect pour le trafic réseau mobile et cliquez sur **OK**.



 ©2025 Palo Alto Networks, Inc.

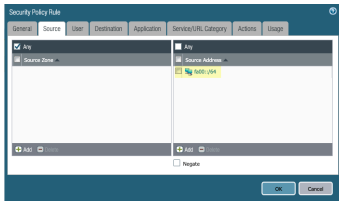
STEP 2 | Activer IPv6 sur l'interface

1. Sélectionnez **Device (Périphérique)** > **Interface** > **Tunnel** et sélectionnez l'**Interface** pour le tunnel que vous utilisez pour le trafic de l'utilisateur mobile.
2. Sélectionnez **IPv6** ; ensuite, sélectionnez **Enable IPv6 on the interface (Activer IPv6 sur l'interface)**.

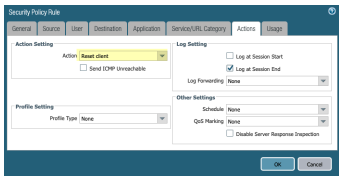


STEP 3 | Ajoutez une stratégie de sécurité pour définir une action de réinitialisation TCP qui mettra fin aux sessions avec un trafic source IPv6 correspondant aux pools IP que vous avez configurés à l'étape 1.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (Ajoutez)** une nouvelle politique de sécurité.
2. Définissez la **Source Address (Adresse source)** dans la règle pour correspondre aux pools IP que vous avez configurés à l'étape 1.



3. Sélectionnez **Actions** ; puis, sélectionnez un **Action Setting (Paramètre d'action)** de **Reset Client (Réinitialiser le client)** et cliquez sur **OK**.



STEP 4 | **Commit (Validez)** vos modifications.

STEP 5 | (Facultatif) Effectuez cette tâche sur tous les pare-feu de passerelle de votre déploiement.

Redistribuer les informations HIP avec Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Pour garantir une application cohérente de la politique HIP (Host Information Profile) et simplifier la gestion des stratégies, vous pouvez redistribuer les informations HIP reçues d'utilisateurs

 ©2025 Palo Alto Networks, Inc.

mobiles et d'utilisateurs de réseaux distants qui utilisent l'application GlobalProtect de Prisma Accès à d'autres passerelles, pare-feu et appareils Panorama de votre entreprise, y compris Panorama qui gère Prisma Access.

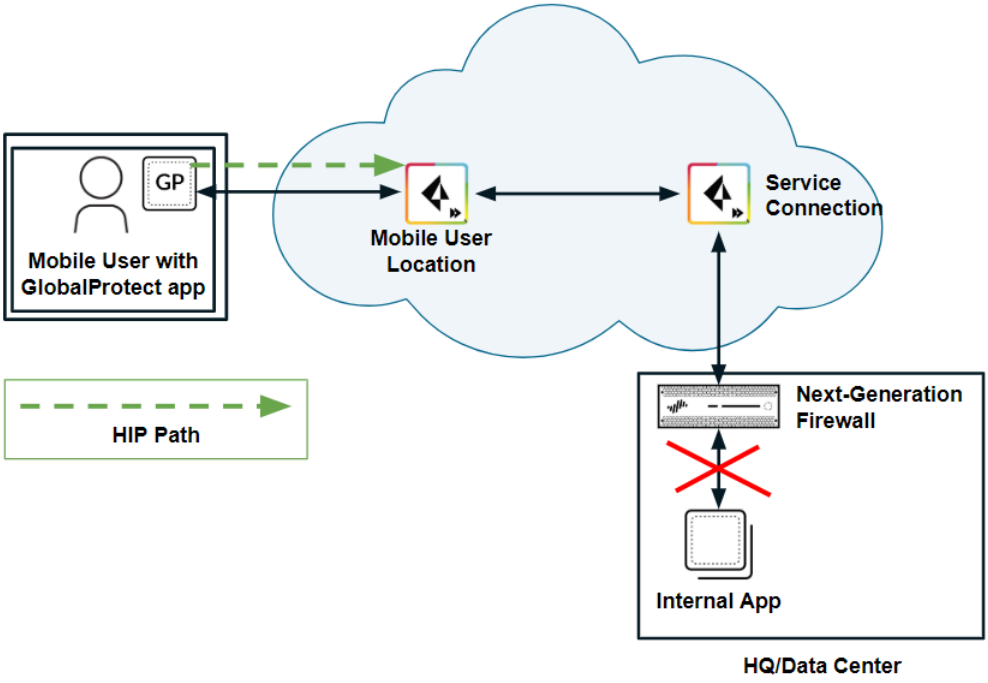
La section suivante décrit certains déploiements Prisma Access courants où la redistribution HIP est utile pour l'application cohérente des politiques et l'affichage des rapports HIP :

- **Redistribution HIP à partir de Prisma Access à un pare-feu de la nouvelle génération** : si vous disposez d'un pare-feu de la nouvelle génération dans le centre de données ou au siège social de votre entreprise et que vous avez configuré ce pare-feu avec des stratégies de sécurité basées sur HIP, vous ne pouvez pas appliquer ces stratégies pour Prisma Access utilisateurs mobiles tant que vous ne redistribuez pas la redistribution HIP à partir de Prisma Access au pare-feu.

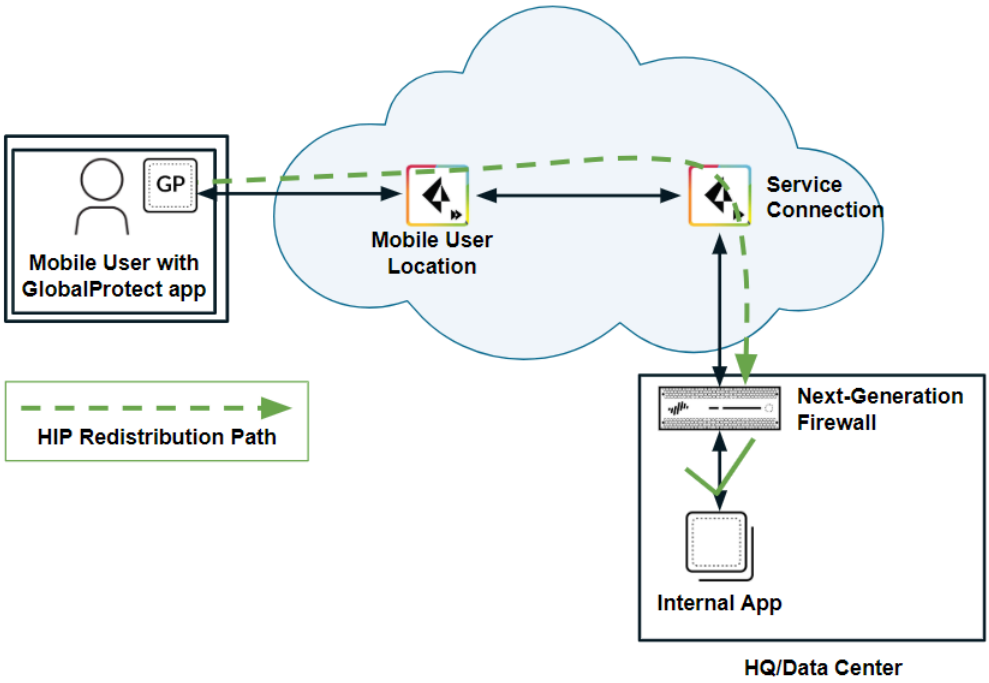
  La figure suivante montre un utilisateur mobile dont le point de terminaison est protégé par l'application GlobalProtect. L'utilisateur tente d'accéder à une application interne à un siège ou à un centre de données dont l'accès est contrôlé par un pare-feu de la nouvelle génération doté de politiques de sécurité basées sur HIP. Lorsque l'utilisateur se connecte à l'application GlobalProtect, celle-ci collecte des informations HIP et les envoie à Prisma Access ; toutefois Prisma Access ne redistribue pas ces informations au pare-feu local. Étant donné que le pare-

 ©2025 Palo Alto Networks, Inc.

feu ne dispose pas des informations HIP de l'utilisateur, il bloque l'accès de l'utilisateur à l'application.



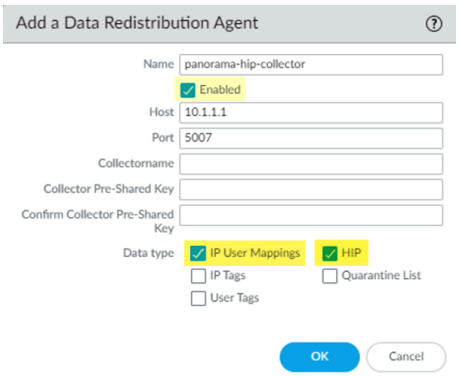
La redistribution HIP vous permet de distribuer les informations HIP des utilisateurs mobiles au pare-feu local. Le pare-feu peut ensuite vérifier les informations HIP de l'utilisateur par rapport à ses stratégies de sécurité configurées et accorder à l'utilisateur l'accès à l'application.



Pour redistribuer les informations HIP à partir de Prisma Access au pare-feu, vous autorisez Prisma Access à redistribuer les informations HIP, puis **Add (Ajouter)** un **(User-ID Agent**

 ©2025 Palo Alto Networks, Inc.

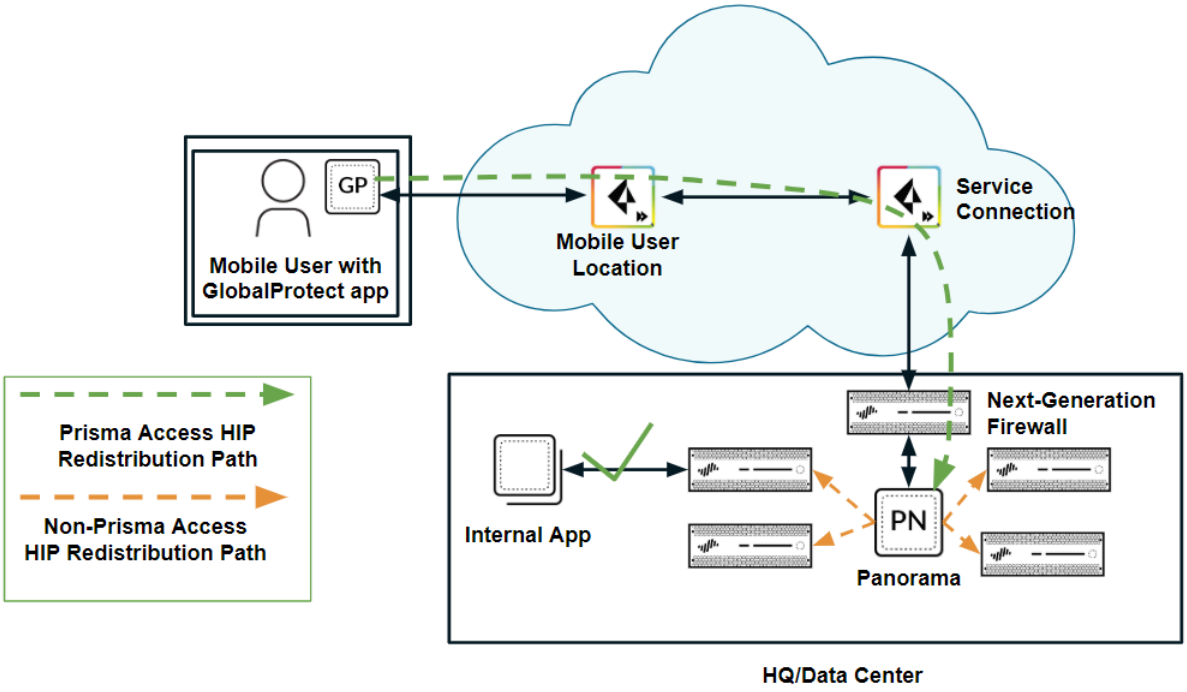
(Agent User-ID) (**Panorama** > **User Identification (Identification de l'utilisateur)** > **User-ID Agents (Agents User-ID)** pour 9.1.*x* Appareils Panorama ou **Panorama** > **Data Redistribution (Redistribution des données)** pour Panorama 10.*x* appliances) sur le pare-feu, et spécifiez Prisma Access **User-ID Agent Address (Adresse de l'agent User-ID)** (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **User-ID Agent Address (Adresse de l'agent User-ID)**) alors que le **Host (Hôte)** (10.1.1.1 dans l'exemple suivant) et **5007 (5007)** comme **Port (Port)**.



- **Redistribution HIP à partir de Prisma Access vers Panorama** : si vous disposez de plusieurs pare-feu ou passerelles dans votre organisation avec des stratégies de sécurité basées sur HIP, vous pouvez redistribuer les informations HIP à partir de Prisma Access à Panorama qui gère Prisma Access en créant un agent User-ID dans Panorama et en spécifiant Prisma Access **User-ID Agent Address (Adresse de l'agent User-ID)** en tant qu'identifiant d'utilisateur **Host (Hôte)**. Vous pouvez alors redistribuer des rapports HIP de cet appareil Panorama vers les autres appareils, passerelles, pare-feu et systèmes virtuels Panorama gérés de votre entreprise, en utilisant le même flux de travail que celui que vous utilisez pour redistribuer les informations

 ©2025 Palo Alto Networks, Inc.

User-ID aux pare-feu gérés et appliquer une politique cohérente pour les applications et les ressources internes, comme illustré dans la figure suivante.



Vous pouvez également configurer chaque pare-feu ou passerelle interne de votre entreprise pour collecter directement des informations HIP à partir de Prisma Access, sans utiliser Panorama comme emplacement central, en créant un agent User-ID dans chaque périphérique. Notons toutefois que Prisma Access utilise les connexions aux services pour envoyer des informations HIP, et la consommation de bande passante de la connexion aux services peut augmenter si Prisma Access envoie un grand nombre de rapports HIP.

- **Redistribution HIP d'un utilisateur d'un réseau distant vers Prisma Access**—Les cas d'utilisation précédents ont montré Prisma Access collecter des informations HIP auprès des utilisateurs mobiles. Si vous souhaitez appliquer des stratégies basées sur HIP dans Prisma Access pour un utilisateur situé sur un emplacement réseau distant, vous avez besoin d'un moyen de distribuer les informations HIP de l'application GlobalProtect de l'utilisateur du réseau distant pour Prisma Access.

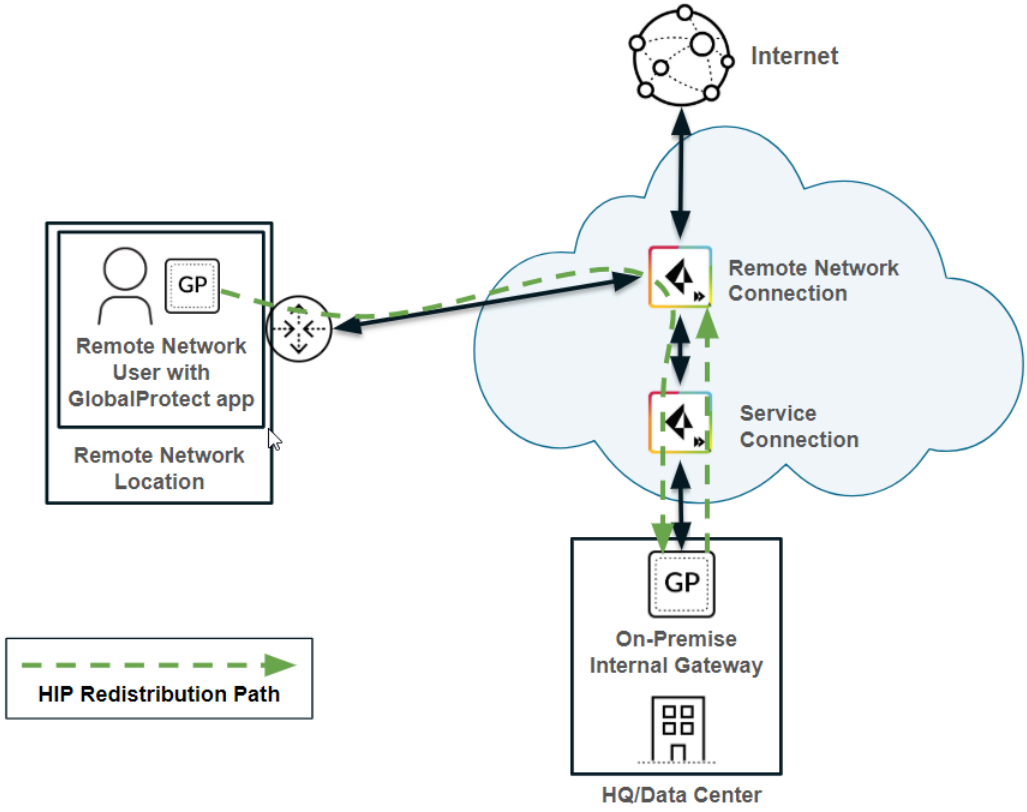
  L'exemple suivant montre un utilisateur d'un emplacement réseau distant dont l'accès à Internet se trouve sur la connexion réseau distante. Dans Prisma Access, vous contrôlez l'accès à Internet de l'utilisateur à l'emplacement du réseau distant à l'aide de stratégies de sécurité créées dans le **Remote_Network_Device_Group** ou dans un groupe de périphériques partagés. Pour appliquer correctement les stratégies à l'emplacement du réseau distant pour l'utilisateur, vous devez configurer Prisma Access pour récupérer les informations HIP de l'utilisateur à partir de la passerelle interne.

  Dans cet exemple, la passerelle GlobalProtect au siège/centre de données qui est configurée en tant que passerelle interne à l'aide de détection d'hôte interne vérifie les informations HIP de l'utilisateur à partir de l'application GlobalProtect de l'utilisateur. La passerelle interne

 ©2025 Palo Alto Networks, Inc.

détecte que l'utilisateur se trouve à l'intérieur de l'emplacement du réseau distant et collecte les informations HIP et User-ID de l'utilisateur.

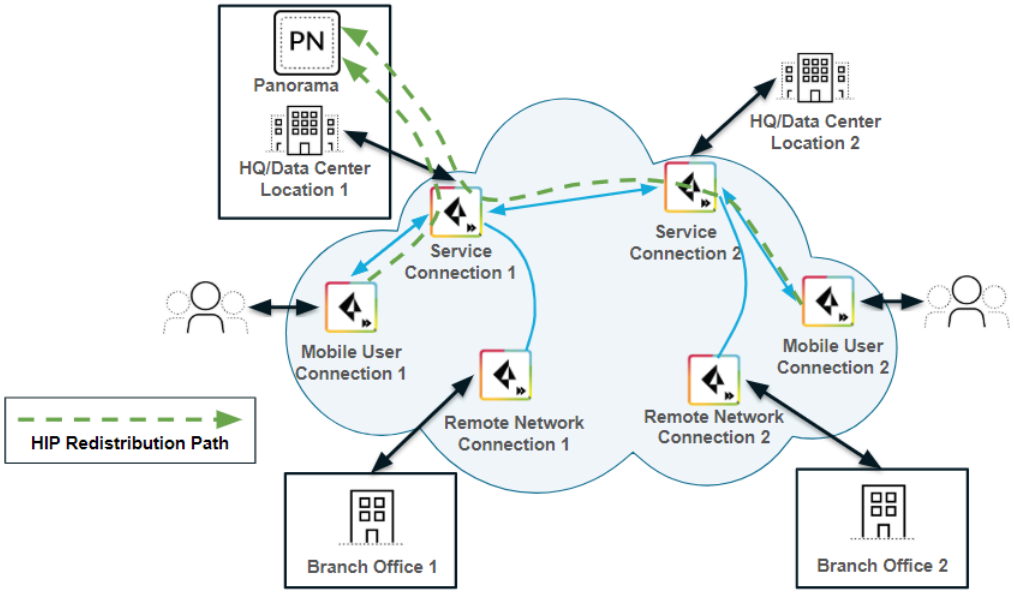
Pour distribuer ces informations HIP de la passerelle interne à Prisma Access, créez un agent User-ID dans Panorama et spécifiez l'adresse IP de la passerelle interne en tant qu'hôte.



- **Afficher les journaux HIP détaillés à partir de Panorama**—Lorsque les utilisateurs mobiles se connectent à l'aide de l'application GlobalProtect, l'application envoie les informations HIP à Prisma Access. Panorama récupère les résultats du journal à partir de Strata Logging Service pour afficher les résultats des journaux de correspondance HIP (**Monitor (Surveiller)** > **Logs (Journaux)** > **HIP Match (Journal de correspondance HIP)**) ; toutefois, vous ne pouvez

 ©2025 Palo Alto Networks, Inc.

pas afficher les rapports HIP détaillés tant que vous n'avez pas configuré Panorama pour redistribuer les détails du rapport HIP à partir de Prisma Access à Panorama.

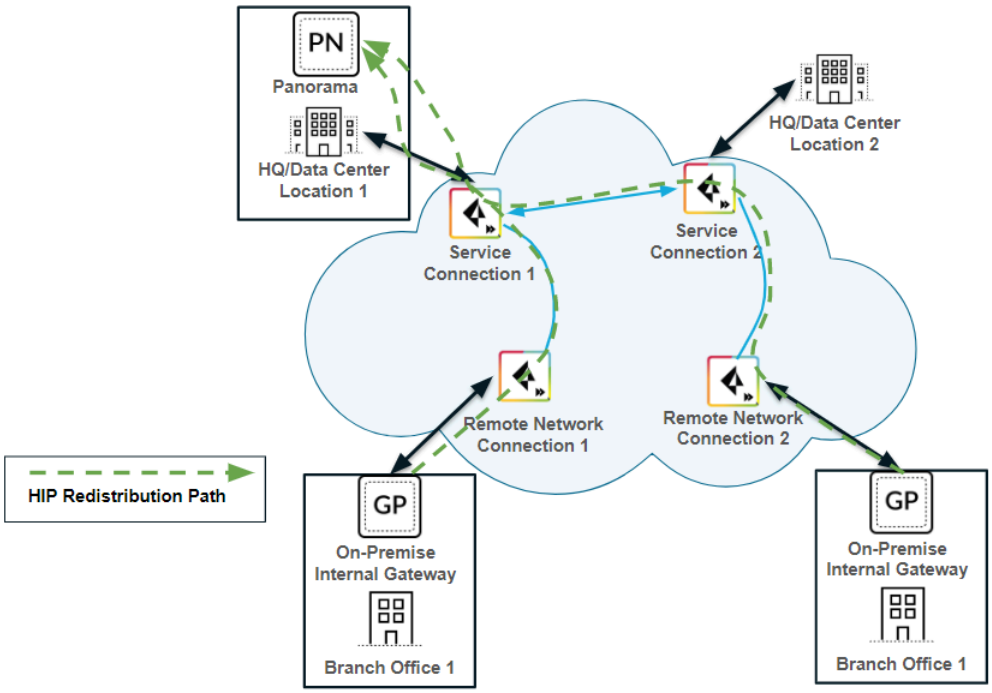


Pour redistribuer des informations HIP détaillées des utilisateurs mobiles vers Panorama, créez un agent User-ID dans Panorama et spécifiez **User-ID Agent Address (Adresse de l'agent User-ID)** (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **User-ID Agent Address (Adresse de l'agent User-ID)**) en tant qu'hôte User-ID.

Si vous avez configuré une passerelle locale en tant que passerelle interne à un emplacement d'utilisateur distant, vous pouvez également envoyer les informations HIP pour les utilisateurs des réseaux distants à Panorama en créant un agent User-ID dans Panorama et en spécifiant l'adresse **EBGP Router (Routeur EBGP)** du réseau distant (**Panorama** > **Cloud Services** > **Status**

 ©2025 Palo Alto Networks, Inc.

(État) > Network Details (Détails du réseau) > Remote Networks (Réseaux distants) > EBGP Router (Routeur EBGP)) en tant qu'hôte User-ID.



Activez et configurez la redistribution HIP dans Prisma Access :

- Configurer la redistribution HIP dans Prisma Access

Configurer la redistribution HIP dans Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access

Lorsque l'application GlobalProtect est installée sur le terminal d'un utilisateur mobile et que celui-ci se connecte à Prisma Access, Prisma Access collecte les informations HIP de l'utilisateur à partir de l'application GlobalProtect du terminal, ce qui rend le rapport HIP disponible dans Prisma Access.

Pour utiliser la redistribution HIP, l'application GlobalProtect doit être installée sur le terminal des utilisateurs. Bien que Prisma Access prenne en charge les VPN sans client, vous ne pouvez pas redistribuer les informations HIP pour les utilisateurs de VPN sans client.

La redistribution HIP peut s'appliquer à la fois aux utilisateurs mobiles et aux utilisateurs de réseaux distants. Toutefois, pour les utilisateurs de réseaux distants, une passerelle sur site doit détecter que l'utilisateur est interne au réseau de l'organisation à l'aide de la détection d'hôte interne avant que la passerelle sur site puisse envoyer des informations HIP à Prisma Access.

 ©2025 Palo Alto Networks, Inc.

Dans Prisma Access, vous configurez la détection d'hôte interne lorsque vous configurez le déploiement de vos utilisateurs mobiles.

Pour assurer une application constante des politiques, vous pouvez utiliser la redistribution HIP pour permettre à Prisma Access de distribuer les informations HIP des utilisateurs vers d'autres périphériques, passerelles, pare-feu et systèmes virtuels Panorama de votre déploiement, ainsi que de distribuer les informations HIP de ces périphériques à Prisma Access dans certains cas. Cette fonctionnalité vous permet d'assurer la constance de l'application des politiques basées sur HIP pour le trafic des utilisateurs, y compris des politiques pour le trafic Internet ou pour le trafic accédant à une application ou à une ressource internes au siège ou au centre de données de votre organisation. La redistribution des informations HIP vers l'appareil Panorama vous permet également d'afficher des informations HIP détaillées pour des utilisateurs Prisma Access de cet appareil.

Gardez à l'esprit que les passerelles internes et externes GlobalProtect ne prennent pas en charge la redistribution HIP bidirectionnelle. Par conséquent, la meilleure pratique consiste à utiliser votre appareil Panorama comme point de redistribution. Dans ce déploiement, vous configureriez vos passerelles internes et externes pour envoyer les rapports HIP à Panorama, et Panorama les transférerait à vos pare-feu pour une application constante des politiques dans votre environnement.

- Strata Cloud Manager
- Panorama

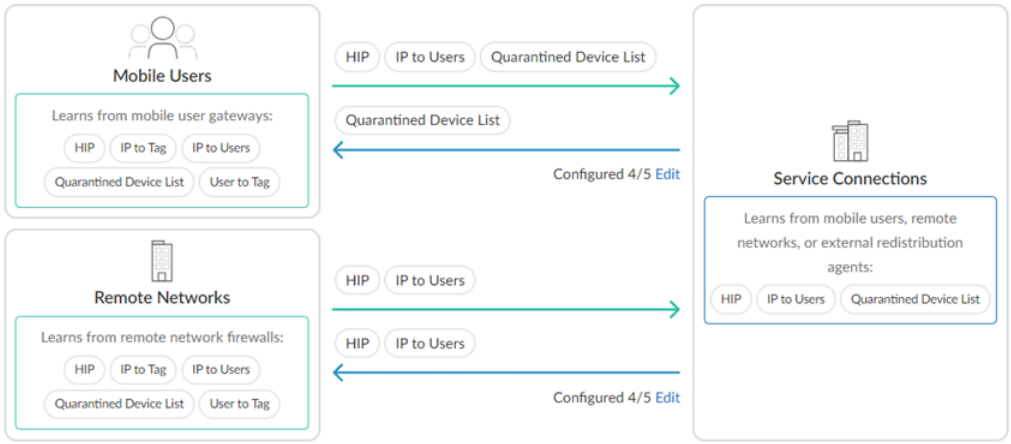
Configurez la redistribution HIP dans Prisma Access (Strata Cloud Manager).

La redistribution des rapports HIP est activée par défaut dans **Strata Cloud Manager**. Pour afficher les détails de la redistribution ou pour la désactiver, suivez les étapes ci-dessous.

STEP 1 | Dans **Strata Cloud Manager**, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identify Services (Identifier les services)** > **Identify Redistribution (Identifier la redistribution)**.

Le Identity Redistribution Diagram (Diagramme de redistribution d'identité) Prisma Access affiche les paramètres de redistribution de rapports HIP par défaut entre les utilisateurs mobiles et les connexions aux services ainsi qu'entre les réseaux distants et les connexions aux services.

Prisma Access Identity Redistribution Diagram



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Pour désactiver la redistribution entre un segment, cliquez sur **Edit (Modifier)**, puis sur **Edit (Modifier)** en regard du réseau distant source concerné.

STEP 3 | Désactivez **HIP**.

Configurez la redistribution HIP dans Prisma Access (Panorama).

Pour autoriser Prisma Access à collecter et à redistribuer les informations HIP, complétez la tâche suivante.

STEP 1 | Autorisez Prisma Access à redistribuer les informations HIP.

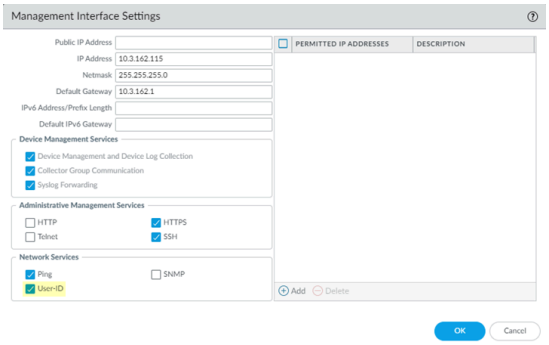
1. Dans Panorama, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)**.
2. Cliquez sur l'engrenage pour modifier les paramètres.
3. Dans l'onglet **Advanced (Avancé)**, sélectionnez **Enable HIP Redistribution (Activer la redistribution HIP)**.

   L'activation de la redistribution HIP permet à Prisma Access de redistribuer les rapports HIP reçus de l'application GlobalProtect vers les pare-feu internes et Panorama.



STEP 2 | Configurez Panorama pour recevoir des rapports HIP de Prisma Access.

1. Sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces**.
2. Sélectionnez l'interface **Management (Gestion)**.
3. Sélectionnez **User-ID (ID utilisateur)**.



STEP 3 | Configurez Panorama pour collecter le mappage User-ID à partir de Prisma Access.

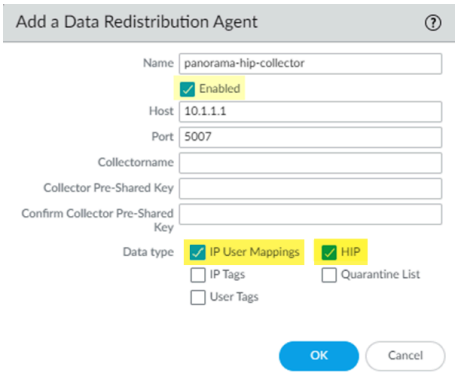
1. Depuis le Panorama qui gère Prisma Access, sélectionnez **Panorama** > **Data Redistribution (Redistribution des données)** > **Agents** (pour les appareils Panorama 10.*x*) ou **Panorama** > **User Identification (Identification utilisateur)** > **User-ID Agents (Agents User-ID)** (pour les appareils Panorama 9.1.*x*).
2. Cliquez sur **Add (Ajouter)** pour ajouter un agent User-ID et donnez-lui un **Name (Nom)**.

 ©2025 Palo Alto Networks, Inc.

3. Entrez l'une des valeurs suivantes dans le champ **Host (Hôte)** en fonction des types d'informations HIP que vous souhaitez collecter.
   - Pour collecter des informations HIP pour les utilisateurs mobiles, entrez l'**User-ID Agent Address (Adresse de l'agent User-ID)** (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Service Connection (Connexion aux services)** > **User-ID Agent Address (Adresse de l'agent User-ID)**).
   - Pour collecter des informations HIP auprès des utilisateurs à des emplacements de réseau distants avec une passerelle interne, entrez l'adresse IP de la passerelle interne.
   - Pour collecter des informations HIP auprès des utilisateurs avec une connexion de réseau distant, entrez l'adresse du **EBGP Router (Routeur EBGP)** (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Remote Networks (Réseaux distants)** > **EBGP Router (Routeur EBGP)**) en tant qu'hôte User-ID.
4. Entrez **5007** dans le champ du port.

   Par défaut, l'agent User-ID utilise le port 5007 pour écouter les requêtes d'informations HIP.

   Assurez-vous que votre réseau ne bloque pas l'accès à ce port entre Prisma Access et le serveur Active Directory ou l'agent User-ID.
5. Sélectionnez **Enabled (Activé)** pour permettre à Panorama de communiquer avec l'agent User-ID.
6. Sélectionnez **IP User Mappings (Mappages d'utilisateurs IP)** et **HIP** pour permettre à Panorama de recevoir des mappages nom d'utilisateur/adresse IP et des données HIP GlobalProtect depuis tous les emplacements d'utilisateurs mobiles.
7. Cliquez sur **OK**.



STEP 4 | Répétez l'étape3 pour chaque connexion aux services pour laquelle vous souhaitez configurer la collecte de rapports HIP.

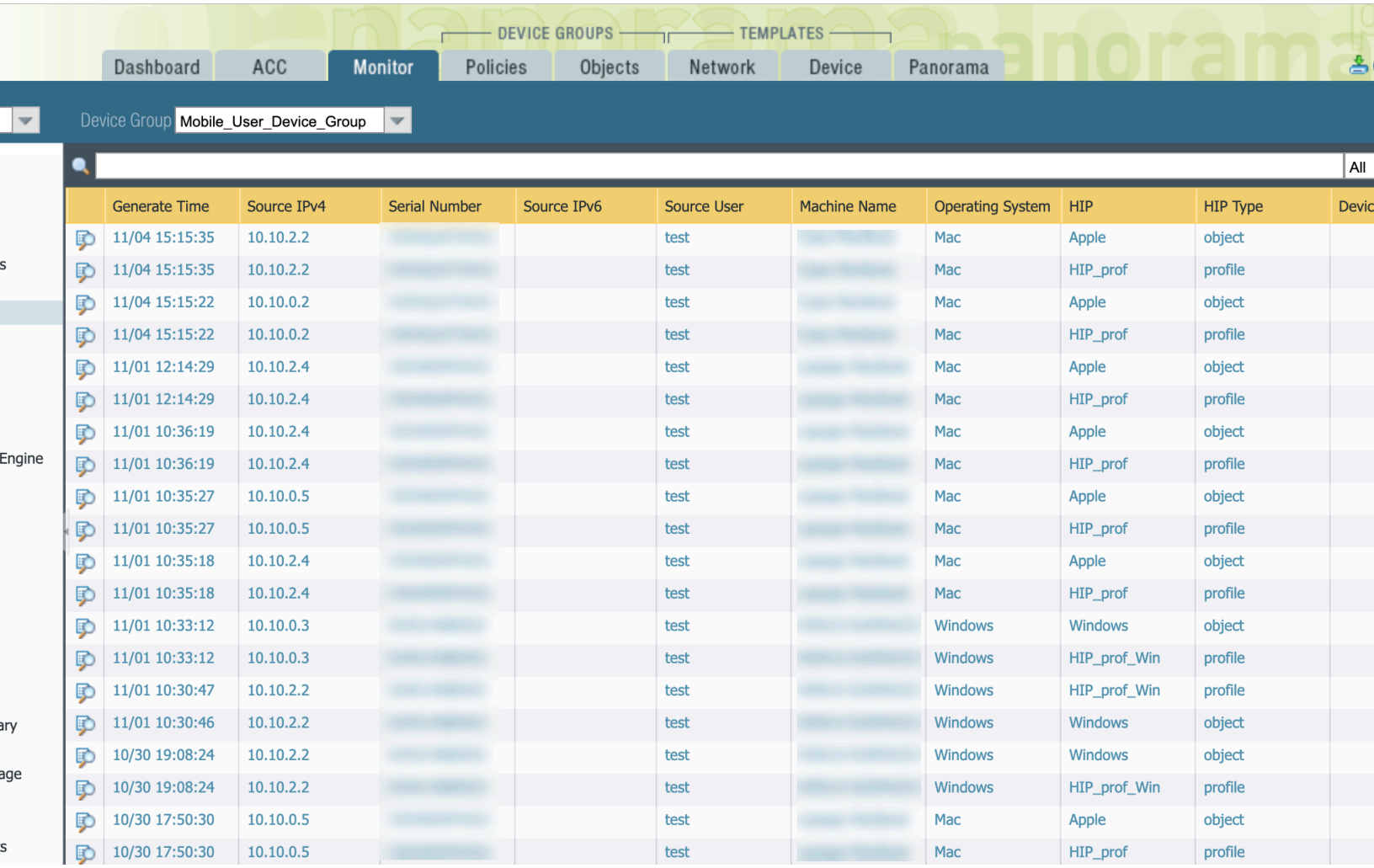
Voir les rapports HIP

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	☐ Licence Prisma Access

 ©2025 Palo Alto Networks, Inc.

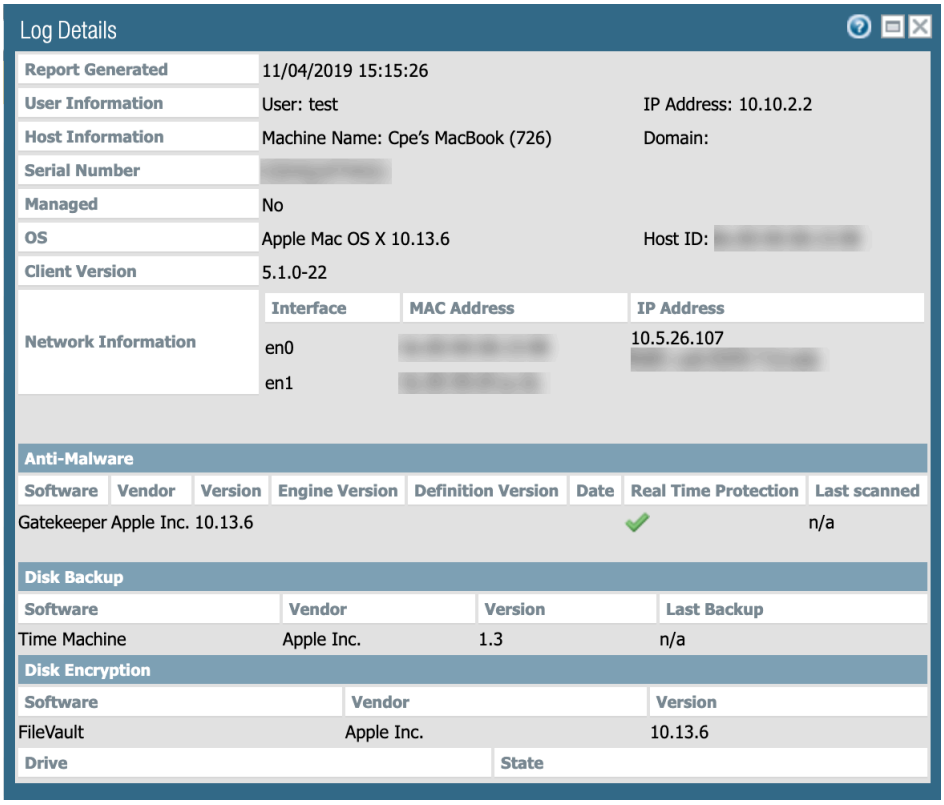
Après avoir configuré Prisma Access pour collecter et redistribuer des informations HIP à Panorama, utilisez le flux de travail suivant pour afficher les informations HIP dans Panorama.

STEP 1 | Sélectionnez **Monitor (Surveiller)** > **Logs (Journaux)** > **HIP Match (Correspondance HIP)** pour afficher les informations HIP.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | Cliquez sur l'icône à gauche d'un enregistrement pour afficher des informations HIP détaillées.



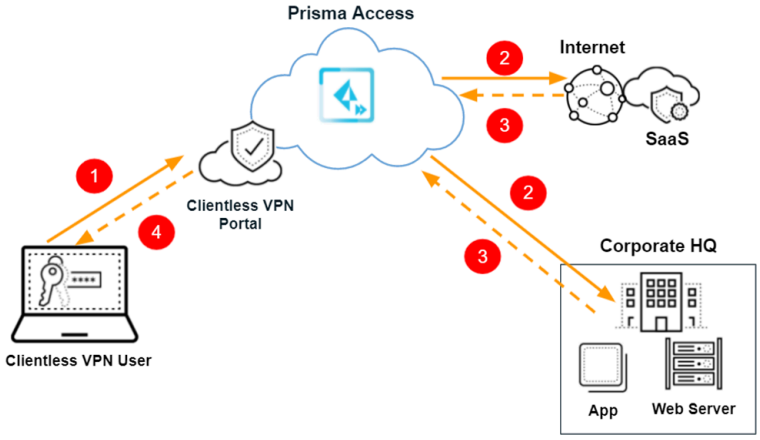
Prise en charge de l'encodage Gzip dans un VPN sans client

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Panorama	• Licence Prisma Access

VPN sans client GlobalProtect offre un accès à distance sécurisé pour les applications Web d'entreprise courantes. Prisma Access Le VPN sans client permet aux utilisateurs mobiles d'accéder à des sites Web compressés Gzip pour utiliser des applications internes et SaaS. La prise en charge de l'encodage Gzip garantit que la demande d'encodage Gzip dans l'en-tête HTTP est acceptée par le portail VPN sans client. Cela garantit que le contenu des pages Web compressées par Gzip est correctement rendu lorsqu'il est accessible via le portail VPN sans client.

Le schéma suivant illustre la prise en charge étendue pour permettre aux utilisateurs d'accéder aux applications internes et SaaS via un VPN sans client dans Prisma Access.

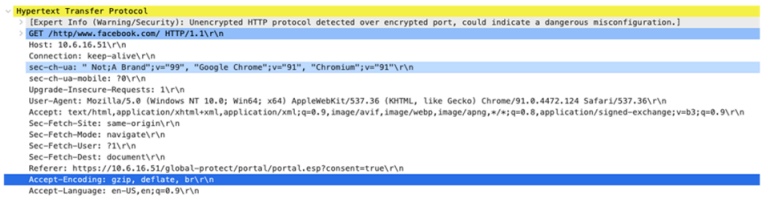
 ©2025 Palo Alto Networks, Inc.



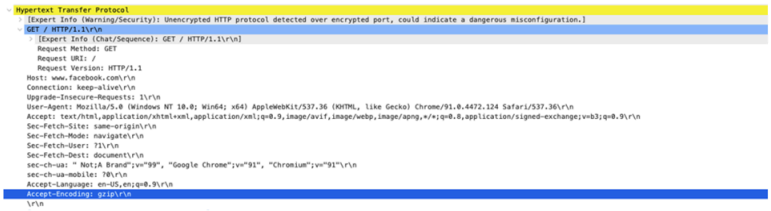
Le VPN sans client peut déterminer s'il doit utiliser l'encodage Gzip en fonction de la requête HTTP du client et de la réponse correspondante de l'application. La valeur **gzip** doit être incluse dans l'une des valeurs d'en-tête Accept-Encoding afin qu'elle soit acceptée par le VPN sans client.

Par exemple, considérez les scénarios suivants lorsque le VPN sans client utilise l'encodage Gzip :

1. Le navigateur envoie une requête HTTP au site Web avec les valeurs d'en-tête Accept-Encoding définies sur **gzip**, **deflate (démonter)** et **Br**, comme illustré dans l'exemple suivant.



2. Le portail VPN sans client dans Prisma Access analyse la requête HTTP entrante du navigateur et définit la valeur de l'en-tête Accept-Encoding sur **gzip** qui indique la prise en charge de l'encodage Gzip, comme illustré dans l'exemple suivant.

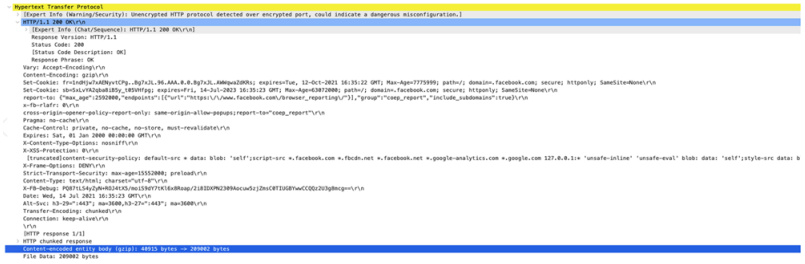


 ©2025 Palo Alto Networks, Inc.

3. Si le site Web prend en charge l'encodage Gzip dans la réponse HTTP, le site Web envoie l'en-tête Content-Encoding en tant que **gzip** qui indique que le contenu est au format Gzip, comme illustré dans l'exemple suivant.



4. Le VPN sans client transmet la réponse reçue du site Web au navigateur Web dans le même format, comme le montre l'exemple suivant.



Si la requête HTTP reçue par le VPN sans client n'inclut pas **gzip** comme l'une des méthodes d'encodage, le VPN sans client n'accepte pas non plus l'encodage Gzip.

Réplication du trafic dans Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Licence complémentaire de réplication du trafic ❑ La réplication du trafic nécessite au minimum Prisma Access 4.1 pour le trafic des utilisateurs mobiles. ❑ La réplication du trafic nécessite au minimum Prisma Access 5.0 pour le trafic des utilisateurs mobiles et du réseau distant. ❑ La prise en charge de TLS 1.3 pour les réseaux distants nécessite an minimum Prisma Access 5.2. ❑ PubSub exige au minimum Prisma Access 5.2.1.

 ©2025 Palo Alto Networks, Inc.

Les enregistreurs réseau sur site sont un outil puissant qui permet aux organisations d'effectuer des investigations et des analyses des violations. Il est courant dans les topologies sur site d'implémenter une infrastructure parallèle de ports TAP, de ports SPAN ou de brokers de paquets qui fournirait une copie du trafic à utiliser pour une telle analyse hors bande.

Cependant, parallèlement à l'adoption accélérée du travail hybride et du cloud, les organisations migrent vers des architectures SASE pour relever ces défis. L'adhésion aux solutions de sécurité cloud SASE a créé des angles morts pour ces outils d'investigation, où une copie du trafic d'un utilisateur distant vers une application SaaS n'est plus disponible.

La réplication du trafic Prisma Access ajoute une visibilité totale sur l'investigation et l'analyse post-mortem impliquant les architectures SASE en mettant à disposition une copie du trafic qui traverse Prisma Access. Voici quelques cas d'utilisation courants où la réplication du trafic est essentielle :

- Investigation et analyse de chasse aux menaces, où les captures de paquets fournissent des preuves irréfutables de l'attaque et de l'approche utilisée
- Réponse à une norme de conformité réglementaire spécifique lorsque les captures de paquets doivent être stockées pendant un certain temps
- Utilisation continue d'outils tiers préférés dans lesquels votre organisation a investi
- Débogage des performances du réseau et des applications au niveau des paquets

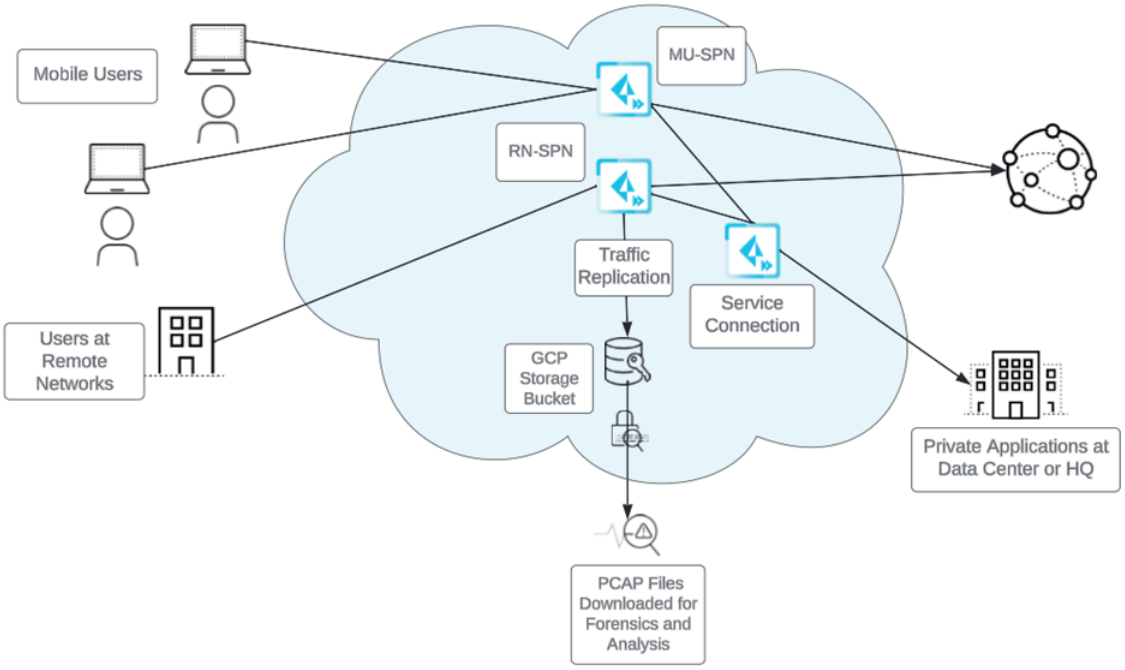
La réplication du trafic permet d'accéder aux captures de paquets (PCAP) du trafic réel des utilisateurs, ce qui permet de détecter et de corriger les menaces qui pourraient s'étendre sur plusieurs sessions ou d'identifier et de répondre aux comportements anormaux afin de réduire les risques et d'assurer la sécurité de l'entreprise.

Lors de l'activation de la réplication du trafic, Prisma Access crée des compartiments de stockage cloud dédiés dans chaque emplacement de calcul Prisma Access où cette fonctionnalité est activée et enregistre en continu les fichiers PCAP contenant une réplique du trafic traversant Prisma Access.

Pour être averti lorsqu'un nouveau fichier PCAP est téléchargé dans le compartiment de stockage, vous pouvez vous abonner aux notifications Pub/Sub. L'utilisation de notifications Pub/Sub pour les nouveaux fichiers PCAP élimine la nécessité de développer des outils qui vous avertissent lorsqu'il y a de nouveaux fichiers dans les compartiments.

Vous devez fournir un compte de service Google Cloud qui sera utilisé pour partager les droits en lecture seule sur ces compartiments de stockage, permettant ainsi un accès sécurisé aux fichiers PCAP. Un chiffrement supplémentaire des fichiers PCAP au repos est appliqué, impliquant une clé publique qui est partagée via un certificat dans Prisma Access. Vous seul disposerez de la clé privée pour décrypter et récupérer les fichiers PCAP d'origine.

 ©2025 Palo Alto Networks, Inc.



Conditions préalables à la réplication du trafic

Avant de commencer à configurer la réplication du trafic, tenez compte des conditions préalables suivantes.

- Assurez-vous d'avoir créé un compte de service dans Google Cloud Platform (GCP).
- Assurez-vous d'avoir créé une clé publique partagée via un certificat dans la page **Objects (Objets)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Custom Certificates (Certificats personnalisés)** > **Generate (Générer)** pour le décryptage SSL.
- L'architecture recommandée exige que le calcul ou le service qui lit les fichiers PCAP à partir de chaque compartiment de stockage soit présent dans la même région GCP à partir de laquelle le compartiment assure la lecture. Bien que la lecture de fichiers PCAP à partir d'un compartiment de stockage d'une autre région GCP ou même en dehors du cloud GCP puisse fonctionner, ces modèles de déploiement ne sont pas pris en charge.

Instructions de réplication du trafic

Suivez ces instructions pour la réplication du trafic :

- **Prise en charge de TLS** : TLS 1.2 est pris en charge pour la réplication du trafic utilisée dans les déploiements d'utilisateurs mobiles. TLS 1.2 et 1.3 sont pris en charge pour la réplication du trafic utilisée dans les déploiements de réseau distant.
- **Algorithmes de tunnel IPSec** : tous les algorithmes de tunnel IPSec pris en charge pour les déploiements d'utilisateurs mobiles et de réseaux distants sont également pris en charge avec la réplication du trafic.

Découvrez comment configurer la réplication du trafic :

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

Réplication du trafic dans Prisma Access (Strata Cloud Manager)

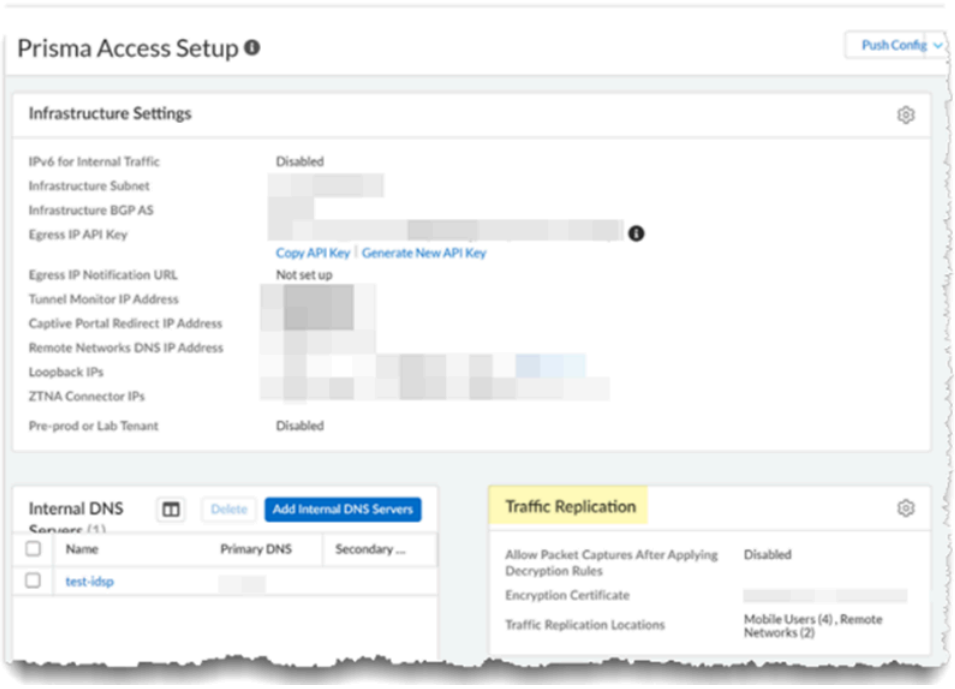
Pour configurer la réplication du trafic et accéder aux fichiers de capture de paquets (PCAP), suivez les étapes suivantes.

STEP 1 | Intégrez et configurez les utilisateurs mobiles — GlobalProtect pour les emplacements où vous souhaitez activer la réplication du trafic et sélectionnez **Commit and Push (Valider et appliquer)** pour vos modifications.

Les emplacements Utilisateurs mobiles — GlobalProtect doivent être activés avant d'activer la réplication du trafic pour ces emplacements.

STEP 2 | (Facultatif) Appliquez le décryptage SSL sur les captures de paquets.

1. Allez dans Prisma Access (Managed by Strata Cloud Manager) et sélectionnez **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Traffic Replication (Réplication du trafic)** et cliquez sur l'engrenage pour modifier les **Settings (Paramètres)**.



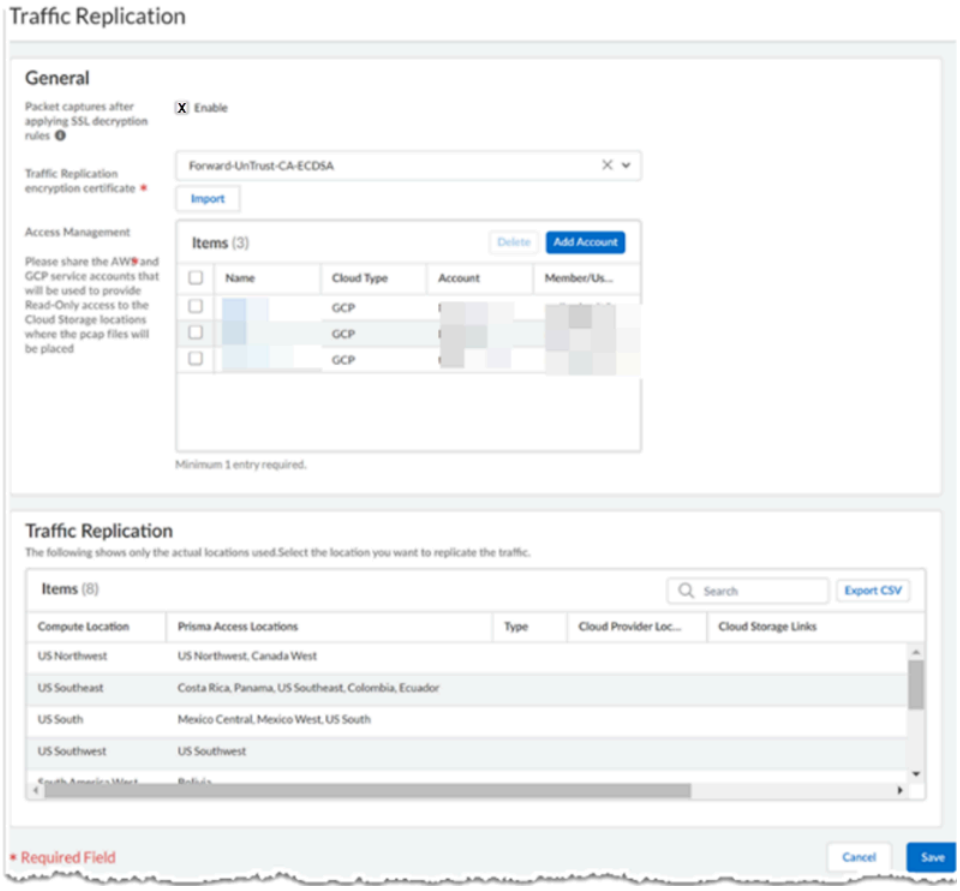
2. Activez **Packet captures after applying SSL decryption rules (Captures de paquets après application des règles de déchiffrement SSL)** pour appliquer vos politiques de décryptage SSL déjà configurées sur les fichiers PCAP.

   Seul le trafic qui correspond à la politique de déchiffrement SSL en ligne sera décrypté.

   Si vous sélectionnez cette option, les fichiers PCAP utiliseront les mêmes règles de décryptage que celles que vous avez spécifiées dans votre déploiement. Si vous

 ©2025 Palo Alto Networks, Inc.

désélectionnez cette option, aucun décryptage ne sera effectué sur les fichiers PCAP, quelles que soient les règles de décryptage que vous avez configurées.



STEP 3 | Pour **Traffic Replication encryption certificate (Certificat de chiffrement de réplication du trafic)**, sélectionnez tout certificat que vous avez ajouté dans la page **Objects (Objets)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Custom Certificates (Certificats personnalisés)** > **Generate (Générer)** ou sélectionnez **Import (Importer)** pour importer le certificat à utiliser pour le décryptage SSL.

Le certificat se compose d'une clé publique et d'une clé privée. Chargez la clé publique dans Prisma Access. Vous devez conserver la clé privée et l'utiliser pour le décryptage lorsque vous téléchargez les fichiers PCAP compressés depuis le compartiment de stockage. De cette manière, vous garantissez que seule votre organisation peut accéder au compartiment de stockage où les fichiers PCAP sont stockés.

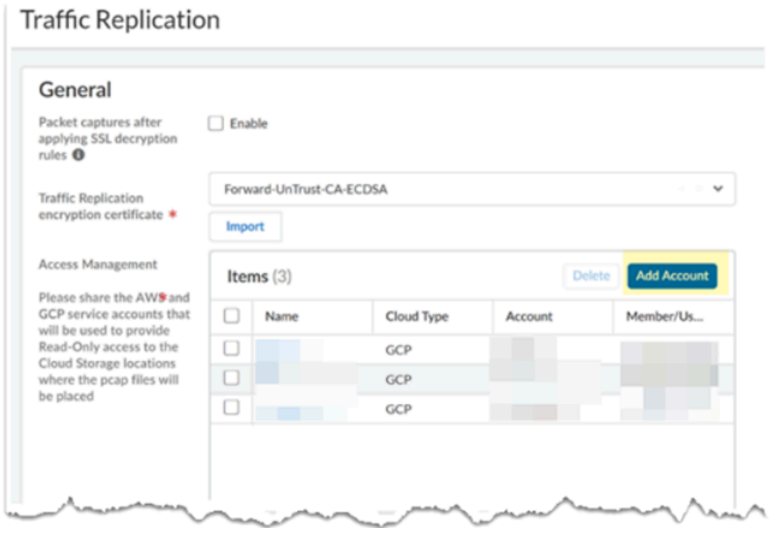
STEP 4 | Configurez le compte de service GCP que vous avez créé à l'étape 1.

La réplication du trafic n'est prise en charge que pour les comptes GCP. Ce compte de service est utilisé pour partager un accès en lecture seule aux compartiments de stockage où les fichiers PCAP sont stockés dans les emplacements où vous avez activé la réplication du trafic. Vous pouvez créer ces comptes de service dans votre compte GCP en utilisant les procédures normales de création de comptes de service GCP. C'est votre responsabilité de contrôler

 ©2025 Palo Alto Networks, Inc.

l'accès des utilisateurs à ces comptes de service. Tout utilisateur ayant à la fois accès aux fichiers PCAP et à la clé privée aura accès aux fichiers PCAP.

1. Dans la section **Access Management (Gestion des accès)**, ajoutez les informations requises dans **Add Account (Ajouter un compte)** pour partager un accès en lecture seule aux compartiments de stockage où les fichiers PCAP sont stockés.



2. Entrez les paramètres suivants :
   - Donnez au compte un **Account Name (Nom du compte)** unique.
   - Spécifiez **GCP** comme **Type** pour le compte.
   - Spécifiez les informations du **Account (Compte)** correspondant au compte de service GCP que vous avez créé.
   - Entrez un nom de **Member/User (Membre/Utilisateur)** pour le compte de service GCP.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | (Facultatif) Si vous souhaitez ajouter des notifications Pub/Sub qui vous préviennent lorsqu'un nouveau dossier ou de nouveaux fichiers sont ajoutés à un compartiment, configurez les notifications Pub/Sub dans votre compte Google Cloud Service.

Prisma Access crée un seul canal Pub/Sub par locataire pour tous les emplacements de ce locataire.

Les notifications Pub/Sub sont prises en charge à partir de Prisma Access 5.2. Si vous avez déjà un compte et que vous souhaitez ajouter des notifications Pub/Sub, faites une mise à niveau vers Prisma Access 5.2, puis choisissez l'une des options suivantes pour ajouter des notifications Pub/Sub :

- *Modifiez le compte de service Google Cloud existant que vous avez déjà configuré dans Prisma Access.*
- *Ajoutez un nouveau compte pour le compte de service existant et spécifiez ce compte dans votre configuration Prisma Access.*

  Si vous ajoutez un nouveau compte, vous devez désactiver la réplication du trafic sur le compte existant et activer la réplication du trafic sur le nouveau compte.
- *Désactivez et activez la réplication du trafic sur l'emplacement existant.*

Prisma Access envoie des messages Pub/Sub avec l'en-tête `panw-traffic-replication-file- notifications-`<*tenantid*>, où <*tenantid*> est l'ID du locataire qui envoie les notifications. Les messages se présentent au format suivant :

```
Message { data: b'' ordering_key: '' attributes:
 { "bucketId": "xxxx-xx-xxx-xxxxxxxxx-us-west1", "eventTime":
 "2024-04-24T23:12:59.xxxxxxx", "eventType": "OBJECT_FINALIZE",
 "notificationConfig": "projects/_/buckets/xxxx-xx-xxx-
xxxxxxxxx-us-west1/notificationConfigs/1", "objectGeneration":
 "xxxxxxxxxxxxxxxx", "objectId": "instance-group-
xxxxxx/12345678_190000_xxxxx.zip", "payloadFormat": "NONE" } }
```

Où :

- `objectGeneration` est le numéro de génération de l'objet modifié.
- `objectID` est le nom de l'objet modifié.

STEP 6 | Configurez la réplication du trafic pour un ou plusieurs emplacements Utilisateurs mobiles.

1. Dans la section **Traffic Replication (Réplication du trafic)**, sélectionnez les emplacements où vous souhaitez activer la réplication du trafic, puis sélectionnez **Mobile Users (Utilisateurs mobiles)**.

   Vous sélectionnez le **Compute Location (Emplacement de calcul)** qui est associé aux **Prisma Access Locations (Emplacements Prisma Access)**. La réplication du trafic est activée pour tous les clients Utilisateurs mobiles connectés aux emplacements sélectionnés.

STEP 7 | Cliquez sur **Save (enregistrer)** pour enregistrer la configuration.

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Validez et appliquez vos modifications.

1. Sélectionnez **Manage (Gestion)** > **Operation (Opérations)** > **Push Config (Transmettre la configuration)**.
2. Sélectionnez **Mobile Users Container (Conteneur d'utilisateurs mobiles)** dans **Push Scope (Étendue de la transmission)**, puis **Push Config (Transmettre la configuration)** et **Push (Transmettre)** pour envoyer vos modifications.
3. Examinez les cibles de transmission et **Push (la transmission)**.

STEP 9 | Vérifiez l'état de la réplication du trafic en allant dans **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access** > **Traffic Replication (Réplication du trafic)**.

STEP 10 | Téléchargez les fichiers PCAP.

Utilisez les **Cloud Storage Links (Liens de stockage Cloud)** pour accéder aux fichiers PCAP dans vos compartiments de stockage GCP.

- Ces compartiments de stockage prennent en charge les mêmes opérations, commandes et requêtes habituelles que tous les autres compartiments de stockage GCP.
- Vous pouvez télécharger des données PCAP pendant 72 heures. Après 72 heures, les fichiers sont définitivement supprimés.
- Les fichiers sont cryptés à l'aide de votre clé publique.
- La taille maximale du fichier est de 200 Mo ou de 5 minutes de capture de paquet, la valeur la plus petite étant retenue.

1. Répertoriez les fichiers de votre service en saisissant `gsutil ls gs://<storage_bucket_link>/`, où *<storage_bucket_link>* est le lien de stockage de votre compte de service GCP où les fichiers sont stockés.
2. Téléchargez les fichiers à partir de votre compte de service en saisissant `gsutil cp gs://<storage_bucket_link>/<file_name> <destination folder>`, où :
   - *<storage_bucket_link>* est le lien de stockage de votre compte de service GCP où les fichiers sont stockés.
   - *<file_name>* est le nom du fichier PCAP.
   - *<destination folder>* est le dossier où vous souhaitez que le fichier PCAP soit téléchargé.
3. Décompressez les fichiers téléchargés.
4. Décryptez les fichiers téléchargés.

Réplication du trafic dans Prisma Access (Panorama)

Pour configurer la réplication du trafic et accéder aux fichiers PCAP, procédez comme suit.

STEP 1 | Intégrez et configurez les utilisateurs mobiles — GlobalProtect (si vous configurez la réplication du trafic pour les utilisateurs mobiles), Réseaux distants (si vous configurez la réplication du trafic pour les réseaux distants) ou les deux (si vous configurez la réplication du trafic pour les utilisateurs mobiles et les réseaux distants).

 ©2025 Palo Alto Networks, Inc.

STEP 2 | (Facultatif) Appliquez le décryptage SSL sur les captures de paquets.

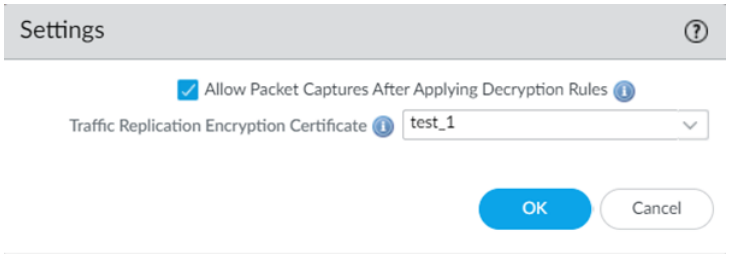
1. Allez dans **Panorama** > **Cloud Services** > **Configuration** > **Traffic Replication (Réplication du trafic)** et cliquez sur l'engrenage pour modifier les **Settings (Paramètres)**.
2. Sélectionnez **Allow packet captures after applying decryption rules (Autoriser les captures de paquets après application des règles de déchiffrement)** pour appliquer vos politiques de décryptage SSL déjà configurées sur les fichiers PCAP.

   Si vous sélectionnez cette option, les fichiers PCAP utiliseront les règles de déchiffrement que vous avez spécifiées dans votre déploiement. Si vous désélectionnez cette option, aucun décryptage ne sera effectué sur les fichiers PCAP, quelles que soient les règles de décryptage que vous avez configurées.

STEP 3 | Sélectionnez le **Traffic Replication Encryption Certificate (Certificat de chiffrement de réplication du trafic)** (clé publique) que vous avez créé lors d'une étape précédente dans **Mobile_User_Template** (pour les déploiements d'utilisateurs mobiles) ou **Remote_Network_Template** (pour les déploiements de réseau à distance) à utiliser pour le décryptage SSL.

Cette étape est obligatoire. Vous pouvez sélectionner n'importe quel certificat que vous avez ajouté dans la section **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats du périphérique)** de **Mobile_User_Template** ou **Remote_Network_Template**. Si vous activez la réplication du trafic pour les utilisateurs mobiles et les réseaux distants, placez le certificat dans **Mobile_User_Template** et **Remote_Network_Template**..

Le certificat se compose d'une clé publique et d'une clé privée. Chargez la clé publique dans Prisma Access ; vous conservez la clé privée et l'utilisez pour le décryptage lorsque vous téléchargez les fichiers PCAP compressés à partir du compartiment de stockage. De cette façon, vous garantissez que seule votre organisation peut accéder au compartiment de stockage où les fichiers PCAP sont stockés.



STEP 4 | Configurez la réplication du trafic pour un ou plusieurs emplacements Utilisateurs mobiles — GlobalProtect, emplacements réseau distants ou les deux en sélectionnant l'emplacement dans la section **Configuration** et en sélectionnant les emplacements où vous souhaitez activer la réplication du trafic, puis en sélectionnant **MU-GP**, **RN**, ou les deux.

Sélectionnez le **Compute Location (Emplacement de calcul)** associé aux **Prisma Access Locations (Emplacements Prisma Access)**. La réplication du trafic est activée pour tous les

 ©2025 Palo Alto Networks, Inc.

clients Utilisateurs mobiles — GlobalProtect, utilisateurs du réseau distants ou les deux, qui sont connectés aux emplacements sélectionnés.

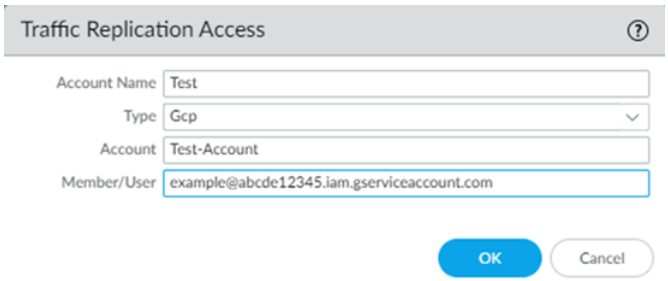


STEP 5 | Ajoutez un compte qui vous permet d'accéder aux données de capture de paquets de réplication du trafic (PCAP).

Ce compte de service est utilisé pour partager l'accès en lecture seule aux compartiments de stockage où les fichiers PCAP sont stockés dans les emplacements où vous avez activé la réplication du trafic. Vous créez ces comptes de service dans votre compte GCP à l'aide des Procédures de création de compte de service GCP. Il est de votre responsabilité de contrôler quels utilisateurs ont accès à ces comptes de service. Tous les utilisateurs qui ont à la fois accès aux fichiers PCAP et à la clé privée auront accès aux fichiers PCAP.

1. Dans la section **Traffic Replication Access (Accès à la réplication du trafic)**, sélectionnez **Add (Ajouter)** pour ajouter un compte.
2. Entrez les paramètres suivants :
   - Donnez au compte un **Account Name (Nom du compte)** unique.
   - Spécifiez **Gcp** comme **Type** pour le compte.

     La réplication du trafic n'est prise en charge que pour les comptes GCP.
   - Spécifiez les informations du **Account (Compte)** correspondant au compte de service GCP que vous avez créé.
   - Entrez un nom de **Member/User (Membre/Utilisateur)** pour le compte de service GCP.



 ©2025 Palo Alto Networks, Inc.

STEP 6 | (Facultatif) Si vous souhaitez ajouter des notifications Pub/Sub qui vous préviennent lorsqu'un nouveau dossier ou de nouveaux fichiers sont ajoutés à un compartiment, configurez les notifications Pub/Sub dans votre compte Google Cloud Service.

Prisma Access crée un seul canal Pub/Sub par locataire pour tous les emplacements de ce locataire.

Les notifications Pub/Sub sont prises en charge à partir de Prisma Access 5.2. Si vous avez déjà un compte et que vous souhaitez ajouter des notifications Pub/Sub, faites une mise à niveau vers Prisma Access 5.2, puis choisissez l'une des options suivantes pour ajouter des notifications Pub/Sub :

- *Modifiez le compte de service Google Cloud existant que vous avez déjà configuré dans Prisma Access.*
- *Ajoutez un nouveau compte pour le compte de service existant et spécifiez ce compte dans votre configuration Prisma Access.*

  Si vous ajoutez un nouveau compte, vous devez désactiver la réplication du trafic sur le compte existant et activer la réplication du trafic sur le nouveau compte.
- *Désactivez et activez la réplication du trafic sur l'emplacement existant.*

Prisma Access envoie des messages Pub/Sub avec l'en-tête `panw-traffic-replication-file- notifications-`<*tenantid*>, où <*tenantid*> est l'ID du locataire qui envoie les notifications. Les messages se présentent au format suivant :

```
Message { data: b'' ordering_key: '' attributes:
 { "bucketId": "xxxx-xx-xxx-xxxxxxxxx-us-west1", "eventTime":
 "2024-04-24T23:12:59.xxxxxxx", "eventType": "OBJECT_FINALIZE",
 "notificationConfig": "projects/_/buckets/xxxx-xx-xxx-
xxxxxxxxx-us-west1/notificationConfigs/1", "objectGeneration":
 "xxxxxxxxxxxxxxxx", "objectId": "instance-group-
xxxxxxx/12345678_190000_xxxxx.zip", "payloadFormat": "NONE" } }
```

Où :

- `objectGeneration` est le numéro de génération de l'objet modifié.
- `objectID` est le nom de l'objet modifié.

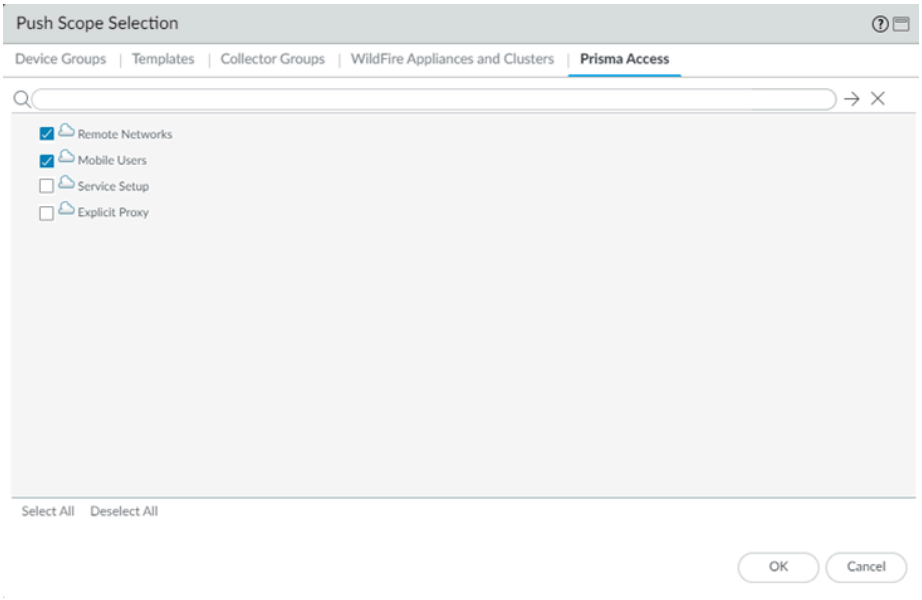
STEP 7 | Validez et appliquez vos modifications, en vous assurant que **Mobile Users (Utilisateurs mobiles)** (pour un déploiement d'utilisateur mobile), **Remote Networks (Réseaux distants)** (pour un déploiement de réseaux distants), ou les deux sont sélectionnés dans **Push Scope (Étendue de la transmission)**.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)**.

 ©2025 Palo Alto Networks, Inc.

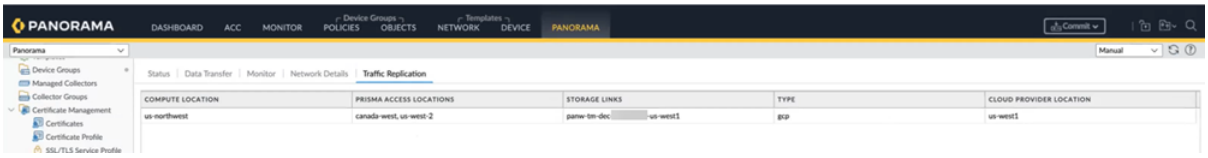
2. **Edit Selections (Modifier les sélections)** et, dans l'onglet **Prisma Access** , assurez-vous que **Mobile Users (Utilisateurs mobiles)** et **Remote Networks (Réseaux distants)** sont sélectionné(s) dans **Push Scope (Étendue de la transmission)**, puis cliquez sur **OK**.

   Il est possible que **Push Scope (Étendue de la transmission)** ne soit pas sélectionné automatiquement.



3. Cliquez sur **Commit and Push (Valider et appliquer)**.

STEP 8 | Vérifiez l'état de la réplication du trafic en accédant à **Panorama** > **Cloud Services** > **Status (État)** > **Traffic Replication (Réplication du trafic)**.



Les **Storage Links (Liens de stockage)** correspondent au nom du compartiment de stockage GCP où vous pouvez accéder aux fichiers PCAP, tandis que le **Cloud Provider Location (Emplacement du fournisseur de cloud)** est l'emplacement où l'instance GCP est intégrée.

 ©2025 Palo Alto Networks, Inc.

STEP 9 | Téléchargez les fichiers PCAP à l'aide de la clé privée que vous seul possédez.

Utilisez les **Storage Links (Liens de stockage)** pour accéder aux fichiers PCAP dans vos compartiments de stockage GCP.

- Ces compartiments de stockage prennent en charge les mêmes opérations, commandes et requêtes habituelles que tous les autres compartiments de stockage GCP.
- Vous pouvez télécharger les données PCAP pendant un maximum de 72 heures. Après 72 heures, les fichiers sont définitivement supprimés.
- Les fichiers sont cryptés à l'aide de votre clé publique.
- La taille maximale du fichier est de 200 Mo ou de 5 minutes de capture de paquet, la valeur la plus petite étant retenue.

1. Répertoriez les fichiers de votre service en saisissant `gsutil ls gs://<storage_bucket_link>/`, où <*storage_bucket_link*> est le lien de stockage de votre compte de service GCP où les fichiers sont stockés.
2. Téléchargez les fichiers à partir de votre compte de service en saisissant `gsutil cp gs://<storage_bucket_link>/<file_name> <destination folder>`, où :
   - <*storage_bucket_link*> est le lien de stockage de votre compte de service GCP où les fichiers sont stockés.
   - <*file_name*> est le nom du fichier PCAP.
   - <*destination folder*> est le dossier dans lequel vous souhaitez télécharger le fichier PCAP.
3. Décompressez les fichiers téléchargés.
4. Décryptez les fichiers téléchargés à l'aide de la clé privée que vous seul possédez.

 ©2025 Palo Alto Networks, Inc.

Prisma Access Déploiements avancés de réseau à distance

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Les sections suivantes vous montrent les déploiements avancés disponibles pour Prisma Access Réseaux distants :

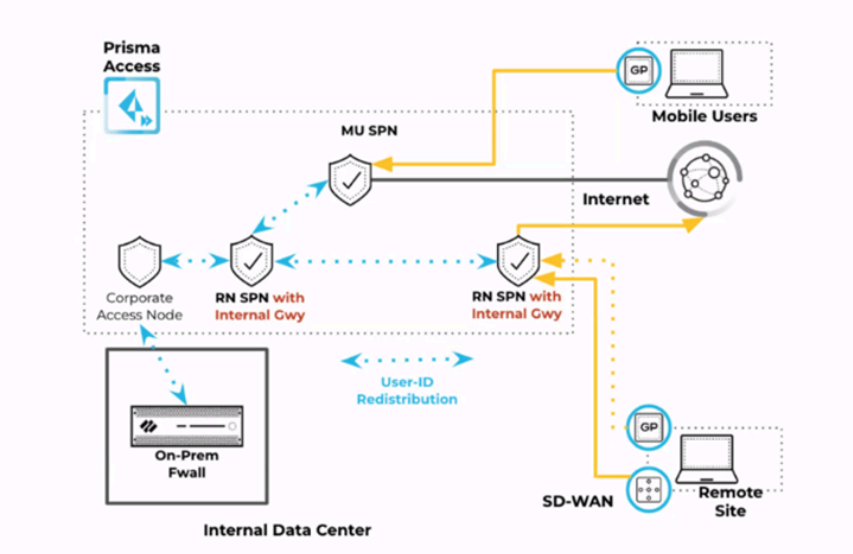
- Fournir un accès sécurisé entrant aux emplacements réseau distants
- Créer un réseau à large bande passante pour un site distant

Passerelle interne Prisma Access

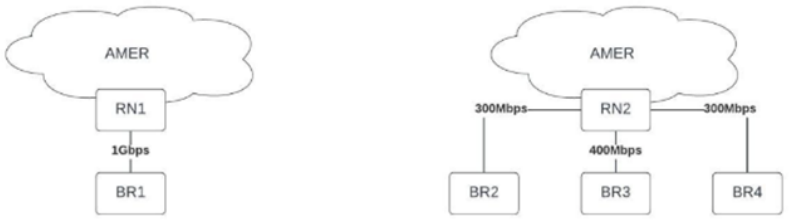
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access et utilisateur mobile ❑ Minimum Required Prisma Access Version : 5.1 ❑ Version du plan de données minimum requise pour Prisma Access (Managed by Panorama) : 10.2.4 ❑ Version minimale requise du client GlobalProtect : 6.0

Auparavant, pour générer des mappages d'utilisateurs IP et HIP pour les hôtes exécutant le logiciel client GlobalProtect dans les réseaux distants Prisma Access, vous devez déployer un NGFW sur site comme passerelle interne. Cette solution n'est pas native du cloud. Grâce à la passerelle interne Prisma Access native au cloud, vous pouvez éviter d'utiliser des passerelles internes sur site, et la passerelle interne Prisma Access génère les mappages des utilisateurs IP et les HIP localement dans les réseaux distants. Les réseaux distants consomment des mappages d'utilisateurs IP et des HIP de la base de données locale pour les contrôles de posture au lieu de les apprendre à partir d'autres pare-feu.

 ©2025 Palo Alto Networks, Inc.

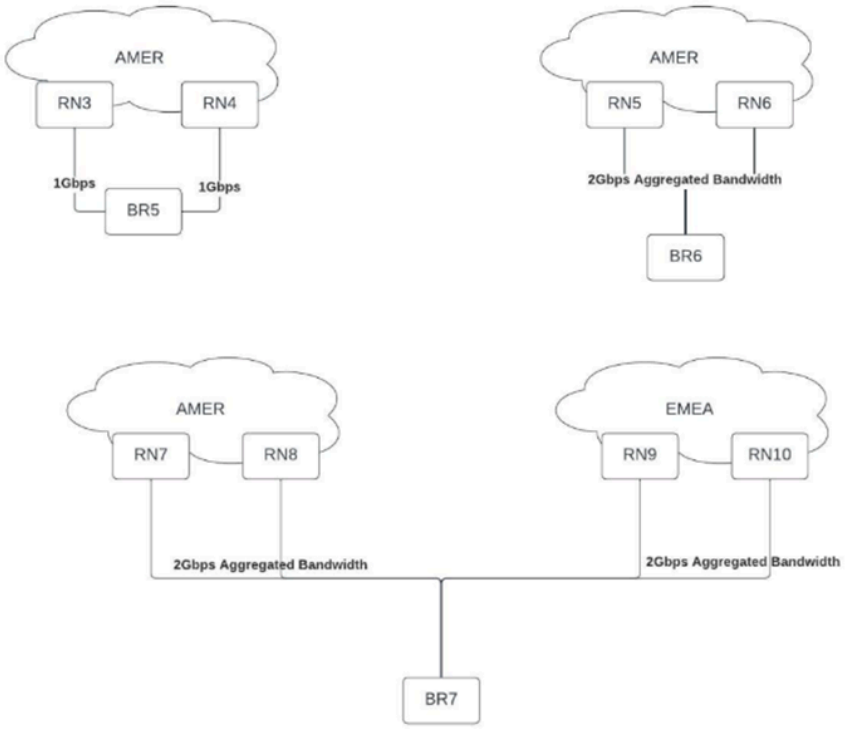


Notez que vous ne pouvez pas déployer une passerelle interne lorsqu'un site distant dispose de plusieurs tunnels IPsec vers différents sites de réseau distant (par exemple, un tunnel actif/actif) ou un site à bande passante élevée. Le diagramme suivant montre un exemple d'environnement pris en charge pour un déploiement de passerelle interne.



Le diagramme suivant donne des exemples de déploiements dans lesquels les passerelles internes ne sont pas prises en charge.

 ©2025 Palo Alto Networks, Inc.



Avant de configurer la passerelle interne Prisma Access, embarquez vos utilisateurs mobiles.

- Strata Cloud Manager
- Panorama

Passerelle interne Prisma Access (Strata Cloud Manager)

Suivez les étapes suivantes pour configurer la passerelle interne Prisma Access.

STEP 1 | Dans Strata Cloud Manager, configurez GlobalProtect, ajoutez des paramètres d'application et intégrez des réseaux distants.

Notez qu'il n'existe actuellement aucune détection d'hôte interne ni de configuration de passerelle interne.

STEP 2 | Prenez note de **Remote Networks DNS IP Address (Adresse IP DNS des réseaux distants)** à partir de **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access**.

STEP 3 | Prenez note des **Gateway FQDNs (FQDN de la passerelle)** à partir de **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Infrastructure** > **GlobalProtect** > **Infrastructure Settings (Paramètres d'infrastructure)** > **Gateway FQDNs (FQDN de la passerelle)**.

STEP 4 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Remote Networks (Réseaux distants)** > **Advanced Settings (Paramètres avancés)**.

 ©2025 Palo Alto Networks, Inc.

STEP 5 | Modifiez les paramètres de la **Prisma Access Internal Gateway (Passerelle interne Prisma Access)** pour activer la passerelle interne et **Save (Enregistrer)** les modifications.

(Facultatif) **Enable Internal Host Detection (Activez la détection d'hôte interne)** pour IPv4 si vous ne souhaitez pas utiliser votre propre serveur DNS. Vous pouvez activer la détection de l'hôte interne seulement après avoir sélectionné **Enable Internal Gateway (Activer la passerelle interne)**.

*Prisma Access prend en charge la détection de l'hôte interne uniquement pour la méthode de connexion **Always On (Toujours activé)**.*

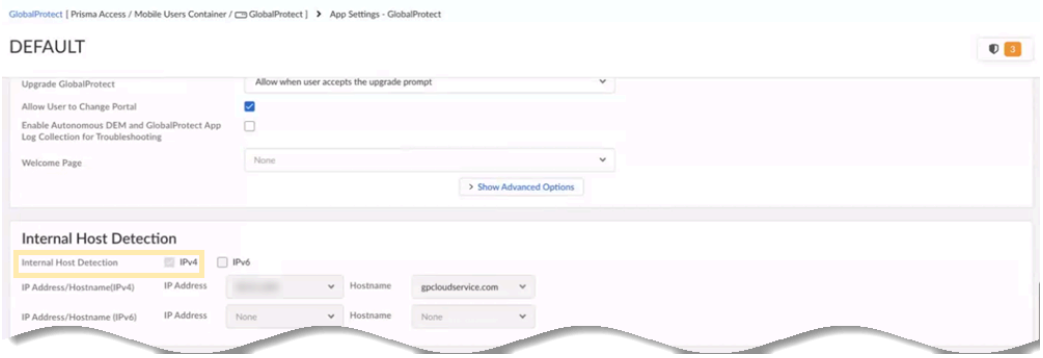


Lorsque vous activez la passerelle interne, les instances du réseau distant agissent comme des passerelles internes. Lorsque vous activez la détection d'hôte interne, Prisma Access crée des enregistrements PTR sur les serveurs proxy DNS du réseau distant pour le processus de détection de l'hôte interne.

STEP 6 | Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Application GlobalProtect)**.

STEP 7 | Sélectionnez un paramètre d'application et affichez les détails de la détection de l'hôte interne et de la passerelle interne.

Lorsque vous activez la passerelle interne et la détection de l'hôte interne à l'étape 5Prisma Access permet également la détection de l'hôte interne IPv4 et la passerelle interne ici. Prisma Access renseigne la valeur de **Remote Networks DNS IP Address (Adresse IP DNS des réseaux distants)**, de l'étape 2, comme adresse IP.

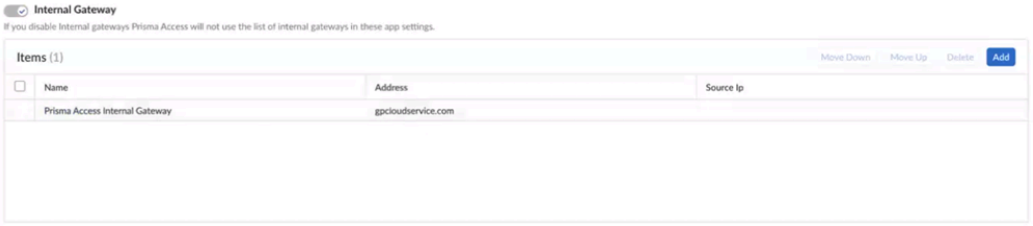


Notez que la détection de l'hôte interne IPv6 sur les proxys DNS Prisma Access ne sont pas pris en charge.

Vous ne pouvez pas supprimer cette entrée**Prisma Access Internal Gateway (Passerelle interne Prisma Access)**. Cependant, vous pouvez ajouter vos passerelles internes auto-déployées. Vous pouvez déployer vos propres serveurs DNS dans le réseau interne pour

 ©2025 Palo Alto Networks, Inc.

la détection de l'hôte interne, mais veillez à ajouter des enregistrements PTR afin que la détection de l'hôte interne soit possible. Prisma Access ajoute la valeur des **Gateway FQDNs (FQDN de la passerelle)**, de l'étape 3, à l'adresse.



Vous pouvez afficher les détails de l'adresse IP du serveur proxy DNS en sélectionnant **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Prisma Access**.

Si vous activez la **Internal Host Detection (Détection de l'hôte interne)**, vérifiez que la résolution DNS fonctionne, effectuez une recherche DNS inversée à partir de votre réseau interne vers l'IP du serveur proxy DNS et assurez-vous qu'elle renvoie un FQDN commençant par **`any-igw`**.

STEP 8 | Vous devez **Push (Transmettre)** les modifications apportées aux utilisateurs mobiles et aux réseaux distants en même temps.

STEP 9 | Connectez-vous au terminal.

Lorsque vous vous connectez à GlobalProtect, vous vous authentifiez d'abord auprès du portail GlobalProtect. La détection de l'hôte interne déclenche la connexion de GlobalProtect à la passerelle interne. Ensuite, pendant que l'agent GlobalProtect continue de fonctionner en mode non tunnel, la deuxième authentification s'affiche et soumet les informations de l'hôte à la passerelle interne sur les réseaux distants.

Passerelle interne Prisma Access (Panorama)

STEP 1 | Dans Panorama, configurez GlobalProtect, ajoutez des paramètres d'application et intégrez des réseaux distants.

Notez qu'il n'existe actuellement aucune détection d'hôte interne ni de configuration de passerelle interne.

STEP 2 | Accédez à **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** > **Settings (Paramètres)**.

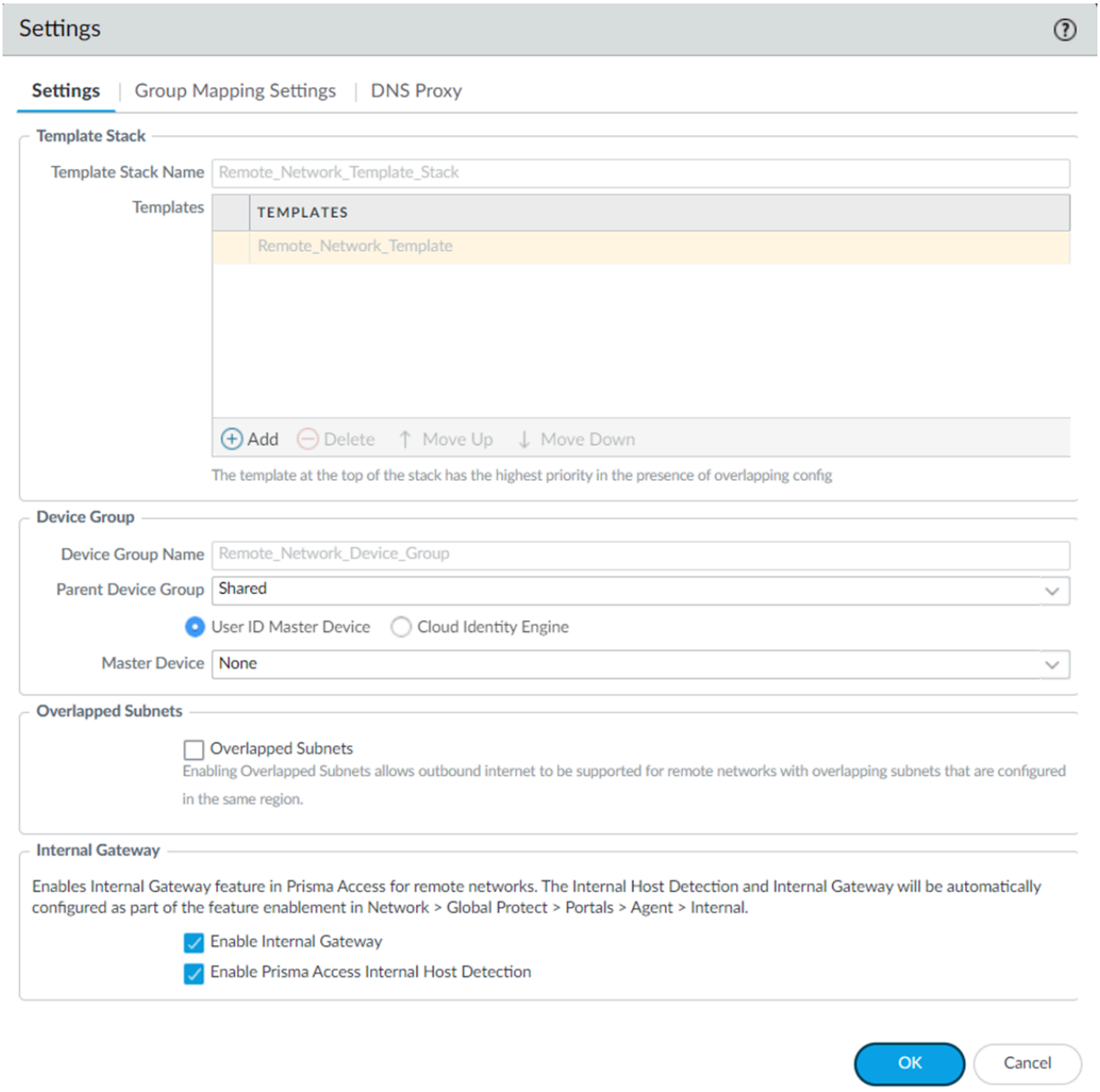
STEP 3 | Cliquez sur **Enable Internal Gateway (Activer la passerelle interne)** pour l'activer et enregistrez les modifications.

(Facultatif) **Enable Prisma Access Internal Host Detection (Activez la détection d'hôte interne Prisma Access)** pour IPv4 si vous ne souhaitez pas utiliser votre propre serveur DNS. Vous

 ©2025 Palo Alto Networks, Inc.

pouvez activer la détection de l'hôte interne seulement après avoir sélectionné **Enable Internal Gateway (Activer la passerelle interne)**.

*Prisma Access prend en charge la détection de l'hôte interne uniquement pour la méthode de connexion **Always On (Toujours activé)**.*



Lorsque vous activez la passerelle interne, les instances du réseau distant agissent comme des passerelles internes. Lorsque vous activez la détection de l'hôte interne, Prisma Access crée des enregistrements PTR sur les serveurs proxy DNS du réseau distant pour le processus de détection de l'hôte interne.

Lorsque vous activez la passerelle interne, Prisma Access crée une configuration de passerelle interne dans un modèle de réseau distant.

 ©2025 Palo Alto Networks, Inc.

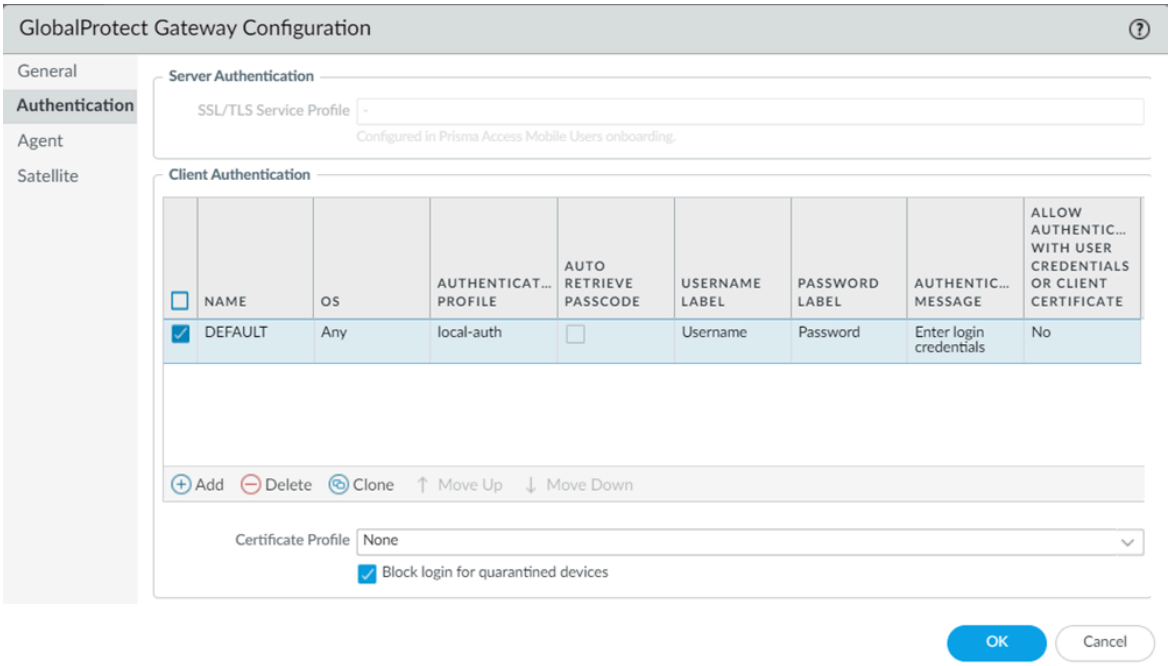
STEP 4 | Accédez à **Templates (Modèles)** > **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** et sélectionnez **Remote_Network_Template**.

Vous trouverez le modèle **GlobalProtect_Internal_Gateway** créé pour la passerelle interne.

 ©2025 Palo Alto Networks, Inc.

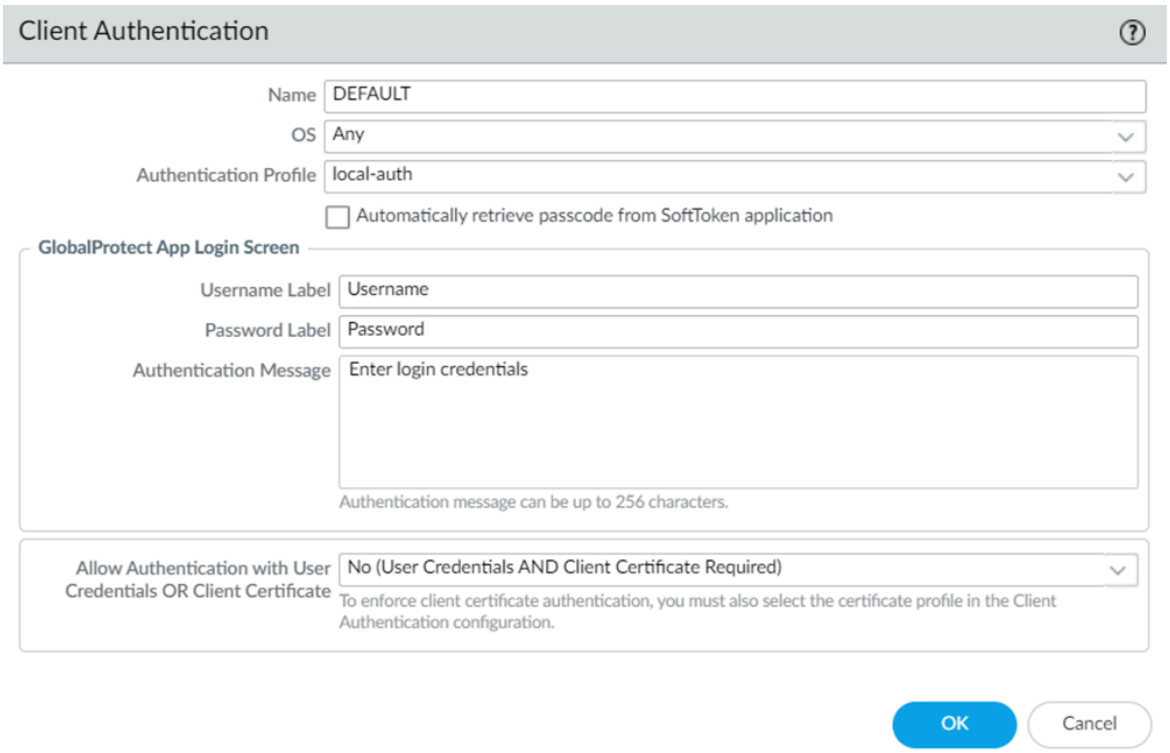
STEP 5 | Créez un profil d'authentification pour ce modèle de réseau distant similaire au profil d'authentification du modèle d'utilisateur mobile.

1. Sélectionnez le modèle de réseau distant, le modèle **GlobalProtect_Internal_Gateway**, le lien hypertexte.
2. Accédez à **Authentication (Authentification)** > **Client Authentication (Authentification du client)**.

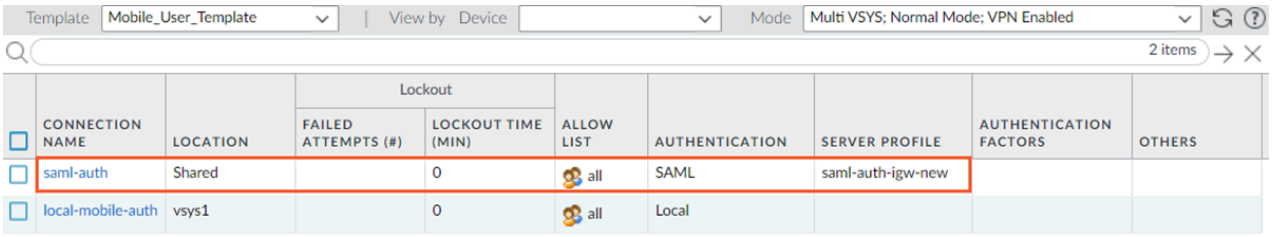


3. Modifiez les détails du profil d'authentification de l'authentification du client **DEFAULT (PAR DÉFAUT)**.

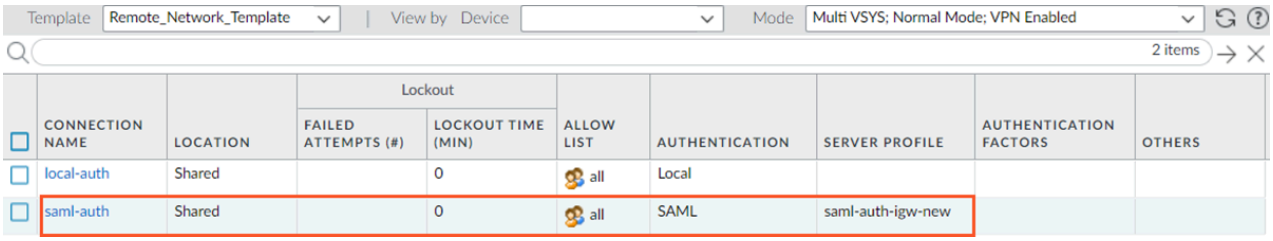
 ©2025 Palo Alto Networks, Inc.



Créez un profil d'authentification identique à celui du modèle d'utilisateur mobile. Vous trouverez le profil d'authentification utilisé dans le modèle d'utilisateur mobile sous **Template (Modèle)** > **Device (Périphérique)** > **Profil d'authentification (Authentication profile)**. Assurez-vous de sélectionner **Mobile_User_Template**.



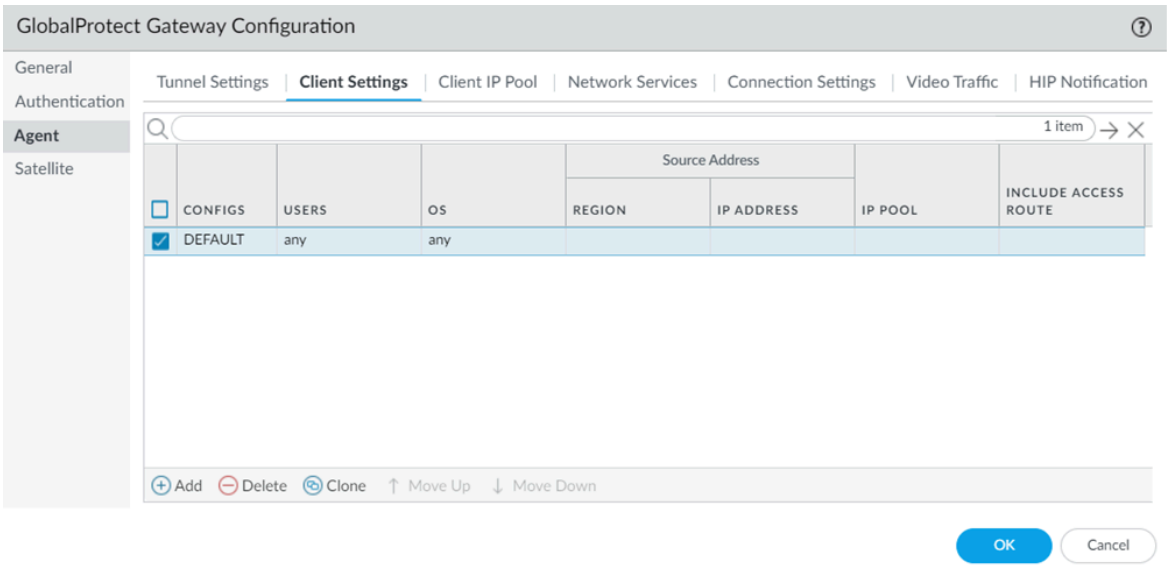
Vous pouvez également afficher le profil d'authentification du modèle de réseau distant en sélectionnant ***Templates (Modèles)*** *>* ***Device (Périphérique)*** *>* ***Authentication profile (Profil d'authentification)****. Sélectionnez* ***Remote_Network_Template****.*



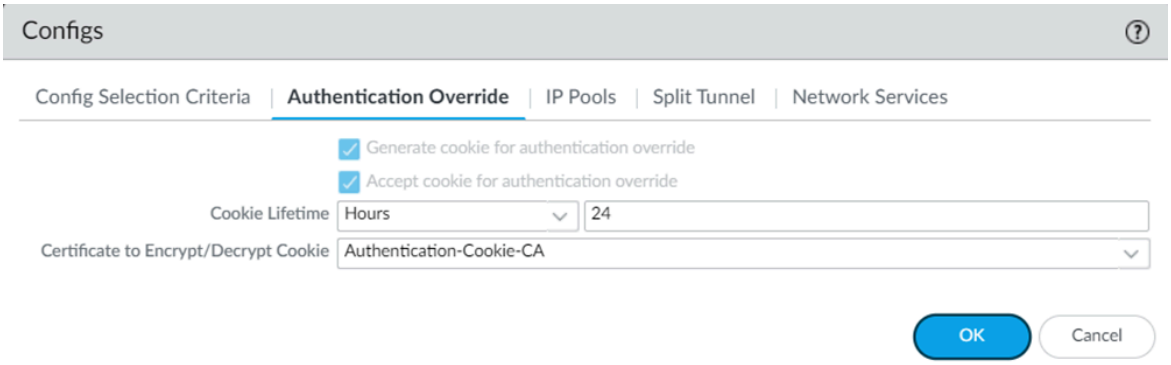
 ©2025 Palo Alto Networks, Inc.

STEP 6 | Créez un certificat de périphérique pour le modèle de réseau distant similaire au certificat de périphérique du modèle d'utilisateur mobile.

1. Sélectionnez le modèle de réseau distant, **GlobalProtect_Internal_Gateway**, le lien hypertexte.
2. Accédez à **Agent** > **Client Settings (Paramètres du client)**.



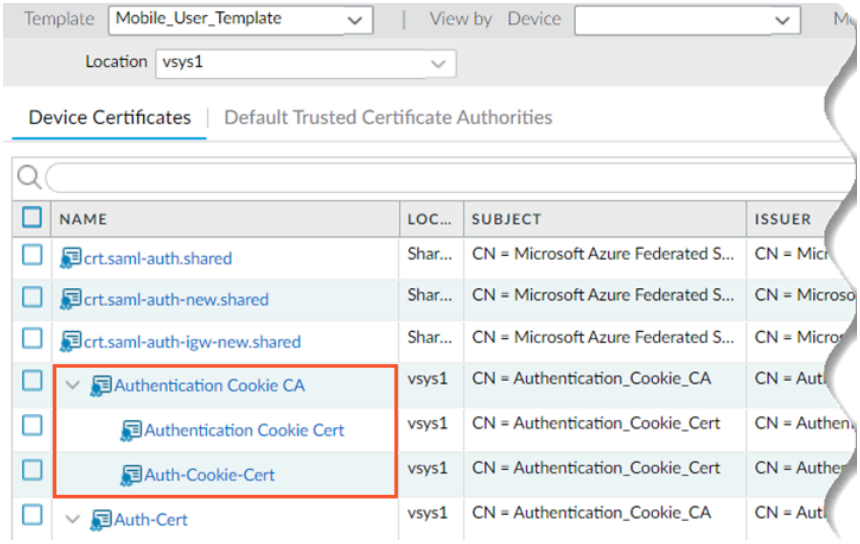
3. Sélectionnez la configuration **DEFAULT (PAR DÉFAUT)**, puis accédez aux paramètres **Authentication Override (Contournement d'authentification)**.
4. Modifiez les paramètres du **Certificate to Encrypt/Decrypt Cookie (Certificat pour crypter/décrypter le cookie)** et créez un nouveau certificat de périphérique.



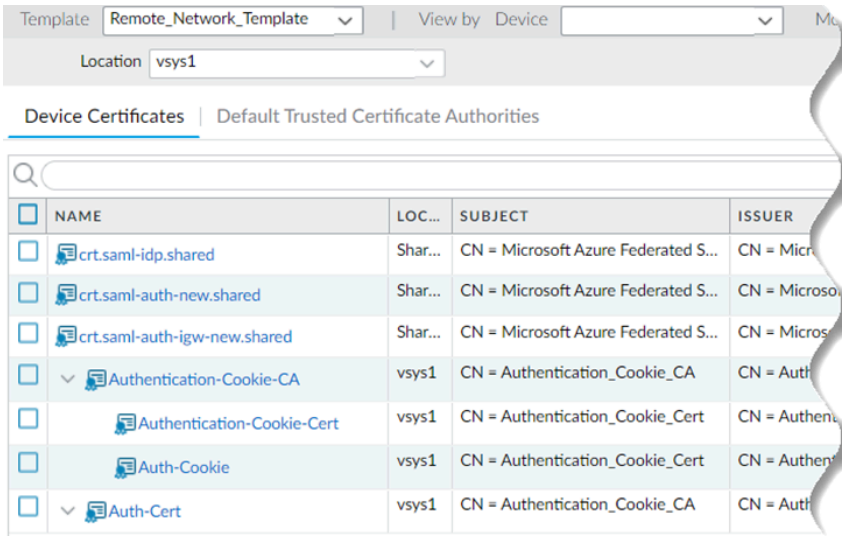
Créez un certificat de périphérique identique à celui du modèle d'utilisateur mobile. Vous trouverez le certificat de périphérique utilisé dans le modèle d'utilisateur mobile sous **Template (Modèle)** > **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphériques)**. Assurez-vous de sélectionner **Mobile_User_Template**. La configuration **DEFAULT (PAR DÉFAUT)** fait référence au certificat **Authentication Cookie CA (Cookie**

 ©2025 Palo Alto Networks, Inc.

d'authentification CA). Suivez la même hiérarchie que celle de **Mobile_User_Template** pour une authentification réussie.



*Vous pouvez également afficher le certificat de périphérique pour le modèle de réseau distant en sélectionnant **Template (Modèle)** > **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphériques)**. Sélectionnez **Remote_Network_Template**.*



STEP 7 | Vous devez **Push (Transmettre)** les modifications apportées aux utilisateurs mobiles et aux réseaux distants en même temps.

 ©2025 Palo Alto Networks, Inc.

Fournir un accès sécurisé entrant aux emplacements réseau distants

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access incluant l'interconnexion réseau pour l'accès Site-à-Site et Utilisateur-à-Site

Si votre organisation héberge des applications accessibles sur Internet à un site réseau distant, fournir l'accès à ces applications expose votre réseau à toutes les menaces posées par un Internet ouvert. Cette section décrit comment Prisma Access fournit un moyen d'accéder de manière sécurisée à ces applications, quand vous devriez l'implémenter et comment le configurer.

- Accès entrant sécurisé pour les sites réseau distants
- Exemples d'accès entrant sécurisé
- Directives pour l'utilisation de l'accès entrant sécurisé
- Configurer l'accès entrant sécurisé pour les sites de réseaux distants

Accès entrant sécurisé pour les sites réseau distants

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• La licence Prisma Access qui inclut Net Interconnect pour l'accès de site à site et d'utilisateur à site

Prisma Access pour les réseaux distants permet l'accès sortant aux applications connectées à Internet. Dans certains cas, votre organisation peut avoir besoin de fournir un accès entrant à une application ou à un site Web sur un site distant, et de fournir un accès sécurisé à cette application à tout utilisateur connecté à Internet, et pas seulement aux utilisateurs protégés par Prisma Access. Par exemple :

- Vous hébergez une application ou un portail personnalisé public sur un site réseau distant.
- Vous disposez d'un labo ou d'un environnement intermédiaire pour lequel vous souhaitez fournir un accès sécurisé.
- Vous devez fournir l'accès à une application ou à un site Web à des utilisateurs qui ne sont pas membres d'un domaine organisationnel.
- Vous avez des périphériques IoT qui nécessitent l'accès à une application interne de gestion des actifs, de suivi ou d'état.

Pour ce faire, créez un réseau distant qui permet un accès entrant sécurisé. Si vous avez besoin d'un accès sortant et d'un accès entrant pour un site réseau distant, créez deux réseaux distants au même emplacement, l'un pour l'accès entrant et l'autre pour l'accès sortant.

 ©2025 Palo Alto Networks, Inc.

Bien que cette solution puisse fournir un accès à un maximum de 50 000 sessions entrantes simultanées par réseau distant, Palo Alto Networks ne recommande pas l'utilisation de cette solution pour fournir l'accès à une application ou à un site Web à volume élevé.

Exemples d'accès entrant sécurisé

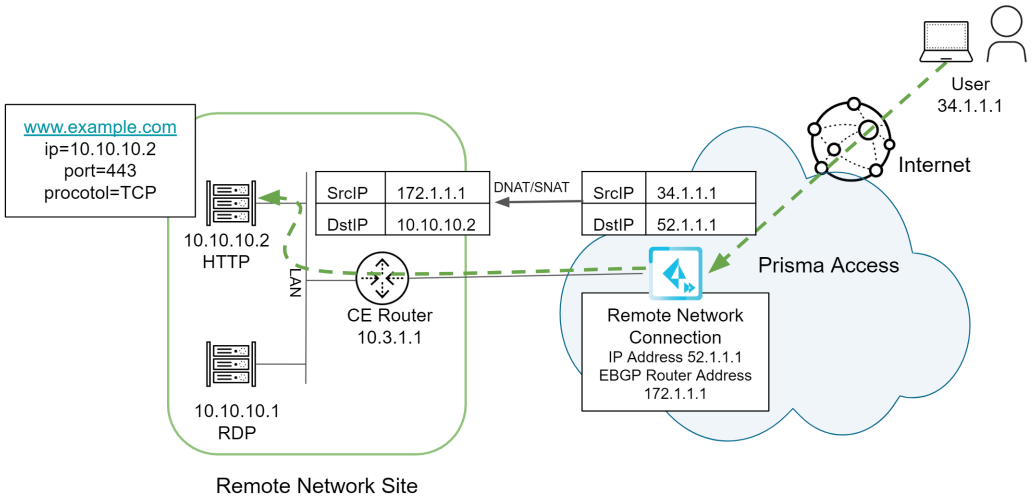
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• LicencePrisma Access qui inclut Net Interconnect pour l'accès site à site et utilisateur à site

Cette section fournit des exemples d'accès entrant, ainsi que les adresses IP que Prisma Access affecte à divers déploiements.

L'exemple suivant montre un exemple de configuration pour activer l'accès entrant pour une application (www.example.com) sur un site réseau distant. Vous attribuez une adresse IP de 10.10.10.2, un port de 443 et un protocole TCP à l'application. Vous entrez ensuite ces valeurs dans Prisma Access lorsque vous configurez l'accès entrant. Après avoir enregistré et validé vos modifications, Prisma Access attribue une adresse IP publique à l'application que vous avez définie, dans ce cas 52.1.1.1.

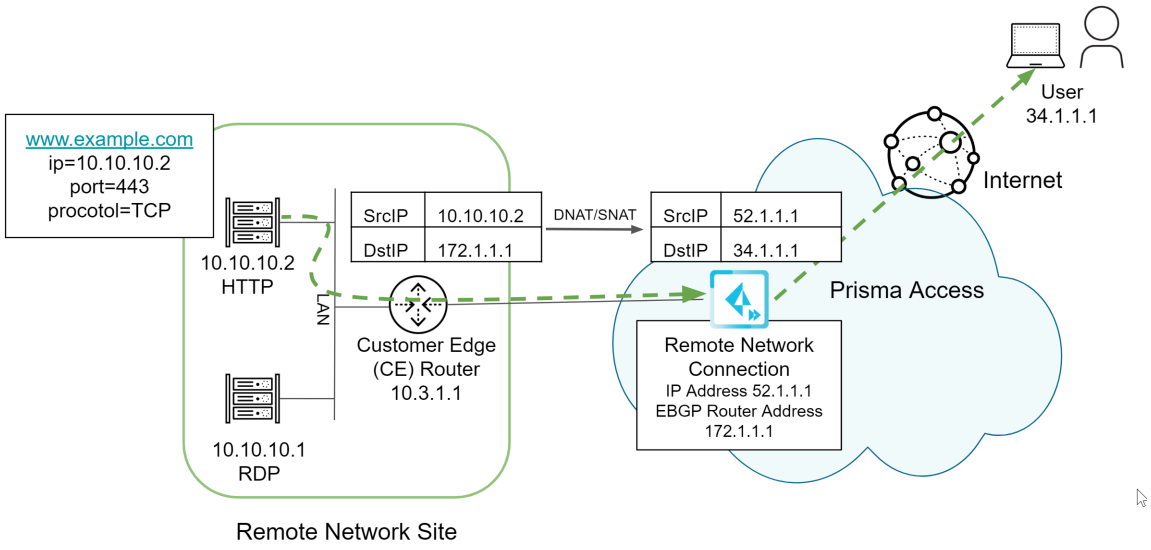
Prisma Access effectue la traduction d'adresse réseau source (NAT source) sur les paquets par défaut. Si le périphérique compatible IPSec sur votre site réseau distant est capable d'effectuer un retour symétrique (comme un pare-feu de la nouvelle génération Palo Alto Networks), vous pouvez désactiver la NAT source.

La figure suivante montre le flux de trafic des utilisateurs vers les applications. Étant donné que la NAT source est activée, l'adresse IP source dans la table de routage passe de l'IP du périphérique de l'utilisateur (34.1.1.1) à l'adresse **EBGP Router (Routeur EBGP)** du réseau distant (**Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails réseau)** > **Remote Networks (Réseaux à distance)** > **EBGP Router (Routeur EBGP)**). (172.1.1.1).

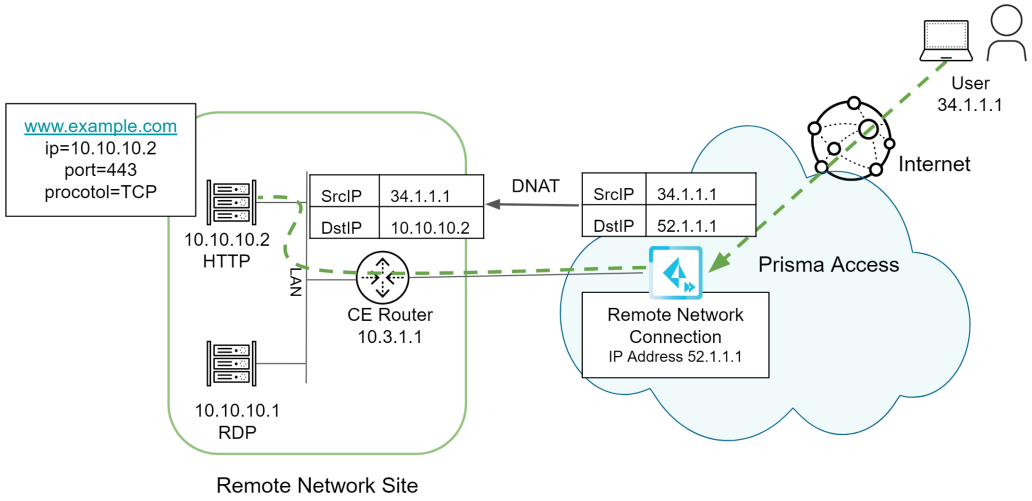


La figure suivante montre le chemin de retour du trafic avec la NAT source activée.

 ©2025 Palo Alto Networks, Inc.

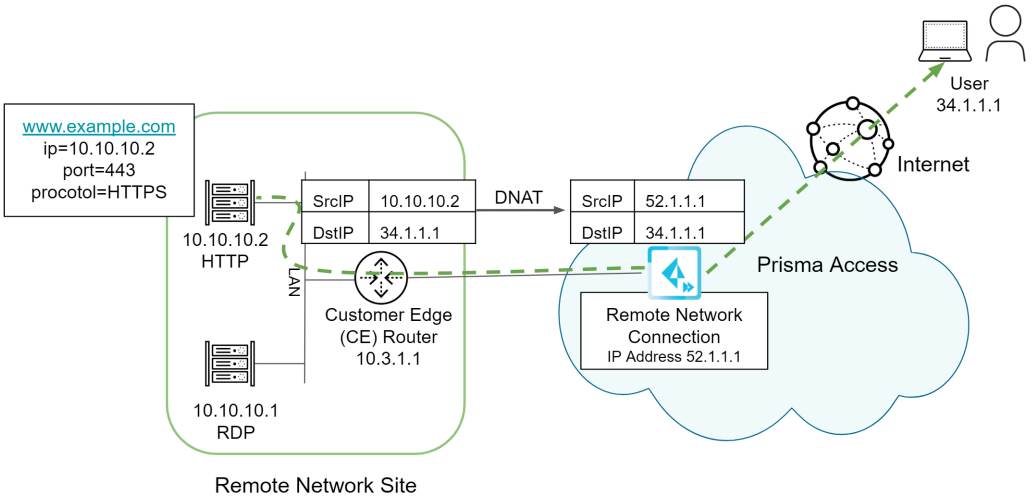


Si vous désactivez la NAT source, Prisma Access exécute toujours la NAT de destination, mais l'adresse IP source de la requête reste inchangée.



Pour le trafic de retour, SNAT est désactivée et l'adresse de destination de toutes les tables de routage est l'adresse IP de l'utilisateur (34.1.1.1).

 ©2025 Palo Alto Networks, Inc.



Si vous disposez d'une ressource qui se trouve sur un site réseau distant sur lequel l'accès entrant est activé et que vous souhaitez que les utilisateurs des sites d'accès non entrant aient accès à cette ressource, vous pouvez **Allow inbound flows to other Remote Networks over the Prisma Access backbone (Autoriser les flux entrants vers d'autres réseaux distants via le backbone Prisma Access)** lorsque vous configurez le réseau distant d'accès non entrant.

Si vous autorisez les flux entrants provenant d'autres réseaux distants, vous devez activer la NAT source.



Directives pour l'utilisation de l'accès entrant sécurisé

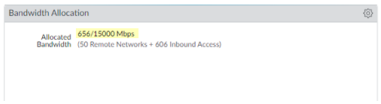
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Licence Prisma Access qui inclut l'interconnexion réseau pour l'accès Site à site et Utilisateur à site

Utilisez les directives et restrictions suivantes lorsque vous configurez un réseau distant pour utiliser un accès entrant sécurisé :

- Lorsque vous configurez un réseau distant pour l'accès entrant, vous ajoutez des unités (Mbps, Mbit/s) de votre licence pour les adresses IP que vous allouez (150 Mbit/s pour 5 adresses IP et 300 Mbit/s pour 10 adresses IP). Pour cette raison, assurez-vous que vous disposez de suffisamment de bande passante sous licence restante pour intégrer les réseaux distants d'accès entrant avant de commencer. Pour vérifier votre bande passante disponible, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** et affichez votre **Bandwidth Allocation (Allocation de bande passante)** sous licence.

 ©2025 Palo Alto Networks, Inc.

Cette zone affiche la bande passante que vous avez déjà allouée, ainsi que la bande passante totale sous licence.



- L'accès entrant sécurisé utilise un sous-ensemble d'emplacements Prisma Access.
- Vous ne pouvez pas modifier un réseau distant existant pour fournir un accès entrant sécurisé ; créez plutôt un nouveau réseau distant.
- La fonctionnalité d'accès entrant n'est pas disponible sur les réseaux distants qui utilisent l'équilibrage de charge ECMP.
- La traduction du port d'application n'est pas prise en charge.
- La fonctionnalité d'importation en masse vers les réseaux distants intégrés ne prend pas en charge l'accès entrant. Utilisez Panorama pour intégrer de nouveaux réseaux distants d'accès entrant.
- N'utilisez pas l'accès entrant au réseau distant avec des règles de transfert de trafic avec des connexions aux services.
- Le trafic sortant provenant de la branche n'est pas autorisé sur le réseau distant entrant.
- L'authentification par User-ID et par application n'est pas prise en charge.
- Prisma Access applique les seuils de limitation de débit suivants pour assurer une protection contre la saturation et mesure le débit en connexions par seconde (CPS) :

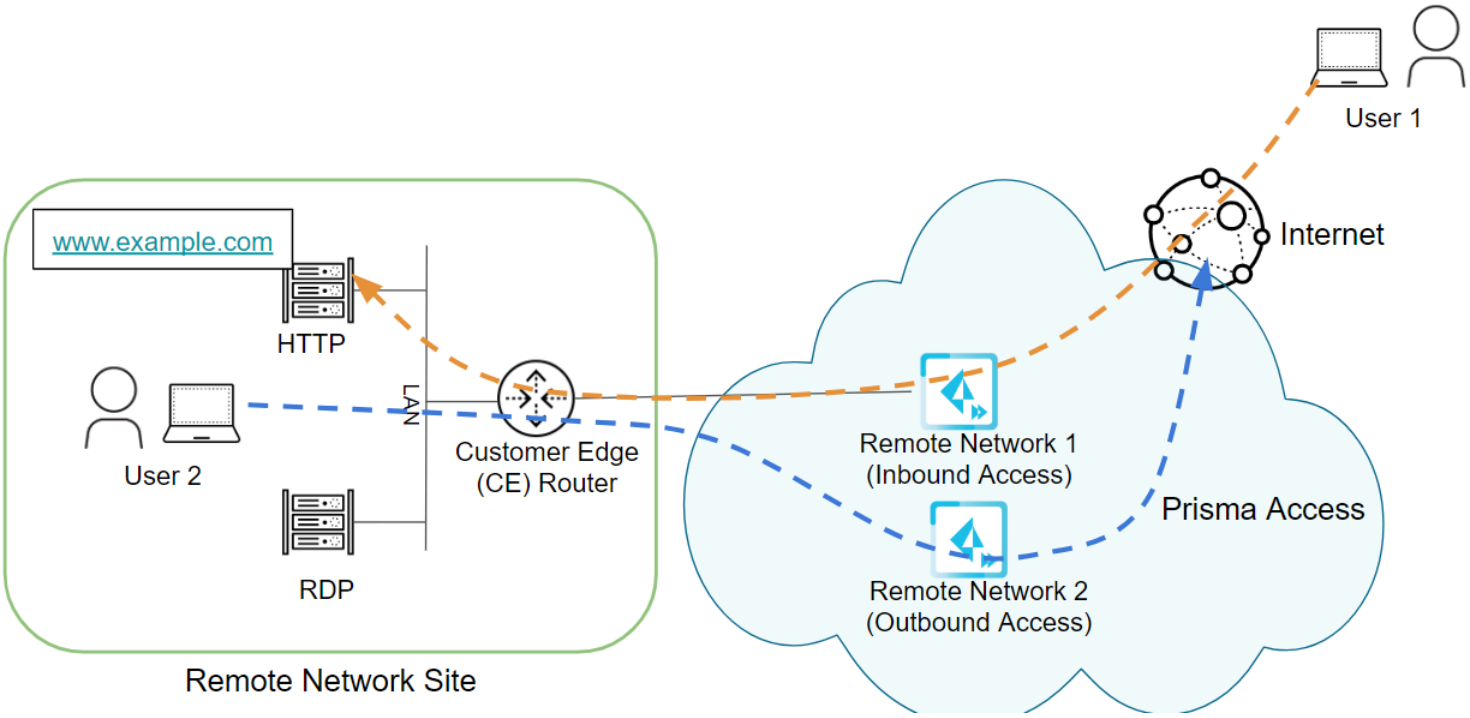
Type de protection contre la saturation	Taux d'alarme en CPS	Taux d'activation en CPS
saturation SYN	10 000	15 000
Saturation ICMP	20	20

Si vous avez besoin d'une meilleure protection contre la saturation de nouvelles sessions, contactez votre équipe Palo Alto Networks.

- Les réseaux distants configurés pour un accès entrant sécurisé ne peuvent être utilisés qu'à cette fin. Si vous avez besoin d'un accès sortant ainsi que d'un accès entrant pour un site de réseau distant, créez deux sites de réseaux distants au même emplacement, un pour l'accès entrant et un pour l'accès sortant, comme illustré dans la figure suivante. Dans cet exemple, User 1 (Utilisateur 1) utilise le Remote Network 1 (Réseau distant 1) pour l'accès entrant à

 ©2025 Palo Alto Networks, Inc.

www.example.com, tandis que User 2 utilise le Remote Network 2 pour l'accès Internet sortant à partir de l'emplacement du réseau distant.



- Si vous avez un déploiement Prisma Access personnalisé où l'un des fournisseurs de cloud est exclu, l'accès entrant peut ne pas être pris en charge. Dans ce cas, vous ne pouvez pas choisir l'emplacement lors de l'intégration du réseau distant.
- L'accès entrant sécurisé n'est pas pris en charge avec les licences d'évaluation.

Configurer l'accès entrant sécurisé pour les sites de réseaux distants

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• La licence Prisma Access qui inclut Net Interconnect pour l'accès site à site et utilisateur à site

Votre déploiement peut intégrer la bande passante par emplacement de calcul ou par emplacement. Les deux méthodes sont prises en charge pour la configuration de l'accès entrant pour un réseau distant. Lorsque vous configurez l'accès entrant pour un réseau distant qui alloue la bande passante par emplacement de calcul, vous spécifiez la bande passante par emplacement. Pour créer un site réseau distant autorisant un accès entrant sécurisé, effectuez l'un des flux de travail suivants :

- Pour configurer un accès entrant sécurisé pour un déploiement de réseau distant qui alloue la bande passante par emplacement de calcul, suivez ce flux de travail.
- Pour configurer un accès entrant sécurisé pour un déploiement de réseau distant qui alloue la bande passante par emplacement, suivez ce flux de travail.

 ©2025 Palo Alto Networks, Inc.

Configurer l'accès entrant sécurisé pour les réseaux distants

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• La licence Prisma Access qui inclut Net Interconnect pour l'accès site à site et utilisateur à site

Pour rendre les applications accessibles sur Internet disponibles à partir d'un site de réseau distant, vous devez d'abord créer une liste des applications auxquelles vous souhaitez fournir un accès, puis attribuer une combinaison IP privée, un numéro de port et un protocole pour chaque application. Si vous utilisez la même adresse IP pour plusieurs applications, la combinaison port/protocole doit être unique pour chaque application. Si vous utilisez la même combinaison port/protocole pour plusieurs applications, chaque adresse IP doit être unique.

Pour commencer la configuration, vous choisissez le nombre d'adresses IP publiques que vous souhaitez associer aux applications. Vous pouvez spécifier 5 ou 10 adresses IP publiques par site de réseau distant. Chaque allocation d'IP publique prend de la bande passante (unités) de votre licence de réseaux distants, en plus de la bande passante que vous avez allouée à l'emplacement de calcul associé au réseau distant. Cinq adresses IP prennent 150 Mbit/s de votre allocation de licence de réseaux distants, et 10 adresses IP prennent 300 Mbit/s.

Après avoir choisi le nombre d'adresses IP publiques, vous entrez ensuite l'application, ainsi que sa combinaison d'adresse IP privée/numéro de port/protocole associée, pour laquelle vous souhaitez sécuriser l'accès entrant.

Vous pouvez décider comment vous souhaitez mapper votre application aux adresses IP publiques. Par défaut, Prisma Access attribue les adresses IP publiques aux applications que vous spécifiez, et plusieurs applications peuvent être attribuées à une seule adresse IP. Si vous devez mapper une seule application à une seule adresse IP publique, vous pouvez cliquer sur **Dedicated IP (IP dédiée)** lors de la configuration du système. Vous pouvez configurer jusqu'à 100 applications entrantes pour chaque groupe d'adresses IP publiques provisionnées (soit 5 ou 10).

- Strata Cloud Manager
- Panorama

Configurer l'accès sécurisé entrant pour les réseaux distants (Strata Cloud Manager)

Voici comment rendre une application accessible depuis un site réseau distant à tous les utilisateurs connectés à Internet (pas seulement aux utilisateurs Prisma Access).

STEP 1 | Si vous ne l'avez pas déjà fait, consultez les directives des réseaux distants à accès entrant.

STEP 2 | Rassemblez les détails de l'application dont vous aurez besoin pour commencer.

Faites une liste des applications auxquelles vous souhaitez fournir un accès, et attribuez une adresse IP privée, un numéro de port et une combinaison de protocole pour chaque application. Si vous utilisez la même adresse IP pour plusieurs applications, la combinaison port/protocole doit être unique pour chaque application. Si vous utilisez la même combinaison port/protocole pour plusieurs applications, chaque adresse IP doit être unique.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Dans Strata Cloud Manager, accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **Remote Networks (Réseaux distants)** > **Inbound Access (Accès entrant)** > **Add Inbound Access (Ajouter un accès entrant)**.

STEP 4 | Entrez les détails requis.

Choisissez le **Number of Public IPs (Nombre d'adresses IP publiques)** que vous souhaitez utiliser pour les applications, soit cinq ou dix.

Chaque allocation d'IP publique consomme de la bande passante de votre licence de réseaux distants, en plus du coût de la licence pour le réseau distant. Cinq adresses IP prennent 150 Mo de votre allocation de licence de réseaux distants, et 10 adresses IP prennent 300 Mo.

À partir de la version 4.1 de Prisma Access, si vous avez une ressource qui se trouve sur un site de réseau distant avec un accès entrant activé et que vous souhaitez que les utilisateurs des sites sans accès entrant aient accès à cette ressource, vous pouvez cliquer sur **Allow inbound flows to other Remote Networks over the Prisma Access backbone (Autoriser les flux entrants vers d'autres réseaux distants via la zone principale de Prisma Access)** lorsque vous configurez le réseau distant à accès non entrant.

À partir de la version 5.0 de Prisma Access, vous pouvez autoriser les flux entrants vers d'autres réseaux distants via la zone principale du fournisseur de services (SP) lorsque vous configurez le réseau distant à accès non entrant.

L'interconnexion des fournisseurs de services ne prend en charge que les éléments suivants :

- *Régions GCP*
- *Nouveaux déploiements Prisma Access*
- *Trafic de sortie de proxy explicite*

STEP 5 | Ajoutez les **Inbound Access Applications (Applications d'accès entrant)** pour lesquelles vous souhaitez sécuriser l'accès.

Ajoutez la combinaison d'adresse IP privée/numéro de port/protocole associée pour l'application.

STEP 6 | Décidez comment vous souhaitez mapper les applications aux adresses IP publiques.

Par défaut, Prisma Access attribue les adresses IP publiques aux applications que vous spécifiez, et plusieurs applications peuvent être attribuées à une seule adresse IP. Si vous devez mapper une seule application à une seule adresse IP publique, vous pouvez cliquer sur **Assign Dedicated IP (Attribuer une IP dédiée)** lors de la configuration du système. Vous pouvez configurer jusqu'à 100 applications entrantes pour chaque groupe d'adresses IP publiques provisionnées (soit 5 ou 10).

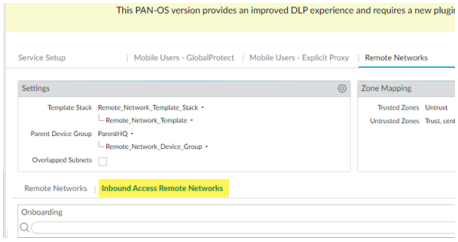
STEP 7 | Terminez la configuration du réseau distant à accès entrant comme vous le feriez pour un site de réseau distant régulier.

 ©2025 Palo Alto Networks, Inc.

Configurer l'accès sécurisé entrant pour les réseaux distants (Panorama)

Si vous avez un déploiement Prisma Access qui alloue la bande passante du réseau distant par emplacement de calcul, configurez l'accès entrant en procédant comme suit.

STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**, et sélectionnez **Inbound Access Remote Networks (Réseaux distants à accès entrant)**.



STEP 2 | Cliquez sur **Add (Ajouter)** pour ajouter un réseau distant à l'accès entrant.

STEP 3 | Spécifiez les paramètres pour la connexion au réseau distant à accès entrant.

1. Saisissez un **Name (Nom)** pour la connexion à accès entrant.
2. Entrez un **Location (Emplacement)**.

   L'accès entrant prend en charge un sous-ensemble d'emplacements.
3. Spécifiez une **Bandwidth (Bande passante)** à utiliser pour la connexion à accès entrant.

   Vous allouez la bande passante aux connexions à accès entrant en fonction de chaque emplacement.
4. Spécifiez le **Number of Public IPs (Nombre d'adresses IP publiques)** à utiliser pour la connexion à accès entrant.

   Spécifiez 5 ou 10 adresses IP publiques. Chaque allocation d'IP publique prend de la bande passante (unités) de votre licence de réseaux distants, en plus de la bande passante que vous avez allouée à l'emplacement de calcul associé au réseau distant.
5. Sélectionnez le tunnel IPSec à utiliser avec la connexion à accès entrant.
6. Sélectionnez si vous souhaitez ou non **Allow inbound flows to other Remote Networks over the Prisma Access Backbone (Autoriser les flux entrants vers d'autres réseaux distants via la zone principale de Prisma Access)**.

   Si vous avez une ressource qui se trouve sur un site de réseau distant avec un accès entrant activé et que vous souhaitez que les utilisateurs des sites sans accès entrant aient accès à cette ressource, vous pouvez cliquer sur **Allow inbound flows to other Remote Networks over the Prisma Access backbone (Autoriser les flux entrants vers d'autres réseaux distants via la dorsale de Prisma Access)** lorsque vous configurez le réseau distant à accès non entrant. Si vous autorisez les flux entrants provenant d'autres réseaux distants, vous devez activer la NAT source.
7. (Facultatif) Si vous disposez d'un lien WAN secondaire à cet emplacement, sélectionnez **Enable Secondary WAN (Activer le WAN secondaire)** et fournissez un **IPSec Tunnel (Tunnel IPSec)** différent du tunnel IPSec principal.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Configurez les éléments **Static Routes (Itinéraires statiques)**, **BGP**et **QoS** pour votre déploiement.

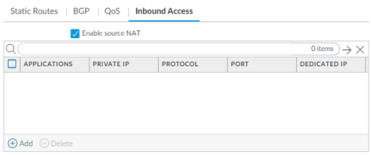
Cette configuration est la même qu'une connexion au réseau distant à accès non entrant.

STEP 5 | Cliquez sur l'onglet **Inbound Access (Accès entrant)** pour configurer les options d'accès entrant.

1. (Facultatif) Pour désactiver la NAT source, décochez **Enable Source NAT (Activer la NAT source)**.

   Par défaut, la NAT source est activée. Si le périphérique compatible IPSec sur votre site réseau distant est capable d'effectuer un retour symétrique (comme un pare-feu nouvelle génération Palo Alto Networks), ou si vous n'avez pas sélectionné **Allow inbound flows to other Remote Networks over the Prisma Access backbone (Autoriser les flux entrants vers d'autres réseaux distants via la zone principale de Prisma Access)**, désélectionnez **Enable source NAT (Activer la NAT source)**.

   *Vous devez **Enable source NAT (Activer la NAT source)** dans l'onglet **Inbound Access (Accès entrant)** si vous cochez cette case. La NAT source est une exigence pour autoriser les flux entrants vers d'autres réseaux distants.*

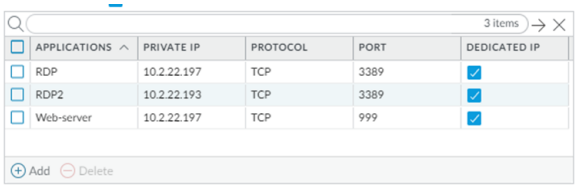


2. Cliquez sur **Add (Ajouter)** pour ajouter les applications afin de fournir un accès entrant sécurisé.

   Vous pouvez configurer jusqu'à 100 applications entrantes pour chaque groupe d'adresses IP publiques provisionnées (soit 5 ou 10). Saisissez une combinaison unique d'adresse **Private IP (IP privée)**, de **Protocol (Protocole)** et de **Port** pour chaque application. Il est acceptable d'utiliser des adresses IP privées et des ports en double pour deux applications, à condition de sélectionner **TCP** pour une application et **UDP** pour une autre application.

   Fournissez les valeurs suivantes :

   - Spécifiez le nom de l'**Application**.
   - Spécifiez l'adresse **Private IP (IP privée)** à utiliser avec cette application.
   - Spécifiez le **Protocol (Protocole)** à utiliser avec l'application (**TCP** ou **UDP**).
   - Spécifiez le **Port** à utiliser avec l'application.
   - Choisissez si vous souhaitez dédier une seule adresse IP publique à une seule application. Pour ce faire, sélectionnez **Dedicated IP (IP dédiée)**.



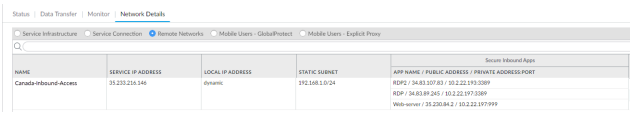
 ©2025 Palo Alto Networks, Inc.

STEP 6 | Cliquez sur **OK** pour enregistrer vos modifications.

STEP 7 | Cliquez sur **Save (Enregistrer)** et **Commit (Valider)** pour enregistrer et valider vos modifications.

STEP 8 | Attendez environ 30 minutes pour que Prisma Access génère les adresses IP publiques. Sélectionnez ensuit **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Remote Networks (Réseaux distants)** et notez la valeur **Public Address (Adresse publique)** qui est associée au **App Name (Nom de l'application)** pour l'application que vous avez créée.

Si vous avez sélectionné **Dedicated IP (IP dédiée)**, recherchez l'application unique associée à **Public Address (Adresse publique)**.

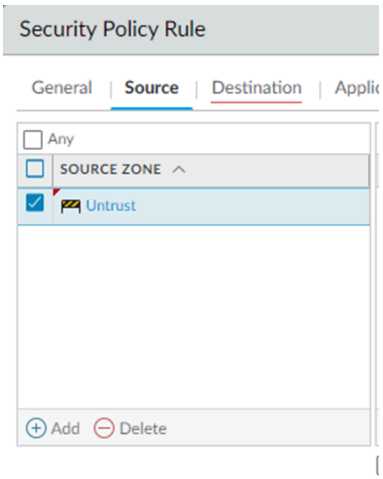


STEP 9 | Créez des politiques de sécurité pour autoriser le trafic des utilisateurs Internet entrants.

Puisque la politique de sécurité par défaut de Prisma Access autorise uniquement le trafic non approuvé vers non approuvé. Vous devez configurer les politiques de sécurité pour autoriser le trafic non approuvé vers approuvé pour vos applications à accès entrant. Palo Alto Networks vous recommande de limiter le type d'accès que vous autorisez aux applications entrantes. Les exemples suivants fournissent un accès aux serveurs SSH, aux portails Web et aux serveurs RDP.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (Ajouter)** pour ajouter une politique.

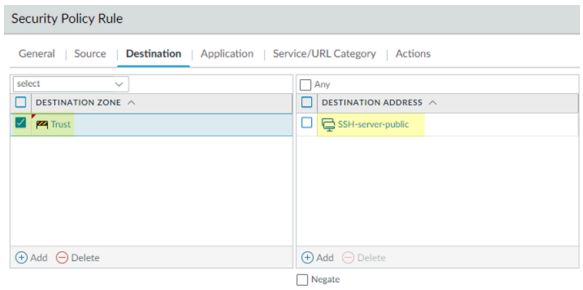
   Assurez-vous de créer cette politique sous le groupe de périphériques **Remote_Network_Device_Group**.
2. Sélectionnez le trafic **Source** comme **Untrust (Non approuvé)**.



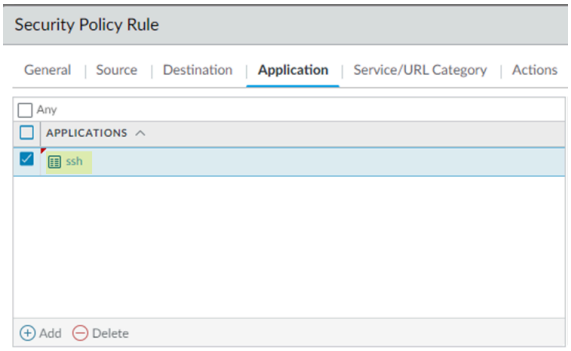
3. Créez une politique pour autoriser le trafic du serveur SSH en sélectionnant la **Destination Zone (Zone de destination)** pour le trafic de destination comme **Trust**

 ©2025 Palo Alto Networks, Inc.

(Approuvé) et en spécifiant une **Destination Address (Adresse de destination)** de **SSH-server-public**. Il s'agit d'un objet Address (Adresse) ou Address Group (Groupe d'adresses) que vous avez créé et qui contient une liste de toutes les adresses IP publiques utilisées pour la connexion SSH.



4. Sélectionnez une **Application ssh**.

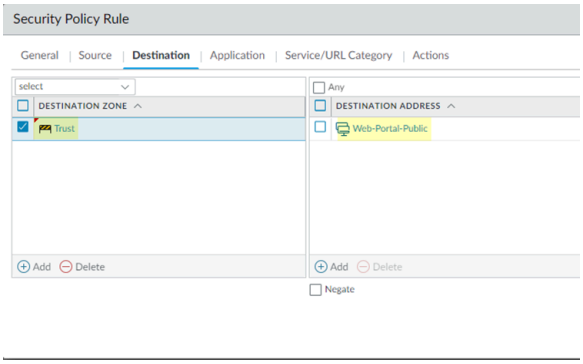


5. Sélectionnez une **Service/URL Category (Catégorie de service/URL) application-default** pour autoriser ou refuser les applications en fonction uniquement de leurs ports par défaut tels que définis par Palo Alto Networks.
6. Sous **Actions**, sélectionnez **Allow (Autoriser)**.
7. Cliquez sur **OK (OK)** pour enregistrer la politique.

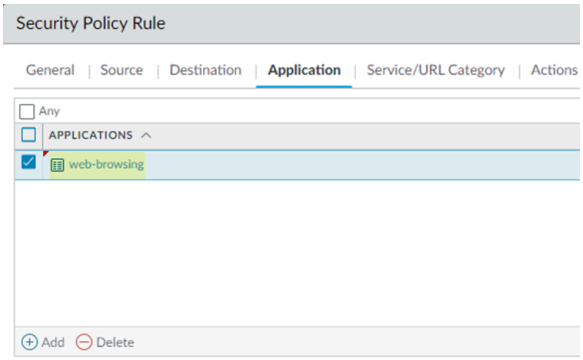
 ©2025 Palo Alto Networks, Inc.

8. Créez une politique pour autoriser l'accès au portail Web en créant une politique dans les étapes précédentes, mais en remplaçant les paramètres suivants dans les onglets **Destination** et **Application** :

   - Sélectionnez une **Destination Address (Adresse de destination)** d'une adresse ou d'un groupe d'adresses **Web-Portal-Public**, qui contient toutes les adresses IP publiques du portail Web.

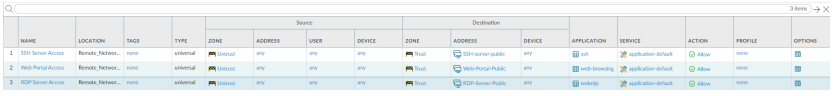


   - Sélectionnez une **Application web-browsing**.



9. Créez une politique de sécurité pour l'accès au serveur RDP, en utilisant les mêmes paramètres que pour les autres politiques, mais en créant un objet Address (Adresse) ou Address Group (Groupe d'adresses) appelé **RDP-Server-Public**, qui contient les adresses IP publiques pour le serveur RDP, comme **Destination Address (Adresse de destination)** et **webrdp** comme **Application**.

   Une fois terminé, vous disposez de trois politiques différentes pour autoriser l'accès au serveur SSH, l'accès au portail Web et l'accès au serveur RDP.

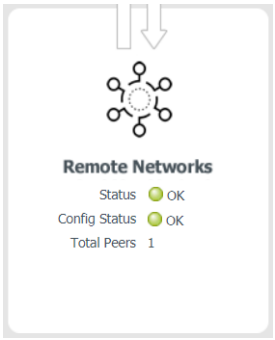


STEP 10 | Cliquez sur **Save (Enregistrer)** et **Commit (Valider)** pour enregistrer et valider vos modifications.

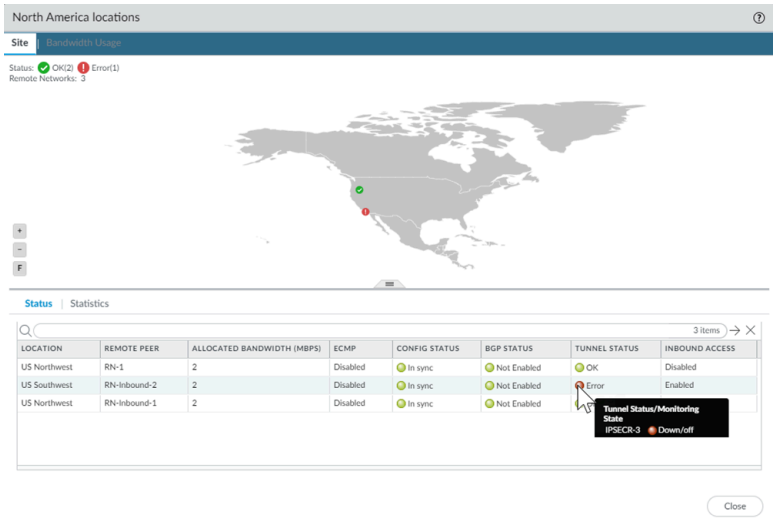
 ©2025 Palo Alto Networks, Inc.

STEP 11 | Vérifiez que la connexion au réseau distant est opérationnelle et traite correctement le trafic entrant.

1. Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > > **Status (État)** > **Remote Networks (Réseaux distants)** et passez la souris sur les zones **Status (État)** et **Config Status (État de la configuration)** pour voir l'état du tunnel.



2. Si vous rencontrez des problèmes, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > > **Monitor (Surveiller)** > **Remote Networks (Réseaux distants)**, sélectionnez l'emplacement du tunnel du réseau distant sur la carte et passez la souris sur la zone **Tunnel Status (État du tunnel)** pour déterminer la cause de l'erreur.



Configurer l'accès entrant sécurisé des sites de réseaux distants pour les emplacements qui allouent la bande passante par emplacement

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• La licence Prisma Access qui inclut l'interconnexion réseau pour l'accès de site à site et d'utilisateur à site

Si vous avez un déploiement Prisma Access qui alloue la bande passante du réseau distant par emplacement, configurez l'accès entrant en procédant comme suit.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)**, cliquez sur **Add (Ajouter)** pour ajouter une connexion, et configurez le réseau distant, y compris les options de routage et de tunnel IPSec.

Pour plus d'informations, reportez-vous à la sectionPrisma Access Réseaux distants. Votre déploiement peut intégrer la bande passante par emplacement de calcul ou par emplacement. Les deux méthodes sont prises en charge pour l'accès entrant.

Assurez-vous de sélectionner l'un des emplacements pris en charge pour l'accès entrant.

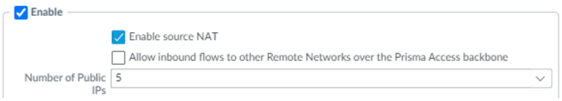
STEP 2 | Cliquez sur l'onglet **Inbound Access (Accès entrant)** pour configurer les options d'accès entrant.

1. Sélectionnez **Enable (Activer)** pour activer l'accès entrant pour le réseau distant.

   Si vous avez sélectionné un emplacement qui n'est pas pris en charge pour l'accès entrant, Prisma Access vous invite à sélectionner un modèle pris en charge.
2. (Facultatif) Pour désactiver la NAT source, décochez **Enable Source NAT (Activer la NAT source)**.

   Par défaut, la NAT source est activée. Si le périphérique compatible IPSec sur votre site réseau distant est capable d'effectuer un retour symétrique (comme un pare-feu nouvelle génération Palo Alto Networks), ou si vous n'avez pas sélectionné **Allow inbound flows to other Remote Networks over the Prisma Access backbone (Autoriser les flux entrants vers d'autres réseaux distants via la zone principale de Prisma Access)**, désélectionnez **Enable source NAT (Activer la NAT source)**.

   *Vous devez **Enable source NAT (Activer la NAT source)** dans l'onglet **Inbound Access (Accès entrant)** si vous cochez cette case. La NAT source est une exigence pour autoriser les flux entrants vers d'autres réseaux distants.*



STEP 3 | Cliquez sur **Add (Ajouter)** pour ajouter les applications afin de fournir un accès entrant sécurisé.

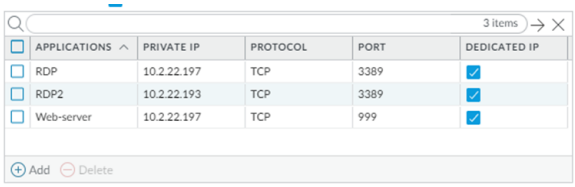
Vous pouvez configurer jusqu'à 100 applications entrantes pour chaque groupe d'adresses IP publiques provisionnées (soit 5 ou 10). Saisissez une combinaison unique d'adresse **Private IP (IP privée)**, de **Protocol (Protocole)** et de **Port** pour chaque application. Il est acceptable

 ©2025 Palo Alto Networks, Inc.

d'utiliser des adresses IP privées et des ports en double pour deux applications, à condition de sélectionner **TCP** pour une application et **UDP** pour une autre application.

Fournissez les valeurs suivantes :

- Spécifiez le nom de l'**Application**.
- Spécifiez l'adresse **Private IP (IP privée)** à utiliser avec cette application.
- Spécifiez le **Protocol (Protocole)** à utiliser avec l'application (**TCP** ou **UDP**).
- Spécifiez le **Port** à utiliser avec l'application.
- Choisissez si vous souhaitez dédier une seule adresse IP publique à une seule application. Pour ce faire, sélectionnez **Dedicated IP (IP dédiée)**.

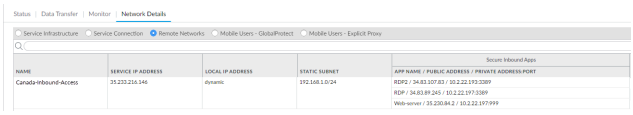


STEP 4 | Cliquez sur **OK** pour enregistrer vos modifications.

STEP 5 | Cliquez sur **Save (Enregistrer)** et **Commit (Valider)** pour enregistrer et valider vos modifications.

STEP 6 | Attendez environ 30 minutes pour que Prisma Access génère les adresses IP publiques. Sélectionnez ensuit **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Remote Networks (Réseaux distants)** et notez la valeur **Public Address (Adresse publique)** qui est associée au **App Name (Nom de l'application)** pour l'application que vous avez créée.

Si vous avez sélectionné **Dedicated IP (IP dédiée)**, recherchez l'application unique associée à **Public Address (Adresse publique)**.



STEP 7 | Créez des politiques de sécurité pour autoriser le trafic des utilisateurs Internet entrants.

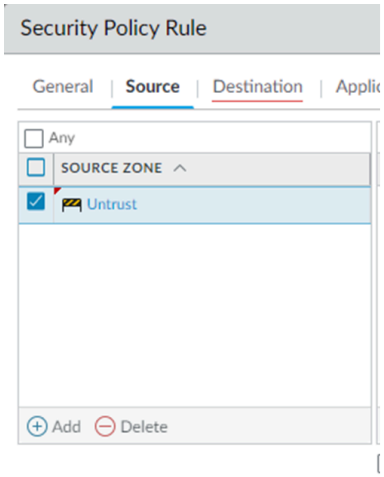
Puisque la politique de sécurité par défaut de Prisma Access autorise uniquement le trafic non approuvé vers non approuvé. Vous devez configurer les politiques de sécurité pour autoriser le trafic non approuvé vers approuvé pour vos applications à accès entrant. Palo Alto Networks vous recommande de limiter le type d'accès que vous autorisez aux applications entrantes. Les exemples suivants fournissent un accès aux serveurs SSH, aux portails Web et aux serveurs RDP.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (Ajouter)** pour ajouter une politique.

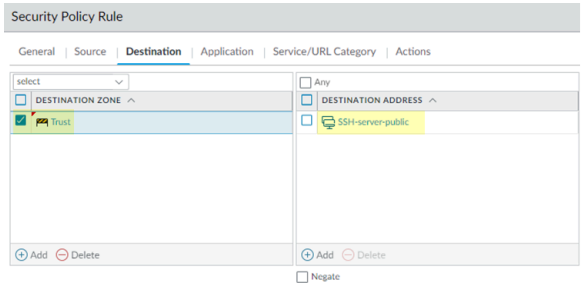
   Assurez-vous de créer cette politique sous le groupe de périphériques **Remote_Network_Device_Group**.

 ©2025 Palo Alto Networks, Inc.

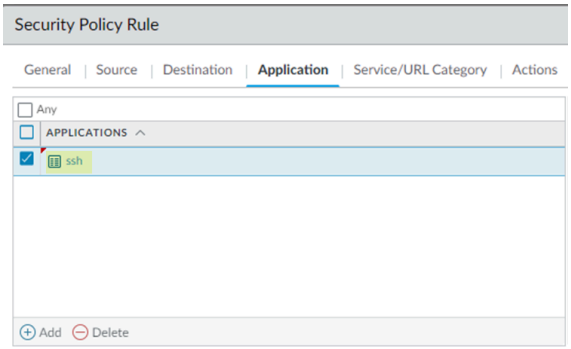
2. Sélectionnez le trafic **Source** comme **Untrust (Non approuvé)**.



3. Créez une politique pour autoriser le trafic du serveur SSH en sélectionnant la **Destination Zone (Zone de destination)** pour le trafic de destination comme **Trust (Approuvé)** et en spécifiant une **Destination Address (Adresse de destination)** de **SSH-server-public**. Il s'agit d'un objet Address (Adresse) ou Address Group (Groupe d'adresses) que vous avez créé et qui contient une liste de toutes les adresses IP publiques utilisées pour la connexion SSH.



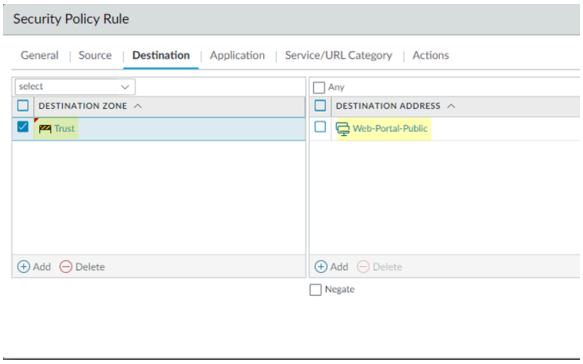
4. Sélectionnez une **Application ssh**.



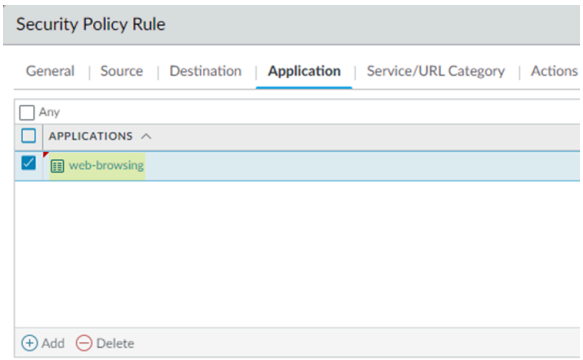
 ©2025 Palo Alto Networks, Inc.

5. Sélectionnez une **Service/URL Category (Catégorie de service/URL) application-default** pour autoriser ou refuser les applications en fonction uniquement de leurs ports par défaut tels que définis par Palo Alto Networks.
6. Sous **Actions**, sélectionnez **Allow (Autoriser)**.
7. Cliquez sur **OK (OK)** pour enregistrer la politique.
8. Créez une politique pour autoriser l'accès au portail Web en créant une politique dans les étapes précédentes, mais en remplaçant les paramètres suivants dans les onglets **Destination** et **Application** :

   - Sélectionnez une **Destination Address (Adresse de destination)** d'une adresse ou d'un groupe d'adresses **Web-Portal-Public**, qui contient toutes les adresses IP publiques du portail Web.

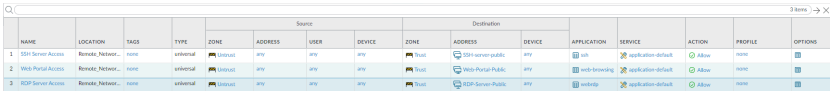


   - Sélectionnez une **Application web-browsing**.



9. Créez une politique de sécurité pour l'accès au serveur RDP, en utilisant les mêmes paramètres que pour les autres politiques, mais en créant un objet Address (Adresse) ou Address Group (Groupe d'adresses) appelé **RDP-Server-Public**, qui contient les adresses IP publiques pour le serveur RDP, comme **Destination Address (Adresse de destination)** et **webrdp** comme **Application**.

   Une fois terminé, vous disposez de trois politiques différentes pour autoriser l'accès au serveur SSH, l'accès au portail Web et l'accès au serveur RDP.

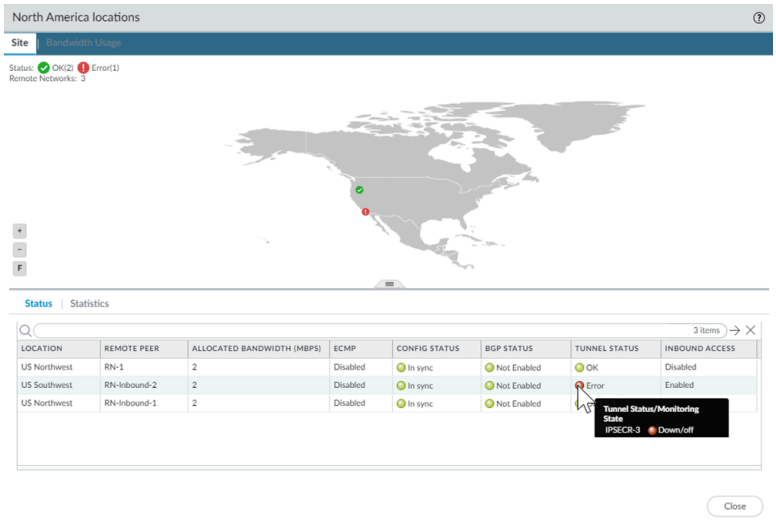


 ©2025 Palo Alto Networks, Inc.

STEP 8 | Cliquez sur **Save (Enregistrer)** et **Commit (Valider)** pour enregistrer et valider vos modifications.

STEP 9 | Vérifiez que la connexion au réseau distant est opérationnelle et traite correctement le trafic entrant.

1. Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > > **Status (État)** > **Remote Networks (Réseaux distants)** et passez la souris sur les zones **Status (État)** et **Config Status (État de la configuration)** pour voir l'état du tunnel.
2. Si vous rencontrez des problèmes, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > > **Monitor (Surveiller)** > **Remote Networks (Réseaux distants)**, sélectionnez l'emplacement du tunnel du réseau distant sur la carte et passez la souris sur la zone **Tunnel Status (État du tunnel)** pour déterminer la cause de l'erreur.



Créer un réseau à large bande passante pour un site distant

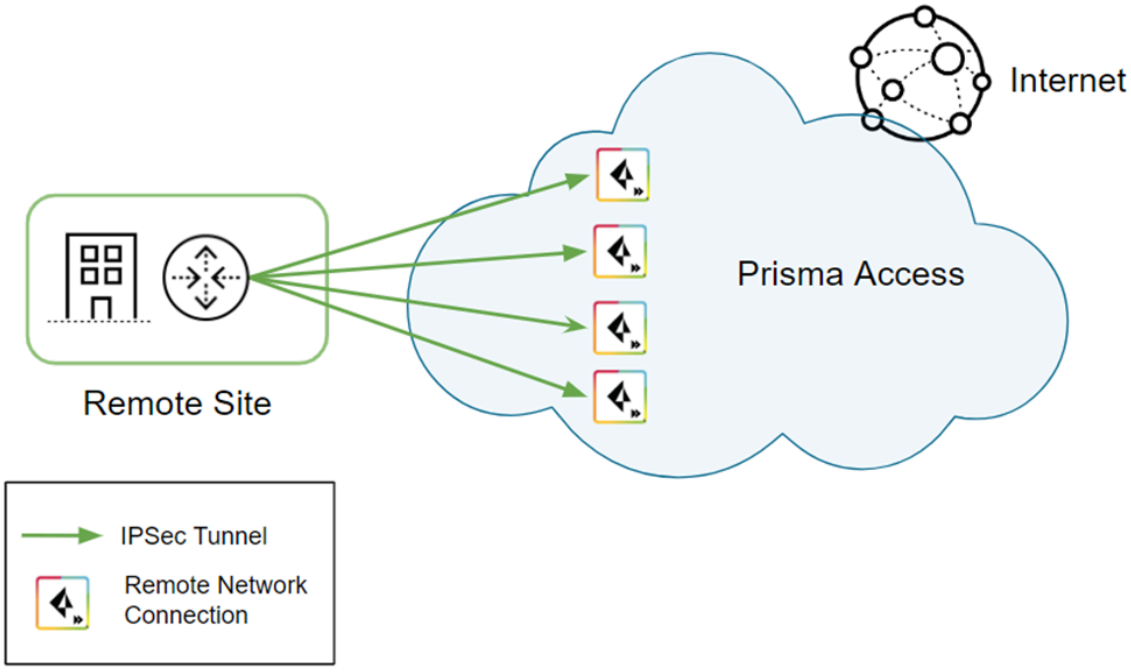
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Si vous souhaitez sécuriser votre succursale ou votre site pour l'accès Internet sortant avec une connexion à large bande passante à Prisma Access, vous pouvez équilibrer la charge du trafic depuis votre succursale ou votre site à l'aide de plusieurs tunnels IPSec en suivant les étapes de cette section.

Le diagramme suivant montre quatre connexions de réseau distant qui utilisent le même site distant. Avant l'intégration, attribuez 4 Gbit/s (4 000 Mbit/s) à l'emplacement de calcul, qui est la Corée du Sud dans cet exemple et correspond au site distant. 4 000 Mbit/s fournissent quatre nœuds de terminaison IPSec et chaque nœud de terminaison IPSec fournit un maximum de 1 000 Mbit/s de bande passante. Attribuez à chaque connexion au réseau distant son propre nœud de terminaison IPSec pendant le processus d'intégration pour utiliser toute la bande passante.

 ©2025 Palo Alto Networks, Inc.

Cet exemple montre quatre tunnels. Le nombre maximal de tunnels que vous pouvez utiliser pour une connexion à large bande passante dans Prisma Access est basé sur le nombre maximal de tunnels IPSec pris en charge par votre équipement sur site client (CPE) avec le protocole d'équilibrage de charge que vous utilisez.



Tenez compte des restrictions et recommandations suivantes avant de déployer cette configuration :

- Utilisez le routage BGP pour les tunnels IPSec ; le routage statique n'est pas pris en charge.
- Utilisez cette configuration uniquement pour l'accès Internet sortant.
- N'utilisez pas la surveillance du tunnel sur Prisma Access ou le CPE. La disponibilité du tunnel IPSec est déterminée par l'appairage BGP entre le CPE et le réseau distant Prisma Access. Si un tunnel IPSec tombe en panne et que la connexion BGP est interrompue, les itinéraires appris via BGP sur ce tunnel sont automatiquement supprimés d'ECMP.
- Puisque vous utilisez BGP pour déterminer quand un tunnel tombe en panne, tenez compte de la valeur HoldTime que vous avez configurée sur votre CPE. La minuterie d'attente détermine la durée pendant laquelle le tunnel est hors service avant de supprimer l'itinéraire. Prisma Access utilise la valeur HoldTime BGP par défaut de 90 secondes telle que définie par la RFC 4271. Si vous configurez un temps d'attente inférieur pour le CPE BGP sur le site réseau distant, BGP utilise la valeur d'attente inférieure. Palo Alto Networks recommande une valeur KeepAlive de 10 secondes et une valeur HoldTime de 30 secondes pour votre CPE avec ce déploiement.

Pour créer une connexion au réseau distant à large bande passante, effectuez la tâche suivante.

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Dans Panorama, configurez les tunnels de réseau distant Prisma Access.

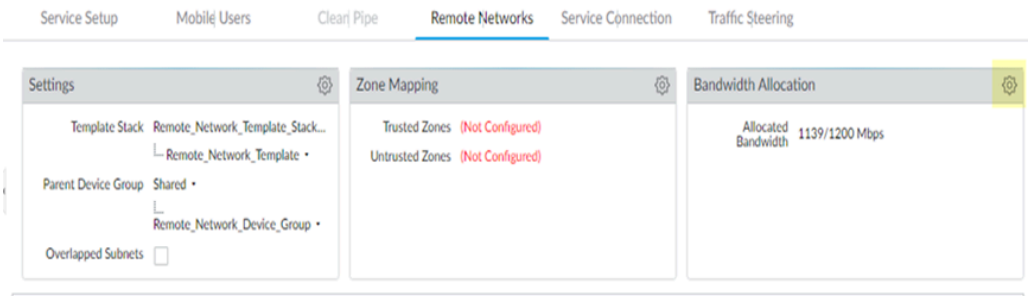
1. (Facultatif) Si vous ne l'avez pas déjà fait, configurez les passerelles IKE, les profils crypto IKE et IPSec et les tunnels IPSec pour les connexions au réseau distant que vous créez.

   Prenez note des profils crypto IKE et IPSec ; spécifiez les mêmes paramètres sur le CPE que vous utilisez pour mettre fin à la connexion au réseau distant dans l'emplacement de réseau distant.
2. Déterminez le type de déploiement de réseau distant dont vous disposez.

   Les déploiements Prisma Access allouent la bande passante en allouant la bande passante par emplacement de calcul ou en allouant la bande passante par emplacement.
3. Intégrez le réseau distant.

   - Pour intégrer le réseau distant qui alloue la bande passante par emplacement de calcul :

     1. Allouez de la bande passante aux emplacements que vous souhaitez intégrer en cliquant sur l'icône d'engrenage dans la zone **Bandwidth Allocation (Allocation de bande passante)**.



     2. Entrez la **Bandwidth Allocation (Allocation de bande passante)** que vous souhaitez pour chaque **Compute Location (Emplacement de calcul)** associé aux

 ©2025 Palo Alto Networks, Inc.

Prisma Access Locations (Emplacements Prisma Access) que vous souhaitez intégrer.

3. Attendez que la bande passante soit reflétée dans le champ **Allocated Total (Total alloué)** en haut de la page, puis cliquez sur **OK**.

- Pour intégrer le réseau distant qui alloue la bande passante par emplacement, passez à l'étape suivante. Allouez la bande passante lors de l'intégration du réseau distant.

4. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Remote Networks (Réseaux distants)** et créez quatre connexions au réseau distant, en spécifiant les paramètres suivants :

   - Sélectionnez le même **Location (Emplacement)** pour chaque connexion.
   - Sélectionnez le **IPSec Termination Node (Nœud de terminaison IPSec)**.

     Sélectionnez un nœud de terminaison IPSec distinct pour chaque connexion au réseau distant.

     *Si vous disposez d'un déploiement qui alloue la bande passante par emplacement, sélectionnez une **Bandwidth (Bande passante)** de **500 Mbps (500 Mbit/s)**.*

     La bande passante que vous sélectionnez ne peut pas dépasser la quantité totale de bande passante dont vous disposez sous licence. Utilisez ce paramètre pour définir la quantité de bande passante totale sous licence que vous souhaitez allouer à cet emplacement.
   - Cliquez sur **Enable (Activer)** pour activer le BGP, puis sur **Advertise Default Route (Publier l'itinéraire par défaut)** et **Don't Advertise Prisma Access Routes (Ne pas publier les itinéraires Prisma Access)**.
   - Spécifiez le même **Peer AS (AS homologue)** pour toutes les connexions au réseau distant.

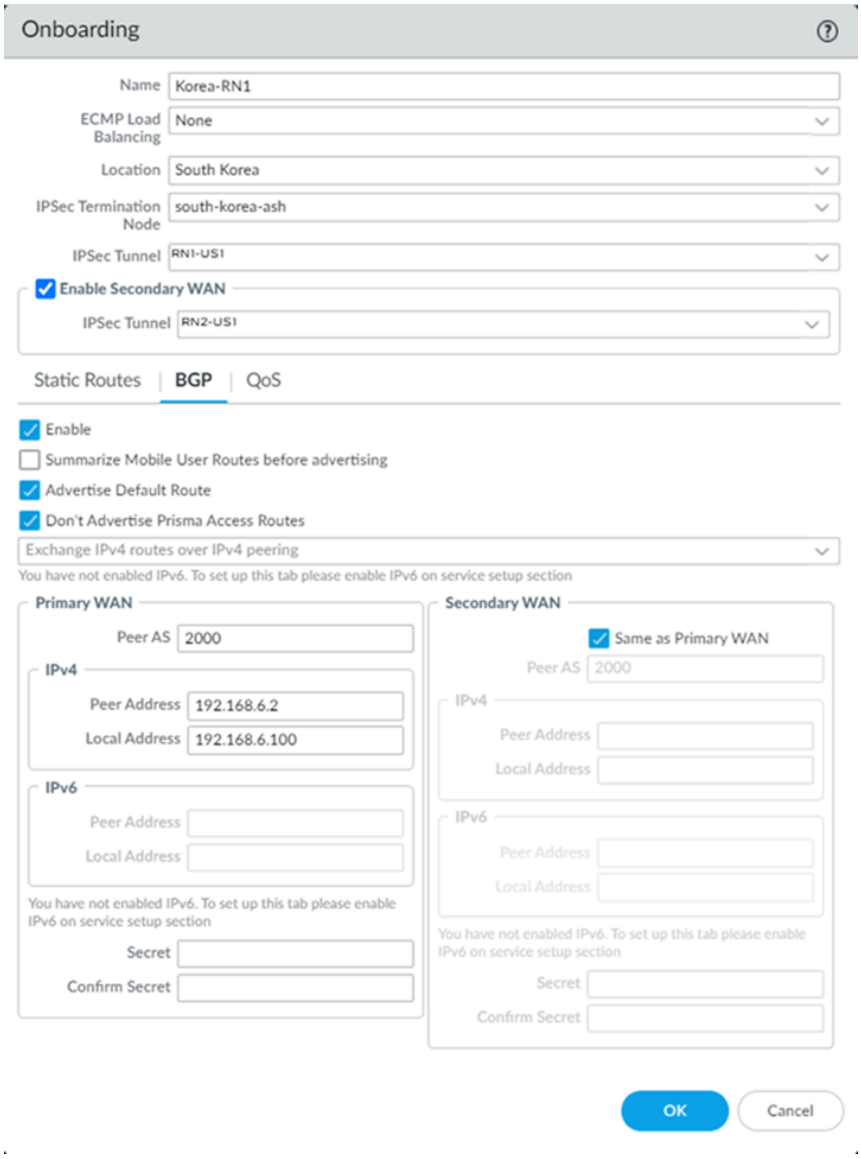
     Cet exemple montre un **Peer AS (AS homologue)** de 2 000. Dans cet exemple, vous sélectionnez un **Peer AS (AS homologue)** de 2 000 pour les quatre connexions.
   - (Facultatif) si vous souhaitez créer un réseau distant de sauvegarde, créez-en un en sélectionnant **Enable Secondary WAN (Activer le WAN secondaire)**, puis,

 ©2025 Palo Alto Networks, Inc.

sélectionnez l'**IPSec Tunnel (Tunnel IPSec)** que vous avez créé pour le tunnel de sauvegarde.

La configuration d'un WAN secondaire n'est pas prise en charge dans les déploiements suivants :

- Si votre WAN secondaire est configuré en mode actif-actif avec le tunnel IPSec principal.
- Si l'équipement de vos locaux clients (CPE) est configuré dans une configuration ECMP (Equal Cost Multipath) avec le tunnel IPSec principal et secondaire.

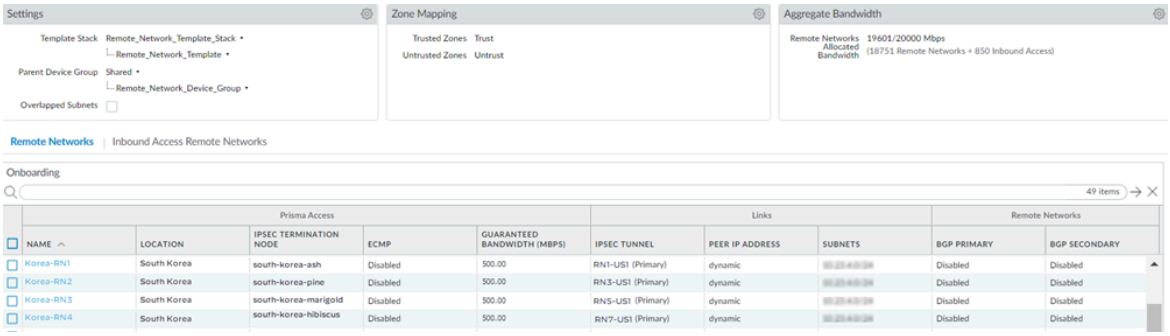


Une fois terminé, vous disposez de quatre connexions au réseau distant de 1 000 Mbit/s pour le même emplacement.

Puisque les déploiements qui allouent la bande passante par emplacement ont une bande passante maximale de 500 Mbit/s, cette configuration vous fournira 500 Mbit/s pour chaque emplacement.

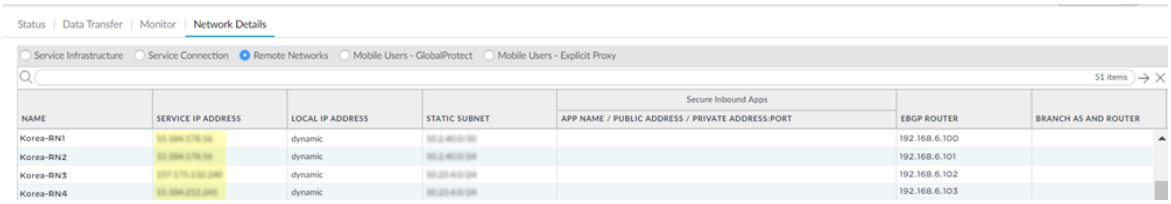
 ©2025 Palo Alto Networks, Inc.

Si vous avez configuré des tunnels de sauvegarde, vous disposez également de quatre tunnels secondaires à utiliser à des fins de basculement.



5. Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Remote Networks (Réseaux distants)** et prenez note des adresses **Service IP Address (Adresse IP du service)** et **EBGP Router (Routeur EBGP)**.

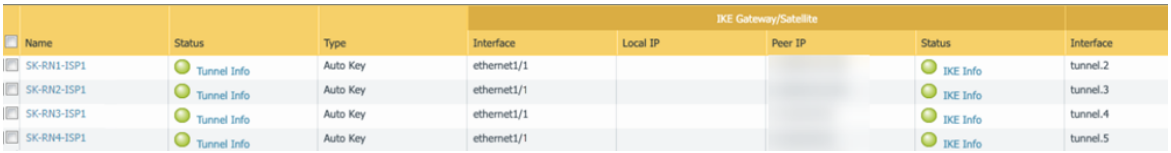
   Vous utilisez l'adresse **Service IP Address (Adresse IP du service)** comme adresse IP lorsque vous configurez le tunnel IPSec sur le CPE dans le site de réseau distant, et vous utilisez ces adresses et les adresses **EBGP Router (Routeur EBGP)** lorsque vous créez des itinéraires statiques sur le CPE.



STEP 2 | Sur le CPE du site de réseau distant, configurez les tunnels du réseau distant.

- *La configuration dans ces étapes utilise les pare-feu nouvelle génération Palo Alto Networks. Vous pouvez utiliser n'importe quel périphérique CPE prenant en charge les tunnels IPSec et ECMP pour ce déploiement.*
- *L'équilibrage de la bande passante dépend du hachage CPE pour ECMP. Cependant, Prisma Access assure un retour symétrique du trafic.*

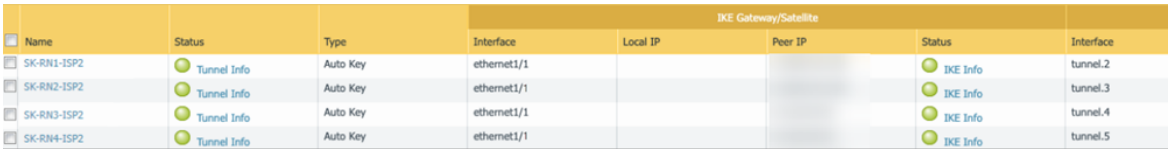
1. Créez quatre tunnels actifs à partir du CPE actif vers chacune des quatre connexions réseau. Pour l'adresse **Peer IP (IP homologue)**, saisissez l'adresse **Service IP Address (Adresse IP du service)** du réseau distant que vous avez reçu de Prisma Access dans une étape précédente.



2. (Facultatif) Si vous créez des tunnels de sauvegarde, créez-les à partir du CPE actif vers chacune des quatre connexions réseau. Pour l'adresse **Peer IP (IP homologue)**, saisissez

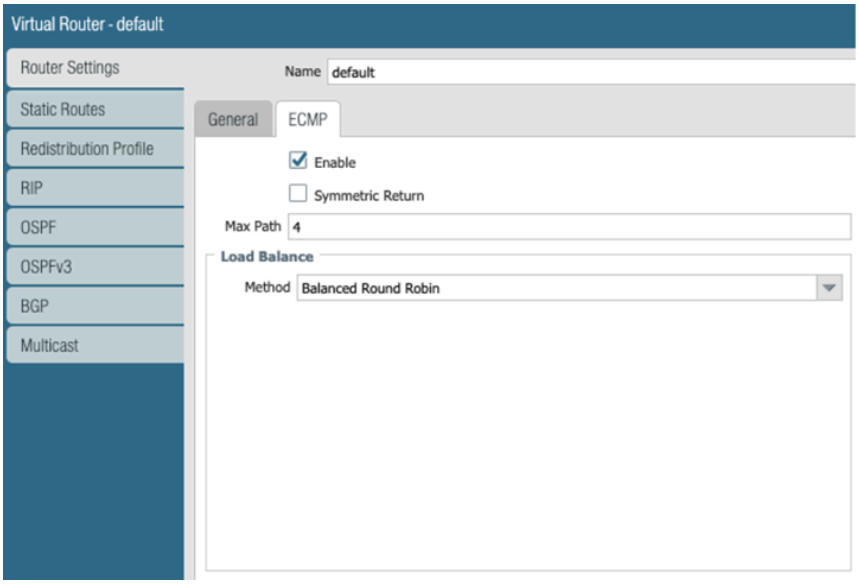
 ©2025 Palo Alto Networks, Inc.

l'adresse **Service IP Address (Adresse IP du service)** du réseau distant que vous avez reçu de Prisma Access dans une étape précédente.



STEP 3 | Configurez ECMP sur le CPE dans le site de réseau distant.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**.
2. Sélectionnez le routeur virtuel **default (par défaut)** ou cliquez sur **Add (Ajouter)** pour ajouter un nouveau routeur virtuel.
3. Sélectionnez **Router Settings (Paramètres du routeur)** > **Enable (Activer)** > **ECMP**, puis **Enable (Activer)** ECMP avec un **Max Path (Chemin maximal)** de **4** et une **Method (Méthode)** d'équilibrage de charge **Balanced Round Robin (Équilibrage comparatif)**.



STEP 4 | Sur le CPE du site de réseau distant, créez des itinéraires statiques vers l'adresse Prisma Access **Service IP Address (Adresse IP du service)** et les adresses IP **EBGP Router (Routeur EBGP)** que vous avez récupérées dans une étape précédente.

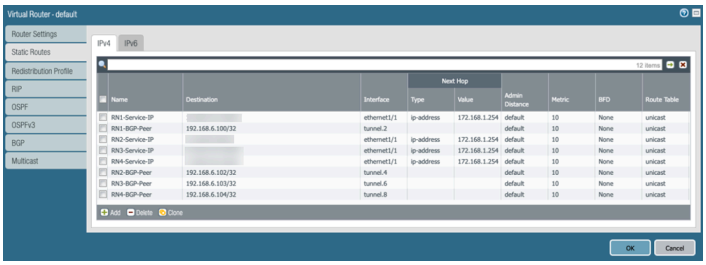
Comme indiqué précédemment, le routage dynamique avec BGP est requis pour cette configuration. Pour faciliter la connexion BGP entre le CPE et le routeur EBGP de Prisma Access, vous devez ajouter un itinéraire statique pour l'adresse IP du routeur eBGP sur le CPE,

 ©2025 Palo Alto Networks, Inc.

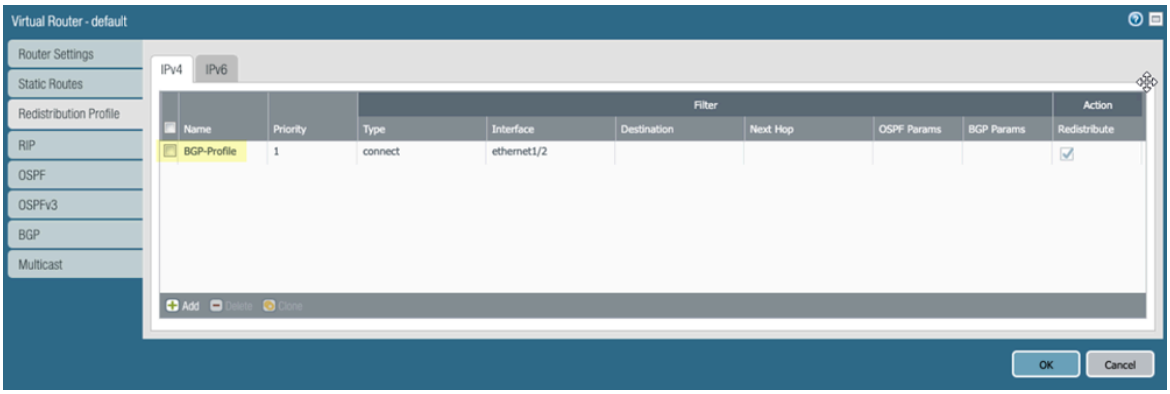
et le saut suivant doit être l'interface du tunnel sur le CPE. Vous devez répéter cette étape pour toutes les autres adresses IP du routeur EBGP du réseau distant sur les tunnels restants.

L'exemple suivant montre l'itinéraire sur le CPE actif. Si vous avez créé des tunnels de sauvegarde sur un CPE de secours, créez le même routage sur le CPE de secours.

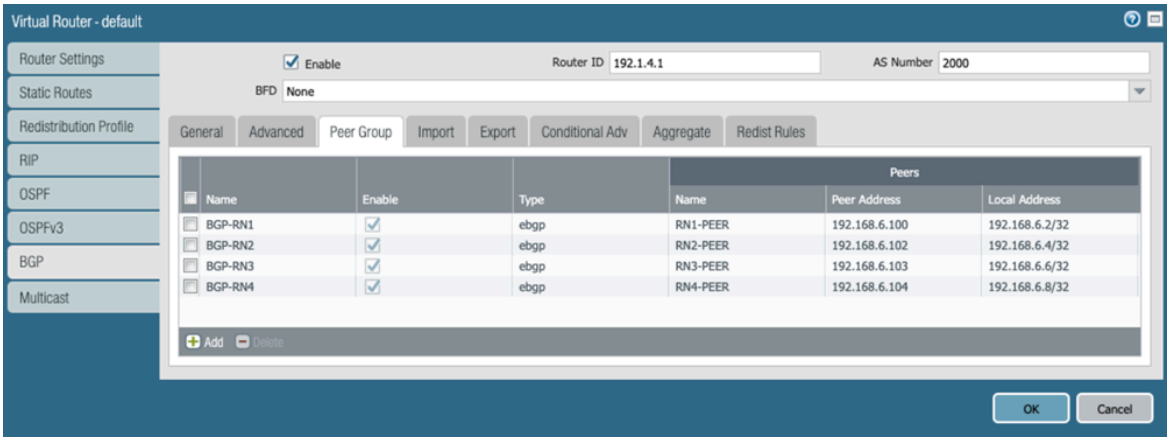
Si vous configurez un pare-feu nouvelle génération Palo Alto Networks, sélectionnez **Static Routes (Itinéraires statiques)** > **IPv4** pour ajouter les itinéraires statiques.



STEP 5 | Activez la redistribution d'itinéraire sur le CPE en sélectionnant **Redistribution Profile (Profil de redistribution)** > **IPv4**, puis cliquez sur **Add (Ajouter)** pour ajouter un profil de redistribution d'itinéraire IPv4.

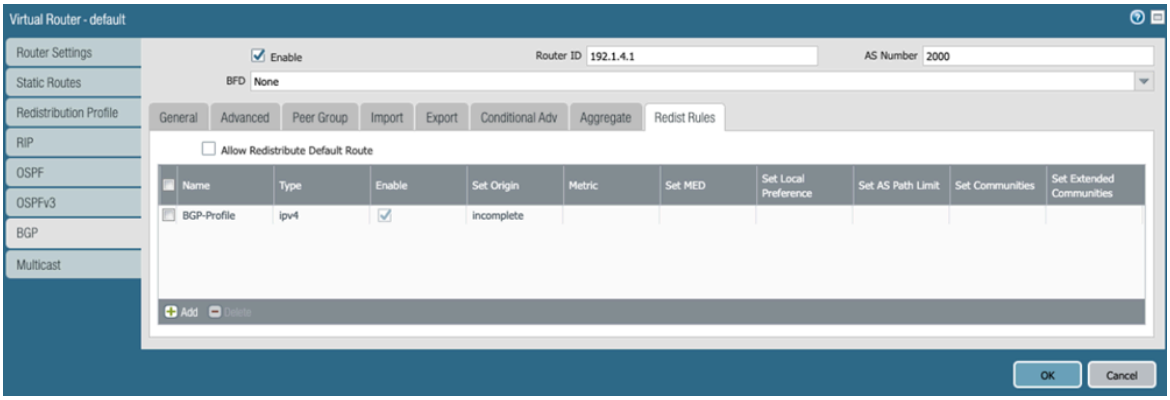


STEP 6 | Sélectionnez **BGP** > **Peer Group (Groupe d'homologues)**, **Enable (Activer)** BGP sur l'instance de routeur virtuel, puis cliquez sur **Add (Ajouter)** pour ajouter des homologues BGP du réseau distant.



 ©2025 Palo Alto Networks, Inc.

STEP 7 | Sélectionnez **BGP** > **Redist Rules (Règles de redistribution)**, puis joignez le profil de redistribution d'itinéraire que vous avez créé à l'étape précédente.

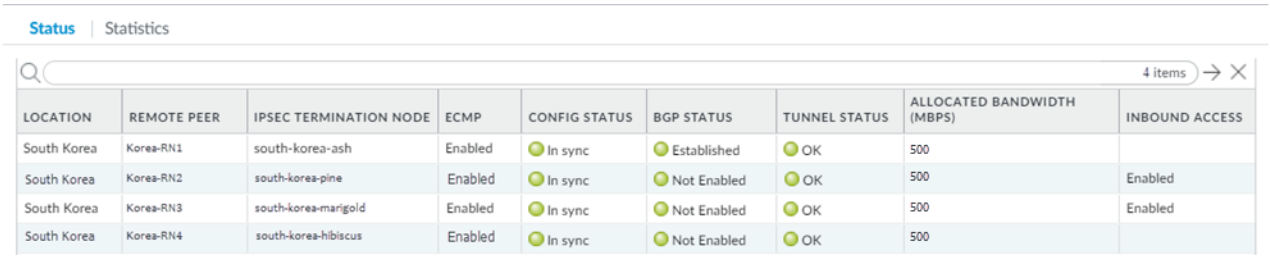


STEP 8 | Validez que le CPE transmet le trafic sur ses quatre tunnels.

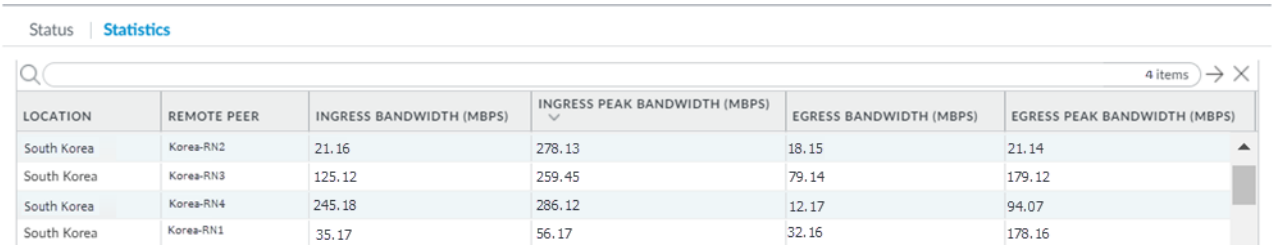
STEP 9 | Vérifiez l'état des connexions compatibles ECMP à partir de Prisma Access.

- Sélectionnez **Panorama** > **Cloud Services** > **Monitor (Surveiller)** > **Remote Networks (Réseaux distants)**, sélectionnez la région dans laquelle vous avez déployé les connexions ECMP, puis sélectionnez **Statut (État)**.

  - *Dans cette zone, **ECMP** s'affiche comme **No (Non)**. Cet état est attendu, car vous ne configurez pas la fonctionnalité Prisma Access d'équilibrage de charge ECMP.*
  - *L'ECMP est directionnel du CPE vers Prisma Access et Prisma Access assure le retour symétrique du trafic depuis le CPE.*



- Sélectionnez **Statistics (Statistiques)** pour voir que le trafic passe par chaque tunnel du réseau distant.



Une fois ce flux de travail terminé, vous avez créé une configuration à large bande passante pour le réseau distant. Notez que cette solution est prise en charge uniquement pour le trafic sortant.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Prisma Access pour Clean Pipe

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Utilisez *Prisma Access pour Clean Pipe* pour configurer rapidement et facilement plusieurs instances de connexions Internet sortantes propres.

Ceci n'est pas pris en charge pour Prisma Access (Managed by Strata Cloud Manager).

Vue d'ensemble de Prisma Access pour Clean Pipe

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Pour permettre aux organisations qui gèrent l'infrastructure informatique d'autres organisations, telles que les prestataires de services, les MSSP ou les firmes de télécommunications, de protéger rapidement et facilement le trafic Internet sortant de leurs locataires, Palo Alto Networks fournit Prisma Access pour Clean Pipe. Un prestataire de services, un MSSP ou une firme de télécommunications peuvent acheminer leurs clients (configurés en tant que locataires) vers Prisma Access pour Clean Pipe à l'aide d'une interconnexion partenaire. Une fois que le trafic a franchi l'interconnexion partenaire, il est envoyé à une instance dédiée au locataire du Clean Pipe pour la sécurité, puis acheminé vers Internet.

Prisma Access pour Clean Pipe fournit également une API que vous pouvez utiliser pour créer rapidement et facilement des Clean Pipes pour vos locataires.

Cas d'utilisation de Clean Pipe

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Utilisez Prisma Access pour Clean Pipe si vous répondez à tous les cas d'utilisation suivants :

- Vous gérez un déploiement réseau avec un grand nombre de locataires.

  Par exemple, vous êtes un prestataire de services, une firme de télécommunications ou un MSSP qui gère et maintient les réseaux de nombreuses organisations différentes (jusqu'à des dizaines de milliers).
- Vous voulez faire en sorte de sécuriser le trafic Internet sortant de chaque locataire de votre déploiement.
- Vous avez besoin d'un moyen rapide et évolutif pour intégrer des Clean Pipes pour les organisations dont vous gérez les réseaux.
- À l'exception de la sécurité Internet sortante, vous n'avez pas d'exigences supplémentaires pour protéger les utilisateurs mobiles, le siège ou les succursales des réseaux que vous gérez.

  Si vous avez des exigences de sécurité supplémentaires, nous vous recommandons de créer plusieurs locataires dans Prisma Access au lieu d'implémenter Clean Pipe, ce qui vous permet de créer et d'appliquer des profils de sécurité pour différents groupes de réseaux distants et d'utilisateurs mobiles.

 ©2025 Palo Alto Networks, Inc.

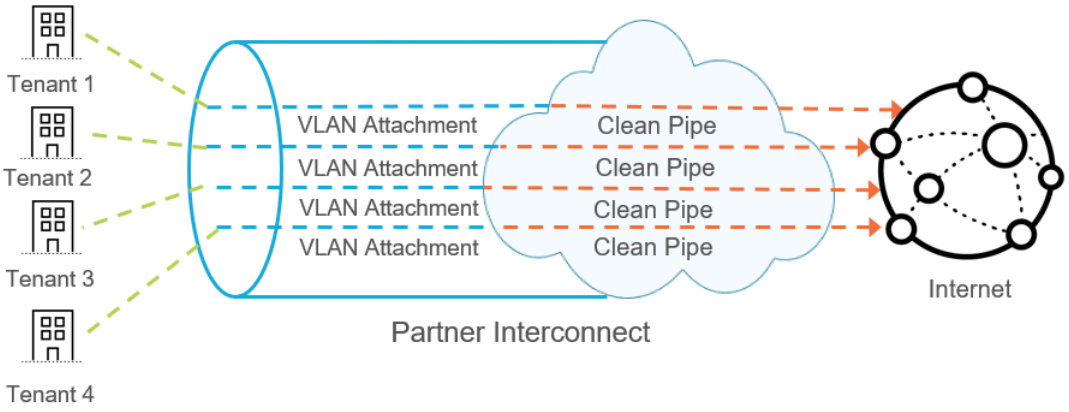
Exemples de configuration Clean Pipe

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

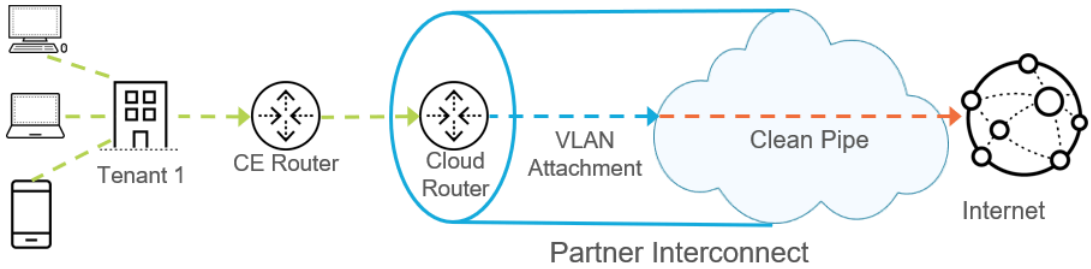
La figure suivante fournit un exemple de Clean Pipes configurés pour un seul locataire, où plusieurs Clean Pipes sont configurés pour le locataire.

Dans cet exemple, le prestataire de services gère la connectivité Internet de quatre organisations et souhaite protéger l'accès Internet sortant pour celles-ci. Le prestataire de services crée une interconnexion partenaire Google Cloud Platform (GCP) et crée un rattachement VLAN pour chaque locataire. Le prestataire de services configure Prisma Access pour Clean Pipe à l'aide de Panorama afin de créer une sécurité pour le rattachement VLAN.

Cet exemple montre un seul Clean Pipe par locataire. Vous pouvez également créer plusieurs Clean Pipes dans un seul locataire. Assurez-vous que chaque Clean Pipe que vous spécifiez pour un locataire utilise un emplacement différent.



La figure suivante montre un seul Clean Pipe plus en détail pour un locataire qui souhaite une connexion à Internet propre. Le routeur périphérique client (Customer Edge, CE) fournit une connectivité WAN au locataire. Le routeur CE se connecte à un routeur cloud et ce dernier fournit la connectivité pour l'interconnexion partenaire. Le prestataire de services crée un rattachement VLAN pour le locataire et configure Prisma Access pour Clean Pipe dans Panorama afin d'assurer la sécurité du rattachement VLAN, qui protège le trafic Internet du locataire.



 ©2025 Palo Alto Networks, Inc.

Exigences relatives à l'interconnexion Clean Pipe et partenaire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access

Avant de commencer, prenez connaissance des exigences suivantes en matière de déploiement de Clean Pipe, ainsi que des différences suivantes entre Prisma Access pour Clean Pipe et d'autres déploiements Prisma Access :

- Vous devez avoir une licence Prisma Access pour Clean Pipe.

  La licence Prisma Access pour Clean Pipe est une licence distincte des autres produits Prisma Access. Cependant, les mêmes exigences pour l'achat et l'installation des licences Panorama et Strata Logging Service s'appliquent à Clean Pipe.
- Prisma Access pour Clean Pipe présente les exigences d'interconnexion partenaire GCP suivantes :
  - Vous devez être en mesure de créer une interconnexion partenaire dans GCP.
  - Vous devez être en mesure de créer des rattachements VLAN dans GCP.
  - Pour les interconnexions partenaires de couche 2 (L2), vous devez avoir accès au routeur périphérique client (Customer Edge, CE) du côté MSSP et être en mesure d'en modifier la configuration.

  Pour plus d'informations sur la configuration du GCP, reportez-vous à la documentation du GCP.
- Tenez compte des exigences minimales en matière de bande passante pour le déploiement de Clean Pipe.

  La licence minimale que vous pouvez acheter est de 1000 Mbit/s. La bande passante allouée minimale pour chaque locataire Clean Pipe est de 100 Mbit/s.

  Après avoir créé un locataire, vous pouvez créer des Clean Pipes dans ce locataire. Chaque Clean Pipe doit être d'au moins 100 Mbit/s. Chaque Clean Pipe partage les domaines d'accès, les modèles, la pile de modèles et le groupe de périphériques du locataire.
- Si vous configurez plusieurs Clean Pipes pour un seul locataire, chaque Clean Pipe doit être un emplacement unique. Si vous souhaitez configurer deux rattachements VLAN pour un seul emplacement Clean Pipe dans une configuration active/de secours pour la redondance intrazone, spécifiez le choix **REDUNDANT (REDONDANT)** lorsque vous ajoutez une nouvelle instance Clean Pipe.
- Lors de la création d'une connexion au sein d'un locataire Clean Pipe, faites correspondre l'allocation de bande passante à celle du rattachement VLAN. Ne créez pas de rattachement VLAN avec une bande passante supérieure ou inférieure à la bande passante de la connexion.
- Une fois que vous avez activé l'architecture mutualisée, ne configurez pas votre déploiement Clean Pipe avec les autres onglets de la zone de configuration, à l'exception du lien **Generate API key (Générer une clé API)** dans l'onglet **Service Setup (Configuration du service)**, qui vous permet de générer une clé API pour récupérer les adresses IP Clean Pipe. Toute la configuration est propre à Prisma Access pour Clean Pipe et doit être séparée des autres

 ©2025 Palo Alto Networks, Inc.

déploiements Prisma Access, tels que Prisma Access pour les réseaux ou Prisma Access pour les utilisateurs.

- N'apportez pas de modifications à une configuration Clean Pipe après l'avoir validée. Si vous modifiez une configuration Clean Pipe après qu'elle a été validée, vous recevrez une erreur de validation lorsque vous la validerez à nouveau. Au lieu de cela, supprimez le Clean Pipe existant et ajoutez-en un nouveau. Programmez cette modification pendant une fenêtre d'interruption du système. Si vous avez déjà apporté des modifications et que vous n'avez pas encore validé, vous pouvez les annuler en modifiant la configuration Clean Pipe pour rétablir ses valeurs précédentes.
- Notez que les emplacements utilisés par Clean Pipe diffèrent des autres déploiements Prisma Access. Prisma Access pour Clean Pipe prend en charge les emplacements suivants :
  - asia-east1
  - asia-east2
  - asia-northeast1
  - asia-south1
  - asia-southeast1
  - australia-southeast1
  - europe-north1
  - europe-west2
  - europe-west3
  - europe-west4
  - northamerica-northeast1
  - southamerica-east1
  - us-central1
  - us-east1
  - us-east4
  - us-west1
  - us-west2
- Prenez note des restrictions de mise en réseau suivantes pour Clean Pipe :
  - La QoS pour Clean Pipe est uniquement prise en charge à l'entrée (d'Internet à la direction Clean Pipe).
  - User-ID n'est pas pris en charge.
  - Clean Pipe prend en charge l'affinité de session en fonction des adresses IP source et de destination, et il n'est pas configurable.
  - Les politiques « approuvé » à « approuvé » sont invalides pour Clean Pipe, car le trafic est toujours lié à Internet. Utilisez uniquement des politiques « approuvé » à « non approuvé ».

 ©2025 Palo Alto Networks, Inc.

Terminer la configuration de Clean Pipe

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• Licence Prisma Access

Pour terminer la configuration de Prisma Access pour Clean Pipe, vous effectuez la configuration dans l'interconnexion partenaire et dans Panorama.

Assurez-vous que vous pouvez accéder et configurer les routeurs CE et cloud du côté de l'interconnexion partenaire (non Prisma Access) de l'interconnexion partenaire.

STEP 1 | Du côté de l'interconnexion partenaire de la configuration, créez un rattachement VLAN à l'aide de la **Pairing Key (Clé de couplage)** que vous avez récupérée dans Panorama.

Pour obtenir plus d'informations sur la création de rattachements VLAN avec des interconnexions partenaires et la configuration de routeurs périphériques client (Customer Edge, CE) pour communiquer avec des routeurs cloud, reportez-vous à la documentation Google Cloud à l'adresse https://cloud.google.com/interconnect/docs/.

Assurez-vous que l'emplacement et la bande passante que vous sélectionnez correspondent au **Location (Emplacement)** que vous avez spécifié dans Panorama. Le fournisseur de services que vous utilisez pour l'interconnexion partenaire utilise la clé de couplage, ainsi que l'emplacement et la capacité de connexion demandés, pour terminer la configuration de votre rattachement VLAN.

STEP 2 | Une fois la connexion établie, revenez à Panorama, sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Network Details (Détails du réseau)** > **Clean Pipe** et notez les adresses IP **MSSP CE** et du **Cloud Router (Routeur cloud)**.

Ces valeurs sont renseignées après avoir saisi la **Pairing Key (Clé de couplage)** de l'autre côté du rattachement VLAN.



STEP 3 | Connectez-vous au routeur CE et effectuez la configuration suivante.

1. Saisissez l'adresse **MSSP CE** comme adresse IP locale.
2. Saisissez l'adresse ID du **Cloud Router (Routeur cloud)** comme adresse IP de l'homologue.
3. Saisissez un ASN BGP qui correspond au **BGP Peer ASN (ASN homologue BGP)** que vous avez saisi lors de la configuration de Clean Pipe dans Panorama.

   Assurez-vous de saisir ces valeurs correctement ; vous ne pouvez pas les modifier.

 ©2025 Palo Alto Networks, Inc.

STEP 4 | Vérifiez l'état de Clean Pipe.

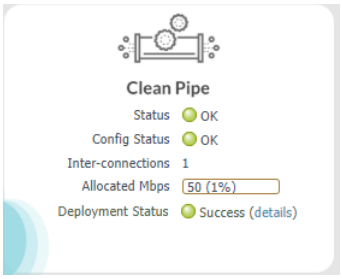
1. Dans Panorama, sélectionnez **Panorama** > **Cloud Services** > **Status (État)**, sélectionnez le **Tenant (Locataire)** dans la liste déroulante et vérifiez le**Status (État)** de Clean Pipe.

   Voir la liste des emplacements Prisma Access pour les valeurs acceptables.

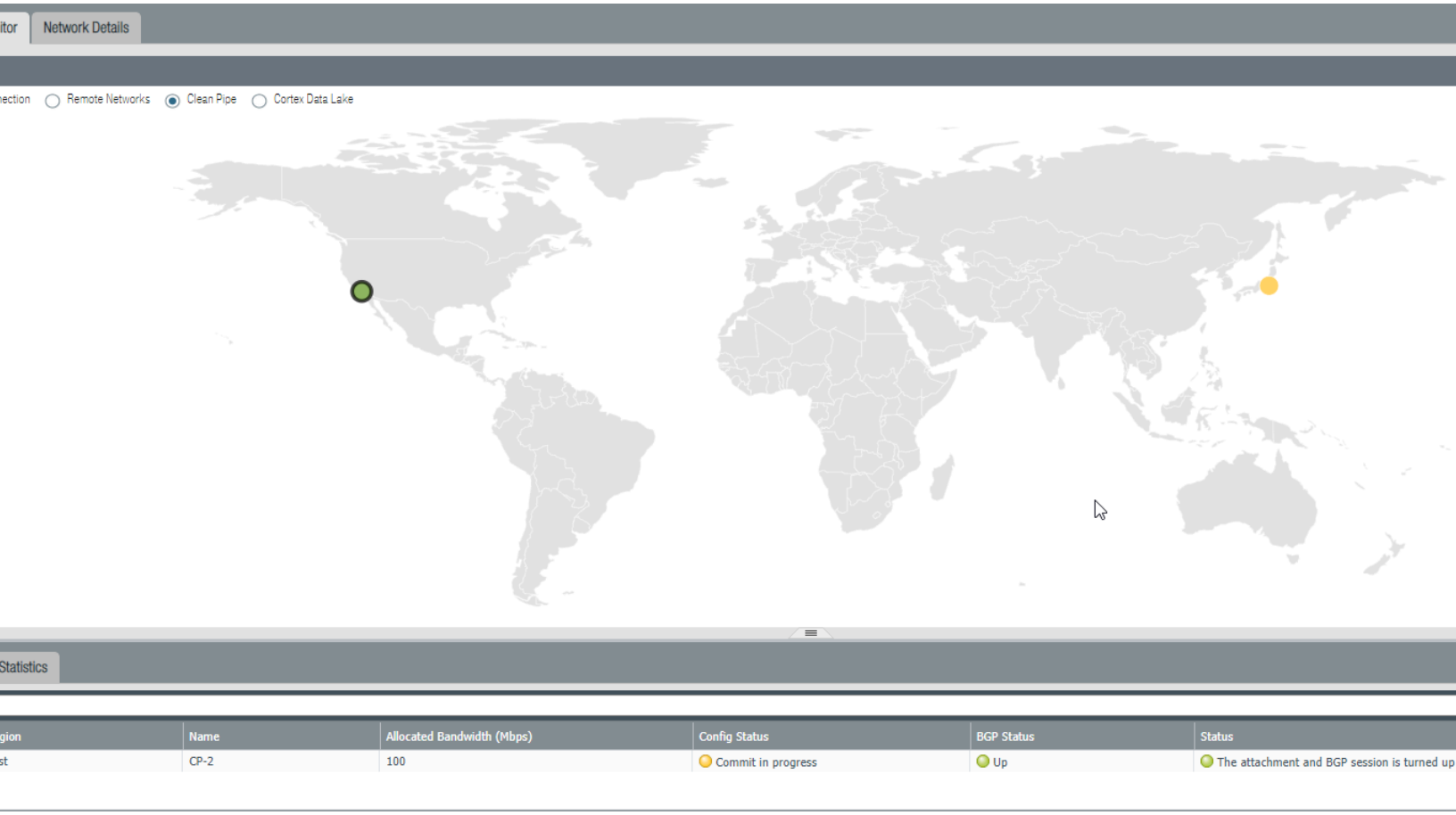
   La zone **Deployment Status (État du déploiement)** vous permet d'afficher la progression des tâches d'intégration et de déploiement avant qu'elles ne soient terminées, ainsi que

 ©2025 Palo Alto Networks, Inc.

de voir plus d'informations sur l'état des tâches terminées. Consultez la progression et l'état du déploiement pour plus de détails.



2. Sélectionnez **Panorama** > **Cloud Services** > **Status (État)** > **Clean Pipe** et cliquez sur l'onglet **Monitor (Surveiller)** pour voir une carte avec l'état des Clean Pipes déployés.



Cliquez sur les onglets sous la carte pour voir des statistiques supplémentaires sur les Clean Pipes.

Onglet **Status (État)** :

- **Compute Region (Région de calcul)** : la région de calcul dans laquelle votre infrastructure de service cloud est déployée pour l'instance de Clean Pipe.
- **Name (Nom)** : le nom de l'instance de Clean Pipe.
- **Allocated Bandwidth (Mbps) (Bande passante allouée (Mbit/s))** : la quantité de bande passante que vous avez allouée à l'instance de Clean Pipe.

 ©2025 Palo Alto Networks, Inc.

- **Config Status (État de la configuration)** : l'état de votre dernière transmission de configuration au service. Si vous avez effectué une modification localement et que vous n'avez pas encore transféré la configuration vers le cloud, l'état indique **Out of sync (Désynchronisé)**. Passez la souris sur l'indicateur d'état pour obtenir des informations plus détaillées. Après avoir validé et appliqué la configuration pour Prisma Access, l'état de la configuration passe à **In sync (En synchronisation)**.
- **BGP Status (État BGP)** : affiche des informations sur l'état BGP entre le pare-feu ou le routeur au niveau de l'instance Clean Pipe et Prisma Access. Bien que vous puissiez voir temporairement l'état passer par les différents états BGP (**Idle (Inactif)**, **Active (Actif)**, **Open send (Envoi ouvert)**, **Open pend (Attente ouverte)**, **Open confirm (Confirmation ouverte)**, le plus souvent, l'état BGP indique :
  - **Connect (Connecter)** : le routeur de l'instance Clean Pipe tente d'établir la relation d'homologue BGP avec le pare-feu cloud.
  - **Established (Établi)** : la relation de l'homologue BGP a été établie.

    Ce champ indiquera également si la connexion BGP est dans un état d'erreur :
  - **Warning (Avertissement)** : il n'y a pas eu de mise à jour de l'état BGP depuis plus de huit minutes. Cela peut indiquer une panne du pare-feu.

 ©2025 Palo Alto Networks, Inc.

  - **Error (Erreur)** : l'état BGP est inconnu.
- **Status (État)** : l'état de fonctionnement de la connexion entre Prisma Access et l'instance Clean Pipe.

Onglet **Statistics (Statistiques)** :

- **Region (Région)** : la région dans laquelle votre infrastructure de service cloud est déployée pour l'instance Clean Pipe.
- **Name (Nom)** : le nom de l'instance de Clean Pipe.
- **Allocated Bandwidth (Mbps) (Bande passante allouée (Mbit/s))** : la quantité de bande passante que vous avez allouée à l'emplacement réseau distant.
- **QoS** : sélectionnez **QoS** pour afficher une page contenant des statistiques QoS graphiques.
- **Avg Egress Bandwidth 5 Min (Mbps) (Bande passante de sortie moyenne sur 5 min (Mbit/s))** : quantité moyenne de bande passante de sortie Clean Pipe sur une période de 5 minutes.
- **Avg Egress Bandwidth 60 Min (Mbps) (Bande passante de sortie moyenne sur 60 min (Mbit/s))** : quantité moyenne de bande passante de sortie Clean Pipe sur une période de 60 minutes.
- **Avg Ingress Bandwidth 5 Min (Mbps) (Bande passante d'entrée moyenne sur 5 min (Mbit/s))** : quantité moyenne de bande passante d'entrée Clean Pipe sur une période de 5 minutes.
- **Avg Ingress Bandwidth 60 Min (Mbps) (Bande passante d'entrée moyenne sur 60 min (Mbit/s))** : quantité moyenne de bande passante d'entrée Clean Pipe sur une période de 60 minutes.
- **Egress Peak Bandwidth 1 Hour (Mbps) (Bande passante de sortie maximale sur 1 heure (Mbit/s))** : quantité de bande passante de sortie maximale pour l'instance Clean Pipe au cours de la dernière heure.
- **Egress Peak Bandwidth 24 Hour (Mbps) (Bande passante de sortie maximale sur 24 heures (Mbit/s))** : quantité de bande passante de sortie maximale pour l'instance Clean Pipe au cours des dernières 24 heures.
- **Egress Peak Bandwidth 7 Days (Mbps) (Bande passante de sortie maximale sur 7 jours (Mbit/s))** : quantité de bande passante de sortie maximale pour l'instance Clean Pipe au cours des 7 derniers jours.
- **Egress Peak Bandwidth 30 Days (Mbps) (Bande passante de sortie maximale sur 30 jours (Mbit/s))** : quantité de bande passante de sortie maximale pour l'instance Clean Pipe au cours des 30 derniers jours.
- **Ingress Peak Bandwidth 1 Hour (Mbps) (Bande passante d'entrée maximale sur 1 heure (Mbit/s))** : quantité de bande passante d'entrée maximale pour l'instance Clean Pipe au cours de la dernière heure.
- **Ingress Peak Bandwidth 24 Hour (Mbps) (Bande passante d'entrée maximale sur 24 heures (Mbit/s))** : quantité de bande passante d'entrée maximale pour l'instance Clean Pipe au cours des dernières 24 heures.

 ©2025 Palo Alto Networks, Inc.

- **Ingress Peak Bandwidth 7 Days (Mbps) (Bande passante d'entrée maximale sur 7 jours (Mbit/s))** : quantité de bande passante d'entrée maximale pour l'instance Clean Pipe au cours des 7 derniers jours.
- **Ingress Peak Bandwidth 30 Days (Mbps) (Bande passante d'entrée maximale sur 30 jours (Mbit/s))** : quantité de bande passante d'entrée maximale pour l'instance Clean Pipe au cours des 30 derniers jours.

Activer le multilocataire et créer un locataire

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	• Licence Prisma Access

Pour commencer la configuration de Clean Pipe, vous créez un déploiement multilocataire dans Panorama et créez un ou plusieurs locataires.

STEP 1 | Installez et activez Prisma Access pour Clean Pipe.

Prisma Access pour Clean Pipe nécessite une licence séparée, et son activation crée des onglets spécifiques à Clean Pipe dans le plug-in Cloud Services. La procédure que vous utilisez pour installer Prisma Access pour Clean Pipe est la même que celle que vous utilisez pour activer et installer une licence Prisma Access, y compris l'installation du plug-in Cloud Services.

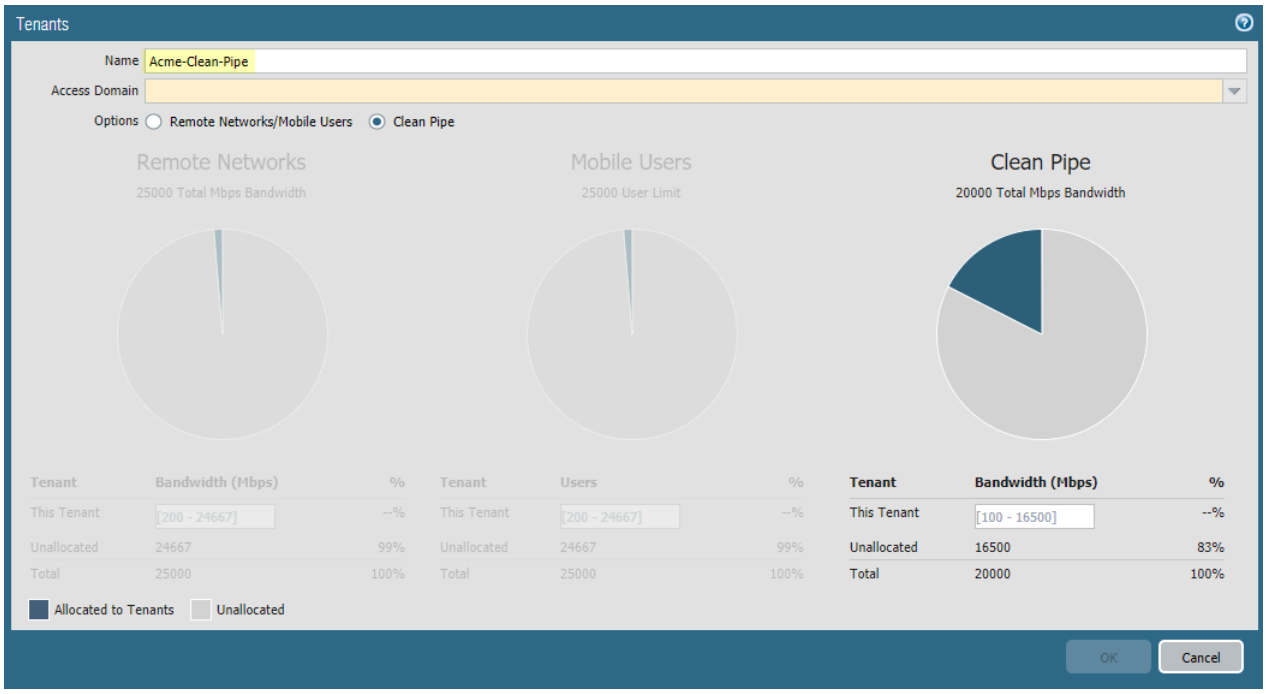
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Activez le multilocataire si vous ne l'avez pas déjà fait.

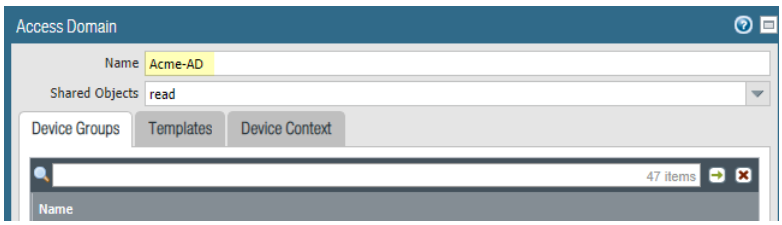
1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration**.
2. Sélectionnez **Enable Multitenancy (Activer le multilocataire)** (situé en haut à droite de la page).
3. Cliquez sur **OK**.

   La page **Tenants (Locataires)** s'affiche.
4. Dans la zone **Options**, sélectionnez **Clean Pipe**.

   Pour configurer un locataire pour des réseaux distants, des utilisateurs mobiles, ou les deux, reportez-vous à la section Gérer plusieurs locataires dans Prisma Access.



5. Saisissez un **Name (Nom)** pour le premier locataire.
6. Créez et configurez un nouveau **Access Domain (Domaine d'accès)** pour le premier locataire et cliquer sur **OK**.



7. Dans la zone **Clean Pipe**, saisissez une **Bandwidth (Mbps) (bande passante (Mbit/s))** pour **This Tenant (Ce locataire)**.

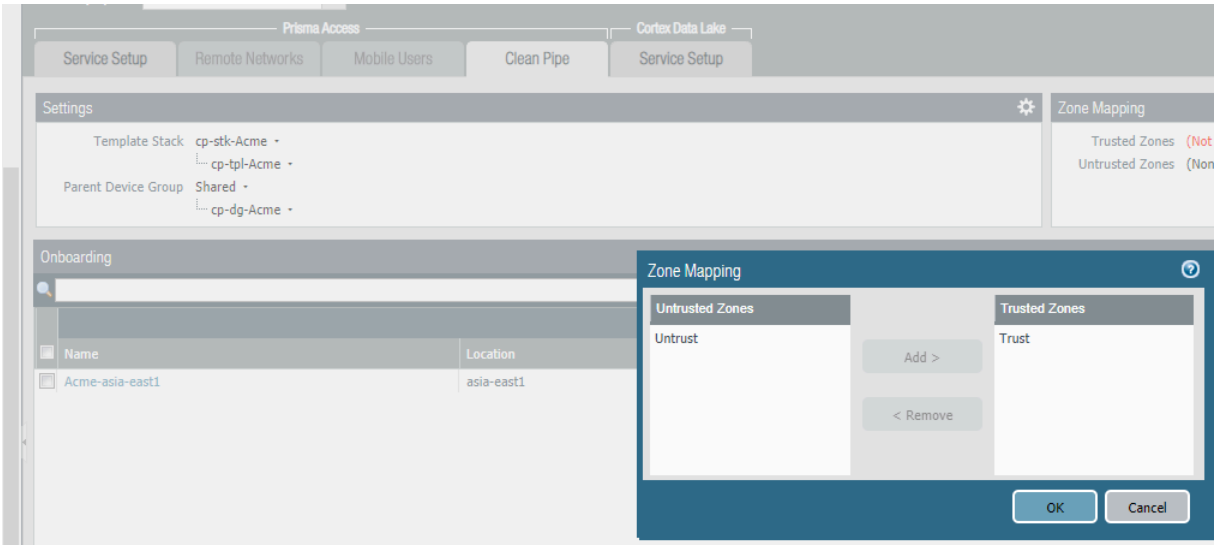
   Saisissez un minimum de 100 Mbit/s pour chaque locataire que vous créez.
8. Cliquez sur **OK**.

 ©2025 Palo Alto Networks, Inc.

STEP 3 | Créez des zones pour le locataire et mappez ces zones pour le locataire.

1. Sélectionnez **Network (Réseau)** > **Zones**.

   Assurez-vous d'avoir sélectionné le **Template (Modèle)** Clean Pipe pour le locataire que vous avez créé (**cp-tpl-***tenant*).
2. Créez des zones pour le locataire (par exemple, **Trust (Approuvée)** et **Untrust (Non approuvée)**).
3. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** et sélectionnez le **Tenant (Locataire)** dans la liste déroulante.
4. Sélectionnez l'onglet **Clean Pipe**.
5. Cliquez sur l'icône de l'engrenage à côté de **Zone Mapping (Mappage de zones)** pour modifier les paramètres.
6. **Add (Ajoutez)** et **Remove (Supprimez)** les zones que vous avez créées pour les mapper aux zones approuvées et non approuvées.



STEP 4 | Intégrer un nouveau Clean Pipe.

1. Sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Clean Pipe**.
2. **Add (Ajoutez)** une nouvelle instance de Clean Pipe pour le locataire, en saisissant les informations suivantes :

   - **Name (Nom)** : spécifiez un nom pour le Clean Pipe.
   - **Bandwidth (Bande passante)** : sélectionnez la bande passante à allouer pour le Clean Pipe.

     Vous pouvez intégrer des instances Clean Pipe par paliers de 100 Mbit/s, 200 Mbit/s, 300 Mbit/s, 400 Mbit/s, 500 Mbit/s, 1 000 Mbit/s, 2 000 Mbit/s, 5 000 Mbit/s et 10 000 Mbit/s. La quantité de bande passante que vous spécifiez doit être dans

 ©2025 Palo Alto Networks, Inc.

l'allocation de bande passante sous licence, et elle doit correspondre à la bande passante de l'attachement VLAN que vous créez dans l'interconnexion partenaire.

- **Edge Availability Domain (Domaine de disponibilité périphérique)** : sélectionnez le domaine de disponibilité que vous souhaitez pour le Clean Pipe. Vous pouvez choisir **1**, **2**, **ANY (TOUT)** ou **REDUNDANT (REDONDANT)**.
  - Spécifiez **ANY (TOUT)** pour un déploiement Clean Pipe non redondant.

    Assurez-vous que votre fournisseur de cloud prend en charge ce choix ; vous devez également sélectionner **ANY (TOUT)** du côté du fournisseur de cloud de l'interconnexion partenaire. Si ce choix n'est pas disponible pour votre fournisseur de cloud, faites un autre choix.
  - Pour spécifier deux attachements VLAN au même emplacement dans une configuration active/de secours au même emplacement, sélectionnez **REDUNDANT (REDONDANT)**.

    Prisma Access crée deux clés de couplage pour une configuration **REDUNDANT (REDONDANTE)** (une pour chaque zone de disponibilité) et ajoute `zone1` au nom du Clean Pipe pour la première zone de disponibilité et `zone2` pour la deuxième zone de disponibilité. Par exemple, si vous spécifiez comme **Name (Nom)** **San Francisco**, Prisma Access crée deux zones nommées **San Francisco-zone1** et **San Francisco-zone2**.

    Assurez-vous de configurer la première zone de disponibilité (zone1) comme la zone principale sur votre CPE.

Vous pouvez également construire une paire de Clean Pipes pour une redondance à locataire unique dans différents emplacements ; pour ce faire, spécifiez **1** pour le

 ©2025 Palo Alto Networks, Inc.

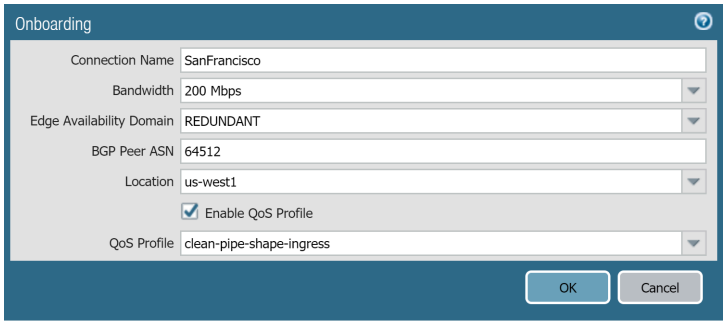
premier Clean Pipe dans un emplacement et **2** pour le deuxième Clean Pipe dans un emplacement différent.

- **BGP Peer ASN (ASN homologue BGP)** : saisissez le numéro de système autonome (ASN) BGP.

  Vous pouvez spécifier soit un ASN BGP privé, soit un ASN BGP public.

  Prenez note de cette valeur ; vous la configurez sur le routeur périphérique client (CE, Customer Edge) lorsque vous terminez la configuration Clean Pipe.
- **Location (Emplacement)** : sélectionnez l'emplacement.

  Nous vous recommandons d'utiliser le même emplacement que celui que vous utilisez lorsque vous créez l'attachement VLAN pour l'interconnexion partenaire.
- Pour activer la QoS, sélectionnez la **QoS**, puis sélectionnez le profil QoS à utiliser avec le Clean Pipe. La QoS de Clean Pipe se forme à l'entrée.

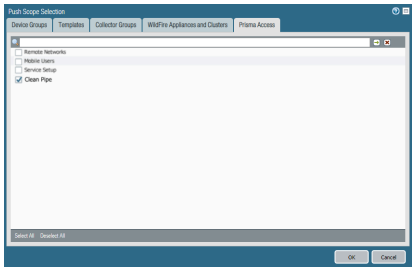


STEP 5 | Ajoutez plus d'instances de Clean Pipe selon les besoins en répétant l'étape 4.

Assurez-vous que chaque Clean Pipe supplémentaire utilise un emplacement différent.

STEP 6 | Validez et transmettez vos modifications pour les rendre actives dans Prisma Access.

1. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** et **Edit Selections (Modifier les sélections)** dans la portée d'application.
2. Sélectionnez **Prisma Access**, puis sélectionnez **Clean Pipe**.



3. Cliquez sur **OK** pour enregistrer les modifications dans la portée d'application.
4. **Commit (Validez)** et **Push (Transmettez)** vos modifications.

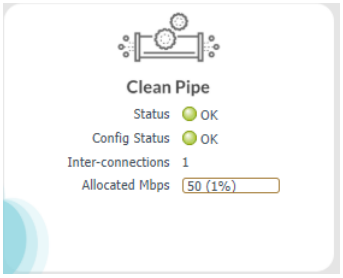
 ©2025 Palo Alto Networks, Inc.

STEP 7 | Vérifiez que votre Clean Pipe a été approvisionné.

1. Sélectionnez **Panorama** > **Cloud Services** > **Status (État)**.
2. Sélectionnez le **Tenant (Locataire)** dans la liste déroulante en haut de la page.
3. Cliquez sur **Status (État)**.

   L'état du Clean Pipe s'affiche.
4. Survolez le **Config Status (État de configuration)** du Clean Pipe et attendez que l'état passe de **Provisioning in Progress (Approvisionnement en cours)** à **Provisioned (Approvisionné)**.

   Cet approvisionnement peut prendre jusqu'à 30 minutes.

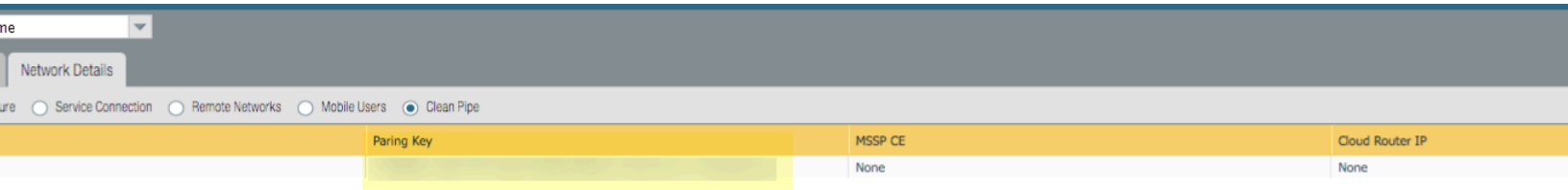


STEP 8 | Cliquez sur l'onglet **Network Details (Détails du réseau)**, cliquez sur le bouton radio **Clean Pipe** et notez la **Pairing Key (Clé de couplage)**.

Les champs **MSSP CE** et **Cloud Router IP (IP de routeur cloud)** sont vides lorsque vous commencez à configurer le Clean Pipe. Ces champs se remplissent après que vous avez créé l'attachement VLAN lorsque vous terminez la configuration du Clean Pipe.

Si vous avez spécifié une connexion **REDUNDANT (REDONDANTE)**, Prisma Access crée deux clés de couplage, une pour chaque zone de disponibilité, et ajoute `zone1` au nom du Clean Pipe pour la première zone de disponibilité et `zone2` pour la deuxième zone de disponibilité. La capture d'écran suivante montre le Clean Pipe **SanFrancisco** avec une configuration redondante ; Prisma Access a créé deux clés de couplage, une pour **SanFrancisco-zone1** et une pour **SanFrancisco-zone2**.

Assurez-vous de configurer la première zone de disponibilité (zone1) comme la zone principale sur votre CPE.



STEP 9 | Terminez la configuration du Clean Pipe.

 ©2025 Palo Alto Networks, Inc.