paloalto TECHDOCS

Guide de l'administrateur réseau PAN-OS®

Version 11.1 & 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

© 2023-2024 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

May 1, 2024

Table of Contents

Mise en réseau 11

Introduction à la mise en réseau 12

Configurer les interfaces 15

Interfaces Tap 16
Interfaces de câble virtuel 18
Paquets des couches 2 et 3 sur un câble virtuel 19
Vitesses des ports des interfaces de câble virtuel 20
LLDP sur un câble virtuel 20
Interfaces regroupées pour un câble virtuel 20
Prise en charge de la haute disponibilité par le câble virtuel 21
Protection de zone pour une interface de câble virtuel 21
Trafic étiqueté VLAN 21
Sous-interfaces de câble virtuel 21
Configuration des câbles virtuels 25
Interfaces de Couche 2 28
Interfaces de couche 2 sans réseau local virtuel (VLAN) 28
Interfaces de couche 2 avec les réseaux locaux virtuels (VLANs) 29
Configuration d'une interface de couche 2 30
Configuration d'une interface de couche 2, une sous-interface et un réseau local virtuel 31
Gestion de la ré-écriture de paquets Per-VLAN Spanning Tree (PVST+) BPDU 31
Interfaces de Couche 3 35
Configurer les interfaces de couche 3 39
Gérer les hôtes IPv6 à l'aide du NDP 49
Interfaces cellulaires 56
Configurer la 5G pour une interface cellulaire 56
Mise à niveau du microprogramme 5G 72
Configurer un client PPPoE sur une sous-interface 83
Configurer un client PPPoE IPv6 89
Configuration d'un groupe d'interfaces agrégé 96
Configurer Bonjour Reflector pour la segmentation du réseau 101
Utilisation des profils de gestion d'interface pour limiter l'accès 104

Routeurs virtuels 107

Vue d'ensemble des routeurs virtuels 108
Configurer des routeurs virtuels 109

 ©2024 Palo Alto Networks, Inc.

Itinéraires de service 111
Vue d'ensemble des itinéraires de service 112
Configurer les itinéraires de service 113
Itinéraires statiques 115
Présentation des itinéraires statiques 116
Suppression d'un itinéraire statique basé sur la surveillance des chemins 117
Configuration d'un itinéraire statique 120
Configuration de la surveillance des chemins pour un itinéraire statique 123
RIP 127
Présentation de RIP 128
Configurer RIP 129
OSPF 131
Concepts d'OSPF 132
OSPFv3 132
Voisins OSPF 133
Zones OSPF 133
Types de routeurs OSPF 134
Configuration d'OSPF 135
Configuration d'OSPFv3 139
Configuration du redémarrage en douceur d'OSPF 143
Confirmation du fonctionnement d'OSPF 145
Affichage de la table de routage 145
Confirmation des adjacences OSPF 145
Confirmation que des connexions OSPF sont établies 145
BGP 147
Présentation de BGP 148
MP-BGP 149
Configuration de BGP 151
Configuration d'un homologue BGP avec le protocole MP-BGP en mode multicast IPv4 ou IPv6 160
Configuration d'un homologue BGP avec le protocole MP-BGP en mode multicast IPv4 164
Confédérations BGP 166
Multidiffusion IP 173
IGMP 174
PIM 176

 ©2024 Palo Alto Networks, Inc.

Shortest-Path Tree (arbre du chemin le plus court ; SPT) et arborescence partagée 178
Mécanisme d'affirmation PIM 180
Renvoi de chemin inverse 180
Configurer la multidiffusion IP 182
Affichage des informations sur la multidiffusion IP 190

Redistribution de route 193
Présentation de la redistribution des itinéraires 194
Configurez la redistribution des itinéraires 195

Tunnels GRE 199
Aperçu du tunnel GRE 200
Création d'un tunnel GRE 202

DHCP 205
Présentation de DHCP 206
Pare-feu en tant que serveur et client DHCP 207
Pare-feu en tant que client DHCPv6 208
Messages DHCP 211
Adressage DHCP 213
Méthodes d'allocation d'adresse DHCP 213
Baux DHCP 214
Options DHCP 215
Options DHCP prédéfinies 215
Plusieurs valeurs pour une option DHCP 216
Options DHCP 43, 55 et 60 et autres options personnalisées 217
Adresses IPv6 dynamiques sur l'interface de gestion 218
Configuration d'une interface en tant que serveur DHCP 222
Configurer une interface en tant que client DHCPv4 227
Configurer une interface en tant que client DHCPv6 avec délégation de préfixes 230
Configuration de l'interface de gestion en tant que client DHCP 247
Configuration de l'interface de gestion pour l'attribution d'adresses IPv6 dynamiques 250
Configuration d'une interface en tant qu'agent de relais DHCP 253
Surveillance et dépannage de DHCP 255
Affichage des informations sur le serveur DHCP 255
Effacer les baux DHCP 255
Affichage des informations sur le client DHCP 256
Obtention du résultat du débogage DHCP 256

 ©2024 Palo Alto Networks, Inc.

DNS 257
Présentation de DNS 258
Objet proxy DNS 261
DNS Server Profile (profil de serveur DNS) 262
Déploiements DNS à plusieurs locataires 263
Configuration d'un objet proxy DNS 265
Configuration d'un profil de serveur DNS 271
Configurer un proxy Web 273
Configurer le proxy explicite 274
Configurer le proxy transparent 289
Configurer l'authentification pour le proxy Web explicite 302
Configurer des exemptions pour l'authentification de proxy explicite 314
Exclure tout le trafic de proxy explicite de l'authentification 318
Cas pratique 1 : Le pare-feu exige une résolution DNS 319
Cas d'utilisation 2 : Le locataire de l'ISP utilise un proxy DNS pour traiter la résolution DNS pour des politiques de sécurité, la génération de rapports et des services de son système virtuel 323
Cas d'utilisation 3 : Le pare-feu sert de proxy DNS entre le client et le serveur 327
Mise en correspondance de la règle de proxy DNS et du FQDN 329
DDNS 335
Présentation des DNS dynamiques 336
Configuration des DNS dynamiques pour les interfaces du pare-feu 339
NAT 343
Règles de politique NAT 344
Présentation de la politique NAT 344
Pools d'adresses NAT identifiés comme des objets adresse 345
Proxy ARP pour les pools d'adresses NAT 346
NAT source et NAT de destination 348
NAT source 348
NAT de destination 352
NAT de destination avec cas d'utilisation de la réécriture DNS 355
Nombre de règles NAT 361
Dépassement d'abonnement NAT DIPP 362
Statistiques de la mémoire NAT du plan de données 363
Configuration de NAT 364
Traduction d'adresses IP clients internes en votre adresse IP publique (NAT DIPP source) 365
Créer une règle source NAT avec DIPP persistant 367
PAN-OS 367

 ©2024 Palo Alto Networks, Inc.

Strata Cloud Manager....369
Autorisation d'accès des clients sur le réseau interne à vos serveurs publics (NAT U-Turn de destination)....371
Activation de la traduction bidirectionnelle d'adresses pour vos serveurs orientés public (NAT source statique)....372
Configuration de la NAT de destination avec réécriture DNS....373
Configuration de la NAT de destination à l'aide des adresses IP dynamiques....374
Modification du taux de dépassement d'abonnement NAT DIPP....376
Réservation d'adresses NAT IP dynamiques....376
Désactivation de la NAT pour un hôte ou une interface spécifique....378
Exemples de configuration NAT....379
Exemple de NAT de destination : mappage un à un....379
Exemple de NAT de destination avec traduction de port....380
Exemple de NAT de destination : mappage un à plusieurs....381
Exemple de NAT source et de NAT de destination....381
Exemple de NAT source dans un câble virtuel....383
Exemple de NAT statique dans un câble virtuel....384
Exemple de NAT de destination dans un câble virtuel....384

NPTv6....387

Présentation de NPTv6....388
Unique Local Address (adresse locale unique - ULA)....388
Raisons de l'utilisation de NPTv6....389
Fonctionnement de NPTv6....390
Mappage indépendant de la somme de contrôle....391
Traduction bidirectionnelle....392
NPTv6 appliqué à un service spécifique....392
Proxy NDP....393
Exemple de fonctionnement de NPTv6 et du proxy NDP....395
Exemple du cache ND dans NPTv6....395
Exemple du proxy NDP dans NPTv6....395
Exemple de la traduction NPTv6 dans NPTv6....396
Les voisins figurant dans le cache ND ne sont pas traduits....396
Création d'une politique NPTv6....397

NAT64....401

Aperçu de NAT64....402
Adresse IPv6 intégrée à IPv4....403
Serveur DNS64....404
Découverte de Chemin MTU....405
Communications initiées par IPv6....406

 ©2024 Palo Alto Networks, Inc.

Configurer NAT64 pour la communication initiée par IPv6 408
Configurer NAT64 pour la communication initiée par IPv4 413
Configurer NAT64 pour la communication initiée par IPv4 avec la traduction de port 416

ECMP 421

Algorithmes d'équilibrage de la charge ECMP 423
Configuration d'ECMP sur un routeur virtuel 425
Activation d'ECMP pour plusieurs systèmes BGP autonomes 428
Vérification d'ECMP 429

LLDP 431

Présentation de LLDP 432
Éléments TLV pris en charge dans LLDP 433
Pièges SNMP et messages Syslog LLDP 435
Configuration de LLDP 436
Affichage de l'état et des paramètres LLDP 438
Effacement des statistiques LLDP 440

BFD 441

Présentation de la BFD 442
Prise en charge du client, de l'interface et du modèle BFD 443
Composants RFC de la BFD non pris en charge 443
BFD pour les itinéraires statiques 443
BFD pour les protocoles de routage dynamiques 444
Configuration de la BFD 446
Référence : Détails de la BFD 453

Paramètres et délais d'expiration de session 459

Sessions de couche de transport 460
TCP 461
Minuteurs Sessions TCP à moitié fermées et Sessions TCP en état time_wait 461
Minuteur RST non vérifié 463
Abandon de l'établissement de liaison de segmentation TCP 463
Maximum Segment Size (taille de segment maximale ; MSS) 464
UDP 466
ICMP 467
Règles de politique de sécurité basées sur les paquets ICMP et ICMPv6 467
Limitation du débit ICMPv6 468
ICMP spécifiques à la commande ou Types et Codes ICMPv6 469
Configuration des délais d'expiration de session 470

 ©2024 Palo Alto Networks, Inc.

Configuration des paramètres de session....473
Politiques de Distribution de Sessions....478
Descriptions des Politiques de Distribution de Sessions....479
Modification des Politiques de Distribution de Sessions et Affichage des Statistiques....481
Prévention de l'établissement de la session de liaison de segmentation TCP....483

Inspection du contenu du tunnel....485
Présentation de l'inspection du contenu du tunnel....486
Configurer l'inspection du contenu du tunnel....490
Afficher l'activité du tunnel inspecté....499
Afficher les informations de tunnel dans les journaux....500
Créer un rapport personnalisé basé sur le trafic de tunnel étiqueté....502
Comportement d'accélération du tunnel....503
Désactivation de l'accélération du tunnel....506

Broker de paquets réseau....507
Présentation du Broker de paquets réseau....508
Fonctionnement du Broker de paquets réseau....511
Préparez-vous à déployer le Broker de paquets de réseau....513
Chaîne de sécurité de la passerelle transparente....516
Configurer les chaînes de sécurité routées de la couche 3....522
Assistance haute disponibilité du broker de paquets réseau....528
Modifications de l'interface utilisateur pour le Broker de paquets de réseau....529
Limitations du Broker de paquets de réseau....531
Dépannage du Broker de paquets réseau....534

Routage avancé....535
Activer le routage avancé....537
Vue d'ensemble du routeur logique....543
Configurer un routeur logique....544
Créer un itinéraire statique....548
Configurer BGP sur un moteur de routage avancé....553
Créer des profils de routage BGP....567
Créer des filtres pour le moteur de routage avancé....580
Configurer OSPFv2 sur un moteur de routage avancé....603
Créer des profils de routage OSPF....611
Configurer OSPFv3 sur un moteur de routage avancé....618
Créer des profils de routage OSPFv3....627
Configurer RIPv2 sur un moteur de routage avancé....633
Créer des profils de routage RIPv2....638
Créer des profils BFD....642

 ©2024 Palo Alto Networks, Inc.

Configurer la multidiffusion IPv4 645
Configurer MSDP 655
Créer des profils de routage multidiffusion 661
Créer un MRoute IPv4 664

Poe 667

Aperçu PoE 668
Configurer PoE 669

 ©2024 Palo Alto Networks, Inc.

Mise en réseau

Tous les pare-feu Palo Alto Networks® de dernière génération disposent d'une architecture flexible de mise en réseau incluant la prise en charge du routage dynamique, du basculement et de la connectivité VPN, elle vous permet ainsi de déployer le pare-feu dans presque tous les environnements de mise en réseau.

- Introduction à la mise en réseau

Introduction à la mise en réseau

La mise en réseau est la pierre angulaire des pare-feu, car ils doivent être en mesure de recevoir des données, de les traiter et de les transmettre. Lors de la configuration des ports Ethernet sur votre pare-feu, vous pouvez choisir entre des déploiements d'interface de type Câble virtuel, Couche 2, Couche 3 ou AE. Aussi, afin de pouvoir procéder à des intégrations dans une variété de segments de réseau, vous pouvez configurer différents types d'interfaces sur différents ports.

Pour commencer la mise en réseau, vous devez d'abord accéder à la rubrique Mise en route du Guide de l'administrateur de PAN-OS®. Vous y apprendrez à segmenter votre réseau et à Configure Interfaces and Zones (configurer des interfaces et des zones); cette tâche initiale illustre comment configurer des interfaces de Couche 3 pour se connecter à Internet, à votre réseau interne et à vos applications de centre de données.

Ce guide de l'administrateur réseau PAN-OS développe ces informations avec des rubriques sur la configuration des interfaces tap, virtual wire, Layer 2, Layer 3 et AE. Une fois vos interfaces réseau configurées, vous pouvez procéder à l'Export Configuration Table Data (Exportation des données du tableau de configuration) au format PDF ou CSV à des fins d'examen interne ou d'audits.

Ce guide explique également comment le pare-feu prend en charge plusieurs routeurs virtuels pour obtenir des itinéraires de couche 3 vers d'autres sous-réseaux et pour gérer des ensembles d'itinéraires distincts. Les chapitres restants décrivent les itinéraires statiques, les protocoles de routage dynamique et les principales fonctionnalités qui prennent en charge la mise en réseau sur le pare-feu.

Vous pouvez décider d'activer Routage avancé. Le moteur de routage avancé utilise desrouteurs logiques au lieu de routeurs virtuels.

- Configurer les interfaces
- Routeurs virtuels
- Itinéraires de service
- Itinéraires statiques
- RIP
- OSPF
- BGP
- Multidiffusion IP
- Redistribution de route
- Tunnels GRE
- DHCP
- DNS
- DDNS
- NAT
- NPTv6

 ©2024 Palo Alto Networks, Inc.

- NAT64
- ECMP
- LLDP
- BFD
- Paramètres et délais d'expiration de session
- Inspection du contenu du tunnel
- Broker de paquets réseau
- Poe

 ©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

Configurer les interfaces

Un pare-feu Palo Alto Networks® de dernière génération peut fonctionner dans plusieurs déploiements simultanément, car ces derniers se font au niveau de l'interface. Par exemple, vous pouvez configurer certaines interfaces de Couche 3 qui permettront d'intégrer le pare-feu à votre environnement de routage dynamique et configurer d'autres interfaces qui s'intégreront à votre réseau de basculement de Couche 2.

Les rubriques suivantes décrivent chaque type de déploiement d'interface et comment le configurer, comment configurer Bonjour Reflector et comment utiliser les profils de gestion d'interface.

- Interfaces Tap
- Interfaces de câble virtuel
- Interfaces de Couche 2
- Interfaces de Couche 3
- Interfaces cellulaires
- (PAN-OS 11.0.1 et versions 11.1 ultérieures)Configurer un client PPPoE sur une sous-interface
- Configurer un client PPPoE IPv6
- Configuration d'un groupe d'interfaces agrégé
- Configurer Bonjour Reflector pour la segmentation du réseau
- Utilisation des profils de gestion d'interface pour limiter l'accès

Interfaces Tap

Un TAP réseau est un équipement permettant d'accéder aux flux de données d'un réseau informatique. Le déploiement en mode TAP vous permet de surveiller de façon passive le flux de trafic d'un réseau au moyen d'un port SPAN de commutation ou d'un port miroir.

Le port SPAN ou miroir permet de copier le trafic d'autres ports sur le commutateur. En dédiant une interface sur le pare-feu en mode TAP et en la connectant à un port SPAN de commutation, ce dernier fournit au pare-feu un trafic en miroir. Une application devient alors visible au sein du réseau sans être dans le flux du trafic réseau.

En déployant le pare-feu en mode Tap, vous pouvez avoir un aperçu des applications qui sont actives sur votre réseau sans avoir à modifier la configuration de votre réseau. De plus, en mode Tap, le pare-feu peut également identifier les menaces sur votre réseau. N'oubliez toutefois pas que, comme le trafic ne passe pas par le pare-feu lorsqu'il est en mode Tap, le pare-feu ne peut pas exercer d'action à l'égard du trafic, comme bloquer le trafic qui présente des menaces ou appliquer un contrôle du trafic QoS.

Pour configurer une interface Tap et commencer à surveiller les applications et les menaces sur votre réseau :

STEP 1 | Décidez le port que vous souhaitez utiliser en tant qu'interface Tap et connectez-le à un commutateur configuré avec SPAN/RSPAN ou la mise en miroir du port.

Vous enverrez votre trafic réseau à partir du port de destination SPAN via le pare-feu, ce qui vous donnera une visibilité des applications et des menaces présentes sur votre réseau.

STEP 2 | À partir de l'interface Web du pare-feu, configurez l'interface que vous souhaitez utiliser en tant que Tap réseau.

1. Sélectionnez **Network (Réseau)** > **Interfaces** et sélectionnez l'interface qui correspond au port que vous venez de câbler.
2. Sélectionnez **Tap** comme **Interface Type (Type d'interface)**.
3. Dans l'onglet **Config (Configuration)**, développez la liste **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**.
4. Dans la boîte de dialogue Zone, donnez un **Name (Nom)** à la nouvelle zone, par exemple, ZoneTap, puis cliquez sur **OK**.

STEP 3 | (Optionnal (Facultatif)) Créez les profils de transfert que vous voulez utiliser.

- Configure Log Forwarding (Configurez le transfert des journaux).
- Configure Syslog Monitoring (Configuration de la surveillance Syslog)

©2024 Palo Alto Networks, Inc.

STEP 4 | Créez des Security Profiles (profils de sécurité) pour analyser votre trafic réseau à la recherche de menaces :

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)**.
2. Pour chaque type de profil de sécurité, **Add (Ajoutez)** un nouveau profil et définissez l'action sur **alert (alerter)**.

   Comme le pare-feu n'est pas en harmonie avec le trafic, vous ne pouvez pas utiliser les actions de blocage ou de réinitialisation. En définissant l'action sur Alert (Alerter), vous serez en mesure de voir les menaces que le pare-feu détecte dans les journaux et l'ACC.

STEP 5 | Créez une règle de politique de sécurité pour autoriser le trafic par l'intermédiaire de l'interface Tap.

Lors de la création d'une règle de politique de sécurité pour le mode Tap, la zone source et la zone de destination doivent être identiques.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **Source**, sélectionnez ZoneTap que vous devez de définir en regard de **Zone source**.
3. Dans l'onglet **Destination**, réglez la **Destination Zone (Zone de destination)** sur la ZoneTap également.
4. Définissez tous les critères de correspondance à la règle (**Applications**, **User (Utilisateur)**, **Service**, **Address (Adresse)**) sur **any (Indifférent)**.
5. Dans l'onglet **Actions**, définissez **Action Setting (Paramètre d'action)** sur **Allow (Autoriser)**.
6. Définissez le **Profile Type (Type de profil)** sur **Profiles (Profils)**, puis sélectionnez que chacun des profils de sécurité que vous avez créés doit vous alerter des menaces.
7. Vérifiez que **Log at Session End (Journalisation en fin de session)** est activé.
8. Cliquez sur **OK**.
9. Placez la règle au haut de votre base de règles.

STEP 6 | ((Supported firewalls onlyPare-feu pris en charge uniquement)) Si l'interface correspond à un port PoE (Power over Ethernet) sur le pare-feu, vous pouvez éventuellement configure PoE (configurer PoE).

STEP 7 | **Commit (Validez)** la configuration.

STEP 8 | Surveillez les journaux du pare-feu (**Monitor (Surveillance)** > **Logs (Journaux)**) et l'**ACC** pour obtenir des renseignements sur les applications et les menaces présentes sur votre réseau.

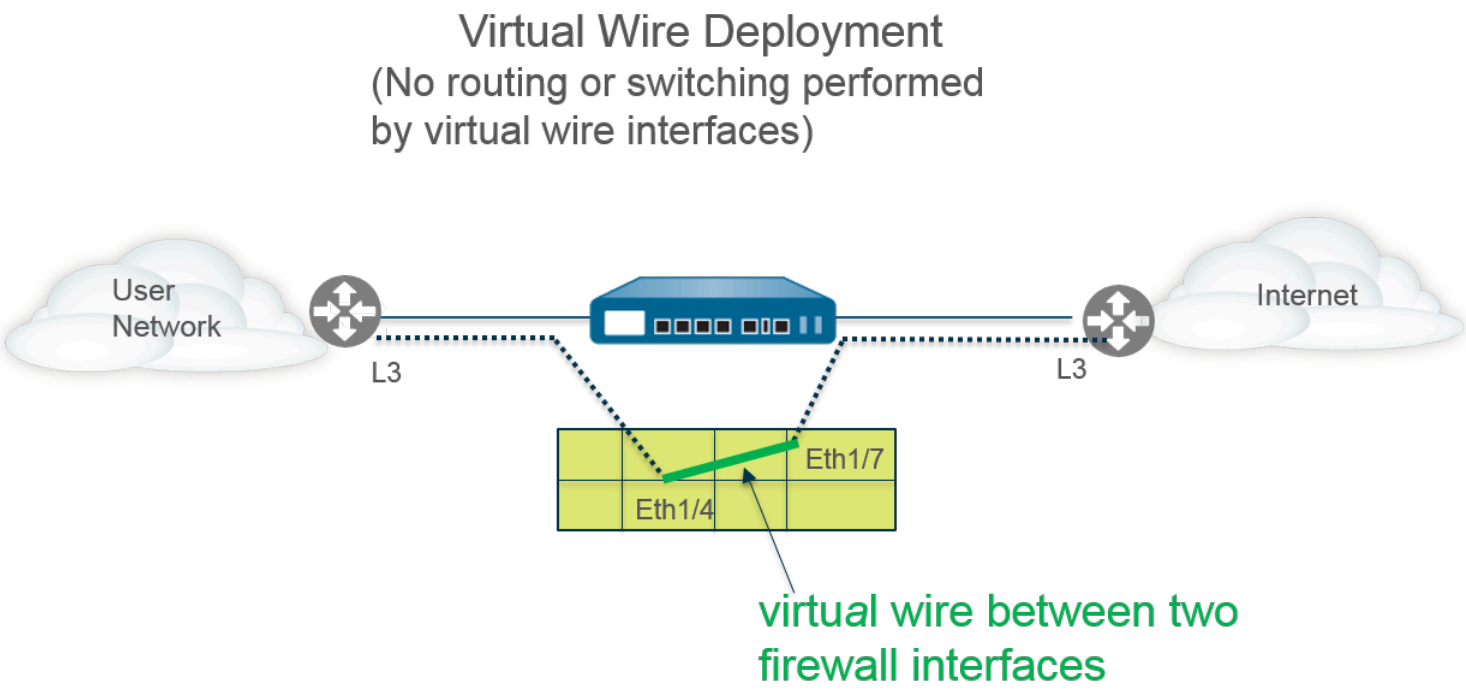
 ©2024 Palo Alto Networks, Inc.

Interfaces de câble virtuel

Pour le déploiement d'un câble virtuel, vous installez un pare-feu de façon transparente sur un segment de réseau en reliant deux ports (interfaces) de pare-feu entre eux. Le câble virtuel connecte de façon logique les deux interfaces ; ainsi, le câble virtuel est interne au pare-feu.

Utilisez un déploiement de câble virtuel uniquement lorsque vous souhaitez facilement intégrer un pare-feu dans une topologie et que les deux interfaces connectées sur le pare-feu ne nécessitent aucun basculement ou routage. Pour ces deux interfaces, le pare-feu est considéré comme une *bosse dans le câble*.

Un déploiement de câble virtuel simplifie l'installation et la configuration d'un pare-feu, car vous pouvez insérer le pare-feu dans une topologie existante sans affecter d'adresses IP ou MAC aux interfaces, revoir la conception du réseau ou reconfigurer les appareils réseau environnants. Le câble virtuel prend en charge le blocage et l'autorisation du trafic en fonction des étiquettes de réseau local virtuel (VLAN) en plus des règles de politique de sécurité, l'App-ID, le Content-ID, l'User-ID, le décryptage, LLDP, la HA active/passive et active/active, QoS, la protection de zone (avec certaines exceptions), la protection contre les protocoles non IP, la protection DoS, la protection contre la mémoire tampon de paquets, l'inspection du contenu du tunnel et NAT.



Chaque interface de câble virtuel est directement connectée à un appareil réseau ou hôte de Couche 2 ou 3. Les interfaces de câble virtuel n'ont pas d'adresses de Couche 2 ou 3. Lorsqu'une des interfaces de câble virtuel reçoit une trame ou un paquet, elle ignore les adresses de Couche 2 ou 3 à des fins de basculement ou de routage, mais applique vos règles de politique NAT ou de sécurité avant de transmettre une trame ou un paquet autorisé du câble virtuel à la deuxième interface et à l'appareil réseau qui y est connecté.

N'utilisez pas de déploiement de câble virtuel pour les interfaces qui doivent prendre en charge le basculement, les tunnels VPN ou le routage, car elles nécessitent une adresse de Couche 2

 ©2024 Palo Alto Networks, Inc.

ou 3. Une interface de câble virtuel n'utilise pas de profil de gestion d'interface, qui contrôle des services comme HTTP et ping, et nécessite donc que l'interface ait une adresse IP.

Tous les pare-feu ont deux ports Ethernet (ports 1 et 2) préconfigurés en tant qu'interfaces de câble virtuel par défaut, et ces interfaces autorisent tout le trafic non étiqueté.

Si vous utilisez des étiquettes de groupe de sécurité (SGT) dans un réseau Cisco TrustSec, il est préférable de déployer des pare-feu en ligne, soit en couche 2, soit en mode câble virtuel. Les pare-feu en mode couche 2 ou câble virtuel peuvent inspecter et fournir une prévention contre les menaces pour le trafic ciblé.

Si vous ne prévoyez pas d'utiliser le câble virtuel préconfiguré, vous devez supprimer cette configuration pour l'empêcher d'interférer avec les autres paramètres que vous configurez sur votre pare-feu. Consultez Configuration de l'accès réseau pour les services externes.

- Paquets des couches 2 et 3 sur un câble virtuel
- Vitesses des ports des interfaces de câble virtuel
- LLDP sur un câble virtuel
- Interfaces regroupées pour un câble virtuel
- Prise en charge de la haute disponibilité par le câble virtuel
- Protection de zone pour une interface de câble virtuel
- Trafic étiqueté VLAN
- Sous-interfaces de câble virtuel
- Configuration des câbles virtuels

Paquets des couches 2 et 3 sur un câble virtuel

Une interface filaire virtuelle permettra aux paquets des couches 2 et 3 provenant des périphériques connectés de passer de manière transparente tant que les stratégies appliquées à la zone ou à l'interface autorisent le trafic. Les interfaces de fils virtuelles elles-mêmes ne participent pas au routage ou à la commutation.

Par exemple, le pare-feu ne décrémente pas le TTL dans un paquet traceroute passant par le lien virtuel car le lien est transparent et ne compte pas comme un saut. Les paquets tels que les unités de données de protocole (PDU) Opérations, Administration et Maintenance (OAM), par exemple, ne se terminent pas sur le pare-feu. Ainsi, le fil virtuel permet au pare-feu de maintenir une présence transparente agissant comme un lien direct, tout en fournissant des services de sécurité, de NAT et de QoS.

Pour que les unités de données de protocole de pont (BPDU) et les autres paquets de contrôle de couche 2 (généralement non balisés) passent à travers un fil virtuel et par défaut, les interfaces doivent être attachées à un objet fil virtuel qui autorise le trafic non marqué. Si le champ **Tag Allowed (Balise autorisée)** de l'objet fil virtuel est vide, le fil virtuel autorise le trafic non balisé. (Les règles de stratégie de sécurité ne s'appliquent pas aux paquets de couche 2).

Pour que les paquets de contrôle de routage (couche 3) passent à travers un fil virtuel, vous devez appliquer une règle de politique de sécurité qui autorise le passage du trafic. Par exemple, appliquez une règle de stratégie de sécurité qui autorise une application telle que BGP ou OSPF.

©2024 Palo Alto Networks, Inc.

Si vous voulez pouvoir appliquer des règles de politique de sécurité au trafic IPv6 qui arrive sur l'interface de câble virtuel, activez la mise en place d'un pare-feu IPv6. Sinon, le trafic IPv6 est transmis de manière transparente sur le réseau.

Si vous activez le filtrage pare-feu multidiffusion pour un objet câblé virtuel et que vous l'appliquez à une interface câblée virtuelle, le pare-feu inspecte le trafic multidiffusion et le transmet ou non, en fonction des règles de politique de sécurité. Si vous n'activez pas le pare-feu multidiffusion, le pare-feu transfère simplement le trafic multidiffusion de manière transparente.

La fragmentation sur un fil virtuel se produit de la même manière que dans les autres modes de déploiement d'interface.

Vitesses des ports des interfaces de câble virtuel

Différents types de pare-feu fournissent divers types de ports en cuivre et en fibre optique, qui fonctionnent à des vitesses différentes. Un câble virtuel peut relier deux ports Ethernet de type analogue (deux interfaces en cuivre ou deux interfaces en fibre optique), ou relier un port en cuivre à un port en fibre optique. Par défaut, la **Link Speed (Vitesse de liaison)** des ports en cuivre sur le pare-feu est définie sur **auto (automatique)**, ce qui signifie que le pare-feu négocie automatiquement la vitesse et le mode de transmission (**Link Duplex (Duplex de la liaison)**). Lors de la Configuration des câbles virtuels, vous pouvez également sélectionner une **Link Speed (Vitesse de liaison)** et un **Link Duplex (Duplex de la liaison)** particuliers, mais les valeurs de ces paramètres doivent être identiques pour les deux ports d'un câble virtuel unique.

LLDP sur un câble virtuel

Les interfaces filaires virtuelles peuvent utiliser LLDP pour découvrir les périphériques voisins et leurs capacités, et LLDP permet aux périphériques voisins de détecter la présence du pare-feu dans le réseau. Le LLDP facilite le dépannage, en particulier sur un fil virtuel, où le pare-feu ne serait généralement pas détecté par un ping ou un traceroute traversant le fil virtuel. LLDP permet aux autres périphériques de détecter le pare-feu sur le réseau. Sans LLDP, il est pratiquement impossible pour les systèmes de gestion de réseau de détecter la présence d'un pare-feu à travers le lien virtuel.

Interfaces regroupées pour un câble virtuel

Vous pouvez effectuez la configuration d'un groupe d'interfaces agrégées d'interfaces de câble virtuel, mais les câbles virtuels n'utilisent pas le protocole LACP. Si vous configurez le protocole LACP sur les périphériques qui relient le pare-feu à d'autres réseaux, le câble virtuel passe alors des paquets LACP de manière transparente sans effectuer de fonctions LACP.

Sur un câble virtuel, le pare-feu Palo Alto Networks peut transmettre le trafic Cisco LACP uniquement lorsque les liens ne sont pas regroupés sur le pare-feu. Sur un câble virtuel, si les liens sont regroupés, le pare-feu pourrait alors transférer les paquets vers le mauvais port dans l'Ethernet agrégé, ce qui empêcherait le LACP de fonctionner entre les pairs.

Pour que les groupes d'interfaces agrégées fonctionnent correctement, assurez-vous que toutes les liaisons appartenant au même groupe LACP qui se trouve du même côté du câble virtuel sont affectées à la même zone.

©2024 Palo Alto Networks, Inc.

Prise en charge de la haute disponibilité par le câble virtuel

Si vous configurez le pare-feu pour effectuer la surveillance des chemins pour la Haute disponibilité à l'aide d'un groupe de chemins de câble virtuel, le pare-feu tente de résoudre ARP pour l'adresse IP de destination configurée en envoyant des paquets ARP à partir des deux interfaces de câble virtuel. L'adresse IP de destination que vous surveillez doit se trouver sur le même sous-réseau qu'un des appareils entourant le câble virtuel.

Les interfaces de câble virtuel prennent en charge à la fois la HA active/passive et la HA active/active. Pour un déploiement de HA active/active, les paquets analysés doivent être renvoyés au pare-feu récepteur afin de protéger le chemin de transfert. Ainsi, si un pare-feu reçoit un paquet qui appartient à la session du pare-feu HA homologue, il envoie le paquet via la liaison HA3 à l'homologue.

Vous pouvez configurer le pare-feu passif dans une paire HA pour autoriser les appareils homologues de chaque côté du pare-feu à pré-négocier LLDP et LACP sur un câble virtuel avant qu'un basculement HA survienne. Une telle configuration pour la Pré-négociation LACP et LLDP pour la HA active/passive accélère les basculements HA.

Protection de zone pour une interface de câble virtuel

Vous pouvez appliquer la protection de zone à une interface de câble virtuel. Cependant, étant donné que les interfaces de câble virtuel n'effectuent pas de routage, vous ne pouvez pas appliquer la Packet Based Attack Protection (Protection contre les attaques basées sur les paquets) à des paquets venant d'une adresse IP usurpée, et vous ne pouvez pas non plus supprimer les paquets d'erreurs de type TTL ICMP expiré ou Fragment ICMP requis.

Par défaut, une interface de câble virtuel transmet tout le trafic non IP qu'elle reçoit. Cependant, vous pouvez appliquer un profil de protection de zone avec la Protection de protocole pour bloquer ou autoriser certains paquets de protocoles non IP entre des zones de sécurité sur un câble virtuel.

Trafic étiqueté VLAN

Les interfaces de câble virtuel autorisent le trafic non étiqueté par défaut. Vous pouvez toutefois utiliser un câble virtuel pour connecter deux interfaces et configurer chacune d'entre elles afin de bloquer ou d'autoriser du trafic en fonction des étiquettes Virtual LAN (LAN virtuel ; VLAN). L'étiquette VLAN « 0 » indique du trafic non étiqueté.

Vous pouvez également créer plusieurs sous-interfaces, les ajouter dans différentes zones, puis classer le trafic en fonction d'une étiquette VLAN, ou d'une combinaison d'une étiquette VLAN et de classificateurs IP (adresse, plage ou sous-réseau), afin d'appliquer un contrôle de politique granulaire à des étiquettes VLAN spécifiques ou à des étiquettes VLAN provenant d'une adresse IP, d'une plage ou d'un sous-réseau source spécifique.

Sous-interfaces de câble virtuel

Les déploiements de câble virtuel peuvent utiliser des sous-interfaces de câble virtuel pour séparer le trafic en zones. Les sous-interfaces de câble virtuel offrent plus de flexibilité via l'application de politiques diverses lorsque vous devez gérer du trafic provenant de plusieurs réseaux clients. Les sous-interfaces vous permettent de séparer et de classer le trafic dans

 ©2024 Palo Alto Networks, Inc.

différentes zones (celles-ci peuvent appartenir à des systèmes virtuels distincts, si nécessaire) à l'aide des critères suivants :

- **Étiquettes VLAN** : l'exemple dans Déploiement de câble virtuel avec des sous-interfaces (étiquettes VLAN uniquement) montre un fournisseur de services Internet qui utilise des sous-interfaces de câble virtuel pour séparer le trafic pour deux clients différents.
- **Étiquettes VLAN avec des classificateurs IP (adresse, plage ou sous-réseau)** : l'exemple suivant montre un ISP avec deux systèmes virtuels séparés sur un pare-feu qui gère le trafic provenant de deux clients différents. Sur chaque système virtuel, l'exemple montre comment les sous-interfaces de câble virtuel avec des étiquettes VLAN et des classificateurs IP sont utilisées pour classer le trafic dans des zones distinctes et pour appliquer la politique appropriée aux clients de chaque réseau.

Flux de travail d'une sous-interface de câble virtuel

- Configurez deux interfaces Ethernet en tant que câble virtuel type, puis affectez un câble virtuel à ces interfaces.

- Créez des sous-interfaces sur le câble virtuel parent afin de séparer le trafic du ClientA et du ClientB. Vérifiez que les étiquettes VLAN définies sur chaque paire de sous-interfaces configurées en tant que câble(s) virtuel(s) sont identiques. Ceci est essentiel car un câble virtuel ne commute pas les étiquettes VLAN.

- Créez de nouvelles sous-interfaces et définissez des classificateurs IP. Cette tâche est facultative et requise uniquement si vous souhaitez ajouter d'autres sous-interfaces avec des classificateurs IP afin de gérer de manière plus approfondie le trafic d'un client sur la base d'une combinaison d'étiquettes VLAN et d'une adresse IP, d'une plage ou d'un sous-réseau source spécifique.

Vous pouvez aussi utiliser des classificateurs d'IP pour gérer le trafic non balisé. Pour cela, vous devez créer une sous-interface avec l'étiquette VLAN « 0 » et définir la ou les sous-interfaces avec des classificateurs IP pour gérer le trafic non étiqueté à l'aide des classificateurs IP.

La classification des adresses IP peut uniquement être utilisée sur les sous-interfaces associées à un côté du câble virtuel. Les sous-interfaces définies sur le côté correspondant du câble virtuel doivent utiliser la même étiquette VLAN, mais ne doivent pas inclure de classificateur IP.

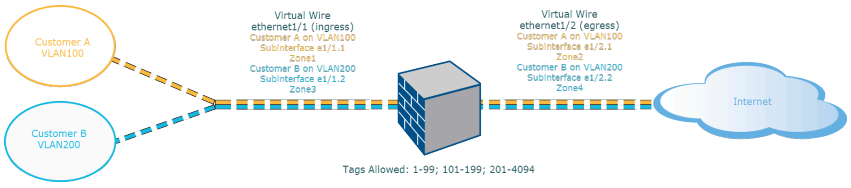


Figure 1: Déploiement de câble virtuel avec des sous-interfaces (étiquettes VLAN uniquement)

Déploiement de câble virtuel avec des sous-interfaces (étiquettes VLAN uniquement) montre que le ClientA et le ClientB sont connectés au pare-feu via une interface physique, ethernet1/1, configurée en tant que câble virtuel ; celle-ci sert d'interface d'entrée. Une deuxième interface

 ©2024 Palo Alto Networks, Inc.

physique, ethernet1/2, fait également partie du câble virtuel ; elle sert d'interface de sortie permettant d'accéder à Internet.

Pour le ClientA, vous disposez également des sous-interfaces ethernet1/1.1 (entrée) et ethernet1/2.1 (sortie). Pour le ClientB, vous disposez des sous-interfaces ethernet1/1.2 (entrée) et ethernet1/2.2 (sortie). Au moment de la configuration des sous-interfaces, vous devez affecter l'étiquette VLAN et la zone appropriées afin d'appliquer des politiques à chaque client. Dans cet exemple, les politiques du ClientA sont créées entre la Zone1 et la Zone2 et les politiques du ClientB sont créées entre la Zone3 et la Zone4.

Lorsque du trafic du ClientA ou ClientB entre dans le pare-feu, l'étiquette VLAN du paquet entrant est comparée en premier lieu avec l'étiquette VLAN définie dans les sous-interfaces d'entrée. Dans cet exemple, une sous-interface unique correspond à l'étiquette VLAN pour un paquet entrant, cette sous-interface est donc sélectionnée. Les politiques définies pour la zone sont évaluées et appliquées avant que le paquet ne sorte de la sous-interface correspondante.

*La même étiquette VLAN ne doit pas être définie sur l'interface de câble virtuel parent et la sous-interface. Vérifiez que les étiquettes VLAN définies dans la liste Étiquettes autorisées de l'interface de câble virtuel parent (**Network (Réseau)** > **Virtual Wires (Câbles virtuels)**) ne sont pas incluses sur une sous-interface.*

Déploiement de câble virtuel avec des sous-interfaces (étiquettes VLAN et classificateurs IP) montre que le ClientA et le ClientB sont connectés à un pare-feu physique qui comprend deux systèmes virtuels (vsys) en plus du système virtuel par défaut (vsys1). Chaque système virtuel est un pare-feu virtuel indépendant qui est géré séparément pour chaque client. Chaque vsys comporte des interfaces/sous-interfaces associées et des zones de sécurité qui sont gérées de manière indépendante.

 ©2024 Palo Alto Networks, Inc.

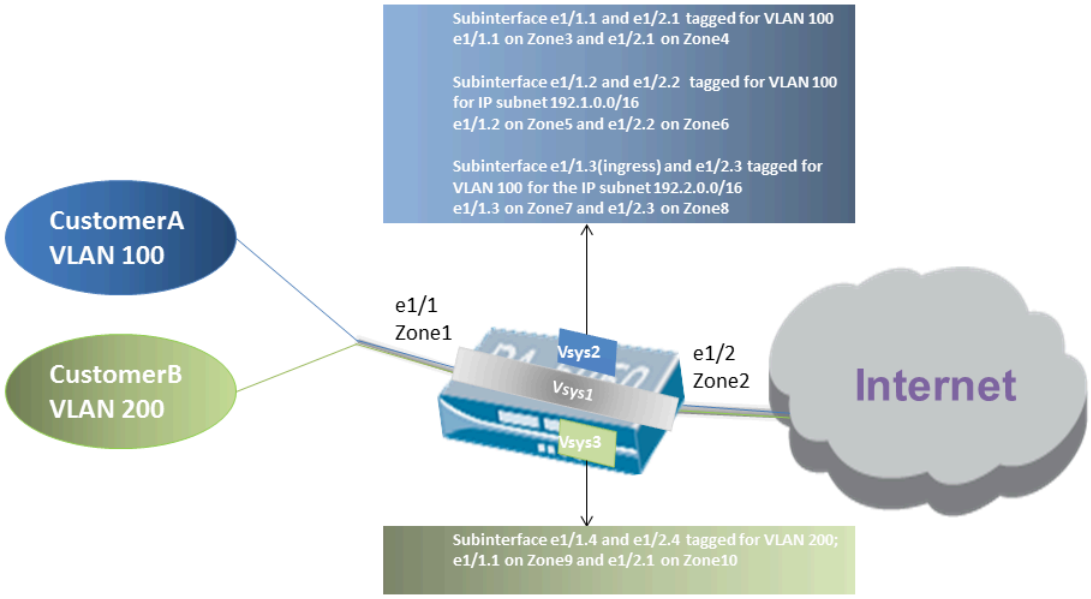


Figure 2: Déploiement de câble virtuel avec des sous-interfaces (étiquettes VLAN et classificateurs IP)

Vsys1 est configuré pour utiliser les interfaces physiques ethernet1/1 et ethernet1/2 en tant que câble virtuel ; ethernet1/1 étant l'interface d'entrée et ethernet1/2 l'interface de sortie qui permet d'accéder à Internet. Ce câble virtuel est configuré pour accepter l'ensemble du trafic étiqueté et non étiqueté à l'exception des étiquettes VLAN 100 et 200 qui sont affectées aux sous-interfaces.

Le ClientA est géré sur vsys2 et le ClientB sur vsys3. Sur vsys2 et vsys3, les sous-interfaces de câble virtuel suivantes sont créées avec les étiquettes VLAN et les zones appropriées pour appliquer des mesures de politique.

Client	Vsys	Sous-interfaces de câble virtuel	Employé	Étiquette VLAN	Classificateur IP
A	2	e1/1.1 (entrée) e1/2.1 (sortie)	Zone3 Zone4	100 100	None
	2	e1/1.2 (entrée) e1/2.2 (sortie)	Zone5 Zone6	100 100	Sous-réseau IP 192.1.0.0/16
	2	e1/1.3 (entrée)	Zone7	100	Sous-réseau IP

©2024 Palo Alto Networks, Inc.

Client	Vsys	Sous-interfaces de câble virtuel	Employé	Étiquette VLAN	Classificateur IP
		e1/2.3 (sortie)	Zone8	100	192.2.0.0/16
B	3	e1/1.4 (entrée) e1/2.4 (sortie)	Zone9 Zone10	200 200	None

Lorsque du trafic du ClientA ou ClientB entre dans le pare-feu, l'étiquette VLAN du paquet entrant est comparée en premier lieu avec l'étiquette VLAN définie dans les sous-interfaces d'entrée. Dans ce cas, pour le ClientA, plusieurs sous-interfaces utilisent la même étiquette VLAN. Le pare-feu limite donc tout d'abord la classification à une sous-interface en fonction de l'adresse IP source du paquet. Les politiques définies pour la zone sont évaluées et appliquées avant que le paquet ne sorte de la sous-interface correspondante.

Pour le trafic de retour, le pare-feu compare l'adresse IP de destination définie dans le classificateur IP de la sous-interface orientée client et sélectionne le câble virtuel approprié pour acheminer le trafic via la sous-interface adéquate.

*La même étiquette VLAN ne doit pas être définie sur l'interface de câble virtuel parent et la sous-interface. Vérifiez que les étiquettes VLAN définies dans la liste Étiquettes autorisées de l'interface de câble virtuel parent (**Network (Réseau)** > **Virtual Wires (Câbles virtuels)**) ne sont pas incluses sur une sous-interface.*

Configuration des câbles virtuels

La tâche suivante indique comment configurer deux Interfaces de câble virtuel (Ethernet 1/3 et Ethernet 1/4 dans le présent exemple) pour créer un câble virtuel. Les deux interfaces doivent posséder la même **Link Speed (Vitesse de liaison)** et mode de transmission (**Link Duplex (Duplex de la liaison)**). Par exemple, un port cuivre en duplex intégral de 1 000 Mbits/s correspond à un port fibre optique de 1 Gbit/s.

STEP 1 | Créez la première interface de câble virtuel.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)**, puis sélectionnez une interface que vous avez câblée (**ethernet1/3** dans le présent exemple).
2. Définissez le **Interface Type (Type d'interface)** sur **Virtual Wire (Câble virtuel)**.

STEP 2 | Associez l'interface à un objet de câble virtuel.

1. Tandis que vous êtes encore sur la même interface Ethernet, à l'onglet **Config (Configuration)**, sélectionnez **Virtual Wire (Câble virtuel)**, puis cliquez sur **New Virtual Wire (Nouveau câble virtuel)**.
2. Donnez un **Name (Nom)** au câble virtuel.
3. Sous **Interface1 (Interface1)**, sélectionnez l'interface que vous venez de configurer (**ethernet1/3 (ethernet1/3)**). (Seules les interfaces configurées en tant qu'interfaces de câble virtuel apparaissent dans la liste.)
4. Sous **Tag Allowed (Étiquettes autorisées)**, saisissez **0 (0)** pour indiquer que le trafic non étiqueté (comme le trafic BPDUs et autre trafic de contrôle de couche 2) est autorisé. L'absence d'étiquette suppose qu'il s'agit de l'étiquette 0. Entrez des étiquettes

©2024 Palo Alto Networks, Inc.

autorisées supplémentaires (nombre entier) ou des plages d'étiquettes, séparées par des virgules (par défaut : 0 ; plage comprise entre 0 et 4 094).

5. Sélectionnez **Multicast Firewalling (Mise en place d'un pare-feu multicast)** si vous voulez appliquer des règles de politique de sécurité au trafic multicast traversant le câble virtuel. Autrement, le trafic multicast est transféré de manière transparente dans le câble virtuel.
6. Sélectionnez **Link State Pass Through (Transmission de l'état des liaisons)** pour que le pare-feu puisse fonctionner de manière transparente. Lorsque le pare-feu détecte qu'une liaison du câble virtuel est inactive, il rend l'autre interface de la paire de câbles virtuels indisponible. Ainsi, les périphériques qui se trouvent des deux côtés du pare-feu constatent un état des liaisons uniforme, comme s'il n'y avait aucun pare-feu entre eux. Si vous ne sélectionnez pas cette option, l'état des liaisons n'est pas propagé dans le câble virtuel.
7. Cliquez sur **OK (OK)** pour enregistrer l'objet de câble virtuel.

STEP 3 | Déterminez la vitesse de liaison de l'interface de câble virtuel.

1. Tandis que vous êtes encore sur la même interface Ethernet, sélectionnez **Advanced (Avancé)** et notez ou modifiez la **Link Speed (Vitesse de liaison)**. Le type de port détermine les paramètres de vitesse qui sont offerts dans la liste. Par défaut, la négociation de la vitesse de liaisons des ports en cuivre est définie sur **auto (auto)**. Les deux interfaces de câble virtuel doivent posséder la même vitesse de liaison.
2. Cliquez sur **OK (OK)** pour enregistrer l'interface ethernet.

STEP 4 | Configurez la deuxième interface de câble virtuel (**ethernet1/4** dans le présent exemple) en répétant les étapes précédentes.

Lorsque vous sélectionnez l'objet de **Virtual Wire (Câble virtuel)** que vous avez créé, le pare-feu ajoute automatiquement la deuxième interface de câble virtuel en tant qu'**Interface2**.

STEP 5 | Créez une zone de sécurité distincte pour chacune des interfaces de câble virtuel.

1. Sélectionnez **Network (Réseau)** > **Zones (Zones)**, puis **Add (Ajouter)** pour ajouter une zone.
2. Saisissez le **Name (Nom)** de la zone, (tel que **`internet`**).
3. Pour **Location (Emplacement)**, sélectionnez le système virtuel auquel la zone s'applique.
4. Sous **Type (Type)**, sélectionnez **Virtual Cable (Câble virtuel)**.
5. **Add (Ajoutez)** l'**Interface** qui appartient à la zone.
6. Cliquez sur **OK**.

STEP 6 | (Facultatif) Créez des règles de politique de sécurité pour autoriser le trafic de couche 3 à transiter.

Pour autoriser le trafic de couche 3 à traverser le câble virtuel, procédez à la création d'une règle de politique de sécurité pour autoriser le trafic à passer de la zone utilisateur à la zone Internet et une autre pour autoriser le trafic à passer de la zone Interner à la zone utilisateur, en sélectionnant les applications que vous souhaitez autoriser, comme BGP ou OSPF.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | (Facultatif) Activez la mise en place d'un pare-feu IPv6.

Si vous voulez pouvoir appliquer des règles de politique de sécurité au trafic IPv6 qui arrive sur l'interface de câble virtuel, activez la mise en place d'un pare-feu IPv6. Sinon, le trafic IPv6 est transféré de manière transparente.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les Session Settings (Paramètres de session).
2. Sélectionnez **Enable IPv6 Firewalling (Activer le pare-feu IPv6)**.
3. Cliquez sur **OK**.

STEP 8 | ((Supported firewalls onlyPare-feu pris en charge uniquement)) Si l'interface correspond à un port PoE (Power over Ethernet) sur le pare-feu, vous pouvez éventuellement configure PoE (configurer PoE).

STEP 9 | **Commit (Validez)** vos modifications.

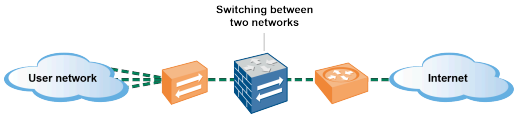
STEP 10 | (Facultatif) Configurez un profil LLDP et appliquez-le aux interfaces de câble virtuel (reportez-vous à la section Configuration de LLDP).

STEP 11 | (Optional (Facultatif)) Appliquez un contrôle des protocoles non-IP sur les zones du câble virtuel (reportez-vous à la section Configure Protocol Protection (Configuration de la protection de protocole)). Sinon, tout le trafic non-IP est transféré par le câble virtuel.

 ©2024 Palo Alto Networks, Inc.

Interfaces de Couche 2

Dans un déploiement de Couche 2, le pare-feu assure un basculement entre deux ou plusieurs réseaux. Les périphériques sont connectés à un segment de couche 2; le pare-feu transmet les trames au port approprié, qui est associé à l'adresse MAC identifiée dans la trame. Configurez une interface de couche 2 lorsque la commutation est requise.



Si vous utilisez des étiquettes de groupe de sécurité (SGT) dans un réseau Cisco TrustSec, il est préférable de déployer des pare-feu en ligne, soit en couche 2, soit en mode câble virtuel. Les pare-feu en mode couche 2 ou câble virtuel peuvent inspecter et fournir une prévention contre les menaces pour le trafic ciblé.

Les rubriques suivantes décrivent les différents types d'interfaces de couche 2 que vous pouvez configurer pour chaque type de déploiement dont vous avez besoin, y compris des détails sur l'utilisation de réseaux locaux virtuels (VLANs) pour la séparation du trafic et des politiques entre groupes. Une autre rubrique décrit la façon dont le pare-feu réécrit le du Port VLAN ID (ID du VLAN du port ; PVID) entrant indiqué en Bridge Protocol Data Unit (unité de données de protocole de pont ; BPDU) d'un per-VLAN spanning tree (arbre recouvrant pour chaque VLAN ; PVST+) ou d'un Rapid PVST +.

- Interfaces de couche 2 sans réseau local virtuel (VLAN)
- Interfaces de couche 2 avec les réseaux locaux virtuels (VLANs)
- Configuration d'une interface de couche 2
- Configuration d'une interface de couche 2, une sous-interface et un réseau local virtuel
- Gestion de la ré-écriture de paquets Per-VLAN Spanning Tree (PVST+) BPDU

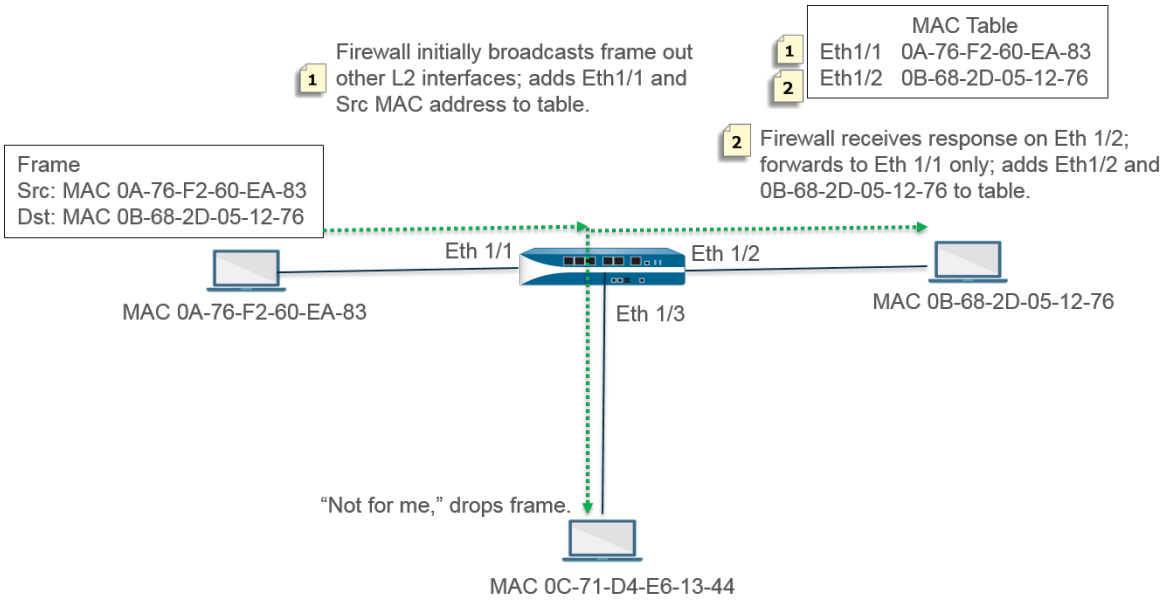
Interfaces de couche 2 sans réseau local virtuel (VLAN)

Configurez une interface de couche 2 sur le pare-feu afin qu'il puisse agir comme un commutateur dans votre réseau de couche 2 (pas à la limite du réseau). Les hôtes de couche 2 sont probablement géographiquement proches les uns des autres et appartiennent à un seul domaine de diffusion. Le pare-feu assure la sécurité entre les hôtes de couche 2 lorsque vous affectez les interfaces aux zones de sécurité et que vous appliquez des règles de sécurité aux zones.

Les hôtes communiquent avec le pare-feu et entre eux au niveau 2 du modèle OSI en échangeant des trames. Une trame contient un en-tête Ethernet qui comprend une adresse de contrôle d'accès au support (MAC) source et de destination, qui est une adresse matérielle physique. Les adresses MAC sont des nombres hexadécimaux 48 bits formatés sous la forme de six octets séparés par un deux-points ou un tiret (par exemple, 00-85-7E-46-F1-B2).

La figure suivante comporte un pare-feu avec trois interfaces de couche 2 qui se connectent chacune à un hôte de couche 2 dans un mappage un-à-un.

©2024 Palo Alto Networks, Inc.



Le pare-feu commence par une table MAC vide. Lorsque l'hôte avec l'adresse source 0A-76-F2-60-EA-83 envoie une trame au pare-feu, le pare-feu n'a pas l'adresse de destination 0B-68-2D-05-12-76 dans sa table MAC, donc il ne sait pas à quelle interface transmettre la trame ; il diffuse la trame à toutes ses interfaces de couche 2. Le pare-feu place l'adresse source 0A-76-F2-60-EA-83 et Eth1 / 1 associée dans sa table MAC.

L'hôte à l'adresse 0C-71-D4-E6-13-44 reçoit la diffusion, mais l'adresse MAC de destination n'est pas sa propre adresse MAC, donc il supprime la trame.

L'interface de réception Ethernet 1/2 transmet la trame à son hôte. Lorsque l'hôte 0B-68-2D-05-12-76 répond, il utilise l'adresse de destination 0A-76-F2-60-EA-83, et le pare-feu ajoute Ethernet 1/2 à sa table MAC comme l'interface pour atteindre 0B -68-2D-05-12-76.

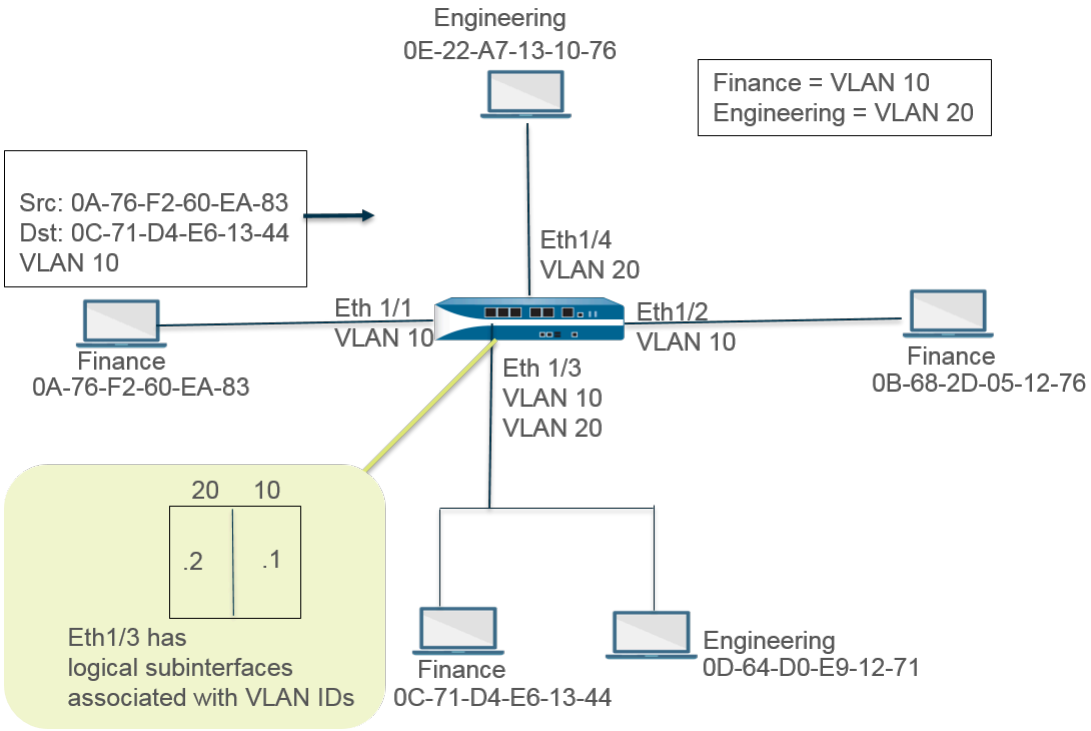
Interfaces de couche 2 avec les réseaux locaux virtuels (VLANs)

Lorsque votre organisation souhaite diviser un réseau local (LAN) en des réseaux locaux virtuels (VLANs) séparés pour garder séparés le trafic et les politiques des différents départements, vous pouvez logiquement regrouper les hôtes de couche 2 en réseaux locaux virtuels et diviser ainsi un segment de réseau de couche 2 en domaines de diffusion. Par exemple, vous pouvez créer des VLAN pour les départements Finance et Ingénierie. Pour ce faire, configurez une interface de couche 2, une sous-interface et un réseau local virtuel.

Le pare-feu agit comme un commutateur pour transférer une trame avec un en-tête Ethernet contenant un VLAN ID, et l'interface de destination doit avoir une sous-interface avec ce VLAN ID pour recevoir cette trame et la transmettre à l'hôte. Vous configurez une interface de couche 2 sur le pare-feu et configurez une ou plusieurs sous-interfaces logiques pour l'interface, chacune avec une balise VLAN (ID).

Dans la figure suivante, le pare-feu dispose de quatre interfaces de couche 2 qui se connectent aux hôtes de couche 2 appartenant à différents départements d'une organisation. L'interface Ethernet 1/3 est configurée avec sous-interface .1 (étiquetée avec VLAN 10) et sous-interface .2 (étiquetée avec VLAN 20), donc il y a deux domaines de diffusion sur ce segment. Les hôtes du VLAN 10 appartiennent à Finance; les hôtes dans le VLAN 20 appartiennent à l'ingénierie.

 ©2024 Palo Alto Networks, Inc.



Dans cet exemple, l'hôte à l'adresse MAC 0A-76-F2-60-EA-83 envoie une trame avec l'ID de VLAN 10 au pare-feu, que le pare-feu diffuse vers ses autres interfaces L2. L'interface Ethernet 1/3 accepte la trame car elle est connectée à l'hôte avec la destination 0C-71-D4-E6-13-44 et sa sous-interface .1 est assignée au VLAN 10. L'interface Ethernet 1/3 transmet la trame à l'hôte Finance.

Configuration d'une interface de couche 2

Configurez des interfaces de couche 2 sans VLAN lorsque vous souhaitez un basculement de couche 2 et que vous n'avez pas besoin de séparer le trafic entre les VLAN.

STEP 1 | Configurez une interface de couche 2.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** et choisissez une interface. Le **Interface Name (Nom de l'interface)** est fixe, comme ethernet1/1.
2. Sous **Interface Type (Type d'interface)**, sélectionnez **Layer2 (Couche 2)**.
3. Sélectionnez l'onglet **Config (Configuration)**, puis affectez l'interface à une **Security Zone (Zone de sécurité)** ou créez une **New Zone (Nouvelle zone)**.
4. Sur le pare-feu, configurez des interfaces de couche 2 supplémentaires qui se connectent à d'autres hôtes de couche 2.

STEP 2 | Validez.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

Configuration d'une interface de couche 2, une sous-interface et un réseau local virtuel

Configurez des interfaces de couche 2 sans VLAN lorsque vous souhaitez un basculement de couche 2 et une séparation du trafic entre les VLAN. Vous pouvez éventuellement contrôler les protocoles non-IP entre les zones de sécurité d'une interface de Couche 2 ou entre les interfaces qui se trouvent au sein d'une seule zone d'un VLAN de couche 2.

STEP 1 | Configurez une interface et une sous-interface de Couche 2 et affectez un ID de VLAN.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** et choisissez une interface. Le **Interface Name (Nom de l'interface)** est fixe, comme ethernet1/1.
2. Sous **Interface Type (Type d'interface)**, sélectionnez **Layer2 (Couche 2)**.
3. Sélectionnez l'onglet **Config (Configuration)**.
4. Sous **VLAN (VLAN)**, laissez le paramètre défini sur **None (Aucun)**.
5. Affectez l'interface à une **Security Zone (Zone de sécurité)** ou créez une **New Zone (Nouvelle zone)**.
6. Cliquez sur **OK**.
7. L'interface ethernet est surlignée ; cliquez sur **Add Subinterface (Ajouter une sous-interface)**.
8. Le **Interface Name (Nom d'interface)** demeure fixe. Après le point, saisissez le numéro de la sous-interface selon une plage comprise entre 1 et 9 999.
9. Saisissez une ID de **Tag (Étiquette)** VLAN selon une plage comprise entre 1 et 4 094.
10. Affectez la sous-interface à une **Security Zone (Zone de sécurité)**.
11. Cliquez sur **OK**.

STEP 2 | Validez.

Cliquez sur **Commit (Valider)**.

STEP 3 | (Facultatif) Appliquez un profil de protection de zone avec protection de protocole pour contrôler les paquets de protocole non IP entre des zones de Couche 2 (ou entre des interfaces qui se trouvent dans une zone de Couche 2).

Configuration de la protection de protocole.

Gestion de la ré-écriture de paquets Per-VLAN Spanning Tree (PVST+) BPDU

Dans un déploiement de couche 2, le pare-feu utilise le numéro du Port VLAN ID (ID du VLAN du port ; PVID) entrant indiqué en Bridge Protocol Data Unit (unité de données de protocole de pont ; BPDU) d'un per-VLAN spanning tree (arbre recouvrant pour chaque VLAN ; PVST+) ou d'un Rapid PVST +, et le réécrit de sorte à le convertir au bon numéro ID du VLAN sortant avant de l'acheminer. Le comportement par défaut depuis PAN-OS 7.1 permet au pare-deu de correctement étiqueter les trames propriétaires Cisco PVST+ et Rapid PVST+ entre les switchs Cisco dans les VLANs des deux côtés du pare-feu afin que la détection de boucle Spanning Tree en utilisant CISCO PVST+ et Rapid PVST+ puisse fonctionner correctement Le pare-feu

 ©2024 Palo Alto Networks, Inc.

ne participe pas au processus d'élection Spanning Tree (STP) et il n'y a pas de changement de comportement pour d'autres types de Spanning Tree

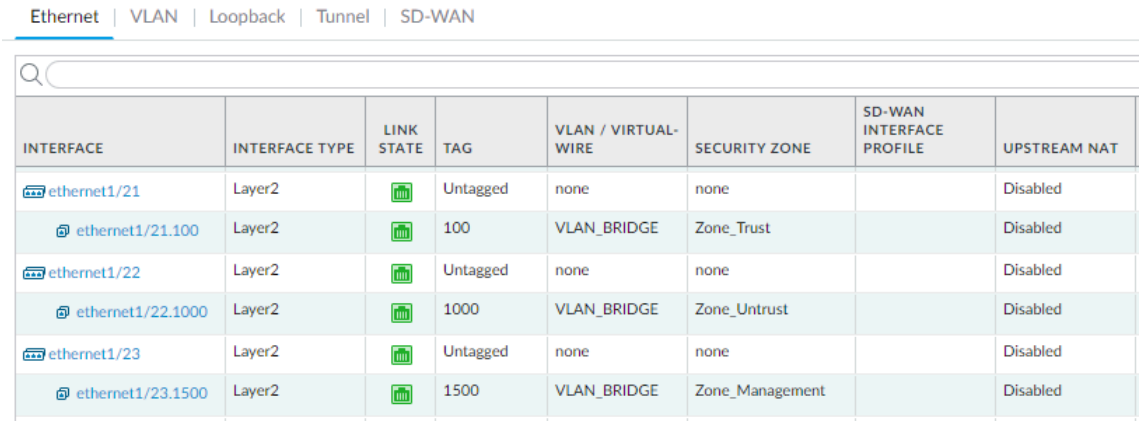
La fonction de protection contre les boucles doit être activée sur un commutateur Cisco pour que la réécriture des BPDU PVST+ ou Rapid PVST+ fonctionne correctement sur le pare-feu.

Le pare-feu ne réécrit les BPDU que sur les interfaces Ethernet de couche 2 et les interfaces Aggregated Ethernet (Ethernet agrégée ; AE). Le pare-feu support un intervalle PVID entre 1 et 4 094 avec un VLAN natif de 1 pour être compatible avec l'implémentation du VLAN natif de Cisco

Pour supporter la fonctionnalité de réécriture PVST+ BPDU, PAN-OS supporte le concept de VLAN natif PVST+ Les trames envoyées et reçues du VLAN natif sont étiquetées avec un PVID égal au VLAN natif Tous les switchs et les pare-feux dans le même déploiement Niveau 2 doivent avoir le même VLAN natif pour que PVST+ fonctionne correctement Bien que le VLAN natif de Cisco soit le VLAN 1, l'ID de VLAN pourrait être un nombre différent de 1

Par exemple, le pare-feu est configuré avec un objet VLAN (appelé VLAN_BRIDGE), qui décrit les interfaces et sous-interfaces qui appartiennent au switch ou au domaine de broadcast Dans cet exemple, le VLAN inclut trois sous-interfaces: ethernet1/21.100 étiqueté avec 100, ethernet1/22.1000 étiqueté avec 1000 et ethernet1/23.1500 étiqueté avec 1500

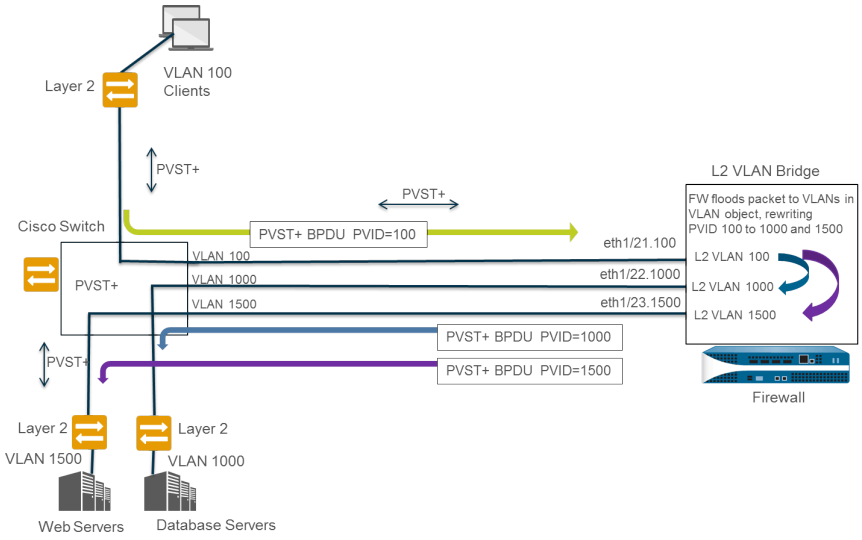
Les sous-interfaces qui appartiennent à VLAN_BRIDGE ressemblent à cela :



INTERFACE	INTERFACE TYPE	LINK STATE	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT
ethernet1/21	Layer2		Untagged	none	none		Disabled
ethernet1/21.100	Layer2		100	VLAN_BRIDGE	Zone_Trust		Disabled
ethernet1/22	Layer2		Untagged	none	none		Disabled
ethernet1/22.1000	Layer2		1000	VLAN_BRIDGE	Zone_Untrust		Disabled
ethernet1/23	Layer2		Untagged	none	none		Disabled
ethernet1/23.1500	Layer2		1500	VLAN_BRIDGE	Zone_Management		Disabled

La séquence utilisée par le pare-feu pour réécrire automatiquement les BPDU PVST+ est présentée dans le graphique ci-dessous avec les explications :

©2024 Palo Alto Networks, Inc.



1. Le port du switch Cisco appartement au VLAN 100 envoie un PBPDU PVST+ -- avec le PVID et l'étiquette 802.1Q de VLAN fixé à 100 -- au pare-feu
2. les interfaces et sous-interfaces du pare-feu sont configurées comme des interfaces de niveau 2 La sous-interface d'entrée du pare-feu est étiqueté avec le VLAN 100, ce qui correspond au PVID et étiquette de VLAN du BPDU entrant, donc le pare-feu accepte le BPDU Le pare-feu inonde le BPDU PVST+ aux autres interfaces appartement au même objet VLAN (dans cet exemple, ethernet1/22.1000 et ethernet1/23.1500) Si les étiquettes VLAN ne correspondent pas, le pare-feu rejette le BPDU
3. Quand le pare-feu inonde le BPDU vers les autres interfaces (appartement au même objet VLAN), le pare-feu réécrit le PVID et toute étiquettes VLAN 802.1Q pour correspondre à l'étiquette de VLAN de l'interface de sortie Dans cet exemple, le pare-feu réécrit le PVID BPDU de 100 à 1000 pour une sous-interface et de 100 à 1500 pour la seconde sous-interface lorsque le BPDU traverse le pont de couche 2 du pare-feu.
4. Chaque switch Cisco reçoit le PVID correct et l'étiquette VLAN du BPDU entrant, et traite le paquet PVST+ pour détecter d'éventuelles boucles réseau

La commande CLI suivante permet de gérer les BPDU PVST+ et Rapid PVST+

- Désactive globalement ou ré-active la réécriture BPDU PVST+ et Rapid PVST)+ du PVID (par défaut, activé)

  ```
  set session rewrite-pvst-pvid <yes|no>
  ```

- Détermine l'ID du VLAN natif pour le pare-feu (intervalle entre 1 et 4094; défaut 1)

  Si l'ID du VLAN natif de votre switch est différent de 1, vous devez fixer l'ID du VLAN natif sur le pare-feu avec la même valeur, autrement, le pare-feu rejettera les paquets avec cet ID de VLAN Cela s'applique aux interfaces trunkées et non trunkées

  ```
  set session pvst-native-vlan-id <vid>
  ```

 ©2024 Palo Alto Networks, Inc.

- Rejette tous les paquets de STP BPDU

  `set session drop-stp-packet <yes|no>`

  Raisons pour lesquelles vous souhaiteriez rejeter les tous les paquets de STP BPDU:

  - S'il n'y a qu'un seul switch de chaque côté du pare-feu et aucune autre connexion entre les switchs qui pourrait causer une boucle, le STP n'est pas requis et peut être désactivé sur le switch ou rejeté par le pare-feu
  - Si un switch sature des BPDU par inadvertance, vous pouvez stopper les paquets STP au niveau du pare-feu en stoppant le flood BPDU

- Vérifiez si la ré-écriture des BPDU PVST+ est activé, visualisez l'ID du VLAN natif PVST, et déterminez si le pare-feu rejette tous les paquets STP BPDU

  `show vlan all`

```
pvst+ tag rewrite: disabled
pvst native vlan id:     5
drop stp:                disabled
total vlans shown:       1
name     interface           virtual interface
bridge   ethernet1/1
         ethernet1/2
         ethernet1/1.1
         ethernet1/2.1
```

- Diagnostiquez les erreurs PVST+ BPDUs

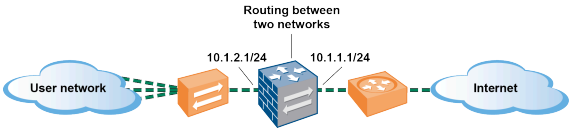
  `show counter global`

  Examinez le compteur `flow_pvid_inconsistent`, qui compte le nombre de fois où une étiquette 802.1Q et les champs PVID d'un paquet PVST+ BPDU ne correspondent pas

 ©2024 Palo Alto Networks, Inc.

Interfaces de Couche 3

Dans un déploiement de couche 3, le pare-feu achemine le trafic entre plusieurs ports. Avant de pouvoir Configure Layer 3 Interfaces (Configurer les interfaces de couche 3), vous devez configurer le routeur virtuel ou le routeur logique que le pare-feu doit utiliser pour acheminer le trafic pour chaque interface de couche 3.



Si vous utilisez des étiquettes de groupe de sécurité (SGT) dans un réseau Cisco TrustSec, il est préférable de déployer des pare-feu en ligne, soit en couche 2, soit en mode câble virtuel. Toutefois, si vous devez utiliser un pare-feu de couche 3 dans un réseau Cisco TrustSec, vous devez déployer le pare-feu de couche 3 entre deux homologues du protocole d'échange SGT (SXP), et configurer le pare-feu pour permettre le trafic entre les homologues SXP.

Autoriser la prise en charge des adresses IP en double

À partir de PAN-OS® 11.1.4 et des versions ultérieures, la prise en charge des adresses IP en double (chevauchement) vous permet d'utiliser la même adresse IP sur plusieurs interfaces de pare-feu lorsque les interfaces utilisent des routeurs logiques différents et utilisent également l'une des combinaisons suivantes :

- Différentes zones et le même système virtuel.
- La même zone et différents systèmes virtuels.
- Différentes zones et différents systèmes virtuels.

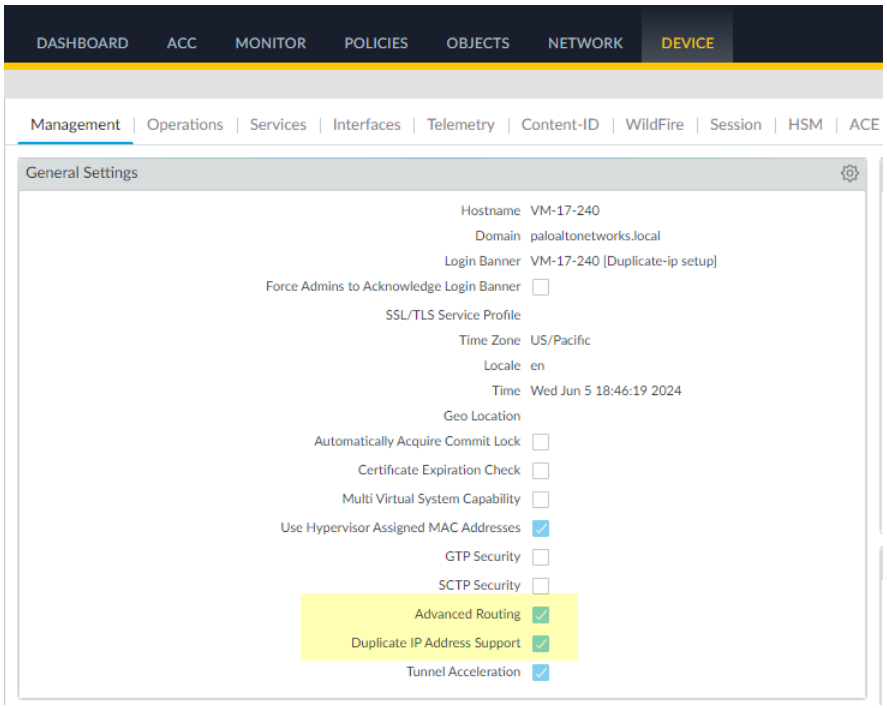
Il est important de comprendre ces exigences, car si vous tentez de configurer des adresses en double sur plusieurs interfaces dans la même zone et sur le même système virtuel, aucun échec de validation n'empêchera une mauvaise configuration.

Plusieurs interfaces sur le même routeur logique ne peuvent pas utiliser la même adresse IP.

Les pare-feu de la série PA-1400, les pare-feu VM-Series et la pile de modèles Panorama prennent en charge les adresses IP qui se chevauchent.

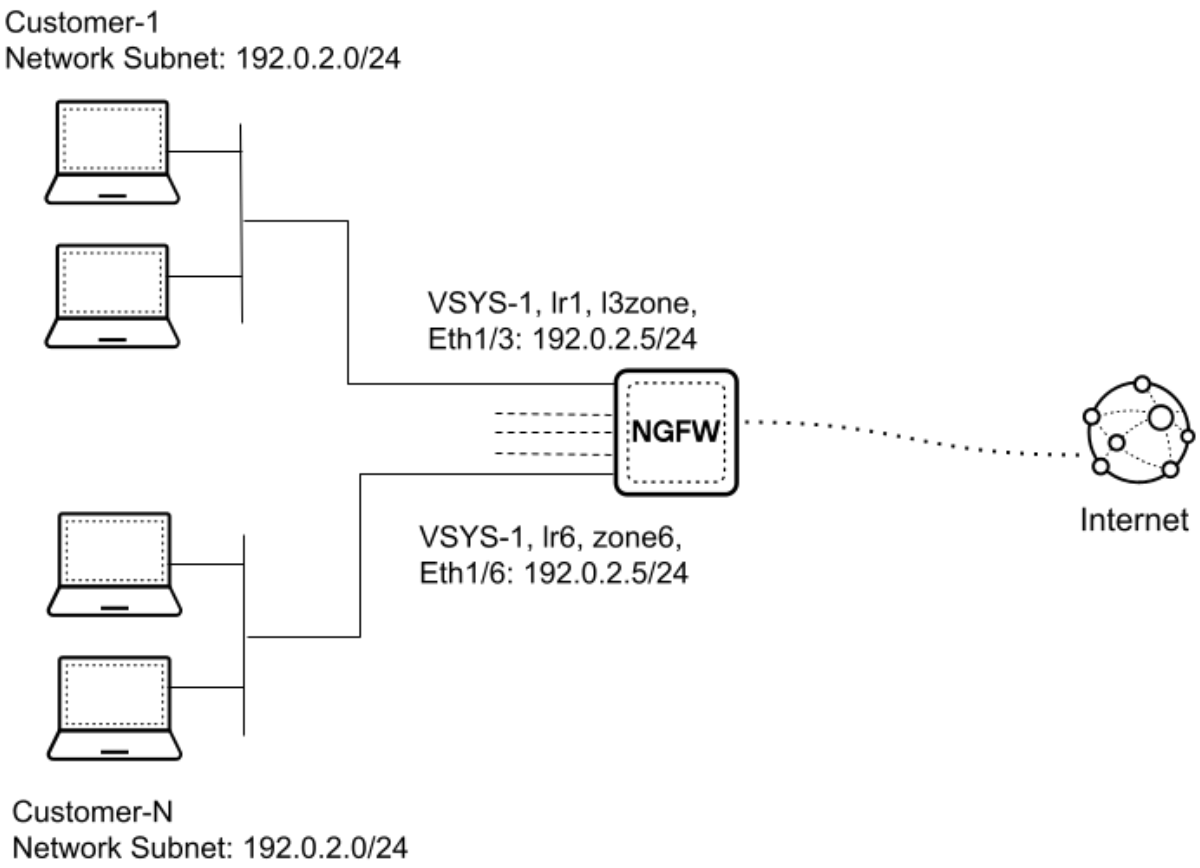
La prise en charge des adresses IP qui se chevauchent nécessite le moteur de routage avancé. Vous activez le Routage Avancé ; vous pouvez ensuite **Duplicate IP Address Support (Autoriser la prise en charge des adresses IP en double)**. Suivez la procédure standard pour valider et redémarrer le pare-feu avant de configurer des adresses IP en double.

©2024 Palo Alto Networks, Inc.

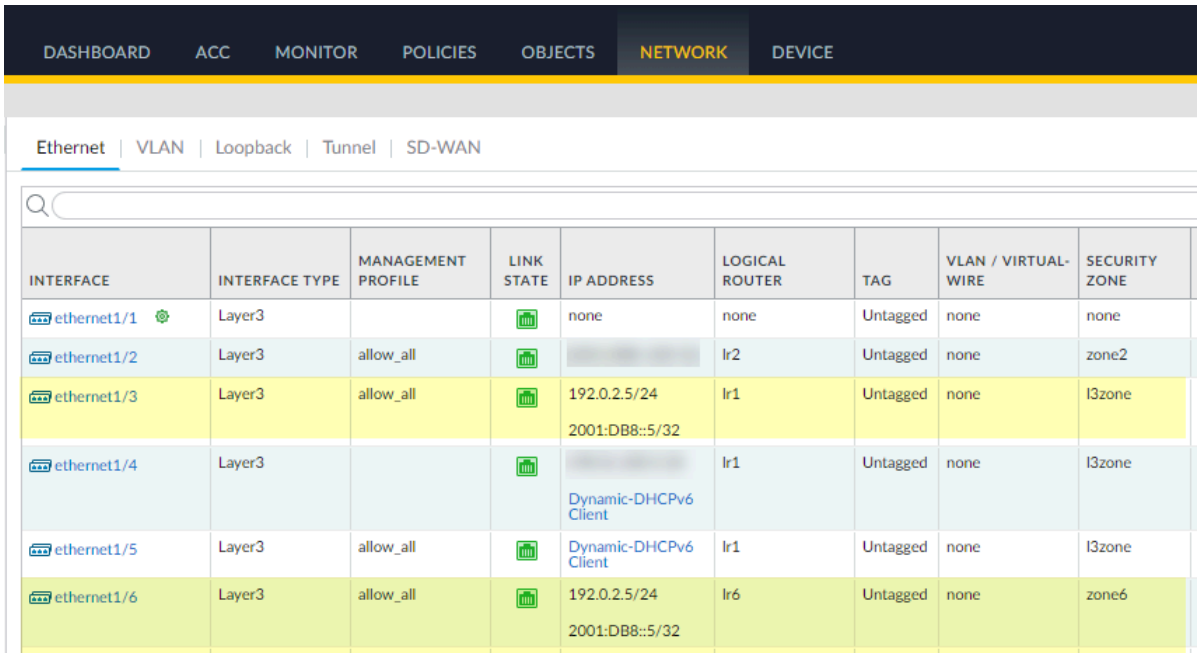


Vous pouvez ensuite procéder à la Configure Layer 3 Interfaces (Configuration des interfaces de couche 3) avec des adresses IP en double. L'exemple de topologie illustre la même adresse IP (192.0.2.5/24) sur deux interfaces (Ethernet1/3 et Ethernet1/6) appartenant à des routeurs logiques différents (lr1 et lr6), le même système virtuel (VSYS-1), et différentes zones (l3zone et zone6).

 ©2024 Palo Alto Networks, Inc.

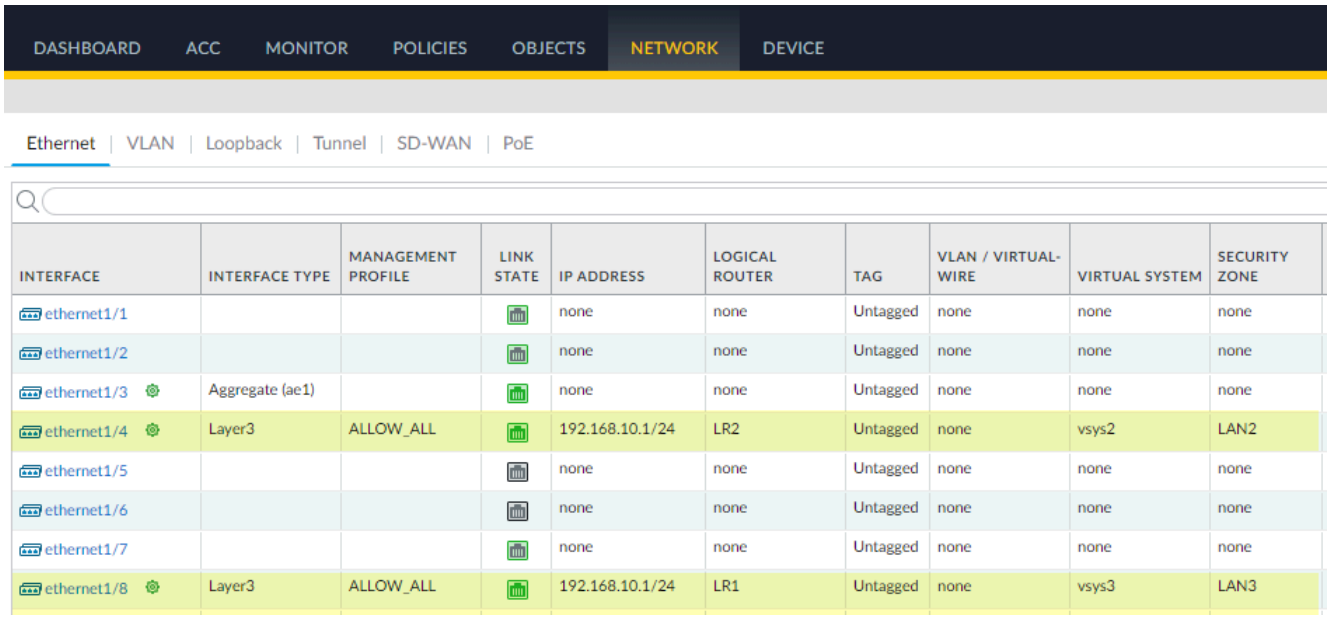


Les interfaces peuvent également partager des adresses IPv6. L'exemple de configuration résultant de l'exemple de topologie serait similaire à ceci :



 ©2024 Palo Alto Networks, Inc.

Un exemple de configuration distinct montre Ethernet1/4 et Ethernet1/8 avec des adresses IP qui se chevauchent configurées pour différents routeurs logiques, différents systèmes virtuels et différentes zones :



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	LOGICAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	VIRTUAL SYSTEM	SECURITY ZONE
ethernet1/1				none	none	Untagged	none	none	none
ethernet1/2				none	none	Untagged	none	none	none
ethernet1/3	Aggregate (ae1)			none	none	Untagged	none	none	none
ethernet1/4	Layer3	ALLOW_ALL		192.168.10.1/24	LR2	Untagged	none	vsys2	LAN2
ethernet1/5				none	none	Untagged	none	none	none
ethernet1/6				none	none	Untagged	none	none	none
ethernet1/7				none	none	Untagged	none	none	none
ethernet1/8	Layer3	ALLOW_ALL		192.168.10.1/24	LR1	Untagged	none	vsys3	LAN3

Les informations générales sur le tableau de bord affichent le paramètre du pare-feu : `Duplicate IP Enabled (Adresse IP en double activée)` ou `Duplicate IP Disabled (Adresse IP en double désactivée)`.

Les adresses IP qui se chevauchent prennent en charge les adresses IPv4 et IPv6 attribuées de manière statique et dynamique. Tous les types d'interfaces de couche 3 (Ethernet, VLAN, tunnel, en boucle, Aggregate Ethernet [AE] et sous-interfaces AE) prennent en charge les adresses IP qui se chevauchent. La prise en charge inclut les interfaces de passerelle.

L'interface de gestion ne prend pas en charge les adresses IP qui se chevauchent.

Les interfaces qui ont des adresses IP en double configurées prennent en charge les services suivants : Ping, SSH, Telnet, HTTP et HTTPS. Lorsque la prise en charge des adresses IP en double est activée, les commandes ping et traceroute vous obligent à spécifier un routeur logique, qui différencie l'adresse IP source parmi les adresses en double. Ainsi, la réponse revient à la bonne adresse IP. Utilisez les commandes opérationnelles CLI :

- **`ping source` *`ip`* `host` *`ip`* `logical-router` *`logical-router-name`***
- **`traceroute source` *`ip`* `host` *`ip`* `logical-router` *`logical-router-name`***

Vous pouvez accéder aux services Interface Management Profile (Profil de gestion d'interface) via des interfaces dont les adresses IP se chevauchent.

Le routage inter-vsys prend en charge le chevauchement des adresses IP afin que vous puissiez effectuer des acheminements entre les systèmes virtuels.

Les commandes CLI supplémentaires liées à la prise en charge des adresses IP en double sont :

©2024 Palo Alto Networks, Inc.

- **set deviceconfig setting duplicate-ip <yes|no>**

  Activez ou désactivez la prise en charge des adresses IP en double.
- **show system info**

  Affichez le paramètre d'adresse IP en double (activé ou désactivé).
- **show counter global name session_duplicate_ip_alt_srcnat_xlat**

  Affichez les compteurs pour la traduction NAT source duplicate-ip alt.

La première rubrique liée ci-dessous décrit comment configurer les interfaces de couche 3. Ce dernier lien de rubrique décrit comment utiliser le protocole NDP (Neighbor Discovery Protocol) pour provisionner les hôtes IPv6 et afficher les adresses IPv6 des appareils sur le réseau local de liaison pour localiser rapidement les périphériques.

- Configurer les interfaces de couche 3
- Gérer les hôtes IPv6 à l'aide du NDP

Configurer les interfaces de couche 3

Il faut suivre la procédure suivante pour configurer des interfaces de Couche 3 (interfaces Ethernet, VLAN, en boucle et de tunnel) avec des adresses IPv4 ou IPv6, pour que le pare-feu puisse effectuer le routage sur ces interfaces. Si un tunnel est utilisé pour le routage ou si la surveillance des tunnels est activée, le tunnel nécessite alors une adresse IP. Avant d'effectuer la tâche suivante, définissez un ou plusieurs routeurs virtuels sur un moteur de routage hérité ou des routeurs logiques sur un moteur de routage avancé.

En général, vous utiliserez cette procédure pour configurer une interface externe qui se connecte à l'Internet et une interface pour votre réseau interne. Vous pouvez configurer les adresses IPv4 et IPv6 sur une seule et même interface.



Les modèles de pare-feu PAN-OS prennent en charge un maximum de 16 000 adresses IP affectées à des interfaces de Couche 3 physiques ou virtuelles ; ce maximum comprend des adresses IPv4 et IPv6. Une seule interface de couche 3 prend en charge plusieurs adresses IPv4 statiques et IPv6 statiques. À tout moment, un type d'interface de couche 3 peut être IPv4 statique, DHCPv4 ou PPPoEv4. À tout moment, un type d'interface de couche 3 peut être statique IPv6, DHCPv6 ou hérité.

Si vous utilisez des itinéraires IPv6, vous pouvez configurer le pare-feu pour qu'il fournisse la configuration de la publication des routeurs IPv6 pour DNS. Le pare-feu fournit aux clients DNS IPv6 des adresses de Recursive DNS Server (serveur DNS récursif ; RDNS) et une liste de recherche DNS pour qu'ils puissent résoudre leurs requêtes DNS IPv6. Le pare-feu agit donc comme un serveur DHCPv6 pour vous.

À partir de PAN-OS 11.1.4, vous pouvez configurer des adresses IP en double (qui se chevauchent) sur les interfaces de couche 3 pour un moteur de routage avancé. Une condition préalable est que vous Activer le routage avancé. Si vous avez besoin d'adresses IP en double (qui se chevauchent), renseignez-vous à leur sujet avant de les activer dans cette procédure.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | (PAN-OS 11.1.4 et versions ultérieures) (Facultatif) Activez les adresses IP qui se chevauchent.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres généraux.
2. Sélectionnez **Duplicate IP Address Support (Prise en charge des adresses IP dupliquées)**.
3. **Commit (Validez)** la modification.

STEP 2 | Sélectionnez une interface et configurez-la avec une zone de sécurité.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et soit **Ethernet (Ethernet)**, **VLAN (VLAN)**, **loopback (En boucle)** ou **Tunnel (Tunnel)**, selon le type d'interface dont vous souhaitez disposer.
2. Sélectionnez l'interface à configurer.
3. Sélectionnez **Interface Type (Type d'interface)**—**Layer3 (De couche 3)**.
4. Dans l'onglet **Config (Configuration)**, sous **Virtual Router (routeur virtuel)**, sélectionnez le routeur virtuel que vous configurez, comme **default (par défaut)**.
5. Sous **Virtual System (Système virtuel)**, sélectionnez le système virtuel que vous configurez s'il se trouve sur un pare-feu de systèmes virtuels multiples.
6. Sous **Security Zone (Zone de sécurité)**, sélectionnez la zone à laquelle l'interface appartient ou créez une **New Zone (Nouvelle zone)**.
7. Cliquez sur **OK**.

STEP 3 | Configurez l'interface avec une adresse IPv4.

Vous pouvez affecter une adresse IPv4 à une interfaces de Couche 3 de l'une des trois façons suivantes :

- **Statique**
- **Client DHCP** : l'interface du pare-feu agit en tant que client DHCP et reçoit une adresse IP affectée de façon dynamique. Le pare-feu permet également de propager les paramètres reçus par l'interface du client DHCP dans un serveur DHCP actif sur le pare-feu. La propagation des paramètres d'un serveur DNS par un Internet Service Provider (fournisseur d'accès à Internet - ISP) est couramment pratiquée dans les machines clientes actives sur le réseau protégé par le pare-feu.
- **PPPoE** : configurez l'interface en tant que point de terminaison Point-to-Point Protocol over Ethernet (protocole point-à-point sur Ethernet ; PPPoE) afin de prendre en charge la connectivité dans un environnement Digital Subscriber Line (ligne d'accès numérique ; DSL) où se trouve un modem DSL, mais aucun autre périphérique PPPoE pour terminer la connexion.

  1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et soit **Ethernet (Ethernet)**, **VLAN (VLAN)**, **loopback (En boucle)** ou **Tunnel (Tunnel)**, selon le type d'interface dont vous souhaitez disposer.
  2. Sélectionnez l'interface à configurer.
  3. Pour configurer l'interface avec une adresse IPv4 statique, à l'onglet **IPv4 (IPv4)**, définissez le **Type (Type)** sur **Static (Statique)**.
  4. **Add (Ajoutez)** un **Name (Nom)** à l'adresse et saisissez éventuellement une **Description (Description)**.

 ©2024 Palo Alto Networks, Inc.

5. Sous **Type (Type)**, sélectionnez l'une des options suivantes :
   - **IP Netmask (Masque réseau IP)** : saisissez l'adresse IP et le masque de réseau à affecter à l'interface, par exemple, 208.80.56.100/24.

     Si vous utilisez un masque de sous-réseau /31 pour l'adresse de l'interface de couche 3, l'interfaces de Couche 3 doit être configurée avec l'adresse .1/31 pour que les utilitaires, comme ping, fonctionnent correctement.

     Si vous configurez une interface en boucle avec une adresse IPv4, elle doit posséder un masque de sous-réseau /32 ; par exemple, 192.168.2.1/32.
   - **IP Range (Plage d'adresses IP)** : saisissez une plage d'adresse IP, comme 192.168.2.1-192.168.2.4.
   - **FQDN (FQDN)** : saisissez le Fully Qualified Domain Name (nom de domaine complet ; FQDN).
6. Sélectionnez les **Tags (Étiquettes)** à appliquer à l'adresse.
7. Cliquez sur **OK**.

STEP 4 | Configurez une interface comme point de terminaison PPPoE.

PPPoE n'est pas pris en charge en mode HA active/active.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et soit **Ethernet (Ethernet)**, **VLAN (VLAN)**, **loopback (En boucle)** ou **Tunnel (Tunnel)**.
2. Sélectionnez l'interface à configurer.
3. Dans l'onglet **IPv4 (IPv4)**, définissez le **Type (Type)** sur **PPPoE (PPPoE)**.
4. À l'onglet **General (Général)**, sélectionnez **Enable (Activer)** pour activer l'interface de la terminaison PPPoE.
5. Saisissez le **Username (Nom d'utilisateur)** pour la connexion de point à point.
6. Saisissez le **Password (Mot de passe)** associé au nom d'utilisateur et **Confirm Password (Confirmer le mot de passe)**.
7. Cliquez sur **OK**.

STEP 5 | Configurer une interface en tant que client DHCPv4 pour qu'il reçoive une adresse IPv4 attribuée de manière dynamique.

Le client DHCP n'est pas pris en charge en mode HA active/active.

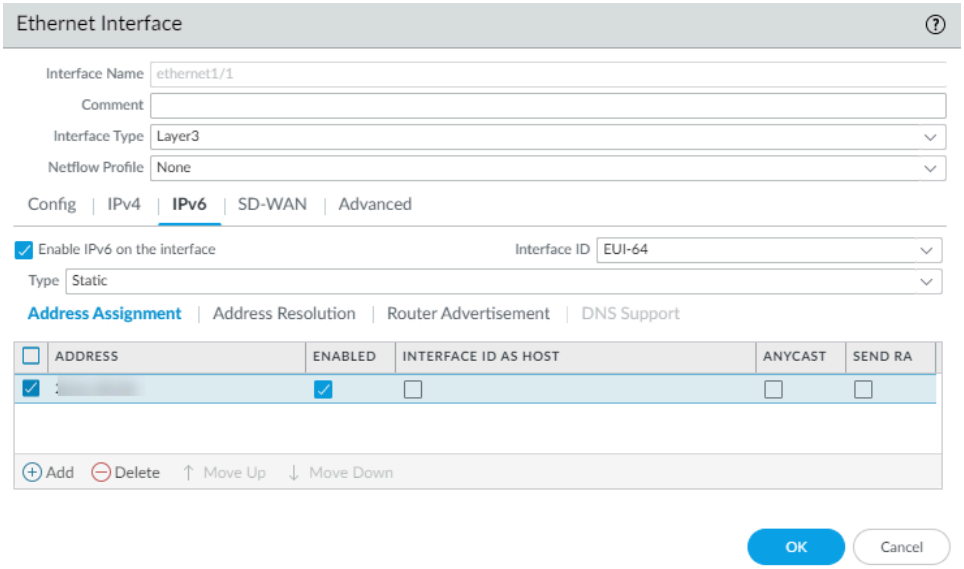
STEP 6 | Configure an Interface as a DHCPv6 Client (Configurez une interface en tant que client) DHCPv6 (avec ou sans délégation de préfixe) afin qu'elle reçoive une adresse IPv6 attribuée dynamiquement.

Le client DHCPv6 n'est pas pris en charge en mode HA active/active.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Configurez une interface avec une adresse IPv6 statique.

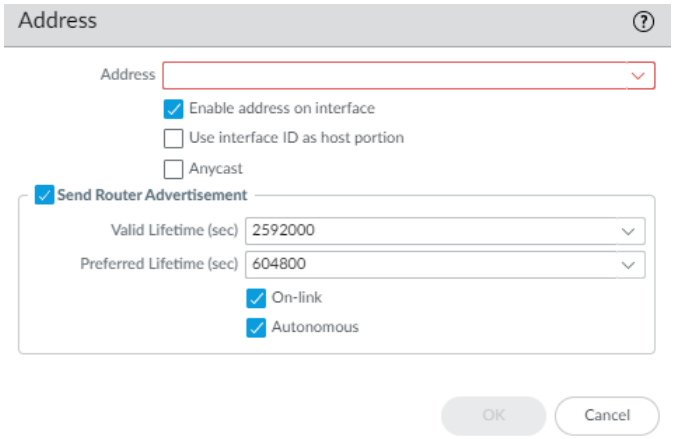
1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et soit **Ethernet (Ethernet)**, **VLAN (VLAN)**, **loopback (En boucle)** ou **Tunnel (Tunnel)**.
2. Sélectionnez l'interface à configurer.
3. À l'onglet **IPv6 (IPv6)**, sélectionnez **Enable IPv6 on the interface (Activer IPv6 sur l'interface)** pour activer l'adressage IPv6 sur l'interface.
4. Sous **Interface ID (ID de l'interface)**, saisissez l'identifiant unique étendu sur 64 bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64 bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
5. Sélectionnez**Address Assignment (Attribution d'adresse)** et **Add (Ajouter)Address (Adresse)** IPv6 ou sélectionnez un groupe d'adresses.



6. Sélectionnez **Enable address on interface (Activer l'adresse sur l'interface)** pour activer l'adresse IPv6 sur l'interface.
7. Sélectionnez **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** pour utiliser l'ID de l'interface comme partie hôte de l'adresse IPv6.
8. (Facultatif) Sélectionnez **Anycast (Anycast)** pour faire de l'adresse IPv6 (itinéraire) une adresse Anycast (itinéraire), ce qui veut dire que plusieurs emplacements peuvent publier

©2024 Palo Alto Networks, Inc.

le même préfixe et que l'adresse IPv6 envoie le trafic anycast au nœud qu'il considère le plus près selon les coûts associés au protocole de routage et d'autres facteurs.



9. (Interface Ethernet uniquement) Sélectionnez **Send Router Advertisement (Envoyer la publication de routeur)** (RA) pour permettre au pare-feu d'envoyer cette adresse dans les publications de routeurs, auquel cas vous devez également activer l'option globale **Enable Router Advertisement (Activer la publication de routeur)** sur l'interface (étape suivante).
10. (Interface Ethernet uniquement) Saisissez la **Valid Lifetime (sec) (Durée de vie valide (sec.))**, en secondes, pendant laquelle le pare-feu considère que l'adresse est valide. La durée de vie valide doit être supérieure ou égale à la **Preferred Lifetime (Durée de vie préférée)** (valeur par défaut de 2 592 000).
11. (Interface Ethernet uniquement) Saisissez la **Preferred Lifetime (sec) (Durée de vie préférée (sec.))** (en secondes) pendant laquelle l'adresse valide est préférée, ce qui signifie que le pare-feu peut l'utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l'adresse pour établir de nouvelles connexions, mais toute connexion existante reste valide jusqu'à ce que la **Valid Lifetime (Durée de vie valide)** expire (valeur par défaut de 604 800).
12. (Interface Ethernet uniquement) Sélectionnez **On-link (Sur la liaison)** si les systèmes qui disposent d'adresses dans le préfixe sont accessibles sans routeur.
13. Interface Ethernet uniquement Sélectionnez **Autonomous (Autonome)** si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l'ID d'une interface.
14. Cliquez sur **OK**.

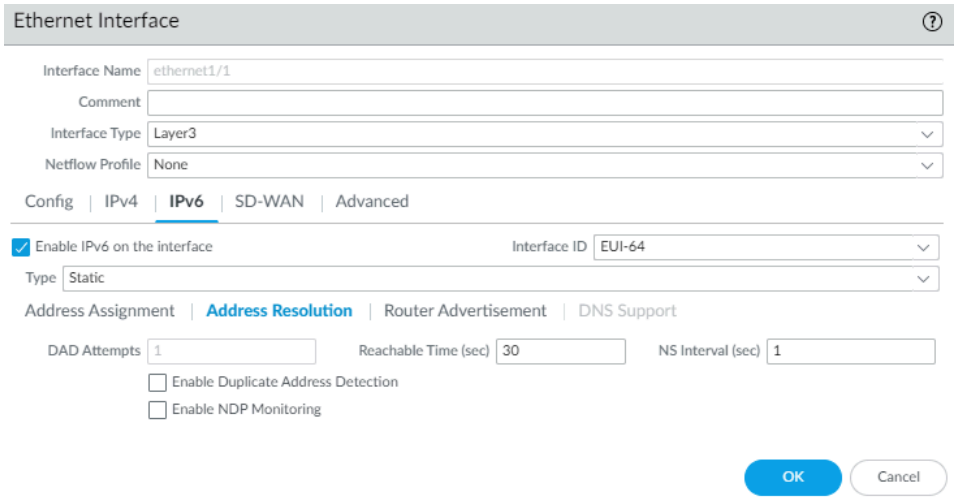
STEP 8 | Pour une interface IPv6 statique, configurez la résolution d'adresses.

1. Sélectionnez **Address Resolution (Résolution d'adresse)**.
2. **Enable Duplicate Address Detection (Activez la détection d'adresses en double (DAD))** si vous souhaitez que l'unicité d'une adresse IPv6 potentielle soit vérifiée avant qu'elle ne soit affectée à l'interface (la valeur par défaut est activée).
3. Si vous avez sélectionné **Enable Duplicate Address Detection (Activer la détection des adresses en double)**, spécifiez le nombre de **DAD Attempts (tentatives DAD)** dans

 ©2024 Palo Alto Networks, Inc.

l'intervalle de sollicitation de voisinage (NS) avant l'échec de la tentative d'identification des voisins ; plage comprise entre 0 et 10 ; la valeur par défaut est 1.

4. Entrez le **Reachable Time (sec) (temps d'accessibilité (sec))**, la durée pendant laquelle le client suppose qu'un voisin est joignable après avoir reçu un message de confirmation d'accessibilité ; la plage est comprise entre 10 et 36 000 ; la valeur par défaut est 30.
5. Entrez **NS Interval (sec) (intervalle NS (sec))** (intervalle de sollicitation de voisin), la durée entre les sollicitations de voisins ; plage comprise entre 1 et 3 600 ; la valeur par défaut est 1.
6. **Enable NDP Monitoring (Activez NDP Monitoring)** pour activer la surveillance du protocole de découverte des voisins. Lorsqu'il est activé, vous pouvez sélectionner l'icone NDP (dans la colonne Fonctions) et afficher des informations telles que l'adresse IPv6 d'un voisin découverte par le pare-feu, l'adresse MAC, User-ID correspondants et le statut (selon la situation la plus favorable).



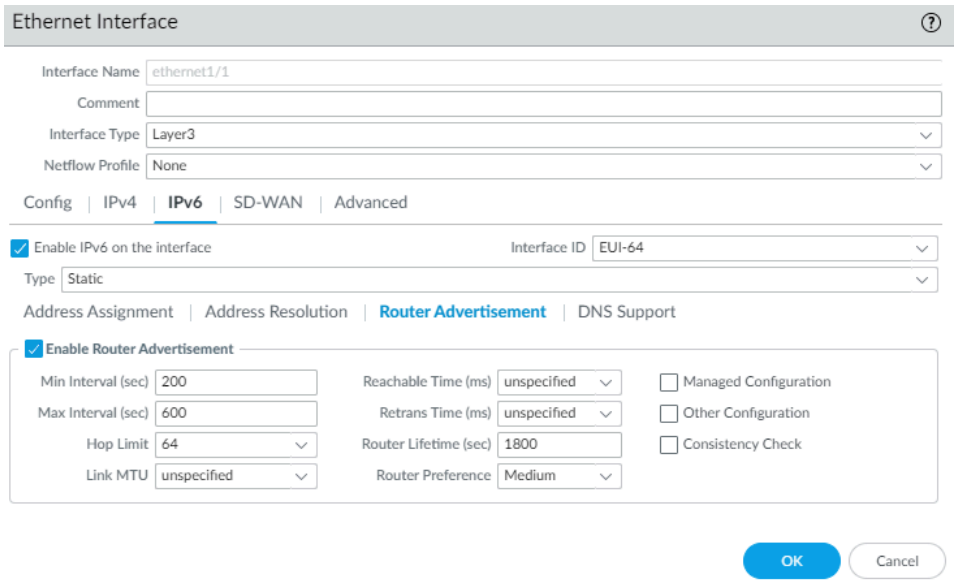
7. Cliquez sur **OK**.

©2024 Palo Alto Networks, Inc.

STEP 9 | (Interface Ethernet ou VLAN utilisant une adresse IPv6 uniquement) Activez l'envoi de Router Advertisements (publications de routeurs ; RA) IPv6 par le pare-feu à partir de l'interface et précisez éventuellement les paramètres RA.

*Précisez les paramètres RA pour l'un ou l'autre des motifs suivants : Pour interagir avec un routeur/un hôte qui utilise des valeurs différentes. Pour une convergence rapide lorsque plusieurs passerelles sont présentes. Par exemple, définissez des valeurs **Min Interval (Intervalle min.)**, **Max Interval (Intervalle max.)** et **Router Lifetime (Durée de vie du routeur)** inférieures pour que le client/hôte IPv6 puisse rapidement modifier la passerelle par défaut en cas d'échec de la passerelle principale et commencer le transfert vers une autre passerelle par défaut au sein du réseau.*

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et **Ethernet (Ethernet)** ou **VLAN (VLAN)**.
2. Sélectionnez l'interface que vous voulez configurer.
3. Sélectionnez **IPv6**.
4. Sélectionnez **Enable IPv6 on the interface (Activer IPv6 sur l'interface)**.
5. À l'onglet **Router Advertisement (Publication de routeur)**, sélectionnez **Enable Router Advertisement (Activer la publication de routeur)** (cette option est désactivée par défaut).



6. (Facultatif) Définissez le **Min Interval (sec) (Intervalle min. (sec.)**, soit l'intervalle minimum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 3 et 1 350 ; valeur par défaut : 200). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales que vous configurez.
7. (Facultatif) Définissez le **Max Interval (sec) (Intervalle max. (sec.))**, soit l'intervalle maximum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 4 et 1 800 ; valeur par défaut : 600). Le pare-feu envoie les publications

 ©2024 Palo Alto Networks, Inc.

de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales que vous configurez.

8. (Facultatif) Définissez la **Hop Limit (Limite de saut)** à appliquer aux clients pour les paquets sortants (intervalle compris entre 1 et 255 ; valeur par défaut : 64). Saisissez 0 pour indiquer l'absence de limite de saut.
9. (Facultatif) Définissez la **Link MTU (MTU de liaison)**, soit la Maximum Transmission Unit (unité de transmission maximale ; MTU) à appliquer aux clients (plage comprise entre 1 280 et 1 500 ; valeur par défaut : **unspecified (non spécifiée)**). Sélectionnez **unspecified (non spécifié)** pour aucune liaison MTU.
10. (Facultatif) Définissez la **Reachable Time (ms) (Durée d'accessibilité (ms))**, soit la durée d'accessibilité, en millisecondes, que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée d'accessibilité (intervalle compris entre 0 et 3 600 000 ; valeur par défaut : **non spécifiée**).
11. (Facultatif) Définissez la **Retrans Time (ms) (Durée de retransmission (ms))**, soit le minuteur de retransmission qui détermine la durée d'attente du client, en millisecondes, avant la retransmission des messages de sollicitation de voisins. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée de retransmission (intervalle compris entre 0 et 4 294 967 295 ; valeur par défaut : **non spécifiée**).
12. (Facultatif) Définissez la **Router Lifetime (sec) (Durée de vie du routeur (s))** pour indiquer la durée, en secondes, pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.
13. Définissez la **Router Preference (Préférence de routeur)**, c'est le champ que le client utilise pour sélectionner un routeur préféré si le segment de réseau dispose de plusieurs routeurs IPv6, **High (Élevée)**, **Medium (Moyenne)** (par défaut) ou **Low (Faible)** est la priorité que le RA publie afin d'indiquer la priorité relative du routeur virtuel du pare-feu par rapport aux autres routeurs se trouvant sur le segment.
14. Sélectionnez **Managed Configuration (Configuration gérée)** pour indiquer au client que les adresses sont disponibles via DHCPv6.
15. Sélectionnez **Other Configuration (Autre configuration)** pour indiquer au client que d'autres informations d'adresse (comme les paramètres associés au DNS) sont disponibles via DHCPv6.
16. Cochez **Consistency Check (Vérification de cohérence)** pour que le pare-feu vérifie que les RA reçues des autres routeurs publient des informations cohérentes sur la liaison. Le pare-feu consigne toute incohérence.
17. Cliquez sur **OK**.

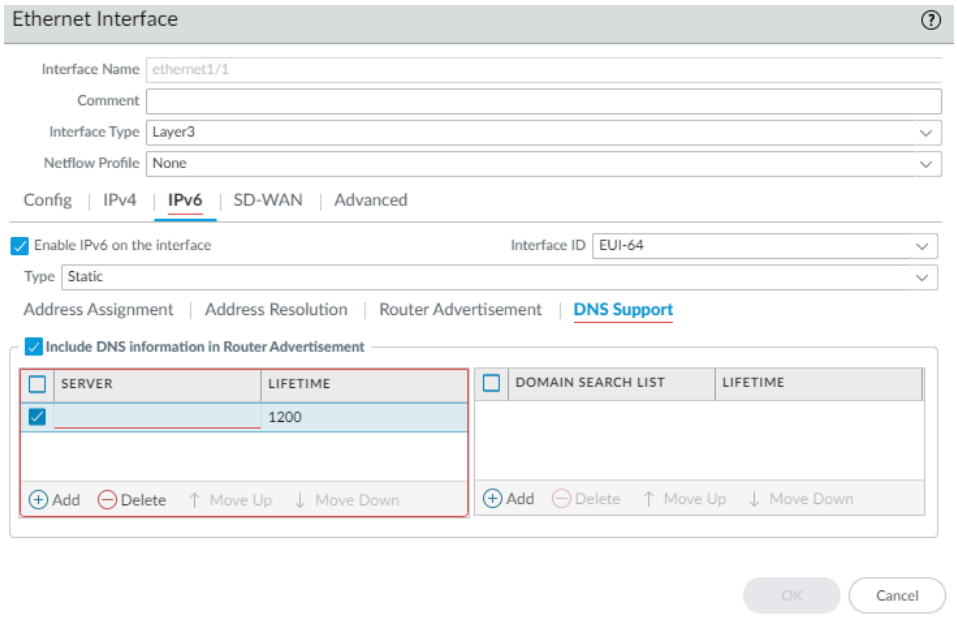
 ©2024 Palo Alto Networks, Inc.

STEP 10 | (Interface Ethernet ou VLAN utilisant une adresse IPv6 uniquement) Indiquez les adresses de serveur DNS récursif et la liste de recherche DNS que le pare-feu publiera dans les publications de routeur ND à partir de cette interface.

Les serveurs RDNS et la liste de recherche DNS font partie de la configuration DNS du client DNS permettant au client de résoudre les requêtes DNS IPv6.

*Vous devez avoir sélectionné **Enable Router Advertisement (Activer la publication du routeur)** dans l'onglet **Router Advertisement (Router Advertisement)** pour rendre l'onglet DNS Support disponible.*

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et **Ethernet (Ethernet)** ou **VLAN (VLAN)**.
2. Sélectionnez l'interface à configurer.
3. Sélectionnez **IPv6 (IPv6)** > **DNS Support (Prise en charge DNS)**.



4. Sélectionnez **Include DNS information in Router Advertisement (Inclure les informations DNS dans la publication de routeur)** pour permettre au pare-feu d'envoyer les informations DNS IPv6.
5. Pour le **Server (serveur)** DNS **Add (ajoutez)** l'adresse IPv6 d'un serveur, DNS récursif (en ajoutant jusqu'à huit serveurs). Le pare-feu envoie des adresses de serveur dans une publication de routeur ICMPv6 dans l'ordre, de haut en bas.
6. Indiquez la **Lifetime (Durée de vie)** en secondes. Il s'agit de la durée de temps maximale pendant laquelle le client peut utiliser le serveur RDNS donné pour résoudre des noms de domaine.
   - La plage de la **Lifetime (Durée de vie)** correspond à toute valeur égale ou se situant entre le **Max Interval (Intervalle Max.)** (que vous avez configuré à l'onglet **Router Advertisement (Publication de routeur)**) et deux fois cet **Max Interval (Intervalle max.)**. Par exemple, si votre intervalle maximum est 600 secondes, la plage de la durée de vie est de 600 à 1 200 secondes.

©2024 Palo Alto Networks, Inc.

- La **Lifetime (Durée de vie)** par défaut est 1 200 secondes.

7. **Add (Ajoutez)** une **Domain Search List (liste de recherche de domaine)** (nom de domaine d'un maximum de 255 octets). Ajoutez jusqu'à huit entrées. Le pare-feu envoie les domaines dans une publication de routeur ICMPv6 dans l'ordre de haut en bas.
8. Indiquez la **Lifetime (Durée de vie)** en secondes. Il s'agit de la durée de temps maximale pendant laquelle le client peut utiliser la liste. La durée de vie possède la même plage et la même valeur par défaut que le **Server (Serveur)**.
9. Cliquez sur **OK**.

STEP 11 | (Interface Ethernet ou VLAN) Indiquez les entrées ARP statiques. Les entrées ARP statiques réduisent le traitement ARP.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et **Ethernet (Ethernet)** ou **VLAN (VLAN)**.
2. Sélectionnez l'interface à configurer.
3. Sélectionnez **Advanced (Avancé)** > **ARP Entries (Entrées ARP)**.
4. **Add (Ajoutez)** une **IP Address (Adresse IP)** et son **MAC Address (Adresse MAC)** correspondante (adresse matérielle ou de commande d'accès au support). Dans le cas d'une interface VLAN, vous devez également sélectionner l'**Interface**.

   Les entrées ARP statiques n'expirent pas. Les entrées ARP auto-apprises qui se trouvent dans le cache expirent en 1 800 secondes par défaut ; vous pouvez customize the ARP cache timeout (personnaliser le délai d'expiration du cache ARP).
5. Cliquez sur **OK**.

STEP 12 | (Interface Ethernet ou VLAN) Indiquez les entrées Neighbor Discovery Protocol (protocole de recherche de voisins ; NDP). NDP pour IPv6 effectue des fonctions semblables à celles fournies par ARP pour IPv4.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et **Ethernet (Ethernet)** ou **VLAN (VLAN)**.
2. Sélectionnez l'interface à configurer.
3. Sélectionnez **Advanced (Avancé)** > **ND Entries (Entrées ND)**.
4. **Add (Ajoutez)** une **IPv6 Address (Adresse IPv6)** et sa **MAC Address (Adresse MAC)** correspondante.
5. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 13 | (Facultatif) Activez les services sur l'interface.

1. Pour activer les services sur l'interface, sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)**, puis **Ethernet (Ethernet)** ou **VLAN (VLAN)**.
2. Sélectionnez l'interface à configurer.
3. Sélectionnez **Advanced (Avancé)** > **Other Info (Autres informations)**.
4. Développez la liste **Management Profile (Profil de gestion)**, puis sélectionnez un profil ou **New Management Profile (Nouveau profil de gestion)**.
5. Saisissez un **Name (Nom)** pour le profil.
6. Sous **Permitted Services (Services autorisés)**, sélectionnez des services, comme **Ping (Ping)**, puis cliquez sur **OK (OK)**.

STEP 14 | **Commit (Validez)** vos modifications.

STEP 15 | Câblez l'interface.

Connectez les câbles directs des interfaces que vous avez configurées au commutateur ou au routeur correspondant sur chaque segment de réseau.

STEP 16 | Vérifiez que l'interface est active.

Dans l'interface Web, sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et vérifiez que l'icône dans la colonne Link State (État de la liaison) est de couleur verte. Vous pouvez également surveiller l'état de la liaison dans le widget **Interfaces (Interfaces)** du **Dashboard (Tableau de bord)**.

STEP 17 | Configurez des itinéraires statiques et/ou un protocole d'acheminement dynamique pour que le routeur virtuel puisse acheminer le trafic.

STEP 18 | Configurez un itinéraire par défaut.

Configure a Static Route (Configurez un itinéraire statique) pour un routeur virtuel ou Créer un itinéraire statique pour un routeur logique et définissez-le par défaut.

STEP 19 | ((Supported firewalls onlyPare-feu pris en charge uniquement)) Si l'interface correspond à un port PoE (Power over Ethernet) sur le pare-feu, vous pouvez éventuellement configure PoE (configurer PoE).

Gérer les hôtes IPv6 à l'aide du NDP

Cette rubrique décrit comment vous pouvez utiliser NDP pour provisionner des hôtes IPv6; par conséquent, vous n'avez pas besoin d'un serveur DHCPv6 distinct à cette fin. Il explique également comment utiliser NDP pour surveiller les adresses IPv6, ce qui vous permet de suivre rapidement l'adresse IPv6 et l'adresse MAC d'un périphérique et l'utilisateur associé qui a enfreint une règle de sécurité.

- Annonces de routeur IPv6 pour la configuration DNS
- Configurer les serveurs RDNS et la liste de recherche DNS pour les Annonces de routeur IPv6
- Surveillance NDP
- Activer la surveillance NDP

 ©2024 Palo Alto Networks, Inc.

Annonces de routeur IPv6 pour la configuration DNS

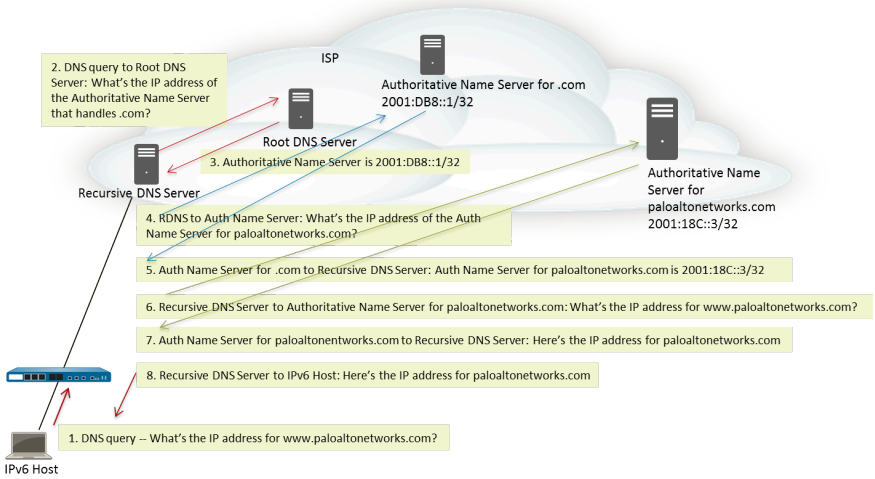
L'implémentation du pare-feu de Neighbor Discovery (ND) est améliorée afin que vous puissiez provisionner les hôtes IPv6 avec l'option RDNSS (Recursive DNS Server) et DNSSL (DNS Search List) selon RFC 6106, Options de publication du routeur IPv6 pour la configuration DNS. Lorsque vous configurez des interfaces de couche 3, vous configurez ces options DNS sur le pare-feu afin que le pare-feu puisse provisionner vos hôtes IPv6; par conséquent, vous n'avez pas besoin d'un serveur DHCPv6 distinct pour provisionner les hôtes. Le pare-feu envoie des annonces de routeur (RA) IPv6 contenant ces options aux hôtes IPv6 dans le cadre de leur configuration DNS afin de les provisionner complètement pour accéder aux services Internet. Ainsi, vos hôtes IPv6 sont configurés avec :

- Les adresses des serveurs RDNS qui peuvent répondre aux requêtes DNS.
- Une liste de noms de domaine (suffixes) que le client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d'entrer le nom de domaine dans une requête DNS.

L'Annonce de routeur IPv6 pour la configuration DNS est prise en charge pour les interfaces Ethernet, les sous-interfaces, les interfaces Ethernet agrégées et les interfaces VLAN de couche 3 sur toutes les plates-formes PAN-OS.

La capacité du pare-feu à envoyer des RAs IPv6 pour la configuration DNS permet au pare-feu d'exécuter un rôle similaire à celui du DHCP et n'a aucun rapport avec le pare-feu en tant que proxy DNS, client DNS ou serveur DNS.

Après avoir configuré le pare-feu avec les adresses des serveurs RDNS, le pare-feu fournit un hôte IPv6 (le client DNS) avec ces adresses. L'hôte IPv6 utilise une ou plusieurs de ces adresses pour atteindre un serveur DNS. DNS récursif fait référence à une série de requêtes DNS par un serveur RDNS, comme indiqué avec trois paires de requêtes et de réponses dans la figure suivante. Par exemple, lorsqu'un utilisateur tente d'accéder à l'adresse www.paloaltonetworks.com, le navigateur local constate qu'il n'a pas l'adresse IP de ce nom de domaine dans son cache, et que le système d'exploitation du client ne l'a pas non plus. Le système d'exploitation du client lance une requête DNS sur un serveur DNS récursif appartenant au fournisseur d'accès Internet local.



 ©2024 Palo Alto Networks, Inc.

Une publication de routeur IPv6 peut contenir plusieurs options d'adresse de serveur DNS récursive, chacune avec des durées de vie identiques ou différentes. Une seule adresse de serveur DNS récursif DNS peut contenir plusieurs adresses de serveur DNS récursif tant que les adresses ont la même durée de vie.

Une liste de recherche DNS est une liste de noms de domaine (suffixes) que le pare-feu annonce à un client DNS. Le pare-feu dispose ainsi le client DNS pour utiliser les suffixes dans ses requêtes DNS non qualifiées. Le client DNS ajoute les suffixes, un à la fois, à un nom de domaine non qualifié avant d'entrer le nom dans une requête DNS, utilisant ainsi un nom de domaine complet (FQDN) dans la requête DNS. Par exemple, si un utilisateur (du client DNS en cours de configuration) essaie de soumettre une requête DNS pour le nom "qualité" sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet une requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête DNS qui résulte du routeur est « quality.company.com » pour le FQDN.

Si la requête DNS échoue, le client ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le client utilise les suffixes DNS dans l'ordre jusqu'à ce qu'une recherche DNS réussisse (en ignorant les suffixes restants) ou le routeur a essayé tous les suffixes de la liste.

Vous configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option ND DNSSL ; le client DNS recevant l'option Liste de recherche DNS est configuré pour utiliser les suffixes dans ses requêtes DNS non qualifiées.

Pour spécifier des serveurs RDNS et une liste de recherche DNS, Configurer les serveurs RDNS et la liste de recherche DNS pour les Annonces de routeur IPv6.

Configurer les serveurs RDNS et la liste de recherche DNS pour les Annonces de routeur IPv6

Effectuez cette tâche pour configurer les publications de routeur IPv6 pour DNS des hôtes IPv6.

STEP 1 | Autorisez le pare-feu à envoyer des publications de routeur IPv6 à partir d'une interface.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et **Ethernet (Ethernet)** ou **VLAN (VLAN)**.
2. Sélectionnez l'interface à configurer.
3. À l'onglet **IPv6 (IPv6)**, sélectionnez **Enable IPv6 on the interface (Activer IPv6 sur l'interface)**.
4. À l'onglet **Router Advertisement (Publication de routeur)**, sélectionnez **Enable Router Advertisement (Activer la publication de routeur)**.
5. Cliquez sur **OK**.

©2024 Palo Alto Networks, Inc.

STEP 2 | Indiquez les adresses de serveur DNS récursif et la liste de recherche DNS que le pare-feu publiera dans les publications de routeur ND à partir de cette interface.

Les serveurs RDNS et la liste de recherche DNS font partie de la configuration DNS du client DNS permettant au client de résoudre les requêtes DNS IPv6.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et **Ethernet (Ethernet)** ou **VLAN (VLAN)**.
2. Sélectionnez l'interface à configurer.
3. Sélectionnez **IPv6 (IPv6)** > **DNS Support (Prise en charge DNS)**.
4. Sélectionnez **Include DNS information in Router Advertisement (Inclure les informations DNS dans la publication de routeur)** pour permettre au pare-feu d'envoyer les informations DNS IPv6.
5. Comme **Server (Serveur)** DNS, **Add (Ajoutez)** l'adresse IPv6 d'un serveur DNS récursif. **Add (Ajoutez)** un maximum de huit serveurs DNS récursifs. Le pare-feu envoie des adresses de serveur dans une publication de routeur ICMPv6 dans l'ordre, de haut en bas.
6. Indiquez la **Lifetime (Durée de vie)** en secondes. Il s'agit de la durée de temps maximale pendant laquelle le client peut utiliser le serveur RDNS donné pour résoudre des noms de domaine.
   - La plage de la **Lifetime (Durée de vie)** correspond à toute valeur égale ou se situant entre le **Max Interval (Intervalle Max.)** (que vous avez configuré à l'onglet **Router Advertisement (Publication de routeur)**) et deux fois cet **Max Interval (Intervalle max.)**. Par exemple, si votre intervalle maximum est 600 secondes, la plage de la durée de vie est de 600 à 1 200 secondes.
   - La **Lifetime (Durée de vie)** par défaut est 1 200 secondes.
7. Pour le suffixe DNS, **Add (Ajoutez)** un **DNS Suffix (Suffixe DNS)** (nom de domaine d'un maximum de 255 octets). **Add (Ajoutez)** un maximum de huit suffixes DNS. Le pare-feu envoie les suffixes dans une publication de routeur ICMPv6 dans l'ordre, de haut en bas.
8. Indiquez la **Lifetime (Durée de vie)** en secondes. Il s'agit de la durée de temps maximale pendant laquelle le client peut utiliser le suffixe. La durée de vie possède la même plage et la même valeur par défaut que le **Server (Serveur)**.
9. Cliquez sur **OK**.

STEP 3 | Validez vos modifications.

Cliquez sur **Commit (Valider)**.

Surveillance NDP

Le protocole NDP (Neighbor Discovery Protocol) pour IPv6 (RFC 4861) exécute des fonctions similaires aux fonctions ARP pour IPv4. Par défaut, le pare-feu exécute NDP, qui utilise des paquets ICMPv6 pour détecter et suivre les adresses de couche liaison et l'état des voisins sur les liaisons connectées.

Activer la surveillance NDP, vous pouvez ainsi afficher les adresses IPv6 des périphériques sur le réseau local de liaison, leur adresse MAC, le nom d'utilisateur associé à User-ID (si l'utilisateur de ce périphérique a utilisé le service d'annuaire pour se connecter), l'état d'accessibilité de l'adresse et le dernier rapport sur la date et l'heure à laquelle le surveillant NDP a reçu une annonce

 ©2024 Palo Alto Networks, Inc.

de routeur de cette adresse IPv6. Le nom d'utilisateur est le meilleur des cas; Il peut y avoir plusieurs périphériques IPv6 sur un réseau sans nom d'utilisateur, tels que des imprimantes, des télécopieurs, des serveurs, etc.

Si vous souhaitez suivre rapidement un périphérique et un utilisateur qui a enfreint une règle de sécurité, il est très utile d'afficher l'adresse IPv6, l'adresse MAC et le nom d'utilisateur au même endroit. Vous avez besoin de l'adresse MAC correspondant à l'adresse IPv6 afin de retracer l'adresse MAC vers un commutateur physique ou un point d'accès.

La surveillance NDP n'est pas garantie pour détecter tous les périphériques, car il peut exister d'autres périphériques réseau entre le pare-feu et le client qui filtrent les messages NDP ou Duplicate Address Detection (Détection d'adresse dupliquée ; DAD). Le pare-feu peut uniquement surveiller les périphériques qu'il apprend sur l'interface.

La surveillance NDP surveille également les paquets DAD (Duplicate Address Detection) provenant des clients et des voisins. Vous pouvez également surveiller les journaux IPv6 ND pour faciliter le dépannage.

La surveillance NDP est prise en charge pour les interfaces Ethernet, les sous-interfaces, les interfaces Ethernet agrégées et les interfaces VLAN sur tous les modèles PAN-OS.

Activer la surveillance NDP

Effectuez cette tâche pour activer la surveillance NDP d'une interface.

STEP 1 | Activer la surveillance NDP.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et **Ethernet (Ethernet)** ou **VLAN (VLAN)**.
2. Sélectionnez l'interface à configurer.
3. Sélectionnez **IPv6**.
4. Sélectionnez **Address Resolution (Résolution d'adresse)**.
5. Select **Enable NDP Monitoring (Activer la surveillance NDP)**.

   *Après avoir activé ou désactivé la surveillance NDP, vous devez **Commit (Valider)** avant que la surveillance NDP puisse commencer ou prendre fin.*
6. Cliquez sur **OK**.

STEP 2 | Validez vos modifications.

Cliquez sur **Commit (Valider)**.

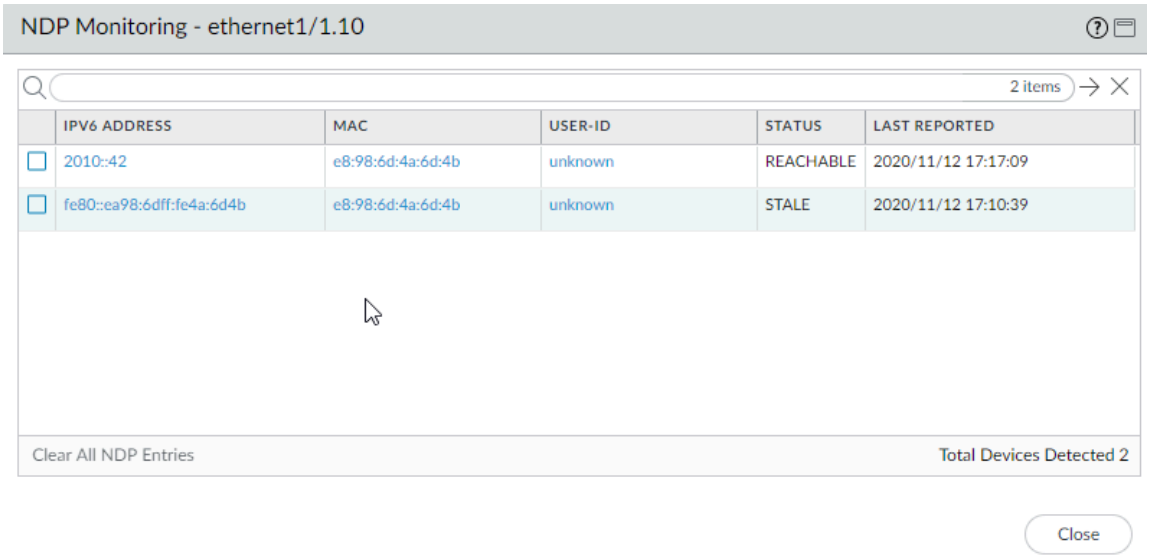
 ©2024 Palo Alto Networks, Inc.

STEP 3 | Surveillance NDP et paquets DAD des clients et voisins.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et **Ethernet (Ethernet)** ou **VLAN (VLAN)**.
2. Pour l'interface pour laquelle vous avez activé la surveillance NDP, dans la colonne Features (Fonctionnalités), passez la souris sur l'icône de la surveillance NDP :

   Le récapitulatif de surveillance NDP de l'interface présente la liste des **Prefixes (Préfixes)** IPv6 que cette interface enverra dans la Router Advertisement (publication de routeur ; RA) si la RA est activée (il s'agit des préfixes IPv6 de l'interface elle-même).

   Le récapitulatif indique également si la prise en charge DAD, de la publication de routeur et de DNS est activée, si les adresses IP de tout serveur DNS récursif sont configurées et si les suffixes DNS de la liste de recherche DNS sont configurés.
3. Cliquez sur l'icône de surveillance NDP pour afficher des renseignements détaillés.



Chaque rangée de la table de surveillance NDP détaillée de l'interface indique l'adresse IPv6 d'un voisin que le pare-feu a découvert, l'adresse MAC correspondante, le User-ID correspondant (dans la mesure du possible), l'état de disponibilité de l'adresse ainsi que la date du dernier rapport et l'heure à laquelle cette surveillance NDP a reçu une RA de cette adresse IP. Un User-ID ne s'affichera pas pour les imprimantes ou les autres hôtes non basés sur l'utilisateur. Si l'état de l'adresse IP est Hors service, le voisin n'est pas connu pour être accessible, conformément au document RFC 4861.

Dans le coin inférieur droit se trouve le nombre de **Total Devices Detected (Périphériques totaux détectés)** sur le réseau de liaison local.

- Entrez une adresse IPv6 dans le champ de filtrage pour chercher une adresse à afficher.
- Cochez les cases pour afficher ou non les adresses IPv6.
- Cliquez sur les numéros, sur la flèche de gauche ou de droite ou sur la barre défilante verticale pour faire défiler les entrées.
- Cliquez sur **Clear All NDP Entries (Supprimer toutes les entrées NDP)** pour supprimer le tableau complet.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Surveillez les journaux ND à des fins d'établissement de rapports.

1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **System (Système)**.
2. Dans la colonne Type (Type), affichez les journaux **ipv6nd** et les descriptions correspondantes.

   Par exemple, `inconsistent router advertisementreceived` indique que le pare-feu a reçu une RA qui diffère de la RA qu'il va envoyer.

©2024 Palo Alto Networks, Inc.

Interfaces cellulaires

L'interface cellulaire 5G est disponible sur la plateforme PA-415-5G. Cette interface vous permet de fournir une connexion Internet principale ou de configurer une connexion secondaire pour la redondance au cas où la connexion principale serait indisponible. Elle fournit une connectivité de données via le réseau mobile 5G et passe automatiquement à un réseau 4G ou 3G si le réseau 5G n'est pas disponible. Vous pouvez également configurer l'interface 5G pour l'équilibrage de charge à l'aide d'un round robin pondéré. Pour surveiller facilement les informations sur l'état du réseau 5G, utilisez les widgets du tableau de bord.

Vous pouvez configurer une carte SIM principale et secondaire (si disponible). Si vous disposez d'une carte SIM secondaire, vous pouvez configurer le pare-feu pour passer d'une carte SIM à une autre si une carte SIM devient indisponible. Pour des raisons de sécurité, activez un code PIN pour la carte SIM afin d'éviter toute utilisation abusive.

À mesure que les opérateurs fournissent des mises à jour apportant de nouvelles fonctionnalités et résolvant les problèmes, vous pouvez télécharger des mises à jour du micrologiciel cellulaire à partir du portail d'assistance client et les installer sur le pare-feu. Cela permet au pare-feu de transmettre les mises à jour aux utilisateurs appropriés de votre réseau. Une interface simplifiée facilite la révision, la gestion et le déploiement des mises à jour du micrologiciel cellulaire sur votre réseau 5G. La mise à jour du micrologiciel cellulaire offre de nouvelles fonctionnalités et capacités et contribue à protéger vos utilisateurs contre les menaces et les vulnérabilités.

Les rubriques suivantes fournissent des conseils sur la configuration d'une interface pour votre réseau 5G et sur comment mettre à niveau le micrologiciel cellulaire sur l'interface 5G.

- Configurer la 5G pour une interface cellulaire
- Mise à niveau du microprogramme 5G

Configurer la 5G pour une interface cellulaire

Vous pouvez activer la fonctionnalité 4G/5G à l'aide du PA-415-5G, qui contient un module 5G intégré. Cette configuration fournit une interface pour une connexion Internet principale ou pour la redondance sous forme de lien via l'interface cellulaire.

Le module 5G nécessite PAN-OS version 11.1 ou versions ultérieures.

La configuration d'une interface cellulaire 5G fournit une connectivité de données utilisant le réseau mobile 5G. Si le réseau 5G est indisponible, le pare-feu bascule automatiquement sur le réseau 4G ou 3G.

À l'initialisation, le modem est actif et l'option radio n'est pas activée par défaut. Si une ou plusieurs cartes SIM sont disponibles et que vous activez l'option radio, le pare-feu tente d'établir une session par paquets à l'aide de la carte SIM que vous configurez dans le profil APN de l'emplacement SIM principal.

*S'il n'y a pas de profil APN personnalisé, le pare-feu utilise le profil APN **auto**.*

©2024 Palo Alto Networks, Inc.

À Mise à niveau du microprogramme 5G, téléchargez les mises à jour du micrologiciel depuis le portail de support client et installez-les sur le pare-feu.

L'interface cellulaire 5G prend en charge les fonctionnalités suivantes :

- Routage (y compris BGP, BFD et itinéraires statiques)

  L'interface cellulaire 5G prend en charge l'équilibrage de charge avec un round robin pondéré. La pile de routage héritée ne prend pas en charge le BGP sur l'interface IP dynamique ; comme alternative, utilisez l'interface en boucle.
- IPv4
- Interfaces de Couche 3
- Encapsulation de couche 2
- Tunnellisation et VPN (y compris IKE, IPSec et GRE)

  L'interface cellulaire 5G prend en charge GRE à l'aide de l'interface en boucle.
- NAT
- PBF

  L'interface cellulaire 5G ne prend pas en charge le retour symétrique.
- Zones et profils de protection de zone
- Politiques de protection DoS
- Inspection des tunnels
- Itinéraires de service utilisant des interfaces en boucle
- HA active/passive (la synchronisation et la continuité de la session ne sont pas prises en charge)

L'interface cellulaire 5G ne prend pas en charge les fonctionnalités suivantes :

- IPv6
- ECMP
- Multi-vsys
- HA active/active
- Trames Jumbo
- OSPF
- Déchargement de multidiffusion ou d'ACL

STEP 1 | Créez un profil de nom de point d'accès (APN).

Vous devez configurer correctement le profil APN pour activer l'accès à Internet. Le profil APN définit le ou les réseaux auxquels le périphérique est autorisé à accéder et détermine si le périphérique reçoit une adresse IP dynamique ou statique. Pour permettre l'accès aux services de données, certains opérateurs de réseaux virtuels mobiles (MVNO) nécessitent un profil APN distinct en plus du profil APN de l'opérateur réseau. En fonction de l'opérateur, vous devrez

 ©2024 Palo Alto Networks, Inc.

peut-être également activer des mesures de sécurité supplémentaires pour limiter l'APN aux utilisateurs authentifiés.

STEP 2 | Configurez les règles de politique de sécurité NAT dynamiques à l'aide d'adresses IP dynamiques pour autoriser le trafic 5G.

STEP 3 | Configurez une interface cellulaire.

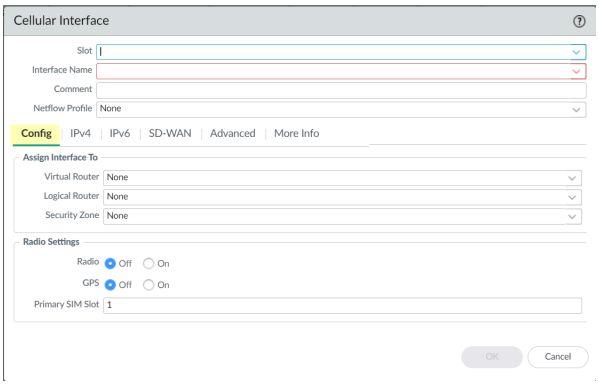
1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Cellular (Cellulaire)**.

   Pour Panorama, sélectionnez **Network (Réseau)**. Sélectionnez le modèle que vous souhaitez utiliser, puis sélectionnez **Interfaces** > **Cellular (Cellulaire)**. Vous pouvez ajouter une configuration pour un périphérique à l'aide d'un modèle, puis appliquer ce modèle à d'autres périphériques.
2. (Panorama uniquement) Sélectionnez le **Slot (Emplacement)**.

   Sélectionnez **Slot 1 (Emplacement 1)** pour un modèle sans châssis.
3. Sélectionnez le **Interface Name (Nom de l'interface)** que vous souhaitez utiliser.
4. (Facultatif) Saisissez un **Comment (Commentaire)** pour décrire l'interface.
5. Sélectionnez un **Netflow Profile (Profil Netflow)** ou créez un **New Netflow Profile (Nouveau profil Netflow)**.

©2024 Palo Alto Networks, Inc.

STEP 4 | Configurez la connexion 5G.



1. Dans l'onglet **Config**, sélectionnez le **Virtual Router (Routeur virtuel)** auquel vous souhaitez attribuer l'interface ou créez un **New Virtual Router (Nouveau routeur virtuel)**.
2. Sélectionnez le **Logical Router (Routeur logique)** auquel vous souhaitez attribuer l'interface ou créez un **New Logical Router (Nouveau routeur logique)**.
3. Sélectionnez la **Security Zone (Zone de sécurité)** ou créez une **New Zone (Nouvelle zone)**.
4. Sélectionnez le paramètre **Radio** du modem.

   Cette option vous permet de réinitialiser les paramètres de la radio lors du dépannage.

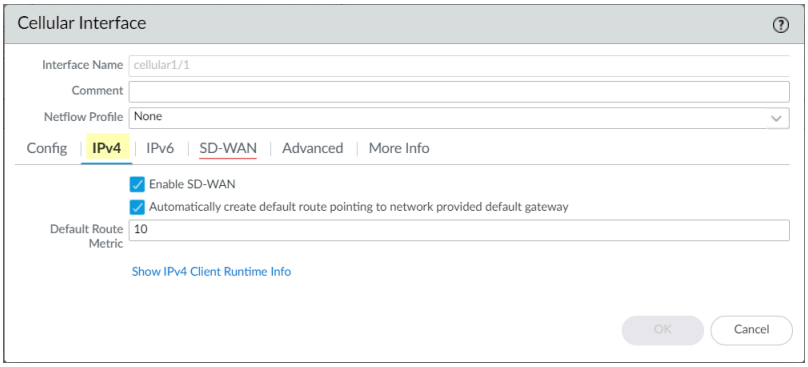
   *Pour activer l'option GPS, vous devez activer l'option **Radio** ainsi que l'option **GPS**.*

   - **Off (Désactivé)** : (Valeur par défaut) désactive le paramètre radio et l'interface cellulaire.
   - **On (Activé)** : active le réglage de la radio et l'interface cellulaire.
5. Sélectionnez le paramètre **GPS**.
   - **Off (Désactivé)** : (Valeur par défaut) désactive le paramètre GPS.
   - **On (Activé)** : active le paramètre GPS.
6. Sélectionnez le **Primary SIM Slot (Emplacement SIM principal)**.

   Par défaut, le pare-feu utilise la carte de l'emplacement 1 (`SIM1`) pour tenter de se connecter au réseau. Si vous configurez un deuxième emplacement SIM, le pare-feu tente automatiquement de se connecter au réseau à l'aide de la carte SIM secondaire si la connectivité à l'aide de la carte SIM principale échoue. Vous pouvez éventuellement configurer le deuxième emplacement (SIM2) comme **Primary SIM Slot (Emplacement SIM principal)**.

©2024 Palo Alto Networks, Inc.

STEP 5 | Configurez les paramètres IPv4.



1. (Facultatif) (PAN-OS 11.2.3 et versions ultérieures 11.2, plug-in SD-WAN 3.3.1 et versions ultérieures 3.3) Dans l'onglet **IPv4**, sélectionnez **Enable SD-WAN (Activer SD-WAN)** pour activer SD-WAN sur l'interface cellulaire. Les interfaces cellulaires compatibles SD-WAN sont automatiquement ajoutées en tant que membres DIA SD-WAN VIF ; et les tunnels sont créés et ajoutés automatiquement au VIF du tunnel SD-WAN. Les tunnels sont créés entre la branche 5G ou le périphérique hub 5G vers l'appareil homologue dont le nom d'interface se termine par « cellulaire ».

   Lorsque vous activez SD-WAN dans l'interface cellulaire, toutes les SD-WAN features (Fonctionnalités SD-WAN) seront prises en charge dans votre interface cellulaire.

   - *Deux interfaces cellulaires ne peuvent pas établir de tunnel SD-WAN.*
   - *La topologie maillée complète n'est pas prise en charge lorsque vous activez SD-WAN dans l'interface cellulaire.*
   - *Nous vous recommandons de configurer les pare-feu compatibles 5G uniquement en tant que périphérique de branche. Si vous n'avez pas activé la fonctionnalité SD-WAN sur un pare-feu, vous pouvez uniquement configurer ce pare-feu 4G/5G en tant que périphérique hub. Notez que vous ne pouvez avoir qu'un seul périphérique hub 4G/5G dans le cluster VPN.*
   - *Il n'existe aucune norme disponible pour les pings de passerelle entre les fournisseurs d'accès à Internet. Pour cette raison, le ping ICMP natif vers la passerelle n'est pas autorisé pour les interfaces cellulaires. Pour cette raison, nous vous recommandons de configurer un profil SaaS au lieu d'un profil ICMP.*

   Les pare-feu suivants prennent en charge la configuration SD-WAN dans l'interface cellulaire :

   - PA-415-5G
   - PA-450R-5G
   - PA-415R-5G
   - PA-455-5G
   - PA-455R-5G

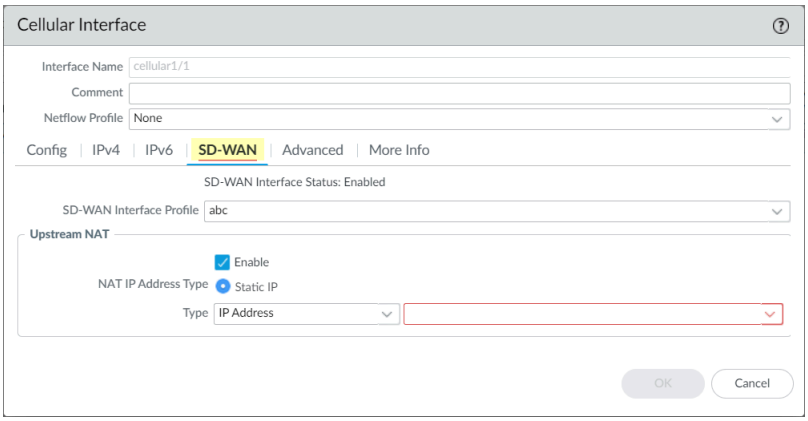
©2024 Palo Alto Networks, Inc.

2. Dans l'onglet **IPv4**, indiquez si vous souhaitez **créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le réseau**.

   Cette option est activée par défaut et crée un itinéraire par défaut vers la passerelle par défaut fournie par le réseau.
3. Spécifiez la **Default Route Metric (Métrique d'itinéraire par défaut)**.

   La valeur par défaut est 10 ; la plage se situe entre 1 et 65535.

STEP 6 | (Facultatif) (PAN-OS 11.2.3 et versions ultérieures 11.2, plug-in SD-WAN 3.3.1 et versions ultérieures 3.3) Configurez les paramètres SD-WAN.



Vous pouvez configurer les paramètres **SD-WAN** uniquement lorsque vous activez SD-WAN dans l'onglet **IPv4**.

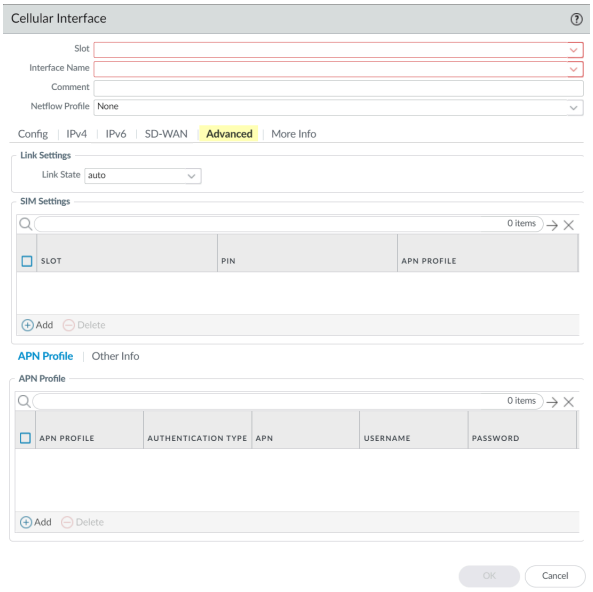
Si vous ajoutez une branche derrière un périphérique effectuant la NAT pour la branche, vous devez spécifier l'adresse IP ou le FQDN de l'interface orientée public sur ce périphérique en amont effectuant la NAT ou sélectionner DDNS pour indiquer que l'adresse IP de l'interface installée sur le périphérique NAT est obtenue auprès du service DDNS de Palo Alto Networks. Par conséquent, la configuration Auto VPN utilise cette adresse IP publique comme terminal du tunnel pour la branche. Il s'agit de l'adresse IP que l'IKE de la branche et les flux IPSec doivent pouvoir l'atteindre. (Vous devez avoir déjà configuré une interface Ethernet pour SD-WAN.)

1. Sélectionnez un profil d'interface SD-WAN déjà configuré ou créez un nouveau profil d'interface SD-WAN.
2. Dans l'onglet **Upstream NAT (NAT en amont)**, activez **Upstream NAT (NAT en amont)**.
3. Sous **NAT IP Address Type (Type d'adresse IP NAT)**, si vous sélectionnez **Static IP (IP statique)**, sélectionnez **IP Address (Adresse IP)** ou **FQDN**, puis saisissez l'adresse IPv4 sans masque de réseau secondaire (par exemple, 192.168.3.4) ou le FQDN du périphérique en amont, respectivement.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Dans l'onglet **Advanced (Avancé)**, sélectionnez le **Link State (État du lien)**.

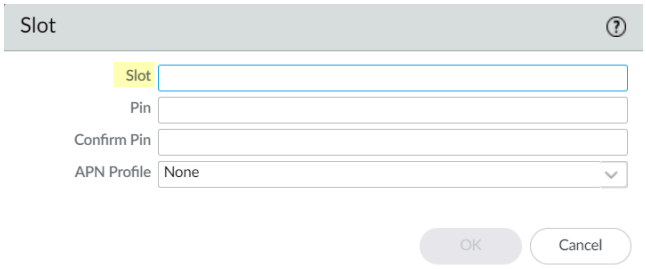
- **auto** : l'interface est disponible uniquement s'il existe une connexion homologue.
- **up** : l'interface est disponible.
- **down** : l'interface n'est pas disponible.



STEP 8 | Configurez les paramètres SIM.

1. **Ajoutez** les **SIM Settings (Paramètres SIM)**.
2. Spécifiez le **Slot (Emplacement)**.

   Un seul emplacement SIM peut être actif à la fois. Par défaut, `SIM1` est l'emplacement SIM actif. Le modem utilise cette carte SIM pour rechercher la connectivité réseau. Si le pare-feu ne parvient pas à établir une session dans les 5 minutes, il tente d'établir la session en utilisant l'autre emplacement SIM.



3. Pour exiger un code PIN afin d'empêcher toute utilisation non autorisée des emplacements SIM, saisissez un **Pin (Code PIN)**, puis cliquez sur **Confirm Pin (Confirmer le code PIN)**.

   Vous pouvez également exiger un code PIN pour accéder à la carte SIM ; pour plus d'informations, voir l'étape 17.

4. Sélectionnez le **APN Profile (Profil APN)**.

   Spécifiez le profil APN que vous souhaitez que la carte SIM utilise par défaut. L'emplacement SIM utilise ce profil APN, sauf si vous le remplacez par un profil APN

 ©2024 Palo Alto Networks, Inc.

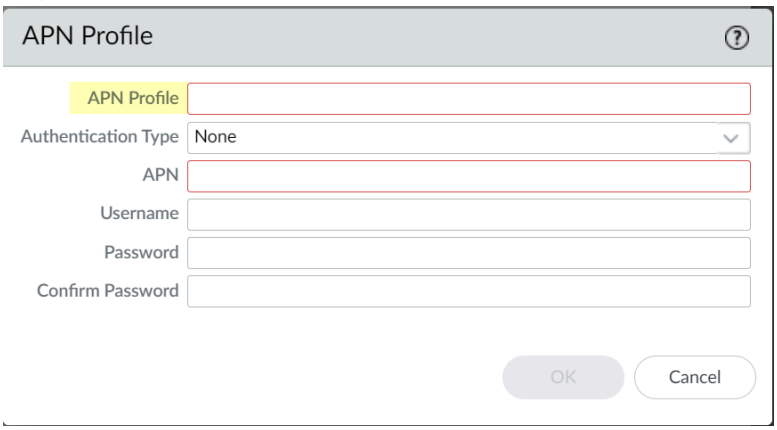
personnalisé. Si vous ne spécifiez pas de profil APN, le pare-feu utilise le profil APN `auto` par défaut. Si vous devez spécifier un profil APN personnalisé, vous pouvez le faire à l'étape 9.a

5. Cliquez sur **OK**.

STEP 9 | Définissez le **APN Profile (Profil APN)**.

1. **Ajoutez** le **APN Profile (Profil APN)** par défaut.

   Si nécessaire, remplacez le profil APN par défaut pour l'emplacement spécifié en sélectionnant un profil APN.

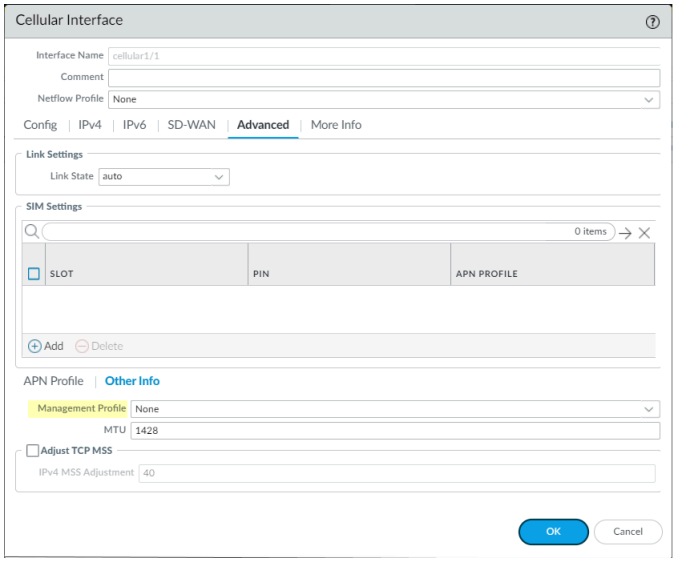


2. Sélectionnez le **Authentication Type (Type d'authentification)** pour la connexion à l'APN.
   - **None** :(Par défaut) le pare-feu ne nécessite pas d'authentification pour la connexion à l'APN.
   - **CHAP** : utilisez le protocole CHAP (Challenge Handshake Authentication Protocol) pour vous connecter à l'APN.
   - **PAP** : utilisez le protocole d'authentification par mot de passe (PAP) pour vous connecter à l'APN.
   - **auto** : autorisez le pare-feu à détecter automatiquement le type d'authentification en fonction du fournisseur de services. Si la connexion au type d'authentification initial échoue, le pare-feu tente la connexion avec l'autre type d'authentification.
3. Entrez l'**APN**.
4. Entrez le **Username (Nom d'utilisateur)**.
5. Entrez le **Password (Mot de passe)** puis cliquez sur **Confirm Password (Confirmer le mot de passe)**.
6. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 10 | Configurez des informations supplémentaires, telles que les unités de transmission maximales (MTU), en fonction des exigences de votre réseau.

1. Sélectionnez l'onglet **Other Info (Autres informations)**.
2. Sélectionnez un **Management Profile (Profil de gestion)**.



3. Spécifiez la **MTU** en octets.

   La valeur par défaut est 1 428 octets ; la plage est comprise entre 576 et 1 500 octets.
4. Si vous souhaitez ajuster la taille du paquet en raison de la latence, vous pouvez **Adjust TCP MSS (Ajuster TCP MSS)** pour configurer la taille maximale du segment et spécifier la valeur **IPv4 MSS Adjustment (Ajustement IPv4 MSS)**.

   La valeur par défaut est 40 ; la plage se situe entre 40 et 300.
5. Cliquez sur **OK**.

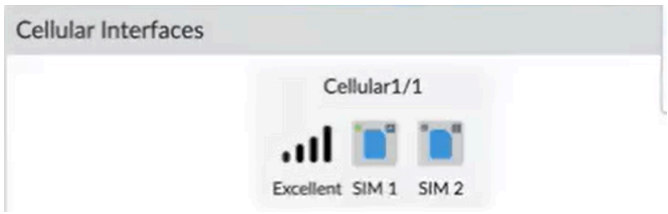
STEP 11 | **Commit (Validez)** vos modifications.

Vous devez valider vos modifications, vous assurer que l'interface est activée et que la connectivité est réussie avant que les informations suivantes soient disponibles sur le pare-feu ou Panorama.

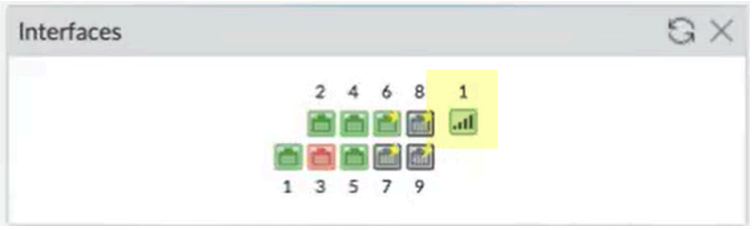
 ©2024 Palo Alto Networks, Inc.

STEP 12 | Utilisez des widgets pour surveiller votre interface cellulaire.

1. Sélectionnez **Dashboard (Tableau de bord)** > **Widgets** > **System (Système)** > **Cellular Interfaces (Interfaces cellulaires)**.
2. Affichez des informations sur l'interface cellulaire, telles que la force du signal. Pour afficher plus d'informations, survolez l'icône.



3. Sélectionnez **Dashboard (Tableau de bord)** > **Widgets** > **System (Système)** > **Interfaces**.
   L'interface cellulaire ainsi que vos autres interfaces configurées s'affichent dans le widget. Pour afficher plus d'informations, survolez l'icône.

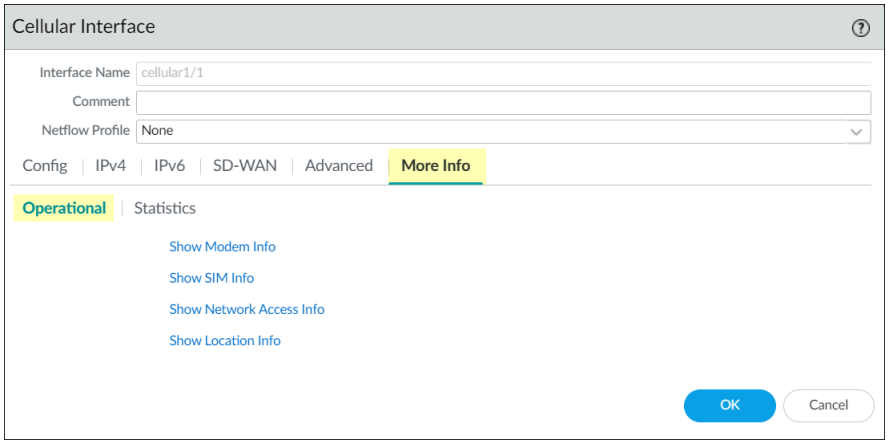


©2024 Palo Alto Networks, Inc.

STEP 13 | Vérifiez que les informations opérationnelles de votre configuration sont correctes.

Pour afficher les statistiques et les informations opérationnelles à l'aide de Panorama, sélectionnez d'abord le périphérique, puis sélectionnez les informations que vous souhaitez afficher.

1. Sélectionnez l'interface cellulaire que vous avez configurée puis cliquez sur **More Info (Plus d'informations)** > **Operational (Opérationnelles)**.



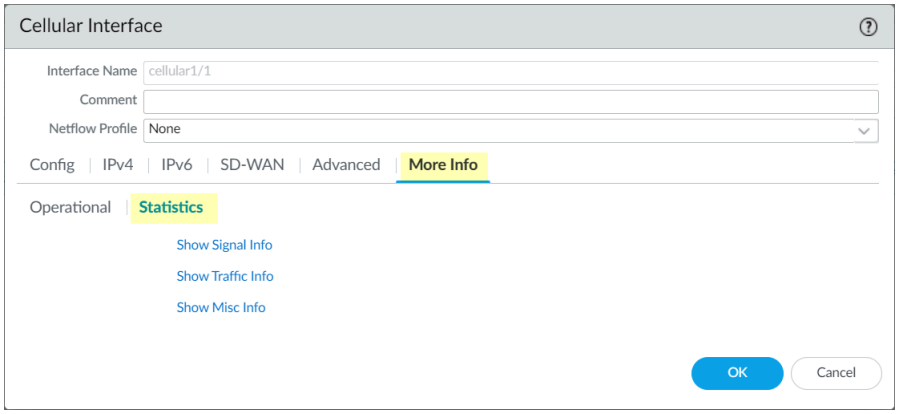
2. Sélectionnez **Show Modem Info (Afficher les informations du modem)** pour vérifier les informations du modem (telles que IMEI et FSN).
3. Sélectionnez **Show SIM Info (Afficher les informations SIM)** pour vérifier les informations SIM, telles que le nombre de cartes SIM et leurs numéros IMSI.
4. Sélectionnez **Show Network Access Info (Afficher les informations d'accès au réseau)** pour vérifier les informations d'accès au réseau (par exemple, la bande de fréquence et l'ID de cellule).
5. Sélectionnez **Show Location Info (Afficher les informations de localisation)** pour vérifier les informations GPS, telles que l'état, la latitude et la longitude.

   Vous devez activer le GPS pour afficher ces informations.

©2024 Palo Alto Networks, Inc.

STEP 14 | Affichez des informations sur l'activité sur l'interface cellulaire.

1. Sélectionnez l'interface cellulaire que vous avez configurée puis cliquez sur **More Info (Plus d'informations)** > **Statistics (Statistiques)**.

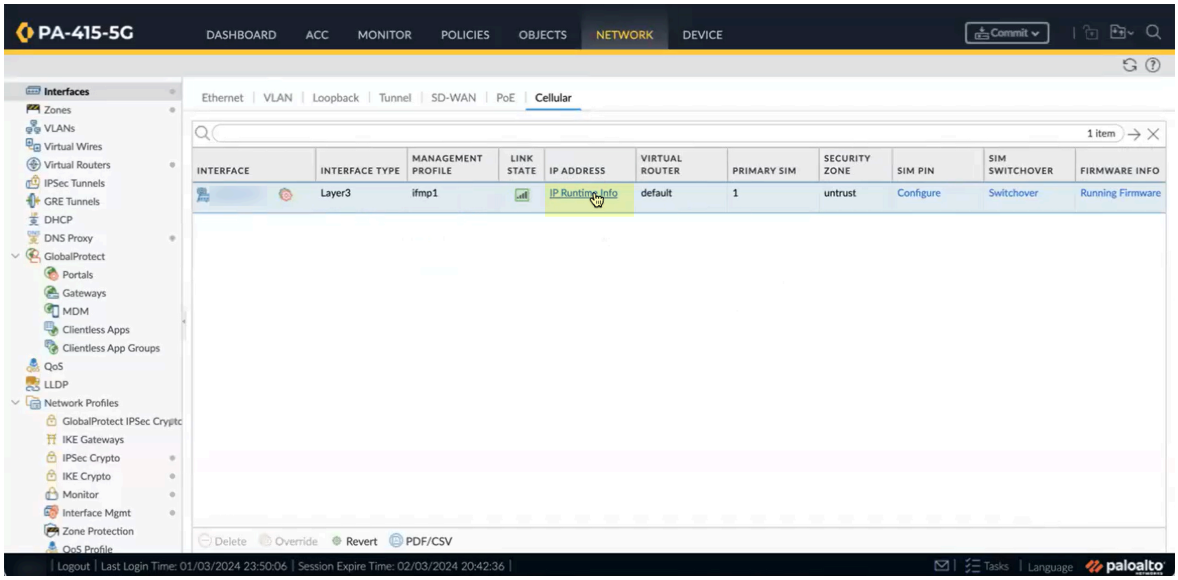


2. Sélectionnez **Show Signal Info (Afficher les informations sur le signal)** pour afficher les informations sur le signal (telles que RSSI et RSRP).
3. Sélectionnez **Show Traffic Info (Afficher les informations de trafic)** pour afficher les informations de trafic, telles que les octets, les abandons, les erreurs et les débordements pour la réception et la transmission.
4. Sélectionnez **Show Misc Info (Afficher les informations diverses)** pour afficher d'autres informations, notamment le nombre de réinitialisations du modem et de la radio, les permutations et les déconnexions du réseau.

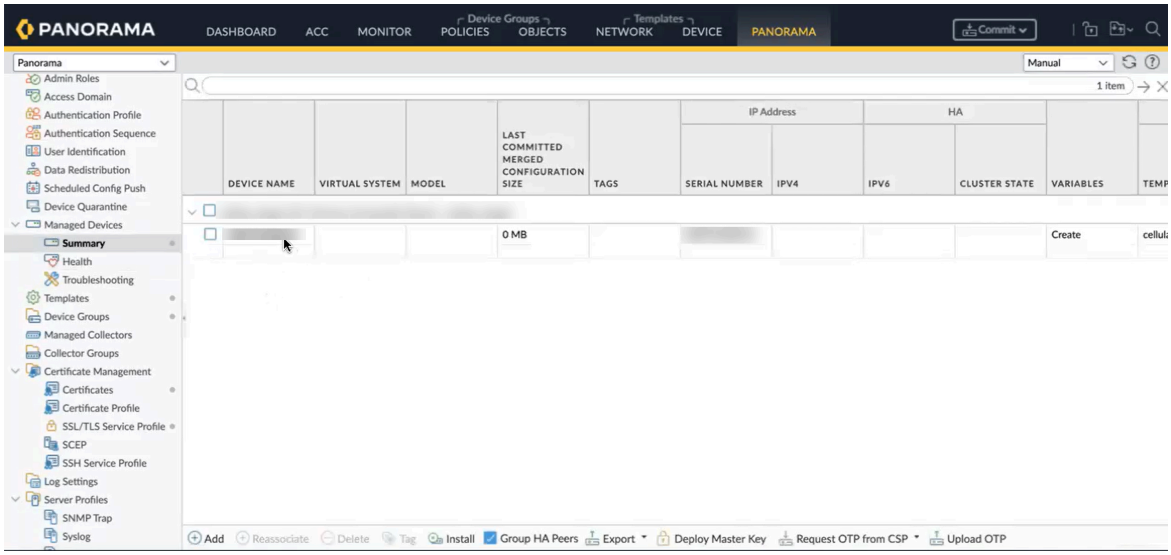
©2024 Palo Alto Networks, Inc.

STEP 15 | Surveillez les informations sur la session en cours sur l'interface cellulaire.

1. Sélectionnez les **IP runtime info (Informations sur l'exécution IP)** pour l'interface cellulaire.



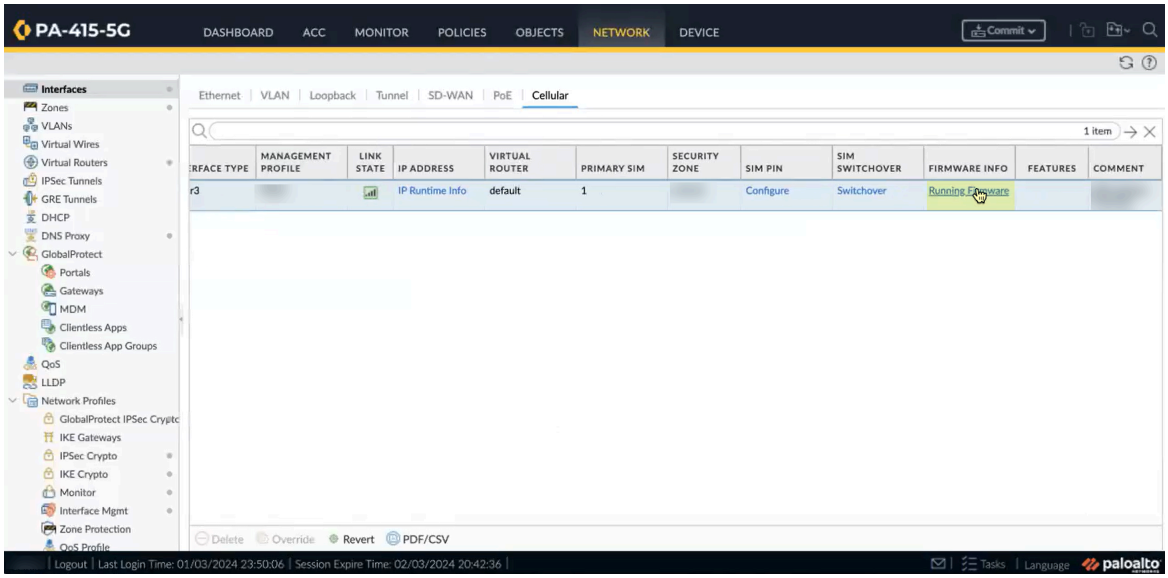
2. Affichez les **Data Session Details (Détails de la session de données)** tels que l'adresse IP, les informations sur la passerelle et les interfaces DNS primaires et secondaires.
3. (Panorama uniquement) Si vous utilisez Panorama, vous pouvez afficher l'interface cellulaire en sélectionnant **Panorama** > **Managed Devices (Appareils gérés)Summary (Résumé)**.



 ©2024 Palo Alto Networks, Inc.

STEP 16 | Affichez les informations du micrologiciel de l'interface.

1. Sélectionnez le **Running Firmware (Micrologiciel en cours d'exécution)** pour l'interface cellulaire.



2. Affichez les **Firmware Details (Détails du micrologiciel)**, notamment la version actuelle, la version de l'interface à débit primaire (PRI) et une liste des PRI avec leurs versions de micrologiciel, versions PRI et opérateurs respectifs.

STEP 17 | (Recommandé) Pour plus de sécurité, activez un code PIN pour votre carte SIM.

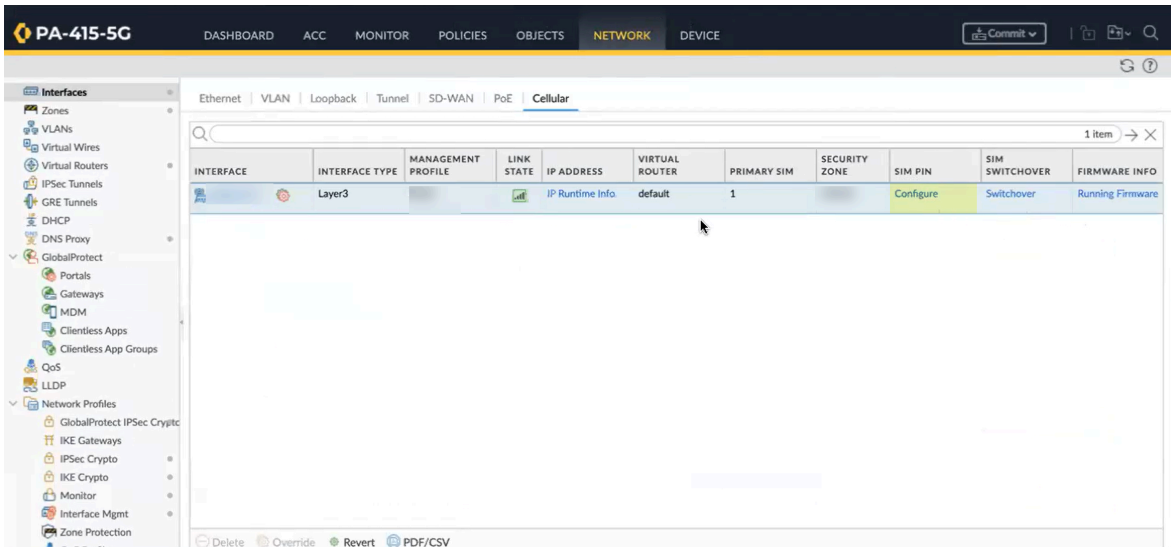
Le code PIN SIM empêche toute utilisation non autorisée des cartes SIM. Si vous activez un code PIN SIM, la carte SIM vous demande de saisir le code PIN pour déverrouiller la carte SIM afin que le modem puisse accéder au réseau cellulaire et démarrer des sessions de données.

Après trois tentatives infructueuses de déverrouillage de la carte SIM, la carte SIM est inaccessible jusqu'à ce que vous saisissiez une clé de déblocage personnelle (PUK). Lorsque la

 ©2024 Palo Alto Networks, Inc.

carte SIM active est inaccessible, un basculement automatique vers une SIM secondaire, le cas échéant, se produit. Pour plus d'informations, voir l'étape 18.

1. **Configure (Configurez)** un **SIM PIN (Code PIN SIM)**.



2. Assurez-vous de **Enable (Activer)** le code PIN comme **SIM PIN Operation (Opération du code PIN SIM)**.
3. Sélectionnez le **SIM Slot (Emplacement SIM)** contenant la carte SIM sur laquelle vous souhaitez activer le code PIN.
4. Entrez le **PIN (Code PIN)** et cliquez sur **Configure (Configurer)**.

STEP 18 | Si vous avez activé le code PIN SIM, gérez les opérations du code PIN SIM.

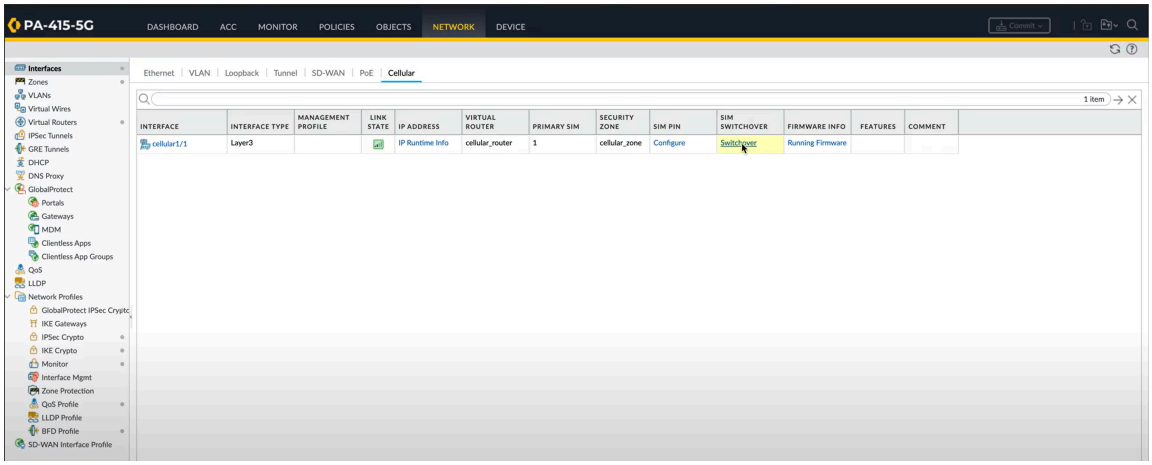
Vous devez activer un code PIN SIM avant de pouvoir configurer un nouveau code PIN, désactiver le code PIN ou débloquer le code PIN.

- Pour désactiver le code PIN SIM, sélectionnez **Disable (Désactiver)** comme **SIM PIN Operation (Opération du code PIN SIM)**, confirmez le **SIM Slot (Emplacement SIM)**, entrez le **PIN (Code PIN)** et cliquez sur **Configure (Configurer)**.
- Pour configurer un nouveau code PIN, sélectionnez **Change (Modifier)** comme **SIM PIN Operation (Opération du code PIN SIM)**, confirmez le **SIM Slot (Emplacement SIM)**, entrez le **PIN (Code PIN)** et le **New PIN (Nouveau code PIN)**, puis cliquez sur **Configure (Configurer)**.
- Pour débloquer un code PIN, sélectionnez **Unblock (Débloquer)** comme **SIM PIN Operation (Opération PIN SIM)**, confirmez le **SIM Slot (Emplacement SIM)**, entrez le **New PIN (Nouveau code PIN)** et la clé de déblocage personnelle (**PUK**), puis cliquez sur **Configure (Configurer)**.

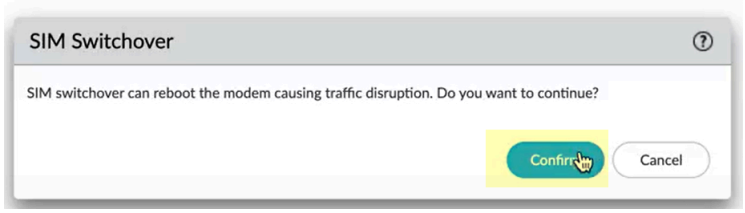
©2024 Palo Alto Networks, Inc.

STEP 19 | Pour passer de la carte SIM active à une autre carte SIM, procédez comme suit.

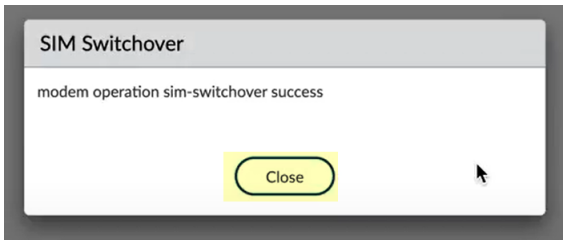
1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Cellular (Cellulaire)**.
2. Cliquez sur **Switchover (Commutation)**.



3. **Confirmez** que vous souhaitez changer de carte SIM actuelle.



4. **Fermez** la fenêtre de notification qui s'affiche pour confirmer le changement de carte SIM.



5. Une fois le changement de carte SIM terminé (environ 40 à 60 secondes), vérifiez le changement à l'aide du widget Dashboard (Tableau de bord) (voir l'étape 12.c).

 ©2024 Palo Alto Networks, Inc.

Mise à niveau du microprogramme 5G

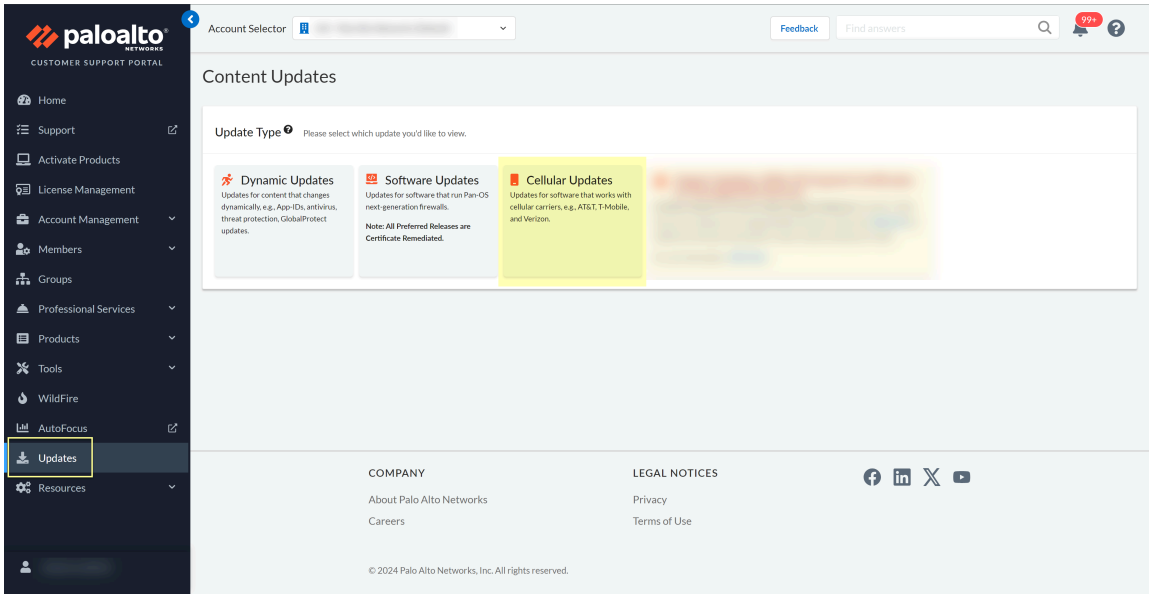
Si vous avez configuré une interface 5G et que vous souhaitez mettre à niveau le microprogramme pour un opérateur sans fil spécifique, suivez les étapes ci-dessous pour télécharger et installer les mises à jour sur le pare-feu.

La mise à jour du microprogramme est une étape clé pour garantir que vous bénéficiez des dernières fonctionnalités et de l'assistance, et que votre réseau et vos utilisateurs sont protégés contre les activités malveillantes.

©2024 Palo Alto Networks, Inc.

STEP 1 | Téléchargez les mises à jour du microprogramme à partir du portail de support client.

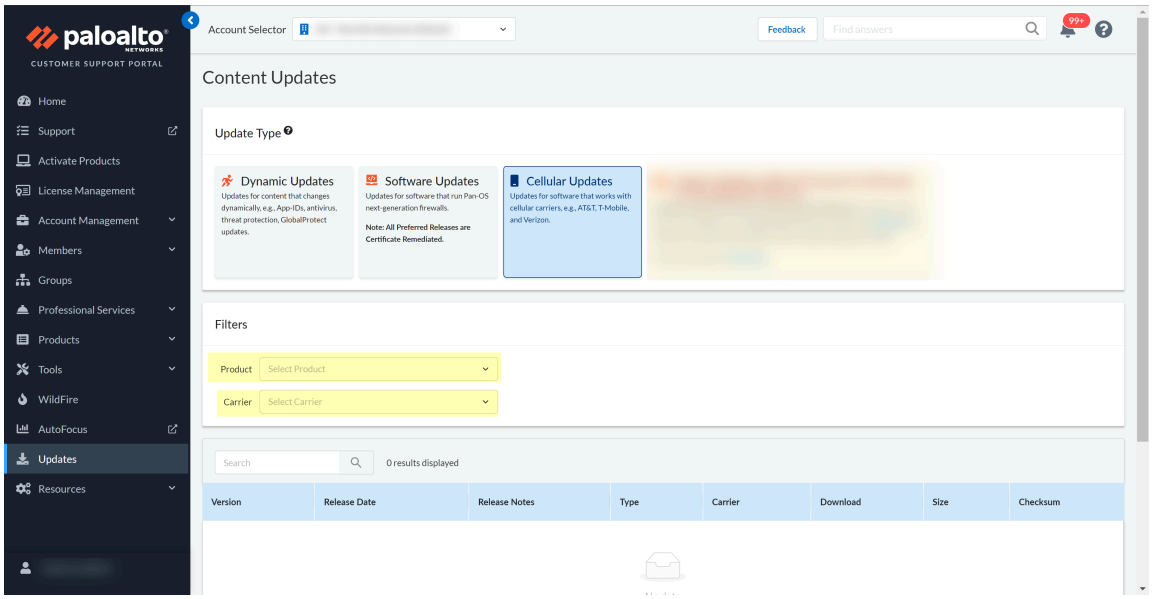
1. Ouvrez une session dans le portail de support client.
2. Sélectionnez **Updates (Mises à jour)** > **Cellular Updates (Mises à jour cellulaires)**.



3. Sélectionnez le **Product (Produit)** et le **Carrier (Transporteur)** que vous souhaitez mettre à jour.
   Vous devez sélectionner les deux pour afficher les mises à jour disponibles.

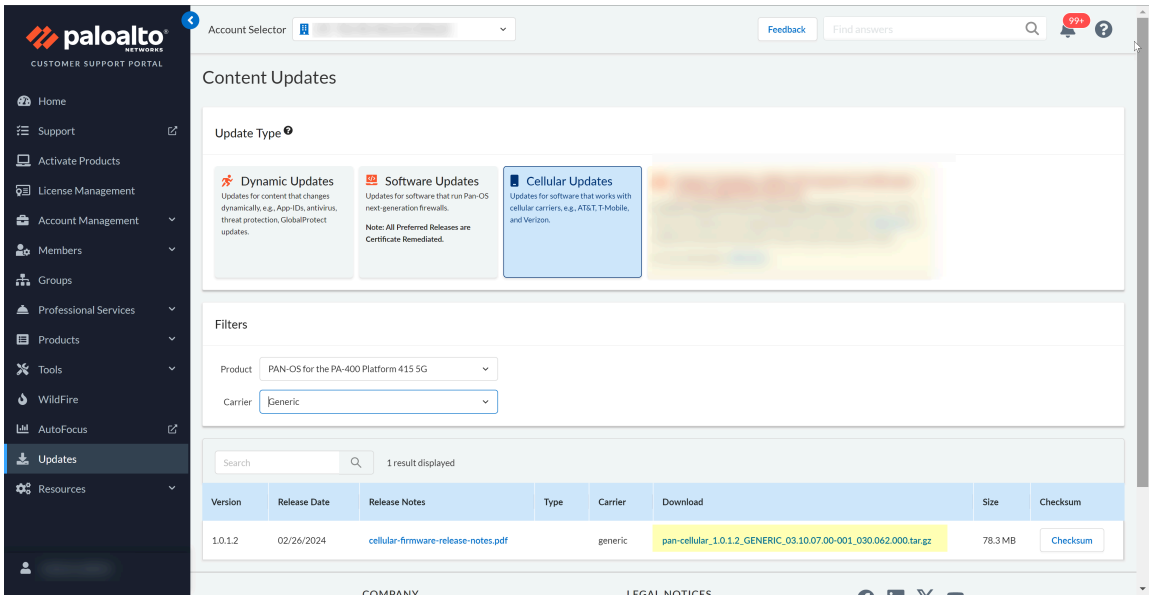
   Le microprogramme disponible diffère selon l'opérateur sans fil spécifié.

 ©2024 Palo Alto Networks, Inc.



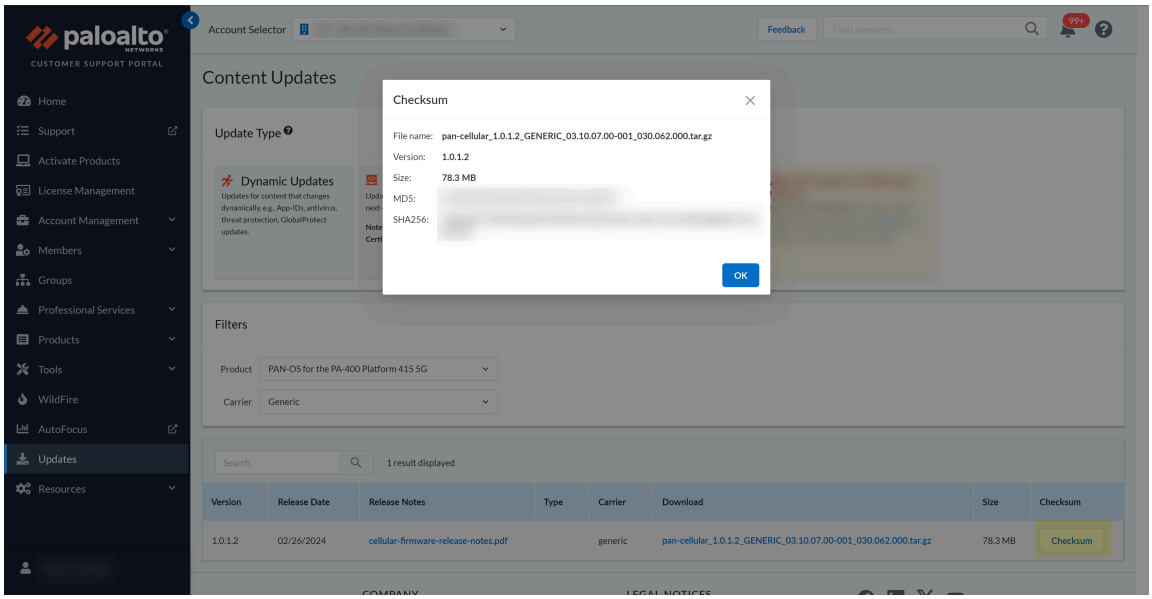
4. **Download (Téléchargez)** les mises à jour du microprogramme que vous souhaitez installer sur le pare-feu.

 ©2024 Palo Alto Networks, Inc.



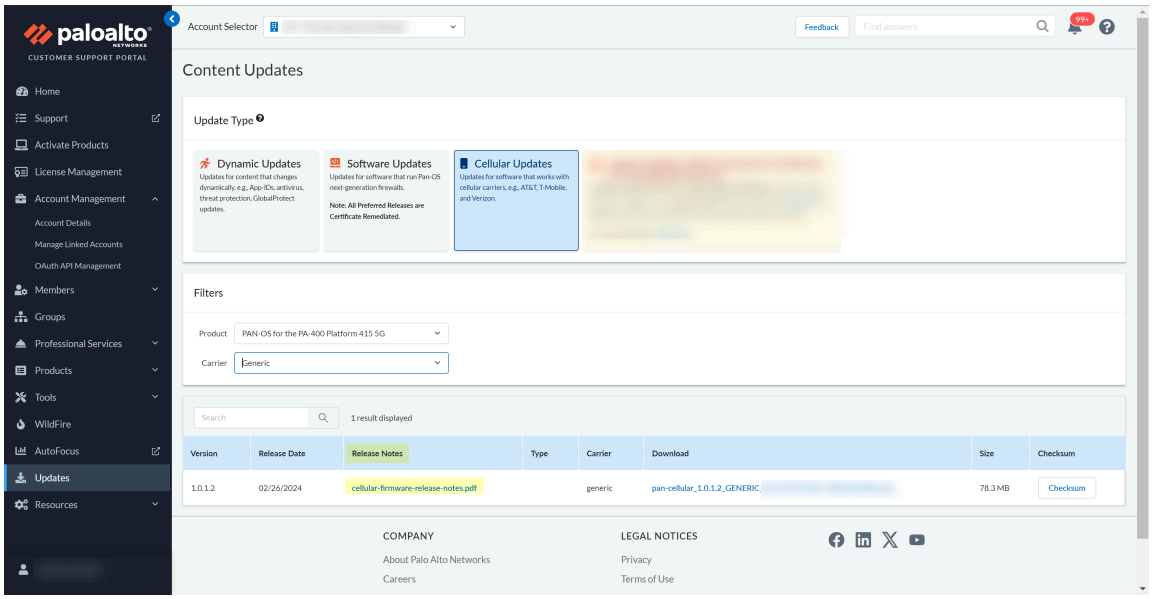
5. (Facultatif) Cliquez sur **Checksum (Somme de contrôle)** pour afficher plus d'informations sur la mise à jour.

 ©2024 Palo Alto Networks, Inc.



6. (Facultatif) Lisez les **Release Notes (Notes de version)** pour en savoir plus sur la mise à jour.

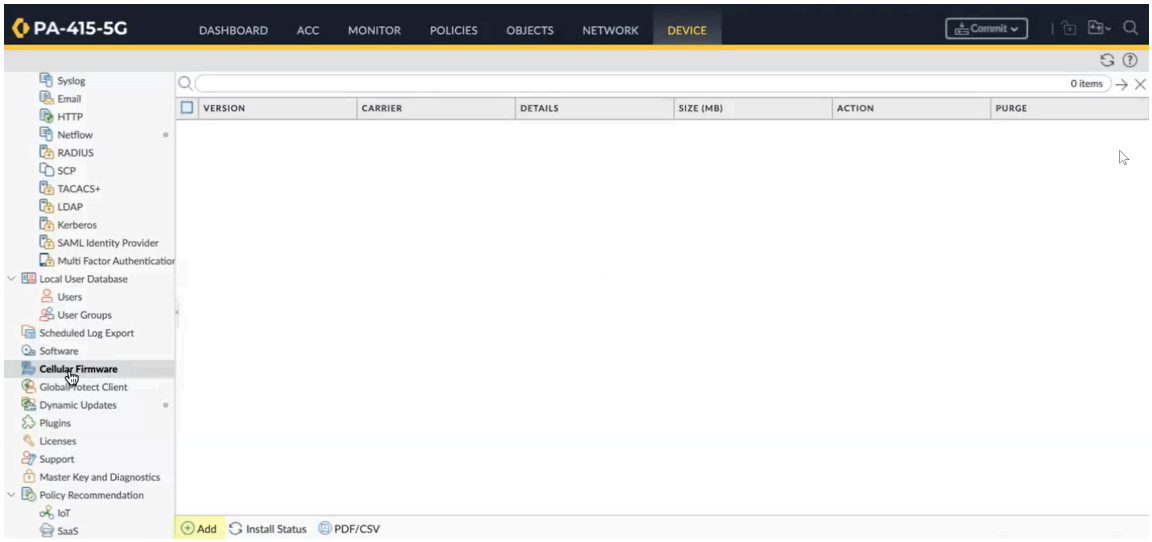
 ©2024 Palo Alto Networks, Inc.



©2024 Palo Alto Networks, Inc.

STEP 2 | Installez les mises à jour du microprogramme sur le pare-feu.

1. Sur le pare-feu, sélectionnez **Device (Périphérique)** > **Cellular Firmware (Microprogramme cellulaire)**.
2. **Add (Ajoutez)** le nouveau microprogramme.

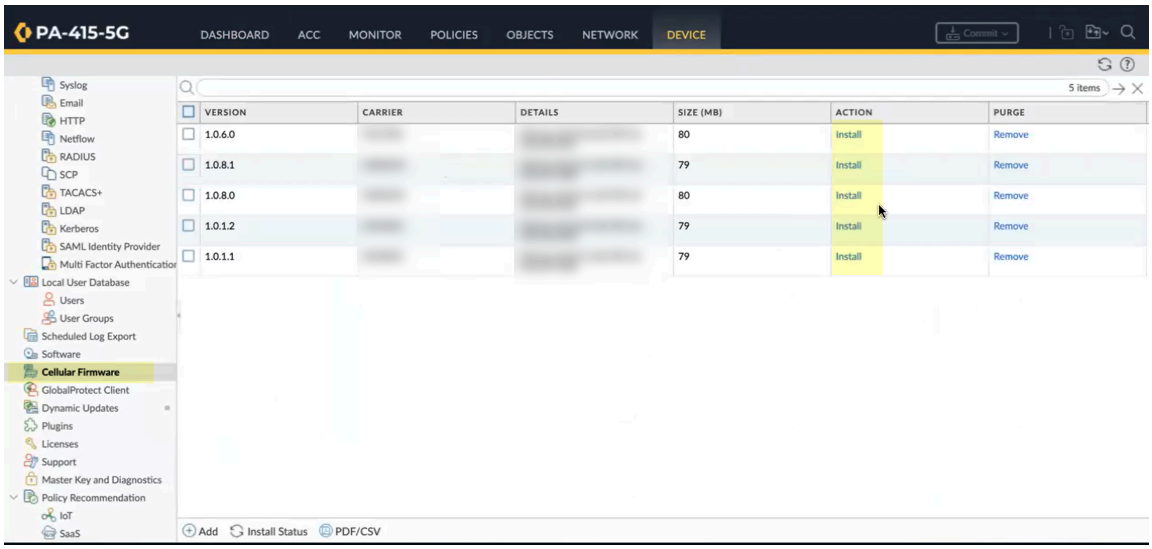


3. **Browse (Accédez)** à l'emplacement du microprogramme que vous avez téléchargé à partir du portail de support client, sélectionnez la mise à jour, puis cliquez sur **OK** pour confirmer votre sélection.



4. **Install (Installez)** le nouveau microprogramme.

 ©2024 Palo Alto Networks, Inc.



5. **Confirm (Confirmez)** que vous souhaitez installer le nouveau microprogramme.

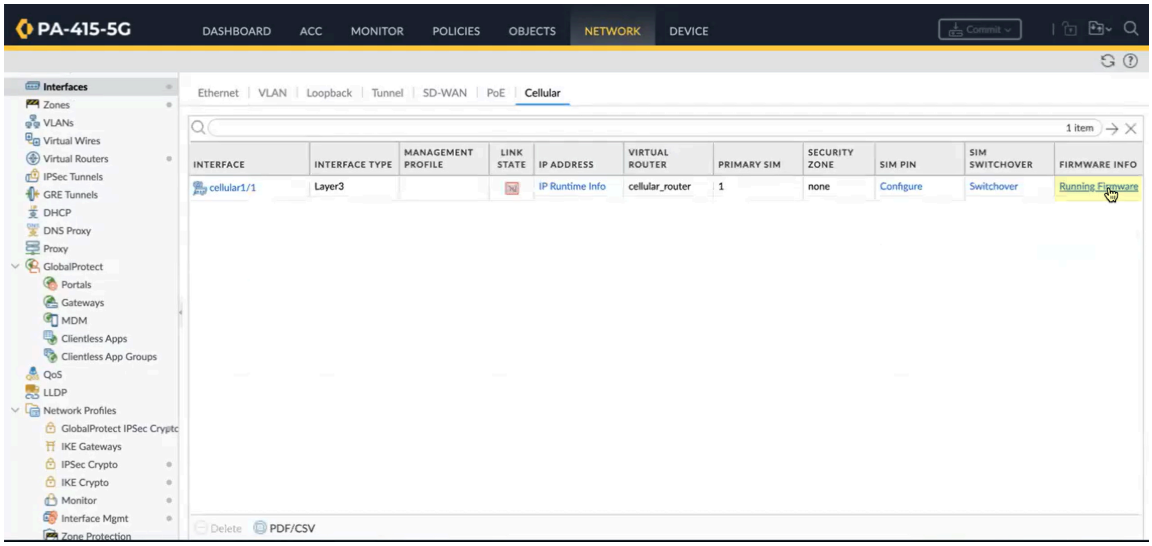


Le pare-feu installe le nouveau microprogramme sur les périphériques concernés lorsque vous validez. Une fois la mise à niveau du microprogramme terminée, les périphériques utilisent le nouveau microprogramme pour ce transporteur particulier comme version actuelle.

©2024 Palo Alto Networks, Inc.

STEP 3 | Vérifiez que la mise à jour du microprogramme est réussie.

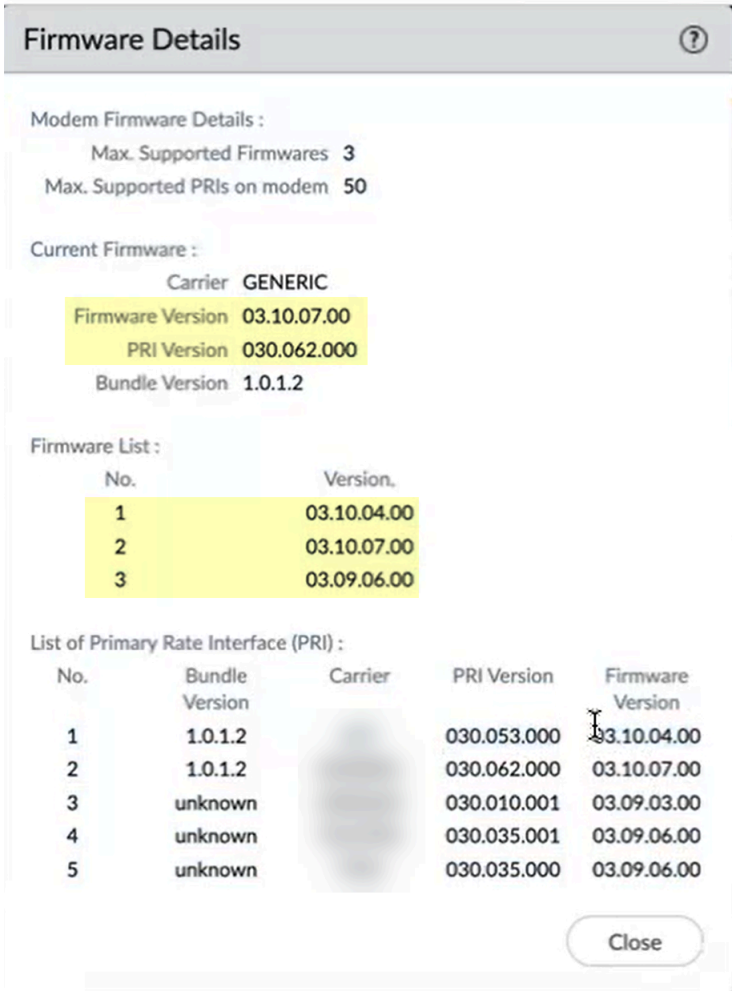
1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Cellular (Cellulaire)**.
2. Cliquez sur **Running Firmware (Exécution du microprogramme)** dans la colonne **Firmware Info (Informations sur le microprogramme)**.



3. Vérifiez que le nouveau microprogramme s'affiche dans la **Firmware List (Liste des microprogrammes)** et est le **Current Firmware (Microprogramme actuel)** pour la

 ©2024 Palo Alto Networks, Inc.

Firmware Version (Version du microprogramme) et la **PRI Version (Version PRI)** pour l'opérateur sans fil spécifié.



 ©2024 Palo Alto Networks, Inc.

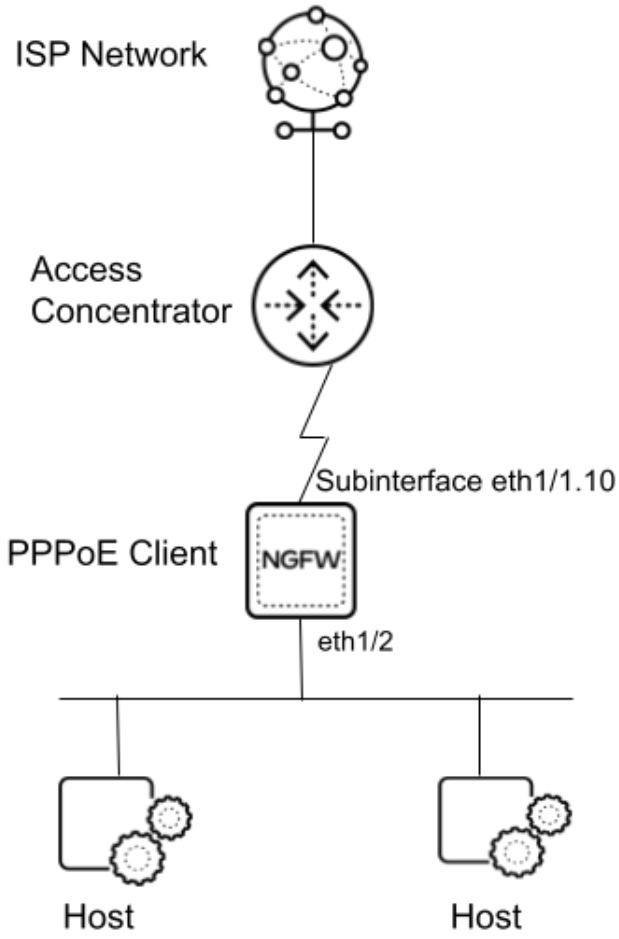
Configurer un client PPPoE sur une sous-interface

À partir de PAN-OS 11.0.1, vous pouvez configurer un client PPPoE (Point-to-Point Protocol over Ethernet) sur une sous-interface de couche 3 lorsque votre FAI indique que PPPoE sur VLAN 802.1Q est le moyen de se connecter à ses services Internet. Le pare-feu établit une connexion PPPoE au FAI à l'aide d'une balise VLAN 802.1Q. Le client PPPoE que vous configurez sur la sous-interface apprend son adresse IPv4 auprès du fournisseur de services Internet, ainsi que d'autres informations telles que l'adresse IP du serveur, les informations DNS et la MTU.

La sous-interface prend en charge une adresse IPv4. Vous pouvez configurer un client PPPOE sur une interface physique ou une sous-interface, mais pas les deux en même temps. Une seule sous-interface PPPoE est prise en charge sur une interface physique. Avant de commencer à configurer un client PPPoE, demandez à votre fournisseur de services Internet quelle balise VLAN utiliser pour votre connexion. Vous devez entrer cette balise lorsque vous configurez le numéro de sous-interface et la **Tag (balise)**. La tâche ci-dessous suppose que vous avez déjà configuré une interface Ethernet de couche 3 sur le pare-feu avec une zone de sécurité.

L'exemple de topologie suivant dispose d'une connexion PPPoE entre le pare-feu et le concentrateur d'accès.

©2024 Palo Alto Networks, Inc.

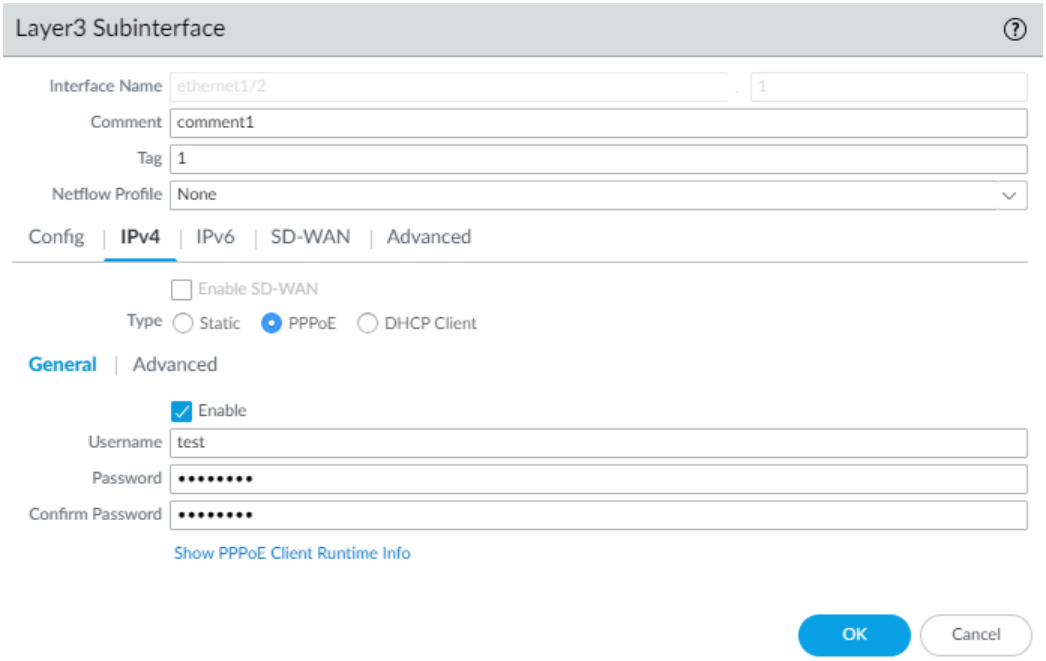


Le pare-feu encapsule le trafic en direction du nord (un paquet PPPoE) d'un hôte dans une trame 802.1Q et l'envoie à l'extrémité opposée de la liaison PPPoE, en route vers le réseau ISP. De même, le pare-feu décapsule le trafic en direction du sud de la trame 802.1Q avant d'envoyer le paquet PPPoE à l'hôte.

©2024 Palo Alto Networks, Inc.

STEP 1 | Configurez une sous-interface en tant que client PPPoE (point de terminaison).

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et mettez en surbrillance une interface Ethernet de couche 3.
2. **Add Subinterface (Ajoutez une Sous-interface)**.
3. À droite du point et du **Interface Name (nom de l'interface)** entrez le numéro de sous-interface ; utilisez le numéro de balise VLAN fourni par votre FAI. Ce numéro de sous-interface est fourni à titre de référence; l'ID de balise VLAN est lu dans le champ Balise.
4. Entrez la **Tag (balise)**, qui est le numéro de balise VLAN fourni par votre FAI. L'ID de balise VLAN réel est lu à partir de ce champ Balise.
5. Sélectionnez **IPv4**.
6. Sélectionnez le **Type** d'adresse **PPPoE**.
7. Sélectionnez **General (Généralités)** et **Enable (Activer)** la sous-interface.
8. Entrez le **Username (nom d'utilisateur)** pour l'authentification que vous choisirez à l'étape suivante.
9. Saisissez le **Password (Mot de passe)** et **Confirm Password (Confirmez le mot de passe)**.



©2024 Palo Alto Networks, Inc.

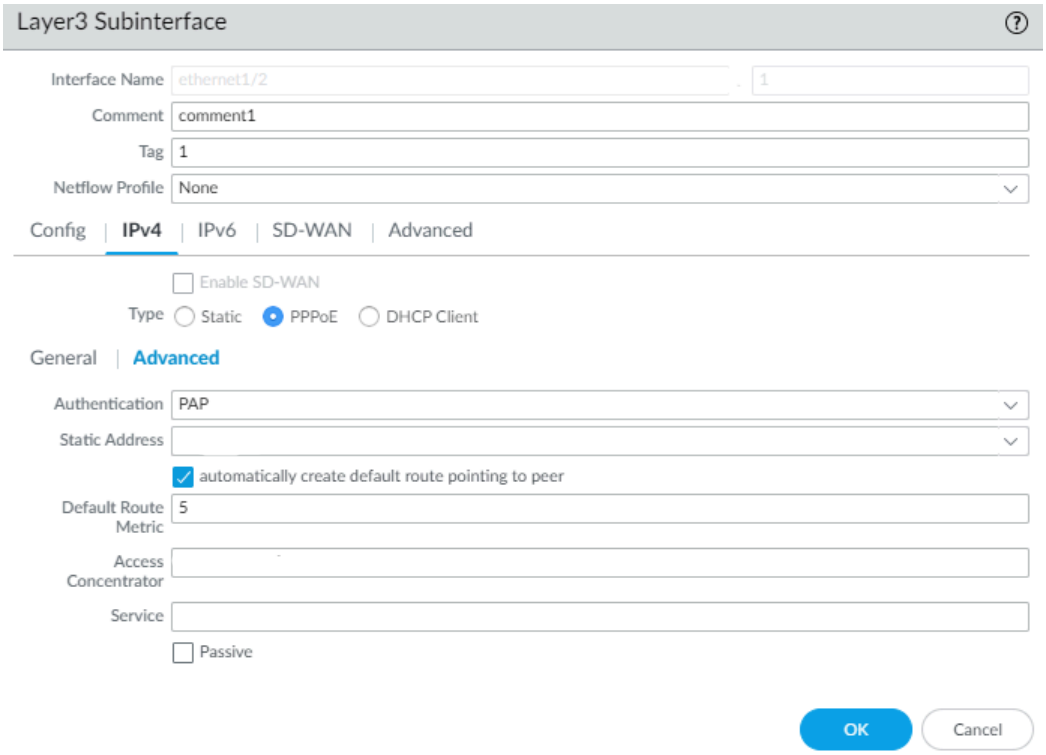
STEP 2 | Configurez des caractéristiques supplémentaires de la sous-interface PPPoE.

1. Sélectionnez **Advanced (Avancé)**.
2. Sélectionnez le type de**Authentication (authentification)** :
   - **None (Aucun)** : (par défaut) Si vous conservez ce paramètre, le pare-feu sélectionne **auto** comme protocole d'authentification.
   - **CHAP** : le pare-feu utilise le protocole CHAP (Challenge Handshake Authentication Protocol).
   - **PAP** : le pare-feu utilise le protocole PAP(Password Authentication Protocol). Le PAP envoie les noms d'utilisateur et les mots de passe en texte brut et est moins sécuritaire que le CHAP.
   - **auto** - Le pare-feu négocie la méthode d'authentification (CHAP ou PAP) avec le serveur PPPoE.
3. Pour demander au serveur PPPoE d'attribuer une certaine adresse IPv4 à la sous-interface, spécifiez une **Static Address (adresse statique)**. (Le serveur PPPoE peut attribuer l'adresse demandée ou une adresse différente à sa discrétion.) Valeur par défaut : **Aucune**.
4. Pour créer automatiquement un itinéraire par défaut qui pointe vers la passerelle par défaut fournie par le serveur PPPoE, sélectionnez **Automatically create default route pointing to peer (Créer automatiquement un itinéraire par défaut pointant vers l'homologue)**.
5. Entrez la **Default Route Metric (métrique de routage par défaut)** (niveau de priorité) de la connexion PPPoE ; plage comprise entre 1 et 65 535 ; valeur par défaut 10. Plus la valeur de l'itinéraire est faible, plus sa priorité de sélection est élevée. Par exemple, un

 ©2024 Palo Alto Networks, Inc.

itinéraire avec une valeur de mesure de 10 est utilisé avant un itinéraire avec une valeur de mesure de 100.

6. Entrez le nom du **Access Concentrator (concentrateur d'accès)** fourni par votre fournisseur de services Internet, le cas échéant (valeur de chaîne de 0 à 255 caractères). Le pare-feu se connectera à ce concentrateur d'accès du côté de l'IPS.
7. Entrez le **Service** fourni par votre fournisseur de services Internet, le cas échéant (valeur de chaîne de 0 à 255 caractères).
8. Si vous souhaitez que le client PPPoE (pare-feu) attende que le serveur PPPoE établisse une connexion, sélectionnez **Passive (Passif)**. Si l'option Passif n'est pas sélectionnée, le pare-feu est autorisé à établir une connexion.



STEP 3 | Cliquez sur **OK**.

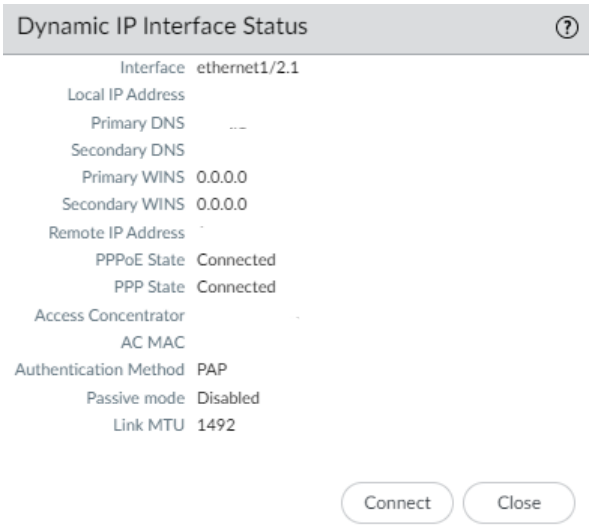
STEP 4 | **Commit (Validez)** les modifications.

©2024 Palo Alto Networks, Inc.

STEP 5 | Afficher des informations sur le client PPPoE. L'adresse IP locale, le DNS principal, le DNS secondaire, le WINS principal, le WINS secondaire, l'adresse IP distante, le nom du concentrateur d'accès et l'adresse MAC AC ont été reçus du serveur PPPoE.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et dans la ligne de la sous-interface que vous avez configurée, sélectionnez **Dynamic-PPPoE (PPPoE dynamique)**.

   *Vous pouvez également sélectionner la sous-interface, **IPv4**, et **Show PPPoE Client Runtime Info (Afficher les informations d'exécution du client PPPoE)**.*



2. **Close (Fermez)** la fenêtre.

 ©2024 Palo Alto Networks, Inc.

Configurer un client PPPoE IPv6

Le pare-feu prend en charge une interface ou sous-interface Ethernet de couche 3 agissant comme un client IPv6 de protocole PPPoE pour atteindre un ISP qui fournit des services Internet IPv6. En mode PPPoE, l'interface ou la sous-interface peut obtenir une adresse IPv6 de manière dynamique à l'aide de DHCPv6 en mode avec ou sans état. En mode avec état, l'interface PPPoE acquiert dynamiquement tous les paramètres de connexion du serveur DHCPv6. En mode sans état, l'adresse IPv6 de l'interface PPPoE est obtenue via la configuration automatique d'adresse sans état (SLAAC), mais les autres paramètres (DNS et délégation de préfixe) sont obtenus via DHCPv6. DHCPv6 avec et sans état réduit les efforts et les erreurs de provisionnement et simplifie la gestion des adresses.

Utilisez DHCPv6 avec état pour attribuer l'adresse client PPPoEv6, car elle est plus sécurisée que la configuration automatique sans état.

Seules les interfaces et sous-interfaces Ethernet de couche 3 prennent en charge un client PPPoE IPv6 (les interfaces tunnel, AE, VLAN et en boucle ne prennent pas en charge un client PPPoE IPv6). Une interface de couche 3 et sa sous-interface ne peuvent pas agir simultanément comme client PPPoEv6.

Une limitation est que l'interface configurée avec PPPoEv6 ne peut pas acquérir une adresse de serveur DNS et/ou un préfixe DNS à partir des annonces de routeur (RA-DNS). Vous devrez compter sur DHCPv6 pour obtenir les informations DNS ou configurer ces paramètres manuellement.

Une fois configurée pour PPPoE, une interface ne peut pas se voir attribuer une adresse IP statique.

Si vous configurez uniquement un client PPPoE à pile unique (IPv4 ou IPv6), vous ne pouvez pas utiliser la connectivité client PPPoE IPv4 et IPv6. Si vous configurez un client PPPoEv4 et vous connectez à un ISP, vous pouvez utiliser uniquement la connectivité IPv4. Si vous configurez un client PPPoEv6 et vous connectez à un ISP, vous pouvez utiliser uniquement la connectivité IPv6. (Si vous configurez un client PPPoE v4/v6 (mode double pile) et que vous vous connectez à un ISP, vous pouvez utiliser la connectivité IPv4 et IPv6.)

Si l'indicateur de configuration d'adresse gérée (drapeau M) dans le RA de la passerelle réseau haut débit (BNG) ou d'un autre périphérique est défini sur 0, le client PPPoE utilisera la configuration automatique sans état. S'il est défini sur 1, le client tentera d'obtenir son adresse IPv6 à partir d'un serveur DHCPv6 à l'aide de DHCPv6 avec état.

Lorsque l'indicateur Autre configuration (O-flag) est défini sur 1, les informations de configuration autres que l'adresse IPv6 doivent être disponibles à partir du serveur DHCPv6, telles que le préfixe délégué et l'adresse des serveurs DNS récursifs.

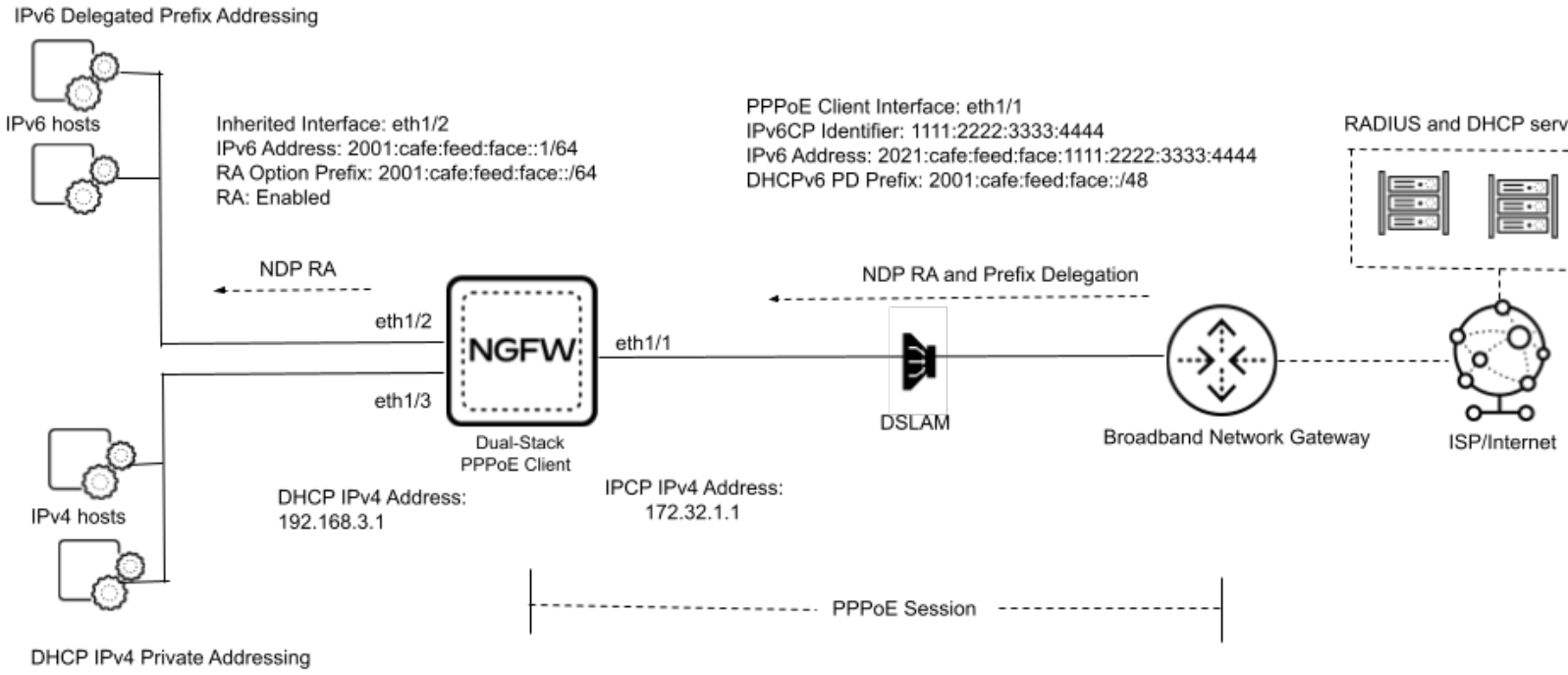
IPv6CP négocie l'identifiant d'interface pour l'interface client.

Le cas d'utilisation suivant concerne DHCPv6 avec état. Le graphique suivant illustre le pare-feu utilisant DHCPv6 avec état pour recevoir son adresse IPv6 et son préfixe délégué. L'interface Ethernet 1/1 agit comme un client PPPoEv6, face soit à un concentrateur d'accès, une passerelle

 ©2024 Palo Alto Networks, Inc.

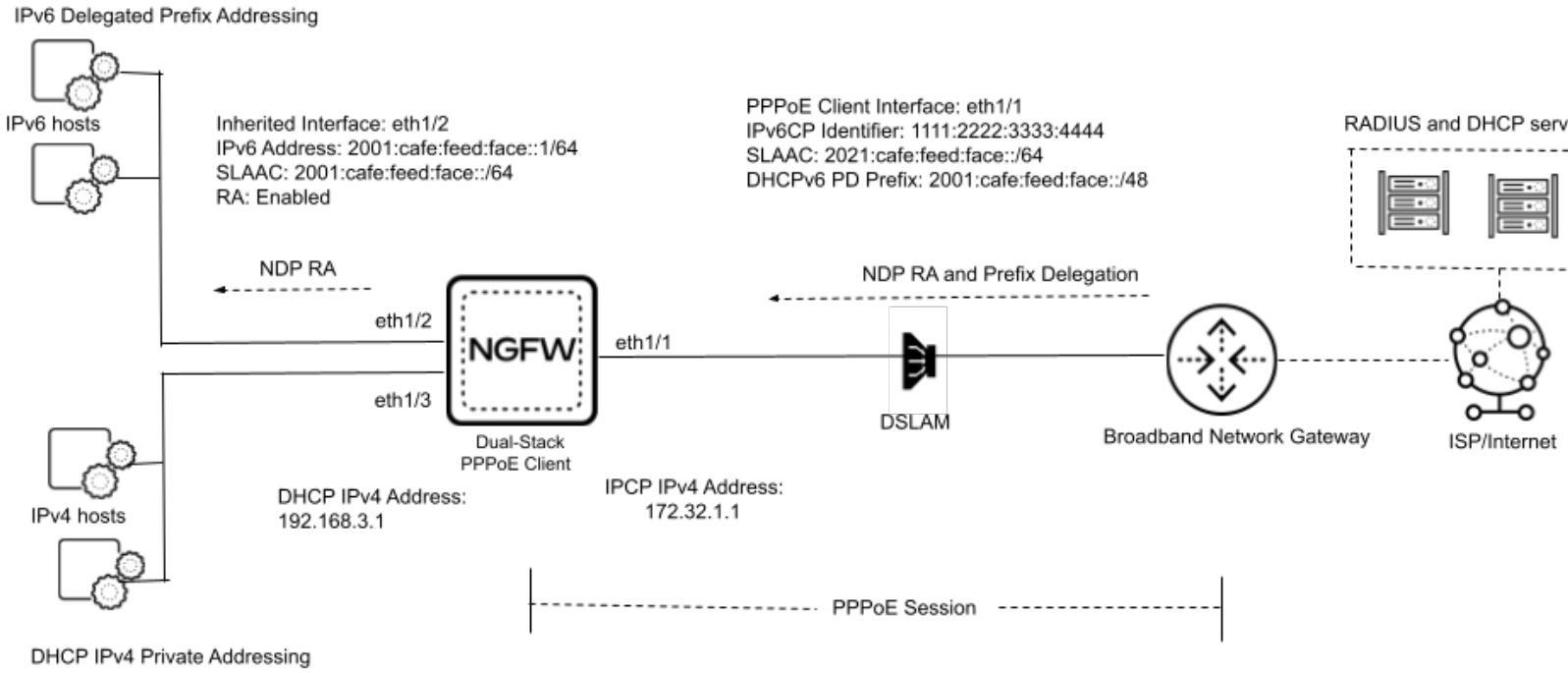
réseau haut débit, un multiplexeur d'accès à la ligne d'abonné numérique (DSLAM) ou un serveur PPPoEv6 (en fonction du déploiement de l'ISP). L'interface client PPPoEv6 apprend son identifiant d'interface IPv6 (IID) via le protocole de contrôle IPv6 (IPv6CP). Une fois ce paramètre IPv6 négocié, il est utilisé pour attribuer l'adresse locale de liaison IPv6 (LLA) à l'interface. Aucune détection d'adresse en double (DAD) n'est effectuée, car l'IID est déjà négocié. La séquence d'événements se poursuit avec l'attribution d'adresses via DHCPv6. La ou les passerelles pour la connexion sont également obtenues à partir de l'annonce de routeur (RA).

Le client PPPoEv6 reçoit un préfixe délégué DHCPv6 de l'ISP. Le client PPPoEv6 peut utiliser ces informations pour l'attribuer à un pool. Le pool peut ensuite être fragmenté en plusieurs préfixes /64, qui à leur tour sont attribués à l'interface héritée eth1/2. Eth1/2 créera une adresse IPv6 en utilisant le mécanisme EUI-64. Les hôtes du segment LAN connecté à eth1/2 utiliseront SLAAC pour créer leur adresse IPv6.



Le cas d'utilisation suivant concerne le DHCPv6 sans état (SLAAC). Le graphique suivant illustre le pare-feu utilisant DHCPv6 sans état pour recevoir son adresse IPv6 et déléguer un préfixe aux hôtes IPv6. L'interface Ethernet 1/1 agit comme un client PPPoEv6, face soit à un concentrateur d'accès, une passerelle réseau haut débit, un DSLAM ou un serveur PPPoEv6 (selon le déploiement de l'ISP). L'interface client PPPoEv6 apprend son identifiant d'interface IPv6 (IID) via le protocole de contrôle IPv6 (IPv6CP). Une fois ce paramètre IPv6 négocié, il est utilisé pour attribuer l'adresse locale de liaison IPv6 (LLA) à l'interface. Aucune DAD n'est effectuée, car l'IID est déjà négocié. La séquence d'événements se poursuit avec l'attribution d'adresses via SLAAC. La ou les passerelles pour la connexion sont également obtenues auprès de la RA.

©2024 Palo Alto Networks, Inc.



Le pare-feu encapsule le trafic en direction du nord (provenant des hôtes IPv6) dans PPPoE et envoie le trafic vers Internet.

STEP 1 | Configurez une interface ou une sous-interface Ethernet de couche 3 en tant que client PPPoE IPv6.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et sélectionnez une interface.
2. Sélectionnez **Interface Type (Type d'interface)** comme **Layer3**.

   Vous pouvez également sélectionner une interface de couche 3, ajouter une sous-interface, saisir un numéro de sous-interface, ajouter une balise et procéder à la configuration de la sous-interface en tant que client PPPoEv6.
3. Sélectionnez **IPv6** et **Enable IPv6 on the interface (Activer IPv6 sur l'interface)**.
4. Sélectionnez **EUI-64** (Extended Unique Identifier), qu'une attribution d'adresse sans état utilise pour qu'un hôte puisse s'attribuer un identifiant d'interface unique de 64 bits version 6.
5. Sélectionnez le **Type** d'attribution d'adresse comme **PPPoEv6 Client (Client PPPoEv6)**.

STEP 2 | Configurez les paramètres généraux du client PPPoEv6.

1. **Activez** l'interface.
2. Si vous disposez déjà d'une interface configurée pour le client PPPoE (IPv4), vous pouvez éventuellement **Apply IPv4 Parameters (Appliquer les paramètres IPv4)**, ce qui permet de copier les paramètres IPv4 sur le client PPPoEv6. (Les paramètres copiés sont le type

 ©2024 Palo Alto Networks, Inc.

d'authentification, le nom d'utilisateur, le mot de passe, le nom du concentrateur d'accès, le service et le paramètre passif.)

- *Si vous reconfigurez ultérieurement un paramètre sur le client PPPoE IPv4, la nouvelle valeur de paramètre est copiée sur le client PPPoE IPv6.*
- *Si vous reconfigurez un paramètre de l'un ou l'autre client, la session est rétablie, ce qui entraîne une interruption du trafic.*

Même si vous configurez indépendamment un client PPPoE IPv4 et un client PPPoE IPv6, vous devez configurer les deux clients avec le même type d'authentification, nom d'utilisateur, mot de passe, nom du concentrateur d'accès, service et paramètre passif.

3. Si vous souhaitez que le client PPPoEv6 (interface) attende que le serveur PPPoEv6 initie une connexion, sélectionnez **Passive (Passif)**. Si l'option Passif n'est pas sélectionnée, l'interface est autorisée à établir une connexion.
4. Sélectionnez le type d'**Authentication (Authentification)** pour l'interface.

   Si vous avez également configuré cette interface en tant que client PPPoE IPv4, vous devez configurer les deux clients avec le même type d'authentification, nom d'utilisateur, mot de passe, nom du concentrateur d'accès et service.

   - **CHAP** : l'interface utilise le protocole CHAP (Challenge Handshake Authentication Protocol).
   - **PAP** : l'interface utilise le protocole PAP (Password Authentication Protocol). Le PAP envoie les noms d'utilisateur et les mots de passe en texte brut et est moins sécuritaire que le CHAP.
   - **auto** : l'interface négocie la méthode d'authentification (CHAP ou PAP) avec le serveur PPPoEv6.
5. Entrez le **Username (Nom d'utilisateur)** pour l'authentification.
6. Saisissez le **Password (Mot de passe)** et **Confirm Password (Confirmez le mot de passe)**.
7. Si votre ISP vous a indiqué le nom du **Access Concentrator (Concentrateur d'accès)** auquel vous connecter, saisissez-le (une chaîne de 0 à 255 caractères).
8. Si vous souhaitez que l'interface en tant que client PPPoEv6 demande un service spécifique au serveur PPPoEv6, saisissez le **Service** (une chaîne de 0 à 255 caractères).

STEP 3 | Configurez les options d'adresse.

1. Sélectionnez **Address Assignment (Attribution d'adresse)**.
2. **Accept Router Advertised Route (Accepter l'itinéraire annoncé par le routeur)** pour permettre au client PPPoEv6 d'accepter la RA.
3. Saisissez la **Default Route Metric (Mesure d'itinéraire par défaut)** pour l'itinéraire entre l'interface et l'ISP ; la plage est de 1 à 65 535 ; la valeur par défaut est 10.
4. Définissez la **Preference (Préférence)** de l'interface client PPPoEv6 : **High (Élevé)** (par défaut), **Medium (Moyen)** ou **Low (Faible)**. Dans le cas où vous disposez de deux interfaces (chacune connectée à un ISP différent pour la redondance), vous pouvez attribuer à l'interface d'un ISP une préférence plus élevée qu'à celle de l'interface de l'autre ISP. Le FAI connecté à l'interface préférée sera le FAI qui fournit le préfixe

 ©2024 Palo Alto Networks, Inc.

délégué à envoyer à une interface faisant face à l'hôte. Si les interfaces ont la même préférence, les deux FAI fournissent un préfixe délégué et l'hôte décide quel préfixe utiliser.

STEP 4 | (Pour une configuration automatique sans état) Demandez au pare-feu de configurer automatiquement l'adresse IPv6 de l'interface à l'aide de l'identifiant d'interface du protocole de contrôle IPv6 (IPv6CP) et du préfixe de la publicité de routeur (à l'aide de SLAAC).

1. Sélectionnez **Autoconfig (Configuration automatique)**.
2. **Enable Autoconfig (Activez la configuration automatique)**.
3. Passez à la configuration de la résolution d'adresse.

STEP 5 | (Pour une configuration avec état) Vous pouvez également configurer l'attribution d'adresse à l'aide de DHCPv6.

1. Dans l'onglet **Address Assignment (Attribution d'adresse)**, sélectionnez **DHCPv6**.
2. **Enable (Activez)** DHCPv6.
3. Sélectionnez **DHCPv6 Options (Options DHCPv6)**.
4. **Enable IPv6 Address (Activez l'adresse IPv6)** pour permettre au client PPPoEv6 d'utiliser l'adresse attribuée par le serveur DHCPv6.
5. Sélectionnez **Rapid Commit (Validation rapide)** pour utiliser le processus DHCPv6 des messages Solliciter et répondre (deux messages), plutôt que le processus des messages Solliciter, annoncer, demander et répondre (quatre messages).
6. Sélectionnez le **DUID Type (Type de DUID)** (**ID**HCPv6 **Unique Identifier** (Identifiant unique)) que l'interface utilise pour s'identifier auprès du serveur DHCPv6 :
   - **DUID-LLT** : l'adresse de la couche de liaison de l'interface, concaténée avec un horodatage.
   - **DUID-LL** : l'adresse de la couche de liaison de l'interface.

STEP 6 | Si vous avez choisi DHCPv6 pour l'attribution d'adresse, configurez la délégation de préfixe.

1. Sélectionnez **Prefix Delegation (Délégation de préfixe)**.
2. **Enable Prefix Delegation (Activez la délégation de préfixe)** pour permettre au pare-feu de prendre en charge la fonctionnalité de délégation de préfixe. Cela signifie que l'interface accepte un préfixe du serveur DHCPv6 amont et place le préfixe dans le pool de préfixes, à partir duquel le pare-feu délègue un préfixe à un hôte via RA. La possibilité d'activer ou de désactiver la délégation de préfixe pour une interface permet au pare-feu de prendre en charge plusieurs FAI (un FAI par interface). L'activation de la délégation de préfixe sur cette interface contrôle quel FAI fournit le préfixe. Le préfixe délégué est utilisé sur l'interface face à l'hôte, et son adresse IPv6 est construite avec l'adresse MAC et l'entrée EUI-64.
3. Sélectionnez **DHCP Prefix Length Hint (Indice de longueur de préfixe DHCP)** pour permettre au pare-feu d'envoyer une longueur de préfixe DHCPv6 préférée au serveur DHCPv6.
4. Entrez la **DHCP Prefix Length (bits) (Longueur de préfixe DHCP préférée)** qui est envoyée comme indication au serveur DHCPv6 ; la plage va de 0 à 128 ; la valeur par

 ©2024 Palo Alto Networks, Inc.

défaut est 48. Le serveur DHCPv6 a le pouvoir discrétionnaire d'envoyer la longueur de préfixe qu'il choisit.

Demander une longueur de préfixe de 48, par exemple, laisse 16 bits restants pour les sous-réseaux (64 moins 48), ce qui indique que vous avez besoin de nombreuses subdivisions de ce préfixe pour déléguer. Demander une longueur de préfixe de 63 laisse 1 bit pour ne déléguer que deux sous-réseaux. Sur les 128 bits, il reste encore 64 bits pour une adresse d'hôte.

L'interface peut recevoir un préfixe /48, mais déléguer un préfixe /64, par exemple, ce qui signifie que le pare-feu subdivise le préfixe qu'il délègue.

5. Entrez un **Prefix Pool Name (Nom de pool de préfixes)** pour le pool où le pare-feu stocke le préfixe reçu. Le nom doit être unique et contenir un maximum de 63 caractères alphanumériques, traits d'union, points et traits de soulignement.

   Utilisez un nom de pool de préfixes qui reflète le FAI pour une reconnaissance facile.

6. Sélectionnez **Show Prefix Pool Assignment (Afficher l'affectation du pool de préfixes)** pour afficher pour chaque interface héritée faisant face à l'hôte : le préfixe hérité (préfixe que l'interface distribue aux hôtes), l'adresse IPv6 assignée de l'interface héritée elle-même (basée sur le préfixe et construite à partir de l'adresse MAC), la préférence du routeur et l'état de l'interface.

STEP 7 | Configurez la résolution d'adresse.

1. Sélectionnez **Address Resolution (Résolution d'adresse)**.
2. **Enable Duplicate Address Detection (Activer la détection des doublons d'adresses)** (DAD)
3. Définissez les **DAD Attempts (Tentatives de DAD)**, le nombre de tentatives DAD dans l'intervalle de sollicitation de voisins (NS) avant que la tentative d'identification n'échoue (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
4. Définissez le **Reachable Time (sec) (Délai d'accessibilité (sec))**, le nombre de secondes pendant lesquelles un voisin reste joignable après une requête et une réponse réussies ; la plage va de 10 à 36 000 ; la valeur par défaut est 30.
5. Définissez le **NS Interval (sec) (Intervalle NS (sec))** ; le nombre de secondes nécessaires aux tentatives de DAD avant l'échec est indiqué ; la plage va de 1 à 3 600 ; la valeur par défaut est 1.
6. **Enable NDP Monitoring (Activer la surveillance NDP)** (Neighbor Discovery Protocol monitoring ; surveillance du protocole de détection de voisins).

 ©2024 Palo Alto Networks, Inc.

STEP 8 | Configurez la prise en charge DNS.

1. Sélectionnez **DNS Support (Assistance DNS)**.
2. Sélectionnez **DNS Recursive Name Server (Serveur de noms récursif DNS)**. Sélectionnez le **Type** :
   - **DHCPv6** : pour que le serveur DHCPv6 envoie les informations de serveur de nom DNS récursif (RDNS).
   - **Manual (Manuel)** : **Add (Ajoutez)** l'adresse IPv6 d'un serveur de noms **RDNS** et la **Lifetime (Durée de vie)**, le nombre maximum de secondes pendant lesquelles le client peut utiliser le serveur RDNS spécifique pour résoudre les noms de domaine ; la plage va de 4 à 3 600 ; la valeur par défaut est 1 200. Sélectionnez Manual si le client PPPoEv6 utilise SLAAC pour configurer automatiquement son adresse IPv6.
3. Sélectionnez **Domain Search List (Liste de recherche de domaine)** et sélectionnez le **Type** :
   - **DHCPv6**— Pour que le serveur DHCPv6 envoie les informations de la liste de recherche de domaine.
   - **Manual** : ajoutez un ou plusieurs noms **Domain (Domaine)** (suffixes) pour la liste de recherche DNS (DNSSL) et la **Lifetime (Durée de vie)**, le nombre maximum de secondes pendant lesquelles le client peut utiliser la liste de recherche de domaine spécifique ; la plage va de 4 à 3 600 ; la valeur par défaut est 1 200. Sélectionnez Manual si le client PPPoEv6 utilise SLAAC pour configurer automatiquement son adresse IPv6.

STEP 9 | Cliquez sur **OK**.

STEP 10 | **Commit** (Valider).

STEP 11 | Affichez les informations du client PPPoEv6.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et sélectionnez l'interface que vous avez configurée.
2. **Afficher les informations d'exécution du client PPPoEv6**.

 ©2024 Palo Alto Networks, Inc.

Configuration d'un groupe d'interfaces agrégé

Un groupe d'interfaces agrégé se base sur la norme IEEE 802.1AX d'agrégation de liens pour combiner de multiples interfaces Ethernet en une seule interface virtuelle qui connecte un pare-feu à un autre périphérique ou pare-feu. Un groupe agrégé augmente la bande passante qui existe entre des homologues en équilibrant la charge du trafic qui passe par les interfaces combinées. Ce dernier assure également la redondance ; en cas de défaillance d'une interface, les autres interfaces continuent de prendre en charge le trafic.

Par défaut, la détection des échecs de l'interface est automatique uniquement au niveau physique entre des homologues connectés directement. Toutefois, si vous activez le Link Aggregation Control Protocol (protocole d'agrégation de liaisons ; LACP), la détection des échecs se fait automatiquement aux niveaux physique et de la liaison de données, peu importe si les homologues sont connectés directement. LACP assure également un basculement automatique aux interfaces qui sont en veille si vous avez configuré des disques de secours. Tous les pare-feu Palo Alto Networks® prennent en charge les groupes agrégés. L'outil Product Selection (Sélection de produit) indique le nombre de groupes agrégés pris en charge par chaque pare-feu. Chaque groupe d'agrégats peut avoir jusqu'à huit interfaces.

Les modèles de pare-feu PAN-OS® prennent en charge un maximum de 16 000 adresses IP affectées à des interfaces de Couche 3 physiques ou virtuelles ; ce maximum comprend des adresses IPv4 et IPv6.

La QoS n'est prise en charge que pour les huit premiers groupes d'agrégats.

Avant de configurer un groupe agrégé, vous devez d'abord configurer les interfaces qui le composent. Parmi les interfaces affectées à un groupe agrégé donné, le matériel peut différer (par exemple, vous pourriez allier la fibre optique et le cuivre), mais la bande passante et le type d'interface doivent être identiques. Voici les options de bande passante et de type d'interface :

- **Bandwidth (Bande passante)** : 1 Gbit/s, 10 Gbit/s, 40 Gbit/s ou 100 Gbit/s.
- **Type d'interface** : HA3, câble virtuel, couche 2 ou couche 3.

Cette procédure décrit les étapes de configuration du pare-feu Palo Alto Networks uniquement. Vous devez configurer le groupe agrégé sur le périphérique homologue. Reportez-vous à la documentation de ce périphérique pour obtenir les instructions.

STEP 1 | Configurez les paramètres généraux du groupe d'interfaces.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)**, puis cliquez sur **Add Aggregate Group (Ajouter un groupe agrégé)**.
2. Dans le champ adjacent au **Interface Name (Nom de l'interface)** en lecture seule, saisissez un nombre pour identifier le groupe. La plage est comprise entre 1 et le nombre maximal de groupes d'interfaces agrégés pris en charge par le pare-feu.
3. Sous **Interface Type (Type d'interface)**, sélectionnez **HA (Haute disponibilité)**, **Virtual Wire (Câble virtuel)**, **Layer2 (Couche 2)** ou **Layer3 (Couche 3)**.
4. Configurez les autres paramètres du **Interface Type (Type d'interface)** que vous avez sélectionné.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Pour une interface de couche 3, si vous souhaitez configurer une adresse IPv4 statique, sélectionnez **IPv4** et reportez-vous à Configurer les interfaces de couche 3 pour configurer une adresse IPv4 statique.

STEP 3 | Pour une interface de couche 3, si vous souhaitez configurer une adresse IPv6 statique, sélectionnez **IPv6** et reportez-vous à Configurer les interfaces de couche 3 pour configurer une adresse IPv6 statique.

STEP 4 | Pour une interface de couche 3, si vous souhaitez configurer l'interface en tant que client DHCP pour recevoir une adresse IPv4, sélectionnez **IPv4** et reportez-vous à Configurer une interface en tant que client DHCPv4 pour configurer un client DHCP.

STEP 5 | Pour une interface de couche 3, si vous souhaitez configurer l'interface en tant que client DHCPv6 pour recevoir une adresse IPv6 (avec ou sans délégation de préfixe), sélectionnez **IPv6** et reportez-vous à Configurer une interface en tant que client DHCPv6 pour configurer un client DHCPv6.

STEP 6 | Configurez les paramètres LACP.

Effectuez cette étape seulement si vous voulez activer LACP pour le groupe agrégé.

Vous ne pouvez pas activer LACP sur les interfaces de câble virtuel.

1. Sélectionnez l'onglet **LACP (LACP)**, puis **Enable LACP (Activer LACP)**.
2. Définissez le **Mode (Mode)** des requêtes sur l'état LACP sur **Passive (Passif)** (le pare-feu ne fait que répondre ; c'est le mode par défaut) ou sur **Active (Actif)** (le pare-feu interroge les périphériques homologues).

   Il est recommandé de définir un homologue LACP sur le mode actif et l'autre, sur le mode passif. LACP ne peut pas fonctionner si les deux homologues sont passifs. Le pare-feu ne peut détecter le mode de son périphérique homologue.
3. Définissez le **Transmission Rate (Taux de transmission)** des requêtes et réponses sur **Slow (Lent)** (toutes les 30 secondes ; c'est la valeur par défaut) ou sur **Fast (Rapide)** (toutes les secondes). Faites votre choix en fonction de la capacité de traitement LACP prise en charge par votre réseau et de la vitesse à laquelle les homologues LACP doivent détecter et résoudre les échecs d'interface.
4. Sélectionnez **Fast Failover (Basculement rapide)** si vous voulez activer le basculement vers une interface en veille en moins d'une seconde. L'option est désactivée par défaut, et le pare-feu se sert de la norme IEEE 802.1ax pour le traitement du basculement, qui prend au moins trois secondes.

   *Il est recommandé d'utiliser l'option **Fast Failover (Basculement rapide)** pour les déploiements dans lesquels vous risquez de perdre des données essentielles lors du délai de basculement standard.*
5. Saisissez le **Max Ports (Nombre maximum de ports)** qui sont actifs (de 1 à 8) au sein du groupe agrégé. Si le nombre d'interfaces affectées au groupe dépasse le **Max Ports (Nombre maximum de ports)**, les interfaces restantes seront en mode veille. Le pare-feu utilise la **LACP Port Priority (Priorité de port LACP)** de chaque interface que vous affectez (étape 3) pour déterminer les interfaces initialement actives et l'ordre dans

 ©2024 Palo Alto Networks, Inc.

lequel les interfaces en veille deviennent actives lors du basculement. Si les valeurs de priorité de port des homologues LACP ne concordent pas, les valeurs de l'homologue ayant les valeurs de **System Priority (Priorité système)** les plus faibles (intervalle compris entre 1 et 65 535 ; valeur par défaut : 32 768) remplaceront celles de l'autre homologue.

6. (Facultatif) Pour les pare-feu actif/passif uniquement, sélectionnez **Enable in HA Passive State (Activer à l'état haute disponibilité passif)** si vous voulez activer la prénégociation LACP du pare-feu passif. La prénégociation LACP accélère le basculement vers le pare-feu passif (pour de plus amples renseignements, reportez-vous à la section Prénégociation LACP et LLDP pour la HA active/passive).

   *Si vous choisissez cette option, vous ne pouvez sélectionner **Same System MAC Address for Active-Passive HA (Adresse MAC identique pour la HD active/passive)** ; la prénégociation exige que chaque pare-feu HD dispose d'adresses MAC d'interface uniques.*

7. (Facultatif) Pour les pare-feu actif/passif uniquement, sélectionnez **Same System MAC Address for Active-Passive HA (Adresse MAC identique pour la haute disponibilité active/passive)**, puis précisez une seule **MAC Address (Adresse MAC)** pour les deux pare-feu. Cette option réduit la latence lors du basculement si les homologues LACP sont virtualisés (s'ils apparaissent sur le réseau comme périphérique unique). Par défaut, l'option est désactivée : chaque pare-feu d'une paire HA dispose d'une adresse MAC unique.

   Si les homologues LACP ne sont pas virtualisés, utilisez les adresses MAC uniques pour réduire la latence lors du basculement.

STEP 7 | Cliquez sur **OK**.

STEP 8 | Affectez des interfaces au groupe agrégé.

Effectuez les étapes suivantes pour chaque interface (de 1 à 8) qui sera membre du groupe agrégé.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** et cliquez sur le nom de l'interface pour la modifier.
2. Définissez le paramètre **Interface Type (Type d'interface)** sur **Aggregated Ethernet (Ethernet agrégé)**.
3. Sélectionnez le **Aggregate Group (groupe agrégé)** que vous venez de définir.
4. Sélectionnez **Link Speed (Vitesse de liaison)**, **Link Duplex (Duplex de la liaison)** et **Link State (État de la liaison)**.

   Il est recommandé de définir les mêmes valeurs de vitesse et duplex de liaison pour chaque interface du groupe. Lorsque les valeurs ne correspondent pas, le pare-feu utilise la vitesse la plus élevée et le duplex intégral.

5. (Facultatif) Saisissez une **LACP Port Priority (Priorité de port LACP)** (la plage est comprise entre 1 et 65 535, et la valeur par défaut est de 32 768) si vous avez activé LACP pour le groupe agrégé. Si le nombre d'interfaces affectées dépasse le **Max Ports (Nombre maximum de ports)** du groupe, les priorités de port déterminent les interfaces

 ©2024 Palo Alto Networks, Inc.

actives et en veille. Les interfaces affichant les valeurs numériques les plus basses (priorités les plus élevées) seront actives.

6. Cliquez sur **OK**.

STEP 9 | Si les pare-feu ont une configuration active/active et que vous agrégez les interfaces HA3, activez le transfert des paquets pour le groupe agrégé.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)** et modifiez la section Packet Forwarding (Transfert des paquets).
2. Sélectionnez le groupe agrégé que vous avez configuré pour la **HA3 Interface (Interface HA3)** et cliquez sur **OK (OK)**.

STEP 10 | ((Supported firewalls onlyPare-feu pris en charge uniquement)) Si l'interface correspond à un port PoE (Power over Ethernet) sur le pare-feu, vous pouvez éventuellement configure PoE (configurer PoE).

STEP 11 | **Commit (Validez)** vos modifications.

STEP 12 | Vérifiez l'état du groupe agrégé.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
2. Vérifiez que la colonne Link State (État de la liaison) affiche une icône verte pour le groupe agrégé, indiquant que toutes les interfaces membres sont actives. Si l'icône est jaune, au moins un membre est inactif. Si l'icône est rouge, tous les membres sont inactifs.
3. Si vous avez configuré LACP, vérifiez que la colonne Features (Fonctions) affiche l'icône LACP activée pour le groupe agrégé.

STEP 13 | (PA-7050 and PA-7080 firewalls only (Pare-feu PA-7050 et PA-7080 uniquement)) Si vous avez un groupe d'interface agrégé dont les interfaces sont situées sur différentes cartes de ligne, il est préférable d'activer le pare-feu afin qu'il puisse gérer les paquets IP fragmentés qu'il reçoit sur plusieurs interfaces du groupe AE qui sont réparties sur plusieurs cartes. Pour ce faire, utilisez la commande opérationnelle CLI suivante avec le mot-clé **`hash (hachage)`**. (Les deux autres mots-clés sont également affichés par souci d'exhaustivité.)

1. Accédez à la CLI.
2. Utilisez la commande d'interface de ligne de commande (CLI) opérationnelle suivante : **`set ae-frag redistribution-policy <self | sXdpX fixe hash>`**
   - **`self (auto)`**—(default) Ce mot-clé est destiné au comportement hérité ; il ne permet pas au pare-feu de gérer les paquets fragmentés reçus sur plusieurs interfaces d'un groupe d'interfaces AE.
   - **`fixed s`**<*slot-number*>**`dp`**<*dataplane-cpu-number*> : remplacez la variable *slot-number* et remplacez la variable *data-plane-cpu-number* par le numéro de dataplane du dataplane qui gérera tous les fragments IP reçus par tous les membres de toutes les interfaces AE. Le mot-clé **`fixed (fixe)`** est principalement destiné à des fins de dépannage et ne doit pas être utilisé en production.

 ©2024 Palo Alto Networks, Inc.

- **hash (hachage)**: permet au pare-feu de gérer les paquets fragmentés qu'il reçoit sur plusieurs interfaces d'un groupe d'interfaces AE situées sur plusieurs cartes de ligne.

©2024 Palo Alto Networks, Inc.

Configurer Bonjour Reflector pour la segmentation du réseau

Apple Bonjour (également connu sous le nom de réseau à configuration zéro) permet la découverte automatique des périphériques et des services sur un réseau local. Par exemple, Bonjour vous permet de vous connecter à une imprimante sans avoir à configurer manuellement l'adresse IP de l'imprimante. Pour traduire les noms en adresses sur un réseau local, Bonjour utilise le Multicast DNS (mDNS). Bonjour utilise une plage de multidiffusion privée pour son trafic, qui ne permet pas le routage du trafic, ce qui empêche l'utilisation dans un environnement qui utilise la segmentation du réseau à des fins de sécurité ou d'administration (par exemple, lorsque les serveurs et les clients se trouvent dans des sous-réseaux différents).

Pour prendre en charge Apple Bonjour dans les environnements réseau qui utilisent la segmentation pour acheminer le trafic, vous pouvez transférer le trafic IPv4 Bonjour entre les interfaces Interfaces de Couche 3 (L3) Ethernet (Ethernet de couche 3) ouAggregate Ethernet (AE) ou les sous-interfaces que vous spécifiez. L'option réflecteur Bonjour vous permet de transmettre des annonces et des requêtes Bonjour multicast à des interfaces ou sous-interfaces Ethernet et AE L3, garantissant à l'utilisateur l'accès aux services et la possibilité de découvrir les périphériques indépendamment des valeurs Time To Live (TTL) ou des limites de saut.

Les plateformes suivantes prennent en charge le transfert de trafic Bonjour :

- *PA-220 series*
- *PA-800 series*
- *PA-3200*

Lorsque vous activez cette option, le pare-feu redirige le trafic Bonjour vers les interfaces et sous-interfaces de couche 3 et AE où vous activez cette option. Vous devez activer cette option sur toutes les interfaces prises en charge que vous souhaitez gérer le trafic Bonjour ; par exemple, si vous souhaitez qu'une interface de couche 3 spécifique transmette le trafic Bonjour à une interface AE, vous devez activer cette option sur les deux interfaces. Vous pouvez activer cette option sur un maximum de 16 interfaces.

Pour éviter les boucles, le pare-feu modifie l'adresse MAC source en adresse MAC de l'interface de sortie du pare-feu. Pour aider à prévenir les attaques par saturation, si le pare-feu reçoit plus que le nombre de paquets par seconde indiqué dans le tableau suivant, le pare-feu supprime les paquets pour protéger le pare-feu et le réseau.

Limite de débit série	*(par seconde)*
PA-220	*100*
PA-400	*N/A PA-800 200 PA-3200 500*

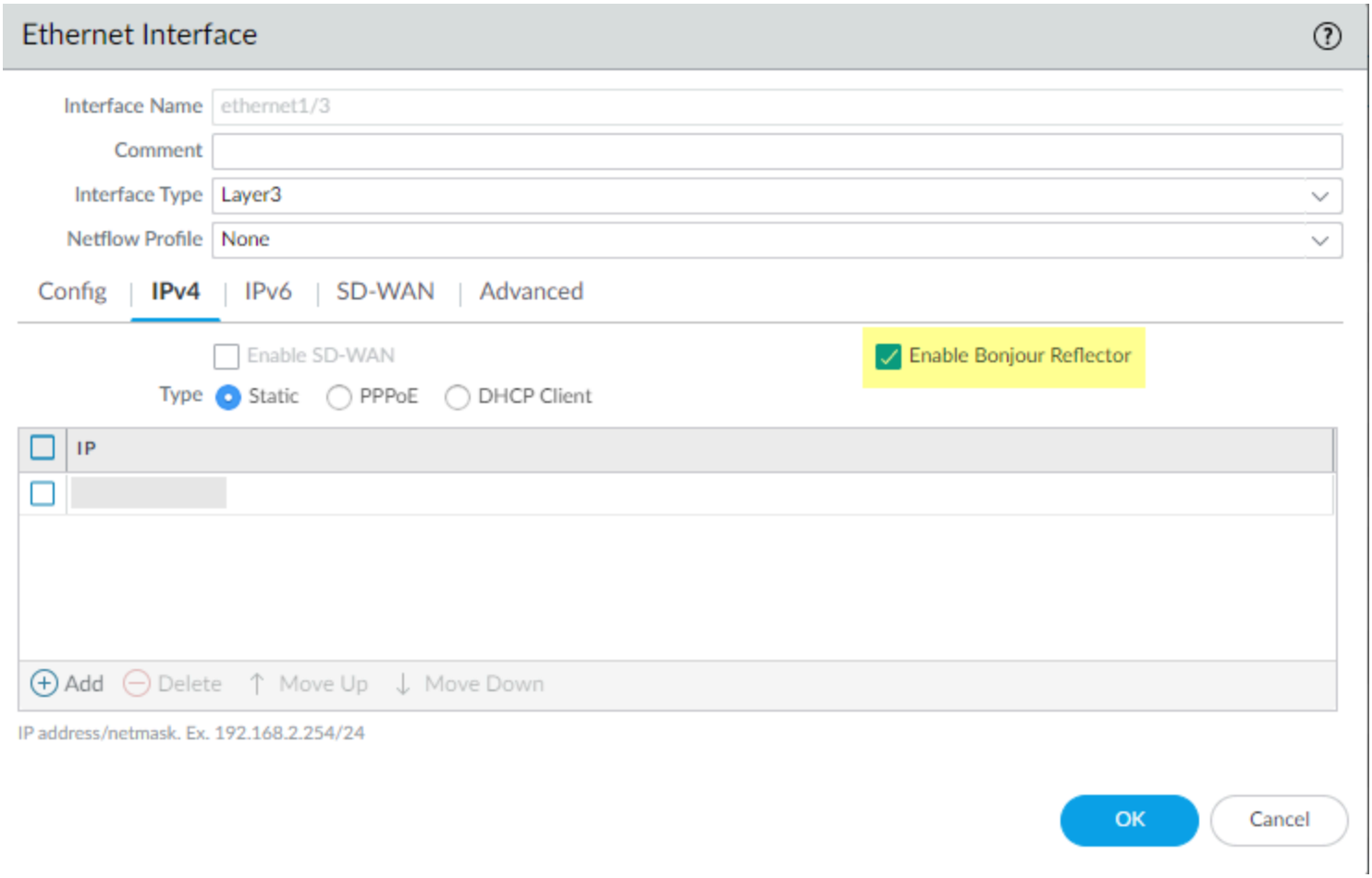
STEP 1 | Sélectionnez **Network (Réseau)** > **Interfaces**.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Sélectionnez ou **Add (Ajoutez)** une interface ou une sous-interface L3 Ethernet ou une interface AE.

*Si vous ajoutez une sous-interface, elle doit utiliser une **Tag (étiquette)** autre que 0.*

STEP 3 | Sélectionnez **IPv4** puis sélectionnez l'option **Enable Bonjour Reflector (Activer le réflecteur Bonjour)**.



STEP 4 | Cliquez sur **OK**.

STEP 5 | Répétez les étapes 1 à 4 pour toutes les interfaces et sous-interfaces de couche 3 (L3) ou AE où vous souhaitez faire suivre le trafic Bonjour.

Vous pouvez activer cette option sur un maximum de 16 interfaces ou sous-interfaces différentes.

STEP 6 | **Commit (Validez)** vos modifications.

STEP 7 | Confirmez que la colonne **Features (Caractéristiques)** pour la ou les interfaces où vous activez l'option réflecteur Bonjour affiche `Bonjour Reflector:yes (Réflecteur Bonjour:oui)` ( ).

 ©2024 Palo Alto Networks, Inc.

STEP 8 | Utilisez la commande CLI `show bonjour interface (afficher l'interface Bonjour)` pour afficher toutes les interfaces où le pare-feu transmet le trafic Bonjour et une liste de compteurs. `rx` représente le nombre total de paquets Bonjour que l'interface reçoit, `tx` représente le nombre total de paquets Bonjour que l'interface transmet et `drop` représente le nombre de paquets que l'interface dépose.

```
admin> show bonjour interface name rx tx drop
 ------------------------------------------------------------
 ethernet1/4 1 1 0 ethernet1/7 0 0 0 ethernet1/7.10 0 0 0
 ethernet1/7.20 4 4 0 ae15 0 0 0 ae16 0 0 0 ae16.30 0 2 0 ae16.40 0
 0 0
```

 ©2024 Palo Alto Networks, Inc.

Utilisation des profils de gestion d'interface pour limiter l'accès

Un profil de gestion de l'interface protège le pare-feu contre un accès non autorisé en définissant les protocoles, les services et les adresses IP qu'une interface du pare-feu autorise pour le trafic de gestion. Vous pourriez, par exemple, vouloir empêcher les utilisateurs d'accéder à l'interface Web du pare-feu plutôt qu'à l'interface ethernet1/1, tout en autorisant la réception par cette interface des interrogations SNMP de votre système de surveillance du réseau. Dans ce cas, vous devriez activer SNMP et désactiver HTTP/HTTPS dans un profil de gestion de l'interface et assigner le profil à ethernet1/1.

Vous pouvez assigner un profil de gestion aux interfaces Ethernet de couche 3 (y compris les sous-interfaces) et aux interfaces logiques (groupe d'interfaces agrégées, interfaces VLAN, interfaces en boucle et interfaces de tunnel). Si vous n'assignez aucun profil de gestion de l'interface à une interface, l'accès sera refusé par défaut à l'ensemble des adresses IP, des protocoles et des services.

L'interface de gestion (MGT) ne nécessite pas de profil de gestion de l'interface. Vous limitez l'accès des protocoles, des services et des adresses IP à l'interface MGT lorsque vous perform initial configuration (procédez à la configuration initiale) du pare-feu. En cas d'échec de l'interface MGT, l'autorisation de l'accès de gestion via une autre interface vous permet de continuer à gérer le pare-feu.

Lorsque vous activez l'accès à une interface du pare-feu au moyen d'un profil de gestion d'interface, n'activez pas l'accès de gestion (HTTP, HTTPS, SSH ou Telnet) à partir d'Internet ou de toute autre zone non approuvée dans les limites de sécurité de votre entreprise. N'activez jamais l'accès HTTP ou Telnet, car ces protocoles transmettent en texte clair. Suivez les Meilleures pratiques pour sécuriser l'accès administratif afin de vous assurer que vous sécurisez correctement l'accès de gestion à votre pare-feu.

STEP 1 | Configurez le profil de gestion d'interface.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Interface Mgmt (Gestion de l'interface)**, puis cliquez sur **Add (Ajouter)**.
2. Sélectionnez les protocoles que l'interface autorise pour la gestion du trafic : **Ping**, **Telnet**, **SSH**, **HTTP**, **HTTP OCSP**, **HTTPS** ou **SNMP**.

   *N'activez pas **HTTP** ou **Telnet**, car ces protocoles transmettent en texte clair et, par conséquent, ne sont pas sûrs.*
3. Sélectionnez les services que l'interface autorise pour la gestion du trafic :
   - **Response Pages (Pages de réponse)** - Utilisez cette fonction pour activer des pages de réponse du portail captif.
     - **Captive Portal (Portail captif)** : pour servir les pages de réponse du portail captif, le pare-feu laisse les ports ouverts sur les interfaces de couche 3 : 6081 pour le portail captif en mode transparent et 6082 pour le portail captif en mode de redirection. Pour plus d'informations, consultez Authentication Policy and Authentication Portal (Politique d'authentification et portail d'authentification).

 ©2024 Palo Alto Networks, Inc.

- **Contrôle prioritaire de l'URL par l'administrateur** : Pour plus d'informations, consultez Autoriser l'accès par mot de passe à certains sites.

- **User-ID (ID utilisateur)** : utilisée pour Redistribute Data and Authentication Timestamps (redistribuer les données et horodatages d'authentification.
- **User-ID Syslog Listener-SSL (Écouteur SSL Syslog User-ID)** ou **User-ID Syslog Listener-UDP (Écouteur UDP Syslog User-ID)** : utilisez ces services pour Configurer l'User-ID pour surveiller les expéditeurs Syslog pour le mappage des utilisateurs via SSL ou UDP.

4. (Facultatif) **Add (Ajoutez)** les adresses IP autorisées qui peuvent accéder à l'interface. Si vous n'ajoutez aucune entrée à la liste, l'interface ne possède aucune restriction d'adresse IP.
5. Cliquez sur **OK**.

STEP 2 | Affectez le profil de gestion d'interface à une interface.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)**, sélectionnez le type d'interface (**Ethernet (Ethernet)**, **VLAN (VLAN)**, **Loopback (En boucle)** ou **Tunnel (De tunnel)**, et sélectionnez l'interface.
2. Sélectionnez **Advanced (Avancé)** > **Other info (Autres informations)**, puis sélectionnez le **Management Profile (Profil de gestion)** d'interface que vous venez de configurer.
3. Cliquez sur **OK**, puis sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Routeurs virtuels

Découvrez comment un routeur virtuel sur le pare-feu participe au routage de couche 3 et configurez un routeur virtuel.

- Vue d'ensemble des routeurs virtuels
- Configurer des routeurs virtuels

Vue d’ensemble des routeurs virtuels

Le pare-feu utilise des routeurs virtuels pour obtenir des itinéraires de Couche 3 vers d'autres sous-réseaux lorsque vous définissez manuellement des itinéraires statiques ou via la participation à un ou plusieurs protocoles de routage de Couche 3 (itinéraires dynamiques). Les itinéraires que le pare-feu obtient par ces méthodes remplissent la base d'informations de routage (RIB) IP du pare-feu. Lorsqu'un paquet est destiné à un autre sous-réseau que celui sur lequel il est arrivé, le routeur virtuel récupère le meilleur itinéraire dans la base d'informations de suivi (FIB), le place dans les informations de suivi et transfère le paquet au routeur Saut suivant défini dans la base FIB. Le pare-feu utilise le basculement Ethernet pour atteindre d'autres périphériques sur le même sous-réseau IP. (Une exception à l'entrée du meilleur itinéraire dans la base FIB survient lorsque vous utilisez ECMP, auquel cas tous les itinéraires de même coût vont dans la FIB.)

Les interfaces Ethernet, VLAN et tunnel définies sur le pare-feu reçoivent et transfèrent le trafic de Couche 3. La zone de destination provient de l'interface sortante en fonction des critères de transfert, et le pare-feu consulte les règles de politique pour identifier les politiques de sécurité à appliquer à chaque paquet. En plus du routage vers d'autres périphériques réseau, les routeurs virtuels peuvent effectuer un routage vers d'autres routeurs virtuels au sein du même pare-feu, à condition que le saut suivant indique qu'il pointe vers un autre routeur virtuel.

Vous pouvez configure Layer 3 interfaces on a virtual router (configurer les interfaces de couche 3 sur un routeur virtuel) pour participer avec des protocoles de routage dynamique (BGP, OSPF, OSPFv3 ou RIP), mais aussi ajouter des itinéraires statiques. Vous pouvez également créer plusieurs routeurs virtuels, chacun gérant un ensemble d'itinéraires distincts qui ne sont pas partagés entre les routeurs virtuels, ce qui vous permet de configurer différents comportements de routage pour différentes interfaces.

Vous pouvez configurer le routage dynamique d'un routeur virtuel à un autre en configurant une interface en boucle dans chaque routeur virtuel, en créant une route statique entre les deux interfaces en boucle, puis en configurant un protocole de routage dynamique pour homologuer entre ces deux interfaces. Le pare-feu ne prend en charge qu’un seul saut entre les routeurs virtuels. Par exemple, avec les routeurs virtuels A, B et C, un itinéraire ne peut pas aller de A à B puis à C ; il faudrait aller de A à C.

Chaque interface en boucle, VLAN, de tunnel ou Ethernet de Couche 3 définie sur le pare-feu doit être associée à un routeur virtuel. Même si chaque interface ne peut appartenir qu'à un seul routeur virtuel, vous pouvez configurer plusieurs protocoles de routage et itinéraires statiques pour un routeur virtuel. Que des itinéraires statiques ou des protocoles de routage dynamiques soient configurés pour un routeur virtuel, une configuration générale est nécessaire :

 ©2024 Palo Alto Networks, Inc.

Configurer des routeurs virtuels

Créez un virtual router (routeur virtuel) sur le pare-feu pour participer au routage de couche 3.

STEP 1 | Contactez votre administrateur réseau pour obtenir les informations requises.

- Les interfaces sur le pare-feu que vous voulez utiliser pour le routage.
- Distances administratives des protocoles statiques, OSPF interne, OSPF externe, IBGP, EBGP et RIP.

STEP 2 | Créez un routeur virtuel et appliquez-lui des interfaces.

Le pare-feu est livré avec un routeur virtuel nommé **default (pare-feu)**. Vous pouvez modifier le routeur virtuel **default (par défaut)** ou ajouter un nouveau routeur virtuel.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**.
2. Sélectionnez un routeur virtuel (celui nommé **default (par défaut)** ou un autre routeur virtuel) ou **Add (Ajoutez)** le **Name (Nom)** d'un nouveau routeur virtuel.
3. Sélectionnez **Router Settings (Paramètres du routeur)** > **General (Général)**.
4. Cliquez sur **Add (Ajouter)** dans la zone **Interfaces (Interfaces)** et sélectionnez une interface déjà définie.

   Répétez cette étape pour toutes les interfaces que vous souhaitez ajouter au routeur virtuel.
5. Cliquez sur **OK**.

STEP 3 | Définissez les distances administratives du routage statique et dynamique.

Définissez les distances administratives pour les types d'itinéraires nécessaires à votre réseau. Lorsque le routeur virtuel a deux itinéraires ou plus vers la même destination, il utilise la distance administrative pour choisir le meilleur chemin entre des protocoles de routage et itinéraires statiques différents, en favorisant une distance plus courte.

- **Static (Statique)** : plage comprise entre 10 et 240 ; valeur par défaut de 10.
- **OSPF Internal (OSPF interne)** : plage comprise entre 10 et 240 ; valeur par défaut de 30.
- **OSPF External (OSPF externe)** : plage comprise entre 10 et 240 ; valeur par défaut de 110.
- **IBGP** : plage comprise entre 10 et 240 ; la valeur par défaut est 200.
- **EBGP** : plage comprise entre 10 et 240 ; la valeur par défaut est 20.
- **RIP**: La plage est comprise entre 10 et 240 ; la valeur par défaut est 120.



Consultez ECMP si vous souhaitez exploiter la présence de plusieurs chemins à coût égal pour le transfert.

STEP 4 | Validez les paramètres généraux du routeur virtuel.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Configurez les interfaces Ethernet, en boucle, VLAN et tunnel comme nécessaire.

Configurez les interfaces de couche 3.

Dans PAN-OS 11.0.1 et versions ultérieures 11.1, pour une interface Ethernet, vous pouvez Configurer un client PPPoE sur une sous-interface.

©2024 Palo Alto Networks, Inc.

Itinéraires de service

Découvrez comment le pare-feu utilise les itinéraires de service pour envoyer des demandes à des services externes et configurer des itinéraires de service.

- Vue d'ensemble des itinéraires de service
- Configurer les itinéraires de service

Vue d’ensemble des itinéraires de service

Le pare-feu utilise l’interface de gestion (MGT) pour accéder aux services externes, tels que les serveurs DNS, les serveurs d'authentification externe, les services Palo Alto Network® comme les logiciels, les mises à jour d'URL, les licences et Autofocus. Une alternative à l'utilisation de l'interface MGT consiste à configurer un port de données (une interface classique) pour accéder à ces services. Le chemin entre l'interface et le service sur un serveur est appelé un *itinéraire de service*. Les paquets de service sortent du pare-feu par le port affecté au système virtuel, et le serveur envoie sa réponse à l'interface source et l'adresse IP source configurées.

Vous avez la possibilité de Configurer les itinéraires de servicede façon générale pour le pare-feu ou de customize service routes for a virtual system (personnaliser des itinéraires de service pour un système virtuel) sur un pare-feu adapté à de multiples systèmes virtuels, afin d'avoir la souplesse d'utilisation des interfaces associées à un système virtuel. Un système virtuel sur lequel aucun itinéraire de service n'est configuré pour un service spécifique hérite de l'interface et de l'adresse IP définies globalement pour ce service.

 ©2024 Palo Alto Networks, Inc.

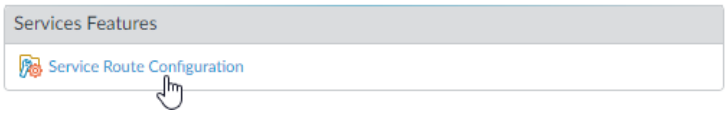
Configurer les itinéraires de service

La procédure suivante vous permet de configurer les itinéraires de service pour modifier l'interface que le pare-feu utilise pour envoyer des demandes à des services externes tels que les services cloud de Palo Alto Network ou pour le transfert de journaux. Pour les pare-feux dans une configuration haute disponibilité (HA) , la configuration de l'itinéraire de service est synchronisée entre les pairs HA

Pour les pare-feu dans une haute disponibilité (HA) active/passive, la route de service que vous avez configurée pour tirer parti d'un service externe ou pour le transfert de journaux ne voit l'activité que sur l'homologue HA `actif` tandis que l'homologue HA `passif` ne voit aucune activité si vous avez configuré une interface Ethernet comme l' **interface source**. Par exemple, vous configurez une route de service avec Ethernet 1/3 comme interface source pour transférer les journaux vers Cortex Data Lake. Dans ce scénario, tous les journaux sont transférés depuis l'homologue HA `actif` , mais aucun journal, y compris les journaux système et de configuration, n'est transféré depuis l'homologue HA `passif` . Toutefois, si vous configurez l'interface MGT en tant qu'**interface source**de la route de service, l'activité se produit à la fois sur les homologues HA `actifs` et `passifs` .

STEP 1 | Personnalisez des Itinéraires de service.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** > **Global** (ignorez Global sur un pare-feu non adapté à de multiples systèmes virtuels), et dans la section Fonctionnalités des Services, cliquez sur **Service Route Configuration (Configuration de l'itinéraire de service.)**.



2. Sélectionnez **Customize (Personnalisez)** puis l'une des options suivantes pour créer un itinéraire de service :
   - Pour un service prédéfini :
     - Sélectionnez **IPv4** ou **IPv6** puis cliquez sur le lien du service pour lequel vous souhaitez personnaliser l'itinéraire de service. Pour utiliser facilement les mêmes adresses de source pour plusieurs services, cochez les cases des services, cliquez sur Set Selected Routes (Définir les itinéraires de services), et passez à l'étape suivante.
     - Pour restreindre la liste Source Address (Adresse source), sélectionnez une **Source Interface (Interface source)**, puis sélectionnez une **Source Address (Adresse source)** (de cette interface) en tant qu'itinéraire de service. Un objet d'adresse peut également être référencé en tant qu'adresse source s'il est déjà configuré sur l'interface sélectionnée. Pour l'Interface Source, le fait de sélectionner **Any (Indifférent)** rend toutes les adresses IP de toutes les interfaces disponibles dans la liste dans laquelle vous sélectionnez une adresse. Le fait de sélectionner **Use Default (Utiliser les paramètres par défaut)** entraîne l'utilisation par le pare-feu de l'interface de gestion pour l'itinéraire de service, à moins que l'adresse IP de destination pour le paquet ne corresponde à l'adresse IP de destination configurée, auquel cas l'adresse IP source est définie par l'**Source Address (Adresse Source)** configurée pour la **Destination**. Le fait de sélectionner **MGT** entraîne

 ©2024 Palo Alto Networks, Inc.

l'utilisation par le pare-feu de l'interface MGT pour l'itinéraire de service, quel que soit l'itinéraire de service de destination.

L'adresse source de l'itinéraire de service n'hérite pas des modifications de configuration de l'interface référencée et vice versa. La modification d'une adresse IP d'interface en une adresse IP ou un objet d'adresse différent ne mettra pas à jour une adresse source d'itinéraire de service correspondante. Cela peut entraîner un échec de validation et vous obliger à mettre à jour les itinéraires de service vers une valeur d'adresse source valide.

- Cliquez sur **OK** pour enregistrer les paramètres.
- Répétez cette étape si vous voulez définir aussi bien une adresse IPv4 qu'une adresse IPv6 pour un service.

- Pour un itinéraire de service de destination :
  - Sélectionnez **Destination** et **Add (Ajoutez)** une adresse IP de **Destination**. Dans ce cas, si un paquet arrive avec une adresse IP de destination correspondant à cette adresse **Destination** configurée, alors l'adresse IP source du paquet sera définie par l'**Source Address (Adresse Source)** configurée dans l'étape suivante.
  - Pour restreindre la liste Source Address (Adresse source), sélectionnez une **Source Interface (Interface source)**, puis sélectionnez une **Source Address (Adresse source)** (de cette interface) en tant qu'itinéraire de service. Pour l'Interface Source, le fait de sélectionner **Any (Indifférent)** rend toutes les adresses IP de toutes les interfaces disponibles dans la liste dans laquelle vous sélectionnez une adresse. Le fait de sélectionner **MGT** entraîne l'utilisation par le pare-feu de l'interface MGT pour l'itinéraire de service.
  - Cliquez sur **OK** pour enregistrer les paramètres.

3. Répétez les étapes précédentes pour chaque itinéraire de service que vous souhaitez personnaliser.
4. Cliquez sur **OK** pour enregistrer la configuration de l'itinéraire de service.

STEP 2 | **Commit** (Valider).

 ©2024 Palo Alto Networks, Inc.

Itinéraires statiques

Les itinéraires statiques sont généralement utilisés conjointement avec les protocoles de routage dynamique. Vous pouvez configurer par exemple un itinéraire statique pour un emplacement qu'un protocole de routage dynamique ne peut atteindre. Les itinéraires statiques nécessitent d'être configurés manuellement sur chaque routeur du réseau, au lieu de laisser le pare-feu entrer des itinéraires dynamiques dans ses tables de routage. Malgré cette configuration nécessaire sur chaque routeur, les itinéraires statiques peuvent se révéler plus préférables, pour des petits réseaux, que la configuration d'un protocole de routage.

- Présentation des itinéraires statiques
- Suppression d'un itinéraire statique basé sur la surveillance des chemins
- Configuration d'un itinéraire statique
- Configuration de la surveillance des chemins pour un itinéraire statique

Présentation des itinéraires statiques

Si vous voulez que le trafic de couche 3 en particulier prenne un certain itinéraire sans participer aux protocoles de routage IP, vous pouvez Configuration d'un itinéraire statique en utilisant des itinéraires IPv4 et IPv6.

Un itinéraire par défaut est un itinéraire statique spécifique. Si vous n'utilisez pas de routage dynamique pour obtenir un itinéraire par défaut pour votre routeur virtuel, vous devez configurer un itinéraire par défaut statique. Quand le routeur virtuel reçoit un paquet entrant et qu'il ne trouve pas de correspondance pour la destination du paquet dans sa table d'itinéraire, le routeur virtuel envoie le paquet sur l'itinéraire par défaut. L'itinéraire IPv4 par défaut est 0.0.0.0/0 ; l'itinéraire IPv6 par défaut est ::/0. Vous pouvez configurer par défaut aussi bien un itinéraire IPv4 qu'un itinéraire IPv6.

Les itinéraires statiques ne changent pas d'eux-mêmes ou alors ils s'adaptent aux environnements réseau, donc le trafic n'est généralement pas réacheminé vers un point de terminaison défini de manière statique si une défaillance se produit. Toutefois, plusieurs possibilités s'offrent à vous pour sauvegarder des itinéraires statiques en cas de problème :

- Vous pouvez configurer un itinéraire statique avec un profil de détection de transmission bidirectionnelle (BFD) pour que, si une session BFD entre le pare-feu et l'homologue BFD échoue, le pare-feu supprime des tables RIB et FIB l'itinéraire qui a entraîné l'échec et utilise un itinéraire alternatif ayant une priorité moindre.
- Vous pouvez Configuration de la surveillance des chemins pour un itinéraire statique pour autoriser le pare-feu à utiliser un autre chemin.

Par défaut, les itinéraires statiques ont une distance administrative de 10. Si le pare-feu a le choix entre deux itinéraires ou plus vers une même destination, il utilisera l'itinéraire avec le moins de distance administrative. En donnant à la distance administrative d'un itinéraire statique une valeur supérieure à celle d'un itinéraire dynamique, vous pouvez utiliser l'itinéraire statique comme itinéraire de secours en cas d'indisponibilité de l'itinéraire dynamique.

Lorsque vous configurez un itinéraire statique, vous pouvez définir si le pare-feu installe un itinéraire statique IPv4 dans la table RIB monodiffusion ou multidiffusion, dans les deux, ou s'il n'en installe aucun. Par exemple, vous pouvez installer un itinéraire statique uniquement dans la table de routage multidiffusion car vous voulez que cet itinéraire soit emprunté uniquement par le trafic de multidiffusion. Cette option vous donne plus de contrôle sur les itinéraires qu'emprunte le trafic. Vous pouvez définir si le pare-feu installe un itinéraire statique IPv6 dans la table de routage ou non.

©2024 Palo Alto Networks, Inc.

Suppression d'un itinéraire statique basé sur la surveillance des chemins

La Configuration de la surveillance des chemins pour un itinéraire statique permet au pare-feu de détecter quand le chemin vers une ou plusieurs destinations est indisponible. Le pare-feu peut alors réacheminer le trafic à l'aide d'itinéraires alternatifs. Le pare-feu utilise la surveillance des chemins pour les itinéraires statiques de la même façon qu'il l'utilise pour la HD ou le transfert basé sur une politique (PBF), à savoir comme suit :

- Le pare-feu envoie des requêtes ICMP (pulsations) à une ou plusieurs destinations surveillées que vous avez identifiées comme étant solides et représentatives de la disponibilité des itinéraires statiques.
- Si les requêtes Ping vers cette destination ou ces destinations échouent, le pare-feu considère que l'itinéraire alternatif est également indisponible et le retire de sa base d'informations de routage (RIB) et de sa base d'informations de transfert (FIB). La table RIB est la table des itinéraires statiques avec laquelle le pare-feu est configuré ainsi que les itinéraires dynamiques qu'il a appris des protocoles de routage. La table FIB est la table de transfert des itinéraires utilisés par le pare-feu pour transférer les paquets. Le pare-feu sélectionne l'itinéraire statique alternatif pour la même destination (basé sur l'itinéraire avec la plus petite mesure) dans la table RIB et le place dans la table FIB.
- Le pare-feu continue à surveiller l'itinéraire indisponible. Quand l'itinéraire est à nouveau disponible, et (basé sur la condition d'échec **Any (Indifférent)** ou **All (n'importe laquelle)**) la surveillance des chemins est à nouveau active et le minuteur de suspension se met en route. La surveillance des chemins doit rester active pendant la durée du minuteur de suspension ; le pare-feu considère alors que l'itinéraire statique est stable et il l'intègre à nouveau dans la table RIB. Le pare-feu compare ensuite les mesures des itinéraires pour la même destination afin de décider quel itinéraire intégrer dans la table FIB.

La surveillance des chemins est un mécanisme souhaitable pour éviter de rejeter silencieusement le trafic pour :

- Un itinéraire statique ou par défaut.
- Un itinéraire statique ou par défaut redistribué dans un protocole de routage.
- Un itinéraire statique ou par défaut lorsqu'un homologue ne prend pas en charge la BFD. (la pratique exemplaire étant de ne pas activer la BFD et la surveillance des chemins sur une seule interface.)
- Un itinéraire statique ou par défaut au lieu d'utiliser la surveillance des chemins pour une règle de transfert basé sur une politique, ce qui ne supprime pas un itinéraire statique défaillant d'une table RIB ou d'une table FIB ou de la politique de redistribution.



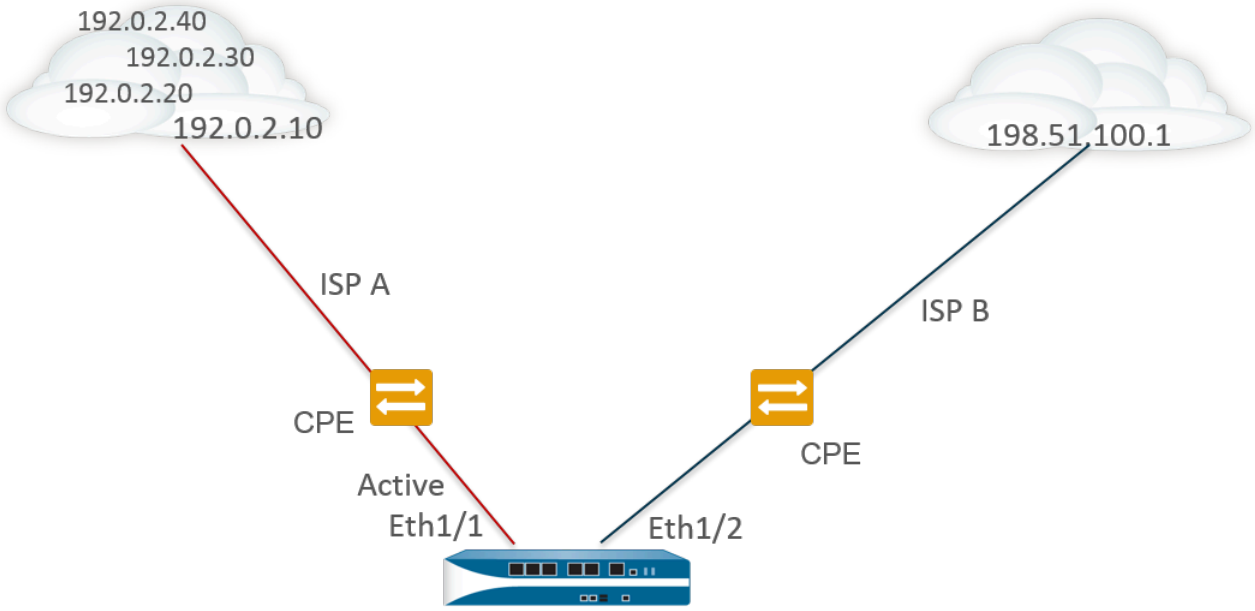
La surveillance des chemins ne s'applique pas aux itinéraires statiques configurés entre routeurs virtuels.

Dans la figure suivante, le pare-feu est connecté à deux ISP pour un routage redondant vers internet. L'itinéraire primaire par défaut 0.0.0.0 (mesure 10) utilise 192.0.2.10 comme adresse de saut suivant ; l'itinéraire secondaire par défaut 0.0.0.0 (mesure 50) utilise 198.51.100.1 comme adresse de saut suivant. Le CPE (Customer-premises equipment) pour l'ISP A maintient le lien physique primaire actif, même lorsque la connexion à internet est interrompue. Le lien étant actif

 ©2024 Palo Alto Networks, Inc.

artificiellement, le pare-feu n'arrive pas à détecter si le lien est indisponible et s'il est nécessaire de remplacer l'itinéraire défaillant avec un itinéraire secondaire dans sa table RIB.

Pour empêcher le rejet silencieux du trafic vers un lien défaillant, configurez la surveillance des chemins sur 192.0.2.20, 192.0.2.30 et 192.0.2.40 et si tous les chemins (ou n'importe lequel de ces chemins) vers ces destinations échouent, le pare-feu suppose que le chemin vers l'adresse de saut suivant 192.0.2.10 est également indisponible, il supprime l'itinéraire statique 0.0.0.0 (qui utilise le saut suivant 192.0.2.10) de sa table RIB et le remplace par l'itinéraire secondaire avec la même destination 0.0.0.0 (qui utilise le saut suivant 198.51.100.1), qui accède également à Internet.



Route Table

Destination	Next Hop	Metric	Interface	
0.0.0.0/0	192.0.2.10	10	ethernet1/1	X Pings to 192.0.2.20, 192.0.2.30, and 192.0.2.40 fail, so static route remove
0.0.0.0/0	198.51.100.1	50	ethernet1/2	

Lors de la Configuration d'un itinéraire statique, un des champs requis est le saut suivant vers une destination. Le type de saut suivant que vous configurez détermine l'action que le pare-feu entreprend lors de la surveillance des chemins, comme suit :

Si le type de Saut Suivant de l'Itinéraire Statique est :	Action du Pare-Feu pour une requête ping ICMP
Adresse IP	Le pare-feu utilise l'adresse IP source et l'interface de sortie de l'itinéraire statique comme adresse source et interface de sortie pour la requête ping ICMP. Il utilise l'adresse IP de destination configurée de la destination surveillée comme adresse de destination pour la requête ping. Il utilise l'adresse de saut suivant de l'itinéraire statique comme adresse de saut suivant pour la requête ping.

©2024 Palo Alto Networks, Inc.

Si le type de Saut Suivant de l'Itinéraire Statique est :	Action du Pare-Feu pour une requête ping ICMP
VR suivant	Le pare-feu utilise l'adresse IP source de l'itinéraire statique comme adresse source pour la requête ping ICMP. L'interface de sortie est basée sur le résultat de la recherche du routeur virtuel du saut suivant. L'adresse IP de destination configurée de la destination surveillée est l'adresse de destination pour la requête ping.
None	Le pare-feu utilise l'adresse IP de destination du chemin de surveillance comme saut suivant et envoie la requête ping ICMP à l'interface définie dans l'itinéraire statique.

Lorsque la surveillance des chemins d'un itinéraire statique ou par défaut échoue, le pare-feu consigne un événement critique (path-monitor-failure). Lorsque l'itinéraire statique ou par défaut se rétablit, le pare-feu consigne un nouvel événement critique (path-monitor-recovery).

Les pare-feux synchronisent les configurations des surveillances des chemins dans un déploiement HD actif/passif, mais le pare-feu bloque les paquets sortants des requêtes ping sur un homologue HD passif car il ne traite pas de trafic activement. Le pare-feu ne synchronise pas les configurations des surveillances des chemins dans les déploiements HD actif/actif.

©2024 Palo Alto Networks, Inc.

Configuration d'un itinéraire statique

Procédez comme suit pour configurer les Itinéraires statiques ou un itinéraire par défaut d'un routeur virtuel sur le pare-feu.

STEP 1 | Configurez un itinéraire statique.

1. Sélectionnez **Network (Réseau)** > **Virtual Router (Routeur virtuel)** et choisissez le routeur virtuel que vous configurez, par exemple **default (défaut)**.
2. Sélectionnez l'onglet **Static Routes (Itinéraires statiques)**.
3. Sélectionnez **IPv4 (IPv4)** ou **IPv6 (IPv6)**, selon le type d'itinéraire statique que vous souhaitez configurer.
4. **Ajoutez** un **nom** (63 caractères maximum) pour l'itinéraire. Le nom doit commencer par un caractère alphanumérique et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement (_), de trait d'union (-), de point (.) et d'espace.
5. Sous **Destination (Destination)**, saisissez l'itinéraire et le masque réseau (par exemple, 192.168.2.2/24 pour une adresse IPv4 ou 2001:db8:123:1::1/64 pour une adresse IPv6). Si vous créez un itinéraire par défaut, saisissez l'itinéraire par défaut (0.0.0.0/0 pour une adresse IPv4 ou ::/0 pour une adresse IPv6). Vous pouvez également créer un objet d'adresse de type Masque réseau IP.
6. (Facultatif) Sous **Interface (Interface)**, spécifiez l'interface sortante que les paquets doivent utiliser pour atteindre le saut suivant. Servez-vous de cette option pour disposer d'un contrôle plus strict quant à l'interface que le pare-feu utilisera au lieu de l'interface figurant dans la table de routage pour le saut suivant de cet itinéraire.
7. Sous **Next Hop (Saut suivant)**, sélectionnez l'une des options suivantes :

   - **IP Address (Adresse IP)** : saisissez l'adresse IP (par exemple, 192.168.56.1 ou 2001:db8:49e:1::1) lorsque vous souhaitez fixer l'itinéraire à suivre pour atteindre un certain saut suivant. Vous devez **Enable IPv6 on the interface (Activer IPv6 sur l'interface)** (lorsque vousConfigurer les interfaces de couche 3) de sorte qu'elles utilisent une adresse IPv6 de saut suivant. Si vous créez un itinéraire par défaut, sous **Next Hop (Saut suivant)** vous devez sélectionner **IP Address (Adresse IP)** et saisir l'adresse IP de votre passerelle Internet (par exemple, 192.168.56.1 ou 2001:db8:49e:1::1). Vous pouvez également créer un objet d'adresse de type Masque réseau IP. L'objet d'adresse doit avoir un masque réseau de /32 pour IPv4 ou de /128 pour IPv6.

     *Pendant la configuration des itinéraires statiques pour un routeur virtuel sur le pare-feu, vous pouvez entrer une adresse IP pour le routeur Next Hop (Saut suivant). Le pare-feu de Palo Alto Networks traite l'adresse IP du **Next Hop (Saut suivant)** comme un objet d'adresse. Par conséquent, si vous configurez la valeur de l'adresse IP du Saut suivant (**Network (Réseau)** > **Virtual Router (routeur virtuel - VR)** > **Static routes (Itinéraires statiques)**) de la même manière que le nom de l'objet Adresse configuré (**Objects (Objets)** > **Addresses (Adresses)**), toutes les modifications apportées à l'objet d'adresse seront également reflétées dans la valeur de l'adresse IP du **Next Hop (Saut suivant)**. Autrement dit, renommer l'objet d'adresse (**Objects (Objets)** > **Addresses (Adresses)**) renommera également l'adresse IP du Saut suivant.*

 ©2024 Palo Alto Networks, Inc.

- **Next VR (Routeur virtuel suivant)** : sélectionnez cette option, puis sélectionnez un routeur virtuel si vous souhaitez effectuer un routage en interne vers un autre routeur virtuel qui se trouve sur le pare-feu.
- **FQDN** —Saisissez un FQDN ou sélectionnez un objet d'adresse qui utilise un FQDN, ou créez un nouvel objet d'adresse de type FQDN.

  Si vous utilisez un FQDN en tant que saut suivant d'un itinéraire statique, ce FQDN doit se résoudre en une adresse IP qui appartient au même sous-réseau comme l'interface que vous avez configurée pour l'itinéraire statique. Sinon, le pare-feu rejette la résolution et le FQDN demeure non résolu.

  Le pare-feu n'utilise qu'une seule adresse IP (de chaque type de famille IPv4 ou IPv6) de la résolution DNS du FQDN. Si la résolution FQDN donne plus d'une adresse, le pare-feu utilise l'adresse IP privilégiée qui correspond au type de famille IP (Ipv4 ou IPv6) configuré pour le saut suivant. L'adresse IP privilégiée est la première adresse que le serveur DNS retourne dans sa réponse initiale. Le pare-feu conserve cette adresse en tant que privilégiée tant que l'adresse apparaît dans les réponses subséquentes, peu importe l'ordre.
- **Discard (Supprimer)** : sélectionnez cette option si vous voulez supprimer les paquets qui sont dirigés vers cette destination.
- **None (Aucun)** : sélectionnez cette option s'il n'existe aucun saut suivant pour l'itinéraire. Par exemple, il n'est pas nécessaire de définir de saut suivant pour une connexion de point à point, car les paquets ne peuvent suivre qu'une direction.

8. Saisissez une **Admin Distance (Distance admin)** si vous souhaitez que l'itinéraire remplace la distance administrative par défaut qui a été définie pour les itinéraires statiques de ce routeur virtuel (plage comprise entre 10 et 240 ; valeur par défaut : 10).
9. Saisissez une **Metric (Mesure)** pour l'itinéraire (plage comprise entre 1 et 65 535).

STEP 2 | Choisissez où installer l'itinéraire.

Sélectionnez la **Route Table (Table de routage)** dans laquelle vous souhaitez que le pare-feu installe l'itinéraire statique :

- **Unicast (monodiffusion)** : installe l'itinéraire dans la table de routage unicast. Choisissez cette option si vous souhaitez que l'itinéraire ne serve qu'au trafic unicast.
- **Multicast (multidiffusion)** : installe l'itinéraire dans la table de routage multicast (disponible pour les itinéraires IPv4 uniquement). Choisissez cette option si vous souhaitez que l'itinéraire ne serve qu'au trafic multicast.
- **Both (Les deux)** : installe l'itinéraire dans la table de routage unicast et multicast (disponible pour les itinéraires IPv4 uniquement). Choisissez cette option si vous souhaitez le trafic unicast ou multicast se serve de cet itinéraire.
- **No Install (Aucune installation)** : l'itinéraire n'est installé dans aucune table de routage.

STEP 3 | (Facultatif) Si le modèle de pare-feu que vous utilisez prend en charge supports la BFD, vous pouvez appliquer un **BFD Profile (Profil BFD)** à l'itinéraire statique. Ainsi, en cas d'échec de l'itinéraire statique, le pare-feu supprime l'itinéraire de la RIB et de la FIB et utilise un autre itinéraire. Valeur par défaut : **Aucune**.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Cliquez deux fois sur **OK**.

STEP 5 | **Commit (Validez)** la configuration.

 ©2024 Palo Alto Networks, Inc.

Configuration de la surveillance des chemins pour un itinéraire statique

Suivez la procédure ci-dessous pour configurer la suppression des itinéraires statiques basée sur la surveillance des chemins.

STEP 1 | Activez la surveillance des chemins pour un itinéraire statique.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez un routeur virtuel.
2. Sélectionnez **Static Routes (Itinéraires statiques)**, sélectionnez **IPv4 (IPv4)** ou **IPv6 (IPv6)**, puis sélectionnez l'itinéraire statique que vous souhaitez surveiller. Vous pouvez surveiller un maximum de 128 itinéraires statiques.
3. Sélectionnez **Path Monitoring (Surveillance des chemins)** pour activer la surveillance des chemins pour l'itinéraire.

STEP 2 | Configurez la ou les destinations surveillées pour l'itinéraire statique.

1. **Add (Ajoutez)** une destination surveillée par **Name (Nom)**. Vous pouvez ajouter un maximum de huit destinations surveillées par itinéraire statique.
2. Sélectionnez **Enable (Activer)** pour surveiller la destination.
3. Sous **Source IP (IP source)**, sélectionnez l'adresse IP que le pare-feu utilise dans la requête ping ICMP qu'il envoie à la destination surveillée :
   - Si l'interface possède plusieurs adresses IP, sélectionnez-en une.
   - Si vous sélectionnez une interface, le pare-feu utilise la première adresse IP affectée à l'interface par défaut.
   - Si vous sélectionnez **DHCP (Use DHCP Client address) (DHCP (Utiliser l'adresse du client DHCP))**, le pare-feu utilise l'adresse que DHCP a affectée à l'interface. Pour consulter l'adresse DHCP, sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet** et dans la ligne de l'interface Ethernet, cliquez sur **Dynamic DHCP Client (Client DHCP dynamique)**. L'adresse IP s'affiche dans la fenêtre Dynamic IP Interface Status (Statut de l'interface IP dynamique).
4. Sous **Destination IP (IP de destination)**, saisissez une adresse IP ou un objet d'adresse vers lequel le pare-feu surveillera les chemins. La destination surveillée et la destination de l'itinéraire statique doivent reposer sur la même famille d'adresses (IPv4 ou IPv6).

   L'adresse IP de destination doit appartenir à un point de terminaison fiable ; vous ne voulez pas fonder la surveillance des chemins sur un périphérique qui est lui-même instable ou non fiable.
5. (Facultatif) Indiquez le **Ping Interval (sec) (Intervalle de la requête ping (sec.)** ICMP en secondes pour déterminer la fréquence à laquelle le pare-feu surveille les chemins (la plage est comprise entre 1 et 60 ; la valeur par défaut est 3).
6. (Facultatif) Indiquez le **Ping Count (nombre de requêtes Ping)** ICMP des paquets qui ne sont pas renvoyés de la destination avant que le pare-feu considère que l'itinéraire

©2024 Palo Alto Networks, Inc.

statique est inactive et qu'il la supprime de la RIB et de la FIB (plage comprise entre 3 et 10 ; par défaut : 5).

7. Cliquez sur **OK**.

STEP 3 | Déterminez si la surveillance des chemins pour l'itinéraire statique est fondée sur une destination surveillée ou sur toutes les destinations surveillées et définissez le délai de maintien de préemption.

1. Sélectionnez une **Failure Condition (Condition d'échec)**, soit que **Any (n'importe laquelle)** ou **All (Toutes)** les destinations surveillées pour l'itinéraire statique sont inaccessibles par ICMP pour que le pare-feu supprime l'itinéraire statique de la RIB et de la FIB et ajoute l'itinéraire statique dont la métrique la plus faible suivante se dirige vers la même destination que la FIB.

   *Sélectionnez **All (Toutes)** pour éviter toute éventualité d'une seule destination surveillée signalant une défaillance d'itinéraire lorsque la destination est simplement hors ligne pour maintenance, par exemple.*

2. (Facultatif) Indiquez le **Preemptive Hold Time (min) (Délai de maintien de préemption (min.)**, soit le nombre de minutes pendant lesquelles une surveillance des chemins indisponibles doit demeurer à l'état Actif avant que le pare-feu ne réinstalle l'itinéraire statique dans la RIB. La surveillance des chemins évalue toute les destinations de l'itinéraire statique qui sont surveillées et est activée selon la condition d'échec définie, soit **Any (N'importe laquelle)** ou **All (Toutes)**. Si une liaison devient inactive ou instable pendant le délai de maintien, lorsque la liaison récupère, la surveillance des chemins peut reprendre et le minuteur redémarre lorsque la surveillance des chemins reprend l'état Actif.

   Un **Preemptive Hold Time (Délai de maintien de préemption)** de zéro permet au pare-feu de réinstaller l'itinéraire statique dans la RIB immédiatement après l'activation de la surveillance des chemins. La plage est comprise entre 0 et 1 440 ; la valeur par défaut est 2.

3. Cliquez sur **OK**.

STEP 4 | Validez.

Cliquez sur **Commit (Valider)**.

STEP 5 | Vérifiez la surveillance des chemins sur les itinéraires statiques.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et, dans la rangée du routeur virtuel qui vous intéresse, sélectionnez **More Runtime Stats (Statistiques d'exécution supplémentaires)**.
2. À l'onglet **Routing (Routage)**, sélectionnez **Static Route Monitoring (Surveillance des itinéraires statiques)**.
3. Pour un itinéraire statique (Destination), vérifiez si la surveillance des chemins est activée ou désactivée. La colonne Status (État) indique si l'itinéraire est Up (Actif), Down

 ©2024 Palo Alto Networks, Inc.

(Inactif) ou Disabled (Désactivé). Les indicateurs applicables à l'itinéraire statique sont les suivants : A—actif, S—statique, E—ECMP.

4. Sélectionnez **Refresh (Actualiser)** périodiquement pour voir l'état le plus récent de la surveillance des chemins (vérification de l'état).
5. Placez le curseur sur l'état d'un itinéraire pour voir les adresses IP surveillées et les résultats des requêtes ping envoyées aux destinations surveillées de cet itinéraire. Par exemple, un résultat de 3/5 indique un intervalle des requêtes ping de 3 secondes et un nombre de requêtes ping de 5 requêtes ping consécutives manquées (le pare-feu ne reçoit pas de requêtes ping au cours des 15 dernières secondes) signifie que la surveillance des chemins détecte un échec de la liaison. Selon la condition d'échec définie, soit **Any (Toutes)** ou **All (N'importe laquelle)**, si l'état de surveillance des chemins est échoué et que le pare-feu reçoit une requête ping après 15 secondes, on peut considérer que le chemin est actif et le **Preemptive Hold Time (Délai de maintien de préemption)** commence.

   L'état indique les résultats de la dernière requête ping des adresses surveillées : réussite ou échec. Un échec indique que la série de paquets de requêtes ping (intervalle des requêtes ping multiplié par le nombre de requêtes ping) n'a pas réussie. L'échec d'un seul paquet de requêtes ping n'indique pas forcément l'échec des requêtes ping.

STEP 6 | Consultez la RIB et la FIB pour vérifier la suppression de l'itinéraire statique.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et, dans la rangée du routeur virtuel qui vous intéresse, sélectionnez **More Runtime Stats (Statistiques d'exécution supplémentaires)**.
2. À partir de l'onglet **Routing (Routage)**, sélectionnez **Route Table (Table de routage)** (RIB) et **Forwarding Table (Table de transfert)** (FIB) pour les afficher.
3. Sélectionnez **Unicast (Monodiffusion)** ou **Multicast (Multidiffusion)** pour afficher la table de routage appropriée.
4. Sous **Display Address Family (Afficher la famille d'adresses)**, sélectionnez **IPv4 and IPv6 (IPv4 et IPv6)**, **IPv4 Only (IPv4 uniquement)** ou **IPv6 Only (IPv6 uniquement)**.
5. (Facultatif) Dans le champ de filtrage, saisissez l'itinéraire que vous cherchez et sélectionnez la flèche ou utilisez la barre de défilement pour parcourir les pages d'itinéraires.
6. Vérifiez si l'itinéraire est supprimé ou présent.
7. Sélectionnez **Refresh (Actualiser)** périodiquement pour voir l'état le plus récent de la surveillance des chemins (vérification de l'état).



*Pour voir les événements de surveillance des chemins qui ont été journalisés, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **System (Système)**. Affichez l'entrée qui se trouve sous **path-monitor-failure (échec de la surveillance des chemins)**, qui indique que la surveillance des chemins d'un itinéraire statique de destination a échoué et que, par conséquent, l'itinéraire a été supprimé. Affichez l'entrée qui se trouve sous **path-monitor-recovery (récupération de la surveillance des chemins)**, qui indique que la surveillance des chemins d'un itinéraire statique de destination a récupéré et que, par conséquent, l'itinéraire a été rétabli.*

 ©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

RIP

Déterminez si RIP est un protocole de routage approprié pour votre réseau et, le cas échéant, configurez RIP.

- Présentation de RIP
- Configurer RIP

Présentation de RIP

Le Routing Information Protocol (protocole d'informations de routage ; RIP) est un Interior Gateway Protocol (protocole de passerelle interne ; IGP) conçu pour les petits réseaux IP. Le protocole RIP s'appuie sur le nombre de sauts pour déterminer les itinéraires, dont les meilleurs affichent un nombre de sauts minimum. Ce protocole se base sur UDP et utilise le port 520 pour les mises à jour d'itinéraires. En limitant les itinéraires à un maximum de 15 sauts, le protocole empêche le développement de boucles de routage, mais limite aussi la taille du réseau pris en charge. Avant de configure RIP (configurer RIP), considérez que si plus de 15 sauts sont requis, le trafic n'est pas acheminé. La convergence du protocole RIP peut être plus longue que pour le protocole OSPF et d'autres protocoles de routage.

Le pare-feu prend en charge le protocole RIP v2.

©2024 Palo Alto Networks, Inc.

Configurer RIP

Utilisez la procédure suivante pour configurer RIP.

STEP 1 | Configurez les paramètres généraux du routeur virtuel.

STEP 2 | Configurez les paramètres généraux de configuration RIP.

1. Sélectionnez un routeur virtuel (**Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**) et pour le routeur virtuel, sélectionnez **RIP**.
2. Sélectionnez **Enable (Activer)** pour activer le protocole RIP.
3. Sélectionnez **Reject Default Route (Rejeter l'itinéraire par défaut)** si vous ne voulez pas apprendre des itinéraires via RIP par défaut. Il s'agit du paramètre par défaut recommandé.

   Décochez la case **Reject Default Route (Rejeter l'itinéraire par défaut)** si vous voulez autoriser la redistribution des itinéraires par défaut via OSPF.

STEP 3 | Configurez des interfaces pour RIP.

1. Dans l'onglet **Interfaces**, sélectionnez une interface dans la section Configuration de l'interface.
2. Sélectionnez une interface déjà définie.
3. Sélectionnez **Enable (Activer)**.
4. Sélectionnez **Advertise Default Route (Publier l'itinéraire par défaut)** pour publier un itinéraire par défaut dans les homologues RIP avec la valeur de la mesure spécifiée.
5. (Facultatif) Sélectionnez un profil dans la liste **Auth Profile (Profil d'authentification)**.
6. Sélectionnez le mode normal, passif ou envoyer uniquement dans la liste **Mode**.
7. (Facultatif) Pour activer BFD globalement RIP pour le routeur virtuel, sélectionnez un profil **BFD.**
8. Cliquez sur **OK**.

STEP 4 | Configurez des minuteurs RIP.

1. Dans l'onglet **Timers (Minuteurs)**, saisissez une valeur d'**Interval Seconds (sec) (Intervalle (s))**. Ce paramètre définit la longueur des intervalles du minuteur RIP suivant en secondes (plage comprise entre 60 et 1 ; valeur par défaut : 1).
2. Indiquez la valeur des **Update Intervals (Intervalles de mise à jour)** pour définir le nombre d'intervalles entre les annonces de mises à jour de l'itinéraire (plage comprise entre 1 et 3 600, valeur par défaut : 30).
3. Indiquez la valeur des **Expire Intervals (Intervalles d'expiration)** pour définir le nombre d'intervalles entre l'heure à laquelle l'itinéraire a été mis à jour pour la dernière fois et son expiration (plage comprise entre 1 et 3 600 ; valeur par défaut : 120).
4. Indiquez la valeur des **Delete Intervals (Intervalles de suppression)** pour définir le nombre d'intervalles entre l'expiration de l'itinéraire et sa suppression (plage comprise entre 1 et 3 600 ; valeur par défaut : 180).

 ©2024 Palo Alto Networks, Inc.

STEP 5 | (Facultatif) Configurez des profils d'authentification.

Par défaut, le pare-feu n'utilise pas l'authentification RIP pour l'échange entre voisins RIP. Vous pouvez éventuellement configurer une authentification RIP entre voisins RIP à l'aide d'un mot de passe simple ou de l'authentification MD5. L'authentification MD5 est recommandée ; elle est plus sécurisée qu'un simple mot de passe.

Authentification RIP par mot de passe simple

1. Sélectionnez **Auth Profiles (Profils d'authentification)** et **Add (Ajoutez)** un nom pour le profil d'authentification afin d'authentifier des messages RIP.
2. Sélectionnez **Simple Password (Mot de passe simple)** comme **Password Type (Type de mot de passe)**.
3. Saisissez un mot de passe simple et confirmez-le.

Authentification RIP MD5

1. Sélectionnez **Auth Profiles (Profils d'authentification)** et **Add (Ajoutez)** un nom pour le profil d'authentification afin d'authentifier des messages RIP.
2. Sélectionnez **MD5** comme **Password Type (Type de mot de passe)**.
3. **Add (Ajoutez)** une ou plusieurs entrées de mot de passe, notamment :
   - ID de clé (plage comprise entre 0 et 255)
   - Clé
4. (Facultatif) Sélectionnez l'état **Preferred (Préféré)**.
5. Cliquez sur **OK** pour spécifier la clé à utiliser pour authentifier un message sortant.
6. Cliquez de nouveau sur **OK** dans la boîte de dialogue Routeur virtuel - Profil d'authentification RIP.

STEP 6 | **Commit (Validez)** vos modifications.

 ©2024 Palo Alto Networks, Inc.

OSPF

Open Shortest Path First (ouverture du chemin le plus court en premier ; OSPF) est un Interior Gateway Protocol (protocole de passerelle interne ; IGP) qui est plus généralement utilisé pour gérer dynamiquement les itinéraires de réseaux d'entreprise d'envergure. Il détermine les itinéraires de façon dynamique en se procurant des informations auprès des autres routeurs et en publiant les itinéraires dans d'autres routeurs à l'aide des publications Link State Advertisements (annonce d'état de liaison ; LSA). Les informations collectées auprès des LSA sont utilisées pour créer une carte topologique du réseau. Cette carte topologique est partagée entre les itinéraires du réseau et utilisée pour renseigner la table de routage IP avec les itinéraires disponibles.

Les modifications apportées à la topologie du réseau sont détectées de manière dynamique afin de générer une nouvelle carte topologique en quelques secondes. Une arborescence de chemin le plus court est calculée pour chaque itinéraire. Les mesures associées à chaque interface de routage sont utilisées pour calculer le meilleur itinéraire. Celles-ci peuvent inclure la distance, le débit du réseau, la disponibilité des liaisons, etc. Ces mesures peuvent également être configurées de manière statique afin de diriger le résultat de la carte topologique OSPF.

L'implémentation d'OSPF de Palo Alto Networks® prend totalement en charge les RFC suivants :

- RFC 2328 (pour IPv4)
- RFC 5340 (pour IPv6)

Les rubriques suivantes fournissent des informations supplémentaires sur OSPF et les procédures de configuration d'OSPF sur le pare-feu :

- Concepts d'OSPF
- Configuration d'OSPF
- Configuration d'OSPFv3
- Configuration du redémarrage en douceur d'OSPF
- Confirmation du fonctionnement d'OSPF

Concepts d'OSPF

Le protocole OSPF détermine les itinéraires de façon dynamique en se procurant des informations auprès des autres routeurs et en publiant les itinéraires sur d'autres routeurs à l'aide des publications LSA (Link State Advertisements). Un routeur conserve des informations concernant les liaisons entre lui et la destination et peut prendre des décisions de routage hautement efficaces. Un coût est assigné à chaque interface de routeur et les meilleurs itinéraires sont ceux dont les coûts sont les plus bas, lorsque ceux de toutes les interfaces de routeur sortant rencontrées sont additionnés avec ceux de l'interface recevant la publication LSA.

Des techniques hiérarchiques sont utilisées pour limiter de nombre d'itinéraires à publier et les publications LSA associées. Étant donné que le protocole OSPF traite dynamiquement un volume considérable d'informations de routage, les exigences relatives à la configuration du processeur et de la mémoire sont beaucoup plus élevées que celles du protocole RIP.

Les rubriques suivantes présentent les concepts d'OSPF que vous devez connaître pour pouvoir configurer le pare-feu afin d'intégrer un réseau OSPF :

- OSPFv3
- Voisins OSPF
- Zones OSPF
- Types de routeurs OSPF

OSPFv3

OSPFv3 permet de prendre en charge le protocole de routage OSPF dans un réseau IPv6. Il permet ainsi de prendre en charge les adresses et préfixes IPv6. Il conserve la plupart de la structure et des fonctions d'OSPFv2 (pour IPv4) avec quelques changements mineurs. Voici certains des ajouts et changements par rapport à OSPFv3 :

- **Prise en charge de plusieurs instances par lien** : OSPFv3 vous permet d'exécuter plusieurs instances du protocole OSPF sur un même lien. Ceci est possible en attribuant un numéro d'identifiant d'instance OSPFv3. Une interface affectée à un identifiant d'instance abandonne les paquets contenant un identifiant différent.
- **Traitement de protocole par lien** : OSPFv3 fonctionne par lien et non par sous-réseau IP comme OSPFv2.
- **Modifications apportées à l'adressage** : les adresses IPv6 ne sont pas présentes dans les paquets OSPFv3, à l'exception des charges utiles LSA dans des paquets de mise à jour de l'état du lien. Les routeurs à proximité sont identifiés par leur identifiant.
- **Modifications apportées à l'authentification** : OSPFv3 n'inclut aucune fonction d'authentification. La configuration d'OSPFv3 sur un pare-feu nécessite un profil d'authentification qui précise la Encapsulating Security Payload (encapsulation de la charge utile de sécurité ; ESP) ou l'Authentication Header (en-tête d'authentification ; AH) IPv6. La procédure de recomposition spécifiée dans le document RFC 4552 n'est pas prise en charge dans cette version.
- **Prise en charge de plusieurs instances par lien** : chaque instance correspond à un ID d'instance contenu dans l'en-tête de paquet OSPFv3.

 ©2024 Palo Alto Networks, Inc.

- **Nouveaux types LSA** : OSPFv3 prend en charge deux nouveaux types LSA : Link LSA et Intra Area Prefix LSA.

Toutes les autres modifications sont décrites en détail dans le document RFC 5340.

Voisins OSPF

Deux routeurs compatibles OSPF connectés par un réseau commun dans la même zone OSPF qui établissent une relation sont appelés des voisins OSPF. La connexion entre ces routeurs peut se faire via un domaine de diffusion commun ou une connexion point-à-point. Cette connexion est établie par l'échange de paquets hello du protocole OSPF. Ces relations de voisinage sont utilisées pour échanger des mises à jour de routage entre les routeurs.

Zones OSPF

OSPF fonctionne dans un Autonomous System (système autonome ; AS) unique. Les réseaux présents dans cet AS unique peuvent toutefois être divisés en plusieurs zones. La Zone 0 est créée par défaut. La Zone 0 peut fonctionner seule ou servir de zone principale OSPF pour un grand nombre de zones. Chaque zone OSPF est nommée à l'aide d'un identifiant 32 bits qui, dans la plupart des cas, prend la même notation décimale séparée par des points qu'une adresse IP4. Par exemple, la Zone 0 se présente généralement sous la forme 0.0.0.0.

La topologie d'une zone est gérée dans sa propre base de données d'état de liaison et masquée des autres zones, réduisant ainsi le trafic de routage demandé par OSPF. La topologie est ensuite partagée sous forme récapitulative entre les zones par le biais d'un routeur.

Type de zone OSPF	Description
Zone principale	La zone principale (Zone 0) est le cœur d'un réseau OSPF. Toutes les autres zones y sont connectées et l'ensemble du trafic entre les zones doit la traverser. L'ensemble du routage entre les zones est distribué via la zone principale. Alors que toutes les autres zones OSPF doivent être connectées à la zone principale, cette connexion ne doit pas nécessairement être directe par le biais d'une liaison virtuelle.
Zone OSPF normale	Une zone OSPF normale ne comporte aucune restriction ; cette zone peut prendre en charge tous les types d'itinéraires.
Zone OSPF souche	Une zone souche ne reçoit pas d'itinéraires des autres systèmes autonomes. Le routage depuis la zone souche se fait via l'itinéraire par défaut en direction de la zone principale.
Zone NSSA	La zone Not So Stubby Area (zone pas si terminale ; NSSA) est un type de zone souche capable d'importer des itinéraires externes avec des exceptions limitées.

©2024 Palo Alto Networks, Inc.

Types de routeurs OSPF

Dans une zone OSPF, les routeurs sont répartis dans les catégories suivantes.

- **Routeur interne**: routeur n'ayant des relations de voisinage OSPF qu'avec des périphériques de la même zone.
- **Area Border Router (routeur de bordure de zone ; ABR)** : routeur ayant des relations de voisinage OSPF avec des périphériques de plusieurs zones OSPF. Les ABR collectent des informations topologiques dans les zones connectées et les transmettent à la zone principale.
- **Routeur principal** : un routeur principal est un routeur qui exécute OSPF et qui possède au moins une interface connectée à la zone OSPF principale. Les ABR étant toujours connectés à la zone principale, ils sont toujours considérés comme des routeurs principaux.
- **Autonomous System Boundary Router (routeur de bordure de systèmes autonomes ; ASBR)** : routeur associé à plusieurs protocoles de routage ; les ASBR échangent des informations de routage entre eux.

©2024 Palo Alto Networks, Inc.

Configuration d'OSPF

Une fois que vous avez Concepts d'OSPF, compris , effectuez la procédure suivante pour configurer OSPF.

STEP 1 | Configurez les paramètres généraux du routeur virtuel.

STEP 2 | Activez OSPF.

1. Sélectionnez l'onglet **OSPF (OSPF)**.
2. Sélectionnez **Enable (Activer)** pour activer le protocole OSPF.
3. Saisissez le **Router ID (ID de routeur)**.
4. Sélectionnez **Reject Default Route (Rejeter l'itinéraire par défaut)** si vous ne voulez pas apprendre des itinéraires via OSPF par défaut. Il s'agit du paramètre par défaut recommandé.

   Décochez la case **Reject Default Route (Rejeter l'itinéraire par défaut)** si vous voulez autoriser la redistribution des itinéraires par défaut via OSPF.

STEP 3 | Configurez le type de zone pour le protocole OSPF.

1. À l'onglet **Areas (Zones)**, **Add (Ajoutez)** un **Area ID (ID de zone)** pour la zone au format *x.x.x.x*. Il s'agit de l'identifiant devant faire partie de la même zone et que chaque voisin doit accepter.
2. Dans l'onglet **Type**, sélectionnez l'une des valeurs suivantes dans la liste **Type** de la zone :
   - **Normal (Normal)** - Aucune restriction n'est appliquée ; la zone peut accepter tout type d'itinéraire.
   - **Stub (Terminale)** : il n'existe aucune sortie issue de la zone. Pour atteindre une destination extérieure à la zone, vous devez passer par la bordure qui se connecte aux autres zones. Si vous sélectionnez cette option, configurez les options suivantes :
     - **Accept Summary (Accepter un récapitulatif)** : les Link State Advertisements (annonces d'état de liaison ; LSA) d'autres zones sont acceptées. Si cette option est désactivée dans une interface Area Border Router (routeur de bordure de zone ; ABR) d'une zone souche, la zone OSPF agira en tant que zone Totally Stubby Area (zone complètement terminale ; TSA) et l'interface ABR ne va propager aucune publication LSA récapitulative.
     - **Advertise Default Route (Publier l'itinéraire par défaut)** : les LSA de l'itinéraire par défaut seront incluses dans les publications destinées à la zone souche, ainsi qu'une valeur de mesure configurée dans la plage entre 1 et 255.
   - **NSSA (Not-So-Stubby Area (Zone pas si terminale ; NSSA))** : le pare-feu ne peut sortir de la zone que par des itinéraires autres que des itinéraires OSPF. Si vous sélectionnez NSSA, sélectionnez **Accept Summary (Accepter un récapitulatif)** et **Advertise Default Route (Publier l'itinéraire par défaut)** comme décrit pour **Stub (Souche)**. Si vous sélectionnez cette option, configurez les options suivantes :
     - **Type (Type)** : sélectionnez le type d'itinéraire **Ext 1(Ext 1)** ou **Ext 2 (Ext 2)** pour publier la LSA par défaut.

 ©2024 Palo Alto Networks, Inc.

- **Ext Ranges (Plages Ext)** : **Add (Ajoutez)** les plages d'itinéraires externes que vous souhaitez **Advertise (Publier)** ou pour lesquelles vous souhaitez **Suppress (Désactiver)** la publication.

3. Cliquez sur **OK**.

STEP 4 | Configurez une plage de zones pour le protocole OSPF.

1. Dans l'onglet **Range (Plage)**, **Add (Ajoutez)** adresses de destination LSA agrégées d'une zone dans des sous-réseaux.
2. **Advertise (Publiez)** ou **Suppress (Supprimez)** des publications LSA correspondant au sous-réseau et cliquez sur **OK**. Répétez cette étape pour ajouter des plages supplémentaires.

STEP 5 | Configurez des interfaces de zone pour le protocole OSPF.

1. Dans l'onglet **Interface (Interface)**, **Add (Ajoutez)** les informations suivantes pour chaque interface à inclure dans la zone :
   - **Interface** : sélectionnez une interface.
   - **Enable (Activer)** : sélectionnez cette option pour appliquer les paramètres de l'interface OSPF.
   - **Passive (Passif)** : sélectionnez cette option si vous ne voulez pas que l'interface OSPF envoie ou reçoive des paquets OSPF. Bien qu'aucun paquet OSPF ne soit envoyé ou reçu si vous choisissez cette option, l'interface est incluse dans la base de données LSA.
   - **Link type (Type de liaison)** : sélectionnez **Broadcast (Diffusion)** si vous voulez que tous les voisins accessibles via l'interface soient détectés automatiquement en multidiffusant des messages Hello OSPF, comme une interface Ethernet. Sélectionnez **p2p** (point-to-point/point à point) pour détecter automatiquement un voisin. Sélectionnez **p2mp** (point-to-multipoint/point-multipoint) lorsque les voisins doivent être définis manuellement et **Add (Ajoutez)** saisissez les adresses IP de tous les voisins accessibles via cette interface.
   - **Metric (Mesure)** : saisissez la mesure OSPF pour cette interface (plage entre 0 et 65 535, par défaut 0).
   - **Priority (Priorité)** : saisissez une priorité OSPF pour cette interface. Il s'agit de la priorité d'élection d'un routeur en tant que Designated Router (routeur désigné - DR) ou en tant que Backup Designated Router (routeur désigné de secours - BDR) (plage entre 0 et 255, par défaut 1). Lorsque la valeur 0 est configurée, le routeur ne sera pas élu en tant que DR ou BDR.
   - **Auth Profile (Profil d'authentification)** : sélectionnez un profil d'authentification précédemment défini.
   - **Timing (Minutage)** : modifiez les paramètres de minutage, si vous le désirez (non recommandé). Pour obtenir des informations détaillées sur ces paramètres, consultez la section Aide en ligne.
2. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Configurez des liaisons virtuelles de zone.

1. Dans l'onglet **Virtual Link (Liaison virtuelle)**, **Add (Ajoutez)** les informations suivantes pour chaque liaison virtuelle à inclure dans la zone principale :
   - **Name (Nom)** : donnez un nom à la liaison virtuelle.
   - **Enable (Activer)** : sélectionnez cette option pour activer la liaison virtuelle.
   - **Neighbor ID (ID du voisin)** : saisissez un ID de routeur (voisin) situé de l'autre côté de la liaison virtuelle.
   - **Transit Area (Zone de transit)** : saisissez l'ID de la zone de transit qui contient physiquement la liaison virtuelle.
   - **Timing (Minutage)** : il est recommandé de conserver les paramètres de minutage par défaut.
   - **Auth Profile (Profil d'authentification)** : sélectionnez un profil d'authentification précédemment défini.
2. Cliquez sur **OK (OK)** pour enregistrer les liaisons virtuelles.
3. Cliquez sur **OK (OK)** pour enregistrer la zone.

STEP 7 | (Facultatif) Configurez des profils d'authentification.

Par défaut, le pare-feu n'utilise pas l'authentification OSPF pour l'échange entre voisins OSPF. Vous pouvez éventuellement configurer une authentification OSPF entre voisins OSPF à l'aide d'un mot de passe simple ou de l'authentification MD5. L'authentification MD5 est recommandée ; elle est plus sécurisée qu'un simple mot de passe.

Authentification OSPF par mot de passe simple

1. Sélectionnez l'onglet **Auth Profiles (Profils d'autorisation)** et **Add (Ajoutez)** un nom pour le profil d'authentification qui authentifiera les messages OSPF.
2. Sélectionnez **Simple Password (Mot de passe simple)** comme **Password Type (Type de mot de passe)**.
3. Saisissez un mot de passe simple et confirmez-le.

Authentification OSPF MD5

1. Sélectionnez l'onglet **Auth Profiles (Profils d'autorisation)** et **Add (Ajoutez)** un nom pour le profil d'authentification qui authentifiera les messages OSPF.
2. Sélectionnez **MD5 (MD5)** comme **Password Type (Type de mot de passe)**, puis **Add (Ajoutez)** une ou plusieurs entrées de mot de passe, y compris :
   - ID de clé (plage comprise entre 0 et 255)
   - Clé
   - Sélectionnez l'option **Preferred (Préféré)** pour spécifier que la clé sera utilisée pour authentifier les messages sortants.
3. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | Configurez des options OSPF avancées.

1. Dans l'onglet **Advanced (Avancé)**, sélectionnez **RFC 1583 Compatibility (Compatibilité RFC 1583)** pour assurer la compatibilité avec RFC 1583.
2. Indiquez une valeur pour le minuteur **SPF Calculation Delay (sec) (Délai du calcul SPF (s))**, qui vous permet d'ajuster le délai écoulé (en secondes) entre la réception de nouvelles informations sur la topologie et la réalisation d'un calcul SPF. Des valeurs inférieures permettent une reconvergence OSPF plus rapide. Les routeurs échangeant du trafic avec le pare-feu doivent utiliser la même valeur afin d'optimiser les délais de convergence.
3. Spécifiez une valeur pour le minuteur **LSA Interval (sec) (Intervalle LSA (s))**, qui indique le délai minimum écoulé entre les transmissions de deux instances de la même LSA (même routeur, même type, même ID LSA). Cela équivaut à MinLSInterval dans le document RFC 2328. Des valeurs inférieures peuvent être utilisées pour réduire les délais de reconvergence en cas de modifications de topologie.
4. Cliquez sur **OK**.

STEP 9 | **Commit (Validez)** vos modifications.

 ©2024 Palo Alto Networks, Inc.

Configuration d'OSPFv3

OSPF prend en charge les adresses IPv4 et IPv6. Vous devez l'utiliser OSPFv3 si vous utilisez IPv6.

STEP 1 | Configurez les paramètres généraux du routeur virtuel.

STEP 2 | Configurez les paramètres généraux de configuration OSPFv3.

1. Sélectionnez l'onglet **OSPFv3 (OSPFv3)**.
2. Sélectionnez **Enable (Activer)** pour activer le protocole OSPF.
3. Saisissez le **Router ID (ID de routeur)**.
4. Sélectionnez **Reject Default Route (Rejeter l'itinéraire par défaut)** si vous ne voulez pas apprendre des itinéraires via OSPFv3 par défaut. Il s'agit du paramètre par défaut recommandé.

   Décochez la case **Reject Default Route (Rejeter l'itinéraire par défaut)** si vous voulez autoriser la redistribution des itinéraires par défaut via OSPFv3.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Configurez un profil d'authentification pour le protocole OSPFv3.

OSPFv3 n'incluant personnellement aucune fonction d'authentification, il repose ainsi entièrement sur IPSec pour sécuriser les communications entre voisins.

Lors de la configuration d'un profil d'authentification, vous devez utiliser l'Encapsulating Security Payload (encapsulation de la charge utile de sécurité ; ESP) (recommandé) ou l'Authentication Header (en-tête d'authentification ; AH) IPv6.

Authentification OSPFv3 ESP

1. À l'onglet **Auth Profiles (Profils d'autorisation)**, **Add (Ajoutez)** un nom pour le profil d'authentification qui authentifiera les messages OSPFv3.
2. Indiquez un Security Policy Index (indice de politique de sécurité ; **SPI**) (valeur en format hexadécimal compris dans une plage allant de 00000000 à FFFFFFFF). Les deux extrémités de l'adjacence OSPFv3 doivent avoir des valeurs SPI correspondantes.
3. Sélectionnez **ESP (ESP)** pour **Protocol (Protocole)**.
4. Sélectionnez un **Crypto Algorithm (Algorithme de chiffrement)**.

   Vous pouvez sélectionner **None (Aucun)** ou un des algorithmes suivants : **SHA1 (SHA1)**, **SHA256 (SHA256)**, **SHA384 (SHA384)**, **SHA512 (SHA512)** ou **MD5 (MD5)**.
5. Si un **Crypto Algorithm (Algorithme crypto)** autre que None (Aucune) est sélectionné, saisissez une valeur de **Key (Clé)**, puis confirmez.

Authentification OSPFv3 AH

1. À l'onglet **Auth Profiles (Profils d'autorisation)**, **Add (Ajoutez)** un nom pour le profil d'authentification qui authentifiera les messages OSPFv3.
2. Spécifiez un **SPI (indice de politique de sécurité)**. Le SPI doit correspondre entre les deux extrémités de l'adjacence OSPFv3. Le numéro SPI doit être une valeur hexadécimale comprise entre 00000000 et FFFFFFFF.
3. Sélectionnez **AH (AH)** pour **Protocol (Protocole)**.
4. Sélectionnez un **Crypto Algorithm (Algorithme de chiffrement)**.

   Vous devez spécifier un des algorithmes suivants : **SHA1 (SHA1)**, **SHA256 (SHA256)**, **SHA384 (SHA384)**, **SHA512 (SHA512)** ou **MD5 (MD5)**.
5. Saisissez une valeur de **Key (Clé)**, puis confirmez.
6. Cliquez sur **OK**.
7. Cliquez de nouveau sur **OK (OK)** dans la boîte de dialogue Virtual Router - OSPF Auth Profile (Routeur virtuel - Profil d'authentification OSPF).

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Configurez le type de zone pour le protocole OSPFv3.

1. À l'onglet **Areas (Zones)**, **Add (Ajoutez)** un **Area ID (ID de zone)**. Il s'agit de l'identifiant devant faire partie de la même zone et que chaque voisin doit accepter.
2. Dans l'onglet **General (Général)**, sélectionnez l'une des valeurs suivantes dans la liste **Type** de la zone :
   - **Normal (Normal)** - Aucune restriction n'est appliquée ; la zone peut accepter tout type d'itinéraire.
   - **Stub (Terminale)** : il n'existe aucune sortie issue de la zone. Pour atteindre une destination extérieure à la zone, vous devez passer par la bordure qui se connecte aux autres zones. Si vous sélectionnez cette option, configurez les options suivantes :
     - **Accept Summary (Accepter un récapitulatif)** : les Link State Advertisements (annonces d'état de liaison ; LSA) d'autres zones sont acceptées. Si cette option est désactivée dans une interface Area Border Router (routeur de bordure de zone ; ABR) d'une zone souche, la zone OSPF agira en tant que zone Totally Stubby Area (zone complètement terminale ; TSA) et l'interface ABR ne va propager aucune publication LSA récapitulative.
     - **Advertise Default Route (Publier l'itinéraire par défaut)** : les LSA de l'itinéraire par défaut seront incluses dans les publications destinées à la zone souche, ainsi qu'une valeur de mesure configurée dans la plage entre 1 et 255.
   - **NSSA (Not-So-Stubby Area (Zone pas si terminale ; NSSA))** : le pare-feu ne peut sortir de la zone que par des itinéraires autres que des itinéraires OSPF. Si cette option est sélectionnée, configurez **Accept Summary (Accepter un récapitulatif)** et **Advertise Default Route (Publier l'itinéraire par défaut)** comme décrit pour **Stub (Souche)**. Si vous sélectionnez cette option, configurez les options suivantes :
     - **Type (Type)** : sélectionnez le type d'itinéraire **Ext 1(Ext 1)** ou **Ext 2 (Ext 2)** pour publier la LSA par défaut.
     - **Ext Ranges (Plages Ext)** : **Add (Ajoutez)** des plages d'itinéraires externes pour lesquelles vous souhaitez activer ou désactiver les publications.

STEP 5 | Associez un profil d'authentification OSPFv3 à une zone ou à une interface.

À une zone

1. Dans l'onglet **Areas (Zones)**, sélectionnez une zone existante dans la table.
2. Dans l'onglet **General (Général)**, sélectionnez un **Authentication Profile (Profil d'authentification)** précédemment défini dans la liste **Authentication (Authentification)**.
3. Cliquez sur **OK**.

À une interface

1. Dans l'onglet **Areas (Zones)**, sélectionnez une zone existante dans la table.
2. Sélectionnez l'onglet **Interface (Interface)** et **Add (Ajoutez)** le profil d'authentification que vous souhaitez associer à l'interface OSPF dans la liste **Auth Profile (Profil d'authentification)**.
3. Cliquez sur **OK**.

STEP 6 | Cliquez de nouveau sur **OK** pour enregistrer les paramètres de zone.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | (Facultatif) Configurez des règles d'exportation.

1. À l'onglet **Export Rules (règles d'exportation)**, sélectionnez **Allow Redistribute Default Route (Autoriser la redistribution des itinéraires par défaut)** si vous voulez autoriser la redistribution des itinéraires par défaut via OSPFv3.
2. Cliquez sur **Add (Ajouter)**.
3. Saisissez le **Name (Nom)** ; la valeur doit être un sous-réseau IPv6 valide ou un nom de profil de redistribution valide.
4. Sélectionnez **New Path Type (Nouveau type de chemin)**, **Ext 1 (Ext 1)** ou **Ext 2 (Ext 2)**.
5. Indiquez une **New Tag (Nouvelle étiquette)** pour l'itinéraire correspondant, en utilisant une valeur de notation décimale séparée par des points de 32 bits.
6. Affectez une **Metric (Mesure)** à la nouvelle règle (plage entre 1 et -16 777 215).
7. Cliquez sur **OK**.

STEP 8 | Configurez des options OSPFv3 avancées.

1. Dans l'onglet **Advanced (Avancé)**, sélectionnez **Disable Transit Routing for SPF Calculation (Désactiver le routage de transit pour le calcul SPF)** si vous souhaitez que le pare-feu soit intégré à la distribution de la topologie OSPF sans être utilisé pour transférer du trafic de transit.
2. Indiquez une valeur pour le minuteur **SPF Calculation Delay (sec) (Délai du calcul SPF (s))**, qui vous permet d'ajuster le délai écoulé (en secondes) entre la réception de nouvelles informations sur la topologie et la réalisation d'un calcul SPF. Des valeurs inférieures permettent une reconvergence OSPF plus rapide. Les routeurs échangeant du trafic avec le pare-feu doivent utiliser la même valeur afin d'optimiser les délais de convergence.
3. Spécifiez une valeur pour le minuteur **LSA Interval (sec) (Intervalle LSA (s))**, qui indique le délai minimum écoulé (en secondes) entre les transmissions de deux instances de la même LSA (même routeur, même type, même ID LSA). Cela équivaut à MinLSInterval dans le document RFC 2328. Des valeurs inférieures peuvent être utilisées pour réduire les délais de reconvergence en cas de modifications de topologie.
4. (Facultatif) Configuration du redémarrage en douceur d'OSPF.
5. Cliquez sur **OK**.

STEP 9 | **Commit (Validez)** vos modifications.

 ©2024 Palo Alto Networks, Inc.

Configuration du redémarrage en douceur d'OSPF

Le redémarrage en douceur d'OSPF instruit aux voisins OSPF de continuer à utiliser des itinéraires via un pare-feu pendant une brève transition lorsqu'il est hors service. Ce comportement améliore la stabilité du réseau en réduisant la fréquence de reconfiguration de la table de routage et le battement de l'itinéraire lié pouvant se produire pendant de courts temps d'arrêt périodiques.

Pour un pare-feu Palo Alto Networks®, le redémarrage en douceur d'OSPF implique les opérations suivantes :

- **Pare-feu en tant que périphérique de redémarrage** : si le pare-feu sera arrêté pendant une brève période de temps ou qu'il est indisponible pendant de courts intervalles, il envoie des LSA de grâce à ses voisins OSPF. Les voisins doivent être configurés pour s'exécuter en mode d'aide de redémarrage en douceur. En mode d'aide, le voisin reçoit les LSA de grâce qui l'informent que le pare-feu va procéder à un redémarrage en douceur dans une période de temps définie en tant que **Grace Period (Période de grâce)**. Pendant la période de grâce, le voisin continue à transférer des itinéraires via le pare-feu et à envoyer des LSA qui annoncent des itinéraires via le pare-feu. Si le pare-feu recommence à fonctionner avant l'expiration de la période de grâce, le transfert du trafic se poursuit comme avant sans interruption réseau. Si le pare-feu ne recommence pas à fonctionner après l'expiration de la période de grâce, les voisins quittent le mode d'aide et reviennent en fonctionnement normal, ce qui implique une reconfiguration de la table de routage afin de contourner le pare-feu.
- **Pare-feu en tant qu'aide de redémarrage en douceur** : si les routeurs à proximité peuvent être arrêtés pendant de courtes périodes, le pare-feu peut être configuré pour fonctionner en mode d'aide de redémarrage en douceur, auquel cas le pare-feu utilise un **Max Neighbor Restart Time (Délai de redémarrage max. du voisin)**. Lorsque le pare-feu reçoit les LSA de grâce de son voisin OSPF, il continuera d'acheminer le trafic vers le voisin et de publier les itinéraires via le voisin jusqu'à ce que la période de grâce ou le délai de redémarrage max. du voisin arrive à expiration. Si aucun n'arrive à expiration avant la remise en service du voisin, le transfert du trafic se poursuit comme avant sans interruption réseau. Si l'une des périodes arrive à expiration avant la remise en service du voisin, le pare-feu quitte le mode d'aide et revient en fonctionnement normal, ce qui implique une reconfiguration de la table de routage afin de contourner le voisin.

STEP 1 | Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel que vous voulez configurer.

STEP 2 | Sélectionnez **OSPF (OSPF)** > **Advanced (Avancé)** ou **OSPFv3 (OSPFv3)** > **Advanced (Avancé)**.

STEP 3 | Vérifiez que les options suivantes sont cochées (elles sont activées par défaut) :

- **Enable Graceful Restart (Activer le redémarrage en douceur)**
- **Enable Helper Mode (Activer le mode Aide)**
- **Enable Strict LSA Checking (Activer la vérification LSA stricte)**

Elles doivent rester cochées, sauf si nécessaire en fonction de votre topologie.

STEP 4 | Configurez une **Grace Period (Période de grâce)** en secondes.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Configurez un **Max Neighbor Restart Time (Délai de redémarrage max. du voisin)** en secondes.

 ©2024 Palo Alto Networks, Inc.

Confirmation du fonctionnement d'OSPF

Une fois qu'une configuration OSPF a été validée, vous pouvez utiliser l'une des opérations suivantes pour confirmer le fonctionnement d'OSPF :

- Affichage de la table de routage
- Confirmation des adjacences OSPF
- Confirmation que des connexions OSPF sont établies

Affichage de la table de routage

L'affichage de la table de routage vous permet de voir si des itinéraires OSPF ont été établis. La table de routage est accessible à partir de l'interface Web ou de la CLI. Si vous utilisez la CLI, utilisez les commandes suivantes :

- **`show routing route`**
- **`show routing fib`**

Si vous utilisez l'interface Web pour afficher la table de routage, utilisez le flux de travail suivant :

STEP 1 | Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et, dans la même rangée que le routeur virtuel qui vous intéresse, cliquez sur le lien **More Runtime Stats (Statistiques d'exécution supplémentaires)**.

STEP 2 | Sélectionnez **Routing (Routage)** > **Route Table (Table d'itinéraire)** et observez la colonne **Flags (Indicateurs)** de la table de routage pour consulter les itinéraires appris par OSPF.

Confirmation des adjacences OSPF

Servez-vous du flux de travail suivant confirmer que les adjacences OSPF ont été établies :

STEP 1 | Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et, dans la même rangée que le routeur virtuel qui vous intéresse, cliquez sur le lien **More Runtime Stats (Statistiques d'exécution supplémentaires)**.

STEP 2 | Sélectionnez **OSPF (OSPF)** > **Neighbor (Voisin)** et consultez la colonne **Status (État)** pour déterminer si des adjacences OSPF ont été établies.

Confirmation que des connexions OSPF sont établies

Affichez le journal système pour confirmer que le pare-feu a établé des connexions OSPF.

STEP 1 | Sélectionnez **Monitor (Surveillance)** > **System (Système)** et recherchez des messages pour confirmer que des adjacences OSPF ont été établies.

STEP 2 | Sélectionnez **OSPF (OSPF)** > **Neighbor (Voisin)** et consultez la colonne **Status (État)** pour déterminer si des adjacences OSPF ont été établies (sont complètes).

©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

BGP

Le protocole BGP (Border Gateway Protocol) est le principal protocole de routage Internet. Il détermine l'accessibilité du réseau en fonction des préfixes IP qui sont disponibles dans les systèmes autonomes (AS) où un AS correspond à un ensemble de préfixes IP qu'un fournisseur de réseau a choisi d'inclure à une politique de routage unique.

- Présentation de BGP
- MP-BGP
- Configuration de BGP
- Configuration d'un homologue BGP avec le protocole MP-BGP en mode multicast IPv4 ou IPv6
- Configuration d'un homologue BGP avec le protocole MP-BGP en mode multicast IPv4
- Confédérations BGP

Présentation de BGP

BGP fonctionne entre des systèmes autonomes (BGP extérieur ou eBGP) ou au sein d'un AS (BGP intérieur ou iBGP) pour échanger des informations de routage et d'accessibilité avec les écouteurs BGP. Le pare-feu fournit une implémentation BGP complète qui inclut les fonctionnalités suivantes :

- La spécification d'une instance de routage BGP pour chaque routeur virtuel.
- Des paramètres BGP par routeur virtuel, qui incluent des paramètres de base comme un identifiant d'itinéraire local et un AS local, ainsi que des options avancées comme la sélection de chemins, un réflecteur d'itinéraires, des confédérations BGP, l'atténuation par oscillation d'itinéraires et le redémarrage en douceur.
- Les paramètres des voisins et des groupes d'homologues, qui incluent l'adresse d'un voisin et un AS distant, ainsi que des options avancées comme les attributs et les connexions des voisins.
- Des politiques de routage pour contrôler les itinéraires d'importation, d'exportation et de publication, le filtrage basé sur un préfixe et l'agrégation d'adresses.
- L'interaction IGP-BGP visant à injecter des itinéraires dans le protocole BGP à l'aide de profils de redistribution.
- Des profils d'authentification, qui indiquent la clé d'authentification MD5 pour les connexions BGP. L'authentification permet de prévenir les fuites d'itinéraires et les attaques DoS réussies.
- L'extension multi-protocole (MP-BGP) permet aux homologues BGP de transporter des itinéraires unicast IPv6 et des itinéraires multicast IPv4 dans les paquets de mise à jour et permet au pare-feu et à un homologue BGP de communiquer entre eux à l'aide d'adresses IPv6.
- BGP prend en charge un maximum de 255 numéros AS dans une liste AS_PATH pour un préfixe.

 ©2024 Palo Alto Networks, Inc.

MP-BGP

BGP prend en charge les préfixes de monodiffusion IPv4, mais un réseau BGP qui utilise des routes de multidiffusion IPv4 ou des préfixes de monodiffusion IPv6 nécessite un multiprotocole BGP (MP-BGP) afin d'échanger des routes de types d'adresse autres que de monodiffusion IPv4. MP-BGP permet aux homologues BGP de transporter des routes de multidiffusion IPv4 et des routes de monodiffusion IPv6 dans les paquets de mise à jour, en plus des routes de monodiffusion IPv4 que les homologues BGP peuvent acheminer sans que MP-BGP ne soit activé.

De cette façon, MP-BGP fournit une connectivité IPv6 à vos réseaux BGP qui utilisent IPv6 natif ou IPv4 et IPv6 à double pile. Les fournisseurs de services peuvent offrir le service IPv6 à leurs clients et les entreprises peuvent utiliser le service IPv6 auprès des fournisseurs de services. Le pare-feu et un homologue BGP peuvent communiquer entre eux en utilisant des adresses IPv6.

Pour que BGP prenne en charge plusieurs protocoles de couche réseau (autres que BGP pour IPv4), extensions multiprotocole pour BGP-4 (RFC 4760) vous devez utiliser le NLRI (Network Layer Reachability Information) dans un attribut NLRI multiprotocole accessible où le pare-feu envoie et reçoit dans les paquets de mise à jour BGP. Cet attribut contient des informations sur le préfixe de destination, y compris ces deux identifiants :

- Le Address Family Identifier (identifiant de famille d'adresses ; AFI), tel que défini par l'IANA dans les Address Family (numéros de famille d'adresse), indique que le préfixe de destination est une adresse IPv4 ou IPv6. (PAN-OS prend en charge les interfaces AFI IPv4 et IPv6.)
- Le Subsequent Address Family Identifier (autre identifiant de famille d'adresses ; SAFI) dans PAN-OS indique que le préfixe de destination est une adresse de monodiffusion ou de multidiffusion (si l'AFI est IPv4) ou que le préfixe de destination est une adresse de monodiffusion (si l'AFI est IPv6). PAN-OS ne prend pas en charge la multidiffusion IPv6.

Si vous activez MP-BGP pour la multidiffusion IPv4 ou si vous configurez une route statique de multidiffusion, le pare-feu prend en charge des tables de routage distinctes en monodiffusion et en multidiffusion pour les routes statiques. Vous pourriez vouloir séparer le trafic monodiffusion et multidiffusion allant à la même destination. Le traffic multicast peut prendre un chemin différent que le traffic de monodifussion, par exemple si ce traffic était dans un état critique et que vous avez besoin d'augmenter son efficacité en réduisant le nombre de sauts ou en réduisant la latence.

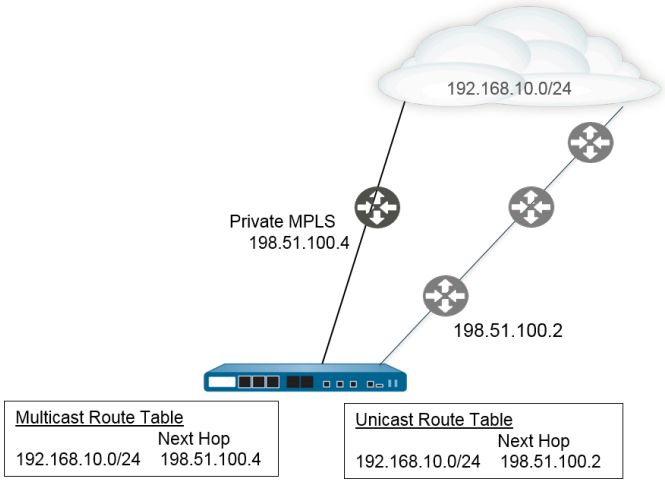
Vous pouvez également exercer plus de contrôle sur la manière dont BGP fonctionne en configurant BGP pour utiliser uniquement les routes de la table de routage monodiffusion ou multidiffusion (ou les deux) lorsque BGP importe ou exporte des routes, envoie des annonces conditionnelles ou effectue une redistribution de route ou une agrégation de route.

Vous pouvez décider d'utiliser une RIB multidiffusion dédiée (table de routage) en activant MP-BGP et en sélectionnant la famille d'adresses IPv4 et la famille d'adresses suivantes de multidiffusion ou en installant une route statique IPv4 dans la table de routage multidiffusion. Une fois que vous avez effectué l'une ou l'autre de ces méthodes pour utiliser la RIB de multidiffusion, le pare-feu utilise la RIB de multidiffusion pour tous les routages de multidiffusion et le transfert de chemin inverse (RPF). Si vous préférez utiliser la RIB unicast pour tous les routages (unicast et multicast), vous ne devez pas activer la RIB multicast par l'une ou l'autre méthode.

Dans la figure suivante, une route statique vers 192.168.10.0/24 est installée dans la table de routage monodiffusion et son prochain tronçon est 198.51.100.2. Cependant, le trafic de multidiffusion peut emprunter un chemin différent vers un nuage privé MPLS ; la même route

 ©2024 Palo Alto Networks, Inc.

statique est installée dans la table de routage de multidiffusion avec un saut suivant différent (198.51.100.4) de sorte que son chemin est différent.



L'utilisation de tables de routage monodiffusion et multidiffusion distinctes vous offre plus de flexibilité et de contrôle lorsque vous configurez ces fonctions BGP :

- Installez une route statique IPv4 dans la table de routage unicast ou multicast, ou les deux, comme décrit dans l'exemple précédent. (Vous pouvez installer un itinéraire statique IPv6 uniquement dans la table de routage monodiffusion).
- Créer une règle d'importation afin que tous les préfixes correspondant aux critères soient importés dans la table de routage monodiffusion ou multidiffusion, ou les deux.
- Créez une règle d'exportation afin que les préfixes correspondant aux critères soient exportés (envoyés à un homologue) à partir de la table de routage monodiffusion ou multidiffusion, ou les deux.
- Configurez une annonce conditionnelle avec un filtre Non Exist (Non Existant) afin que le pare-feu recherche la table de routage monodiffusion ou multidiffusion (ou les deux) pour s'assurer que la route n'existe pas dans cette table et donc le pare-feu annonce une route différente.
- Configurez une annonce conditionnelle avec un filtre d'Annonce afin que le pare-feu annonce les routes correspondant aux critères de la table de routage monodiffusion ou multidiffusion, ou les deux.
- Redistribuez une route qui apparaît dans la table de routage monodiffusion ou multidiffusion, ou les deux.
- Configurez l'agrégation de route avec un filtre d'annonce afin que les routes agrégées à annoncer proviennent de la table de routage monodiffusion ou multidiffusion, ou les deux.
- Inversement, configurez l'agrégation de route avec un filtre de suppression afin que les routes agrégées qui doivent être supprimées (non annoncées) proviennent de la table de routage monodiffusion ou multidiffusion, ou les deux.

Lorsque vous configurez un homologue avec MP-BGP à l'aide d'une famille d'adresses IPv6, vous pouvez utiliser les adresses IPv6 dans les champs préfixe d'adresse et saut suivant d'une règle d'importation, d'une règle d'exportation, d'une annonce conditionnelle (filtre d'annonce et filtre non existant), et d'une règle d'agrégation (filtre d'annonce, filtre de suppression et attribut route agrégée).

 ©2024 Palo Alto Networks, Inc.

Configuration de BGP

Procédez comme suit pour configurer BGP.

STEP 1 | Configurez les paramètres généraux du routeur virtuel.

STEP 2 | Activer le BGP pour le routeur virtuel, affectez un ID de routeur et affectez le routeur virtuel à un AS.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez un routeur virtuel.
2. Sélectionnez **BGP (BGP)**.
3. **Enable (Activez)** BGP pour ce routeur virtuel.
4. Affectez un **Router ID (ID de routeur)** au BGP pour le routeur virtuel ; il s'agit généralement d'une adresse IPv4, ce qui permet de garantir que l'ID de routeur est unique.
5. Affectez le **AS Number (Numéro de l'AS)** : le numéro de l'AS auquel appartient le routeur virtuel, en fonction de l'ID du routeur (place comprise entre 1 et 4 294 967 295).
6. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Configurez les paramètres généraux de configuration de BGP.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez un routeur virtuel.
2. Sélectionnez **BGP (BGP)** > **Général (Général)**.
3. Sélectionnez **Reject Default Route (Rejeter l'itinéraire par défaut)** pour ignorer les itinéraires par défaut publiés par les homologues BGP.
4. Sélectionnez **Install Route (Installer l'itinéraire)** pour installer des itinéraires BGP dans la table de routage générale.
5. Sélectionnez **Aggregate MED (Agréger MED)** pour activer l'agrégation d'un itinéraire, même lorsque des itinéraires affichent différentes valeurs Multi-Exit Discriminator (discriminateur Multi-Sortie ; MED)).
6. Indiquez la **Default Local Preference ((Préférence locale par défaut))** qui peut être utilisée pour déterminer des préférences entre différents chemins.
7. Sélectionnez le **AS Format (Format de l'AS)** à des fins d'interopérabilité :
   - **2 octets** (par défaut)
   - **4 octets**

   Les statistiques d'exécution affichent des numéros AS BGP de 4 octets à l'aide d'une notation asplain conforme à la norme RFC 5396.
8. Activez ou désactivez chacun des paramètres de **Path Selection (Sélection des chemins)** suivants :
   - **Always Compare MED (Toujours comparer les MED)** - Activez cette comparaison afin de sélectionner des chemins provenant de voisins de différents systèmes autonomes.
   - **Deterministic MED Comparison (Comparaison de MED déterministe)** - Activez cette comparaison afin de sélectionner un itinéraire parmi ceux qui sont publiés par des homologues IBGP (homologues BGP figurant dans le même système autonome).
9. Sous **Auth Profiles (Profils d'authentification)**, **Add (Ajoutez)** un profil d'authentification :
   - **Profile Name (Nom du profil)** - Saisissez un nom pour identifier le profil.
   - **Secret/Confirm Secret (Phrase secrète/Confirmer une phrase secrète)** - Saisissez et confirmez une phrase secrète pour les communications d'homologues BGP. La phrase secrète sert de clé lors de l'authentification MD5.
10. Cliquez deux fois sur **OK**.

STEP 4 | (Facultatif) Configurez des paramètres de BGP.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez un routeur virtuel.
2. Sélectionnez **BGP (BGP)** > **Advanced (Avancés)**.
3. Sélectionnez **ECMP Multiple AS Support (Prise en charge d'ECMP par plusieurs systèmes autonomes)** si vous avez configuré ECMP et que vous souhaitez exécuter ECMP sur plusieurs systèmes BGP autonomes.
4. **Enforce First AS for EBGP (Appliquez eBGP au premier système autonome)** (activé par défaut) pour amener le pare-feu à supprimer un paquet de Mise à jour entrant d'un

 ©2024 Palo Alto Networks, Inc.

homologue eBGP qui ne répertorie pas le numéro AS de l'homologue eBGP comme premier numéro AS dans l'attribut AS_PATH.

5. Sélectionnez **Graceful Restart (Redémarrage en douceur)** et configurez les minuteurs suivants :
   - **Stale Route Time (sec) (Durée d'itinéraire hors service (s))** : spécifiez la durée (en secondes) pendant laquelle un itinéraire peut rester à l'état hors service (plage comprise entre 1 et 3 600, valeur par défaut : 120).
   - **Local Restart Time (sec) (Délai de redémarrage local (s))** : spécifiez le délai d'attente (en secondes) du périphérique local avant de redémarrer. Cette valeur est publiée chez les homologues (intervalle compris entre 1 et 3 600 ; valeur par défaut : 120).
   - **Max Peer Restart Time (sec) (Délai maximum de redémarrage des homologues (s))** : indiquez la durée maximale (en secondes) qu'un équipement local accepte comme délai de redémarrage en période de grâce pour des périphériques homologues (plage comprise entre 1 et 3 600 ; valeur par défaut : 120).
6. Sous **Reflector Cluster ID (ID du groupe de réflecteurs)**, indiquez un identifiant IPv4 pour représenter un groupe de réflecteurs.
7. Sous **Confederation Member AS (As membre de la confédération)**, indiquez le numéro d'identification du système autonome (également nommé numéro de système sous-autonome) qui n'est visible qu'au sein de la confédération BGP. Pour plus d'informations, consultez Confédérations BGP.
8. **Add (Ajoutez)** les informations suivantes pour chaque profil d'atténuation que vous souhaitez configurer, sélectionnez **Enable (Activer)**, puis cliquez sur **OK (OK)** :
   - **Profile Name (Nom du profil)** - Saisissez un nom pour identifier le profil.
   - **Cutoff (Limite)** - Indiquez le seuil de retrait d'itinéraires au-delà duquel une publication d'itinéraire est supprimée (intervalle compris entre 0,0 et 1 000,0 ; valeur par défaut : 1,25).
   - **Reuse (Réutiliser)** - Indiquez le seuil de retrait d'itinéraires au-dessous duquel un itinéraire supprimé est réutilisé (intervalle compris entre 0,0 et 1 000,0 ; valeur par défaut : 5).
   - **Max Hold Time (sec) (Délai d'attente max. (s))** : indiquez la durée maximale (en secondes) au bout de laquelle un itinéraire peut être supprimé, quel que soit son degré d'instabilité (plage comprise entre 0 et 3 600 ; valeur par défaut 900).
   - **Decay Half Life Reachable (sec) (Réduction de moitié pendant l'état accessible (s))** : indiquez la durée (en secondes) au bout de laquelle la mesure de stabilité d'un itinéraire est réduite de moitié si l'itinéraire est jugé comme étant accessible (plage comprise entre 0 et 3 600 secondes ; valeur par défaut : 300).
   - **Decay Half Life Reachable (sec) (Réduction de moitié pendant l'état inaccessible (s))** : indiquez la durée (en secondes) au bout de laquelle la mesure de stabilité d'un itinéraire est réduite de moitié si l'itinéraire est jugé comme étant inaccessible (plage comprise entre 0 et 3 600 ; valeur par défaut : 300).
9. Cliquez deux fois sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Configurez un groupe d'homologues BGP.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez un routeur virtuel.
2. Sélectionnez **BGP (BGP)** > **Peer Group (Groupe d'homologues)**, **Add (Ajoutez)** un **Name (Nom)** pour le groupe d'homologues, puis **Enable (Activez)**-le.
3. Sélectionnez **Aggregated Confed AS Path (Chemin d'AS de confédération agrégé)** pour inclure un chemin vers un AS de confédération agrégé configuré.
4. Sélectionnez **Soft Reset with Stored Info (Réinitialisation logicielle avec infos stockées)** pour procéder à une réinitialisation logicielle du pare-feu après avoir mis à jour les paramètres des homologues.
5. Sélectionnez le **Type (Type)** de groupe d'homologues :
   - **IBGP** - **Export Next Hop (Exporter le saut suivant)** : Sélectionnez **Original (Original)** ou **Use self (Utiliser auto)**.
   - **EBGP Confed (Confédération EBGP)** - **Export Next Hop (Exporter le saut suivant)** : Sélectionnez **Original (Original)** ou **Use self (Utiliser auto)**.
   - **EBGP Confed (Confédération EBGP)** - **Export Next Hop (Exporter le saut suivant)** : Sélectionnez **Original (Original)** ou **Use self (Utiliser auto)**.
   - **EBGP (EBGP)** - **Import Next Hop (Importer le saut suivant)** : Sélectionnez **Original (Original)** ou **Use self (Utiliser auto)** ; puis **Export Next Hop (Exportez le saut suivant)** : Spécifiez **Resolve (Résoudre)** ou **Use self (Utiliser auto)**. Sélectionnez **Remove Private AS (Supprimer l'AS privé)** si vous voulez forcer le protocole BGP à supprimer des numéros d'AS privés provenant de l'attribut AS_PATH des mises à jour que le pare-feu envoie à un homologue d'un autre AS.
6. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Configurez un homologue BGP qui appartient au groupe d'homologues et précisez son adressage.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez un routeur virtuel.
2. Sélectionnez **BGP (BGP)** > **Peer Group (Groupe d'homologues)**, puis sélectionnez le groupe d'homologues que vous avez créé.
3. Sous Peer (homologue), **Add (Ajoutez)** un homologue en indiquant son **Name (Nom)**.
4. **Enable (Activez)** l'homologue.
5. Saisissez le **Peer AS (AS de l'homologue)** auquel le routeur virtuel appartient.
6. Sélectionnez **Addressing (Adressage)**.
7. Sous **Local Address (Adresse locale)**, sélectionnez l'**Interface (Interface)** pour laquelle vous configurez BGP. Si l'interface possède plus d'une adresse **IP (IP)**, saisissez l'adresse IP de cette interface qui doit lui permettre de servir d'homologue BGP.
8. Sous **Peer Address (Adresse de l'homologue)**, sélectionnez **IP** et saisissez l'adresse IP ou sélectionnez ou créez un objet d'adresse, ou sélectionnez **FQDN** et saisissez le FQDN ou l'objet d'adresse de type FQDN.

   Le pare-feu n'utilise qu'une seule adresse IP (de chaque type de famille IPv4 ou IPv6) de la résolution DNS du FQDN. Si la résolution FQDN donne plus d'une adresse, le pare-feu utilise l'adresse IP privilégiée qui correspond au type de famille IP (Ipv4 ou IPv6) configuré pour l'homologue BGP. L'adresse IP privilégiée est la première adresse que le serveur DNS retourne dans sa réponse initiale. Le pare-feu conserve cette adresse en tant que privilégiée tant que l'adresse apparaît dans les réponses subséquentes, peu importe l'ordre.
9. Cliquez sur **OK**.

STEP 7 | Configurez les paramètres de connexion de l'homologue BGP.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez un routeur virtuel.
2. Sélectionnez **BGP (BGP)** > **Peer Group (Groupe d'homologues)**, puis sélectionnez le groupe d'homologues que vous avez créé.
3. Sélectionnez le **Peer (Homologue)** que vous avez configuré.
4. Sélectionnez les **Connection Options (Options de connexion)**.
5. Sélectionnez un **Auth Profile (Profil d'authentification)** pour l'homologue.
6. Définissez un **Keep Alive Interval (sec) (Intervalle Keep Alive (sec)** : il s'agit de l'intervalle après lequel les itinéraires d'un homologue sont supprimés conformément au paramètre de durée d'attente (intervalle compris entre 0 et 1 200 ; valeur par défaut : 30).
7. Définissez la valeur **Multi Hop (Plusieurs sauts)** : il s'agit de la valeur Time-To-Live (durée de vie ; TTL) dans l'en-tête IP (intervalle compris entre 0 et 255 ; valeur par défaut : 0.) La valeur par défaut de 0 signifie 1 pour IBGP. La valeur par défaut de 0 signifie 255 pour IBGP.
8. Définissez le **Open Delay Time (sec) (Délai avant ouverture (sec.))** : le délai écoulé, en secondes, entre l'établissement d'une liaison TCP et l'envoi par le pare-feu du premier

 ©2024 Palo Alto Networks, Inc.

message d'ouverture BGP pour établir une connexion BGP (intervalle compris entre 0 et 240 ; valeur par défaut : 0).

9. Indiquez le **Hold Time (sec) (Temps d'attente (sec.)** : la durée du temps, en secondes, qui peut s'écouler entre des messages Keepalive ou Update successifs émis par l'homologue avant la fermeture de la connexion (plage comprise entre 3 et 3 600 ; valeur par défaut : 90).
10. Indiquez la **Idle Hold Time (sec) (Durée d'attente en inactivité (sec.)**, soit la durée d'attente (en secondes) avant de retenter une connexion à l'homologue (intervalle compris entre 1 et 3 600 ; valeur par défaut : 15).
11. Définissez le **Min Route Advertisement Interval (sec) (Intervalle de publication de l'itinéraire min (sec).)** : la quantité de temps, en secondes, entre deux messages de mise à jour successifs qu'un haut-parleur BGP (le pare-feu) envoie à un homologue BGP qui publie des itinéraires ou des retraits d'itinéraires (la plage est comprise entre 1 et 600 ; valeur par défaut : 30).
12. Sous **Incoming Connections (Connexions entrantes)**, saisissez un **Remote Port (Port distant)** et sélectionnez **Allow (Autoriser)** pour autoriser le trafic entrant vers ce port.
13. Sous **Outgoing Connections (Connexions sortantes)**, saisissez un **Local Port (Port local)** et sélectionnez **Allow (Autoriser)** pour autoriser le trafic sortant de ce port.
14. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | Configurez les paramètres Client réflecteur d'itinéraire, Type d'échange de trafic, Nombre maximal de préfixes et Bidirectional Forwarding Detection (détection de transmission bidirectionnelle ; BFD) de l'homologue BGP.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez un routeur virtuel.
2. Sélectionnez **BGP (BGP)** > **Peer Group (Groupe d'homologues)**, puis sélectionnez le groupe d'homologues que vous avez créé.
3. Sélectionnez le **Peer (Homologue)** que vous avez configuré.
4. Sélectionnez **Advanced (Avancé)**.
5. Sous **Reflector Client (Client réflecteur)**, sélectionnez l'une des options suivantes :
   - **non-client (non-client)** (par défaut) : l'homologue n'est pas un client réflecteur d'itinéraire.
   - **client (client)** : l'homologue est un client réflecteur d'itinéraire.
   - **Client avec maillage**
6. Sous **Peering Type (Type d'échange de trafic)**, sélectionnez l'une des options suivantes :
   - **Bilateral (Bilatéral)** : Les deux homologues BGP établissent une connexion entre homologues.
   - **Unspecified (non spécifiée)** (par défaut).
7. Pour **Max Prefixes (Nombre maximal de préfixes)**, entrez le nombre maximal de préfixes IP à importer à partir de l'homologue (plage comprise entre 1 et 100 000) ou sélectionnez **unlimited (illimité)**.
8. Pour activer **BFD (BFD)** pour l'homologue (et ainsi appliquer un contrôle prioritaire sur le paramètre BFD pour BGP, pourvu que BFD ne soit pas activé pour BGP au niveau du routeur virtuel), sélectionnez l'une des options suivantes :
   - **default (par défaut)** : l'homologue n'utilise que les paramètres par défaut.
   - **Inherit-vr-global-setting (Hériter des paramètres généraux du routeur virtuel)** (par défaut) : l'homologue hérite du profil BFD que vous avez sélectionné globalement pour le BGP du routeur virtuel.
   - Un profil BFD que vous avez configuré ; voir la section Création d'un profil BFD.

   *Sélectionnez **Disable BFD (Désactiver la BFD)** pour désactiver la BFD sur l'homologue BGP.*
9. Cliquez sur **OK**.

STEP 9 | Configurez des règles d'importation et d'exportation.

Les règles d'importation et d'exportation servent à importer et à exporter des itinéraires d'autres routeurs ou vers d'autres routeurs (par exemple, importer l'itinéraire par défaut de votre fournisseur d'accès à Internet).

1. Sélectionnez **Importer**, **Ajouter** un nom (maximum de 63 caractères) dans le champ **Règles** . Le nom doit commencer par un caractère alphanumérique et peut contenir une

 ©2024 Palo Alto Networks, Inc.

combinaison de caractères alphanumériques, de trait de soulignement (_), de trait d'union (-), de point (.) et d'espace.

2. **Enable (Activez)** la règle.
3. **Add (Ajoutez)** le **Peer Group (Groupe d'homologues)** duquel les itinéraires seront importés.
4. Sélectionnez **Match (Correspondance)** et définissez les options utilisées pour filtrer les informations de routage. Vous pouvez également définir la valeur MED (Multi-Exit Discriminator) et une valeur de saut suivant vers des routeurs ou sous-réseaux pour le filtrage des itinéraires. L'option MED est une mesure externe qui permet aux voisins de connaître le chemin préféré dans un AS. Une valeur faible est préférée à une valeur élevée.
5. Sélectionnez **Action (Action)** et définissez l'action à entreprendre (autoriser ou refuser) en fonction des options de filtrage définies dans l'onglet **Match (Correspondance)**. Si vous sélectionnez **Deny (Refuser)**, vous n'avez pas à définir d'options supplémentaires. Si vous sélectionnez **Allow (Autoriser)**, vous devez alors définir les autres attributs.
6. Cliquez sur **OK**.
7. Sélectionnez **Export (Exportation)** et définissez des attributs d'exportation, qui sont similaires aux paramètres **Import (Importation)**, mais qui sont utilisés pour contrôler les informations d'itinéraire exportées du pare-feu vers les voisins. Le nom de la règle d'exportation peut comporter un maximum de 31 caractères.

STEP 10 | Configurez la publication conditionnelle, qui vous permet de contrôler l'itinéraire à publier au cas où un itinéraire différent ne serait pas disponible dans la table de routage BGP local (LocRIB) et indiquerait un échec de partage de réseau ou d'accessibilité.

Ceci est utile dans les cas où vous souhaitez forcer des itinéraires vers un AS en direction d'un autre. Par exemple, lorsque vous disposez de liaisons vers Internet passant par plusieurs ISP et que vous voulez que le trafic soit acheminé vers un fournisseur à la place d'un autre, sauf s'il y a une perte de connectivité avec le fournisseur préféré.

1. Sélectionnez **Conditional Adv (Publication conditionnelle)**, puis **Add (Ajoutez)** un nom de **Policy (Politique)**.
2. **Enable (Activez)** la publication conditionnelle.
3. Dans la section **Used By (Utilisé par)**, **Add (Ajoutez)** les groupes d'homologues qui utiliseront la politique de publication conditionnelle.
4. Sélectionnez **Non Exist Filter (Filtre inexistant)** et définissez le ou les préfixes réseau de l'itinéraire préféré. Ceci indique l'itinéraire que vous voulez publier, s'il est disponible dans la table de routage BGP local. Si la publication d'un préfixe est prévue et qu'il correspond à un filtre inexistant, la publication sera supprimée.
5. Sélectionnez **Advertise Filters (Publier des filtres)** et définissez les préfixes de l'itinéraire dans la table de routage RIB local devant être publiés au cas où un itinéraire du filtre inexistant serait indisponible dans la table de routage local. Si la publication d'un préfixe est prévue et qu'il ne correspond pas à un filtre inexistant, la publication aura lieu.
6. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 11 | Configurez des options d'agrégation de récapitulatif des itinéraires dans la configuration de BGP.

L'agrégation d'itinéraire BGP est utilisée pour contrôler comment BGP agrège les adresses. Chaque entrée de la table entraîne la création d'une adresse agrégée. Une entrée agrégée est ainsi créée dans la table de routage lorsqu'au moins un itinéraire spécifique correspondant à l'adresse spécifiée est appris.

1. Sélectionnez **Aggregate (Agréger)**, puis **Add (Ajoutez)** un nom à l'adresse agrégée.
2. Saisissez le **Prefix (Préfixe)** réseau qui sera le préfixe agrégé principal.
3. Sélectionnez **Suppress Filters (Supprimer des filtres)** et définissez les attributs qui entraîneront la suppression des itinéraires correspondants.
4. Sélectionnez **Advertise Filters (Publier des filtres)** et définissez les attributs qui entraîneront la publication aux homologues des itinéraires correspondants.
5. Cliquez sur **OK**.

STEP 12 | Configurez des règles de redistribution.

Cette règle est utilisée pour redistribuer des itinéraires hôtes et inconnus qui ne figurent pas dans la RIB locale vers les routeurs homologues.

1. Sélectionnez **Redist Rules (Règles de redistribution)**, puis **Add (Ajoutez)** une nouvelle règle de redistribution.
2. Saisissez le **Name (Nom)** d'un sous-réseau IP ou sélectionnez un profil de redistribution. Si nécessaire, vous pouvez également configurer un nouveau profil de redistribution.
3. **Enable (Activez)** la règle.
4. Saisissez la **Metric (Mesure)** d'itinéraire qui sera utilisée pour la règle.
5. Dans la liste **Set Origin (Origine définie)**, sélectionnez **incomplete (incomplète)**, **igp (igp)** ou **egp (egp)**.
6. (Facultatif) Définissez des valeurs de MED, de préférence locale, de limite de chemins AS et de communauté.
7. Cliquez sur **OK**.

STEP 13 | **Commit (Validez)** vos modifications.

 ©2024 Palo Alto Networks, Inc.

Configuration d'un homologue BGP avec le protocole MP-BGP en mode multicast IPv4 ou IPv6

Après la configure du protocole BGP, configurez un homologue BGP avec le protocole MP-BGP en mode unicast pour l'une ou l'autre des raisons suivantes :

- Pour que votre homologue BGP transporte les itinéraires unicast IPv6, configurez MP-BGP en indiquant **IPv6 (IPv6)** comme type de famille d'adresses et **Unicast (Unicast)** comme famille d'adresses subséquentes pour que l'homologue puisse envoyer les mises à jour BGP qui incluent des itinéraires unicast IPv6. Les adresses des homologues BGP (adresse locale et adresse de l'homologue) peuvent être des adresse IPv4 ou IPv6.
- Pour procéder à l'homologation BGP sur les adresses IPv6 (la **Local Address (Adresse locale)** et la **Peer Address (Adresse de l'homologue)** utilisent des adresses IPv6).

La tâche suivante illustre comment activer MP-BGP sur un homologue BGP afin qu'il puisse transporter des itinéraires unicast IPv6 et échanger du trafic en utilisant des adresses IPv6.

La tâche illustre également comment afficher des tables de routage unicast et multicast et comment afficher la table de transfert, la table de routage BGP RIB local ou la table de routage BGP RIB Out (itinéraire envoyés aux voisins) pour voir les itinéraires de la table de routage unicast ou multicast ou une famille d'adresses particulière (IPv4 ou IPv6).

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Sélectionnez Enable MP-BGP Extensions (Activer les extensions MP-BGP) pour un homologue.

Configurez les éléments suivants pour qu'un homologue BGP puissent transporter des itinéraires unicast IPv4 ou IPv6 dans les paquets de mise à jour et que le pare-feu puisse utiliser des adresses IPv4 ou IPv6 pour communiquer avec son homologue.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel que vous configurez.
2. Sélectionnez **BGP (BGP)**.
3. Sélectionnez **Peer Group (Groupe d'homologues)** et sélectionnez un groupe d'homologues.
4. Sélectionnez un homologue BGP (routeur).
5. Sélectionnez **Addressing (Adressage)**.
6. Sélectionnez **Enable MP-BGP Extensions (Activer les extensions MP-BGP)** pour l'homologue.
7. Sous **Address Family Type (Type de famille d'adresses)**, sélectionnez **IPv4 (IPv4)** ou **IPv6 (IPv6)**. Par exemple, sélectionnez IPv6.
8. Sous **Subsequent Address Family (Famille d'adresses subséquentes)**, **Unicast (Unicast)** est sélectionné. Si vous choisissez **IPv4 (IPv4)** comme famille d'adresses, vous pouvez également sélectionnez **Multicast (Multicast)**.
9. Sous **Local Address (Adresse locale)**, sélectionnez une **Interface (Interface)** et éventuellement une adresse **IP (IP)**, par exemple, 2001:DB8:55::/32.
10. Sous **Peer Address (Adresse de l'homologue)**, saisissez l'adresse **IP (IP)** de l'homologue, en utilisant la même famille d'adresses (IPv4 ou IPv6) que pour l'adresse locale, par exemple, 2001:DB8:58::/32.
11. Sélectionnez **Advanced (Avancé)**.
12. (Facultatif) **Enable Sender Side Loop Detection (Activez la détection des boucles côté expéditeur).** Lorsque vous activez la détection des boucles côté expéditeur, le pare-feu vérifiera l'attribut AS_PATH d'un itinéraire dans le BGP RIB avant d'envoyer l'itinéraire dans une mise à jour afin de s'assurer que le numéro AS de l'homologue n'est pas sur la liste AS_PATH. Le pare-feu n'annonce pas la route si le numéro AS de l'homologue figure au sein de la liste AS_PATH. Généralement, le récepteur détecte les boucles, mais cette fonctionnalité d'optimisation permet d'effectuer la détection des boucles par l'expéditeur. Désactivez cette fonctionnalité pour que le récepteur effectue la détection des boucles.
13. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | (Facultatif) Créez un itinéraire statique et installez-le dans une table de routage unicast, car vous voulez que l'itinéraire soit utilisé uniquement à des fins unicast.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel que vous configurez.
2. Sélectionnez **Static Routes (Itinéraires statiques)**, sélectionnez **IPv4 (IPv4)** ou **IPv6 (IPv6)**, puis **Add (Ajoutez)** un itinéraire.
3. Saisissez un **Name (Nom)** pour l'itinéraire statique.
4. Saisissez le masque réseau et le préfixe de **Destination (Destination)** IPv4 ou IPv6p, selon que vous avez choisi IPv4 ou IPv6.
5. Sélectionnez l'**Interface (Interface)** de sortie.
6. Sélectionnez le **Next Hop (Saut suivant)** en tant que **IPv6 Address (Adresse IPv6)** (en tant que **IP Address (Adresse IP)** si vous avez choisi IPv4) et saisissez l'adresse IP du saut suivant vers lequel vous souhaitez acheminer le trafic unicast de cet itinéraire statique.
7. Saisissez une **Admin Distance (Distance admin)**.
8. Entrez une **Metric (Mesure)**.
9. Sous **Route Table (Table de routage)**, sélectionnez **Unicast (Unicast)**.
10. Cliquez sur **OK**.

STEP 3 | Commit (Validez) la configuration.

Cliquez sur **Commit (Valider)**.

STEP 4 | Affichez la table de routage multicast ou unicast.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**.
2. Dans la rangée du routeur virtuel, cliquez sur **More Runtime Stats (Statistiques d'exécution supplémentaires)**.
3. Sélectionnez **Routing (Routage)** > **Route Table (Table de routage)**.
4. Sous **Route Table (Table de routage)**, sélectionnez **Unicast (Unicast)** ou **Multicast (Multicast)** pour n'afficher que ces itinéraires.
5. Sous **Display Address Family (Afficher la famille d'adresses)**, sélectionnez **IPv4 Only (IPv4 uniquement)**, **IPv6 Only (IPv6 uniquement)** ou **IPv4 and IPv6 (IPv4 et IPv6)** pour afficher uniquement les itinéraires qui sont associés à cette famille d'adresses.

   *La sélection de **Multicast (Multicast)** avec **IPv6 Only (IPv6 uniquement)** n'est pas prise en charge.*

STEP 5 | Affichez la table de transfert.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**.
2. Dans la rangée du routeur virtuel, cliquez sur **More Runtime Stats (Statistiques d'exécution supplémentaires)**.
3. Sélectionnez **Routing (Routage)** > **Forwarding Table (Table de transfert)**.
4. Sous **Display Address Family (Afficher la famille d'adresses)**, sélectionnez **IPv4 Only (IPv4 uniquement)**, **IPv6 Only (IPv6 uniquement)** ou **IPv4 and IPv6 (IPv4 et IPv6)** pour afficher uniquement les itinéraires qui sont associés à cette famille d'adresses.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Affichez les tables BGP RIB.

1. Affichez la table de routage BGP RIB local, qui présente les itinéraires BGP que le pare-feu utilise pour acheminer les paquets BGP.
   1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**.
   2. Dans la rangée du routeur virtuel, cliquez sur **More Runtime Stats (Statistiques d'exécution supplémentaires)**.
   3. Sélectionnez **BGP (BGP)** > **Local RIB (RIB locale)**.
   4. Sous **Route Table (Table de routage)**, sélectionnez **Unicast (Unicast)** ou **Multicast (Multicast)** pour n'afficher que ces itinéraires.
   5. Sous **Display Address Family (Afficher la famille d'adresses)**, sélectionnez **IPv4 Only (IPv4 uniquement)**, **IPv6 Only (IPv6 uniquement)** ou **IPv4 and IPv6 (IPv4 et IPv6)** pour afficher uniquement les itinéraires qui sont associés à cette famille d'adresses.

      *La sélection de **Multicast (Multicast)** avec **IPv6 Only (IPv6 uniquement)** n'est pas prise en charge.*
2. Affichez la table de routage BGP RIB Out, qui présente les itinéraires que le pare-feu envoie aux voisins BGP.
   1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**.
   2. Dans la rangée du routeur virtuel, cliquez sur **More Runtime Stats (Statistiques d'exécution supplémentaires)**.
   3. Sélectionnez **BGP (BGP)** > **RIB Out (RIB Out)**.
   4. Sous **Route Table (Table de routage)**, sélectionnez **Unicast (Unicast)** ou **Multicast (Multicast)** pour n'afficher que ces itinéraires.
   5. Sous **Display Address Family (Afficher la famille d'adresses)**, sélectionnez **IPv4 Only (IPv4 uniquement)**, **IPv6 Only (IPv6 uniquement)** ou **IPv4 and IPv6 (IPv4 et IPv6)** pour afficher uniquement les itinéraires qui sont associés à cette famille d'adresses.

      *La sélection de **Multicast (Multicast)** avec **IPv6 Only (IPv6 uniquement)** n'est pas prise en charge.*

 ©2024 Palo Alto Networks, Inc.

Configuration d'un homologue BGP avec le protocole MP-BGP en mode multicast IPv4

Après la configuration du protocole BGP, configurez un homologue BGP avec le protocole MP-BGP en mode multicast IPv4, si vous souhaitez que votre homologue BGP soit en mesure de connaître et de traverser les itinéraires multicast IPv4 dans les mises à jour BGP. Vous serez en mesure de séparer le trafic unicast du trafic multicast ou de vous servir des fonctionnalités énumérées à la section MP-BGP pour utiliser les itinéraires de la table de routage unicast ou multicast uniquement, ou encore les itinéraires des deux tables.

Si vous souhaitez prendre en charge le trafic multicast uniquement, vous devez utiliser un filtre pour éliminer le trafic unicast.

Le pare-feu ne prend pas en charge ECMP pour le trafic multicast.

STEP 1 | Activez les extensions MP-BGP pour qu'un homologue BGP puisse échanger des itinéraires multicast IPv4.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel que vous configurez.
2. Sélectionnez **BGP (BGP)**.
3. Sélectionnez **Peer Group (Groupe d'homologues)**, sélectionnez un groupe d'homologues et un homologue BGP.
4. Sélectionnez **Addressing (Adressage)**.
5. Sélectionnez **Enable MP-BGP Extensions (Activer les extensions MP-BGP)**.
6. Sous **Address Family Type (Type de famille d'adresses)**, sélectionnez **IPv4 (IPv4)**.
7. Sous **Subsequent Address Family (Famille d'adresses subséquentes)**, sélectionnez **Unicast (Unicast)**, puis **Multicast (Multicast)**.
8. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | (Facultatif) Créez un itinéraire statique IPv4 et installez-le dans la table de routage multicast uniquement

afin d'acheminer le trafic multicast d'un homologue BGP vers un saut suivant donné, comme l'illustre la topologie présentée à la section MP-BGP.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel que vous configurez.
2. Sélectionnez **Static Routes (Itinéraires statiques)** > **IPv4 (IPv4)**, puis **Add (Ajoutez)** un **Name (Nom)** à donner à l'itinéraire.
3. Saisissez le masque réseau et le préfixe de la **Destination (Destination)** IPv4.
4. Sélectionnez l'**Interface (Interface)** de sortie.
5. Sélectionnez le **Next Hop (Saut suivant)** en tant que **IP Address (Adresse IP)** et saisissez l'adresse IP du saut suivant vers lequel vous souhaitez acheminer le trafic multicast de cet itinéraire statique.
6. Saisissez une **Admin Distance (Distance admin)**.
7. Entrez une **Metric (Mesure)**.
8. Sous **Route Table (Table de routage)**, sélectionnez **Multicast (Multicast)**.
9. Cliquez sur **OK**.

STEP 3 | Commit (Validez) la configuration.

Cliquez sur **Commit (Valider)**.

STEP 4 | Afficher la table de routage.

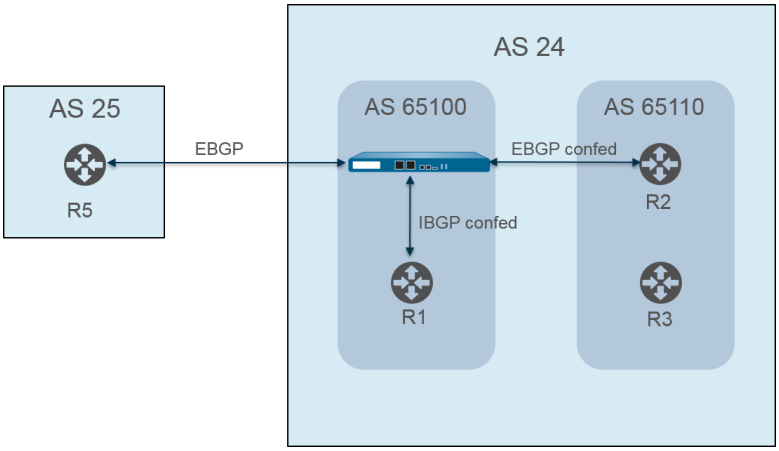
1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**.
2. Dans la rangée du routeur virtuel, cliquez sur **More Runtime Stats (Statistiques d'exécution supplémentaires)**.
3. Sélectionnez **Routing (Routage)** > **Route Table (Table de routage)**.
4. Sous **Route Table (Table de routage)**, sélectionnez **Unicast (Unicast)** ou **Multicast (Multicast)** pour n'afficher que ces itinéraires.
5. Sous **Display Address Family (Afficher la famille d'adresses)**, sélectionnez **IPv4 Only (IPv4 uniquement)**, **IPv6 Only (IPv6 uniquement)** ou **IPv4 and IPv6 (IPv4 et IPv6)** pour afficher uniquement les itinéraires qui sont associés à cette famille d'adresses.

STEP 5 | Pour afficher la table de transfert, la table de routage BGP RIB local ou la table de routage BGP RIB Out, reportez-vous à la section Configuration d'un homologue BGP avec le protocole MP-BGP en mode unicast IPv4 ou IPv6.

 ©2024 Palo Alto Networks, Inc.

Confédérations BGP

Les confédérations BGP offrent une façon de diviser un Autonomous System (système autonome ; AS) en au moins deux Sub-Autonomous Systems (sous-systèmes autonomes ; sous-AS) pour réduire le fardeau que l'exigence de maillage complet inflige à IBGP. Les pare-feu (ou autres périphériques de routage) au sein du sous-AS doivent toujours disposer d'un maillage iBGP complet avec les autres pare-feu du même sous-AS. Vous avez besoin de l'appairage BGP entre les systèmes sous-autonomes pour bénéficier de la connectivité complète avec le AS principal. Les pare-feu qui établissent des paires entre eux au sein du sous-AS forment un appairage de confédération IBGP. Le pare-feu d'un sous-AS qui établit une paire avec un pare-feu d'un autre sous-AS forme un appairage de confédération EBGP. Deux pare-feu de deux systèmes autonomes différents qui se connectent sont des homologues EBGP.



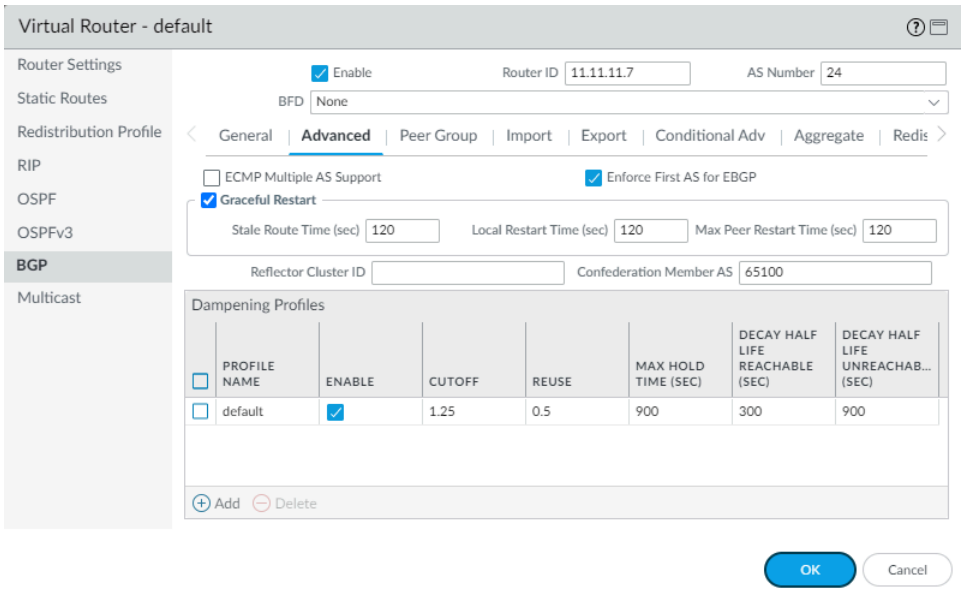
Les systèmes autonomes sont identifiés au moyen d'un numéro AS public (globalement attribué), comme AS 24 et AS 25 dans la figure précédente. Dans un environnement PAN-OS, vous affectez à chaque sous-AS un numéro AS de membre de la confédération, soit un numéro privé qui n'est visible qu'au sein de l'AS. Dans cette figure, les confédérations sont AS 65100 et AS 65110. (RFC6996, Réservation de systèmes autonomes à des fins d'utilisation privée, indique que l'IANA réserve les numéros AS 64512 à 65534 à des fins privées.)

Les confédérations de sous-AS ressemblent à des systèmes autonomes complets pour les autres membres de l'AS. Cependant, lorsque le pare-feu envoie un chemin AS à un homologue EBGP, seul le numéro AS privé apparaît dans le chemin ; aucun numéro de sous-AS privé (AS membre de la confédération) n'est compris.

L'appairage BGP se produit entre le pare-feu et le routeur R2 ; le pare-feu dans la figure possède ces paramètres de configuration pertinents :

- Numéro AS : 24
- Membre AS de la confédération : 65100
- Type d'appairage : conféd. EBGP
- AS homologue : 65110

©2024 Palo Alto Networks, Inc.



Le routeur 2 (R2) de l'AS 65110 est configuré comme suit :

- Numéro AS : 24
- Membre AS de la confédération : 65110
- Type d'appairage : conféd. EBGP
- AS homologue : 65100

L'appairage BGP se produit également entre le pare-feu et le routeur R1. Le pare-feu possède la configuration supplémentaire suivante :

- Numéro AS : 24
- Membre AS de la confédération : 65100
- Type d'appairage : conféd. IBGP
- AS homologue : 65110

R1 est configuré comme suit :

- Numéro AS : 24
- Membre AS de la confédération : 65110
- Type d'appairage : conféd. IBGP
- AS homologue : 65100

L'appairage BGP se produit entre le pare-feu et le routeur R5. Le pare-feu possède la configuration supplémentaire suivante :

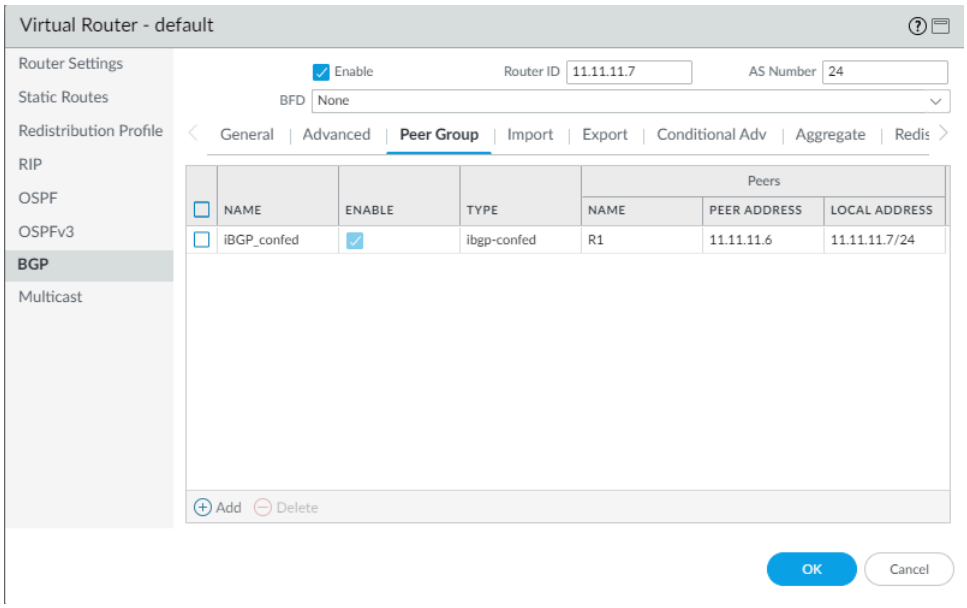
- Numéro AS : 24
- Membre AS de la confédération : 65100
- Type d'appairage : EBGP
- AS Homologue : 25

R5 est configuré comme suit :

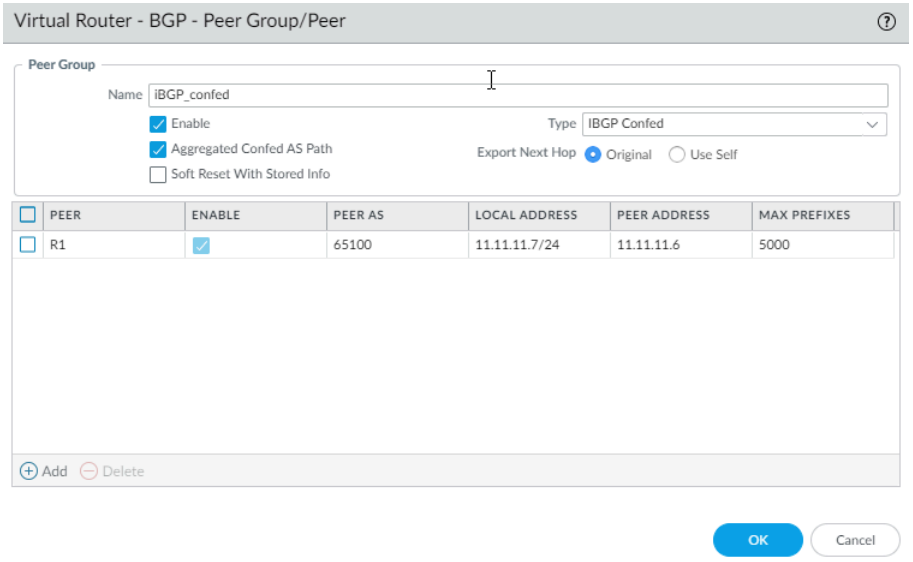
 ©2024 Palo Alto Networks, Inc.

- AS—25
- Type d'appairage : EBGP
- AS Homologue : 24

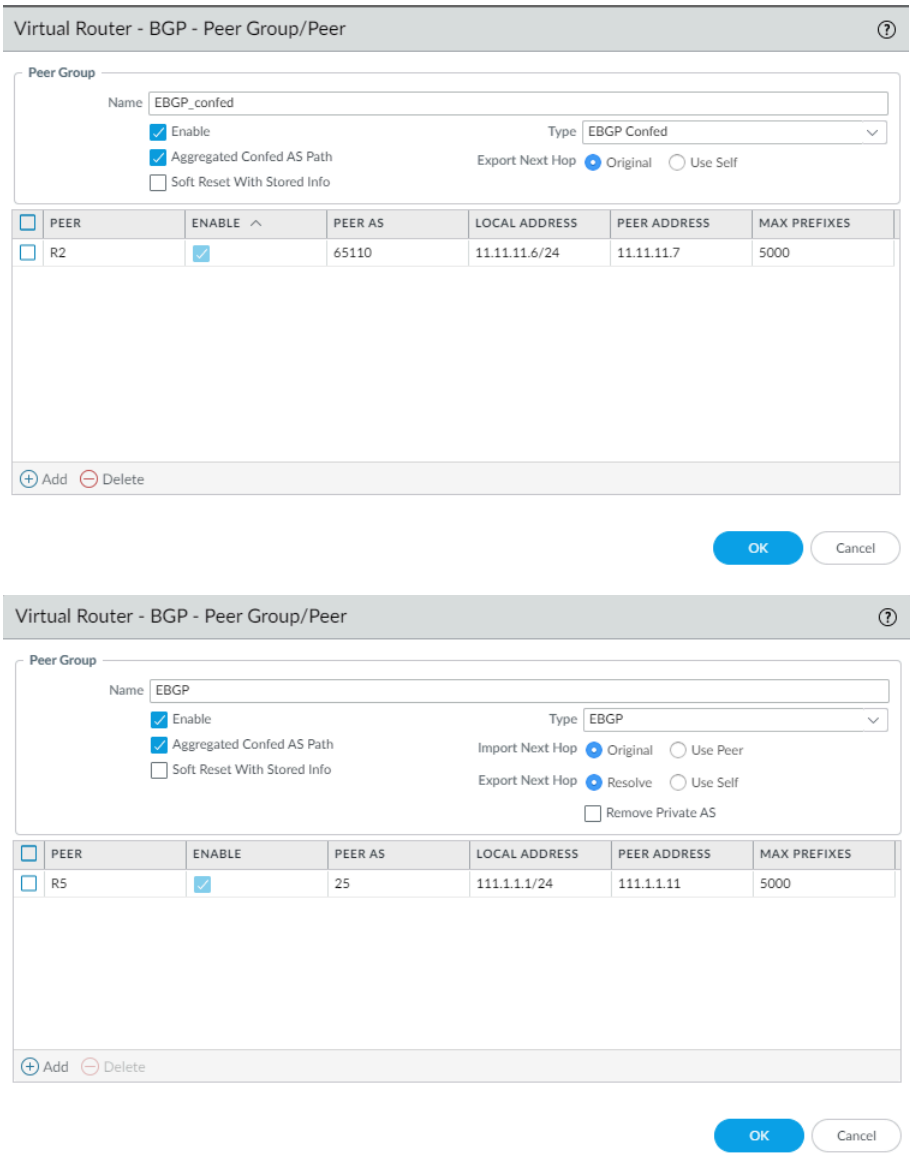
Une fois que le pare-feu est configuré pour s'appairer au R1, au R2 et au R5, ses homologues sont visibles à l'onglet **Peer Group (Group (Groupe d'homologues)** :



Le pare-feu montre les homologues R1, R2 et R5 :

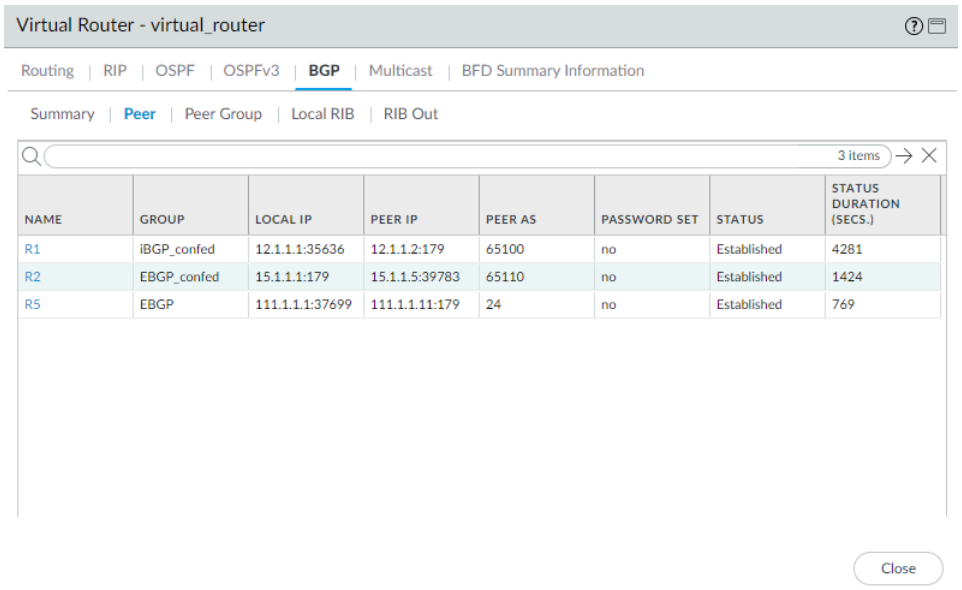


 ©2024 Palo Alto Networks, Inc.

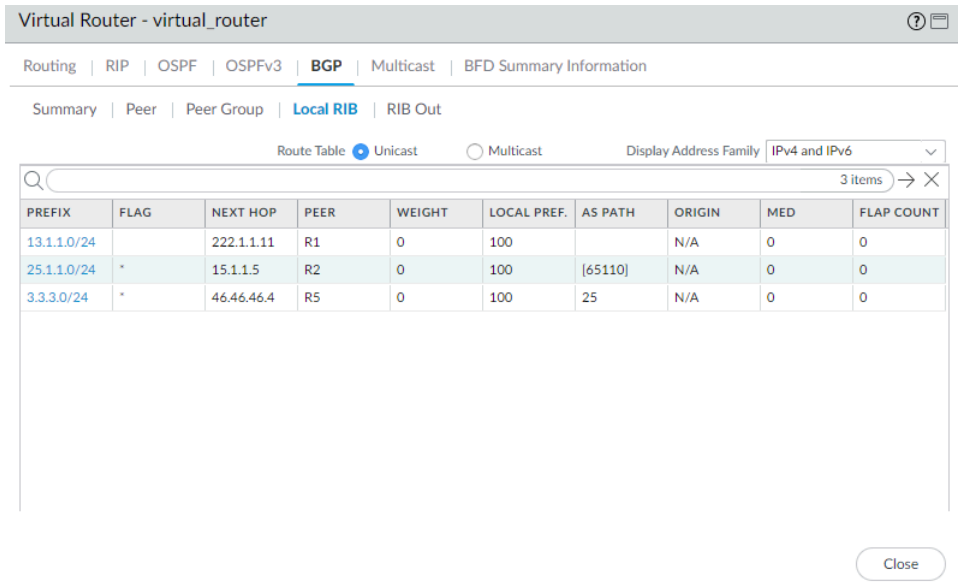


Pour vérifier que les itinéraires du pare-feu aux homologues sont établis, à l'écran du routeur virtuel, sélectionnez **More Runtime Stats (Statistiques d'exécution supplémentaires)**, puis sélectionnez l'onglet **Peer (Homologue)**.

 ©2024 Palo Alto Networks, Inc.

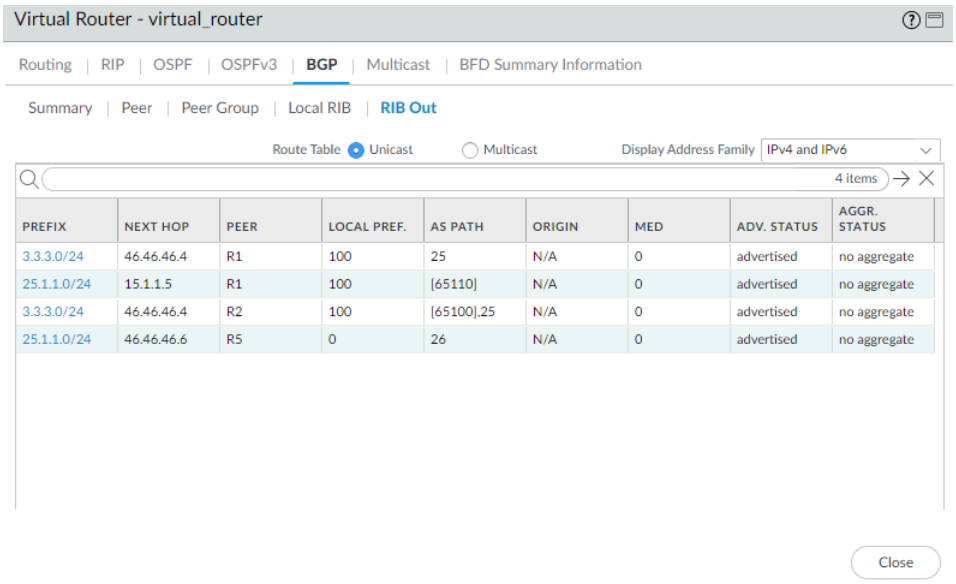


Sélectionnez l'onglet **Local RIB (RIB locale)** pour afficher des informations sur les itinéraires stockés dans la Routing Information Base (base d'informations de routage ; RIB).



Sélectionnez ensuite l'onglet **RIB Out (RIB sortante)**.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Multidiffusion IP

La multidiffusion IP est un ensemble de protocoles que les périphériques réseau utilisent pour envoyer des datagrammes de multidiffusion IP à un groupe de récepteurs intéressés en utilisant une transmission intéressés plutôt que d'utiliser la monodiffusion du trafic vers plusieurs récepteurs, ce qui permet d'économiser la bande passante. La multidiffusion IP convient à la communication à partir d'une source (ou de plusieurs sources) vers de nombreux récepteurs, comme l'audio ou la vidéo en continu, IPTV, la vidéo-conférence, et la distribution d'autres communications, telles que les actualités et les données financières.

Une adresse multidiffusion identifie un groupe de récepteurs qui veulent recevoir le trafic allant à cette adresse. Vous ne devez pas utiliser les adresses multidiffusion réservées à des usages particuliers, telles que les adresses de la plage allant de 224.0.0.0 à 224.0.0.255 ou de la plage allant de 239.0.0.0 à 239.255.255.255. Le trafic multidiffusion utilise UDP, qui ne renvoie pas les paquets manqués.

Les pare-feu Palo Alto Networks® prennent en charge la multidiffusion IP et le Protocol Independent Multicast (Protocole de multidiffusion indépendant ; PIM) sur une interface de couche 3 que vous configurez pour un routeur virtuel sur le pare-feu.

Pour le routage multidiffusion, le type d'interface de couche 3 peut être Ethernet, Ethernet agrégée, VLAN, en boucle ou de tunnel. Les groupes d'interfaces vous permettent de configurer plus d'une interface de pare-feu à la fois avec le même protocole Internet Group Management Protocol (protocole de gestion de groupe IGMP ; IGMP) et les paramètres PIM ainsi qu'avec les mêmes permissions de groupe (groupes multidiffusion autorisés à accepter le trafic provenant d'une source ou d'une source spécifique uniquement). Une interface ne peut appartenir qu'à un seul groupe d'interfaces.

Le pare-feu prend en charge la multidiffusion IPv4 ; il ne prend pas en charge la multidiffusion IPv6. Le pare-feu ne prend également pas en charge le mode PIM Dense Mode (PIM-DM), le proxy IGMP, les jointures statiques IGMP, le RP Anycast, GRE ou les configurations multidiffusion sur un type d'interface de couche 2 ou de câble virtuel. Cependant une interface de câble virtuel peut passer les paquets multidiffusion. De plus, une interface de couche 2 peut commuter les paquets multidiffusion IPv4 de Couche 3 entre les différents VLAN, et le pare-feu étiquettera de nouveau l'ID VLAN en utilisant l'ID VLAN de l'interface de sortie.

Vous devez activer la multidiffusion pour un routeur virtuel et activer PIM pour une interface d'entrée et de sortie pour que les interfaces reçoivent ou transfèrent des paquets multidiffusion. En plus de PIM, vous devez également activer IGMP sur les interfaces de sortie qui ont orientées vers les récepteurs. Vous devez configurer une règle de politique de sécurité pour autoriser le trafic multidiffusion IP à entrer dans une zone de destination de couche 3 nommée **multicast (multidiffusion)** ou dans **any (n'importe quelle)** zone de destination.

- IGMP
- PIM
- Configurer la multidiffusion IP
- Affichage des informations sur la multidiffusion IP

IGMP

Le Internet Group Management Protocol (Protocole de gestion des groupes Internet ; IGMP) est un protocole IPv4 qu'un récepteur multidiffusion utilise pour communiquer avec une interface sur un pare-feu Palo Alto Networks® et que le pare-feu utilise pour suivre l'adhésion des groupes multidiffusion. Lorsqu'un hôte veut recevoir le trafic multidiffusion, sa mise en œuvre d'IGMP envoie un rapport d'adhésion IGMP et le routeur récepteur, à son tour, envoie un message de jointure PIM au groupe d'adresses multidiffusion du groupe que l'hôte veut joindre. Un routeur compatible avec IGMP sur le même réseau physique (comme un segment Ethernet) utilise ensuite PIM pour communiquer avec d'autres routeurs compatibles avec PIM pour déterminer un chemin entre la source et les récepteurs intéressés.

Activez IGMP uniquement sur les interfaces qui sont orientées vers un récepteur multidiffusion. Les récepteurs ne peuvent se trouver qu'à un saut de couche 3 du routeur virtuel. Les messages IGMP sont des messages de couche 2 qui possèdent une valeur TTL de un. De ce fait, ils ne peuvent pas aller à l'extérieur du LAN.

Lorsque vous configurez la multidiffusion IP, spécifiez si une interface utilise la Version 1 d'IGMP, la Version 2 d'IGMP ou la Version 3 d'IGMP. Vous pouvez appliquer l'option IP d'alerte du routeur, RFC 2113, pour que les paquets IGMP entrants qui utilisent IGMPv2 ou IGMPv3 disposent de l'option IP d'alerte du routeur.

Par défaut, une interface accepte les rapports d'adhésion IGMP de tous les groupes multidiffusion. Vous pouvez configurer les autorisations de groupe multidiffusion pour contrôler les groupes pour lesquels le routeur virtuel accepte les rapports d'adhésion provenant de toute source (Any-Source Multicast (Multidiffusion de toute source ; ASM)), soit le PIM Sparse Mode (PIM-SM). Vous pouvez également spécifier les groupes pour lesquels le routeur virtuel accepte les rapports d'adhésion d'une source spécifique (Source-Specific multicast PIM-PIM [SSM]). Si vous spécifiez des autorisations pour l'un ou l'autre des groupes ASM ou SSM, le routeur virtuel refuse les rapports d'adhésion des autres groupes. L'interface doit utiliser IGMPv3 pour passer le trafic PIM-SSM.

Vous pouvez spécifier le nombre maximal de sources et le nombre maximal de groupes multidiffusion que IGMP peut traiter simultanément pour une interface.

Le routeur virtuel multidiffuse une requête IGMP à des intervalles réguliers à tous les récepteurs d'un groupe multidiffusion. Un récepteur répond à une requête IGMP en lui transmettant un rapport d'adhésion IGMP qui confirme que le récepteur souhaite toujours recevoir le trafic multidiffusion pour ce groupe. Le routeur virtuel conserve une table des groupes multidiffusion qui disposent de récepteurs ; le routeur virtuel transfère un paquet multidiffusion vers le saut suivant s'il y a encore un récepteur sur cet arbre de distribution multidiffusion qui se joint au groupe. Le routeur virtuel ne suit pas exactement les récepteurs qui sont joints à un groupe. Un seul routeur d'un sous-réseau répond aux requêtes IGMP : c'est le requérant IGMP, soit le routeur possédant l'adresse IP la plus faible.

Vous pouvez configurer une interface avec un intervalle de requête IGMP et la durée de temps autorisée pour qu'un récepteur réponde à une requête (le temps max. de réponse aux requêtes). Lorsqu'un routeur virtuel reçoit un message d'abandon IGMP d'un récepteur l'invitant à quitter un groupe, le routeur virtuel vérifie que l'interface qui a reçu le message d'abandon n'est pas configurée avec l'option Abandon immédiat. En l'absence de l'option Abandon immédiat, le routeur virtuel envoie une requête pour déterminer si le groupe comprend encore des récepteurs membres. Le Dernier intervalle de requête d'un membre spécifie le nombre de secondes qui sont

 ©2024 Palo Alto Networks, Inc.

autorisées pour que les récepteurs restants de ce groupe répondent et confirment qu'ils veulent toujours recevoir le trafic multidiffusion de ce groupe.

Une interface prend en charge le variable de robustesse IGMP, que vous pouvez ajuster, pour que le pare-feu puisse ensuite affiner l'intervalle d'appartenance au groupe, l'intervalle Autre requérant présent, le nombre de requêtes au démarrage et le nombre de requêtes d'un membre dernier. Un variable de robustesse plus élevé peut prendre en charge un sous-réseau qui est susceptible d'abandonner des paquets.

Afficher des informations sur la multidiffusion IP pour voir les interfaces sur lesquelles IGMP est activé, la version IGMP, l'adresse du requérant, le paramètre de robustesse, les nombres limites de groupes et sources multidiffusion de même que pour savoir si l'option Abandon immédiat est configurée sur l'interface. Vous pouvez également voir les groupes multidiffusion auxquels les interfaces appartiennent et les informations sur l'adhésion IGMP.

 ©2024 Palo Alto Networks, Inc.

PIM

La multidiffusion IP utilise le protocole de routage Protocol Independent Multicast (Protocole de multidiffusion indépendant ; PIM) entre les routeurs pour déterminer le chemin de l'arbre de distribution que les paquets multidiffusion transmettent de la source aux récepteurs (membres du groupe multidiffusion). Les routeurs virtuels (sur un moteur de routage hérité) et les routeurs logiques (sur un moteur de routage avancé) prennent en charge PIM.

Un pare-feu Palo Alto Networks® firewall prend en charge le mode PIM Sparse Mode (PIM-SM) (RFC 4601), la Any-Source Multicast (Multidiffusion de toute source ; ASM) (parfois nommée PIM Sparse Mode) et la PIM Source-Specific Multicast (Multidiffusion propre à une source ; SSM) En mode PIM-SM, la source ne transfère aucun trafic multidiffusion jusqu'à ce qu'un récepteur (utilisateur) appartenant à un groupe de multifidiffusion demande que la source envoie le trafic. Lorsqu'un hôte veut recevoir le trafic multidiffusion, sa mise en œuvre d'IGMP envoie un rapport d'adhésion IGMP et le routeur récepteur envoie ensuite un message de jointure PIM au groupe d'adresses multidiffusion du groupe qu'il veut joindre.

- En mode **ASM**, le récepteur utilise IGMP pour demander du trafic pour un groupe d'adresses multidiffusion ; n'importe quelle source pourrait être à l'origine du trafic. Par conséquent, le récepteur ne connaît pas nécessairement les expéditeurs, et le récepteur pourrait recevoir du trafic multidiffusion dans lequel il n'a aucun intérêt.
- En mode **SSM** (RFC 4607), le récepteur utilise IGMP pour demander le trafic d'une ou de plusieurs sources vers une adresse de groupes multidiffusion. Le récepteur connaît l'adresse IP des expéditeurs et reçoit uniquement le trafic multidiffusion qu'il veut recevoir. SSM exige IGMPv3. L'espace d'adressage SSM par défaut (232.0.0.0/8) peut être remplacé en ajustant l'espace d'adressage spécifique à la source. Les autorisations de groupe doivent également être ajustées.

Lorsque vous Configure IP Multicast (configurez la multidiffusion IP) sur un pare-feu Palo Alto Networks®, vous devez activer PIM pour qu'une interface transfère le trafic multidiffusion, même sur les interfaces orientées vers les récepteurs. Cela diffère de IGMP, que vous n'activez que sur les interfaces orientées vers les récepteurs.

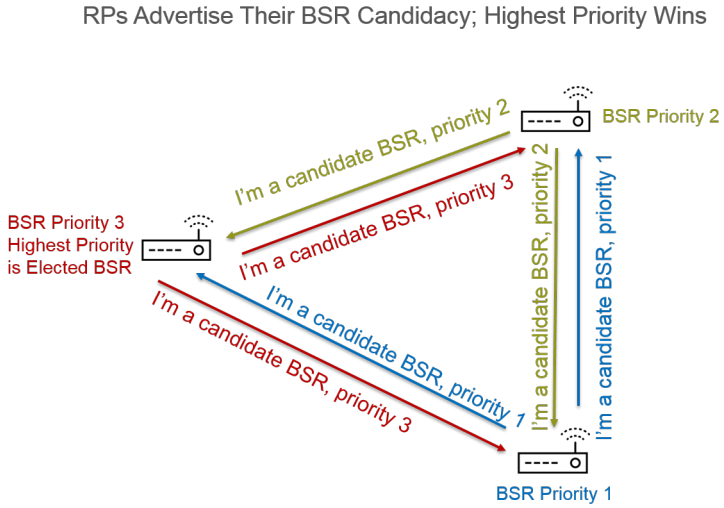
ASM exige un *rendezvous point (point de rendez-vous* ; RP), qui est un routeur à la jonction ou à la racine d'un arbre de distribution partagée. Le RP d'un domaine multidiffusion fait office de point unique auquel tous les membres du groupe multifidiffusion envoient leurs messages de jointure. Ce comportement réduit la probabilité que se produise une boucle de routage, laquelle se produirait probablement si des membres du groupe envoyaient leurs messages de jointure à plusieurs routeurs. (SSM n'a pas besoin d'un RP, car la multicast spécifique à la source utilise le chemin le plus court et, par conséquent, n'a pas besoin d'un RP.)

Dan un environnement ASM, le routeur virtuel peut déterminer quel routeur est le RP d'un groupe multidiffusion de deux façons :

- **Mappage RP statique à groupe** : configure le routeur virtuel sur le pare-feu pour qu'il agisse en tant que RP pour les groupes multidiffusion. Vous configurez un RP local, soit en configurant une adresse RP statique, soit en spécifiant que le RP local est un RP candidat et que le RP est choisi de manière dynamique (selon la valeur de la priorité la plus faible). Vous pouvez également configurer statiquement un ou plusieurs RP externes pour des plages d'adresses de groupes différents qui ne sont pas couvertes par le RP local, ce qui vous aide à équilibrer la charge du trafic multidiffusion pour éviter qu'un RP soit surchargé.

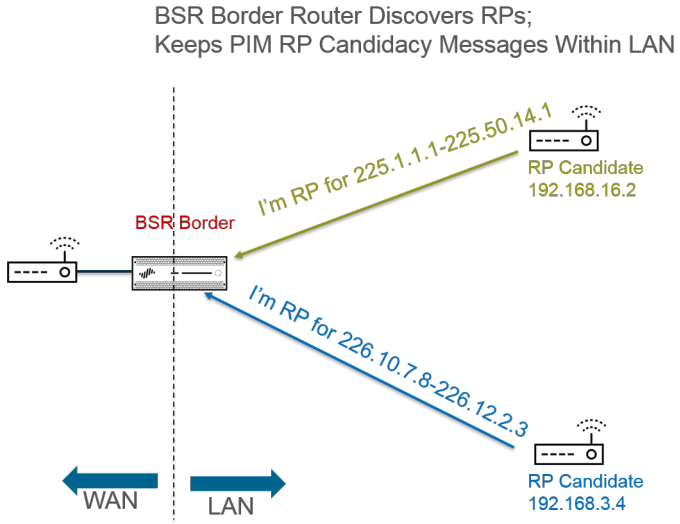
 ©2024 Palo Alto Networks, Inc.

- **Bootstrap Router (routeur bootstrap ; BSR)** : (RFC 5059) : définit le rôle d'un BSR. D'abord, les candidats au BSR publie leur priorité entre eux, puis le candidat ayant la priorité la plus élevée est choisi en tant que BSR, comme l'illustre la figure suivante :



Ensuite, le BSR découvre les RP lorsque les RP candidats transmettent périodiquement en monodiffusion un message BSR au BSR contenant leur adresse IP et la plage du groupe multidiffusion pour lequel ils agiront en tant que RP. Vous pouvez configurer le routeur virtuel local en tant que RP candidat. Dans ce cas, le routeur virtuel annonce sa candidature RP pour un ou des groupes multidiffusion spécifiques. Le BSR envoie des informations RP aux autres RP dans le domaine PIM.

Lorsque vous configurez PIM pour une interface, vous pouvez sélectionner BSR lorsque l'interface qui figure au pare-feu est à une limite de l'entreprise, à l'opposé du réseau d'entreprise. Le paramètre de bordure BSR empêche le pare-feu d'envoyer les messages BSR de candidature RP à l'extérieur du réseau local. Dans l'illustration suivante, la bordure BSR est activée pour l'interface orientée vers le réseau local et c'est l'interface qui possède la priorité la plus haute. Si le routeur virtuel possède un RP statique et un RP dynamique (appris du BSR), vous pouvez spécifier si le RP statique devrait remplacer le RP appris d'un groupe lorsque vous configurez le RP statique local.



 ©2024 Palo Alto Networks, Inc.

Pour que le mode PIM Sparse Mode avise le RP qu'il a du trafic à faire descendre l'arbre partagé, le RP doit connaître la source. L'hôte avise le RP qu'il envoie du trafic à une adresse de groupe multidiffusion lorsque le designated router (*routeur désigné* ;DR) encapsule le premier paquet de l'hôte dans un message PIM Register message et transmet le paquet en monodiffusion au RP sur son réseau local. Le DR transfère également les messages d'élagage qu'un récepteur envoie au RP. Le RP maintient la liste d'adresses IP que les sources envoient à un groupe multidiffusion et le RP peut transférer les paquets multidiffusion des sources.

Pourquoi les routeurs d'un domaine PIM ont-ils besoin d'un DR ? Lorsqu'un routeur envoie un message de jointure PIM vers un commutateur, deux routeurs pourraient le recevoir et le transmettre au même RP, ce qui entraînerait la redondance du trafic et le gaspillage de la bande passante. Pour empêcher le trafic inutile, les routeurs PIM choisissent un DR (le routeur ayant l'adresse IP la plus élevée), et seul le DR transfère le message de jointure au RP. Vous pouvez également affecter une priorité DR à un groupe d'interfaces, qui l'emporte sur les comparaisons d'adresses IP. À titre de rappel, le DR transfère (en monodiffusion) les messages PIM, il ne transfère pas en multidiffusion les paquets IP multidiffusion IP.

Vous pouvez spécifier les adresses IP des voisins PIM (routeurs) que le groupe d'interfaces autorisera à s'associer au routeur virtuel. Par défaut, tous les routeurs compatibles avec PIM peuvent être des voisins PIM, mais visant la limitation des voisins constitue une étape vers la sécurisation du routeur virtuel dans votre environnement PIM.

- Shortest-Path Tree (arbre du chemin le plus court ; SPT) et arborescence partagée
- Mécanisme d'affirmation PIM
- Renvoi de chemin inverse

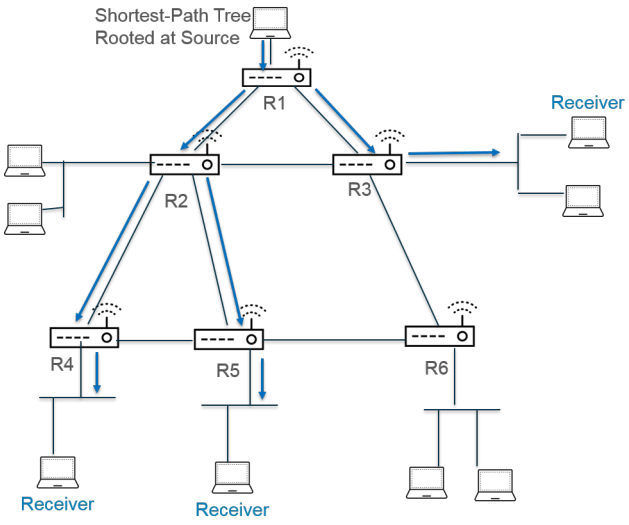
Shortest-Path Tree (arbre du chemin le plus court ; SPT) et arborescence partagée

Une fois qu'un récepteur s'est joint à un groupe de multidiffusion, les routeurs du réseau à accès multiple construisent les chemins de routage nécessaires pour envoyer des données à chacun des récepteurs du groupe. Chaque datagramme IP envoyé à un groupe de multidiffusion est distribué (transféré) à tous les membres. Les chemins de routage sont un type d'arbre de distribution d'un paquet multicast. L'objectif d'un arbre de distribution multidiffusion consiste à permettre au routeur de répliquer un paquet multidiffusion lorsque le paquet atteint des chemins divergents et que le routeur doit envoyer le paquet sur plusieurs chemins pour atteindre tous les membres du groupe ; cependant, l'arbre de distribution doit éviter d'envoyer des paquets sur des chemins qui ne contiennent aucun récepteur intéressé. L'arbre de distribution est l'un des suivants :

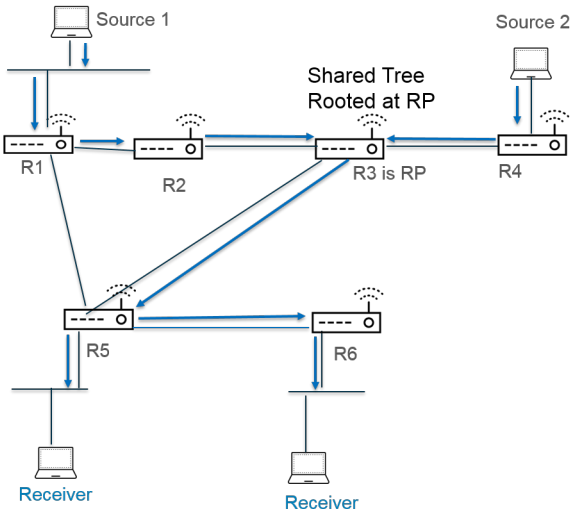
- Un **arbre source** : un chemin allant d'une source multidiffusion (la racine de l'arbre) via la réseau jusqu'aux récepteurs du groupe multidiffusion. L'arbre source est le chemin le plus court qu'un paquet multicast peut prendre de la source jusqu'au récepteur, c'est pourquoi on l'appelle également **shortest-path tree (chemin le plus court ; SPT)**. L'expéditeur et le récepteur sont annotés comme étant une source et la paire de groupes multidiffusion, raccourcie à (S, G) ; par

 ©2024 Palo Alto Networks, Inc.

exemple, (192.168.1.1, 225.9.2.6). La figure suivante montre trois arbres du chemin le plus court de la source à trois récepteurs.



- Une **arborescence partagée** : un chemin ancré au RP, et non à la source multidiffusion. Une arborescence partagée est également connue sous le nom d'arbre RP ou de RPT. Les routeurs transmettent des paquets multidiffusion de diverses sources vers le RP, et le RP transmet les paquets le long de l'arbre partagé. Un arbre partagé est annoté en tant que (*, G), au moyen d'un caractère spécial en tant que source, car toutes les sources appartenant au groupe multidiffusion partagent le même arbre de distribution à partir du RP. Un exemple d'annotation d'arbre partagé serait (*, 226.3.1.5). La figure suivante montre un arbre partagé de la racine (RP) jusqu'aux récepteurs.



La Source-Specific Multicast (Multidiffusion propre à une source ; SSM) utilise la distribution de l'arbre source. Lorsque vous configurez la multidiffusion IP pour utiliser la Any Source Multicast (Multidiffusion de toute source ; ASM), vous pouvez spécifier l'arbre de distribution que le routeur virtuel sur votre pare-feu de Palo Alto Networks® utilise pour livrer les paquets multidiffusion à un groupe en définissant un seuil SPT pour le groupe :

 ©2024 Palo Alto Networks, Inc.

- Par défaut, le routeur virtuel bascule le routage multidiffusion de l'arborescence partagée à une distribution en arborescence source lorsqu'il reçoit le premier paquet multidiffusion pour un groupe ou un préfixe (le **SPT Threshold (Seuil SPT)** est défini sur 0).
- Vous pouvez configurer le routeur virtuel pour basculer vers SPT lorsque le nombre total de kilobits contenus dans les paquets qui arrivent pour le préfixe ou le groupe multicast à toute interface sur une période de temps déterminé atteint un certain nombre.
- Vous pouvez configurer le routeur virtuel pour qu'il ne bascule jamais vers le SPT pour le groupe ou le préfixe (il continue d'utiliser l'arborescence partagée).

Le SPT exige plus de mémoire, vous devez donc choisir vos paramètres en fonction du niveau de trafic multidiffusion pour le groupe. Si le routeur virtuel bascule vers le SPT, les paquets arrivent alors de la source (plutôt que du RP) et le routeur virtuel envoie un message d'élagage au RP. La source envoie des paquets multidiffusion subséquents pour ce groupe le long du chemin le plus court.

Mécanisme d'affirmation PIM

Pour empêcher des routeurs sur un réseau à accès multiple de transférer le même type de trafic multidiffusion pour le même saut suivant (ce qui provoquerait un trafic redondant et le gaspillage de la bande passante), PIM utilise le mécanisme d'affirmation pour choisir un seul porteur PIM pour le réseau à accès multiple.

Si le routeur virtuel reçoit un paquet multidiffusion provenant d'une source sur une interface que le routeur virtuel associe déjà en tant qu'interface de sortie pour la même paire (S,G) identifiée dans le paquet, cela signifie que c'est un paquet double. Par conséquent, le routeur virtuel envoie un message d'affirmation contenant ses mesures aux autres routeurs du réseau à accès multiple. Les routeurs choisissent ensuite un porteur PIM de la manière suivante :

1. Le porteur PIM est le routeur possédant la distance administrative la plus faible jusqu'à la source multidiffusion.
2. En cas d'égalité en matière de distance administrative la plus faible, le porteur PIM est le routeur possédant la meilleure mesure de routage monodiffusion jusqu'à la source.
3. En cas d'égalité en matière de meilleure mesure, le porteur PIM est le routeur possédant l'adresse IP la plus élevée.

Les routeurs qui ne sont pas choisis comme Porteur PIM cesseront de transférer le trafic vers le groupe multidiffusion identifié dans la paire (S,G).

Lorsque vous configurez la multidiffusion IP, vous pouvez configurer l'intervalle auquel le routeur virtuel envoie un message d'affirmation PIM depuis une interface (l'intervalle d'affirmation). Lorsque vous affichez des informations sur la multidiffusion IP, l'onglet **PIM Interface (Interface PIM)** affiche l'intervalle d'affirmation d'une interface.

Renvoi de chemin inverse

PIM utilise le reverse-path forwarding (transfert de chemin inverse ; RPF) pour empêcher les boucles de routage multidiffusion en exploitant la table de routage monodiffusion du routeur virtuel. Lorsque le routeur virtuel reçoit un paquet multidiffusion, il cherche la source du paquet multidiffusion dans sa table de routage unicast pour voir si l'interface sortante associée à cette adresse IP source est l'interface sur laquelle ce paquet est arrivé. Si les interfaces correspondent, le routeur virtuel duplique le paquet et le redirige vers les récepteurs multidiffusion du groupe. Si

 ©2024 Palo Alto Networks, Inc.

les interfaces ne correspondent pas, le routeur virtuel abandonne le paquet. La table de routage monodiffusion se fonde sur les routes statiques sous-jacentes ou le Interior Gateway Protocol (protocole de passerelle interne ; IGP) utilisé par votre réseau, tel que OSPF.

PIM utilise également RPF pour construire une arborescence du chemin le plus court pour atteindre une source, un saut de routeur PIM à la fois. Le routeur virtuel possède l'adresse de la source multidiffusion. Le routeur virtuel sélectionne donc, comme prochain saut vers la source, le voisin PIM en amont que le routeur virtuel utiliserait pour transférer les paquets monodiffusion à la source. Le routeur de saut suivant fait la même chose.

Une fois que RPF a réussi et qu'une entrée d'itinéraire figure dans la base d'informations de routage multidiffusion (mRIB) du routeur virtuel, celui-ci conserve les entrées d'arborescence basées sur la source (S, G) et les entrées d'arborescence partagées (*, G) dans sa base d'informations de transfert multidiffusion (table de transfert multidiffusion ou mFIB). Chaque entrée comprend l'adresse IP source, le groupe multidiffusion, l'interface entrante (interface RPF) et la liste des interfaces sortantes. Il peut y avoir plusieurs interfaces sortantes pour une entrée, car l'arborescence du chemin le plus court peut joindre le routeur, et celui-ci doit transmettre le paquet à plusieurs interfaces pour atteindre les récepteurs du groupe situés dans des chemins différents. Lorsque le routeur virtuel utilise la mFIB pour transférer un paquet multidiffusion, il fait correspondre une entrée (S, G) avant de tenter de faire correspondre une entrée (*, G).

Si vous publiez des préfixes sources multidiffusion dans BGP (vous avez configuré MP-BGP avec la famille d'adresses IPv4 et la famille d'adresses subséquentes de multidiffusion), le pare-feu effectue toujours la vérification RPF sur les itinéraires BGP reçus par le pare-feu dans la famille d'adresses ultérieures de multidiffusion.

Affichez les informations de multidiffusion IP pour voir comment afficher les entrées mFIB et mRIB. N'oubliez pas que la table de routage de multidiffusion (mRIB) est une table distincte de la table de routage unicast (RIB).

 ©2024 Palo Alto Networks, Inc.

Configurer la multidiffusion IP

Configurez les interfaces sur un routeur virtuel d'un pare-feu Palo Alto Networks® pour la réception et la transmission des paquets Multidiffusion IP. Vous devez activer la multidiffusion IP pour le routeur virtuel, configurer le Protocol Independent Multicast (Protocole de multidiffusion indépendant ; PIM) sur les interfaces d'entrée et de sortie, puis configurer Internet Group Management Protocol (Protocole de gestion des groupes Internet ; IGMP) sur les interfaces orientées récepteur.

STEP 1 | Activez la multidiffusion IP sur un routeur virtuel.

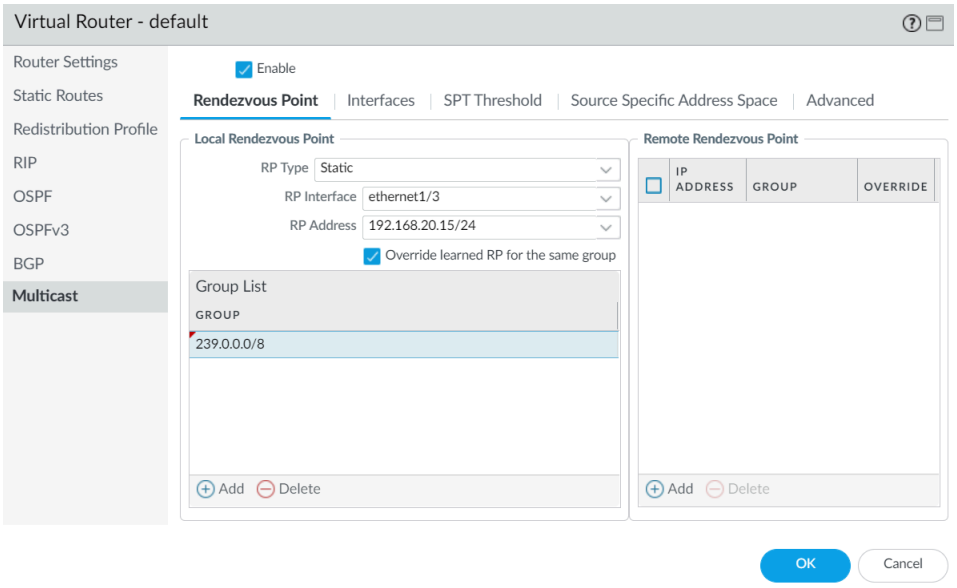
1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez un routeur virtuel.
2. Sélectionnez **Multicast** et **Enable (Activez)** la multidiffusion IP.

©2024 Palo Alto Networks, Inc.

STEP 2 | (ASM uniquement) Si le domaine multicast dans lequel le routeur virtuel est situé utilise Any-Source Multicast (Multidiffusion de toute source ; ASM), identifiez et configurez les points de rendez-vous (RP) des groupes multicast.

1. Sélectionnez **Rendezvous Point**.
2. Sélectionnez un **RP Type (Type de RP)**, qui détermine la façon dont le RP est choisi (les options sont **Static (Statique)**, **Candidate (Candidat)** ou **None (Aucun)**) :

   - **Static (Statique)** : Établit un mappage statique d'un RP à des groupes de multidiffusion. La configuration d'un RP statique vous demande de configurer explicitement le même RP sur d'autres routeurs PIM du domaine PIM.
     - Sélectionner la **RP Interface (Interface du RP)**. Les types d'interfaces valides sont les suivantes : couche 3, câble virtuel, en boucle, VLAN, Ethernet agrégée et de tunnel.
     - Sélectionnez la **RP Address (Adresse du RP)**. Les adresses IP de l'interface RP que vous avez sélectionnée renseignent la liste.
     - Sélectionnez **Override learned RP for the same group (Écraser le RP appris pour le même groupe)** pour que ce RP agisse en tant que RP au lieu du RP choisi pour les groupes qui figurent dans la liste des groupes.
     - **Add (Ajoutez)** un ou plusieurs **Groups (Groupes)** de multidiffusion pour lesquels le RP agit à titre de RP.



   - **Candidate (Candidat)** : Établit un mappage dynamique d'un RP à des groupes multicast en fonction de la priorité. Ainsi, chaque routeur d'un domaine PIM choisit automatiquement le même RP.
     - Sélectionnez la **RP Interface (Interface du RP)** candidat. Les types d'interfaces valides sont les suivantes : couche 3, en boucle, VLAN, Ethernet agrégée et de tunnel.
     - Sélectionnez la **RP Address (Adresse du RP)** du RP candidat. Les adresses IP de l'interface RP que vous avez sélectionnée renseignent la liste.

 ©2024 Palo Alto Networks, Inc.

- (Facultatif) Modifiez la **Priority (Priorité)** du RP candidat. Le pare-feu compare la priorité du RP candidat à la priorité d'autres RP candidats pour déterminer celui qui agit en tant que RP pour les groupes spécifiés ; le pare-feu sélectionne le RP candidat ayant la priorité la plus faible (la plage est comprise entre 0 et 255 ; la valeur par défaut est 192).
- (Facultatif) Modifiez le **Advertisement Interval (sec) (Intervalle de publication (sec)** (la plage est comprise entre 1 et 26 214 ; la valeur par défaut est 60).
- Entrez une **Group List (Liste de groupes)** multicast qui communiquent avec le RP.

- **None (Aucun)** : sélectionnez cette option si ce routeur virtuel n'est pas un RP.

3. **Add (Ajoutez)** un point de rendez-vous distant, puis saisissez la **IP Address (Adresse IP)** de ce RP distant (externe).
4. **Add (Ajoutez)** les **Group Addresses (adresses de groupe)** multicast pour lesquels l'adresse du RP distant spécifié agit en tant que RP.
5. Sélectionnez **Override learned RP for the same group (Écraser le RP appris pour le même groupe)** pour que le RP externe que vous avez configuré de manière statique agisse en tant que RP au lieu d'un RP appris de manière dynamique (choisi) pour les groupes qui figurent dans la liste des adresses du groupe.
6. Cliquez sur **OK**.

STEP 3 | Spécifiez un groupe d'interfaces qui partagent une configuration multicast (IGMP, PIM et autorisations du groupe).

1. À l'onglet **Interfaces**, **Add (Ajoutez)** un **Name (Nom)** à donner au groupe d'interfaces.
2. Saisissez une **Description (Description)**.
3. **Add (Ajoutez)** une **Interface**, puis sélectionnez au moins une interface de couche 3 qui appartient au groupe d'interfaces.

STEP 4 | (Facultatif) Configurez des autorisations de groupe multicast pour le groupe d'interfaces. Par défaut, le groupe d'interfaces accepte les rapports d'adhésion IGMP et les messages de jointure PIM de tous les groupes.

1. Sélectionnez les **Group Permissions (Autorisations du groupe)**.
2. Pour configurer des groupes Any-Source Multicast (Multidiffusion de toute source ; ASM) pour ce groupe d'interfaces, dans la fenêtre Any Source (N'importe quelle source), **Add (Ajoutez)** un **Name (Nom)** pour identifier un groupe multidiffusion qui accepte les rapports d'adhésion IGMP et les messages de jointure PIM provenant de toute source.
3. Entrez l'adresse du **Group (Groupe)** multidiffusion ou l'adresse du groupe et le préfixe qui peuvent recevoir des paquets multidiffusion provenant de n'importe quelle source sur ces interfaces.
4. Sélectionnez **Included (Inclus)** pour inclure l'adresse de **Group (Groupe)** ASM dans le groupe d'interfaces (par défaut). Décochez **Included (Inclus)** pour facilement exclure un groupe ASM du groupe d'interfaces, notamment pendant les tests.
5. **Add (Ajoutez)** des **Groups (Groupes)** de multidiffusion supplémentaires (pour le groupe d'interfaces) qui veulent recevoir des paquets multicast de n'importe quelle source.
6. Pour configurer des groupes Source-Specific Multicast (Multidiffusion propre à une source ; SSM) pour ce groupe d'interfaces, dans la fenêtre Source Specific (Propre à la source), **Add (Ajoutez)** un **Name (Nom)** pour identifier un groupe multidiffusion et une

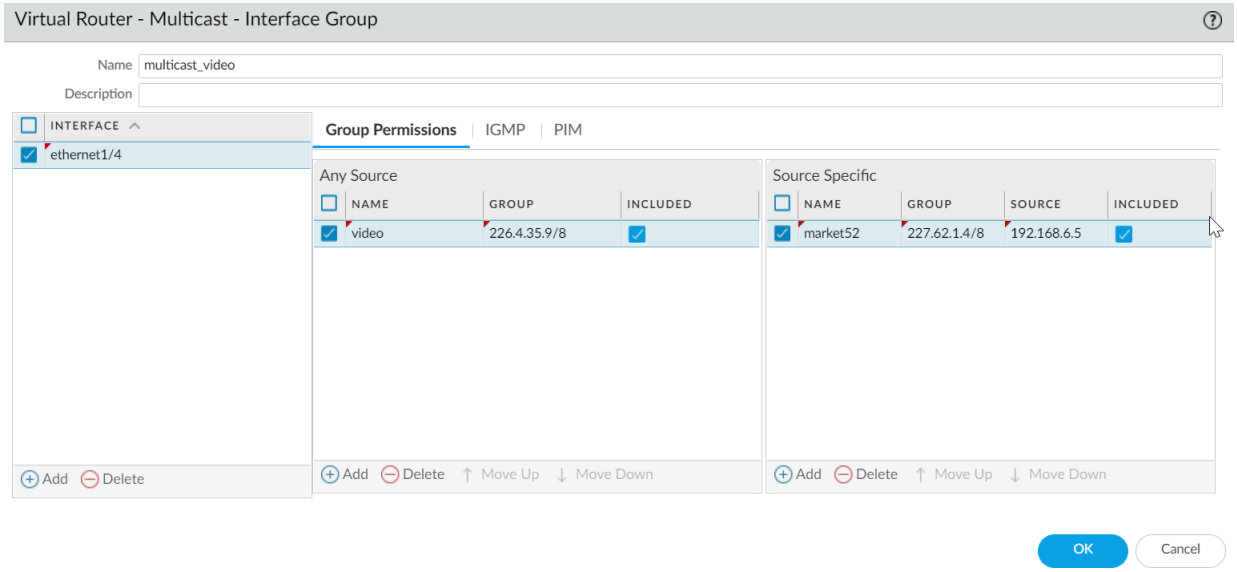
 ©2024 Palo Alto Networks, Inc.

paire d'adresses source. Évitez d'utiliser un nom que vous avez utilisé pour la diffusion Any Source (N'importe quelle source). (Vous devez utiliser IGMPv3 pour configurer SSM.)

7. Entrez l'adresse du **Group (Groupe)** ou l'adresse du groupe et le préfixe de groupe qui souhaite recevoir des paquets multidiffusion provenant de la source spécifiée uniquement (et qui peut recevoir les paquets sur ces interfaces).

   *Un groupe spécifique auquel vous spécifiez des autorisations est un groupe qui le routeur virtuel doit traiter comme propre à la source. Configurez la **Source Specific Address Space (Espace d'adresses spécifique à la source)** (étape 9) qui inclut les groupes propres à la source pour lesquels vous avez configuré l'autorisation.*

8. Entrez l'adresse IP **Source** à partir de laquelle ce groupe multidiffusion peut recevoir les paquets multidiffusion.
9. Sélectionnez **Included (Inclus)** pour inclure l'adresse de Groupe SSM et la paire d'adresses source dans le groupe d'interfaces (par défaut). Décochez **Included (Inclus)** pour facilement exclure la paire du groupe d'interfaces, notamment pendant les tests.
10. **Add (Ajoutez)** les **Groups (Groupes)** multidiffusion supplémentaires (pour le groupe d'interfaces) qui reçoivent des paquets multidiffusion d'une source donnée uniquement.



STEP 5 | Configurez IGMP pour le groupe d'interfaces si une interface est orientée vers les récepteurs multidiffusion, qui doivent utiliser IGMP pour joindre un groupe.

1. À l'onglet **IGMP**, **Enable (Activez)** IGMP (par défaut).
2. Spécifiez les paramètres IGMP des interfaces dans le groupe d'interfaces :
   - **IGMP Version (Version IGMP)**—**1**, **2** ou **3** (par défaut).
   - **Enforce Router-Alert IP Option (Appliquer l'option IP d'alerte du routeur)** (désactivée par défaut) : Sélectionnez cette option si vous exigez que les paquets IGMP qui utilisent IGMPv2 ou IGMPv3 disposent de l'option IP d'alerte du routeur, RFC 2113.
   - **Robustness (Robustesse)** : une variable que le pare-feu utilise pour affiner l'intervalle d'appartenance au groupe, l'intervalle Autre requérant présent, le nombre de requêtes

 ©2024 Palo Alto Networks, Inc.

au démarrage et le nombre de requêtes d'un membre dernier (plage comprise entre 1 et 7 ; valeur par défaut de 2). Augmentez la valeur si le sous-réseau sur lequel le pare-feu se trouve a tendance à perdre des paquets.

- **Max Sources (Max. de sources)** : nombre maximal de sources que IGMP peut traiter simultanément pour une interface (plage comprise entre 1 et 65 535 ; valeur par défaut **unlimited (illimitée)**).
- **Max Groups (Max. de groupes)** : nombre maximal de groupes que IGMP peut traiter simultanément pour une interface (plage comprise entre 1 et 65 535 ; valeur par défaut **unlimited (illimitée)**).
- **Query Interval (Intervalle de requête)** : nombre de secondes entre les messages de requête d'adhésion IGMP que le routeur virtuel envoie à un récepteur pour déterminer si le récepteur souhaite toujours recevoir les paquets multicast pour un groupe (la plage est comprise entre 1 et 31 744 ; la valeur par défaut est 125).
- **Max Query Response Time (sec) (Temps max. de réponse aux requêtes (sec.)** : nombre maximal de secondes dont dispose le récepteur pour répondre à un message de requête d'adhésion IGMP avant que le routeur virtuel détermine que le récepteur ne souhaite plus recevoir les paquets multidiffusion pour un groupe (la plage est comprise entre 1 et 3 174,4 ; la valeur par défaut est 10).
- **Last Member Query Interval (sec) (Dernier intervalle de requête d'un membre (sec.)** : nombre de secondes dont dispose un récepteur pour répondre à une requête propre à un groupe que le routeur virtuel envoie après qu'un récepteur envoie un message d'abandon de groupe (la plage est comprise entre 0,1 et 3 174,4 ; la valeur par défaut est 1).
- **Immediate Leave (Abandon immédiat)** (désactivé par défaut) : Lorsqu'il n'y a qu'un seul membre dans un groupe multidiffusion et que le routeur virtuel reçoit un message d'abandon IGMP pour ce groupe, le paramètre d'abandon immédiat entraîne la suppression immédiate par le routeur virtuel de ce groupe et de l'interface de sortie de la multicast routing information base (base d'informations de routage multidiffusion ; mRIB) et de la multicast forwarding information base (base d'informations de transfert multidiffusion ; mFIB) plutôt que d'attendre l'expiration du dernier intervalle de requête d'un membre. Le paramètre d'abandon immédiat épargner les ressources du réseau. Vous ne pouvez pas sélectionner Immediate Leave (Abandon immédiat) si le groupe d'interfaces utilise IGMPv1.

STEP 6 | Configurez le PIM Sparse Mode (PIM-SM) pour le groupe d'interfaces.

1. À l'onglet **PIM**, **Enable (Activez)** PIM (activé par défaut).
2. Spécifiez les paramètres PIM du groupe d'interfaces :
   - **Asset Interval (Intervalle d'affirmation)** : nombre de secondes entre les messages d'affirmation PIM que le routeur virtuel envoie à d'autres routeurs PIM sur le réseau à accès multiple lorsqu'il choisit un porteur PIM (plage de 0 à 65 534 ; la valeur par défaut est 177).
   - **Hello Interval (Intervalle Hello)** : nombre de secondes entre les messages Hello PIM que le routeur virtuel envoie à ses voisins PIM de chaque interface dans le groupe d'interfaces (plage de 0 à 18 000 ; la valeur par défaut est 30).
   - **Join Prune Interval (Intervalle de jointure/élagage)** : nombre de secondes entre les messages de jointure PIM (et entre les messages d'élagage PIM) que le routeur virtuel

 ©2024 Palo Alto Networks, Inc.

envoie en amont vers une source multicast (plage de 1 à 18 000 ; la valeur par défaut est 60).

- **DR Priority (Priorité du DR)** : priorité du Designated Router (routeur désigné - DR) qui contrôle quel routeur d'un réseau à accès multiple transmet les messages de jointure et d'élagage PIM au RP (plage comprise entre 0 et 4 294 967 295 ; la valeur par défaut est 1). La priorité du DR l'emporte sur les comparaisons d'adresses IP pour le choix du DR.
- **BSR Border (Bordure BSR)** : sélectionnez cette option si les interfaces du groupe d'interfaces se trouvent sur un routeur virtuel qui est le BSR situé à la bordure d'un LAN d'entreprise. Cela empêchera les messages BSR de la candidature RP de quitter le LAN.

3. **Add (Ajoutez)** un ou plusieurs **Permitted PIM Neighbors (Voisins PIM autorisés)** en spécifiant la **IP Address (Adresse IP)** de chaque routeur duquel le routeur virtuel accepte des paquets multidiffusion.

STEP 7 | Cliquez sur **OK (OK)** pour enregistrer les paramètres du groupe d'interfaces.

STEP 8 | (Facultatif) Modifiez le seuil du Shortest-Path Tree (chemin le plus court ; SPT), comme décrit à la section Chemin le plus court et arborescence partagée.

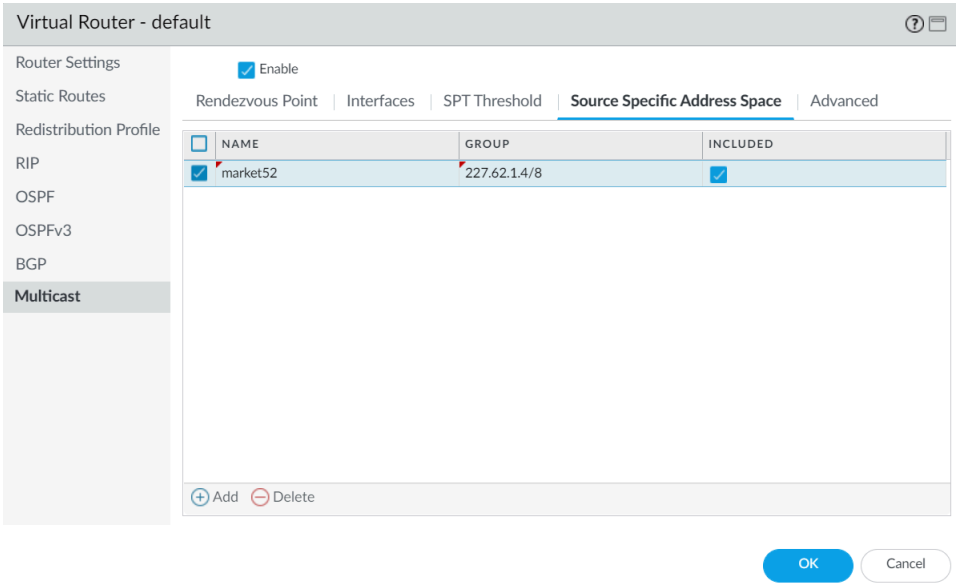
1. Sélectionnez le **SPT Threshold (Seuil SPT)** et **Add (Ajoutez)** un **Multicast Group/Prefix (Groupe/préfixe multidiffusion)**, le groupe ou le préfixe multidiffusion pour lequel vous spécifiez l'arbre de distribution.
2. Spécifiez le **Threshold (kb) (Seuil (ko)** : le stade auquel le routage vers le préfixe ou le groupe multidiffusion spécifié va basculer d'une distribution en arborescence partagée (issue du point de rendez-vous) à une distribution en arborescence source :
   - **0 (switch on first data packet) (commuter au premier paquet de données)** (par défaut) : la routeur virtuel bascule de l'arborescence partagée à une distribution en arborescence source pour le groupe ou le préfixe lorsque le routeur virtuel reçoit le premier paquet de données du groupe ou du préfixe.
   - **never (do not switch to spt) (jamais (ne pas basculer vers SPT))** : le routeur virtuel continue d'utiliser l'arborescence partagée pour transférer les paquets vers le groupe ou le préfixe.
   - Saisissez le nombre total de kilobits provenant des paquets multicast qui peuvent arriver pour le préfixe ou le groupe multicast à toute interface sur une période de temps déterminée, à quel moment le routeur virtuel bascule vers une distribution en arborescence source pour ce groupe ou préfixe multidiffusion.

STEP 9 | Identifiez les groupes multidiffusion ou les groupes et préfixes qui acceptent les paquets multidiffusion seulement d'une source spécifique.

1. Sélectionnez **Source Specific Address Space (Espace d'adresses spécifique à la source)**, puis **Add (Ajoutez)** le **Name (Nom)** de l'espace.
2. Entrez l'adresse du **Group (Groupe)** multidiffusion avec la longueur de préfixe pour identifier l'espace d'adresses qui reçoit des paquets multidiffusion provenant d'une source donnée. Si le routeur virtuel reçoit un paquet multidiffusion d'un groupe SSM, mais le groupe n'est pas couvert pas un **Source Specific Address Space (Espace d'adresses spécifique à la source)**, le routeur virtuel abandonne le paquet.

 ©2024 Palo Alto Networks, Inc.

3. Sélectionnez **Included (Inclus)** pour inclure l'espace d'adresses spécifique à la source en tant que plage d'adresses de groupes multidiffusion à partir de laquelle le routeur virtuel acceptera les paquets multidiffuson qui tirent leur origine d'une source spécifique autorisée. Décochez **Included (Inclus)** pour facilement exclure un espace d'adresses de groupes aux fins des tests.
4. Ajoutez une adresses spécifique à la source pour inclure tous ces groupes pour lesquels vous avez configuré l'autorisation du groupe SSM.



STEP 10 | (Facultatif) Modifiez la durée de temps pendant laquelle un itinéraire multidiffusion demeure dans la mRIB après la fin de la session entre un groupe multidiffusion et une source.

1. Sélectionnez l'onglet **Advanced (Avancé)**.
2. Précisez les **Multicast Route Age Out Time (sec) ((Paramètres d'expiration de l'itinéraire multidiffusion (sec))** (plage comprise entre 210 et 7 200 ; valeur par défaut de 210).

STEP 11 | Cliquez sur **OK** pour enregistrer la configuration multidiffusion.

STEP 12 | Créez une règle de politique de sécurité pour autoriser le trafic multidiffusion à destination de la zone de destination.

1. Créez une règle de politique de sécurité et, à l'onglet **Destination**, sélectionnez **multicast (multidiffusion)** ou **any (indifférent)** pour la **Destination Zone (Zone de destination)**. La zone **multicast (multidiffusion)** une zone de couche 3 prédéfinie qui met en correspondance tout le trafic multidiffusion. La **Destination Address (Adresse de destination)** peut correspondre à une adresse de groupes multidiffusion.
2. Configurez le reste de la règle de politique de sécurité.

STEP 13 | (Facultatif) Activez la mise en tampon des paquets multidiffusion avant l'établissement d'un itinéraire.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les Session Settings (Paramètres de session).
2. Activez la **Multicast Route Setup Buffering (Mise en tampon de configuration de route multidiffusion)** (désactivée par défaut). Le pare-feu peut préserver le premier paquet

©2024 Palo Alto Networks, Inc.

d'un flux multidiffusion lorsqu'une entrée du groupe de multidiffusion correspondant n'existe pas dans la Multicast Forwarding Table (Table de transfert multidiffusion ; mFIB). La **Buffer Size (Taille de tampon)** contrôle le nombre de paquets que le pare-feu met le flux en mémoire tampon. Une fois l'itinéraire installé dans le mFIB, le pare-feu transmet automatiquement le premier paquet au récepteur. (Si vos serveurs de contenu sont directement connectés au pare-feu et que votre application multidiffusion ne peut pas prendre en charge le premier paquet dans la session en cours de suppression, vous n'avez qu'à activer la mise en tampon de configuration de route multidiffusion.)

3. (Facultatif) Modifiez la **Buffer Size (Taille de tampon)**. La taille de tampon est le nombre de paquets par flux multidiffusion que le pare-feu peut mettre en mémoire tampon jusqu'à ce que l'entrée mFIB soit configurée (plage comprise entre 1 et 2 000 ; valeur par défaut de 1 000). Le pare-feu peut mettre en tampon un maximum de 5 000 paquets totaux (pour tous les flux).
4. Cliquez sur **OK**.

STEP 14 | **Commit (Validez)** vos modifications.

STEP 15 | Affichage des informations sur la multidiffusion IP pour consulter les entrées de la mRIB et de la mFIB , les paramètres de l'interface IGMP, les adhésions au groupe IGMP, les modes PIM ASM et SSM, les mappages de groupe à RP, les adresses des DR, les paramètres PIM, les voisins PIM et bien plus encore.

STEP 16 | Si vous configurez un itinéraire statique pour le trafic multidiffusion, vous pouvez installer l'itinéraire uniquement sur la table de routage multidiffusion (et non sur la table de routage monodiffusion), pour que l'itinéraire soit utilisé pour le trafic multidiffusion uniquement.

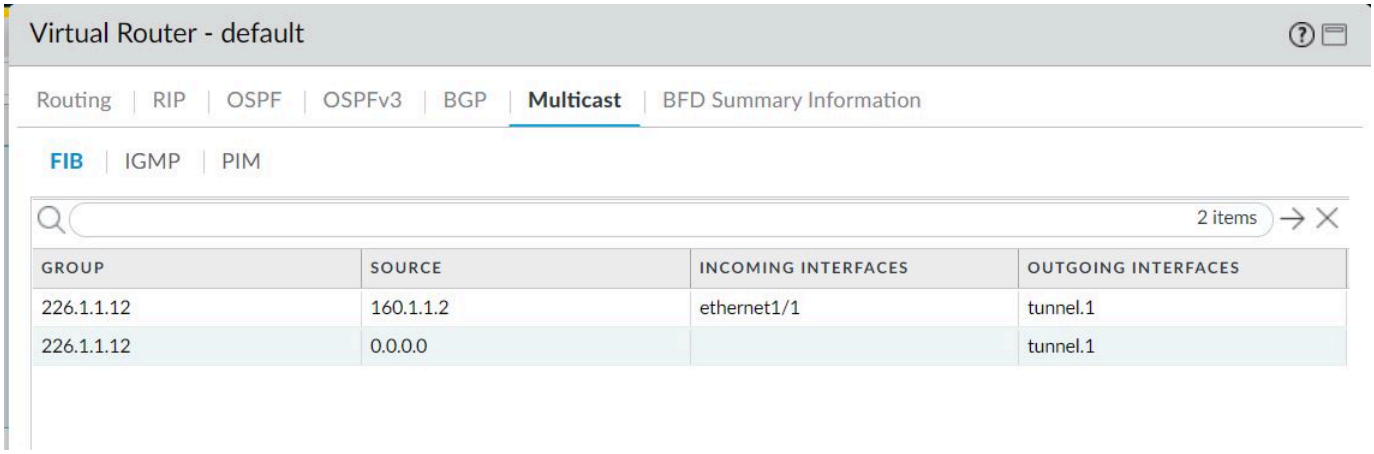
STEP 17 | Si vous activez la multidiffusion IP, il n'est pas nécessaire de configurer BGP avec MP-BGP pour la multidiffusion IPv4 , sauf si vous disposez d'une topologie multidiffusion logique distincte d'une topologie monodiffusion logique. Vous configurez les extensions MP-BGP avec la famille d'adresses IPv4 et la famille d'adresses multidiffusion subséquentes uniquement lorsque vous souhaitez publier des préfixes multidiffusion source dans BGP sous la famille d'adresses multidiffusion subséquentes.

 ©2024 Palo Alto Networks, Inc.

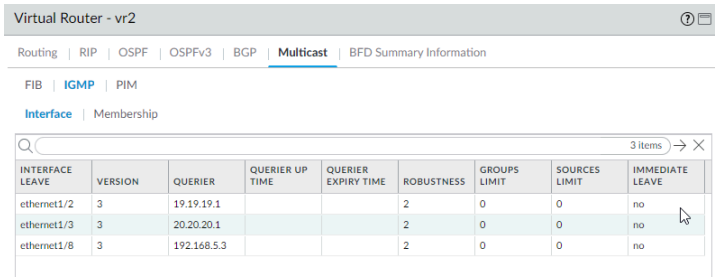
Affichage des informations sur la multidiffusion IP

Après avoir configurer l'itinéraire IP multicast, affichez les itinéraires multicast, les entrées de transfert et les informations relatives à vos interfaces IGMP et PIM.

- Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et, dans la rangée du routeur virtuel que vous avez configuré, cliquez sur **More Runtime Stats (Statistiques d'exécution supplémentaires)**.
  1. Sélectionnez **Routing (Routage)** > **Route Table (Table de routage)**, puis le bouton radio **Multicast** pour afficher uniquement les itinéraires multicast (groupe d'adresses IP multicast de destination, le saut suivant vers ce groupe et l'interface de sortie). Ces informations proviennent du mRIB.
  2. Sélectionnez **Multicast** > **FIB** pour afficher les informations sur les itinéraires multicast du mFIB : les groupes multicast auxquels le routeur virtuel appartient, la source correspondante, les interfaces d'entrée et les interfaces de sortie vers les récepteurs.

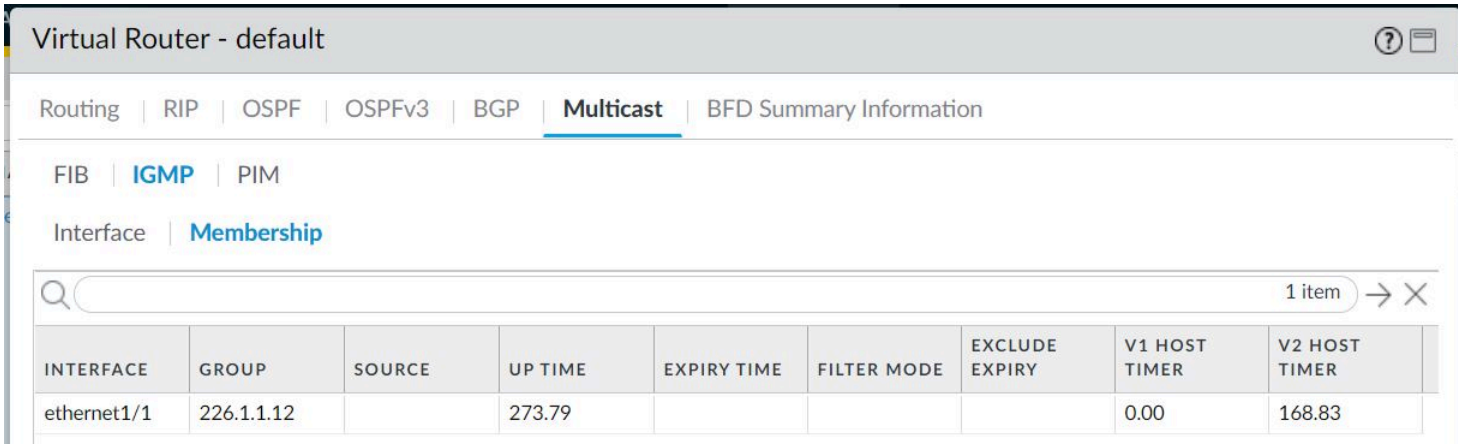


  3. Sélectionnez **Multicast** > **IGMP** > **Interface** pour afficher les interfaces sur lesquelles IGMP est activé, la version IGMP associée, l'adresse IP du requérant IGMP, le délai d'activation et d'expiration du requérant, le paramètre de robustesse, les nombres limites de groupes et sources multicast de même que pour savoir si l'option Quitter immédiatement est configurée sur l'interface.

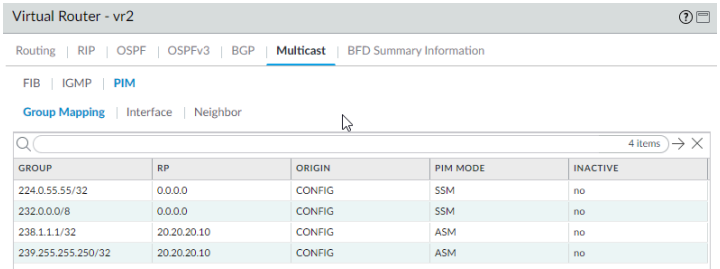


 ©2024 Palo Alto Networks, Inc.

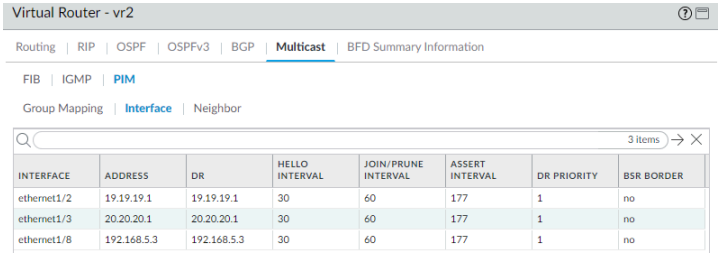
4. Sélectionnez **Multicast** > **IGMP** > **Membership (Appartenance)** pour voir les interfaces sur lesquelles IGMP est activé et les groupes multicast auxquels elles appartiennent, la source et les autres informations sur IGMP.



5. Sélectionnez **Multicast** > **PIM** > **Group Mapping (Mappage de groupes)** pour voir les groupes mappés au RP, l'origine du mappage RP, le mode PIM du groupe (ASM ou SSM) et pour voir si le groupe est inactif. Les groupes en mode SSM n'utilisent pas de RP, l'adresse RP qui s'affiche est donc 0.0.0.0. Le groupe SSM par défaut est 232.0.0.0/8.

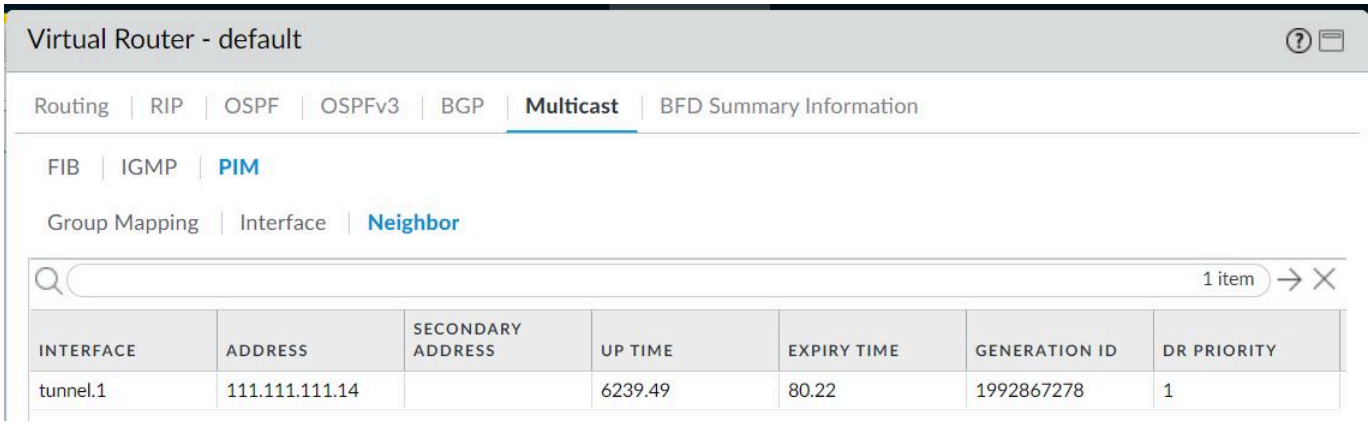


6. Sélectionnez **Multicast** > **PIM** > **Interface** pour afficher l'adresse IP du DR d'une interface ; la priorité DR ; les intervalles Hello, Join/Prune et d'affirmation et pour voir si l'interface est un routeur bootstrap (BSR).



 ©2024 Palo Alto Networks, Inc.

7. Sélectionnez **Multicast** > **PIM** > **Neighbor (Voisin)** pour voir les informations sur les routeurs qui sont des voisins PIM du virtuel routeur.



 ©2024 Palo Alto Networks, Inc.

Redistribution de route

Découvrez et configurez la redistribution des itinéraires pour augmenter l'accessibilité du trafic réseau.

- Présentation de la redistribution des itinéraires
- Configurez la redistribution des itinéraires.

Présentation de la redistribution des itinéraires

La redistribution d'itinéraire par le pare-feu consiste à rendre des itinéraires acquis par un protocole de routage (ou par un itinéraire statique ou connecté) accessibles à un différent protocole de routage, augmentant ainsi la facilité d'accès du trafic réseau. Sans redistribution d'itinéraire, un routeur ou un routeur virtuel ne publie et ne partage des itinéraires qu'avec d'autres routeurs fonctionnant sur le même protocole de routage. Vous pouvez redistribuer des itinéraires IPv4 ou IPv6 BGP, connectés, ou encore statiques dans le RIB OSPF, et redistribuer des itinéraires OSPFv3, connectés, ou statiques dans le RIB BGP.

Cela signifie, par exemple, que vous pouvez rendre des réseaux spécifiques, qui n'étaient jusqu'à présent disponibles que par configuration manuelle d'itinéraires statiques sur des routeurs spécifiques, accessibles aux systèmes autonomes BGP ou aux zones OSPF. Vous pouvez également publier des itinéraires connectés en local, comme les itinéraires du réseau d'un laboratoire privé, dans des systèmes autonomes BGP ou des zones OSPF.

Vous voulez peut-être donner la possibilité aux utilisateurs de votre réseau OSPFv3 interne d'accéder au BGP pour qu'ils puissent se connecter à des périphériques sur internet. Dans ce cas, vous pouvez redistribuer des itinéraires BGP dans la table de routage OSPFv3.

À l'inverse, vous voulez peut-être donner la possibilité à vos utilisateurs externes d'accéder à certaines parties de votre réseau interne ; vous pouvez rendre vos réseaux OSPFv3 internes accessibles par BGP en redistribuant des itinéraires OSPFv3 dans le RIB BGP.

Pour Configurez la redistribution des itinéraires. , commencez par créer un profil de redistribution.

 ©2024 Palo Alto Networks, Inc.

Configurez la redistribution des itinéraires.

Effectuez la procédure suivante pour configurer la route redistribution (redistribution des routes).

STEP 1 | Créez un profil de redistribution.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez un routeur virtuel.
2. Sélectionnez **Redistribution Profile (Profil de redistribution)** et **IPv4** ou **IPv6** et **Add (Ajoutez)** un profil.
3. Saisissez un **Name (Nom)** à donner au profil, lequel doit commencer par un caractère alphanumérique et doit contenir des zéros ou des traits de soulignement (_), des traits d'union (-), des points (.) ou des espaces (maximum de 16 caractères).
4. Saisissez une **Priority (Priorité)** pour le profil dans la plage comprise entre 1 et 255. Le pare-feu met les itinéraires en correspondance avec les profils par ordre de priorité (valeur la plus basse en premier). Les règles de priorité supérieure prennent le pas sur les règles de priorité inférieure.
5. Pour **Redistribute (Redistribuer)**, sélectionnez l'une des options suivantes :
   - **Redist** - Sélectionnez cette option pour la redistribution les itinéraires qui correspondent à ce filtre.
   - **No Redist (Ne pas redist)** - Sélectionnez cette option pour la redistribution les itinéraires qui correspondent aux profils de redistribution exceptés les itinéraires qui correspondent à ce filtre. Cette sélection considère le profil comme une liste de blocage spécifiant quels itinéraires ne pas sélectionner pour la redistribution. Par exemple, si vous avez de multiples profils de redistribution BGP, vous pouvez créer un profil **No Redist (Ne pas redist)** pour exclure plusieurs préfixes, puis un profil de redistribution général avec une priorité inférieure (valeur plus élevée) à la suite. Les deux profils cohabitent et le profil de priorité supérieure prend le pas sur l'autre. Vous ne pouvez pas avoir que des profils **No Redist (Ne pas redist)** ; un profil **Redist** est toujours nécessaire pour la redistribution d'itinéraires.

 ©2024 Palo Alto Networks, Inc.

6. Dans l'onglet **General Filter (Filtre Général)**, pour le Type de Source, sélectionnez un ou plusieurs types d'itinéraires à redistribuer :
   - **bgp** - Redistribuer des itinéraires BGP correspondant au profil.
   - **connect (connectés)** - Redistribuer des itinéraires connectés correspondant au profil.
   - **ospf** (IPv4 uniquement) - Redistribuer des itinéraires BGP correspondant au profil.
   - **rip** (IPv4 uniquement) - Redistribuer des itinéraires BGP correspondant au profil.
   - **ospfv3** (IPv6 uniquement) - Redistribuer des itinéraires OSPFv3 correspondant au profil.
   - **static (statiques)** - Redistribuer des itinéraires statiques correspondant au profil.
7. (Facultatif) Pour l'**Interface**, **Add (Ajoutez)** une ou plusieurs interfaces de sorties ou des itinéraires associés correspondants à redistribuer. Pour supprimer une entrée, cliquez sur **Delete (Supprimer)**.
8. (Facultatif) Pour la**Destination**, **Add (Ajoutez)** une ou plusieurs destinations IPv4 ou IPv6 d'itinéraires correspondants à redistribuer. Pour supprimer une entrée, cliquez sur **Delete (Supprimer)**.
9. (Facultatif) Pour le**Next Hop (Saut Suivant)**, **Add (Ajoutez)** une ou plusieurs adresses IPv4 ou IPv6 de saut suivant d'itinéraires correspondants à redistribuer. Pour supprimer une entrée, cliquez sur **Delete (Supprimer)**.
10. Cliquez sur **OK**.

STEP 2 | (Facultatif—Quand Filtre Général inclut ospf ou ospfv3) Créez un filtre OSPF pour mieux préciser quels itinéraires OSPF ou OSPFv3 sont à redistribuer.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel.
2. Sélectionnez **Redistribution Profile (Profil de redistribution)** et **IPv4** ou **IPv6**, puis sélectionnez le profil que vous avez créé.
3. Sélectionnez **OSPF Filter (Filtre OSPF)**.
4. Pour le Type de chemin, sélectionnez un ou plusieurs types de chemin OSPF à redistribuer : **ext-1**, **ext-2**, **inter-area (inter-zone)** ou **intra-area (intra-zone)**.
5. Pour spécifier une **Area (Zone)** de départ pour lé redistribution d'itinéraires OSPF ou OSPFv3, **Add (Ajoutez)** une zone au format adresse IP.
6. Pour spécifier une **Tag (Étiquette)**, **Add (Ajoutez)** une étiquette au format adresse IP.
7. Cliquez sur **OK**.

STEP 3 | (Facultatif—Quand Filtre Général inclut bgp) Créez un filtre BGP pour mieux préciser quels itinéraires BGP sont à redistribuer.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel.
2. Sélectionnez **Redistribution Profile (Profil de redistribution)** et **IPv4** ou **IPv6**, puis sélectionnez le profil que vous avez créé.
3. Sélectionnez **BGP Filter (Filtre OSPF)**.
4. Pour **Community (Communauté)**, sélectionnez **Add (Ajouter)** pour choisir dans une liste de communauté, comme des communautés notoires : **local-as**, **no-advertise**, **no-**

 ©2024 Palo Alto Networks, Inc.

export ou **nopeer**. Vous pouvez également saisir une valeur 32 bits au format décimal, hexadécimal ou AS:VAL ; où AS et VAL sont tous deux dans la plage de 0 à 65 535. Saisissez un maximum de 10 entrées.

5. Pour **Extended Community (Communauté étendue)**, **Add (Ajoutez)** une valeur de 64 bits au format hexadécimal ou au format TYPE:AS:VAL ou au format TYPE:IP:VAL. TYPE est de 16 bits, AS ou IP sont de 16 bits et VAL est de 32 bits. Saisissez un maximum de 5 entrées.
6. Cliquez sur **OK**.

STEP 4 | Sélectionnez le protocole dans lequel vous redistribuez les itinéraires, et saisissez les attributs de ces itinéraires.

Cette tâche illustre la redistribution d'itinéraires dans un protocole BGP.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel.
2. Sélectionnez **BGP** > **Redist Rules (Règles de redistribution)**.
3. Sélectionnez **Allow Redistribute Default Route (Autoriser la redistribution de l'itinéraire par défaut)** pour autoriser le pare-feu à redistribuer l'itinéraire par défaut.
4. Cliquez sur **Add (Ajouter)**.
5. Sélectionnez **Address Family Type (Type de famille d'adresses)** : **IPv4** ou **IPv6** pour préciser dans quelle table les itinéraires redistribués seront mis.
6. Sélectionnez le **Name (Nom)** du profil de redistribution que vous avez créé, pour sélectionner l'itinéraire à redistribuer.
7. **Enable (Activez)** la règle de redistribution.
8. (Facultatif) Saisissez l'une des valeurs suivantes, que le pare-feu va appliquer aux itinéraires redistribués :
   - **Metric (Métrique)** dans la plage allant de 1 à 65 535.
   - **Set Origin (Saisissez l'origine)** - l'origine de l'itinéraire : **igp**, **egp** ou **incomplete**.
   - **Set MED (Définir le MED)** - valeur du MED dans la plage allant de 0 à 4 294 967 295.
   - **Set Local Preference (Définir la Préférence locale)** - valeur de la préférence locale dans la plage allant de 0 à 4 294 967 295.
   - **Set AS Path Limit (Définir la limite de chemin d'AS)** - quantité maximale de systèmes autonomes dans le AS_PATH dans la plage allant de 1 à 255.
   - **Set Community (Définir la Communauté)** - sélectionnez ou saisissez une valeur 32 bits au format décimal, hexadécimal ou AS:VAL ; où AS et VAL sont tous deux dans la plage allant de 0 à 65 525. Saisissez un maximum de 10 entrées.
   - **Set Extended Community (Saisissez la Communauté Étendue)** - Sélectionnez ou saisissez une valeur de 64 bits au format hexadécimal ou au format TYPE:AS:VAL ou au format TYPE:IP:VAL. TYPE est de 16 bits, AS ou IP sont de 16 bits et VAL est de 32 bits. Saisissez un maximum de 5 entrées.
9. Cliquez sur **OK**.

STEP 5 | **Commit (Validez)** vos modifications.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Tunnels GRE

Le protocole de tunnel de Generic Routing Encapsulation (encapsulation générique de routage ; GRE) est un protocole de transport qui encapsule un protocole de charge utile. Le paquet GRE lui-même est encapsulé dans un protocole de transport (IPv4 ou IPv6).

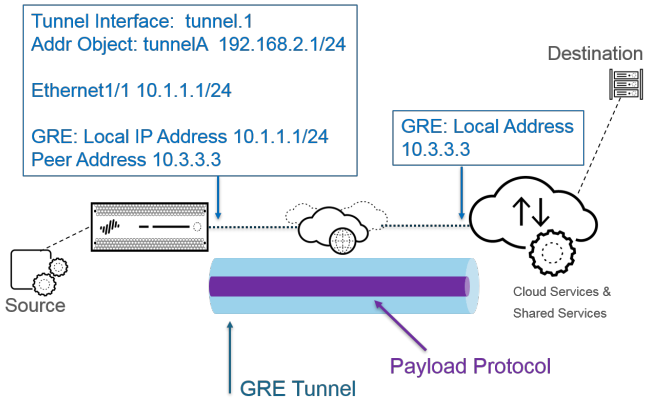
- Aperçu du tunnel GRE
- Création d'un tunnel GRE

Aperçu du tunnel GRE

Un tunnel Generic Routing Encapsulation (encapsulation générique de routage ; GRE) connecte deux points de terminaison (un pare-feu et un autre appareil) en une liaison logique de point à point. Le pare-feu peut mettre fin aux tunnels GRE ; vous pouvez acheminer les paquets vers un tunnel GRE ou les y transférer. Les tunnels GRE sont simples à utiliser. C'est souvent le protocole de tunnellisation de choix pour la connectivité de point à point, spécialement aux services dans le clous ou aux réseaux partenaires.

Créez un tunnel GRE lorsque vous voulez que les paquets qui sont destinés à une adresse IP prennent un chemin point à point donné, par exemple vers un proxy dans le cloud ou un réseau partenaire. Les paquets passent par le tunnel GRE (par l'intermédiaire d'un réseau de transit, comme l'Internet) vers le service Cloud lors de leur transit vers l'adresse de destination. Le service Cloud peut ainsi appliquer ses services ou politiques sur les paquets.

La figure suivante est une exemple d'un tunnel GRE se connectant au pare-feu par l'intermédiaire de l'Internet vers un service Cloud.



Pour accroître la performance et pour éviter l'échec des points uniques, répartissez les connexions vers le pare-feu entre plusieurs tunnels GRE, plutôt que d'utiliser un seul tunnel. Chaque tunnel GRE a besoin d'une interface de tunnel.

Lorsque le pare-feu autorise un paquet à passer (selon une correspondance de politique) et que le paquet sort vers une interface de tunnel GRE, le pare-feu ajoute l'encapsulation ; il ne génère pas de session. Le pare-feu n'effectue aucune recherche de règle de politique de sécurité pour le trafic GRE encapsulé. Vous n'avez donc pas besoin d'une règle de politique de sécurité pour le trafic GRE que le pare-feu encapsule. Cependant, lorsque le pare-feu reçoit le trafic GRE, il génère une session et applique toutes les politiques à l'en-tête GRE IP en plus du trafic encapsulé. Le pare-feu traite les paquets GRE reçus comme tout autre paquet. Par conséquent :

- Si la pare-feu reçoit le paquet GRE sur une interface qui possède la même zone que l'interface de tunnel associée au tunnel GRE (par exemple, tunnel.1), la zone source est identique à la zone de destination. Par défaut, le trafic est autorisé au sen d'une zone (trafic intra-zone). Le trafic GRE entrant est donc autorisé par défaut.
- Cependant, si vous avez configuré votre propre règle de politique de sécurité intra-zone pour refuser ce type de trafic, vous devez explicitement autoriser le trafic GRE.

 ©2024 Palo Alto Networks, Inc.

- Également, si la zone de l'interfaces de tunnel qui est associée au tunnel GRE (par exemple, tunnel.1) est différente de la zone de l'interface d'entrée, vous devez configurer une règle de politique de sécurité pour autoriser le trafic GRE.

Comme la pare-feu encapsule le paquet tunnellisé dans un paquet GRE, les 24 octets supplémentaires d'en-tête GRE donne automatiquement lieu à une Maximum Segment Size (taille de segment maximale ; MSS) plus faible dans la maximum transmission unit (unité de transmission maximale ; MTU). Si vous ne modifiez pas la Taille d'ajustement MSS IPv64 de l'interface, le pare-feu réduit par défaut la MTU de 64 octets (40 octets d'en-tête IP + 24 octets d'en-tête GRE). Cela signifie que si la MTU par défaut est de 1 500 octets, la MSS est de 1 436 octets (1 500 - 40 - 24 = 1 436). Si vous configurez une taille d'ajustement MSS de 300 octets, par exemple, la MSS ne sera alors que de 1 176 octets (1 500 - 300 - 24 = 1 176).

Le pare-feu ne prend pas en charge le routage d'un tunnel GRE ou IPSec vers un tunnel GRE, mais vous pouvez acheminer un tunnel GRE vers un tunnel IPSec. De plus :

- Un tunnel GRE ne prend pas en charge la QoS.
- Le pare-feu ne prend pas en charge une interface simple faisant office de point de terminaison du tunnel GRE et d'agent de déchiffrement.
- La tunellisation GRE ne prend pas en charge la NAT entre les points de terminaison GRE.

Si vous avez besoin de vous connecter à un réseau d'un autre éditeur, nous vous recommandons de set up an IPSec tunnel (configurer un tunnel IPSec)*, pas un tunnel GRE ; vous ne devriez utiliser un tunnel GRE que si c'est le seul mécanisme de tunnel point-à-point supporté par l'éditeur Vous pouvez également activer GRE sur IPSec si le point de terminaison distant l'exige en cliquant sur* ***Add GRE Encapsulation (Ajouter l'encapsulation GRE)****. Ajoutez l'encapsulation GRE dans les cas où le point de terminaison distant exiger l'encapsulation du trafic dans un tunnel GRE avant son chiffrement par IPSec. Par exemple, certaines applications exigent l'encapsulation du trafic multidiffusion avant son chiffrement par IPSec. S'il s'agit d'une exigence de votre environnement et que le tunnel GRE et le tunnel IPSec partagent la même adresse IP, sélectionnez* ***Add GRE Encapsulation (Ajouter l'encapsulation GRE)*** *lors de la configuration du tunnel IPSec.*

*Si vous ne prévoyez pas de mettre fin à un tunnel GRE sur le pare-feu, mais que vous souhaitez disposer de la capacité d'inspecter et de contrôler le trafic qui traverse le pare-feu à l'intérieur d'un tunnel GRE, ne créez pas de tunnel GRE. Effectuez plutôt l'*Inspection du contenu du tunnel *du trafic GRE. Grâce à l'inspection du contenu du tunnel, vous inspectez le trafic GRE qui transite par le pare-feu et appliquez à ce dernier la politique sans créer de liaison point à point logique pour acheminer le trafic.*

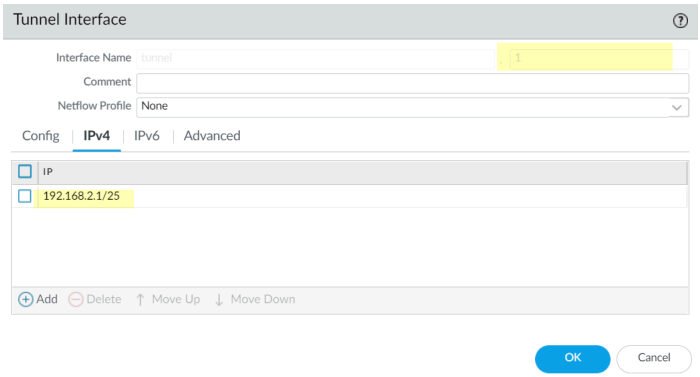
 ©2024 Palo Alto Networks, Inc.

Création d'un tunnel GRE

Un tunnel Generic Routing Encapsulation (encapsulation générique de routage ; GRE) connecte deux points de terminaison en une liaison logique de point à point.

STEP 1 | Créez une interface de tunnel.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Tunnel**.
2. **Add (Ajoutez)** un tunnel, puis entrez le **Interface Name (Nom d'interface)** du tunnel, suivi d'un point et d'un numéro se situant entre 1 et 9 999 ; par exemple, tunnel.1. Par exemple, **`tunnel.1`**.
3. Dans l'onglet **Config (Configuration)**, affectez l'interface du tunnel à un **Virtual Router (routeur virtuel)**.
4. Affectez l'interface du tunnel à un **Virtual System (Système virtuel)** si le pare-feu prend en charge plusieurs systèmes virtuels.
5. Affectez l'interface du tunnel à une **Security Zone (Zone de sécurité)**.



6. Affectez une adresse IP à l'interface du tunnel. (Vous devez affecter une adresse IP si vous souhaitez acheminer le trafic vers ce tunnel ou surveiller le point de terminaison du tunnel.) Sélectionnez **IPv4** ou **IPv6** ou configurez les deux options.

   Cette adresse et l'adresse correspondante de l'interface du tunnel de l'homologue doivent se trouver sur le même sous-réseau, car il s'agit d'une liaison point à point logique.

   - À l'onglet IPv4, **Add (Ajoutez)** une adresse IPv4 ou sélectionnez un objet d'adresse, ou cliquez sur **New Address (Nouvelle adresse)** et spécifiez le **Type** d'adresse et saisissez-le. Par exemple, saisissez 192.168.2.1.
   - (IPv6 uniquement) Sous l'onglet **IPv6 activez IPv6 sur l'interface**.
     1. Pour **ID d'interface**, sélectionnez **EUI-64 (identificateur unique étendu 64 bits par défaut).**
     2. **Add (Ajoutez)** une nouvelle **Address (Adresse)** ou sélectionnez un objet d'adresse IPv6, ou cliquez sur **New Address (Nouvelle adresse)** et spécifiez un **Name (Nom)**

 ©2024 Palo Alto Networks, Inc.

d'adresse. **Enable address on interface (Activez l'adresse sur l'interface)**, puis cliquez sur **OK**.

3. Sélectionnez le **Type** d'adresse et saisissez l'adresse IPv6 ou le FQDN et cliquez sur **OK** pour enregistrer la nouvelle adresse.
4. Sélectionnez **Enable address on interface (Activer l'adresse sur l'interface)**, puis cliquez sur **OK**.

7. Cliquez sur **OK**.

STEP 2 | Créez un tunnel GRE pour diriger les paquets vers un chemin point à point donné.

1. Sélectionnez **Network (Réseau)** > **GRE Tunnels (Tunnels GRE)** et **Add (Ajoutez)** un tunnel en fonction du **Name (Nom)**.
2. Sélectionnez l'**interface** à utiliser en tant que point de terminaison du tunnel GRE local (interface source), soit une interface ou une sous-interface Ethernet, une interface Aggregate Ethernet (AE), une interface de bouclage ou une interface VLAN.
3. Sélectionnez **IP** en que **Local Address (Adresse locale)** , puis sélectionnez l'adresse IP de l'interface que vous venez de sélectionner.
4. Saisissez la **Peer Address (Adresse de l'homologue)**, à savoir l'adresse IP du point de terminaison opposé du tunnel GRE.
5. Sélectionnez la **Tunnel Interface (Interface de tunnel)** que vous avez créé à l'étape 1. (Cette interface identifie le tunnel lorsqu'il correspond à l'**Interface** de sortie pour le routage.)
6. Saisissez la **TTL** du paquet IP encapsulé dans le paquet GRE (plage comprise entre 1 et 255 ; la valeur par défaut est 64).
7. 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 entrant vers l'en-tête IP sortant des paquets encapsulés afin de conserver les informations ToS d'origine. Sélectionnez cette option si votre réseau utilise QoS et qu'il dépend des octets ToS pour appliquer les politiques QoS.



 ©2024 Palo Alto Networks, Inc.

STEP 3 | (Recommandé) Activez la fonction Keep Alive du tunnel GRE.

Si vous activez la fonction Keep Alive, il faut trois paquets keep alive non retournés (nouvelles tentatives) à des intervalles de dix secondes pour que le tunnel GRE échoue, et il faut cinq intervalles Délai de maintien à des intervalles de dix secondes pour que le tunnel GRE redevienne actif.

1. Sélectionnez **Keep Alive** pour activer la fonction Keep Alive du tunnel GRE (désactivée par défaut).
2. (Facultatif) Définissez l'**Interval (sec) (Intervalle [sec])** (en secondes) entre des paquets keepalive que l'extrémité locale du tunnel GRE envoie au tunnel homologue. Il s'agit également de l'intervalle qui, lorsque multiplié par la **Hold Timer (Minuterie d'attente)**, correspond à la durée de temps pendant laquelle le pare-feu doit constater des paquets keepalive réussis avant que le tunnel GRE soit de nouveau disponible (la plage est comprise entre 50 et 10 ; la valeur par défaut est 1). Si vous définissez un intervalle trop court, de nombreux paquets keepalive qui pourraient être inutiles pénètreront dans votre et vous aurez besoin d'une bande passante et d'un traitement supplémentaires. Si vous définissez un intervalle trop long, vous pourriez retarder le basculement, car les conditions d'erreur pourraient ne pas être identifiées immédiatement.
3. (Facultatif) Saisissez le paramètre de **Retry (Nouvelle tentative)**, soit le nombre d'intervalles pendant lesquels aucun paquet keepalive sont retournés avant que le pare-feu considère que le tunnel homologue est indisponible (valeur par défaut : 1 ; plage comprise entre 255 et 3). Lorsque le tunnel est indisponible, le pare-feu supprime les itinéraires qui y sont associés dans la table de transfert. La configuration d'un paramètre de nouvelle tentative permet d'éviter que des mesures soient prises à l'égard d'un tunnel qui n'est pas réellement indisponible.
4. (Facultatif) Saisissez la **Hold Timer (Minuterie d'attente)**, soit le nombre d'**Intervals (Intervalles)** pendant lesquels les paquets keepalive sont réussis, après quoi le pare-feu rétablit la connexion avec le tunnel homologue (valeur par défaut : 1 ; plage comprise entre 64 et 5).

STEP 4 | Cliquez sur **OK**.

STEP 5 | Configurez un protocole de routage ou un itinéraire statique pour acheminer le trafic vers la destination, en passant par le tunnel GRE. Par exemple, Configuration d'un itinéraire statique au réseau du serveur de destination et spécifiez que l'**Interface** de sortie doit être le point de terminaison du tunnel local (ethernet1/1). Configurez l'adresse IP du tunnel à l'autre extrémité en tant que saut suivant. Par exemple : 192.168.2.3.

STEP 6 | **Commit (Validez)** vos modifications.

STEP 7 | Configurez l'extrémité opposée du tunnel avec son adresse IP publique, ses adresses IP locales et d'homologues (cela correspond aux adresses IP locales et de l'homologue, respectivement, du tunnel GRE sur le pare-feu), et son protocole de routage ou son itinéraire statique.

STEP 8 | Vérifiez que le pare-feu peut communiquer avec son tunnel homologue via le tunnel GRE.

1. Accédez à la CLI.
2. > **`ping source 192.168.2.1 host 192.168.2.3`**

 ©2024 Palo Alto Networks, Inc.

DHCP

Cette section décrit le protocole Dynamic Host Configuration Protocol (protocole de configuration dynamique des hôtes - DHCP) et les tâches permettant de configurer une interface sur un pare-feu Palo Alto Networks® pour agir en tant que serveur, client ou agent de relais DHCP. En affectant ces rôles à différentes interfaces, le pare-feu peut remplir plusieurs rôles.

- Présentation de DHCP
- Pare-feu en tant que serveur et client DHCP
- Pare-feu en tant que client DHCPv6
- Messages DHCP
- Adressage DHCP
- Options DHCP
- Configuration d'une interface en tant que serveur DHCP
- Configurer une interface en tant que client DHCPv4
- Configurer une interface en tant que client DHCPv6 avec délégation de préfixes
- Configuration de l'interface de gestion en tant que client DHCP
- Configuration de l’interface de gestion pour l’attribution d’adresses IPv6 dynamiques
- Configuration d'une interface en tant qu'agent de relais DHCP
- Surveillance et dépannage de DHCP

Présentation de DHCP

DHCP est un protocole normalisé défini dans le document RFC 2131, Dynamic Host Configuration Protocol (protocole de configuration dynamique des hôtes ; DHCP). DHCP a deux fonctions principales : fournir les paramètres de configuration de couche de liaison et TCP/IP, et fournir des adresses réseau aux hôtes configurés de manière dynamique sur un réseau TCP/IP.

DHCP utilise un modèle de communication client/serveur. Ce modèle est composé de trois rôles que le périphérique peut remplir : client DHCP, serveur DHCP et agent de relais DHCP.

- Un équipement agissant comme un client (hôte) DHCP peut demander une adresse IP et d'autres paramètres de configuration à un serveur DHCP. Les utilisateurs sur les périphériques gagnent ainsi du temps lors de la configuration et n'ont pas besoin de connaître le plan d'adressage du réseau ou d'autres ressources et options héritées du serveur DHCP.
- Un équipement agissant comme un serveur DHCP peut servir des clients. L'utilisation de l'un des trois mécanismes d'Adressage DHCP permet à l'administrateur réseau de gagner du temps lors de la configuration et de réutiliser un nombre limité d'adresses IP lorsqu'un client n'a plus besoin de connexion réseau. Le serveur peut fournir l'adressage IP et diverses options DCHP à de nombreux clients.
- Un équipement agissant comme un agent de relais DHCP transmet des messages DHCP entre les clients et les serveurs DHCP.

DHCP utilise User Datagram Protocol (Protocole de datagramme utilisateur, UDP), à savoir RFC 768 comme protocole de transport. Un client envoie des messages DHCP à un serveur sur le port 67 bien connu (port UDP utilisé par BOOTP et DHCP). Les Messages DHCP qu'un serveur envoie à un client sont envoyés sur le port 68.

Une interface sur un pare-feu Palo Alto Networks® peut remplir le rôle d'un serveur, d'un client ou d'un agent de relais DHCP. L'interface d'un serveur ou d'un agent de relais DHCP doit être une interface Ethernet de Couche 3, Aggregated Ethernet ou VLAN de Couche 3. Configurez les interfaces du pare-feu avec les paramètres appropriés pour toute combinaison de rôles. Le comportement de chaque rôle est récapitulé dans la section Pare-feu en tant que serveur et client DHCP.

Le pare-feu peut également fonctionner comme un DHCPv6 client (client DHCPv6), avec ou sans délégation de préfixe.

Le pare-feu prend en charge le serveur DHCPv4 et le relais DHCPv6.

L'implémentation d'un serveur DHCP par Palo Alto Networks prend en charge les adresses IPv4 uniquement. L'implémentation de relais DHCP prend en charge IPv4 et IPv6. Le client DHCP supporte les adresses IPv4 et IPv6. Le client DHCP n'est pas pris en charge en mode haute disponibilité active/active.

L'interface de gestion du pare-feu prend en charge à la fois le client DHCP et l'attribution d'adresses IPv6 dynamiques.

 ©2024 Palo Alto Networks, Inc.

Pare-feu en tant que serveur et client DHCP

Le pare-feu peut fonctionner comme un serveur DHCP et un client DHCP. Dynamic Host Configuration Protocol (protocole de configuration dynamique des hôtes - DHCP) (RFC 2131), a été conçu pour prendre en charge les adresses IPv4 et IPv6. L'implémentation d'un serveur DHCP par Palo Alto Networks® prend en charge les adresses IPv4 uniquement.

Le serveur DHCP du pare-feu fonctionne de la manière suivante :

- Lorsque le serveur DHCP reçoit un message DHCPDISCOVER d'un client, il répond par un message DHCPOFFER contenant toutes les options prédéfinies et personnalisées dans l'ordre dans lequel elles s'affichent dans la configuration. Le client sélectionne les options dont il a besoin et répond par un message DHCPREQUEST.
- Lorsque le serveur DHCP reçoit un message DHCPREQUEST d'un client, il répond par un message DHCPACK contenant uniquement les options indiquées dans la demande.

Le client DHCP du pare-feu fonctionne de la manière suivante :

- Lorsque le client DHCP reçoit un message DHCPOFFER du serveur, il met automatiquement en cache toutes les options fournies en vue d'une utilisation ultérieure, quelles que soient les options envoyées dans son message DHCPREQUEST.
- Par défaut et afin d'économiser de la mémoire, le client met en cache la première valeur de chaque code d'option uniquement s'il reçoit plusieurs valeurs pour un code.
- La longueur des messages DHCP n'est pas limitée, à moins que le client DHCP n'indique un maximum dans l'option 47 dans ses messages DHCPDISCOVER ou DHCPREQUEST.

  Le pare-feu peut également fonctionner comme un DHCPv6 client (client DHCPv6).

À partir de PAN-OS 11.1.4 et des versions ultérieures, le pare-feu prend en charge les adresses IPv4 et IPv6 doubles (chevauchement) sur les interfaces de couche 3 qui utilisent des routeurs logiques différents. Découvrez cette fonctionnalité avant d'activer la prise en charge des adresses IP doubles et de configurer les adresses IP qui se chevauchent.

 ©2024 Palo Alto Networks, Inc.

Pare-feu en tant que client DHCPv6

Le pare-feu peut agir en tant que client DHCPv6 pour demander une adresse IPv6 pour son interface et un préfixe IPv6 et les options associées (telles que le DNS et la liste de recherche de domaine) à partir d'un serveur DHCPv6, fournissant ainsi un Ethernet de couche 3, un VLAN ou un Ethernet agrégé (AE). L'interface compatible IPv6 envoie un message de sollicitation de routeur au routeur délégant pour obtenir des informations supplémentaires, telles que la passerelle. Le client DHCPv6 réduit vos efforts de provisionnement d'adresses IPv6 et les erreurs potentielles, et automatise la tâche d'accès de vos hôtes au réseau.

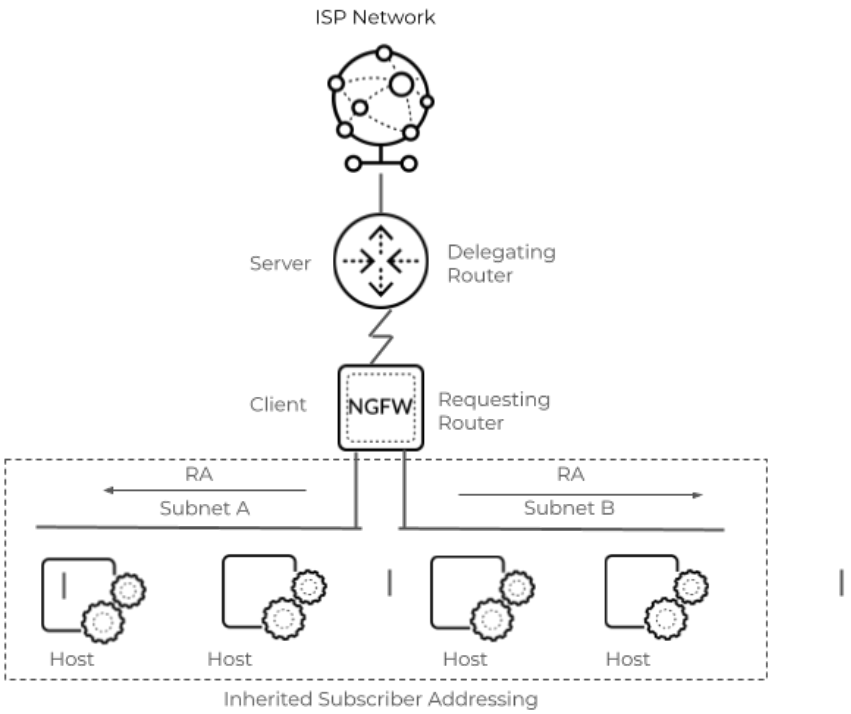
De plus, le pare-feu client DHCPv6 prend en charge la délégation de préfixe. Un FAI attribue des préfixes (avec une longueur de préfixe de /48 à /64) à un serveur DHCPv6, qui à son tour attribue des préfixes au pare-feu client DHCPv6. Le pare-feu attribue ensuite un sous-réseau du pool de préfixes de préfixes délégués à une ou plusieurs de ses interfaces côté hôte. Les interfaces déléguées distribuent les adresses du pool délégué au réseau local à l'aide du protocole NDP (Neighbor Discovery Protocol) avec SLAAC. Les interfaces déléguées fournissent également d'autres paramètres à l'aide de NDP. Configurez la délégation de préfixe si des hôtes connectés au pare-feu nécessitent un adressage IPv6 dynamique. La délégation de préfixe simplifie le provisionnement du réseau sur les réseaux LAN orientés client.

Pour configurer une interface de pare-feu qui fait face aux hôtes sur le réseau, vous configurez le type d'interface à **hériter**. Seules les interfaces héritées peuvent annoncer ces préfixes sélectionnés du pool de préfixes aux hôtes (via une RA). Chaque hôte construit sa propre adresse IPv6 en utilisant le préfixe délégué et son adresse MAC ou EUI-64 (Extended Unique Identifier), à la discrétion de l'hôte. Seul le préfixe est délégué (hérité), pas l'adresse complète.

DHCPv6 fonctionne différemment de DHCPv4 en ce sens que le pare-feu ne reçoit pas d'adresses IPv6 complètes à attribuer aux hôtes. Le pare-feu ne connaît pas les adresses IPv6 complètes des hôtes.

L'exemple de topologie suivant comporte un pare-feu, un serveur DHCPv6 au nord du pare-feu et des hôtes sur deux réseaux locaux au sud du pare-feu.

 ©2024 Palo Alto Networks, Inc.



L'interface de pare-feu qui fait face au routeur délégant est un client SLAAC (Stateless Address Autoconfiguration). L'interface de pare-feu qui fait face à l'hôte est un serveur SLAAC ; l'hôte est un client SLAAC. Le client DHCPv6 alloue un préfixe /64 du pool de préfixes à l'interface héritée. Le pare-feu configure une adresse IPv6 sur une interface héritée à l'aide de SLAAC et envoie des RA avec le préfixe pour configurer automatiquement les interfaces hôtes à l'aide de SLAAC.

RFC 8415 définit une association d'identité (IA) comme un ensemble de baux attribués à un client. Le serveur DHCPv6 fournit :

- IA_NA (Identity Association for **N**on-temporary **A**ddresses) et IA_TA (Identity Association for **T**emporary **A**ddresses) que le pare-feu doit attribuer aux interfaces qui font face au routeur délégant et au FAI.
- IA_PD (Identity Association pour les préfixes délégués) pour le pare-feu à attribuer à un pool de préfixes ; les interfaces de pare-feu qui font face aux hôtes héritent du préfixe. Le pare-feu sélectionne un préfixe dans le pool et le distribue aux hôtes via RA. Les hôtes reçoivent le préfixe et construisent leur propre adresse IPv6.

Lorsque vous configure the firewall interface (configurez l'interface de pare-feu) qui fait face au FAI, vous configurez le type d'interface sur **DHCPv6 Client**. Le pare-feu demande une adresse non temporaire ou une adresse temporaire (ou les deux) pour son interface. Le pare-feu prend en charge un seul serveur DHCPv6 par interface. Vous pouvez avoir plusieurs interfaces, chacune faisant face à un FAI différent, de sorte que si une connexion à un FAI tombe en panne, vous avez accès à un autre FAI.

Vous configurez la délégation de préfixe sur l'interface qui fait face au FAI car c'est l'interface qui fait face au serveur DHCPv6, qui fournit le préfixe. Si vous avez plusieurs interfaces faisant face à un FAI, utilisez la Préférence pour contrôler quel FAI fournit le préfixe délégué aux hôtes.

 ©2024 Palo Alto Networks, Inc.

Si le pare-feu est le consommateur final du trafic IPv6 et n'a pas de LAN connecté, le pare-feu peut simplement être un client DHCPv6 et aucune délégation de préfixe n'est nécessaire.

Si vous avez activé le routage avancé, l'interface de couche 3 que vous configurez est affectée à un routeur logique.

À partir de PAN-OS 11.1.4 et des versions ultérieures, le pare-feu prend en charge les adresses IPv4 et IPv6 doubles (chevauchement) sur les interfaces de couche 3 qui utilisent des routeurs logiques différents. Découvrez cette fonctionnalité avant d'activer la prise en charge des adresses IP doubles et de configurer les adresses IP qui se chevauchent.

 ©2024 Palo Alto Networks, Inc.

Messages DHCP

DHCP utilise huit types de messages standard, identifiés par un nombre de types d'options dans les messages DHCP. Par exemple, lorsqu'un client souhaite rechercher un serveur DHCP, il diffuse un message DHCPDISCOVER sur son sous-réseau physique local. Si aucun serveur DHCP ne se trouve sur son sous-réseau et si DHCP Helper ou DHCP Relay n'est pas correctement configuré, le message est transféré aux serveurs DHCP sur un autre sous-réseau physique. Autrement, le message n'ira pas plus loin que le sous-réseau duquel il provient. Un ou plusieurs serveurs DHCP répondront par un message DHCPOFFER qui contient une adresse réseau disponible et d'autres paramètres de configuration.

Lorsque le client a besoin d'une adresse IP, il envoie un message DHCPREQUEST à un ou plusieurs serveurs. Bien entendu, si le client demande une adresse IP, c'est qu'il n'en a pas encore une ; par conséquent, le document RFC 2131 exige que le message de diffusion envoyé par le client ait une adresse de 0 dans son en-tête IP.

Lorsqu'un client demande des paramètres de configuration à un serveur, il peut recevoir des réponses de plusieurs serveurs. Une fois qu'un client a reçu son adresse IP, il dispose au moins d'une adresse IP et éventuellement d'autres paramètres de configuration *liés*. Les serveurs DHCP gèrent la liaison des paramètres de configuration aux clients.

Le tableau suivant répertorie les messages DHCP.

Message DHCP	Description
DHCPDISCOVER	Message du client recherchant les serveurs DHCP disponibles.
DHCPOFFER	Réponse du serveur au message DHCPDISCOVER du client, fournissant les paramètres de configuration.
DHCPREQUEST	Message du client demandant à un ou plusieurs serveurs d'effectuer l'une des tâches suivantes : • Obtenir les paramètres de configuration (demande à un seul serveur et refus implicite des offres d'autres serveurs). • Confirmer qu'une adresse IP précédemment affectée est correcte, après, par exemple, un redémarrage du système. • Prolonger la durée du bail d'une adresse réseau.
DHCPACK	Message d'accusé de réception du serveur au client contenant les paramètres de configuration, y compris une adresse réseau confirmée.
DHCPNAK	Accusé de réception négatif du serveur au client indiquant que la compréhension de l'adresse réseau par le client est incorrecte (par exemple, si le client a déplacé un nouveau sous-réseau) ou si le bail d'un client a expiré.

 ©2024 Palo Alto Networks, Inc.

Message DHCP	Description
DHCPDECLINE	Message du client au serveur indiquant que l'adresse réseau est déjà utilisée.
DHCPRELEASE	Message du client au serveur libérant l'utilisateur de l'adresse réseau et annulant la durée restante du bail.
DHCPINFORM	Message du client au serveur demandant des paramètres de configuration locaux uniquement ; le client dispose d'une adresse réseau configurée en externe.

©2024 Palo Alto Networks, Inc.

Adressage DHCP

- Méthodes d'allocation d'adresse DHCP
- Baux DHCP

Méthodes d'allocation d'adresse DHCP

Un serveur DHCP affecte ou envoie une adresse IP à un client de trois manières différentes :

- **Automatic allocation (Allocation dynamique)** : le serveur DHCP affecte une adresse IP permanente de ses **IP Pools (pools d'adresses IP)** à un client. Sur le pare-feu, un **Lease (Bail)** spécifié comme **Unlimited (Illimité)** signifie que l'allocation est permanente.
- **Dynamic allocation (Allocation dynamique)** : le serveur DHCP affecte une adresse IP réutilisable de ses **IP Pools (pools d'adresses IP)** à un client, pour une durée maximale, appelée *bail*. Cette méthode d'allocation d'adresse est utile lorsque le client dispose d'un nombre limité d'adresses IP ; celles-ci peuvent être affectées aux clients qui ont besoin d'un accès temporaire au réseau. Reportez-vous à la section Baux DHCP.
- **Static allocation (Allocation statique)** : l'administrateur réseau choisit l'adresse IP à affecter au client et le serveur DHCP l'envoie au client. Une allocation DHCP statique est permanente ; elle est effectuée en configurant un serveur DHCP et en choisissant une **Reserved Address (Adresse réservée)** correspondant au paramètre **MAC Address (Adresse MAC)** du périphérique client. L'allocation DHCP demeure même si le client se déconnecte, redémarre ou subit une coupure de courant.

  L'allocation statique d'une adresse IP est utile, par exemple, si vous disposez d'une imprimante sur un réseau local et que vous ne souhaitez pas que cette adresse IP change, car elle est associée à un nom d'imprimante via DNS. Un autre exemple est si un équipement client est utilisé pour des tâches essentielles et doit conserver la même adresse IP, même si le périphérique est désactivé, déconnecté, redémarré ou subi une coupure de courant.

  Souvenez-vous des points suivants lors de la configuration d'une **Reserved Address (Adresse réservée)** :

  - Il s'agit d'une adresse des **IP Pools (Pools d'adresses IP)**. Vous pouvez configurer plusieurs adresses IP réservées.
  - Si vous ne configurez aucune **Reserved Address (Adresse réservée)**, les clients du serveur recevront de nouvelles allocations DHCP du pool lorsque leur bail expirera ou quand ils redémarreront, etc. (à moins que vous n'indiquiez un **Lease (Bail) Unlimited (Illimité)**).
  - Si vous affectez toutes les adresses des **IP Pools (Pools d'adresses IP)** en tant que **Reserved Address (Adresse réservée)**, il ne reste aucune adresse dynamique à affecter au prochain client DHCP demandant une adresse.
  - Vous pouvez configurer une **Reserved Address (Adresse réservée)** sans configurer de **MAC Address (Adresse MAC)**. Dans ce cas, le serveur DHCP n'affecte la **Reserved Address (Adresse réservée)** à aucun périphérique. Vous pouvez réserver plusieurs adresses du pool et les affecter de manière statique à une imprimante et un fax, par exemple, sans utiliser DHCP.

 ©2024 Palo Alto Networks, Inc.

Baux DHCP

Un bail est la durée pendant laquelle un serveur DHCP affecte une adresse réseau à un client. Le bail peut être prolongé (renouvelé) sur demande. Si le client n'a plus besoin de l'adresse, il peut la libérer sur le serveur avant la fin du bail. Le serveur peut ensuite affecter cette adresse à un autre client s'il vient à manquer d'adresses non affectées.

La durée du bail configurée pour un serveur DHCP s'applique à toutes les adresses qu'un(e) serveur (interface) DHCP affecte de manière dynamique à ses clients. Autrement dit, toutes les adresses de cette interface affectées de manière dynamique ont une durée **Unlimited (Illimitée)** ou ont la même valeur de **Timeout (Délai d'expiration)**. Un autre serveur DHCP configuré sur le pare-feu peut avoir une durée de bail différente pour ses clients. Une **Reserved Address (Adresse réservée)** est une allocation d'adresse statique qui n'est pas sujette à la durée d'un bail.

Conformément à la norme DHCP (RFC 2131), un client DHCP n'attend pas l'expiration du bail car une nouvelle adresse risque de lui être affectée. À la place, lorsqu'un client est à mi-chemin de la durée de son bail, il tente de le prolonger de manière à conserver la même adresse IP. Ainsi, la durée du bail est comme une fenêtre dynamique.

Généralement, si une adresse IP est affectée à un équipement, ce dernier est par la suite retiré du réseau et son bail n'est pas prolongé ; le serveur DHCP laissera le bail expirer. Comme le client se trouve hors du réseau et qu'il n'a plus besoin de l'adresse, la durée du bail sur le serveur est atteinte et l'état du bail est « expiré ».

Le pare-feu dispose d'un minuteur de suspension qui empêche l'adresse IP expirée d'être immédiatement réaffectée. Ce comportement réserve temporairement l'adresse pour le périphérique au cas où il reviendrait sur le réseau. Mais si le pool d'adresses vient à manquer d'adresses, le serveur réaffecte cette adresse expirée avant l'expiration du minuteur de suspension. Les adresses expirées sont automatiquement effacées lorsque le système a besoin d'autres adresses ou lorsque le minuteur de suspension les libère.

Dans la CLI, utilisez la commande **`show dhcp server lease`** pour afficher les informations de bail des adresses IP affectées. Si vous ne souhaitez pas attendre la libération automatique des baux expirés, vous pouvez utiliser la commande **`clear dhcp lease interface <interface> expired-only`** pour effacer les baux expirés, rendant ainsi ces adresses à nouveau disponibles dans le pool. Vous pouvez utiliser la commande **`clear dhcp lease interface<interface> ip <ip_address>`** pour libérer une adresse IP particulière. Utilisez la commande **`clear dhcp lease interface <interface> mac <mac_address>`** pour libérer une adresse MAC particulière.

 ©2024 Palo Alto Networks, Inc.

Options DHCP

L'histoire de DHCP et des options DHCP remonte au protocole Bootstrap (BOOTP). BOOTP était utilisé par un hôte pour se configurer lui-même de manière dynamique lors de sa procédure de démarrage. Un hôte pouvait recevoir une adresse IP et un fichier contenant un lien de téléchargement vers un programme de démarrage sur un serveur, ainsi que l'adresse du serveur et l'adresse d'une passerelle Internet.

Un champ d'informations sur le fournisseur était inclus dans le paquet BOOTP ; celui-ci pouvait contenir un nombre de champs identifiés contenant divers types d'informations, notamment le masque de sous-réseau, la taille du fichier BOOTP et de nombreuses autres valeurs. Le document RFC 1497 décrit les Extensions fournisseur BOOTP. DHCP remplace BOOTP ; BOOTP n'est pas pris en charge sur le pare-feu.

Ces extensions ont finalement été étendues avec l'utilisation de DHCP et des paramètres de configuration d'hôte DHCP, également appelés options. Similaire aux extensions fournisseur, les options DHCP sont des éléments de données identifiés qui fournissent des informations à un client DHCP. Ces options sont envoyées dans un champ de longueur variable à la fin d'un message DHCP. Par exemple, le type de message DHCP est l'option 53 et une valeur de 1 indique le message DHCPDISCOVER. Les options DHCP sont définies dans RFC 2132, DHCP Options and BOOTP Vendor Extensions (Options DHCP et extensions fournisseur BOOTP).

Un client DHCP peut négocier avec le serveur, en lui indiquant d'envoyer uniquement les options demandées.

- Options DHCP prédéfinies
- Plusieurs valeurs pour une option DHCP
- Options DHCP 43, 55 et 60 et autres options personnalisées

Options DHCP prédéfinies

Les pare-feu Palo Alto Networks® prennent en charge les options DHCP prédéfinies et personnalisées dans l'implémentation d'un serveur DHCP. Ces options sont configurées sur le serveur DHCP et envoyées aux clients qui ont envoyé un message DHCPREQUEST au serveur. On dit que les clients *héritent* et implémentent les options qu'ils ont été programmés pour accepter.

Le pare-feu prend en charge les options prédéfinies suivantes sur ses serveurs DHCP ; celles-ci sont affichées dans l'ordre dans lequel elles apparaissent sur l'écran de configuration du **DHCP Server (Serveur DHCP)** :

Option DHCP	Nom de l'option DHCP
51	Durée du bail
3	Passerelle
1	Sous-réseau du pool d'adresses IP (masque)

©2024 Palo Alto Networks, Inc.

Option DHCP	Nom de l'option DHCP
6	Adresse du serveur Domain Name System (DNS) (système de noms de domaine ; DNS) (principale et secondaire)
44	Adresse du serveur Windows Internet Name Service (service de nom Internet Windows ; WINS) (principale et secondaire)
41	Adresse du serveur Network Information Service (service d'informations réseau ; NIS) (principale et secondaire)
42	Adresse du serveur Network Time Protocol (protocole d'heure réseau ; NTP) (principale et secondaire)
70	Adresse du serveur Post Office Protocol Version 3 (protocole du bureau de poste version 3 ; POP3)
69	Adresse du serveur Simple Mail Transfer Protocol (protocole simple de transfert de courrier ; SMTP)
15	Suffixe DNS

Comme indiqué, vous pouvez également configurer des options personnalisées ou spécifiques au fournisseur, qui prennent en charge une grande variété de périphériques de bureau, tels que les téléphones IP et les périphériques sans fil. Chaque code d'option prend en charge plusieurs valeurs, qui peuvent être de type Adresse IP, ASCII ou Hexadécimal. Grâce à la prise en charge améliorée des options DHCP par le pare-feu, les filiales n'ont pas besoin d'acheter ni de gérer leurs propres serveurs DHCP afin de fournir des options personnalisées et spécifiques au fournisseur aux clients DHCP.

Plusieurs valeurs pour une option DHCP

Vous pouvez saisir plusieurs valeurs d'option pour un **Option Code** (Code d'option) ayant le même **Option Name** (Nom d'option), mais toutes les valeurs pour une combinaison code/nom particulière doivent être du même type (Adresse IP, ASCII ou Hexadécimal). Si un type est hérité ou saisi et qu'un autre type est saisi ultérieurement pour la même combinaison code/nom, le second type remplace le premier.

Vous pouvez saisir un **Option Code (Code d'option)** plusieurs fois en utilisant un autre **Option Name (Nom d'option)**. Dans ce cas, le **Option Type (Type d'option)** du code d'option peut différer entre les noms d'option. Par exemple, si l'option Coastal Server (code d'option 6) est configurée avec le type Adresse IP, l'option Server XYZ (code d'option 6) avec le type ASCII est également autorisée.

Le pare-feu envoie plusieurs valeurs (enchaînées) pour une option à un client dans l'ordre, de haut en bas. Par conséquent, lorsque vous saisissez plusieurs valeurs pour une option, saisissez-les dans l'ordre de préférence, sinon, déplacez les options pour atteindre l'ordre de préférence de la liste. L'ordre des options dans la configuration du pare-feu détermine l'ordre dans lequel les options s'affichent dans les messages DHCPOFFER et DHCPACK.

 ©2024 Palo Alto Networks, Inc.

Vous pouvez saisir un code d'option qui existe déjà en tant que code d'option prédéfini ; le code d'option personnalisé remplace alors l'option DHCP prédéfinie et le pare-feu émet un avertissement.

Options DHCP 43, 55 et 60 et autres options personnalisées

Le tableau suivant décrit le comportement des différentes options définies dans le document RFC 2132.

Code d'optio	Nom de l'option	Description/Comportement de l'option
43	Informations spécifiques au fournisseur	Option envoyée du serveur au client. Informations spécifiques au fournisseur que le serveur DHCP fournira au client. Les informations sont envoyées au client uniquement si le serveur dispose d'un Vendor Class Identifier (identifiant de classe de fournisseur - VCI) dans sa table qui correspond au VCI du message DHCPREQUEST du client. Un paquet Option 43 contient plusieurs informations spécifiques au fournisseur. Il peut également inclure des extensions de données spécifiques au fournisseur encapsulées.
55	Liste de demande de paramètres	Option envoyée du client au serveur. Liste des paramètres de configuration (codes d'option) demandée par un client DHCP, probablement dans l'ordre de préférence du client. Le serveur tente de répondre avec des options dans le même ordre.
60	Vendor Class Identifier (identifiant de classe de fournisseur - VCI)	Option envoyée du client au serveur. Type et configuration du fournisseur d'un client DHCP. Le client DHCP envoie le code d'option 60 dans un message DHCPREQUEST au serveur DHCP. Lorsque le serveur reçoit l'option 60, il voit que le VCI trouve le VCI correspondant dans sa propre table, puis renvoie l'option 43 avec la valeur (qui correspond au VCI), relayant ainsi les informations spécifiques au fournisseur au bon client. Le client et le serveur ont connaissance du VCI.

Vous pouvez envoyer des codes d'option personnalisés et spécifiques au fournisseur qui ne sont pas définis dans le document RFC 2132. Les codes d'option peuvent être compris dans une plage de 1 à 254 et de longueur fixe ou variable.

Les options DHCP personnalisées ne sont pas validées par le serveur DHCP ; vous devez vous assurer de saisir des valeurs correctes pour les options que vous créez.

Pour les types d'options DHCP ASCII et Hexadécimal, la valeur de l'option peut être de 255 octets maximum.

 ©2024 Palo Alto Networks, Inc.

Adresses IPv6 dynamiques sur l’interface de gestion

L'interface de gestion (MGT) sur le NGFW prend en charge l'affectation d'adresses IPv6 dynamiques. Configurer l’interface de gestion pour l’affectation d’adresses IPv6 dynamiques (plutôt qu’une adresse statique) facilite l’insertion et la gestion du pare-feu dans un réseau IPv6.

Vous avez le choix entre deux types d'adressage : avec état ou sans état. Sur le segment de réseau, vous contrôlez le routeur où vous définissez des indicateurs pour indiquer que l'interface MGT sera l'un des éléments suivants :

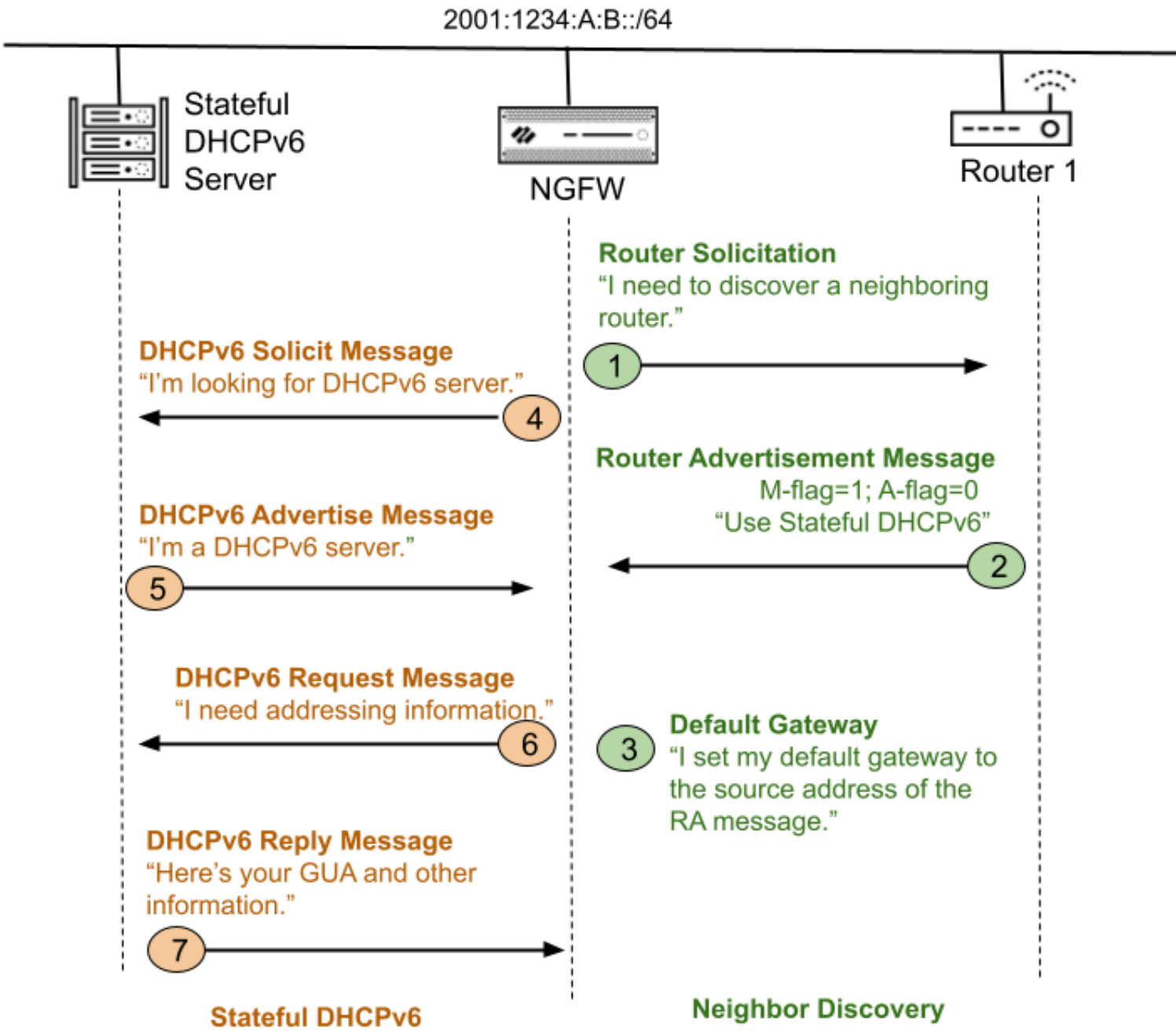
- Un client DHCPv6 avec état, qui reçoit son adresse IPv6, sa longueur de préfixe et toute autre configuration d'un serveur DHCPv6.
- Un client de configuration automatique d'adresse sans état IPv6 (SLAAC), qui génère automatiquement son adresse IPv6. Une adresse IPv6 sans état évite à un serveur DHCPv6 d'avoir à stocker des informations d'état dynamiques sur les clients ; cela est utile dans les environnements possédant un grand nombre de terminaux.

Le pare-feu utilise le protocole NDP (Neighbor Discovery Protocol) pour envoyer une sollicitation de routeur à tous les routeurs sur la liaison. Les indicateurs dans la publicité de routeur (RA) que le routeur unique (ou routeur préféré) sur la liaison envoie au pare-feu contrôlent si le pare-feu utilisera SLAAC ou DHCPv6 avec état pour obtenir une adresse dynamique pour l'interface MGT.

Cependant, la situation actuelle est que lorsque l’indicateur Autonomous (Autonome ; A) est défini dans le message de RA, le pare-feu choisit à la fois une adresse DHCPv6 et une adresse SLAC. Idéalement, le pare-feu devrait choisir uniquement l'adresse SLAAC et ne devrait pas envoyer de message de sollicitation DHCPv6. En raison de ce problème connu, s'il existe un serveur DHCPv6 sur le segment et qu'il peut affecter une adresse IPv6, le pare-feu préfère l'affectation d'adresse DHCPv6 à SLAAC.

L'exemple suivant illustre l'affectation d'adresses DHCPv6 avec état.

 ©2024 Palo Alto Networks, Inc.



Dans l'exemple de topologie, le pare-feu est connecté à un routeur faisant office de passerelle par défaut. Le pare-feu est un client IPv6 SLAAC/DHCPv6 connecté à un serveur DHCPv6. Après avoir activé IPv6 sur l'interface MGT, sélectionnez le type d'adresse dynamique et le type de passerelle dynamique par défaut, et validez. Le processus suivant se produit.

 ©2024 Palo Alto Networks, Inc.

1. L'affectation de passerelle par défaut se produit à l'aide d'une sollicitation de routeur (RS) et d'une publicité de routeur (RA) (côté droit du graphique).

   Les hôtes définissent leur passerelle par défaut en fonction de l'adresse source du routeur unique (ou préféré) attaché à la liaison. Le pare-feu utilise le protocole NDP (Neighbor Discovery Protocol) pour envoyer une RS à tous les routeurs sur la liaison. Si un seul routeur est attaché à la liaison, le pare-feu utilise l'adresse source des messages de RA ICMPv6 de ce routeur comme adresse de passerelle par défaut. Si le pare-feu reçoit des RA de plusieurs routeurs attachés à la liaison, le pare-feu utilise l'adresse source du message de RA qui a la préférence par défaut la plus élevée (faible, moyenne ou élevée) comme adresse de passerelle par défaut.

   En réponse à la RA, les indicateurs dans la RA que le routeur envoie au pare-feu indiquent si le pare-feu utilisera SLAAC ou DHCPv6 avec état pour obtenir une adresse dynamique pour l'interface de gestion, comme suit :

   - Un indicateur Autonomous (Autonome ; A) défini sur 1 indique au pare-feu de générer automatiquement une adresse de monodiffusion globale (GUA) en utilisant SLAAC. Le pare-feu utilise le préfixe des options de préfixe dans le message de RA ainsi que l'ID d'interface EUI-64 de l'interface MGT pour créer une GUA pour l'interface MGT. L'ID d'interface est créé à partir de l'adresse MAC de l'interface de gestion. (Si l'indicateur est défini sur 0, la configuration automatique n'est pas autorisée sur le segment.)
   - Un indicateur Other Configuration (Autre configuration ; O) défini sur 1 indique au pare-feu qu'il peut obtenir une liste de serveurs DNS et un nom de domaine à partir d'un serveur DHCPv6 sans état (mais pas d'informations d'adressage). Habituellement, l'indicateur O fonctionne avec la configuration automatique SLAAC et l'indicateur A et l'indicateur O ont tous deux la valeur 1.

     Actuellement, il y a un problème connu avec l'indicateur O (DHCPv6 sans état), qui n'est pas pris en charge dans cette version.
   - Un indicateur Managed (Géré ; M) défini sur 1 indique au pare-feu d'obtenir ses paramètres de réseau IPv6 (tels que son adresse globale, DNS et un nom de domaine) à partir d'un serveur DHCPv6 avec état. Le pare-feu contacte un serveur DHCPv6 pour demander une GUA et les autres informations. Généralement, cela signifie que l'adressage automatique SLAAC n'est pas autorisé sur le segment et que l'indicateur A et l'indicateur O ont tous deux la valeur 0.

     Actuellement, un problème connu est que le pare-feu envoie un message de sollicitation DHCPv6 même lorsque l'indicateur M n'est pas défini.

   Les étapes suivantes correspondent aux légendes dans le graphique.

   - Étape 1 : le pare-feu envoie un RS à l'adresse multicast bien connue pour tous les routeurs (FF02::2).
   - Étape 2 : en réponse, le routeur 1 génère une RA avec l'indicateur M défini sur 1 et l'indicateur A défini sur 0, indiquant au pare-feu que SLAAC n'est pas autorisé sur le segment et qu'il doit utiliser DHCPv6 avec état pour l'adressage et d'autres configurations.

 ©2024 Palo Alto Networks, Inc.

- Étape 3 : à la réception de la RA, le pare-feu définit l'adresse IPv6 source du routeur 1 comme passerelle par défaut. Comme l'indicateur A est défini sur 0, le pare-feu n'effectue pas de SLAAC.

2. L'affectation d'adresses dynamiques se produit en utilisant DHCPv6 (côté gauche du graphique).
   - Étape 4 : en fonction de l'indicateur M défini sur 1 dans la RA, le pare-feu envoie un message de sollicitation DHCPv6 à l'adresse multicast bien connue pour tous les agents DHCPv6 (FF01::1:2), recherchant un serveur DHCPv6.
   - Étape 5 : dès la réception du message de sollicitation, le serveur monodiffuse un message de publicité DHCPv6 à l'adresse locale du lien du pare-feu.
   - Étape 6 : le pare-feu sait que le service DHCPv6 est disponible et envoie une demande d'informations d'adressage.
   - Étape 7 : dès la réception de la demande, le serveur envoie une réponse DHCPv6 contenant la GUA et toutes les autres informations disponibles à affecter. (Les informations DNS proviennent du serveur DHCPv4, pas du serveur DHCPv6.)
   - Le pare-feu effectue la détection d'adresses en double (DAD) sur la GUA qu'il reçoit pour confirmer que la GUA est unique. Si la DAD détermine que l'adresse IPv6 est un doublon (que ce soit un SLAAC, DHCPv6, ou même une adresse link-local), l'adresse IPv6 n'est pas vue dans l'interface.

Alternativement, vous pouvez configurer le routeur 1 pour qu'il utilise IPv6 SLAAC (non montré dans le graphique) pour l'affectation d'adresses dynamiques. Dans ce cas, le routeur 1 envoie une RA avec l'indicateur A défini sur 1, indiquant que le pare-feu doit créer sa GUA en utilisant SLAAC. Vous pouvez configurer les options de préfixe dans le message de RA avec l'indicateur A. Le pare-feu utilise le préfixe provenant des options de préfixe de la RA (qui est 2001:1234:A:B::/64 dans la topologie d'exemple) en plus de l'ID d'interface EUI-64 pour créer une ou plusieurs GUA. L'ID d'interface peut être créé en fonction de l'adresse MAC de l'interface MGT (EUI-64).

La configuration de l'interface MGT en tant que client DHCPv6 implique de demander une adresse non temporaire ou temporaire, l'option de validation rapide, le type de type d'ID unique DHCPv6 et de spécifier une adresse de passerelle par défaut statique ou dynamique.

Procédez à la configuration de l'interface de gestion pour l'attribution d'adresses IPv6 dynamiques.

 ©2024 Palo Alto Networks, Inc.

Configuration d'une interface en tant que serveur DHCP

Les prérequis pour cette tâche sont les suivants :

- Configurez une interface Ethernet ou VLAN de Couche 3.
- Affectez l'interface à un routeur virtuel et à une zone.
- Déterminez un pool valide d'adresses IP de votre plan réseau que vous pouvez désigner pour être affecté aux clients par votre serveur DHCP.
- Collectez les options et valeurs DHCP et les Vendor Class Identifiers (identifiants de classe de fournisseur - VCI) que vous envisagez de configurer.

Les capacités sont les suivantes :

- Pour les modèles de pare-feu autre que les pare-feu PA-5200 Series et PA-7000 Series, voyez l'outil de sélection de produits.
- Sur les pare-feu PA-5220, vous pouvez configurer un maximum de 500 serveurs DHCP et un maximum de 2 048 agents de relais DHCP, moins le nombre de serveurs DHCP configurés. Par exemple, si vous configurez 500 serveurs DHCP, vous pouvez configurer 1 548 agents de relais DHCP.
- Sur les pare-feu PA-5250, 5260 et PA-7000, vous pouvez configurer un maximum de 500 serveurs DHCP et un maximum de 4 096 agents de relais DHCP, moins le nombre de serveurs DHCP configurés. Par exemple, si vous configurez 500 serveurs DHCP, vous pouvez configurer 3 596 agents de relais DHCP.

Procédez comme suit pour configurer une interface sur le pare-feu pour agir en tant que serveur DHCP.

STEP 1 | Sélectionnez une interface pour être un serveur DHCP.

1. Sélectionnez **Network (Réseau)** > **DHCP (DHCP)** > **DHCP Server (Serveur DHCP)** et **Add (Ajoutez)** un nom d'**Interface (Interface)** ou sélectionnez-en un.
2. Pour **Mode (Mode)**, sélectionnez **enabled (activé)** ou **auto (automatique)**. Le mode automatique active le serveur et le désactive si un autre serveur DHCP est détecté sur le réseau. Le paramètre **disabled (désactivé)** désactive le serveur.
3. (Facultatif) Sélectionnez **Ping IP when allocating new IP (Envoyer une requête ping à l'adresse IP lors de l'allocation d'une nouvelle adresse IP)**, si vous souhaitez que le serveur envoie un message ping avant d'affecter l'adresse IP à son client.

   Si la requête ping reçoit une réponse, cela signifie qu'un autre équipement dispose déjà de cette adresse ; celle-ci n'est donc pas disponible. Le serveur affecte alors l'adresse suivante du pool. Ce comportement est similaire à la fonction DAD (Optimistic Duplicate Address Detection) pour IPv6 (RFC 4429).

   Après avoir défini les options et être revenu dans l'onglet DHCP Server (Serveur DHCP), la colonne ***Probe IP (Sonder l'adresse IP)*** *de l'interface indique si l'option* ***Ping IP when allocating new IP (Envoyer une requête ping à l'adresse IP lors de l'allocation d'une nouvelle adresse IP)*** *a été sélectionnée.*

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configurez les options DHCP prédéfinies que le serveur envoie à ses clients.

- Dans la section Options, sélectionnez un type de **Lease (Bail)** :
- **Unlimited (Illimité)** : le pare-feu choisit de manière dynamique les adresses IP de ses **IP Pools (Pools d'adresses IP)** et les affecte définitivement aux clients.
- **Timeout (Délai d'expiration)** : cette option détermine la durée du bail. Saisissez le nombre de **Days (Jours)**, de**Hours (Heures)** et éventuellement de **Minutes (Minutes)**.
- **Inheritance Source (Source de l'héritage)** : laissez **None (Aucune)** ou sélectionnez une interface client PPPoE ou DHCP source pour propager les divers paramètres du serveur sur le serveur DHCP. Si vous indiquez la **Inheritance Source (Source de l'héritage)**, sélectionnez une ou plusieurs options **inherited (héritées)** de cette source ci-dessous.

L'indication de la source de l'héritage permet au pare-feu d'ajouter rapidement des options DHCP d'un serveur en amont reçues par le client DHCP, ainsi que de mettre à jour des options du client si la source modifie une option. Par exemple, si la source remplace son serveur NTP (qui a été identifié comme serveur **Primary NTP (NTP principal)**), le client héritera automatiquement de la nouvelle adresse en tant que son serveur **Primary NTP (NTP principal)**.

> *Lors de l'héritage d'options DHCP contenant plusieurs adresses IP, le pare-feu utilise uniquement la première adresse IP contenue dans l'option pour conserver la mémoire cache. Si vous avez besoin de plusieurs adresses IP pour une seule option, configurez les options DHCP directement sur ce pare-feu au lieu de configurer l'héritage.*

- **Check inheritance source status (Vérifier l'état de la source de l'héritage)** : si vous avez sélectionné une **Inheritance Source (Source de l'héritage)**, cliquez sur ce lien pour ouvrir la fenêtre **Dynamic IP Interface Status (État de l'interface IP dynamique)**, qui affiche les options héritées du client DHCP.
- **Gateway (Passerelle)** : adresse IP de la passerelle réseau (une interface sur le pare-feu) permettant d'accéder à chaque périphérique situé sur un autre réseau local que ce serveur DHCP.
- **Subnet Mask (Masque de sous-réseau)** : masque réseau utilisé avec les adresses figurant dans le champ **IP Pools (Pools d'adresses IP)**.

Dans les champs suivants, cliquez sur la flèche vers le bas et sélectionnez **None (Aucun)** ou **inherited (Hérité)**, ou saisissez l'adresse IP d'un serveur distant que votre serveur DHCP enverra aux clients pour accéder à ce service. Si vous sélectionnez **inherited (hérité)**, le

 ©2024 Palo Alto Networks, Inc.

serveur DHCP hérite des valeurs du client DHCP source indiqué comme **Inheritance Source (Source de l'héritage)**.

- **Primary DNS (DNS principal)**, **Secondary DNS (DNS secondaire)** : adresse IP des serveurs Domain Name System (système de noms de domaine ; DNS) préféré et alternatif.
- **Primary WINS (WINS principal)**, **Secondary WINS (WINS secondaire)** : adresse IP des serveurs Windows Internet Name Service (Service d'attribution de nom Internet Windows ; WINS) préférés et alternatifs.
- **Primary NIS (NIS principal)**, **Secondary NIS (NIS secondaire)** : adresse IP des serveurs Network Information Service (service d'informations réseau ; NIS) préférés et alternatifs.
- **Primary NTP(NTP principal)**, **Secondary NTP (NTP secondaire)** : adresse IP des serveurs Network Time Protocol (protocole de synchronisation réseau ; NTP) préférés et alternatifs.
- **POP3 Server (Serveur POP3)** : adresse IP du serveur Post Office Protocol (protocole de bureau de poste ; POP3).
- **SMTP Server (Serveur SMTP)** : adresse IP du serveur Simple Mail Transfer Protocol (protocole simple de transfert de courrier ; SMTP).
- **DNS Suffix (Suffixe DNS)** : suffixe que le client pourra utiliser localement lors de la saisie d'un nom d'hôte non qualifié irrésoluble.

STEP 3 | (Facultatif) Configurez une option DHCP spécifique au fournisseur ou personnalisée que le serveur DHCP envoie à ses clients.

1. Dans la section Custom DHCP Options (Options DHCP personnalisées), **Add (Ajoutez)** un **Name (Nom)** descriptif pour identifier l'option DHCP.
2. Saisissez le paramètre **Option Code (Code option)** que le serveur fournira (plage entre 1 et 254). (Pour les codes d'option, reportez-vous au document RFC 2132)
3. Si le paramètre **Option Code (Code d'option)** est **43** (43), le champ **Vendor Class Identifier (Identifiant de classe de fournisseur)** s'affiche. Saisissez un VCI, qui est une chaîne ou une valeur hexadécimale (avec un préfixe 0x) utilisée comme correspondance à une valeur qui provient de la demande du client contenant l'option 60. Le serveur recherche le VCI entrant dans sa table, le trouve et renvoie l'option 43, ainsi que la valeur d'option correspondante.
4. **Inherit from DHCP server inheritance source (Hériter de la source de l'héritage du serveur DHCP)** : sélectionnez cette option uniquement si vous avez indiqué une **Inheritance Source (Source de l'héritage)** pour les options prédéfinies du serveur DHCP et que vous souhaitez que les options personnalisées et spécifiques au fournisseur soient également **inherited (Héritées)** de cette source.
5. **Check inheritance source status (Vérifier l'état de la source de l'héritage)** : si vous avez sélectionné une **Inheritance Source (Source de l'héritage)**, cliquez sur ce lien pour ouvrir la fenêtre **Dynamic IP Interface Status (État de l'interface IP dynamique)**, qui affiche les options héritées du client DHCP.
6. Si vous n'avez pas sélectionnez **Inherit from DHCP server inheritance source (Hériter de la source de l'héritage du serveur DHCP)**, sélectionnez un **Option Type (Type d'option)** : **IP Address (Adresse IP)**, **ASCII (ASCII)** ou **Hexadecimal (Hexadécimal)**. Les valeurs hexadécimales doivent commencer par le préfixe 0x.

 ©2024 Palo Alto Networks, Inc.

7. Saisissez le paramètre **Option Value (Valeur de l'option)** que le serveur DHCP fournira pour ce **Option Code (Code d'option)**. Vous pouvez saisir plusieurs valeurs sur des lignes distinctes.
8. Cliquez sur **OK**.

STEP 4 | (Facultatif) Ajoutez une autre option DHCP spécifique au fournisseur ou personnalisée.

1. Répétez l'étape précédente pour saisir une autre option DHCP personnalisée.
   - Vous pouvez saisir plusieurs valeurs d'option pour un **Option Code (Code d'option)** ayant le même **Option Name (Nom d'option)**, mais toutes les valeurs pour un **Option Code (Code d'option)** doivent être du même type (**IP Address (Adresse IP)**, **ASCII (ASCII)** ou **Hexadecimal (Hexadécimal)**). Si un type est hérité ou saisi et qu'un autre type est saisi pour le même **Option Code (Code d'option)** et le même **Option Name (Nom d'option)**, le second type remplace le premier.

     Lorsque vous saisissez plusieurs valeurs pour une option, saisissez-les dans l'ordre de préférence, sinon, déplacez les options DHCP personnalisées pour atteindre l'ordre de préférence de la liste. Sélectionnez une option et cliquez sur **Move Up (Monter)** ou **Move Down (Descendre)**.
   - Vous pouvez saisir un **Option Code (Code d'option)** plusieurs fois en utilisant un autre **Option Name (Nom d'option)**. Dans ce cas, le **Option Type (Type d'option)** du code d'option peut différer entre les noms d'option.
2. Cliquez sur **OK**.

STEP 5 | Identifiez le pool d'adresses IP dynamiques dans lequel le serveur DHCP choisit une adresse et l'affecte à un client DHCP.

Si vous n'êtes pas l'administrateur réseau de votre réseau, demandez à l'administrateur réseau un pool d'adresses IP valide du plan réseau qui peut être désigné pour être affecté par votre serveur DHCP.

1. Dans le champ **IP Pools (Pools d'adresses IP)**, **Add (Ajoutez)** la plage d'adresses IP à partir de laquelle ce serveur affecte une adresse à un client. Saisissez un sous-réseau IP et un masque de sous-réseau (par exemple : 192.168.1.0/24) ou une plage d'adresses IP (par exemple : 192.168.1.10 - 192.168.1.20).
   - Pour l'attribution d'adresses IP dynamiques, vous devez absolument préciser un pool d'adresses IP ou une **Reserved Address (Adresse réservée)**.
   - Il n'est pas nécessaire de préciser un pool d'adresses pour l'attribution d'adresses IP statiques, tant que les adresses IP statiques que vous attribuez font partie du sous-réseau que l'interface du pare-feu prend en charge.
2. (Facultatif) Répétez cette étape pour indiquer un autre pool d'adresses IP.

STEP 6 | (Facultatif) Indiquez une adresse IP des pools d'adresses IP qui ne sera pas affectée de manière dynamique. Si vous indiquez également une **MAC Address (Adresse MAC)**, la

 ©2024 Palo Alto Networks, Inc.

Reserved Address (Adresse réservée) est affectée à ce périphérique lorsqu'il demande une adresse IP via DHCP.

*Pour plus d'informations sur l'allocation d'une **Reserved Address (Adresse réservée)**, reportez-vous à la section* Adressage DHCP.

1. Dans le champ **Reserved Address (Adresse réservée)**, cliquez sur **Add (Ajouter)**.
2. Saisissez une adresse IP des **IP Pools (pools d'adresses IP)** (format *x.x.x.x*) que vous ne souhaitez pas voir affectée de manière dynamique par le serveur DHCP.
3. (Facultatif) Indiquez éventuellement le paramètre **MAC Address (Adresse MAC)** (au format *xx:xx:xx:xx:xx:xx*) du périphérique auquel vous souhaitez affecter de manière permanente l'adresse IP que vous venez de spécifier.
4. (Facultatif) Répétez les deux étapes précédentes pour réserver une autre adresse.

STEP 7 | Validez vos modifications.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

Configurer une interface en tant que client DHCPv4

Avant de configurer une interface de pare-feu en tant que client DHCP, assurez-vous d'avoir configuré une interface de couche 3 (Ethernet, sous-interface Ethernet, VLAN, sous-interface VLAN, agrégée ou sous-interface agrégée) et de l'avoir affectée à un routeur virtuel et à une zone. Configurez une interface en tant que client DHCP si vous devez utiliser DHCP pour demander une adresse IPv4 pour l'interface.

Vous pouvez également effectuer la Configuration de l'interface de gestion en tant que client DHCP.

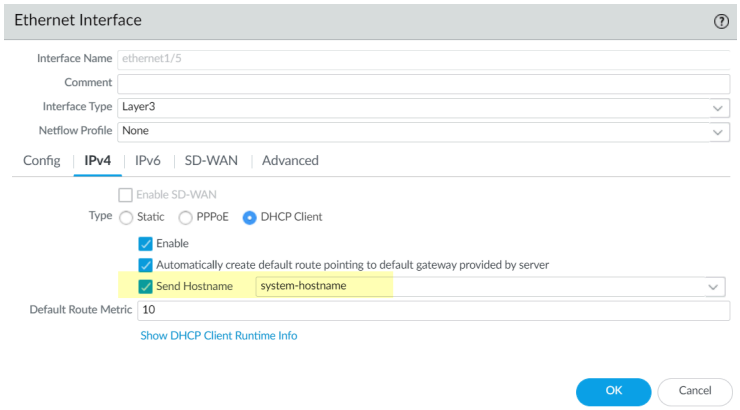
Si l'interface du pare-feu a besoin d'une adresse IPv6 dynamique, configurez une interface en tant que client *DHCPv6 (avec ou sans délégation de préfixe)*.

STEP 1 | Configurez une interface en tant que client DHCP.

1. Sélectionnez **Network (Réseau)** > **Interfaces**.
2. Dans l'onglet **Ethernet** ou **VLAN**, **Add (Ajoutez)** une interface de couche 3 ou sélectionnez une interface de couche 3 configurée que vous souhaitez configurer en tant que client DHCPv4.
3. Sélectionnez l'onglet **IPv4** et, sous **Type**, sélectionnez **DHCP Client (Client DHCP)**.
4. Sélectionnez **Enable (Activer)**.
5. (Facultatif) Activez l'option vous permettant de **Automatically create default route pointing to default gateway provided by server (Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur** activée par défaut). L'activation de cette option entraîne alors la création par le pare-feu d'un itinéraire statique vers la passerelle par défaut, qui est utile lorsque les clients tentent d'accéder à de nombreuses destinations qui n'ont pas besoin de conserver des itinéraires dans une table de routage sur le pare-feu.
6. (Facultatif) Activez l'option vous permettant de **Send Hostname (Envoyer le nom d'hôte)** pour affecter un nom d'hôte à l'interface du client DHCP et envoyer ce nom d'hôte (Option 12) à un serveur DHCP. qui peut ensuite enregistrer le nom d'hôte auprès du serveur DNS. Le serveur DNS peut ensuite gérer automatiquement les résolutions de nom d'hôte/adresse IP dynamique. Les hôtes externes peuvent identifier l'interface par son nom d'hôte. La valeur par défaut indique **system-hostname (nom de l'hôte système)**, qui correspond au nom d'hôte du pare-feu que vous avez configuré sous **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **General Settings (Paramètres généraux)**. Vous pouvez également saisir un nom d'hôte pour l'interface,

 ©2024 Palo Alto Networks, Inc.

d'un maximum de 64 caractères, y compris des lettres majuscules et minuscules, des chiffres, des points (.), des tirets (-) et des traits de soulignement (_).



7. (Facultatif) Saisissez une **Default Route Metric (Mesure d'itinéraire par défaut)** (niveau de priorité) pour l'itinéraire entre le pare-feu et le serveur DHCP (plage entre 1 et 65 535 ; valeur par défaut : 10). Plus la valeur de l'itinéraire est faible, plus sa priorité de sélection est élevée. Par exemple, un itinéraire avec une valeur de mesure de 10 est utilisé avant un itinéraire avec une valeur de mesure de 100.

   *La **Default Route Metric (Mesure d'itinéraire par défaut)** pour l'itinéraire entre le pare-feu et le serveur DHCP est de 10 par défaut. Si l'itinéraire statique par défaut 0.0.0.0/0 utilise l'interface DHCP comme interface de sortie, la **Metric (Mesure)** par défaut de cet itinéraire est alors de 10. Il existe alors deux itinéraires d'une mesure de 10, et le pare-feu peut aléatoirement choisir l'un des itinéraires une fois et l'autre itinéraire une autre fois.*

   *Si vous activez l'option **Automatically create default route pointing to default gateway provided by server (Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur)**, sélectionnez un routeur virtuel, ajoutez un itinéraire statique pour une interface de couche 3, modifiez la **Metric (Mesure)** (établie par défaut à 10) en indiquant une valeur supérieure à 10 (dans cet exemple, 100) et validez les modifications que vous avez apportées. La mesure de l'itinéraire indiquée dans la table d'itinéraires ne sera pas 100. La valeur par défaut de 10 sera plutôt indiquée, comme prévu, car cette valeur (10) l'emporte sur la valeur configurée (100). Cependant, si vous modifiez la **Metric (Mesure)** de l'itinéraire statique par une valeur inférieure à 10 (par exemple, 6), la table d'itinéraires est mise à jour et indique la mesure configurée (6).*

8. (Facultatif) Activez l'option **Show DHCP Client Runtime Info (Afficher les informations d'exécution du client DHCP)** pour voir tous les paramètres que le client a hérités de son serveur DHCP.

STEP 2 | Validez vos modifications.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

L'interface Ethernet devrait alors indiquer **Dynamic-DHCP Client (Client DHCP dynamique)** en tant que **IP Address (Adresse IP)** sous l'onglet **Ethernet**.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | (Facultatif) Affichez les interfaces sur le pare-feu qui sont configurées en tant que clients DHCP.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et vérifiez la **IP Address (Adresse IP)** pour voir les interfaces qui indiquent DHCP Client (Client DHCP).
2. Sélectionnez **Network (Réseau)** > **Interfaces** > **VLAN** et vérifiez la **IP Address (Adresse IP)** pour voir les interfaces qui indiquent DHCP Client (Client DHCP).

 ©2024 Palo Alto Networks, Inc.

Configurer une interface en tant que client DHCPv6 avec délégation de préfixes

Avant de configurer DHCPV6 Client, découvrez comment une interface Ethernet, VLAN ou AE de couche 3 sur le pare-feu peut fonctionner comme un client DHCPv6, avec ou sans délégation de préfixe.

La tâche suivante commence par montrer comment configurer l'interface face au serveur DHCPv6 pour être un client DHCPv6 et demander une adresse Non Temporary ou Temporary pour lui-même. Cette interface demande également un préfixe délégué au nom de l'interface faisant face à l'hôte. La tâche montre ensuite comment configurer une interface face aux hôtes en tant qu'interface **héritée** qui fournit une délégation de préfixe aux hôtes LAN.

STEP 1 | Sélectionnez une interface Ethernet, AE ou VLAN (qui fait face au serveur DHCPv6 et au FAI) pour être un client DHCPv6.

1. SélectionnezNetwork (Réseau) > **Interfaces** > **Ethernet** ou sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et sélectionnez une interface AE ou sélectionnezNetwork (Réseau) > **Interfaces** > **VLAN**.
2. Sous **Interface Type (Type d'interface)**, sélectionnez **Layer3 (Couche 3)**.
3. (Optional (Facultatif)) **Add Subinterface (Ajouter une sous-interface)** si vous souhaitez qu'une seule interface Ethernet ou VLAN face au FAI soit séparée en sous-interfaces.
4. Dans l'onglet **Config (Configurer)**, affectez l'interface à un **Virtual Router (routeur virtuel)** et à une **Security zone (zone de sécurité)**.

STEP 2 | Sélectionnez **IPv6**.

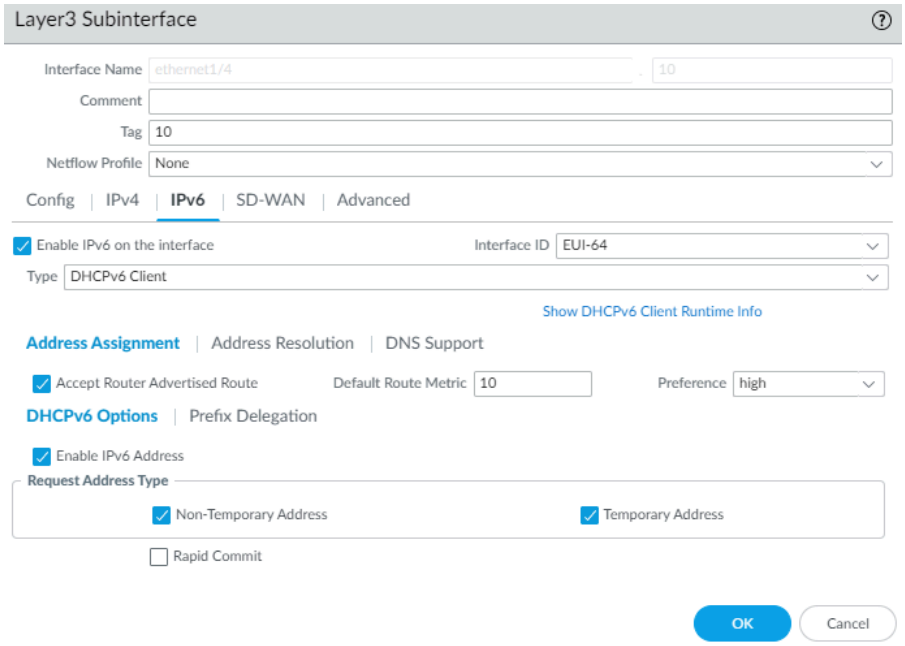
STEP 3 | **Enable IPv6 on the interface (Activer IPv6 sur l'interface)**

STEP 4 | Sous **Interface ID (ID de l'interface)**, saisissez **EUI-64 (identifiant unique étendu sur 64 bits par défaut)** au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Configurez l'interface qui fait face au FAI pour être un client DHCPv6 et demandez son adresse IPv6 temporaire louée et/ou son adresse IPv6 non temporaire.

1. Pour **Type**, sélectionnez **Client DHCPv6**.
2. Sélectionnez **Address Assignment (Attribution d'adresse)** et **Accept Router Advertised Route (Accepter l'itinéraire annoncé du routeur)** pour permettre au client DHCPv6 d'accepter l'annonce du routeur.



3. Entrez une **Default Route Metric (métrique de routage par défaut)** pour l'itinéraire de l'interface au FAI; la plage est de 1 à 65 535; la valeur par défaut est 10.
4. Sélectionnez **Préférence** de l'interface client DHCPv6 (**low (faible)**, **medium (moyenne)** ou **high (élevée)**) afin que, dans le cas où vous avez deux interfaces (chacune connectée à un FAI différent pour la redondance), vous puissiez attribuer à l'interface à un FAI une préférence plus élevée que l'interface à l'autre FAI. Le FAI connecté à l'interface préférée sera le FAI qui fournit le préfixe délégué à envoyer à une interface faisant face à l'hôte.

 ©2024 Palo Alto Networks, Inc.

Si les interfaces ont la même préférence, les deux FAI fournissent un préfixe délégué et l'hôte décide quel préfixe utiliser.

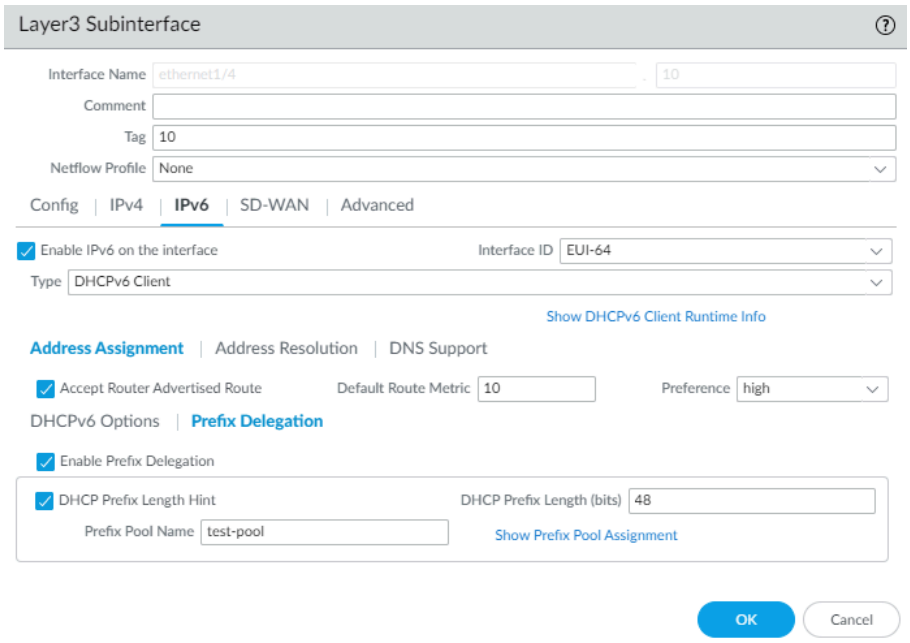
5. Sélectionnez **Options DHCPv6** et **Enable IPv6 Address (Activer l'adresse IPv6)**.
6. Dans la zone Type d'adresse de demande, sélectionnez **Non-Temporary Address (Adresse non temporaire)** (paramètre par défaut). Ce type d'adresse a une durée de vie plus longue.
7. Sélectionnez **Temporary Address (Adresse temporaire)** pour un plus grand niveau de sécurité car l'adresse est destinée à être utilisée pendant une courte période.

   Que vous demandiez une adresse non temporaire ou une adresse temporaire pour l'interface dépend de votre discrétion et de la capacité du serveur DHCPv6; certains serveurs ne peuvent fournir qu'une adresse temporaire. La meilleure pratique consiste à sélectionner à la fois Adresse non temporaire et Adresse temporaire, auquel cas le pare-feu préférera l'Adresse non temporaire.
8. Sélectionnez **Rapid Commit (Validation rapide)** pour utiliser le processus DHCPv6 des messages Solliciter et répondre (deux messages), plutôt que le processus des messages Solliciter, annoncer, demander et répondre (quatre messages).
9. Sélectionnez **Prefix Delegation (Délégation de préfixe)** et **Enable Prefix Delegation (Activer la délégation de préfixe)** pour permettre au pare-feu de prendre en charge la fonctionnalité de délégation de préfixe. Cela signifie que l'interface accepte un préfixe du serveur DHCPv6 amont et place le préfixe dans le pool de préfixes, à partir duquel le pare-feu délègue un préfixe à un hôte via RA. La possibilité d'activer ou de désactiver la délégation de préfixe pour une interface permet au pare-feu de prendre en charge

 ©2024 Palo Alto Networks, Inc.

plusieurs FAI (un FAI par interface). L'activation de la délégation de préfixe sur cette interface contrôle quel FAI fournit le préfixe.

Le préfixe délégué est utilisé sur l'interface face à l'hôte, et son adresse IPv6 est construite avec l'adresse MAC et l'entrée EUI-64. Dans notre exemple, l'interface héritée reçoit le préfixe hérité affiché dans l'étape de visualisation des informations DHCPv6.



10. Sélectionnez **DHCP Prefix Length Hint (Indice de longueur de préfixe DHCP)** pour permettre au pare-feu d'envoyer une longueur de préfixe DHCPv6 préférée au serveur DHCPv6.
11. Entrez **DHCP Prefix Length (bits) (longueur de préfixe DHCP préférée)** dans la plage de 48 à 64, qui est envoyée comme indication au serveur DHCPv6. Le serveur DHCPv6 a la discrétion d'envoyer la longueur de préfixe qu'il choisit.

    Demander une longueur de préfixe de 48, par exemple, laisse 16 bits restants pour les sous-réseaux (64-48), ce qui indique que vous avez besoin de nombreuses subdivisions de ce préfixe pour déléguer. Par contre, demander une longueur de préfixe de 63 laisse 1 bit pour déléguer seulement deux sous-réseaux. Sur les 128 bits, il reste 64 bits de plus pour l'adresse hôte.

    L'interface peut recevoir un préfixe /48, mais déléguer un préfixe /64, par exemple, ce qui signifie que le pare-feu subdivise le préfixe qu'il délègue.
12. Entrez un **Prefix Pool Name (nom de pool de préfixes)** pour le pool où le pare-feu stocke le préfixe reçu. Le nom doit être unique et contenir au maximum 63 caractères alphanumériques, traits d'union, points et soulignements.

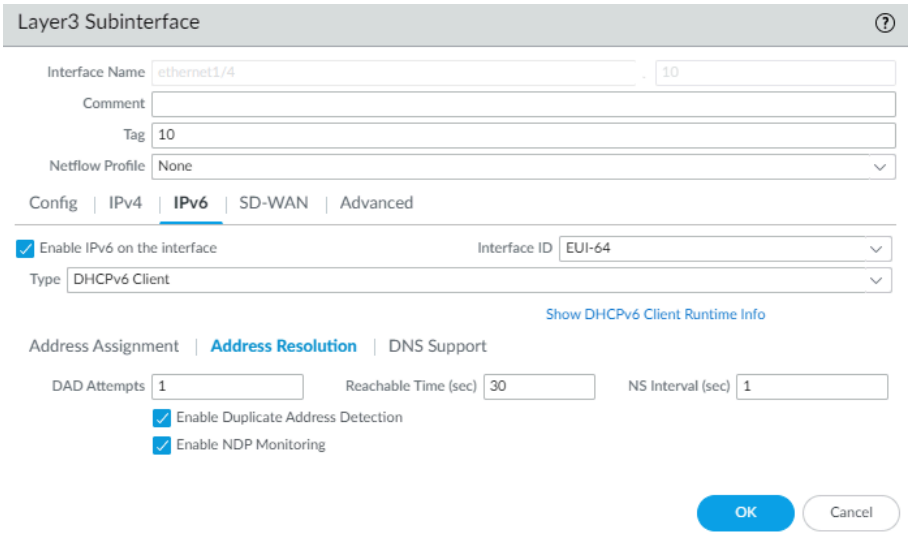
    Utilisez un nom de pool de préfixes qui reflète le FAI pour faciliter la reconnaissance.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Pour un client DHCPv6, configurez la résolution d'adresse.

1. Sélectionnez **Address Resolution (Résolution d'adresse)**.
2. **Enable Duplicate Address Detection (Activez la détection d'adresses en double)** (DAD) si vous souhaitez que l'unicité d'une adresse IPv6 potentielle soit vérifiée avant qu'elle ne soit attribuée à l'interface (activée par défaut).
3. Si vous avez sélectionné **Enable Duplicate Address Detection (Activer la détection d'adresses en double)**, spécifiez le nombre de **DAD Attempts (tentatives DAD)** dans l'intervalle de sollicitation des voisins (NS) avant que la tentative d'identification des voisins échoue; la plage est de 1 à 10; la valeur par défaut est 1.
4. Entrez le **Reachable Time (sec) (temps atteignable (sec)**, la durée en secondes pendant laquelle le client suppose qu'un voisin est joignable après avoir reçu un message de confirmation d'atteinte; la plage est de 10 à 36 000; la valeur par défaut est de 30.
5. Entrez **NS Interval (sec) (intervalle NS (sec))**, qui est la durée entre les sollicitations des voisins; la plage est de 1 à 3 600; la valeur par défaut est 1.

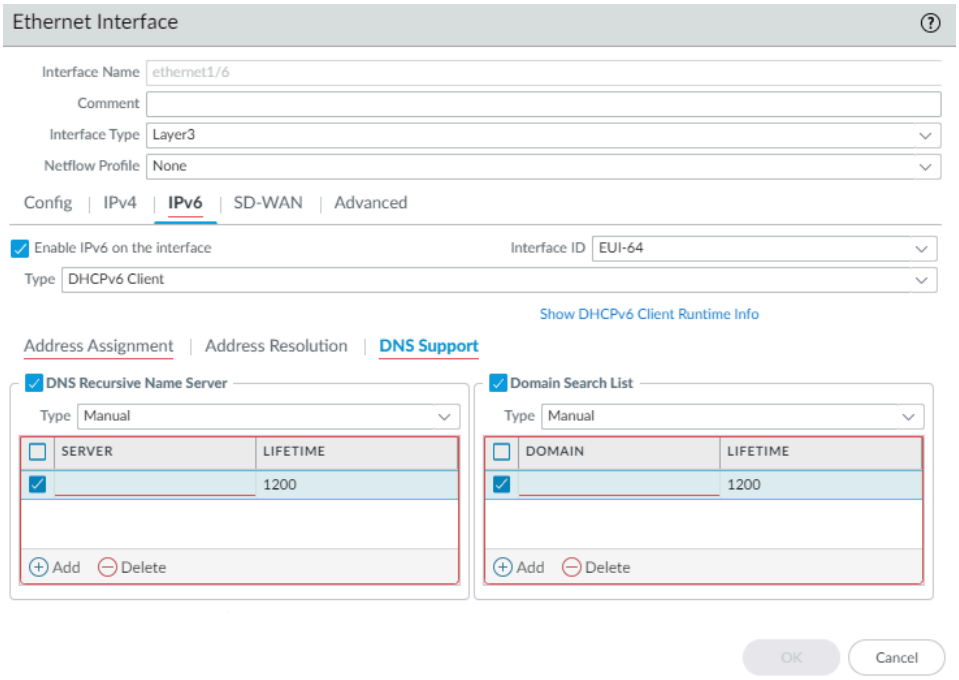
   Les sollicitations des voisins sont envoyées chaque seconde en utilisant un groupe multidiffusé bien connu. L'interface demande si un périphérique avec la même adresse IPv6 existe sur le réseau en envoyant NS, y compris sa propre adresse dans la requête. Si un autre appareil a la même adresse, il répond à ces demandes.
6. **Enable NDP Monitoring (Activez NDP Monitoring)** pour activer la surveillance du protocole de découverte des voisins. Lorsqu'il est activé, vous pouvez sélectionner l'icone NDP (dans la colonne Fonctions) et afficher des informations telles que l'adresse IPv6 d'un voisin découverte par le pare-feu, l'adresse MAC, User-ID correspondants et le statut (selon la situation la plus favorable).



 ©2024 Palo Alto Networks, Inc.

STEP 7 | Pour un client DHCPv6, configurez le support DNS.

1. Sélectionnez **DNS Support (Assistance DNS)**.
2. Activez **DNS Recursive Name Server (Serveur du nom récursif DNS)** et sélectionnez :
   - **DHCPv6** — Pour que le serveur DHCPv6 envoie les informations DNS Recursive Name Server au client.
   - **Manual (Manuel)** — Pour configurer manuellement le serveur de noms DNS Recursive. **Add (Ajoutez)** l'adresse IPv6 du **Server (Serveur)**, par exemple 2001:4860:4860:0:0:0:8888. Saisissez la **Lifetime (Durée de vie)** en secondes. Il s'agit de la durée de temps maximale pendant laquelle le client peut utiliser le serveur de nom récursif DNS donné pour résoudre des noms de domaine. La plage de durée de vie est de 4 à 3 600; par défaut est de 1 200.



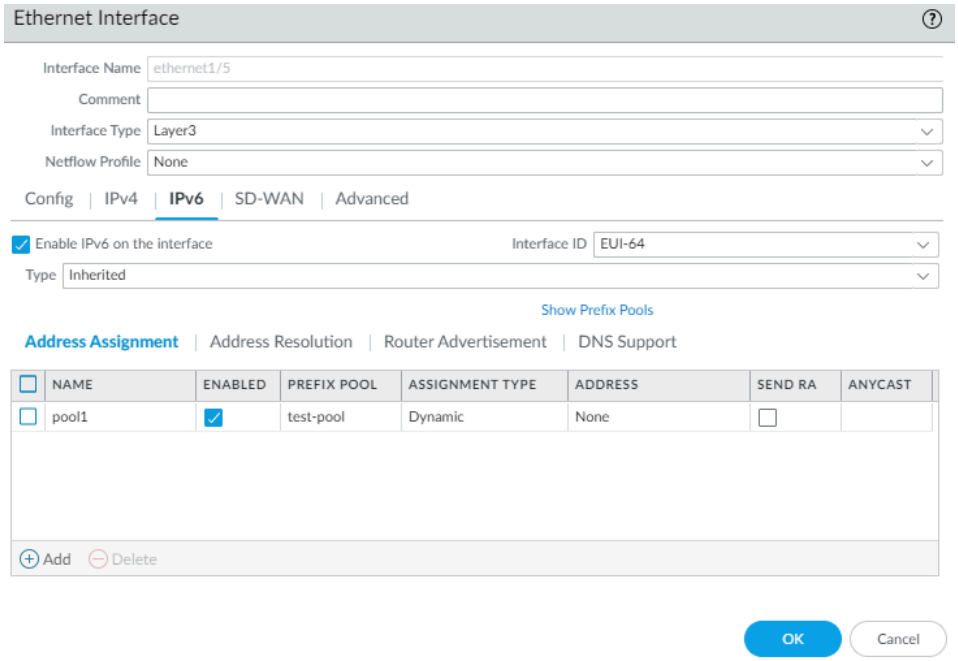
3. Activez la **Domain Search List (liste de recherche de domaine)** et sélectionnez :
   - **DHCPv6**—Pour que le serveur DHCPv6 envoie les informations de la liste de recherche de domaine au client.
   - **Manuak (Manuel)** — Pour configurer manuellement la liste de recherche de domaine. **Add (Ajouter)** un suffixe de **Domain (domaine)** à ajouter à un nom partiel dans DNS pour former un nom de domaine complet. Par exemple, entrez company.org. Entrez une **Lifetime (durée de vie)** en secondes pour la liste; la plage est de 4 à 3 600; par défaut est de 1 200.

STEP 8 | Cliquez sur **OK** pour enregistrer la configuration du client DHCPv6.

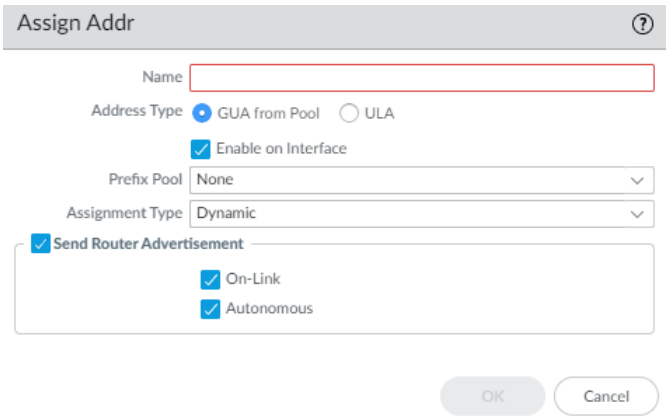
 ©2024 Palo Alto Networks, Inc.

STEP 9 | Configurer une interface orientée hôte pour hériter du préfixe IPv6 et annoncer les préfixes /64 alloués du pool aux hôtes.

1. Sélectionnez**Network (Réseau)** > **Interfaces** > **Ethernet** ou sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et sélectionnez une interface AE ou sélectionnez**Network (Réseau)** > **Interfaces** > **VLAN**.
2. Sélectionnez une interface de couche 3.
3. Sélectionnez **IPv6**.
4. **Enable IPv6 on the interface (Activer IPv6 sur l'interface)**
5. Pour **Type**, sélectionnez **Inherited (Hérité)**.



6. Sélectionnez **Address Assignment (Affectation d'adresse)** et **Add (Ajoutez)** une adresse en saisissant un **Name (nom)**. Le nom peut comporter au maximum 63 caractères alphanumériques, traits d'union, points et soulignements.



7. Pour **Address Type (Type d'adresse=**, sélectionnez l'une des options suivantes :
   - **AUG from Pool (AUG de Pool)**—Adresse Unicast globale (AUG) qui provient du pool de préfixes choisi ci-dessous.

 ©2024 Palo Alto Networks, Inc.

- **ULA**—Unique Local Address est une adresse privée dans la plage d'adresses fc00::/7 pour la connectivité au sein d'un réseau privé. Sélectionnez ULA s'il n'y a pas de serveur DHCPv6. Le serveur DHCPv6 a la discrétion d'envoyer la longueur de préfixe qu'il choisit.

  Il est recommandé de configurer également un ULA pour maintenir la connectivité locale au cas où la connexion au serveur DHCPv6 serait perdue.

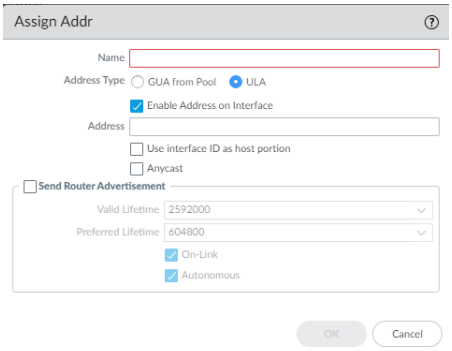
8. **Enable on Interface (Activer l'interface)** (AUG) ou **Enable Address on Interface (Activer l'adresse sur l'interface)** (ULA) pour activer cette adresse.
9. (GUA only (AUG uniquement)) Sélectionnez le **pool de préfixes** à partir duquel obtenir l'AUG
10. (GUA only (AUG seulement)) Sélectionnez **Assignment Type (Type d'affectation)** :
    - **Dynamic (Dynamique)** — Le client DHCPv6 est responsable du choix d'un identifiant pour configurer l'interface héritée.
    - **Dynamic with Identifier (Dynamique avec identificateur)** — Vous êtes responsable du choix d'un identificateur entre 0 et 4 000 et du maintien d'un identificateur unique sur les clients DHCPv6.

      *Si vous avez reçu un préfixe /64 du serveur DHCPv6, ne sélectionnez pas **Dynamic with Identifier (Dynamique avec identificateur)**.*

      *Si vous appliquez **Dynamic with Identifier (Dynamique avec identificateur)** à plus d'une adresse, attribuez la valeur d'identificateur la plus faible à la première adresse et une valeur d'identificateur plus élevée à chaque adresse suivante que vous configurez.*
11. (ULA only (ULA seulement)) Entrez une **Address (Adresse)**.
12. (ULA only (ULA uniquement)) Select **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** pour utiliser l'ID de l'interface de la portion hébergée de l'adresse IPv6.
13. (ULA only (ULA uniquement)) Sélectionnez **Anycast (Anycast)** pour faire de l'adresse IPv6 (itinéraire) une adresse Anycast (itinéraire), ce qui veut dire que plusieurs emplacements peuvent publier le même préfixe et que l'adresse IPv6 envoie le trafic

 ©2024 Palo Alto Networks, Inc.

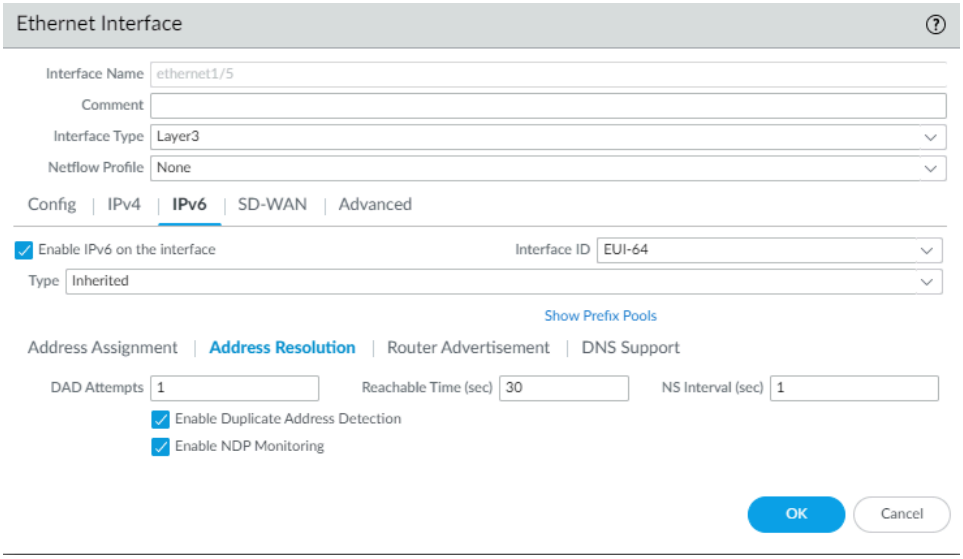
anycast au nœud qu'il considère le plus près selon les coûts associés au protocole de routage et d'autres facteurs.



14. Sélectionnez **Send Router Advertisement (Envoyer une annonce de routeur)** pour envoyer des RA de l'interface héritée aux hôtes du réseau local.
15. Si vous avez choisi ULA, entrez une **Valid Lifetime (durée de vie valide)** et une **Preferred Lifetime (durée de vie préférée)**.
16. Sélectionnez **On-link (Sur la liaison)** si les systèmes qui disposent d'adresses dans le préfixe sont accessibles sans routeur.
17. Sélectionnez **Autonomous (Autonome)** si les systèmes peuvent créer une adresse IPv6 de façon indépendante en combinant le préfixe publié et l'ID d'une interface.
18. Cliquez sur **OK** pour enregistrer l'attribution d'adresse.

STEP 10 | Pour Inherited interface, configurez la résolution d'adresse.

1. Sélectionnez **Address Resolution (Résolution d'adresse)**.



2. **Enable Duplicate Address Detection (Activez Duplicate Address Detection)** (DAD) si vous souhaitez une telle détection (activée par défaut).
3. Si vous avez sélectionné **Enable Duplicate Address Detection (Activer la détection d'adresses en double)**, spécifiez le nombre de **DAD Attempts (tentatives DAD)** dans

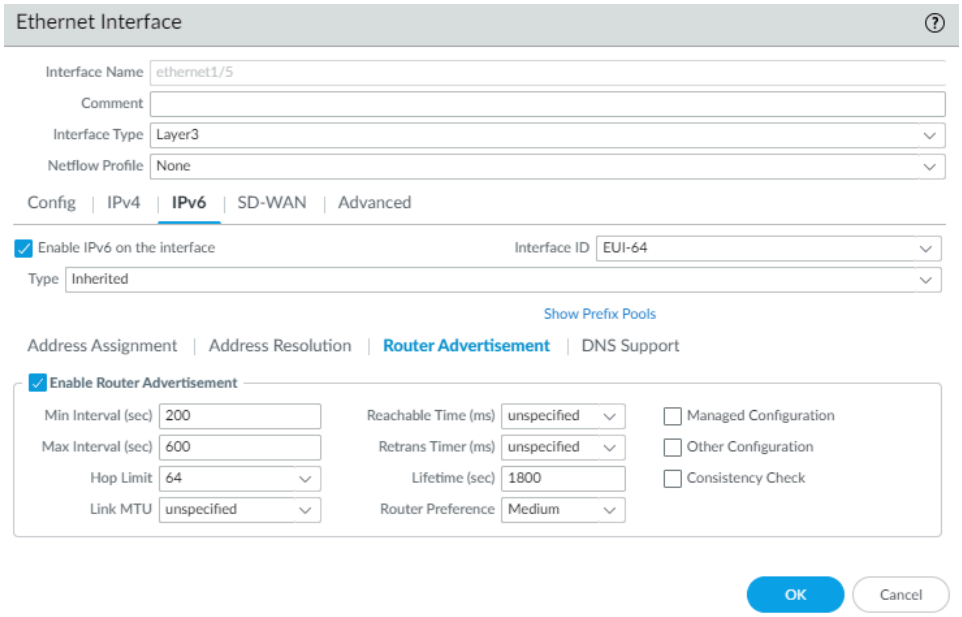
 ©2024 Palo Alto Networks, Inc.

l'intervalle de sollicitation des voisins (NS) avant que la tentative d'identification des voisins échoue; la plage est de 1 à 10; la valeur par défaut est 1.

4. Indiquez la **Reachable Time (sec) (durée d'accessibilité, en secondes)**, que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité.
5. Entrez **NS Interval (sec) (intervalle NS (sec))**, qui est la durée entre les demandes de sollicitation de voisins; la plage est de 1 à 3 600; la valeur par défaut est 1.
6. **Enable NDP Monitoring (Activez NDP Monitoring)** pour activer la surveillance du protocole de découverte des voisins. Lorsqu'il est activé, vous pouvez sélectionner l'icone NDP (dans la colonne Fonctions) et afficher des informations telles que l'adresse IPv6 d'un voisin découverte par le pare-feu, l'adresse MAC, User-ID correspondants et le statut (selon la situation la plus favorable).

STEP 11 | Pour Inherited interface, configurez Router Advertisement afin que cette interface puisse envoyer des RA aux hôtes annonçant le préfixe que les hôtes peuvent utiliser pour construire leur propre adresse IPv6.

1. Sélectionnez **Router Advertisement (Annonce de routeur)** et **nable Router Advertisement (Activer l'annonce de routeur)** afin que cette interface puisse répondre aux sollicitations de routeur des hôtes en envoyant des AR aux hôtes (la valeur par défaut est activée). Les 11 champs suivants concernent tous l'AR.



2. Définissez le **Min Interval (sec) (Intervalle min. (sec.)**, soit l'intervalle minimum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 3 et 1 350 ; valeur par défaut : 200). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales que vous configurez.
3. Définissez le **Max Interval (sec) (Intervalle max. (sec.))**, soit l'intervalle maximum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 4 et 1 800 ; valeur par défaut : 600). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales que vous configurez.

 ©2024 Palo Alto Networks, Inc.

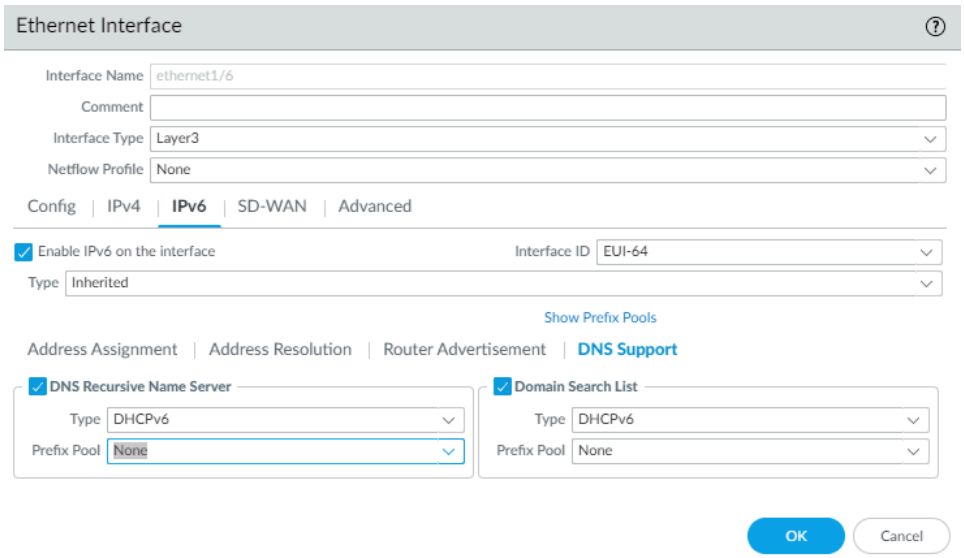
4. Définissez la **Hop Limit (Limite de saut)** à appliquer aux clients pour les paquets sortants (intervalle compris entre 1 et 255 ; valeur par défaut : 64). Sélectionnez **unspecified (non spécifié)** pour utiliser la valeur par défaut du système.
5. Définissez la **Link MTU (MTU de liaison)**, soit la Maximum Transmission Unit (unité de transmission maximale ; MTU) à appliquer aux clients (plage comprise entre 1 280 et 9 216 ; valeur par défaut : **unspecified (non spécifiée)**).
6. Définissez la **Reachable Time (ms) (Durée d'accessibilité (ms))**, soit la durée d'accessibilité, en millisecondes, que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité (la fourchette est de 0 à 3 600 000, la valeur par défaut est **unspecified**).
7. Définissez la **Retrans Time (ms) (Durée de retransmission (ms))**, soit le minuteur de retransmission qui détermine la durée d'attente du client, en millisecondes, avant la retransmission des messages de sollicitation de voisins. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée de retransmission (intervalle compris entre 0 et 4 294 967 295 ; valeur par défaut : **non spécifiée**).
8. Définissez la **Router Lifetime (sec) (Durée de vie du routeur (s))** pour indiquer la durée, en secondes, pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.
9. Définissez **Router Preference (Préférence Routeur)** au cas où il y aurait deux ou plusieurs interfaces héritées sur des routeurs différents envoyant des RA à un hôte. **Élevé**, **Moyen** ou **Bas** est la priorité que l'AR annonce indiquant la priorité relative et l'hôte utilise le préfixe du routeur à priorité plus élevée.
10. Sélectionnez **Managed Configuration (Configuration gérée)** pour indiquer au client que les adresses sont disponibles via DHCPv6.
11. Sélectionnez **Other Configuration (Autre configuration)** pour indiquer au client que d'autres informations d'adresse (comme les paramètres associés au DNS) sont disponibles via DHCPv6.
12. Cochez **Consistency Check (Vérification de cohérence)** pour que le pare-feu vérifie que les RA reçues des autres routeurs publient des informations cohérentes sur la liaison. Le pare-feu consigne toute incohérence.

STEP 12 | Pour Inherited interface, configurez DNS Support.

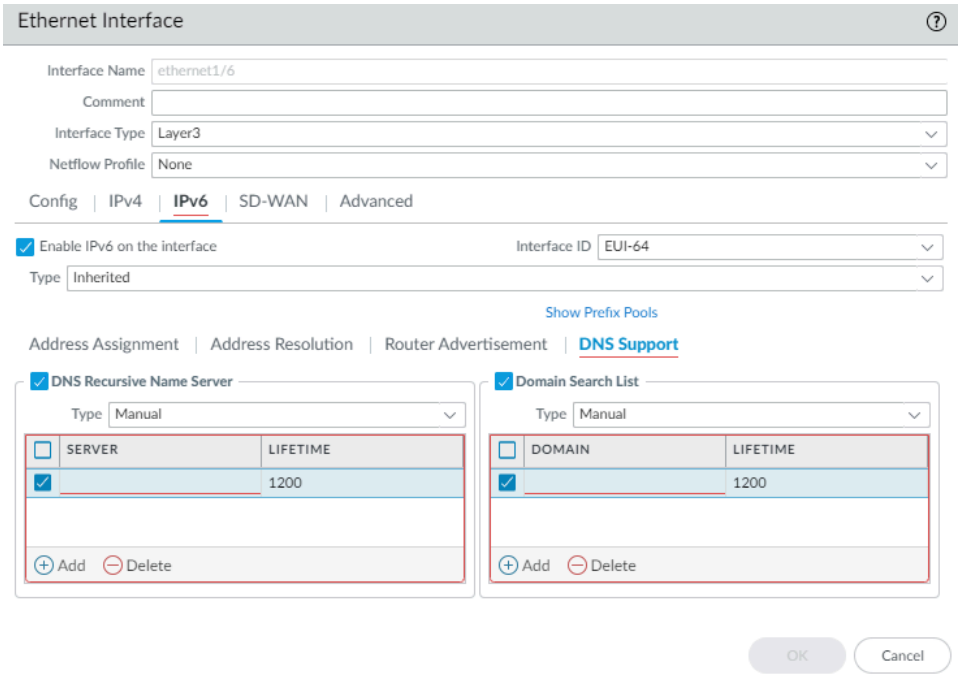
1. Sélectionnez **DNS Support (Assistance DNS)**.
2. Activez **DNS Recursive Name Server** et sélectionnez **DHCPv6** ou **Manuel** :
   - **DHCPv6**—Pour que le serveur DHCPv6 envoie les informations DNS Recursive Name Server. Sélectionnez **Prefix Pool (ensemble de préfixes)**. Lorsque le serveur DNS Recursive Namer Server provient du serveur DHCPv6, une interface héritée peut dériver des informations indirectement de l'ensemble de préfixes. (Si dans l'onglet

 ©2024 Palo Alto Networks, Inc.

Address Assignment (Affectation d'adresses) vous avez configuré le Type d'adresse comme **ULA**, l'ensemble de préfixes sera **None (Aucun)**.)



- **Manual (Manuel)** — Pour configurer manuellement le serveur de noms DNS Recursive. **Add (Ajoutez)** une adresse IPv6 du **Server (Serveur)**, par exemple 2001:4860:4860:0:0:0:8888. La plage de la **Lifetime (Durée de vie)** correspond à toute valeur égale ou se situant entre le **Max Interval (Intervalle Max.)** (que vous avez configuré à l'onglet **Router Advertisement (Publication de routeur))** et deux fois cet Max Interval (Intervalle max.). La valeur par défaut est 1200 secondes.



3. Activez la **Domain Search List (liste de recherche de domaine)** et sélectionnez :
   - **DHCPv6**—pour que le serveur DHCPv6 envoie les informations de la liste de recherche de domaine. Sélectionnez **Prefix Pool (ensemble de préfixes)**. Lorsque la liste de recherche de domaine provient du serveur DHCPv6, une interface héritée peut dériver des informations indirectement du pool de préfixes. (Si dans l'onglet

 ©2024 Palo Alto Networks, Inc.

Address Assignment (Affectation d'adresses) vous avez configuré le Type d'adresse comme **ULA**, l'ensemble de préfixes sera **None (Aucun).)**

- **Manuak (Manuel)** — Pour configurer manuellement la liste de recherche de domaine. **Add (Ajouter)** un suffixe de **Domain (domaine)** à ajouter à un nom partiel dans DNS pour former un nom de domaine complet. Par exemple, entrez company.org. Saisissez **Lifetime (Durée de vie)** pour le domaine, la plage correspond à toute valeur égale ou se situant entre le **Max Interval (Intervalle Max.)** (que vous avez configuré à l'onglet **Router Advertisement (Publication de routeur))** et deux fois cet Max Interval (Intervalle max.). La valeur par défaut est 1200.

STEP 13 | Cliquez sur **OK** pour enregistrer l'interface Héritée.

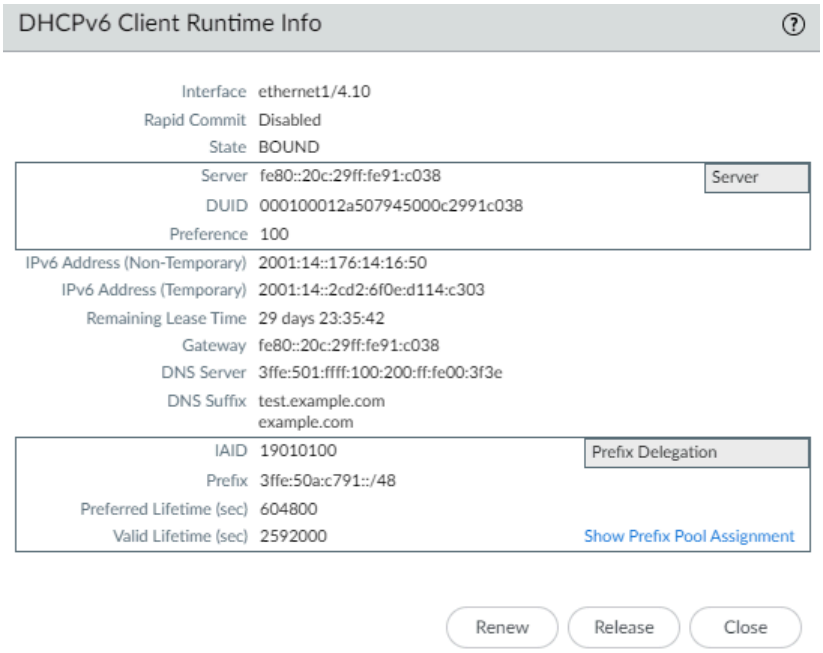
STEP 14 | **Commit** (Valider).

 ©2024 Palo Alto Networks, Inc.

STEP 15 | Affichez les informations DHCPv6 pour une interface.

1. Sélectionnez**Network (Réseau)** > **Interfaces** > **Ethernet** ou **VLAN** ou **AE Group (groupe AE)**.
2. Dans la ligne de votre interface configurée, sélectionnez le lien **Dynamic-DHCP Client (Client Dynamique-DHCP)** dans la colonne Adresse IP pour afficher les paramètres assignés par le serveur DHCPv6 à ce client DHCPv6.

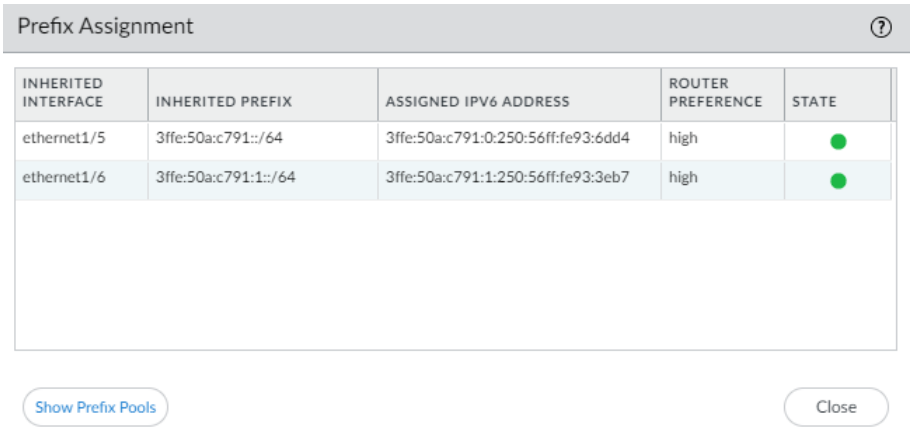
   *Sinon, vous pouvez sélectionner l'interface, puis **Show DHCPv6 Client Runtime Info (Afficher les informations d'exécution du client DHCPv6)**.*
3. Consultez les informations.
   - Dans l'exemple suivant, la section du milieu montre que l'interface face au FAI a reçu une adresse Non Temporaire et une adresse Temporaire pour elle-même. Le Temps de location restant s'applique aux deux adresses.
   - La section Délégation de préfixe montre que l'interface a également reçu un préfixe que l'interface héritée face à l'hôte peut annoncer dans les AR aux hôtes.



4. Sélectionnez **Show Prefix Pool Assignment (Afficher l'affectation du pool de préfixes)** à afficher pour chaque interface héritée faisant face à l'hôte : le préfixe hérité (préfixe que l'interface distribue aux hôtes), l'adresse IPv6 assignée de l'interface héritée elle-même

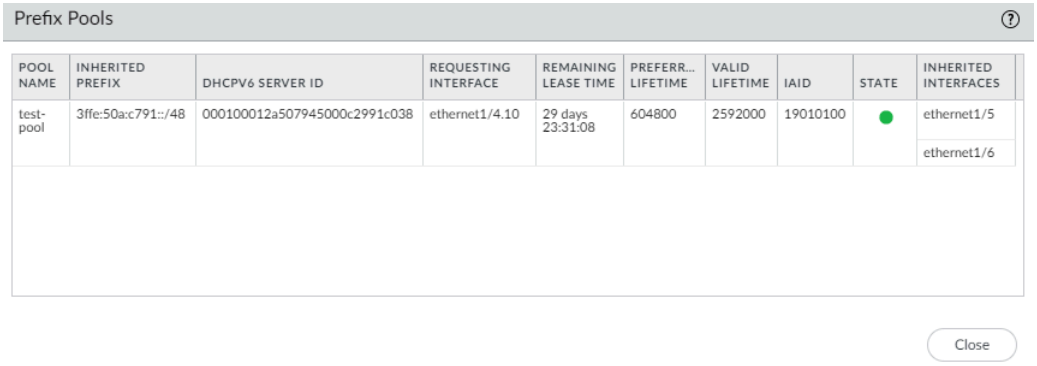
 ©2024 Palo Alto Networks, Inc.

(basée sur le préfixe et construite à partir de l'adresse MAC), la préférence du routeur et l'état de l'interface.



Le client DHCPv6 a demandé une longueur de préfixe de /48 au serveur et l'a reçue, mais a ensuite divisé ce préfixe en préfixes /64 et les a délégués aux interfaces héritées. Les interfaces héritées annoncent les préfixes /64 aux hôtes.

5. Sélectionnez **Show Prefix Pools (Afficher les pools de préfixes)** pour voir les pools de préfixes créés.

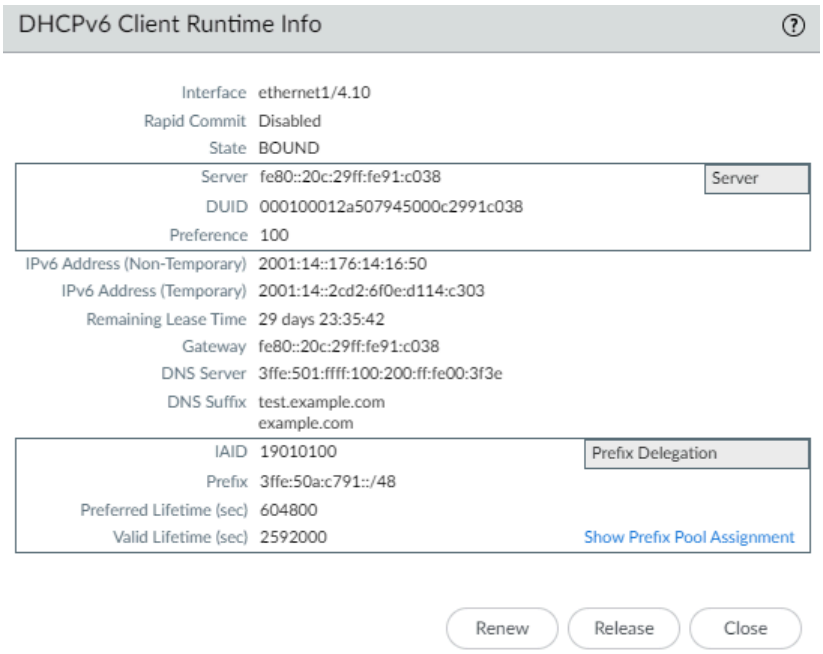


6. **Close (Fermez)** la liste des pools de préfixes.

 ©2024 Palo Alto Networks, Inc.

STEP 16 | Renouveler un bail DHCPv6 avec le serveur DHCPv6 (quelle que soit la durée du bail) si vous souhaitez renouveler plus tôt que le renouvellement automatique demandé par le pare-feu.

1. SélectionnezNetwork (Réseau) > **Interfaces** > **Ethernet** ou **VLAN** ou **AE Group (groupe AE)**.
2. Dans la ligne de votre interface configurée, sélectionnez le lien **Dynamic-DHCP Client** dans la colonne Adresse IP.
3. Sélectionnez **Renew (Renouveler)** à partir de l'écran Informations d'exécution du client DHCPv6.



4. **Close (Fermez)** les informations d'exécution du client DHCPv6.

 ©2024 Palo Alto Networks, Inc.

STEP 17 | Relâchez les options DHCP suivantes provenant du serveur DHCPv6 si vous n'en avez plus besoin avant l'expiration de la durée de vie.

- Préfixe
- Adresse IPv6 (non temporaire)
- Adresse IPv6 (temporaire)
- Durée restante du bail
- Passerelle
- Serveur DNS
- Suffixe DNS

Une résiliation libère l'adresse IP ; la connexion réseau sera coupée et le pare-feu sera ingérable si aucune autre interface n'est configurée pour l'accès de gestion.

1. Sélectionnez**Network (Réseau)** > **Interfaces** > **Ethernet** ou **VLAN** ou **AE Group (groupe AE)**.
2. Dans la ligne de votre interface configurée, sélectionnez le lien **Dynamic-DHCP Client** dans la colonne Adresse IP.
3. Sélectionnez **Release (Libérer)** dans l'écran Informations d'exécution du client DHCPv6.
4. **Close (Fermez)** les informations d'exécution du client DHCPv6.

 ©2024 Palo Alto Networks, Inc.

Configuration de l'interface de gestion en tant que client DHCP

L'interface de gestion du pare-feu prend en charge le client DHCP pour IPv4, qui permet à l'interface de gestion de recevoir son adresse IPv4 d'un serveur DHCP. L'interface de gestion prend également en charge les options DHCP 12 et 61, qui permettent au pare-feu d'envoyer son nom d'hôte et son identifiant du client, respectivement, à des serveurs DHCP.

À partir de PAN-OS 11.1.0, l'interface de gestion prend également en charge la Dynamic IPv6 Address Assignment (Attribution d'adresses IPv6 dynamiques).

Plutôt que d'utiliser une adresse IP statique, les pare-feu VM-Series déployés dans AWS et dans Azure™ utilisent, par défaut, l'interface de gestion en tant que client DHCP pour l'obtention de leur adresse IP, puisque les déploiements de cloud dépendent de l'automation que cette fonctionnalité offre. La fonctionnalité DHCP est désactivée par défaut sur l'interface de gestion des pare-feu VM-Series, à l'exception des pare-feu VM-Series qui sont déployés dans AWS et dans Azure. Les interfaces de gestion des modèles WildFire et Panorama ne prennent pas en charge cette fonctionnalité DHCP.

- *Pour ce qui est des modèles de pare-feu matériels (autres que VM-Series), configurez l'interface de gestion au moyen d'une adresse IP statique, dans la mesure du possible.*
- *Si le pare-feu obtient une adresse pour son interface de gestion via DHCP, affectez une adresse MAC réservée sur le serveur DHCP qui prend en charge ce pare-feu. Vous vous assurez ainsi que le pare-feu conservera son adresse IP de gestion à l'issue d'un redémarrage. Si le serveur DHCP est un pare-feu Palo Alto Networks®, reportez-vous à l'étape 6 de*Configure an Interface as a DHCP Server (Configuration d'une interface en tant que serveur DHCP)*, qui explique comment réserver une adresse.*

Si vous configurez l'interface de gestion en tant que client DHCP, les restrictions suivantes s'appliquent :

- Vous ne pouvez utiliser l'interface de gestion dans une configuration de type HA Liaison de contrôle (HA1 ou HA de secours), Liaison de données (HA2 ou HA2 de secours) ou Transfert des paquets (HA3).
- Vous ne pouvez sélectionner **MGT** en tant que Source Interface (Interface source) lorsque vous personnalisez les itinéraires de service (**Device (Périphérique)** > **Setup (Configuration)** > **Services (Services)** > **Service Route Configuration (Configuration des itinéraires de service)** > **Customize (Personnaliser)**). Vous pouvez toutefois sélectionner **Use default (Utiliser les paramètres par défaut)** pour acheminer les paquets via l'interface de gestion.
- Vous ne pouvez utiliser l'adresse IP dynamique de l'interface de gestion pour vous connecter à un Hardware Security Module (module de sécurité matériel ; HSM). L'adresse IP du pare-feu client HSM doit être statique, car le HSM authentifie le pare-feu au moyen d'une adresse IP, et les opérations sur le HSM cesseraient si l'adresse IP devait changer au cours de l'exécution.

Pour pouvoir accomplir cette tâche, il est essentiel que l'interface de gestion puisse joindre un serveur DHCP.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Configurez l'interface de gestion en tant que client DHCP pour qu'elle puisse obtenir son adresse IP (IPv4), son masque de réseau (IPv4) et sa passerelle par défaut d'un serveur DHCP.

Vous pouvez éventuellement envoyer le nom d'hôte et l'identifiant du client de l'interface de gestion au serveur DHCP si le système d'orchestration que vous utilisez accepte ces informations.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Interfaces** et sélectionnez l'interface **Management (Gestion)**.

   Les sélections sans rapport avec une adresse dynamique (telles que la vitesse, la MTU, les adresses IP autorisées, les services de gestion administrative et les services réseau) sont documentées dans le Guide de l'administrateur PAN-OS : Getting Started / Integrate the Firewall into Your Management Network / Initial Configuration (Mise en route /Intégration du pare-feu dans votre réseau de gestion / Configuration initiale).

2. Sélectionnez **IPv4**.
3. Pour **Type**, sélectionnez **DHCP Client (Client DHCP)**.
4. (Facultatif) Sélectionnez une option, ou les deux options, pour que le pare-feu envoie des messages DHCPDISCOVER ou DHCPREQUEST au serveur DHCP :
   - **Send Hostname (Envoyer le nom d'hôte)** : envoie le **Hostname (Nom d'hôte)** (tel qu'il est défini dans **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**) dans le cadre de l'Option DHCP 12.
   - **Send Client ID (Envoyer l'identifiant du client)** : envoie l'identifiant du client dans le cadre de l'Option DHCP 61. Un identifiant du client identifie de manière unique un client DHCP, et le serveur DHCP s'en sert pour indexer sa base de données des paramètres de configuration.
5. Cliquez sur **OK**.

STEP 2 | (Facultatif) Configurez le pare-feu pour qu'il accepte le nom d'hôte et le domaine qui proviennent du serveur DHCP.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les General Settings (Paramètres généraux).
2. Sélectionnez l'une des options suivantes, ou les deux :
   - **Accept DHCP server provided Hostname (Accepter le nom d'hôte fourni par le serveur DHCP)** : permet au pare-feu d'accepter le nom d'hôte reçu du serveur DHCP (s'il est valide). Lorsque cette option est activée, le nom d'hôte reçu du serveur DHCP remplace tout **Hostname (Nom d'hôte)** existant qui a été indiqué dans **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**. Évitez de sélectionner cette option si vous souhaitez configurer manuellement le nom de l'hôte.
   - **Accept DHCP server provided Domain (Accepter le domaine fourni par le serveur DHCP)** : permet au pare-feu d'accepter le domaine reçu du serveur DHCP. Le domaine (suffixe DNS) reçu du serveur DHCP remplace tout **Domain (Domaine)** qui a été spécifié dans **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**. Évitez de sélectionner cette option si vous souhaitez configurer manuellement un domaine.

 ©2024 Palo Alto Networks, Inc.

3. Cliquez sur **OK**.

STEP 3 | Validez vos modifications.

Cliquez sur **Commit (Valider)**.

STEP 4 | Affichez les informations sur le client DHCP.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Interfaces (Interfaces)** et modifiez les paramètres de l'interface de gestion.
2. Cliquez sur **Show DHCP Client Runtime Info (Afficher les informations d'exécution du client DHCP)**.

STEP 5 | (Facultatif) Renouvelez le Bail DHCP du serveur DHCP, peu importe la durée du bail.

Cette option est utile si vous testez ou résolvez des problèmes liés au réseau.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Interfaces (Interfaces)** et modifiez les paramètres de l'interface de gestion.
2. Cliquez sur **Show DHCP Client Runtime Info (Afficher les informations d'exécution du client DHCP)**.
3. Cliquez sur **Renew (Renouveler)**.

STEP 6 | (Facultatif) Libérez les options DHCP suivantes obtenues du serveur DHCP :

- Adresse IP
- netmask
- Passerelle par défaut
- Serveur DNS (principal et secondaire)
- Serveur NTP (principal et secondaire)
- Domaine (suffixe DNS)

Une résiliation libère l'adresse IP ; la connexion réseau sera coupée et le pare-feu sera ingérable si aucune autre interface n'est configurée pour l'accès de gestion.

Utilisez la commande CLI opérationnelle **`request dhcp client management-interface release`**.

 ©2024 Palo Alto Networks, Inc.

Configuration de l'interface de gestion pour l'attribution d'adresses IPv6 dynamiques

Avant de configurer l'interface de gestion (MGT) pour l'attribution d'adresses IPv6 dynamiques, consultez la section Dynamic IPv6 Addressing (Adressage IPv6 dynamique) sur l'interface de gestion pour comprendre comment la configuration automatique d'adresses sans état IPv6 (SLAAC) ou DHCPv6 détermine l'adresse.

Les interfaces de gestion des modèles WildFire et Panorama ne prennent pas en charge cette fonctionnalité DHCPv6.

- *Pour ce qui est des modèles de pare-feu matériels (autres que VM-Series), configurez l'interface de gestion au moyen d'une adresse IPv6 statique, dans la mesure du possible.*
- *Si le pare-feu obtient une adresse pour son interface de gestion via DHCPv6, affectez une adresse MAC réservée sur le serveur DHCPv6 qui prend en charge ce pare-feu. Vous vous assurez ainsi que le pare-feu conservera son adresse IP de gestion à l'issue d'un redémarrage.*

Si vous utilisez le mode sans état (SLAAC/autoconfig), utilisez-le dans un environnement sécurisé.

Au lieu d'utiliser l'attribution d'adresses IPv6 dynamiques sur l'interface de gestion, vous pouvez Configuration de l'interface de gestion en tant que client DHCP *à l'aide d'IPv4.*

Si vous configurez l'interface MGT en tant que client DHCPv6, les restrictions suivantes s'appliquent :

- Vous ne pouvez pas utiliser l'interface MGT dans une configuration de type HA Liaison de contrôle (HA1 ou HA de secours), Liaison de données (HA2 ou HA2 de secours) ou Transfert des paquets (HA3).
- Vous ne pouvez pas sélectionner **MGT** en tant que Source Interface (Interface source) lorsque vous personnalisez les itinéraires de service (**Device (Périphérique)** > **Setup (Configuration)** > **Services (Services)** > **Service Route Configuration (Configuration des itinéraires de service)** > **Customize (Personnaliser)**). Vous pouvez toutefois sélectionner **Use default (Utiliser les paramètres par défaut)** pour acheminer les paquets via l'interface de gestion.
- Vous ne pouvez pas utiliser l'adresse IP dynamique de l'interface MGT pour vous connecter à un Hardware Security Module (module de sécurité matériel ; HSM). L'adresse IP du pare-feu client HSM doit être statique, car le HSM authentifie le pare-feu au moyen d'une adresse IP, et les opérations sur le HSM cesseraient si l'adresse IP devait changer au cours de l'exécution.
- Une limitation supplémentaire est que lorsque la durée de vie préférée de l'adresse IPv6 sur l'interface MGT expire, les sessions IPv6 existantes sont déconnectées. Pour élaborer, la configuration est envoyée par le serveur DHCPv6 et le serveur RADVD. Le pare-feu prend la durée de vie valide et la durée de vie préférée de ces messages RA à partir des serveurs et définit les temps en fonction des valeurs reçues. La RFC 8415 indique que les communications

 ©2024 Palo Alto Networks, Inc.

existantes doivent rester pendant toute la durée de vie valide si la durée de vie préférée expire (les sessions doivent être actives pendant la période comprise entre la durée de vie préférée et la durée de vie valide). Toutefois, la limitation du NGFW est que les sessions sont perdues à l'expiration de la durée de vie préférée.

Pour obtenir une adresse DHCPv6, il est essentiel que l'interface MGT soit en mesure d'atteindre un serveur DHCPv6.

STEP 1 | Configurez l'interface MGT pour l'attribution d'adresses IPv6 dynamiques.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Interfaces** et sélectionnez l'interface **Management (Gestion)**.

   Les sélections sans rapport avec une adresse dynamique (telles que la vitesse, la MTU, les adresses IP autorisées, les services de gestion administrative et les services réseau) sont documentées dans le Guide de l'administrateur PAN-OS : Effectuer la configuration initiale.

2. Sélectionnez **IPv6** et **Enable IPv6 (Activer IPv6)**.
3. Définissez le **Type (type)** sur **Dynamic (Dynamique)**.

STEP 2 | Dans la section DHCPv6 Client Options (Options du client DHCPv6), sélectionnez **Non Temporary Address (Adresse non temporaire)** (paramètre par défaut). Ce type d'adresse a une durée de vie plus longue qu'une adresse temporaire.

Que vous demandiez une adresse non temporaire ou une adresse temporaire pour l'interface dépend de votre discrétion et de la capacité du serveur DHCPv6; certains serveurs ne peuvent fournir qu'une adresse temporaire. Vous pouvez choisir Non Temporary Address (Adresse non temporaire) ou Temporary Address (Adresse temporaire), mais pas les deux.

STEP 3 | Sélectionnez **Temporary Address (Adresse temporaire)** pour un plus grand niveau de sécurité car l'adresse est destinée à être utilisée pendant une courte période.

L'adresse IPv6 n'est pas renouvelée automatiquement et expire lorsque le temps valide atteint 0.

STEP 4 | Sélectionnez **Rapid Commit (Validation rapide)** pour utiliser le processus DHCPv6 des messages Solliciter et répondre (deux messages), plutôt que le processus des messages Solliciter, annoncer, demander et répondre (quatre messages).

STEP 5 | Sélectionnez le **DUID Type (Type DUID)** (**D**HCPv6 **U**nique **Id**entifier (Identifiant unique DHCPv6)) (RFC-6355) que l'interface MGT utilise pour s'identifier auprès du serveur DHCPv6 :

- **duid-type-llt**—DUID-LLT ; l'adresse de la couche de liaison de l'interface MGT, concaténée par un horodatage.
- **duid-type-ll**—DUID-LL ; l'adresse de la couche liaison de l'interface MGT.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Choisissez un **Default Gateway Type (Type de passerelle par défaut)** :

- **Static (Statique)** : saisissez la **Default IPv6 Gateway Address (Adresse de passerelle IPv6 par défaut)**.
- **Dynamic (Dynamique)** : le pare-feu apprend l'adresse de passerelle par défaut IPv6 pour l'interface MGT à partir des messages d'annonce de routeur (RA) provenant d'un routeur voisin (passerelle) en réponse à une sollicitation de routeur (RS). S'il n'y a qu'un seul routeur attaché à la liaison, l'adresse source (adresse link-local) du routeur annonçant le RA est configurée comme adresse de passerelle par défaut pour l'interface MGT. L'adresse link-local est spécifique à l'interface et est configurée automatiquement à l'aide de la méthode EUI-64. S'il y a plusieurs routeurs attachés à la liaison, le pare-feu définit son adresse de passerelle par défaut à l'adresse source des messages RA qui ont la valeur de préférence de routeur la plus élevée (basse, moyenne, élevée).

STEP 7 | **Commit (Validez)** vos modifications.

STEP 8 | (Facultatif) Affichez l'adresse de la passerelle DHCPv6.

1. Accédez à la CLI.
2. **>show dhcp client ipv6-gateway-address**

STEP 9 | (Facultatif) Affichez les informations sur le client DHCPv6.

1. **>show dhcp client mgmt6-interface-state**
2. Voir le nom d'hôte, l'adresse IPv6, life-starts, max-life, preferred-life et dhcpv6-server.

STEP 10 | (Facultatif) Renouvelez le DHCP lease (Bail DHCPv6) du serveur DHCP, peu importe la durée du bail.

Cette option est utile si vous testez ou résolvez des problèmes liés au réseau.

1. **>show dhcp client mgmt6-interface-state**
2. Renouveler.

STEP 11 | (Facultatif) Publiez l'adresse DHCPv6 obtenue à partir du serveur DHCPv6. (Une adresse SLAAC n'est pas publiée.)

Une résiliation libère l'adresse IPv6 ; la connexion réseau sera coupée et le pare-feu sera ingérable si aucune autre interface n'est configurée pour l'accès de gestion.

1. **>show dhcp client mgmt6-interface-state**
2. Publier.

 ©2024 Palo Alto Networks, Inc.

Configuration d'une interface en tant qu'agent de relais DHCP

Pour qu'une interface de pare-feu puisse transmettre des messages DHCP entre les clients et les serveurs, vous devez configurer le pare-feu en tant qu'agent de relais DHCP. L'interface peut transmettre des messages à un maximum de huit serveurs DHCP IPv4 externes et de huit serveurs DHCP IPv6 externes. Un message DHCPDISCOVER du client est envoyé à tous les serveurs configurés ; le message DHCPOFFER du premier serveur qui répond est relayé au client qui a effectué la demande.

Les capacités sont les suivantes :

- Vous pouvez configurer un total combiné de 500 serveurs DHCP (IPv4) et agents de relais DHCP (IPv4 et IPv6) sur tous les modèles de pare-feu, à l'exception des pare-feu PA-5200 Series et PA-7000 Series.
- Sur les pare-feu PA-5220, vous pouvez configurer un maximum de 500 serveurs DHCP et un maximum de 2 048 agents de relais DHCP, moins le nombre de serveurs DHCP configurés. Par exemple, si vous configurez 500 serveurs DHCP, vous pouvez configurer 1 548 agents de relais DHCP.
- Sur les pare-feu PA-5250, 5260 et PA-7000, vous pouvez configurer un maximum de 500 serveurs DHCP et un maximum de 4 096 agents de relais DHCP, moins le nombre de serveurs DHCP configurés. Par exemple, si vous configurez 500 serveurs DHCP, vous pouvez configurer 3 596 agents de relais DHCP.

Avant de configurer un agent de relais DHCP, assurez-vous d'avoir configuré une interface Ethernet ou VLAN de Couche 3 et de l'avoir affectée à un routeur virtuel et à une zone.

STEP 1 | Sélectionnez un relais DHCP.

Sélectionnez **Network (Réseau)** > **DHCP (DHCP)** > **DHCP Relay (Relais DHCP)**.

STEP 2 | Indiquez l'adresse IP de chaque serveur DHCP avec lequel l'agent de relais DHCP communiquera.

1. Dans le champ **Interface**, sélectionnez l'interface que vous souhaitez être l'agent de relais DHCP.
2. Sélectionnez **IPv4 (IPv4)** ou **IPv6 (IPv6)** pour indiquer le type de serveur DHCP que vous allez préciser.
3. Si vous avez coché **IPv4 (IPv4)**, dans le champ **DHCP Server IP Address (Adresse IP du serveur DHCP)**, **Add (Ajoutez)** l'adresse IP du serveur DHCP duquel et auquel vous relayerez les messages DHCP.
4. Si vous avez coché **IPv6 (IPv6)**, dans le champ **DHCP Server IP Address (Adresse IP du serveur DHCP)**, **Add (Ajoutez)** l'adresse IP du serveur DHCP duquel et auquel vous relayerez les messages DHCP. Si vous indiquez une adresse de *multidiffusion*, indiquez également une **Interface (Interface)** sortante.
5. (Facultatif) Répétez les trois étapes précédentes pour saisir un maximum de huit adresses de serveur DHCP par famille d'adresses IP.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Commit (Validez) la configuration.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

Surveillance et dépannage de DHCP

Vous pouvez afficher l'état des baux des adresses dynamiques que votre serveur DHCP ou votre client DHCP a affectées (à l'aide de commandes de la CLI. Vous pouvez également effacer les baux avant leur expiration et leur libération automatiques.

- Affichage des informations sur le serveur DHCP
- Effacer les baux DHCP
- Affichage des informations sur le client DHCP
- Obtention du résultat du débogage DHCP

Affichage des informations sur le serveur DHCP

Effectuez cette tâche pour afficher les statistiques des pools DHCP, les adresses IP affectées par le serveur, l'adresse MAC correspondante, l'état et la durée du bail, ainsi que la date et l'heure de début du bail. Si l'adresse a été configurée comme **Reserved Address (adresse réservée)**, la colonne `state` indique `reserved` et aucune colonne `duration` ou `lease_time` ne s'affiche. Si le bail a été configuré comme **Unlimited (Illimité)**, la colonne `duration` affiche une valeur de `0`.

- Affichez les statistiques du pool DHCP, l'adresse IP du serveur DHCP affecté, l'adresse MAC, l'état et la durée de bail, et l'heure de début du bail.

```
admin@PA-220> show dhcp server lease interface all
```

```
interface: "ethernet1/2" Allocated IPs: 1, nombre total
 d'adresses IP dans le pool : 5. 20.0000% used ip mac state
 duration lease_time 192.168.3.11 f0:2f:af:42:70:cf committed 0 Wed
 Jul 2 08:10:56 2014 admin@PA-220>
```

- Affichez les options qu'un serveur DHCP a affectées aux clients.

```
admin@PA-220> show dhcp server settings all
```

```
Interface    GW           DNS1        DNS2       DNS-Suffix Inherit
 source
 ------------------------------------------------------------------------
 ethernet1/2  192.168.3.1  10.43.2.10  10.44.2.10
             ethernet1/3 admin@PA-220>
```

Effacer les baux DHCP

Plusieurs options s'offrent à vous pour effacer les baux DHCP.

 ©2024 Palo Alto Networks, Inc.

- Libérez les baux DHCP expirés d'une interface (serveur), comme ethernet1/2, avant que le minuteur de suspension ne les libère automatiquement. Ces adresses seront à nouveau disponibles dans le pool d'adresses IP.

```
admin@PA-220> clear dhcp lease interface ethernet1/2 expired-only
```

- Libérez le bail d'une adresse IP donnée, par exemple, 192.168.3.1.

```
admin@PA-220> clear dhcp lease interface ethernet1/2 ip 192.168.3.1
```

- Libérez le bail d'une adresse MAC donnée, par exemple, f0:2c:ae:29:71:34.

```
admin@PA-220> clear dhcp lease interface ethernet1/2 mac
 f0:2c:ae:29:71:34
```

Affichage des informations sur le client DHCP

Pour afficher l'état des baux d'adresse IP envoyés au pare-feu lorsqu'il agit en tant que client DHCP, utilisez l'une de ces commandes de CLI.

- admin@PA-220>**show dhcp client state *<interface_name>***
- admin@PA-220> **show dhcp client state all**

```
Interface State IP Gateway Leased-until
 ----------------------------------------------------------------------------
 ethernet1/1 Bound 10.43.14.80 10.43.14.1 70315 admin@PA-220>
```

Obtention du résultat du débogage DHCP

Pour obtenir le résultat du débogage DHCP, utilisez l'une des commandes suivantes :

- admin@PA-220> **déboguer dhcpd**
- admin@PA-220> **déboguer management-server dhcpd**

 ©2024 Palo Alto Networks, Inc.

DNS

Domain Name System (système de noms de domaine ; DNS) est un protocole qui traduit (résout) un nom de domaine convivial, comme www.paloaltonetworks.com, en une adresse IP pour permettre aux utilisateurs d'accéder aux ordinateurs, aux sites Web, aux services ou aux autres ressources qui se trouvent sur l'Internet ou sur des réseaux privés.

- Présentation de DNS
- Objet proxy DNS
- DNS Server Profile (profil de serveur DNS)
- Déploiements DNS à plusieurs locataires
- Configuration d'un objet proxy DNS
- Configuration d'un profil de serveur DNS
- Configurer un proxy Web
- Cas pratique 1 : Le pare-feu exige une résolution DNS
- Cas d’utilisation 2 : Le locataire de l'ISP utilise un proxy DNS pour traiter la résolution DNS pour des politiques de sécurité, la génération de rapports et des services de son système virtuel
- Cas d’utilisation 3 : Le pare-feu sert de proxy DNS entre le client et le serveur
- Mise en correspondance de la règle de proxy DNS et du FQDN

Présentation de DNS

DNS joue un rôle crucial dans l'accès des utilisateurs aux ressources de réseau, car, grâce à lui, les utilisateurs n'ont pas à se souvenir des adresses IP et les ordinateurs individuels n'ont pas à stocker d'importants volumes de noms de domaines mappés à des adresses IP. DNS se sert d'un modèle client/serveur ; un serveur DNS résout une requête pour un client DNS en cherchant le domaine dans son cache et, au besoin, en envoyant des requêtes à d'autres serveurs, jusqu'à ce qu'il puisse répondre au client avec l'adresse IP correspondante.

La structure DNS des noms de domaine est hiérarchique ; le Top-Level Domain (domaine de premier niveau ; TLD) d'un nom de domaine peut être générique (gTLD) : com, edu, gov, int, mil, net, ou org (gov et mil ne sont utilisés qu'aux États-Unis) ou un code de pays (ccTLD), comme au (Australie) ou us (États-Unis). Les ccTLD sont généralement réservés aux pays et aux territoires indépendants.

Un fully qualified domain name (nom de domaine complet ; FQDN) comprend au moins un nom d'hôte, un domaine de deuxième niveau et un TLD pour indiquer complètement l'emplacement de l'hôte dans la structure DNS. Par exemple, www.paloaltonetworks.com est un FQDN.

Lorsqu'un pare-feu Palo Alto Networks® utilise un FQDN dans l'interface utilisateur ou la CLI, le pare-feu doit résoudre ce FQDN en utilisant DNS. Selon l'origine de la requête FQDN, le pare-feu détermine les paramètres DNS à utiliser pour résoudre la requête.

Un enregistrement DNS d'un FQDN comprend une valeur Time-to-Live (Durée de vie ; TTL), et, par défaut, le pare-feu actualise chaque FQDN dans son cache en fonction de la TTL individuelle fournie pour chaque serveur DNS, tant que la TTL est supérieure ou égale à la Fréquence d'actualisation minimale du FQDN que vous configurez sur le pare-feu ou au paramètre par défaut, soit 30 secondes, si vous ne configurez pas de minimum. L'actualisation du FQDN en fonction de sa valeur de TTL s'avère particulièrement utile pour sécuriser l'accès aux services de la plateforme cloud, qui, bien souvent, exigent des actualisations fréquentes du FQDN pour garantir la haute disponibilité des services. Par exemple, les environnements dans le cloud qui prennent en charge la mise à l'échelle automatique dépendent des résolutions des FQDN pour élargir ou réduire les services, et la rapidité des résolutions des FQDN est essentielle dans des environnements où les délais revêtent une si grande importance.

En configurant une fréquence d'actualisation FQDN minimale, vous limitez la plus petite valeur de TTL que le pare-feu respecte. Si vos adresses IP ne changent pas fréquemment, vous pourrez souhaiter définir une fréquence d'actualisation FQDN minimale plus élevée afin d'éviter que le pare-feu n'actualise inutilement des entrées. Le pare-feu utilise la valeur la plus élevée entre le TTL du DNES et la fréquence d'actualisation FQDN minimale configurée.

Par exemple, deux FQDN ont les valeurs TTL suivantes. La fréquence d'actualisation FQDN minimale remplace les valeurs TTL les plus faibles (les plus rapides).

	TTL	Si l'actualisation minimale du FQDN = 26	Fréquence d'actualisation réelle
FQDN A	20		26
FQDN B	30		30

 ©2024 Palo Alto Networks, Inc.

La minuterie d'actualisation du FQDN commence lorsque le pare-feu reçoit une réponse DNS d'un serveur DNS ou d'un objet de proxy DNS qui résout le FQDN.

Vous pouvez également définir un délai de temporisation des entrées obsolètes pour configurer la durée de temps pendant laquelle le pare-feu continu d'utiliser des résolutions de FQDN obsolètes (expirées) dans l'éventualité où le serveur DNS est indisponible. À l'issue de la période d'expiration des entrées obsolètes, si le serveur DNS demeure indisponible, les entrées FQDN obsolètes deviennent non résolues (le pare-feu supprime les entrées FQDN qui sont obsolètes).

À partir de PAN-OS 11.2.1 et des versions ultérieures, vous pouvez utiliser des DNS chiffrés pour le proxy DNS. Vous pouvez également utiliser des DNS chiffrés pour l'interface de gestion, que l'interface de gestion se connecte aux serveurs DNS ou qu'elle utilise un proxy DNS. Le DNS chiffré augmente la confidentialité et la sécurité des utilisateurs pour le trafic DNS entre un client et un serveur en empêchant les attaques par hôte interposé. Un DNS chiffré se produit entre ces périphériques :

- Pour l'interface de gestion, le DNS chiffré se produit entre le pare-feu et le serveur DNS.
- Pour le proxy DNS, vous pouvez configurer un DNS chiffré dans les deux sens ; vous spécifiez un ou plusieurs types de DNS chiffrés que le pare-feu acceptera du client DNS, et vous spécifiez un seul type de DNS chiffré que le pare-feu utilisera avec le serveur DNS.

Le pare-feu prend en charge deux types de chiffrement DNS : DNS sur HTTPS (DoH) et DNS sur TLS (DoT). Vous avez la possibilité que le pare-feu revienne sur le DNS traditionnel (cleartext) si le serveur DNS rejette le DNS chiffré ou expire (ne reçoit aucune réponse du serveur DNS principal ou secondaire dans la période d'expiration TCP configurée). Lorsque le DNS chiffré est configuré pour une interface, cette interface ne doit pas héberger d'autre trafic sur les ports TCP 443 ou 853.

Les tâches du pare-feu suivantes sont liées à DNS :

- Configurez au moins un serveur DNS sur votre pare-feu pour lui permettre de résoudre les noms d'hôte. Configurez des serveurs DNS principaux et secondaires ou un objet de proxy DNS qui précise ces serveurs, comme illustré dans le Cas pratique 1 : Le pare-feu exige une résolution DNS.
- (PAN-OS 11.2.1 et versions ultérieures) Configurez les DNS chiffrés pour l'interface de gestion, comme indiqué dans Perform Initial Configuration (Exécuter la configuration initiale).
- Configuration d'un objet proxy DNS.
- (PAN-OS 11.2.1 et versions ultérieures) Configurez le DNS chiffré pour un DNS Proxy Object (Objet de proxy DNS)..
- Personnalisez la manière dont le pare-feu traite la résolution DNS initiée par des règles de politique de sécurité, des rapports et des services services de gestion (par exemple, e-mail, Kerberos, SNMP, Syslog, etc.) pour chaque système virtuel, comme illustré dans le Cas pratique 2 : Le locataire de l'ISP utilise un proxy DNS pour traiter la résolution DNS pour des politiques de sécurité, la génération de rapports et des services de son système virtuel.
- Configurez le pare-feu pour qu'il agisse en tant que serveur DNS d'un client, comme illustré dans le Cas pratique 3 : Le pare-feu sert de proxy DNS entre le client et le serveur.
- Configurez un profil antispyware pour l'utilisation de requêtes DNS pour identifier des hôtes infectés sur le réseau.
- Procédez à l'activation des signatures d'évasion, puis activez les signatures d'évasion pour la prévention des menaces.

 ©2024 Palo Alto Networks, Inc.

- Procédez à la configuration d'une interface en tant que serveur DHCP. Le pare-feu pourra alors servir de serveur DHCP et envoyer des informations DNS à ses clients DHCP. Les clients DHCP dimensionnés peuvent ainsi joindre leurs serveurs DNS respectifs.

 ©2024 Palo Alto Networks, Inc.

Objet proxy DNS

Lorsqu'il est configuré en tant que proxy DNS, le pare-feu est un intermédiaire entre les clients et les serveurs DNS ; il agit comme un serveur DNS en résolvant les requêtes de son cache du proxy DNS. S'il ne trouve pas le nom de domaine dans le cache du proxy DNS, le pare-feu recherche une correspondance avec le nom de domaine parmi les entrées dans l'objet proxy DNS spécifique (l'interface sur laquelle la requête DNS est arrivée). Le pare-feu transmet la requête vers le serveur DNS qui est approprié en fonction des résultats correspondants. S'il n'y a aucune correspondance, le pare-feu utilise les serveurs DNS par défaut.

Un objet proxy DNS vous permet de configurer les paramètres qui déterminent comment le pare-feu fonctionne comme un proxy DNS. Vous pouvez affecter un objet proxy DNS à un seul système virtuel ou il peut être partagé entre tous les systèmes virtuels.

- Si l'objet proxy DNS est affecté à un système virtuel, vous pouvez spécifier un DNS Server Profile (profil de serveur DNS), qui indique les adresses des serveurs DNS principal et secondaire, ainsi que d'autres informations. Le profil de serveur DNS simplifie la configuration.
- Si l'objet proxy DNS est partagé, vous devez indiquer au minimum l'adresse principale d'un serveur DNS.

> *Lorsque vous configurez plusieurs locataires (abonnés d'ISP) avec des services DNS, un proxy DNS propre doit être défini sur chaque locataire, qui préserve la séparation du service DNS du locataire des services d'autres locataires.*

Dans l'objet proxy, vous spécifiez les interfaces pour lesquelles le pare-feu sert de proxy DNS. Le proxy DNS de l'interface n'utilise pas l'itinéraire de service ; les réponses aux requêtes DNS sont toujours envoyées à l'interface associée au routeur virtuel sur laquelle la requête DNS est arrivée.

Lorsque vous procédez à la Configuration d'un objet proxy DNS, vous pouvez associer des mappages FQDN/adresse statiques au proxy DNS. Vous pouvez également créer des règles de proxy DNS qui déterminent le serveur DNS vers lequel les demandes de nom de domaine (qui correspondent aux règles de proxy) sont dirigées. Vous pouvez configurer jusqu'à un maximum de 256 objets proxys DNS sur un pare-feu. Vous devez activer **Cache** et **Cache EDNS Responses (Réponses EDNS Cache)** (sous **Network [Réseau]** > **DNS Proxy [Proxy DNS]** > **Advanced [Avancé]**) si cet objet de proxy DNS est affecté à **Device (Périphérique)** > **Setup (Configuration)** > **Services** > **DNS** ou à **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)** > **vsys** > **General (Général)** > **DNS Proxy (Proxy DNS)**. De plus, si les **DNS proxy rules (règles de proxy DNS)** sont configurées pour cet objet proxy DNS, le cache doit également être activé pour ces règles (**Turn on caching of domains resolved by this mapping [Activer la mise en cache des domaines résolus par ce mappage]**).

Lorsque le pare-feu reçoit une requête FQDN (et que le nom de domaine ne se trouve pas dans le cache du proxy DNS), le pare-feu compare le nom de domaine de la requête FQDN aux noms de domaine des règles de proxy DNS de l'objet de proxy DNS. Si vous indiquez plusieurs noms de domaine dans une seule règle de proxy DNS, une requête correspond à la règle dès qu'elle correspond à n'importe lequel des noms de domaine qui y figure. Mise en correspondance de la règle de proxy DNS et du FQDNdécrit la manière dont le pare-feu déterminer si un FQDN correspond à un nom de domaine qui se trouve dans une règle de proxy DNS. Une requête DNS qui correspond à une règle est envoyée au serveur DNS principal configuré pour l'objet de proxy afin d'être résolue.

 ©2024 Palo Alto Networks, Inc.

DNS Server Profile (profil de serveur DNS)

Pour simplifier la configuration d'un système virtuel, un profil de serveur DNS vous permet de préciser le système virtuel configuré, une source de l'héritage ou les adresses IP principale et secondaire des serveurs DNS, ainsi qu'une interface source et une adresse source (itinéraire de service) qui seront utilisées dans les paquets envoyés au serveur DNS. L'interface source détermine le routeur virtuel, qui comporte une table de routage. L'adresse IP de destination est recherchée dans la table de routage du routeur virtuel auquel l'interface source est affectée. Il est possible que le résultat de l'interface de sortie IP de destination soit différent de celui de l'interface source. Le paquet devrait provenir de l'interface de sortie IP de destination déterminée par la recherche de la table de routage, mais l'adresse IP source pourrait être l'adresse configurée. L'adresse source est utilisée comme adresse de destination dans la réponse du serveur DNS.

Le rapport du système virtuel et le profil de serveur du système virtuel envoient leurs demandes au serveur DNS spécifié pour le système virtuel (si applicable). (Le serveur DNS utilisé est défini dans **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)** > **General (Général)** > **DNS Proxy (Proxy DNS)**.) Si aucun serveur DNS n'est spécifié pour le système virtuel, le serveur DNS spécifié pour le pare-feu est interrogé.

Vous procédez à la Configuration d'un profil de serveur DNS pour un système virtuel uniquement, et non pour un emplacement Shared (Partagé) global.

 ©2024 Palo Alto Networks, Inc.

Déploiements DNS à plusieurs locataires

Le pare-feu détermine comment traiter les requêtes DNS en fonction de l'origine de la requête. Un environnement dans lequel un fournisseur de services Internet a plusieurs locataires sur un pare-feu est appelé hébergement multiclient. Trois cas pratiques pour les déploiements DNS à plusieurs locataires sont disponibles :

- **Résolution DNS de gestion globale** : le pare-feu a besoin d'une résolution DNS pour lui-même, par exemple, lorsque la requête provient du plan de gestion pour résoudre un FQDN pour un événement de gestion tel qu'un service de mise à jour logicielle. Le pare-feu utilise la route de service pour accéder à un serveur DNS car la requête DNS ne parvient pas sur un routeur virtuel spécifique.
- **Résolution FQDN de politique et de rapport pour un système virtuel** : pour les requêtes DNS provenant d'une stratégie de sécurité, d'un rapport ou d'un service, vous pouvez spécifier un ensemble de serveurs DNS spécifique au système virtuel (locataire) ou spécifier les serveurs DNS globaux par défaut. Si votre cas d'utilisation nécessite un ensemble différent de serveurs DNS par système virtuel, vous devez configurer un objet proxy DNS. La résolution est spécifique au système virtuel auquel le proxy DNS est affecté. Si vous ne disposez pas de serveurs DNS spécifiques applicables à ce système virtuel, le pare-feu utilise les paramètres DNS globaux.
- **Résolution DNS de plan de données pour un système virtuel** : cette méthode est également appelée Requête réseau de résolution DNS. Le système virtuel du locataire peut être configuré de sorte que des noms de domaines spécifiés soient résolus sur le serveur DNS du locataire de son réseau. Cette méthode prend en charge la *segmentation DNS*, à savoir que le locataire peut également utiliser ses propres serveurs DNS d'ISP pour les requêtes DNS non résolues sur son propre serveur. Les règles d'objet proxy DNS contrôlent la segmentation DNS ; le domaine du locataire redirige les requêtes DNS vers ses serveurs DNS, qui sont configurés dans un profil de serveur DNS. Le profil de serveur DNS inclut des serveurs DNS principal et secondaire désignés, ainsi que des itinéraires de service DNS pour IPv4 et IPv6, qui remplacent les paramètres DNS par défaut.

Le tableau suivant récapitule les types de résolution DNS. L'emplacement de liaison détermine l'objet proxy DNS utilisé pour la résolution. À titre d'illustration, les cas pratiques montrent comment un fournisseur de services peut configurer des paramètres DNS pour fournir des services DNS de résolution de requêtes DNS nécessaires sur le pare-feu et pour les systèmes virtuels du locataire (abonné).

Type de résolution	Emplacement : Partagé	Emplacement : Vsys spécifique
Résolution DNS du pare-feu, effectuée par le plan de gestion	Liaison : Globale Illustrée dans le Cas pratique 1	S. O.
Résolution du profil de sécurité, de la génération de rapports et du profil de serveur, effectuée par le plan de gestion	Liaison : Globale Même comportement que le Cas pratique 1	Liaison : Vsys spécifique Illustrée dans le Cas pratique 2

 ©2024 Palo Alto Networks, Inc.

Type de résolution	Emplacement : Partagé	Emplacement : Vsys spécifique
Résolution de proxy DNS pour des hôtes clients DNS connectés à l'interface sur le pare-feu, passant par le pare-feu en direction d'un serveur DNS, effectuée par le plan de données	Liaison : Interface Itinéraire de service : Interface et adresse IP sur lesquelles la requête DNS a été reçue. Illustrée dans le Cas pratique 3	

- Cas pratique 1 : Le pare-feu exige une résolution DNS
- Cas pratique 2 : Le locataire de l'ISP utilise un proxy DNS pour traiter la résolution DNS pour des politiques de sécurité, la génération de rapports et des services de son système virtuel
- Cas d'utilisation 3 : Le pare-feu sert de proxy DNS entre le client et le serveur

©2024 Palo Alto Networks, Inc.

Configuration d'un objet proxy DNS

Si votre pare-feu doit servir de proxy DNS, effectuez cette tâche pour configurer un objet proxy DNS. L'objet proxy peut être partagé entre tous les systèmes virtuels ou appliqué à un système virtuel spécifique.

Lorsque le pare-feu est autorisé à servir de proxy DNS, les signatures d'évasion qui ont détecté des requêtes HTTPS ou TLS fabriquées peuvent envoyer une alerte pour informer des instances sur lesquelles un client se connecte à un domaine qui ne correspond pas aux domaines indiqués dans la requête DNS d'origine. Il est recommandé de procéder à l'activation des signatures d'évasion après avoir configuré le proxy DNS pour qu'il déclenche une alerte si des requêtes fabriques sont détectées.

STEP 1 | Configurez les paramètres de base d'un objet proxy DNS.

1. Sélectionnez **Network (Réseau)** > **DNS Proxy (Proxy DNS)** et cliquez sur **Add (Ajouter)** pour ajouter un nouvel objet.
2. Vérifiez que **Enable (Activer)** est sélectionné.
3. Saisissez un **Name (Nom)** pour l'objet.
4. Pour **Location (Emplacement)**, sélectionnez le système virtuel auquel l'objet s'applique. Si vous sélectionnez **Shared (Partagé)**, vous devez spécifier au minimum une adresse de serveur DNS **Primary (Principal)**, et éventuellement une adresse **Secondary (Secondaire)**.
5. Si vous avez sélectionné un système virtuel, pour **Server Profile (Profil de serveur)**, sélectionnez un profil de serveur DNS ou cliquez sur **DNS Server Profile (Profil de serveur DNS)** pour configurer un nouveau profil. Reportez-vous à la section Configuration d'un profil de serveur DNS.
6. Sous Inheritance Source (Source de l'héritage), sélectionnez une source de laquelle hériter des paramètres du serveur DNS par défaut. La valeur par défaut est **None (Aucun)**.
7. Pour **Interface (Interface)**, cliquez sur **Add (Ajouter)** et spécifiez les interfaces auxquelles l'objet proxy DNS s'applique.
   - Si vous utilisez l'objet proxy DNS pour effectuer des recherches DNS, une interface est requise. Le pare-feu écoutera les requêtes DNS sur cette interface, puis les transmettra en tant que proxy.
   - Si vous utilisez l'objet proxy DNS pour un itinéraire de service, l'interface est facultative.

STEP 2 | (Facultatif) Spécifiez des règles de proxy DNS.

1. Dans l'onglet **DNS Proxy Rules (Règles de proxy DNS)**, cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** pour la règle.
2. Cochez **Turn on caching of domains resolved by this mapping (Activer la mise en cache des domaines résolus par ce mappage)** si vous souhaitez que le pare-feu mette en cache les domaines résolus.
3. Sous **Domain Name (Nom de domaine)**, **Add (Ajoutez)** au moins un domaine, en indiquant une entrée par ligne, auquel le pare-feu compare les requêtes FQDN. Si une requête est mise en correspondance avec l'un des domaines de la règle, celle-ci est

 ©2024 Palo Alto Networks, Inc.

envoyée aux fins de résolution à l'un des serveurs suivants (selon les configurations effectuées à l'étape précédente) :

- Le serveur DNS **Primary (Principal)** ou **Secondary (Secondaire)** directement indiqué pour cet objet proxy.
- Le serveur DNS **Primary (Principal)** ou **Secondary (Secondaire)** indiqué dans le profil de serveur DNS de cet objet proxy.

La mise en correspondance de la règle de proxy DNS et du FQDN décrit comment le pare-feu met en correspondance les noms de domaine d'un FQDN avec une règle de proxy DNS. Si aucune correspondance n'est trouvée, la requête est résolue par les serveurs DNS définis par défaut.

4. Procédez de l'une des manières suivantes, selon la configuration de **Location (Emplacement)** :
   - Si vous avez choisi un système virtuel, sélectionnez un **DNS Server profile (Profil de serveur DNS)**.
   - Si vous avez choisi **Shared (Partagé)**, saisissez une adresse **Primary (Principale)** et, éventuellement, une adresse **Secondary (Secondaire)**.
5. Cliquez sur **OK**.

STEP 3 | (Facultatif) Associez des entrées FQDN/adresse statiques au proxy DNS. Les entrées DNS statiques permettent au pare-feu de résoudre le FQDN en adresse IP sans envoyer de requête au serveur DNS.

1. Dans l'onglet **Static Entries (Entrées statiques)**, **Add (Ajoutez)** un **Name (Nom)**.
2. Saisissez le Fully Qualified Domain Name (nom de domaine complet ; FQDN) (**FQDN (FQDN)**).
3. Pour **Address (Adresse)**, **Add (Ajoutez) l'adresse IP** à laquelle le FQDN doit être mappé.

   Vous pouvez fournir des adresses IP supplémentaires pour une entrée. Le pare-feu fournit toutes les adresses IP dans sa réponse DNS, et le client choisit l'adresse à utiliser.
4. Cliquez sur **OK**.

STEP 4 | (PAN-OS 11.2.1 et versions ultérieures) (Facultatif) Configurez le proxy DNS pour accepter les requêtes DNS chiffrées des clients DNS et envoyer des requêtes DNS chiffrées aux serveurs DNS.

1. Dans l'onglet **Encrypted DNS (DNS chiffré)**, cliquez sur **Enable Encrypted DNS (Activer DNS chiffré)**.

   *Si **Enable Encrypted DNS (Activer DNS chiffré)** n'est pas sélectionné, le proxy DNS envoie des requêtes DNS en texte en clair aux serveurs DNS, que la requête DNS client soit chiffrée ou non.*
2. Pour les paramètres du serveur, sélectionnez un **Connection Type (Type de connexion)** que le pare-feu (proxy DNS) utilisera pour communiquer avec les serveurs DNS :
   - **DoH** : DNS sur HTTPS (Hypertext Transfer Protocol Secure). DoH utilise le port 443. Lorsque le DNS chiffré est activé et que DoH est le type de connexion :
     - Une adresse DNS principale est requise et le proxy DNS envoie toutes les requêtes DNS au serveur DNS principal à l'aide de DoH. Si aucune réponse n'arrive du

 ©2024 Palo Alto Networks, Inc.

serveur DNS principal, le proxy DNS envoie des requêtes DoH au serveur DNS secondaire.

- Aucun autre service HTTPS n'est autorisé sur l'interface faisant office de proxy DNS.
- Une politique de décryptage SSL doit être configurée du client DNS au serveur DNS afin que le proxy DNS puisse décrypter le trafic DoH.

- **DoT** : DNS sur TLS (Transport Layer Security). DoT utilise le port 853, qui est dédié au trafic DoT. Lorsque le DNS chiffré est activé et que DoT est le type de connexion :
  - Une adresse DNS principale est requise et le proxy DNS envoie toutes les requêtes DNS au serveur DNS principal à l'aide de DoT. Si aucune réponse n'arrive du serveur DNS principal, le proxy DNS envoie des requêtes DoT au serveur DNS secondaire.
  - Aucun autre service TLS n'est autorisé sur l'interface faisant office de proxy DNS.
- **Origin** : le proxy DNS envoie toutes les requêtes DNS au serveur DNS principal en utilisant le même type DNS que celui reçu du client. Une adresse DNS principale est requise. Si le proxy DNS ne reçoit aucune réponse DNS du serveur DNS principal pendant la période d'expiration TCP, le proxy DNS envoie la requête DNS au serveur DNS secondaire.
- **Cleartext** : trafic DNS simple et non chiffré.

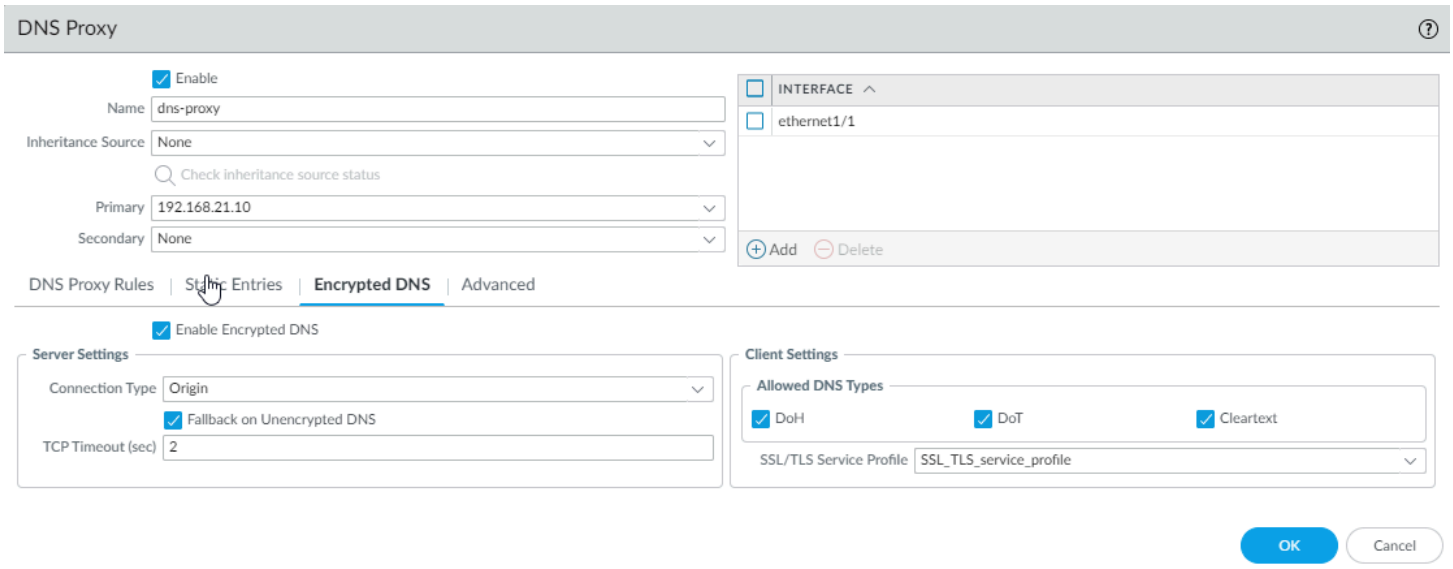
3. Sélectionnez **Fallback on Unencrypted DNS (Retour au DNS non chiffré)** pour que le proxy DNS revienne au DNS traditionnel (texte en clair) si le serveur DNS rejette le DNS chiffré ou expire (le proxy DNS ne reçoit aucune réponse du type de connexion configuré [DoH ou DoT] du serveur DNS principal ou secondaire pendant la période d'expiration TCP configurée).
4. Entrez le **TCP Timeout (sec) (Délai d'expiration TCP (sec))** en secondes, la durée pendant laquelle le serveur DNS principal doit répondre avant que la requête DNS n'aille au serveur DNS secondaire, et la durée pendant laquelle le serveur DNS secondaire doit répondre avant que la requête DNS ne revienne dans les communications DNS en texte en clair ; la plage va de 1 à 10 ; la valeur par défaut est de 1 seconde.

 ©2024 Palo Alto Networks, Inc.

5. Pour les paramètres client, sélectionnez un ou plusieurs **Allowed DNS Types (Types DNS autorisés)** que le proxy DNS acceptera du client :
   - **DoH** : le proxy DNS doit décrypter le trafic DoH et le proxy DNS comme spécifié pour les paramètres du serveur :
     - Si Origin est le paramètre de serveur, le proxy DNS envoie des requêtes DNS en tant que DoH.
     - Si DoH est le paramètre de serveur, le proxy DNS envoie des requêtes DNS en tant que DoH.
     - Si DoT est le paramètre de serveur, le proxy DNS envoie des requêtes DNS en tant que DoT.
   - **DoT** : le proxy DNS doit décrypter le trafic DoT et le proxy DNS comme spécifié pour les paramètres du serveur :
     - Si Origin est le paramètre du serveur, le proxy DNS envoie des requêtes DNS en tant que DoT.
     - Si DoH est le paramètre de serveur, le proxy DNS envoie des requêtes DNS en tant que DoH.
     - Si DoT est le paramètre de serveur, le proxy DNS envoie des requêtes DNS en tant que DoT.
   - **Cleartext** : le proxy DNS doit mettre en proxy les requêtes DNS comme spécifié pour les paramètres du serveur :
     - Si Origin est le paramètre de serveur, le proxy DNS envoie des requêtes DNS en tant que texte en clair.
     - Si DoH est le paramètre de serveur, le proxy DNS envoie des requêtes DNS en tant que DoH.
     - Si DoT est le paramètre de serveur, le proxy DNS envoie des requêtes DNS en tant que DoT.

     Si le texte en clair est désactivé pour les paramètres client, le proxy DNS ignore ou supprime le trafic en texte en clair.
6. Sélectionnez un **SSL/TLS Service Profile (Profil de service SSL/TLS)** ou créez un nouveau profil de service SSL/TLS à utiliser pour le chiffrement DNS entre le client et le proxy DNS, ou sélectionnez **None (Aucun)**.
7. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.



STEP 5 | Activez la mise en cache et configurez d'autres paramètres avancés pour le proxy DNS.

1. À l'onglet **Advanced (Avancé)**, cochez **TCP Queries (Requêtes TCP)** pour activer des requêtes DNS à l'aide de TCP.
   - **Max Pending Requests (Nombre max. de demandes en attente)** : saisissez le nombre maximum de requêtes DNS TCP en attente simultanées que le pare-feu va prendre en charge (plage de 256 à 64, par défaut 64).
2. Pour **UDP Queries Retries (Tentatives de requêtes UDP)**, saisissez les informations suivantes :
   - **Interval (sec) (Intervalle (sec))** : la durée (en secondes) au bout de laquelle une autre requête est envoyée en l'absence de réponse (intervalle compris entre 1 et 30 ; valeur par défaut : 2).
   - **Attempts (Tentatives)** : le nombre maximum de tentatives de requêtes UDP (hormis la première) après lesquelles le serveur DNS suivant est interrogé (plage de 1 à 30, par défaut 5).
3. Sélectionnez **Cache (Cache)** pour permettre au pare-feu de mettre en cache les mappages FQDN/adresse dont il prend connaissance. Vous devez activer la fonction **Cache** (activée par défaut) si cet objet proxy DNS est utilisé pour des requêtes que le pare-feu génère (c'est-à-dire dans la section **Device [Périphérique]** > **Setup [Configuration]** > **Services** > **DNS**, ou dans la section **Device [Périphérique]** > **Virtual Systems [Systèmes virtuels]** et vous sélectionnez un système virtuel et ensuite **General [Général]** > **DNS Proxy [Proxy DNS]**).
   - Sélectionnez **Enable TTL (Activer TTL)** pour restreindre la durée pendant laquelle le pare-feu met en cache les entrées de résolution DNS pour l'objet proxy. Cette option est désactivée par défaut.
     - Saisissez la **Time to Live (sec) (Durée de vie (sec.))**, soit le nombre de secondes au bout desquelles toutes les entrées de l'objet proxy mises en cache sont supprimées. Une fois les entrées supprimées, de nouvelles requêtes DNS doivent être résolues et remises en cache. Plage comprise entre 60 et 86 400. Il n'y a pas

 ©2024 Palo Alto Networks, Inc.

de TTL par défaut ; les entrées restent jusqu'à ce que le pare-feu n'ait plus de mémoire cache.

- **Cache EDNS Responses (Réponses EDNS Cache)** : Vous devez activer ce paramètre si cet objet proxy DNS est utilisé pour des requêtes que le pare-feu génère (dans la section **Device [Périphérique]** > **Setup [Configuration]** > **Services** > **DNS**, ou dans la section **Device [Périphérique]** > **Virtual Systems [Systèmes virtuels]**, puis vous sélectionnez un système virtuel et ensuite **General [Général]** > **DNS Proxy [Proxy DNS]**).

STEP 6 | Validez vos modifications.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

Configuration d'un profil de serveur DNS

Configurez un profil de serveur DNS, ce qui simplifiera la configuration d'un système virtuel. L'adresse **Primary DNS (DNS principal)** ou **Secondary DNS (DNS secondaire)** est utilisée pour créer la requête DNS que le système virtuel envoie au serveur DNS.

STEP 1 | Donnez un nom au profil de serveur DNS, sélectionnez le système virtuel auquel il s'applique, et spécifiez les adresses des serveurs DNS principal et secondaire.

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **DNS (DNS)** et **Add (Ajoutez)** un **Name (Nom)** pour le profil de serveur DNS.
2. Pour **Location (Emplacement)**, sélectionnez le système virtuel auquel le profil s'applique.
3. Pour **Inheritance Source (Source de l'héritage)**, sélectionnez **None (Aucune)** si les adresses du serveur DNS ne sont pas héritées. Sinon, précisez le serveur DNS duquel le profil doit hériter des paramètres. Si vous choisissez un serveur DNS, cliquez sur **Check inheritance source status (Vérifier l'état de la source de l'héritage)** pour afficher ces informations.
4. Indiquez l'adresse IP du serveur **Primary DNS (DNS principal)**, ou conservez la valeur **inherited (hérité)** si vous avez choisi une **Inheritance Source (Source de l'héritage)**.

   *N'oubliez pas que si vous spécifiez un FQDN au lieu d'une adresse IP, le DNS de ce FQDN est résolu dans **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)** > **DNS Proxy (Proxy DNS)**.*
5. Indiquez l'adresse IP du serveur **Secondary DNS (DNS secondaire)**, ou conservez la valeur **inherited (Hérité)** si vous avez choisi une **Inheritance Source (Source de l'héritage)**.

STEP 2 | Configurez l'itinéraire de service que le pare-feu utilise automatiquement, en fonction du type de famille d'adresses IP IPv4 ou IPv6 du serveur DNS cible.

1. Cliquez sur **Service Route IPv4 (IPv4 de l'itinéraire de service)** pour autoriser l'utilisation de l'interface et de l'adresse IPv4 suivantes en tant qu'itinéraire de service, si l'adresse DNS cible est une adresse IPv4.
2. Spécifiez la **Source Interface (Interface source)** pour sélectionner l'adresse IP source du serveur DNS qui sera utilisée par l'itinéraire de service. Le pare-feu détermine le routeur virtuel associé à l'interface, puis recherche un itinéraire dans la table de routage du routeur virtuel pour atteindre le réseau de destination (en fonction de l'adresse **Primary DNS (DNS principal)**).
3. Indiquez la **Source Address (Adresse source)** IPv4 de laquelle les paquets destinés au serveur DNS proviennent.
4. Cliquez sur **Service Route IPv6 (IPv6 de l'itinéraire de service)** pour autoriser l'utilisation de l'interface et de l'adresse IPv6 suivantes en tant qu'itinéraire de service, si l'adresse DNS cible est une adresse IPv6.
5. Spécifiez la **Source Interface (Interface source)** pour sélectionner l'adresse IP source du serveur DNS qui sera utilisée par l'itinéraire de service. Le pare-feu détermine le routeur virtuel associé à l'interface, puis recherche un itinéraire dans la table de routage du routeur virtuel pour atteindre le réseau de destination (en fonction de l'adresse **Primary DNS (DNS principal)**).

 ©2024 Palo Alto Networks, Inc.

6. Indiquez la **Source Address (Adresse source)** IPv6 de laquelle les paquets destinés au serveur DNS proviennent.
7. Cliquez sur **OK**.

STEP 3 | Commit (Validez) la configuration.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

Configurer un proxy Web

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré dans le cloud) • NGFW (géré par PAN-OS ou Panorama)	❑ Licence proxy Web ❑ (Pour les NGFW gérés dans le cloud) Licence AIOps for NGFW Premium.

Si votre réseau utilise un périphérique proxy pour la sécurité, vous pouvez désormais bénéficier du même niveau de protection en utilisant la capacité de proxy Web sur site avec PAN-OS 11.0. Les fonctionnalités de proxy web permettent des options supplémentaires pour migrer d'une architecture proxy web existante vers une console de gestion unifiée simple. L'utilisation de la fonctionnalité proxy Web avec Prisma Access fournit une méthode transparente pour migrer, déployer et maintenir des configurations de passerelle Web sécurisée (SWG) à partir d'une interface simple d'utilisation et simplifiée. Web proxy vous aide pendant la transition entre le cloud et le cloud sans perte de sécurité ou d'efficacité.

Le proxy web supporte deux méthodes pour acheminer le trafic:

- Pour la méthode proxy explicite, la requête contient l'adresse IP de destination du proxy configuré et le navigateur client envoie directement les requêtes au proxy. Vous pouvez utiliser l'une des méthodes suivantes pour authentifier les utilisateurs avec le proxy explicite:
  - Kerberos, qui nécessite une licence proxy web.
  - SAML 2.0, qui nécessite Panorama, une licence Prisma Access, le plugin Cloud Services 3.2.1 (et versions ultérieures) et la licence proxy web complémentaire.
  - Cloud Identity Engine, qui nécessite Panorama, une licence Prisma Access, le plugin Cloud Services 3.2.1 (et versions ultérieures) et la licence proxy web complémentaire.
- Pour la méthode du proxy transparent, la requête contient l'adresse IP de destination du serveur web et le proxy intercepte de manière transparente la requête client (soit en étant en ligne, soit par pilotage du trafic). Il n'y a pas de configuration client et Panorama est facultatif. Le proxy transparent nécessite une interface de bouclage, une configuration User-ID dans la zone proxy et des règles DNAT (Destination NAT) spécifiques. Le proxy transparent ne prend pas en charge X-Authenticated Users (XAU) ou Web Cache Communications Protocol (WCCP).

Vous pouvez également utiliser le routage avancé avec un proxy Web.

Les produits suivants supportent le proxy web:

- Pare-feu PA-1400 Series
- Pare-feu de la série PA-3400
- Pare-feu de la série PA-5400 (sauf PA-5450)
- Pare-feu VM-Series (avec un minimum de quatre vCPU)
- Systèmes de gestion de panorama exécutant PAN-OS 11.1

Pour configurer explicit proxy (proxy explicite) à l'aide de SAML authentication (authentification SAML), web proxy nécessite le plugin Cloud Services 3.2.1 ou une version ultérieure.

 ©2024 Palo Alto Networks, Inc.

Web proxy prend en charge IPv4.

Pour savoir comment configurer un proxy Web, sélectionnez le type de proxy ou la fonctionnalité de proxy que vous souhaitez configurer :

- Configurer le proxy explicite
- Configurer le proxy transparent
- Configurer l'authentification pour le proxy Web explicite
- Configurer des exemptions pour l'authentification de proxy explicite

Configurer le proxy explicite

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré dans le cloud) • NGFW (géré par PAN-OS ou Panorama)	☐ Licence proxy Web ☐ (Pour les NGFW gérés dans le cloud) Licence AIOps for NGFW Premium.

Un proxy explicite est l'un des types de proxy Web que vous pouvez configurer sur vos pare-feu. Le proxy Web vous permet d'exploiter les mêmes fonctionnalités qu'un périphérique proxy tout en fournissant une interface simple et unifiée à partir de laquelle gérer le proxy.

La méthode proxy explicite en particulier vous permet de résoudre les problèmes plus facilement, car le navigateur client est conscient de l'existence du proxy.

- PAN-OS
- Cloud Management

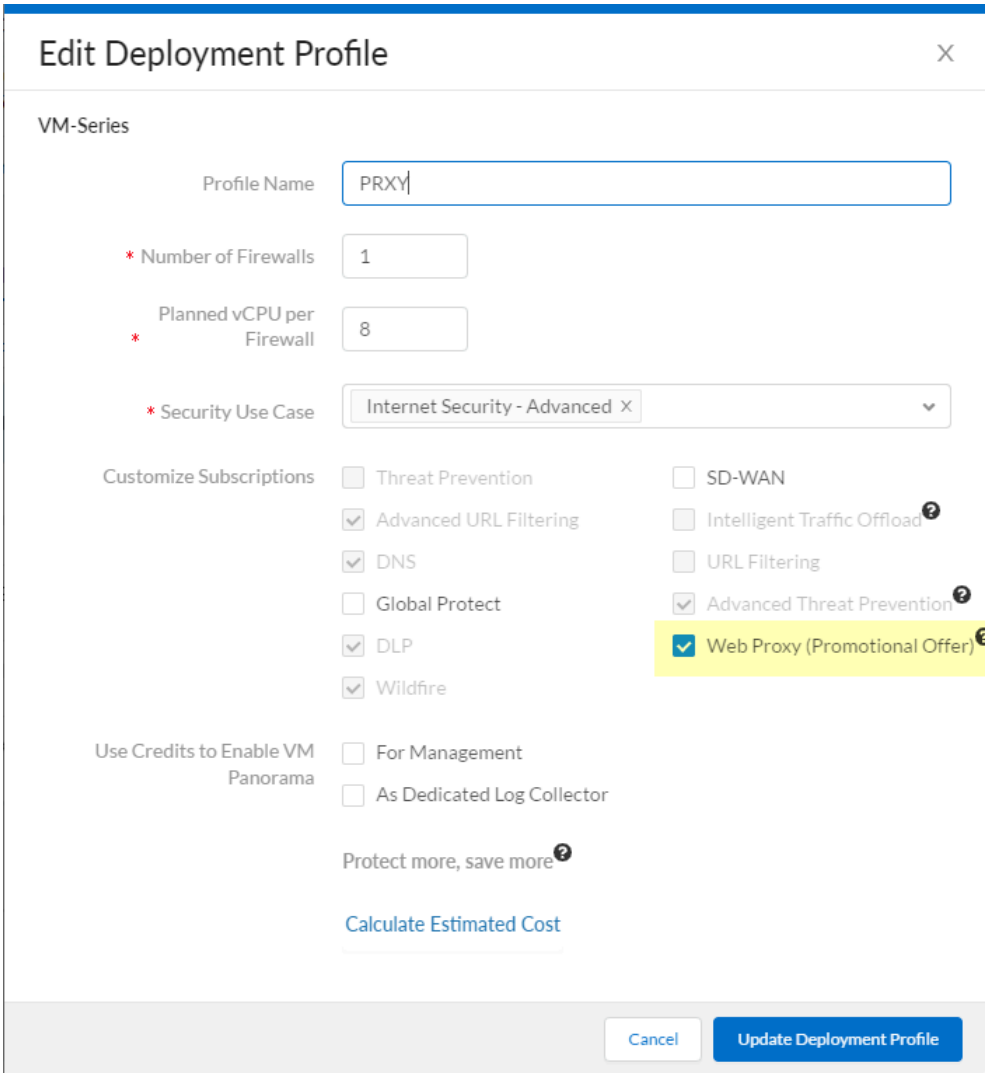
PAN-OS

©2024 Palo Alto Networks, Inc.

STEP 1 | (VM Series only (Série de machines virtuelles uniquement)) Si vous ne l'avez pas déjà fait, activez la licence pour le proxy Web.

Vous devez activer la licence de proxy Web pour les séries PA-1400, PA-3400 et VM. Découvrez comment activate your subscription licenses (activer vos licences d'abonnement) pour les séries PA-1400 et PA-3400 ou activer la licence proxy Web pour la série VM à l'étape suivante.

1. Connectez-vous au portail de service clientèle (CSP).
2. **Edit (Modifiez)** le deployment profile (profil de déploiement).
3. Sélectionnez **Web Proxy (Promotional Offer) (Proxy Web (offre promotionnelle)).**



4. Cliquez sur **Update Deployment Profile (Mettre à jour le profil de déploiement)**.
5. Sur le pare-feu, récupérez les license keys (clés de licence) du serveur.

Si la récupération de la clé de licence échoue, redémarrez le pare-feu et répétez cette étape avant de continuer.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configurez les interfaces et les zones nécessaires.

Il est recommandé d'utiliser la couche 3 (L3) pour les trois interfaces utilisées par le proxy Web et de configurer une zone distincte pour chaque interface au sein des mêmes routeurs virtuels et des mêmes systèmes virtuels.

1. Configurez une interface pour le trafic client.

   *Veillez à copier soigneusement l'adresse IP de cette interface et à l'enregistrer dans un emplacement sécurisé, car vous devez l'entrer en tant qu'adresse **Proxy IP** lorsque vous configurez le proxy Web.*
2. Configurez une interface pour le trafic sortant vers Internet.
3. Configurez une interface de bouclage pour le proxy.

   Tout le trafic entrant est acheminé via cette interface vers le proxy.

STEP 3 | Configurez le proxy DNS pour le proxy explicite.

1. Configurez un DNS proxy object (objet proxy DNS) pour la connexion proxy.
2. Configurez un DNS Server profile (profil de serveur DNS) avec des serveurs DNS principaux et secondaires.

   Vous devez configurer un serveur DNS principal et un serveur DNS secondaire pour le proxy Web.
3. Spécifiez l'interface de la connexion proxy.

   Spécifiez l'interface d'entrée de trafic ou une interface de loopback (bouclage).

STEP 4 | Pour activer le déchiffrement pour la détection MITM, créez un self-signed root CA certificate (certificat d'autorité de certification racine auto-signé) ou importez un certificat signé par votre autorité de certification d'entreprise. Pour plus d'informations, reportez-vous aux best practices for administrative access (bonnes pratiques en matière d'accès administratif).

STEP 5 | Assurez-vous d'avoir effectué les étapes préalables au déploiement de la méthode d'authentification que vous souhaitez configurer.

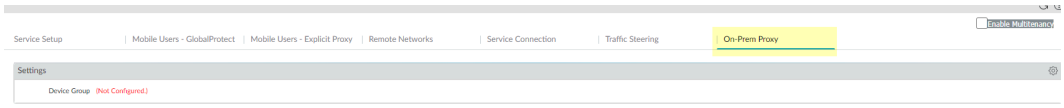
- Configurer l'authentification Kerberos
- Configuration de l'authentification SAML
- Configurer l'authentification Cloud Identity Engine

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Si vous disposez d'un abonnement de sécurité DNS, intégrez le pare-feu du proxy Web au proxy explicite pour récupérer toutes les demandes correspondant aux catégories de sécurité DNS que vous spécifiez.

1. Sélectionnez **Panorama** > **Cloud Services (Services Cloud)** > **Configuration** > **On-Prem Proxy (Proxy sur site)**.
2. **Modifiez** les paramètres, puis sélectionnez le **Device Group (groupe d'appareils)** que le pare-feu du proxy Web doit utiliser ou **Add (Ajouter)** un nouveau groupe d'appareils.

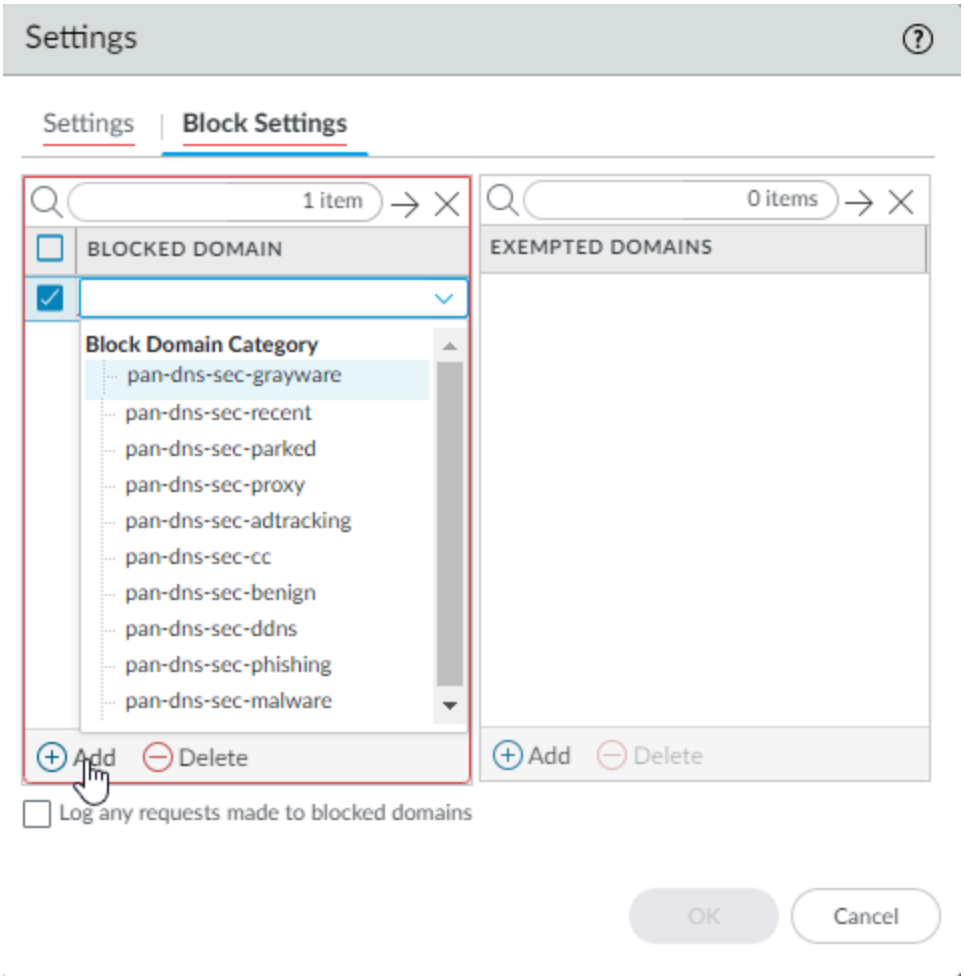
   Pour intégrer le pare-feu de proxy Web à Prisma Access, vous devez configurer le pare-feu de proxy Web dans un groupe de périphériques distinct qui ne contient aucun autre pare-feu ou système virtuel. Si le pare-feu est déjà membre d'un groupe d'appareils, créez un groupe d'appareils enfant en tant que sous-groupe et déplacez le pare-feu vers le groupe d'appareils enfants.



3. (Facultatif) Sélectionnez **Block settings (Bloquer les paramètres)** pour **Add (ajouter)** un **Blocked Domain (domaine bloqué)** ou tous domaines qui sont des **Exempted Domains**

 ©2024 Palo Alto Networks, Inc.

(domaines exemptés) parce qu'ils sont en entonnoir en raison de la correspondance d'une ou plusieurs catégories de sécurité DNS.



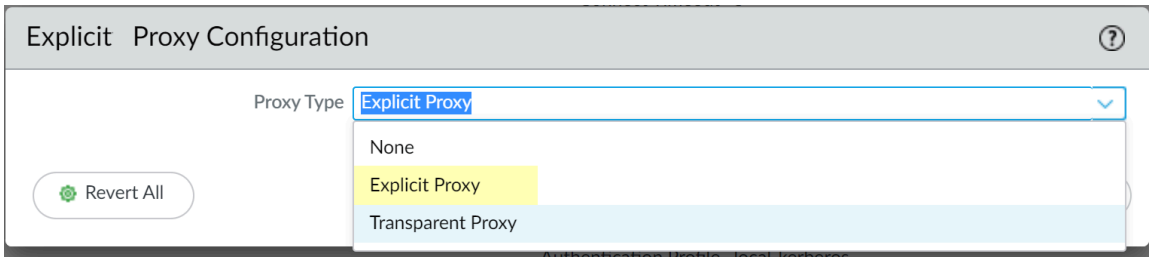
4. (Facultatif) Indiquez si vous souhaitez **Log any requests made to blocked domains (consigner toutes les demandes adressées aux domaines bloqués)**.
5. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

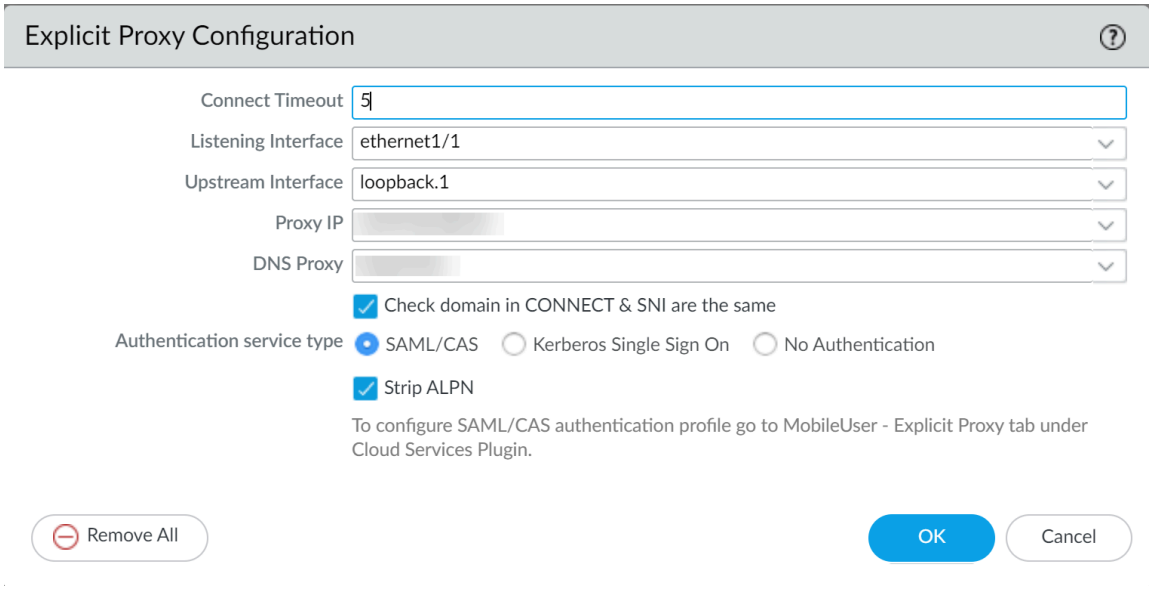
STEP 7 | Configurez le proxy explicite.

1. Sur le pare-feu, sélectionnez **Network (Réseau)** > **Proxy** puis **Edit (Modifier)** les paramètres **Proxy Enablement (Activation proxy)**.
2. Sélectionnez **Explicit Proxy (proxy explicite)** comme **Proxy Type (type de proxy)**, puis cliquez sur **OK** pour confirmer les modifications.

   Si la seule option disponible est Aucune, vérifiez que vous disposez d'une licence active pour la fonctionnalité de proxy Web.



3. **Edit (Modifiez)** la **Explicit Proxy Configuration (Configuration de proxy explicite)**.



4. Spécifiez le **Connect Timeout (délai d'expiration de connexion)** pour définir (en secondes) combien de temps le proxy attend une réponse du serveur Web. S'il n'y a pas de réponse après l'expiration du délai spécifié, le proxy ferme la connexion.
5. Sélectionnez **Listening Interface (interface d'écoute)** qui contient le pare-feu dans lequel vous souhaitez activer le proxy Web.

   Spécifiez l'interface d'entrée pour le trafic client.

 ©2024 Palo Alto Networks, Inc.

6. Sélectionnez **Upstream Interface (interface en amont)** qui contient l'interface avec le proxy Web qui redirige le trafic vers le serveur.

   *Si vous utilisez une interface de bouclage, spécifiez cette interface comme **Upstream Interface (interface en amont)**.*

7. Spécifiez l'adresse IP de l'interface d'écoute en tant qu'adresse **IP proxy**.

   Saisissez l'adresse IP de l'interface que vous avez créée lors d'une étape précédente.

8. Spécifiez l'objet **DNS Proxy (Proxy DNS)** que vous avez créé lors d'une étape précédente.
9. Sélectionnez **Check domain in CONNECT & SNI are the same (Vérifier le domaine dans CONNECT et SNI sont identiques)** pour empêcher les attaques frontales de domaine en spécifiant des domaines différents entre la requête CONNECT et le champ Indication de nom de serveur (SNI) dans l'en-tête HTTP.
10. Sélectionnez le **Authentication service type (type de service d'authentification)** que vous souhaitez utiliser (soit **SAML/CAS**ou **Kerberos Single Sign On (authentification unique Kerberos)**).

    Veillez à effectuer toutes les étapes de prédéploiement et de configuration nécessaires pour la méthode d'authentification que vous sélectionnez. Sélectionnez une seule des méthodes d'authentification suivantes :

    - Configurer l'authentification Kerberos
    - Configuration de l'authentification SAML
    - Configurer l'authentification Cloud Identity Engine

11. Cliquez sur **OK** pour confirmer les modifications.

STEP 8 | Configurez les règles de stratégie de sécurité nécessaires pour déchiffrer le trafic et rediriger le trafic applicable vers le proxy.

Vous devrez créer les types de règles suivants :

- Source NAT (le cas échéant)
- Decryption (déchiffrage)
- Security (Sécurité)

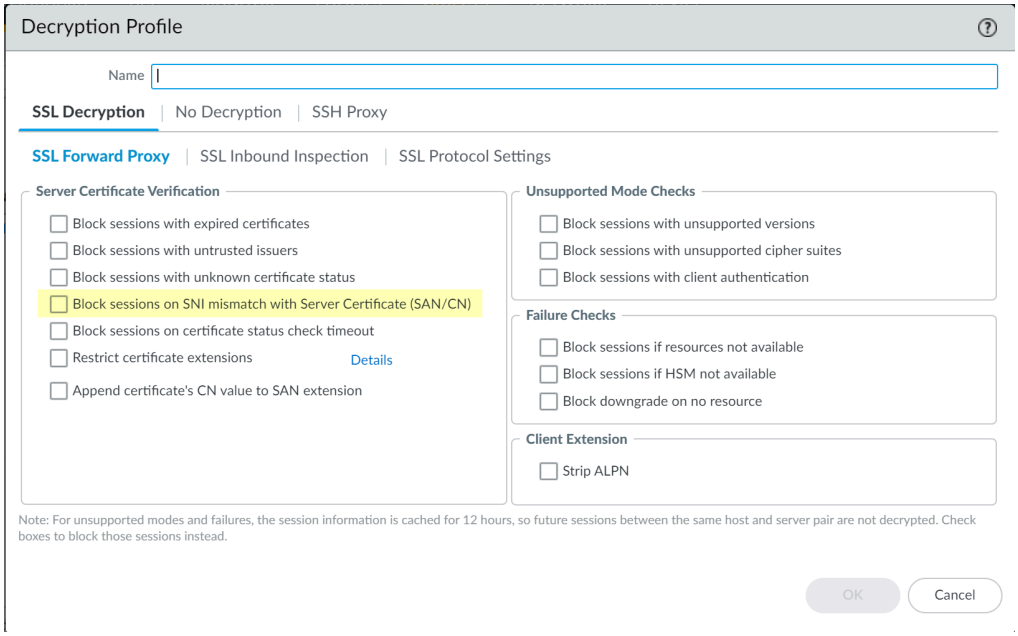
1. Configurez une stratégie de déchiffrement pour decrypt (déchiffrer) le trafic afin qu'il puisse être redirigé si nécessaire.

   Pour éviter de déchiffrer le trafic deux fois, sélectionnez la zone qui contient l'interface en amont comme zone source pour la stratégie de déchiffrement.

2. (Facultatif mais recommandé) Sélectionnez **Objects (Objets)** > **Decryption Profile (Profil de déchiffrage)** et sélectionnez **Block sessions on SNI mismatch with Server Certificate (SAN/CN) (Bloquer les sessions en cas de non-concordance SNI avec le certificat de**

 ©2024 Palo Alto Networks, Inc.

serveur (SAN/CN))pour refuser automatiquement toutes les sessions où l'indication de nom de serveur (SNI) ne correspond pas au certificat de serveur.



3. Configurez les règles de stratégie de sécurité nécessaires.
   - Créez une règle de stratégie de sécurité pour autoriser le trafic du client vers l'interface que vous avez sélectionnée comme interface d'écoute.
   - Configurez une règle de stratégie de sécurité pour autoriser le trafic de la zone qui contient l'interface en amont vers Internet.
   - Configurez une règle de stratégie de sécurité pour autoriser le trafic de la zone proxy DNS vers Internet.
4. Configurez une règle de politique de sécurité à l'aide du profil d'authentification que vous avez configuré lors d'une étape précédente pour acheminer le trafic vers le proxy, le cas échéant.
5. S'il s'agit de votre configuration initiale de proxy Web transparent, apportez une modification à votre configuration de proxy (**Network (Réseau)** > **DNS Proxy (Proxy DNS)**) et à la configuration de votre interface (**Network (Réseau)** > **Interfaces**), puis **Commit (Validez)** vos modifications pour vous assurer que la configuration du proxy Web transparent est correctement renseignée sur le pare-feu.

Cloud Management

Le proxy Web explicite pour Strata Cloud Manager n'est pris en charge qu'avec la pile de routeurs héritée. Si vous souhaitez que cela soit activé, veuillez contacter l'équipe de votre compte.

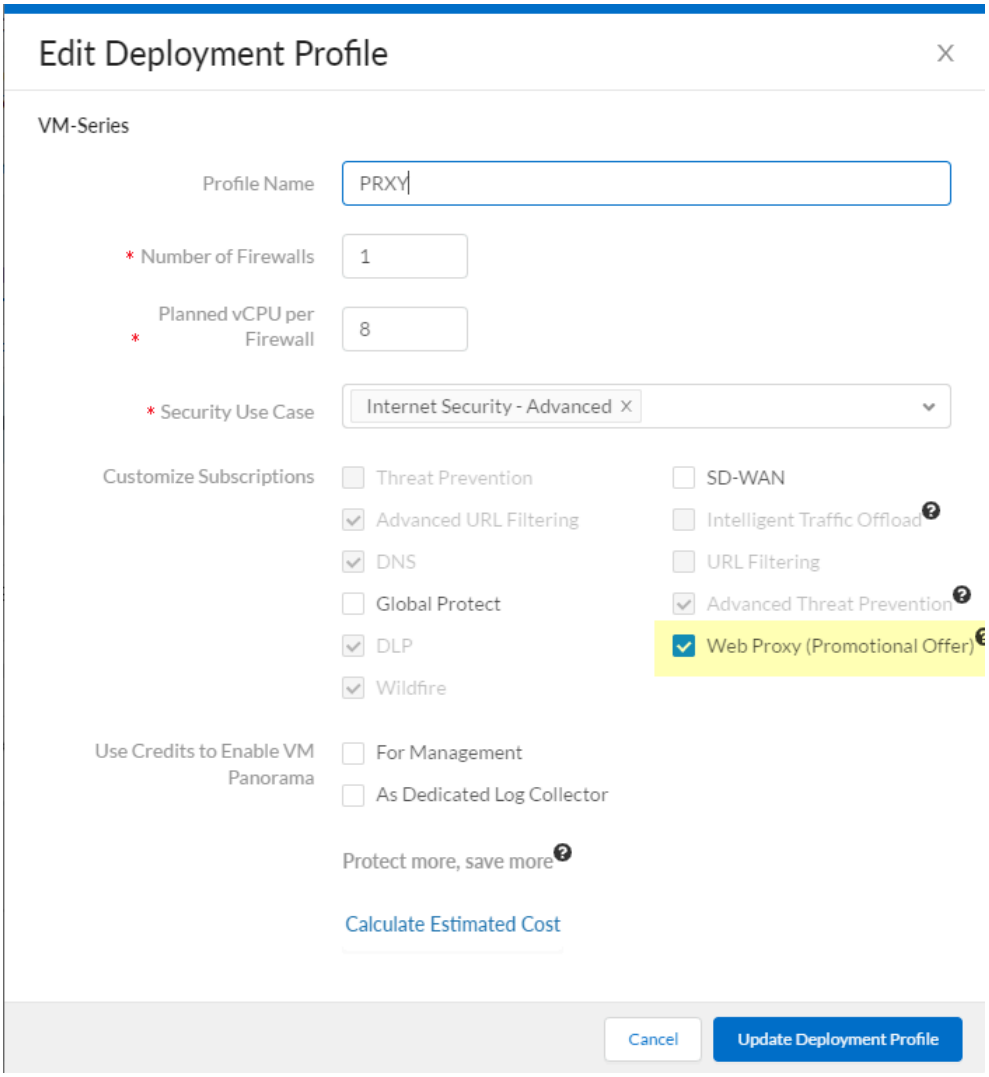
Vous pouvez configurer un proxy Web explicite sur les pare-feu gérés dans le cloud à l'aide de Strata Cloud Manager.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | (VM Series only (Série de machines virtuelles uniquement)) Si vous ne l'avez pas déjà fait, activez la licence pour le proxy Web.

Vous devez activer la licence de proxy Web pour les séries PA-1400, PA-3400 et VM. Découvrez comment activate your subscription licenses (activer vos licences d'abonnement) pour les séries PA-1400 et PA-3400 ou activer la licence proxy Web pour la série VM à l'étape suivante.

1. Connectez-vous au portail de service clientèle (CSP).
2. **Edit (Modifiez)** le deployment profile (profil de déploiement).
3. Sélectionnez **Web Proxy (Promotional Offer) (Proxy Web (offre promotionnelle)).**



4. Cliquez sur **Update Deployment Profile (Mettre à jour le profil de déploiement)**.
5. Sur le pare-feu, récupérez les license keys (clés de licence) du serveur.

Si la récupération de la clé de licence échoue, redémarrez le pare-feu et répétez cette étape avant de continuer.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configurez les interfaces et les zones nécessaires.

*Ne modifiez pas la zone **proxy**.*

Il est recommandé d'utiliser la couche 3 (L3) pour les trois interfaces utilisées par le proxy Web et de configurer une zone distincte pour chaque interface au sein des mêmes routeurs virtuels et des mêmes systèmes virtuels.

1. Configurez une interface pour le trafic client.

   *Veillez à copier soigneusement l'adresse IP de cette interface et à l'enregistrer dans un emplacement sécurisé, car vous devez l'entrer en tant qu'adresse **Proxy IP** lorsque vous configurez le proxy Web.*
2. Configurez une interface pour le trafic sortant vers Internet.
3. (Facultatif) Configurez une interface en boucle pour le proxy.

   Strata Cloud Manager crée automatiquement une interface en boucle. N'en configurez une que si vous souhaitez utiliser une autre interface en boucle.

   Tout le trafic entrant est acheminé via cette interface vers le proxy.

STEP 3 | Pour activer le déchiffrement pour la détection MITM, créez un self-signed root CA certificate (certificat d'autorité de certification racine auto-signé) ou importez un certificat signé par votre autorité de certification d'entreprise. Pour plus d'informations, reportez-vous aux best practices for administrative access (bonnes pratiques en matière d'accès administratif).

STEP 4 | Assurez-vous d'avoir effectué les étapes préalables au déploiement de la méthode d'authentification que vous souhaitez configurer.

- Si vous utilisez SAML, vous devez avoir configuré Explicit Proxy for Mobile Users (Proxy explicite pour les utilisateurs mobiles).
- Si vous utilisez Kerberos, vous devez avoir terminé les exigences préalables au déploiement pour Kerberos.

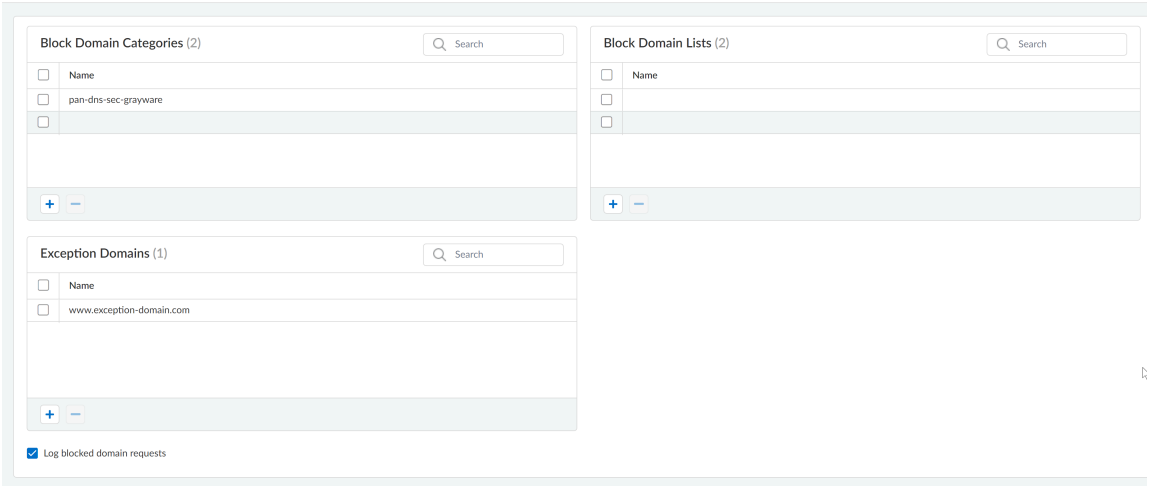
STEP 5 | Si vous disposez d'un abonnement de sécurité DNS, intégrez le pare-feu du proxy Web au proxy explicite pour récupérer toutes les demandes correspondant aux catégories de sécurité DNS que vous spécifiez.

1. Dans Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (Accès NGSW et Prisma)** > **Device Settings (Paramètres de périphérique)** > **Proxy** > **Block Domains (Bloquer domaines)** > **Customize (¨Personnaliser)**.
2. (Facultatif)Ajoutez **Block Domain Categories (Bloquer catégories de domaines)**, **Block Domain Lists (Bloquer listes de domaines)** ou tout domaine **Exception Domains**

 ©2024 Palo Alto Networks, Inc.

(Domaines d'exception), car ils sont mis en entonnoir en raison de la correspondance d'une ou plusieurs catégories de sécurité DNS.

Block Domains

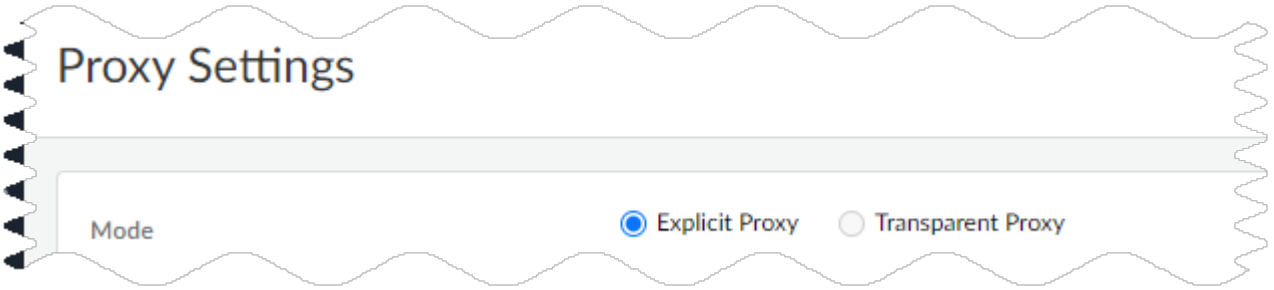


3. (Facultatif) Sélectionnez si vous souhaitez **Log blocked domain requests (Consigner les demandes de domaine bloquées)**.
4. **Save (Enregistrez)** vos sélections.

©2024 Palo Alto Networks, Inc.

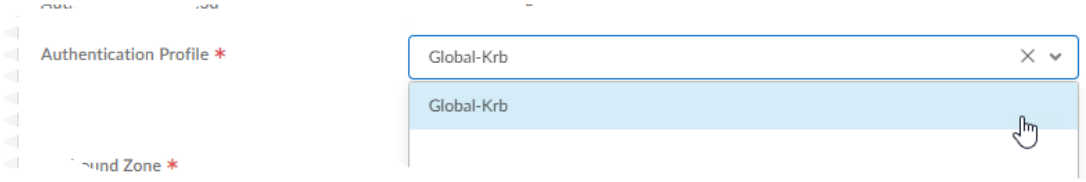
STEP 6 | Configurez le proxy explicite.

1. Dans Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (Accès NGSW et Prisma)** > **Device Settings (Paramètres du périphérique)** > **Configuration Scope (Étendue de la configuration)**.
2. Sélectionnez le dossier ou l'extrait pour lequel vous souhaitez configurer un proxy explicite.
3. Sélectionnez **Device Settings (Paramètres du périphérique)** > **Proxy** > **Proxy Settings (Paramètres du proxy)** > **Customize (Personnaliser)**.
4. Sélectionnez **Explicit Proxy (Proxy explicite)** comme **Mode**.



5. Sélectionnez la **Authentication Method (Méthode d'authentification)** que vous souhaitez utiliser (soit **Kerberos Single Sign On (Authentification unique Kerberos)**, soit **SAML/CAS**).

   Veillez à effectuer toutes les étapes de prédéploiement et de configuration nécessaires pour la méthode d'authentification que vous sélectionnez.
6. Si vous avez sélectionné **Kerberos Single Sign On (Authentification unique Kerberos)**, spécifiez le **Authentication Profile (Profil d'authentification)** que vous avez créé lors de la configuration de Kerberos.



7. Spécifiez la **Client Facing Interface (Interface côté client)**.

   Il s'agit de l'interface pour le trafic client que vous avez configurée lors d'une étape précédente.
8. Spécifiez une **Outbound Zone (Zone sortante)** pour le trafic sortant vers Internet.

   Vous pouvez **Create New (Créer nouveau)** si vous n'avez pas déjà configuré de zone sortante.
9. Spécifiez les adresses IP des serveurs DNS principal et secondaire auxquels vous souhaitez vous connecter.
10. Spécifiez l'interface de la connexion proxy DNS.
11. (Facultatif) Spécifiez le **Connect Timeout (Délai d'expiration de connexion)** pour définir (en secondes) combien de temps le proxy attend une réponse du serveur Web. S'il n'y a

©2024 Palo Alto Networks, Inc.

pas de réponse après l'expiration du délai spécifié, le proxy ferme la connexion. La valeur par défaut est 5 secondes.

12. (Facultatif) Spécifiez le **Web Traffic Service Port (Port du service de trafic Web)** si vous souhaitez que le trafic Web utilise des ports spéciaux. Les ports par défaut sont 80 et 443.
13. (Facultatif) Spécifiez l'interface de bouclage du proxy que vous avez configurée à l'étape précédente.
14. (Facultatif) En cas de besoin commercial légitime, désélectionnez **Reset if SNI does not match HTTP CONNECT (Réinitialiser si SNI ne correspond pas à HTTP CONNECT)**.

    Il est recommandé de laisser cette option activée pour éviter les attaques frontales de domaine en spécifiant des domaines différents entre la demande CONNECT et le champ SNI (Server Name Indication) dans l'en-tête HTTP.
15. Sélectionnez **Save (Sauvegarder)** pour confirmer les modifications.

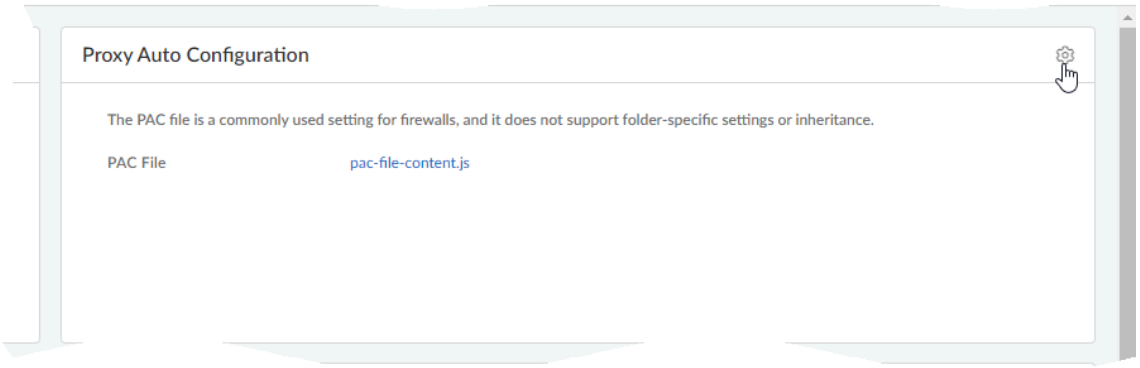
STEP 7 | Si cela s'applique à votre déploiement, créez une Source NAT policy rule (Règle de politique NAT source).

STEP 8 | Customize web access policies (Personnaliser les politiques d'accès Web) pour toute exception aux politiques par défaut dont vous pourriez avoir besoin.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | S'il s'agit de votre configuration initiale de proxy Web explicite, apportez une modification à votre fichier de configuration automatique de proxy (PAC).

1. Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (Accès NGSW et Prisma)** > **Device Settings (Paramètres de périphérique)** > **Proxy** > **Proxy Auto Configuration (Configuration automatique du proxy)**



2. Suivez les PAC file guidelines (Directives relatives aux fichiers PAC) afin d'apporter les modifications nécessaires au fichier PAC.

 ©2024 Palo Alto Networks, Inc.



3. Lorsque vous avez terminé d'apporter des modifications, **Save (Enregistrez)** le fichier.

Le fichier PAC s'applique à tous les pare-feu associés à votre locataire Strata Cloud Manager. Si vous avez besoin de fichiers PAC différents pour différents pare-feu, vous devrez télécharger manuellement un autre fichier PAC sur ces pare-feu.

 ©2024 Palo Alto Networks, Inc.

Configurer le proxy transparent

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré dans le cloud) • NGFW (géré par PAN-OS ou Panorama)	❑ Licence proxy Web ❑ (Pour les NGFW gérés dans le cloud) Licence AIOps for NGFW Premium.

Avec un proxy transparent, le navigateur client n'est pas au courant du proxy. Le proxy transparent prend en charge le déploiement en mode inline et ne prend pas en charge le protocole WCCP (Web cache communication protocol). Le proxy transparent est transparent pour l'utilisateur sans nécessiter d'authentification supplémentaire.

- PAN-OS
- Strata Cloud Manager

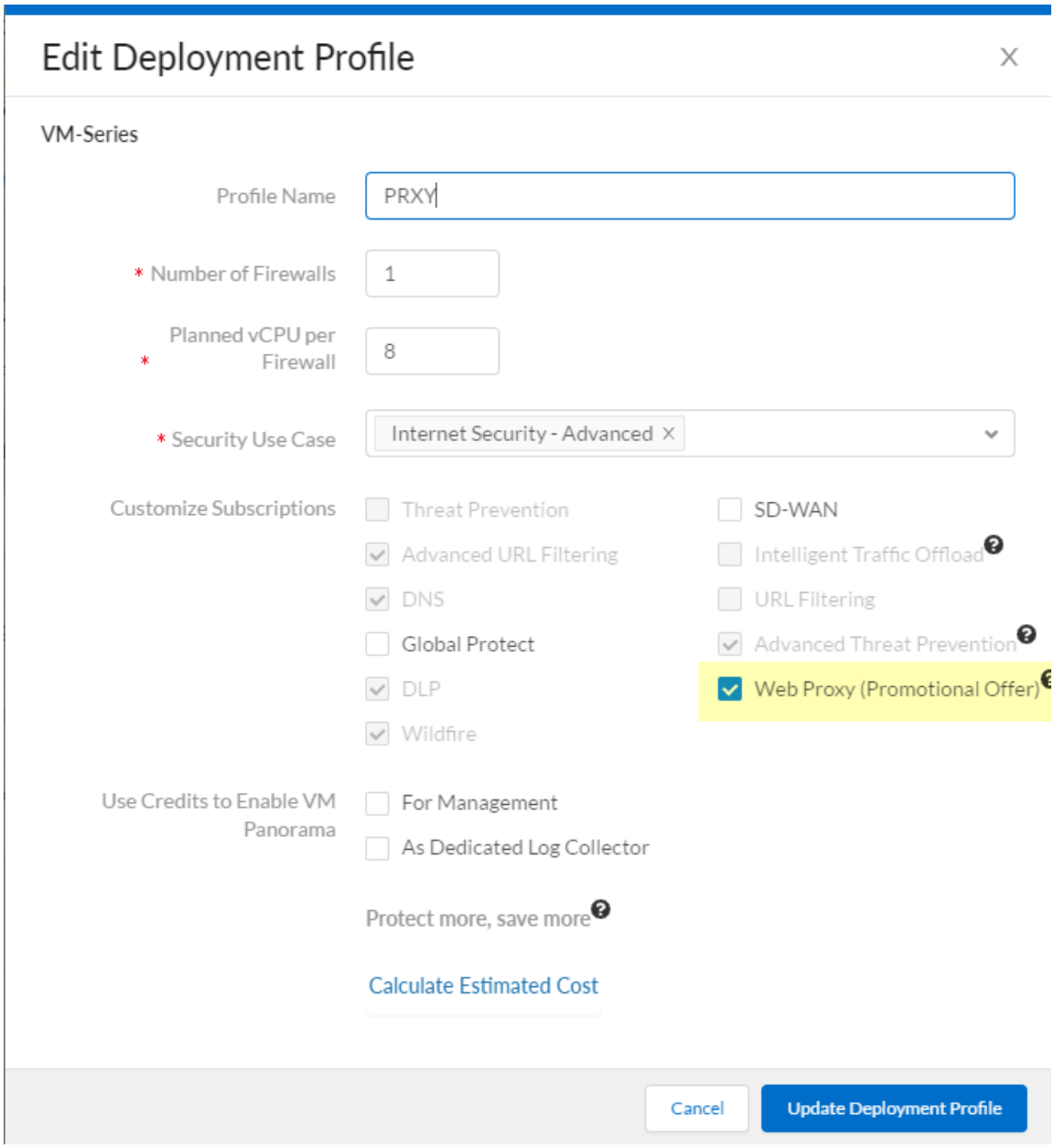
©2024 Palo Alto Networks, Inc.

PAN-OS

STEP 1 | (VM Series only (Série de machines virtuelles uniquement)) Si vous ne l'avez pas déjà fait, activez la licence pour le proxy Web.

Cette étape est requise pour les séries PA-1400, PA-3400 et VM. Les étapes suivantes concernent la série VM; pour le PA-1400 et le PA-3400, suivez les étapes pour activate subscription license (sactiver les licences d'abonnement).

1. Connectez-vous au portail de service clientèle (CSP).
2. **Edit (Modifiez)** le deployment profile (profil de déploiement).
3. Sélectionnez **Web Proxy (Promotional Offer) (Proxy Web (offre promotionnelle)).**



4. Cliquez sur **Update Deployment Profile (Mettre à jour le profil de déploiement).**

 ©2024 Palo Alto Networks, Inc.

5. Sur le pare-feu, récupérez les license keys (clés de licence) du serveur.

   Si la récupération de la clé de licence échoue, redémarrez le pare-feu et répétez cette étape avant de continuer.

STEP 2 | Mettre en place des zones et des interfaces.

Comme meilleure pratique, utilisez la couche 3 (L3) pour toutes les interfaces et configurez une zone distincte pour chaque interface au sein des mêmes routeurs virtuels et des mêmes systèmes virtuels.

1. Configurez une interface pour le client.
2. Configurez une interface pour le trafic sortant vers Internet.
3. Configurez une interface de bouclage pour le proxy.

   *Tout le trafic entrant est acheminé via cette interface vers le proxy. Veillez à copier soigneusement l'adresse IP de cette interface et à l'enregistrer dans un emplacement sécurisé, car vous devez l'entrer en tant qu'adresse **Proxy IP** lorsque vous configurez le proxy Web.*

STEP 3 | Configurez le proxy DNS pour Transparent Proxy.

1. Configurez un DNS proxy object (objet proxy DNS) pour la connexion proxy.
2. Configurez un DNS Server profile (profil de serveur DNS) avec des serveurs DNS principaux et secondaires.

   Vous devez configurer un serveur DNS principal et un serveur DNS secondaire pour le proxy Web.
3. Spécifiez l'interface de bouclage pour la connexion proxy.

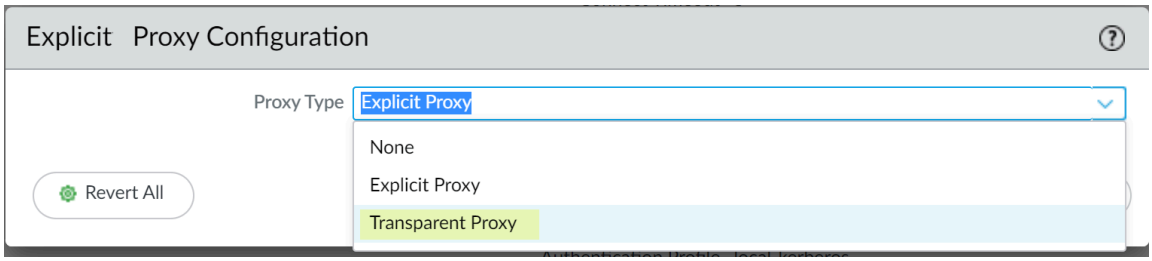
STEP 4 | Pour activer le déchiffrement pour la détection MITM, créez un self-signed root CA certificate (certificat d'autorité de certification racine auto-signé) ou importez un certificat signé par votre autorité de certification d'entreprise. Pour plus d'informations, reportez-vous aux best practices for administrative access (bonnes pratiques en matière d'accès administratif).

 ©2024 Palo Alto Networks, Inc.

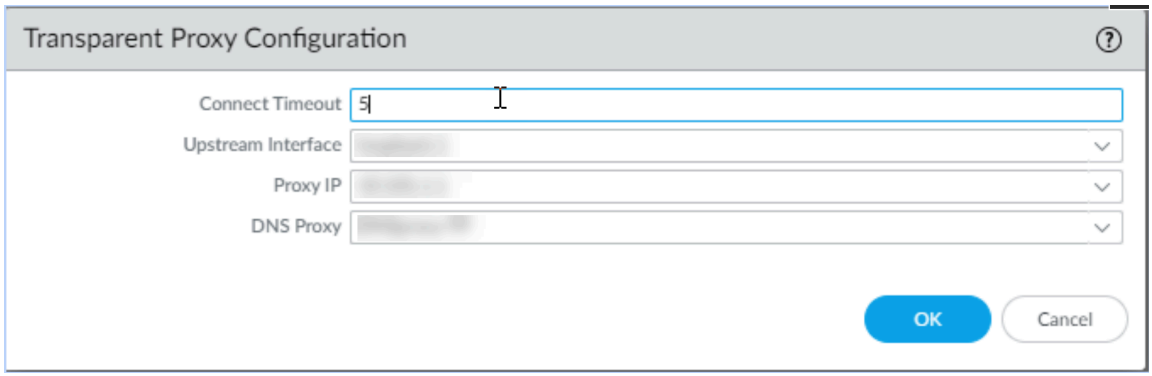
STEP 5 | Configurez le proxy transparent.

1. Sur le pare-feu, sélectionnez **Network (Réseau)** > **Proxy** puis **Edit (Modifier)** les paramètres **Proxy Enablement (Activation proxy)**.
2. Sélectionnez **Transparent Proxy (Proxy transparent)** comme **Proxy type (type de proxy)** puis cliquez sur **OK** pour confirmer les modifications.

   Si la seule option disponible est Aucune, vérifiez que vous disposez d'une licence active pour la fonctionnalité de proxy Web.



3. **Edit (Modifier)** the **Transparent Proxy Configuration (Configuration de proxy transparent)**.



4. Spécifiez le **Connect Timeout (délai de connexion)** pour définir (en secondes) combien de temps le proxy attend une réponse TCP du serveur Web. S'il n'y a pas de réponse après l'expiration du délai spécifié, le proxy ferme la connexion.
5. Sélectionnez **Upstream Interface (interface en amont)**.

   L'interface amont doit être une interface de bouclage qui n'est associée à aucun autre sous-réseau.
6. Spécifiez l'adresse IP de l'interface de bouclage en tant qu'**IP proxy**.

   Saisissez l'adresse IP de l'interface que vous avez configurée lors d'une étape précédente.
7. Spécifiez l'objet **DNS Proxy (Proxy DNS)** que vous avez créé lors d'une étape précédente.

 ©2024 Palo Alto Networks, Inc.

Spécifiez l'interface de bouclage comme ***Upstream Interface (interface en amont)****.*

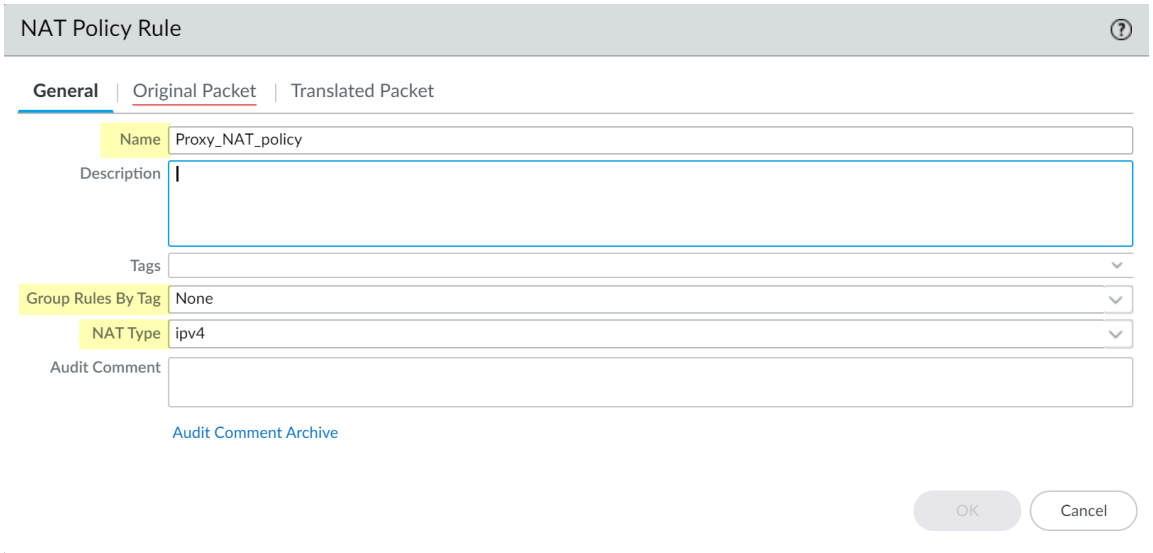
8. Cliquez sur **OK** pour confirmer les modifications.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Configurez la stratégie de traduction d'adresses réseau de destination (DNAT).

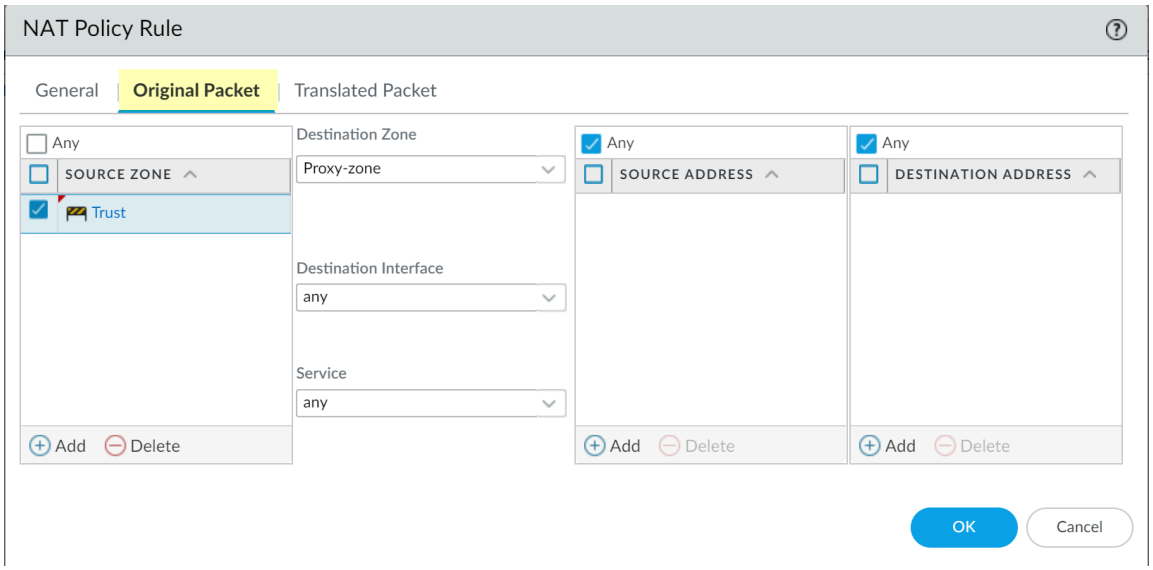
Vous devez configurer la règle de stratégie DNAT exactement comme décrit dans les étapes suivantes pour que le pare-feu puisse utiliser avec succès le proxy Web pour acheminer le trafic. Assurez-vous de configurer la règle de stratégie DNAT afin qu'elle précède la règle de stratégie de traduction d'adresses réseau source (SNAT).

1. Sélectionnez **Policies (Politiques)** > **NAT**, puis **Add (Ajoutez)** une règle de politique NAT.
2. Entrez un **Name (Nom)** unique et vérifiez que les **Group Rules (Règles de groupe)** sont **None (Aucunes)** puis sélectionnez le **NAT Type (Type NAT)**.

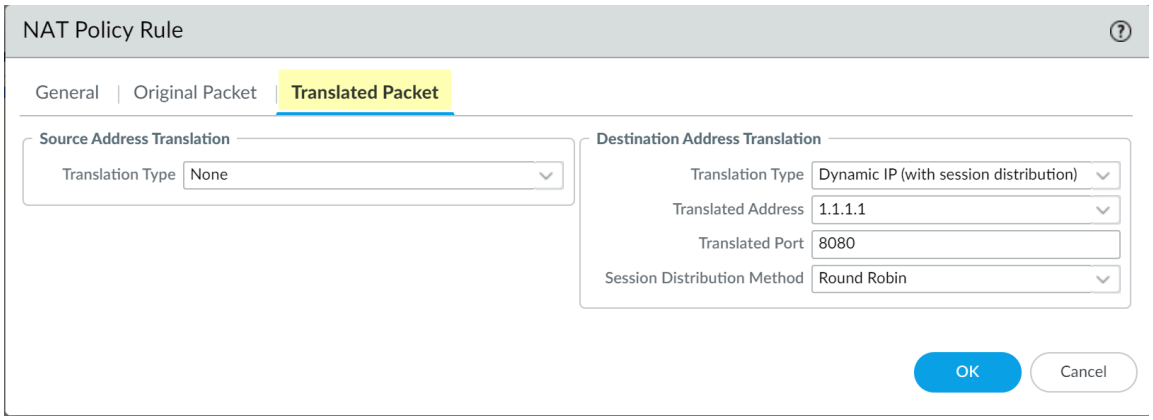


3. Sélectionnez **Original Packet (Paquet d'origine)** et **Add (Ajoutez)** une zone de confiance comme **source Zone (zone source)** et la **Destination Zone (zone de destination)** comme interface contenant le proxy Web.

 ©2024 Palo Alto Networks, Inc.



4. Sélectionnez **Translated Packet (Packet traduit)** et vérifiez que **Translation Type (type de traduction)**pour **Source Address Translation (Traduction de l'adresse source)** est **None (Aucun)**.



5. Sélectionnez **Dynamic IP (with session distribution) (IP dynamique (avec distribution de session))** comme **Translation Type (type de traduction)** pour la **Destination Address Translation (traduction d'adresse de destination)**.
6. Entrez l'adresse IP du proxy web comme **Translated Address (Adresse traduite)**.

   Entrez la même adresse IP que l'adresse IP du proxy spécifiée lors d'une étape précédente.
7. Entrez **`8080`** comme **Translated Port (port traduit)**.
8. Sélectionnez une **Session Distribution Method (méthode de distribution de la session)** (par exemple, **Round Robin**).

 ©2024 Palo Alto Networks, Inc.

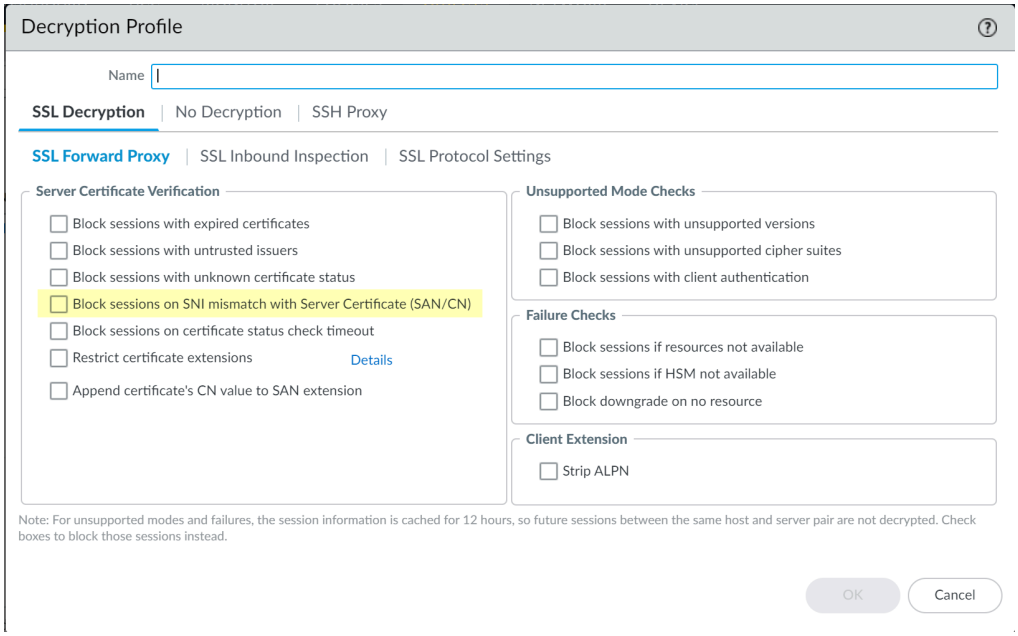
La méthode de distribution de session n'est pas applicable pour le proxy Web.

9. Cliquez sur **OK** et sur **Commit (Valider)** pour enregistrer les modifications.

STEP 7 | Configurez une stratégie de sécurité pour autoriser et acheminer le trafic proxy.

1. Configurez une règle de stratégie de traduction d'adresses réseau source (SNAT) après la règle DNAT.
2. Configurez une stratégie de déchiffrement pour decrypt (déchiffrer) le trafic.

   Sélectionnez la zone qui contient l'interface proxy comme zone source.
3. (Facultatif mais recommandé) Sélectionnez **Objects (Objets)** > **Decryption Profile (Profil de déchiffrage)** et sélectionnez **Block sessions on SNI mismatch with Server Certificate (SAN/CN) (Bloquer les sessions en cas de non-concordance SNI avec le certificat de serveur (SAN/CN))**pour refuser automatiquement toutes les sessions où l'indication de nom de serveur (SNI) ne correspond pas au certificat de serveur.



4. Configurez les règles de stratégie pour autoriser l'accès aux serveurs proxy DNS pour le client et le proxy.
5. Configurez une règle de stratégie pour autoriser le trafic du client vers le proxy.
6. Configurez une règle de stratégie pour autoriser le trafic du proxy vers Internet.

STEP 8 | S'il s'agit de votre configuration initiale de proxy Web transparent, apportez une modification à votre configuration de proxy (**Network (Réseau)** > **DNS Proxy (Proxy DNS)**) et à la configuration de votre interface (**Network (Réseau)** > **Interfaces**), puis **Commit (Validez)** vos modifications pour vous assurer que la configuration du proxy Web transparent est correctement renseignée sur le pare-feu.

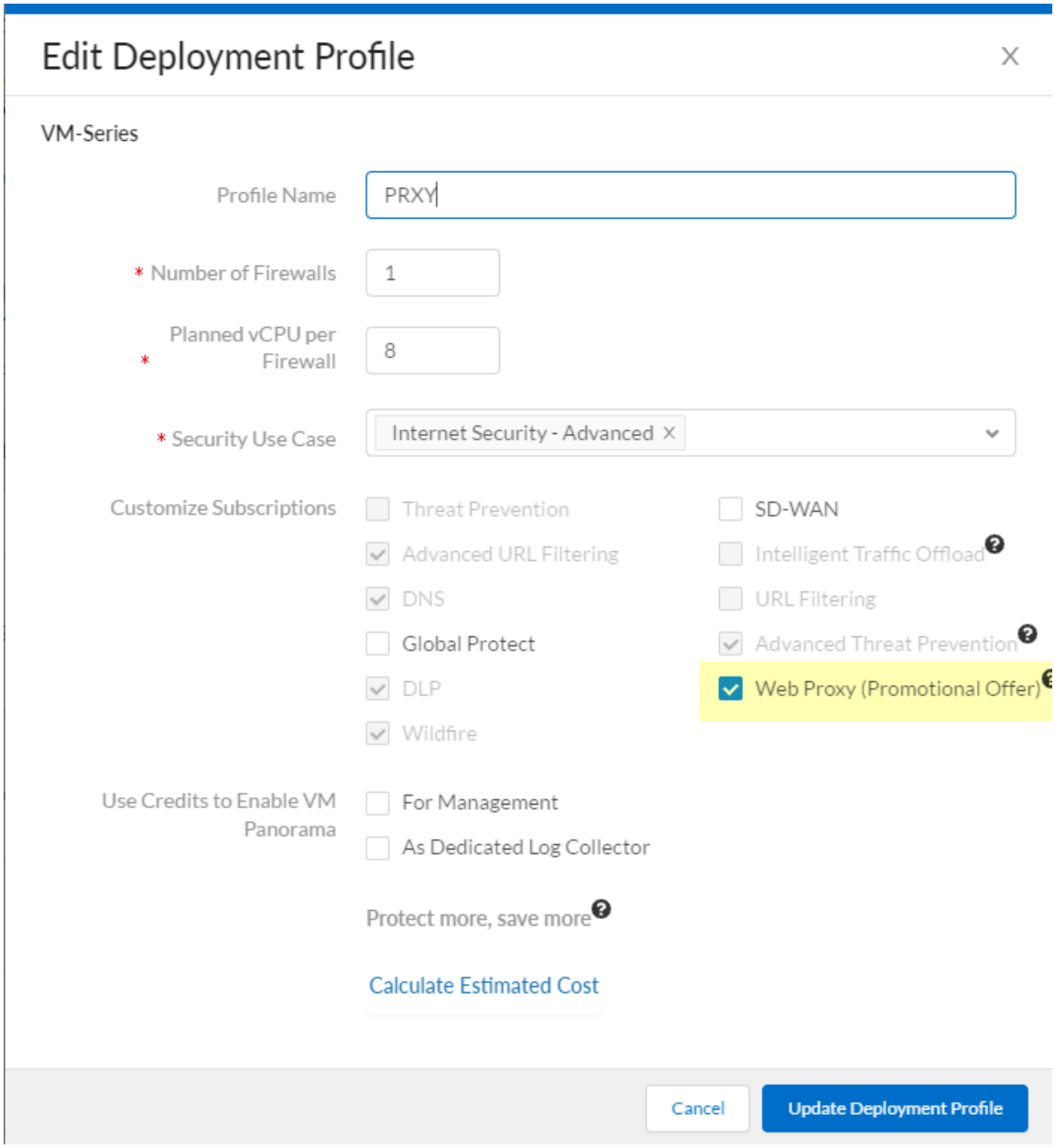
Strata Cloud Manager

 ©2024 Palo Alto Networks, Inc.

STEP 1 | (VM Series only (Série de machines virtuelles uniquement)) Si vous ne l'avez pas déjà fait, activez la licence pour le proxy Web.

Cette étape est requise pour les séries PA-1400, PA-3400 et VM. Les étapes suivantes concernent la série VM; pour le PA-1400 et le PA-3400, suivez les étapes pour activate subscription license (sactiver les licences d'abonnement).

1. Connectez-vous au portail de service clientèle (CSP).
2. **Edit (Modifiez)** le deployment profile (profil de déploiement).
3. Sélectionnez **Web Proxy (Promotional Offer) (Proxy Web (offre promotionnelle)).**



4. Cliquez sur **Update Deployment Profile (Mettre à jour le profil de déploiement)**.
5. Sur le pare-feu, récupérez les license keys (clés de licence) du serveur.

 ©2024 Palo Alto Networks, Inc.

Si la récupération de la clé de licence échoue, redémarrez le pare-feu et répétez cette étape avant de continuer.

STEP 2 | Configurez les interfaces et les zones nécessaires.

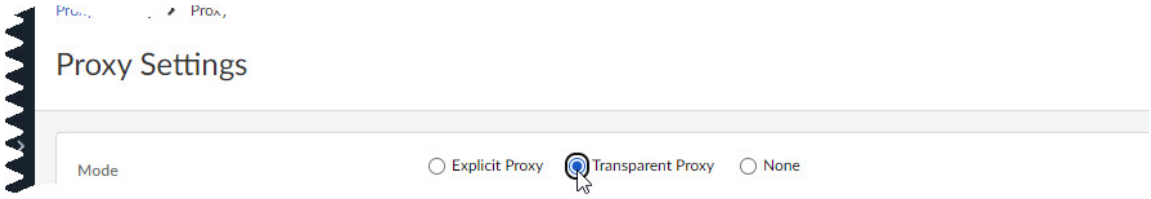
*Ne modifiez pas la zone **proxy**.*

Comme meilleure pratique, utilisez la couche 3 (L3) pour toutes les interfaces et configurez une zone distincte pour chaque interface au sein des mêmes routeurs virtuels et des mêmes systèmes virtuels.

1. Configurez une interface pour le client.
2. Configurez une interface pour le trafic sortant vers Internet.

STEP 3 | Configurez le proxy transparent.

1. Dans Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (Accès NGSW et Prisma)** > **Device Settings (Paramètres du périphérique)** > **Configuration Scope (Étendue de la configuration)**.
2. Sélectionnez le dossier, l'extrait ou le périphérique pour lequel vous souhaitez configurer un proxy transparent.
3. Sélectionnez **Device Settings (Paramètres du périphérique)** > **Proxy** > **Proxy Settings (Paramètres du proxy)** > **Customize (Personnaliser)**.
4. Sélectionnez **Transparent Proxy (Proxy transparent)** comme **Mode**.



5. Spécifiez la **Client Facing Interface (Interface côté client)**.
   Il s'agit de l'interface pour le trafic client que vous avez configurée lors d'une étape précédente.
6. Spécifiez une **Outbound Zone (Zone sortante)** pour le trafic sortant vers Internet.
   Vous pouvez **Create New (Créer nouveau)** si vous n'avez pas déjà configuré de zone sortante.
7. Spécifiez les adresses IP des serveurs DNS principal et secondaire auxquels vous souhaitez vous connecter ainsi que l'interface pour la connexion au proxy DNS.
   Après avoir transmis votre configuration, Strata Cloud Manager créera automatiquement un objet de proxy DNS avec ces spécifications sur vos périphériques. Vous pouvez visualiser l'objet sur les périphériques eux-mêmes, mais pas dans Strata Cloud Manager.
8. (Facultatif) Spécifiez le **Connect Timeout (Délai d'expiration de connexion)** pour définir (en secondes) combien de temps le proxy attend une réponse du serveur Web. S'il n'y a

 ©2024 Palo Alto Networks, Inc.

pas de réponse après l'expiration du délai spécifié, le proxy ferme la connexion. La valeur par défaut est 5 secondes.

9. (Facultatif) Spécifiez le **Web Traffic Service Port (Port du service de trafic Web)** si vous souhaitez que le trafic Web utilise des ports spéciaux. Les ports par défaut sont 80 et 443.
10. (Facultatif) Utilisez l'interface en boucle par défaut (**loopback.999**) ou saisissez-en une autre.

    L'interface en boucle doit suivre le format **loopback.x**, x étant n'importe quelle valeur entière.

    Après avoir transmis votre configuration, Strata Cloud Manager créera automatiquement une interface en boucle avec ces spécifications sur vos périphériques. Vous pouvez visualiser l'interface sur les périphériques eux-mêmes, mais pas dans Strata Cloud Manager.
11. (Facultatif) Choisissez **Whether to nat outbound traffic (S'il faut natter le trafic sortant)** et entrez une **Outbound Interface (Interface sortante)**.

    Cela crée une règle NAT source. Sélectionnez cette option si votre réseau ne peut pas accéder directement à Internet.
12. **Save (Enregistrer)**.

STEP 4 | Configurez **Transparent Proxy Policy Rules (Règles de politique de proxy transparent)**.

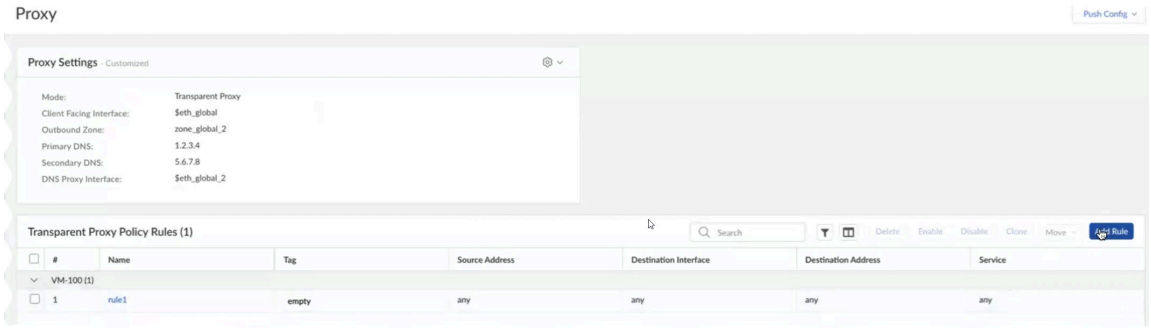
Il s'agit d'un ensemble de règles qui déterminent le trafic qui transite par le proxy. Une fois votre configuration transmise, ces règles créent des règles de Destination NAT (NAT de

 ©2024 Palo Alto Networks, Inc.

destination) sur vos périphériques, qui appliquent le NAT au trafic qui transite par l'interface en boucle configurée précédemment.

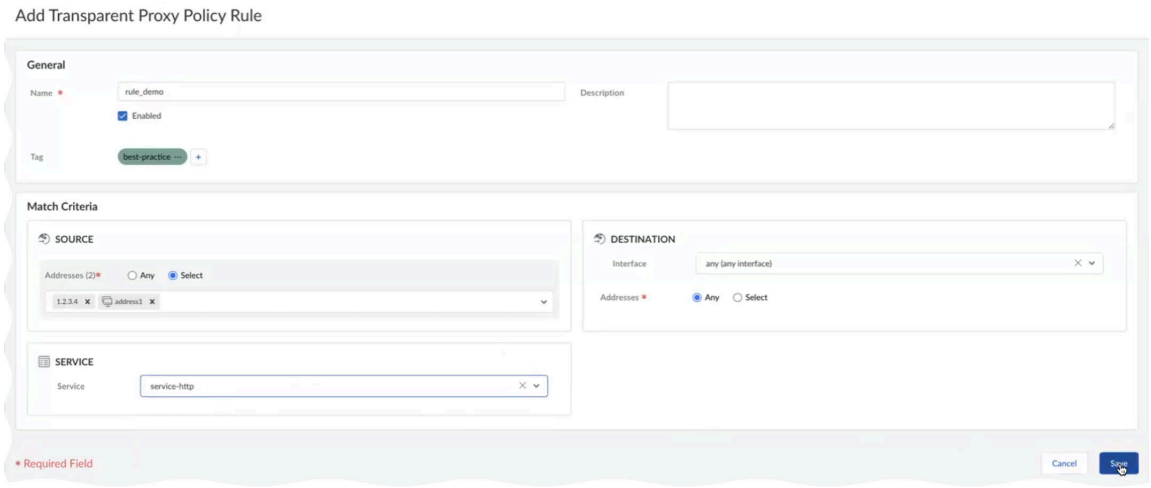
Dans Strata Cloud Manager, cependant, les règles de politique de proxy transparent ne sont visibles que dans la configuration du proxy Web, et non sous **NAT** ailleurs dans l'application.

1. Cliquez sur **Add rule (Ajouter une règle)**.



2. **Name (Nommez)** la règle.
3. (Facultatif) Ajoutez des balises pour étiqueter votre règle.
4. Spécifiez une adresse source ou laissez-la sur **Any (N'importe laquelle)**.
5. Spécifiez une adresse de destination ou laissez-la sur **Any (N'importe laquelle)**.
   (Facultatif) Spécifiez une interface de destination.
6. (Facultatif) Sélectionnez un **Service**.
7. **Save (Enregistrer)**.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

STEP 5 | Push your configuration (Transmettez votre configuration) et vérifiez sur vos pare-feu.

1. Pour effectuer la vérification, connectez-vous au pare-feu et sélectionnez **Network (Réseau)** > **Proxy**.
2. Vous devriez voir des informations correspondant au proxy transparent que vous venez de configurer.



Configurer l'authentification pour le proxy Web explicite

Lorsque vous configure an explicit web proxy (configurez un proxy Web explicite), configurez l'une des méthodes d'authentification utilisateur suivantes :

- Configurer l'authentification Kerberos
- Configuration de l'authentification SAML
- Configurer l'authentification Cloud Identity Engine

Si vous souhaitez exempter le trafic de périphériques spécifiques, tels que des imprimantes, de l'authentification, vous pouvez Configurer des exemptions pour l'authentification de proxy explicite.

Si vous n'avez pas besoin de configurer l'authentification pour votre trafic proxy Web, vous pouvez Exclure tout le trafic de proxy explicite de l'authentification.

Configurer l'authentification Kerberos

STEP 1 | Créez un compte de service pour l'annuaire (s'il n'est pas déjà configuré) et activez la prise en charge du chiffrement AES128 et AES256 dans les propriétés du compte de service.

STEP 2 | Inscrivez le nom principal du service (SPN) pour le nom de domaine complet du proxy et create a keytab file (créez un fichier keytab) pour l'authentification uniqueKerberos.

Le nom principal du keytab Kerberos doit correspondre au nom d'hôte résolu en adresse IP de l'interface proxy.

STEP 3 | Sur le pare-feu, créez un profil de serveur pour le serveur Kerberos .

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Configurez un profil d'authentification pour utiliser Kerberos et importez le keytab dans le authentication profile (profil d'authentification).

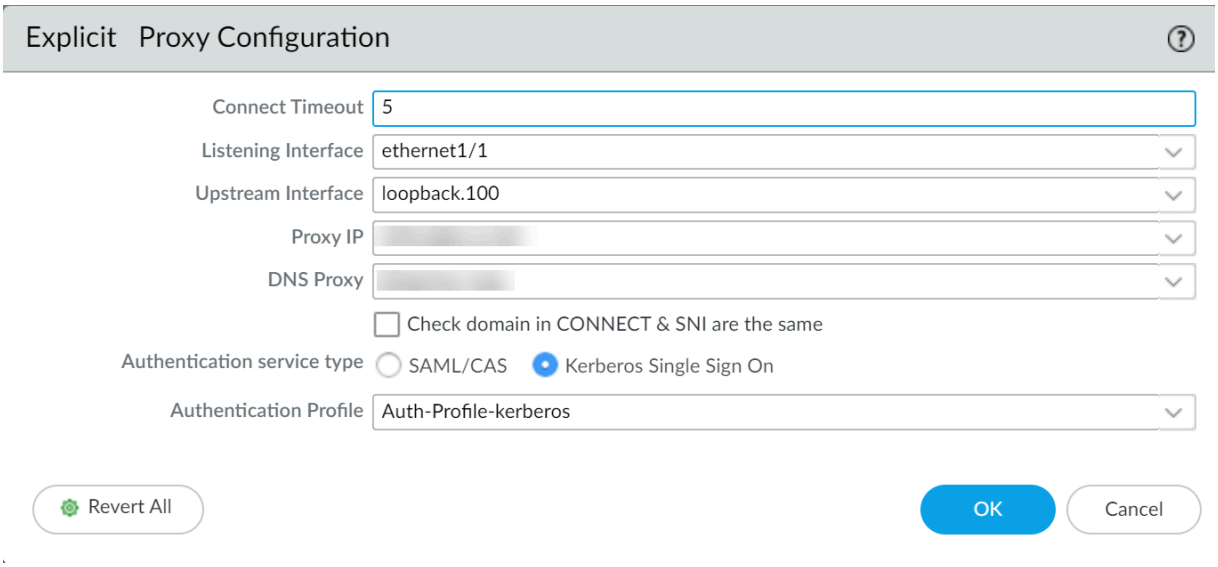
STEP 5 | (Facultatif mais recommandé) Si vous utilisez Panorama pour gérer vos pare-feu, configurez un log forwarding profile (profil de transfert de journaux) pour transférer les journaux vers Cortex Data Lake (CDL),Panorama ou les deux.

Par défaut, le pare-feu ne transfère pas les journaux vers CDL ou Panorama. Le transfert des journaux garantit que les informations complètes du journal d'authentification sont disponibles pour aider à résoudre les problèmes d'authentification potentiels.

Il est recommandé d'utiliser Panorama pour gérer le pare-feu du proxy Web, configurez tous les objets utilisés par le proxy dans un emplacement Panorama partagé et configurez le pare-feu du proxy Web dans un groupe de périphériques distinct qui ne contient aucun autre pare-feu ou système virtuel. Si le pare-feu est déjà membre d'un groupe d'appareils, créez un groupe d'appareils enfant en tant que sous-groupe et déplacez le pare-feu vers le groupe d'appareils enfants.

Si vous rencontrez des problèmes avec le test du navigateur lors de l'utilisation du navigateur Chrome, nous vous recommandons d'utiliser un autre navigateur.

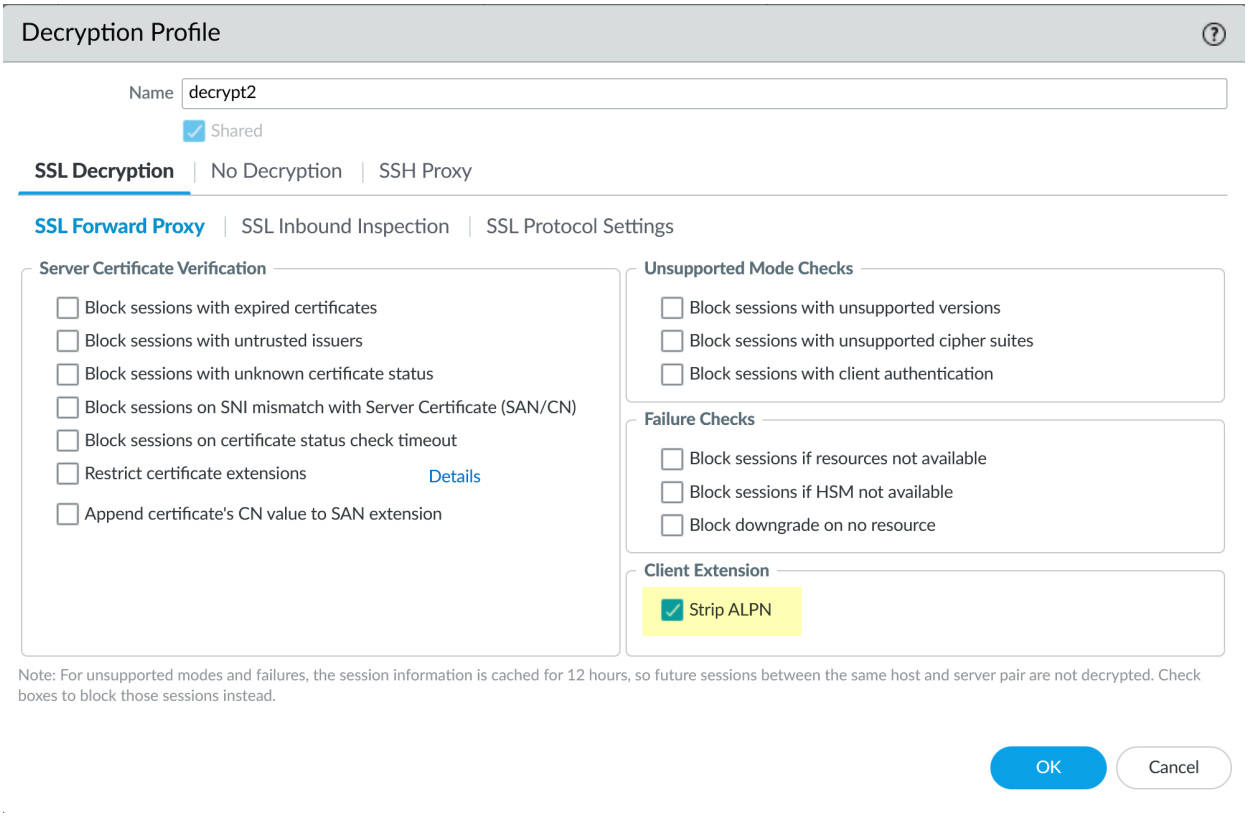
STEP 6 | Dans la**Explicit Proxy Configuration (configuration explicite du proxy)** (**Network (Réseau)** > **Proxy** > **Explicit Proxy Configuration (configuration explicite du proxy)**), sélectionnez**Kerberos Single Sign On (Authentification unique Kerberos)** en tant que **Authentication service type (type de service d'authentification)**.



 ©2024 Palo Alto Networks, Inc.

STEP 7 | (Facultatif mais recommandé) Si vous utilisez une stratégie de déchiffrement pour le trafic, sélectionnez **Strip ALPN (Supprimer ALPN)** pour supprimer la valeur dans la négociation ALPN (Application-Layer Protocol Négociation).

Cette option nécessite HTTPS.



STEP 8 | Sélectionnez le **Authentication Profile (Profil d'authentification)** que vous avez créé à l'étape 4

STEP 9 | Effectuez les étapes restantes pour Configurer un proxy Web.

Configuration de l'authentification SAML

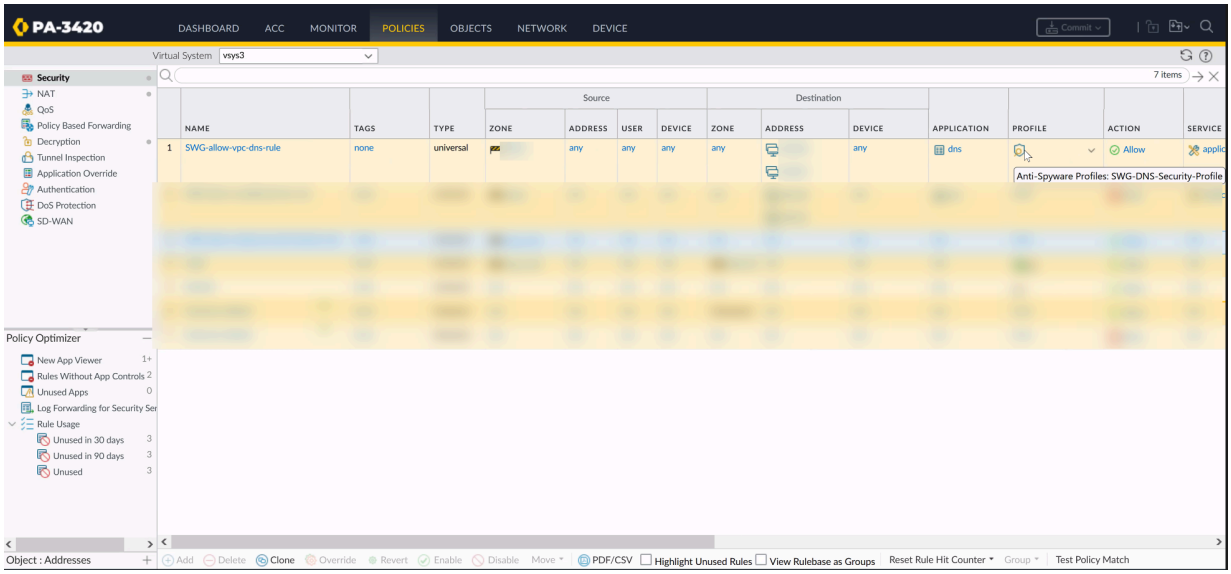
L'authentification SAML pour le proxy Web explicite nécessite Panorama et le plug-in Cloud Services version 3.2.1 (et versions ultérieures).

Pour simplifier la configuration de l'authentification SAML pour le proxy Web explicite, le pare-feu ou Panorama génère automatiquement les règles suivantes pour autoriser le trafic nécessaire. Si vous utilisez Panorama, vous devez sélectionner un pare-feu individuel pour afficher les règles.

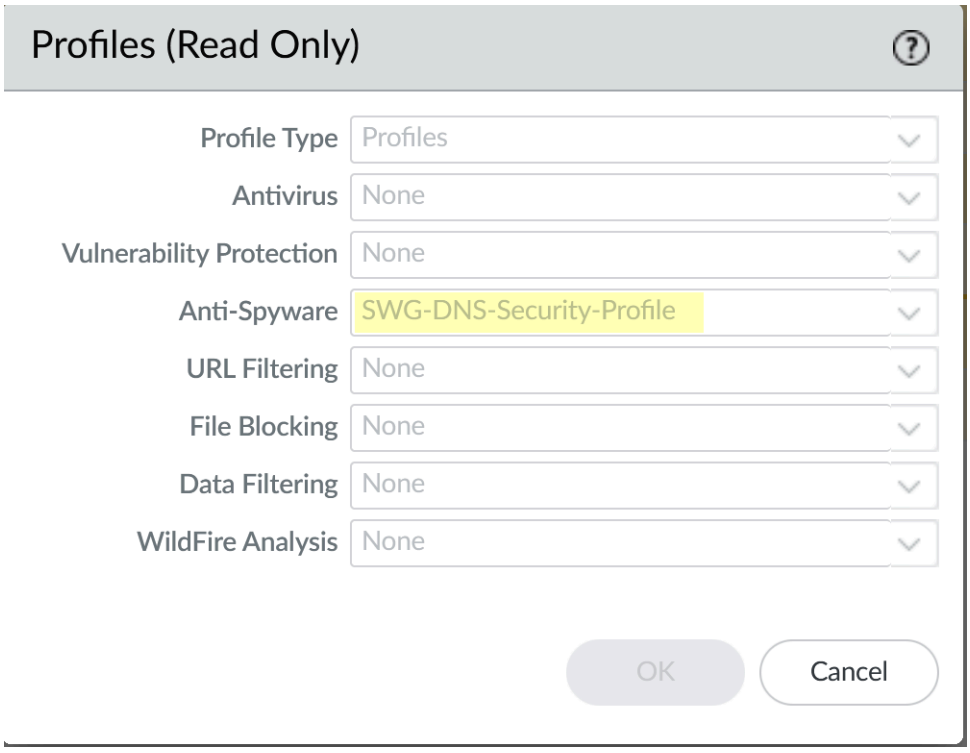
	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PRO
1	SWG-allow-vpc-dns-rule	none	universal	swg	any	any	any	any		any	dns	application-...	Allow	
2	SWG-block-unsollicited-dns-rule	none	universal	swg	any	any	any	any		any	dns	application-...	Drop	none
3	SWG-allow-outbound-auth-domain-rule	none	universal	swg	any	any	any	any	any	any	any	any	Allow	none

©2024 Palo Alto Networks, Inc.

- **SWG-allow-vpc-dns-rule** — Autorise le trafic de la zone où se trouve l'interface amont du proxy Web vers les adresses de serveur DNS principal et secondaire du proxy Web.

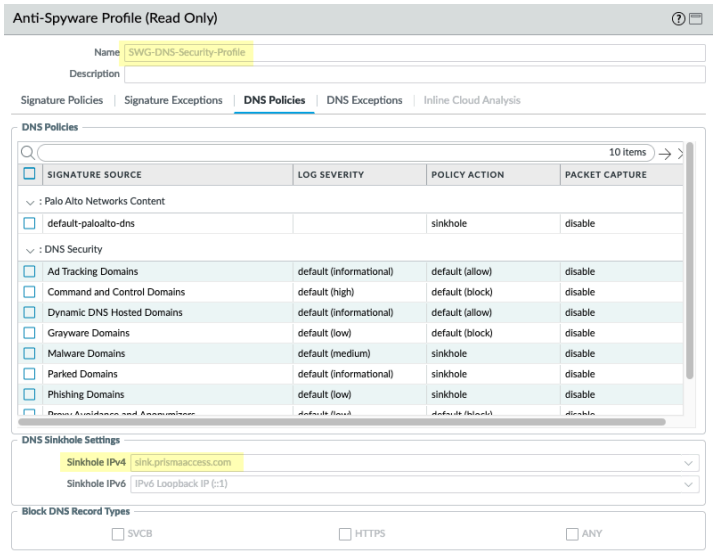


Le pare-feu génère également un profil anti-spyware, `SWG-DNS-Security-Profile` pour autoriser le trafic requis.



La règle générée automatiquement `SWG-allow-vpc-dns-rule` applique ce profil au trafic applicable.

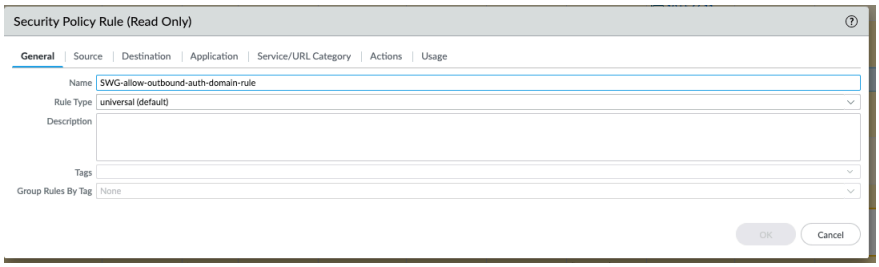
©2024 Palo Alto Networks, Inc.



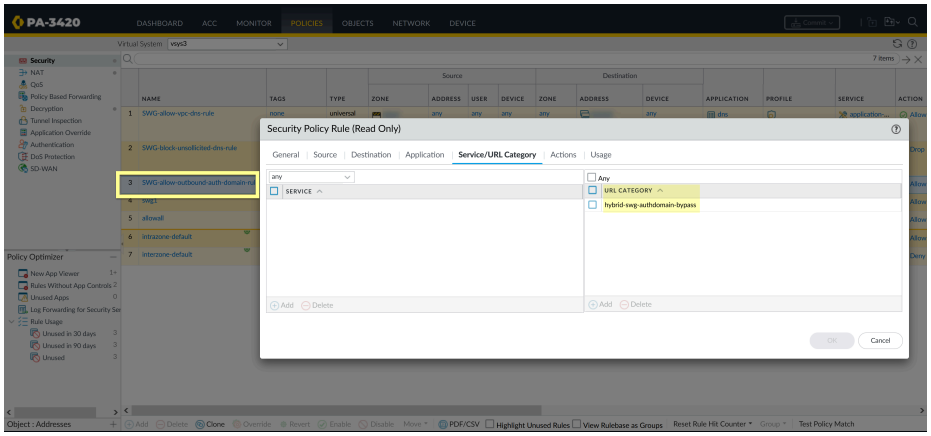
- **SWG-block-unsolicited-dns-rule** —Bloque le trafic non autorisé vers les adresses des serveurs DNS principal et secondaire pour le proxy Web.

 ©2024 Palo Alto Networks, Inc.

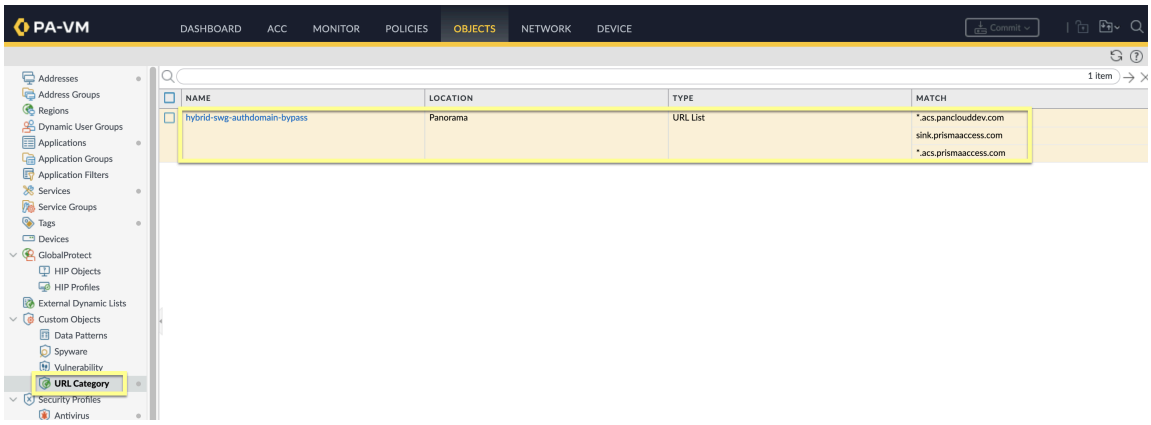
- **SWG-allow-outbound-auth-domain-rule** — (Proxy explicite avec authentification SAML uniquement) Autorise le trafic de la zone où se trouve l'interface amont du proxy Web vers le plug-in Cloud Services.



La règle générée automatiquement `SWG-allow-outbound-auth-domain-rule` applique la catégorie d'URL `hybride-swg-authdomain-bypass` au trafic applicable.



La catégorie d'URL,`hybrid-swg-authdomain-bypass` contient les entrées prédéfinies nécessaires pour les domaines requis.



STEP 1 | Si vous ne l'avez pas déjà fait, configurez le Explicit Proxy for mobile users (proxy explicite pour les utilisateurs mobiles).

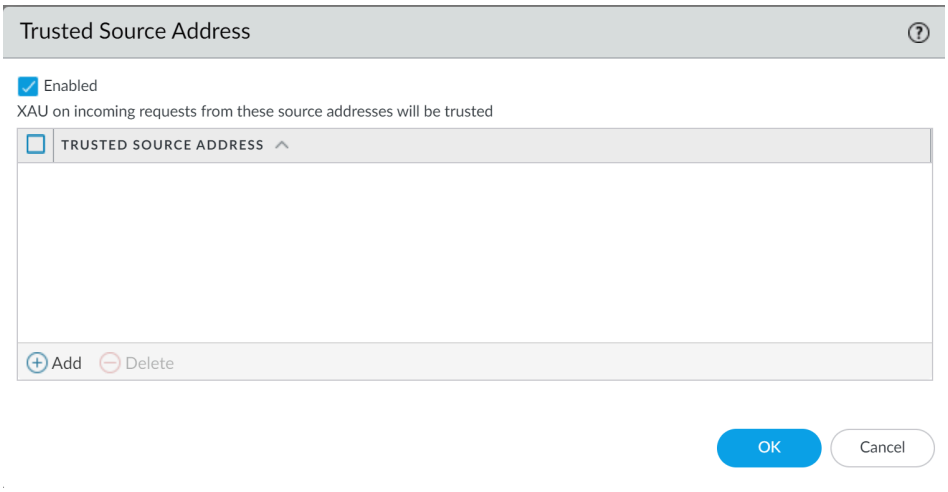
Il s'agit d'une méthode d'authentification typique pour l'authentification par proxy web local et Prisma Access Explicit Proxy, qui nécessite une licence. Les paramètres de proxy explicite de Prisma Access pour les valeurs de cookie et de délai d'expiration s'appliquent également à une configuration de proxy Web explicite. Vous devez valider les modifications et les pousser vers les pare-feu appropriés avant de continuer.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Si vous ne l'avez pas déjà fait, configurez un SAML Authentication profile (profil d'authentification SAML).

STEP 3 | (Required for XAU only (Requis pour XAU uniquement)) Si le proxy en aval envoie l'en-tête XAU, configurez une adresse source approuvée pour le proxy en aval.

1. Sélectionnez **Device (appareil)** > **User Identification (Identification de l'utilisateur)** > **Trusted Source Address (Adresse source approuvée)**.
2. **Edit (Modifiez)** les paramètres de l'adresse source approuvée pour définir l'état sur **Enabled (Activé)**.

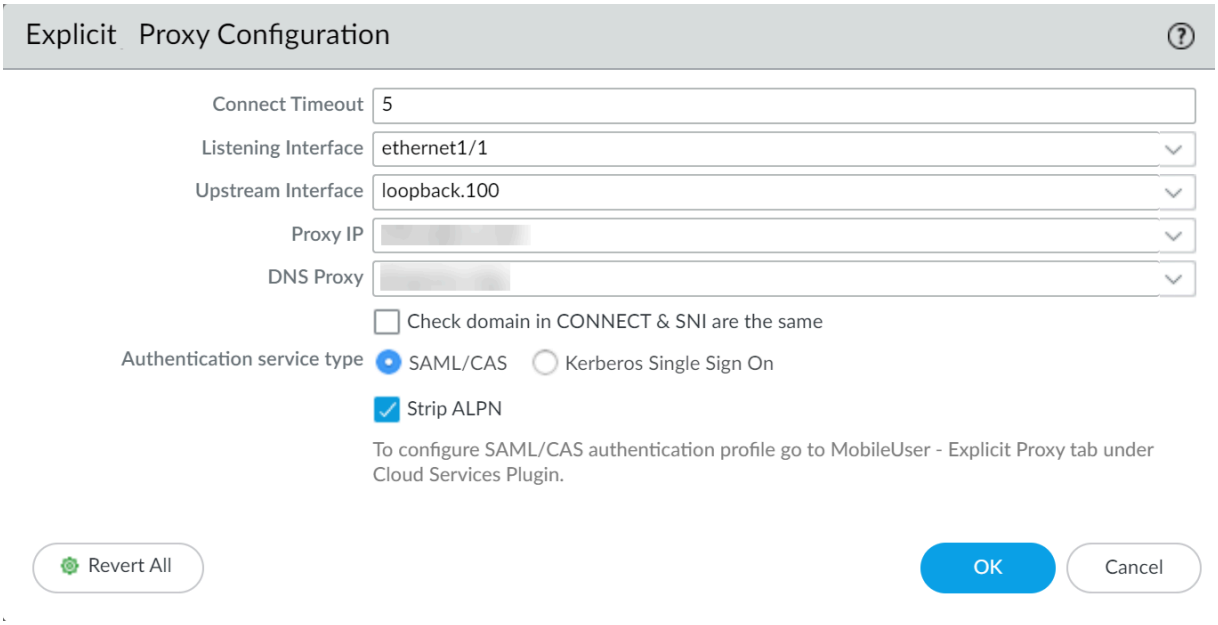


3. **Add (Ajoutez)** les objets d'adresse que vous souhaitez autoriser à l'utilisateur authentifié X (XAU).

   Un proxy Web explicite nécessite un objet d'adresse IP pour l'adresse source approuvée.
4. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Dans la **Explicit Proxy Configuration (Configuration explicite du proxy)** (**Network (Réseau)** > **Proxy** > **Explicit Proxy Configuration (configuration explicite du proxy)**), sélectionnez **SAML/CAS** en tant que **Authentication service type (type de service d'authentification)**.



STEP 5 | (Facultatif mais recommandé) Si vous utilisez une stratégie de déchiffrement pour le trafic, sélectionnez **Strip ALPN (Supprimer ALPN)** pour supprimer la valeur dans la négociation ALPN (Application-Layer Protocol Négociation).

Cette option nécessite HTTPS.

STEP 6 | Effectuez les étapes restantes pour configurer le Configurer un proxy Web.

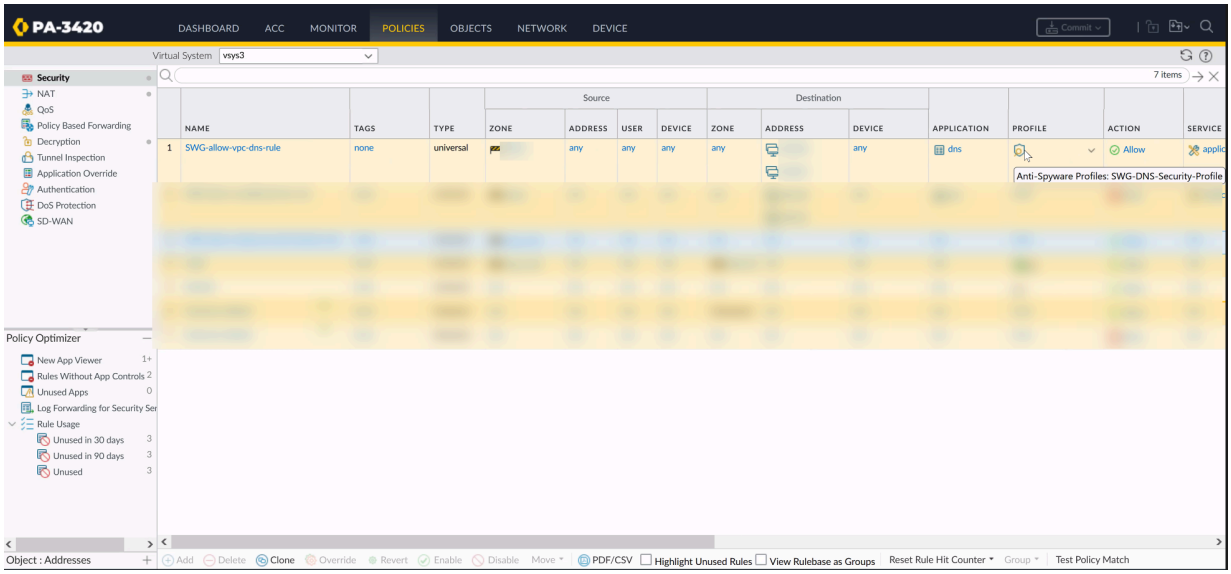
Configurer l'authentification Cloud Identity Engine

Pour simplifier la configuration de l'authentification SAML pour le proxy Web explicite, le pare-feu ou Panorama génère automatiquement les règles suivantes pour autoriser le trafic nécessaire. Si vous utilisez Panorama, vous devez sélectionner un pare-feu individuel pour afficher les règles.

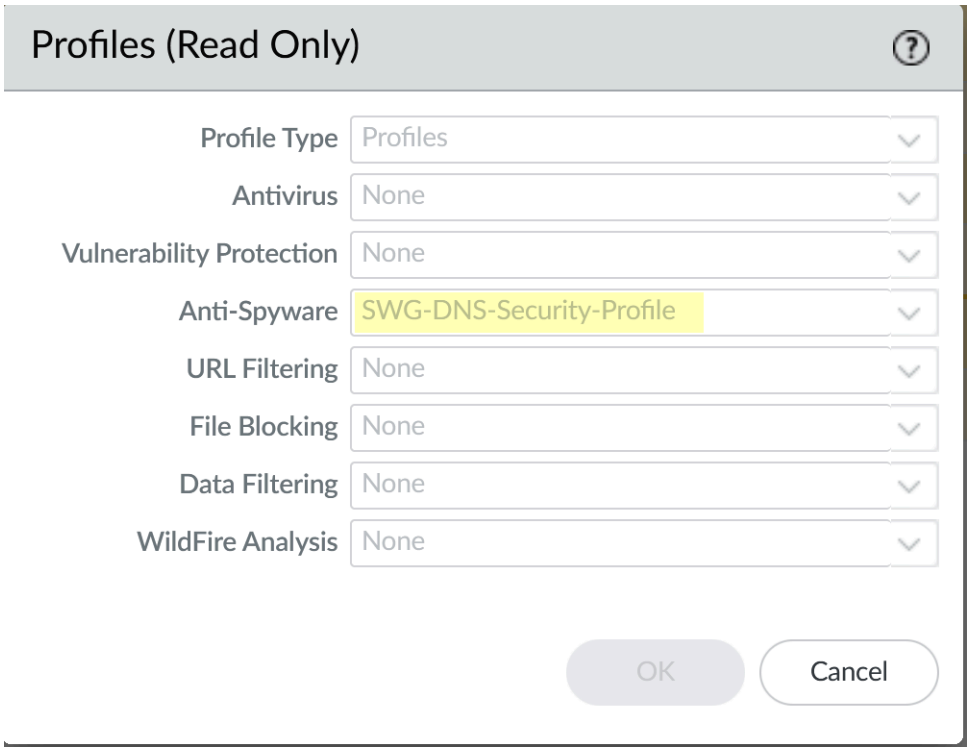
	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PRO
1	SWG-allow-vpc-dns-rule	none	universal	swg	any	any	any	any		any	dns	application-...	Allow	
2	SWG-block-unsollicited-dns-rule	none	universal	swg	any	any	any	any		any	dns	application-...	Drop	none
3	SWG-allow-outbound-auth-domain-rule	none	universal	swg	any	any	any	any	any	any	any	any	Allow	none

©2024 Palo Alto Networks, Inc.

- **SWG-allow-vpc-dns-rule** — Autorise le trafic de la zone où se trouve l'interface amont du proxy Web vers les adresses de serveur DNS principal et secondaire du proxy Web.

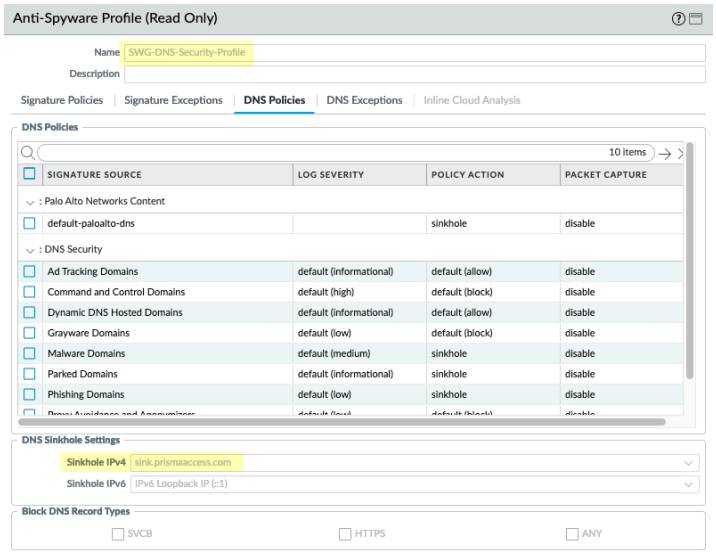


Le pare-feu génère également un profil anti-spyware, `SWG-DNS-Security-Profile` pour autoriser le trafic requis.



La règle générée automatiquement `SWG-allow-vpc-dns-rule` applique ce profil au trafic applicable.

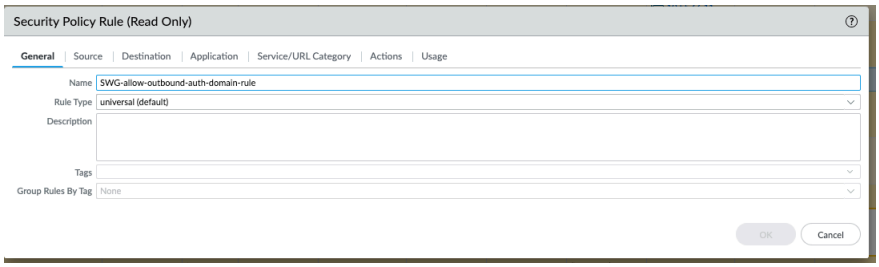
©2024 Palo Alto Networks, Inc.



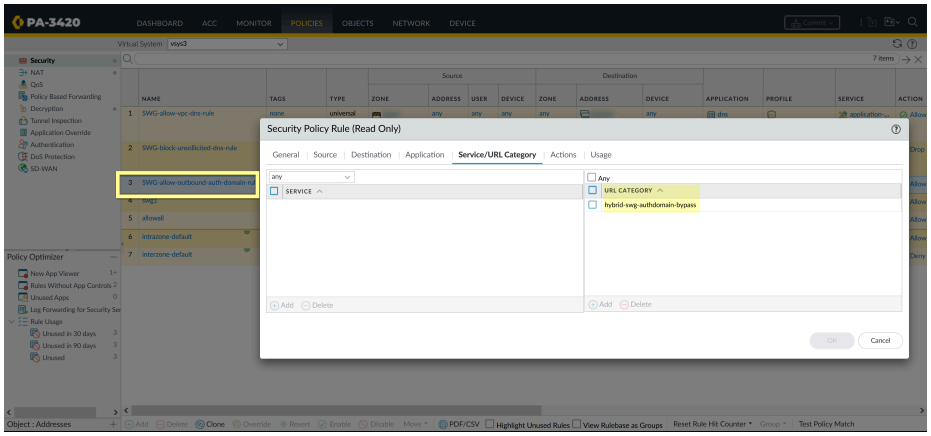
- **SWG-block-unsolicited-dns-rule** —Bloque le trafic non autorisé vers les adresses des serveurs DNS principal et secondaire pour le proxy Web.

 ©2024 Palo Alto Networks, Inc.

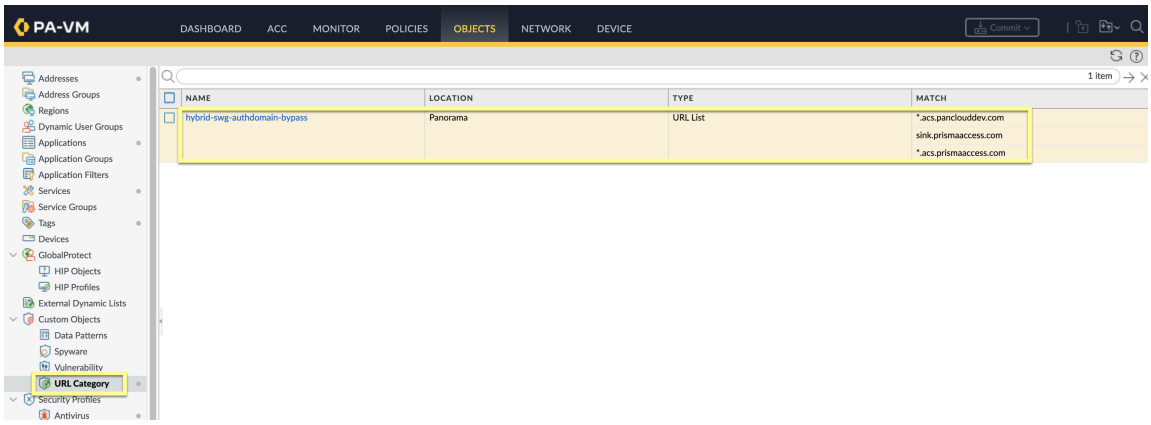
- **SWG-allow-outbound-auth-domain-rule** — (Proxy explicite avec authentification SAML uniquement) Autorise le trafic de la zone où se trouve l'interface amont du proxy Web vers le plug-in Cloud Services.



La règle générée automatiquement `SWG-allow-outbound-auth-domain-rule` applique la catégorie d'URL `hybride-swg-authdomain-bypass` au trafic applicable.



La catégorie d'URL,`hybrid-swg-authdomain-bypass` contient les entrées prédéfinies nécessaires pour les domaines requis.



STEP 1 | Si vous ne l'avez pas déjà fait, configurez le Explicit Proxy for mobile users (proxy explicite pour les utilisateurs mobiles).

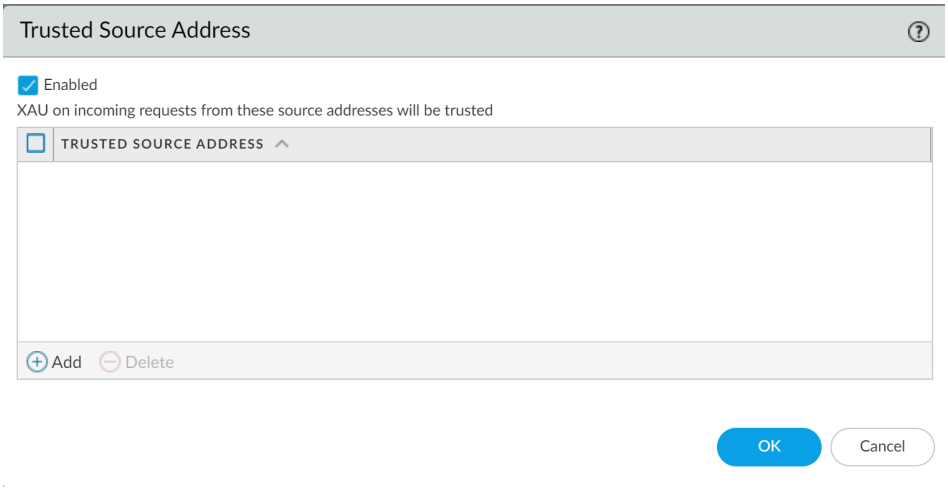
Vous devez valider les modifications et les pousser vers les pare-feu appropriés avant de continuer.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Si vous ne l'avez pas déjà fait, configurez authentication using the Cloud Identity Engine (authentification à l'aide de Cloud Identity Engine) et configurez un Cloud Identity Engine authentication profile (profil d'authentification Cloud Identity Engine).

STEP 3 | (Required for XAU only (Requis pour XAU uniquement)) Si le proxy en aval envoie l'en-tête XAU, configurez une adresse source approuvée pour le proxy en aval.

1. Sélectionnez **Device (appareil)** > **User Identification (Identification de l'utilisateur)** > **Trusted Source Address (Adresse source approuvée)**.
2. **Edit (Modifiez)** les paramètres de l'adresse source approuvée pour définir l'état sur **Enabled (Activé)**.

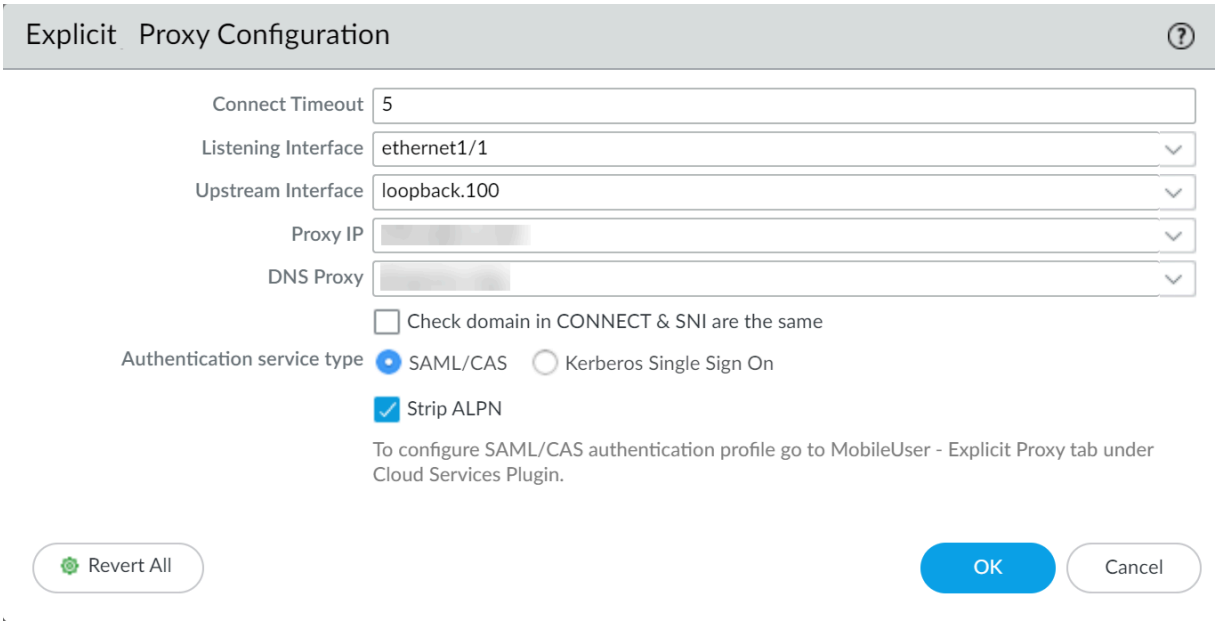


3. **Add (Ajoutez)** les objets d'adresse que vous souhaitez autoriser à l'utilisateur authentifié X (XAU).

   Un proxy Web explicite nécessite un objet d'adresse IP pour l'adresse source approuvée.
4. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Dans la **Explicit Proxy Configuration (Configuration explicite du proxy)** (**Network (Réseau)** > **Proxy** > **Explicit Proxy Configuration (configuration explicite du proxy)**), sélectionnez **SAML/CAS** en tant que **Authentication service type (type de service d'authentification)**.



STEP 5 | (Facultatif mais recommandé) Sélectionnez **Strip ALPN (Supprimer ALPN)** pour supprimer la valeur dans la négociation ALPN (Application-Layer Protocol Négociation).

Cette option nécessite HTTPS.

STEP 6 | Effectuez les étapes restantes pour configurer le Configurer un proxy Web.

Configurer des exemptions pour l'authentification de proxy explicite

L'utilisation d'un proxy Web vous permet d'utiliser les informations des périphériques proxy de votre réseau via une interface unifiée. Cependant, les ressources telles que les imprimantes ou autres périphériques IoT ne peuvent pas répondre aux demandes d'authentification du proxy ni prendre en charge un certificat ou un fichier PAC.

Vous pouvez exempter ces périphériques de la demande d'authentification du proxy en utilisant un objet d'adresse pour la source, une liste d'exceptions de catégorie d'URL personnalisée comme destination, ou les deux. La configuration d'une exemption d'authentification pour le proxy explicite garantit que le trafic de ces ressources clés n'est pas interrompu et permet au trafic de ces périphériques de confiance de passer par le proxy conformément à votre architecture de réseau.

Vous pouvez créer jusqu'à 20 exemptions de proxy Web dans votre politique d'authentification.

Si vous n'avez pas besoin d'authentifier votre trafic de proxy explicite, vous pouvez Exclure tout le trafic de proxy explicite de l'authentification.

©2024 Palo Alto Networks, Inc.

STEP 1 | Si vous ne l'avez pas déjà fait, Configurer le proxy explicite puis définissez le type de trafic de proxy que vous souhaitez exempter des demandes d'authentification.

Vous pouvez exempter le trafic en fonction de la source, du domaine de destination ou des deux.

- Configurez un objet d'adresse (**Objects (Objets)** > **Addresses (Adresses)**) qui contient les adresses IP sources de vos périphériques de confiance. L'adresse IP source peut être une adresse ou un groupe d'adresses.
- Configurez une liste d'exceptions de catégorie d'URL personnalisée (**Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)**) qui contient le ou les domaines d'URL de destination des services Web que vous souhaitez autoriser.

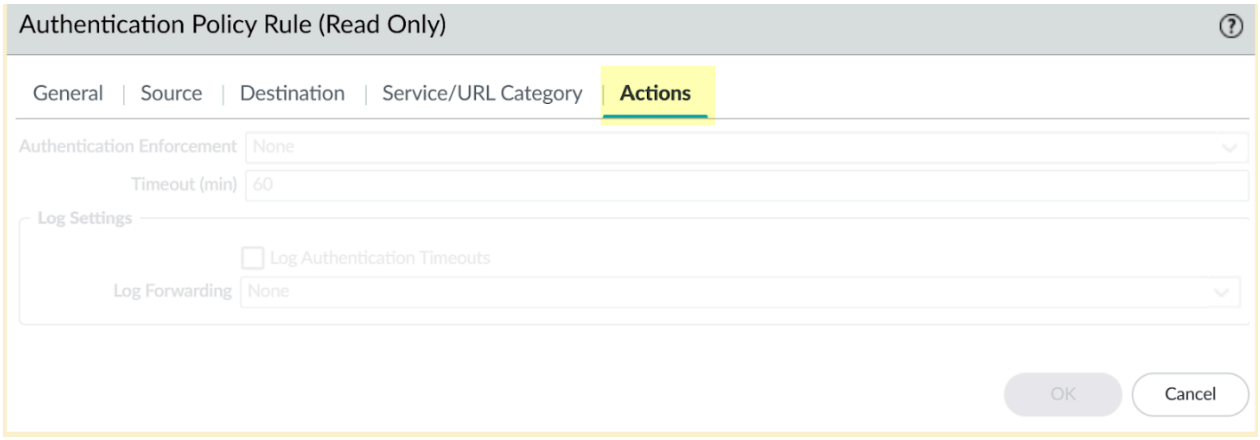
STEP 2 | Activez le Authentication Portal (Portail d'authentification) si vous ne l'avez pas déjà fait.

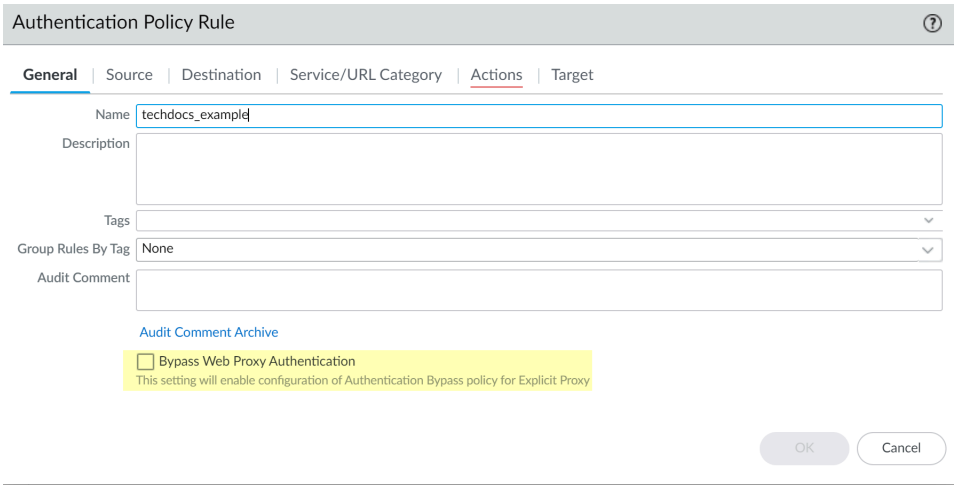
Cette étape est requise pour appliquer la règle de politique.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Modifiez ou créez votre règle de politique d'authentification (**Policies (Politiques)** > **Authentication (Authentification)**) et sélectionnez **Bypass Web Proxy Authentication (Contourner l'authentification du proxy Web)**.

*Lorsque vous activez l'option **Bypass Web Proxy Authentication (Contourner l'authentification du proxy Web)**, l'option **Authentication Enforcement (Application de l'authentification)** dans l'onglet **Action** est définie sur **None (Aucune)** ; vous ne pouvez pas modifier ce paramètre lorsque l'option **Bypass Web Proxy Authentication (Contourner l'authentification du proxy Web)** est activée.*





 ©2024 Palo Alto Networks, Inc.

STEP 4 | Définissez le type de trafic de proxy que vous souhaitez exempter de l'authentification dans votre règle de politique d'authentification et **Commit (Validez)** vos modifications.

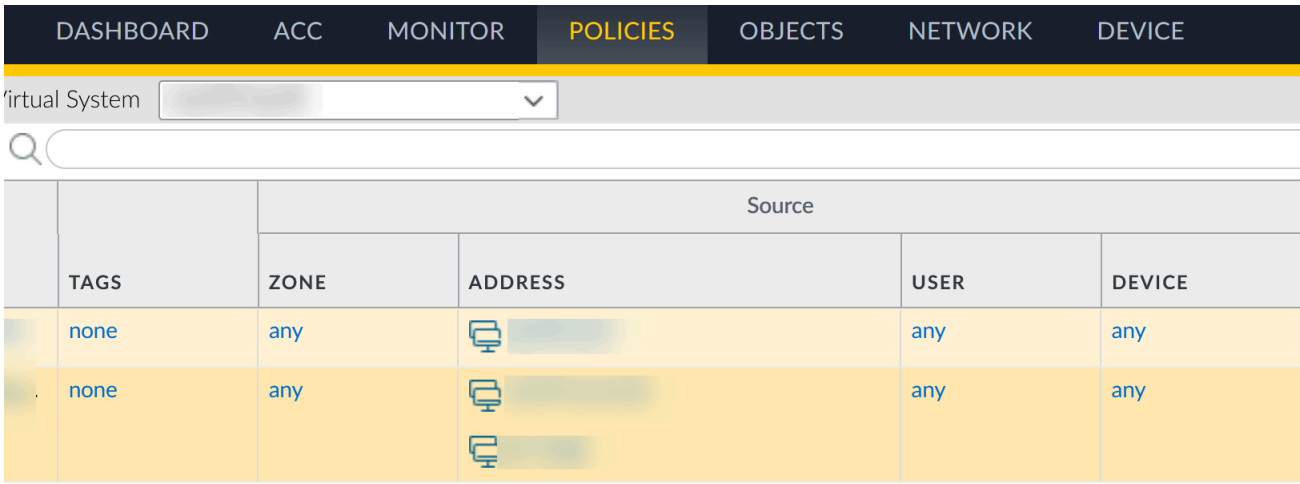
Vous pouvez exempter une source, une destination ou les deux.

- Sélectionnez l'onglet **Source**, puis sélectionnez l'objet d'adresse que vous avez configuré lors de la première étape comme **Source Address (Adresse source)** et cliquez sur **OK**.
- Sélectionnez l'onglet **Destination**, puis sélectionnez la catégorie d'URL que vous avez configurée lors de la première étape.

> *Vous devez créer la liste d'exceptions de catégorie d'URL personnalisée avant de pouvoir la sélectionner comme destination. Vous ne pouvez pas créer une nouvelle liste d'exceptions de catégorie d'URL personnalisée comme destination au cours de cette étape.*

STEP 5 | **Commit (Validez)** vos modifications et vérifiez votre configuration.

1. Affichez vos règles de politique (**Policies (Politiques)** > **Authentication (Authentification)**) et confirmez qu'une coche s'affiche dans la colonne **Bypass Web Proxy Authentication (Contourner l'authentification du proxy Web)** pour les règles pour lesquelles vous avez activé l'exemption.



2. En fonction de votre méthode d'authentification, utilisez les commandes CLI pour afficher les exemptions pour le trafic de proxy.
   - Si vous utilisez la méthode d'authentification SAML, vous pouvez utiliser la commande **`show counter global name ctd_eproxy_skip_auth_url_match`** pour vérifier la configuration. Cette commande affiche le nombre d'exemptions d'authentification SAML pour le trafic de proxy.
   - Si vous utilisez le type de service d'authentification Kerberos, vous pouvez utiliser la commande **`show counter global name flow_swg_ep_kerberos_skip_auth`** pour vérifier la configuration. Cette commande affiche le nombre d'exemptions d'authentification Kerberos pour le trafic de proxy.

 ©2024 Palo Alto Networks, Inc.

Exclure tout le trafic de proxy explicite de l'authentification

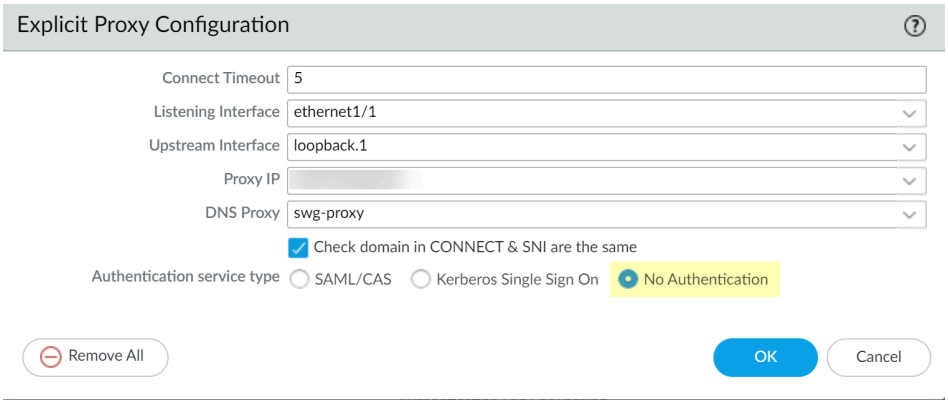
Si vous ne souhaitez pas configurer d'authentification pour le trafic de proxy explicite, vous pouvez exclure tout le trafic de proxy explicite de l'authentification. Lorsque vous excluez tout le trafic de proxy de l'authentification, le pare-feu ou Panorama n'authentifie pas les connexions de proxy et ne crée aucun journal pour les événements d'authentification.

Pour exempter uniquement un trafic spécifique de l'authentification, vous pouvez Configurer des exemptions pour l'authentification de proxy explicite.

STEP 1 | Si vous ne l'avez pas déjà fait, Configurer le proxy explicite pour votre trafic de proxy web.

STEP 2 | Modifiez ou créez la configuration de votre proxy web (**Network (Réseau)** > **Proxy** > **Explicit Proxy (Proxy explicite)**) et sélectionnez **No authentication (Pas d'authentification)** comme le **Authentication service type (Type de service d'authentification)**, puis cliquez sur **OK**.

Si vous sélectionnez cette option, toutes les connexions de proxy ne sont pas authentifiées et le pare-feu ou Panorama ne crée pas de journaux pour les événements d'authentification.

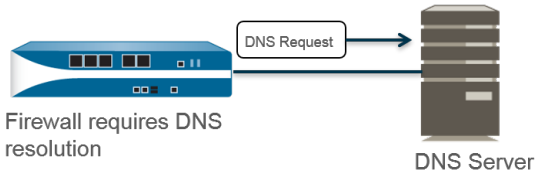


STEP 3 | **Commit (Validez)** vos modifications.

©2024 Palo Alto Networks, Inc.

Cas pratique 1 : Le pare-feu exige une résolution DNS

Dans ce cas d'utilisation, le pare-feu est le client qui demande la résolution DNS des FQDN pour les règles de politique de sécurité, les rapports, les services de gestion (comme le e-mail, Kerberos, SNMP, syslog, etc.) et les événements de gestion, comme les services de mises à jour logicielles, les mises à jour logicielles dynamiques et WildFire. Dans les environnements dynamiques, les FQDN changent plus fréquemment ; les résolutions DNS exactes permettent au pare-feu d'appliquer la politique avec exactitude, de fournir des rapports et des services de gestion et de gérer les événements de gestion. Les services DNS globaux partagés procèdent à la résolution DNS pour les fonctions du plan de gestion.



STEP 1 | Modifiez les paramètres des services (**Device (Périphérique)** > **Setup (Configuration)** > **Services** > **Global** pour les pare-feu qui prennent en charge plusieurs systèmes virtuels ; **Device (Périphérique)** > **Setup (Configuration)** > **Services** pour ceux qui ne le font pas.

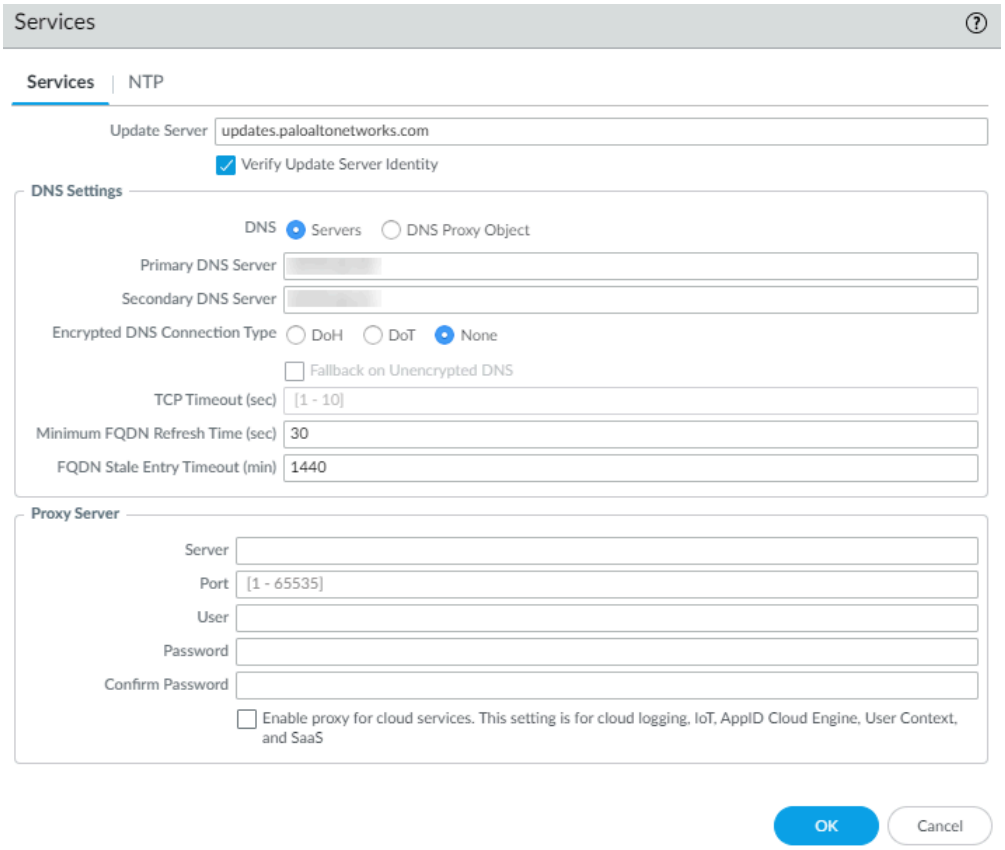
STEP 2 | Configurez la connexion aux serveurs DNS pouvant fournir des résolutions DNS.

Vous devez configurer manuellement au moins un serveur DNS sur le pare-feu, sinon il ne pourra pas résoudre les noms d'hôtes ; le pare-feu ne peut utiliser les paramètres de serveur DNS d'une autre source, telle qu'un FAI.

1. Dans l'onglet **Services (Services)**, pour **DNS (DNS)**, sélectionnez **Servers (Serveurs)** et saisissez l'adresse du **Primary DNS Server (Serveur DNS principal)** et l'adresse du **Secondary DNS Server (Serveur DNS secondaire)**.
2. (PAN-OS 11.2.1 et versions ultérieures) (Facultatif) Pour configurer un DNS chiffré pour les connexions au serveur :
   1. Sélectionnez un **Encrypted DNS Connection Type (Type de connexion DNS chiffrée)** (autre que **None (Aucun)**, qui est le paramètre par défaut) :
      - **DoH** : DNS sur HTTPS (Hypertext Transfer Protocol Secure). DoH utilise le port 443. Lorsque DoH est le type de connexion, une adresse DNS principale est requise et le pare-feu envoie toutes les requêtes DNS au serveur DNS principal à l'aide de DoH. Si aucune réponse n'arrive du serveur DNS principal, le pare-feu envoie des requêtes DoH au serveur DNS secondaire.
      - **DoT** : DNS sur TLS (Transport Layer Security). DoT utilise le port 853, qui est dédié au trafic DoT. Lorsque DoT est le type de connexion, une adresse DNS principale est requise et le pare-feu envoie toutes les requêtes DNS au serveur DNS principal à l'aide de DoT. Si aucune réponse n'arrive du serveur DNS principal, le pare-feu envoie des requêtes DoT au serveur DNS secondaire.
      - **None (Aucun)** : paramètre par défaut. Aucun DNS chiffré n'est spécifié pour les connexions au serveur.

 ©2024 Palo Alto Networks, Inc.

2. Sélectionnez **Fallback on Unencrypted DNS (Retour au DNS non chiffré)** pour que le pare-feu revienne au DNS traditionnel (texte en clair) si le serveur DNS rejette le DNS chiffré ou expire (le pare-feu ne reçoit aucune réponse du type de connexion configuré [DoH ou DoT] du serveur DNS principal ou secondaire pendant la période d'expiration TCP configurée).
3. Entrez le **TCP Timeout (sec) (Délai d'expiration TCP (sec))**, la plage est comprise entre 1 et 10 ; la valeur par défaut est 1 seconde.



3. Passez à l'étape 4.

STEP 3 | Au lieu de spécifier des serveurs DNS, vous pouvez configurer un DNS Proxy Object (Objet proxy DNS) si vous souhaitez configurer des fonctions DNS avancées comme la segmentation DNS, le contrôle prioritaire du proxy DNS, les règles de proxy DNS, les entrées statiques ou l'héritage DNS. À partir de PAN-OS 11.2.1, le proxy DNS prend en charge le DNS chiffré.

1. Dans l'onglet **Services (Services)**, pour **DNS (DNS)**, sélectionnez **DNS Proxy Object (Objet proxy DNS)**.

 ©2024 Palo Alto Networks, Inc.

2. Dans la liste **DNS Proxy (Proxy DNS)**, sélectionnez le proxy DNS que vous souhaitez utiliser pour configurer des services DNS globaux, ou sélectionnez **DNS Proxy (Proxy DNS)** pour configurer un nouvel objet proxy DNS, comme suit :
   1. **Enable (Activez)**, puis saisissez un **Name (Nom)** pour l'objet proxy DNS.
   2. Pour les pare-feu qui prennent en charge plusieurs systèmes virtuels, sous **Location (Emplacement)**, sélectionnez **Shared (Partagé)** pour les services proxy DNS globaux à l'ensemble du pare-feu.

      Les objets proxy DNS partagés n'utilisent pas de profils de serveur DNS car un itinéraire de service spécifique appartenant à un système virtuel de locataire n'est pas nécessaire.
   3. Saisissez l'adresse IP du serveur DNS **Primary (Principal)**. (Facultatif) Saisissez une adresse IP de serveur DNS **Secondary (Secondaire)**.
3. (PAN-OS 11.2.1 et versions ultérieures) (Facultatif) Configurez l'objet de proxy DNS avec un DNS chiffré.
4. Sélectionnez l'onglet **Advanced (Avancé)**. Assure-vous que l'option **Cache** est activée et que l'option **Cache EDNS Responses (Réponses EDNS Cache)** est activé (les deux options sont activées par défaut).
5. Cliquez sur **OK** pour enregistrer l'objet de proxy DNS.

STEP 4 | (Facultatif) Définissez une **Minimum FQDN Refresh Time (sec) [Fréquence d'actualisation minimale du FQDN (sec)]** pour limiter la fréquence à laquelle le pare-feu actualise les entrées de FQDN mises en cache.

Par défaut, le pare-feu actualise chaque FQDN qui figure dans sa mémoire cache en fonction de la TTL individuelle du FQDN figurant dans un enregistrement DNS, tant que la TTL est supérieure ou égale à cette fréquence d'actualisation minimale du FQDN (ou tant que la TTL est supérieur ou égale au paramètre par défaut de 30 secondes, si vous ne configurez pas de fréquence d'actualisation minimale du FQDN). Pour définir une fréquence d'actualisation minimale du FQDN, saisissez une valeur en secondes (plage comprise entre 0 et 14 400 ; valeur par défaut : 30). Si le paramètre est défini sur 0, le pare-feu actualise les FQDN en fonction de la valeur TTL des enregistrements DNS ; le pare-feu n'applique pas de fréquence d'actualisation du FQDN minimale. Le pare-feu utilise la valeur la plus élevée entre le TTL du DNS et la fréquence d'actualisation minimale du FQDN.

Si la TTL du FQDN du DNS est courte, mais que vos résolutions FQDN ne changent pas aussi souvent que le délai TTL, une fréquence d'actualisation plus rapide n'est pas nécessaire. Vous devriez donc définir une fréquence d'actualisation minimale du FQDN pour éviter d'effectuer des tentatives d'actualisation du FQDN plus souvent que nécessaire.

STEP 5 | (Facultatif) Spécifiez un **FQDN Stale Entry Timeout (min) [Délai de temporisation des entrées obsolètes du FQDN])**, qui correspond au nombre de minutes pendant lesquelles le

 ©2024 Palo Alto Networks, Inc.

pare-feu continu à utiliser les résolutions FQDN obsolètes en cas d'indisponibilité du serveur DNS (plage comprise entre 0 et 10 080 ; valeur par défaut : 1 440).

Un paramètre nul indique que le pare-feu ne continue pas d'utiliser une entrée FQDN obsolète.

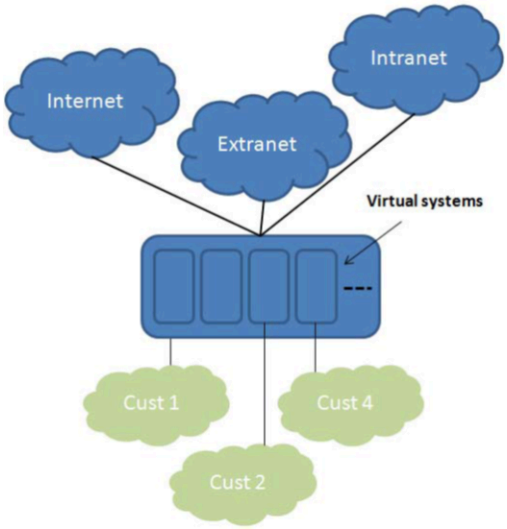
Assurez-vous que la valeur de FQDN Stale Entry Timeout (Délai de temporisation des entrées obsolètes du FQDN) est suffisamment courte pour ne pas autoriser le transfert incorrect de trafic (qui peut présenter un risque à la sécurité), mais suffisamment longue pour permettre la continuité du trafic sans causer de panne réseau non planifiée.

STEP 6 | Cliquez sur **OK**, puis sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

Cas d’utilisation 2 : Le locataire de l'ISP utilise un proxy DNS pour traiter la résolution DNS pour des politiques de sécurité, la génération de rapports et des services de son système virtuel

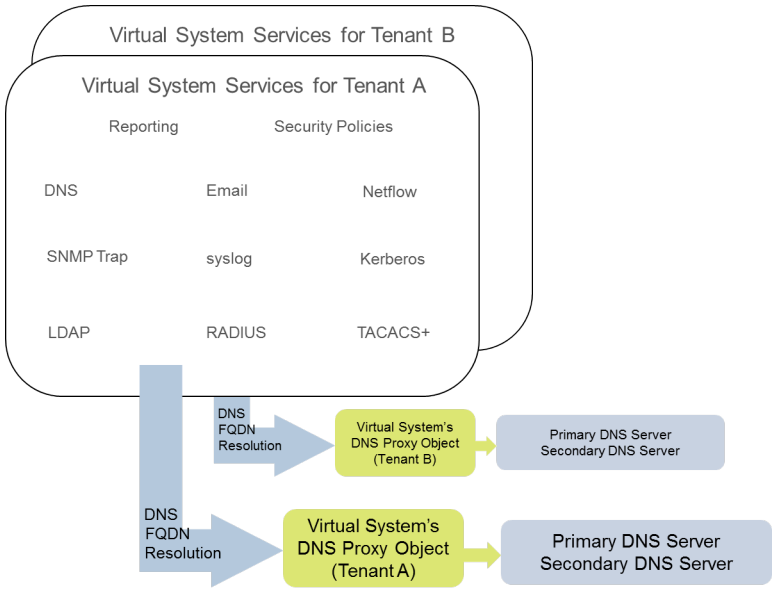
Dans ce cas pratique, plusieurs locataires (abonnés d'ISP) sont définis sur le pare-feu et chaque locataire se voit affecter un système virtuel (vsys) distinct et un routeur virtuel pour segmenter ses services et domaines administratifs. La figure ci-dessous illustre plusieurs systèmes virtuels dans un pare-feu.



Chaque locataire dispose de profils de serveur propres pour les règles de politiques de sécurité, la génération de rapport et les services de gestion (comme la messagerie, Kerberos, SNMP, Syslog, et bien d'autres encore) définis sur ses propres réseaux.

Pour les résolutions DNS lancées par ces services, chaque système virtuel est configuré avec un Objet proxy DNS propre pour permettre à chaque locataire de personnaliser la gestion de la résolution DNS dans son système virtuel. Tout service incluant un **Location (Emplacement)** utilisera l'objet proxy DNS configuré pour le système virtuel afin de déterminer le serveur DNS principal (ou secondaire) pour résoudre les FQDN, comme illustré dans la figure ci-dessous.

©2024 Palo Alto Networks, Inc.



STEP 1 | Pour chaque système virtuel, spécifiez le proxy DNS à utiliser.

1. Sélectionnez **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)** et **Add (Ajouter)** pour ajouter l'**ID (ID)** du système virtuel (plage de 1 à 255), et éventuellement un **Name (Nom)**. Dans cet exemple, Corp1 Corporation.
2. Dans l'onglet **General (Général)**, choisissez un **DNS Proxy (Proxy DNS)** ou créez-en un nouveau. Dans cet exemple, le proxy DNS Corp1 est sélectionné comme proxy du système virtuel de Corp1 Corporation.
3. Sélectionnez **Interfaces (Interfaces)**, puis cliquez sur **Add (Ajouter)**. Dans cet exemple, Ethernet1/20 est dédié à ce locataire.
4. Pour **Virtual Routers (Routeurs virtuels)**, cliquez sur **Add (Ajouter)**. Un routeur virtuel nommé Corp1 VR est associé au système virtuel pour distinguer les fonctions de routage.
5. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configurez un proxy DNS et un profil de serveur pour prendre en charge la résolution DNS pour un système virtuel.

1. Sélectionnez **Network (Réseau)** > **DNS Proxy (Proxy DNS)**, puis cliquez sur **Add (Ajouter)**.
2. Cliquez sur **Enable (Activer)** et saisissez un **Name (Nom)** pour le proxy DNS.
3. Pour **Location (Emplacement)**, sélectionnez le système virtuel du locataire, dans cet exemple, Corp1 Corporation (vsys6). (Vous pourriez également choisir la ressource de proxy DNS **Shared (Partagé)**.)
4. Pour **Server Profile (Profil de serveur)**, sélectionnez ou créez un profil afin de personnaliser les serveurs DNS à utiliser pour les résolutions DNS de la politique de sécurité, génération de rapports et services de profil de serveur de ce locataire.

   Si le profil n'est pas déjà configuré, dans le champ **Server Profile (Profil de serveur)**, cliquez sur **DNS Server Profile (Profil de serveur DNS)** pour procéder à la Configuration d'un profil de serveur DNS.

   Le profil de serveur DNS identifie les adresses IP des serveurs DNS principal et secondaire à utiliser pour la gestion des résolutions DNS de ce système virtuel.
5. Pour ce profil de serveur, vous pouvez également configurer une adresse **Service Route IPv4 (IPv4 d'itinéraire de service)** et/ou une adresse **Service Route IPv6 (IPv6 d'itinéraire de service)** pour indiquer au pare-feu la **Source Interface (Interface source)** à utiliser dans ses requêtes DNS. Si cette interface comporte plusieurs adresses IP, configurez également la **Source Address (Adresse source)**.
6. Sélectionnez l'onglet **Advanced (Avancé)**. Assure-vous que l'option **Cache** est activée et que l'option **Cache EDNS Responses (Réponses EDNS Cache)** est activé (les deux options sont activées par défaut). Cette façon de faire est obligatoire si l'objet proxy DNS est utilisé sous **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)** > **vsys** > **General (Général)** > **DNS Proxy (Proxy DNS)**.
7. Cliquez sur **OK**.
8. Cliquez sur **OK**, puis sur **Commit (Valider)**.

   *Des fonctions avancées facultatives comme la segmentation DNS peuvent être configurées à l'aide des **DNS Proxy Rules (Règles de proxy DNS)**. Un profil de serveur DNS distinct peut être utilisé pour rediriger les résolutions DNS correspondant au **Domain Name (Nom de domaine)** dans une **DNS Proxy Rule (Règle de proxy DNS)** vers un autre ensemble de serveurs DNS, si nécessaire. Le cas pratique 3 utilise la segmentation DNS.*

   Si vous utilisez deux profils de serveur DNS distincts dans un même objet proxy DNS, un pour le proxy DNS et l'autre pour la règle de proxy DNS, les comportements suivants surviennent :

   - Si un itinéraire de service est défini dans le profil de serveur DNS utilisé par le proxy DNS, il est prioritaire et est utilisé.
   - Si un itinéraire de service est défini dans le profil de serveur DNS utilisé dans les règles de proxy DNS, il n'est pas utilisé. Si l'itinéraire de service est différent de

 ©2024 Palo Alto Networks, Inc.

celui défini dans le profil de serveur DNS utilisé par le proxy DNS, le message d'avertissement suivant s'affiche pendant l'opération **Commit (Valider)** :

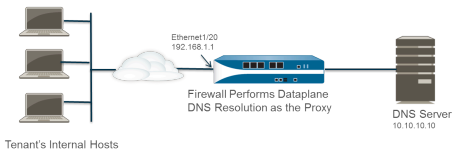
```
Attention : L’itinéraire de service DNS défini dans l’objet
 proxy DNS est différent de l’itinéraire de service de la
 règle de proxy DNS. Utilisation de l’itinéraire de service de
 l’objet proxy DNS.
```

- Si aucun itinéraire de service n'est défini dans aucun profil de serveur DNS, l'itinéraire de service global est utilisé si nécessaire.

 ©2024 Palo Alto Networks, Inc.

Cas d'utilisation 3 : Le pare-feu sert de proxy DNS entre le client et le serveur

Dans ce cas pratique, le pare-feu se trouve entre un client DNS et un serveur DNS. Un proxy DNS sur le pare-feu est configuré pour servir de serveur DNS aux hôtes se trouvant sur le réseau du locataire connecté à l'interface du pare-feu. Dans ce scénario, le pare-feu effectue la résolution DNS sur son plan de données.



Ce scénario implique l'utilisation de la *segmentation DNS*, une configuration dans laquelle des règles de proxy DNS sont configurées pour rediriger des requêtes DNS vers un ensemble de serveurs DNS en fonction d'une correspondance de nom de domaine. Si aucune correspondance n'est trouvée, le profil de serveur détermine les serveurs DNS auxquels envoyer la requête, d'où les deux méthodes de résolution DNS segmentée.

Pour les résolutions DNS du plan de données, l'adresse IP source du proxy DNS dans PAN-OS vers le serveur DNS externe serait l'adresse du proxy (l'adresse IP de destination de la requête d'origine). Les itinéraires de service définis dans le profil de serveur DNS ne sont pas utilisés. Par exemple, si la requête provient de l'hôte 172.16.1.1 vers le proxy DNS à l'adresse 192.168.1.1, la requête vers le serveur DNS (à l'adresse 10.10.10.10) devrait utiliser la source 192.168.1.1 et la destination 10.10.10.10.

STEP 1 | Sélectionnez **Network (Réseau)** > **DNS Proxy (Proxy DNS)**, puis cliquez sur **Add (Ajouter)**.

STEP 2 | Cliquez sur **Enable (Activer)** et saisissez un **Name (Nom)** pour le proxy DNS.

STEP 3 | Pour **Location (Emplacement)**, sélectionnez le système virtuel du locataire, dans cet exemple, Corp1 Corporation (vsys6).

STEP 4 | Pour **Interface (Interface)**, sélectionnez l'interface qui recevra les requêtes DNS des hôtes du locataire, dans cet exemple, Ethernet1/20.

STEP 5 | Sélectionnez ou créez un **Server Profile (Profil de serveur)** afin de personnaliser les serveurs DNS pour résoudre les requêtes DNS de ce locataire.

STEP 6 | Dans l'onglet **DNS Proxy Rules (Règles de proxy DNS)**, cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** pour la règle.

STEP 7 | (Facultatif) Cochez **Turn on caching of domains resolved by this mapping (Activer la mise en cache des domaines résolus par ce mappage)**.

STEP 8 | Cliquez sur **Add (Ajouter)** et saisissez un ou plusieurs **Domain Name (Nom de domaine)**, à raison d'une entrée par ligne. Règle de proxy DNS et correspondance FQDN décrit comment le pare-feu fait correspondre les FQDN aux noms de domaine dans une règle de proxy DNS.

©2024 Palo Alto Networks, Inc.

STEP 9 | Comme **DNS Server profile (profil de serveur DNS)**, sélectionnez un profil. Le pare-feu compare le nom de domaine dans la requête DNS avec le(s) nom(s) de domaine(s) défini(s) dans les **DNS Proxy Rules (Règles de proxy DNS)**. Si une correspondance est trouvée, le **DNS Server profile (Profil de serveur DNS)** défini dans la règle est utilisé pour déterminer le serveur DNS.

STEP 10 | Dans cet exemple, si le domaine dans la requête correspond à myweb.corp1.com, le serveur DNS défini dans le profil de serveur DNS myweb est utilisé. Si aucune correspondance n'est trouvée, le serveur DNS défini dans **Server Profile (Profil de serveur)** (profil de serveur DNS Corp1) est utilisé.

STEP 11 | Cliquez deux fois sur **OK**.

 ©2024 Palo Alto Networks, Inc.

Mise en correspondance de la règle de proxy DNS et du FQDN

Lorsque vous configurez le pare-feu avec un objet de proxy DNS qui utilise des règles de proxy DNS, le pare-feu compare un FQDN d'une requête DNS au nom de domaine d'une règle de proxy DNS. La comparaison effectuée par le pare-feu se déroule comme suit :

Comparaison entre le FQDN et la règle de proxy DNS	Par exemple
Le pare-feu décompose en jetons les FQDN et les noms de domaine dans les règles de proxy DNS. Dans un nom de domaine, une chaîne délimitée par un point (.) est un jeton.	**`*.boat.fish.com`** comprend quatre jetons : **`[*] [boat][fish][com]`**
Le processus de mise en correspondance est une mise en correspondance exacte des jetons du FQDN et du nom de domaine dans la règle ; les chaînes partielles ne sont pas mises en correspondance.	Règle : **`hameçonnage`** FQDN :**`hameçon`** : **aucune correspondance**
L'utilisation de l'astérisque (*) est une exception à la règle de la correspondance exacte. L'astérisque (*) correspond à un ou plusieurs jetons. C'est-à-dire qu'une règle qui ne comprend qu'un caractère générique (*) est mise en correspondance avec tout FQDN qui comporte un ou plusieurs jetons.	Règle : **`*.boat.com`** FQDN : **`www.boat.com`** : correspondance FQDN : **`www.blue.boat.com`** : correspondance FQDN : **`boat.com`** : **aucune correspondance**
	Règle : **`*`** FQDN : **`boat`** : correspondance FQDN : **`www.boat.com`** : correspondance FQDN : **`www.boat.com`** : correspondance
Vous pouvez utiliser l'astérisque (*) à n'importe quelle position : devant les jetons, entre les jetons ou après les jetons (mais il ne faut pas la jumeler à d'autres caractères à l'intérieur d'un jeton simple).	Règle : **`www.*.com`** FQDN : **`www.boat.com`** : correspondance FQDN : **`www.blue.boat.com`** : correspondance
	Règle : **`www.boat.*`** FQDN : **`www.boat.com`** : correspondance

©2024 Palo Alto Networks, Inc.

Comparaison entre le FQDN et la règle de proxy DNS	Par exemple
	FQDN : **www.boat.fish.com** : correspondance
	Règle : **www.boat*.com** : **non valide**
Plusieurs caractères génériques (*) peuvent apparaître à n'importe quelle position du nom de domaine : devant les jetons, entre les jetons ou après les jetons. Chaque astérisque (*) non consécutif correspond à un ou plusieurs jetons.	Règle : **a.*.d.*.com** FQDN : **a.b.d.e.com** : correspondance FQDN : **a.b.c.d.e.f.com** : correspondance FQDN : **a.d.d.e.f.com** : correspondance (Le premier astérisque (*****) est mis en correspondance avec le **d** ; le deuxième astérisque (*****) est mis en correspondance avec le **e** et le **f**.) FQDN : **a.d.e.f.com** : **aucune correspondance** (Le premier astérisque (*****) est mis en correspondance avec le **d** ; le deuxième **d** de la règle n'est pas mis en correspondance.)
Lorsque des caractères génériques sont utilisés dans des jetons consécutifs, le premier astérisque (*) est mis en correspondance avec un ou plusieurs jetons ; le second astérisque (*) est mis en correspondance avec un jeton. C'est-à-dire qu'une règle qui ne comprend que *.* est mise en correspondance avec tout FQDN qui comporte au moins deux jetons.	Caractères génériques devant les jetons : Règle : ***.*.boat.com** FQDN : **www.blue.boat.com** : correspondance FQDN : **www.blue.sail.boat.com** : correspondance
	Caractères génériques entre des jetons : Règle : **www.*.*.boat.com** FQDN : **www.blue.sail.boat.com** : correspondance FQDN: **www.big.blue.sail.boat.com** : correspondance
	Caractères génériques après les jetons : Règle : **www.boat.*.*** FQDN : **www.boat.fish.com** : correspondance FQDN : **www.boat.fish.ocean.com** : correspondance

 ©2024 Palo Alto Networks, Inc.

Comparaison entre le FQDN et la règle de proxy DNS	Par exemple
	Caractères génériques uniquement : Règle : *.* FQDN : **boat** : **aucune correspondance** FQDN : **www.boat.com** : correspondance FQDN : **www.boat.com** : correspondance
Des caractères génériques consécutifs et non consécutifs peuvent apparaître dans la même règle.	Règle : **a.*.d.*.*.com** FQDN : **a.b.c.d.e.f.com** : correspondance (Le premier astérisque (*) est mis en correspondance avec le **b** et le **c** ; le deuxième astérisque (*) est mis en correspondance avec le **e** ; le troisième astérisque (*) est mis en correspondance avec le **f**.) FQDN : **a.b.c.d.e.com** : **aucune correspondance** (Le premier astérisque (*) est mis en correspondance avec le **b** et le **c** ; le deuxième astérisque (*) est mis en correspondance avec le **e** ; le troisième astérisque (*) n'est pas mis en correspondance.)
Le comportement de la règle de correspondance implicite des éléments de queue fournit un autre raccourci : Tant que le dernier jeton de la règle n'est pas un astérisque (*), une comparaison sera mise en correspondance si tous les jetons de la règle correspondent au FQDN, même lorsque le FQDN possède des jetons de droite que la règle ne possède pas.	Règle : **www.boat.fish** FQDN : **www.boat.fish.com** : correspondance FQDN : **www.boat.fish.ocean.com** : correspondance FQDN : **www.boat.fish** : correspondance
Cette règle se termine pas un astérisque (*), la règle de correspondance implicite des éléments de queue ne s'applique donc pas. L'astérisque (*) se comporte comme tel ; il correspond à un ou plusieurs jetons.	Règle : **www.boat.fish.*** FQDN : **www.boat.fish.com** : correspondance FQDN : **www.boat.fish.ocean.com** : correspondance FQDN : **www.boat.fish** : **aucune correspondance** (aucun jeton de ce FQDN ne peut être mis en correspondance avec l'astérisque (*) de la règle.)
Dans l'éventualité où un FQDN correspond à plus d'une règle,	Règle 1 : ***.fish.com** : correspondance Règle 2 : ***.com** : correspondance

 ©2024 Palo Alto Networks, Inc.

Comparaison entre le FQDN et la règle de proxy DNS	Par exemple
un algorithme de partage permet sélectionne la règle la plus précise (la plus longue) ; c'est-à-dire que l'algorithme privilégie la règle qui contient le plus grand nombre de jetons et le plus faible nombre de caractères génériques (*).	Règle 3 : **boat.fish.com** : correspondance et partage FQDN : **boat.fish.com** Le FQDN est mis en correspondance avec les trois règles ; le pare-feu se sert de la Règle 3, car c'est elle qui est la plus précise.
	Règle 1 : ***.fish.com** : **aucune correspondance** Règle 2 : ***.com** : correspondance Règle 3 : **boat.fish.com** : **aucune correspondance** FQDN : **fish.com** Le FQDN ne peut être mis en correspondance avec la Règle 1, car l'astérisque (*) ne peut correspondre à aucun jeton.
	Règle 1 : ***.fish.com** : correspondance et partage Règle 2 : ***.com** : correspondance Règle 3 : **boat.fish.com** : **aucune correspondance** FQDN : **blue.boat.fish.com** Le FQDN est mis en correspondance avec la Règle 1 et la Règle 2 (parce que l'astérisque (*) correspond à au moins un jeton). Le pare-feu se sert de la Règle 1, car c'est elle qui est la plus précise.
Lorsque vous travaillez avec des caractères génériques (*) et les règles de correspondance implicite des éléments de queue, il se peut que le FQDN corresponde à plus d'une règle et que l'algorithme de partage considère que les règles ont la même importance. Pour éviter toute ambiguïté, si les règles qui possèdent une correspondance implicite des éléments de queue ou un caractère générique (*) peuvent se chevaucher, remplacez une règle de correspondance implicite des éléments de queue en précisant le jeton de queue.	Remplacez cette : Règle : **www.boat** par cette : Règle : **www.boat.com**

©2024 Palo Alto Networks, Inc.

Comparaison entre le FQDN et la règle de proxy DNS	Par exemple
Lorsque vous créez des règles de proxy DNS, il est recommandé d'éviter toute ambiguïté et tous résultats inattendus.	
Incluez un domaine de premier niveau dans le nom de domaine pour éviter d'invoquer une correspondance implicite des éléments de queue qui pourrait faire correspondre le FQDN à plus d'une règle.	**boat.com**
Si vous utilisez un caractère générique (*), utilisez-le uniquement pour représenter le jeton de gauche. Cette approche respecte la compréhension commun des enregistrements de caractères génériques DNS et la nature hiérarchique de DNS.	***.boat.com**
N'utilisez pas plus d'un astérisque (*) par règle.	
Utilisez l'astérisque (*) pour établir une règle de base associée avec un serveur DNS, et utilisez les règles contenant un plus grand nombre de jetons pour créer des exceptions à la règle, que vous pouvez associer aux différents serveurs. L'algorithme de partage sélectionnera la correspondance la plus précise, selon le nombre de jetons qui ont été mis en correspondance.	Règle : ***.corporation.com** : serveur DNS A Règle :**www.corporation.com** : serveur DNS B Règle : ***.internal.corporation.com** : serveur DNS C Règle :**www.internal.corporation.com** : serveur DNS D FQDN : **mail.internal.corporation.com** : correspondance avec le serveur DNS C FQDN : **mail.corporation.com** : correspondance avec le serveur DNS A

©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

DDNS

Découvrez comment le service DNS dynamique (DDNS) met à jour les mappages des noms de domaine aux adresses IP pour fournir des adresses IP précises aux clients DNS.

- Présentation des DNS dynamiques
- Configuration des DNS dynamiques pour les interfaces du pare-feu

Présentation des DNS dynamiques

Lorsque des services sont hébergés derrière le pare-feu et que vous utilisez des politiques NAT de destination sur le pare-feu pour accéder à ces services ou lorsque vous devez fournir un accès à distance au pare-feu, vous pouvez enregistrer les modifications d'adresses IPv4 (que l'interface soit un client DHCP qui reçoit une adresse dynamique ou qui possède une statique) ou les modifications d'adresses IPv6 (adresse statique uniquement) pour l'interface ayant un fournisseur de services DNS dynamique (DDNS). Le service dDNS met automatiquement à jour les mappages nom de domaine/adresse IP pour fournir des adresses IP exactes aux clients DNS, qui, à leur tour, peuvent accéder au pare-feu et aux services derrière le pare-feu. DDNS est souvent utilisé dans les déploiements de branches qui hébergent des services. Sans la prise en charge DDNS pour les interfaces du pare-feu, vous auriez besoin de composantes externes pour fournir des adresses IP exactes aux clients.

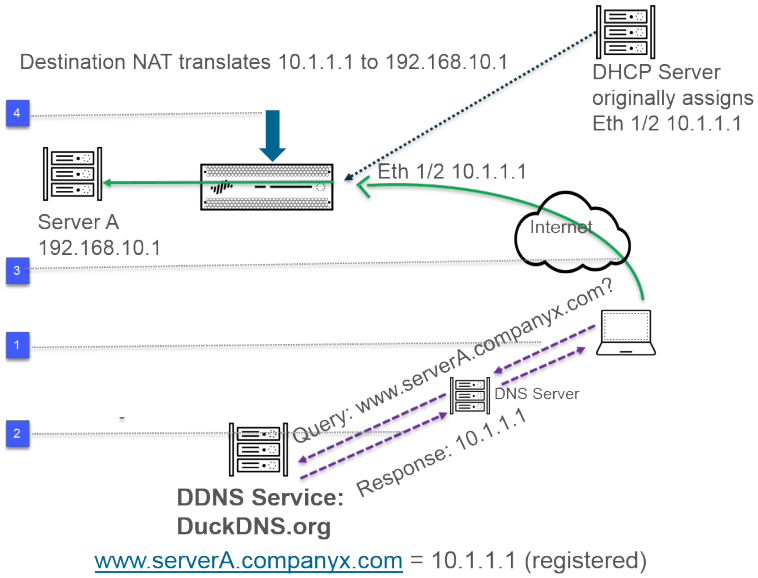
Le pare-feu prend en charge les fournisseurs de service DDNS suivants : DuckDNS, DynDNS, FreeDNS Afraid.org Dynamic API, FreeDNS Afraid.org et No-IP. Le fournisseur de service DDNS individuel détermine les services qu'il fournit, comme le nombre d'adresses IP qu'il prend en charge pour un nom d'hôte et s'il prend en charge les adresses IPv6. Palo Alto Networks® utilise les mises à jour du contenu pour ajouter de nouveaux fournisseurs de service DDNS et pour fournir des mises à jour à leurs services.

Pour les configuration HA, assurez-vous que les versions du contenu qui sont installées sur les pare-feu homologues HA (actif/passive ou actif/actif) sont synchronisées, car le pare-feu préserve la configuration DDNS en fonction de la version de contenu Palo Alto Networks actuelle. Palo Alto Networks peut modifier ou rabaisser les services DDNS existants dans le cadre d'une version de contenu. De plus, un fournisseurs de service DDNS peut modifier les services qu'il offre. Une inadéquation des versions de contenu utilisées par les homologues HA peuvent causer des problèmes quant à leur capacité à utiliser le service DDNS.

Le pare-feu ne prend pas en charge DDNS sur une interface qui est un point de terminaison Point-to-Point Protocol over Ethernet (protocole point-à-point sur Ethernet ; PPPoE).

Dans l'exemple suivant, le pare-feu est un client DDNS d'un fournisseur de service DDNS. Initialement, le serveur DHCP affecte l'adresse IP 10.1.1.1 à l'interface Ethernet 1/2. Une politique NAT de destination traduit l'adresse publique 10.1.1.1 en l'adresse réelle du serveur A (192.168.10.1), situé derrière le pare-feu.

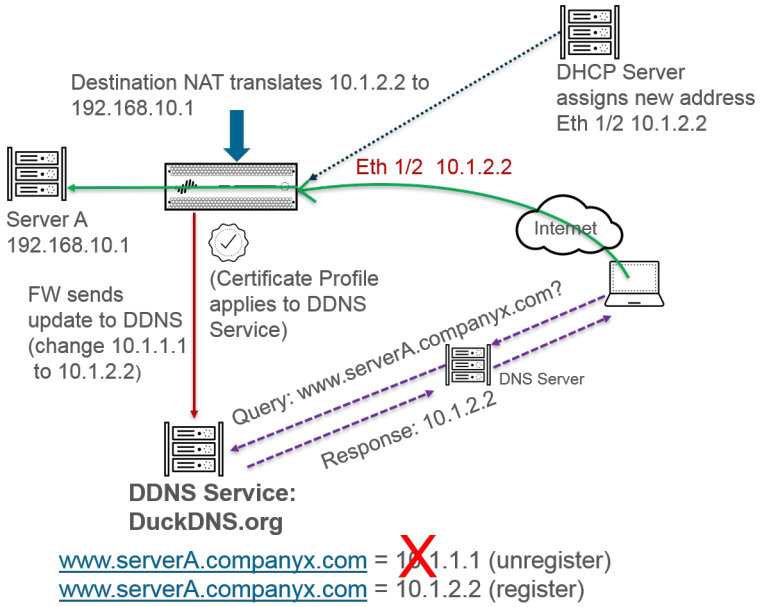
©2024 Palo Alto Networks, Inc.



1. Lorsqu'un utilisateur tente de contacter www.serveurA.compagniex.com, l'utilisateur interroge son serveur DNS local afin d'obtenir l'adresse IP. Le www.serveurA.compagniex.com (défini, par exemple, en tant que CNAME de votre enregistrement duckdns.org : serveurA.compagniex.duckdns.org) est un domaine qui appartient au fournisseur DDNS (DuckDNS dans l'exemple présent). Le serveur DNS cherche l'enregistrement auprès du fournisseur DDNS pour résoudre la requête.
2. Le serveur DNS répond à l'utilisateur en indiquant 10.1.1.1, soit l'adresse IP de www.serveurA.compagniex.com.
3. Le paquet de l'utilisateur dont la destination est 10.1.1.1 se rend à l'interface Ethernet 1/2 du pare-feu.
4. Dans cet exemple, le pare-feu effectue la NAT de destination et traduit 10.1.1.1 en 192.168.11.1 avant d'envoyer le paquet à sa destination.

Après un certain temps, DHCP affecte une nouvelle adresse IP à l'interface du pare-feu, ce qui déclenche une mise à jour DDNS, comme suit :

 ©2024 Palo Alto Networks, Inc.



1. Le serveur DHCP affecte une nouvelle adresse IP (10.1.2.2) à l'interface Ethernet 1/2.
2. Lorsque le pare-feu reçoit la nouvelle adresse, il envoie une mise à jour au service DDNS contenant la nouvelle adresse de www.serveurA.compagniex.com, que le service DDNS enregistre. (Le pare-feu envoie également des mises à jour régulières selon l'intervalle de mise à jour que vous avez configuré. Le pare-feu envoie les mises à jour DDNS sur le port HTTPS 443.)

Par conséquent, la prochaine fois que le client interroge le serveur DNS au sujet de l'adresse IP de www.serveurA.compagniex.com et que le serveur DNS vérifie auprès du service DDNS, le service DDNS envoie l'adresse mise à jour (10.1.2.2). Ainsi, l'utilisateur réussit à accéder à un service ou à une application par l'intermédiaire de l'interface du pare-feu en utilisant l'adresse mise à jour de l'interface.

Si votre pare-feu est configuré pour le mode HA actif/passif, sachez que le pare-feu envoie les mises à jour DDNS au service DNS lorsque les deux états des pare-feu HA convergent. Une fois que les états HA ont convergé, DDNS est désactivé sur le pare-feu passif. Par exemple, lors du démarrage initial des deux pare-feu HA, ils envoient tous deux des mises à jour DDNS jusqu'à ce qu'ils établissent s'ils sont en mode HA actif ou passif. Au cours de cet intervalle, des mises à jour DDNS sont toujours présentes dans les journaux systèmes. Une fois que la convergence des états HA est terminée et que chaque pare-feu a avise ses clients de son état (actif ou passif), le pare-feu passif n'envoie plus de mises à jour DDNS. (En mode HA actif/actif, chaque pare-feu possède une configuration DDNS indépendante. La configuration DDNS n'est donc pas synchronisée.)

 ©2024 Palo Alto Networks, Inc.

Configuration des DNS dynamiques pour les interfaces du pare-feu

Avant de configurer DDNS pour une interface de pare-feu :

- Déterminez le nom d'hôte que vous avez enregistré auprès de votre fournisseur DDNS.
- Obtenez le certificat SSL public du service DDNS et importez-le dans le pare-feu.
- (Si vous utilisez FreeDNS Afraid.org v1 ou FreeDNS Afraid.org Dynamic API v1) Sur le serveur DDNS, l'onglet Service DNS dynamique comprend l'option suivante : **Link updates of the same IP together? (Lier les mises à jour de la même adresse IP?)** Lorsque cette option est activée, le service DDNS met à jour tous les noms d'hôte dans les enregistrements DNS qui contiennent la vieille adresse IP qui change, et pas seulement l'enregistrement DNS d'un seul nom d'hôte et d'adresse IP. Pour éviter de mettre à jour les enregistrements DNS des hôtes que vous n'aviez pas l'intention de mettre à jour, vous devrez désactiver l'option **Link updates of the same IP together? (Lier les mises à jour de la même adresse IP?)** pour que le serveur DDNS mette uniquement à jour l'enregistrement DNS qui contient le nom d'hôte spécifique avec la nouvelle adresse IP qui se trouve dans la mise à jour DDNS.

STEP 1 | Configurez DDNS.

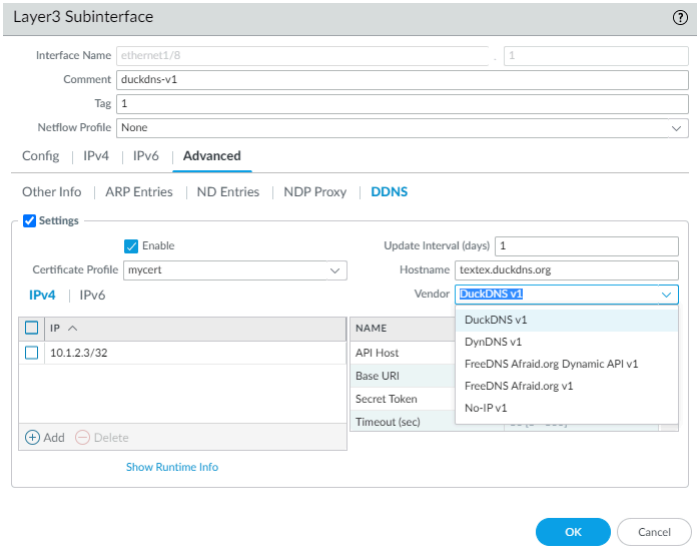
1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**, puis sélectionnez une interface de couche 3, une sous-interface ou une interface Aggregate Ethernet (AE) ; ou sélectionnez **Network (Réseau)** > **Interfaces** > **VLAN** et sélectionnez une interface ou une sous-interface.
2. Sélectionnez **Advanced (Avancé)** > **DDNS**, puis sélectionnez **Settings (Paramètres).**.
3. **Enable (Activez)** DDNS. Vous devez d'abord activer DDNS pour le configurer. (Si vous n'avez pas terminé de configurer DDNS, vous pouvez enregistrer la configuration sans l'activer, ce qui vous évitera de perdre la configuration partielle.)
4. Saisissez le **Update Interval (days) [Intervalle de mise à jour (jours)]**, c'est-à-dire le nombre de jours entre les mises à jour que le pare-feu envoie au service DDNS pour mettre à jour les adresses IP associées aux FQDN (la plage est comprise entre 1 et 30 ; la valeur par défaut est 1). Choisissez un intervalle basé sur la fréquence à laquelle vos adresses IP changent. (Les mises à jour que le pare-feu envoie à intervalles réguliers s'ajoutent aux mises à jour que le pare-feu envoie lors de la réception d'un changement d'adresse. Les mises à jour envoyées à intervalles réguliers visent à s'assurer que les mises à jour envoyées lors d'un changement d'adresse ne sont pas perdues, par exemple.)
5. Saisissez un **Hostname (Nom d'hôte)** pour l'interface, qui est déjà inscrit auprès du serveur DDNS (par exemple, www.serveurA.societex.com ou serveurA).

   Assurez-vous que ce nom d'hôte correspond au nom d'hôte que vous avez enregistré auprès de votre service DDNS. Vous devriez saisir un FQDN pour le nom d'hôte ; le pare-feu ne valide pas le nom d'hôte, sauf pour confirmer que la syntaxe utilise uniquement les caractères valides autorisés par DNS pour un nom de domaine.
6. Sélectionnez **IPv4** et sélectionnez une ou plusieurs adresses IPv4 attribuées à l'interface ou **Add (Ajoutez)** une adresse IPv4 à associer au nom d'hôte (par exemple, 10.1.1.1).

 ©2024 Palo Alto Networks, Inc.

Vous pouvez sélectionner le nombre d'adresses IPv4 que le serveur DDNS permet. Toutes les adresses IPv4 sélectionnées sont enregistrées auprès du fournisseur DDNS. Sélectionnez au moins une adresse IPv4 ou une adresse IPv6.

7. Sélectionnez **IPv6** et sélectionnez une ou plusieurs adresses IPv6 attribuées à l'interface ou **Add (Ajoutez)** une adresse IPv6 à associer au nom d'hôte. Vous pouvez sélectionner le nombre d'adresses IPv6 que le serveur DDNS permet. Toutes les adresses IPv6 sélectionnées sont enregistrées auprès du fournisseur DDNS. Sélectionnez au moins une adresse IPv4 ou une adresse IPv6.
8. Sélectionnez ou créez un nouveau profil de certificat (**Certificate Profile [Profil de certificat]**) à l'aide du certificat SSL importé depuis le service DDNS pour vérifier le certificat SSL du service DDNS lorsque le premier pare-feu se connecte à un service DDNS pour enregistrer une adresse IP et à chaque mise à jour. Lorsque le pare-feu se connecte au service DDNS pour envoyer des mises à jour, le service DDNS présente au pare-feu un certificat SSL signé par l'autorité de certification, pour que le pare-feu puisse authentifier le service DDNS.
9. Sélectionnez le **Vendor (Fournisseur)** (et le numéro de version) que vous utilisez pour le service DDNS.



Palo Alto Networks® pourrait modifier les fournisseurs de service DDNS pris en charge via une mise à jour de contenu.

Dans le champ Fournisseur, la sélection Palo Alto Network DDNS est un service DDNS réservé pour les fonctionnalités Palo Alto Networks telles que SD-WAN et ZTP, et ne doit pas être sélectionnée pour cette tâche en cours. Si vous sélectionnez par erreur Palo Alto Networks DDNS alors que la fonctionnalité de prise en charge correspondante n'est pas activée, un message d'erreur s'affiche.

10. Le choix de fournisseur détermine les champs **Name (Nom)** et **Value (Valeur)** propres au fournisseur sous le champ relatif à ce dernier. Certains champs de valeur sont en lecture seule pour vous aviser des paramètres que le pare-feu utiliser pour se connecter au service DDNS. Configurez les autres champs de valeur, comme un mot de passe que le service DDNS vous fournit et le délai que le pare-feu utilise s'il ne reçoit pas de mise à jour du service DDNS.

 ©2024 Palo Alto Networks, Inc.

11. Cliquez sur **OK**.

STEP 2 | (Facultatif) Si vous voulez que le pare-feu communiquer avec le service DDNS à l'aide d'une interface autre qu'une interface de gestion, configurez un itinéraire de service pour DDNS (Configuration de l'accès réseau pour les services externes).

STEP 3 | **Commit (Validez)** vos modifications.

STEP 4 | Affichez les informations DDNS pour l'interface.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**ou **Network (Réseau)** > **Interfaces** > **VLAN**, puis sélectionnez l'interface que vous avez configurée. (Les interfaces pour lesquelles DDNS a été configuré affiche l'icône DDNS [] dans le champ Features [Fonctions]).
2. Sélectionnez **Advanced (Avancé)** > **DDNS**, puis sélectionnez **Settings (Paramètres)**..
3. Cliquez sur **Show Runtime Info (Afficher les informations d'exécution)** pour voir les informations DDNS pour l'interface, u compris le dernier code retour (résultat de la dernière mise à jour du FQDN) et la dernière fois (date et heure) où le service DDNS à reçu une mise à jour FQDN.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

NAT

Cette section décrit la Network Address Translation (traduction d'adresse réseau ; NAT), ainsi que la configuration des fonctions NAT sur le pare-feu. NAT vous permet de traduire les adresses IPv4 privées non routables en une ou plusieurs adresses IPv4 globalement routables, conservant ainsi les adresses IP routables d'une entreprise. NAT vous permet de ne pas révéler les adresses IP réelles des hôtes qui ont besoin d'accéder aux adresses publiques et de gérer le trafic en effectuant le réacheminement des ports. Vous pouvez utiliser NAT pour résoudre des problèmes de conception réseau et permettre ainsi aux réseaux disposant de sous-réseaux IP identiques de communiquer entre eux. Le pare-feu prend en charge NAT sur les interfaces de Couche 3 et de câble virtuel.

L'option NAT64 effectue la traduction entre les adresses IPv6 et IPv4, permettant d'établir la connexion entre des réseaux utilisant différents modèles d'adressage IP et, par conséquent, un chemin de migration vers l'adressage IPv6. IPv6-to-IPv6 Network Prefix Translation (NPTv6) (traduction du préfixe réseau IPv6 ;) traduit un préfixe IPv6 en un autre préfixe IPv6. PAN-OS prend en charge toutes ces fonctions

Si vous utilisez des adresses IP privées dans vos réseaux internes, vous devez utiliser NAT pour traduire les adresses privées en adresses publiques pouvant être acheminées sur des réseaux externes. Dans PAN-OS, créez des règles de politique NAT indiquant au pare-feu les adresses et les ports des paquets devant être traduits ainsi que les adresses et les ports traduits.

- Règles de politique NAT
- NAT source et NAT de destination
- NAT de destination avec cas d’utilisation de la réécriture DNS
- Nombre de règles NAT
- Dépassement d'abonnement NAT DIPP
- Statistiques de la mémoire NAT du plan de données
- Configuration de NAT
- Exemples de configuration NAT

Règles de politique NAT

- Présentation de la politique NAT
- Pools d'adresses NAT identifiés comme des objets adresse
- Proxy ARP pour les pools d'adresses NAT

Présentation de la politique NAT

Configurez une règle NAT pour mettre en correspondance au moins la zone source et la zone de destination d'un paquet. Outre les zones, vous pouvez configurer des critères de correspondance en fonction du service, de l'adresse source et de destination, et de l'interface de destination du paquet. Vous pouvez configurer plusieurs règles NAT. Le pare-feu évalue les règles dans l'ordre de haut en bas. Une fois qu'un paquet correspond aux critères d'une règle NAT, le paquet n'est pas soumis à d'autres règles NAT. Par conséquent, votre liste de règles NAT doit être ordonnée de la plus spécifique à la moins spécifique, de manière à ce que les paquets soient soumis à la règle la plus spécifique créée pour eux.

Il est important de comprendre que dans les règles de stratégie de pare-feu (y compris NAT), l'ensemble d'adresses IPv4 est traité comme un sous-ensemble de l'ensemble d'adresses IPv6. Toutefois, l'ensemble d'adresses IPv6 n'est pas un sous-ensemble de l'ensemble d'adresses IPv4. Une adresse IPv4 peut correspondre à un ensemble ou à une plage d'adresses IPv6 ; mais une adresse IPv6 ne peut pas correspondre à un ensemble ou à une plage d'adresses IPv4.

Dans tous les types de stratégie, le mot-clé **any** pour une adresse source ou de destination désigne toute adresse IPv4 ou IPv6. Le mot-clé **any** est équivalent à ::/0. Si vous souhaitez exprimer « n'importe quelle adresse IPv4 », spécifiez 0.0.0.0/0.

Lors de la correspondance de stratégie, le pare-feu convertit une adresse IPv4 en un préfixe IPv6 où les 96 premiers bits sont 0. Une adresse de ::/8 signifie correspondre à la règle si les 8 premiers bits sont 0. Toutes les adresses IPv4 correspondront à ::/8, ::/9, ::/10, ::/11, ... ::/16, ... ::/32, ... jusqu'à ::/96.

Si vous souhaitez exprimer « n'importe quelle adresse IPv6, mais pas d'adresse IPv4 », vous devez configurer deux règles. La première règle refuse 0.0.0.0/0 pour refuser toute adresse IPv4 (en tant qu'adresse source ou de destination), et la seconde règle a ::/0 pour désigner toute adresse IPv6 (en tant qu'adresse source ou de destination), pour répondre à vos besoins.

Les règles NAT statiques sont prioritaires par rapport aux autres formes de NAT. Par conséquent, pour que NAT statique fonctionne, les règles NAT statiques doivent se trouver au-dessus de toutes les autres règles NAT de la liste sur le pare-feu.

Les règles NAT permettent la traduction d'adresses et sont différentes des règles de politique de sécurité, qui autorisent ou refusent des paquets. Il est important de comprendre la logique de flux du pare-feu lorsqu'il applique des règles NAT et des règles de politique de sécurité afin de pouvoir déterminer les règles dont vous avez besoin en fonction des zones que vous avez définies. Vous devez configurer des règles de politique de sécurité pour autoriser le trafic NAT.

Dès l'entrée d'un paquet, le pare-feu l'inspecte et effectue une recherche d'itinéraire pour déterminer l'interface et la zone de sortie. Ensuite, le pare-feu détermine si le paquet correspond à l'une des règles NAT définies, en fonction de la zone source et/ou de destination. Il évalue et applique ensuite toute politique de sécurité correspondant au paquet en fonction des adresses

 ©2024 Palo Alto Networks, Inc.

sources et de destination d'origine (pré-NAT), ainsi que des zones post-NAT. Enfin, à la sortie du paquet, pour une règle NAT correspondante, le pare-feu traduit l'adresse source et/ou de destination, ainsi que les numéros de ports.

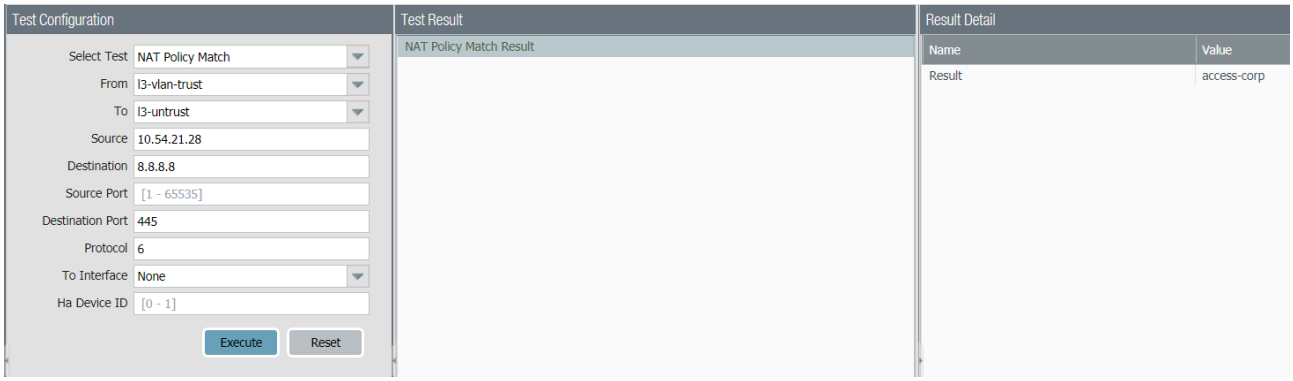
N'oubliez pas que la traduction de l'adresse IP et du port n'est effectuée qu'au moment où le paquet quitte le pare-feu. Les règles NAT et les politiques de sécurité s'appliquent à l'adresse IP d'origine (l'adresse pré-NAT). Une règle NAT est configurée en fonction de la zone associée à une adresse IP pré-NAT.

Les politiques de sécurité diffèrent des règles NAT, car elles examinent les zones post-NAT pour déterminer si le paquet est autorisé ou non. Comme la nature même de NAT est de modifier les adresses source ou de destination, ce qui peut entraîner la modification de l'interface et de la zone sortantes du paquet, les politiques de sécurité sont appliquées à la zone post-NAT.

Il arrive parfois que le son d'un appel SIP ne fonctionne que dans un sens lorsque ce dernier traverse le pare-feu, parce que le gestionnaire de l'appel envoie un message SIP pour le téléphone afin d'établir la connexion. Lorsque le message du gestionnaire de l'appel atteint le pare-feu, le SIP ALG doit faire transiter l'adresse IP de l'appel par la NAT. Si le gestionnaire de l'appel et les téléphones ne se trouvent pas dans la même zone de sécurité, la recherche NAT de l'adresse IP du téléphone se fait à partir de la zone du gestionnaire de l'appel. La politique NAT doit tenir compte de cet élément.

Les règles non NAT sont configurées de manière à autoriser l'exclusion d'adresses IP spécifiées dans la plage des règles NAT définies ultérieurement dans la politique NAT. Pour définir une politique non NAT, précisez l'ensemble des critères de correspondance et sélectionnez No Source Translation (Pas de traduction source) dans la colonne adéquate.

Vous pouvez vérifier les règles NAT traitées en sélectionnant **Device (Périphérique)** > **Troubleshooting (Résolution des problèmes)** et en testant les correspondances de trafic pour la règle NAT. Par exemple :



Pools d'adresses NAT identifiés comme des objets adresse

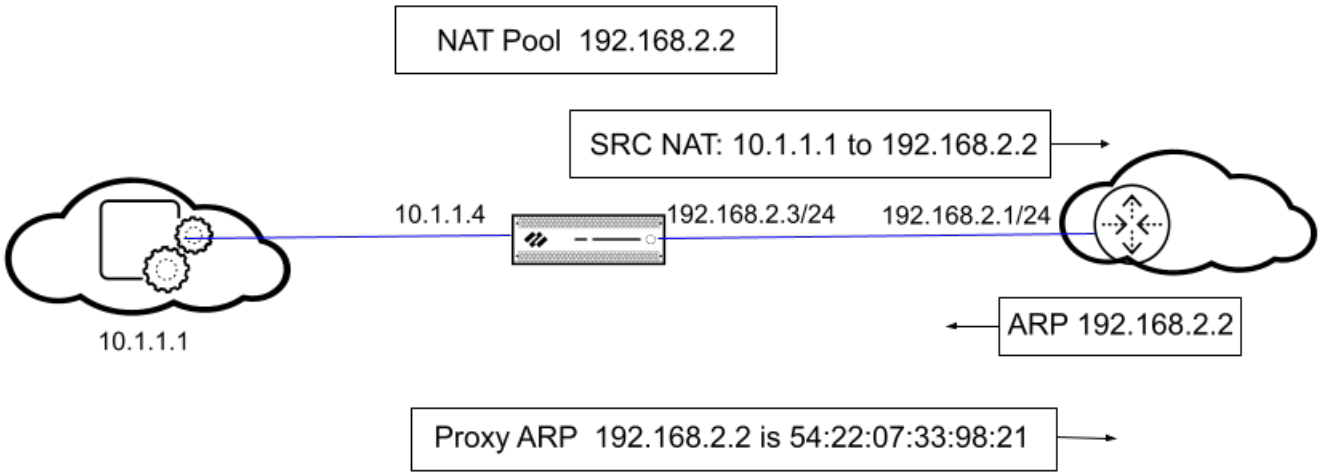
Lors de la configuration d'un pool d'adresses NAT **Dynamic IP (Adresse IP dynamique)** ou **Dynamic IP and Port (Adresse IP et port dynamiques)** dans une règle de politique NAT, il est courant de configurer le pool d'adresses traduites avec des objets adresse. Chaque objet adresse peut être une adresse IP hôte, une plage d'adresses IP ou un sous-réseau IP.

 ©2024 Palo Alto Networks, Inc.

Comme les règles NAT et les règles de politique de sécurité utilisent des objets adresse, il est recommandé de les différencier en nommant un objet adresse utilisé pour NAT avec un préfixe, tel que « NAT-nom ».

Proxy ARP pour les pools d'adresses NAT

Les pools d'adresses NAT ne sont liés à aucune interface. La figure suivante illustre le comportement du pare-feu lorsqu'il utilise le proxy ARP pour une adresse d'un pool d'adresses NAT.



Le pare-feu procède à la NAT source d'un client, traduisant l'adresse source 10.1.1.1 vers l'adresse 192.168.2.2. du pool NAT. Le paquet traduit est envoyé à un routeur.

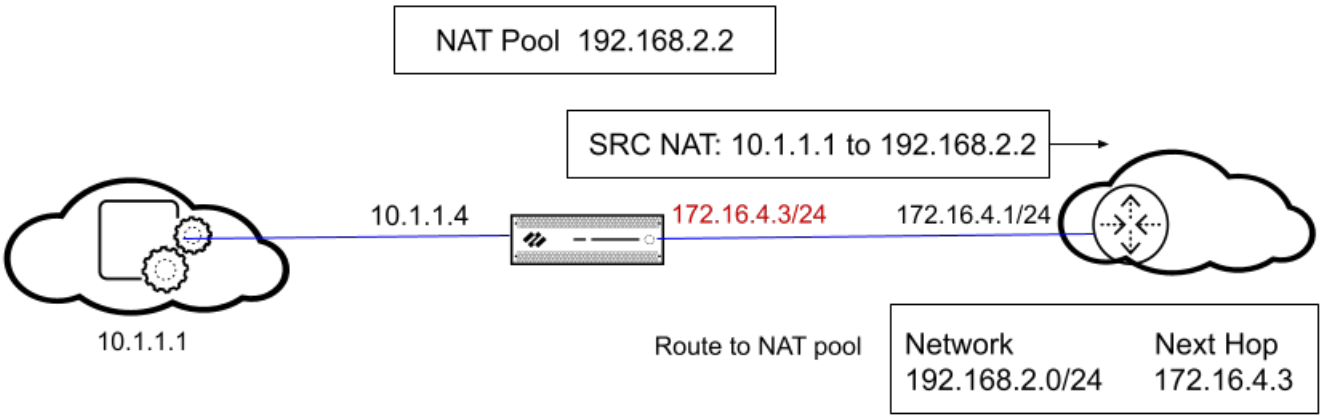
Pour le trafic de retour, le routeur ne sait pas comment atteindre 192.168.2.2 (car cette adresse IP n'est qu'une adresse du pool d'adresses NAT) ; par conséquent, il envoie un paquet de requête ARP au pare-feu.

Dans notre premier scénario, lorsque l'adresse du pool NAT (192.168.2.2) se trouve dans le même sous-réseau que l'adresse IP de l'interface de sortie/d'entrée (192.168.2.3/24), le pare-feu peut envoyer une réponse de proxy ARP au routeur, spécifiant que l'adresse MAC de couche 2 pour 192.168.2.2 est 54:22:07:33:98:21, comme indiqué dans la figure ci-dessus.

Pas de proxy ARP lorsque l'adresse du pool NAT n'est pas un sous-réseau de l'interface de sortie/d'entrée

Dans notre deuxième scénario, l'adresse du pool NAT (192.168.2.2) n'est pas un sous-réseau d'une interface sur le pare-feu. Le pare-feu n'enverra donc pas de réponse de proxy ARP au routeur. Le routeur doit ainsi être configuré avec l'itinéraire nécessaire pour savoir où envoyer des paquets destinés à 192.168.2.2, afin de s'assurer que le trafic de retour est réacheminé vers le pare-feu, comme indiqué dans la figure ci-dessous.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

NAT source et NAT de destination

Le pare-feu prend en charge la traduction de l'adresse et/ou du port source et la traduction de l'adresse et/ou du port de destination.

- NAT source
- NAT de destination

NAT source

La NAT source est généralement utilisée par des utilisateurs internes pour accéder à Internet ; l'adresse source est traduite et ainsi gardée privée. Il existe plusieurs types de NAT source : IP statique, IP dynamique et IP et port dynamiques (DIPP). Un DIPP peut être configuré comme non persistant ou persistant.

- **Adresse IP statique** : permet la traduction statique, un à un, d'une adresse IP source, mais laisse le port source inchangé. Un scénario courant de traduction d'adresses IP statiques est un serveur interne qui doit être accessible par Internet.
- **Adresse IP dynamique** : permet la traduction dynamique, 1 à 1, d'une adresse IP source uniquement (pas du numéro de port) vers l'adresse disponible suivante du pool d'adresses NAT. La taille du pool NAT doit être égale au nombre d'hôtes internes qui nécessitent des traductions d'adresses. Par défaut, si le pool d'adresses source est plus important que le pool d'adresses NAT et si toutes les adresses NAT ont été affectées, les nouvelles connexions qui ont besoin d'être traduites sont perdues. Pour remplacer ce comportement par défaut, utilisez **Advanced (Dynamic IP/Port Fallback) (Avancé (DIPP de secours))** pour permettre l'utilisation d'adresses DIPP si nécessaire. Dans tous les cas, lorsque les sessions prennent fin, les adresses du pool deviennent disponibles et peuvent être affectées pour traduire les nouvelles connexions.

  La NAT d'adresses IP dynamiques permet une Réservation d'adresses NAT IP dynamiques.
- **Dynamic IP and Port (adresse IP et port dynamiques - DIPP)** : permet à plusieurs hôtes d'avoir leurs adresses IP source traduites en adresse IP identique avec différents numéros de ports. La traduction dynamique est effectuée vers l'adresse disponible suivante du pool d'adresses NAT, que vous configurez en tant que pool d'**adresses traduites**, qui peut être une adresse IP, une plage d'adresses, un sous-réseau ou une combinaison de ces éléments.

  En tant qu'alternative à l'adresse suivante du pool d'adresses NAT, DIPP vous permet d'indiquer l'adresse de l'**Interface (Interface)** elle-même. L'avantage d'indiquer l'interface dans la règle NAT est que cette dernière est automatiquement mise à jour pour utiliser toute adresse acquise par la suite par l'interface. DIPP est parfois connue sous le nom de NAT basée sur l'interface ou la Network Address Port Translation (traduction de port d'adresse réseau ; NAPT).

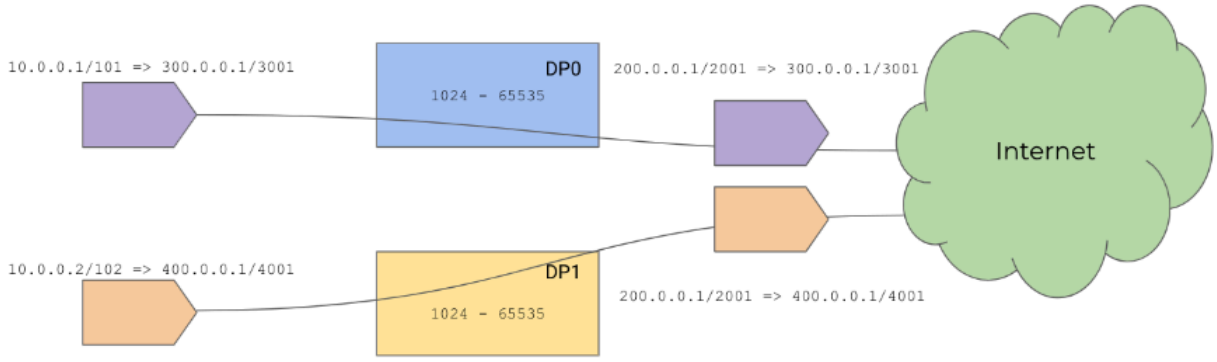
  DIPP dispose d'un taux de dépassement d'abonnement NAT, qui est le nombre de fois qu'une adresse IP traduite et une paire de ports identiques peuvent être utilisées simultanément. Pour

 ©2024 Palo Alto Networks, Inc.

plus d'informations, reportez-vous aux sections Dépassement d'abonnement NAT DIPP et Modification du taux de dépassement d'abonnement NAT DIPP.

> *(N'affecte que les pare-feux série PA-7000 qui n'utilisent pas les cartes de management de seconde génération PA-7050-SMC-B ou PA-7080-SMC-B) Quand vous utilisez un protocole de tunnel point-à-point (PPTP) avec du NAT DIPP, le pare-feu est limité à n'utiliser qu'une paire d'IP et de ports translatée pour une seule connexion; le pare-feu ne supporte pas le NAT DIPP La solution de contournement est de mettre à jour le pare-feu série 7000 avec une carte de seconde génération SMC-B.*

Lorsque vous configurez un DIPP standard (non persistant) sur un modèle de pare-feu multi-plans de données (DP), le taux de dépassement d'abonnement s'applique au pool local ; il n'est pas appliqué à tous les DP. Un port source d'un DP peut être réutilisé par un autre DP. La réutilisation des ports pour le DIPP standard est une bonne chose, car le trafic standard va vers différentes destinations. Dans ce graphique, la source des deux sessions est traduite en 200.0.0.1/2001 :



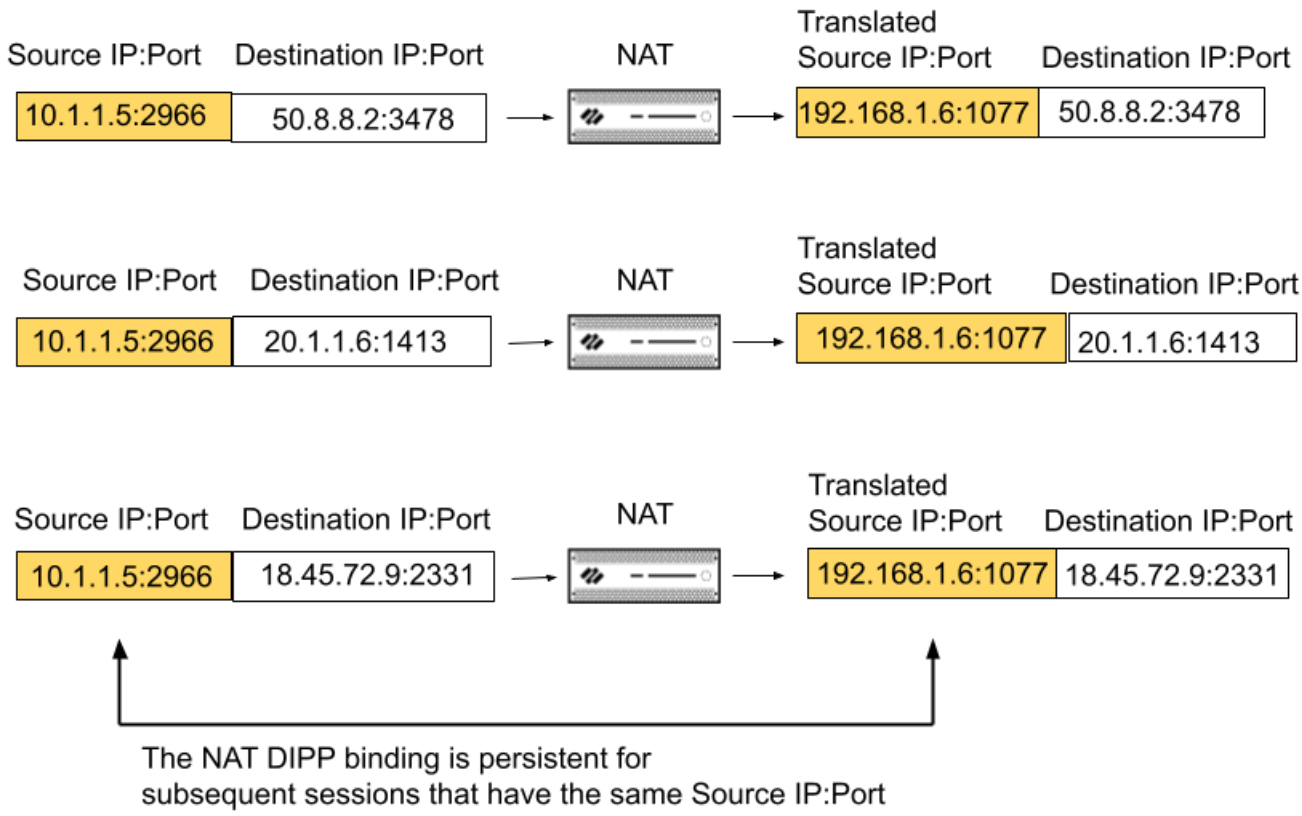
- (PAN-OS 11.1.0 et versions antérieures) **NAT persistant pour DIPP** (également appelé DIPP persistant ou NAT persistant) : disponible sur tous les pare-feu. La VoIP, la vidéo, la vidéoconférence basée sur le cloud, l'audioconférence et d'autres applications utilisent souvent DIPP et peuvent nécessiter le protocole STUN (Session Traversal Utilities for NAT). DIPP NAT utilise NAT symétrique, qui peut avoir des problèmes de compatibilité avec les applications qui utilisent STUN. Pour atténuer ces problèmes, persistent NAT for DIPP (NAT persistant pour DIPP) fournit une prise en charge supplémentaire pour la connectivité avec ces applications.

  Dans PAN-OS 11.1.0 et les versions antérieures, lorsque vous activez la NAT persistante pour DIPP, cela s'applique à toutes les règles NAT et NAT64 ; c'est un cadre global. Les journaux du plan de gestion ou du plan de données indiqueront `que la prise en charge NAT DIPP/STUN a été activée`.

  Lorsque NAT persistant pour DIPP est activé, la liaison d'une paire adresse IP/port source privée à une paire adresse IP/port source publique (traduite) spécifique persiste pour les

 ©2024 Palo Alto Networks, Inc.

sessions suivantes qui arrivent avec la même paire adresse IP source / port d'origine. L'exemple suivant montre trois sessions :



Dans cet exemple, l'adresse/port IP source d'origine 10.1.1.5:2966 est lié à l'adresse/port IP source traduit 192.168.1.6:1077 dans la session 1. Cette liaison est persistante dans les sessions 2 et 3, qui ont la même adresse IP/port source d'origine, mais des adresses de destination différentes. La persistance de la liaison se termine après la fin de toutes les sessions pour cette paire adresse IP source/port.

Dans la session 1 de l'exemple, le port de destination est 3478, le port STUN par défaut.

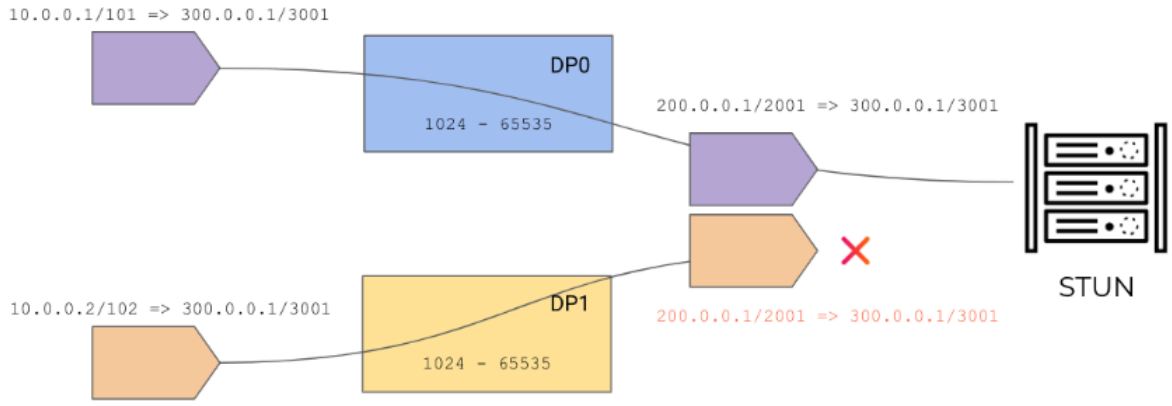
Le paramètre NAT persistant pour DIPP (activé ou désactivé) survit lors des redémarrages du pare-feu.

Avec les règles NAT DIPP standard, plusieurs paires de la même combinaison [adresse IP source/port] envoyant du trafic vers différentes destinations obtiendront des traductions différentes. Avec les règles DIPP persistantes, plusieurs paires de la même combinaison

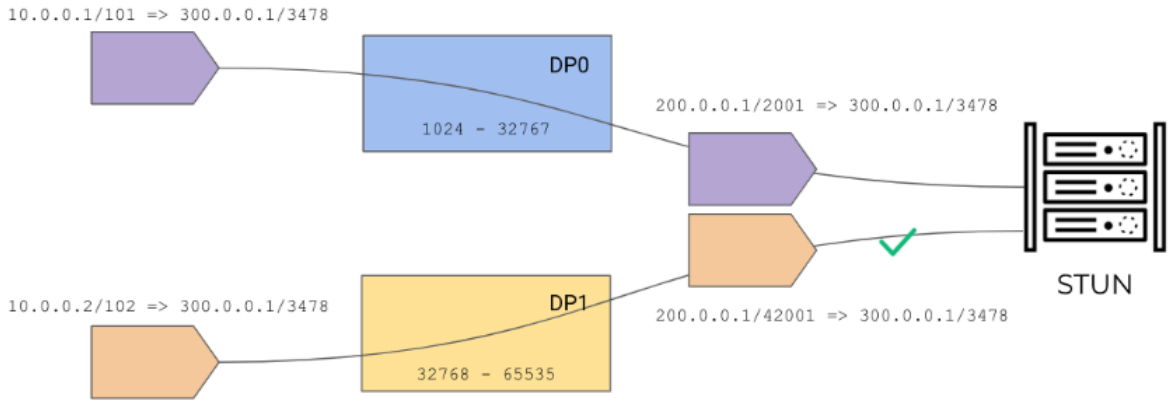
 ©2024 Palo Alto Networks, Inc.

[adresse IP source/port] envoyant du trafic vers différentes destinations obtiendront la même traduction, comme illustré dans les trois sessions ci-dessus.

La NAT persistante ne peut pas réutiliser les numéros de port entre les DP, car si plusieurs DP essayaient d'utiliser le même numéro de port, certaines sessions pourraient ne pas parvenir à atteindre STUN, comme indiqué ici :



La solution consiste à partitionner les ports sources entre les DP ; ainsi les numéros de port seront uniques et vous éviterez les sessions en double :



- (PAN-OS 11.1.1 et versions ultérieures) **DIPP persistant par stratégie** : à partir de PAN-OS 11.1.1 et versions ultérieures, vous configurez le DIPP persistant dans des règles de politique NAT individuelles plutôt que globalement. Lorsque vous utilisez NAT ou NAT64 pour des applications vidéo ou vocales derrière le pare-feu et que vous devez accéder à STUN, créez une règle de politique NAT à l'aide d'un type de traduction **Persistent Dynamic IP and Port (adresse IP et port dynamiques persistants)**.

  Le DIPP persistant par politique permet au DIPP standard (non persistant) et au DIPP persistant de coexister, car le DIPP persistant n'est pas global ; la granularité s'inscrit dans une règle de politique NAT. Lorsque le DIPP persistant est configuré globalement, seuls 64 512 ports sources sont disponibles dans l'ensemble du système, ce qui limite le nombre total de traductions, même pour le trafic DIPP standard. En permettant aux règles DIPP standard et DIPP persistantes de coexister dans le système, le DIPP standard n'a pas besoin de partager

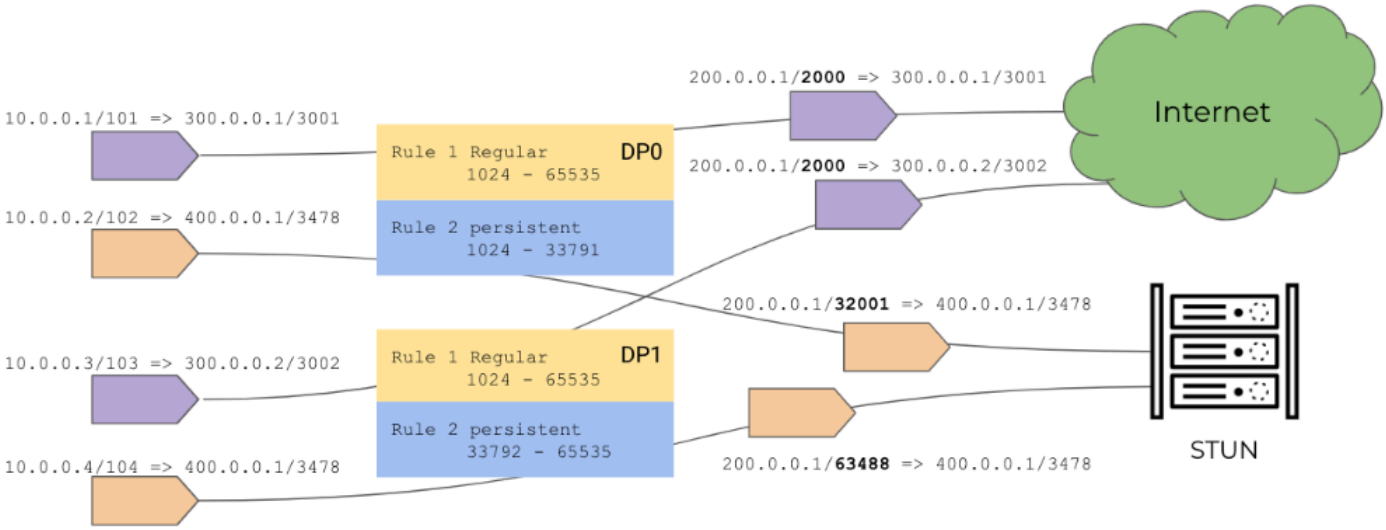
 ©2024 Palo Alto Networks, Inc.

des ports avec le DIPP persistant et peut avoir un taux de dépassement d'abonnement supérieur à 1, libérant ainsi le nombre total de traductions DIPP régulières.

Les règles DIPP persistantes et les règles DIPP standard peuvent être traduites dans les mêmes plages d'adresses IP. Pour obtenir les meilleures performances, configurez un DIPP persistant et un DIPP standard pour gérer des pools de ports sources distincts, car le trafic doit être dirigé vers des destinations différentes. Des pools de ports distincts peuvent avoir des plages de ports qui se chevauchent.

Pour les règles de DIPP persistants, le taux de dépassement d'abonnement est de 1 (pas de dépassement d'abonnement). Les règles de DIPP standard utilisent le taux de dépassement d'abonnement défini dans la configuration du système. Cette conception donne les meilleures performances lorsque le DIPP persistant est activé sur le pare-feu.

Comme le montre ce graphique, les sessions violettes de DP0 et DP1 utilisent une règle NAT standard et utilisent la même adresse IP/port source traduite (200.0.0.1/2000). Elles ont des adresses IP de destination différentes pour Internet. Les sessions orange de DP0 et DP1 sont destinées à un port STUN. Elles utilisent une règle NAT de DIPP persistant et utilisent la même adresse IP source traduite (200.0.0.1), mais des numéros de port différents (32001 et 63488).



En résumé, le DIPP persistant par politique permet à deux types de trafic de coexister sur un pare-feu (DIPP standard et DIPP persistant). Les règles de DIPP standard et les règles de DIPP persistants peuvent partager une seule adresse IP traduite (notez que les quatre sessions dans le graphique ont toutes une adresse source traduite de 200.0.0.1). Les règles de DIPP standard peuvent partager la même adresse IP et le même port source traduits (les sessions violettes), car elles ont des destinations différentes. Le type de règle de DIPP standard et le type de règle de DIPP persistant peuvent chacun contrôler son propre pool de ports source.

Le DIPP persistant ne prend pas en charge la permutation à chaud des cartes de ligne.

NAT de destination

La NAT de destination est effectuée sur les paquets entrants lorsque le pare-feu traduit une adresse de destination en une adresse de destination différente. Par exemple, elle traduit une

 ©2024 Palo Alto Networks, Inc.

adresse de destination publique en une adresse de destination privée. La NAT de destination permet également la traduction ou le réacheminement des ports.

La NAT de destination permet la traduction statique et dynamique :

- **IP statique** : vous pouvez configurer une traduction 1 à 1 statique en plusieurs formats. Vous pouvez préciser que le paquet d'origine possède une seule adresse IP de destination, une plage d'adresses IP ou un masque réseau IP, tant que le paquet traduit possède le même format et précise le même nombre d'adresses IP. Chaque fois, le pare-feu traduit de manière statique l'adresse de destination d'origine en la même adresse de destination traduite. C'est-à-dire que s'il existe plus d'une adresse de destination, le pare-feu traduit la première adresse de destination configurée pour le paquet d'origine en la première adresse de destination configurée pour le paquet traduit, puis traduit la deuxième adresse de destination configurée pour le paquet d'origine en la deuxième adresse de destination configurée pour le paquet traduit, ainsi de suite, en utilisant toujours la même traduction.

  Si vous utilisez la NAT de destination pour traduire une adresse IPv4 statique, vous pouvez également utiliser les services DNS sur un côté du pare-feu pour résoudre les FQDN d'un client qui se trouve de l'autre côté. Lorsque la réponse DNS qui contient l'adresse IPv4 traverse le pare-feu, le serveur DNS fournit une adresse IP interne à un périphérique externe, ou vice-versa. À compter de PAN-OS 9.0.2 et dans les versions 9.0 ultérieures, vous pouvez configurer le pare-feu pour qu'il réécrive l'adresse IP dans la réponse DNS (qui correspond à la règle) pour que le client reçoive l'adresse appropriée afin d'atteindre le service de destination. Le cas d'utilisation de la réécriture DNS détermine la manière dont vous configurez une telle réécriture.
- **Dynamic IP (with session distribution) (IP dynamique (avec distribution de session))** : La NAT de destination vous permet de traduire l'adresse de destination d'origine en un hôte ou serveur de destination qui comporte une dynamic IP address (adresse IP dynamique), comme un groupes d'adresses ou un objet d'adresse qui utilise un masque réseau IP, une plage d'adresses IP ou un FQDN, qui peuvent tous renvoyer plusieurs adresses depuis DNS. L'adresse IP dynamique (avec distribution de session) prend en charge les adresses IPv4 uniquement. Une NAT de destination qui utilise une adresse IP dynamique s'avère particulièrement utile dans des déploiements de cloud, qui se servent d'adresses IP dynamiques.

  Si l'adresse de destination translatée se résout en plus d'une adresse, le pare-feu distribue les sessions NAT entrante parmi les adresses multiples pour améliorer la distribution des sessions. La distribution se fonde sur l'une de plusieurs méthodes : permutation circulaire (la méthode par défaut), hachage IP source, modulo IP, hachage IP ou moins de sessions. Si un serveur DNS renvoie plus de 32 adresses IPv4 pour un FQDN, le pare-feu utilise les 32 premières adresses du paquet.

  > *Si l'adresse traduite est un objet d'adresse de type FQDN qui se résout uniquement en adresses IPv6, la règles de politique NAT de destination considère que le FQDN n'a pas été résolu.*

  L'utilisation de **Dynamic IP (with session distribution) (IP dynamique (avec distribution de sessions)** vous permet de traduire plusieurs adresses IP de destination pré-NAT *M* en plusieurs adresses IP de destination post-NAT *N*. Dans une traduction plusieurs à plusieurs, il existe *M* x *N* traductions de NAT de destination à partir d'une seule règle NAT.

  Vous devez sélectionner le **Translation Type (Type de traduction)** de l'adresse de destination (**Policy (Politique)** > **NAT** > **Translated Packet (Paquet traduit)**) comme **Dynamic IP (IP**

 ©2024 Palo Alto Networks, Inc.

dynamique (avec distribution de session)) lorsque vous configurez l'adresse pré-NAT en tant qu'objet FQDN dans **Policy (Politique)** > **NAT** > **Original Packet (Paquet d'origine)**.

Pour la NAT de destination, il est recommandé de :

- *Utilisez la traduction d'adresses **Static IP (IP statiques)** pour les adresses IP statiques, ce qui permet au pare-feu de vérifier et de s'assurer que le nombre d'adresses IP des destination originales équivaut au nombre d'adresses IP de destination traduites.*
- *Utilisez la traduction de **Dynamic IP (with session distribution) (Adresse IP dynamique [avec distribution de session]** uniquement pour les adresses dynamiques basées sur le FQDN (le pare-feu ne vérifie pas le nombre d'adresses IP).*

Vous trouverez ci-dessous des exemples courants des traductions de NAT de destination que le pare-feu autorise :

Type de traduction	L'adresse de destination du paquet d'origine	correspond à l'adresse de destination du paquet traduit	Remarques
IP statique	192.168.1.1	2.2.2.2	Le paquet d'origine et le paquet traduit possèdent tous deux une adresse de destination possible.
	192.168.1.1-192.168.1.4	2.2.2.1-2.2.2.4	Le paquet d'origine et le paquet traduit possèdent tous deux quatre adresses de destination possibles : 192.168.1.1 correspond toujours à 2.2.2.1 192.168.1.2 correspond toujours à 2.2.2.2 192.168.1.3 correspond toujours à 2.2.2.3 192.168.1.4 correspond toujours à 2.2.2.4
	192.168.1.1/30	2.2.2.1/30	Le paquet d'origine et le paquet traduit possèdent tous deux quatre adresses de destination possibles : 192.168.1.1 correspond toujours à 2.2.2.1 192.168.1.2 correspond toujours à 2.2.2.2

 ©2024 Palo Alto Networks, Inc.

Type de traduction	L'adresse de destination du paquet d'origine	correspond à l'adresse de destination du paquet traduit	Remarques
			192.168.1.3 correspond toujours à 2.2.2.3 192.168.1.4 correspond toujours à 2.2.2.4
Adresse IP dynamique (avec distribution de session)	192.168.1.1/30	domainname.com	Le paquet original contient quatre adresses de destination et si, par exemple, le FQDN de l'adresse de destination traduite forme cinq adresses IP, c'est qu'il y a 20 traductions de NAT de destination possibles dans une seule règle NAT.

Un usage courant de la NAT de destination est de configurer plusieurs règles NAT qui mappent une adresse de destination publique à plusieurs adresses hôtes de destination privées affectées à des serveurs ou services. Dans ce cas, les numéros de ports de destination permettent d'identifier les hôtes de destination. Par exemple :

- **Réacheminement des ports** : traduction d'une adresse de destination publique et d'un numéro de port en adresse de destination privée, mais en gardant le même numéro de port.
- **Traduction des ports** : traduction d'une adresse de destination publique et d'un numéro de port en adresse de destination privée et numéro de port différent, permettant ainsi de garder privé le numéro de port réel. La traduction du port est configurée en saisissant le **Translated Port (Port traduit)** dans l'onglet **Translated Packet (Paquet traduit)** de la règle de politique NAT. Reportez-vous à la section Exemple de NAT de destination avec traduction de port.

NAT de destination avec cas d'utilisation de la réécriture DNS

Lorsque vous utilisez la NAT de destination pour effectuer la traduction statique d'une adresse IPv4 vers une autre adresse IPv4, vous pouvez également utiliser les services DNS sur un côté du pare-feu pour résoudre les FQDN d'un client. Lorsque la réponse DNS contenant l'adresse IP traverse le pare-feu pour se rendre au client, le pare-feu n'effectue pas la NAT sur cette adresse IP. Le serveur DNS fournit donc une adresse IP interne à un périphérique externe, ou vice-versa, ce qui empêche le client DNS d'arriver à se connecter au service de destination.

Pour éviter ce problème, vous pouvez configurer le pare-feu de manière à réécrire l'adresse IP dans la réponse DNS (à partir de l'enregistrement A) en fonction de l'adresse IP traduite configurée pour la règle de politique NAT. Le pare-feu effectue la NAT sur l'adresse IPv4 (résolution du FQDN) dans la réponse DNS avant de transférer la réponse au client. Par conséquent, le client reçoit l'adresse appropriée pour atteindre le service de destination. Une seule règle de politique NAT pousse le pare-feu à effectuer la NAT sur les paquets qui

 ©2024 Palo Alto Networks, Inc.

correspondent à la règle et pousse également le pare-feu à effectuer la NAT sur les adresses IP dans les réponses DNS qui correspondent à l'adresse de destination. d'origine ou à l'adresse de destination traduite dans la règle.

La réécriture du DNS se fait au niveau global ; le pare-feu fait correspondre l'adresse de destination de l'onglet Original Packet (Paquet d'origine) à l'adresse de destination de l'onglet Translated Packet (Paquet traduit). Tous les autres champs de l'onglet Original Packet (Paquet d'origine) sont ignorés. Lorsqu'un paquet de réponse DNS arrive, le pare-feu vérifie si la réponse contient un enregistrement A qui correspond à l'une des adresses de destination mappées, en fonction de la direction, comme suit.

Vous devez spécifier la manière dont le pare-feu effectue la NAT sur l'adresse IP dans la réponse DNS relative à la règle NAT :**reverse (inverser)** ou **forward (transférer)**.

- **reverse (inverse)** : si la réponse DNS correspond à l'adresse de destination **Translated (Traduite)** dans la règle, traduisez la réponse DNS en utilisant la translation inverse que la règle utilise. Par exemple, si la règle traduit l'adresse IP **1.1.1.10 en 192.168.1.10**, le pare-feu réécrit une réponse DNS **192.168.1.10 en 1.1.1.10**.
- **forward (directe)** : si la réponse DNS correspond à l'adresse de destination **Original (Originale)** dans la règle, traduisez la réponse DNS en utilisant la même traduction que la règle utilise. Par exemple, si la règle traduit l'adresse IP **1.1.1.10 en 192.168.1.10**, le pare-feu réécrit une réponse DNS **1.1.1.10 en 192.168.1.10**.

*Si vous avez une règle NAT en chevauchant d'autres pour laquelle la réécriture DNS est désactivée et une règle NAT en dessous pour laquelle la réécriture DNS est activée et que cette dernière est incluse dans le chevauchement, le pare-feu réécrit la réponse DNS en fonction de la règle NAT chevauchée (selon le paramètre **reverse [inverse]** ou **forward [direct]**). La réécriture a priorité et l'ordre des règles NAT est ignoré.*

Tenez compte des cas d'utilisation pour la configuration de la réécriture DNS :

- NAT de destination avec cas d'utilisation de la réécriture DNS dans le sens inverse
- NAT de destination avec cas d'utilisation de la réécriture DNS dans le sens direct

NAT de destination avec cas d'utilisation de la réécriture DNS dans le sens inverse

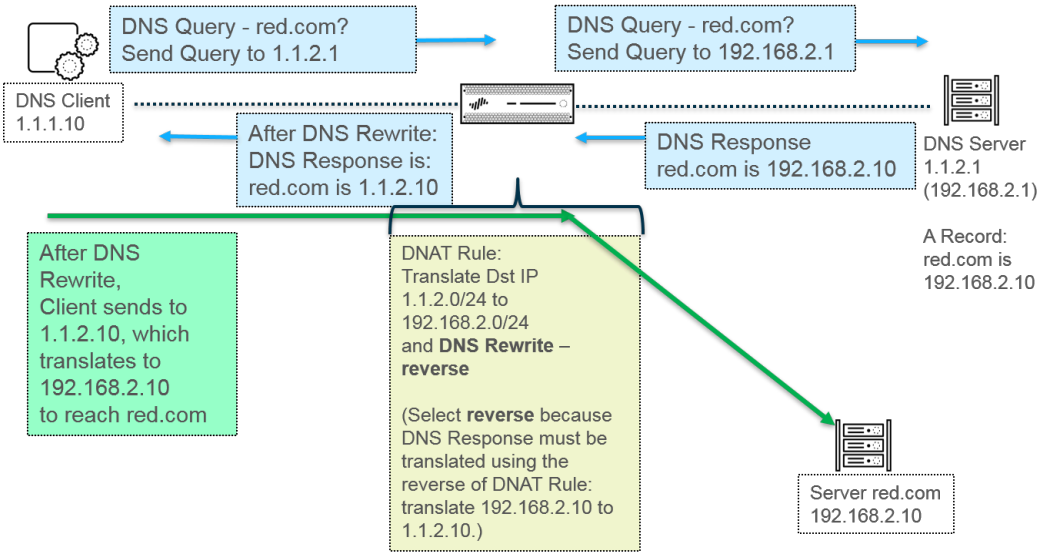
Les cas d'utilisation suivants illustrent la NAT de destination avec réécriture DNS dans le sens du **reverse (inverse)**. La différence entre ces deux cas d'utilisation repose tout simplement sur l'emplacement du client DNS, du serveur DNS et du serveur de destination, soit du côté public ou du côté interne du pare-feu. Dans les deux cas, le client DNS se situe du côté opposé du pare-feu par rapport à son serveur de destination final. (Si votre client DNS et son serveur de destination final se situent sur le même côté du pare-feu, considérez les NAT de destination avec cas d'utilisation de la réécriture DNS dans le sens direct 3 et 4.)

Le cas d'utilisation 1 illustre le client DNS sur le côté public du pare-feu, tandis que le serveur DNS et le serveur de destination final se trouvent tous deux du côté interne. Ce cas exige la réécriture DNS dans le sens inverse. Le client DNS demande l'adresse IP de red.com. Selon la règle NAT, le pare-feu traduit la demande (initialement dirigée à l'adresse publique 1.1.2.1) en adresse interne 192.168.2.1. Le serveur DNS répond que l'adresse IP du site red.est 192.168.2.10. La règle inclut **Enable DNS Rewrite - forward (Activer la réécriture DNS - direct)** et la réponse DNS (192.168.2.10) correspond à l'adresse de destination traduite, soit 192.168.2.0/24 dans la règle. Le pare-feu traduit donc la réponse DNS en utilisant la traduction

 ©2024 Palo Alto Networks, Inc.

reverse (inverse) par rapport à celle qu'utilise la règle. La règle indique de traduire 1.1.2.0/24 en 192.168.2.0/24 ; le pare-feu réécrit donc la réponse DNS 192.168.2.10 en 1.1.2.10. Le client DNS reçoit la réponse et l'envoie à 1.1.2.10, que la règle traduit en 192.168.2.10 pour joindre le serveur red.com.

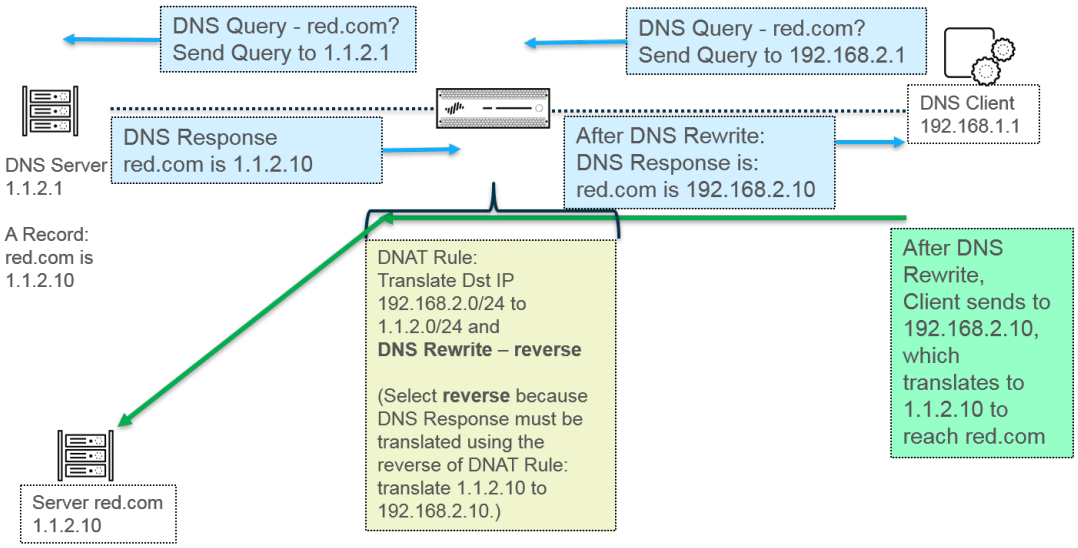
Récapitulatif du cas d'utilisation 1 : Le client DNS et le serveur de destination se situent sur les côtés opposés du pare-feu. Le serveur DNS fournit une adresse qui correspond à l'adresse de destination traduite dans la règle NAT ; il traduit donc la réponse DNS à l'aide de la traduction contraire (**reverse [inverse]**) à la règle NAT.



Le cas d'utilisation 2 illustre le client DNS sur le côté interne du pare-feu, tandis que le serveur DNS et le serveur de destination final se trouvent tous deux du côté public. Ce cas exige la réécriture DNS dans le sens inverse. Le client DNS demande l'adresse IP de red.com. Selon la règle NAT, le pare-feu traduit la demande (initialement dirigée à l'adresse interne 192.168.2.1) en adresse publique 1.1.2.1. Le serveur DNS répond que l'adresse IP du site red.est 1.1.2.10. La règle inclut **Enable DNS Rewrite - forward (Activer la réécriture DNS - direct)** et la réponse DNS (1.1.2.10) correspond à l'adresse de destination traduite, soit 1.1.2.0/24 dans la règle. Le pare-feu traduit donc la réponse DNS en utilisant la traduction **reverse (inverse)** par rapport à celle qu'utilise la règle. La règle indique de traduire 192.168.2.0/24 en 1.1.2.0/24 ; le pare-feu réécrit donc la réponse DNS 1.1.2.10 en 192.168.2.10. Le client DNS reçoit la réponse et l'envoie à 192.168.2.10, que la règle traduit en 1.1.2.10 pour joindre le serveur red.com.

Le récapitulatif du cas d'utilisation 2 est le même que le récapitulatif du cas d'utilisation 1 : Le client DNS et le serveur de destination se situent sur les côtés opposés du pare-feu. Le serveur DNS fournit une adresse qui correspond à l'adresse de destination traduite dans la règle NAT ; il traduit donc la réponse DNS à l'aide de la traduction contraire (**reverse [inverse]**) à la règle NAT.

 ©2024 Palo Alto Networks, Inc.



Pour applique la réécriture DNS, Configuration de la NAT de destination avec réécriture DNS.

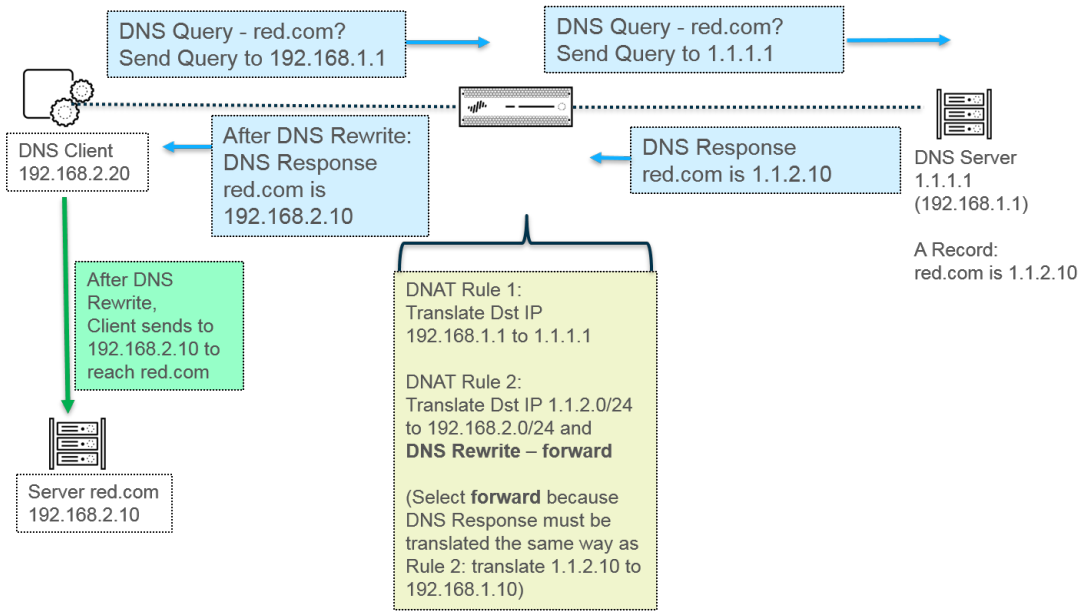
NAT de destination avec cas d'utilisation de la réécriture DNS dans le sens direct

Les cas d'utilisation suivants illustrent la NAT de destination avec réécriture DNS dans le sens **forward (direct)**. La différence entre ces deux cas d'utilisation repose tout simplement sur l'emplacement du client DNS, du serveur DNS et du serveur de destination, soit du côté public ou du côté interne du pare-feu. Dans les deux cas, le client DNS se situe du même côté du pare-feu que son serveur de destination final. (Si votre client DNS et son serveur de destination final se situent sur des côtés opposés du pare-feu, considérez les NAT de destination avec cas d'utilisation de la réécriture DNS dans le sens inverse 1 et 2.)

Le cas d'utilisation 3 illustre le client DNS et le serveur de destination final se trouvant tous deux sur le côté interne du pare-feu, tandis que le serveur DNS se situe du côté public. Ce cas exige la réécriture DNS dans le sens direct. Le client DNS demande l'adresse IP de red.com. Selon la règle 1, le pare-feu traduit la demande (initialement dirigée à l'adresse interne 192.168.1.1) en 1.1.1.1. Le serveur DNS répond que l'adresse IP du site red.est 1.1.2.10. La règle 2 inclut **Enable DNS Rewrite - forward (Activer la réécriture DNS - direct)** et la réponse DNS (1.1.2.10) correspond à l'adresse de destination d'origine, soit 1.1.2.0/24, dans la règle 2. Le pare-feu traduit donc la réponse DNS en utilisant la **même** traduction que la règle utilise. La règle 2 indique de traduire 1.1.2.0/24 en 192.168.2.0/24 ; le pare-feu réécrit la réponse DNS 1.1.2.10 en 192.168.2.10. Le client DNS reçoit la réponse et l'envoie à 192.168.2.10 pour joindre le serveur red.com.

Récapitulatif du cas d'utilisation 3 : Le client DNS et le serveur de destination se situent sur le même côté du pare-feu. Le serveur DNS fournit une adresse qui correspond à l'adresse de destination d'origine dans la règle NAT ; il traduit donc la réponse DNS à l'aide de la même traduction (**forward [direct]**) que la règle NAT.

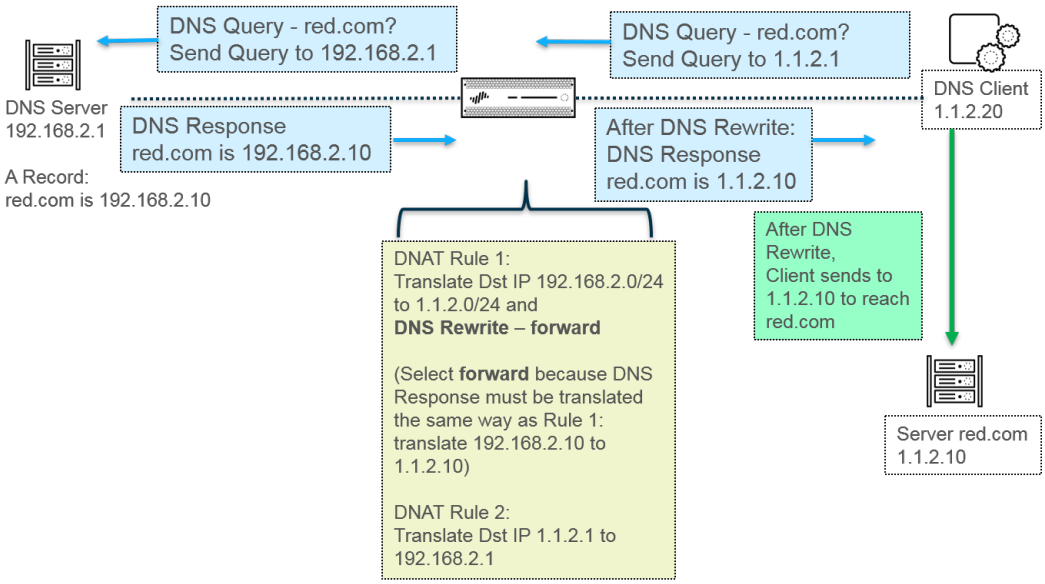
 ©2024 Palo Alto Networks, Inc.



Le cas d'utilisation 4 illustre le client DNS et le serveur de destination final se trouvant tous deux sur le côté public du pare-feu, tandis que le serveur DNS se situe du côté interne. Ce cas exige la réécriture DNS dans le sens direct. Le client DNS demande l'adresse IP de red.com. Selon la règle 2, le pare-feu traduit la demande (initialement dirigée à la destination publique 1.1.2.1) en 192.168.2.1. Le serveur DNS répond que l'adresse IP du site red.est 192.168.2.10. La règle 1 inclut **Enable DNS Rewrite - forward (Activer la réécriture DNS - direct)** et la réponse DNS (192.168.2.10) correspond à l'adresse de destination d'origine, soit 192.168.2.0/24, dans la règle 1. Le pare-feu traduit donc la réponse DNS en utilisant la **même** traduction que la règle utilise. La règle 1 indique de traduire 192.168.2.0/24 en 1.1.2.0/24 ; le pare-feu réécrit la réponse DNS 192.168.2.10 en 1.1.2.10. Le client DNS reçoit la réponse et l'envoie à 1.1.2.10 pour joindre le serveur red.com.

Le récapitulatif du cas d'utilisation 4 est le même que le récapitulatif du cas d'utilisation 3 : Le client DNS et le serveur de destination se situent sur le même côté du pare-feu. Le serveur DNS fournit une adresse qui correspond à l'adresse de destination d'origine dans la règle NAT ; il traduit donc la réponse DNS à l'aide de la même traduction (**forward [direct]**) que la règle NAT.

 ©2024 Palo Alto Networks, Inc.



Pour applique la réécriture DNS, Configuration de la NAT de destination avec réécriture DNS.

 ©2024 Palo Alto Networks, Inc.

Nombre de règles NAT

Le nombre de règles NAT autorisées est défini en fonction du modèle de pare-feu. Les limites de chaque règle sont définies pour la NAT DIPP, d'adresses IP statiques et d'adresses IP dynamiques. Le nombre de règles utilisées pour ces types NAT ne peut pas dépasser le nombre maximum de règles NAT. Pour DIPP, la limite de la règle est définie en fonction du paramètre de dépassement d'abonnement (8, 4, 2 ou 1) du pare-feu et de la supposition d'une adresse IP traduite par règle. Pour voir les limites d'adresse IP traduite et de règle NAT propres à chaque modèle, utilisez l'outil Comparer les pare-feu.

Tenez compte des points suivants lors de l'utilisation de règles NAT :

- Si vous venez à manquer de ressources de pool, vous ne pouvez pas créer d'autres règles NAT, même si le nombre maximum de règles du modèle n'a pas été atteint.
- Si vous consolidez les règles NAT, la journalisation et la génération de rapports sont également consolidées. Les statistiques sont fournies pour la règle et non pour l'ensemble des adresses dans la règle. Si vous avez besoin d'une journalisation et d'une génération de rapports granulaires, ne combinez pas les règles.

 ©2024 Palo Alto Networks, Inc.

Dépassement d'abonnement NAT DIPP

La NAT Dynamic IP and Port (adresse IP et port dynamiques - DIPP) vous permet d'utiliser chaque adresse IP traduite et paire de ports plusieurs fois (8, 4 ou 2 fois) dans des sessions simultanées. La capacité de réutilisation d'une adresse IP et d'un port (appelée dépassement d'abonnement) offre une certaine évolutivité aux clients qui ne disposent pas suffisamment d'adresses IP publiques. Le modèle est défini en fonction de la supposition que les hôtes se connectent à différentes destinations ; par conséquent, les sessions peuvent être identifiées de manière unique et les collisions sont peu probables. Le taux de dépassement d'abonnement multiplie en fait la taille d'origine du pool d'adresses/de ports par 8, 4 ou 2. Par exemple, la limite par défaut de 64 000 sessions simultanées autorisées, multipliée par un taux de dépassement d'abonnement de 8, équivaut à 512 000 sessions simultanées autorisées.

Le taux de dépassement d'abonnement autorisé est défini en fonction du modèle. Ce taux est global ; il s'applique au pare-feu. Le taux de dépassement d'abonnement est défini par défaut et consomme de la mémoire, même si vous disposez suffisamment d'adresses IP publiques disponibles pour rendre le dépassement d'abonnement inutile. Vous pouvez réduire le taux par défaut et définir un paramètre inférieur ou même de 1 (aucun dépassement d'abonnement). La configuration d'un taux de dépassement d'abonnement réduit entraîne la diminution du nombre de traductions de périphérique source possibles, mais augmente le nombre de règles NAT DIPP et d'adresses IP dynamiques. Pour modifier le taux par défaut, reportez-vous à la section Modification du taux de dépassement d'abonnement NAT DIPP.

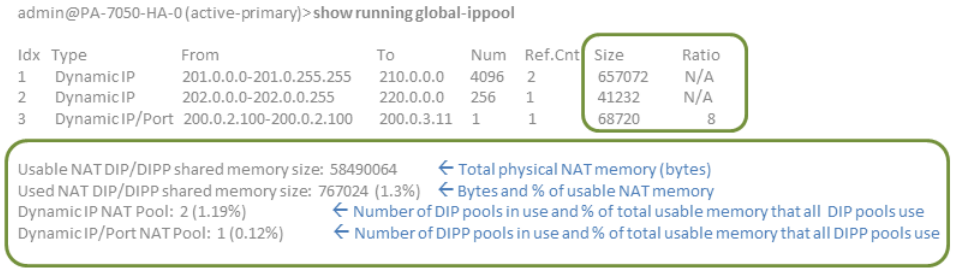
Si vous sélectionnez **Platform Default (Valeur par défaut de la plate-forme)**, votre configuration explicite du taux de dépassement d'abonnement est désactivée et le taux de dépassement d'abonnement du pool DIPP par défaut NAT du modèle s'applique, comme indiqué dans l'Outil de sélection du produit. Le paramètre **Platform Default (Valeur par défaut de la plate-forme)** permet la mise à niveau vers une version logicielle ultérieure ou antérieure.

Le pare-feu prend en charge 256 adresses IP traduites maximum par règle NAT, et chaque modèle prend en charge un nombre maximum d'adresses IP traduites (pour toutes les règles NAT combinées). Si le dépassement d'abonnement entraîne le dépassement du nombre maximum d'adresses traduites par règle (256), le pare-feu réduit automatiquement le taux de dépassement d'abonnement de manière à ce que la validation puisse être effectuée. Toutefois, si vos règles NAT entraînent des traductions qui dépassent le nombre maximum d'adresses traduites du modèle, la validation échouera.

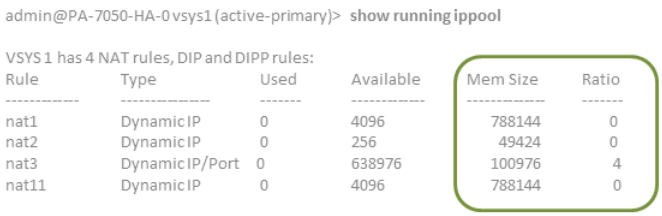
 ©2024 Palo Alto Networks, Inc.

Statistiques de la mémoire NAT du plan de données

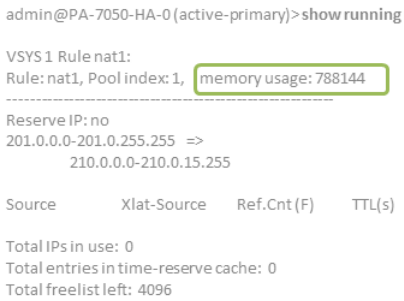
La commande **`show running global-ippool`** permet d'afficher les statistiques relatives à la consommation de mémoire NAT d'un pool. La colonne Taille affiche le nombre d'octets de mémoire que le pool de ressources utilise. La colonne Taux affiche le taux de dépassement d'abonnement (pour les pools DIPP uniquement). Les lignes de statistiques de la mémoire et du pool sont expliquées dans l'exemple de résultat suivant :



Pour les statistiques du pool d'un système virtuel, la commande **`show running ippool`** affiche des colonnes indiquant la taille de la mémoire utilisée par règle NAT et le taux de dépassement d'abonnement utilisé (pour les règles DIPP). Vous trouverez ci-dessous un exemple de résultat de cette commande.



Un champ du résultat de la commande **`show running nat-rule-ippool rule`** indique la mémoire (en octets) utilisée par règle NAT. Vous trouverez ci-dessous un exemple de résultat de cette commande (avec l'utilisation de la mémoire pour la règle entourée).



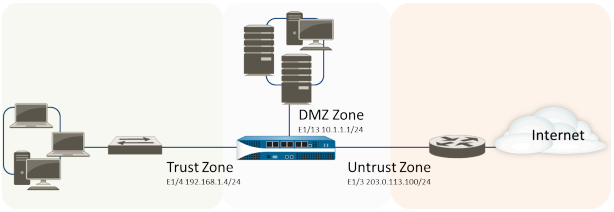
 ©2024 Palo Alto Networks, Inc.

Configuration de NAT

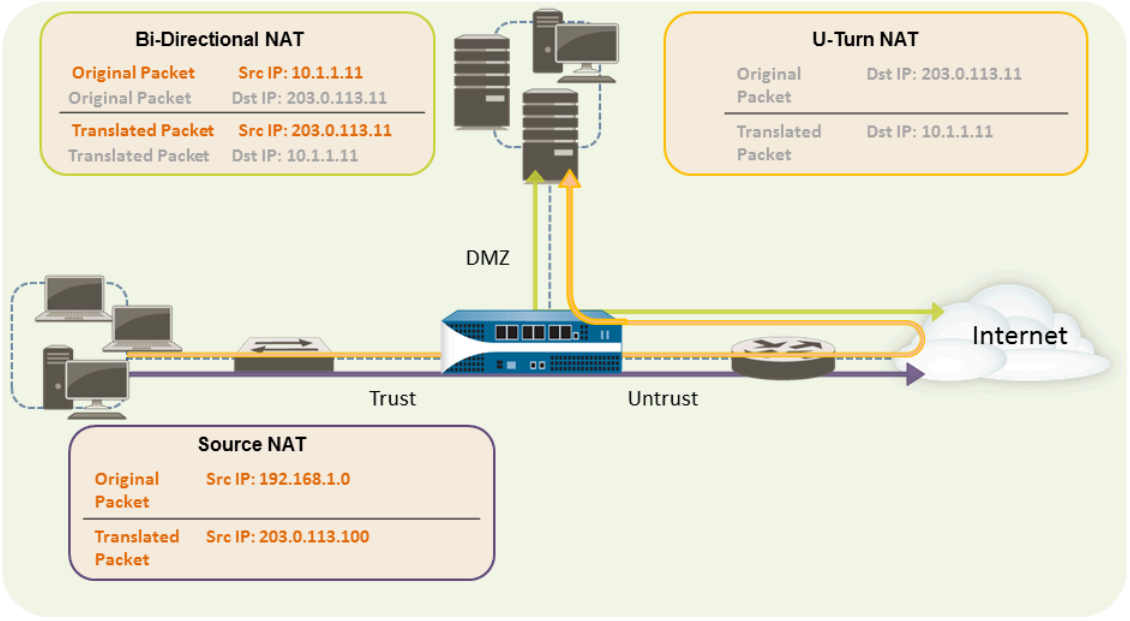
Procédez comme suit pour configurer divers aspects de NAT. Outre les exemples ci-dessous, vous trouverez d'autres exemples dans la section Exemples de configuration NAT.

- Traduction d'adresses IP clients internes en votre adresse IP publique (NAT DIPP source)
- Créer une règle source NAT avec DIPP persistant
- Autorisation d'accès des clients sur le réseau interne à vos serveurs publics (NAT U-Turn de destination)
- Activation de la traduction bidirectionnelle d'adresses pour vos serveurs orientés public (NAT source statique)
- Configuration de la NAT de destination avec réécriture DNS
- Configuration de la NAT de destination à l'aide des adresses IP dynamiques
- Modification du taux de dépassement d'abonnement NAT DIPP
- Réservation d'adresses NAT IP dynamiques
- Désactivation de la NAT pour un hôte ou une interface spécifique

Les trois premiers exemples NAT de cette section reposent sur la topologie suivante :



Selon cette topologie, il y a trois politiques NAT que nous devons créer, comme suit :



- Pour permettre aux clients du réseau interne d'accéder aux ressources disponibles sur Internet, les adresses internes 192.168.1.0 devront être traduites en adresses pouvant être acheminées

 ©2024 Palo Alto Networks, Inc.

en public. Dans ce cas, nous allons configurer la NAT source (la flèche et le boîtier violets ci-dessus) en utilisant l'adresse de l'interface de sortie, 203.0.113.100, en tant qu'adresse source pour tous les paquets quittant le pare-feu de la zone interne. Pour connaître les instructions, reportez-vous à la section Traduction d'adresses IP clients internes en votre adresse IP publique (NAT DIPP source).

- Pour permettre aux clients du réseau interne d'accéder au serveur Web public dans la zone DMZ, nous devons configurer une règle NAT qui redirige un paquet du réseau externe, dans lequel la recherche de la table de routage d'origine va déterminer son itinéraire en fonction de l'adresse de destination 203.0.113.11 affichée dans le paquet, vers l'adresse actuelle 10.1.1.11 du serveur Web sur le réseau DMZ. Pour ce faire, vous devez créer une règle NAT de la zone approuvée (où se trouve l'adresse source dans le paquet) vers la zone non approuvée (où se trouve l'adresse de destination d'origine) pour traduire l'adresse de destination en adresse dans la zone DMZ. Ce type de NAT de destination porte le nom de *NAT U-Turn* (la flèche et le boîtier jaunes ci-dessus). Pour obtenir les instructions, reportez-vous à la section Autorisation d'accès des clients sur le réseau interne à vos serveurs publics (NAT U-Turn de destination).
- Pour que le serveur Web, qui dispose d'une adresse IP privée sur le réseau DMZ et d'une adresse orientée public permettant l'accès aux utilisateurs externes, puisse envoyer et recevoir des demandes, le pare-feu doit traduire les paquets entrants de l'adresse IP publique en adresse IP privée et les paquets sortants de l'adresse IP privée en adresse IP publique. Pour ce faire, sur le pare-feu, utilisez une politique NAT source statique, bidirectionnelle et unique (la flèche et le boîtier verts ci-dessus). Reportez-vous à la section Activation de la traduction bidirectionnelle d'adresses pour vos serveurs orientés public (NAT source statique).

Traduction d'adresses IP clients internes en votre adresse IP publique (NAT DIPP source)

Lorsqu'un client de votre réseau interne envoie une demande, l'adresse source du paquet contient l'adresse IP du client de votre réseau interne. Si vous utilisez des plages d'adresses IP privées en interne, les paquets du client ne pourront pas être acheminés vers Internet, à moins de traduire l'adresse IP source des paquets sortant du réseau en une adresse pouvant être acheminée en public.

Pour ce faire, sur le pare-feu, configurez une politique NAT source qui traduit l'adresse source (et éventuellement le port) en une adresse publique. Une autre solution consiste à traduire l'adresse source de l'ensemble des paquets dans l'interface de sortie de votre pare-feu, comme indiqué dans la procédure suivante.

Cette tâche couvre le DIPP standard et inclut également l'étape d'activation du NAT persistant pour DIPP dans PAN-OS 11.1.0 et les versions antérieures. Pour activer le NAT persistant pour DIPP dans PAN-OS 11.1.1 et les versions ultérieures, Créer une règle source NAT avec DIPP persistant.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Créez un objet adresse pour l'adresse IP externe que vous souhaitez utiliser.

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)** et **Add (Ajoutez)** un **Name (Nom)** et éventuellement une **Description (Description)** pour l'objet.
2. Sélectionnez **IP Netmask (Masque de réseau IP)** sous **Type**, puis saisissez l'adresse IP de l'interface externe sur le pare-feu, 203.0.113.100 dans cet exemple.
3. Cliquez sur **OK**.



Bien que vous ne soyez pas obligé d'utiliser des objets adresse dans vos politiques, cette pratique est recommandée car elle simplifie l'administration en vous permettant d'effectuer des mises à jour dans un emplacement, au lieu d'avoir à mettre à jour toutes les politiques dans lesquelles l'adresse est référencée.

STEP 2 | Créez une politique NAT.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)**, puis cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, donnez un **Name (nom)** descriptif à la politique.
3. (Facultatif) Saisissez une étiquette, qui est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques.
4. Pour **NAT Type (Type de NAT)**, sélectionnez **ipv4** (paramètre par défaut).
5. Dans l'onglet **Original Packet (Paquet d'origine**, sélectionnez la zone que vous avez créée pour votre réseau interne dans la section **Source Zone (Zone source)** (cliquez sur **Add (Ajouter)**, puis sélectionnez la zone) et la zone que vous avez créée pour le réseau externe dans la liste **Destination Zone (Zone de destination)**.
6. Dans l'onglet **Translated Packet (Paquet traduit)**, sélectionnez **Dynamic IP And Port (Adresse IP et port dynamiques)** dans la liste **Translation Type (Type de traduction)** de la section Traduction de l'adresse source affichée à l'écran.
7. Pour **Address Type (Type d'adresse)**, deux choix s'offrent à vous. Vous pouvez sélectionner **Translated Address (Adresse traduite)**, puis cliquer sur **Add (Ajouter)**. Sélectionnez l'objet adresse que vous venez de créer.

   Un **Address Type (Type d'adresse)** alternatif est **Interface Address (Adresse de l'interface)**, auquel cas l'adresse traduite sera l'adresse IP de l'interface. Pour ce choix, sélectionnez une **Interface (Interface)** et éventuellement une **IP Address (Adresse IP)** si l'interface dispose de plusieurs adresses IP.
8. Cliquez sur **OK**.

STEP 3 | Validez vos modifications.

Cliquez sur **Commit (Valider)**.

STEP 4 | (PAN-OS 11.1.0 et versions antérieures) Activez le NAT persistant pour DIPP. (Ignorez cette étape pour le DIPP standard.)

1. Accédez à la CLI.
2. **>set system setting persistent-dipp enable yes**
3. **>request restart system**
4. Si vous avez configuré la haute disponibilité, répétez cette étape sur l'autre homologue HA.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | ((optional (Facultatif)) Vérifiez la traduction.

1. Utilisez la commande **`show session all`** pour afficher la table de sessions, où vous pouvez vérifier l'adresse IP source et le port, ainsi que l'adresse IP et le port traduits correspondants.
2. Utilisez la commande *show session id <id_number>* pour afficher plus d'informations sur une session.
3. Si vous avez configuré la NAT d'adresses IP dynamiques, utilisez la commande **`show counter global filter aspect session severity drop | match nat`** pour voir si des sessions ont échoué en raison de l'allocation d'adresses NAT IP. Si toutes les adresses du pool NAT d'adresses IP dynamiques sont affectées lorsqu'une nouvelle connexion est censée être traduite, le paquet est abandonné.

Créer une règle source NAT avec DIPP persistant

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (Strata Cloud Manager) : renseignez-vous auprès de votre représentant de compte d'assistance pour activer cette fonctionnalité. • NGFW (géré par PAN-OS ou Panorama)	☐ AIOps pour NGFW Premium est requis pour gérer les NGFW avec Strata Cloud Manager

À partir de PAN-OS 11.1.1 et des versions ultérieures, vous configurez le DIPP persistant dans une règle de politique NAT individuelle. Lorsque vous utilisez NAT pour des applications vidéo ou vocales derrière le pare-feu et que vous devez accéder à STUN, créez votre règle de politique à l'aide d'un type de traduction d'adresse IP et de port dynamiques persistants.

- PAN-OS
- Strata Cloud Manager

PAN-OS

Pour PAN-OS, suivez cette procédure pour créer une règle NAT source avec DIPP persistant.

STEP 1 | Créez un objet adresse pour l'adresse IP externe que vous souhaitez utiliser.

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)** et **Add (Ajoutez)** un **Name (Nom)** et éventuellement une **Description** pour l'objet.
2. Sélectionnez **IP Netmask (Masque de réseau IP)** sous **Type**, puis saisissez l'adresse IP de l'interface externe sur le pare-feu, 203.0.113.100 dans cet exemple.
3. Cliquez sur **OK**.



Bien que vous ne soyez pas obligé d'utiliser des objets adresse dans vos politiques, cette pratique est recommandée car elle simplifie l'administration en vous permettant d'effectuer des mises à jour dans un emplacement, au lieu d'avoir à mettre à jour toutes les politiques dans lesquelles l'adresse est référencée.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Créez une politique NAT.

1. Sélectionnez **Policies (Politiques)** > **NAT**, puis cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, donnez un **Name (nom)** descriptif à la politique.
3. (Facultatif) Saisissez une étiquette, qui est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques.
4. Pour **NAT Type (Type de NAT)**, sélectionnez **ipv4** (paramètre par défaut).
5. Dans l'onglet **Original Packet (Paquet d'origine**, sélectionnez la zone que vous avez créée pour votre réseau interne dans la section **Source Zone (Zone source)** (cliquez sur **Add (Ajouter)**, puis sélectionnez la zone) et la zone que vous avez créée pour le réseau externe dans la liste **Destination Zone (Zone de destination)**.
6. Sous l'onglet **Translated Packet (Paquet traduit)**, pour **Translation Type (Type de traduction)**, sélectionnez **Persistent Dynamic IP And Port (Adresse IP et port dynamiques persistants)**.
7. Pour **Address Type (Type d'adresse)**, deux choix s'offrent à vous. Vous pouvez sélectionner **Translated Address (Adresse traduite)**, puis cliquer sur **Add (Ajouter)**. Sélectionnez l'objet d'adresse que vous avez créé ou saisissez l'adresse source traduite.

   Un **Address Type (Type d'adresse)** alternatif est **Interface Address (Adresse de l'interface)**, auquel cas l'adresse traduite sera l'adresse IP de l'interface. Pour ce choix, sélectionnez une **Interface (Interface)** et éventuellement une **IP Address (Adresse IP)** si l'interface dispose de plusieurs adresses IP.
8. Cliquez sur **OK**.

STEP 3 | **Commit (Validez)** vos modifications.

STEP 4 | (Facultatif) Utilisez les commandes CLI opérationnelles pour afficher les informations DIPP persistantes.

1. Accédez à la CLI.
2. > **`show running persistent-dipp-pool`**
3. > **`show running persistent-dipp-client pool <nat-pool-index>`**
4. > **`show running persistent-dipp-client-translation ip <client-ip-address>`**



Utilisez les deux dernières commandes show lors de l'exécution pour suivre l'utilisation des ressources NAT persistantes par adresse IP du client.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | (Facultatif) Utilisez les commandes CLI de configuration pour surveiller l'utilisation du pool DIPP persistant. Un syslog est généré si l'utilisation des ressources dépasse le seuil que vous avez configuré.

1. Accédez à la CLI.
2. > **configure**
3. **# set deviceconfig setting session persistent-dipp-alert-enable <no|yes>**
4. **# set deviceconfig setting session persistent-dipp-alert-threshold <1-99>**
5. **# set deviceconfig setting session persistent-dipp-alert-interval <5-120>**

Strata Cloud Manager

À partir de SCM R3, Strata Cloud Manager prend en charge une règle NAT qui utilise le DIPP persistant.

STEP 1 | Dans Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (Accès NGFW et Prisma).**

STEP 2 | Sélectionnez **Network Policies (Politiques réseau)** > **NAT**

STEP 3 | **Add Rule (Ajoutez une règle)** et saisissez un **Name (Nom)** pour la règle de politique NAT source.

STEP 4 | Configurez les zones et adresses sources des paquets, la zone de destination, l'interface et les adresses, ainsi que le service.

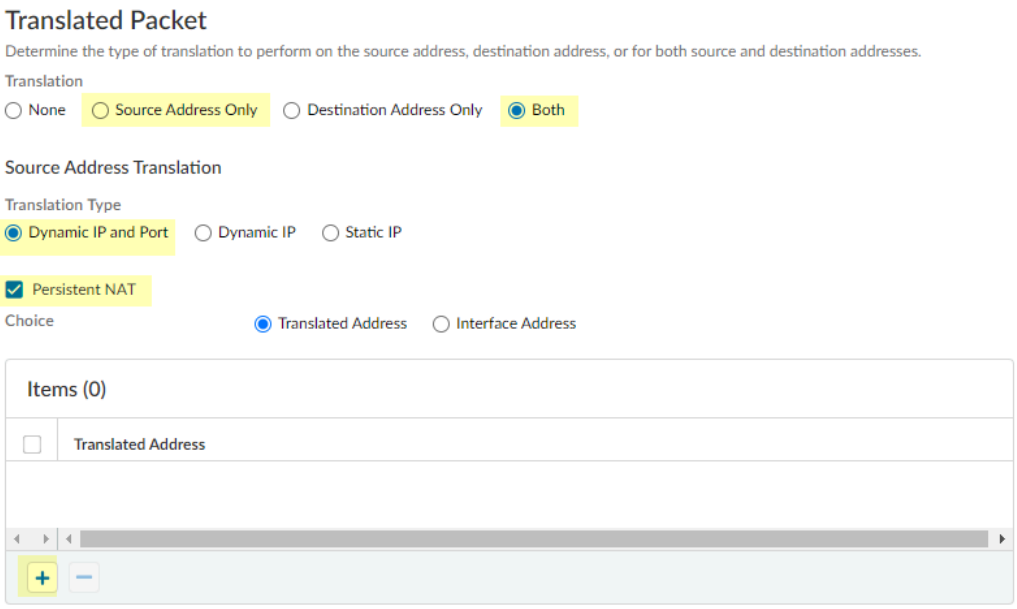
STEP 5 | Pour le paquet traduit, sélectionnez **Source Address Only (Adresse source uniquement)** ou **Both (Les deux)** (adresse source et adresse de destination).

STEP 6 | Pour Translation Type (Type de traduction), sélectionnez **Dynamic IP and Port (Adresse IP et port dynamiques)**.

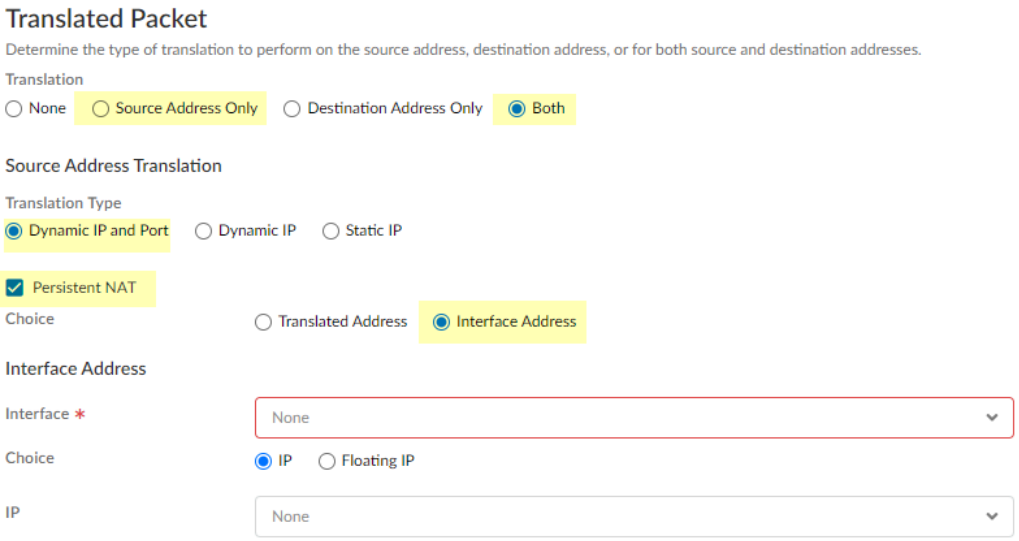
STEP 7 | Sélectionnez **Persistent NAT (NAT persistant)**.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | Vous pouvez sélectionner **Translated Address (Adresse traduite)**, puis sélectionner le + pour sélectionner l'objet d'adresse que vous avez créé ou entrer l'adresse source traduite.



STEP 9 | Vous pouvez également sélectionner **Interface Address (Adresse de l'interface)**, auquel cas l'adresse traduite sera l'adresse IP de l'interface. Pour ce choix, sélectionnez une **Interface** et une adresse **IP** si l'interface dispose de plusieurs adresses IP. Ou vous pouvez sélectionner **Floating IP (IP flottante)** (et sélectionner un objet d'adresse).



STEP 10 | Si vous avez sélectionné **Both (Les deux)** traductions source et destination, continuez en configurant la **Translated Address (Adresse traduite)** et le **Translated Port (Port traduit)** de destination.

STEP 11 | Cliquez sur **Save (enregistrer)** pour enregistrer la configuration.

 ©2024 Palo Alto Networks, Inc.

Autorisation d'accès des clients sur le réseau interne à vos serveurs publics (NAT U-Turn de destination)

Lorsqu'un utilisateur du réseau interne envoie une demande d'accès au serveur Web de l'entreprise dans la zone DMZ, le serveur DNS va résoudre cette demande en adresse IP publique. Lors du traitement de la demande, le pare-feu va utiliser la destination d'origine du paquet (adresse IP publique) et acheminer le paquet vers l'interface de sortie de la zone non approuvée. Pour que le pare-feu sache qu'il doit traduire l'adresse IP publique du serveur Web en adresse sur le réseau DMZ lors de la réception des demandes d'utilisateurs de la zone approuvée, vous devez créer une règle NAT de destination qui va autoriser le pare-feu à envoyer la demande à l'interface de sortie de la zone DMZ de la manière suivante.

STEP 1 | Créez un objet adresse pour le serveur Web.

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)** et **Add (Ajoutez)** un **Name (Nom)** et éventuellement une **Description (Description)** pour l'objet d'adresse.
2. Sous **Type (Type)**, sélectionnez **IP Netmask (Masque réseau IP)**, puis entrez l'adresse IP publique du serveur Web, dans cet exemple : 203.0.113.11.

   Vous pouvez faire passer le type d'objet d'adresse de **IP Netmask (Masque réseau IP)** à **FQDN** en cliquant sur **Resolve (Résoudre)**, et lorsque le FQDN apparaît, cliquez sur **Use this FQDN (Utiliser ce FQDN)**. Sous **Type**, vous pouvez également sélectionner **FQDN** et saisir le FQDN à utiliser pour cet objet d'adresse. Si vous saisissez un FQDN et que vous cliquez sur **Resolve (Résoudre)**, l'adresse IP dont le FQDN prend la forme s'affiche dans le champ. Pour faire passer le **Type** d'un objet d'adresse de FQDN à un masque réseau IP en utilisant cette adresse IP, cliquez sur **Use this address (Utiliser cette adresse)**, et le **Type** passera à **IP Netmask (Masque réseau IP)** et l'adresse IP apparaîtra dans le champ.
3. Cliquez sur **OK**.

STEP 2 | Créez une politique NAT.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)**, puis cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la règle NAT.
3. Dans l'onglet **Original Packet (Paquet d'origine**, sélectionnez la zone que vous avez créée pour votre réseau interne dans la section **Source Zone (Zone source)** (cliquez sur **Add (Ajouter)**, puis sélectionnez la zone) et la zone que vous avez créée pour le réseau externe dans la liste **Destination Zone (Zone de destination)**.
4. Dans la section **Destination Address (Adresse de destination)**, **Add (Ajoutez)** l'objet d'adresse que vous avez créé pour votre serveur Web public.
5. Dans l'onglet **Translated Packet (Paquet traduit)**, sous Destination Address Translation (Traduction de l'adresse de destination) et sous **Translation Type (Type de traduction)**, sélectionnez **Static IP (IP statique)**, puis saisissez l'adresse IP affectée à l'interface du serveur Web sur le réseau DMZ, 10.1.1.11 dans cet exemple. Vous pouvez également sélectionner **Dynamic IP (with session distribution) (IP dynamique (avec distribution de session)** comme **Translation Type (Type de traduction)**, puis indiquer une **Translated Address (Adresse traduite)** qui correspond à un objet d'adresse ou à un groupe d'adresses qui utilise un masque réseau IP, une plage d'adresses IP ou un FQDN. Ils peuvent tous retourner plusieurs adresses de DNS. Si l'adresse de destination translatée se résout en plus d'une adresse, le pare-feu distribue les sessions NAT entrante parmi

 ©2024 Palo Alto Networks, Inc.

les adresses multiples en fonction d'une des nombreuses méthodes que vous pouvez sélectionner : **Round Robin (permutation circulaire)** (la méthode par défaut), **Source IP Hash (Hachage IP source)**, **IP Modulo (Modulo IP)**, **IP Hash (Hachage IP)** ou **Least Sessions (Moins de sessions)**.

6. Cliquez sur **OK**.

STEP 3 | Cliquez sur **Commit (Valider)**.

Activation de la traduction bidirectionnelle d'adresses pour vos serveurs orientés public (NAT source statique)

Lorsque vos serveurs orientés public disposent d'adresses IP privées affectées au segment de réseau dans lequel elles sont physiquement présentes, vous aurez besoin d'une règle NAT source pour traduire l'adresse source du serveur en adresse externe lors de sa sortie. Créez une règle NAT statique pour traduire l'adresse source interne, 10.1.1.11, en adresse de serveur Web externe, 203.0.113.11 dans notre exemple.

Cependant, un serveur orienté public doit pouvoir envoyer et recevoir des paquets. Vous avez besoin d'une politique réciproque qui traduit l'adresse publique (l'adresse IP de destination des paquets entrants issus d'utilisateurs Internet) en adresse privée afin que le pare-feu puisse correctement acheminer les paquets vers votre réseau DMZ. Créez une règle NAT statique bidirectionnelle, comme décrit dans la procédure suivante. La traduction bidirectionnelle est une option de la NAT statique uniquement.

STEP 1 | Créez un objet adresse pour l'adresse IP interne du serveur Web.

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)** et **Add (Ajoutez)** un **Name (Nom)** et éventuellement une **Description (Description)** pour l'objet.
2. Sélectionnez **IP Netmask (Masque de réseau IP)** dans la liste **Type (Type)**, puis saisissez l'adresse IP du serveur Web sur le réseau DMZ, 10.1.1.11 dans cet exemple.
3. Cliquez sur **OK**.

Si vous n'avez pas déjà créé un objet adresse pour l'adresse publique de votre serveur Web, il est conseillé de créer cet objet maintenant.

STEP 2 | Créez une politique NAT.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)**, puis cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la règle NAT.
3. Dans l'onglet **Original Packet (Paquet d'origine**, sélectionnez la zone que vous avez créée pour votre DMZ dans la section **Source Zone (Zone source)** (cliquez sur **Add (Ajouter)**, puis sélectionnez la zone) et la zone que vous avez créée pour le réseau externe dans la liste **Destination Zone (Zone de destination)**.
4. Dans la section **Source Address (Adresse source)**, **Add (Ajoutez)** l'objet d'adresse que vous avez créé pour l'adresse de votre serveur Web interne.
5. Dans l'onglet **Translated Packet (Paquet traduit)**, sélectionnez **Static IP (Adresse IP statique)** dans la liste **Translation Type (Type de traduction)** de la section **Source Address Translation (Traduction de l'adresse source)**, puis sélectionnez l'objet adresse

 ©2024 Palo Alto Networks, Inc.

que vous avez créé pour l'adresse de votre serveur Web externe dans la liste **Translated Address (Adresse traduite)**.

6. Dans le champ **Bi-directional (Bidirectionnelle)**, sélectionnez **Yes (Oui)**.
7. Cliquez sur **OK**.

STEP 3 | Validez.

Cliquez sur **Commit (Valider)**.

Configuration de la NAT de destination avec réécriture DNS

Lorsque vous configurez une règle de politique NAT de destination qui effectue la traduction statique des adresses IPv4, vous pouvez également configurer la règle afin que le pare-feu réécrive l'adresse IPv4 dans une réponse DNS en fonction de l'adresse IP d'origine ou traduite configurée pour la règle. Le pare-feu effectue la NAT sur l'adresse IPv4 (résolution du FQDN) dans une réponse DNS (qui correspond à la règle) avant de transférer la réponse au client. Par conséquent, le client reçoit l'adresse appropriée pour atteindre le service de destination.

Consultez les cas d'utilisation de la réécriture DNS pour vous aider à déterminer si vous devez spécifier si la réécriture doit se produire dans le sens **reverse (inverse)** ou **forward (direct)**.

*Vous ne pouvez pas activer la traduction **Bi-directional (bidirectionnelle)** de l'adresse source dans la même règle de NAT où vous activer la réécriture DNS.*

STEP 1 | Créez une règle de politique NAT de destination qui précise que le pare-feu effectue la traduction statique des adresses IPv4 qui correspondent à la règle, et qui précise également que le pare-feu réécrit les adresses IP dans les réponses DNS lorsque l'adresse IPv4 (de l'enregistrement A) correspond à l'adresse de destination d'origine ou traduite qui figure dans la règle NAT.

1. Sélectionnez **Policies (Politiques)** > **NAT**, puis **Add (Ajoutez)** une règle de politique NAT.
2. (Facultatif) Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la règle.
3. Pour **NAT Type (Type de NAT)**, sélectionnez **ipv4**.
4. Sur l'onglet **Original Packet (Paquet d'origine)**, **Add (Ajoutez)** une **Destination Address (Adresse de destination)**.

   *Vous devrez également sélectionner une zone source ou **Any (Toute)** zone source, mais la réécriture de DNS se fait au niveau global ; seule l'adresse de destination de l'onglet Paquet d'origine correspond. La réécriture de DNS ignore tous les autres champs de l'onglet Paquet d'origine.*
5. À l'onglet **Translated Packet (Paquet traduit)**, par la traduction de l'adresse de destination, sélectionnez **Static IP (IP statique)** comme **Translation Type (Type de traduction)** .
6. Sélectionnez une **Translated Address (Adresse traduite)** ou saisissez une nouvelle adresse.
7. **Enable DNS Rewrite (Activez la réécriture DNS)**, puis sélectionnez un **Direction (Sens)** :
   - Sélectionnez **reverse (inverser)** (par défaut) lorsque l'adresse IP qui figure dans la réponse DNS exige la traduction opposée à celle que la règle NAT indique. Si la réponse DNS correspond à l'adresse de destination **Translated (Traduite)** dans la

 ©2024 Palo Alto Networks, Inc.

règle, traduisez la réponse DNS en utilisant la translation inverse que la règle utilise. Par exemple, si la règle traduit l'adresse IP 1.1.1.10 en 192.168.1.10, le pare-feu réécrit une réponse DNS 192.168.1.10 en 1.1.1.10.

- Sélectionnez **forward (directe)** lorsque l'adresse IP qui figure dans la réponse DNS exige la même traduction que celle indiquée dans la règle NAT indique. Si la réponse DNS correspond à l'adresse de destination **Original (originale)** dans la règle, traduisez la réponse DNS en utilisant la même traduction que la règle utilise. Par exemple, si la règle traduit l'adresse IP 1.1.1.10 en 192.168.1.10, le pare-feu réécrit une réponse DNS 1.1.1.10 en 192.168.1.10.

8. Cliquez sur **OK**.

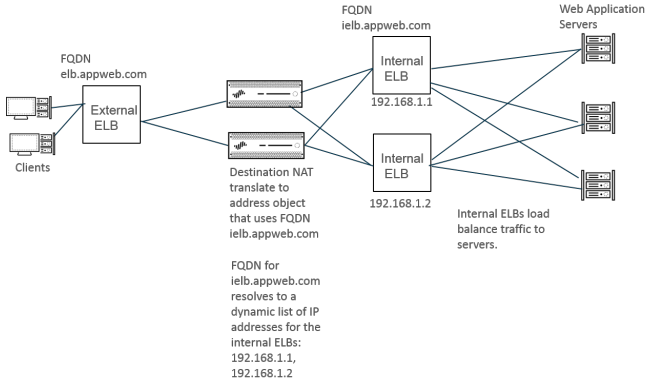
STEP 2 | **Commit (Validez)** vos modifications.

Configuration de la NAT de destination à l'aide des adresses IP dynamiques

Utilisez la NAT de destination pour translater l'adresse de destination initiale en un serveur ou un hôte de destination qui possède une adresse IP dynamique et utilise un FQDN. Une NAT de destination qui utilise une adresse IP dynamique s'avère particulièrement utile dans des déploiements de cloud, qui se servent généralement d'adresses IP dynamiques. Lorsque l'hôte ou le serveur du cloud possède de nouvelles adresses IP (dynamiques), vous n'avez pas à mettre manuellement à jour la règle de politique NAT en interrogeant continuellement le serveur DNS. Vous n'avez pas non plus à utiliser un composant externe distinct pour mettre à jour le serveur DNS avec le plus récent mappage FQDN-adresse IP.

Lorsque vous configurez le NAT de destination à l'aide d'adresses IP dynamiques, vous devez utiliser uniquement un FQDN (pas un masque de réseau IP ou une plage IP).

Dans la topologie d'exemples suivante, les clients veulent joindre des serveurs qui hébergent des applications Web dans le cloud. Un Elastic Load Balancer (Équilibrage de charge élastique ; ELB) connecte les pare-feu, qui se connectent aux ELB internes, qui connectent aux serveurs. Au fil du temps, Amazon Web Services (AWS), par exemple, ajoute (et supprime) des adresses pour le FQDN affectées aux ELB internes, selon la demande de services. La flexibilité que procure l'utilisation d'un FQDN pour NAT au ELB interne aide la politique à résoudre différentes adresses IP à des moments différents, ce qui facilite l'utilisation de NAT de destination, car les mises à jour sont dynamiques.



 ©2024 Palo Alto Networks, Inc.

STEP 1 | Créez un objet d'adresse qui utilise le FQDN du serveur en lequel vous souhaitez traduire l'adresse.

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)** et **Add (Ajoutez)** un objet d'adresse en indiquant son **Name (Nom)**, comme **`post-NAT-Internal-ELB`**.
2. Sélectionnez **FQDN** comme **Type**, puis saisissez le FQDN. Dans cet exemple, le FQDN est **`ielb.appweb.com`**.
3. Cliquez sur **OK**.

STEP 2 | Créez la politique NAT de destination.

1. Sélectionnez **Policies (Politiques)** > **NAT** et **Add (Ajoutez)** une règle de politique NAT en indiquant son **Name (Nom)** à l'onglet **General (Général)**.
2. Sélectionnez **ipv4** comme **NAT Type (Type de NAT)**.
3. À l'onglet **Original Packet (Paquet d'origine)**, **Add (Ajoutez)** la **Source Zone (Zone source)** et la **Destination Zone (Zone de destination)**.
4. À l'onglet **Translated Packet (Paquet traduit)**, à la section Destination Address Translation (Traduction de l'adresse de destination), sélectionnez **Dynamic IP (with session distribution) (Adresse IP dynamique (avec distribution de session)** comme **Translation Type (Type de traduction)**.
5. Sous **Translated Address (Adresse traduire)**, sélectionnez l'objet d'adresse que vous avez créé pour le FQDN. Dans cet exemple, le FQDN est **`post-NAT-Internal-ELB`**.
6. Sous **Session Distribution Method (Méthode de Distribution de Sessions)**, sélectionnez l'une des options suivantes :

   - **Round Robin (Pondération comparative)** : (par défaut) affecte de nouvelles sessions à des adresses IP en ordre rotatif. Sauf si vous avez une raison de modifier la méthode de distribution, la distribution par pondération comparative convient probablement.
   - **Source IP Hash (Hachage IP source)** : affecte de nouvelles sessions en fonction du hachage de l'adresse IP source. Si vous avez du trafic entrant provenant d'une seule adresse IP source, ne sélectionnez pas le hachage IP source ; sélectionnez une autre méthode.
   - **IP Modulo (Modulo IP)** : Le pare-feu tient compte de l'adresse IP source et de destination du paquet entrant ; le pare-feu effectue une opération XOR et une opération modulo. Le résultat détermine à quelle adresse IP le pare-feu affecte les nouvelles sessions.
   - **IP Hash (Hachage IP)** : affecte de nouvelles sessions en fonction d'un hachage d'adresses IP source et de destination.
   - **Least Sessions (Le moins de sessions)** : affecte de nouvelles sessions à l'adresse IP qui possède le moins de sessions concurrentes. Si vous disposez de nombreuses

 ©2024 Palo Alto Networks, Inc.

sessions de courte durée, l'option **Least Sessions (le moins de sessions)** vous fournit une distribution plus équilibrée des sessions.

Le pare-feu ne supprime pas les adresses IP doubles de la liste des adresse IP de destination avant de distribuer des sessions aux adresses IP. Le pare-feu distribue des sessions aux adresses doubles de la même façon qu'il distribue des sessions aux adresses non doubles. (Des adresses doubles dans le pool de traduction peuvent se produire, par exemple, si l'adresse translatée est un groupe d'adresses d'objets d'adresse et qu'un objet d'adresse est un FQDN qui se résout en une adresse IP et qu'un autre objet d'adresse correspond à une plage qui comprend la même adresse IP.)

7. Cliquez sur **OK**.

STEP 3 | **Commit (Validez)** vos modifications.

STEP 4 | (Facultatif) Vous pouvez configurer la fréquence à laquelle le pare-feu actualise un FQDN (Cas pratique 1 : Le pare-feu exige une résolution DNS).

Modification du taux de dépassement d'abonnement NAT DIPP

Si vous disposez suffisamment d'adresses IP publiques pour ne pas avoir besoin d'utiliser le dépassement d'abonnement NAT DIPP, vous pouvez réduire le taux de dépassement d'abonnement et autoriser ainsi un plus grand nombre de règles NAT DIPP et d'adresses IP dynamiques.

STEP 1 | Affichez le taux de dépassement d'abonnement NAT DIPP.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** > **Session Settings (Paramètres de session)**. Affichez le paramètre **Taux de sursouscription NAT**.

STEP 2 | Définissez le taux de dépassement d'abonnement NAT DIPP.

1. Modifiez la section Session Settings (Paramètres de session).
2. Dans la liste **NAT Oversubscription Rate (Taux de sursouscription NAT)**, sélectionnez **1x**, **2x**, **4x** ou **8x**, en fonction du taux souhaité.

   *Le paramètre **Platform Default (Valeur par défaut de la plate-forme)**applique le taux de sursouscription par défaut du modèle. Si vous ne souhaitez aucune sursouscription, sélectionnez **x 1**.*

3. Cliquez sur **OK** et sur **Commit (Valider)** pour enregistrer la modification.

Réservation d'adresses NAT IP dynamiques

Vous pouvez réserver des adresses NAT IP dynamiques (pour une période configurable) afin d'empêcher leur affectation en tant qu'adresses traduites à une autre adresse IP source qui doit être traduite. Une fois configurée, la réservation s'applique à toutes les traductions d'adresses IP dynamiques en cours et à toute nouvelle traduction.

Pour les traductions en cours et les nouvelles, lorsqu'une adresse IP source est traduite vers une adresse IP traduite disponible, cet appariement est conservé, même après l'expiration de toutes les sessions relatives à cette adresse IP source spécifique. Le minuteur de réservation

 ©2024 Palo Alto Networks, Inc.

de chaque adresse IP source démarre après l'expiration de toutes les sessions relatives à la traduction de cette adresse IP source. La NAT d'adresses IP dynamiques est une traduction 1 à 1 ; une adresse IP source est traduite vers une adresse IP traduite qui est choisie de manière dynamique parmi les adresses disponibles du pool configuré. Par conséquent, une adresse IP traduite réservée n'est disponible pour aucune autre adresse IP source jusqu'à l'expiration de la réservation, car une nouvelle session n'a pas démarré. Le minuteur est réinitialisé au démarrage de chaque nouvelle session relative à un mappage adresse IP source/adresse IP traduite, après une certaine période d'inactivité de session.

Par défaut, aucune adresse n'est réservée. Vous pouvez réserver des adresses NAT IP dynamiques pour le pare-feu ou un système virtuel.

- Réservation d'adresses NAT IP dynamiques pour un pare-feu.

  Entrez les commandes suivantes :

  ```
  admin@PA-3250# set setting nat reserve-ip yes
  ```

  ```
  admin@PA-3250# set setting nat reserve-time <1-604800 secs>
  ```

- Réservation d'adresses NAT IP dynamiques pour un système virtuel.

  Entrez les commandes suivantes :

  ```
  admin@PA-3250# set vsys <vsysid> setting nat reserve-ip yes
  ```

  ```
  admin@PA-3250# set vsys <vsysid> setting nat reserve-time <1-604800
   secs>
  ```

  Par exemple, supposons qu'un pool NAT d'adresses IP dynamiques dispose de 3 adresses et que 20 traductions sont en cours lorsque le paramètre **nat reserve-time** est défini sur 28 800 secondes (8 heures). Ces 20 traductions sont maintenant réservées ; par conséquent, lors de l'expiration de la dernière session (de toute application) qui utilise chaque mappage adresse IP source/adresse IP traduite, l'adresse IP traduite est réservée uniquement pour l'adresse IP source pendant 8 heures, au cas où cette adresse IP source doit être de nouveau traduite. De plus, tant que les 10 adresses traduites restantes sont affectées, elles sont réservées pour cette adresse IP source, chacune avec un minuteur qui démarre après l'expiration de la dernière session relative à cette adresse IP source.

  De cette manière, chaque adresse IP source peut être traduite de façon répétée vers son adresse NAT identique du pool ; aucune adresse IP traduite réservée du pool ne sera affectée à un autre hôte, même si aucune session n'est active pour cette adresse traduite.

  Supposons que toutes les sessions relatives à un mappage adresse IP source/adresse IP traduite expirent et que le minuteur de réservation de 8 heures démarre. Au démarrage d'une nouvelle session relative à cette traduction, le minuteur s'arrête et les sessions continuent

 ©2024 Palo Alto Networks, Inc.

jusqu'à ce qu'elles se terminent, auquel cas le minuteur de réservation redémarre, réservant ainsi l'adresse traduite.

Le minuteur de réservation reste effectif sur le pool NAT d'adresses IP dynamiques jusqu'à ce que vous le désactiviez en saisissant la commande **`set setting nat reserve-ip no`** ou modifiez la valeur du paramètre **`nat reserve-time`**.

Les commandes CLI pour les réservations n'affectent pas les pools NAT DIPP ou d'adresses IP statiques.

Désactivation de la NAT pour un hôte ou une interface spécifique

Les règles NAT source et de destination peuvent être configurées pour désactiver la traduction d'adresses. Il se peut qu'il y ait des exceptions où vous ne souhaitez pas que la NAT soit effectuée pour un certain hôte d'un sous-réseau ou pour le trafic quittant une interface spécifique. La procédure suivante décrit comment désactiver la NAT source pour un hôte.

STEP 1 | Créez une politique NAT.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)** et cliquez sur **Add (Ajouter)** pour donner un **Name (Nom)** descriptif à la politique.
2. Dans l'onglet **Original Packet (Paquet d'origine**, sélectionnez la zone que vous avez créée pour votre réseau interne dans la section **Source Zone (Zone source)** (cliquez sur **Add (Ajouter)**, puis sélectionnez la zone) et la zone que vous avez créée pour le réseau externe dans la liste **Destination Zone (Zone de destination)**.
3. Pour **Source Address (Adresse source)**, cliquez sur **Add (Ajouter)** et saisissez l'adresse de l'hôte. Cliquez sur **OK**.
4. Dans l'onglet **Translated Packet (Paquet traduit)**, sélectionnez **None (Aucun)** dans la liste **Translation Type (Type de traduction)** de la section Source Address Translation (Traduction de l'adresse source) affichée à l'écran.
5. Cliquez sur **OK**.

STEP 2 | Validez vos modifications.

Cliquez sur **Commit (Valider)**.

Les règles NAT sont traitées dans l'ordre, de haut en bas ; par conséquent, placez la politique d'exemption NAT avant les autres politiques NAT de façon à ce qu'elle soit traitée avant la traduction d'adresses des sources que vous souhaitez exempter.

 ©2024 Palo Alto Networks, Inc.

Exemples de configuration NAT

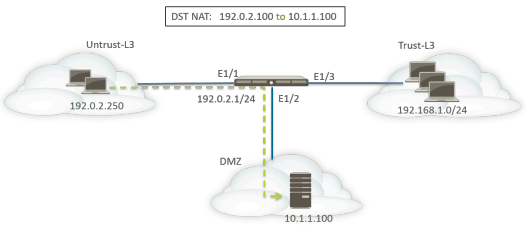
- Exemple de NAT de destination : mappage un à un
- Exemple de NAT de destination avec traduction de port
- Exemple de NAT de destination : mappage un à plusieurs
- Exemple de NAT source et de NAT de destination
- Exemple de NAT source dans un câble virtuel
- Exemple de NAT statique dans un câble virtuel
- Exemple de NAT de destination dans un câble virtuel

Exemple de NAT de destination : mappage un à un

Les erreurs les plus courantes lors de la configuration de règles NAT et de sécurité sont les références aux zones et aux objets adresse. Les adresses utilisées dans les règles NAT de destination font toujours référence à l'adresse IP dans le paquet d'origine (c'est-à-dire l'adresse prétraduite). La zone de destination dans la règle NAT est déterminée après la recherche d'itinéraire de l'adresse IP de destination dans le paquet d'origine (c'est-à-dire l'adresse IP de destination pré-NAT).

Les adresses dans la politique de sécurité font également référence à l'adresse IP dans le paquet d'origine (c'est-à-dire l'adresse pré-NAT). Cependant, la zone de destination est la zone dans laquelle l'hôte final est physiquement connecté. Autrement dit, la zone de destination dans la règle de sécurité est déterminée après la recherche d'itinéraire de l'adresse IP de destination post-NAT.

Dans l'exemple suivant d'un mappage NAT un à un, les utilisateurs de la zone nommée Untrust-L3 accèdent au serveur 10.1.1.100 dans la zone nommée DMZ en utilisant l'adresse IP 192.0.2.100.



Avant de configurer les règles NAT, prenez en compte la séquence d'événements de ce scénario.

- L'hôte 192.0.2.250 envoie une requête ARP à l'adresse 192.0.2.100 (l'adresse publique du serveur de destination).
- Le pare-feu reçoit le paquet de requête ARP pour la destination 192.0.2.100 sur l'interface Ethernet1/1 et traite la demande. Le pare-feu répond à la requête ARP avec sa propre adresse MAC en raison de la règle NAT de destination configurée.
- Les règles NAT sont évaluées pour une correspondance. Une règle NAT de destination de la zone untrust-l3 doit être créée pour traduire l'adresse IP de destination 192.0.2.100 en 10.1.1.100.
- Après la détermination de l'adresse traduite, le pare-feu effectue une recherche d'itinéraire pour la destination 10.1.1.100 afin de définir l'interface de sortie. Dans cet exemple, l'interface de sortie est Ethernet1/2 dans la zone DMZ.

 ©2024 Palo Alto Networks, Inc.

- Le pare-feu effectue une recherche d'itinéraire pour voir si le trafic est autorisé de la zone Untrust-L3 à la zone DMZ.

  Le sens de la politique correspond à la zone d'entrée et à celle où le serveur se trouve physiquement.

  La politique de sécurité fait référence à l'adresse IP de destination 192.0.2.100 dans le paquet d'origine.

- Le pare-feu transfère le paquet au serveur via l'interface de sortie Ethernet1/2. L'adresse de destination est modifiée en 10.1.1.100 lorsque le paquet quitte le pare-feu.

Dans cet exemple, les objets adresse sont configurés pour le serveur Web privé (10.1.1.100) et le serveur Web public (192.0.2.100). La règle NAT configurée devrait ressembler à ce qui suit :

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Webserver-public	any	none	destination-translation address: webserver-private

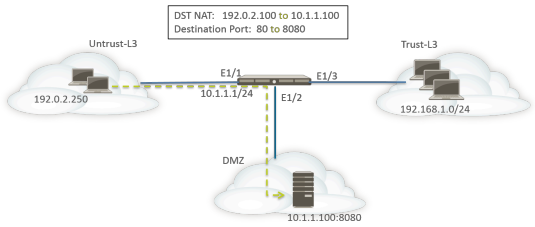
Le sens des règles NAT est basé sur le résultat de la recherche d'itinéraire.

La politique de sécurité configurée permettant l'accès au serveur de la zone untrust-l3 devrait ressembler à ce qui suit :

	Source		Destination						
NAME	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Webserver access	Untrust-L3	any	DMZ	Webserver-pu...	web-browsing	any	Allow	none	

Exemple de NAT de destination avec traduction de port

Dans cet exemple, le serveur Web est configuré pour écouter le trafic HTTP sur le port 8080. Les clients accèdent au serveur Web en utilisant l'adresse IP 192.0.2.100 et le port TCP 80. La règle NAT de destination est configurée pour traduire l'adresse IP en 10.1.1.100 et le port TCP en 8080. Les objets adresse sont configurés pour le serveur Web privé (10.1.1.100) et les serveurs publics (192.0.2.100).



Les règles NAT et de sécurité suivantes doivent être configurées sur le pare-feu :

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	any	none	destination-translation address: webserver-private port: 8080

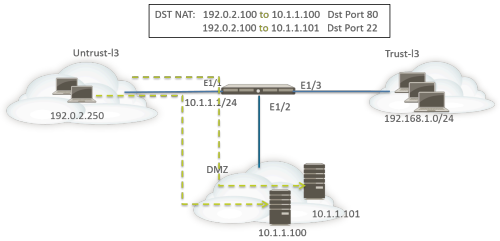
			Source				Destination					
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow

Utilisez la commande CLI **`show session all`** pour vérifier la traduction.

 ©2024 Palo Alto Networks, Inc.

Exemple de NAT de destination : mappage un à plusieurs

Dans cet exemple, une adresse IP correspond à deux hôtes internes différents. Le pare-feu utilise l'application pour identifier l'hôte interne auquel le pare-feu transfère le trafic.



L'ensemble du trafic HTTP est envoyé à l'hôte 10.1.1.100 et le trafic SSH est envoyé au serveur 10.1.1.101. Les objets adresse suivants sont requis :

- L'objet adresse pour l'adresse IP prétraduite du serveur.
- L'objet adresse pour l'adresse IP réelle du serveur SSH.
- L'objet adresse pour l'adresse IP réelle du serveur Web.

Les objets adresse correspondants sont créés :

- Serveurs publics : 192.0.2.100
- Serveur SSH : 10.1.1.101
- Serveur Web privé : 10.1.1.100

Les règles NAT devraient ressembler à ce qui suit :

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	service-http	none	destination-translation address: webserver-private
Dst NAT-SSH	none	Untrust-L3	Untrust-L3	any	any	Servers-public	custom-ssh	none	destination-translation address: SSH-server

Les règles de sécurité devraient ressembler à ce qui suit :

			Source				Destination					
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow
SSH access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	ssh	any	Allow

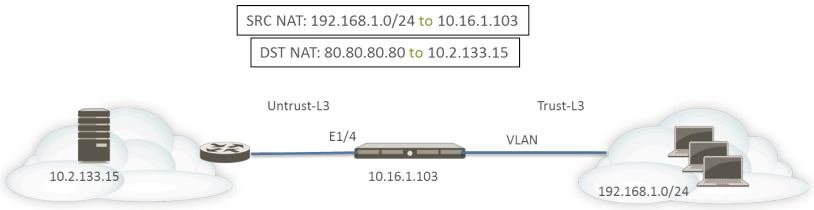
Exemple de NAT source et de NAT de destination

Dans cet exemple, les règles NAT traduisent les adresses IP source et de destination des paquets entre les clients et le serveur.

- NAT source : les adresses source dans les paquets des clients dans la zone Trust-L3 au serveur dans la zone Untrust-L3 sont traduites depuis les adresses privées sur le réseau 192.168.1.0/24 vers l'adresse IP de l'interface de sortie sur le pare-feu (10.16.1.103). La traduction DIPP entraîne également la traduction des numéros de port.

©2024 Palo Alto Networks, Inc.

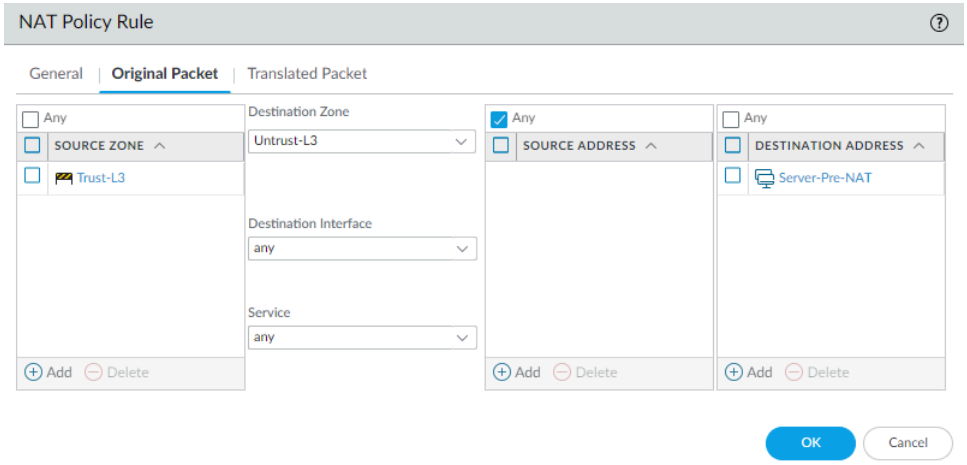
- NAT de destination : les adresses de destination dans les paquets des clients au serveur sont traduites depuis l'adresse publique du serveur (80.80.80.80) vers l'adresse privée du serveur (10.2.133.15).

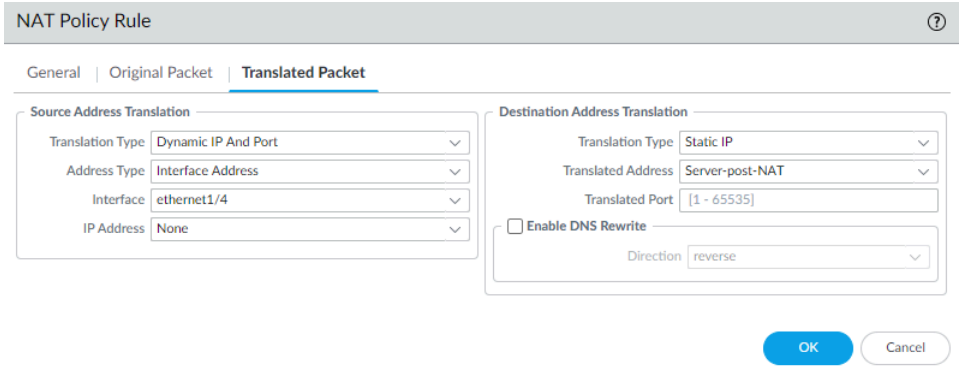


Les objets adresse suivants sont créés pour la NAT de destination.

- Pré-NAT du serveur : 80.80.80.80
- Post-NAT du serveur : 10.2.133.15

Les captures d'écran suivantes illustrent la configuration des politiques NAT source et de destination dans cet exemple.





Pour vérifier les traductions, utilisez la commande CLI **`show session all filter destination 80.80.80.80`**. Veuillez noter qu'une adresse de client 192.168.1.11 et son numéro de port sont traduits en 10.16.1.103 et un numéro de port. L'adresse de destination 80.80.80.80 est traduite en 10.2.133.15.

©2024 Palo Alto Networks, Inc.

Exemple de NAT source dans un câble virtuel

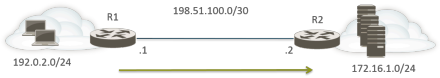
Le déploiement de câble virtuel pour un pare-feu Palo Alto Networks® permet notamment d'assurer la sécurité des périphériques finaux de façon transparente. Il est possible de configurer une NAT pour les interfaces configurées dans un câble virtuel. Tous les types de NAT sont autorisés : NAT source (d'adresses IP dynamiques, DIPP et d'adresses IP statiques) et NAT de destination.

Comme aucune adresse IP n'est affectée aux interfaces dans un câble virtuel, il n'est pas possible de traduire une adresse IP en adresse IP d'interface. Vous devez configurer un pool d'adresses IP.

Lors de la traduction d'adresses réseau sur des interfaces de câble virtuel, il est recommandé de traduire l'adresse source vers un sous-réseau différent de celui sur lequel les périphériques voisins communiquent. Le pare-feu n'utilise pas le proxy ARP pour les adresses NAT. Un routage correct doit être configuré sur les routeurs en amont et en aval afin que les paquets soient traduits en mode Câble virtuel. Les périphériques voisins ne pourront résoudre les requêtes ARP que pour les adresses IP qui résident sur l'interface du périphérique à l'autre extrémité du câble virtuel. Consultez Proxy ARP pour les pools d'adresses NAT pour plus d'explications sur le proxy ARP.

Dans l'exemple de NAT source ci-dessous, les politiques de sécurité (non affichées) sont configurées depuis la zone de câble virtuel nommée vw-trust vers la zone nommée vw-untrust.

Dans la topologie suivante, deux routeurs sont configurés pour permettre la connectivité entre les sous-réseaux 192.0.2.0/24 et 172.16.1.0/24. La liaison entre les routeurs est configurée sur le sous-réseau 198.51.100.0/30. Le routage statique est configuré sur les deux routeurs pour établir la connectivité entre les réseaux. Avant de déployer le pare-feu dans l'environnement, la topologie et la table de routage de chaque routeur ressemblent à ce qui suit :



Itinéraire sur R1 :

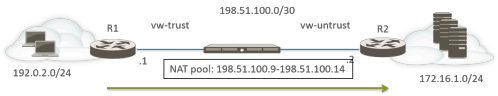
Destination	Saut suivant
172.16.1.0/24	198.51.100.2

Itinéraire sur R2 :

Destination	Saut suivant
192.0.2.0/24	198.51.100.1

Le pare-feu est alors déployé en mode Câble virtuel entre les deux périphériques de Couche 3. Un pool d'adresses IP NAT dont la plage est comprise entre 198.51.100.9 et 198.51.100.14 est configuré sur le pare-feu. Toutes les communications des clients sur le sous-réseau 192.0.2.0/24 accédant aux serveurs sur le réseau 172.16.1.0/24 arriveront au routeur R2 avec une adresse source traduite dans une plage comprise entre 198.51.100.9 et 198.51.100.14. La réponse des serveurs est dirigée vers ces adresses.

©2024 Palo Alto Networks, Inc.



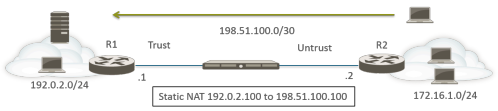
Pour que la NAT source puisse fonctionner, vous devez configurer un routage correct sur le routeur R2, de façon à ce que les paquets destinés à d'autres adresses ne soient pas abandonnés. La table de routage ci-dessous est la table de routage modifiée sur le routeur R2 ; l'itinéraire assure que le trafic vers les destinations comprises entre 198.51.100.9 et 198.51.100.14 (c'est-à-dire les hôtes sur le sous-réseau 198.51.100.8/29) est renvoyé via le pare-feu au routeur R1.

Itinéraire sur R2 :

Destination	Saut suivant
198.51.100.8/29	198.51.100.1

Exemple de NAT statique dans un câble virtuel

Dans cet exemple, les politiques de sécurité sont configurées depuis la zone de câble virtuel nommée Trust vers la zone de câble virtuel nommée Untrust. L'hôte 192.0.2.100 est traduit de manière statique vers l'adresse 198.51.100.100. Lorsque l'option **Bi-directional (Bidirectionnelle)** est activée, le pare-feu génère une politique NAT depuis la zone Untrust vers la zone Trust. Les clients qui se trouvent dans la zone Untrust accèdent au serveur Web en utilisant l'adresse IP 198.51.100.100, que le pare-feu traduit vers l'adresse 198.0.2.100. Toutes les connexions initiées par le serveur à l'adresse 192.0.2.100 sont traduites vers l'adresse IP source 198.51.100.100.



Itinéraire sur R2 :

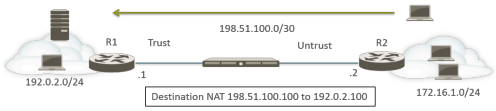
Destination	Saut suivant
198.51.100.100/32	198.51.100.1

	Original Packet						Translated Packet	
NAME	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Static NAT	Trust	Untrust	any	webserver-private	any	any	static-ip webserver-public bi-directional: yes	none

Exemple de NAT de destination dans un câble virtuel

Les clients qui se trouvent dans la zone Untrust accèdent au serveur Web en utilisant l'adresse IP 198.51.100.100, que le pare-feu traduit vers l'adresse 192.0.2.100. Les politiques NAT et de sécurité doivent être configurées depuis la zone Untrust vers la zone Trust.

 ©2024 Palo Alto Networks, Inc.



Itinéraire sur R2 :

Destination	Saut suivant
198.51.100.100/32	198.51.100.1

	Original Packet						Translated Packet	
NAME	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
DST NAT	Untrust	Trust	any	any	webserver-public	any	none	destination-translation address: webserver-private

©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

NPTv6

IPv6-to-IPv6 Network Prefix Translation (traduction du préfixe réseau IPv6 ; NPTv6) effectue la traduction statique et sans état d'un préfixe IPv6 en un autre préfixe IPv6 (les numéros de ports ne changent pas). Les quatre principaux avantages de NPTv6 sont les suivants :

- Vous pouvez empêcher les problèmes de routage asymétriques résultant des adresses de type Provider Independent (PI) publiées par plusieurs centres de données.
- NPTv6 permet la publication d'itinéraires plus spécifiques de façon à ce que le trafic de retour arrive au même pare-feu que celui qui a transmis le trafic.
- Les adresses publiques et privées sont indépendantes ; vous pouvez en modifier une sans affecter l'autre.
- Vous pouvez traduire des Unique Local Address (adresse locale unique - ULA) en adresses globalement routables.

Cette rubrique suppose une compréhension de base de NAT. Assurez-vous de connaître les concepts de NAT avant de configurer NPTv6.

- Présentation de NPTv6
- Fonctionnement de NPTv6
- Proxy NDP
- Exemple de fonctionnement de NPTv6 et du proxy NDP
- Création d'une politique NPTv6

Présentation de NPTv6

Cette section décrit IPv6-to-IPv6 Network Prefix Translation (traduction du préfixe réseau IPv6 - NPTv6) et sa configuration. NPTv6 est défini dans RFC 6296. Palo Alto Networks® n'implémente pas toutes les fonctionnalités définies dans le document RFC, mais celles qui sont implémentées le sont conformément au document RFC.

NPTv6 effectue la traduction sans état d'un préfixe IPv6 en un autre préfixe IPv6. En effet, NPTv6 ne suit ni les ports ni les sessions relatifs aux adresses traduites. NPTv6 diffère de NAT66, qui est une traduction avec état. Palo Alto Networks prend en charge la traduction de préfixe NPTv6 (RFC 6296), mais pas NAT66.

Comme le nombre d'adresses est limité dans l'espace IPv4, une NAT était nécessaire pour traduire les adresses IPv4 privées ne pouvant pas être acheminées vers une ou plusieurs adresses IPv4 globalement routables. Les entreprises utilisant l'adressage IPv6 n'ont pas besoin de traduire les adresses IPv6 en adresses IPv6 en raison de l'abondance d'adresses IPv6. Cependant, il y a des Raisons de l'utilisation de NPTv6 pour traduire les préfixes IPv6 sur le pare-feu.

Il est important de comprendre que NPTv6 ne fournit aucune sécurité. En général, la traduction d'adresses réseau sans état ne fournit aucune sécurité ; sa fonction est uniquement la traduction d'adresses. NPTv6 ne masque ni ne traduit aucun numéro de port. Vous devez configurer des politiques de sécurité du pare-feu correctement dans les deux sens de façon à ce que le trafic soit contrôlé comme souhaité.

NPTv6 traduit la partie préfixe en adresse IPv6 mais pas la partie hôte ni les numéros de ports de l'application. La partie hôte est simplement copiée et reste ainsi identique de chaque côté du pare-feu. La partie hôte reste également visible dans l'en-tête de paquet.

NPTv6 est pris en charge sur les modèles suivants (NPTv6 avec recherche de matériel, mais les paquets passent par le processeur) :

- Pare-feu PA-7000 Series
- Pare-feu PA-5400 Series
- Pare-feu PA-5200 Series
- Pare-feu PA-3200 Series
- Pare-feu PA-800
- Pare-feu PA-220

Les pare-feu VM-Series prennent en charge NPTv6, mais ne permettent pas au matériel d'effectuer une recherche de session.

- Unique Local Address (adresse locale unique - ULA)
- Raisons de l'utilisation de NPTv6

Unique Local Address (adresse locale unique - ULA)

Le document RFC 4193, Adresses de monodiffusion IPv6 locales uniques, définit les Unique Local Addresses (adresses locales uniques - ULA), qui sont des adresses de monodiffusion IPv6. Elles peuvent être considérées comme des équivalents IPv6 des adresses IPv4 identifiées dans le

 ©2024 Palo Alto Networks, Inc.

document RFC 1918, Allocation d'adresses pour les réseaux Internet privés, qui ne peuvent pas être globalement acheminées.

Une ULA est globalement unique, mais non susceptible d'être globalement routable. Elle est destinée aux communications locales et peut être acheminée dans une zone limitée, telle qu'un site, ou entre un petit nombre de sites. Palo Alto Networks® ne recommande pas l'affectation d'ULA, mais un pare-feu configuré avec NPTv6 traduit les préfixes qui lui sont envoyés, y compris les ULA.

Raisons de l'utilisation de NPTv6

Bien qu'il n'y ait aucune pénurie d'adresses IPv6 publiques globalement routables, il y a des raisons pour lesquelles vous pouvez avoir recours à la traduction d'adresses IPv6. NPTv6 :

- **Empêche le routage asymétrique** : un routage asymétrique peut se produire si un espace d'adressage PI (/48, par exemple) est publié par plusieurs centres de données sur Internet. NPTv6 vous permet de publier des itinéraires plus spécifiques depuis des pare-feu régionaux de façon à ce que le trafic de retour arrive au même pare-feu que celui sur lequel l'adresse IP source a été traduite par le traducteur.
- **Empêche l'indépendance des adresses** : vous n'avez pas besoin de modifier les préfixes IPv6 utilisés sur votre réseau local si les préfixes globaux sont modifiés (par exemple, par un ISP ou suite à la fusion d'entreprises). Inversement, vous pouvez modifier les adresses internes au besoin, sans affecter les adresses utilisées pour accéder aux services sur le réseau privé depuis Internet. Dans tous les cas, mettez à jour une règle NAT au lieu de réaffecter les adresses réseau.
- **Traduit les ULA pour le routage** : les Unique Local Address (adresse locale unique - ULA) affectées sur votre réseau privé peuvent être traduites par le pare-feu en adresses globalement routables. Ainsi, vous bénéficiez de la commodité de l'adressage privé et des fonctionnalités des adresses traduites pouvant être acheminées.
- **Réduit l'exposition aux préfixes IPv6** : les préfixes IPv6 sont moins exposés que si vous n'aviez pas traduit les préfixes réseau ; NPTv6 n'est toutefois pas une mesure de sécurité. La partie identifiant d'interface de chaque adresse IPv6 n'est pas traduite ; elle reste identique de chaque côté du pare-feu et visible par toute personne pouvant voir l'en-tête de paquet. De plus, les préfixes ne sont pas sécurisés ; ils peuvent être déterminés par d'autres.

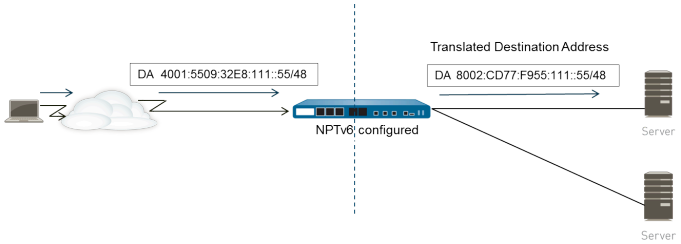
 ©2024 Palo Alto Networks, Inc.

Fonctionnement de NPTv6

Lors de la configuration d'une politique pour NPTv6, le pare-feu Palo Alto Networks® effectue une traduction IPv6 1 à 1 statique dans les deux sens. La traduction est basée sur l'algorithme décrit dans le document RFC 6296.

Dans un cas pratique, le pare-feu procédant à NPTv6 se trouve entre un réseau interne et un réseau externe (tel qu'Internet) qui utilise des préfixes globalement routables. Lorsque les datagrammes sortent du pare-feu, le préfixe source interne est remplacé par le préfixe externe ; c'est ce que l'on appelle la traduction source.

Dans un autre cas pratique, lorsque les datagrammes entrent sur le pare-feu, le préfixe de destination est remplacé par le préfixe interne ; c'est ce que l'on appelle la traduction de destination. La figure ci-dessous illustre la traduction de destination et une caractéristique de NPTv6 : seule la partie préfixe d'une adresse IPv6 est traduite. La partie hôte de l'adresse n'est pas traduite et reste ainsi identique de chaque côté du pare-feu. Dans la figure ci-dessous, l'identifiant hôte est 111::55 de chaque côté du pare-feu.



Il est important de comprendre que NPTv6 ne fournit aucune sécurité. Lors de la planification de vos politiques NAT NPTv6, pensez également à configurer des politiques de sécurité dans les deux sens.

L'adresse source et l'adresse traduite d'une règle de politique NAT ou NPTv6 ne peuvent pas être toutes les deux définies sur Indifférent.

Dans un environnement où vous souhaitez procéder à la traduction de préfixes IPv6, trois fonctionnalités de pare-feu fonctionnent ensemble : les politiques NAT NPTv6, les politiques de sécurité et le proxy NDP.

Le pare-feu ne traduit pas ce qui suit :

- Les adresses contenues dans le cache de détection de voisins (ND) du pare-feu.
- Le sous-réseau 0xFFFF (conformément au document RFC 6296, Annexe B).
- Les adresses IP multicast.
- Les adresses IPv6 dont la longueur de préfixe est de /31 ou inférieure.
- Les adresses locales de liaison. Si le pare-feu fonctionne en mode Câble virtuel, aucune adresse IP ne doit être traduite et le pare-feu ne traduit aucune adresse locale de liaison.
- Les adresses relatives aux sessions TCP qui authentifient les homologues à l'aide de l'option d'authentification TCP (RFC 5925).

Lors de l'utilisation de NPTv6, les performances du trafic sont affectées car NPTv6 se produit lentement.

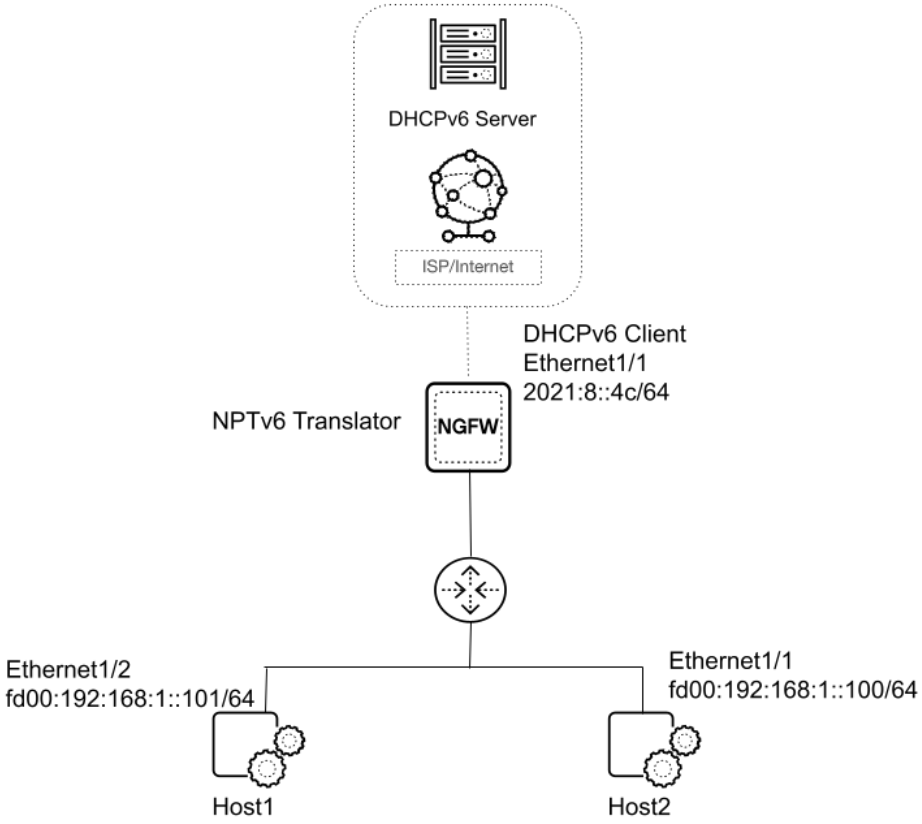
©2024 Palo Alto Networks, Inc.

NPTv6 fonctionne avec IPSec IPv6 uniquement si le pare-feu se trouve au début et à la fin du tunnel. Le trafic IPSec de transit échoue si l'adresse IPv6 source et/ou l'adresse IPv6 de destination est/sont modifiée(s). Une technique de parcours NAT qui encapsule le paquet permet à IPSec IPv6 de fonctionner avec NPTv6.

- Mappage indépendant de la somme de contrôle
- Traduction bidirectionnelle
- NPTv6 appliqué à un service spécifique

NPTv6 avec préfixe d'adresse IPv6 assignée dynamiquement

À partir de PAN-OS 11.1.5, le pare-feu prend en charge NPTv6 en utilisant des préfixes d'adresse IPv6 assignées dynamiquement.



Mappage indépendant de la somme de contrôle

Les traductions de mappage NPTv6 effectuées par le pare-feu sont indépendantes de la somme de contrôle. En effet, « il en résulte des en-têtes IP qui génèrent la même somme de contrôle de pseudo-en-tête IPv6 lorsque la somme de contrôle est calculée en utilisant l'algorithme de somme de contrôle Internet standard » (RFC 1071). Pour plus d'informations sur le mappage indépendant de la somme de contrôle, reportez-vous au document RFC 6296.

 ©2024 Palo Alto Networks, Inc.

Si vous utilisez NPTv6 pour procéder à la NAT de destination, vous pouvez fournir l'adresse IPv6 interne et la longueur de préfixe/le préfixe externe de l'interface du pare-feu dans la syntaxe de la commande CLI **`test nptv6`**. La CLI répond avec une adresse IPv6 publique indépendante de la somme de contrôle à utiliser dans votre configuration NPTv6 pour atteindre cette destination.

Traduction bidirectionnelle

Lors de la Création d'une politique NPTv6, l'option **Bi-directional (Bidirectionnelle)** de l'onglet **Translated Packet (Paquet traduit)** est une façon pratique qui s'offre à vous de permettre au pare-feu de créer une traduction NAT ou NPTv6 dans le sens opposé de la traduction configurée. Par défaut, la traduction **Bi-directional (Bidirectionnelle)** est désactivée.

*Si vous activez la traduction **bidirectionnelle**, vérifiez que vous avez mis en place des politiques de sécurité pour contrôler le trafic dans les deux sens. Sans ces politiques, l'option de traduction **bidirectionnelle** autorisera (sans votre accord) la traduction automatique des paquets dans les deux sens.*

NPTv6 appliqué à un service spécifique

L'implémentation de NPTv6 par Palo Alto Networks permet de filtrer les paquets afin de limiter la traduction à certains paquets. N'oubliez pas que NPTv6 ne procède pas à la traduction de port. Le concept de traduction Dynamic IP and Port (adresse IP et port dynamiques ; DIPP) n'existe pas, car NPTv6 traduit uniquement les préfixes IPv6. Cependant, vous pouvez indiquer que seuls les paquets d'un certain port de service font l'objet d'une traduction NPTv6. Ainsi, la Création d'une politique NPTv6 vous permet de spécifier un **Service** (Service) dans le paquet d'origine.

 ©2024 Palo Alto Networks, Inc.

Proxy NDP

Neighbor Discovery Protocol (protocole de découverte des voisins ; NDP) pour IPv6 effectue des fonctions semblables à celles fournies par Address Resolution Protocol (protocole de résolution d'adresse ; ARP) pour IPv4. Le document RFC 4861 définit la détection de voisins pour IPv6 (IP version 6). Les hôtes, les routeurs et les pare-feu utilisent NDP pour déterminer les adresses de couche de liaison des voisins sur les liaisons connectées, suivre les voisins accessibles et mettre à jour les adresses de couche de liaison des voisins qui ont changé. Les homologues publient leurs propres adresses MAC et IPv6 mais ils sollicitent également des adresses d'autres homologues.

NDP prend également en charge le concept de *proxy*, lorsqu'un nœud dispose d'un équipement voisin capable de transférer des paquets au nom du nœud. Le périphérique (pare-feu) joue le rôle de proxy NDP.

Les pare-feu Palo Alto Networks® prennent en charge NDP et le proxy NDP sur leurs interfaces. La configuration du pare-feu de façon à ce qu'il agisse en tant que proxy NDP pour les adresses lui permet d'envoyer des publications de détection de voisins (ND) et de répondre à des sollicitations ND des homologues qui demandent les adresses MAC ou les préfixes IPv6 affectés aux périphériques derrière le pare-feu. Vous pouvez également configurer des adresses pour lesquelles le pare-feu ne répond pas aux requêtes proxy (adresses refusées).

En fait, NDP est activé par défaut et vous devez configurer le proxy NDP lors de la configuration de NPTv6 pour les raisons suivantes :

- La nature sans état de NPTv6 nécessite un moyen d'ordonner au pare-feu de répondre aux paquets ND envoyés aux adresses de proxy NDP spécifiées et de ne pas répondre à celles refusées.

  Il est recommandé de refuser les adresses de vos voisins dans la configuration de proxy NDP, car le proxy NDP indique que le pare-feu atteint ces adresses derrière le pare-feu, mais les voisins ne se trouvent pas derrière le pare-feu.

- NDP entraîne l'enregistrement des adresses MAC et IPv6 des voisins par le pare-feu dans son cache ND (reportez-vous à la figure de la section Exemple de fonctionnement de NPTv6 et du proxy NDP.) Le pare-feu ne procède pas à la traduction NPTv6 des adresses trouvées dans son cache ND, car cela pourrait créer un conflit. Si la partie hôte d'une adresse contenue dans le cache chevauche la partie hôte de l'adresse d'un voisin et que le préfixe figurant dans le cache est traduit vers le même préfixe que celui du voisin (car l'interface de sortie sur le pare-feu appartient au même sous-réseau que celui du voisin), l'adresse traduite est exactement la même que l'adresse IPv6 légitime du voisin et un conflit se produit alors. (Si une tentative de traduction NPTv6 est effectuée sur une adresse contenue dans le cache ND, un message Syslog d'information consigne l'événement : `NPTv6 Translation Failed.`)

Lorsqu'une interface sur laquelle le proxy NDP est activé reçoit une sollicitation ND demandant une adresse MAC pour une adresse IPv6, la séquence suivante se produit :

- Le pare-feu vérifie que l'adresse IPv6 de la sollicitation ne se trouve pas dans le cache ND. Si l'adresse y figure, le pare-feu ignore la sollicitation ND.
- Si l'adresse IPv6 source est de 0, le paquet est un paquet de détection des doublons d'adresses et le pare-feu ignore alors la sollicitation ND.

 ©2024 Palo Alto Networks, Inc.

- Le pare-feu effectue une recherche de correspondance du préfixe le plus long des adresses de proxy NDP et trouve la meilleure correspondance avec l'adresse de la sollicitation. Si la case Negate (Refuser) en regard de la correspondance est cochée, le pare-feu abandonne la sollicitation ND.
- Le proxy NDP répond à la sollicitation ND uniquement si la recherche de correspondance du préfixe le plus long correspond et si l'adresse correspondante n'est pas refusée. Le pare-feu répond par un paquet ND, fournissant sa propre adresse MAC en tant qu'adresse MAC du saut suivant vers la destination interrogée.

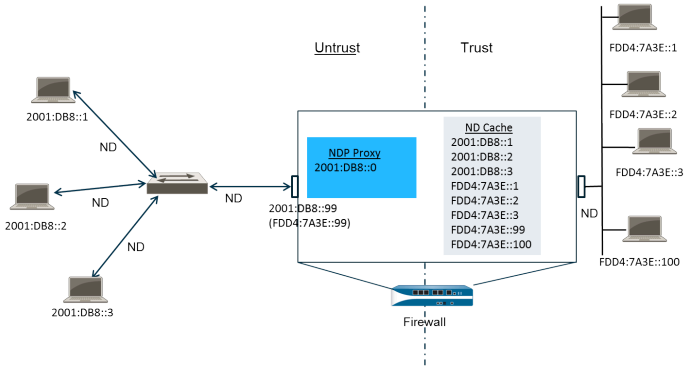
Pour une prise en charge réussie de NDP, le pare-feu ne joue pas le rôle de proxy NDP pour ce qui suit :

- La fonction Duplicate Address Detection (détection des doublons d'adresses ; DAD).
- Les adresses contenues dans le cache ND (car ces adresses n'appartiennent pas au pare-feu, mais aux voisins détectés).

 ©2024 Palo Alto Networks, Inc.

Exemple de fonctionnement de NPTv6 et du proxy NDP

La figure suivante illustrent le fonctionnement conjoint de NPTv6 et du proxy NDP.



- Exemple du cache ND dans NPTv6
- Exemple du proxy NDP dans NPTv6
- Exemple de la traduction NPTv6 dans NPTv6
- Les voisins figurant dans le cache ND ne sont pas traduits

Exemple du cache ND dans NPTv6

Dans l'exemple ci-dessus, plusieurs homologues se connectent au pare-feu via un commutateur ; la détection de voisins se produit entre les homologues et le commutateur, entre le commutateur et le pare-feu, et entre le pare-feu et les périphériques du côté approuvé.

À mesure que le pare-feu détecte les homologues, il enregistre leurs adresses dans son cache ND. Les homologues approuvés FDDA:7A3E::1, FDDA:7A3E::2 et FDDA:7A3E::3 sont connectés au pare-feu du côté approuvé. FDDA:7A3E::99 est l'adresse traduite du pare-feu ; son adresse publique est 2001:DB8::99. L'adresse des homologues du côté non approuvé ont été détectées et apparaissent dans le cache ND : 2001:DB8::1, 2001:DB8::2 et 2001:DB8::3.

Exemple du proxy NDP dans NPTv6

Dans notre scénario, nous souhaitons que le pare-feu agisse en tant que proxy NDP pour les préfixes des périphériques derrière le pare-feu. Lorsque le pare-feu joue le rôle de proxy NDP pour un ensemble donné d'adresses/de plages/de préfixes et qu'il voit une adresse de cette plage dans une sollicitation ou une publication ND, il répond tant qu'un équipement disposant de cette adresse spécifique ne répond pas en premier, l'adresse n'est pas refusée dans la configuration de proxy NDP et l'adresse ne se trouve pas dans le cache ND. Le pare-feu procède à la traduction du préfixe (décrite ci-dessous) et envoie le paquet au côté approuvé, où l'adresse peut être ou non affectée à un équipement.

Dans cet exemple, la table de proxy ND contient l'adresse réseau 2001:DB8::0. Lorsque l'interface voit une détection de voisins pour 2001:DB8::100, aucun autre équipement sur le commutateur de couche 2 ne demande le paquet ; par conséquent, la plage proxy entraîne la demande du paquet par le pare-feu et, après traduction en FDD4:7A3E::100, son envoi au coté approuvé.

©2024 Palo Alto Networks, Inc.

Exemple de la traduction NPTv6 dans NPTv6

Dans cet exemple, le paramètre **Original Packet (Paquet d'origine)** est configuré avec une **Source Address (Adresse source)** de FDD4:7A3E::0 et une **Destination (Destination)** de **Any (Indifférent)**. Le **Translated Packet (Paquet traduit)** est configuré avec une **Translated Address (Adresse traduite)** de 2001:DB8::0.

Par conséquent, les paquets sortants disposant d'une adresse source de FDD4:7A3E::0 sont traduits en 2001:DB8::0. Les paquets entrants ayant un préfixe de destination sur le réseau 2001:DB8::0 sont traduits en FDD4:7A3E::0.

Les voisins figurant dans le cache ND ne sont pas traduits

Dans notre exemple, les hôtes dont les identifiants sont :1, :2 et :3 se trouvent derrière le pare-feu. Si les préfixes de ces hôtes sont traduits vers un préfixe qui existe derrière le pare-feu et si ces périphériques disposent également des identifiants hôte :1, :2 et :3, car la partie identifiant hôte de l'adresse reste inchangée, l'adresse traduite résultante appartient au périphérique existant et un conflit d'adressage se produit alors. Afin d'éviter le chevauchement d'identifiants hôte et la création d'un conflit, NPTv6 ne traduit pas les adresses trouvées dans le cache ND.

©2024 Palo Alto Networks, Inc.

Création d'une politique NPTv6

Effectuez cette tâche lorsque vous souhaitez configurer une NPTv6 politique NAT IPv6 pour traduire un préfixe en un autre préfixe IPv6. Les prérequis pour cette tâche sont les suivants :

- Activez IPv6. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session**. Cliquez sur **Edit (Modifier)** et sélectionnez **IPv6 Firewalling (Activer le pare-feu IPv6)**.
- Configurez une interface Ethernet de Couche 3 avec une adresse IPv6 valide et sur laquelle IPv6 est activé. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)**, choisissez une interface, puis dans l'onglet **IPv6**, sélectionnez **Enable IPv6 on the interface (Activer IPv6 sur l'interface)**.
- Créez des politiques de sécurité réseau, car NPTv6 ne fournit aucune sécurité.
- Déterminez si vous souhaitez procéder à la traduction source, la traduction de destination ou les deux.
- Identifiez les zones auxquelles vous voulez appliquer la politique NPTv6.
- Identifiez vos préfixes IPv6 d'origine et traduit.

STEP 1 | Créez une nouvelle politique NPTv6.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)**, puis cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la règle de politique NPTv6.
3. (Facultatif) Saisissez une **Description (Description)** et une **Tag (Étiquette)**.
4. Pour **NAT Type (Type de NAT)**, sélectionnez **NPTv6**.

STEP 2 | Indiquez les critères de correspondance des paquets entrants ; les paquets correspondants à tous les critères font l'objet d'une traduction NPTv6.

Les zones sont requises pour les deux types de traduction.

1. Dans l'onglet **Original Packet (Paquet d'origine)**, pour **Source Zone (Zone source)**, laissez **Any (Indifférent)** ou **Add (Ajoutez)** la zone source à laquelle la politique s'applique.
2. Saisissez la **Destination Zone (Zone de destination)** à laquelle la politique s'applique.
3. (Facultatif) Sélectionnez une **Destination Interface (Interface de destination)**.
4. (Facultatif) Sélectionnez un **Service (Service)** pour limiter le type de paquets traduits.
5. Si vous procédez à la traduction source, saisissez une **Source Address (Adresse source)** ou sélectionnez **Any (Indifférent)**. L'adresse peut être un objet adresse. Les contraintes suivantes s'appliquent aux paramètres **Source Address (Adresse source)** et **Destination Address (Adresse de destination)** :
   - Les préfixes des paramètres **Source Address (Adresse source)** et **Destination Address (Adresse de destination)** du **Original Packet (Paquet d'origine)** et du **Translated Packet (Paquet traduit)** doivent être au format xxxx:xxxx::/yy, bien que les zéros non significatifs du préfixe soient abandonnés.
   - L'adresse IPv6 ne peut pas contenir une partie identifiant d'interface (hôte) définie.
   - La plage des longueurs de préfixe prises en charge est comprise entre /32 et /112.

 ©2024 Palo Alto Networks, Inc.

- Les paramètres **Source Address (Adresse source)** et **Destination Address (Adresse de destination)** ne peuvent pas être tous les deux définis sur **Any (Indifférent)**.

6. Si vous procédez à la traduction source, vous pouvez éventuellement saisir une **Destination Address (Adresse de destination)**. Si vous procédez à la traduction de destination, le paramètre **Destination Address (Adresse de destination)** doit être défini. L'adresse de destination (un objet d'adresse est autorisé) doit être un masque réseau, pas une adresse IPv6 ni une plage. La longueur du préfixe doit être une valeur comprise entre /32 et /112, inclusivement. Par exemple, 2001:db8::/32.

STEP 3 | Indiquez le paquet traduit.

1. Dans l'onglet **Translated Packet (Paquet traduit)**, si vous souhaitez procéder à la traduction source, dans la section Traduction de l'adresse source, pour **Translation Type (Type de traduction)**, sélectionnez **Static IP (Adresse IP statique)**. Si vous ne voulez pas procéder à la traduction source, sélectionnez **None (Aucune)**.
2. Si vous choisissez **Static IP (Adresse IP statique)**, le champ **Translated Address (Adresse traduite)** s'affiche. Saisissez l'objet adresse ou le préfixe IPv6 traduit. Reportez-vous aux contraintes répertoriées à l'étape précédente.

   *Il est recommandé de configurer votre **Translated Address (Adresse traduite)** en tant que préfixe de l'adresse de l'interface non approuvée de votre pare-feu. Par exemple, si votre interface non approuvée dispose d'une adresse 2001:1a:1b:1::99/64, votre **Translated Address (Adresse traduite)** est 2001:1a:1b:1::0/64.*
3. (Facultatif) Sélectionnez **Bi-directional (Bidirectionnelle)** si vous souhaitez que le pare-feu puisse créer une traduction NPTv6 correspondante dans le sens opposé de la traduction configurée.

   *Si vous activez la traduction **Bi-directional (Bidirectionnelle)**, vérifiez que vous avez mis en place des règles de politique de sécurité pour contrôler le trafic dans les deux sens. Sans ces règles de politique, la traduction **Bi-directional (Bidirectionnelle)** autorise (sans votre accord) la traduction automatique des paquets dans les deux sens.*
4. Si vous voulez procéder à la traduction de destination, sélectionnez **Destination Address Translation (Traduction de l'adresse de destination)**. Dans le champ **Translated Address (Adresse traduite)**, choisissez un objet adresse ou saisissez votre adresse de destination interne.
5. Cliquez sur **OK**.

STEP 4 | Configuration du proxy NDP.

La configuration du pare-feu de façon à ce qu'il agisse en tant que proxy NDP pour les adresses lui permet d'envoyer des publications de détection de voisins (ND) et de répondre à

 ©2024 Palo Alto Networks, Inc.

des sollicitations ND des homologues qui demandent les adresses MAC ou les préfixes IPv6 affectés aux périphériques derrière le pare-feu.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** et choisissez une interface.
2. Dans l'onglet **Advanced (Avancé)** > **NDP Proxy (Proxy NDP)**, sélectionnez **Enable NDP Proxy (Activer le proxy NDP)** et cliquez sur **Add (Ajouter)**.
3. Saisissez la/les **IP Address(es) (Adresse(s) IP)** pour laquelle/lesquelles le proxy NDP est activé. Il peut s'agir d'une adresse, d'une plage d'adresses ou d'un préfixe et d'une longueur de préfixe. L'ordre des adresses IP n'a pas d'importance. Ces adresses sont, dans l'idéal, identiques aux adresses traduites que vous avez configurées dans une politique NPTv6.

   *Si l'adresse est un sous-réseau, le proxy NDP répond à toutes les adresses du sous-réseau ; par conséquent, vous devez répertorier les voisins se trouvant sur ce sous-réseau et pour lesquels l'option **Negate (Refuser)** est sélectionnée, comme décrit à l'étape suivante.*
4. (Facultatif) Saisissez une ou plusieurs adresses pour lesquelles vous ne souhaitez pas activer le proxy NDP et sélectionnez **Negate (Refuser)**. Par exemple, vous pouvez refuser un ensemble d'adresses dans une plage de préfixes ou d'adresses IP configurée à l'étape précédente. Il est recommandé de refuser les adresses des voisins du pare-feu.

STEP 5 | Commit (Validez) la configuration.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

NAT64

NAT64 fournit un moyen de passer à IPv6 pendant que vous avez encore besoin de communiquer avec les réseaux IPv4. Lorsque vous devez communiquer à partir d'un réseau IPv6 uniquement vers un réseau IPv4, vous utilisez NAT64 pour convertir les adresses source et de destination d'IPv6 en IPv4 et vice versa. Le NAT64 permet aux clients IPv6 d'accéder aux serveurs IPv4 et aux clients IPv4 d'accéder aux serveurs IPv6. Vous devez comprendre le NATavant de configurer le NAT64.

- Aperçu de NAT64
- Adresse IPv6 intégrée à IPv4
- Serveur DNS64
- Découverte de Chemin MTU
- Communications initiées par IPv6
- Configurer NAT64 pour la communication initiée par IPv6
- Configurer NAT64 pour la communication initiée par IPv4
- Configurer NAT64 pour la communication initiée par IPv4 avec la traduction de port

Aperçu de NAT64

Vous pouvez configurer deux types de traduction NAT64 sur un pare-feu Palo Alto Networks® ; chacune effectue une traduction bidirectionnelle entre les deux familles d'adresses IP :

- Le pare-feu prend en charge NAT64 pour Communications initiées par IPv6, qui mappe plusieurs adresses IPv6 sur une adresse IPv4, préservant ainsi les adresses IPv4. (Il ne prend pas en charge NAT64 sans état, qui mappe une adresse IPv6 à une adresse IPv4 et ne conserve donc pas les adresses IPv4.) Configurer NAT64 pour la communication initiée par IPv6.
- Le pare-feu prend en charge la communication initiée par IPv4 avec une liaison statique qui mappe une adresse IPv4 et un numéro de port à une adresse IPv6. Configurer NAT64 pour la communication initiée par IPv4. Il prend également en charge la réécriture de port, qui préserve encore plus d'adresses IPv4 en traduisant une adresse IPv4 et un numéro de port en adresse IPv6 avec plusieurs numéros de port. Configurer NAT64 pour la communication initiée par IPv4 avec la traduction de port.

Une seule adresse IPv4 peut être utilisée pour NAT44 et NAT64 ; vous ne réservez pas un pool d'adresses IPv4 pour NAT64 uniquement.

NAT64 fonctionne sur les interfaces de couche 3, les sous-interfaces et les interfaces de tunnel. Pour utiliser NAT64 sur un pare-feu Palo Alto Networks pour une communication initiée par IPv6, vous devez avoir un tiers Serveur DNS64 ou une solution en place pour séparer la fonction de requête DNS de la fonction NAT. Le serveur DNS64 se traduit entre votre hôte IPv6 et un serveur DNS IPv4 en codant l'adresse IPv4 qu'il reçoit d'un serveur DNS public dans une adresse IPv6 pour l'hôte IPv6.

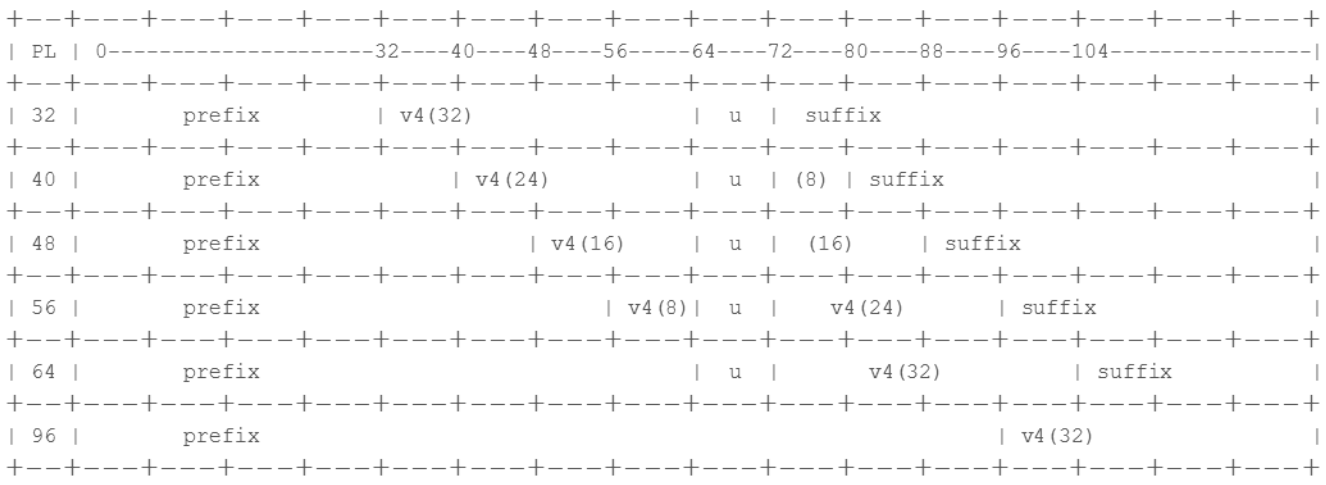
Palo Alto Networks prend en charge les fonctionnalités NAT64 suivantes :

- NAT persistant pour DIPP
- Hairpinning (NAT U-Turn) (Épingle à cheveux (demi-tour sur le NAT)) ; En outre, NAT64 empêche les attaques par boucle en épingle à cheveux en supprimant tous les paquets IPv6 entrants qui ont un préfixe source de 64::/n.
- La traduction des paquets TCP / UDP / ICMP selon la RFC 6146 et le pare-feu fait de son mieux pour traduire d'autres protocoles qui n'utilisent pas une passerelle au niveau de l'application (ALG). Par exemple, le pare-feu peut traduire un paquet GRE. Cette traduction a la même limitation que le NAT44: si vous n'avez pas d'ALG pour un protocole qui peut utiliser un canal de contrôle et de données séparé, le pare-feu peut ne pas comprendre le flux de trafic de retour.
- La traduction entre IPv4 et IPv6 de l'attribut de longueur ICMP du champ de datagramme d'origine, par RFC 4884.

 ©2024 Palo Alto Networks, Inc.

Adresse IPv6 intégrée à IPv4

NAT64 utilise une adresse IPv6 intégrée à IPv4, comme décrit dans la norme RFC 6052, à la section IPv6 Addressing of IPv4/IPv6 Translators (Adressage IPv6 des traducteurs IPv4/IPv6). Une adresse IPv6 intégrée à IPv4 est une adresse IPv6 dans laquelle 32 octets ont une adresse IPv4 encodée. La longueur de préfixe IPv6 (PL dans la figure) détermine où l'adresse IPv4 est encodée dans l'adresse IPv6, comme suit :



Le pare-feu prend en charge la traduction des sous-réseaux /32, /40, /48, /56, /64 et /96 qui utilisent ces préfixes. Un pare-feu unique prend en charge plusieurs préfixes : chaque règle NAT64 utilise un préfixe. Il peut s'agir d'un préfixe bien connu (64:FF9B::/96) ou d'un Network-Specific Prefix (préfixe spécifique au réseau ; NSP) qui est unique à l'organisation qui contrôle le traducteur d'adresse (le périphérique DNS64). Un NSP est généralement un réseau au sein du préfixe IPv6 de l'organisation. Le périphérique DNS54 définit généralement le suffixe et le champ u sur zéro ; le pare-feu ignore ces champs.

 ©2024 Palo Alto Networks, Inc.

Serveur DNS64

Si vous devez utiliser un DNS et que vous souhaitez effectuer une traduction NAT64 à l'aide de la Communication initiée par IPv6, vous devez utiliser un serveur DNS64 tiers ou une autre solution DNS64 pour laquelle le préfixe bien connu ou votre NSP est défini. Lorsqu'un hôte IPv6 tente d'accéder à un domaine ou un hôte IPv4 sur l'Internet, le serveur DNS64 interroge un serveur DNS faisant autorité pour obtenir l'adresse IPv4 qui est mappée à ce nom d'hôte. Le serveur DNS envoie au serveur DNS64 un enregistrement d'adresse A (enregistrement A) qui contient l'adresse IPv4 et le nom d'hôte.

À son tour, le serveur DNS64 convertit l'adresse IPv4 en une valeur hexadécimale et l'encode sur les octets appropriés de votre préfixe IPv6 qu'il doit utiliser (préfixe bien connu ou votre NSP) selon la longueur du préfixe, ce qui donne une Adresse IPv6 intégrée à IPv4. Le serveur DNS64 envoie un enregistrement AAAA à l'hôte IPv6 qui mappe l'adresse IPv6 avec adresse IPv4 intégrée au nom d'hôte IPv4.

 ©2024 Palo Alto Networks, Inc.

Découverte de Chemin MTU

IPv6 ne fragmente pas les paquets, donc le pare-feu utilise deux méthodes pour réduire le besoin de fragmenter les paquets :

- Lorsque le pare-feu traduit des paquets IPv4 dans lesquels l'octet Do Not Fragment (ne pas fragmenter ; DF) est défini sur zéro, c'est que l'expéditeur s'attend à ce que le pare-feu fragmente les paquets qui sont trop volumineux, mais que le pare-feu ne fragmente pas les paquets pour le réseau IPv6 (après la traduction), car IPv6 ne fragmente pas les paquets. Vous pouvez plutôt configurer la taille minimale de la fragmentation des paquets IPv4 avant leur traduction. La valeur **NAT64 IPv6 Minimum Network MTU (MTU IPv6 min. pour le réseau NAT64)** correspond à ce paramètre, qui respecte la norme RFC 6145, l'algorithme de traduction IP/ICMP. Vous pouvez définir le **NAT64 IPv6 Minimum Network MTU (MTU IPv6 min. pour le réseau NAT64)** sur sa valeur maximale (**Device (Périphérique)** > **Setup (Configuration)** > **Session**), qui pousse le pare-feu à fragmenter les paquets IPv4 en leur taille IPv6 minimale avant de les traduire en IPv6. (Le **NAT64 IPv6 Minimum Network MTU (MTU IPv6 min. pour le réseau NAT64)** ne change pas le MTU de l'interface.)
- L'autre méthode que le pare-feu utilise pour réduire la fragmentation est la Path MTU Discovery (Découverte de Chemin MTU ; PMTUD). Dans une communication initiée par IPv4, si l'octet DF du paquet IPv4 devant être traduit est défini et que le MTU de l'interface de sortie est plus petit que le paquet, le pare-feu utilise la PMTUD pour abandonner le paquet et renvoie à la source un message ICMP indiquant que la destination n'a pu être atteinte et que la fragmentation est obligatoire (Destination Unreachable - fragmentation needed). La source réduit le MTU du chemin de cette destination et renvoie le paquet jusqu'à ce que les réductions successives du MTU du chemin permettent au paquet d'être livré.

©2024 Palo Alto Networks, Inc.

Communications initiées par IPv6

La communication initiée par IPv6 vers le pare-feu est similaire à NAT source pour une topologie IPv4. Configurez NAT64 pour la communication initiée par IPv6 lorsque votre hôte IPv6 doit communiquer avec un serveur IPv4.

Dans la règle de stratégie NAT64, configurez la source d'origine pour qu'elle soit une adresse hôte IPv6 ou Any. Configurez l'adresse IPv6 de destination en tant que préfixe connu ou NSP utilisé par le serveur DNS64. (Vous ne configurez pas l'adresse de destination IPv6 complète dans la règle.)

Si vous devez utiliser un DNS, vous devez utiliser un serveur DNS64 pour convertir un résultat "A" DNS IPv4 en un résultat "AAAA" fusionné avec le préfixe NAT64. Si vous n'utilisez pas de DNS, vous devez créer l'adresse en utilisant l'adresse de destination IPv4 et le préfixe NAT64 configuré sur le pare-feu, conformément aux règles RFC 6052.

Pour les environnements qui utilisent un DNS, l'exemple de topologie ci-dessous illustre la communication avec le serveur DNS64. Le serveur DNS64 doit être configuré pour utiliser le préfixe bien connu 64:FF9B::/96 ou votre préfixe spécifique au réseau, qui doit être conforme à RFC 6052 (/32, /40, /48, /56, /64 ou /96).

Sur le côté traduit du pare-feu, le type de traduction doit être IP dynamique et port afin d'implémenter NAT64 avec état. Vous configurez l'adresse traduite source comme l'adresse IPv4 de l'interface de sortie sur le pare-feu. Vous ne configurez pas le champ de traduction de destination; le pare-feu traduit l'adresse en trouvant d'abord la longueur du préfixe dans l'adresse de destination d'origine de la règle, puis en fonction du préfixe, en extrayant l'adresse IPv4 codée de l'adresse IPv6 de destination d'origine dans le paquet entrant.

Avant que le pare-feu n'examine la règle NAT64, le pare-feu doit effectuer une recherche d'itinéraire pour trouver la zone de sécurité de destination pour un paquet entrant. Vous devez vous assurer que le préfixe NAT64 peut être atteint via l'affectation de la zone de destination, car le préfixe NAT64 ne doit pas être routable par le pare-feu. Le pare-feu affectera probablement le préfixe NAT64 à la route par défaut ou supprimera le préfixe NAT64 car il n'y a pas de route pour cela. Le pare-feu ne trouvera pas de zone de destination car le préfixe NAT64 ne figure pas dans sa table de routage, associée à une interface et une zone de sortie.

Vous devez également configurer une interface de tunnel (sans point de terminaison). Appliquez le préfixe NAT64 au tunnel ainsi que la zone adéquate pour garantir que le trafic IPv6 avec préfixe NAT64 est affecté à la bonne zone de destination.. Le tunnel présente également l'avantage de supprimer le trafic IPv6 avec le préfixe NAT64 si le trafic ne correspond pas à la règle NAT64. Votre protocole de routage configuré sur le pare-feu recherche le préfixe IPv6 dans sa table de routage pour rechercher la zone de destination, puis examine la règle NAT64.

La figure suivante illustre le rôle du serveur DNS64 dans le processus de résolution de noms. Dans cet exemple, le serveur DNS64 est configuré pour utiliser le préfixe bien connu 64: FF9B :: / 96.

1. Un utilisateur de l'hôte IPv6 entre l'URL www.abc.com, qui génère une recherche de serveur de noms (nslookup) sur le serveur DNS64.

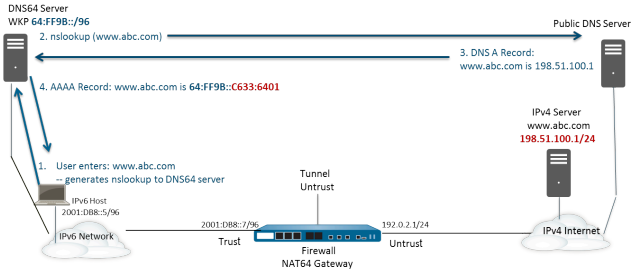
2. Le serveur DNS64 envoie un nslookup au serveur DNS publique pour www.abc.com, en demandant son adresse IPv4.

3. Le serveur DNS renvoie un enregistrement A qui fournit l'adresse IPv4 au serveur DNS64.

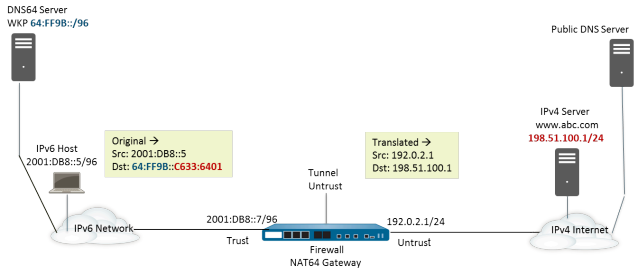
 ©2024 Palo Alto Networks, Inc.

4. Le serveur DNS64 envoie un enregistrement AAAA à l'utilisateur IPv6, convertissant l'adresse décimale à points IPv4 198.51.100.1 en hexadécimal C633: 6401 et l'intégrant dans son propre préfixe IPv6, 64: FF9B :: / 96. [198 = C6 hex; 51 = 33 hex; 100 = 64 hex; 1 = 01 hex.] Le résultat est l'adresse IPv6 IPv4-Embedded 64: FF9B :: C633: 6401.

Gardez à l'esprit que dans un préfixe / 96, l'adresse IPv4 est les quatre derniers octets codés dans l'adresse IPv6. Si le serveur DNS64 utilise un préfixe / 32, / 40, / 48, / 56 ou / 64, l'adresse IPv4 est codée comme indiqué dans la RFC 6052.



Lors de la résolution de nom transparente, l'hôte IPv6 envoie un paquet au pare-feu contenant son adresse source IPv6 et son adresse IPv6 de destination 64:FF9B::C633:6401 comme déterminé par le serveur DNS64. Le pare-feu exécute la traduction NAT64 en fonction de votre règle NAT64.



 ©2024 Palo Alto Networks, Inc.

Configurer NAT64 pour la communication initiée par IPv6

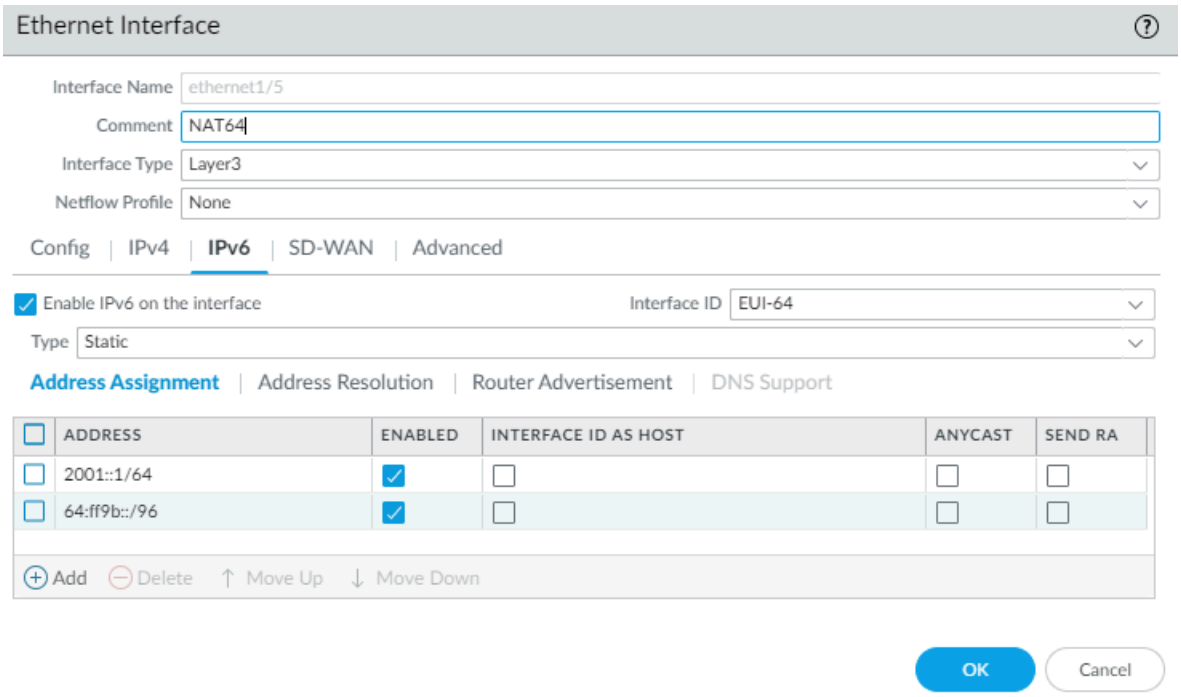
La tâche de configuration et ses adresses correspondent aux figures présentées à la section Communications initiées par IPv6.

STEP 1 | Autorisez IPv6 à fonctionner sur le pare-feu.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les Session Settings (Paramètres de session).
2. Sélectionnez **Enable IPv6 Firewalling (Activer le pare-feu IPv6)**.
3. Cliquez sur **OK**.

STEP 2 | Configurez l'interface avec l'adressage IPv6.

1. Sélectionnez **Network (Réseau)** > **Interfaces** et sélectionnez l'interface qui effectue le NAT.
2. Sélectionnez l'onglet **IPv6**.
3. Sélectionnez **Enable IPv6 address on interface (Activer l'adresse IPv6 sur l'interface)**.
4. **Add (Ajoutez)** votre préfixe IPv6 privé.
5. **Add (Ajoutez)** le préfixe bien connu 64:ff9b::/96.
6. Cliquez sur **OK**.



©2024 Palo Alto Networks, Inc.

STEP 3 | Créez un objet d'adresse pour l'adresse IPv6 de destination (prétraduction).

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)**, puis cliquez sur **Add (Ajouter)**.
2. Donnez un **Name (Nom)** à l'objet, par exemple, nat64-IPv4 Server.
3. Sous **Type (Type)**, sélectionnez **IP Netmask (Masque réseau IP)**, puis saisissez le préfixe IPv6 avec un masque réseau qui est conforme à RFC 6052 (/32, /40, /48, /56, /64 ou /96). Il s'agit du préfixe bien connu ou du préfixe propre à votre réseau, lequel a été configuré sur le serveur DNS64.

   Dans cet exemple, indiquez 64:FF9B::/96.

   La source et la destination doivent avoir le même masque réseau (longueur de préfixe).

   (Vous ne devez pas entrer d'adresse de destination complète, parce que, selon la longueur du préfixe, le pare-feu extrait l'adresse IPv4 encodée de l'adresse IPv6 de destination initiale dans le paquet entrant. Dans cet exemple, le préfixe du paquet entrant est encodé au format hexadécimal (C633:6401), ce qui correspond à l'adresse IPv4 de destination 198.51.100.1.)
4. Cliquez sur **OK**.

STEP 4 | (Facultatif) Créez un objet d'adresse pour l'adresse IPv6 source (prétraduction).

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** pour l'objet.
3. Sous **Type (Type)**, sélectionnez **IP Netmask (Masque réseau IP)**, puis entrez l'adresse de l'hôte IPv6, dans cet exemple : 2001:DB8::5/96.
4. Cliquez sur **OK**.

STEP 5 | (Facultatif) Créez un objet d'adresse pour l'adresse IPv4 source (traduite).

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** pour l'objet.
3. Sous **Type (Type)**, sélectionnez **IP Netmask (Masque réseau IP)**, puis entrez l'adresse IPv4 de l'interface de sortie du pare-feu, dans cet exemple : 192.0.2.1.
4. Cliquez sur **OK**.

STEP 6 | Créez la règle NAT64.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)**, puis cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, entrez un **Name (Nom)** pour la règle NAT64, par exemple, nat64_ipv6_init.
3. (Facultatif) Saisissez une **Description (Description)**.
4. Pour **NAT Type (Type de NAT)**, sélectionnez **nat64**.

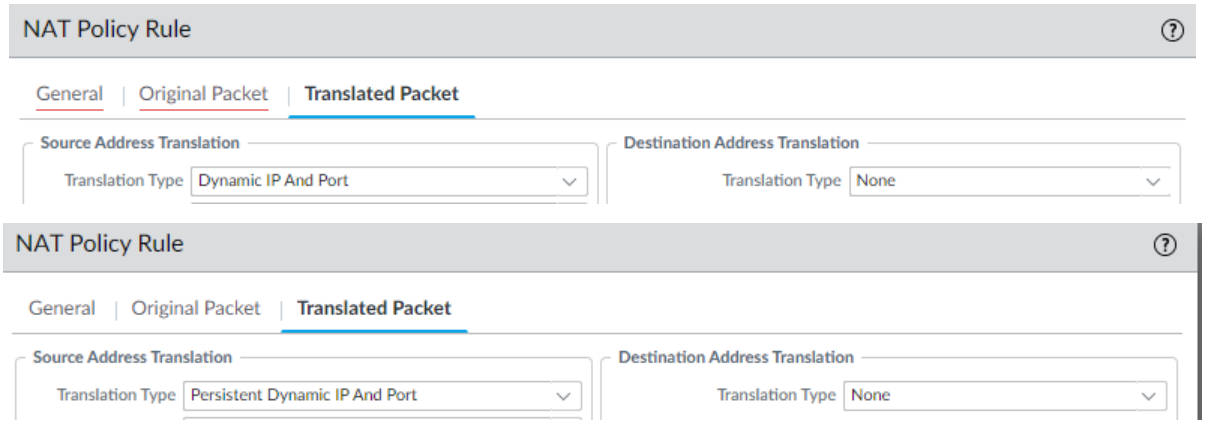
 ©2024 Palo Alto Networks, Inc.

STEP 7 | Indiquez les renseignements relatifs à la source et à la destination d'origine.

1. Sous **Original Packet (Paquet d'origine)**, **Add (Ajoutez)** la **Source Zone (Zone source)**, probablement une zone approuvée.
2. Sélectionnez la **Destination Zone (Zone de destination)**, dans cet exemple : la zone non approuvée.
3. (Facultatif) Sélectionnez une **Destination Interface (Interface de destination)** ou la valeur par défaut (**any (indifférent)**).
4. Sous **Source Address (Adresse source)**, sélectionnez **Any (Toute)** ou **Add (Ajoutez)** l'objet d'adresse que vous avez créé pour l'hôte IPv6.
5. Sous **Destination Address (Adresse de destination)**, **Add (Ajoutez)** l'objet d'adresse que vous avez créé pour l'adresse IPv6 de destination, dans le cas présent, nat64-IPv4 Server.
6. (Facultatif) Sous **Service (Service)**, sélectionnez **any (indifférent)**.

STEP 8 | Indiquez les renseignements relatifs au paquet traduit.

1. Pour le **Translated Packet (Paquet traduit)**, dans **Source Address Translation (Traduction de l'adresse source)**, pour DIPP standard, pour **Translation Type (Type de traduction)**, sélectionnez **Dynamic IP et Port (Adresse IP et port dynamiques)**. Pour un DIPP persistant dans PAN-OS 11.0 et les versions antérieures, sélectionnez **Dynamic IP and Port (Adresse IP et port dynamiques)**. Pour un DIPP persistant dans les versions postérieures à PAN-OS 11.0, sélectionnez **Persistent Dynamic IP and Port (Adresse IP et port dynamiques persistants)**.



2. Sous **Address Type (Type d'adresse)**, effectuez l'une des actions suivantes :
   - Sélectionnez **Translated Address (Adresse traduite)** et **Add (Ajoutez)** l'objet d'adresse que vous avez créé pour l'adresse IPv4 source.
   - Sélectionnez **Interface Address (Adresse de l'interface)**, auquel cas l'adresse source traduite et l'adresse IP et le masque réseau de l'interface de sortie du pare-feu. Pour ce choix, sélectionnez une **Interface (Interface)** et éventuellement une **IP Address (Adresse IP)** si l'interface dispose de plusieurs adresses IP.
3. Ne cochez pas **Destination Address Translation (Traduction de l'adresse de destination)**. (Le pare-feu extrait l'adresse IPv4 du préfixe IPv6 qui figure dans le paquet entrant, selon la longueur de préfixe indiquée dans la destination d'origine de la règle NAT64.)
4. Cliquez sur **OK (OK)** pour enregistrer la règle de politique NAT64.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Configurez une interface de tunnel pour émuler une interface avec retour de boucle dont le masque réseau est autre que 128.

1. Sélectionnez **Network (Réseau)** > **Interface** > **Tunnel** et **Add (Ajoutez)** un tunnel.
2. Sous **Interface Name (Nom de l'interface)**, saisissez un suffixe numérique, tel que .2.
3. À l'onglet **Config (Configuration)**, sélectionnez le **Virtual Router (Routeur virtuel)** sur lequel vous configurez NAT64.
4. Pour **Security Zone (Zone de sécurité)**, sélectionnez la zone de destination associée à la destination du serveur IPv4 (zone non approuvée).
5. À l'onglet **IPv6 (IPv6)**, sélectionnez **Enable IPv6 on the interface (Activer IPv6 sur l'interface)**.
6. Cliquez sur **Add (Ajouter)** et, sous **Address (Adresse)**, sélectionnez **New Address (Nouvelle adresse)**.
7. Donnez un **Name (Nom)** à l'adresse.
8. (Facultatif) Saisissez une **Description (Description)** de l'adresse du tunnel.
9. Sous **Type (Type)**, sélectionnez **IP Netmask (Masque réseau IP)**, puis entrez votre préfixe IPv6 ainsi que la longueur de préfixe ; dans cet exemple : 64:FF9B::/96.
10. Cliquez sur **OK**.
11. Sélectionnez **Enable address on interface (Activer l'adresse sur l'interface)**, puis cliquez sur **OK (OK)**.
12. Cliquez sur **OK**.
13. Cliquez sur **OK (OK)** pour enregistrer le tunnel.

STEP 10 | Créez une politique de sécurité pour autoriser le trafic NAT en provenance de la zone approuvée.

1. Sélectionnez **Policies (Stratégies)** > **Security (Securité)**, puis **Add (Ajoutez)** un **Name (Nom)** de règle.
2. Sélectionnez **Source (Source)** et **Add (Ajoutez)** une **Source Zone (Zone source)** ; sélectionnez **Trust (Approuvée)**.
3. Sous **Source Address (Adresse source)**, sélectionnez **Any (Indifférent)**.
4. Sélectionnez **Destination (Destination)** et **Add (Ajoutez)** une **Destination Zone (Zone de destination)** ; sélectionnez **Untrust (Non approuvée)**.
5. Sous **Application (Application)**, sélectionnez **any (indifférent)**.
6. Sous **Actions (Actions)**, sélectionnez **Allow (Autoriser)**.
7. Cliquez sur **OK**.

STEP 11 | Validez vos modifications.

Cliquez sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

STEP 12 | (Pour activer le DIPP persistant dans PAN-OS 11.1.0 et les versions antérieures uniquement) Activez le NAT persistant pour DIPP.

1. Accédez à la CLI.
2. **>set system setting persistent-dipp enable yes**
3. **>request restart system**
4. Si vous avez configuré la haute disponibilité, répétez cette étape sur l'autre homologue HA.

STEP 13 | Dépannez ou affichez une session NAT64.

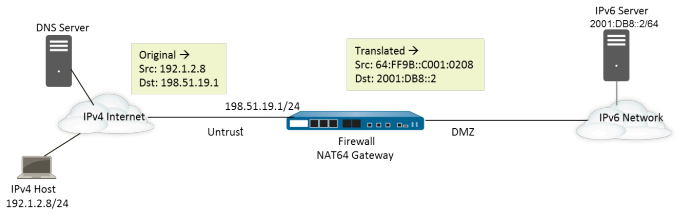
```
> afficher l'ID de session<session-id>
```

 ©2024 Palo Alto Networks, Inc.

Configurer NAT64 pour la communication initiée par IPv4

La traduction des communications initiées par IPv4 vers un serveur IPv6 est semblable à la traduction NAT de destination dans une topologie IPv4. L'adresse IPv4 de destination effectue un mappage vers l'adresse IPv6 de destination via une traduction 1 à 1 d'une adresse IP statique (pas une traduction plusieurs à un).

Le pare-feu encode l'adresse IPv4 source en un préfixe bien connu 64:FF9B::/96 conformément au protocole RFC 6052. L'adresse de destination traduite est l'adresse IPv6. Une communication initiée par IPv4 s'avère généralement utile lorsqu'une organisation fournit un accès depuis la zone publique non approuvée vers un serveur IPv6 qui se trouve dans la zone DMZ de l'organisation. Cette topologie n'a pas recours à un serveur DNS64.



STEP 1 | Autorisez IPv6 à fonctionner sur le pare-feu.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les Session Settings (Paramètres de session).
2. Sélectionnez **Enable IPv6 Firewalling (Activer le pare-feu IPv6)**.
3. Cliquez sur **OK**.

STEP 2 | (Facultatif) Lorsque l'octet DF d'un paquet IPv4 est défini sur zéro (et parce que IPv6 ne fragmente pas les paquets), veillez à ce que le paquet IPv6 traduit n'excède pas la valeur du chemin MTU du réseau IPv6 de destination.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les Session Settings (Paramètres de session).
2. Sous **NAT64 IPv6 Minimum Network MTU (MTU IPv6 min. pour le réseau NAT64)**, saisissez le plus petit nombre d'octets pour la fragmentation, par le pare-feu, des paquets IPv4 devant être traduits en IPv6 (plage comprise entre 1 280 et 9 216, valeur par défaut : 1280).

   Si vous ne voulez pas que le pare-feu fragmente un paquet IPv4 avant la traduction, définissez la valeur MTU à 9216. Si le paquet IPv6 traduit dépasse toujours cette valeur, le pare-feu abandonne le paquet et émet un paquet ICMP pour indiquer que la destination n'a pu être atteinte et que la fragmentation est obligatoire.
3. Cliquez sur **OK**.

©2024 Palo Alto Networks, Inc.

STEP 3 | Créez un objet d'adresse pour l'adresse IPv4 de destination (prétraduction).

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)**, puis cliquez sur **Add (Ajouter)**.
2. Donnez un **Name (Nom)** à l'objet, par exemple, nat64_ip4server.
3. Sous **Type (Type)**, sélectionnez **IP Netmask (Masque réseau IP)** et saisissez l'adresse IPv4 de l'interface du pare-feu se trouvant dans la zone non approuvée. L'adresse ne doit utiliser aucun masque réseau. Autrement, elle peut utiliser un masque réseau /32 uniquement. Cet exemple utilise l'adresse 198.51.19.1/32.
4. Cliquez sur **OK**.

STEP 4 | Créez un objet d'adresse pour l'adresse IPv6 source (traduite).

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)**, puis cliquez sur **Add (Ajouter)**.
2. Donnez un **Name (Nom)** à l'objet, par exemple, nat64_ip6source.
3. Sous **Type (Type)**, sélectionnez **IP Netmask (Masque réseau IP)**, puis saisissez l'adresse IPv6 NAT64 avec un masque réseau qui est conforme à RFC 6052 (/32, /40, /48, /56, /64 ou /96).

   Dans cet exemple, indiquez 64:FF9B::/96.

   (Le pare-feu encode le préfixe avec l'adresse IPv4 source 192.1.2.8, soit C001:0208 au format hexadécimal.)
4. Cliquez sur **OK**.

STEP 5 | Créez un objet d'adresse pour l'adresse IPv6 de destination (traduite).

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)**, puis cliquez sur **Add (Ajouter)**.
2. Donnez un **Name (Nom)** à l'objet, par exemple, nat64_server_2.
3. Sous **Type (Type)**, sélectionnez **IP Netmask (Masque réseau IP)**, puis saisissez l'adresse IPv6 du serveur IPv6 (de destination). L'adresse ne doit utiliser aucun masque réseau. Autrement, elle peut utiliser un masque réseau /128 uniquement. Cet exemple utilise l'adresse 2001:DB8::2/128.
4. Cliquez sur **OK**.

STEP 6 | Créez la règle NAT64.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)**, puis cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, entrez un **Name (Nom)** pour la règle NAT64, par exemple, nat64_ipv4_init.
3. Pour **NAT Type (Type de NAT)**, sélectionnez **nat64**.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Indiquez les renseignements relatifs à la source et à la destination d'origine.

1. Sous **Original Packet (Paquet d'origine)**, **Add (Ajoutez)** la **Source Zone (Zone source)**, probablement une zone non approuvée.
2. Sélectionnez la **Destination Zone (Zone de destination)**, probablement une zone DMZ ou approuvée.
3. Sous **Source Address (Adresse source)**, sélectionnez **Any (Toute)** ou **Add (Ajoutez)** l'objet d'adresse de l'hôte IPv4.
4. Sous **Destination Address (Adresse de destination)**, **Add (Ajoutez)** l'objet d'adresse de la destination IPv4, dans le cas présent, nat64_ip4server.
5. Sous **Service (Service)**, sélectionnez **any (indifférent)**.

STEP 8 | Indiquez les renseignements relatifs au paquet traduit.

1. Sous **Translated Packet (Paquet traduit)**, **Source Address Translation (Traduction de l'adresse source)**, **Translation Type (Type de traduction)**, sélectionnez **Static IP (IP statique)**.
2. Sous **Translated Address (Adresse traduite)**, sélectionnez l'objet d'adresse source traduit que vous avez créez, soit nat64_ip6source.
3. Sous **Destination Address Translation (Traduction de l'adresse de destination)**, pour **Translated Address (Adresse traduite)**, indiquez une seule adresse IPv6 (l'objet d'adresse, soit, dans cet exemple, nat64_server_2, ou l'adresse IPv6 du serveur).
4. Cliquez sur **OK**.

STEP 9 | Créez une politique de sécurité pour autoriser le trafic NAT en provenance de la zone non approuvée.

1. Sélectionnez **Policies (Stratégies)** > **Security (Securité)**, puis **Add (Ajoutez)** un **Name (Nom)** de règle.
2. Sélectionnez **Source (Source)** et **Add (Ajoutez)** une **Source Zone (Zone source)** ; sélectionnez **Untrust (Non approuvée)**.
3. Sous **Source Address (Adresse source)**, sélectionnez **Any (Indifférent)**.
4. Sélectionnez **Destination (Destination)** et **Add (Ajoutez)** une **Destination Zone (Zone de destination)** ; sélectionnez **DMZ (DMZ)**.
5. Sous **Actions (Actions)**, sélectionnez **Allow (Autoriser)**.
6. Cliquez sur **OK**.

STEP 10 | Validez vos modifications.

Cliquez sur **Commit (Valider)**.

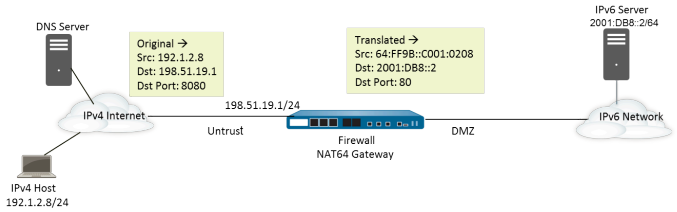
STEP 11 | Dépannez ou affichez une session NAT64.

```
> afficher l'ID de session<session-id>
```

 ©2024 Palo Alto Networks, Inc.

Configurer NAT64 pour la communication initiée par IPv4 avec la traduction de port

Cette tâche découle de la tâche liée à la configuration de NAT64 pour les communications initiées par IPv4, mais l'organisation qui contrôle le réseau IPv6 préfère traduire le numéro de port de destination public en un numéro de port de destination interne afin qu'il soit privé et que les utilisateurs qui se trouvent du côté IPv4 non approuvé du pare-feu ne puissent pas le voir. Dans cet exemple, le port 8080 est traduit en port 80. Pour ce faire, dans le paquet d'origine de la règle de politique NAT64, créez un nouveau service qui précise que le port de destination est 8080. Le port du paquet traduit est 80.



STEP 1 | Autorisez IPv6 à fonctionner sur le pare-feu.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les Session Settings (Paramètres de session).
2. Sélectionnez **Enable IPv6 Firewalling (Activer le pare-feu IPv6)**.
3. Cliquez sur **OK**.

STEP 2 | (Facultatif) Lorsque l'octet DF d'un paquet IPv4 est défini sur zéro (et parce que IPv6 ne fragmente pas les paquets), veillez à ce que le paquet IPv6 traduit n'excède pas la valeur du chemin MTU du réseau IPv6 de destination.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les Session Settings (Paramètres de session).
2. Sous **NAT64 IPv6 Minimum Network MTU (MTU IPv6 min. pour le réseau NAT64)**, saisissez le plus petit nombre d'octets pour la fragmentation, par le pare-feu, des paquets IPv4 devant être traduits en IPv6 (plage comprise entre 1 280 et 9 216, valeur par défaut : 1280).

   Si vous ne voulez pas que le pare-feu fragmente un paquet IPv4 avant la traduction, définissez la valeur MTU à 9216. Si le paquet IPv6 traduit dépasse toujours cette valeur, le pare-feu abandonne le paquet et émet un paquet ICMP pour indiquer que la destination n'a pu être atteinte et que la fragmentation est obligatoire.
3. Cliquez sur **OK**.

©2024 Palo Alto Networks, Inc.

STEP 3 | Créez un objet d'adresse pour l'adresse IPv4 de destination (prétraduction).

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)**, puis cliquez sur **Add (Ajouter)**.
2. Donnez un **Name (Nom)** à l'objet, par exemple, nat64_ip4server.
3. Sous **Type (Type)**, sélectionnez **IP Netmask (Masque réseau IP)** et saisissez l'adresse IPv4 et le masque réseau de l'interface du pare-feu se trouvant dans la zone non approuvée. Cet exemple utilise l'adresse 198.51.19.1/24.
4. Cliquez sur **OK**.

STEP 4 | Créez un objet d'adresse pour l'adresse IPv6 source (traduite).

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)**, puis cliquez sur **Add (Ajouter)**.
2. Donnez un **Name (Nom)** à l'objet, par exemple, nat64_ip6source.
3. Sous **Type (Type)**, sélectionnez **IP Netmask (Masque réseau IP)**, puis saisissez l'adresse IPv6 NAT64 avec un masque réseau qui est conforme à RFC 6052 (/32, /40, /48, /56, /64 ou /96).

   Dans cet exemple, indiquez 64:FF9B::/96.

   (Le pare-feu encode le préfixe avec l'adresse IPv4 source 192.1.2.8, soit C001:0208 au format hexadécimal.)
4. Cliquez sur **OK**.

STEP 5 | Créez un objet d'adresse pour l'adresse IPv6 de destination (traduite).

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)**, puis cliquez sur **Add (Ajouter)**.
2. Donnez un **Name (Nom)** à l'objet, par exemple, nat64_server_2.
3. Sous **Type (Type)**, sélectionnez **IP Netmask (Masque réseau IP)**, puis saisissez l'adresse IPv6 du serveur IPv6 (de destination). Cet exemple utilise l'adresse 2001:DB8::2/64.

   La source et la destination doivent avoir le même masque réseau (longueur de préfixe).
4. Cliquez sur **OK**.

STEP 6 | Créez la règle NAT64.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)**, puis cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, entrez un **Name (Nom)** pour la règle NAT64, par exemple, nat64_ipv4_init.
3. Pour **NAT Type (Type de NAT)**, sélectionnez **nat64**.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Indiquez les informations source et de destination d'origine et créez un service pour limiter la traduction à un seul numéro de port d'entrée.

1. Sous **Original Packet (Paquet d'origine)**, **Add (Ajoutez)** la **Source Zone (Zone source)**, probablement une zone non approuvée.
2. Sélectionnez la **Destination Zone (Zone de destination)**, probablement une zone DMZ ou approuvée.
3. Sous **Service (Service)**, sélectionnez nouveau **Service (Service)**.
4. Saisissez un **Name (Nom)** pour le service, tel que Port_8080.
5. Sélectionnez **TCP (TCP)** en tant que **Protocol (Protocole)**.
6. Sous **Destination Port (Port de destination)**, saisissez 8080.
7. Cliquez sur **OK (OK)** pour enregistrer le service.
8. Sous **Source Address (Adresse source)**, sélectionnez **Any (Toute)** ou **Add (Ajoutez)** l'objet d'adresse de l'hôte IPv4.
9. Sous **Destination Address (Adresse de destination)**, **Add (Ajoutez)** l'objet d'adresse de la destination IPv4, dans le cas présent, nat64_ip4server.

STEP 8 | Indiquez les renseignements relatifs au paquet traduit.

1. Sous **Translated Packet (Paquet traduit)**, **Source Address Translation (Traduction de l'adresse source)**, **Translation Type (Type de traduction)**, sélectionnez **Static IP (IP statique)**.
2. Sous **Translated Address (Adresse traduite)**, sélectionnez l'objet d'adresse source traduit que vous avez créez, soit nat64_ip6source.
3. Sous **Destination Address Translation (Traduction de l'adresse de destination)**, pour **Translated Address (Adresse traduite)**, indiquez une seule adresse IPv6 (l'objet d'adresse, soit, dans cet exemple, nat64_server_2, ou l'adresse IPv6 du serveur).
4. Indiquez le numéro de **Translated Port (Port traduit)** de destination privé auquel le pare-feu traduit le numéro de port de destination public ; soit, dans cet exemple, 80.
5. Cliquez sur **OK**.

STEP 9 | Créez une politique de sécurité pour autoriser le trafic NAT en provenance de la zone non approuvée.

1. Sélectionnez **Policies (Stratégies)** > **Security (Securité)**, puis **Add (Ajoutez)** un **Name (Nom)** de règle.
2. Sélectionnez **Source (Source)** et **Add (Ajoutez)** une **Source Zone (Zone source)** ; sélectionnez **Untrust (Non approuvée)**.
3. Sous **Source Address (Adresse source)**, sélectionnez **Any (Indifférent)**.
4. Sélectionnez **Destination (Destination)** et **Add (Ajoutez)** une **Destination Zone (Zone de destination)** ; sélectionnez **DMZ (DMZ)**.
5. Sous **Actions (Actions)**, sélectionnez **Allow (Autoriser)**.
6. Cliquez sur **OK**.

STEP 10 | Validez vos modifications.

Cliquez sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

STEP 11 | Dépannez ou affichez une session NAT64.

```
> afficher l'ID de session<session-id>
```

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

ECMP

Le traitement ECMP (Equal Cost Multiple Path/chemin multiple à coût égal) est une fonction réseau qui permet au pare-feu d'utiliser jusqu'à quatre itinéraires de coût égal vers la même destination. Sans cette fonction, s'il existe plusieurs itinéraires de coût égal vers la même destination, le routeur virtuel choisit l'un de ces itinéraires dans la table de routage et l'ajoute à sa table de transfert ; il n'utilise aucun autre itinéraire à moins qu'il n'y ait une interruption dans l'itinéraire choisi.

L'activation de la fonctionnalité ECMP sur un routeur virtuel permet au pare-feu d'avoir jusqu'à quatre chemins de coût égal vers une destination dans sa table de transfert, grâce auxquels il peut :

- Équilibrer la charge des flux (sessions) vers la même destination sur plusieurs liaisons de coût égal.
- Utiliser efficacement l'ensemble de la bande passante disponible sur les liaisons vers la même destination plutôt que de laisser certaines liaisons inutilisées.
- Déplacer le trafic de façon dynamique d'un autre membre ECMP vers la même destination en cas de défaillance d'une liaison, au lieu d'attendre que le protocole de routage ou la table RIB choisisse un autre chemin/itinéraire. Cela peut permettre de réduire les périodes d'indisponibilité en cas de défaillance de la liaison.

ECMP est pris en charge sur les modèles Palo Alto Networks®, avec la prise en charge du transfert par le matériel sur les pare-feu PA-7000 Series, PA-5200 et PA-3200. Les pare-feu VM-Series prennent en charge ECMP uniquement via le logiciel. Les performances des sessions sont affectées lorsque ces dernières ne peuvent pas être déchargées sur le matériel.

ECMP est pris en charge sur les interfaces Aggregated Ethernet, de tunnel, VLAN, de Couche 3 et sous-interfaces de Couche 3.

ECMP peut être configuré pour les itinéraires statiques et tous les protocoles de routage dynamique pris en charge par le pare-feu.

ECMP affecte la capacité de la table de routage, car cette capacité est basée sur le nombre de chemins ; par conséquent, un itinéraire ECMP disposant de quatre chemins utilise quatre entrées de la capacité de la table de routage. L'implémentation d'ECMP peut légèrement réduire la capacité de la table de routage, car les étiquettes basées sur la session utilisent plus de mémoire pour le mappage des flux de trafic vers des interfaces particulières.

Le routage d'un routeur virtuel à un autre utilisant des itinéraires statiques ne prend pas en charge ECMP.

Pour obtenir des informations sur la sélection d'un chemin ECMP en cas d'échec d'un homologue HA, reportez-vous à la section ECMP en mode HA active/active.

Les sections suivantes décrivent ECMP et sa configuration.

- Algorithmes d'équilibrage de la charge ECMP
- Configuration d'ECMP sur un routeur virtuel
- Activation d'ECMP pour plusieurs systèmes BGP autonomes

- Vérification d'ECMP

 ©2024 Palo Alto Networks, Inc.

Algorithmes d'équilibrage de la charge ECMP

Supposons que la Routing Information Base (base d'informations de routage - RIB) du pare-feu dispose de plusieurs chemins de coût égal vers une même destination. Par défaut, le nombre maximum de chemins de coût égal est de 2. ECMP choisit les deux meilleurs chemins de coût égal de la Routing Information Base (base d'informations de routage - RIB) à copier dans la Forwarding Information Base (base d'informations de transfert - FIB). ECMP détermine ensuite, en fonction de la méthode d'équilibrage de la charge, le chemin de la FIB qui sera utilisé par le pare-feu pour la destination lors de cette session.

L'équilibrage de la charge ECMP est effectuée au niveau de la session et non du paquet ; une nouvelle session démarre lorsque le pare-feu (ECMP) choisit un chemin de coût égal. Les chemins de coût égal vers une même destination sont considérés comme des membres de chemin ou de groupe ECMP. ECMP détermine le chemin de la FIB qui sera utilisé pour un flux ECMP, en fonction de l'algorithme d'équilibrage de la charge que vous avez défini. Un routeur virtuel peut utiliser uniquement un algorithme d'équilibrage de la charge.

L'activation, la désactivation ou la modification d'un routeur virtuel existant entraîne son redémarrage par le pare-feu, ce qui peut mettre fin aux sessions existantes.

Les quatre choix d'algorithme mettent en évidence différentes priorités, comme suit :

- **Les algorithmes basés sur le hachage donnent la priorité à l'adhérence de session** : les algorithmes **IP Modulo (Module IP)** et **IP Hash (Hachage IP)** utilisent des hachages basés sur les informations contenues dans l'en-tête de paquet, telles que les adresses source et de destination. Comme l'en-tête de chaque flux d'une session donnée contient les mêmes informations source et de destination, ces options donnent la priorité à l'*adhérence* de session. Si vous choisissez l'algorithme **IP Hash (Hachage IP)**, le hachage peut être basé sur les adresses sources et de destination, ou le hachage peut être basé sur l'adresse source uniquement (Pour PAN-OS 8.0.3 et les versions ultérieures). Lorsqu'un hachage IP en fonction de l'adresse source uniquement est utilisé, toutes les sessions appartenant à cette même adresse IP source prennent toujours le même chemin parmi les multiples chemins disponibles. On considère donc que ce chemin est prudent et qu'il est plus facile de le dépanner, au besoin. Vous pouvez éventuellement définir une **Hash Seed (Valeur initiale de hachage)** pour randomiser davantage l'équilibrage de la charge si vous disposez d'un grand nombre de sessions vers la même destination et qu'elles n'ont pas été réparties de façon égale entre les liaisons ECMP.
- **L'algorithme équilibré donne la priorité à l'équilibrage de la charge** : l'algorithme **Balanced Round Robin (Permutation circulaire équilibrée)** répartit les sessions entrantes de façon égale entre les liaisons, favorisant l'équilibrage de la charge par rapport à l'adhérence de session (la permutation circulaire indique une séquence dans laquelle l'élément le moins récemment choisi est choisi). De plus, si de nouveaux itinéraires sont ajoutés ou supprimés d'un groupe ECMP (par exemple, si un chemin du groupe devient inactif), le routeur virtuel rééquilibre les sessions entre les liaisons du groupe. Enfin, si le flux d'une session doit changer d'itinéraire en raison d'une panne, lorsque l'itinéraire d'origine associé à la session redevient disponible, le flux de la session revient vers l'itinéraire d'origine lorsque le routeur virtuel rééquilibre de nouveau la charge.
- **Weighted algorithm prioritizes link capacity and/or speed (l'algorithme pondéré donne la priorité à la capacité et/ou à la vitesse de liaison)** : afin d'étendre le protocole ECMP normalisé, l'implémentation par Palo Alto Networks® permet l'équilibrage de la charge à **Weighted Round**

 ©2024 Palo Alto Networks, Inc.

Robin (Permutation circulaire pondérée), qui prend en compte différentes capacités et vitesses de liaison sur les interfaces de sortie du pare-feu. Cette option vous permet d'affecter des **ECMP Weights (Pondérations ECMP)** (plage entre 1 et 100, par défaut 255) aux interfaces, en fonction des facteurs de performance de liaison, tels que la capacité de liaison, la vitesse ou la latence de liaison, de façon à ce que les charges soient équilibrées et les liaisons disponibles pleinement exploitées.

Par exemple, supposons que le pare-feu dispose de liaisons redondantes vers un ISP : ethernet1/1 (100 Mbits/s) et ethernet1/8 (200 Mbits/s). Bien qu'il s'agisse de chemins de coût égal, la liaison ethernet1/8 fournit une bande passante plus large et peut ainsi gérer une charge supérieure à celle pouvant être traitée par la liaison ethernet1/1. Par conséquent, afin que la fonctionnalité d'équilibrage de la charge prenne en compte la capacité et la vitesse de liaison, vous pouvez affecter une pondération de 200 à ethernet1/8 et de 100 à ethernet1/1. Le coefficient de pondération de 2:1 entraîne l'envoi de deux fois plus de sessions par le routeur virtuel à ethernet1/8 que celles envoyées à ethernet1/1. Cependant, comme le protocole ECMP est fondamentalement basé sur la session, lors de l'utilisation de l'algorithme **Weighted Round Robin (Permutation circulaire pondérée)**, le pare-feu peut équilibrer la charge entre les liaisons ECMP uniquement dans la mesure du possible.

N'oubliez pas que les pondérations ECMP sont affectées aux interfaces pour déterminer l'équilibrage de la charge (afin d'influencer le choix du chemin *de coût égal*) et non pour la sélection de l'itinéraire (le choix d'un itinéraire parmi les itinéraires qui peuvent avoir des coûts différents).



Affectez une pondération inférieure aux liaisons de vitesse ou de capacité plus faible. Affectez une pondération supérieure aux liaisons de vitesse ou de capacité plus élevée. De cette manière, le pare-feu peut répartir les sessions en fonction de ces coefficients, au lieu de surcharger une liaison de faible capacité qui est l'un des chemins de coût égal.

 ©2024 Palo Alto Networks, Inc.

Configuration d'ECMP sur un routeur virtuel

Utilisez la procédure suivante pour activer ECMP sur un routeur virtuel. Les prérequis sont les suivants :

- Indiquez les interfaces qui appartiennent à un routeur virtuel (**Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** > **Router Settings (Paramètres des routeurs)** > **General (Général)**).
- Spécifiez le protocole de routage IP.

L'activation, la désactivation ou la modification d'un routeur virtuel existant entraîne son redémarrage par le système, ce qui peut mettre fin aux sessions existantes.

STEP 1 | Activez ECMP sur un routeur virtuel.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, puis choisissez le routeur virtuel sur lequel vous souhaitez activer ECMP.
2. Sélectionnez **Router Settings (Paramètres des routeurs)** > **ECMP (ECMP)** et sélectionnez **Enable (Activer)**.

STEP 2 | (Facultatif) Activez le retour symétrique des paquets du serveur au client.

Sélectionnez l'option **Symmetric Return (Retour symétrique)** pour que les paquets de retour sortent de la même interface que celle sur laquelle les paquets d'entrée associés sont arrivés. Autrement dit, le pare-feu utilisera l'interface d'entrée sur laquelle envoyer des paquets de retour, au lieu de l'interface ECMP. Le paramètre **Symmetric Return (Retour symétrique)** applique un contrôle prioritaire sur l'équilibrage de la charge. Ce comportement se produit uniquement pour les flux de trafic du serveur au client.

STEP 3 | Activez **Strict Source Path (Chemin d'accès source strict)** pour vous assurer que le trafic IKE et IPSec en provenance du pare-feu sort de l'interface physique à laquelle appartient l'adresse IP source du tunnel IPSec.

Lorsque vous activez ECMP, IKE et IPSec, le trafic provenant du pare-feu sort par défaut d'une interface qu'une méthode d'équilibrage de charge ECMP détermine. Vous pouvez également vous assurer que le trafic IKE et IPSec en provenance du pare-feu sort toujours de l'interface physique à laquelle appartient l'adresse IP source du tunnel IPSec en activant le chemin d'accès source strict. Vous activerez cette fonction lorsque le pare-feu a plus d'un ISP qui offre des chemins d'accès à coût égal vers la même destination. Les ISP effectuent généralement une vérification de Transfert de chemin d'accès inversé (RPF) (ou une vérification différente afin d'empêcher l'usurpation d'adresse IP) pour confirmer que le trafic sort de la même interface que celle sur laquelle il est arrivé. Parce que le traitement ECMP choisira une interface de sortie sur la base de la méthode ECMP configurée (au lieu de choisir l'interface source comme interface de sortie), ce n'est pas ce à quoi l'ISP s'attend et l'ISP pourra bloquer le trafic de retour légitime. Dans ce cas, activez le chemin d'accès strict afin que le pare-feu utilise l'interface de sortie correspondant à l'interface à laquelle appartient l'adresse IP source du tunnel IPSec, le contrôle du RPF réussit, et l'ISP autorise le trafic de retour.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Indiquez le nombre maximum de chemins de coût égal (vers un réseau de destination) qui peut être copié de la Routing Information Base (base d'informations de routage - RIB) à la Forwarding Information Base (base d'informations de transfert - FIB).

Pour **Max Path (Nombre maximum de chemins)**, sélectionnez **2 (2)**, **3 (3)** ou **4 (4)**. Par défaut : 2.

STEP 5 | Sélectionnez l'algorithme d'équilibrage de la charge pour le routeur virtuel. Pour plus d'informations sur les méthodes d'équilibrage de la charge et leurs différences, reportez-vous à la section Algorithmes d'équilibrage de la charge ECMP.

Pour **Load Balance (Équilibrage de la charge)**, sélectionnez l'une des options suivantes dans la liste **Method (Méthode)** :

- **IP Modulo (Module IP)** (paramètre par défaut) : utilise un hachage des adresses IP source et de destination dans l'en-tête de paquet pour déterminer l'itinéraire ECMP à utiliser.
- **Hachage IP**— Il existe deux méthodes de hachage IP qui déterminent la route ECMP à utiliser (sélectionnez les options de hachage à l'étape 5) :
  - Utilisez un hachage de l'adresse source (disponible dans PAN-OS 8.0.3 et versions ultérieures).
  - Utilisez un hachage des adresses IP source et de destination (la méthode de hachage IP établie par défaut).
- **Balanced Round Robin (Permutation circulaire équilibrée)** : utilise la permutation circulaire entre les chemins ECMP et rééquilibre les chemins lorsque le nombre de chemins change.
- **Weighted Round Robin (Permutation circulaire pondérée)** : utilise la permutation circulaire et une pondération relative pour la sélection parmi les chemins ECMP. Spécifiez les pondérations à l'étape 6 ci-dessous.

STEP 6 | (Hachage IP uniquement) Configurez les options de hachage IP.

Si vous avez sélectionné **IP Hash (Hachage IP)** comme **Method (Méthode)** :

1. Sélectionnez **Use Source Address Only (Utiliser l'adresse source uniquement)** (disponible dans PAN-OS 8.0.3 et dans les versions ultérieures) si vous voulez vous assurer que toutes les sessions appartenant à la même adresse IP prennent toujours le même chemin parmi les multiples chemins disponibles. Cette option de hachage IP garantit l'adhérence de session et facilite le dépannage. Si vous ne sélectionnez pas cette option ou que vous utilisez une version antérieure à PAN-OS 8.0.3, le hachage IP est basé sur les adresses IP source et de destination (méthode de hachage IP par défaut).

   *Si vous sélectionnez **Use Source Address Only (Utiliser l'adresse source uniquement)**, vous ne devez pas transmettre la configuration de Panorama aux pare-feu exécutant PAN-OS 8.0.2, 8.0.1 ou 8.0.0.*

2. Sélectionnez **Use Source/Destination Ports (Utiliser les ports source ou de destination)** si vous souhaitez utilisez les numéros de port source ou de destination dans le calcul **IP Hash (Hachage IP)**.

   *L'activation de cette option ainsi que de l'option **Use Source Address Only (Utiliser l'adresse source uniquement)** rendra la sélection du chemin aléatoire même pour les sessions qui appartiennent à la même adresse IP source.*

 ©2024 Palo Alto Networks, Inc.

3. Saisissez une **Hash Seed (Valeur initiale de hachage)** (un nombre entier de neuf chiffres maximum). Spécifiez une **Hash Seed (Valeur initiale de hachage)** pour randomiser davantage l'équilibrage de la charge. L'indication d'une valeur initiale de hachage est utile si vous disposez d'un grand nombre de sessions contenant les mêmes informations de tuple.

STEP 7 | (Permutation circulaire pondérée uniquement) Définissez une pondération pour chaque interface du groupe ECMP.

Si vous avez sélectionné **Weighted Round Robin (Permutation circulaire pondérée)** comme **Method (Méthode)**, définissez une pondération pour chacune des interfaces de sortie, afin que le trafic soit acheminé vers les mêmes destinations (autrement dit, les interfaces qui font partie d'un groupe ECMP, telles que les interfaces qui fournissent des liaisons redondantes à votre ISP ou les interfaces des applications métier sur votre réseau d'entreprise).

Plus la valeur de pondération est élevée, plus ce chemin de coût égal sera sélectionné pour une nouvelle session.

Donnez aux liaisons plus rapides une pondération supérieure à celle des liaisons plus lentes, de manière à ce que le trafic ECMP passe par la liaison plus rapide.

1. Pour créer un groupe ECMP, cliquez sur **Add (Ajouter)**, puis sélectionnez une **Interface (Interface)**.
2. Cliquez sur **Add (Ajouter)** pour ajouter les autres interfaces au groupe ECMP.
3. Cliquez sur **Weight (Pondération)** et indiquez la pondération relative pour chaque interface (plage entre 1 et 255, par défaut 100).

STEP 8 | Enregistrer la configuration.

1. Cliquez sur **OK**.
2. Lorsque vous serez invité à modifier la configuration ECMP, cliquez sur **Yes (Oui)** pour redémarrer le routeur virtuel. Le redémarrage du routeur virtuel peut mettre fin aux sessions existantes.

   Ce message s'affiche uniquement si vous modifiez un routeur virtuel existant sur lequel ECMP est activé.

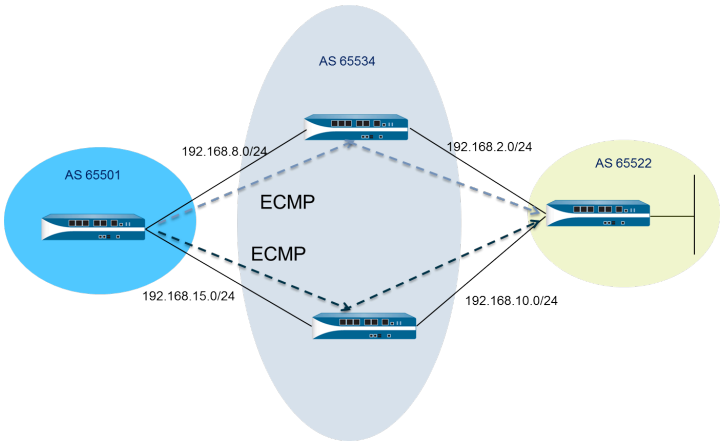
STEP 9 | Validez vos modifications.

Commit (Validez) la configuration.

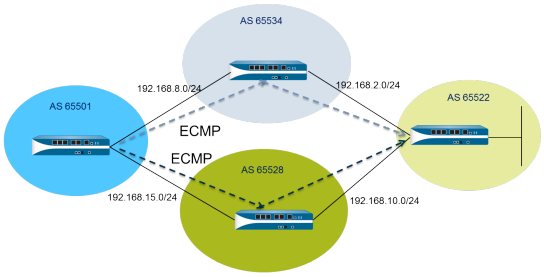
 ©2024 Palo Alto Networks, Inc.

Activation d'ECMP pour plusieurs systèmes BGP autonomes

Effectuez la tâche suivante si vous avez configuré BGP et si vous souhaitez activer ECMP pour plusieurs systèmes autonomes. Cette tâche suppose que BGP est déjà configuré. Dans la figure suivante, deux chemins ECMP vers une destination vont vers deux pare-feu appartenant à un même ISP dans un système BGP autonome unique.



Dans la figure suivante, deux chemins ECMP vers une destination vont vers deux pare-feu appartenant à deux ISP dans différents systèmes BGP autonomes.



STEP 1 | Configurez ECMP.

Reportez-vous à la section Configuration d'ECMP sur un routeur virtuel.

STEP 2 | Pour le routage BGP, activez ECMP pour plusieurs systèmes autonomes.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel sur lequel vous souhaitez activer ECMP pour plusieurs systèmes BGP autonomes.
2. Sélectionnez **BGP (BGP)** > **Advanced (Avancé)**, puis **ECMP Multiple AS Support (Prise en charge d'ECMP par plusieurs systèmes autonomes)**.

STEP 3 | Validez vos modifications.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

Vérification d'ECMP

Un routeur virtuel configuré pour ECMP indique les itinéraires ECMP dans la table Forwarding Information Base (base d'informations de transfert ; FIB). L'étiquette ECMP (E) d'un itinéraire indique qu'il participe à ECMP pour l'interface de sortie vers le saut suivant. Pour vérifier ECMP, utilisez la procédure suivante pour vérifier que certains itinéraires de la FIB sont des chemins ECMP.

STEP 1 | Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**.

STEP 2 | Dans la rangée correspondant au routeur virtuel pour lequel vous avez activé ECMP, cliquez sur **More Runtime Stats (Plus de statistiques d'exécution)**.

STEP 3 | Sélectionnez **Routing (Routage)** > **Forwarding Table (Table de transfert)** pour voir la FIB.



Dans la table, plusieurs itinéraires vers la même destination (provenant de différentes interfaces) portent l'étiquette « E ». Un astérisque (*) indique le chemin préféré du groupe ECMP.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

LLDP

Les pare-feu Palo Alto Networks® prennent en charge Link Layer Discovery Protocol (protocole de découverte de la couche de liaison ; LLDP), qui fonctionne sur la couche de liaison et permet de détecter les périphériques voisins et leurs fonctionnalités. LLDP permet au pare-feu et à d'autres périphériques réseau d'envoyer et de recevoir des unités de données LLDP (LLDPDU) depuis et vers les voisins. Le périphérique de réception stocke les informations dans une MIB, accessible par le protocole Simple Network Management Protocol (protocole simple de gestion réseau ; SNMP). LLDP facilite la résolution des problèmes, en particulier pour les déploiements de câble virtuel où le pare-feu n'est pas détecté par les utilitaires ping et traceroute.

- Présentation de LLDP
- Éléments TLV pris en charge dans LLDP
- Pièges SNMP et messages Syslog LLDP
- Configuration de LLDP
- Affichage de l'état et des paramètres LLDP
- Effacement des statistiques LLDP

Présentation de LLDP

Link Layer Discovery Protocol (LLDP) fonctionne à la couche 2 du modèle OSI, en utilisant des adresses MAC. Une LLDPDU est une séquence d'éléments Type-Length-Value (type-longueur-valeur TLV) encapsulée dans une trame Etherrnet. La norme IEEE 802.1AB définit trois adresses MAC pour les LLDPDU : 01-80-C2-00-00-0E, 01-80-C2-00-00-03 et 01-80-C2-00-00-00.

Le pare-feu Palo Alto Networks® prend en charge une seule adresse MAC pour la transmission et la réception d'unités de données LLDP : 01-80-C2-00-00-0E. Lors de la transmission, le pare-feu utilise 01-80-C2-00-00-0 comme adresse MAC de destination. Lors de la réception, le pare-feu traite les datagrammes avec 01-80-C2-00-00-0 comme adresse MAC de destination. Si le pare-feu reçoit l'une des deux autres adresses MAC pour les LLDPDU sur ses interfaces, il entreprend la même action de transfert que celle entreprise avant cette fonctionnalité, comme suit :

- S'il s'agit d'une interface de câble virtuel, le pare-feu transfère le datagramme à l'autre port.
- S'il s'agit d'une interface de Couche 2, le pare-feu envoie le datagramme vers le reste du VLAN.
- S'il s'agit d'une interface de Couche 3, le pare-feu abandonne le datagramme.

Panorama et l'appareil WildFire ne sont pas pris en charge.

Les types d'interfaces qui ne prennent pas en charge LLDP sont TAP, High Availability (haute disponibilité ; HA), Miroir de déchiffrement, les sous interfaces de câble virtuel/VLAN/de Couche 3 et les interfaces Log Processing Card (carte de traitement des journaux ; LPC) des pare-feu PA-7000 Series.

Une trame Ethernet LLDP a le format suivant :

Preamble	Destination MAC	Source MAC	Ethertype	Chassis ID TLV	Port ID TLV	Time To Live TLV	Optional TLVs	End of LLDPDU TLV	Frame Check Sequence
	01:80:C2:00:00:0E or 01:80:C2:00:00:03 or 01:80:C2:00:00:00	Station's Address	0x88CC	Type=1	Type=2	Type=3	Zero or more complete TLVs	Type=0, Length=0	

Dans la trame Ethernet LLDP, la structure TLV a le format suivant :

TLV Type	TLV Information String Length	TLV Information String
7 bits	9 bits	0-511 octets

 ©2024 Palo Alto Networks, Inc.

Éléments TLV pris en charge dans LLDP

Les LLDPDU incluent des éléments TLV obligatoires et facultatifs. Le tableau suivant répertorie les éléments TLV obligatoires pris en charge par le pare-feu :

Éléments TLV obligatoires	Type d'élément	Description
ID de châssis	1	Identifie le châssis du pare-feu. Chaque pare-feu doit disposer d'un ID de châssis unique. Le sous-type d'ID de châssis est de 4 (adresse MAC). Les modèles Palo Alto Networks® utiliseront l'adresse MAC de Eth0 pour assurer l'unicité.
ID de port	2	Identifie le port depuis lequel la LLDPDU est envoyée. Chaque pare-feu utilise un ID de port pour chaque message LLDPDU transmis. Le sous-type d'ID de port est de 5 (nom de l'interface) et identifie de façon unique le port de transmission. Le pare-feu utilise la valeur ifname de l'interface comme ID de port.
Time-To-Live (durée de vie ; TTL)	3	Indique la durée (en secondes) pendant laquelle les informations LLDPDU reçues de l'homologue sont considérées comme valides sur le pare-feu local (plage entre 0 et 65 535). La valeur est un multiple de la valeur du multiplicateur de temps d'attente LLDP. Lorsque la valeur TTL est de 0, les informations associées au périphérique ne sont plus valides et le pare-feu supprime alors cette entrée de la MIB.
Fin de la LLDPDU	0	Indique la fin des éléments TLV dans la trame Ethernet LLDP.

Le tableau suivant répertorie les éléments TLV facultatifs pris en charge par le pare-feu Palo Alto Networks :

Éléments TLV facultatifs	Type d'élément	Objectif et remarques relatives à l'implémentation du pare-feu
Description du port	4	Décrit le port du pare-feu au format alphanumérique. L'objet ifAlias est utilisé.
Nom du système	5	Nom configuré du pare-feu au format alphanumérique. L'objet sysName est utilisé.
Description du système	6	Décrit le pare-feu au format alphanumérique. L'objet sysDescr est utilisé.

©2024 Palo Alto Networks, Inc.

Éléments TLV facultatifs	Type d'élément	Objectif et remarques relatives à l'implémentation du pare-feu
Fonctionnalités du système	7	Décrit le mode de déploiement de l'interface, comme suit : • Une interface de Couche 3 est publiée avec la fonctionnalité de routeur (bit 6) et l'autre bit (bit 1). • Une interface de Couche 2 est publiée avec la fonctionnalité de pont MAC (bit 3) et l'autre bit (bit 1). • Une interface de câble virtuel est publiée avec la fonctionnalité de répéteur (bit 2) et l'autre bit (bit 1).
Adresse de gestion	8	Une ou plusieurs adresses IP utilisées pour la gestion du pare-feu, comme suit : • Adresse IP de l'interface de gestion (MGT) • Adresse IPv4 et/ou IPv6 de l'interface • Adresse de bouclage • Adresse personnalisée saisie dans le champ de l'adresse de gestion Si aucune adresse IP de gestion n'est fournie, le paramètre par défaut est l'adresse MAC de l'interface de transmission. Le numéro d'interface de l'adresse de gestion donnée est inclus. L'OID d'interface matérielle est également inclus avec l'adresse de gestion donnée (le cas échéant). Si plusieurs adresses de gestion sont indiquées, elles sont envoyées dans l'ordre de saisie, en commençant par le haut de la liste. Quatre adresses de gestion maximum sont prises en charge. Il s'agit d'un paramètre facultatif qui peut être désactivé.

 ©2024 Palo Alto Networks, Inc.

Pièges SNMP et messages Syslog LLDP

Le pare-feu stocke les informations LLDP dans les MIB, qui peuvent être surveillées par un gestionnaire SNMP. Si vous souhaitez que le pare-feu envoie des notifications de piège SNMP et des messages Syslog relatifs aux événements LLDP, vous devez activer l'option **SNMP Syslog Notification (Notification Syslog SNMP)** dans un profil LLDP.

Conformément aux documents RFC 5424, The Syslog Protocol (Le protocole Syslog), et RFC 1157, A Simple Network Management Protocol (Un Simple Network Management Protocol (protocole simple de gestion réseau ; SNMP), LLDP envoie des messages Syslog et de piège SNMP lorsque des modifications sont apportées à la MIB. La fréquence de ces messages est limitée par l'option **Notification Interval (Intervalle de notification)**, un paramètre LLDP général qui peut être configuré et dont la valeur par défaut est de 5 secondes.

Comme la fréquence des messages Syslog LLDP et de piège SNMP est limitée, il se peut que certaines informations LLDP fournies à ces processus ne correspondent pas aux statistiques LLDP visibles lorsque vous Afficher les informations d'état LLDP. Ceci est un comportement normal et attendu.

5 MIB maximum peuvent être reçues par interface (Ethernet ou AE). Chaque source différente dispose d'une MIB. Si cette limite est dépassée, le message d'erreur `tooManyNeighbors` est renvoyé.

 ©2024 Palo Alto Networks, Inc.

Configuration de LLDP

Pour configurer LLDP et créer un profil LLDP, vous devez être un super utilisateur ou un administrateur de périphérique (deviceadmin). Une interface de pare-feu prend en charge cinq homologues LLDP maximum.

STEP 1 | Activez LLDP sur le pare-feu.

Sélectionnez **Network (Réseau)** > **LLDP (LLDP)**, puis modifiez la section LLDP General (LLDP - Général) ; sélectionnez **Enable (Activer)**.

STEP 2 | (Facultatif) Modifiez les paramètres LLDP généraux.

1. Pour **Transmit Interval (sec) (Intervalle de transmission (s))**, indiquez l'intervalle (en secondes) dans lequel les LLDPDU sont transmises La plage est comprise entre 1 et 3600 ; la valeur par défaut est 30.
2. Pour **Transmit Delay (sec) (Délai de transmission (s))**, indiquez le délai (en secondes) entre les transmissions LLDP envoyées après la modification d'un élément TLV. Ce délai permet d'éviter la saturation du segment avec les LLDPDU si de nombreuses modifications réseau dépassent le nombre de modifications LLDP ou en cas de battement de l'interface. Le **Transmit Delay (Délai de transmission)** doit être inférieur au **Transmit Interval (Intervalle de transmission)**. La plage est comprise entre 1 et 600 ; la valeur par défaut est 2.
3. Pour **Hold Time Multiple (Multiple du temps d'attente)**, indiquez une valeur qui est multipliée par le paramètre **Transmit Interval (Intervalle de transmission)** pour déterminer le temps d'attente TTL La plage est comprise entre 1 et 100 ; la valeur par défaut est 4. Le temps d'attente TTL maximum est de 65 535 secondes, quelle que soit la valeur du multiplicateur.
4. Pour **Notification Interval (Intervalle de notification)**, indiquez l'intervalle (en secondes) auquel les pièges SNMP et messages Syslog LLDP sont transmis lorsque des modifications sont apportées à la MIB. La plage est comprise entre 1 et 3600 ; la valeur par défaut est 5.
5. Cliquez sur **OK**.

STEP 3 | Créez un profil LLDP.

Pour obtenir la description des éléments TLV facultatifs, reportez-vous à la section Éléments TLV pris en charge dans LLDP.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **LLDP Profile (Profil LLDP)**, puis **Add (Ajoutez)** un **Name (Nom)** au profil LLDP.
2. Pour **Mode (Mode)**, sélectionnez **transmit-receive (Transmission/Réception)** (paramètre par défaut), **transmit-only (Transmission uniquement)** ou **receive-only (Réception uniquement)**.
3. Sélectionnez **SNMP Syslog Notification (Notification Syslog SNMP)** pour activer les notifications SNMP et les messages Syslog. Si cette option est activée, le paramètre général **Notification Interval (Intervalle de notification)** est utilisé. Le pare-feu envoie des événements Syslog et de piège SNMP, tel que configuré dans **Device (Périphérique)**

 ©2024 Palo Alto Networks, Inc.

> **Log Settings (Paramètres des journaux)** > **System (Système)** > **SNMP Trap Profile (Profil de piège SNMP)** et **Syslog Profile (Profil Syslog)**.

4. Pour les éléments TLV facultatifs, sélectionnez les éléments TLV à transmettre :
   - **Description du port**
   - **Nom du système**
   - **Description du système**
   - **Fonctionnalités du système**
5. (Facultatif) Sélectionnez **Management Address (Adresse de gestion)** pour ajouter une ou plusieurs adresses de gestion et **Add (Ajoutez)** un **Name (Nom)**.
6. Sélectionnez l'**Interface (Interface)** depuis laquelle obtenir l'adresse de gestion. Au moins une adresse est requise si l'élément TLV **Management Address (Adresse de gestion)** est activé. Si aucune adresse IP de gestion n'est configurée, le système utilise l'adresse MAC de l'interface de transmission comme élément TLV d'adresse de gestion.
7. Sélectionnez **IPv4** (IPv4) ou **IPv6 (IPv6)**, puis, dans le champ adjacent, choisissez une adresse IP dans la liste (qui répertorie les adresses configurées sur l'interface sélectionnée) ou saisissez-en une nouvelle.
8. Cliquez sur **OK**.
9. Quatre adresses de gestion maximum sont autorisées. Si plusieurs **Management Address (Adresse de gestion)** sont indiquées, elles sont envoyées dans l'ordre de saisie, en commençant par le haut de la liste. Pour changer l'ordre des adresses, sélectionnez une adresse et utilisez les boutons **Move Up (Monter)** et **Move Down (Descendre)**.
10. Cliquez sur **OK**.

STEP 4 | Affectez un profil LLDP à une interface.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et choisissez l'interface à laquelle vous souhaitez affecter un profil LLDP.
2. Sélectionnez **Advanced (Avancé)** > **LLDP**.
3. Sélectionnez **Enable LLDP (Activer LLDP)** pour affecter un profil LLDP à l'interface.
4. Pour **Profile (Profil)**, sélectionnez le profil que vous avez créé. La sélection du paramètre **None (Aucun)** active les fonctionnalités de base de LLDP : envoi des trois éléments TLV obligatoires et activation du mode **transmit-receive (Transmission/Réception)**.

   Si vous souhaitez créer un nouveau profil, cliquez sur **LLDP Profile (Profil LLDP)** et suivez les instructions présentées à l'étape ci-dessus.
5. Cliquez sur **OK**.

STEP 5 | **Commit (Validez)** vos modifications.

 ©2024 Palo Alto Networks, Inc.

Affichage de l'état et des paramètres LLDP

Suivez la procédure ci-dessous pour afficher l'état et les paramètres LLDP.

STEP 1 | Affichez les paramètres LLDP généraux.

Sélectionnez **Network (Réseau)** > **LLDP (LLDP)**.

Dans l'écran LLDP General (LLDP - Général), la case **Enable (Activer)** indique si LLDP est activé ou non.

- Si LLDP est activé, les paramètres généraux configurés (Intervalle de transmission, Délai de transmission, Multiple du temps d'attente et Intervalle de notification) s'affichent.
- Si ce n'est pas le cas, les valeurs par défaut des paramètres généraux s'affichent.

Pour la description de ces valeurs, consultez la deuxième étape dans Configurer LLDP.

STEP 2 | Affichez les informations relatives à l'état de LLDP.

1. Sélectionnez l'onglet **Status (État)**.
2. (Facultatif) Saisissez un filtre pour limiter les informations affichées.

   Informations sur l'interface :

   - **Interface (Interface)** : nom de l'interface à laquelle un profil LLDP est affecté.
   - **LLDP** : état de LLDP (activé ou désactivé).
   - **Mode (Mode)** : mode LLDP de l'interface : Transmission/Réception, Transmission uniquement ou Réception uniquement.
   - **Profile (Profil)** : nom du profil affecté à l'interface.

   Informations sur la transmission :

   - **Total Transmitted (Total transmis)** : nombre de LLDPDU transmises depuis l'interface.
   - **Dropped Transmit (Transmission abandonnée)** : nombre de LLDPDU non transmises depuis l'interface en raison d'une erreur. Par exemple, une erreur de longueur lorsque le système construit une LLDPDU pour la transmission.

   Information sur la réception :

   - **Total Received (Total reçu)** : nombre de trames LLDP reçues sur l'interface.
   - **Dropped TLV (Éléments TLV abandonnés)** : nombre de trames LLDP supprimées à la réception.
   - **Errors (Erreurs)** : nombre d'éléments TLV reçus sur l'interface qui contiennent des erreurs. Les types d'erreurs TLV sont les suivants : un ou plusieurs éléments TLV obligatoires sont manquants, hors service, contiennent des informations en dehors de la plage admise, ou erreur de longueur.
   - **Unrecognized (Non reconnu)** : nombre d'éléments TLV reçus sur l'interface qui ne sont pas reconnus par l'agent LLDP local. Par exemple, le type TLV se trouve dans la plage TLV réservée.
   - **Aged Out (Expiré)** : nombre d'éléments supprimés de la MIB de réception en raison de l'expiration de la TTL.

©2024 Palo Alto Networks, Inc.

STEP 3 | Affichez les informations LLDP récapitulatives pour chaque voisin visible sur une interface.

1. Sélectionnez l'onglet **Peers (Homologues)**.
2. (Facultatif) Saisissez un filtre pour limiter les informations affichées.

   Interface locale : interface sur le pare-feu qui a détecté le périphérique voisin.

   ID de châssis distant : ID de châssis de l'homologue. L'adresse MAC sera utilisée.

   ID de port : ID de port de l'homologue.

   Nom : nom de l'homologue.

   Plus d'informations : cette option fournit les informations suivantes relatives à l'homologue distant, basées sur les éléments TLV obligatoires et facultatifs :

   - Type de châssis : adresse MAC :
   - Adresse MAC : Adresse MAC de l'homologue.
   - Nom du système : Nom de l'homologue.
   - Description du système : Description de l'homologue.
   - Description du port : Description du port de l'homologue.
   - Type de port : Nom de l'interface.
   - ID de port : le pare-feu utilise la valeur ifname de l'interface.
   - Fonctionnalités du système : Fonctionnalités du système. O=Other (autre), P=Repeater (répéteur), B=Bridge (pont), W=Wireless-LAN (réseau local sans fil), R=Router (routeur), T=Telephone (téléphone)
   - Fonctionnalités activées : Fonctionnalités activées sur l'homologue.
   - Adresse de gestion : Adresse de gestion de l'homologue.

 ©2024 Palo Alto Networks, Inc.

Effacement des statistiques LLDP

Vous pouvez effacer les statistiques LLDP pour des interfaces spécifiques.

Effacez les statistiques LLDP pour des interfaces spécifiques.

1. Sélectionnez **Network (Réseau)** > **LLDP (LLDP)** > **Status (État)** dans la colonne de gauche et choisissez une ou plusieurs interfaces pour lesquelles vous souhaitez effacer les statistiques LLDP.
2. Cliquez sur **Clear LLDP Statistics (Effacer les statistiques LLDP)** au bas de la fenêtre.

 ©2024 Palo Alto Networks, Inc.

BFD

Le pare-feu prend en charge la Bidirectional Forwarding Detection (détection de transmission bidirectionnelle ; BFD) (RFC 5880), un protocole qui reconnaît tout échec du chemin bidirectionnel entre deux homologues de routage. La détection de l'échec BFG est extrêmement rapide, ce qui assure un basculement plus rapide que ce que l'on pourrait atteindre en surveillant les liaisons ou en effectuant fréquemment des vérifications de l'état de santé du routage dynamique, comme des pulsations ou des paquets Hello. Les réseaux et les centres de données stratégiques qui ont besoin de la haute disponibilité et d'un basculement extrêmement rapide doivent pouvoir compter sur la détection extrêmement rapide de l'échec que leur offre la BFD.

- Présentation de la BFD
- Configuration de la BFD
- Référence : Détails de la BFD

Présentation de la BFD

Lorsque vous activez la BFD, celle-ci établit une session entre un point de terminaison (le pare-feu) et son homologue BFD qui se trouve sur le point de terminaison d'une liaison qui se sert de l'établissement de la connexion en trois étapes. Les paquets de contrôles établissent la connexion et négocient les paramètres configurés dans le profil BFD, y compris les intervalles minimaux auxquels les homologues peuvent envoyer et recevoir des paquets de contrôles. Les paquets de contrôles BFD sont transmis via le port 3784 UDP, tant pour IPv4 que pour IPv6. Les paquets de contrôles BFD pour la prise en charge à sauts multiples sont transmis via le port 4784 UDP. Les paquets de contrôles BFD transmis via l'un ou l'autre de ces ports sont encapsulés dans les paquets UDP.

Une fois la session BFD établie, la BFD de Palo Alto Networks® s'exécute de façon asynchrone, ce qui signifie que les deux points de terminaison s'envoient des paquets de contrôles (qui fonctionnent comme des paquets Hello) en respectant l'intervalle négocié. Si un homologue ne reçoit pas de paquet de contrôles au cours du délai de détection (calculé en tant qu'intervalle de transmission négocié multiplié par un multiplicateur de délai de détection), ce dernier considère que la session est inactive. (Le pare-feu ne prend pas en charge le mode à la demande, dans le cadre duquel les paquets de contrôles ne sont envoyés que si cela s'avère nécessaire, plutôt que sur une base régulière.)

Lorsque vous activez la BFD pour un itinéraire statique et qu'une session BFD entre le pare-feu et l'homologue BFD échoue, le pare-feu supprime des tables RIB et FIB l'itinéraire qui a entraîné l'échec et autorise l'utilisation d'un autre chemin ayant une priorité moindre. Lorsque vous activez la BFD pour un protocole de routage, elle avise le protocole de routage d'utiliser un autre chemin vers l'homologue. Le pare-feu et l'homologue BFD reconverge ainsi vers un nouveau chemin.

Un profil BFD vous permet de procéder à la Configuration de la BFD et d'appliquer les paramètres BFD à un ou plusieurs protocoles de routage ou à un ou plusieurs itinéraires statiques sur le pare-feu. Si vous avez activé la BFD sans avoir configuré un profil, le pare-feu utilisera le profil BDF par défaut (ainsi que tous ses paramètres par défaut). Vous ne pouvez pas modifier le profil BFD par défaut.

Lorsqu'une interface exécute plusieurs protocoles qui utilisent des profils BFD différents, la BFD se sert du profil qui possède le **Desired Minimum Tx Interval** (Intervalle de transmission minimum souhaité) le moins élevé. Reportez-vous à la section BFD pour les protocoles de routage dynamiques.

Les homologues HA actif/passif synchronisent les sessions et les configurations BFD, tandis que les homologues HA actif/actif ne le font pas.

La BFD est normalisée dans RFC 5880. PAN-OS ne prend pas en charge tous les éléments de la RFC 5880 ; reportez-vous à la section Composants RFC de la BFD non pris en charge.

PAN-OS prend également en charge RFC 5881, www.rfc-editor.org/rfc/rfc5881.txt. Dans ce cas, la BFD suit un saut unique entre deux systèmes qui utilisent IPv4 ou IPv6, de sorte que les deux systèmes soient directement reliés. La BFD suit également les sauts multiples provenant d'homologues connectés par BGP. PAN-OS suit l'encapsulation BFD comme décrit dans la RFC 5883, www.rfc-editor.org/rfc/rfc5883.txt. PAN-OS ne prend toutefois pas en charge l'authentification.

- Prise en charge du client, de l'interface et du modèle BFD

 ©2024 Palo Alto Networks, Inc.

- Composants RFC de la BFD non pris en charge
- BFD pour les itinéraires statiques
- BFD pour les protocoles de routage dynamiques

Prise en charge du client, de l'interface et du modèle BFD

Les modèles de pare-feu suivants ne prennent pas en charge la BFD : pare-feu PA-800 Series, PA-220 et VM-50. Les modèles qui prennent en charge un nombre maximal de sessions BFD, comme indiqué dans l'outil Sélection des produits.

La BFD s'exécute sur les interfaces Ethernet physiques, Aggregated Ethernet (Ethernet agrégées ; AE), VLAN et de tunnel (VPN de site à site et LSVPN) ainsi que sur les sous-interfaces de Couche 3.

Les clients BFD pris en charge sont les suivants :

- Itinéraires statiques (IPv4 et IPv6) représentant un saut unique
- OSPFv2 et OSPFv3 (les types d'interfaces sont les suivantes : diffusion, point-à-point et point-à-multipoint)
- BGP IPv4 et IPv6 (IBGP, EBGP) représentant un saut unique ou des multi-sauts
- RIP (saut unique)

Composants RFC de la BFD non pris en charge

- Mode à la demande
- Authentification
- Envoi ou réception de paquets Echo ; le pare-feu transmettra toutefois les paquets Echo qui arrivent sur une interface de câble virtuel ou Tap. (Les paquets Echo BFD possèdent des adresse IP source et de destination identiques.)
- Séquences de sondage
- Contrôle de la congestion
- BFD pour LACP (micro-BFD avec interfaces LAG)

BFD pour les itinéraires statiques

Pour utiliser la BFD pour un itinéraire statique, le pare-feu et l'homologue qui se trouvent aux extrémités de l'itinéraire statique doivent prendre en charge les sessions BFD. Un itinéraire statique peut disposer d'un profil BFD seulement si le type de **Next Hop (Saut suivant)** est **IP Address (Adresse IP)**.

Si un ou plusieurs itinéraires statiques vers un homologue sont configurés sur une interface (la session BFD possède des adresses IP source et de destination identiques), une seule session BFD gère automatiquement les itinéraires statiques multiples. Ce comportement réduit le nombre de sessions BFD. Si les itinéraires statiques possèdent des profils BFD différents, c'est le profil qui possède le plus petit **Desired Minimum Tx Interval (Intervalle minimum de transmission souhaité)** qui s'applique.

Dans un déploiement dans lequel vous souhaitez configurer la BFD pour un itinéraire statique d'une interface client DHCP ou PPPoE, vous devez effectuer deux validations. Pour pouvoir

 ©2024 Palo Alto Networks, Inc.

activer la BFD pour un itinéraire statique, il est essentiel que le type de **Next Hop (Saut suivant)** soit **IP Address (Adresse IP)**. Toutefois, au moment de procéder à la validation de l'interface DHCP ou PPPoE, l'adresse IP de l'interface et l'adresse IP du saut suivant (passerelle par défaut) sont inconnues.

Vous devez d'abord activer un client DHCP ou PPPoE pour l'interface, effectuer une validation et attendre que le serveur DHCP ou PPPoE envoie au pare-feu l'adresse IP du client ainsi que l'adresse IP de la passerelle par défaut. Vous pouvez ensuite configurer l'itinéraire statique (en utilisant l'adresse de la passerelle par défaut du client DHCP ou PPPoE en tant que saut suivant) et effectuer une seconde validation.

BFD pour les protocoles de routage dynamiques

En plus de prendre en charge la BFD pour les itinéraires statiques, le pare-feu prend en charge la BFD pour les protocoles de routage BGP, OSPF et RIP.



L'implémentation de la BDF à sauts multiples de Palo Alto Networks® respecte la portion d'encapsulation de RFC 5883, Bidirectional Forwarding Detection (BFD) pour Multihop Paths *mais l'authentification n'est pas prise en charge. Une solution de rechange consiste à configurer la BFD dans un tunnel VPN pour le routage BGP. Le tunnel VPN peut offrir l'authentification sans dédoubler l'authentification BFD.*

Lorsque vous activez la BFD pour les interfaces de diffusion OSPFv2 et OSPFv3, OSPF établit une session BFD uniquement avec son Designated Router (routeur désigné ; DR) et son Backup Designated Router (routeur désigné de secours ; BDR). Sur les interfaces point-à-point, OSPF établit une session BFD avec le voisin immédiat. Sur les interfaces point-à-multipoint, OSPF établit une session BFD avec chaque homologue.

Le pare-feu ne prend pas en charge la BFD sur une liaison virtuelle OSPF ou OSPFv3.

Chaque protocole de routage peut disposer de sessions BFD indépendantes sur une interface. Deux protocoles de routage (BGP, OSPF et RIP) ou plus peuvent également partager une session BFD commune sur une interface.

Lorsque vous activez la BFD pour de multiples protocoles sur la même interface, et que les adresses IP source et de destination des protocoles sont également identiques, les protocoles partagent une seule session BFD, ce qui réduit la charge du processeur du plan de données et le volume de trafic sur l'interface. Si vous configurez différents profils BFD pour ces protocoles, un seul profil BFD est utilisé : celui qui possède le plus petit **Desired Minimum Tx Interval (Intervalle minimum de transmission souhaité)**. Si les profils possèdent le même **Desired Minimum Tx Interval (Intervalle minimum de transmission souhaité)**, c'est le profil qui est utilisé par la session qui a été créée en premier qui s'applique. Dans une situation où un itinéraire statique et OSPF partagent la même session, c'est le profil de l'itinéraire statique qui s'applique, étant donné qu'une session statique est créée immédiatement après une validation, alors que OSPF attend qu'une adjacence devienne inactive.

Dans ces situations, le recours à une seule session BFD a l'avantage de contribuer à une utilisation plus efficace des ressources. Le pare-feu peut utiliser les ressources non utilisées pour prendre en charge un plus grand nombre de sessions BFD sur différentes interfaces ou pour prendre en charge la BFD pour des paires d'adresses IP source et de destination différentes.

L'utilisation d'IPv4 et d'IPv6 sur une même interface ont toujours pour effet de créer des sessions BFD différentes, même si le même profil BFD peut être utilisé.

 ©2024 Palo Alto Networks, Inc.

*Si vous mettez en œuvre la BFD pour BGP et la surveillance des chemins HA, Palo Alto Networks vous recommande de ne pas mettre en œuvre le redémarrage en douceur BGP. En cas d'échec de l'interface de l'homologue BFD et de la surveillance des chemins, la BFD **peut** supprimer les itinéraires touchés de la table de routage et synchroniser cette modification avec le pare-feu HA passif avant que le redémarrage en douceur ait lieu. Si vous décidez de mettre en œuvre la BFD pour BGP, le redémarrage en douceur BGP et la surveillance des chemins HA, vous devriez établir un intervalle de transmission minimum souhaité et un multiplicateur de délai de détection de la BFD supérieurs aux valeurs définies par défaut.*

 ©2024 Palo Alto Networks, Inc.

Configuration de la BFD

Après avoir lu la Présentation de la BFD, qui inclut les modèles de pare-feu et les interfaces pris en charge, effectuez ce qui suit avant de configurer la BFD :

- Configurez un ou plusieurs virtual routers (routeurs virtuels).
- Configurez un ou plusieurs itinéraires statiques si vous appliquez la BFD aux itinéraires statiques.
- Configurez un protocole de routage (BGP, OSPF, OSPFv3 ou RIP) si vous appliquez la BFD à un protocole de routage.

L'efficacité de votre implémentation BFD repose sur une diversité de facteurs, tels que le volume du trafic, les conditions du réseau, le caractère agressif de vos paramètres BFD et la charge de votre plan de données.

STEP 1 | Créez un profil BFD.

Si vous modifiez un paramètre d'un profil BFD qu'une session BFD existante utilise et que vous validez cette modification, avant de supprimer cette session BFD et de la recréer en tenant compte de ce nouveau paramètre, le pare-feu envoie un paquet BFD dans lequel l'état local est défini sur `admin down`. Le périphérique homologue peut effectuer, ou non, le battement du protocole de routage ou de l'itinéraire statique, selon son implémentation de RFC 5882, section 3.2.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **BFD Profile (Profil BFD)**, puis **Add (Ajoutez)** un **Name (Nom)** au profil BFD. Celui-ci est sensible à la casse et doit être unique sur le pare-feu. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
2. Sélectionnez le **Mode (Mode)** sous lequel la BFD fonctionne :
   - **Active (Actif)** : la BFD initie l'envoi de paquets de contrôle vers l'homologue (par défaut). Au moins l'un des homologues BFD doit être actif ; ils peuvent être actifs tous les deux.
   - **Passive (Passif)** : la BFD attend que l'homologue envoie des paquets de contrôles et réponde comme il se doit.

STEP 2 | Configurez les intervalles de la BFD.

1. Saisissez le **Desired Minimum Tx Interval (ms) (Intervalle de transmission minimum souhaité (ms))**. Il s'agit de l'intervalle minimal, en millisecondes, auquel vous voulez que le protocole BFD (appelé BFD) envoie des paquets de contrôles BFD ; vous négociez ainsi l'intervalle de transmission avec l'homologue. La valeur minimale est de 50 sur les

 ©2024 Palo Alto Networks, Inc.

pare-feu PA-7000 et PA-5200 Series et de 200 sur les pare-feu VM-Series. (La valeur maximale est 2 000 ; la valeur par défaut est 1 000).

*Il est recommandé de définir le **Desired Minimum Tx Interval (Intervalle de transmission minimum souhaité)** sur un pare-feu PA-7000 sur 100 ou une valeur plus grande ; une valeur inférieure à 100 risquerait de causer des battements BFD.*

*Si vous disposez de plusieurs protocoles de routage qui utilisent des profils BFD différents sur la même interface, configurez les profils BFD avec le même **Desired Minimum Tx Interval (Intervalle de transmission minimum souhaité)**.*

2. Saisissez le **Required Minimum Tx Interval (ms) (Intervalle de transmission minimum requis (ms))**. Il s'agit de l'intervalle minimum (en millisecondes) auquel la BFD peut recevoir les paquets de contrôles BFD. La valeur minimale est de 50 sur les pare-feu PA-7000 et PA-5200 Series et de 200 sur les pare-feu VM-Series. (La valeur maximale est 2 000 ; la valeur par défaut est 1 000).

   *Il est recommandé de définir le **Required Minimum Tx Interval (Intervalle de transmission minimum requis** sur un pare-feu PA-7000 sur 100 ou une valeur plus grande ; une valeur inférieure à 100 risquerait de causer des battements BFD.*

STEP 3 | Configurez le multiplicateur de délai de détection de la BFD.

Saisissez le **Detection Time Multiplier (Multiplicateur de délai de détection)**. Le système local calcule le délai de détection en tant que **Detection Time Multiplier (Multiplicateur de délai de détection)** reçu du système distant multiplié par l'intervalle de transmission du système distant convenu (la valeur la plus élevée entre le **Required Minimum Rx Interval (Intervalle de réception minimum requis)** et le dernier **Desired Minimum Tx Interval (Intervalle de transmission minimum souhaité)** reçu. Si la BFD ne reçoit pas de paquet de contrôles BFD de son homologue avant l'expiration du délai de détection, c'est qu'un échec a eu lieu. La plage est comprise entre 2 et 50 ; la valeur par défaut est 3.

Par exemple, un intervalle de transmission de 300 ms x 3 (Multiplicateur de délai de détection) = délai de détection de 900.

Lors de la configuration d'un profil BFD, tenez compte du fait que le pare-feu est un périphérique basé sur une session qui se trouve généralement en périphérie d'un réseau ou d'un centre de données et dont les liaisons peuvent être plus lentes que celles d'un routeur dédié. Par conséquent, il est fort probable que le pare-feu devra disposer d'un intervalle plus long et d'un multiplicateur plus élevé que les paramètres les plus rapides permis. Un délai de détection qui est trop court peut entraîner de fausses détections d'échec liées à la congestion du trafic.

STEP 4 | Configurez le Temps d'attente de la BFD.

Saisissez le **Hold Time (ms) (Temps d'attente (ms))**. Il s'agit du délai, en millisecondes, entre l'apparition d'une liaison et la transmission des paquets de contrôles BFD par la BFD. Le **Hold Time (Temps d'attente)** ne s'applique qu'au mode Actif de la BFD. Si la BFD reçoit des paquets de contrôles BFD pendant le **Hold Time (Temps d'attente)**, ceux-ci sont ignorés. La plage est comprise entre 0 et 120 000. Le paramètre défini par défaut de 0 signifie qu'aucun **Hold**

 ©2024 Palo Alto Networks, Inc.

Time (Temps d'attente) n'est utilisé ; le pare-feu envoie et reçoit les paquets de contrôles BFD immédiatement après l'établissement de la liaison.

STEP 5 | (Facultatif—Pour une implémentation de BGP IPv4 uniquement) Configurez les paramètres liés aux sauts du profil BFD.

1. Sélectionnez **Multihop (Multi-sauts)** pour activer la BFD pour le protocole BGP à sauts multiples.
2. Saisissez la **Minimum Rx TTL (TTL de réception minimum)**. Il s'agit de la valeur Time-to-Live (Durée de vie ; TTL) minimale (nombre de sauts) que la BFD acceptera (recevra) dans un paquet de contrôles BFD lorsque le protocole BGP prend en charge la BFD à sauts multiples. (Plage comprise entre 1 et 254 ; aucune valeur par défaut).

   Le pare-feu abandonne le paquet s'il reçoit une TTL inférieure à la **Minimum Rx TTL (TTL de réception minimum)** qui a été configurée. Par exemple, si l'homologue se trouve à cinq sauts et qu'il transmet au pare-feu un paquet BFD ayant une TTL de 100, et que la **Minimum Rx TTL (TTL de réception minimum)** du pare-feu est de 96 ou plus, le pare-feu abandonne le paquet.

STEP 6 | Enregistrez le profil BFD.

Cliquez sur **OK**.

STEP 7 | (Facultatif) Activez la BFD pour un itinéraire statique.

Le pare-feu et l'homologue qui se trouvent aux extrémités de l'itinéraire statique doivent prendre en charge les sessions BFD.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel sur lequel l'itinéraire statique est configuré.
2. Sélectionnez l'onglet **Static Routes (Itinéraires statiques)**.
3. Sélectionnez l'onglet **IPv4 (IPv4)** ou **IPv6 (IPv6)**.
4. Sélectionnez l'itinéraire statique auquel vous voulez appliquer la BFD.
5. Sélectionnez une **Interface (Interface)** (même si vous utilisez une adresse DHCP). Le paramètre correspondant à l'**Interface (Interface)** ne peut être **None (Aucun)**.
6. Sous **Next Hop (Saut suivant)**, sélectionnez **IP Address (Adresse IP)**, puis entrez l'adresse IP, si elle n'est pas déjà indiquée.
7. Sous **BFD Profile (Profil BFD)**, sélectionnez l'une des options suivantes :
   - **default (défaut)** : n'utilise que les paramètres par défaut.
   - Un profil BFD que vous avez configuré ; voir la section Création d'un profil BFD.
   - **New BFD Profile (Nouveau profil BFD)** : vous permet de procéder à la création d'un profil BFD.

   *Sélectionnez **None (Disable BFD) (Aucun (Désactiver la BFD))** pour désactiver la BFD pour cet itinéraire statique.*
8. Cliquez sur **OK**.

Une colonne BFD à l'onglet **IPv4 (IPv4)** ou **IPv6 (IPv6)** indique le profil BFD qui est configuré pour l'itinéraire statique.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | (Facultatif) Activez la BFD sur toutes les interfaces BGP ou sur un seul homologue BGP.

Si vous activez ou désactivez la BFG globalement, toutes les interfaces qui exécutent BGP seront désactivées et réactivées avec la fonctionnalité BFD, ce qui pourrait interrompre le trafic BGP. Lorsque vous activez la BFD sur l'interface, le pare-feu arrête la connexion BGP vers l'homologue pour programmer la BFD sur l'interface. La connexion BGP est abandonnée sur le périphérique homologue, ce qui peut entraîner une reconvergence. Activez la BFD sur les interfaces BGP lors des périodes creuses où une reconvergence n'influera pas sur le trafic de production.

Si vous mettez en œuvre la BFD pour BGP et la surveillance des chemins HA, Palo Alto Networks vous recommande de ne pas mettre en œuvre le redémarrage en douceur BGP. En cas d'échec de l'interface de l'homologue BFD et de la surveillance des chemins, la BFD peut supprimer les itinéraires touchés de la table de routage et synchroniser cette modification avec le pare-feu HA passif avant que le redémarrage en douceur ait lieu. Si vous décidez de mettre en œuvre la BFD pour BGP, le redémarrage en douceur BGP et la surveillance des chemins HA, vous devriez établir un intervalle de transmission minimum souhaité et un multiplicateur de délai de détection de la BFD supérieurs aux valeurs définies par défaut.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel sur lequel le BGP est configuré.
2. Sélectionnez l'onglet **BGP (BGP)**.
3. (Facultatif) Pour appliquer la BFD à toutes les interfaces BGP du routeur virtuel, dans la liste **BFD (BFD)**, sélectionnez l'une des options suivantes, et cliquez sur **OK (OK)** :
   - **default (défaut)** : n'utilise que les paramètres par défaut.
   - Un profil BFD que vous avez configuré ; voir la section Création d'un profil BFD.
   - **New BFD Profile (Nouveau profil BFD)** : vous permet de procéder à la création d'un profil BFD.

     *Sélectionnez **None (Disable BFD) (Aucun (Désactiver la BFD))** pour désactiver la BFD sur toutes les interfaces BGP du routeur virtuel ; vous ne pouvez pas activer la BFD sur une seule interface BGP.*
4. (Facultatif) Pour activer la BFD sur une seule interface homologue BGP (remplaçant ainsi le paramètre **BFD (BFD)** du BGP s'il n'est pas désactivé), accomplissez les tâches suivantes :
   1. Sélectionnez l'onglet **Peer Group (Groupe d'homologues)**.
   2. Sélectionnez un groupe d'homologues.
   3. Sélectionnez un homologue.
   4. Dans la liste **BFD**, sélectionnez l'une des options suivantes :

      default (défaut) : n'utilise que les paramètres par défaut.

      Inherit-vr-global-setting (Hériter des paramètres généraux du routeur virtuel) (par défaut) : l'homologue BGP hérite du profil BFD que vous avez sélectionné globalement pour le BGP du routeur virtuel.

      Un profil BFD que vous avez configuré ; voir la section Création d'un profil BFD.

 ©2024 Palo Alto Networks, Inc.

> *La sélection de **Disable BFD (Désactiver la BFD)** désactive la BFD sur l'homologue BGP.*

5. Cliquez sur **OK**.
6. Cliquez sur **OK**.

Une colonne BFD de la liste BGP - Peer Group/Peer (BGP - Groupe d'homologues/ Homologue) indique le profil BFD qui est configuré sur l'interface.

STEP 9 | (Facultatif) Activez la BFD pour OSPF ou OSPFv3 globalement ou sur une interface OSPF.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel sur lequel OSPF ou OSPFv3 est configuré.
2. Sélectionnez l'onglet **OSPF (OSPF)** ou **OSPFv3 (OSPFv3)**.
3. (Facultatif) Dans la liste **BFD**, sélectionnez l'une des options suivantes pour activer la BFD sur l'ensemble des interfaces OSPF ou OSPFv3, puis cliquez sur **OK (OK)** :
   - **default (défaut)** : n'utilise que les paramètres par défaut.
   - Un profil BFD que vous avez configuré ; voir la section Création d'un profil BFD.
   - **New BFD Profile (Nouveau profil BFD)** : vous permet de procéder à la création d'un profil BFD.

   > *La sélection de **None (Disable BFD) (Aucun (Désactiver la BFD))** désactive la BFD sur toutes les interfaces OSPF du routeur virtuel ; vous ne pouvez pas activer la BFD sur une seule interface OSPF.*
4. (Facultatif) Pour activer la BFD sur une seule interface homologue OSPF (remplaçant ainsi le paramètre **BFD (BFD)** d'OSPF s'il n'est pas désactivé), accomplissez les tâches suivantes :
   1. Sélectionnez l'onglet **Areas (Zones)**, puis sélectionnez une zone.
   2. Dans l'onglet **Interface (Interface)**, sélectionnez une interface.
   3. Dans la liste **BFD**, sélectionnez l'une des options suivantes pour configurer la BFD sur l'homologue OSPF indiqué :

      default (défaut) : n'utilise que les paramètres par défaut.

      Inherit-vr-global-setting (Hériter des paramètres généraux du routeur virtuel) (par défaut : l'homologue OSPF hérite du paramètre **BFD(BFD)** de l'OSPF ou de l'OSPFv3 pour le routeur virtuel.

      Un profil BFD que vous avez configuré ; voir la section Création d'un profil BFD.

      > *La sélection de **Disable BFD (Désactiver la BFD)** désactive la BFD sur l'interface OSPF ou OSPFv3.*
   4. Cliquez sur **OK**.
5. Cliquez sur **OK**.

Une colonne BFD à l'onglet **Interface (Interface)** de l'OSPF indique le profil BFD qui est configuré sur l'interface.

 ©2024 Palo Alto Networks, Inc.

STEP 10 | (Facultatif) Activez la BFD sur toutes les interfaces RIP ou sur une seule interface RIP.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel sur lequel le RIP est configuré.
2. Sélectionnez l'onglet **RIP (RIP)**.
3. (Facultatif) Dans la liste **BFD**, sélectionnez l'une des options suivantes pour activer la BFD sur l'ensemble des interfaces RIP du routeur virtuel, puis cliquez sur **OK (OK)** :
   - **default (défaut)** : n'utilise que les paramètres par défaut.
   - Un profil BFD que vous avez configuré ; voir la section Création d'un profil BFD.
   - **New BFD Profile (Nouveau profil BFD)** : vous permet de procéder à la création d'un profil BFD.

   *La sélection de **None (Disable BFD) (Aucun (Désactiver la BFD))** désactive la BFD sur toutes les interfaces RIP du routeur virtuel ; vous ne pouvez pas activer la BFD sur une seule interface RIP.*
4. (Facultatif) Pour activer la BFD sur une seule interface RIP (remplaçant ainsi le paramètre **BFD (BFD)** du RIP s'il n'est pas désactivé), accomplissez les tâches suivantes :
   1. Sélectionnez l'onglet **Interfaces (Interfaces)**, puis sélectionnez une interface.
   2. Dans la liste **BFD**, sélectionnez l'une des options suivantes :

      default (défaut) : n'utilise que les paramètres par défaut.

      Inherit-vr-global-setting (Hériter des paramètres généraux du routeur virtuel) (par défaut) : l'homologue BGP hérite du profil BFD que vous avez sélectionné globalement pour le BGP du routeur virtuel.

      Un profil BFD que vous avez configuré ; voir la section Création d'un profil BFD.

      *La sélection de **None (Disable BFD) (Aucun (Désactiver la BFD))** désactive la BFD sur l'interface RIP.*
   3. Cliquez sur **OK**.
5. Cliquez sur **OK**.

La colonne BFD de l'onglet **Interface (Interface)** indique le profil BFD qui est configuré sur l'interface.

STEP 11 | Commit (Validez) la configuration.

Cliquez sur **Commit (Valider)**.

STEP 12 | Affichage du récapitulatif et des détails de la BFD

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, trouvez le routeur virtuel qui vous intéresse, et cliquez sur le lien **More Runtime Stats (Statistiques d'exécution supplémentaires)**.
2. Sélectionnez l'onglet **BFD Summary Information (Informations récapitulatives sur la BFD)** pour consulter les informations récapitulatives, telles que l'état de la BFD et les statistiques d'exécution.
3. (Facultatif) Sélectionnez **details (détails)** dans la rangée de l'interface qui vous intéresse pour afficher la section Référence : Détails de la BFD.

 ©2024 Palo Alto Networks, Inc.

STEP 13 | Surveillez les profils BFD référencés par une configuration de routage ; surveillez les statistiques et l'état de la BFD.

Utilisez les commandes opérationnelles CLI suivantes :

- **show routing bfd active-profile [***<name>***]**
- **afficher les détails du routage bfd [interface** *<name>***][local-ip***<ip>***][multihop][peer-ip** *<ip>***][identifiant de session][routeur virtuel***<name>***]**
- **show routing bfd drop-counters session-id***<session-id>*
- **afficher le compteur mondial | match bfd**

STEP 14 | (Facultatif) Supprimez les compteurs de transmission, de réception et d'abandon de la BFD.

```
clear routing bfd counters session-id all | <1-1024>
```

STEP 15 | (Facultatif) Supprimez les sessions BFD à des fins de débogage.

```
clear routing bfd session-state session-id all | <1-1024>
```

 ©2024 Palo Alto Networks, Inc.

Référence : Détails de la BFD

Pour afficher les informations suivantes sur la BFD d'un routeur virtuel, reportez-vous aux étapes Configuration de la BFDAfficher résumé et détails de la BFD.

Nom	Valeur (Exemple)	Description
ID de session	1	Numéro d'identification de la session BFD.
Interface	Ethernet 1/12	Interface que vous avez sélectionnée sur laquelle la BFD s'exécute.
Protocole	OSPF (IPV4) STATIQUE	Itinéraire statique (famille d'adresses IP de l'itinéraire statique) et/ou protocole de routage dynamique qui exécute la BFD sur l'interface.
Adresse IP locale	10.55.55.2	Adresse IP de l'interface.
Adresse IP du voisin	10.55.55.1	Adresse IP du voisin BFD.
Profil BFD	défaut *(Cette session BFD possède de multiples profils BFD. La valeur 'Desired Minimum Tx Interval (ms)' (Intervalle de transmission minimum souhaité (ms)) la moins élevée permet de sélectionner le profil en vigueur.)	Nom du profil BFD appliqué à l'interface. Étant donné qu'un itinéraire statique et OSPF exécutent la BDF à l'aide de profils différents sur l'interface modèle, le pare-feu utilise le profil qui possède la valeur **Desired Minimum Tx Interval (Intervalle de transmission minimum souhaité (ms))** la moins élevée. Dans cet exemple, le profil par défaut est utilisé.
État (local/distant)	actif/actif	Les états BFD des homologues BFD locaux et distants. Les états possibles sont les suivants : inactif sur le plan administratif, inactif, initialisation et actif.
Délai d'activation	2 h 36 min 21 s 419 ms	Délai pendant lequel BFD a été activé (heures, minutes, secondes et millisecondes).

©2024 Palo Alto Networks, Inc.

Nom	Valeur (Exemple)	Description
Discriminateur (local/distant)	1391591427/1	Les discriminateurs des homologues BFD locaux et distants.
Mode	Actif	Mode sur lequel la BFD est configurée sur l'interface : Actif ou passif
Mode à la demande	Désactivé	PAN-OS ne prend pas en charge le mode à la demande de la BFD ; le mode est donc toujours défini sur Désactivé.
Sauts multiples	Désactivé	BFD à sauts multiples : Activée ou désactivée
TTL des sauts multiples		TTL des sauts multiples ; plage comprise entre 1 et 254. Le champ est vide si la fonction Sauts multiples est désactivée.
Code de diagnostic local	0 (pas de diagnostic)	Les codes de diagnostic indiquent la raison du dernier changement d'état du système local : 0 : pas de diagnostic 1 : expiration du délai de détection de contrôles 2 : échec de la fonction Echo 3 : le voisin a signalé l'inactivité de la session 4 : réinitialisation du plan de transfert 5 : chemin inactif 6 : chemin inactif concaténé 7 : inactif sur le plan de l'administration 8 : chemin inactif concaténé à l'envers
Dernier code de diagnostic à distance reçu	0 (pas de diagnostic)	Dernier code de diagnostic reçu de la part de l'homologue BFD.
Temps d'attente pour la transmission	0 ms	Délai, en millisecondes, entre l'apparition d'une liaison et la transmission des paquets de contrôles BFD par la BFD. Un délai de 0ms signifie que la transmission doit avoir lieu immédiatement. Plage comprise entre 0 et 120 000 ms.
Intervalle de réception min. reçu	1000 ms	Intervalle de réception minimum reçu de la part de l'homologue ; l'intervalle auquel l'homologue BFD peut recevoir des paquets de contrôles. Maximum de 2 000 ms.

©2024 Palo Alto Networks, Inc.

Nom	Valeur (Exemple)	Description
Intervalle de transmission négocié	1000 ms	Intervalle de transmission (en millisecondes) auquel les homologues BFD ont convenu de s'envoyer des paquets de contrôles BFD. Maximum de 2 000 ms.
Multiplicateur de réception	3	Valeur du multiplicateur de délai de détection reçue de la part de l'homologue BFD. Le délai de transmission multiplié par le multiplicateur équivaut au délai de détection. Si la BFD ne reçoit pas de paquet de contrôles BFD de son homologue avant l'expiration du délai de détection, c'est qu'un échec a eu lieu. La plage est comprise entre 2 et 50.
Délai de détection (dépassé)	3000ms (0)	Délai de détection calculé (Délai de transmission négocié multiplié par le multiplicateur) et le nombre de millisecondes correspondant au dépassement du délai de détection.
Paquets de contrôles de transmission (dernier)	9383 (il y a 420 ms)	Nombre de paquets de contrôles BFD qui ont été transmis (et temps écoulé depuis que la BDF a transmis le plus récent paquet de contrôles).
Paquets de contrôles de réception (dernier)	9384 (il y a 407 ms)	Nombre de paquets de contrôles BFD reçus (et temps écoulé depuis que la BDF a reçu le plus récent paquet de contrôles).
Panneau de données de l'agent	Logement 1 - plan de données 0	Sur les pare-feux PA-7000 Series, le processeur du plan de données qui est affecté à la gestion des paquets de cette session BFD.
Erreurs	0	Nombre d'erreurs BFD.
Dernier paquet ayant entraîné un changement d'état		
Version	1	Version de la BFD
Bit d'interrogation	0	Bit d'interrogation BFD ; 0 signifie qu'il n'a pas été défini.
Intervalle de transmission min. souhaité	1000 ms	Intervalle de transmission minimum souhaité du dernier paquet ayant entraîné un changement d'état.
Intervalle de réception minimum requis	1000 ms	Intervalle de réception minimum requis du dernier paquet ayant causé un changement d'état.

©2024 Palo Alto Networks, Inc.

Nom	Valeur (Exemple)	Description
Multiplicateur de détection	3	Multiplicateur de détection du dernier paquet ayant entraîné un changement d'état.
Mon discriminateur	1	Discriminateur distant. Un discriminateur est une valeur unique et non nulle que les homologues utilisent pour distinguer plusieurs sessions BFD entre eux.
Votre discriminateur	1391591427	Discriminateur local. Un discriminateur est une valeur unique et non nulle que les homologues utilisent pour distinguer plusieurs sessions BFD entre eux.
Code de diagnostic	0 (pas de diagnostic)	Code de diagnostic du dernier paquet ayant entraîné un changement d'état.
Longueur	24	Longueur du paquet de contrôles BFD en octets.
Bit de demande	0	PAN-OS ne prend pas en charge le mode à la demande de la BFD ; le bit de demande est donc toujours défini sur 0 (désactivé).
Bit final	0	PAN-OS ne prend pas en charge la séquence d'interrogation; le bit final est donc toujours défini sur 0 (désactivé).
Bit multipoint	0	Ce bit est destiné aux extensions point-à-multipoint futures de la BFD. Il doit être de zéro à la réception et à la transmission.
Bit indépendant de plan de commande	1	• Si ce bit est défini sur 1, l'implémentation BFD du système de transmission n'est pas traitée de la même façon que le plan de commande (c.-à-d. la BDF est implémentée dans le plan de transmission et peut continuer à fonctionner malgré les perturbations du plan de commande). Dans PAN-OS, ce bit est toujours défini sur 1. • S'il est défini sur 0, l'implémentation BFD du système de transmission est traitée de la même façon que le plan de commande.
Bit de présence d'authentification	0	PAN-OS ne prend pas en charge l'authentification BFD ; le bit de présence d'authentification est donc toujours défini sur 0.

©2024 Palo Alto Networks, Inc.

Nom	Valeur (Exemple)	Description
Intervalle de réception Echo minimum requis	0 ms	PAN-OS ne prend pas en charge la fonction Echo BFD ; cet intervalle sera donc toujours de 0ms.

©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Paramètres et délais d'expiration de session

Cette section décrit les paramètres globaux qui affectent les sessions TCP, UDP et ICMPv6, en plus du dépassement d'abonnement NAT, NAT64, IPv6, de la taille des trames Jumbo, de l'unité de transmission maximale, du vieillissement accéléré et de l'authentification du portail captif. Un autre paramètre (Rematch Sessions (Revérifier les sessions)) vous permet d'appliquer les nouvelles politiques de sécurité configurées aux sessions en cours.

Les premières rubriques ci-dessous fournissent un bref récapitulatif de la couche de transport du modèle OSI, et des protocoles TCP, UDP et ICMP. Pour plus d'informations sur les protocoles, reportez-vous à leurs RFC respectifs. Les rubriques restantes décrivent les paramètres et délais d'expiration de session.

- Sessions de couche de transport
- TCP
- UDP
- ICMP
- ICMP spécifiques à la commande ou Types et Codes ICMPv6
- Configuration des délais d'expiration de session
- Politiques de Distribution de Sessions
- Configuration des paramètres de session
- Prévention de l'établissement de la session de liaison de segmentation TCP

Sessions de couche de transport

Une session réseau est un échange de messages qui se produit entre deux périphériques de communication ou plus et qui dure un certain temps. Une session est établie et arrêtée lorsqu'elle se termine. Différents types de sessions se produisent au niveau de trois couches du modèle OSI : la couche de transport, la couche de session et la couche d'application.

La couche de transport est la couche 4 du modèle OSI, qui fournit et contrôle un flux de données fiables ou non fiables de bout en bout. Les protocoles Internet qui implémentent des sessions au niveau de la couche de transport sont notamment Transmission Control Protocol (protocole de contrôle de transmission ; TCP) et User Datagram Protocol (protocole de datagramme utilisateur ; UDP).

 ©2024 Palo Alto Networks, Inc.

TCP

TCP (RFC 793) est l'un des principaux protocoles de la suite IP (Internet Protocol) et il est si courant qu'il est fréquemment référencé conjointement avec IP (*TCP/IP*). TCP est considéré comme un protocole de transport fiable car il permet la vérification des erreurs, tout en transmettant et en recevant des segments, reconnaît les segments reçus et réordonne les segments qui arrivent dans le désordre. TCP demande et fournit également la retransmission des segments qui ont été perdus. TCP est un protocole avec état orienté connexion, autrement dit, une connexion entre l'expéditeur et le destinataire est établie pour la durée de la session. TCP permet de contrôler les paquets et de gérer ainsi la congestion sur les réseaux.

TCP établit une liaison lors de la configuration de la session afin d'initier et de reconnaître cette dernière. Une fois les données transférées, la session est fermée de manière ordonnée ; chaque côté transmet un paquet FIN et le reconnaît avec un paquet ACK. L'établissement de liaison qui initie une session TCP est souvent l'établissement d'une connexion en trois étapes (un échange de trois messages) entre l'initiateur et l'écouteur, ou il peut être une variante, telle que l'établissement de liaison de segmentation en quatre ou cinq étapes, ou l'ouverture de sessions simultanées. La section Abandon de l'établissement de liaison de segmentation TCP explique comment Prévention de l'établissement de la session de liaison de segmentation TCP.

Les applications qui utilisent TCP comme protocole de transport sont notamment Hypertext Transfer Protocol (protocole de transfert hypertexte ; HTTP), HTTP Secure (HTTP sécurisé ; HTTPS), File Transfer Protocol (protocole de transfert de fichiers ; FTP), Simple Mail Transfer Protocol (protocole simple de transfert de courrier ; SMTP), Telnet, Post Office Protocol version 3 (protocole de bureau de poste version 3 ; POP3), Internet Message Access Protocol (protocole d'accès aux messages Internet ; IMAP) et Secure Shell (coquille sécurisée ; SSH).

Les rubriques suivantes décrivent en détail l'implémentation de TCP par PAN-OS.

- Minuteurs Sessions TCP à moitié fermées et Sessions TCP en état time_wait
- Minuteur RST non vérifié
- Abandon de l'établissement de liaison de segmentation TCP
- Maximum Segment Size (taille de segment maximale ; MSS)

Vous pouvez configurer packet-based attack protection (protection contre les attaques basées sur les paquets) et abandonner les paquets IP, TCP et IPv6 avec des caractéristiques indésirables ou retirer des options indésirables des paquets avant de les autoriser dans la zone. Vous pouvez également configurer une protection contre les saturations, en définissant la quantité de connexions SYN par seconde (sans correspondance avec une session existante) provoquant le déclenchement d'une alarme, entraînant le pare-feu à abandonner des paquets SYN ou à utiliser des cookies SYN de manière aléatoire, et entraînant le pare-feu à abandonner des paquets SYN qui dépassent la quantité maximale.

Minuteurs Sessions TCP à moitié fermées et Sessions TCP en état time_wait

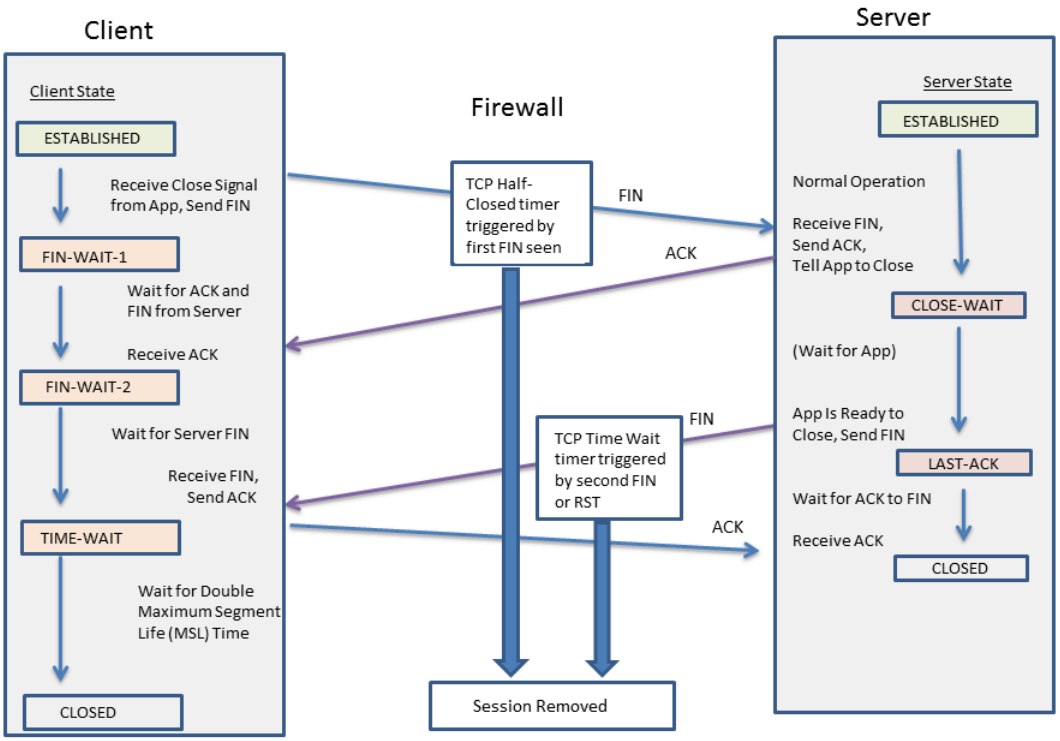
La procédure d'arrêt de session TCP utilise un minuteur Sessions TCP à moitié fermées, qui est déclenché par le premier paquet FIN que le pare-feu voit pour une session. Le minuteur est

 ©2024 Palo Alto Networks, Inc.

nommé Sessions TCP à moitié fermées, car un côté de la connexion a envoyé un paquet FIN. Un second minuteur, Sessions TCP en état time_wait, est déclenché par le second paquet FIN ou RST.

Si un seul minuteur est déclenché par le premier paquet FIN, un paramètre trop court peut fermer prématurément les sessions à moitié fermées. Inversement, un paramètre trop long peut entraîner le développement excessif de la table de sessions et l'utilisation de toutes les sessions. Deux minuteurs vous permettent de définir un paramètre Sessions TCP à moitié fermées relativement long et un autre paramètre Sessions TCP en état time_wait court, vieillissant ainsi rapidement les sessions complètement fermées et contrôlant la taille de la table de sessions.

La figure suivante illustre le déclenchement des deux minuteurs du pare-feu lors de la procédure d'arrêt de connexion TCP.



Le minuteur Sessions TCP en état time_wait doit être défini sur une valeur inférieure à celle du minuteur Sessions TCP à moitié fermées pour les raisons suivantes :

- L'autorisation d'un délai plus long après que le premier paquet FIN a été vu donne à l'autre côté de la connexion du temps pour fermer complètement la session.
- Un paramètre Sessions TCP en état time_wait plus court est utilisé lorsque la session n'a pas besoin de rester ouverte longtemps après que le second paquet FIN ou RST a été vu. Un paramètre Sessions TCP en état time_wait plus court libère des ressources plus rapidement, mais donne assez de temps au pare-feu pour voir le paquet ACK final et une possible retransmission des autres datagrammes.

Si vous configurez un minuteur Sessions TCP en état time_wait sur une valeur supérieure à celle du minuteur Sessions TCP à moitié fermées, la validation sera acceptée mais, en pratique, la valeur

 ©2024 Palo Alto Networks, Inc.

du minuteur Sessions TCP en état time_wait ne dépassera pas celle du minuteur Sessions TCP à moitié fermées.

Les minuteurs peuvent être définis globalement ou par application. Les paramètres globaux sont utilisés pour toutes les applications par défaut. Si vous configurez ces minuteurs au niveau de l'application, ils remplacent les paramètres globaux.

Minuteur RST non vérifié

Si le pare-feu reçoit un paquet RST (Reset) qui ne peut pas être vérifié (car il dispose d'un numéro de séquence inattendu dans la fenêtre TCP ou il provient d'un chemin asymétrique), le minuteur RST non vérifié contrôle le vieillissement de la session (par défaut : 30 secondes ; plage entre 1 et 600 secondes). Le minuteur RST non vérifié fournit une mesure de sécurité supplémentaire, expliquée dans le deuxième point ci-dessous.

Un paquet RST aura l'un des trois résultats possibles suivants :

- Un paquet RST qui se trouve hors de la fenêtre TCP est perdu.
- Un paquet RST qui se trouve dans la fenêtre TCP mais qui ne dispose pas du numéro de séquence exact attendu n'est pas vérifié et sujet au minuteur RST non vérifié. Ce comportement permet d'empêcher les attaques de déni de service (DoS) qui tentent d'interrompre les sessions existantes en envoyant des paquets RST aléatoires au pare-feu.
- Un paquet RST qui se trouve dans la fenêtre TCP et dispose du numéro de séquence exact attendu est sujet au minuteur Sessions TCP en état time_wait.

Abandon de l'établissement de liaison de segmentation TCP

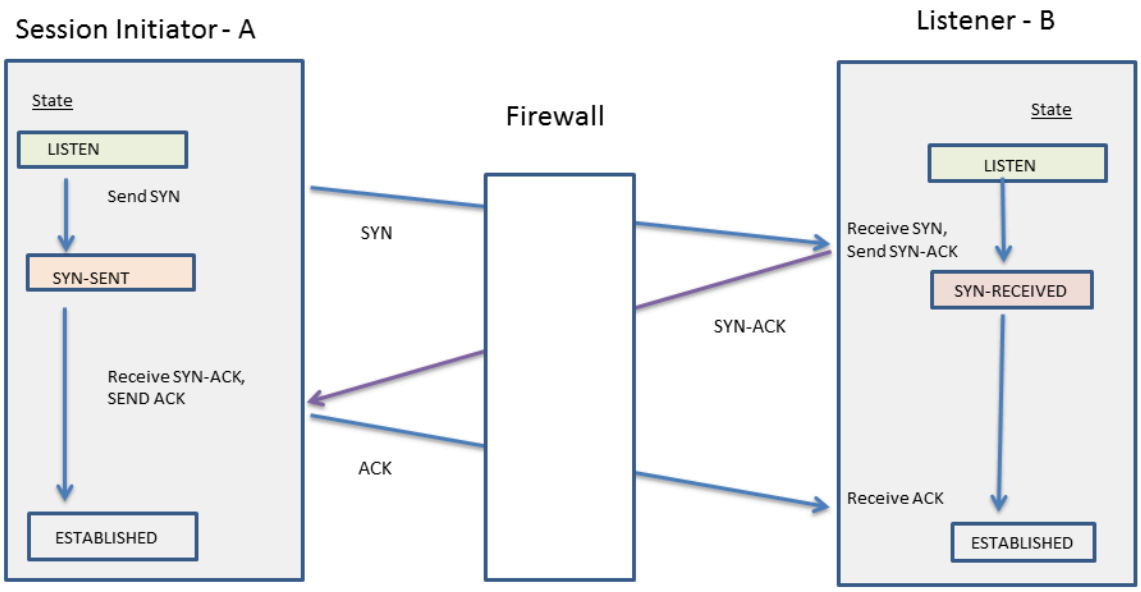
L'option **Split Handshake (Établissement de liaison de segmentation)** dans un profil de protection de zone empêchera l'établissement d'une session TCP si la procédure d'établissement de session n'utilise pas l'établissement de la connexion en trois étapes bien connu, mais plutôt une variante, telle que l'établissement de liaison de segmentation en quatre ou cinq étapes, ou l'ouverture de sessions simultanées.

Le pare-feu Palo Alto Networks® de dernière génération gère correctement les sessions et tous les processus de Couche 7 pour l'établissement de liaison de segmentation et l'ouverture de sessions simultanées sans activer l'option Split Handshake (Établissement de liaison de segmentation). Toutefois, l'option **Split Handshake (Établissement de liaison de segmentation)** (qui entraîne l'abandon de l'établissement de liaison de segmentation TCP) est disponible. Lorsque l'option **Split Handshake (Établissement de liaison de segmentation)** est configurée pour un profil de protection de zone et que celui-ci est appliqué à une zone, les sessions TCP des interfaces de cette zone doivent être établies à l'aide de l'établissement de la connexion en trois étapes ; les variantes ne sont pas autorisées.

L'option **Split Handshake (Établissement de liaison de segmentation)** est désactivée par défaut.

La figure suivante illustre l'établissement de la connexion en trois étapes standard utilisé pour établir une session TCP avec un pare-feu PAN-OS entre l'initiateur (généralement un client) et l'écouteur (généralement un serveur).

 ©2024 Palo Alto Networks, Inc.



L'option **Split Handshake (Établissement de liaison de segmentation)** est configurée pour un profil de protection de zone affecté à une zone. Une interface membre de la zone abandonne tout paquet de synchronisation (SYN) envoyé par le serveur, empêchant les variantes d'établissement de liaison suivantes. La lettre A dans la figure indique l'initiateur de session et B l'écouteur. Chaque segment numéroté de l'établissement de liaison dispose d'une flèche indiquant le sens du segment de l'expéditeur au destinataire, et chaque segment indique le paramètre de bit(s) de contrôle.

4-Way Split Handshake (Version 1)	4-Way Split Handshake (Version 2)	Simultaneous Open	5-Way Split Handshake
1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B SYN-ACK	1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B SYN-ACK 5. A ← B ACK

Possibilité de Prévention de l'établissement de liaison de segmentation TCP.

Maximum Segment Size (taille de segment maximale ; MSS)

La Maximum Transmission Unit (unité de transmission maximale ; MTU) est une valeur qui indique le plus grand nombre d'octets pouvant être transmis dans un seul paquet TCP. La MTU comprend la longueur des en-têtes. Ainsi, la MTU moins le nombre d'octets compris dans les en-têtes équivaut à la Maximum Segment Size (taille de segment maximale ; MSS), soit le nombre maximal d'octets de données pouvant être transmis dans un seul paquet.

 ©2024 Palo Alto Networks, Inc.

Une taille d'ajustement MSS configurable (illustrée ci-dessous) permet à votre pare-feu d'acheminer le trafic ayant des en-têtes qui dépassent la valeur permise par le paramètre par défaut. L'encapsulation rallonge les en-têtes. Vous devez donc augmenter la taille d'ajustement MSS de façon à autoriser le nombre d'octets nécessaires pour laisser passer, par exemple, un en-tête MPLS ou le trafic tunnellisé ayant une étiquette VLAN.



Si l'octet Do Not Fragment (ne pas fragmenter ; DF) est défini pour un paquet, il s'avère utile de disposer d'une taille d'ajustement MSS plus importante et d'une MSS plus petite afin que les en-têtes particulièrement longs n'entraînent pas une longueur de paquet qui dépasse la valeur MTU permise. Si l'octet DF était défini et que la valeur MTU permise était dépassée, les paquets les plus gros seraient abandonnés.

Vous pouvez configurer le pare-feu globalement pour fragmenter les paquets IPv4 qui dépassent la MTU de l'interface de sortie, même si le bit DF est fixé dans le paquet Activez cela pour les interfaces physiques de niveau 3 et les interfaces de tunnel IPSEC en utilisant la commande CLI ***debug dataplane set ip4-df-ignore yes****. Restaurez le pate-feu au comportement par défaut en utilisant la commande CLI* ***debug dataplane set ipv4-df-ignore no****.*

Le pare-feu prend en charge une taille d'ajustement MSS configurable pour les adresses IPv4 et IPv6 sur les types d'interface de couche 3 suivants : Ethernet, sous-interfaces, Aggregated Ethernet (ethernet agrégé ; AE), VLAN et en boucle. La taille d'ajustement MSS pour les adresses IPv6 ne s'applique que si IPv6 est activé sur l'interface.

Si IPv4 et IPv6 sont activés sur une interface et que la taille d'ajustement MSS diffère entre les deux formats d'adresses IP, c'est la valeur MSS correspondant au bon type d'adresse IP qui est utilisée pour le trafic TCP.

Pour les adresses IPv4 et IPv6, le pare-feu acheminera des en-têtes TCP plus longs que prévu. Si la longueur de l'en-tête d'un paquet TCP est supérieure à la valeur que vous aviez prévue, le pare-feu choisit la plus importante des deux valeurs suivantes en tant que taille d'ajustement MSS :

- la taille d'ajustement MSS configurée ;
- la somme de la longueur de l'en-tête TCP (20) + la longueur des en-têtes IP du paquet de synchronisation TCP.

Cette façon de faire signifie que le pare-feu remplacera la taille d'ajustement MSS configurée, au besoin. Par exemple, si la taille d'ajustement MSS que vous avez configurée est 43, vous vous attendez à ce que la MSS soit égale à 1 458 (la taille MTU par défaut moins la taille d'ajustement [1 500 - 42]). Cependant, le paquet TCP possède 4 octets supplémentaires d'options IP dans son en-tête. Ainsi, la taille d'ajustement MSS (20+20+4) correspond à 44, soit une valeur qui est supérieure à la taille d'ajustement MSS de 42. La MSS qui en résulte est 1 500 - 44 = 1 456 octets, une valeur inférieure à ce que vous aviez prévu.

Pour configurer la taille d'ajustement MSS, consultez Configuration des paramètres de session.

 ©2024 Palo Alto Networks, Inc.

UDP

User Datagram Protocol (protocole de datagramme utilisateur - UDP) (RFC 768) est un autre protocole principal de la suite IP qui est une alternative à TCP. UDP est sans état et sans connexion. Autrement dit, lors de sa configuration, aucune session ni aucune connexion n'est établie entre l'expéditeur et le destinataire ; les paquets peuvent prendre différents chemins pour accéder à une même destination. UDP est considéré comme un protocole peu fiable, car il ne permet pas la reconnaissance, la vérification des erreurs, la retransmission ni la réorganisation des datagrammes. Sans la surcharge requise pour fournir ces fonctions, UDP offre une latence réduite et est plus rapide que TCP. UDP est un protocole minimum, car il ne dispose d'aucun mécanisme permettant de garantir l'arrivée des messages à leur destination.

Un datagramme UDP est encapsulé dans un paquet IP. Bien qu'UDP utilise une somme de contrôle pour l'intégrité des données, il n'effectue aucune vérification des données au niveau de l'interface réseau. La vérification des erreurs est censée être inutile ou est effectuée par l'application au lieu d'UDP lui-même. UDP ne dispose d'aucun mécanisme permettant de contrôler le flux des paquets.

UDP est souvent utilisé pour les applications qui nécessitent une vitesse plus élevée et une fourniture de données prioritaire et en temps réel, telles que Voice over IP (voix sur IP ; VoIP), la diffusion audio et vidéo en continu et les jeux en ligne. UDP est orienté transaction ; par conséquent, il est également utilisé pour les applications qui répondent à des requêtes peu volumineuses de nombreux clients, telles que Domain Name System (système de noms de domaine ; DNS) et Trivial File Transfer Protocol (protocole simplifié de transfert de fichiers ; TFTP).

Vous pouvez utiliser les Profil de protection de zone sur le pare-feu pour configurer flood protection (protection contre la saturation) et ainsi spécifier le débit de connexions UDP par seconde (ne correspondant pas à une session existante) qui déclenche une alarme, déclenche l'abandon aléatoire de paquets UDP par le pare-feu et cause l'abandon par le pare-feu des paquets UDP qui dépassent le taux maximal. (Même si UDP fonctionne sans connexion, le pare-feu trace les datagrammes UDP dans des paquets IP pour chaque session. Ainsi, si le paquet UDP ne correspond pas à une session existante, il est considéré comme une nouvelle session et il compte comme une connexion pour les seuils.)

 ©2024 Palo Alto Networks, Inc.

ICMP

ICMP (Internet Control Message Protocol) (RFC 792) est un autre protocole principal de la suite Internet Protocol qui fonctionne au niveau de la couche réseau du modèle OSI. ICMP est utilisé à des fins de diagnostic et de contrôle, pour envoyer des messages d'erreur sur les opérations IP, des messages sur les services demandés ou sur l'accessibilité d'un hôte ou d'un routeur. Des utilitaires réseau tels que traceroute et ping sont implémentés en utilisant divers messages ICMP.

ICMP est un protocole sans connexion qui n'ouvre ni ne gère aucune session réelle. Toutefois, les messages ICMP entre deux périphériques peuvent être considérés comme une session.

Les pare-feux Palo Alto Networks® prennent en charge ICMPv4 et ICMPv6. Vous pouvez contrôler les paquets ICMPv4 et ICMPv6 de plusieurs façons :

- Créez les Règles de politique de sécurité basées sur les paquets ICMP et ICMPv6 et sélectionnez l'application **icmp** ou **ipv6-icmp** dans la règle.
- Contrôlez la Limitation du débit ICMPv6 lorsque vous procédez à la Configuration des paramètres de session.
- Configurez Flood Protection (protection contre la saturation), en indiquant le taux des connexions ICMP ou ICMPv6 par seconde (ne correspondant pas avec une session existante) qui ont déclenché une alarme et l'abandon aléatoire par le pare-feu des paquets ICMP ou ICMPv6 et amené le pare-feu à abandonner les paquets ICMP ou ICMPv6 qui dépassent la taille maximale.
- Configurer Packet-Based Attack Protection (protection contre les attaques basées sur les paquets) :
  - Pour ICMP, vous pouvez abandonner certains types de paquets ou supprimer l'envoi de certains paquets.
  - Pour les paquets ICMPv6 (Types 1, 2, 3, 4 et137), vous pouvez indiquer que le pare-feu utilise la clé de session ICMP pour correspondre à une règle de politique de sécurité, qui détermine si le paquet ICMPv6 est autorisé ou non. (Le pare-feu utilise la règle de politique de sécurité pour appliquer un contrôle prioritaire sur le comportement par défaut et utiliser le paquet intégré pour déterminer une correspondance de session.) Lorsque le pare-feu abandonne des paquets ICMPv6 qui correspondent à une règle de politique de sécurité, le pare-feu journalise les détails and les journaux du trafic.

Règles de politique de sécurité basées sur les paquets ICMP et ICMPv6

Le pare-feu autorise l'envoi de paquets ICMP ou ICMPv6 seulement si une règle de politique de sécurité autorise la session (comme le fait le pare-feu pour d'autres types de paquets). Le pare-feu détermine une correspondance de session de deux façons, selon qu'il s'agit d'un paquet d'erreur ou un paquet redirigé ICMP ou ICMPv6, ou bien d'un paquet d'information.

- **ICMP Types 3, 5, 11, et 12 et ICMPv6 Types 1, 2, 3, 4 et 137** - par défaut, le pare-feu recherche dans le paquet IP intégré des octets d'information provenant du datagramme original ayant causé l'erreur (le paquet incriminé). Si une correspondance est établie entre le paquet intégré et une session existante, le pare-feu abandonne le paquet ICMP ou ICMPv6 conformément à l'action définie dans la règle de politique de sécurité correspondant à la

 ©2024 Palo Alto Networks, Inc.

session en question. (Vous pouvez utiliser Packet-Based Attack Protection (Protection en cas d'attaque basée sur les paquets) pour contourner le comportement par défaut des types d'ICMPv6.)

- **Types de paquets ICMP ou ICMPv6 restants** - le pare-feu traite le paquet ICMP ou ICMPv6 comme s'il faisait partie d'une nouvelle session. Si une règle de sécurité correspond à un paquet (que le pare-feu identifie comme une session **icmp** ou **icmpv6**), le pare-feu transmet ou abandonne le paquet conformément à l'action définie dans la règle de politique de sécurité. Les guichets des politiques de sécurité et les journaux de trafic reflètent ces actions.

  Si aucune règle de sécurité ne correspond à un paquet, le pare-feu applique sa règle de politique de sécurité par défaut, qui autorise le trafic intra-zone mais bloque le trafic interzone (par défaut, la journalisation est désactivée pour ces règles).

  Même si vous pouvez contourner les règles par défaut pour autoriser la journalisation ou changer l'action par défaut, il est déconseillé de modifier le comportement par défaut pour un cas précis car cela aura une incidence sur tout le trafic concerné par ces règles. Créez plutôt des règles de politique de sécurité qui contrôlent et enregistrent précisément les paquets ICMP ou ICMPv6.

  Il existe deux façons de créer des règles de politique de sécurité pour gérer les paquets ICMP ou ICMPv6 qui ne sont pas des paquets d'erreur ou des paquets redirigés.

  - **Créez une règle de politique de sécurité qui autorise (ou bloque) tous les paquets ICMP ou ICMPv6** : dans la règle de politique de sécurité, définissez l'application **icmp** ou **ipv6-icmp** ; le pare-feu autorise ou bloque tous les paquets IP correspondants, respectivement, au protocole numéro (1) ou au protocole numéro (58), à travers le pare-feu.
  - **Créez une application propre et une règle de politique de sécurité qui autorise (ou bloque) des paquets en provenance de ou vers l'application** : cette approche plus granulaire vous permet de ICMP spécifiques à la commande ou Types et Codes ICMPv6.

Limitation du débit ICMPv6

La limitation du débit ICMPv6 est un mécanisme de limitation permettant d'empêcher la saturation et les tentatives DDoS. L'implémentation utilise un nombre de paquets d'erreur et un seau à jetons, qui fonctionnent conjointement pour activer la limitation et s'assurer que les paquets ICMP ne saturent pas les segments de réseau protégés par le pare-feu.

D'abord, le **ICMPv6 Error Packet Rate (per sec) (Taux de paquets d'erreur ICMPv6 (par s))** global contrôle le débit auquel les paquets d'erreur ICMPv6 sont autorisés via le pare-feu (par défaut 100, plage entre 10 et 65 535 paquets par seconde). Si le pare-feu atteint le taux de paquets d'erreur ICMPv6, le seau à jetons entre en jeu et la limitation se produit comme suit.

Un seau à jetons logiques permet de contrôler le débit auquel les messages ICMP peuvent être transmis. Le nombre de jetons d'un seau peut être configuré, et chaque jeton représente un message ICMPv6 qui peut être envoyé. Le nombre de jetons est diminué chaque fois qu'un message ICMPv6 est envoyé ; lorsque le seau atteint zéro jeton, aucun autre message ICMPv6 ne peut être envoyé jusqu'à ce qu'un autre jeton soit ajouté au seau (taille par défaut du seau à jetons : 100 jetons ; plage entre 10 et 65 535 jetons).

Pour modifier la taille du seau à jetons ou le taux de paquets d'erreur par défaut, reportez-vous à la section Configuration des paramètres de session.

 ©2024 Palo Alto Networks, Inc.

ICMP spécifiques à la commande ou Types et Codes ICMPv6

Cette tâche vous permet de créer une application ICMP ou ICMPv6 personnalisée et de créer une règle de politique de sécurité pour autoriser ou refuser cette application.

STEP 1 | Créez une application personnalisée pour les codes et les types de message ICMP ou ICMPv6.

1. Sélectionnez **Object (Objet)** > **Applications (Applications)**, puis **Add (Ajoutez)** une application personnalisée.
2. À l'onglet **Configuration (Configuration)**, donnez un **Name (Nom)** et une **Description (Description)** à l'application personnalisée. Par exemple, entrez le nom ping6.
3. Sous **Category (Catégorie)**, sélectionnez **networking (mise en réseau)**.
4. Sous **Subcategory (Sous-catégorie)**, sélectionnez **ip-protocol (protocole IP)**.
5. Sous **Technology (Technologie)**, sélectionnez **network-protocol (protocole réseau)**.
6. Cliquez sur **OK**.
7. À l'onglet **Advanced (Avancé)**, sélectionnez **ICMP Type (Type ICMP)** ou **ICMPv6 Type (Type ICMPv6)**.
8. Sous **Type (Type)**, saisissez le numéro (plage comprise entre 0 et 255) qui désigne le type de message ICMP ou ICMPv6 que vous souhaitez autoriser ou refuser. Par exemple, le numéro d'un message de demande d'écho (ping) est 128.
9. Si le Type comprend des codes, indiquez le numéro du **Code (Code)** (plage comprise entre 0 et 255) qui s'applique au **Type (Type)** que vous souhaitez autoriser ou refuser. Certains **Type (Types)** ne permettent que le Code 0.
10. Cliquez sur **OK**.

STEP 2 | Créez une règle de politique de sécurité qui autorise ou refuse l'application personnalisée que vous avez créée.

Création d'une règle de politique de sécurité. À l'onglet **Application (Application)**, précisez le nom de l'application personnalisée que vous venez de créer.

STEP 3 | Validez vos modifications.

Cliquez sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

Configuration des délais d'expiration de session

Un délai d'expiration de session définit la durée pendant laquelle PAN-OS maintient une session sur le pare-feu après son inactivité. Par défaut, lorsque le délai du protocole expire, PAN-OS ferme la session. Vous pouvez définir plus particulièrement un délai d'expiration pour les sessions TCP, UDP et ICMP. Le délai d'expiration par défaut s'applique à tout autre type de session. Les délais d'expiration sont globaux, ce qui signifie qu'ils s'appliquent à toutes les sessions de ce type sur le pare-feu.

Vous pouvez également configurer un paramètre d'expiration du cache ARP, qui contrôle la durée pendant laquelle le pare-feu conserve les entrées ARP (mappages des adresses IP aux adresses matérielles) dans son cache.

Outre les paramètres généraux, vous pouvez définir des délais d'expiration pour une application particulière dans l'onglet **Objects (Objets)** > **Applications**. Le pare-feu applique les délais d'expiration d'application à une application qui se trouve dans un état établi. Une fois configurés, les délais d'expiration d'une application remplacent les délais d'expiration de session TCP ou UDP généraux.

Si vous modifiez les minuteurs TCP ou UDP au niveau de l'application, ces minuteurs pour les applications prédéfinies ou les applications personnalisées partagées seront appliqués à l'ensemble des systèmes virtuels. Si vous avez besoin que les minuteurs d'une application soient différents pour un système virtuel, vous devez créer une application personnalisée, lui affecter des minuteurs uniques, puis affecter l'application personnalisée à un système virtuel unique.

Effectuez les tâches facultatives suivantes si vous devez modifier les valeurs par défaut des paramètres d'expiration de session globaux pour TCP, UDP, ICMP, l'authentification du portail captif ou d'autres types de sessions. Toutes les valeurs sont en secondes.

Les valeurs par défaut sont optimales. Toutefois, vous pouvez les modifier selon vos besoins en matière de réseau. La définition d'une valeur trop faible peut engendrer une certaine sensibilité aux retards mineurs sur le réseau et une impossibilité d'établir une connexion avec le pare-feu, tandis qu'une valeur trop élevée peut entraîner un retard dans la détection des échecs.

STEP 1 | Accédez aux délais d'expiration de session.

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les délais d'expiration de session.

STEP 2 | (Facultatif) Modifiez les délais d'expiration divers.

- **Default** (Par défaut) : durée maximale pendant laquelle une session non TCP/UDP ou non ICMP peut être ouverte sans aucune réponse (plage entre 1 et 15 999 999, par défaut 30).
- **Discard Default** (Sessions en état de rejet par défaut) : durée maximale pendant laquelle une session non TCP/UDP reste ouverte après que PAN-OS l'a refusée en fonction

 ©2024 Palo Alto Networks, Inc.

des politiques de sécurité configurées sur le pare-feu (plage entre 1 et 15 999 999, par défaut 60).

- **Scan** (Analyse) : durée maximale pendant laquelle une session reste ouverte après qu'elle a été considérée comme inactive ; une application est considérée comme inactive lorsqu'elle dépasse le seuil de ruissellement d'application défini (plage entre 5 et 30, par défaut 10).
- **Authentication Portal (Portail d'authentification)** : délai d'expiration de session d'authentification du formulaire Web du portail captif. Pour accéder au contenu demandé, l'utilisateur doit saisir les informations d'identification d'authentification dans ce formulaire et être authentifié avec succès (plage entre 1 et 15 999 999, par défaut 30).
- Pour définir d'autres délais d'expiration de Portail d'authentification, tels que le minuteur d'inactivité et le délai d'expiration avant la réauthentification de l'utilisateur, sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Authentication Portal Settings (Paramètres du Portail d'authentification)**. Reportez-vous à la section Configuration du portail d'authentification.

STEP 3 | (Facultatif) Modifiez les délais d'expiration TCP.

- **Sessions TCP en état de rejet** : durée maximale pendant laquelle une session TCP reste ouverte après qu'elle ait été refusée en fonction d'une politique de sécurité configurée sur le pare-feu. La plage est comprise entre 1 et 15,999,999 ; la valeur par défaut est 90.
- **TCP** : durée maximale pendant laquelle une session TCP reste ouverte sans aucune réponse, une fois qu'elle se trouve dans un état établi (après que la liaison ait été établie et/ou que les données aient été transmises). La plage est comprise entre 1 et 15 999 999 ; la valeur par défaut est 3 600.
- **Établissement de liaison TCP** : durée maximale autorisée entre la réception du paquet SYN-ACK et le paquet ACK suivant pour établir la session. La plage est comprise entre 1 et 60 ; la valeur par défaut est 10.
- **Initialisation TCP** : durée maximale autorisée entre la réception du paquet SYN et le paquet SYN-ACK avant de démarrer le minuteur d'établissement de liaison TCP. La plage est comprise entre 1 et 60 ; la valeur par défaut est 5.
- **Sessions TCP à moitié fermées** : durée maximale entre la réception du premier paquet FIN et celle du second paquet FIN ou RST. La plage est comprise entre 1 et 604,800 ; la valeur par défaut est 120.
- **Sessions TCP en état time_wait** : durée maximale après la réception du second paquet FIN ou RST. La plage est comprise entre 1 et 600 ; la valeur par défaut est 15.
- **RST non vérifié** : durée maximale après la réception d'un paquet RST qui ne peut pas être vérifié (le paquet RST se trouve dans la fenêtre TCP, mais dispose d'un numéro de séquence inattendu ou provient d'un chemin asymétrique). La plage est comprise entre 1 et 600 ; la valeur par défaut est 30.
- Consultez également les délais d'expiration **Scan (Analyse)** à la section (Facultatif) Modifiez les délais d'expiration divers.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | (Facultatif) Modifiez les délais d'expiration UDP.

- **Sessions UDP en état de rejet** : durée maximale pendant laquelle une session TCP reste ouverte après qu'elle ait été refusée en fonction d'une politique de sécurité configurée sur le pare-feu. La plage est comprise entre 1 et 15,999,999 ; la valeur par défaut est 60.
- **UDP** : durée maximale pendant laquelle une session UDP reste ouverte sans aucune réponse UDP. La plage est comprise entre 1 et 15,999,999 ; la valeur par défaut est 30.
- Consultez également les délais d'expiration **Scan (Analyse)** à la section (Facultatif) Modifiez les délais d'expiration divers.

STEP 5 | (Facultatif) Modifiez les délais d'expiration ICMP.

- **ICMP** : durée maximale pendant laquelle une session ICMP peut être ouverte sans aucune réponse ICMP. La plage est comprise entre 1 et 15,999,999 ; la valeur par défaut est 6.
- Consultez également les délais d'expiration **Discard Default (Sessions en état de rejet par défaut)** et **Scan (Analyse)** à la section (Facultatif) Modifiez les délais d'expiration divers.

STEP 6 | Cliquez sur **OK**, puis sur **Commit (Valider)**.

STEP 7 | (Facultatif) Modifiez les délais d'expiration du cache ARP.

1. Accédez à la CLI et précisez le nombre de secondes pendant lesquelles le pare-feu conserve les entrées ARP dans son cache. Utilisez la commande opérationnelle **`set system setting arp-cache-timeout`** <*valeur*>, où la plage se situe entre 60 et 65 535 ; et la valeur par défaut est 1 800.

   Si vous diminuez le délai d'expiration et que les entrées existantes dans le cache possèdent une TTL supérieure au nouveau délai d'expiration, le pare-feu supprime ces entrées et actualise le cache ARP. Si vous augmentez le délai d'expiration et que les entrées existantes dans le cache possèdent une TTL inférieure au nouveau délai d'expiration, elles expirent selon la TTL et le pare-feu met en cache les nouvelles entrées en se basant sur la valeur de temporisation le plus importante.
2. Affichez le paramètre d'expiration du cache ARP avec la commande de la CLI opérationnelle **`show system setting arp-cache-timeout`**.

 ©2024 Palo Alto Networks, Inc.

Configuration des paramètres de session

Cette rubrique décrit les divers paramètres des sessions autres que les valeurs de délai d'expiration. Effectuez ces tâches si vous devez modifier les paramètres par défaut.

STEP 1 | Modifiez les paramètres de session.

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les Session Settings (Paramètres de session).

STEP 2 | Précisez s'il faut appliquer les nouvelles règles de politique de sécurité configurées aux sessions en cours.

Sélectionnez **Rematch all sessions on config policy change (Revérifier toutes les sessions après modification de la politique de configuration)** pour appliquer les nouvelles règles de politique de sécurité configurées aux sessions en cours. Cette option est activée par défaut. Si vous décochez cette case, toute modification de règle de politique que vous apportez s'appliquera uniquement aux sessions initiées après que vous avez validé le changement.

Par exemple, si une session Telnet commence alors qu'une règle de politique associée a été configurée pour autoriser Telnet et que vous validez par la suite une modification de politique pour refuser Telnet, le pare-feu applique la politique révisée à la session en cours et la bloque.

STEP 3 | Configuration des paramètres IPv6.

- **ICMPv6 Token Bucket Size (Taille du seau à jetons ICMPv6)** : par défaut : 100 jetons. Reportez-vous à la section Limitation du débit ICMPv6.
- **ICMPv6 Error Packet Rate (per sec) (Taux de paquets d'erreur ICMPv6 (par s))** : par défaut : 100. Reportez-vous à la section Limitation du débit ICMPv6.
- **Enable IPv6 Firewalling (Activer le pare-feu IPv6)** : active les fonctionnalités du pare-feu pour IPv6. Toutes les configurations basées sur IPv6 sont ignorées si l'option IPv6 est désactivée. Même si IPv6 est activé pour une interface, le paramètre **IPv6 Firewalling (Activer le pare-feu IPv6)** doit également être sélectionné pour qu'IPv6 fonctionne.

STEP 4 | Activez les trames Jumbo et définissez la MTU.

1. Sélectionnez **Enable Jumbo Frame (Activer les trames Jumbo)** pour activer la prise en charge des trames Jumbo sur les interfaces Ethernet. Les trames Jumbo disposent d'une unité de transmission maximale (MTU) de 9,216 octets et sont disponibles sur certains modèles uniquement.

 ©2024 Palo Alto Networks, Inc.

2. Définissez la **Global MTU (MTU globale)**, selon que vous voulez activer ou non les trames Jumbo :
   - Si vous n'avez pas activé les trames Jumbo, la **Global MTU (MTU globale)** est de 1 500 octets par défaut et la plage est comprise entre 576 et 1 500 octets.
   - Si vous avez activé les trames Jumbo, la **Global MTU (MTU globale)** est de 9 192 octets par défaut et la plage est comprise entre 9 192 et 9 216 octets.

   Les trames Jumbo peuvent utiliser jusqu'à cinq fois plus de mémoire que les paquets normaux et peuvent réduire le nombre de mémoires tampons des paquets disponibles de 20 %. Ceci réduit la taille de la file d'attente dédiée aux tâches hors service et d'identification des applications, ainsi qu'aux autres tâches similaires de traitement des paquets. Depuis PAN-OS 8.1, si vous activez la configuration MTU globale de trames jumbo et redémarrez votre pare-feu, les mémoires tampons des paquets sont alors redistribuées pour traiter les trames jumbo plus efficacement.

   Si vous activez les trames Jumbo et qu'une MTU spécifique n'est pas configurée sur certaines interfaces, ces dernières héritent automatiquement de la taille de trame Jumbo. Par conséquent, avant d'activer les trames Jumbo, si vous ne souhaitez pas qu'une interface ait des trames Jumbo, vous devez définir la MTU de cette interface sur 1 500 octets ou une autre valeur.

   *Si vous importez (**Device (Périphérique)** > **Setup (configuration)** > **Operations (Opérations)** > **Import (Importer)**) et chargez une configuration sur laquelle Jumbo Frame est activé, puis que vous validez avec un pare-feu sur lequel Jumbo Frame n'est pas encore activé, le **Enable Jumbo Frame (paramètre Activer Jumbo Frame)** n'est pas validé dans la configuration. Vous devez d'abord **Enable Jumbo Frame (activer Jumbo Frame)**, redémarrer, puis importer, charger et valider la configuration.*

STEP 5 | Ajustez les paramètres de session NAT.

- **NAT64 IPv6 Minimum Network MTU (MTU IPv6 min. pour le réseau NAT64)** : définit la MTU globale du trafic traduit en IPv6. La valeur par défaut de 1 280 octets est basée sur la MTU minimum standard du trafic IPv6.
- **NAT Oversubscription Rate (Taux de sursouscription NAT)** : si la traduction NAT est configurée pour être une traduction Dynamic IP and Port (adresse IP et port dynamiques ; DIPP), un taux de sursouscription peut être défini pour multiplier le nombre de fois que la même adresse IP traduite et la paire de ports peuvent être utilisées simultanément. Le taux est de 1, 2, 4 ou 8. Le paramètre par défaut est défini en fonction du modèle du pare-feu.
- Un taux de 1 signifie qu'aucun dépassement d'abonnement n'est effectué ; chaque adresse IP traduite et paire de ports ne peut être utilisée qu'une à la fois.
- Si ce paramètre est **Platform Default (Valeur par défaut de la plate-forme)**, la configuration du taux de dépassement d'abonnement par l'utilisateur est désactivée et le taux de dépassement d'abonnement par défaut du modèle s'applique.

La réduction du taux de dépassement d'abonnement diminue le nombre de traductions de périphérique source, mais augmente le nombre de règles NAT.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Ajustez les paramètres de vieillissement accéléré.

Sélectionnez **Accelerated Aging (Vieillissement accéléré)** pour permettre d'accélérer le vieillissement des sessions inactives. Vous pouvez également modifier le seuil (%) et le facteur d'échelle :

- **Accelerated Aging Threshold (Seuil du vieillissement accéléré)** : pourcentage de la capacité de la table de sessions lorsque le vieillissement accéléré commence. La valeur par défaut est de 80 % Lorsque la table de sessions atteint ce seuil (% de sa capacité), PAN-OS applique le facteur d'échelle du vieillissement accéléré aux calculs de vieillissement de toutes les sessions.
- **Accelerated Aging Scaling Factor (Facteur d'échelle du vieillissement accéléré)** : facteur d'échelle utilisé dans les calculs de vieillissement accéléré. Le facteur d'échelle par défaut est de 2, ce qui signifie que le vieillissement accéléré se produit à un taux deux fois plus élevé que la durée d'inactivité configurée. La durée d'inactivité configurée divisée par 2 a pour conséquence un délai plus court réduit de 50 %. Pour calculer le vieillissement accéléré de la session, PAN-OS divise la durée d'inactivité configurée (pour ce type de session) par le facteur d'échelle afin de déterminer un délai plus court.

Par exemple, si le facteur d'échelle est de 10, une session qui expirerait normalement au bout de 3 600 secondes expirerait 10 fois plus vite (en 1/10e du temps), c'est-à-dire au bout de 360 secondes.

STEP 7 | Activez la protection de la mémoire tampon des paquets.

1. Sélectionnez **Packet Buffer Protection (Protection de la mémoire tampon des paquets)** pour permettre au pare-feu de prendre des mesures contre les sessions qui risquent de submerger la mémoire tampon des paquets et qui entraînent l'abandon du trafic légitime ; activé par défaut.
2. Si vous activez la protection de la mémoire tampon des paquets, vous pouvez préciser les seuils et les minuteurs qui indiquent la réponse du pare-feu à un abus de la mémoire tampon des paquets.
   - **Alert (%) (Alerte (%))** : lorsque l'utilisation de la mémoire tampon des paquets dépasse ce seuil, le pare-feu crée un événement de journal. Le seuil par défaut est de 50 % et la plage est comprise entre 0 % et 99 %. Si la valeur est définie sur 0 %, le pare-feu ne crée pas de journaux d'événements.
   - **Activate (%) (Activer (%))** : lorsque l'utilisation de la mémoire tampon des paquets dépasse ce seuil, le pare-feu applique le Random Early Drop (Abandon anticipé aléatoire ; RED) aux sessions abusives. Le seuil par défaut est de 80 % et la plage est comprise entre 0 % et 99 %. Si la valeur est définie sur 0 %, le pare-feu n'applique pas la RED.

     Les événements d'alerte sont consignés dans le journal du système. Les événements relatifs à l'abandon de trafic, au rejet de sessions et au blocage d'adresses IP sont consignés dans le journal des menaces.

   - **Block Hold Time (sec) (Délai de maintien du blocage (sec.))** : la période pendant laquelle une session atténuée par la RED est autorisée à se poursuivre avant qu'elle ne soit abandonnée. Par défaut, le délai de maintien du blocage est de 60 secondes. La plage est comprise entre 0 et 65 535 secondes. Si la valeur est définie sur 0, le

 ©2024 Palo Alto Networks, Inc.

pare-feu n'abandonne pas les sessions en fonction de la protection de la mémoire tampon des paquets.

- **Block Duration (sec) (Période de blocage (sec.))** : ce paramètre définit la durée pendant laquelle une session est rejetée ou une adresse IP est bloquée. La valeur par défaut est de 3 600 secondes avec une plage allant de 0 seconde à 15 999 999 secondes. Si cette valeur est de 0, le pare-feu n'abandonne pas les sessions ou ne bloque pas les adresses IP en fonction de la protection de la mémoire tampon des paquets.

STEP 8 | Activez la mise en tampon des paquets de configuration de route multidiffusion.

1. Sélectionnez **Multicast Route Setup Buffering (Mise en tampon de configuration de route multidiffusion)** pour permettre au pare-feu de préserver le premier paquet dans une session multidiffusion lorsque l'entrée de la route multidiffusion ou de la Forwarding Information Base (base d'informations de transfert ; FIB) n'existe pas encore pour le groupe multidiffusion correspondant. Par défaut, le pare-feu ne procède pas à la mise en tampon du premier paquet multidiffusion dans une nouvelle session ; il utilise plutôt le premier paquet pour paramétrer la route multidiffusion. Ce comportement est normal pour le trafic multicast. Si vos serveurs de contenu sont directement connectés au pare-feu et que votre application personnalisée ne peut pas prendre en charge le premier paquet dans la session en cours de suppression, vous n'avez qu'à activer la mise en tampon de configuration de route multidiffusion. Cette option est désactivée par défaut.
2. Si vous activez la mise en tampon, vous pouvez également ajuster la **Buffer Size (Taille de tampon)**, qui précise la taille de tampon par flux. Le pare-feu peut mettre en tampon un maximum de 5 000 paquets.

*Vous pouvez également ajuster le délai, en secondes, pendant lequel un itinéraire multidiffusion demeure dans la table de routage sur le pare-feu à la fin de la session en configurant les paramètres de multidiffusion sur le routeur virtuel qui gère votre routeur virtuel (définissez les **Multicast Route Age Out Time (sec) (Paramètres d'expiration de l'itinéraire multidiffusion (sec))** à l'onglet **Multicast (Multidiffusion)** > **Advanced (Avancé)** de la configuration du routeur virtuel.*

STEP 9 | Enregistrez les paramètres de session.

Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 10 | Ajustez les paramètres de Maximum Segment Size (taille de segment maximale ; MSS) applicables à une interface de Couche 3.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)**, sélectionnez **Ethernet (Ethernet)**, **VLAN (VLAN)** ou **Loopback (En boucle)**, puis sélectionnez une interface de Couche 3.
2. Sélectionnez **Advanced (Avancé)** > **Other Info (Autres informations)**.
3. Sélectionnez **Adjust TCP MSS (Ajuster TCP MSS)**, puis saisissez une valeur pour l'un des éléments suivants, ou pour les deux :
   - **IPv4 MSS Adjustment Size (Taille d'ajustement MSS IPv64)** (intervalle compris entre 40 et 300 octets ; valeur par défaut : 40 octets).
   - **IPv6 MSS Adjustment Size (Taille d'ajustement MSS IPv64)** (intervalle compris entre 60 et 300 octets ; valeur par défaut : 60 octets).
4. Cliquez sur **OK**.

STEP 11 | Validez vos modifications.

Cliquez sur **Commit (Valider)**.

STEP 12 | Redémarrez le pare-feu après avoir modifié la configuration de la trame Jumbo.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**.
2. Cliquez sur **Reboot Device (Redémarrer le périphérique)**.

 ©2024 Palo Alto Networks, Inc.

Politiques de Distribution de Sessions

Les politiques de distribution de sessions définissent comment les pare-feu des séries PA-5200, PA-7000 et PA-7500 distribuent des processus de sécurité (App-ID, Content-ID, filtrage des URL, décryptage SSL, et IPSec) entre des processeurs de plan de données (DP) sur le pare-feu. Chaque politique est conçue spécifiquement pour un environnement de réseau donné et une configuration de pare-feu donnée, pour permettre au pare-feu de distribuer des sessions avec une efficacité maximale. Par exemple, une politique de distribution de sessions avec fonction de hachage correspond mieux aux environnements utilisant des NAT sources de grande échelle.

La quantité de DP sur un pare-feu varie selon le modèle de pare-feu :

Firewall Model (Modèle de pare-feu)	Processeur(s) de plan de données
Série PA-7500	Dépend du nombre de cartes de traitement de données (DPC) installées. Chaque DPC dispose de six processeurs de plan de données. *Lorsque les pare-feu de la série PA-7500 sont des nœuds dans un cluster NGFW, les nœuds doivent utiliser le même type de politique de distribution de session (fixe, hachage, emplacement d'entrée, aléatoire, round-robin, charge de session ou hachage symétrique).*
PA-7000 Series	Dépend du nombre de cartes de traitement du réseau (NPC). Chaque NPC compte de multiples processeurs de plan de données (DP) et vous pouvez installer de multiples NPC sur le pare-feu.
Pare-feu PA-5220	1 *Le pare-feu PA-5220 ne compte qu'un seul DP, donc les politiques de distribution de sessions n'ont pas d'importance. Laissez la politique définie par défaut (round-robin).*
Pare-feu PA-5250	2
Pare-feu PA-5260 et PA-5280	3
Pare-feu PA-5450	Dépend du nombre de cartes de traitement de données (DPC) installées.

Les rubriques suivantes fournissent des informations sur les politiques de distribution de sessions disponibles, sur la manière de modifier une politique active et sur la manière d'afficher les statistiques de distribution de sessions.

 ©2024 Palo Alto Networks, Inc.

- Descriptions des Politiques de Distribution de Sessions
- Modification des Politiques de Distribution de Sessions et Affichage des Statistiques

Descriptions des Politiques de Distribution de Sessions

Le tableau suivant fournit des informations sur les Politiques de Distribution de Sessions pour vous aider à choisir quelle politique correspond le mieux à votre environnement et à la configuration de votre pare-feu.

Politique de Distribution de Sessions	Description
Fixe	Vous permet de définir le processeur de plan de données (DP) que le pare-feu va utiliser pour les processus de sécurité. Utilisez cette politique à des fins de débogage.
Hachage	Le pare-feu distribue des sessions basées sur le hachage d'une adresse source et d'une adresse de destination. La distribution basée sur le hachage améliore l'efficacité de la gestion de ressources pour les adresses NAT, et réduit la latence pour la configuration de session NAT en évitant les éventuels conflits de port ou d'adresse. Utilisez cette politique dans des environnements utilisant des NAT sources de grande échelle avec traduction de l'IP dynamique, traduction du port et de l'IP dynamique, ou les deux. Si vous utilisez la traduction de l'IP dynamique, sélectionnez l'option adresse **`source`**. Si vous utilisez la traduction de l'IP dynamique et du port, sélectionnez l'option adresse **`destination`**.
Ingres-slot (par défaut sur les pare-feu PA-7000 Series)	(Pare-feu PA-7000 Series uniquement) Les nouvelles sessions sont affectées au DP de la NPC sur laquelle le premier paquet de la session est arrivé. Le choix du DP est basé sur l'algorithme session-load mais, dans ce cas précis, les sessions sont limitées aux DP sur les entrées NPC. Selon le trafic et la topologie du réseau, cette politique réduit généralement la probabilité que le trafic doive traverser la matrice de commutation. Utilisez cette politique pour réduire la latence si l'entrée et la sortie se trouvent toutes deux sur la même NPC. Si le pare-feu compte un mélange de NPC (comme le PA-700020G et le PA-7000 20GXM, par exemple), cette politique peut isoler la capacité accrue au NPC

 ©2024 Palo Alto Networks, Inc.

Politique de Distribution de Sessions	Description
	correspondant et aider à isoler l'impact des défaillances de NPC.
Aléatoire	Le pare-feu choisit de manière aléatoire un DP pour les traitements de session.
Round-robin (par défaut sur les pare-feu PA-5200 Series)	Le pare-feu sélectionne le DP basé sur l'algorithme round-robin parmi des plans de données actifs, afin que les saisies, les résultats ainsi que les fonctions de processus de sécurité soient partagés entre tous les plans de données. Utilisez cette politique dans des environnements aux exigences faibles à moyennes, où un algorithme d'équilibrage de la charge, simple et prévisible, est suffisant. Dans des environnements très exigeants, nous vous recommandons d'utiliser un algorithme à répartition de session.
Répartition de session	Cette politique est semblable à la politique round-robin mais elle utilise un algorithme pondéré pour déterminer comment distribuer les sessions et atteindre un équilibre parmi les DP. À cause des variables affectant la durée de vie d'une session, les DP ne peuvent pas toujours connaître une charge équilibrée. Par exemple, si le pare-feu compte trois DP et que DP0 est à 25% de ses capacités, DP1 à 25% et DP2 à 50%, une attribution de nouvelle session sera pondérée vers le DP avec les capacités les plus faibles. Cela permet d'améliorer l'équilibrage de charge sur le long terme. Utilisez cette politique dans des environnements où les sessions sont distribuées à travers de nombreux emplacements de NPC, comme dans un groupe d'interfaces agrégé inter-emplacements, ou des environnements avec une transmission asymétrique. Vous pouvez également utiliser cette politique ou la politique avec emplacements d'entrée si le pare-feu compte une combinaison de NPC avec différentes capacités de sessions (comme une combinaison de NPC PA-7000 20G et PA-7000 20GXM).
Hachage symétrique	(Pare-feu PA-5200 Series et PA-7000 Series fonctionnant sous PAN-OS 8.0 ou ultérieur) Le pare-feu sélectionne le DP par un hachage d'adresses IP sources et destinations triées. Cette politique fournit les mêmes résultats pour

©2024 Palo Alto Networks, Inc.

Politique de Distribution de Sessions	Description
	du trafic serveur-client (s2c) et client-serveur c2s) (en supposant que le pare-feu n'utilise pas NAT). Utilisez cette politique pour des déploiements GTP ou IPSec à exigences élevées. Avec ces protocoles, chaque direction est traitée comme un flot unidirectionnel où les tuples du flot ne peuvent pas être dérivés les uns des autres. Cette politique améliore la performance et réduit la latence en veillant à ce que les deux directions soient assignées au même DP, éliminant ainsi le besoin de communication entre DP.

Modification des Politiques de Distribution de Sessions et Affichage des Statistiques

Le tableau suivant décrit comment afficher et modifier les politiques de distribution de session et comment afficher les statistiques de sessions associées à chaque Dataplane Processor (processeur du panneau de données ; DP) du pare-feu.

Tâche	Commande
Afficher la politique de distribution de session active.	Utilisez la commande **show session distribution policy** pour afficher la politique de distribution de session active. Le résultat suivant est obtenu d'un pare-feu PA-7080 disposant de quatre NPC, installées dans les fentes 2, 10, 11 et 12 et dont la politique de distribution des logements d'entrée est activée : **> afficher la politique de Distribution de Sessions** Politique de répartition de la propriété : fente d'entrée Cartes de ligne compatibles avec le flux : [2, 10, 11, 12]Cartes de ligne activées pour le traitement des paquets : [2, 10, 11, 12]
Modifier la politique de distribution de session active.	Utilisez la commande **set session distribution-policy *<politique>*** pour modifier la politique de distribution de session active. Par exemple, pour sélectionner la politique de partage de charge de session, saisissez la commande suivante :

©2024 Palo Alto Networks, Inc.

Tâche	Commande
	`> définir la distribution-stratégie de session-load` *Lorsque les pare-feu de la série PA-7500 sont des nœuds dans un cluster NGFW, les nœuds doivent utiliser le même type de politique de distribution de session (fixe, hachage, emplacement d'entrée, aléatoire, round-robin, charge de session ou hachage symétrique).*
Afficher les statistiques relatives aux sessions de distribution.	Utilisez la commande **`show session distribution statistics`** pour afficher les Dataplane Processors (processeur de panneau de données ; DP) sur le pare-feu et le nombre de sessions sur chaque DP actif. Le résultat suivant provient d'un pare-feu PA-7080 : `> afficher les statistiques de distribution de session DP Active Dispatched Dispatched/sec ---------- s1dp0 78698 7829818 1473 s1dp1 78775 7831384 1535 s3dp0 7796 736639 1488 s3dp1 7707 737026 1442` La `DP Active column` énumère chaque plan de données des NPC installées. Les deux premiers caractères indiquent le numéro de fente et les trois derniers indiquent le numéro de plan de données. Par exemple, s1dp0 indique qu'il s'agit du plan de données 0 de la NPC qui se trouve dans la fente 1 et s1dp1 indique qu'il s'agit du plan de données 1 de la NPC qui se trouve dans la fente 1. La colonne `Dispatched` présente le nombre totale de sessions que le plan de données a traitées depuis le dernier redémarrage du pare-feu. La colonne `Dispatched/sec` indique le taux de répartition. Si vous additionnez les chiffres qui sont indiqués dans la colonne `Dispatched`, le total obtenu équivaut au nombre de sessions qui sont actives sur le pare-feu. Vous pouvez également visualiser le nombre total de sessions actives en exécutant la commande **`show session info CLI`**. *Le résultat obtenu d'un pare-feu PA-5200 Series sera semblable, sauf que le nombre de DP dépend du modèle et que la NPC ne possède qu'une seule fente.*

 ©2024 Palo Alto Networks, Inc.

Prévention de l'établissement de la session de liaison de segmentation TCP

Vous pouvez configurer un Abandon de l'établissement de liaison de segmentation TCP dans un profil de protection de zone pour empêcher l'établissement des sessions TCP, à moins qu'elles n'utilisent l'établissement de liaison en trois étapes standard. Cela suppose que vous avez affecté une zone de sécurité à l'interface pour laquelle vous souhaitez empêcher l'établissement de liaison de segmentation TCP.

STEP 1 | Configurez un profil de protection de zone pour empêcher les sessions TCP qui utilisent une autre méthode que l'établissement de liaison en trois étapes.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)**, puis cliquez sur **Add (Ajouter)** pour créer un nouveau profil (ou sélectionnez un profil existant).
2. Si vous créez un nouveau profil, saisissez un **Name (Nom)** pour le profil et éventuellement une **Description (Description)**.
3. Sélectionnez **Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)** > **TCP Drop (Abandon TCP)** puis sélectionnez **Split Handshake (Établissement de liaison de segmentation)**.
4. Cliquez sur **OK**.

STEP 2 | Appliquez le profil à une ou plusieurs zones de sécurité.

1. Sélectionnez **Network (Réseau)** > **Zones (Zones)**, puis choisissez la zone dans laquelle vous souhaitez affecter le profil de protection de zone.
2. Dans la liste **Zone Protection Profile (Profil de protection de zone)** de la fenêtre Zone, sélectionnez le profil que vous avez configuré à l'étape précédente.

   Sinon, vous pouvez commencer à créer un nouveau profil en cliquant sur **Zone Protection Profile (Profil de protection de zone)**, auquel cas continuez en conséquence.
3. Cliquez sur **OK**.
4. (Facultatif) Répétez les étapes 1 à 3 pour appliquer le profil à des zones supplémentaires.

STEP 3 | Validez vos modifications.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Inspection du contenu du tunnel

Le pare-feu peut inspecter le contenu du trafic des protocoles de tunnel en texte clair sans mettre fin au tunnel :

- Generic Routing Encapsulation (Encapsulation générique de routage ; GRE) (RFC 2784)
- Trafic IPsec non crypté [Algorithme de cryptage NULL pour IPsec (RFC 2410) et mode de transport IPsec AH]
- General Packet Radio Service (Service de paquets radio général ; GPRS) Protocole de mise en tunnel pour les données utilisateur (GTP-U)
- Virtual Extensible Local Area Network (un réseau local virtuel extensible ; VXLAN) (RFC 7348)

L'inspection du contenu des tunnels est effectuée pour les tunnels en texte clair, et non pour les tunnels VPN ou LSVPN, qui transportent du trafic crypté.

Vous pouvez utiliser l'inspection du contenu du tunnel pour appliquer les règles de sécurité, la Protection DoS et les politiques de trafic QoS dans ces types de tunnels et sur le trafic imbriqué dans un autre tunnel de texte en clair (par exemple, un tunnel IPsec crypté Null à l'intérieur d'un tunnel GRE). Vous pouvez consulter les journaux d'inspection de tunnel et l'activité du tunnel dans l'ACC pour vérifier que le trafic par tunnel est conforme aux politiques de sécurité et d'utilisation de votre entreprise.

Tous les modèles de pare-feu prennent en charge l'inspection du contenu des tunnels pour GRE, IPsec non crypté et les protocoles VXLAN. Seuls les pare-feu qui prennent en charge la sécurité GTP prennent en charge l'inspection du contenu du tunnel GTP-U. Voir les versions PAN-OS par modèle qui prennent en charge la sécurité GTP et SCTP dans la matrice de compatibilité.

Par défaut, les pare-feu pris en charge effectuent l'accélération du tunnel pour améliorer les performances et le débit du trafic passant par les tunnels GRE, VXLAN et GTP-U. L'accélération du tunnel permet de décharger le matériel afin de réduire le temps nécessaire pour effectuer les recherches de flux et de répartir plus efficacement le trafic du tunnel en fonction du trafic intérieur. Toutefois, vous pouvez Désactivation de l'accélération du tunnel pour le dépannage.

- Présentation de l'inspection du contenu du tunnel
- Configurer l'inspection du contenu du tunnel
- Afficher l'activité du tunnel inspecté
- Afficher les informations de tunnel dans les journaux
- Créer un rapport personnalisé basé sur le trafic de tunnel étiqueté
- Comportement d'accélération du tunnel
- Désactivation de l'accélération du tunnel

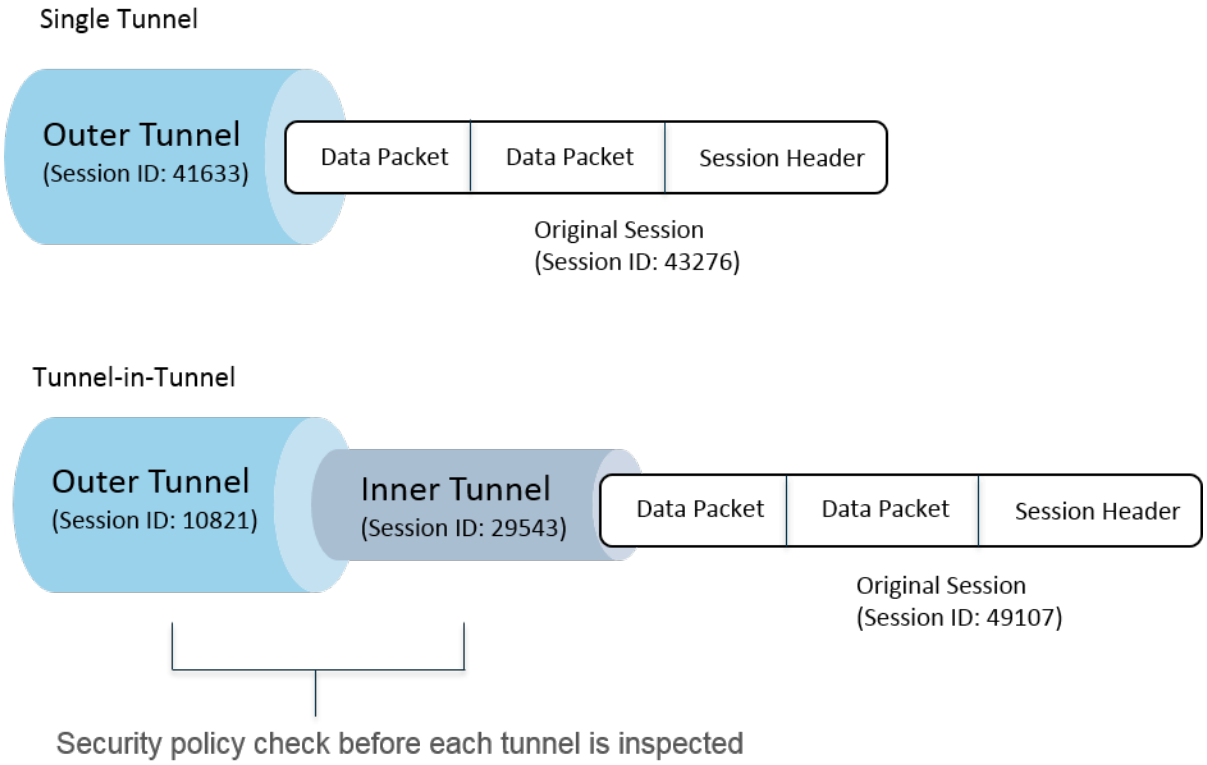
Présentation de l'inspection du contenu du tunnel

Votre pare-feu peut inspecter le contenu du tunnel n'importe où sur le réseau où vous n'avez pas la possibilité de terminer le tunnel d'abord. Tant que le pare-feu est dans le chemin d'un tunnel GTP-U, IPsec non crypté, GRE ou VXLAN, le pare-feu peut inspecter le contenu du tunnel.

- Les clients d'entreprise qui ont besoin de l'inspection du contenu du tunnel peuvent mettre en tunnel une partie ou la totalité du trafic avec GRE, VXLAN ou IPsec non crypté. Pour des raisons de sécurité, de QoS et de production de rapports, vous souhaiterez inspecter le trafic à l'intérieur du tunnel.
- Les clients du fournisseur de services utilisent GTP-U pour mettre en tunnel le trafic des appareils mobiles. Vous souhaitez inspecter le contenu interne sans arrêter le protocole de tunnel, et vous souhaitez enregistrer les données utilisateur de vos utilisateurs.

Le pare-feu prend en charge l'inspection du contenu du tunnel sur les interfaces Ethernet, les sous-interfaces, les interfaces AE, les interfaces VLAN et les interfaces de tunnel VPN et LSVPN. (Le tunnel en texte clair que le pare-feu inspecte peut se trouver dans un tunnel VPN ou LSVPN qui se termine au niveau du pare-feu, d'où l'interface de tunnel VPN ou LSVPN. En d'autres termes, lorsque le pare-feu est un point de terminaison VPN ou LSVPN, le pare-feu peut inspecter le trafic de tout protocole de tunnel non crypté que l'inspection du contenu du tunnel prend en charge.)

L'inspection du contenu du tunnel est prise en charge dans les interfaces de Couche 3, de Couche 2, le câble virtuel et les déploiements Tap. L'inspection du contenu du tunnel fonctionne sur les passerelles partagées et sur les communications de système vers système virtuel.



©2024 Palo Alto Networks, Inc.

L'illustration précédente illustre les deux niveaux d'inspection du tunnel que le pare-feu peut effectuer. Lorsqu'un pare-feu configuré avec des règles de politique d'inspection des tunnels reçoit un paquet :

- Le pare-feu détermine d'abord un contrôle de politique de sécurité pour déterminer si le protocole de tunnel (application) dans le paquet est autorisé ou refusé. (les paquets IPv4 et IPv6 sont des protocoles pris en charge à l'intérieur d'un tunnel.)
- Si la politique de sécurité autorise le paquet, le pare-feu fait correspondre le paquet à une règle de politique d'inspection des tunnels sur la base d'une zone source, d'une adresse source, d'un utilisateur source, d'une zone de destination et d'une adresse de destination. La règle de politique d'inspection des tunnels détermine les protocoles de tunnel que le pare-feu inspecte, le niveau maximum d'encapsulation autorisé (un seul tunnel ou un tunnel dans un tunnel), si les paquets contenant un protocole de tunnel ne passant pas l'inspection stricte des en-têtes selon RFC 2780 sont autorisés, et si les paquets contenant des protocoles inconnus sont autorisés.
- Si le paquet répond aux critères de correspondance de la règle de politique d'inspection des tunnels, le pare-feu inspecte le contenu interne, qui est soumis à votre politique de sécurité (requise) et aux politiques facultatives que vous pouvez spécifier. (Les types de politique pris en charge pour la session d'origine figurent dans le tableau suivant.)
- Si le pare-feu trouve un autre tunnel à la place, le pare-feu analyse par récursivité le paquet pour le deuxième en-tête et est maintenant au niveau deux d'encapsulation. Ainsi, la deuxième règle de politique d'inspection des tunnels, qui correspond à une zone de tunnel, doit autoriser un niveau d'inspection des tunnels maximal de deux niveaux pour que le pare-feu continue à traiter le paquet.
  - Si votre règle autorise deux niveaux d'inspection, le pare-feu effectue un contrôle de politique de sécurité sur ce tunnel intérieur, puis le contrôle de politique d'inspection des tunnels. Le protocole de tunnel que vous utilisez dans un tunnel intérieur peut différer du protocole de tunnel que vous utilisez dans le tunnel extérieur.
  - Si votre règle n'autorise pas deux niveaux d'inspection, le pare-feu adapte son action selon que vous l'avez ou non configuré pour abandonner les paquets qui ont plus de niveaux d'encapsulation que le niveau d'inspection des tunnels maximal que vous avez configuré.

Par défaut, le contenu encapsulé dans un tunnel appartient à la même zone de sécurité que le tunnel, et est soumis aux règles de politique de sécurité qui protègent cette zone. Cependant, vous pouvez configurer une *zone de tunnel*, ce qui vous donne la flexibilité nécessaire pour configurer des règles de politique de sécurité pour le contenu intérieur qui diffèrent des règles de politique de sécurité pour le tunnel. Si vous utilisez une politique d'inspection des tunnels différente pour la zone du tunnel, elle doit avoir un niveau d'inspection des tunnels maximum de deux niveaux, car par définition le pare-feu observe le deuxième niveau d'encapsulation.

Le pare-feu ne prend pas en charge une règle de politique d'inspection des tunnels qui correspond au trafic pour un tunnel qui se termine sur le pare-feu ; le pare-feu abandonne les paquets qui correspondent à la session de tunnel intérieur. Par exemple, lorsqu'un tunnel IPsec se termine sur le pare-feu, ne créez pas de règle de politique d'inspection des tunnels qui correspond au tunnel que vous terminez. Le pare-feu inspecte déjà le trafic du tunnel intérieur, aussi aucune règle de politique d'inspection du tunnel n'est requise.

 ©2024 Palo Alto Networks, Inc.

Bien que l'inspection du contenu du tunnel fonctionne sur les passerelles partagées et sur les communications système vers système virtuel, vous ne pouvez pas affecter de zones de tunnel à des passerelles partagées ou à des communications système vers système virtuel : elles sont soumises aux mêmes règles de politique de sécurité que les zones auxquelles elles appartiennent.

Les sessions de tunnel intérieur et les sessions de tunnel extérieur comptent tous deux pour la capacité de sessions maximale pour le modèle de pare-feu.

Le tableau suivant indique avec une coche les types de politique que vous pouvez appliquer à une session de tunnel extérieur, une session de tunnel intérieur, et la session d'origine, à l'intérieur :

Type de politique	Session de tunnel extérieur	Session de tunnel intérieur	Session d'origine, à l'intérieur
App-Override	✓ VXLAN uniquement	–	✓
Protection DoS	✓	✓	✓
NAT	✓	–	–
Policy-Based Forwarding (suivi basé sur la politique ; PBF) et retour symétrique	✓	–	–
QoS	–	–	✓
Sécurité (requis)	✓	✓	✓
User-id	✓	✓	✓
protection de zones	✓	✓	✓

VXLAN est différent des autres protocoles. Le pare-feu peut utiliser l'un ou l'autre des deux ensembles différents de clés de session pour créer des session de tunnel extérieur pour VXLAN.

- Session VXLAN UDP : un clé à six uplets (zone, IP source, IP de destination, protocole, port source et port de destination) crée une session VXLAN UDP.
- Session VNI : une clé à cinq uplets qui intègre l'ID de tunnel (l'identificateur de réseau VXLAN ou VNI) et utilise la zone, l'IPsource IP, l'IP de destination, le protocole et l'ID de tunnel (VNI) pour créer une session VNI.

Vous pouvez Afficher l'activité du tunnel inspecté sur l'ACC ou Afficher les informations de tunnel dans les journaux. Pour faciliter la visualisation rapide, configurez un tag de surveillance pour pouvoir surveiller l'activité du tunnel et filtrer les résultats de journalisation avec ce tag.

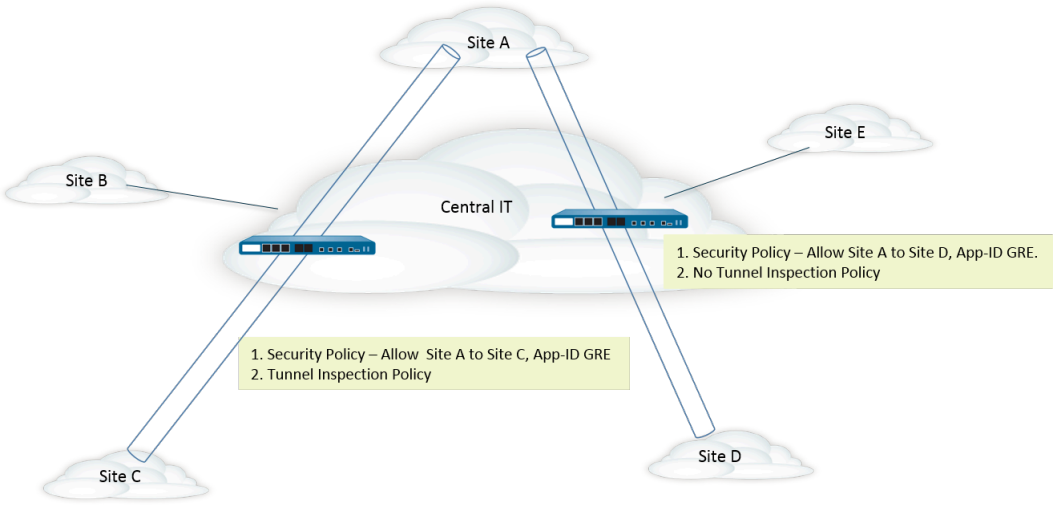
©2024 Palo Alto Networks, Inc.

L'activité du tunnel ACC fournit des données dans diverses vues. Pour l'utilisation de l'ID de tunnel, le tag de surveillance de tunnel et l'utilisation de l'application du tunnel, les données pour **bytes (octets)**, **sessions (sessions)**, **threats (menaces)**, **content (contenu)** et **URLs (URL)** proviennent de la base de données de résumé du trafic. Pour l'utilisateur du tunnel, l'IP source mise en tunnel et l'activité d'IP de destination mise en tunnel, les données pour **bytes (octets)** et **sessions (sessions)** proviennent du résumé du trafic, les données pour **threats (menaces)** proviennent du résumé des menaces, les données **URLs (URL)** proviennent du résumé des URL, et les données **contents (contenu)** proviennent de la base de données Data, qui est un sous-ensemble des journaux de menace.

Si vous activez NetFlow sur l'interface, NetFlow capturera les statistiques pour le tunnel extérieur uniquement, afin d'éviter le double comptage (comptage d'octets à la fois pour les flux intérieurs et extérieurs).

Pour connaître la règle de politique d'inspection des tunnels et les capacités des zones de tunnel pour votre modèle de pare-feu, consultez l'Outil de sélection de produits.

L'illustration suivante présente une entreprise qui exploite plusieurs divisions et utilise différentes politiques de sécurité et une politique d'inspection des tunnels. Une équipe informatique centrale assure la connectivité entre les régions. Un tunnel relie le Site A au Site C, un autre le Site A au Site D. L'informatique centrale place un pare-feu sur le chemin de chaque tunnel : le pare-feu dans le tunnel entre les Sites A et C assure l'inspection des tunnels, celui entre les Sites A et D n'a aucune politique d'inspection des tunnels, car le trafic est très sensible.



 ©2024 Palo Alto Networks, Inc.

Configurer l'inspection du contenu du tunnel

Effectuez cette tâche pour configurer l'inspection du contenu du tunnel d'un protocole que vous autorisez à traverser un tunnel.

STEP 1 | Créez une règle de politique de sécurité pour autoriser les paquets qui utilisent une application donnée (comme l'application GRE) à passer de la zone source à la zone de destination via le tunnel.

Création d'une règle de politique de sécurité

*Le pare-feu peut créer des journaux d'inspection des tunnels au début d'une session, à la fin d'une session, ou aux deux. Lorsque vous spécifiez les **Actions (Actions)** d'une règle de politique de sécurité, sélectionnez **Log at Session Start (Journaliser en début de session)** pour les sessions de tunnel durables, comme les sessions GRE.*

STEP 2 | Créez une règle de politique d'inspection des tunnels.

1. Sélectionnez **Policies (Politiques)** > **Tunnel Inspection (Inspection des tunnels)** et **Add (Ajoutez)** une règle de politique.
2. À l'onglet **General (Général)**, saisissez un **Name (Nom)** pour la règle de politique d'Inspection des tunnels, commençant par un caractère alphanumérique et pouvant contenir des zéros ou d'autres caractères alphanumériques, des traits de soulignement, des traits d'union, des points et des espaces.
3. (Facultatif) Saisissez une **Description (Description)**.
4. (Facultatif) À des fins de journalisation et de génération de rapports, indiquez une **Tag (Étiquette)** qui identifie les paquets qui sont soumis à la règle de politique d'inspection des tunnels.

STEP 3 | Précisez les critères qui déterminent la source des paquets auxquels la règle de politique d'inspection des tunnels s'applique.

1. Sélectionnez l'onglet **Source (Source)**.
2. **Add (Ajoutez)** une **Source Zone (Zone source)** dans la liste des zones (l'option **Any (Indifférent)** est sélectionnée par défaut).
3. (Facultatif) **Add (Ajoutez)** une **Source Address (Adresse source)**. Vous pouvez saisir une adresse IPv4 ou IPv6, un groupe d'adresses ou un objet d'adresse ou un objet d'adresse géographique (**Any (Indifférent)**).
4. (Facultatif) Sélectionnez **Negate (Refuser)** pour choisir n'importe quelle adresse sauf celles que vous spécifiez.
5. (Facultatif) **Add (Ajoutez)** un **Source User (Utilisateur source)** (**any (indifférent)** est sélectionné par défaut). Un **Known-user (Utilisateur connu)** est un utilisateur qui s'est authentifié ; un utilisateur **Unknown (Inconnu)** ne s'est pas authentifié.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Précisez les critères qui déterminent la destination des paquets auxquels la règle de politique d'inspection des tunnels s'applique.

1. Sélectionnez l'onglet **Destination (Destination)**.
2. **Add (Ajoutez)** une **Destination Zone (Zone de destination)** dans la liste des zones (l'option **Any (Indifférent)** est sélectionnée par défaut).
3. (Facultatif) **Add (Ajoutez)** une **Destination Address (Adresse de destination)**. Vous pouvez saisir une adresse IPv4 ou IPv6, un groupe d'adresses ou un objet d'adresse ou un objet d'adresse géographique (l'option **Any (Indifférent)** est sélectionnée par défaut).

   Vous pouvez également configurer une nouvelle adresse ou un nouveau groupe d'adresses.
4. (Facultatif) Sélectionnez **Negate (Refuser)** pour choisir n'importe quelle adresse sauf celles que vous spécifiez.

STEP 5 | Indiquez les protocoles de tunnel que le pare-feu inspectera pour cette règle.

1. Sélectionnez l'onglet **Inspection (Inspection)**.
2. Veuillez **Add (Ajouter)** un ou plusieurs **Protocols (Protocoles)** de tunnels que vous souhaitez que le pare-feu inspecte :
   - **GRE (GRE)** – Le pare-feu inspecte les paquets qui utilisent la Generic Route Encapsulation (Encapsulation générique de routage ; GRE) dans le tunnel.
   - **GTP-U (GTP-U)** – Le pare-feu inspecte les paquets qui utilisent le protocole de tunnellisation General Packet Radio Service (service général de radiocommunication par paquets ; GPRS) dans le tunnel.
   - **IPSec non chiffré)** – Le pare-feu inspecte les paquets qui utilisent le protocole IPSec non chiffré (IPSec non chiffré ou mode de transport AH IPSec) dans le tunnel.
   - **VXLAN** — Le pare-feu inspecte les paquets qui utilisent le protocole de tunnellisation Virtual Extensible Local Area Network (réseau local virtuel extensible ; VXLAN) dans le tunnel.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Indiquez le nombre de niveaux d'encapsulation que le pare-feu inspecte et les conditions d'abandon d'un paquet par le pare-feu.

1. Sélectionnez **Inspect Options (Options d'inspection)**.
2. Sélectionnez les **Maximum Tunnel Inspection Levels (Niveaux maximaux d'inspection des tunnels)** que le pare-feu inspecte :
   - **Un niveau** (par défaut) : le pare-feu inspecte uniquement le contenu qui se trouve dans le tunnel externe.

     Pour VXLAN, le pare-feu inspecte une charge utile VXLAN pour trouver le contenu ou les applications encapsulés dans le tunnel. Vous devez sélectionner **One Level (Un niveau)**, car l'inspection ne se produit que sur le tunnel extérieur.
   - **Two Levels (Tunnel In Tunnel) (Deux niveaux (Tunnel dans le tunnel)** : le pare-feu inspecte le contenu du tunnel extérieur et du tunnel interne.
3. Sélectionnez la totalité, une partie ou aucun des éléments suivants pour préciser si le pare-feu abandonne un paquet lorsque chacun des conditions se présente :
   - **Drop packet if over maximum tunnel inspection level (Abandonner le paquet si le niveau maximal d'inspection des tunnels est dépassé)** : le pare-feu abandonne un paquet qui contient plus de niveaux d'encapsulation que le nombre configuré à l'option **Maximum Tunnel Inspection Levels (Niveaux maximaux d'inspection des tunnels)**.
   - **Drop packet if tunnel protocol fails strict header check (Abandonner le paquet si le protocole de tunnel échoue la vérification stricte de l'en-tête)** : le pare-feu abandonne un paquet qui contient un protocole de tunnel qui utilise un en-tête qui n'est pas conforme au document RFC pour ce protocole. Les en-têtes non conformes peuvent indiquer des paquets suspects. Cette option permet au pare-feu de vérifier les en-têtes GRE par rapport au document RFC 2890.

     *Si votre pare-feu tunnellise GRE avec un périphérique qui met en œuvre une version de GRE antérieure à la RFC 2890, vous ne devriez pas activer l'option **Drop packet if tunnel protocol fails strict header check (Abandonner le paquet si le protocole de tunnel échoue la vérification stricte de l'en-tête)**.*
   - **Drop packet if unknown protocol inside tunnel (Abandonner le paquet si un protocole inconnu se trouve à l'intérieur du tunnel)** : le pare-feu abandonne un paquet dont le pare-feu ne peut identifier le protocole qui se trouve à l'intérieur du tunnel.

     Par exemple, si cette option est sélectionnée, le pare-feu abandonne les paquets IPSec cryptés qui correspondent à la règle de politique d'inspection des tunnels, parce que le pare-feu ne peut les lire. Vous pouvez donc autoriser les paquets IPSec, et le pare-feu n'autorisera que les paquets IPSec et AH IPSec non cryptés.
   - **Return scanned VXLAN tunnel to source (Retourner le tunnel VXLAN analysé vers la source)** : Lorsque le trafic est redirigé (orienté) vers le pare-feu, le protocole VXLAN encapsule le paquet. L'orientation du trafic est particulièrement courante dans les environnements de cloud public. Activez l'option **Return scanned VXLAN tunnel to source (Retourner le tunnel VXLAN analysé vers la source)** pour retourner le paquet encapsulé vers le VXLAN tunnel endpoint (Point de terminaison du tunnel VXLAN ;

 ©2024 Palo Alto Networks, Inc.

VTEP) de départ. Cette option n'est prise en charge que sur la couche 3, la sous-interface de couche 3, l'interface agrégée de couche 3 et VLAN.

4. Cliquez sur **OK**.

STEP 7 | Gérez les règles de politique d'inspection des tunnels.

Utilisez les procédures suivantes pour gérer les règles de la politique d'inspection des tunnels :

- (Champ de filtrage) : n'affiche que les règles de la politique d'inspection des tunnels nommées dans le champ de filtrage.
- **Delete (Supprimer)** : supprime les règles de politique d'inspection des tunnels sélectionnées.
- **Clone (Cloner)** : une option de rechange au bouton **Add (Ajouter)** ; reproduit la règle sélectionnée en lui donnant un nouveau nom, ce qui vous permet de la revoir.
- **Enable (Activer)** : active les règles de politique d'inspection des tunnels qui sont sélectionnées.
- **Disable (Désactiver)** : désactive les règles de politique d'inspection des tunnels qui sont sélectionnées.
- **Move (Déplacer)** : déplace les règles de politique d'inspection des tunnels vers le haut ou le bas de la liste ; les paquets sont comparés aux règles selon leur ordre d'apparition, de haut en bas.
- **Highlight Unused Rules (Surligner les règles inutilisées)** : surligne les règles de politique d'inspection des tunnels auxquelles aucun paquet n'a correspondu depuis le dernier redémarrage du pare-feu.

STEP 8 | (Facultatif) Créez une zone source du tunnel ou une zone de destination du tunnel pour le contenu du tunnel et configurez une règle de politique de sécurité pour chaque zone.

Il est recommandé de créer des zones de tunnel pour votre trafic de tunnel. Ainsi, le pare-feu crée des sessions distinctes pour les paquets tunnellisés et non tunnellisés qui possèdent les cinq même tuples (adresse IP et port source, adresse IP et port de destination et protocole).

Sur un pare-feu PA-5200 Series, si vous affectez des zones de tunnel au trafic de tunnel, le pare-feu effectuera l'inspection des tunnels dans le logiciel ; l'inspection des tunnels n'est pas transférée au matériel.

1. Si vous souhaitez que le contenu de tunnel soit soumis à des règles de politique de sécurité différentes de celles applicables à la zone du tunnel extérieur (configurées

 ©2024 Palo Alto Networks, Inc.

précédemment), sélectionnez **Network (Réseau)** > **Zones (Zones)** et **Add (Ajoutez)** un **Name (Nom)** pour la zone source du tunnel.

2. Sous **Location (Emplacement)**, sélectionnez le système virtuel.
3. Sous **Type (Type)**, sélectionnez **Tunnel (Tunnel)**.
4. Cliquez sur **OK**.
5. Répétez ces sous-étapes pour créer la zone de destination du tunnel.
6. Configurez une règle de politique de sécurité pour la zone source du tunnel.

   *Comme il se peut que vous ne connaissiez pas l'initiateur du trafic de tunnel ou le sens du trafic et que vous ne voulez pas interdire par erreur le trafic d'une application de passer par le tunnel, spécifiez les deux zones de tunnel comme **Source Zone (Zone source)** et **Destination Zone (Zone de destination)** dans votre règle de politique de sécurité ou sélectionnez **Any (Indifférent)** pour les zones source et de destination ; puis indiquez les **Applications (Applications)**.*
7. Configurez une règle de politique de sécurité pour la zone de destination du tunnel. Les conseils donnés à l'étape précédente pour configurer une règle de politique de sécurité pour la zone source du tunnel s'appliquent également à la zone de destination du tunnel.

STEP 9 | (Facultatif) Indiquez la zone source du tunnel et la zone de destination du tunnel pour le contenu interne.

1. Indiquez la zone source du tunnel et la zone de destination du tunnel (que vous venez d'ajouter) pour le contenu interne. Sélectionnez **Policies (Politiques)** > **Tunnel Inspection (Inspection des tunnels)**, puis à l'onglet **General (Général)**, sélectionnez le **Name (Nom)** de la règle de politique d'inspection des tunnels que vous avez créée.
2. Sélectionnez **Inspection (Inspection)**.
3. Sélectionnez les **Security Options (Options de sécurité)**.
4. **Enable Security Options (Activez les options de sécurité)** (désactivées par défaut) pour amener le contenu source interne à appartenir à la **Tunnel Source Zone (Zone source du tunnel)** que vous indiquez et le contenu de destination interne à appartenir à la **Tunnel Destination Zone (Zone de destination du tunnel)** que vous indiquez.

   Si vous n'effectuez pas l'action consistant à **Enable Security Options (Activer les options de sécurité)**, le contenu source interne appartient à la même zone source que la source extérieure du tunnel et le contenu de destination interne appartient à la même zone de destination que la destination extérieure du tunnel, ce qui signifie qu'elles sont soumises aux mêmes règles de politique de sécurité qui s'appliquent à ces zones extérieures.
5. Sous **Tunnel Source Zone (Zone source du tunnel)**, sélectionnez la zone de tunnel appropriée que vous avez créée à l'étape précédente afin que les politiques associées à cette zone s'appliquent à la zone source du tunnel. Autrement, le contenu source interne utilise par défaut la même zone que la source extérieure du tunnel utilise, et les politiques de la zone de la source extérieure du tunnel s'appliquent également à la zone de contenu source interne.
6. Sous **Tunnel Destination Zone (Zone de destination du tunnel)**, sélectionnez la zone de tunnel appropriée que vous avez créée à l'étape précédente afin que les politiques associées à cette zone s'appliquent à la zone de destination du tunnel. Autrement, le contenu de destination interne utilise par défaut la même zone que la destination

 ©2024 Palo Alto Networks, Inc.

extérieure du tunnel utilise, et les politiques de la zone de destination extérieure du tunnel s'appliquent également à la zone de contenu de destination interne.

*Si vous configurez une **Tunnel Source Zone (Zone source du tunnel)** et une **Tunnel Destination Zone (Zone de destination du tunnel)** pour la règle de politique d'inspection des tunnels, vous devriez configurer une **Source Zone (Zone source)** donnée (à l'étape 3) et une **Destination Zone (Zone de destination)** donnée (à l'étape 4) dans les critères de correspondance de la règle de politique d'inspection des tunnels, plutôt que d'indiquer **Any (Indifférent)** pour la **Source Zone (Zone source)** et **Any (Indifférent)** pour la **Destination Zone (Zone de destination)**. Ces conseils permettent de garantir que le sens de la réaffectation de zone correspond comme il se doit à celui des zones parents.*

Sur un pare-feu PA-5200 Series ou PA-7080, si vous utilisez la sous-couche multicast lors de l'inspection VXLAN, la session interne serait répliquée sur plusieurs plans de données et une situation de course pourrait se produire. Pour éviter l'abandon de certains paquets, les exigences suivantes s'appliquent :

- *Vous devez configurer une règle d'inspection du contenu du tunnel distincte pour mettre en correspondance les paquets VXLAN extérieurs dirigés vers chaque point de terminaison du tunnel VXLAN.*
- *Dans la règle distincte, vous affectez une zone de tunnel. L'utilisation d'une autre zone de tunnel ferait en sorte de rendre chaque session interne différente pour chaque point de terminaison. La situation de course ne se produirait pas, et aucun abandon de paquet ne serait constaté.*

7. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 10 | Définissez des options de surveillance pour le trafic qui correspond à une règle de politique d'inspection des tunnels.

1. Sélectionnez **Policies (Politiques)** > **Tunnel Inspection (Inspection des tunnels)**, puis sélectionnez la règle de politique d'inspection des tunnels que vous avez créée.
2. Sélectionnez **Inspection (Inspection)** > **Monitor Options (Options de surveillance)**.
3. Saisissez un **Monitor Name (Nom de surveillance)** pour regrouper le trafic similaire à des fins de journalisation et de génération de rapports.
4. Saisissez un **Monitor Tag (number) (numéro de balise de surveillance)** pour regrouper le trafic similaire pour la journalisation et la génération de rapports (plage de 1 à 16 777 215). Le numéro de tag est défini de manière globale.

   Ce champ ne s'applique pas au protocole VXLAN. Les journaux VXLAN utilisent automatiquement l'ID VNI dans l'en-tête VXLAN.

   Si vous étiquetez le trafic de tunnel, vous pouvez ultérieurement appliquer un filtre sur l'étiquette de surveillance dans le journal d'inspection des tunnels et utiliser l'ACC pour voir l'activité du tunnel en fonction de cette étiquette.
5. **Override Security Rule Log Setting (Remplacez le paramètre du journal des règles de sécurité)** pour activer les options de journalisation et de transfert des journaux pour les sessions qui correspondent à la règle de politique d'inspection des tunnels sélectionnée. Si vous ne sélectionnez pas ce paramètre, la génération du journal des tunnels et le transfert des journaux sont déterminés par les paramètres des journaux applicables à la règle de politique de sécurité qui s'applique au trafic du tunnel. Vous pouvez remplacer les paramètres de transfert des journaux dans les règles des politiques de sécurité qui contrôlent les journaux de trafic en configurant les paramètres des journaux d'inspection des tunnels de sorte qu'ils stockent les journaux des tunnels distinctement des journaux du trafic. Les journaux d'inspection des tunnels stockent les sessions du tunnel extérieur (GRE, IPSec non chiffré, VXLAN ou GTP-U) et les journaux du trafic stockent les flux du trafic interne.
6. Sélectionnez **Log at Session Start (Journaliser en début de session)** pour journaliser le trafic au début de la session.

   Pour les journal des tunnels, il est recommandé de procéder à la journalisation au début et à la fin de la session, car les tunnels peuvent demeurer actifs très longtemps. Par exemple, les tunnels GRE peuvent être créés lors du démarrage du routeur pour prendre fin uniquement au redémarrage du routeur. Si vous ne journalisez pas en début de session, vous ne verrez jamais dans l'ACC qu'il y a un tunnel GRE actif.
7. Sélectionnez **Log at Session End (Journaliser en fin de session)** pour journaliser le trafic à la fin de la session.
8. Sélectionnez un profil de **Log Forwarding (Transfert des journaux)** qui détermine où le pare-feu transfère les journaux des tunnels pour les sessions qui satisfont la règle d'inspection des tunnels. Vous pouvez également créer un nouveau profil de transfert des journaux, si vous Configurez le transfert des journaux.
9. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 11 | (Facultatif, VXLAN uniquement) **Configurez un ID VXLAN (VNI)**. Par défaut, toutes les interfaces réseau VXLAN (VNI) sont inspectées. Si vous configurez un ou plusieurs ID de VXLAN, la politique n'inspecte que ces VNIs.

Seul le protocole VXLAN utilise l'onglet Tunnel ID (ID de tunnel) pour spécifier le VNI).

1. Sélectionnez l'onglet **Tunnel ID (ID de tunnel)**, cliquez sur **Add (Ajouter)**.
2. Affectez un **Name (Nom)**. Le nom sert d'élément pratique, mais ne sert pas de facteur dans la journalisation, la surveillance ou l'établissement de rapports.
3. Dans le champ **VXLAN ID (VNI) [ID VXLAN (VNI)]**), saisissez un seul VNI, une liste de VNI séparés par des virgules, une plage de VNI (un tiret faisant office de séparateur), ou une combinaison de ces éléments. Par exemple, vous pouvez spécifier les éléments suivants :

   `1677002,1677003,1677011-1677038,1024`

STEP 12 | (Facultatif) Si vous avez activé l'option **Rematch Sessions (Revérifier les sessions)** (**Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)**), assurez-vous que le pare-feu n'abandonne pas les sessions existantes lors de la création ou de la révision d'une politique d'inspection des tunnels, en désactivant l'option **Reject Non-SYN TCP (Rejeter le protocole TCP non-SYN)** pour les zones qui contrôlent les règles de politique de sécurité de votre tunnel.

Le pare-feu affiche les avertissements suivants lorsque vous :

- Créez une règle de politique d'inspection des tunnels.
- Modifiez une règle de politique d'inspection des tunnels en ajoutant un **Protocol (Protocole)** ou en augmentant les **Maximum Tunnel Inspection Levels (Niveaux maximaux d'inspection des tunnels)**, en les faisant passer de **One Level (Un niveau)** à **Two Levels (Deux niveaux)**.
- **Enable Security Options (Activez les options de sécurité)** à l'onglet **Security Options (Options de sécurité)** en ajoutant de nouvelles zones ou en passant d'une zone à l'autre.

*Attention : Si vous activez des politiques d'inspection des tunnels sur des sessions de tunnel existantes, les sessions TCP existantes à l'intérieur du tunnel seront alors traitées comme des flux non-syn-tcp. Pour vous assurer que les sessions existantes ne sont pas abandonnées lorsque la politique d'inspection des tunnels est activée, définissez le paramètre **Reject Non-SYN TCP (Rejeter le protocole TCP non-SYN)** d'une ou de plusieurs zones sur **no (non)** et utilisez un profil de protection de zone que vous appliquerez aux zones qui contrôlent les politiques de sécurité du tunnel. Lorsque les sessions existantes ont été reconnues par le pare-feu, vous pouvez réactiver le paramètre **Reject Non-SYN TCP ((Rejeter le protocole TCP non-SYN))** en le définissant sur **yes (oui)** ou sur **global (global)**.*

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)**, puis **Add (Ajouter)** un profil.
2. Saisissez un **Name (Nom)** pour le profil.
3. Sélectionnez **Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)** > **TCP Drop (Abandon TCP)**.

 ©2024 Palo Alto Networks, Inc.

4. Sous **Reject Non-SYN TCP (Rejeter le protocole TCP non-SYN)**, sélectionnez **no (non)**.
5. Cliquez sur **OK**.
6. Sélectionnez **Network (Réseau)** > **Zones (Zones)**, puis sélectionnez la zone qui contrôle les règles de politique de sécurité de votre tunnel.
7. Sous **Zone Protection Profile (Profil de protection de zone)**, sélectionnez le profil de protection de zone que vous venez de créer.
8. Cliquez sur **OK**.
9. Reprenez les trois sous-étapes précédentes (12.f, 12.g et 12.h) pour appliquer le profil de protection de zone à des zones supplémentaires qui contrôlent les règles de politique de sécurité de votre tunnel.
10. Une fois que le pare-feu a reconnu les sessions existantes, vous pouvez réactiver l'option **Reject Non-SYN TCP (Rejeter le protocole TCP non-SYN)** en la définissant sur **yes (oui)** ou sur **global (global)**.

STEP 13 | (Facultatif) Limitez la fragmentation du trafic d'un tunnel.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection(Protection des zones)** et **Add (Ajoutez)** un profil selon le **Name (Nom)**.
2. Saisissez une **Description (Description)**.
3. Sélectionnez **Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)** > **IP Drop (Abandon d'IP)** > **Fragmented traffic (Trafic fragmenté)**.
4. Cliquez sur **OK**.
5. Sélectionnez **Network (Réseau)** > **Zones (Zones)**, puis choisissez la zone de tunnel dans laquelle vous souhaitez limiter la fragmentation.
6. Sous **Zone Protection Profile (Profil de protection de zone)**, sélectionnez le profil que vous venez de créer pour appliquer le profil de protection de zone à la zone de tunnel.
7. Cliquez sur **OK**.

STEP 14 | **Commit (Validez)** vos modifications.

 ©2024 Palo Alto Networks, Inc.

Afficher l'activité du tunnel inspecté

Effectuez la tâche suivante pour visualiser l'activité des tunnels inspectés.

STEP 1 | Sélectionnez **ACC (ACC)** et sélectionnez un **Virtual System (Système virtuel)** ou **All (Tous)** les systèmes virtuels.

STEP 2 | Sélectionnez l'activité du tunnel.

STEP 3 | Sélectionnez une période à afficher, par exemple les 24 dernières heures ou les 30 derniers jours.

STEP 4 | Pour utiliser les filtres globaux, cliquez sur les boutons + et - pour utiliser les filtres ACC sur l'activité du tunnel.

STEP 5 | Affichez l'activité du tunnel inspecté. Vous pouvez afficher et trier les données par **bytes (octets)**, **sessions (sessions)**, **threats (menaces)**, **content (contenu)** et **URLs (URL)**. Chaque fenêtre affiche un aspect différent des données du tunnel sous forme de graphique et de tableau :

- **Tunnel ID Usage (Utilisation de l'ID de tunnel)** : Chaque protocole de tunnel répertorie les ID des tunnels utilisant ce protocole. Les tableaux fournissent les totaux d'octets, sessions, menaces, contenu et URL pour le protocole. Survolez l'ID de tunnel pour obtenir les détails par ID de tunnel.
- **Tunnel Monitor Tag (Étiquette de surveillance de tunnel)** : Chaque protocole de tunnel répertorie les étiquettes de surveillance des tunnels utilisant cette étiquette. Les tableaux fournissent les totaux d'octets, sessions, menaces, contenu et URL pour l'étiquette et pour le protocole. Survolez l'étiquette de surveillance de tunnel pour obtenir les détails par étiquette.
- **Tunneled Application Usage (Utilisation de l'application en tunnel)** : Les catégories d'application affichent visuellement les types d'applications groupés par support, intérêt général, collaboration et réseau, avec un code couleur selon le risque. Les tableaux d'application incluent également le nombre d'utilisateurs par application.
- **Tunneled User Activity (Activité d'utilisateur en tunnel)** : Affiche un graphique des octets envoyés et reçus, par exemple le long d'un axe X de date et heure. Survolez un point du graphique pour visualiser les données à ce point. Le tableau d'utilisateur source et d'utilisateur de destination fournit des données par utilisateur.
- **Tunneled Source IP Activity (Activité IP source en tunnel)** : Affiche des graphiques et tableaux d'octets, sessions et menaces, par exemple pour un pirate à une certaine adresse IP. Survolez un point du graphique pour visualiser les données à ce point.
- **Tunneled Destination IP Activity (Activité IP destination en tunnel)** : Affiche des graphiques et tableaux en fonction des adresses IP de destination. Affichez les menaces par victime à une certaine adresse IP, par exemple. Survolez un point du graphique pour visualiser les données à ce point.

 ©2024 Palo Alto Networks, Inc.

Afficher les informations de tunnel dans les journaux

Vous pouvez visualiser les journaux d'inspection du tunnel eux-mêmes ou consulter les informations d'inspection du tunnel dans les autres types de journaux.

Protocoles GRE, IPSec non chiffré, VXLAN et GTP-U

- Lorsqu'il y a une correspondance avec les règles de trafic TCI, les protocoles GRE, IPSec et GTP-U sont journalisés dans le journal d'inspection du tunnel et le type de journal de tunnel, le protocole mis en correspondance et le nom de la surveillance et l'étiquette de la surveillance (numéro) configurés sont indiqués.
- Lorsqu'il n'y a aucune correspondance avec les règles TCI, tous les protocoles sont journalisés dans les journaux du trafic.

Protocole VXLAN

- Lorsqu'il n'y a aucune correspondance avec les règles TCI, le protocole VXLAN est journalisé dans le journal d'inspection du tunnel et le type de journal de tunnel (VXLAN), le nom de la surveillance configuré et l'ID de tunnel (VNI) sont indiqués.

  Dans le journal du trafic de la session interne, l'indicateur de tunnel inspecté indique la présence d'une session VNI. La session parent correspond à la session qui était active lors de la création de la session interne, il se peut donc que l'ID ne corresponde pas à l'ID de session.
- Lorsqu'il n'y a aucune correspondance avec les règles TCI, les sessions VNI sont journalisées dans les journaux du trafic et le protocole UDP, le port souce 0 et le port de destination 4789 (par défaut) sont indiqués.

- Affichez les journaux d'inspection du tunnel.
  1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Tunnel Inspection (Inspection des tunnels)** et affichez les données du journal pour identifier les **Applications (Applications)** de tunnel utilisées dans votre trafic et les nombres élevés de paquets échouant au Contrôle strict des en-têtes.
  2. Cliquez sur la vue détaillée du journal () pour voir les détails d'un journal.

- Affichez les autres journaux pour obtenir des renseignements sur l'inspection des tunnels.
  1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)**.
  2. Sélectionnez **Traffic (Trafic)**, **Threat (Menace)**, **URL Filtering (Filtrage d'URL)**, **WildFire Submissions (Envois WildFire)**, **Data Filtering (Filtrage de données)** ou **Unified (Unifié)**.
  3. Pour une entrée de journal, cliquez sur la vue détaillée du journal ().
  4. Dans la fenêtre Indicateurs, vérifiez si l'indicateur **Tunnel Inspected (Tunnel inspecté)** est coché. Un indicateur de tunnel inspecté indique que le pare-feu a utilisé une règle de politique d'inspection de tunnel pour vérifier le contenu ou tunnel intérieur. Les informations sur la session parent se rapportent à un tunnel extérieur (par rapport à un tunnel intérieur) ou à un tunnel intérieur (par rapport au contenu intérieur).

     Dans les journaux **Traffic (Trafic)**, **Threat (Menace)**, **URL Filtering (Filtrage des URL)**, **WildFire Submissions (Envois WildFire)**, **Data Filtering (Filtrage des données)**, seules les informations parent s'affichent dans la vue détaillée du journal de session intérieure, et non dans les informations du journal du tunnel. Si vous avez configuré deux niveaux

©2024 Palo Alto Networks, Inc.

d'inspection de tunnel, vous pouvez sélectionner la session parent de ce parent direct pour afficher le deuxième journal parent. (Vous devez surveiller le journal **Tunnel Inspection (Inspection des tunnels)** comme illustré lors de l'étape précédente pour afficher les informations du journal du tunnel.)

5. Si vous visualisez le journal d'une session intérieure avec inspection des tunnels, cliquez sur le lien **View Parent Session (Afficher la session parent)** dans la section Général pour afficher les informations de la session extérieure.

©2024 Palo Alto Networks, Inc.

Créer un rapport personnalisé basé sur le trafic de tunnel étiqueté

Vous pouvez créer un rapport pour recueillir des informations en fonction de l'étiquette que vous avez appliquée au trafic du tunnel.

STEP 1 | Sélectionnez **Monitor (Surveillance)** > **Manage Custom Reports (Gérer les rapports personnalisés)** et cliquez sur **Add (Ajouter)**.

STEP 2 | Sous Database (Base de données), sélectionnez le journal du trafic, des menaces, des URL, du filtrage des données ou des envois WildFire.

STEP 3 | Sous Available Columns (Colonnes disponibles), sélectionnez Flags and Monitor Tag (Étiquette des indicateurs et de surveillance) ainsi que les autres données que vous aimeriez que le rapport contienne.

Vous pouvez également générer des rapports personnalisés.

©2024 Palo Alto Networks, Inc.

Comportement d'accélération du tunnel

Les sections suivantes fournissent des informations générales sur l'accélération des tunnels GTP-U, GRE et VXLAN, qu'il peut être utile de connaître avant de décider de Désactivation de l'accélération du tunnel.

- GTP-U
- GRE
- VXLAN

GTP-U

Critères à respecter avant d'activer l'accélération du tunnel GTP:

1. L'accélération générique du tunnel est activée sous **Device (appareil)** > **Setup (Configuration)** > **Management (Gestion)** dans Paramètres généraux, l'accélération du tunnel est cochée).
2. GTP Security est activé sous **Device (Appareil)** > **Setup (Configuration)** > **Management (gestion)** (dans les paramètres généraux, GTP Security est coché).
3. Aucune règle de stratégie d'inspection de tunnel avec le protocole GTP-U n'est activée.
4. Après avoir validé la configuration, vous devez redémarrer pour charger le programme d'analyse GTP-U.

Critères d'identification des paquets GTP-U dans le matériel:

1. Le port de destination UDP est 2152.
2. GTP.version vaut 1 et GTP.protocol_type vaut 1.

Comment l'accélération du tunnel modifie l'ID du flux:

- Si le paquet GTP-U satisfait aux deux critères d'identification, le pare-feu définit la clé de flux suivante :
  - Bit d'encodage : 1
  - port de destination UDP : identifiant de point d'extrémité tunnel (TEID)
  - Adresse source : 0
- Sinon, le paquet est traité comme un paquet UDP normal.

Avantages de l'accélération du tunnel GTP-U

Si l'accélération GTP-U est activée, le principal avantage se produit s'il y a beaucoup de trafic tunnelisé qui peut être déchargé. Un grand pourcentage du trafic GTP provient de périphériques mobiles et est principalement du trafic Web, qui ne sera pas déchargé lorsque la charge utile interne est inspectée.

La fonctionnalité GTP Security est entièrement fonctionnelle sans accélération et le bénéfice de performance est lié à la quantité de trafic interne de charge utile qui peut être déchargé par le matériel. Par exemple, tout ce qui devrait normalement être marqué comme `L7 complet` sera déchargé et géré uniquement dans le matériel comme une application interne à GTP.

 ©2024 Palo Alto Networks, Inc.

GRE

Critère d'accélération du tunnel prenant effet avec le GRE:

- L'accélération générique du tunnel est activée sous **Device (Appareil)** > **Setup (Configuration)(** > **Management (gestion)** dans Paramètres généraux, l'accélération du tunnel est cochée).

Critère d'identification des paquets GRE dans le matériel:

- Protocole IP 47

Comment l'accélération du tunnel modifie l'ID du flux:

- La clé de débit est la même avec et sans accélération du tunnel.

Avantages de l'accélération du tunnel GRE

- **With TCI (Avec TCI)** : Le trafic de passage du GRE augmentera d'environ 30 % les performances en matière de traitement des flux avec accélération du tunnel par rapport au même trafic sans accélération du tunnel.
- **Without TCI (Sans TCI)** : Il n'y a pas d'impact sur les performances du trafic GRE lors de la désactivation de l'accélération du tunnel si aucune stratégie d'inspection du contenu du tunnel (TCI) n'est utilisée.

VXLAN

Critère d'accélération du tunnel prenant effet avec VXLAN:

- L'accélération générique du tunnel est activée sous **Device (Appareil)** > **Setup (Configuration)(** > **Management (gestion)** dans Paramètres généraux, l'accélération du tunnel est cochée).

Critère d'identification des paquets VXLAN dans le matériel:

- Le port de destination UDP est 4789.

Ce qui est changé:

- Le port de destination UDP est modifié en valeur VNI (VXLAN network identifier) depuis l'en-tête VXLAN.
- L'encodage est changé à 2.

Avantages de l'accélération du tunnel VXLAN

- **Generic (Générique)** : Moins de ressources de session consommées car nous n'avons besoin que de la session VNI et non de la session UDP VXLAN externe. Pour VXLAN, nous allons analyser l'en-tête VXLAN pour extraire le VNI et utiliser le VNI pour obtenir un ID de flux unique pour chaque VNI dans un tunnel VXLAN.
- **With TCI (Avec TCI)** : Le trafic VXLAN passthrough connaîtra une augmentation d'environ 30% des performances dans la gestion du flux avec l'accélération du tunnel par rapport au même trafic sans l'accélération du tunnel.
- **Without TCI (Sans TCI)** : Même sans TCI, nous verrons une amélioration d'environ 10 % des performances dans la gestion des flux avec accélération du tunnel par rapport au même trafic sans accélération du tunnel. Les différents ID de flux pourraient faire en sorte que les flux soient placés sur des plans de données différents et donc causer une différence dans la façon dont la charge d'un tunnel VXLAN unique est répartie pour les différents VNI qui seraient

 ©2024 Palo Alto Networks, Inc.

passés dans le tunnel. À moins de flux VXLAN avec plusieurs VNI, l'impact sur les performances sera presque négligeable.

 ©2024 Palo Alto Networks, Inc.

Désactivation de l'accélération du tunnel

Par défaut, les pare-feu pris en charge effectuent une tunnel acceleration (accélération du tunnel) pour améliorer les performances et le débit du trafic passant par les tunnels GRE, VXLAN et GTP-U. L'accélération du tunnel permet de décharger le matériel afin de réduire le temps nécessaire pour effectuer les recherches de flux et de répartir plus efficacement le trafic du tunnel en fonction du trafic intérieur.

L'accélération des tunnels GRE et VXLAN est prise en charge par les pare-feu des séries PA-3200 et les pare-feu de la série PA-5450 avec PA-7000-100G-NPC-A et PA-7000-SMC-B ou PA-7050-SMC-B. Vous pouvez désactiver l'accélération du tunnel pour résoudre les problèmes. Lorsque vous désactivez l'accélération du tunnel, vous le faites simultanément pour les tunnels GRE, VXLAN et GTP-U.

Il n'y a pas d'impact sur les performances du trafic GRE lors de la désactivation de l'accélération du tunnel si aucune stratégie d'inspection du contenu du tunnel (TCI) n'est utilisée.

STEP 1 | Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les General Settings (Paramètres généraux).

STEP 2 | Désélectionnez **Tunnel Acceleration (Accélération du tunnel)** pour la désactiver.

STEP 3 | Cliquez sur **OK**.

STEP 4 | **Commit** (Valider).

STEP 5 | Redémarrez le pare-feu.

STEP 6 | (Facultatif) Vérifier l'état de l'accélération du tunnel.

1. Accédez à la CLI.
2. > **`show tunnel-acceleration`**

   La sortie du système est `Enabled (Activée)` ou `Disabled (Désactivée)`. État supplémentaires et raison pour GTP-U uniquement :

   - `Disabled (Désactivée)` : l'accélération du tunnel GTP-U n'est pas prise en charge par le modèle de pare-feu ou la sécurité GTP est désactivée.
   - `Error (TCI with GTP-U configured unexpectedly) (Erreur (TCI avec GTP-U configuré de manière inattendue)` (: Le protocole TCI avec GTP-U est configuré lorsque l'option Tunnel Acceleration (Accélération du tunnel) est activée.
   - `Enabled (Activée)` : L'accélération du tunnel est activée ; l'accélération du tunnel GTP-U n'est pas encore en cours d'exécution. La sécurité GTP est activée, mais doit encore être redémarrée.
   - `Installed (Installée)` : l'accélération du tunnel GTP-U est en cours d'exécution.

 ©2024 Palo Alto Networks, Inc.

Broker de paquets réseau

Le Broker de paquets de réseau filtre et transfère le trafic réseau vers une chaîne de sécurité externe d'une ou plusieurs appliances de sécurité tierces. Le Broker de paquets de réseau remplace la fonctionnalité de Broker de déchiffrement introduite dans PAN-OS 8.1 et étend ses capacités pour inclure le transfert du trafic TLS non déchiffré et du trafic non TLS (texte clair) ainsi que du trafic TLS déchiffré. La capacité de gérer tous les types de trafic est particulièrement précieuse dans les environnements de très haute sécurité tels que les institutions financières et gouvernementales.

Le broker de paquets réseau est pris en charge sur les périphériques des séries PA-7000b, PA-5400, PA-5200, PA-3400, PA-3200 et les modèles VM-300 et VM-700. Il faut activer le déchiffrement du proxy de transfert SSL et établir le pare-feu en tant que tiers de confiance (homme du milieu) pour le trafic de la session.



Une interface de pare-feu ne peut être un agent de déchiffrement et un point de terminaison du tunnel GRE.

- Présentation du Broker de paquets réseau
- Fonctionnement du Broker de paquets réseau
- Préparez-vous à déployer le Broker de paquets de réseau
- Chaîne de sécurité de la passerelle transparente
- Configurer les chaînes de sécurité routées de la couche 3
- Assistance haute disponibilité du broker de paquets réseau
- Modifications de l'interface utilisateur pour le Broker de paquets de réseau
- Limitations du Broker de paquets de réseau
- Dépannage du Broker de paquets réseau

Présentation du Broker de paquets réseau

Si vous utilisez un ou plusieurs dispositifs de sécurité tiers (une chaîne de sécurité) dans le cadre de votre suite de sécurité globale, vous pouvez utiliser le Broker de paquets de réseau pour filtrer et transférer le trafic réseau vers ces dispositifs de sécurité. Le Broker de paquets de réseau remplace la fonctionnalité du Broker de déchiffrement introduite dans PAN-OS 8.1.

Comme le Broker de déchiffrement, le Broker de paquets de réseau fournit des capacités de déchiffrement et de gestion de la chaîne de sécurité. Cela simplifie votre réseau en éliminant les complications liées à la prise en charge de périphériques dédiés pour ces fonctions et réduit les coûts d'investissement et d'exploitation. Tout comme le Broker de déchiffrement, le Broker de paquets de réseau fournit des contrôles de santé pour s'assurer que le chemin d'accès à la chaîne de sécurité est sain et des options pour gérer le trafic si une chaîne tombe en panne.

Le Broker de paquets de réseau étend les capacités de transfert de la chaîne de sécurité du pare-feu afin que vous puissiez filtrer et transférer non seulement le trafic TLS déchiffré, mais également le trafic TLS et non TLS (texte clair) non déchiffré vers une ou plusieurs chaînes de sécurité en fonction des applications, des utilisateurs et des appareils , les adresses IP et les zones. Ces fonctionnalités sont particulièrement utiles dans les environnements à très haute sécurité tels que les institutions financières et gouvernementales.

Mettre à niveau et rétrograder :

- Lorsque vous effectuez une mise à niveau vers PAN-OS 11.1 sur des pare-feu disposant d'une licence du Broker de décryptage :
  - Le nom de la licence change automatiquement en Broker de paquets de réseau après le redémarrage du pare-feu.

    Vous devez redémarrer le pare-feu pour que la licence prenne effet et mettre à jour l'interface utilisateur, que le pare-feu soit un pare-feu autonome, qu'il fasse partie d'une paire haute disponibilité ou que vous transfériez les licences du Broker de paquets de réseau aux pare-feu depuis Panorama.
  - PAN-OS traduit tous les profils de transfert de broker de déchiffrement existants (**Profiles (Profils)** > **Decryption (déchiffrement)** > **Forwarding Profile (Profil de transfert de déchiffrement)**) en profils de courtier de paquets.
  - PAN-OS traduit toutes les règles de Politique de déchiffrement existantes pour transférer le trafic vers les chaînes de sécurité en règles de politique de Broker de paquets de réseau.
  - PAN-OS supprime le profil de Broker de déchiffrement de l'interface utilisateur et le remplace par le profil du Broker de paquets de réseau (**Profiles (Profils)** > **Packet Broker (Broker de paquets**), et ajoute également la politique du Broker de paquets de réseau (**Policies (Politiques)** > **Network Packet Broker (Broker de paquets de réseau)**).

 ©2024 Palo Alto Networks, Inc.

- Lorsque vous passez à PAN-OS 10.0 à partir de PAN-OS 10.1 :
  - PAN-OS traduit tous les profils de Broker de paquets existants en profils de transfert de broker de déchiffrement.
  - PAN-OS supprime la base de règles du Broker de paquets de réseau et imprime un message d'avertissement. Vous devez reconfigurer les règles de politique du Broker de paquets de réseau en tant que règles de stratégie de déchiffrement pour le transfert de déchiffrement.
  - Le nom de la licence reste Broker de paquets de réseau (le nom de la licence passe de Broker de déchiffrement à Broker de paquets de réseau dans toutes les versions PAN-OS après un redémarrage et n'affecte pas le fonctionnement de Broker de déchiffrement). Cependant, la fonctionnalité est la fonctionnalité de Broker de déchiffrement, et non la fonctionnalité de Broker de paquets de réseau.
  - PAN-OS supprime le profil de Broker de paquets de réseau de l'interface utilisateur et le remplace par le profil de transfert de déchiffrement, et supprime également la politique du Broker de paquets de réseau de l'interface utilisateur (il n'y a pas de remplacement ; vous utilisez les règles de politique de déchiffrement pour transférer uniquement les transferts déchiffrés Trafic proxy vers les chaînes de sécurité).

Conditions requises pour utiliser le Broker de paquets de réseau :

- Vous devez installer une licence gratuite Broker de paquets sur le pare-feu. Sans la licence gratuite, vous ne pouvez pas accéder à la politique et au profil de Broker de paquets dans l'interface.
- Le pare-feu doit avoir au moins deux interfaces Ethernet de couche 3 disponibles à utiliser comme une paire dédiée d'interfaces de transfert de broker de paquets.
  - Vous pouvez configurer plusieurs paires d'interfaces de transfert de Broker de paquets de réseau dédiées pour vous connecter à différentes chaînes de sécurité.
  - Pour chaque chaîne de sécurité, la paire d'interfaces de Broker de paquets de réseau dédiées doit se trouver dans la même zone de sécurité.

    *La stratégie de sécurité doit autoriser le trafic entre chaque ensemble apparié d'interfaces Network Packet Broker. La règle de stratégie de sécurité **intrazone-default** autorise le trafic à l'intérieur de la même zone par défaut. Cependant, si vous avez une règle de politique « Tout refuser » plus tôt dans la base de règles de politique, vous devez créer une règle d'autorisation explicite pour autoriser le trafic Network Packet Broker.*
  - La paire d'interfaces dédiées se connecte aux premier et dernier appareils d'une chaîne de sécurité.

    Broker de paquets de réseau prend en charge les chaînes de sécurité routées de couche 3 et les chaînes de sécurité de passerelle transparente de Couche 1. Pour les chaînes de couche 3 routées, une paire d'interfaces de transfert de broker de paquets peut se connecter à plusieurs chaînes de sécurité de couche 3 à l'aide d'un commutateur, d'un routeur ou d'un autre périphérique correctement configuré pour effectuer le routage de couche 3 requis entre le pare-feu et les chaînes de sécurité.
- Les interfaces de transfert du Broker de paquets de réseau dédiées ne peuvent pas utiliser de protocoles de routage dynamique.

 ©2024 Palo Alto Networks, Inc.

- Aucun des dispositifs de la chaîne de sécurité ne peut modifier l'adresse IP source ou de destination, le port source ou de destination, ou le protocole de la session d'origine car le pare-feu ne serait pas en mesure de faire correspondre la session modifiée à la session d'origine et donc supprimerait le trafic .
- Vous devez activer le pare-feu pour **autoriser le transfert de contenu** déchiffré (**Device** > **Setup** > **Content-ID).**

Le broker de paquets de réseau prend en charge :

- Trafic TLS déchiffré, TLS non déchiffré et non TLS.
- SSL Forward Proxy, SSL Inbound Inspection et trafic SSH chiffré.
- Chaînes de sécurité de couche 3 acheminées.
- Chaînes de sécurité de couche 1 de passerelle transparente.

  Vous pouvez configurer les chaînes de sécurité de passerelle transparents de couche 3 et de couche 1 routées sur le même pare-feu, mais vous devez utiliser différentes paires d'interfaces de transfert pour chaque type.
- Flux de trafic unidirectionnel à travers la chaîne : tout le trafic vers la chaîne sort du pare-feu sur une interface dédiée et retourne au pare-feu sur une autre interface dédiée, de sorte que tout le trafic circule dans le même sens via la paire d'interfaces de Broker de paquets de réseau dédiées.

  Les deux interfaces de transfert de pare-feu doivent se trouver dans la même zone.
- Flux de trafic bidirectionnel à travers la chaîne de sécurité :
  - Le trafic client-serveur (c2s) sort du pare-feu sur une interface de courtier de pare-feu dédiée et retourne au pare-feu sur une autre interface de broker de pare-feu dédiée.
  - Le trafic serveur-client (s2c) utilise les deux mêmes interfaces de pare-feu dédiées que le trafic c2s, mais le trafic circule dans le sens opposé à travers la chaîne de sécurité. L'interface du broker de pare-feu sur laquelle le trafic s2c va vers la chaîne est la même interface sur laquelle le trafic c2s revient de la chaîne vers le pare-feu. L'interface du broker de pare-feu sur laquelle le trafic s2c retourne au pare-feu est la même interface sur laquelle le trafic c2s sort vers la chaîne.

    Les deux interfaces de transfert de pare-feu doivent se trouver dans la même zone.

Le Broker de paquets de réseau ne prend pas en charge le trafic SSH de multidiffusion, de diffusion ou déchiffré.

 ©2024 Palo Alto Networks, Inc.

Fonctionnement du Broker de paquets réseau

Le flux de travail de haut niveau pour connecter le pare-feu à une chaîne de dispositifs de sécurité tiers est :

1. Identifiez le trafic TLS non déchiffré, TLS déchiffré et non TLS (TCP et UDP) à transférer.
2. Identifiez la topologie de la chaîne de sécurité. Déterminez si les périphériques de chaque chaîne de sécurité transfèrent le trafic de manière transparente (par passerelle) ou si les périphériques acheminent le trafic en fonction des informations de la couche 3. L'utilisation de plusieurs chaînes de sécurité permet d'équilibrer la charge du trafic. En outre, décidez s'il faut contourner la chaîne de sécurité (le trafic passe par un traitement normal sur le pare-feu et est transféré ou bloqué en conséquence) ou bloquer le trafic si une chaîne de sécurité échoue à un contrôle d'intégrité.
3. Installez la licence gratuite du Broker de paquets de réseau sur les pare-feu qui transféreront le trafic vers la ou les chaînes de sécurité.
4. Identifiez une ou plusieurs paires d'interfaces de pare-feu pour transférer le trafic vers une ou plusieurs chaînes de sécurité et activez le Broker de paquets de réseau sur ces interfaces.
5. Configurez au moins un profil de Broker de paquets.
6. Configurez au moins une politique de Broker de paquets de réseau.

Pour utiliser une chaîne de dispositifs de sécurité tiers pour inspecter le trafic, vous configurez trois objets sur le pare-feu :

- **Interfaces** : une ou plusieurs paires d'interfaces de pare-feu Ethernet de couche 3 pour transférer le trafic du pare-feu vers la chaîne de sécurité et recevoir le trafic traité en retour de la chaîne de sécurité. Configurez les paires d'interfaces du Broker de paquets de réseau avant de configurer les profils et les règles de stratégie, car vous devez spécifier les paires d'interfaces dans les profils.
- **Packet Broker profiles (profils du broker de paquets)** : les profils contrôlent la manière de transférer le trafic que vous définissez dans une stratégie vers une chaîne de sécurité. Chaque règle de politique du Broker de paquets de réseau est associée à un profil de Broker de paquets. Les profils définissent si la chaîne de sécurité est une chaîne de couche 3 routée ou une chaîne de passerelle transparente de couche 1, le sens du trafic à travers la chaîne (unidirectionnel ou bidirectionnel), les interfaces de pare-feu du Broker de paquets de réseau dédiées et comment surveiller la santé de la connexion entre le pare-feu et la chaîne de sécurité. Pour plusieurs chaînes de sécurité de couche 3 routées, vous pouvez spécifier le premier et le dernier périphérique de chaque chaîne et une méthode de distribution de session (équilibrage de charge) pour le trafic associé.
- **Network Packet Broker policy rules**: (Règles de politique du broker de paquets de réseau) : les règles de stratégie définissent le trafic d'application à transmettre à chaque chaîne de sécurité ou à équilibrer la charge pour plusieurs chaînes acheminées (couche 3). Les règles de politique définissent la source et la destination, les utilisateurs, les applications et les services du trafic à transmettre à une chaîne de sécurité. Les règles de politique définissent également le type de trafic à transmettre à une chaîne de sécurité : vous pouvez sélectionner le trafic TLS déchiffré, le trafic TLS non déchiffré, le trafic non TLS ou toute combinaison de types de trafic. Vous ajoutez également un profil de Broker de paquets dans chaque règle de politique pour spécifier

 ©2024 Palo Alto Networks, Inc.

la chaîne de sécurité vers laquelle transférer le trafic (et toutes les autres caractéristiques du profil).

Utilisez Policy Optimizer (Optimisateur de police) pour réviser et renforcer les règles de politique du Broker de paquets de réseau.

Pour faire correspondre le trafic des applications aux règles de politique du Broker de paquets de réseau, le Broker de paquets de réseau recherche les applications dans le cache App-ID du pare-feu. Si l'application n'est pas dans le cache App-ID, le pare-feu contourne la chaîne de sécurité et applique au trafic toute inspection des menaces configurée dans la règle d'autorisation de la politique de sécurité. Si l'application se trouve dans le cache App-ID, le pare-feu transfère le trafic à la chaîne de sécurité de la manière spécifiée par la règle de politique du Broker de paquets de réseau et son profil de Broker de paquets associé.

Pour le trafic TLS et non TLS non déchiffré, le pare-feu installe l'application dans le cache App-ID lors de la première session, de sorte que le pare-feu traite le trafic comme spécifié dans la stratégie et le profil du Broker de paquets de réseau

Pour le trafic TLS déchiffré, lors de la *first session (première session)* d'une application, le Broker de paquets de réseau ne sait pas que la session est en cours de déchiffrement et considère « ssl » comme l'application. L'application spécifique sous-jacente n'est pas encore connue ou installée dans le cache App-ID, donc la recherche du courtier échoue et le trafic contourne la chaîne de sécurité. Le trafic est toujours soumis à toute inspection de menace configurée sur la règle d'autorisation de la politique de sécurité. Lorsque le pare-feu décrypte le trafic, le pare-feu apprend l'application spécifique et l'installe dans le cache App-ID. Pour la deuxième session déchiffrée et les suivantes pour la même application, les recherches du Broker de paquets de réseau réussissent car l'application spécifique se trouve désormais dans le cache App-ID et le pare-feu transfère le trafic vers la chaîne de sécurité comme prévu.

 ©2024 Palo Alto Networks, Inc.

Préparez-vous à déployer le Broker de paquets de réseau

Effectuez les actions suivantes pour préparer le déploiement du Broker de paquets de réseau :

1. Obtenez et activez la licence gratuite du Broker de paquets de réseau.
   1. Ouvrez une session dans le portail de support client.
   2. Sélectionnez **Assets (Ressources)** > **Devices (Périphériques)** sur le panneau de navigation de gauche.
   3. Trouvez le périphérique sur lequel vous souhaitez activer l'agent de déchiffrement ou la mise en miroir du port de décryptage, puis sélectionnez **Actions** (l'icône en forme de crayon).
   4. Sous Activate Licenses (Activer les licences), sélectionnez **Activate Feature License (Activer la licence de fonctionnalité)**
   5. Sélectionnez la licence gratuite **Network Packet Broker (Broker de paquets de réseau)**.
   6. Cliquez sur **Agree and Submit (Accepter et envoyer)**.
2. Installez la licence sur le pare-feu.
   1. Sélectionnez **Device (Périphériques)** > **Licenses (Licences)**.
   2. Cliquez sur **Retrieve license keys from license server (Récupérer les clés de licence auprès du serveur de licences)**.
   3. Vérifiez que la page **Device** > **Licenses** (licences de périphérique) indique que la licence **Network Packet Broker (Broker de paquets de réseau)** est désormais active sur le pare-feu.
   4. Redémarrez le pare-feu (**Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**). Le Broker de paquets de réseau n'est pas disponible pour la configuration tant que le pare-feu n'a pas redémarré.

   Vous pouvez pousser la licence du Broker de paquets de réseau de Panorama vers des pare-feu gérés. Vous devez redémarrer les pare-feu pour que la licence prenne effet et mettre à jour l'interface utilisateur.

©2024 Palo Alto Networks, Inc.

3. Activez le cache App-ID pour le Broker de paquets de réseau
   1. Le cache App-ID est désactivé par défaut. Activez-le à l'aide de la commande CLI du mode de configuration :

      ```
      admin@PA-3260# set deviceconfig setting application cache yes
      ```

   2. Activer le pare-feu pour utiliser le cache App-ID pour identifier les applications :

      ```
      admin@PA-3260# set deviceconfig setting application use-cache-
      for-identification yes
      ```

   Vérifiez que les paramètres indiquent que le `cache d'application` est défini sur `yes` et que `Use cache for appid` est défini sur `yes`:

   ```
   admin@PA-3260> show running application setting Application
    setting : Cache d'application : oui Supernode : oui Heuristique :
    oui Seuil de cache : 1 Contourner lorsque la limite de file
    d'attente dépasse : pas d'appid Traceroute : oui Seuil TTL
    Traceroute : 30 Utiliser le cache pour appid : oui Utiliser des
    appsigs simples pour ident : oui Utiliser le cache AppID sur SSL/
   SNI : no Capture inconnue : sur Max. sessions inconnues : 5000
    Sessions inconnues en cours : 33 Capture d'application : hors
   ```

   ```
   utilisation actuelle de la mémoire de signature APPID : 16768 Ko
    (16461 Ko réels) TCP 1 C2S : regex 11898 états TCP 1 S2C : regex
    4549 états UDP 1 C2S : regex 4263 états UDP 1 S2C : regex 1605
    états
   ```

4. Activez le pare-feu pour **Allow forwarding of decrypted content (autoriser le transfert de contenu décrypté)** (**Device (Appareil)** > **Setup (Configuration)** > **Content-ID (ID de contenu)**).
5. Identifiez le trafic que vous souhaitez transférer vers une ou plusieurs chaînes de sécurité.
6. Identifiez la topologie de chaque chaîne de sécurité et déterminez s'il faut utiliser le transfert de passerelle transparente de couche 1 ou le transfert de couche 3 acheminé, qui détermine le type de chaîne de sécurité que vous configurez sur le pare-feu. Les considérations comprennent :
   - Que vous souhaitiez équilibrer la charge du trafic sur plusieurs chaînes (utilisez une chaîne de sécurité de couche 3 routée pour répartir les sessions sur plusieurs chaînes via un routeur, un commutateur ou un autre périphérique de routage), utilisez une seule chaîne ou utilisez différentes chaînes de sécurité pour différents types de trafic. Pour plusieurs chaînes de passerelle transparente de couche 1, vous avez besoin d'une paire d'interfaces de pare-feu dédiées pour chaque chaîne de sécurité car la connexion de couche 1 n'est pas routée.
   - S'il faut utiliser un flux de trafic unidirectionnel ou bidirectionnel à travers la chaîne de sécurité.
7. Décidez des paires d'interfaces de pare-feu à utiliser comme interfaces de transfert du Broker de paquets de réseau dédiées.
   - Pour les chaînes de passerelle transparente de couche 1, vous avez besoin d'une paire d'interfaces de pare-feu dédiées pour chaque chaîne de sécurité de couche 1. Vous pouvez

 ©2024 Palo Alto Networks, Inc.

configurer des règles de politique pour envoyer un trafic spécifique à différentes chaînes de sécurité.

- Pour les chaînes de couche 3 routées, une paire dédiée d'interfaces de pare-feu peut équilibrer la charge du trafic entre plusieurs chaînes de sécurité de couche 3 via un commutateur, un routeur ou un autre périphérique compatible avec le routage.
- Pour les chaînes de couche 3 routées, vous pouvez utiliser plusieurs paires d'interfaces de pare-feu dédiées pour envoyer un trafic spécifique à différentes chaînes de sécurité en utilisant différentes règles de politique.



La stratégie de sécurité doit autoriser le trafic entre chaque ensemble apparié d'interfaces Network Packet Broker. La règle de stratégie de sécurité ***intrazone-default*** *autorise le trafic à l'intérieur de la même zone par défaut. Cependant, si vous avez une règle de politique « Tout refuser » plus tôt dans la base de règles de politique, vous devez créer une règle d'autorisation explicite pour autoriser le trafic Network Packet Broker.*

 ©2024 Palo Alto Networks, Inc.

Chaîne de sécurité de la passerelle transparente

Une chaîne de sécurité de la passerelle transparent de couche 1 transfère le trafic d'une interface de pare-feu via une série de dispositifs de sécurité d'inspection et de traitement des données directement connectés, puis vers une autre interface de pare-feu sans avoir besoin d'acheminer le trafic.

Avant de configurer une chaîne de sécurité de couche 1 Transparent Bridge, procédez comme Préparez-vous à déployer le Broker de paquets de réseau, notamment en vous assurant que les connexions physiques entre le pare-feu et les périphériques de la chaîne de sécurité sont correctes et que vous autorisez le pare-feu à transférer le contenu décrypté.

Pour répartir les sessions sur plusieurs chaînes de sécurité de la passerelle transparente, créez une chaîne de sécurité de la passerelle transparente de couche 1 sur le pare-feu pour chacune des chaînes de sécurité que vous souhaitez utiliser pour équilibrer la charge du trafic. Chaque chaîne de sécurité de la passerelle transparente sur le pare-feu nécessite deux interfaces Ethernet de couche 3 dédiées. Vérifiez que vous disposez de suffisamment d'interfaces Ethernet libres pour la topologie que vous souhaitez configurer.



Les chaînes de sécurité de la passerelle transparente de couche 1 ne peuvent pas basculer vers une autre chaîne de sécurité car elles ne sont pas routées.

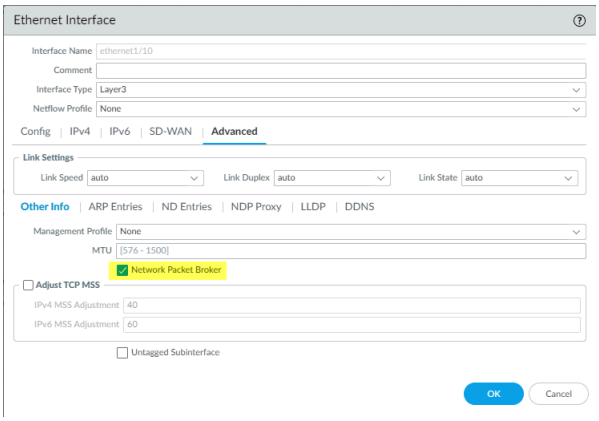
 ©2024 Palo Alto Networks, Inc.

STEP 1 | Activez deux interfaces Ethernet de couche 3 en tant qu'interfaces de transfert du Broker de paquets de réseau.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
2. Sélectionnez une interface Ethernet inutilisée à utiliser comme l'une des deux interfaces de transfert de Broker de paquets de réseau.
3. Définissez **Interface Type (Type d'interface)** sur **Layer 3 (Couche 3)**.
4. Dans l'onglet **Config**, sélectionnez une zone à laquelle affecter l'interface.

   Vous devez configurer les deux interfaces de la chaîne de sécurité dans la même zone.

   La stratégie de sécurité doit autoriser le trafic entre chaque ensemble apparié d'interfaces Network Packet Broker. La règle de stratégie de sécurité ***intrazone-default*** *autorise le trafic à l'intérieur de la même zone par défaut. Cependant, si vous avez une règle de politique « Tout refuser » plus tôt dans la base de règles de politique, vous devez créer une règle d'autorisation explicite pour autoriser le trafic Network Packet Broker.*
5. Dans l'onglet **Config**, afin d'appliquer les bonnes pratiques, utilisez ou créez un routeur virtuel dédié auquel attribuer l'interface. L'utilisation d'un routeur virtuel dédié garantit que le trafic de l'interface du Broker de paquets de réseau reste séparé du reste du trafic.
6. Sélectionnez **Advanced (Avancé)**, puis sélectionnez **Network Packet Broker (Broker de paquets de réseau)** pour activer l'interface.



7. Cliquez sur **OK** pour enregistrer la configuration de l'interface.
8. Répétez cette procédure sur une autre interface Ethernet inutilisée pour configurer l'autre interface de transfert du Broker de paquets de réseau.

 ©2024 Palo Alto Networks, Inc.

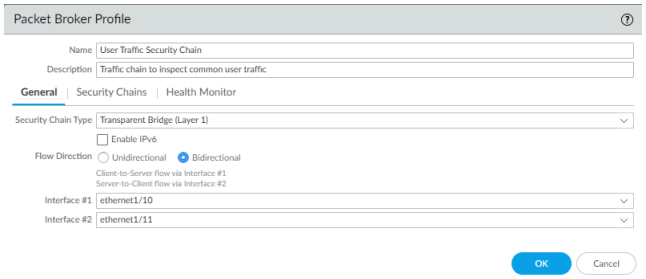
STEP 2 | Configurez un profil Broker de paquets pour contrôler comment transférer le trafic vers la chaîne de sécurité de la passerelle transparente de couche 1.

1. Sélectionnez **Objects (Objets)** > **Packet Broker Profile (profil du Broker de paquets)** et **Add (ajoutez)** un nouveau profil ou modifiez un profil existant.
2. Donnez au profil un **Name (nom)** et une **Description** afin d'identifier facilement son objectif.
3. Dans l'onglet **General (Général)** :
   - Sélectionnez **Transparent Bridge (Layer 1) (Passerelle transparente (couche 1))** comme **Security Chain Type (type de chaîne de sécurité)**.
   - **Enable IPv6 (Activez IPv6)** si le trafic est IPv6.
   - Sélectionnez **Flow Direction (sens du flux)**.

     La topologie de votre réseau détermine s'il faut utiliser des flux unidirectionnels ou bidirectionnels. La performance est approximativement la même avec l'une ou l'autre méthode.

     Pour utiliser une interface de pare-feu pour transférer les flux de session c2s et s2c vers la chaîne de sécurité et utiliser l'autre interface de pare-feu pour recevoir les deux flux de session en retour de la chaîne de sécurité, sélectionnez **Unidirectional (Unidirectionnel)**.

     Pour utiliser l'**interface n°1** pour transférer le flux c2s vers la chaîne de sécurité et recevoir le flux s2c de la chaîne de sécurité, et utiliser l'**interface n°2** pour transférer le flux s2c vers la chaîne de sécurité et recevoir le flux c2s de la chaîne de sécurité, sélectionnez **Bidirectional (Bidirectionnel)**.
   - Spécifiez la paire d'interfaces de transfert de broker de paquets de réseau dans **Interface #1** et **Interface #2**. Les deux interfaces doivent déjà être activées pour que le Broker de paquets de réseau (voir Préparez-vous à déployer le Broker de paquets de réseau) puisse être utilisé. Faites attention à faire attention à la directionnalité du flux lorsque vous configurez quelle interface est l' **Interface n°1** et quelle interface est l'**interface n°2**.



4. L'onglet **Security Chains (Chaînes de sécurité)** n'est pas utilisé pour les passerelles transparentes
5. Dans l'onglet **Health Monitor (Moniteur de santé)** :
   - Sélectionnez le ou les types de surveillance de l'intégrité que vous souhaitez effectuer afin de pouvoir contrôler ce qui se passe en cas de défaillance de la chaîne de sécurité. Vous pouvez en sélectionner un, deux ou tous parmi **Path Monitoring (Surveillance des**

 ©2024 Palo Alto Networks, Inc.

chemins), **HTTP Monitoring (Surveillance HTTP)** et **HTTP Monitoring Latency (Latence de la surveillance HTTP)**.

Path Monitoring (Surveillance des chemins) : vérifie la connectivité de l'appareil à l'aide de pings.

HTTP Monitoring (surveillance HTTP) pour vérifier la disponibilité des périphériques et les temps de réponse.

HTTP Monitoring Latency (Latence de surveillance HTTP) : vérifie la vitesse et l'efficacité du traitement de l'appareil. Lorsque vous sélectionnez cette option, **HTTP Monitoring (surveillance HTTP)** est également activée automatiquement.

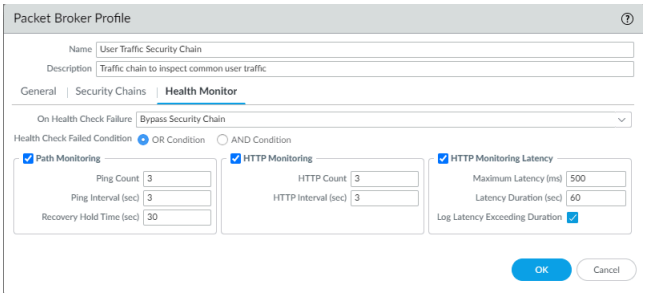
- L'activation d'un ou plusieurs types de surveillance de l'intégrité active les options **On Health Check Failure (En cas d'échec du contrôle d'intégrité)**, qui déterminent comment le pare-feu gère le trafic de la chaîne de sécurité en cas de défaillance de l'intégrité de la chaîne de sécurité. Les options sont **Bypass Security Chain (Contourner la chaîne de sécurité)** et **Block Session (Bloquer la session)**.

  Bypass Security Chain (Contourner la chaîne de sécurité) : le pare-feu transfère le trafic vers sa destination plutôt que vers la chaîne de sécurité et applique les profils de sécurité et les protections configurés au trafic.

  Block Session (Bloquer la session) : le pare-feu bloque la session.

  La méthode que vous sélectionnez dépend de la façon dont vous souhaitez traiter le trafic si vous ne pouvez pas faire passer le trafic à travers la chaîne de sécurité.

- Si vous sélectionnez plusieurs options de vérification de l'état, indiquez si vous souhaitez que le pare-feu considère la vérification de l'état comme ayant échoué (**Health Check Failed Condition (condition d'échec de la vérification de l'état)** si l'une des options de surveillance enregistre une condition d'échec (**OR Condition (condition OU)**) ou uniquement si tous les les options de surveillance sélectionnées enregistrent une condition d'échec (**AND Condition (condition ET)**). Par exemple, si vous activez les trois options de contrôle de santé et que l'une des options enregistre une condition d'échec, si vous avez sélectionné **OR Condition (Condition OU)**, le pare-feu considère que la connexion de la chaîne de sécurité a échoué et exécute l'action que vous avez spécifiée dans **On Health Check Failure (En cas d'échec du contrôle de santé)**. Si vous avez sélectionné **AND Condition (Condition ET)**, le pare-feu considérera toujours que la connexion est saine car deux des métriques de santé sont toujours correctes.



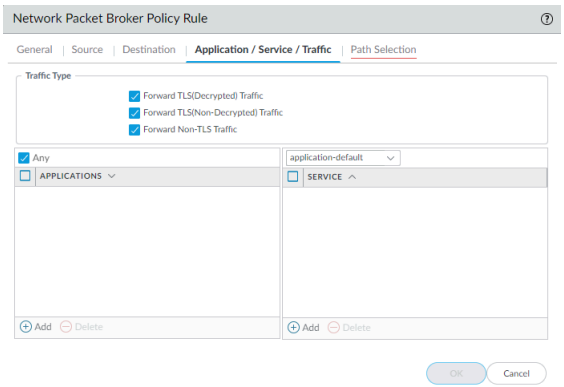
6. Cliquez sur **OK** pour enregistrer le profil.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Configurez une stratégie Broker de paquets pour définir le trafic à transférer vers la chaîne de sécurité de la passerelle transparente de couche 1.

1. Sélectionnez**Policies (Politiques)** > **Network Packet Broker (broker de paquets de réseau)**et **Add (ajoutez)** une nouvelle règle de politique ou modifiez une règle de politique existante.
2. Dans l'onglet **General (Général)**, attribuez un **Name (nom)** et une **Description** à la règle de stratégie afin d'identifier facilement son objectif, ajoutez un **Audit Comment (commentaire d'audit)** et appliquez des balises si vous les utilisez.
3. Dans l'onglet **Source**, identifiez les zones sources, les adresses IP, les utilisateurs et les appareils du trafic que vous souhaitez que la règle transmette à la chaîne de sécurité.
4. Dans l'onglet **Destination**, identifiez les zones de destination, les adresses IP et les périphériques du trafic que vous souhaitez que la règle transmette à la chaîne de sécurité.
5. Dans l'onglet **Application/Service/Traffic (Application/Service/Trafic)**, identifiez les applications et les services que vous souhaitez que la règle transmette à la chaîne de sécurité. À moins que les applications de contrôle de règle que vous prévoyez d'utiliser des ports non standard, telles que les applications personnalisées internes, la meilleure pratique consiste à définir le **Service** sur **Application Default** afin que les applications qui présentent un comportement évasif en utilisant des ports non standard soient bloquées.

   Pour le **Traffic Type (type de trafic)**, sélectionnez tous les types de trafic que vous souhaitez que la règle transmette à la chaîne de sécurité. **Forward TLS(Decrypted) Traffic (Transférer le trafic TLS (déchiffré))** est la sélection par défaut. Vous pouvez sélectionner n'importe quelle combinaison de **Forward TLS(Decrypted) Traffic (transfert de trafic TLS (déchiffré))**, de **Forward TLS(Non-Decrypted) (transfert de TLS (non déchiffré))** et de **Forward Non-TLS Traffic (transfert de trafic non TLS)** à transférer vers la chaîne de sécurité.



6. Dans l'onglet **Path Selection (Sélection du chemin)**, sélectionnez le profil Packet Broker que vous avez créé en Step 2 (étape) ou créez un nouveau profil pour contrôler comment envoyer le trafic contrôlé par la règle de politique vers la chaîne de sécurité.

STEP 4 | Répétez les étapes de Step 1 (étape 1) à Step 3 (étape 3) pour créer d'autres chaînes de sécurité de passerelle transparente de couche 1.

Pour chaque chaîne de sécurité de la passerelle transparente de couche 1 :

- Les deux interfaces Ethernet utilisées comme interfaces de transfert de broker de paquets de réseau doivent être dédiées à chaque chaîne de sécurité. Les interfaces Ethernet utilisées

 ©2024 Palo Alto Networks, Inc.

pour une chaîne de sécurité de passerelle transparente ne peuvent pas être utilisées à d'autres fins ni transporter aucun autre trafic.

- Chaque paire d'interfaces de transfert broker de paquets de réseau se connecte à une chaîne de sécurité de passerelle transparente de couche 1.

Vous pouvez équilibrer la charge du trafic en créant des règles de stratégie de broker de paquets de réseau qui divisent le trafic de manière relativement égale entre les chaînes de sécurité de la passerelle transparente. Vous pouvez également utiliser des règles de politique pour diriger un trafic et des types de trafic spécifiques à travers des chaînes de sécurité spécifiques.

*Les chaînes de sécurité de la passerelle transparente de couche 1 ne peuvent pas basculer vers une autre chaîne de sécurité car elles ne sont pas routées. Utilisez l'onglet **Health Monitor (Surveillance de l'intégrité)** dans le broker de paquets pour configurer la gestion du trafic en cas d'échec d'une chaîne de sécurité de la passerelle transparente.*

©2024 Palo Alto Networks, Inc.

Configurer les chaînes de sécurité routées de la couche 3

Une chaîne de sécurité de couche 3 acheminée transfère le trafic vers une série de dispositifs de sécurité d'inspection et de traitement des données, puis vers le pare-feu à l'aide de deux interfaces de transmission dédiées sur le pare-feu.

Avant de configurer une chaîne de sécurité de couche 3 routée, suivez les étapes pour Préparez-vous à déployer le Broker de paquets de réseau, notamment en vous assurant que les connexions physiques entre le pare-feu et les dispositifs de la chaîne de sécurité sont correctes et que vous autorisez le pare-feu à transférer le contenu déchiffré. Vérifiez que vous disposez de suffisamment d'interfaces Ethernet libres sur le pare-feu pour la topologie que vous souhaitez configurer.

Chaque chaîne de sécurité de couche 3 routée que vous configurez sur le pare-feu nécessite deux interfaces Ethernet de couche 3 dédiées, qui peuvent se connecter à une chaîne de sécurité de couche 3 ou distribuer des sessions (équilibrage de charge) jusqu'à 64 chaînes de sécurité de couche 3 avec un routeur correctement configuré, commutateur ou dispositif similaire entre le pare-feu et les chaînes de sécurité.



Le broker de paquets de réseau ne peut pas transférer le trafic IPv6 sur une chaîne de sécurité de couche 3 routée. Pour transférer le trafic IPv6, utilisez une chaîne de sécurité Transparent Bridge (Passerelle transparente) (couche 1).

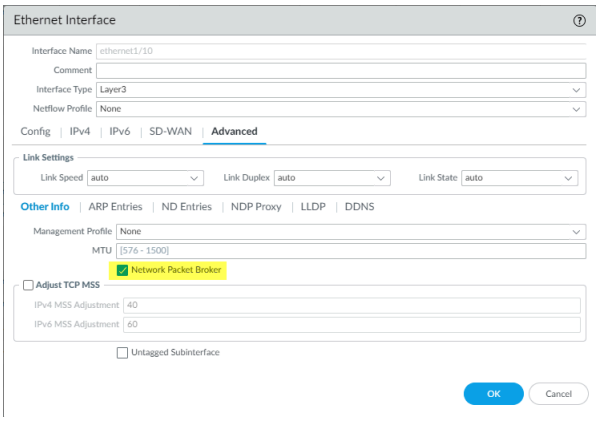
 ©2024 Palo Alto Networks, Inc.

STEP 1 | Activez deux interfaces Ethernet de couche 3 en tant qu'interfaces de transfert du broker de paquets de réseau.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
2. Sélectionnez une interface Ethernet inutilisée à utiliser comme l'une des deux interfaces de transfert de Broker de paquets de réseau.
3. Définissez **Interface Type (Type d'interface)** sur **Layer 3 (Couche 3)**.
4. Dans l'onglet **Config**, sélectionnez une zone à laquelle affecter l'interface.

   Vous devez configurer les deux interfaces de la chaîne de sécurité dans la même zone.

   La stratégie de sécurité doit autoriser le trafic entre chaque ensemble apparié d'interfaces Network Packet Broker. La règle de stratégie de sécurité ***intrazone-default*** *autorise le trafic à l'intérieur de la même zone par défaut. Cependant, si vous avez une règle de politique « Tout refuser » plus tôt dans la base de règles de politique, vous devez créer une règle d'autorisation explicite pour autoriser le trafic Network Packet Broker.*
5. Dans l'onglet **Config**, afin d'appliquer les bonnes pratiques, utilisez ou créez un routeur virtuel dédié auquel attribuer l'interface. L'utilisation d'un routeur virtuel dédié garantit que le trafic de l'interface du Broker de paquets de réseau reste séparé du reste du trafic.
6. Sélectionnez **Advanced (Avancé)**, puis sélectionnez **Network Packet Broker (Broker de paquets de réseau)** pour activer l'interface.



7. Cliquez sur **OK** pour enregistrer la configuration de l'interface.
8. Répétez cette procédure sur une autre interface Ethernet inutilisée pour configurer l'autre interface de transfert du broker de paquets de réseau.

 ©2024 Palo Alto Networks, Inc.

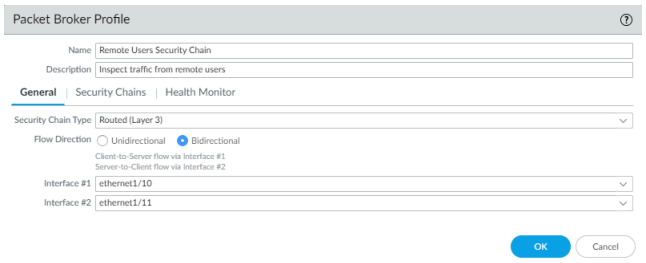
STEP 2 | Configurez un profil de broker de paquets pour contrôler comment transférer le trafic vers la chaîne de sécurité de couche 3 routée.

1. Sélectionnez **Objects (Objets)** > **Packet Broker Profile (profil de broker de paquets)** et **Add (ajoutez)** un nouveau profil ou modifiez un profil existant.
2. Donnez au profil un **Name (nom)** et une **Description** afin d'identifier facilement son objectif.
3. Dans l'onglet **General (Général)** :
   - Sélectionnez **Routed (Layer 3) (Routé (couche 3)** comme **Security Chain Type (type de chaîne de sécurité)**.
   - Sélectionnez **Flow Direction (sens du flux)**.

     La topologie de votre réseau détermine s'il faut utiliser des flux unidirectionnels ou bidirectionnels. La performance est approximativement la même avec l'une ou l'autre méthode.

     Pour utiliser une interface de pare-feu pour transférer les flux de session c2s et s2c vers la chaîne de sécurité et utiliser l'autre interface de pare-feu pour recevoir les deux flux de session en retour de la chaîne de sécurité, sélectionnez **Unidirectional (Unidirectionnel)**.

     Pour utiliser l'**interface n°1** pour transférer le flux c2s vers la chaîne de sécurité et recevoir le flux s2c de la chaîne de sécurité, et utiliser l'**interface n°2** pour transférer le flux s2c vers la chaîne de sécurité et recevoir le flux c2s de la chaîne de sécurité, sélectionnez **Bidirectional (Bidirectionnel)**.
   - Spécifiez la paire d'interfaces de transfert de broker de paquets de réseau dans **Interface #1** et **Interface #2**. Les deux interfaces doivent déjà être activées pour que le Broker de paquets de réseau (voir Step 1 (l'étape 1) puisse être utilisé. Faites attention à faire attention à la directionnalité du flux lorsque vous configurez quelle interface est l' **Interface n°1** et quelle interface est l'**interface n°2**.



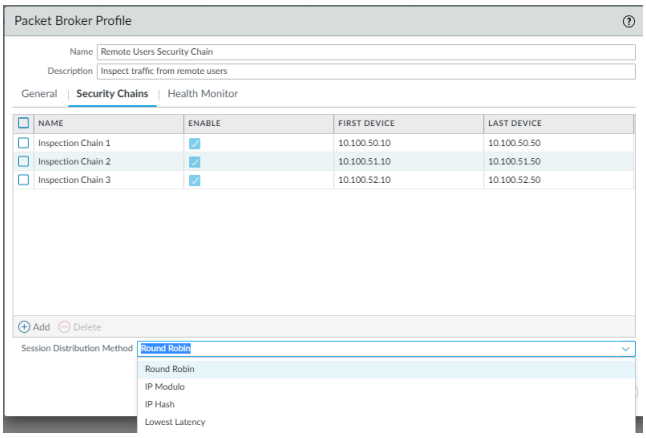
La distribution de session (équilibrage de charge) s'applique uniquement aux nouvelles sessions. Le pare-feu ne rééquilibre pas le trafic au milieu d'une session. Le pare-feu ne distribue les sessions qu'aux chaînes de sécurité dont l'état est « up » (actif, sain).

4. Dans l'onglet **Security Chains (Chaînes de sécurité)Add (ajoutez)** les adresses IP du premier et du dernier périphérique de chaque chaîne de sécurité de couche 3 routée à laquelle vous souhaitez vous connecter. Vous devez spécifier au moins une chaîne de sécurité ou le pare-feu ne peut pas acheminer le trafic vers une chaîne et vous ne pouvez pas enregistrer le profil.

   Si vous spécifiez plusieurs chaînes de sécurité de couche 3 routées, vous devez également placer un routeur, un commutateur ou un périphérique similaire correctement configuré

 ©2024 Palo Alto Networks, Inc.

entre le pare-feu et les chaînes de sécurité pour effectuer le routage approprié. En outre, spécifiez la **Session Distribution Method (méthode de distribution de session)** pour équilibrer la charge du trafic entre les chaînes de sécurité.



5. Dans l'onglet **Health Monitor (Moniteur de santé)** :

   - Sélectionnez le ou les types de surveillance de l'intégrité que vous souhaitez effectuer afin de pouvoir contrôler ce qui se passe en cas de défaillance de la chaîne de sécurité.

     Vous pouvez en sélectionner un, deux ou tous parmi **Path Monitoring (Surveillance des chemins)**, **HTTP Monitoring (Surveillance HTTP)** et **HTTP Monitoring Latency (Latence de la surveillance HTTP)**.

     Path Monitoring (Surveillance des chemins) : vérifie la connectivité de l'appareil à l'aide de pings.

     HTTP Monitoring (surveillance HTTP) pour vérifier la disponibilité des périphériques et les temps de réponse.

     HTTP Monitoring Latency (Latence de surveillance HTTP) : vérifie la vitesse et l'efficacité du traitement de l'appareil. Lorsque vous sélectionnez cette option, **HTTP Monitoring (surveillance HTTP)** est également activée automatiquement.

   - L'activation d'un ou plusieurs types de surveillance de l'intégrité active les options **On Health Check Failure (En cas d'échec du contrôle d'intégrité)**, qui déterminent comment le pare-feu gère le trafic de la chaîne de sécurité en cas de défaillance de l'intégrité de la chaîne de sécurité.

     Si vous configurez plusieurs chaînes de sécurité sur un ensemble d'interfaces Network Packet Broker de couche 3 routées, en cas de défaillance de la chaîne de sécurité, le trafic bascule vers les chaînes de sécurité saines restantes. Si aucune chaîne de sécurité n'est disponible pour gérer le trafic de basculement, le pare-feu exécute l'action configurée **On Health Check Failure (En cas d'échec de la vérification de l'état)**. Les

 ©2024 Palo Alto Networks, Inc.

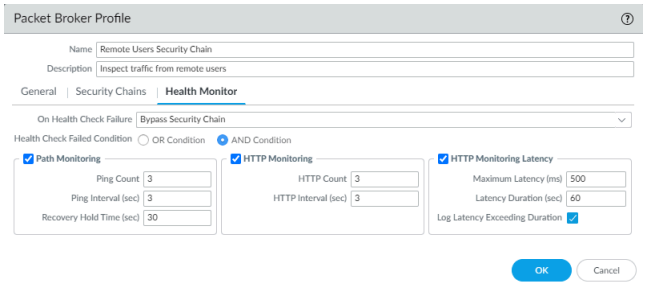
options sont **Bypass Security Chain (Contourner la chaîne de sécurité)** et **Block Session (Bloquer la session)**.

Bypass Security Chain (Contourner la chaîne de sécurité) : le pare-feu transfère le trafic vers sa destination plutôt que vers la chaîne de sécurité et applique les profils de sécurité et les protections configurés au trafic.

Block Session (Bloquer la session) : le pare-feu bloque la session.

La méthode que vous sélectionnez dépend de la façon dont vous souhaitez traiter le trafic si vous ne pouvez pas faire passer le trafic à travers la chaîne de sécurité.

- Si vous sélectionnez plusieurs options de vérification de l'état, indiquez si vous souhaitez que le pare-feu considère la vérification de l'état comme ayant échoué (**Health Check Failed Condition (condition d'échec de la vérification de l'état)** si l'une des options de surveillance enregistre une condition d'échec (**OR Condition (condition OU)**) ou uniquement si tous les les options de surveillance sélectionnées enregistrent une condition d'échec (**AND Condition (condition ET)**). Par exemple, si vous activez les trois options de contrôle de santé et que l'une des options enregistre une condition d'échec, si vous avez sélectionné **OR Condition (Condition OU)**, le pare-feu considère que la connexion de la chaîne de sécurité a échoué et exécute l'action que vous avez spécifiée dans **On Health Check Failure (En cas d'échec du contrôle de santé)**. Si vous avez sélectionné **AND Condition (Condition ET)**, le pare-feu considérera toujours que la connexion est saine car deux des métriques de santé sont toujours correctes.



6. Cliquez sur **OK** pour enregistrer le profil.

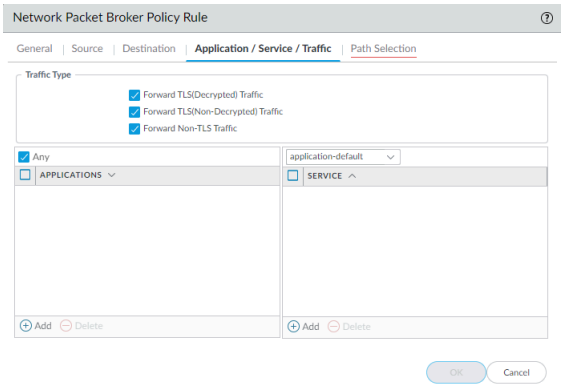
STEP 3 | Configurez une politique de broker de paquets pour définir le trafic à transférer vers la chaîne de sécurité de couche 3 routée.

1. Sélectionnez **Policies (Politiques)** > **Network Packet Broker (Broker de paquets de réseau)** et **Add (Ajoutez)** une nouvelle règle de politique ou modifiez une règle de politique existante.
2. Dans l'onglet **General (Général)**, attribuez un **Name (nom)** et une **Description** à la règle de stratégie afin d'identifier facilement son objectif, ajoutez un **Audit Comment (commentaire d'audit)** et appliquez des balises si vous les utilisez.
3. Dans l'onglet **Source**, identifiez les zones sources, les adresses IP, les utilisateurs et les appareils du trafic que vous souhaitez que la règle transmette à la chaîne de sécurité.
4. Dans l'onglet **Destination**, identifiez les zones de destination, les adresses IP et les périphériques du trafic que vous souhaitez que la règle transmette à la chaîne de sécurité.
5. Dans l'onglet **Application/Service/Traffic (Application/Service/Trafic)**, identifiez les applications et les services que vous souhaitez que la règle transmette à la chaîne de sécurité. À moins que les applications de contrôle de règle que vous prévoyez d'utiliser des

 ©2024 Palo Alto Networks, Inc.

ports non standard, telles que les applications personnalisées internes, la meilleure pratique consiste à définir le **Service** sur **Application Default** afin que les applications qui présentent un comportement évasif en utilisant des ports non standard soient bloquées.

Pour le **Traffic Type (type de trafic)**, sélectionnez tous les types de trafic que vous souhaitez que la règle transmette à la chaîne de sécurité. **Forward TLS(Decrypted) Traffic (Transférer le trafic TLS (déchiffré))** est la sélection par défaut. Vous pouvez sélectionner n'importe quelle combinaison de **Forward TLS(Decrypted) Traffic (transfert de trafic TLS (déchiffré))**, de **Forward TLS(Non-Decrypted) (transfert de TLS (non déchiffré))** et de **Forward Non-TLS Traffic (transfert de trafic non TLS)** à transférer vers la chaîne de sécurité.



6. Dans l'onglet **Path Selection (Sélection du chemin)**, sélectionnez le profil Packet Broker que vous avez créé en Step 2 (étape) ou créez un nouveau profil pour contrôler comment envoyer le trafic contrôlé par la règle de politique vers la chaîne de sécurité.

STEP 4 | Si vous souhaitez créer des chaînes de sécurité de couche 3 routées distinctes qui utilisent différentes paires d'interfaces de pare-feu dédiées, répétez les étapes deStep 1 (étape 1) à Step 3 (étape pour créer d'autres chaînes de sécurité Broker de paquets de réseau. Les deux interfaces Ethernet de couche 3 utilisées comme interfaces de transfert de Broker de paquets réseau doivent être dédiées à la chaîne de sécurité et ne peuvent pas être utilisées à d'autres fins ni acheminer tout autre trafic.

 ©2024 Palo Alto Networks, Inc.

Assistance haute disponibilité du broker de paquets réseau

En plus de la surveillance de l'état du chemin et de la latence disponible dans le profil Packet Broker pour se protéger contre les défaillances de la chaîne de sécurité, vous pouvez également configurer High Availability (haute disponibilité (HA)) sur les pare-feu dotés d'interfaces de transfert du Broker de paquets de réseau pour se protéger contre les défaillances du pare-feu. La configuration à la fois de la surveillance des chemins et de la haute disponibilité protège non seulement contre les défaillances de la chaîne de sécurité, mais également contre les défaillances du pare-feu.

Le Broker de paquets de réseau prend en charge les paires HA active/passive. Les paires Active/Active HA ne sont pas prises en charge car les interfaces de transfert de broker dédiées doivent être spécifiées dans le profil du broker de paquets.

Après un basculement, le trafic SSL déchiffré est réinitialisé car l'état SSL n'est pas synchronisé entre les nœuds haute disponibilité. Le trafic en clair reprend si la session est correctement synchronisée et la séquence TCP est correctement réappris.

©2024 Palo Alto Networks, Inc.

Modifications de l'interface utilisateur pour le Broker de paquets de réseau

Le Broker de paquets de réseau remplace la fonctionnalité du Broker de déchiffrement introduite dans PAN-OS 8.1 et étend ses capacités pour inclure le transfert du trafic TLS et non-TLS non déchiffré ainsi que le trafic TLS déchiffré vers une chaîne de sécurité. Pour prendre en charge le Broker de paquets de réseau, l'interface utilisateur de PAN-OS 11.1 comporte les modifications suivantes :

- Une nouvelle politique (**Policies (Policies)** > **Network Packet Broker (Broker de paquets de réseau)**) vous permet de configurer le trafic spécifique à transférer vers la chaîne de sécurité et d'attacher un profil Packet Broker pour contrôler comment transférer le trafic spécifié vers la chaîne de sécurité.

  Le Broker de déchiffrement a utilisé des règles de stratégie de déchiffrement pour transmettre uniquement le trafic TLS déchiffré à la chaîne de sécurité. Les nouvelles règles de politique du Broker de paquets de réseau vous permettent de sélectionner non seulement le trafic TLS déchiffré, mais également le trafic TLS chiffré et le trafic non-TLS.

- Un nouveau profil (**Objects** > **Packet Broker Profile (Profil de broker de paquets d'objets)**) remplace l'ancien profil **Objects** > **Decryption (déchiffrement)** > **Decryption Broker Profile (Profil de broker de déchiffrement)** et vous permet de configurer exactement comment transférer le trafic vers la chaîne de sécurité et surveiller l'état du chemin et de la latence. Dans l'onglet **General (Général)**, les noms des champs dans lesquels vous saisissez la paire d'interfaces de transfert Network Packet Broker du pare-feu dédié sont passés de « Interface principale » et « Interface secondaire » à **Interface 1** et **Interface 2** respectivement.
- Lorsque vous sélectionnez **Policies (Politiques)** > **Network Packet Broker (Broker de paquets de réseau)**, vous pouvez ensuite sélectionner l'une des options de Rule Usage (utilisation des règles) dans **Policy Optimizer (optimisateur de politique)** pour afficher les informations d'utilisation de la politique du Broker des paquets de réseau. Les statistiques de **Rule Usage (utilisation des règles)** vous aident à évaluer si vous devez conserver les règles du Broker des paquets de réseau inutilisées ou si vous pouvez les supprimer et renforcer la base de règles pour réduire la surface d'attaque.
- Étant donné que le Broker des paquets de réseau a remplacé le Broker de déchiffrement, la politique de déchiffrement ne gère plus le trafic de courtage vers une chaîne de sécurité. Pour cette raison, dans l'onglet **Options**, l'option **Decrypt and Forward (Déchiffrer et transférer)** n'est plus une **Action** que la politique peut accepter, et le champ **Forwarding Profile (Profil de transfert)** a également été supprimé car désormais, seuls les profils de déchiffrement sont valides sur les politiques de déchiffrement.
- Dans **Network (réseau)** > **Interfaces** > , lorsque vous définissez **Interface Type (Type d'interface** sur Couche 3, puis sélectionnez l'onglet **Advanced (Avancé)**, le nom de la case à cocher pour activer l'interface en tant qu'interface de transfert pour le Broker de paquets de réseau est passé de « Decrypt Forward » à **Network Packet Broker (Broker de paquets de réseau)**.

 ©2024 Palo Alto Networks, Inc.

- Pour les **Device (périphérique)** > **Admin Roles (rôles d'administrateur)** dans l'onglet **Web UI**, il y a deux changements :
  - Sous **Policies (Politiques)**, vous pouvez désormais configurer les autorisations du rôle d'administrateur de **Network Packet Broker (Broker de paquets de réseau)**.
  - Sous **Objects (Objets)**, l'option **Decryption (déchiffrement)** > **Forwarding Profile (Profil de transfert)** est supprimée et remplacée par l'option **Packet Broker Profile (Profil de paquets de réseau)** pour les autorisations de rôle d'administrateur.
- Sur les pare-feu, pour **Monitor (Surveiller)** > **Manage Custom Reports (Gérer les rapports personnalisés)**, lorsque vous sélectionnez **Traffic Log (Journal de trafic)** dans les journaux détaillés comme **Database (base de données)**, dans la liste **Available Columns (colonnes disponibles)**, vous pouvez désormais sélectionner **Forwarded to Security Chain (Transféré à la chaîne de sécurité)**.

  Sur Panorama, pour **Monitor (Surveiller)** > **Manage Custom Reports (gérer les rapports personnalisés)**, lorsque vous sélectionnez **Panorama Traffic Log (Journal de trafic Panorama)** dans les journaux détaillés en tant que **Database (base de données)**, dans la liste des **Available Columns (colonnes disponibles)**, vous pouvez désormais sélectionner **Forwarded to Security Chain (Transféré à la chaîne de sécurité)**.
- Dans le journal du trafic, la colonne « Decrypt Forward » est renommée **Forwarded to Security Chain (Transféré à la chaîne de sécurité)**. Dans la vue détaillée du journal du trafic, dans la section **Flags (Indicateurs)**, la case à cocher « Décrypter le transfert » est renommée en **Forwarded to Security Chain (Transféré vers la chaîne de sécurité)**.
- La licence gratuite pour la fonctionnalité est renommée de « Decryption Broker » en **Packet Broker (Broker de paquets)**. Si vous disposez de la licence gratuite du Broker de déchiffrement sur votre pare-feu, le nom change automatiquement lors de la mise à niveau vers PAN-OS 10.1. Le changement ne concerne que le nom et n'a aucun effet sur la fonctionnalité.

 ©2024 Palo Alto Networks, Inc.

Limitations du Broker de paquets de réseau

La plupart des plates-formes Palo Alto Networks prennent en charge le Broker de paquets de réseau, mais quelques-unes ne le font pas et quelques-unes ont des limites :

- L'assistance n'est pas disponible dans Prisma Access ou dans NSX.
- AWS, Azure et GCP ne prennent en charge que les chaînes de sécurité de couche 3 routées.

Le Broker de paquets de réseau a quelques limitations sur Panorama pour les pare-feu gérés et quelques limitations d'utilisation. Sur Panorama

- Si vous transférez des licences du Broker de paquets de réseau vers des pare-feu gérés, vous devez redémarrer les pare-feu pour que les licences et les éléments d'interface utilisateur associés soient installés.
- Vous ne pouvez pas créer un profil de Broker de paquets dans un contexte **partagé** car vous configurez des interfaces spécifiques dans le profil du Broker de paquets.
- Différents groupes de périphériques ne peuvent pas partager les mêmes profils du Broker de paquets.
- Panorama ne peut pas instaurer une configuration du Broker de paquets de réseau (règles et profils de la politique du Broker de paquets de réseau) vers un groupe de périphériques contenant des pare-feu exécutant une version PAN-OS antérieure à 10.1.

  Si vous souhaitez utiliser le Broker de paquets de réseau dans un groupe d'appareils qui contient des pare-feu sur plusieurs versions de PAN-OS et que certains de ces pare-feu exécutent une version de PAN-OS antérieure à 10.1, vous devez soit mettre à niveau les pare-feu antérieurs à 11.1 vers PAN-OS 11.1 ou supprimer les pare-feu antérieurs à la version 11.1 du groupe d'appareils avant d'instaurer la configuration du Broker de paquets de réseau.

  *Vous pouvez utiliser Panorama pour instaurer un profil de Broker de paquets lié à une règle de politique de déchiffrement aux pare-feu antérieurs à la version 10.1 sur lesquels des licences d'agent de déchiffrement sont installées. L'**Action** de la règle (onglet **Options**) doit être **Decrypt and Forward (Déchiffrer et transférer)** et vous devez lier le profil du Broker de paquets à la règle (paramètre **Decryption Profile (Profil de déchiffrement**dans l'onglet **Options**). Les pare-feu antérieurs à la version 11.1 utilisent le profil du broker de paquets comme profil de transfert de décryptage pour le broker de décryptage. La règle de politique de déchiffrement détermine le trafic auquel le pare-feu applique le profil.*

  Le trafic contrôlé par la règle de politique de déchiffrement doit être un trafic SSL déchiffré (le broker de déchiffrement ne prend pas en charge le trafic SSL chiffré ou le trafic en texte clair).
- Lorsque vous effectuez une mise à niveau de PAN-OS 10.0 vers PAN-OS 10.1, seules les règles de stratégie de déchiffrement locales qui sont utilisées pour le Broker de déchiffrement sont migrées vers les règles du Broker de paquets de réseau. Les règles de politique du broker de déchiffrement qui ont été transmises de Panorama aux pare-feu sont migrées automatiquement sur Panorama mais ne sont pas migrées automatiquement sur le pare-feu. Les règles de politique du Broker de déchiffrement configurées localement sur un pare-feu sont migrées vers les règles du Broker de paquets de réseau sur ce pare-feu uniquement. Pour

 ©2024 Palo Alto Networks, Inc.

les règles configurées sur Panorama, Panorama doit effectuer une autre poussée de validation vers le pare-feu pour synchroniser les règles du Broker de déchiffrement qui ont été migrées vers les règles du Broker de paquets de réseau sur Panorama.

- Lorsque vous passez de PAN-OS 11.1 à PAN-OS 10.0, les règles du Broker de paquets de réseau sont automatiquement supprimées.

Le Broker de paquets de réseau a également quelques limitations d'utilisation :

- Si le pare-feu du Broker de paquets de réseau exécute également la traduction d'adresses réseau source (SNAT) et que le trafic est un trafic en texte clair, le pare-feu exécute le NAT sur le trafic et transmet le trafic à la chaîne de sécurité. Les appareils de la chaîne de sécurité ne voient que les adresses NAT, pas les adresses sources d'origine :

  1. Le pare-feu effectue un NAT sur le trafic du client.
  2. Le pare-feu transmet le trafic à la chaîne de sécurité et tout routage doit être basé sur l'adresse NAT.
  3. Étant donné que l'adresse source dans le paquet est désormais l'adresse NAT, les appareils de la chaîne de sécurité ne voient que l'adresse NAT. Ils ne voient pas l'adresse source réelle du client.
  4. Lorsque la chaîne de sécurité renvoie le trafic au pare-feu, le résultat est que le pare-feu ne sait pas qui est l'utilisateur.

  Vous pouvez découvrir qui était l'utilisateur source pour une session en vérifiant les journaux de trafic pour cette session et en corrélant le paquet avec ces journaux. Les journaux de trafic incluent à la fois l'adresse source d'origine, à partir de laquelle vous pouvez déterminer l'utilisateur source, et l'adresse SNAT.

  Vous pouvez éviter ce scénario en effectuant un NAT sur un périphérique autre que le pare-feu.

- Le trafic SSH, multidiffusion et diffusion déchiffré n'est pas pris en charge.
- L'authentification client n'est pas prise en charge pour l'inspection SSL entrante lorsque des certificats RSA sont utilisés.
- En mode Passerelle transparente de couche 1, si une chaîne de sécurité échoue, il n'y a pas de basculement car lorsque vous utilisez des connexions Passerelle transparente, chaque paire d'interfaces de pare-feu du Broker de paquets de réseau dédiées se connecte à une seule chaîne de sécurité. (Vous ne pouvez pas acheminer le trafic sur la couche 1, vous ne pouvez le transférer qu'au prochain appareil connecté.)
- Vous ne pouvez transférer le trafic IPv6 qu'en mode Passerelle transparente de couche 1. Vous ne pouvez pas transférer le trafic IPv6 en mode Routé (couche 3).
- Vous ne pouvez pas utiliser les interfaces de tunnel ou de bouclage en tant qu'interfaces du Broker de paquets de réseau.
- Les interfaces du Broker de paquets de réseau ne peuvent pas utiliser de protocoles de routage dynamique.
- Les deux interfaces doivent être dans la même zone.
- Les périphériques d'une chaîne de sécurité ne peuvent pas modifier l'adresse IP source, l'adresse IP de destination, le port source, le port de destination ou le protocole de la session d'origine, car le pare-feu serait incapable de faire correspondre la session modifiée à la session d'origine et supprimerait donc le trafic

 ©2024 Palo Alto Networks, Inc.

- La haute disponibilité pour le Broker de paquets de réseau est prise en charge uniquement pour les paires de pare-feu HA actif/passif. La haute disponibilité pour le Broker de paquets de réseau n'est pas prise en charge pour les paires de pare-feu actif/actif.
- La haute disponibilité n'est pas prise en charge pour le trafic SSL. Les sessions SSL sont réinitialisées lors des basculements.
- Lorsque vous effectuez une mise à niveau de PAN-OS 10.0 vers PAN-OS 10.1, les règles de stratégie de déchiffrement locales qui sont utilisées pour le Broker de déchiffrement sont migrées vers les règles du Broker de paquets de réseau.
- Lorsque vous passez de PAN-OS 11.1 à PAN-OS 10.0, les règles du Broker de paquets de réseau sont automatiquement supprimées.

 ©2024 Palo Alto Networks, Inc.

Dépannage du Broker de paquets réseau

Si vous rencontrez des problèmes lors de la configuration du Broker de paquets de réseau, vérifiez les éléments suivants :

- Configuration du pare-feu :
  - Vérifiez l'itinéraire du tronçon suivant sur les paires d'interface de transfert pour vous assurer qu'il spécifie l'interface de périphérique correcte.
  - Adresses IP des périphériques de chaîne et des interfaces de pare-feu et assurez-vous qu'elles sont correctement entrées dans le profil du Broker de paquets.
  - Si la haute disponibilité est activée, vérifiez que les interfaces correctes sont spécifiées dans le profil.
  - Vérifiez le sens de circulation du trafic à travers la chaîne.
  - Assurez-vous que le profil indique le type de chaîne de sécurité approprié.
- Configuration de la chaîne de sécurité; vérifier:
  - Adresses IP, adresses du tronçon suivant et passerelles par défaut pour chaque appareil de la chaîne de sécurité.
  - Configuration de tous les périphériques entre le pare-feu et la chaîne de sécurité (routeurs, commutateurs, etc.) pour l'adressage IP, le tronçon suivant et la mauvaise configuration de la passerelle par défaut.
  - Chemin entre le pare-feu et la chaîne.
- Vérifiez les journaux de trafic du pare-feu pour vérifier que l'indicateur « Transféré » est défini comme prévu pour le trafic négocié.
- Les commandes CLI utiles incluent :
  - `show rulebase network-packet-broker (afficher rulebase network-packet-broker)`
  - `show running network-packet-broker status (afficher l'état d'exécution de network-packet-broker)`
  - `(show running network-packet-broker statisticsafficher les statistiques network-packet-broker en cours d'exécution)`
  - `show running application-cache all (afficher l'exécution du cache d'application tout)`
  - `show running application setting (afficher le paramètre d'application en cours d'exécution)` : vérifiez que le cache App-ID est activé et que le cache est utilisé pour App-ID, vérifiez le paramètre de seuil de cache, etc.

 ©2024 Palo Alto Networks, Inc.

Routage avancé

PAN-OS® fournit un moteur de routage avancé qui permet au pare-feu d'évoluer et de fournir des fonctions de routage stables, hautement performantes et hautement disponibles aux grands centres de données, aux FAI, aux entreprises et aux utilisateurs du cloud. Le moteur de routage avancé simplifie les opérations avec une configuration basée sur des normes, ce qui réduit votre courbe d'apprentissage car elle est similaire à celle des autres fournisseurs de routeurs. Les profils de configuration de protocole et un profil de filtrage granulaire fonctionnent sur plusieurs routeurs logiques et systèmes virtuels. La redistribution d'itinéraire est simplifiée avec un profil de redistribution. Les groupes de pairs BGP et les homologues peuvent hériter de la configuration pour rendre BGP plus agile.

Le moteur de routage avancé prend en charge les itinéraires statiques, BGP, MP-BGP, OSPFv2, OSPFv3, RIPv2, le routage multidiffusion IPv4, BFD, la redistribution, le filtrage d'itinéraire dans le RIB, les listes d'accès, les listes de préfixes et les cartes de routage.

Utilisez le Advanced Routing Engine Migration Reference (Guide de référence de migration du moteur de routage avancé) pour planifier votre migration à partir du moteur de routage hérité et pour voir les différences entre les moteurs de routage hérités et avancés et les exceptions.

Les modèles suivants prennent en charge le moteur de routage avancé :

- PA-7000 Series
- Série PA-5400
- PA-5200 Series
- Série PA-3400
- PA-3200 Series
- Série PA-1400
- Série PA-400
- Série CN
- VM-Series
- Appareil M-700
- Appareil M-600
- Appareil M-500
- Appareil M-300
- Appareil M-200

Découvrez les profils de routage avancés et effectuez les tâches suivantes pour configurer le routage avancé :

- Activer le routage avancé
- Vue d'ensemble du routeur logique
- Configurer un routeur logique
- Créer un itinéraire statique

- Configurer BGP sur un moteur de routage avancé
- Créer des profils de routage BGP
- Créer des filtres pour le moteur de routage avancé
- Configurer OSPFv2 sur un moteur de routage avancé
- Créer des profils de routage OSPF
- Configurer OSPFv3 sur un moteur de routage avancé
- Créer des profils de routage OSPFv3
- Configurer RIPv2 sur un moteur de routage avancé
- Créer des profils de routage RIPv2
- Créer des profils BFD
- Configurer la multidiffusion IPv4
- Configurer MSDP
- Créer des profils de routage multidiffusion
- Créer un MRoute IPv4

 ©2024 Palo Alto Networks, Inc.

Activer le routage avancé

Bien qu'un pare-feu pris en charge puisse avoir une configuration qui utilise le moteur de routage hérité et une configuration qui utilise le moteur de routage avancé, un seul moteur de routage est en vigueur à la fois. Chaque fois que vous modifiez le moteur que le pare-feu utilisera (vous activez ou désactivez le routage avancé pour accéder au moteur avancé ou au moteur hérité, respectivement), vous devez valider la configuration et redémarrer le pare-feu pour que la modification prenne effet.



Avant de passer au moteur de routage avancé, effectuez une sauvegarde de votre configuration actuelle.

De même, si vous configurez Panorama avec un modèle qui active ou désactive le routage avancé, après avoir validé et poussé le modèle vers les périphériques, vous devez redémarrer les périphériques dans le modèle pour que la modification prenne effet.



Lors de la configuration de Panorama, créez des groupes de périphériques et des modèles pour les appareils qui utilisent tous le même paramètre de routage avancé (tous activés ou tous désactivés). Panorama ne transmettra pas les configurations avec le routage avancé activé vers les pare-feu bas de gamme qui ne prennent pas en charge le routage avancé. Pour ces pare-feu, Panorama transmettra une configuration héritée si elle est présente.

Le moteur de routage avancé prend en charge plusieurs routeurs logiques (appelés routeurs virtuels sur le moteur de routage hérité). Le nombre de routeurs logiques pris en charge dépend du modèle de pare-feu et est identique au nombre de routeurs virtuels pris en charge sur le moteur de routage hérité. Le moteur de routage avancé dispose d'options de menu plus pratiques et il existe de nombreux paramètres que vous pouvez facilement configurer dans un profil (authentification, minuteurs, famille d'adresses ou profil de redistribution) que vous appliquez à un groupe d'homologues ou à un homologue BGP, par exemple. Il existe également de nombreux paramètres de routage statique, OSPF, OSPFv3, RIPv2, multidiffusion et BFD sur le moteur de routage avancé.

Le moteur de routage avancé prend en charge le filtrage RIB, ce qui signifie que vous pouvez créer une carte d'itinéraire pour faire correspondre les itinéraires statiques ou les itinéraires reçus d'autres protocoles de routage et ainsi filtrer les itinéraires installés dans le RIB pour le routeur logique. Cette fonction est utile sur les pare-feu avec une capacité RIB ou FIB plus petite; vous pouvez toujours propager les mises à jour de routage nécessaires sans utiliser la mémoire nécessaire ailleurs.

STEP 1 | Effectuez une sauvegarde de votre configuration actuelle avant d'activer le routage avancé.

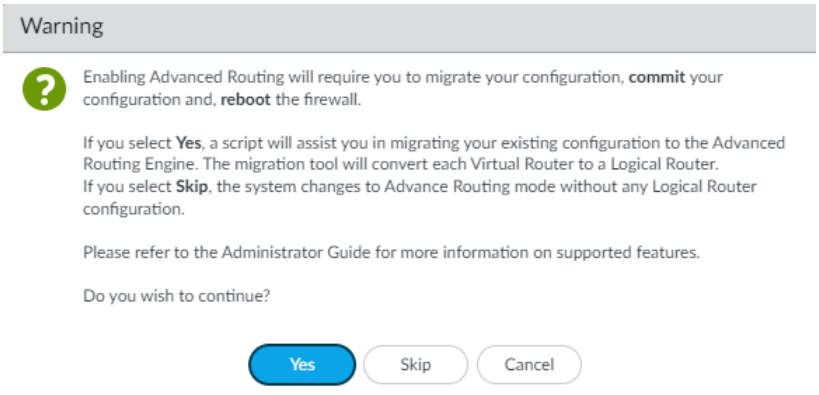
 ©2024 Palo Alto Networks, Inc.

STEP 2 | Activez le moteur de routage avancé.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres généraux.
2. Activer le module de routage avancé



3. Avant de cliquer sur OK, assurez-vous d'avoir effectué une sauvegarde de votre configuration pour le moteur de routage hérité.
4. Cliquez sur **OK**.
5. Un avertissement apparaît:

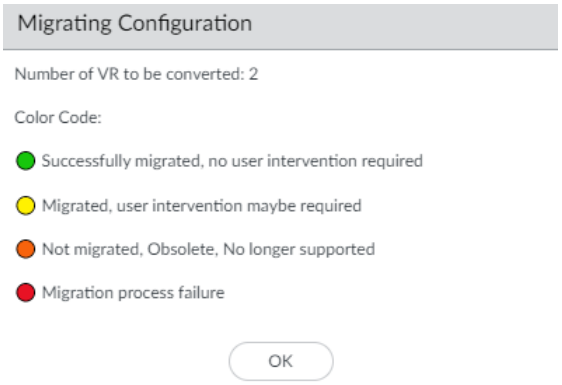


Sélectionnez **Yes (Oui)** pour que le script de migration convertisse chaque routeur virtuel en routeur logique et migre votre configuration vers le moteur de routage avancé. Vous pouvez sélectionner **Skip (Ignorer)** ici pour redémarrer le système avec une configuration

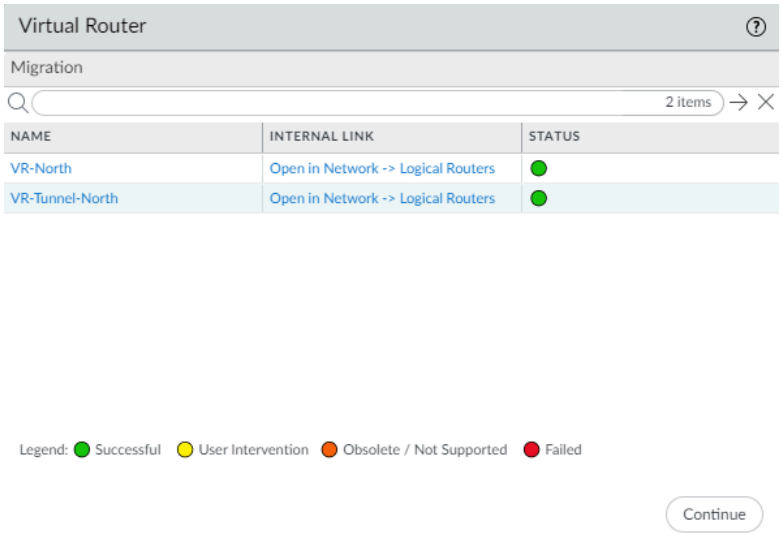
 ©2024 Palo Alto Networks, Inc.

vide. Sélectionnez **Cancel (Annuler)** pour annuler le processus afin d'activer le routage avancé.)

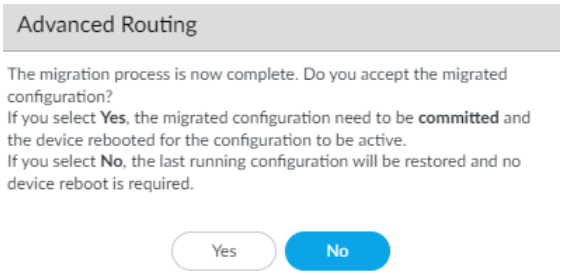
6. Cliquez sur **OK** pour approuver la migration.



7. Les routeurs virtuels, les liens vers les routeurs logiques et leur statut de code couleur sont répertoriés. Résoudre tout problème nécessitant l'intervention de l'utilisateur. Sélectionnez **Continue (Continuer)**

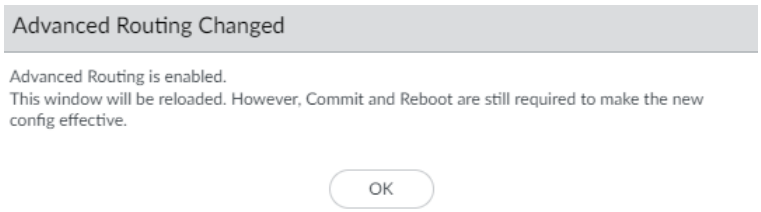


8. Cliquez sur **Yes (Oui)** pour accepter la configuration migrée.



9. (PAN-OS 11.0.2 et versions 11.1 ultérieures) Cliquez sur **OK**

 ©2024 Palo Alto Networks, Inc.



10. **Commit (Validez)**, puis sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)** et **Reboot Device (Redémarrer le périphérique)**. Reconnectez-vous au pare-feu.

    Si la migration échoue, générez le fichier de support technique, connectez-vous au Palo Alto Networks Customer Support Portal (Portail de support client de Palo Alto Networks) et signalez vos problèmes pour obtenir de l'aide sur votre produit.

11. (Facultatif) Après une migration réussie, vous pouvez supprimer tous les routeurs virtuels en utilisant la commande CLI du mode de configuration :

    1. Accédez à la CLI.
    2. Exécutez la commande suivante pour supprimer toutes les configurations du moteur de routage hérité :

    ```
    username@hostname# delete network virtual-router <vr-name>
    ```

    > *Vous pouvez supprimer les routeurs virtuels si vous allez apporter des modifications à la configuration du routeur logique, ce qui rend la configuration du routeur virtuel obsolète, provoquant des échecs de validation. Bien que la suppression des routeurs virtuels évitera les échecs de validation, sachez que la suppression des routeurs virtuels supprimera également définitivement toute la configuration du moteur de routage hérité et que vous ne pourrez pas la récupérer.*

    3. Validez les modifications sur le pare-feu.

    ```
    username@hostname# commit
    ```

    > *Lors de la configuration dans Panorama, vous pouvez sélectionner **Network (Réseau) > (Routeurs virtuels)** pour supprimer tous les routeurs virtuels. Vous devez valider les modifications et les transmettre aux pare-feu appropriés avant de continuer.*

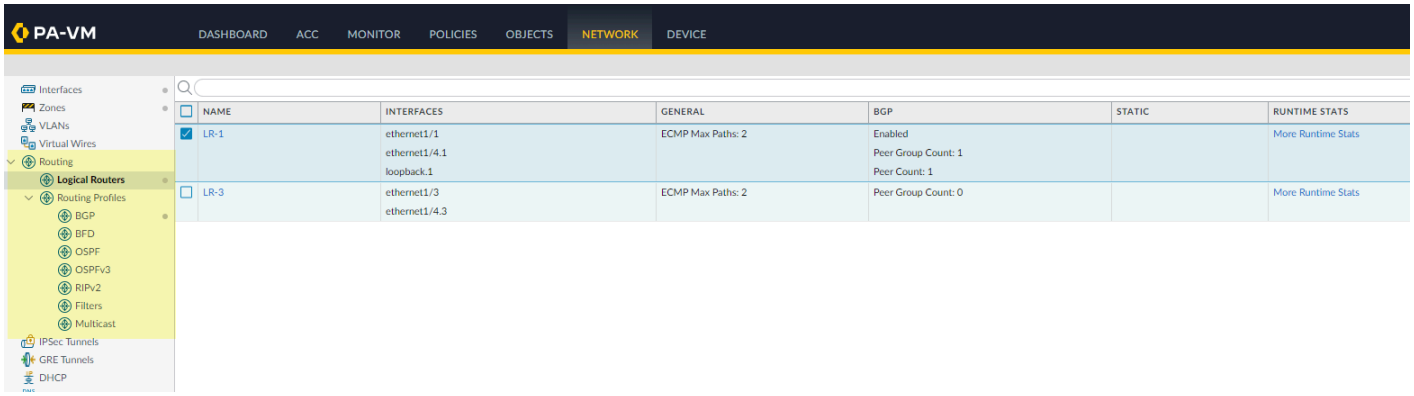
STEP 3 | Reconnectez-vous au pare-feu.

STEP 4 | Sélectionnez **Réseau**.

Notez les éléments de menu, qui sont plus standard de l'industrie et plus détaillés que l'élément unique (routeurs virtuels) du menu hérité. Le **Routage** inclut les **Routeurs logiques**

 ©2024 Palo Alto Networks, Inc.

et les **Profils de routage**, qui incluent**BGP**, **BFD OSPF**, **OSPFv3**, **RIPv2**, les **Filtres**, et la **Multidiffusion**.



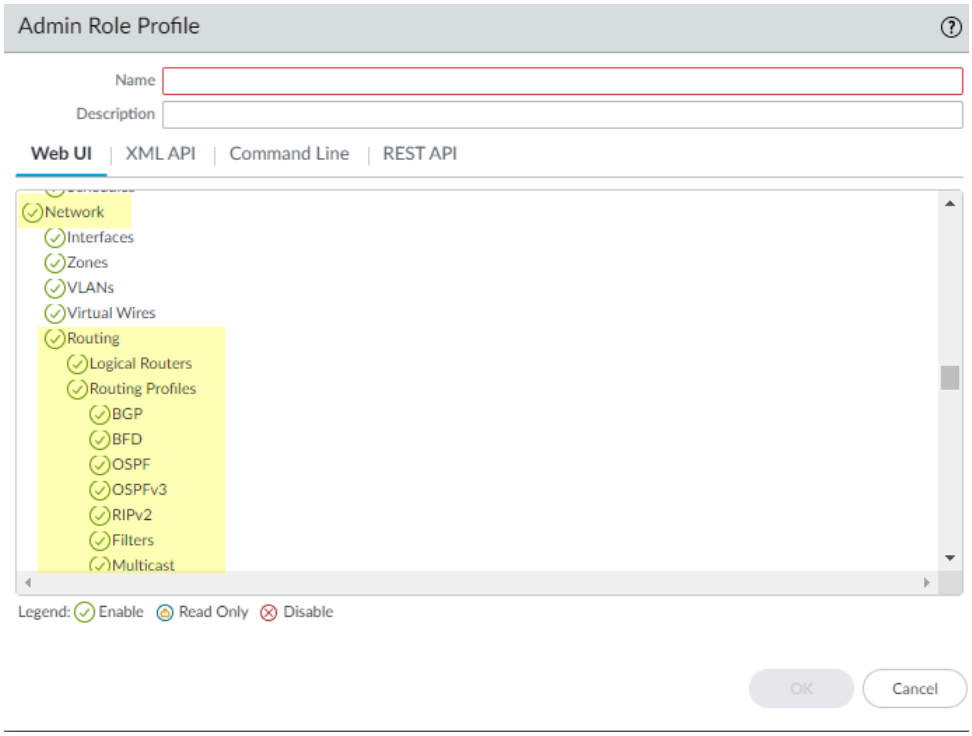
STEP 5 | Sélectionnez **Interfaces** et configurez une ou plusieurs interfaces de couche 3 avec une adresse IP statique ou en tant que client DHCPv4 pour recevoir une adresse attribuée dynamiquement.

STEP 6 | (Facultatif) Créez un profil de rôle d'administrateur pour contrôler l'accès granulaire aux routeurs logiques et aux profils de routage pour un moteur de routage avancé.

1. Sélectionnez **Device (Périphérique)** > **Admin Roles (Rôles administrateur)** et cliquez sur **Add (Ajouter)** pour ajouter un Admin Role Profile (Profil de rôle administrateur) par **Name (Nom)**.
2. Sélectionnez **Web UI**.
3. **Activez**, **désactivez**, ou sélectionnez **Lecture seule** les options suivantes : **Network (Réseau)**, **Routing (Routage)**, **Logical Routers (Routeurs logiques)**, **Routing Profiles**

 ©2024 Palo Alto Networks, Inc.

(Profils de routage), **BGP**, **BFD**, **OSPF**, **OSPFv3**, **RIPv2**, **Filters (Filtres)**, et **Multicast (Multidiffusion)** (Activé par défaut).



4. Cliquez sur **OK**.
5. Affectez le rôle à un administrateur. Configuration du compte administrateur du pare-feu.

STEP 7 | **Commit (Validez)** les modifications.

STEP 8 | Continuez en configurant un routeur logique.

 ©2024 Palo Alto Networks, Inc.

Vue d’ensemble du routeur logique

Le pare-feu utilise des routeurs logiques pour obtenir des itinéraires de Couche 3 vers d'autres sous-réseaux lorsque vous définissez manuellement des itinéraires statiques ou via la participation à un ou plusieurs protocoles de routage de Couche 3 (itinéraires dynamiques). Les itinéraires que le pare-feu obtient par ces méthodes remplissent la base d'informations de routage (RIB) IP du pare-feu. Lorsqu'un paquet est destiné à un autre sous-réseau que celui sur lequel il est arrivé, le routeur logique récupère le meilleur itinéraire dans la base d'informations de suivi (FIB), le place dans les informations de suivi et transfère le paquet au routeur Saut suivant défini dans la base FIB. Le pare-feu utilise le basculement Ethernet pour atteindre d'autres périphériques sur le même sous-réseau IP. (Une exception à l'entrée du meilleur itinéraire dans la base FIB survient lorsque vous utilisez ECMP, auquel cas tous les itinéraires de même coût vont dans la FIB.)

Les interfaces Ethernet, VLAN et tunnel définies sur le pare-feu reçoivent et transfèrent le trafic de Couche 3. La zone de destination provient de l'interface sortante en fonction des critères de transfert, et le pare-feu consulte les règles de politique pour identifier les politiques de sécurité à appliquer à chaque paquet. En plus du routage vers d'autres périphériques réseau, les routeurs logiques peuvent effectuer un routage vers d'autres routeurs logiques au sein du même pare-feu, à condition que le saut suivant indique qu'il pointe vers un autre routeur logique.

Vous pouvez Configurer les interfaces de couche 3 participer avec des protocoles de routage dynamique (BGP, OSPF, OSPFv3 ou RIP) ainsi que d’ajouter des itinéraires statiques. Vous pouvez également créer plusieurs routeurs logiques, chacun gérant un ensemble d'itinéraires distincts qui ne sont pas partagés entre les routeurs logiques, ce qui vous permet de configurer différents comportements de routage pour différentes interfaces.

Vous pouvez configurer le routage dynamique d'un routeur logique à un autre en configurant une interface en boucle dans chaque routeur logique, en créant une route statique entre les deux interfaces en boucle, puis en configurant un protocole de routage dynamique pour homologuer entre ces deux interfaces. Le pare-feu ne prend en charge qu'un seul saut entre les routeurs logiques. Par exemple, avec les routeurs logiques A, B et C, un itinéraire ne peut pas aller de A à B puis à C ; il faudrait aller de A à C.

Chaque interface en boucle, VLAN, de tunnel ou Ethernet de Couche 3 définie sur le pare-feu doit être associée à un routeur logique. Même si chaque interface ne peut appartenir qu'à un seul routeur logique, vous pouvez configurer plusieurs protocoles de routage et itinéraires statiques pour un routeur logique. Que des itinéraires statiques ou des protocoles de routage dynamiques soient configurés pour un routeur logique, une configuration générale est nécessaire :

 ©2024 Palo Alto Networks, Inc.

Configurer un routeur logique

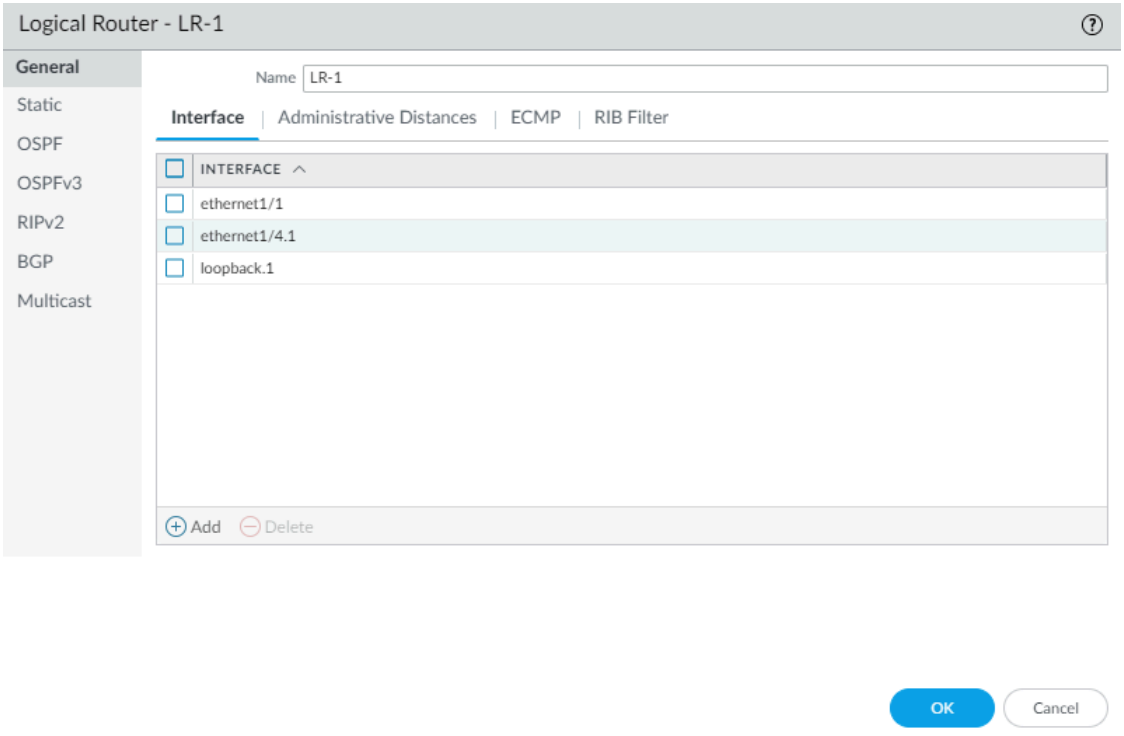
Pour effectuer le routage réseau, le moteur de routage avancé vous oblige à configurer au moins un routeur logique ; il n'y a pas de routeur logique par défaut. Un routeur logique maintient une base d'informations de routage distincte et empêche les itinéraires d'être exposés à d'autres routeurs logiques. Le nombre de routeurs logiques pris en charge pour un moteur de routage avancé varie en fonction du modèle de pare-feu.

Avant de pouvoir configurer un routeur logique, vous devez Activer le routage avancé.

STEP 1 | Sélectionnez **Réseau** > **Routage** > **Routeurs logiques** et **Ajouter** un routeur logique par**Nom** en utilisant un maximum de 31 caractères. Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement (_) ou de trait d'union (-). Aucun point (.) ou espace n'est autorisé.

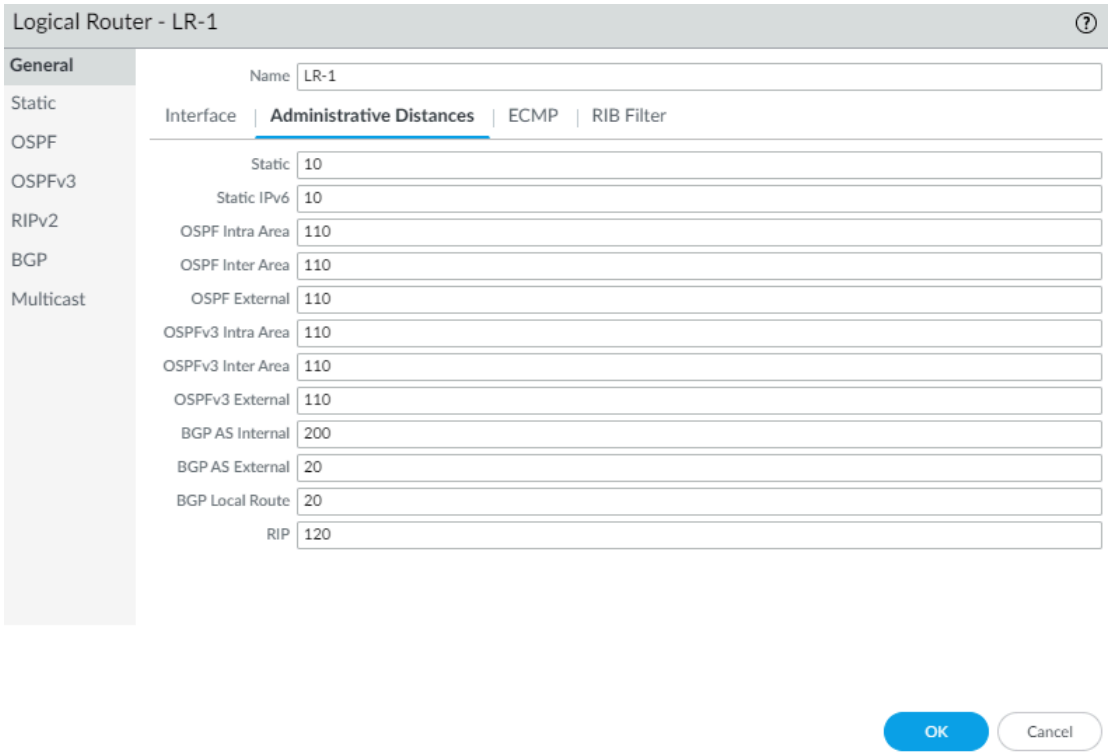
STEP 2 | Ajoutez des interfaces au routeur logique.

1. Toujours sous l'onglet **Général** du routeur logique, sélectionnez l'onglet **Interface** .
2. **Ajoutez** une interface au routeur logique en sélectionnant dans la liste des interfaces. Une interface ne peut appartenir qu'à un seul routeur logique. Répétez l'opération pour ajouter d'autres interfaces, comme dans l'exemple suivant pour le routeur logique nommé LR-1 :



 ©2024 Palo Alto Networks, Inc.

STEP 3 | (Facultatif) Sélectionnez **Distances administratives** pour modifier la distance administrative globale (à partir du paramètre par défaut) pour différents types d'itinéraires.



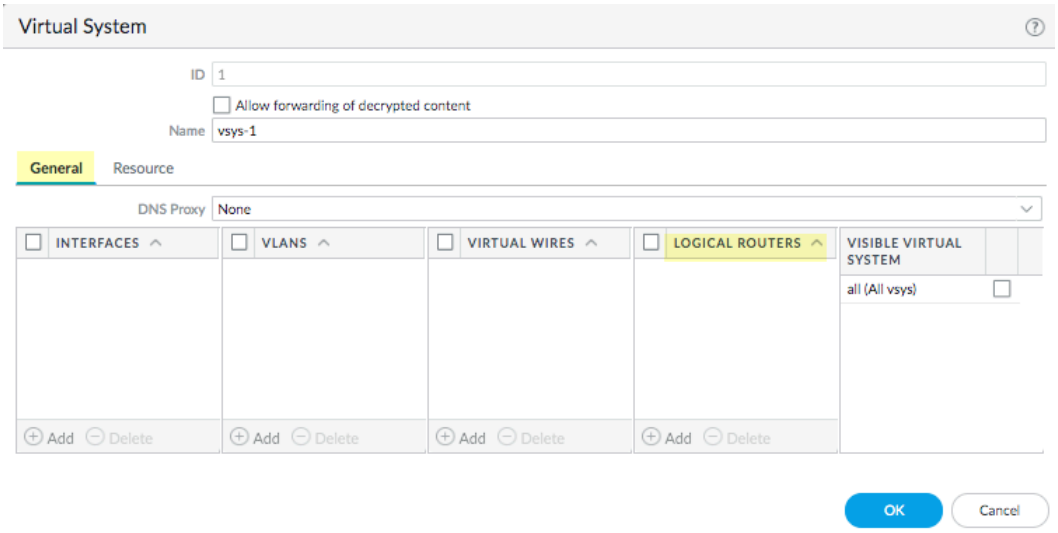
- **Static (Statique)** : plage comprise entre 1 et 255 ; valeur par défaut de 10.
- **Static IPv6 (IPv6 Statique)** : plage comprise entre 1 et 255 ; valeur par défaut de 10.
- **OSPF Intra Area (Zone intra OSPF) :**plage comprise entre 1 et 255 ; la valeur par défaut est 110.
- **OSPF Inter Area (Zone inter OSPF):** plage comprise entre 1 et 255 ; la valeur par défaut est 110.
- **OSPF External (OSPF externe)** : plage comprise entre 1 et 255 ; valeur par défaut de 110.
- **OSPFv3 Intra Area (Zone intra OSPv3F) :**plage comprise entre 1 et 255 ; la valeur par défaut est 110.
- **OSPFv3 Inter Area :**plage comprise entre 1 et 255 ; la valeur par défaut est 110.
- **OSPFv3 External (OSPFv3 externe)** : plage comprise entre 1 et 255 ; valeur par défaut de 110.
- **BGP AS Internal (BGP AS interne)** : plage comprise entre 1 et 255 ; valeur par défaut de 200.
- **BGP AS External (BGP AS externe)** : plage comprise entre 1 et 255 ; valeur par défaut de 20.
- **BGP Local Route (itinéraire local BGP) :**la plage est comprise entre 1 et 255 ; la valeur par défaut est 20.
- **RIP**: La plage est comprise entre 1 et 255 ; la valeur par défaut est 120.

STEP 4 | Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | (Sur un pare-feu prenant en charge plusieurs systèmes virtuels) Affectez les routeurs logiques à un système virtuel.

1. Sélectionnez **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)** et sélectionnez un système virtuel puis **General**.
2. **Ajoutez** un ou plusieurs **routeurs logiques**.
3. Cliquez sur **OK**.



STEP 6 | Cliquez sur **OK**.

STEP 7 | (Facultatif) Configurez ECMP pour un routeur logique en allant dans**Réseau** > **Routage** > **Routeurs logiques**, en sélectionnant un routeur logique puis **General** > **ECMP**. Configurez ECMP pour un routeur logique comme vous le feriez pour un routeur virtuel sur un moteur de routage hérité.

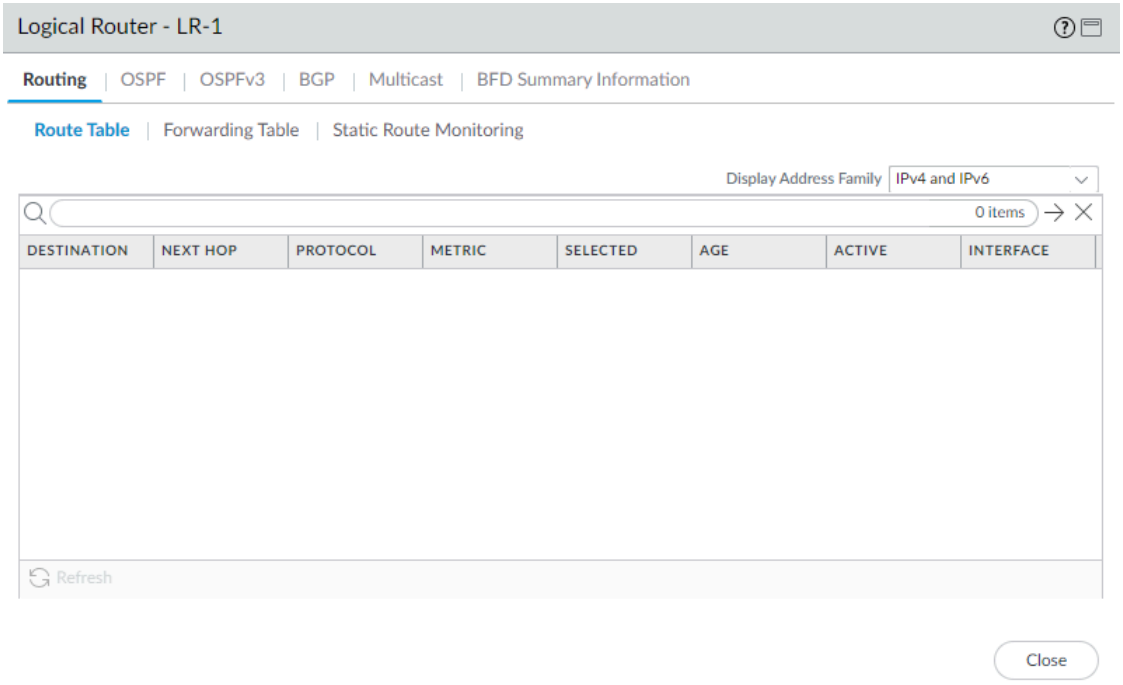
STEP 8 | **Commit (Validez)** les modifications.

STEP 9 | Pour un pare-feu avec une configuration préexistante, sélectionnez **Device (périphérique)** > **Setup (Configuration)** > **Operations (Opérations)** et **Reboot Device (Redémarrer le périphérique)**. Reconnectez-vous au pare-feu.

©2024 Palo Alto Networks, Inc.

STEP 10 | (Facultatif) Affichez les statistiques d'exécution pour un routeur logique.

1. SélectionnezNetwork (Réseau) > Routing (Routage) > Logical Routers (Routeurs logiques) et pour un routeur logique spécifique, sélectionnez **More Runtime Stats (Plus de stats de fonctionnement)** à l'extrême droite.
2. Pour afficher les tables de routage de tous les protocoles, sous l'onglet **Routage** sélectionnez **Tableau de routage** et **Afficher la famille d'adresses**: **IPv4 et IPv6**, **IPv4 uniquement**, ou **IPv6 uniquement**.



3. Pour afficher les entrées de la base d'informations de transfert (FIB), sélectionnez **Tableau de transfert**.
4. Sélectionnez **Surveillance des itinéraires statiques** pour afficher les itinéraires statiques que vous surveillez.
5. Sélectionnez l'onglet **BGP** puis **Résumé** pour afficher les paramètres BGP.
6. Sélectionnez **Homologue** pour afficher les paramètres d'homologue BGP.
7. Sélectionnez **Groupe d'homologues** pour afficher les paramètres du groupe d'homologues BGP.
8. Sélectionnez **Itinéraire** et **Afficher la famille d'adresses**: **IPv4 et IPv6**, **IPv4 uniquement**, ou **IPv6 uniquement** pour voir les attributs des itinéraires BGP.

STEP 11 | Accédez à l'interface de ligne de commande pour afficher les informations de routage avancées. Le Démarrage rapide de l'interface de ligne de commande PAN-OS répertorie les commandes de la feuille de triche de l'interface de ligne de commande : Networking (Suivant : mise en réseau).

©2024 Palo Alto Networks, Inc.

Créer un itinéraire statique

Créez un itinéraire statique pour un routeur logique dans un moteur de routage avancé.

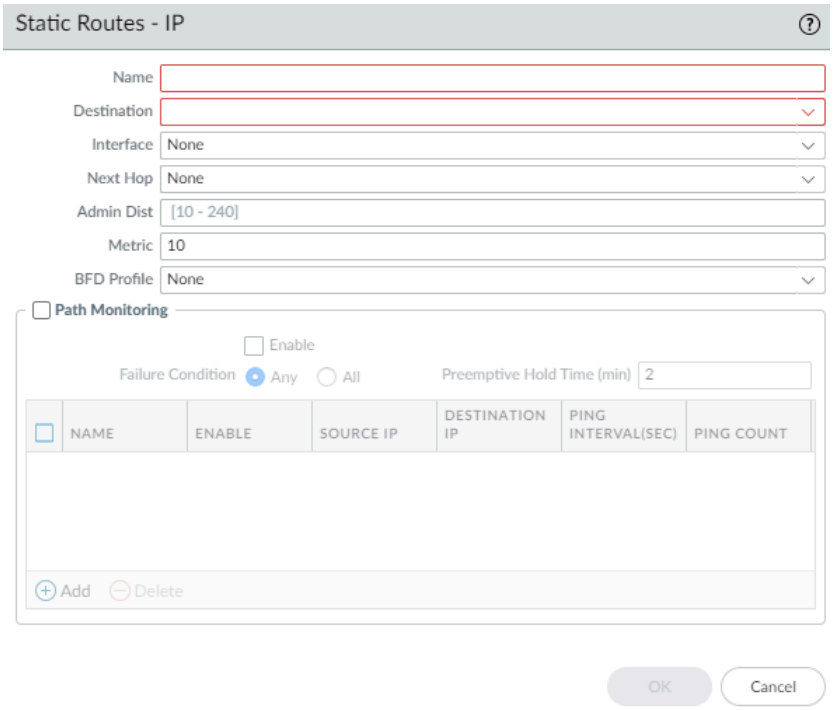
STEP 1 | Configurer un routeur logique.

STEP 2 | Créez un itinéraire statique.

1. Sélectionnez **Réseau** > **Routage** > **Routeurs logiques** et sélectionnez le routeur logique.
2. Sélectionnez **Statique** et **Ajoutez** un **itinéraire statique IPv4** ou **IPv6** par **nom** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.
3. Sous **Destination**, saisissez l'itinéraire et le masque réseau (par exemple, 192.168.2.0/24 pour une adresse IPv4 ou 2001:db8:123:1::0/64 pour une adresse IPv6). Si vous créez un itinéraire par défaut, saisissez l'itinéraire par défaut (0.0.0.0/0 pour une adresse IPv4 ou ::/0 pour une adresse IPv6). Vous pouvez également sélectionner ou créer un objet d'adresse de type Masque réseau IP.
4. Pour **Interface**, spécifiez l'interface sortante que les paquets doivent utiliser pour atteindre le saut suivant. Indiquer une interface permet de disposer d'un contrôle plus strict quant à l'interface que le pare-feu utilisera au lieu d'utiliser l'interface figurant dans la table de routage pour le saut suivant de cet itinéraire statique.
5. Sous **Next Hop (Saut suivant)**, sélectionnez l'une des options suivantes :
   - **IP Address (Adresse IP)** ou **IPv6 Address (adresse IPv6)** : saisissez l'adresse IP (par exemple, 192.168.56.1 ou 2001:IPv6:db8:1::1) lorsque vous souhaitez fixer l'itinéraire à suivre pour atteindre un certain saut suivant. Vous devez **Enable IPv6 on the interface (Activer IPv6 sur l'interface)** (lorsque vousConfigurer les interfaces de couche 3) de sorte qu'elles utilisent une adresse IPv6 de saut suivant. Si vous créez un itinéraire par défaut, sous **Next Hop (Saut suivant)** vous devez sélectionner **IP Address (Adresse IP)** et saisir l'adresse IP de votre passerelle Internet (par exemple, 192.168.56.1 ou 2001:db8:49e:1::1). Vous pouvez également créer un objet d'adresse de type Masque réseau IP. L'objet d'adresse doit avoir un masque réseau de /32 pour IPv4 ou de /128 pour IPv6.
   - **LR suivant (Next LR)** : sélectionnez cette option pour faire du routeur logique suivant (dans la liste des routeurs logiques) le tronçon suivant.
   - **FQDN (FQDN)** : saisissez le Fully Qualified Domain Name (nom de domaine complet ; FQDN).
   - **Discard (Supprimer)** : sélectionnez cette option si vous voulez supprimer les paquets qui sont dirigés vers cette destination.
   - **None (Aucun)** : sélectionnez cette option s'il n'existe aucun saut suivant pour l'itinéraire. Par exemple, il n'est pas nécessaire de définir de saut suivant pour une connexion de point à point, car les paquets ne peuvent suivre qu'une direction.
6. Entrez l'**Admin Dist** pour l'itinéraire statique (la plage est comprise entre 10 et 240 ; la valeur par défaut est 10). Cette valeur remplace la distance administrative **IPv6 statique** ou **statique** spécifiée pour le routeur logique.

 ©2024 Palo Alto Networks, Inc.

7. Indiquez une **mesure** valide pour l'itinéraire statique (fourchette de 1 à 65 535 ; par défaut 10).
8. (Facultatif) Si vous souhaitez utiliser BFD, sélectionnez un **profil BFD** que vous avez créé, ou sélectionnez le profil **par défaut** ou créez un profil BFD à appliquer à l'itinéraire statique ; la valeur par défaut est **Aucun (Désactiver BFD).**



STEP 3 | (Facultatif) Configurez la surveillance des chemins pour l'itinéraire statique ; vous pouvez surveiller jusqu'à 128 itinéraires statiques.

1. Sélectionnez **Surveillance des chemins** pour autoriser la configuration de la surveillance des chemins (la valeur par défaut est désactivée).
2. **Activez** la surveillance des chemins d'accès (la valeur par défaut est désactivée).
3. **La condition de défaillance** détermine si la surveillance du chemin d'accès pour l'itinéraire statique est basée sur une (toute) ou toutes les destinations surveillées. Sélectionnez **Any (n'importe laquelle)** ou **All (Toutes)** les destinations surveillées pour l'itinéraire statique sont inaccessibles par ICMP pour que le pare-feu supprime l'itinéraire statique de la RIB et de la FIB et ajoute l'itinéraire statique dont la métrique la plus faible suivante se dirige vers la même destination que la FIB.

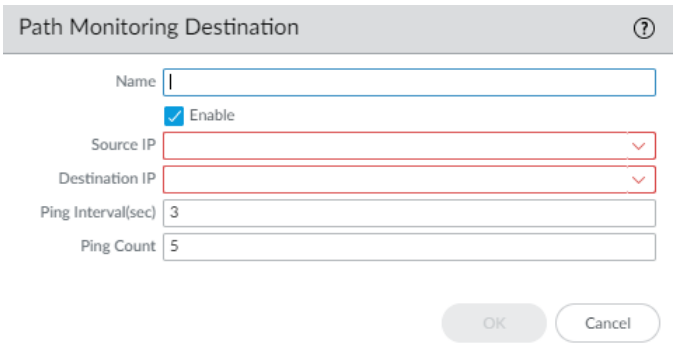
   *Sélectionnez **All (Toutes)** pour éviter toute éventualité d'une seule destination surveillée signalant une défaillance d'itinéraire lorsque la destination est simplement hors ligne pour maintenance, par exemple.*
4. (Facultatif) Indiquez le **Preemptive Hold Time (min) (Délai de maintien de préemption (min.)**, soit le nombre de minutes pendant lesquelles une surveillance des chemins indisponibles doit demeurer à l'état Actif avant que le pare-feu ne réinstalle l'itinéraire statique dans la RIB; la plage est de 0 à 1 440, la valeur par défaut est 2. Un

©2024 Palo Alto Networks, Inc.

paramètre de 0 (zéro) permet au pare-feu de réinstaller l'itinéraire statique dans la RIB immédiatement après l'activation de la surveillance des chemins.

La surveillance des chemins évalue toute les destinations de l'itinéraire statique qui sont surveillées et est activée selon la condition d'échec définie, soit **Any (N'importe laquelle)** ou **All (Toutes)**. Si un lien tombe en panne ou clignote pendant le temps de maintien, lorsque le lien remonte, le moniteur de chemin reprend et le temps de maintien préventif est réinitialisé, ce qui entraîne le redémarrage du minuteur à partir de zéro.

5. **Ajoutez** une destination de surveillance de chemin par **nom**.



6. **Activez** la destination de surveillance des chemins d'accès.
7. Sous **Source IP (IP source)**, sélectionnez l'adresse IP que le pare-feu utilise dans la requête ping ICMP qu'il envoie à la destination surveillée :
   - Si une interface possède plusieurs adresses IP, sélectionnez-en une.
   - Si vous sélectionnez une interface, le pare-feu utilise la première adresse IP affectée à l'interface par défaut.
   - Si vous sélectionnez **DHCP (Use DHCP Client address) (DHCP (Utiliser l'adresse du client DHCP))**, le pare-feu utilise l'adresse que DHCP a affectée à l'interface. Pour consulter l'adresse DHCP, sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet** et dans la ligne de l'interface Ethernet, cliquez sur **Dynamic DHCP Client (Client DHCP dynamique)**. L'adresse IP s'affiche dans la fenêtre Dynamic IP Interface Status (Statut de l'interface IP dynamique).
8. Sous **Destination IP (IP de destination)**, saisissez une adresse IP ou un objet d'adresse vers lequel le pare-feu surveillera les chemins. La destination surveillée et la destination de l'itinéraire statique doivent reposer sur la même famille d'adresses (IPv4 ou IPv6).

   L'adresse IP de destination doit appartenir à un point de terminaison fiable ; vous ne devez pas fonder la surveillance des chemins sur un périphérique qui est lui-même instable ou non fiable.
9. (Facultatif) Indiquez le **Ping Interval (sec) (Intervalle de la requête ping (sec.)** ICMP en secondes pour déterminer la fréquence à laquelle le pare-feu surveille les chemins (la plage est comprise entre 1 et 60 ; la valeur par défaut est 3).
10. (Facultatif) Indiquez le **Ping Count (nombre de requêtes Ping)** ICMP des paquets qui ne sont pas renvoyés de la destination avant que le pare-feu considère que l'itinéraire statique est inactive et qu'il la supprime de la RIB et de la FIB (plage comprise entre 3 et 10 ; par défaut : 5).
11. Cliquez sur **OK** pour enregistrer la destination du moniteur de chemin d'accès.

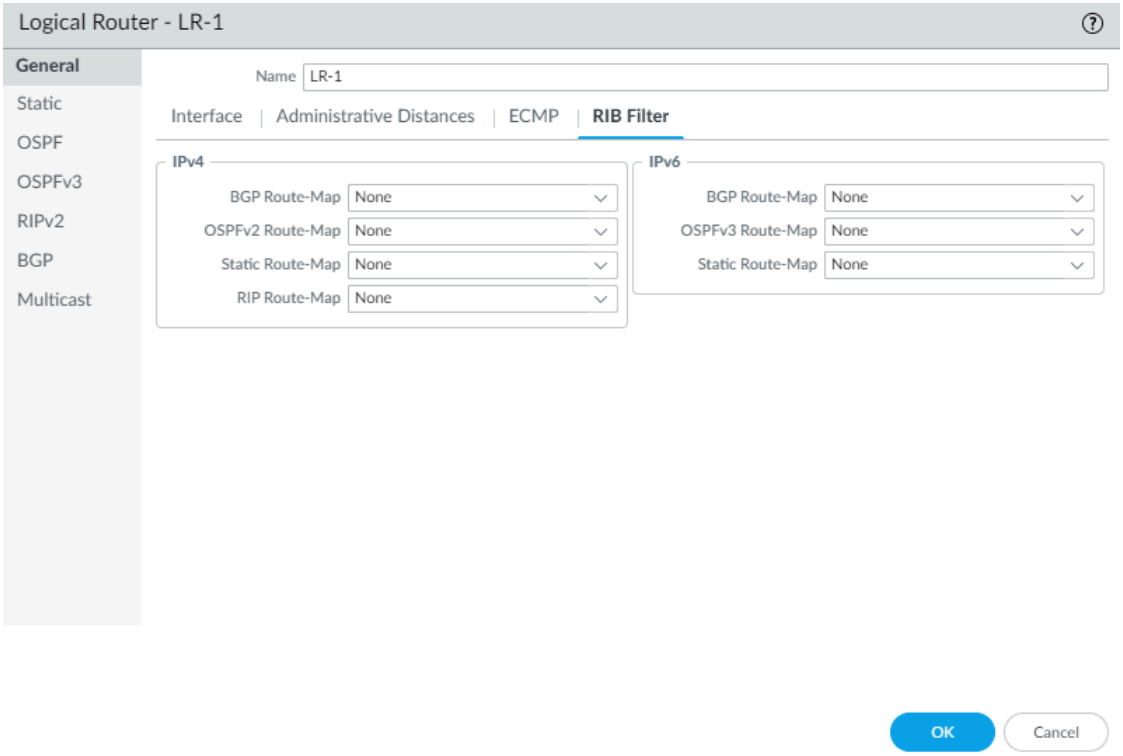
 ©2024 Palo Alto Networks, Inc.

12. Cliquez deux fois sur **OK** pour enregistrer l'itinéraire statique.

STEP 4 | (Facultatif) Contrôlez les itinéraires statiques placés dans le RIB global.

Vous pouvez configurer des itinéraires statiques et les redistribuer, mais vous ne les souhaitez pas dans la table de routage locale ou globale du protocole. Vous souhaiterez peut-être ajouter uniquement des itinéraires statiques spécifiques au RIB global.

1. Sélectionnez **Routeurs logiques** > **routage** > **réseau** et sélectionnez un routeur logique.
2. Sélectionnez **Filtre RIB** pour autoriser l'ajout d'itinéraires dans le RIB global ou empêcher l'ajout d'itinéraires à celui-ci.



3. Pour filtrer les itinéraires statiques IPv4 et les itinéraires connectés, pour **Carte d'itinéraires statique**, sélectionnez une carte d'itinéraire de redistribution ou créez-en une nouvelle.
4. Pour filtrer les itinéraires statiques IPv6 et les itinéraires connectés, pour **Carte d'itinéraire statique**, sélectionnez une carte d'itinéraires de redistribution ou créez-en une nouvelle.
5. Cliquez sur **OK**.

STEP 5 | (Facultatif) Modifiez les distances administratives par défaut pour les itinéraires IPv4 statiques et IPv6 statiques au sein d'un routeur logique.

STEP 6 | **Commit (Validez)** les modifications.

STEP 7 | Accédez à l'interface de ligne de commande pour afficher le moniteur de chemin d'itinéraire statique : **`affichez le moniteur de chemin d'itinéraire statique de routage avancé`**. Le Démarrage rapide de l'interface de ligne de commande PAN-OS

 ©2024 Palo Alto Networks, Inc.

répertorie les commandes supplémentaires dans la feuille de triche de l'interface de ligne de commande : Networking (Suivant : mise en réseau).

 ©2024 Palo Alto Networks, Inc.

Configurer BGP sur un moteur de routage avancé

Effectuez la tâche suivante pour configurer BGP pour un routeur logique sur un moteur de routage avancé.

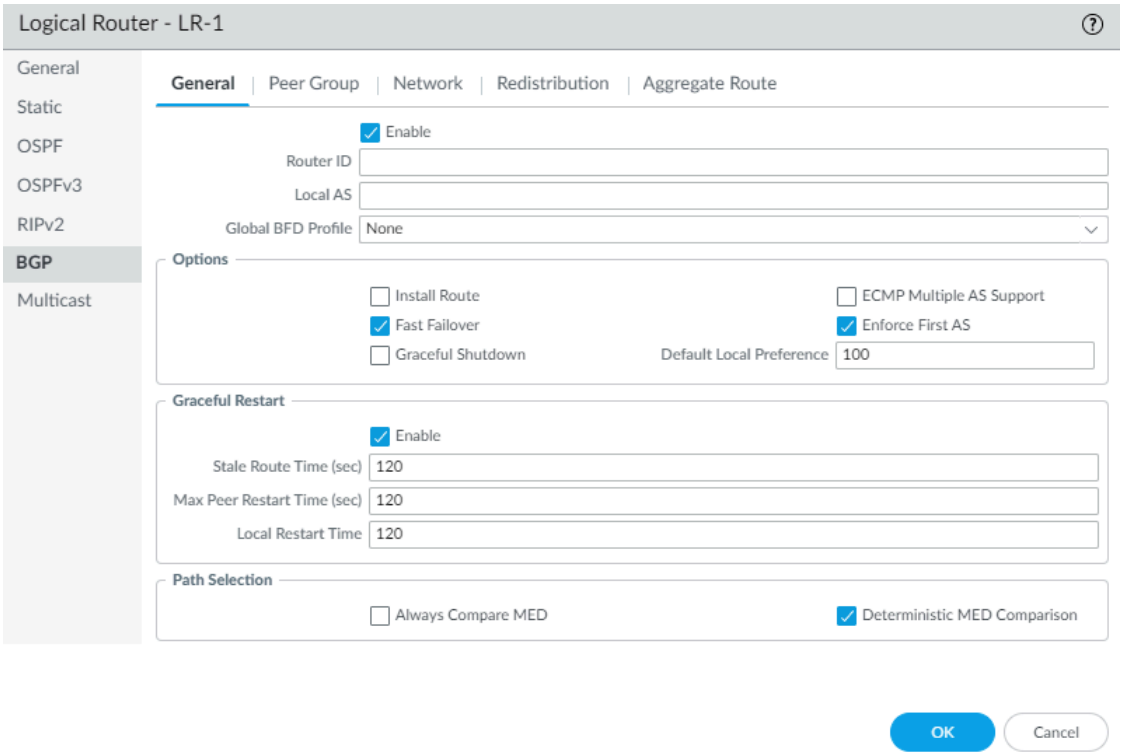
Avant de configurer BGP, tenez compte des nombreux profilset filtres de routage utiles que vous pouvez appliquer aux groupes d'homologues BGP, aux homologues, aux règles de redistribution et aux stratégies d'itinéraire agrégées, et ainsi gagner du temps de configuration et maintenir la cohérence. Vous pouvez créer des profils et des filtres à l'avance ou au fur et à mesure de votre progression dans la configuration de BGP.

STEP 1 | Configurer un routeur logique.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Activez BGP et configurez les paramètres BGP généraux.

1. Sélectionnez **Réseau** > **Routage** > **Routeurs logiques** et sélectionnez un routeur logique.
2. Sélectionnez **BGP** > **Général** et **Activer** BGP pour ce routeur logique.



3. Affectez un **ID de routeur** au BGP pour le routeur logique; il s'agit généralement d'une adresse IPv4, ce qui permet de garantir que l'ID de routeur est unique.
4. Attribuez **AS local**, qui est le numéro de l'AS auquel appartient le routeur logique ; la plage est comprise entre 1 et 4 294 967 295.
5. Si vous souhaitez appliquer BFD à BGP, pour **Profil BFD global**, sélectionnez un profil BFD que vous avez créé, sélectionnez le profil par **défaut** ou créez un nouveau profil BFD ; la valeur par défaut est **Aucun (Désactiver BFD).**
6. Sélectionnez **Installer l'itinéraire** pour installer les itinéraires BGP appris dans la table de routage globale ; la valeur par défaut est désactivée.
7. Sélectionnez **Basculement rapide** pour que BGP mette fin à une session avec un homologue adjacent si le lien vers cet homologue tombe en panne, sans attendre l'expiration du temps d'attente la valeur par défaut est activée.
8. Sélectionnez **Arrêt progressif** pour que BGP réduise la préférence des liens d'appairage eBGP pendant une opération de maintenance afin que BGP puisse choisir et propager d'autres chemins, en fonction de la RFC 8326; la valeur par défaut est désactivée.
9. Sélectionnez **ECMP Multiple AS Support (Prise en charge d'ECMP par plusieurs systèmes autonomes)** si vous avez configuré ECMP et que vous souhaitez exécuter ECMP sur plusieurs systèmes BGP autonomes; désactivé par défaut.
10. **Enforce First AS (Appliquez premier système autonome)** pour amener le pare-feu à supprimer un paquet de Mise à jour entrant d'un homologue eBGP qui ne répertorie pas

 ©2024 Palo Alto Networks, Inc.

le numéro AS de l'homologue eBGP comme premier numéro AS dans l'attribut AS_PATH; activé par défaut.

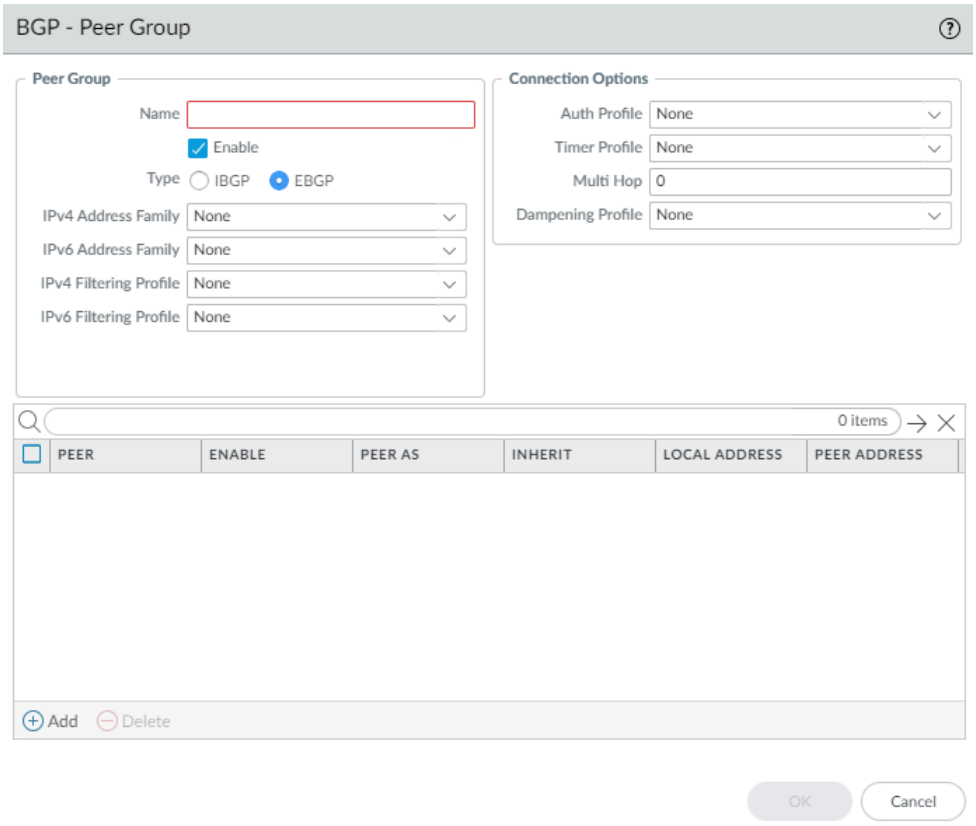
11. Indiquez la **préférence locale par défaut** qui peut être utilisée pour déterminer des préférences entre différents chemins; plage de 0 à 4, 294, 967, 295 ; valeur par défaut de 100.
12. **Activez** Graceful Restart (Redémarrage en douceur) et configurez les minuteurs suivants :
    - **Stale Route Time (sec) (Durée d'itinéraire hors service (s))** : spécifiez la durée (en secondes) pendant laquelle un itinéraire peut rester à l'état hors service (plage comprise entre 1 et 3 600, valeur par défaut : 120).
    - **Max Peer Restart Time (sec) (Délai maximum de redémarrage des homologues (s))** : indiquez la durée maximale (en secondes) qu'un équipement local accepte comme délai de redémarrage en période de grâce pour des périphériques homologues (plage comprise entre 1 et 3 600 ; valeur par défaut : 120).
    - **Local Restart Time (Délai de redémarrage local)** : spécifie le délai d'attente, en secondes, du périphérique local avant de redémarrer. Cette valeur est publiée chez les homologues (intervalle compris entre 1 et 3 600 ; valeur par défaut : 120).
13. Pour la **sélection du chemin**:
    - **Always Compare MED (Toujours comparer les MED)** - Activez cette comparaison afin de sélectionner des chemins provenant de voisins de différents systèmes autonomes; désactivé par défaut.
    - **Deterministic MED Comparison (Comparaison de MED déterministe)** - Activez cette comparaison afin de sélectionner un itinéraire parmi ceux qui sont publiés par des homologues IBGP (homologues BGP figurant dans le même système autonome), activé par défaut.
14. Cliquez sur **OK**.

STEP 3 | Configurez un groupe d'homologues BGP.

1. Sélectionnez > **Routage** > **Routeurs logiques** et sélectionnez un routeur logique.
2. Sélectionnez **BGP** > **Groupe d'homologues** et **Ajoutez** un groupe d'homologues BGP par **Nom** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et peut contenir des caractères alphanumériques, des traits de soulignement, des traits d'union

 ©2024 Palo Alto Networks, Inc.

et des points. L'espace n'est pas autorisée. Le nom doit être unique dans le routeur logique et sur tous les routeurs logiques.



3. **Activez** le groupe d'homologues.
4. Sélectionnez le **Type (Type)** de groupe d'homologues : **IBGP** ou **EBGP**.
5. Pour spécifier de nombreuses **options de famille d'adresses** IPv4 pour le groupe d'homologues, sélectionnez un **profil** AFI que vous avez créé, sélectionnez le **profil par défaut** ou créez un nouveau profilde famille d'adresses BGP ; la valeur par défaut est **Aucun**.
6. Pour spécifier de nombreuses **options de famille d'adresses** IPv6 pour le groupe d'homologues, sélectionnez un **profil** AFI que vous avez créé, sélectionnez le **profil par défaut** ou créez un nouveau profilde famille d'adresses BGP ; la valeur par défaut est **Aucun**.
7. Pour appliquer les **options de profil** de filtrage IPv4 au groupe d'homologues, sélectionnez un **profil** de filtrage BGP que vous avez créé ou créez un nouveau profilde filtrage BGP ; la valeur par défaut est **Aucun**.

Un profil de filtrage BGP décrit comment configurer de nombreuses options BGP pour IPv4, telles que l'importation ou l'exportation d'itinéraires BGP, accepter ou empêcher l'ajout d'itinéraires au RIB BGP local, publier conditionnellement des itinéraires et annuler la suppression des itinéraires amortis ou résumés.

©2024 Palo Alto Networks, Inc.

8. Pour appliquer les **options de profil de filtrage IPv6** au groupe d'homologues, sélectionnez un **profil de filtrage BGP** que vous avez créé ou créez un nouveau profil de filtrage BGP ; la valeur par défaut est **Aucun**.

   Un profil de filtrage BGP décrit comment configurer de nombreuses options BGP pour IPv6, telles que l'importation ou l'exportation de routes BGP, accepter ou empêcher l'ajout d'itinéraires à l'infrastructure RIB BGP locale, publier conditionnellement des itinéraires et annuler la suppression des itinéraires amortis ou résumés.
9. Pour Options de connexion, sélectionnez un **profil d'authentification** ou créez un nouveau profil d'authentification BGP pour contrôler l'authentification MD5 entre les homologues BGP du groupe d'homologues. Valeur par défaut : **Aucune**.
10. Sélectionnez un **profil de minuteur** ou créez un nouveau profil de minuterie BGP pour contrôler divers minuteurs BGP qui affectent les messages keepalive et de mise à jour qui annoncent des itinéraires. Valeur par défaut : **Aucune**.
11. Définissez la valeur **Multi Hop (Plusieurs sauts)** : il s'agit de la valeur Time-To-Live (durée de vie ; TTL) dans l'en-tête IP (intervalle compris entre 0 et 255 ; valeur par défaut : 0.) La valeur par défaut de 0 signifie 1 pour IBGP. La valeur par défaut de 0 signifie 255 pour IBGP.
12. Sélectionnez un **profil d'amortissement** ou créez un nouveau profil d'amortissement pour déterminer comment pénaliser un itinéraire de battement afin de le supprimer de son utilisation jusqu'à ce qu'il se stabilise. Valeur par défaut : **Aucune**.

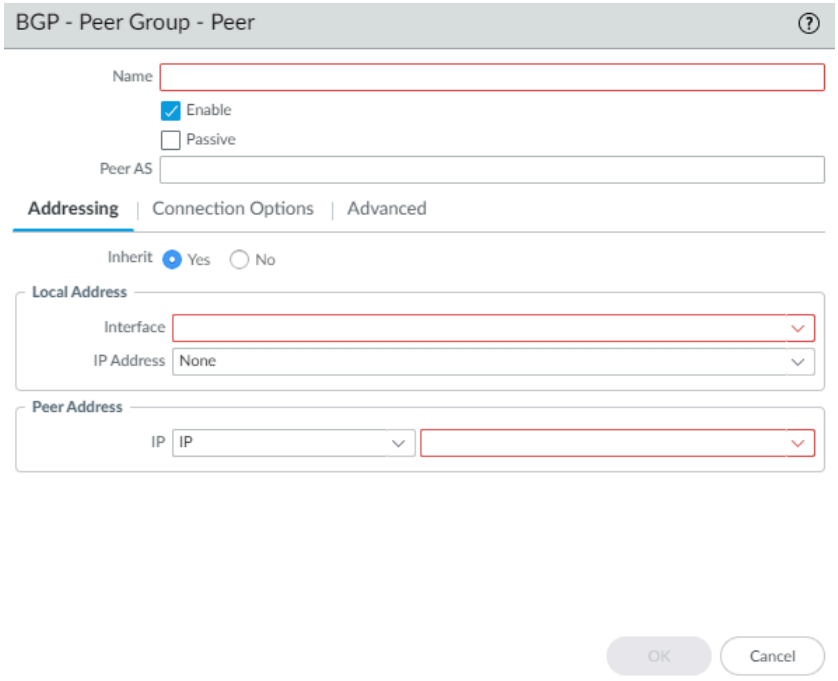
STEP 4 | Ajoutez un homologue BGP au groupe d'homologues.

1. **Ajoutez** un homologue par **nom** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir des caractères alphanumériques, des traits de soulignement et des traits d'union. L'espace n'est pas autorisée. Le nom doit être unique dans le routeur logique et sur tous les routeurs logiques.
2. **Activez** l'homologue ; la valeur par défaut est activée.
3. Sélectionnez **Passif** pour empêcher l'homologue de lancer une session avec ses voisins ; la valeur par défaut est désactivée.
4. Saisissez l'**AS homologue** auquel l'homologue appartient ; plage de 1 à 4 294 967 295.
5. Sélectionnez **Adressage** et indiquez si l'homologue **héritera** des profils AFI IPv4 et IPv6 et des profils de filtrage du groupe d'homologues : **Oui** (par défaut) ou **Non**.

©2024 Palo Alto Networks, Inc.

6. Si vous avez choisi **Oui**, spécifiez les éléments suivants pour l'homologue :
   - Sous **Local Address (Adresse locale)**, sélectionnez l'**Interface (Interface)** pour laquelle vous configurez BGP. Si l'interface possède plus d'une adresse IP, saisissez l'**adresse IP** de cette interface qui doit lui permettre de servir d'homologue BGP.
   - Sous **Peer Address (Adresse de l'homologue)**, sélectionnez **IP** et saisissez l'adresse IP ou sélectionnez ou créez un objet d'adresse, ou sélectionnez **FQDN** et saisissez le FQDN ou l'objet d'adresse de type FQDN.

   Le pare-feu n'utilise qu'une seule adresse IP (de chaque type de famille IPv4 ou IPv6) de la résolution DNS du FQDN. Si la résolution FQDN donne plus d'une adresse, le pare-feu utilise l'adresse IP privilégiée qui correspond au type de famille IP (Ipv4 ou IPv6) configuré pour l'homologue BGP. L'adresse IP privilégiée est la première adresse que le serveur DNS retourne dans sa réponse initiale. Le pare-feu conserve cette adresse en tant que privilégiée tant que l'adresse apparaît dans les réponses subséquentes, peu importe l'ordre.



7. Si vous avez choisi **Non** pour **Hériter** de l'adressage du groupe d'homologues, spécifiez les éléments suivants pour l'homologue :
   - Pour spécifier de nombreuses options de **famille d'adresses IPv4** pour l'homologue, sélectionnez un **profil AFI** que vous avez créé, sélectionnez le profil **par défaut**

©2024 Palo Alto Networks, Inc.

sélectionnez **hériter (Hériter du groupe d'homologues)**, ou créez un nouveau profil de famille d'adresses BGP ; la valeur par défaut est **aucune (Désactiver IPv4 AFI)**.

Le profil AFI vous permet de spécifier que l'homologue est un client Route Reflector. Le réflecteur d'itinéraire reflète toutes les publicités de tous ses pairs à tous les autres pairs, évitant ainsi que l'iBGP soit entièrement maillé. Si vous déclarez l'homologue client De réflecteur de routage, le processus BGP reflète toutes les mises à jour de cet homologue.

- Pour spécifier de nombreuses **options de famille d'adresses** IPv6 pour l'homologue, sélectionnez un **profil AFI** que vous avez créé, sélectionnez **hériter (Hériter du groupe d'homologues)**, ou créez un nouveau profil de famille d'adresses BGP ; la valeur par défaut est **none (Désactiver IPv6 AFI)**.

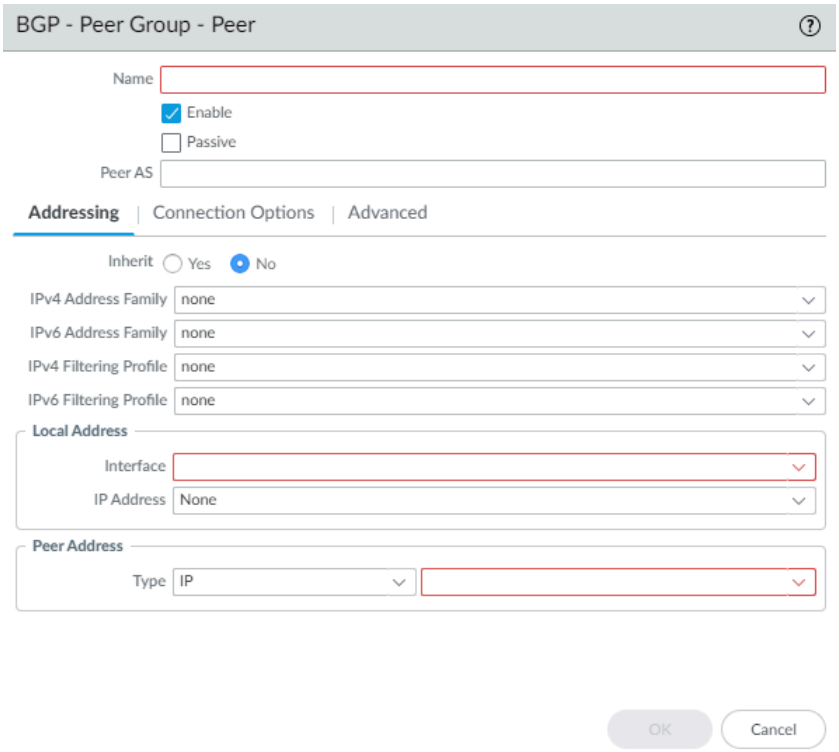
  Le profil AFI vous permet de spécifier que l'homologue est un client Route Reflector. Le réflecteur d'itinéraire reflète toutes les publicités de tous ses pairs à tous les autres pairs, évitant ainsi que l'iBGP soit entièrement maillé. Si vous déclarez l'homologue client De réflecteur de routage, le processus BGP reflète toutes les mises à jour de cet homologue.

- Pour appliquer les options de **profil de filtrage IPv4** à l'homologue, sélectionnez un **profil de filtrage BGP** que vous avez créé, sélectionnez **hériter (Hériter du groupe d'homologues)**, ou créez un nouveau profil de filtrage BGP ; la valeur par défaut est **none (Désactiver le filtrage IPv4).**
- Pour appliquer les options de **profil de filtrage IPv6** à l'homologue, sélectionnez un **profil de filtrage BGP** que vous avez créé, sélectionnez **hériter (Hériter du groupe**

 ©2024 Palo Alto Networks, Inc.

d'homologues), ou créez un nouveau profil de filtrage BGP ; la valeur par défaut est **aucune (Désactiver le filtrage IPv6).**

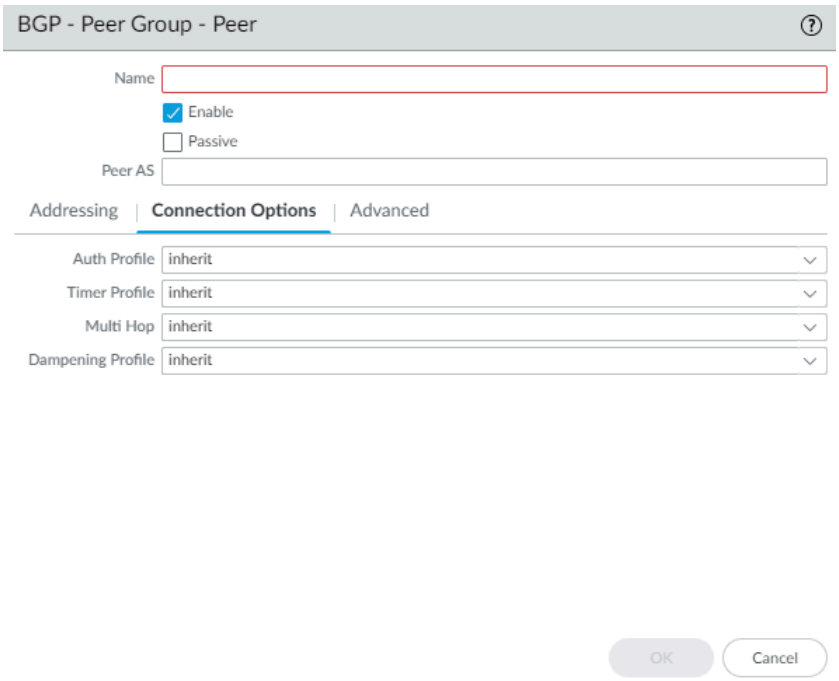
- Sous **Local Address (Adresse locale)**, sélectionnez l'**Interface (Interface)** pour laquelle vous configurez BGP. Si l'interface possède plus d'une adresse IP, sélectionnez l'**adresse IP** de cette interface qui doit lui permettre de servir d'homologue BGP.
- Sous **Peer Address (Adresse de l'homologue)**, sélectionnez **IP** et saisissez l'adresse IP ou sélectionnez ou créez un objet d'adresse, ou sélectionnez **FQDN** et saisissez le FQDN ou l'objet d'adresse de type FQDN.



Un groupe de pairs BGP (ou un pair) peut se voir appliquer à la fois un profil Famille d'adresses IPv4 et un profil Famille d'adresses IPv6. Tous les pairs appartenant à ce groupe de pairs auront automatiquement Adressage réglé sur héritage du ***N°****. Tous les homologues du groupe d'homologues auront également le profil de famille d'adresses IPv4, le profil de famille d'adresses IPv6, le profil de filtrage IPv4 et le profil de filtrage IPv6 définis sur* ***aucun*** *par défaut. Pour que le routage fonctionne correctement, l'interface de peering doit avoir à la fois une adresse IPv4 et une adresse IPv6. Vous pouvez sélectionner hériter (Hériter du groupe d'homologues) ou remplacer le groupe d'homologues en sélectionnant un profil spécifique pour l'homologue. Par exemple, vous pouvez configurer un homologue pour* ***hériter*** *du profil de famille d'adresses IPv4 et* ***hériter*** *du profil de filtrage IPv4, puis sélectionner un profil de famille d'adresses IPv6 et un profil de filtrage IPv6 pour remplacer ces profils du groupe d'homologues.*

8. Sélectionnez **Options de connexion** pour l'homologue afin d'appliquer des paramètres différents de ceux du groupe d'homologues.

©2024 Palo Alto Networks, Inc.

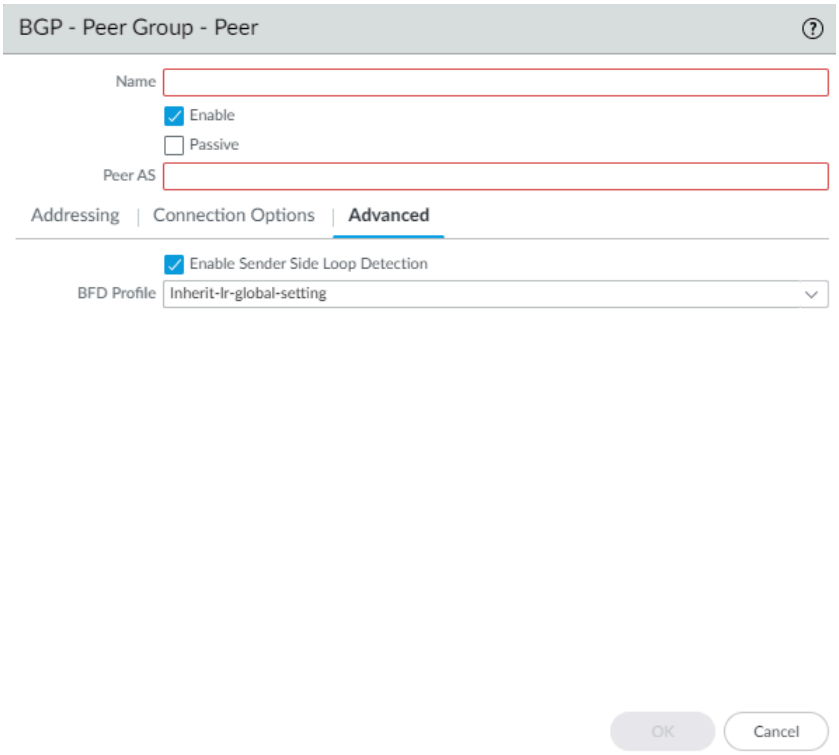


9. Sélectionnez un **profil d'authentification**, **héritez (Hériter du groupe d'homologues) (valeur par défaut)** ou créez un nouveau profil d'authentification BGP pour contrôler l'authentification MD5 entre les homologues BGP.
10. Sélectionnez un **profil de minuteur**,**héritez (Hériter du groupe d'homologues)** (par défaut), créez un nouveau profil de minuteur BGP ou sélectionnez le profil **par défaut** pour contrôler divers minuteurs BGP qui affectent keepalive et mettre à jour les messages qui annoncent des itinéraires.
11. Définissez **Multi Hop (Plusieurs sauts)**, qui est la valeur Time-To-Live (durée de vie ; TTL) dans l'en-tête IP (intervalle compris entre 0 et 255, valeur par défaut : 255. Le paramètre par défaut est **inherit (Inherit from Peer-Group).**
12. Sélectionnez un **profil d'amortissement**, **héritez (Hériter d'un groupe d'homologues)** (valeur par défaut) ou créez un nouveau profil d'amortissement pour déterminer comment pénaliser un itinéraire de battement afin de le supprimer jusqu'à ce qu'il se stabilise.
13. Sélectionnez **Advanced (Avancé)** et **Enable Sender Side Loop Detection (Activez la détection des boucles côté expéditeur)**, le pare-feu vérifiera l'attribut AS_PATH d'un itinéraire dans le BGP RIB avant d'envoyer l'itinéraire dans une mise à jour afin de s'assurer que le numéro AS de l'homologue n'est pas sur la liste AS_PATH. Le pare-feu n'annonce pas la route si le numéro AS de l'homologue figure au sein de la liste AS_PATH. Généralement, le récepteur détecte les boucles, mais cette fonctionnalité

 ©2024 Palo Alto Networks, Inc.

d'optimisation permet d'effectuer la détection des boucles par l'expéditeur. Désactivez cette fonctionnalité pour que le récepteur effectue la détection des boucles.

14. Pour appliquer un **profil BFD** à l'homologue (qui remplace le paramètre BFD pour BGP, tant que BFD n'est pas désactivé pour BGP au niveau du routeur logique), sélectionnez l'une des options suivantes :
    - Définir le profil **par défaut**.
    - Un profil BFD existant.
    - **Inherit-lr-global-setting (profil BFD global du protocole Inherit) (par défaut)** : l'homologue hérite du profil BFD que vous avez sélectionné globalement pour BGP pour le routeur logique.
    - **Aucun (Désactiver BFD)** pour l'homologue.
    - Créer nouveau profil BFD.



15. Cliquez sur **OK**.

STEP 5 | Spécifiez les préfixes réseau à publier auprès des voisins.

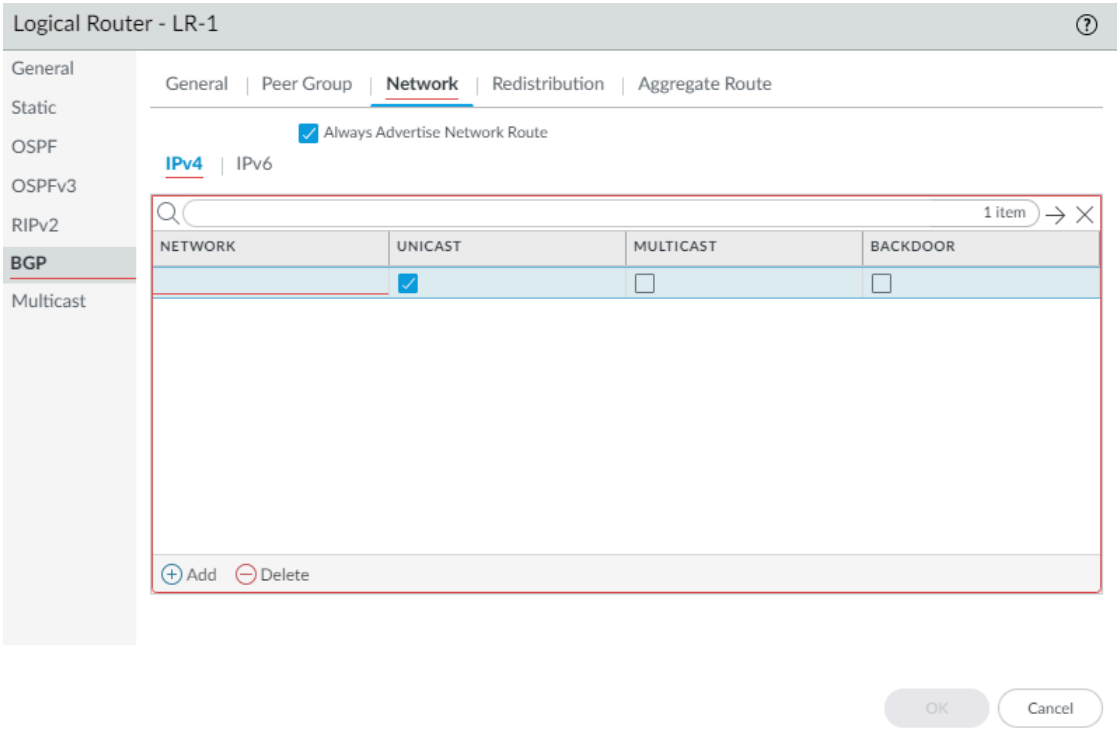
*La fonctionnalité **Réseau** est particulièrement utile après le déplacement d'un pare-feu vers un autre sous-réseau ou après une modification temporaire d'un réseau.*

1. Sélectionnez **Réseau**.
2. **Toujours publier l'itinéraire réseau** (la valeur par défaut est activée) pour toujours publier les itinéraires réseau configurés sur les homologues BGP, qu'ils soient accessibles ou

 ©2024 Palo Alto Networks, Inc.

non. Si cette case n'est pas cochée, le pare-feu n'annonce les routes réseau que si elles sont résolues à l'aide de la table de routage locale.

3. Sélectionnez **IPv4** ou **IPv6** pour sélectionner le type de préfixe.
4. **Ajoutez** un préfixe **réseau** pour faire de la publicité auprès des voisins.
5. Sélectionnez **Unicast** pour publier cet itinéraire réseau dans la famille d'adresses Unicast ; la valeur par défaut est activée. S'il n'est pas coché, le pare-feu n'annonce pas l'itinéraire dans unicast SAFI.
6. (IPv4 uniquement) Sélectionnez Multidiffusion pour annoncer cette route réseau dans la famille d'adresses de multidiffusion. La valeur par défaut est désactivée ; le pare-feu n'annonce pas cette route réseau dans le SAFI multidiffusion.
7. (IPv4 uniquement) Sélectionnez **Backdoor** pour empêcher BGP de publier le préfixe en dehors de l'AS et conserver l'itinéraire dans l'AS. Une porte dérobée est une route BGP qui a une distance administrative plus élevée qu'une route IGP. En interne, la distance administrative pour le préfixe est augmentée de sorte que le préfixe n'est pas préféré, mais est toujours disponible si nécessaire, en cas de défaillance d'un lien ailleurs. La valeur par défaut est désactivée.

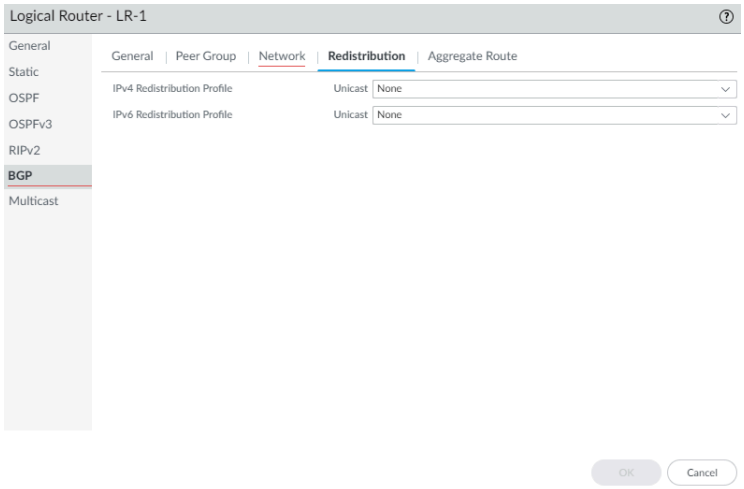


 ©2024 Palo Alto Networks, Inc.

STEP 6 | Redistribuez les routes statiques, connectées, OSPF, OSPFv3 ou RIPv2 dans BGP.

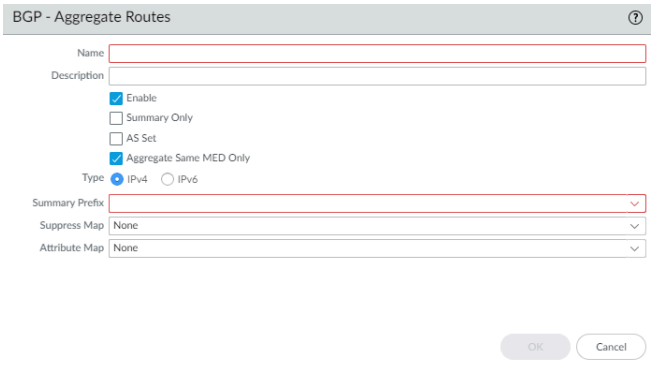
Dans un profil de redistribution BGP, utilisez la flexibilité des cartes routières pour spécifier les conditions qui déterminent les itinéraires à redistribuer et pour spécifier les attributs à définir.

1. Sélectionnez **Redistribution**.
2. Pour redistribuer des itinéraires IPv4, pour **Profil de redistribution IPv4 -- Monodiffusion**, sélectionnez un profil de redistribution BGP ou créez un nouveau profil de redistribution ; la valeur par défaut est **Aucun**.
3. Pour redistribuer des itinéraires IPv6, pour **Profil de redistribution IPv6 -- Monodiffusion**, sélectionnez un profil de redistribution BGP ou créez un nouveau profil de redistribution ; la valeur par défaut est **Aucun**.



STEP 7 | Créez une stratégie d'itinéraire agrégée pour résumer les itinéraires que BGP apprend, puis publie auprès de ses homologues.

1. Sélectionnez **Agréger l'itinéraire** et **Ajouter** une stratégie d'itinéraire agrégé par **nom** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir des caractères alphanumériques, des traits de soulignement et des traits d'union. L'espace n'est pas autorisée.
2. Entrez une **Description** utile de la stratégie.
3. **Activez** la stratégie.



 ©2024 Palo Alto Networks, Inc.

4. Sélectionnez **Résumé uniquement** pour publier aux voisins uniquement le **préfixe Résumé** et non les itinéraires qui ont été résumés ; cela réduit le trafic et évite d'augmenter inutilement la taille des tables de routage des voisins (la valeur par défaut est désactivée). Si vous souhaitez publier à la fois l'itinéraire agrégé et les itinéraires individuels qui composent l'itinéraire agrégé, laissez l'option **Résumé uniquement** décochée.

   ***Summary Only** et **Suppress Map** s'excluent mutuellement ; vous ne pouvez pas spécifier les deux.*

   *Si vous souhaitez utiliser **résumé uniquement**, mais que, vous souhaitez également publier un itinéraire individuel, vous créez un* profil de filtrage BGP *qui inclut une carte d'itinéraire **Unsuppress Map** qui correspond à l'itinéraire individuel.*
5. Sélectionnez **AS Set** pour publier le préfixe avec la liste des numéros AS qui composent l'itinéraire agrégé ; la valeur par défaut est désactivée.
6. Sélectionnez **Aggregate Same MED Uniquement** pour provoquer l'agrégation d'itinéraires uniquement si les itinéraires ont les mêmes valeurs MED (Multi-Exit Discriminator) ; la valeur par défaut est activée.
7. Sélectionnez le **Type** d'itinéraire agrégé : **IPv4** ou **IPv6**.
8. Calculez les itinéraires que vous souhaitez résumer, puis entrez le **préfixe de résumé** qui couvre ces itinéraires, en spécifiant une adresse IP/un masque de réseau ou un objet d'adresse.
9. Pour empêcher l'agrégation d'itinéraires individuels (supprimer l'agrégation), sélectionnez une carte d'itinéraire **Supprimer la carte** ou créez une nouvelle carte d'itinéraire BGP dont le critère de correspondance spécifie une liste d'accès aux adresses IPv4 ou IPv6 ou une liste de préfixes qui inclut ces itinéraires ; la valeur par défaut est **Aucun**.

   *N'oubliez pas que le but de la carte de route Suppress est d'empêcher que certains itinéraires ne soient agrégés dans une annonce. Par conséquent, dans la carte d'itinéraire, vous **autorisez** l'agrégation des itinéraires que vous souhaitez supprimer (vous ne **refusez** pas l'agrégation des itinéraires que vous souhaitez supprimer).*

   ***Summary Only** et **Suppress Map** s'excluent mutuellement ; vous ne pouvez pas spécifier les deux.*
10. Pour définir des informations d'attribut pour le préfixe de résumé (qui n'a pas d'attributs car vous venez de créer cette combinaison d'itinéraires), sélectionnez une carte d'itinéraire de **Carte d'attributs** ou créez une nouvelle carte d'itinéraire BGP et définissez les attributs du préfixe de résumé (aucun critère de correspondance). S'il n'y a pas de carte de routage (**Aucun**), le préfixe de résumé aura les attributs par défaut. Valeur par défaut : **Aucune**.

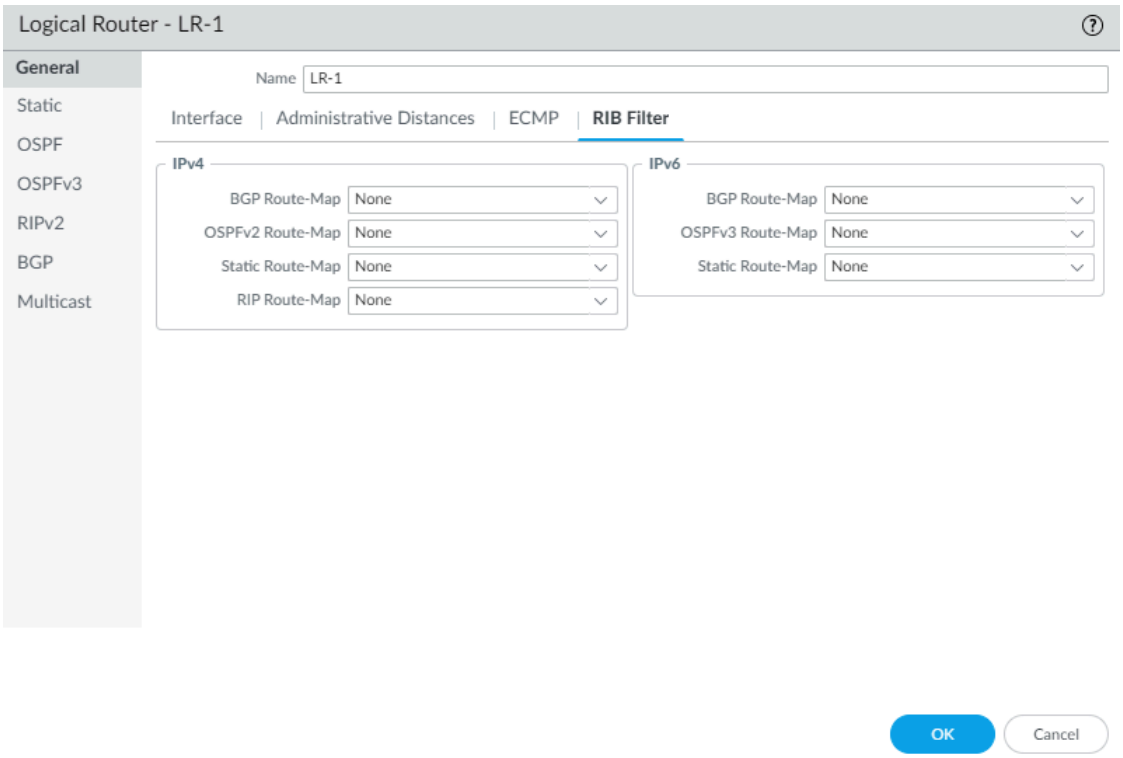
STEP 8 | Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | (Facultatif) Contrôlez les itinéraires BGP placés dans le RIB global.

Vous pouvez apprendre des itinéraires et les redistribuer, mais vous ne les souhaitez pas dans la table de routage locale ou le RIB global du protocole. Vous souhaiterez peut-être ajouter uniquement des itinéraires spécifiques au RIB global.

1. Sélectionnez **Routeurs logiques** > **routage** > **réseau** et sélectionnez un routeur logique.
2. Sélectionnez **Filtre RIB** pour autoriser l'ajout d'itinéraires dans le RIB global ou empêcher l'ajout d'itinéraires à celui-ci.



3. Pour filtrer les itinéraires BGP IPv4, dans la zone IPv4, pour **BGP Route-Map**, sélectionnez une carte, d'itinéraire de redistribution ou créez-en une nouvelle.
4. Pour filtrer les itinéraires BGP IPv6, dans la zone IPv6, pour **Carte d'itinéraire BGP, sélectionnez une carte**, d'itinéraire de redistribution ou créez-en une nouvelle.
5. Cliquez sur **OK**.

©2024 Palo Alto Networks, Inc.

Créer des profils de routage BGP

Sur un moteur de routage avancé, BGP dispose de nombreux paramètres que vous pouvez facilement configurer dans un profil, puis appliquer à un groupe d'homologues ou à un homologue BGP ou à des règles de redistribution. Réutilisez les profils pour les appliquer à plusieurs routeurs logiques et systèmes virtuels. Créez plusieurs profils du même type pour gérer différemment différents groupes d'homologues et homologues. Les groupes de pairs BGP et les pairs héritent de profils globaux ; vous pouvez également créer un profil pour un groupe d'homologues BGP afin de remplacer le profil global et créer un profil pour un homologue BGP, qui remplace le profil du groupe d'homologues auquel l'homologue appartient.

Cette rubrique décrit les profils de routage BGP et explique comment les créer.

- **Profils d'authentification BGP** : spécifiez la clé secrète pour l'authentification MD5, qui est utilisée entre homologues BGP pendant la négociation pour déterminer s'ils peuvent communiquer entre eux. Référencez le profil dans un groupe d'homologues BGP ou une configuration d'homologue.
- **Profils de minuterie BGP**: contrôlez divers minuteurs BGP qui affectent keepalive et mettez à jour les messages qui annoncent des itinéraires. Référencez le profil dans un groupe d'homologues BGP ou une configuration d'homologue.
- **Profils de famille d'adresses BGP** : déterminez le comportement d'IPv6 ou d'IPv4 lorsqu'un système autonome BGP utilise les deux types d'adresses. Référencez le profil dans un groupe d'homologues BGP ou une configuration d'homologue.
- **Profils d'amortissement BGP** : déterminez comment pénaliser une voie de battement pour l'empêcher d'être utilisée jusqu'à ce qu'elle se stabilise. Référencez le profil dans un groupe d'homologues BGP ou une configuration d'homologue.
- **Profils de redistribution BGP** : redistribuez les itinéraires statiques, connectés, OSPF, OSPFv3 ou RIP (qui répondent aux critères de la carte d'itinéraire attribuée) dans BGP et appliquez les attributs set de carte de routage aux itinéraires redistribués. Référencez le profil sur **Network** > **Routing** > **Logical Routers** > **BGP** > **Redistribution**.
- **Profils de filtrage BGP** :appliquez simultanément plusieurs filtres à un groupe d'homologues ou à un homologue pour effectuer les opérations suivantes :
  - Acceptez les itinéraires provenant d'un chemin AS spécifique (en fonction de la liste d'accès au chemin AS).
  - Annoncez les itinéraires qui ont un chemin AS spécifique (basé sur la liste d'accès AS Path).
  - Acceptez les itinéraires vers le RIB BGP local en fonction d'une liste de distribution ou d'une liste de préfixes (pas les deux dans le même profil de filtrage). Une liste de distribution est

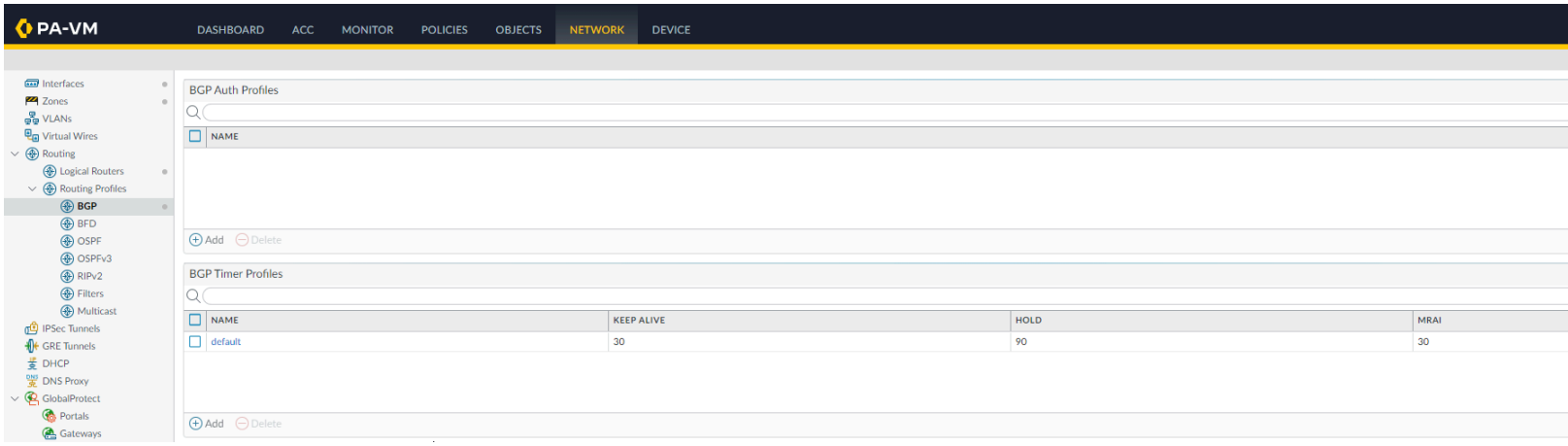
 ©2024 Palo Alto Networks, Inc.

basée sur l'adresse IP source avec un masque générique pour obtenir une plage de préfixes. Une liste de préfixes est basée sur l'adresse réseau/la longueur du préfixe.

- Annoncez des itinéraires à partir du RIB BGP local en fonction d'une liste de distribution ou d'une liste de préfixes (pas les deux dans le même profil de filtrage).
- Acceptez les itinéraires qui répondent aux critères d'attribut de carte de routage dans le RIB BGP local et définissez éventuellement des attributs.
- Publiez des itinéraires qui répondent aux critères d'attribut de carte d'itinéraire et définissez éventuellement des attributs.
- Annoncez conditionnellement les itinéraires qui existent (répondent aux critères d'existence).
- Annoncer conditionnellement des itinéraires autres que ceux qui répondent aux critères (satisfaire à des critères inexistants).
- Rétablir les itinéraires amortis ou résumés.

STEP 1 | Créez un profil d'authentification BGP.

1. Sélectionnez **Network** > **Routing** > **Routing Profiles** > **BGP**.

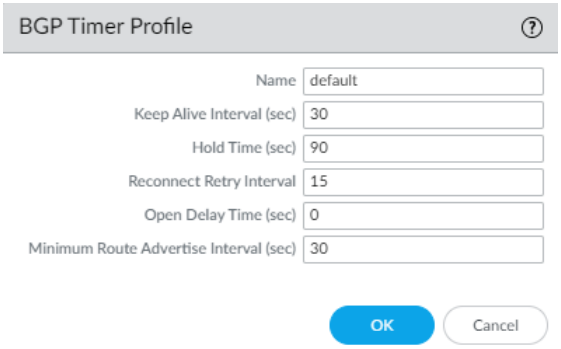


2. **Ajoutez** un **profil d'authentification BGP** par **nom** (un maximum de 63 caractères) pour identifier le profil. Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et peut contenir des caractères alphanumériques, des traits de soulignement, des traits d'union et des points. L'espace n'est pas autorisée.
3. Saisissez la **Phrase secrète** et **Confirm Secret (confirmez la phrase secrète)** La phrase secrète sert de clé lors de l'authentification MD5.
4. Cliquez sur **OK**.

©2024 Palo Alto Networks, Inc.

STEP 2 | Créez un profil BGP Timer.

1. Sélectionnez **Network** > **Routing** > **Routing Profiles** > **BGP**.
2. Dans la fenêtre Profils du minuteur BGP, sélectionnez le profil du minuteur BGP **par défaut** pour afficher les paramètres de profil par défaut :

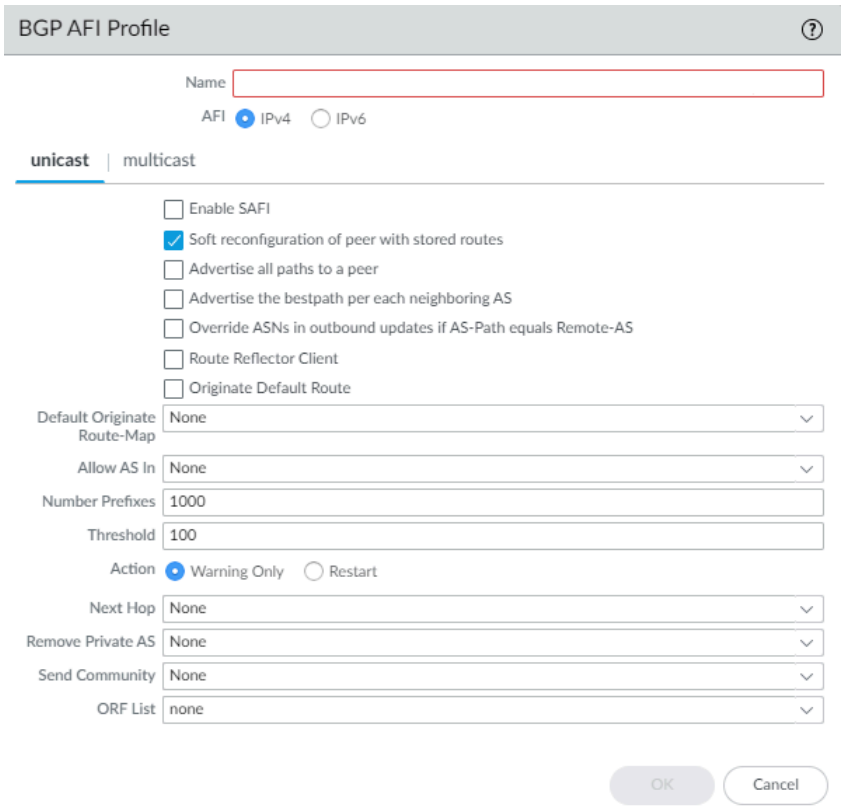


3. Si les paramètres par défaut du profil du minuteur BGP ne sont pas ceux dont vous avez besoin, **ajoutez** un **profil du** minuteur BGP par **nom** (un maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et peut contenir des caractères alphanumériques, des traits de soulignement, des traits d'union et des points. L'espace n'est pas autorisée.
4. Définissez l'intervalle **Keep Alive (sec),**l'intervalle, en secondes, auquel le haut-parleur BGP envoie des Keepalives à l'homologue (plage comprise entre 0 et 1 200 ; la valeur par défaut est 30). Si aucun Keepalive n'est reçu d'un homologue pendant un intervalle de temps d'attente, l'appairage BGP est fermé. Souvent, le temps d'attente est trois fois supérieur à l'intervalle Keep Alive pour permettre trois Keepalives manqués avant que l'appairage BGP ne soit abaissé.
5. Indiquez le **Hold Time (sec) (Temps d'attente (sec.)** : la durée du temps, en secondes, qui peut s'écouler entre des messages Keepalive ou Update successifs émis par l'homologue avant la fermeture de la connexion (plage comprise entre 3 et 3 600 ; valeur par défaut : 90).
6. Définissez le **Reconnect Retry Interval (intervalle de nouvelle tentative de reconnexion)** : nombre de secondes à attendre à l'état Inactif avant de réessayer de se connecter à l'homologue (plage comprise entre 1 et 3 600 ; la valeur par défaut est 15).
7. Définissez le **Open Delay Time (sec) (délai d'ouverture (sec)),**c'est-à-dire le nombre de secondes de délai entre l'ouverture de la connexion TCP à l'homologue et l'envoi du premier message d'ouverture BGP pour établir une connexion BGP (plage comprise entre 0 et 240 ; la valeur par défaut est 0).
8. Définissez **Minimum Route Advertise Interval (sec) (intervalle minimum d'annonce d'itinéraire (sec))**c'est-à-dire le temps minimum, en secondes, qui doit s'écouler entre une publicité et/ou le retrait d'itinéraires vers une destination particulière par un haut-parleur BGP vers un homologue (plage de 1 à 600 ; la valeur par défaut est de 30).
9. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Pour utiliser MP-BGP, créez un profil AFI (Address Family Identifier) BGP d'attributs partagés.

1. Sélectionnez **Network** > **Routing** > **Routing Profiles** > **BGP**.
2. **Ajoutez** un **profil de famille d'adresses BGP** par **nom** (un maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et peut contenir des caractères alphanumériques, des traits de soulignement, des traits d'union et des points. L'espace n'est pas autorisée.



3. Sélectionnez **IPv4** ou **IPv6** AFI pour spécifier le type de profil.
4. Sélectionnez **monodiffusion** ou **multidiffusion**.

> ***La multidiffusion*** *est prise en charge uniquement pour un* ***profil AFI IPv4*** *.*

5. Sous l'onglet **monodiffusion Activez SAFI** pour activer le SAFI unicast pour le profil. Sous l'onglet **multidiffusion activez SAFI** pour activer la multidiffusion SAFI pour le profil. Si **l'option Activer SAFI** est cochée pour la **monodiffusion** et **la multidiffusion**, les deux SAFI sont activés. Au moins un SAFI doit être activé pour que le profil BGP soit valide.
6. Sélectionnez **Reconfiguration logicielle de l'homologue avec des itinéraires stockés** pour que le pare-feu effectue une réinitialisation logicielle de lui-même après la mise à jour des paramètres de l'un de ses homologues BGP. (Cette option est activée par défaut.)
7. **Annoncez tous les chemins aux pairs**: pour que BGP publie tous les chemins connus vers le voisin afin de préserver les capacités multichemins au sein d'un réseau.
8. **Annoncez le meilleur chemin pour chaque AS voisin** pour que BGP publie les chemins les plus connus vers les voisins afin de préserver les capacités multichemins au sein

 ©2024 Palo Alto Networks, Inc.

d'un réseau. Désactivez si vous souhaitez publier le même chemin d'accès pour tous les systèmes autonomes.

9. **Remplacer les ASN dans les mises à jour sortantes si AS-Path est égal à Remote-AS**: ce paramètre est utile si vous avez plusieurs sites appartenant au même numéro AS (AS 64512, par exemple) et qu'il existe un autre AS entre eux. Un routeur entre les deux sites reçoit une mise à jour publiant un itinéraire qui peut accéder à AS 64512. Afin d'éviter que le deuxième site annule la mise à jour parce qu'elle est aussi dans AS 64521, le routeur intermédiaire remplace AS 64512 par son propre numéro AS (ASN), AS 64522, par exemple.
10. Activez **Route Reflector Client** pour faire de l'homologue BGP un client Route Reflector dans un réseau IBGP.
11. **Origine de l'itinéraire par défaut (Originate Default Route**) : sélectionnez cette option pour générer un itinéraire par défaut et le placer dans le RIB BGP local.
12. **Carte d'itinéraire d'origine par défaut (Default Originate Route-Map**) : sélectionnez ou créez une carte d'itinéraire pour contrôler les attributs de l'itinéraire par défaut.
13. **Autorisez AS dans** :
    - **Origin (Origine)** : Accepte les itinéraires même si l'AS du pare-feu est présent dans AS_PATH.
    - **Occurrence** : nombre de fois où l'AS du pare-feu peut être dans un AS_PATH.
    - **None (Aucun)** : (paramètre par défaut) Aucune action.
14. **Nombre de préfixes (Number Prefixes**) : nombre maximal de préfixes à accepter (apprendre) de l'homologue. La plage est comprise entre 1 et 4 294 967 295 ; la valeur par défaut est 1,000.
15. **Threshold (Seuil)** : Saisissez le pourcentage de seuil du nombre maximum de préfixes. Les préfixes sont ajoutés au RIB local BGP. Si l'homologue publie plus que le seuil, le pare-feu applique l'Action indiquée (**Warning only (avertissement uniquement)** ou **Restart (redémarrage)**. La plage est de 1 à 100; la valeur par défaut est 100.
16. **Action :** : **Warning only (message d'avertissement uniquement)** dans les journaux système ou **Restart (Redémarrez)** la connexion d'homologue BGP après le dépassement du nombre maximal de préfixes.
17. Sélectionnez le **saut suivant** :
    - **Self** : permet au pare-feu de modifier l'adresse du tronçon suivant (dans les mises à jour qu'il reçoit) en sa propre adresse IP dans la mise à jour avant de l'envoyer. Ceci est utile lorsque le pare-feu communique avec un routeur EBGP (dans un autre AS) et avec un routeur IBGP (dans son propre AS). Par exemple, supposons que l'adresse next hop dans une mise à jour BGP qui arrive à AS 64512 est l'adresse IP de l'interface de sortie du routeur 2 où la mise à jour a été sortie AS 64518. La mise à jour indique que pour atteindre les réseaux dont le routeur 2 fait de la publicité, utilisez l'adresse du tronçon suivant du routeur 2. Toutefois, si le pare-feu envoie cette mise à jour à un voisin iBGP dans AS 64512, le tronçon suivant inchangé du routeur 2 est en dehors de AS 64512 et le voisin iBGP n'a pas de route vers celui-ci. Lorsque vous sélectionnez **Self**, le pare-feu remplace le Next Hop par sa propre adresse IP afin qu'un voisin iBGP puisse utiliser ce Next Hop pour atteindre le pare-feu, qui à son tour peut atteindre le routeur eBGP.

 ©2024 Palo Alto Networks, Inc.

- **Self Force (Force indépendante)** : Force le saut suivant en mode indépendant pour les itinéraires repris.
- **Aucun**(paramètre par défaut) Conservez le tronçon suivant d'origine dans l'attribut.

18. Pour que BGP supprime des numéros d'AS privés provenant de l'attribut AS_PATH des mises à jour que le pare-feu envoie à un homologue d'un autre AS, dans **Supprimer AS privé**, sélectionnez parmi ce qui suit :
    - **All (Tous)**: Supprime tous les numéros AS.
    - **Replace AS (Remplacer AS)** : Remplace tous les numéros AS par le numéro AS du pare-feu.
    - **None (Aucun)** : (paramètre par défaut) Aucune action.
19. Pour **Envoyer la communauté**, sélectionnez le type d'attribut de communauté BGP à envoyer dans les paquets de mise à jour sortants :
    - **All (toutes)** : envoie toutes les communautés.
    - **Both (les deux)** : envoie les communautés standard et étendues.
    - **Extended (étendues)** : envoie les communautés étendues.
    - **Large (grandes)** : envoie les grandes communautés.
    - **Standard** : envoie les communautés standard (RFC 1997).
    - **Aucun**: (paramètre par défaut) N'envoyez aucune communauté.
20. Pour **la liste ORF :**annoncez la capacité du groupe d'homologues ou de l'homologue à envoyer une liste de préfixes et/ou à recevoir une liste de préfixes pour implémenter le filtrage d'itinéraire sortant (ORF) à la source, et ainsi minimiser l'envoi ou la réception de préfixes indésirables dans les mises à jour. Sélectionnez un paramètre de fonctionnalité ORF :
    - **none**: (paramètre par défaut) Le groupe d'homologues ou l'homologue (où ce profil AFI est appliqué) n'a pas de fonctionnalité ORF.
    - **les deux**: annoncez que le groupe d'homologues ou l'homologue (où ce profil AFI est appliqué) peut **envoyer** une liste de préfixes et **recevoir** une liste de préfixes pour implémenter ORF.
    - **recevoir**: annoncez que le groupe d'homologues ou l'homologue (où ce profil AFI est appliqué) peut recevoir une liste de préfixes pour implémenter ORF. L'homologue local reçoit la capacité ORF et la liste de préfixes de l'homologue distant, qu'il implémente en tant que filtre d'itinéraire sortant.
    - **envoyer :**annoncez que le groupe d'homologues ou l'homologue (où ce profil AFI est appliqué) peut envoyer une liste de préfixes pour implémenter ORF. L'homologue distant (avec capacité de réception) reçoit la fonctionnalité ORF et implémente la liste de préfixes qu'il a reçue en tant que filtre d'itinéraire sortant lors de la publicité achemine vers l'expéditeur.

    ORF est une solution à deux problèmes potentiels: a) gaspiller de la bande passante en annonçant des itinéraires indésirables et b) filtrer les préfixes de route que le pair récepteur veut peut-être. Mettre en œuvre ORF en procédant comme suit :

    1. Spécifiez la fonctionnalité ORF dans le profil Famille d'adresses.

 ©2024 Palo Alto Networks, Inc.

2. Pour un groupe d'homologues ou un homologue qui est un expéditeur (capacité d'**envoi** ou **les deux**), créez une liste de préfixes contenant l'ensemble de préfixes que le groupe d'homologues/homologues souhaite recevoir.
3. Créez un profil de filtrage BGP et, dans la liste des préfixes entrants, sélectionnez la liste de préfixes que vous avez créée.
4. Pour le groupe d'homologues BGP, sélectionnez le profil de famille d'adresses que vous avez créé pour l'appliquer au groupe d'homologues. Dans le cas de l'expéditeur, sélectionnez également le profil de filtrage que vous avez créé (qui indique la liste des préfixes). Si le groupe d'homologues ou l'homologue est un récepteur ORF uniquement, il n'a pas besoin du profil de filtrage ; il n'a besoin que du profil Famille d'adresses pour indiquer la capacité de **réception** ORF.

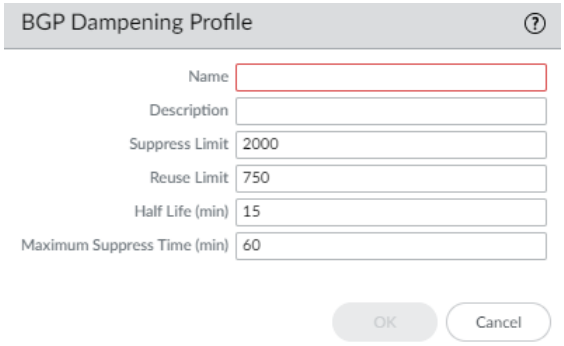
21. Cliquez sur **OK**.

STEP 4 | Créez un profil d'amortissement BGP.

1. Sélectionnez **Network** > **Routing** > **Routing Profiles** > **BGP**.
2. **Ajoutez** un **profil d'amortissement BGP** par **nom**. Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et peut contenir des caractères alphanumériques, des traits de soulignement, des traits d'union et des points. L'espace n'est pas autorisée.
3. Saisissez une **Description** utile.
4. **Supprimer la limite (Suppress Limit**) : entrez la valeur suppress (valeur cumulée des pénalités pour le battement), après quoi toutes les routes provenant d'un homologue sont amorties. La plage est comprise entre 1 et 20 000 ; la valeur par défaut est 2 000.
5. **Limite de réutilisation (Reuse Limit**) : entrez la valeur qui contrôle le moment où un itinéraire peut être réutilisé en fonction de la procédure décrite pour **Half Life**. La plage est comprise entre 1 et 20 000 ; la valeur par défaut est 750.
6. **Half Life (min) (Demi-vie (min))** :entrez le nombre de minutes pour la demi-durée de vie pour contrôler la mesure de stabilité (pénalité) appliquée à un itinéraire de battement. La plage est comprise entre 1 et 45 ; la valeur par défaut est 15. La mesure de stabilité commence à 1 000. Une fois qu'un itinéraire pénalisé s'est stabilisé, le compte à rebours de la demi-vie jusqu'à son expiration, auquel cas la mesure de stabilité suivante appliquée à l'itinéraire ne représente que la moitié de la valeur précédente (500). Les coupes successives se poursuivent jusqu'à ce que la mesure de stabilité soit inférieure à la moitié de la limite de réutilisation, puis la mesure de stabilité est supprimée de l'itinéraire.

 ©2024 Palo Alto Networks, Inc.

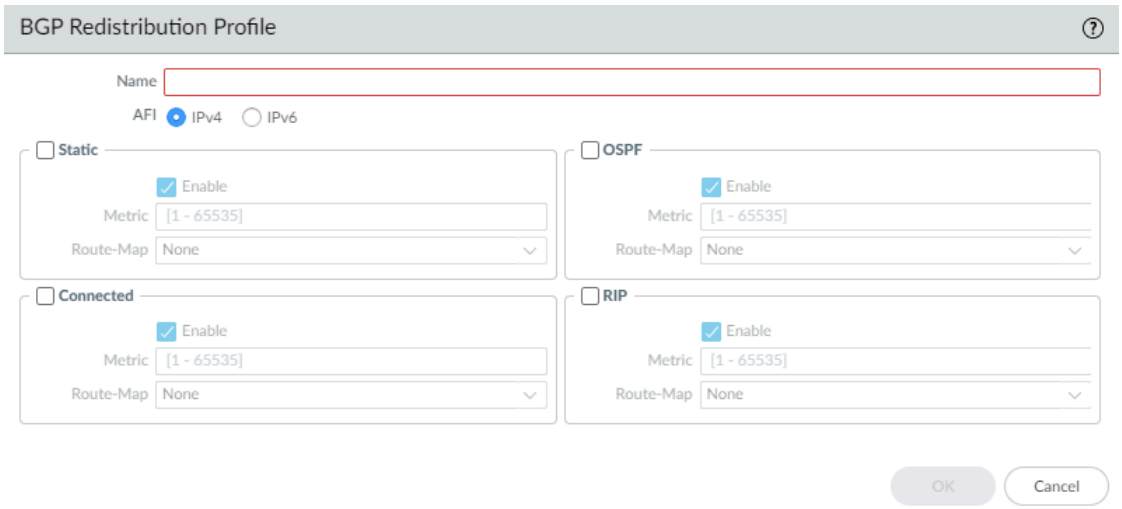
7. **Maximum Suppress Time (min) (Temps de suppression maximal (min))**: entrez le nombre maximal de minutes pendant lesquelles un itinéraire peut être supprimé, quel que soit son instabilité. La plage est comprise entre 1 et 255 ; la valeur par défaut est 60.



8. Cliquez sur **OK**.

STEP 5 | Créez un profil de redistribution BGP pour redistribuer des itinéraires statiques, connectés et OSPF (qui correspondent à la carte d'itinéraire correspondante) vers BGP.

1. Sélectionnez **Network** > **Routing** > **Routing Profiles** > **BGP**.
2. **Ajoutez** un **profil de redistribution BGP** par **nom** (un maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et peut contenir des caractères alphanumériques, des traits de soulignement, des traits d'union et des points. L'espace n'est pas autorisée.
3. Sélectionnez l'**AFI** des itinéraires à redistribuer : **IPv4** ou **IPv6**.



4. Sélectionnez **Statique** pour configurer la redistribution d'itinéraire statique.
5. **Activez** la redistribution des itinéraires statiques IPv4 ou IPv6 (en fonction de l'AFI que vous avez sélectionné).
6. Configurez la **mesure** à appliquer aux itinéraires statiques qui sont redistribués dans BGP (plage de 1 à 65 535).
7. Sélectionnez une **carte de routage** pour spécifier les critères de correspondance qui déterminent les itinéraires statiques à redistribuer. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de

 ©2024 Palo Alto Networks, Inc.

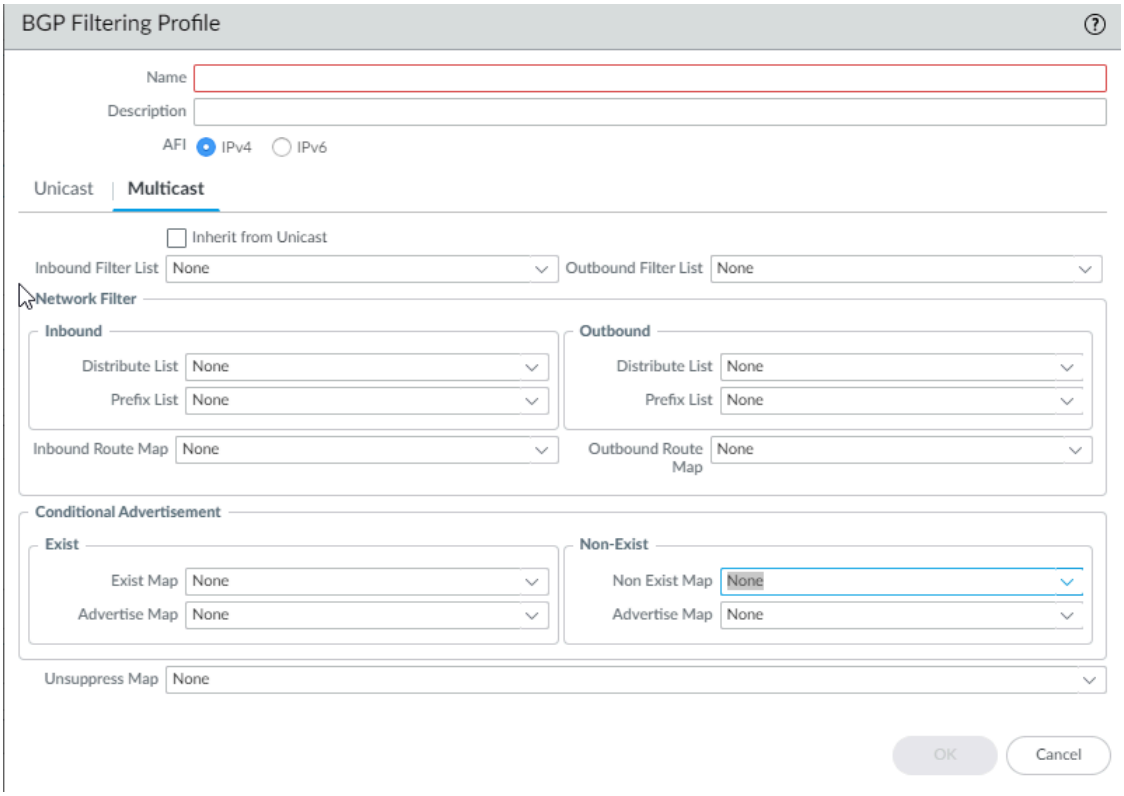
mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.

8. Sélectionnez **Connecté** pour configurer la redistribution des itinéraires connectés.
9. **Activez** la redistribution des itinéraires IPv4 ou IPv6 connectés localement (en fonction de l'AFI que vous avez sélectionné).
10. Configurez la **mesure** à appliquer aux itinéraires connectés qui sont redistribués dans BGP (plage de 1 à 65 535).
11. Sélectionnez une **carte routière** pour spécifier les critères de correspondance qui ont déterminé les itinéraires connectés à redistribuer. La valeur par défaut est Aucune. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
12. (IPv4 AFI uniquement) Sélectionnez **OSPFv2** pour configurer la redistribution d'itinéraire OSPFv2.
13. **Activez** la redistribution des itinéraires OSPFv2.
14. Configurez la **mesure** à appliquer aux itinéraires statiques qui sont redistribués dans BGP (plage de 1 à 65 535).
15. Sélectionnez une **carte de routage** pour spécifier les critères de correspondance qui déterminent les itinéraires OSPF à redistribuer. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
16. (IPv4 AFI uniquement) Sélectionnez **RIPv2** pour configurer la redistribution d'itinéraire RIPv2.
17. **Activer la** redistribution des itinéraires RIPv2.
18. Configurez la **mesure** à appliquer aux itinéraires statiques qui sont redistribués dans BGP (plage de 1 à 65 535).
19. Sélectionnez une **carte de routage** pour spécifier les critères de correspondance qui déterminent les itinéraires RIP à redistribuer. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
20. (IPv6 AFI uniquement) Sélectionnez **OSPFv3** pour configurer la redistribution de route OSPFv3.
21. **Activez** la redistribution des itinéraires OSPFv3.
22. Saisissez la **mesure** à appliquer aux itinéraires statiques qui sont redistribués dans BGP (plage de 1 à 65 535).
23. Sélectionnez une **carte de routage** pour spécifier les critères de correspondance qui déterminent les itinéraires OSPFv3 à redistribuer. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
24. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Créez un profil de filtrage BGP.

1. Sélectionnez **Network** > **Routing** > **Routing Profiles** > **BGP**.
2. **Ajoutez** un **profil de filtrage BGP** par **nom** (un maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et peut contenir des caractères alphanumériques, des traits de soulignement, des traits d'union et des points. L'espace n'est pas autorisée.
3. Saisissez une **Description** utile.
4. Sélectionnez **IPv4** ou **IPv6** Address Family Identifier (AFI) pour indiquer le type d'itinéraire à filtrer.



5. Sélectionnez **Unicast (Monodiffusion)** ou **Multicast (Multidiffusion)** Subsequent Address Family Identifier (SAFI).
6. Pour **unicast (monodiffusion)**, **Inbound Filter List (Liste de filtres entrants)** : sélectionnez une liste d'accès AS Path ou créez une nouvelle liste d'accès AS Path pour spécifier que, lors de la réception d'itinéraires d'homologues, seuls les itinéraires ayant le même as Path sont importés à partir du groupe d'homologues ou de l'homologue, c'est-à-dire ajoutés au RIB BGP local.
7. Dans la zone Filtre réseau, **Entrant—Liste de distribution** : Utilisez une liste d'accès (adresse source uniquement, et non adresse de destination) pour filtrer les informations

 ©2024 Palo Alto Networks, Inc.

de routage BGP reçues par BGP. Mutuellement exclusif avec la liste de préfixes entrants dans un seul profil de filtrage.

8. **Liste de préfixes** : utilisez une liste de préfixes pour filtrer les informations de routage BGP que BGP reçoit, en fonction d'un préfixe réseau. Mutuellement exclusif avec la liste de distribution entrante dans un seul profil de filtrage.
9. **Carte d'itinéraire entrante** : utilisez une carte d'itinéraire pour avoir encore plus de contrôle sur les itinéraires autorisés dans le RIB BGP local (critères de correspondance) et pour définir des attributs pour les itinéraires (Définir les options). Par exemple, vous pouvez contrôler la préférence d'itinéraire en faisant précéder un AS du chemin AS d'un itinéraire.

   Si une carte d'itinéraire entrante est configurée avec une liste de distribution entrante ou une liste de préfixes, les conditions de la carte d'itinéraire et de la liste doivent être remplies (LOGIQUE ET).
10. **Liste de filtres sortants** : sélectionnez une liste d'accès AS Path ou créez une nouvelle liste d'accès AS Path pour spécifier que seuls les itinéraires avec le même AS Path sont publiés sur un routeur homologue (groupe homologue ou homologue où ce filtre est appliqué).
11. **Sortant** :**Liste de distribution :**utilisez une liste d'accès pour filtrer les informations de routage BGP que BGP publie, en fonction de l'adresse IP de la destination. Mutuellement exclusif avec la liste de préfixes sortants dans un seul profil de filtrage.
12. **Liste de préfixes** : utilisez une liste de préfixes pour filtrer les informations de routage BGP que BGP publie, en fonction d'un préfixe réseau. Mutuellement exclusif avec la liste de distribution sortante dans un seul profil de filtrage.
13. **Carte d'itinéraire sortante** : utilisez une carte d'itinéraire pour avoir encore plus de contrôle sur les itinéraires annoncés par BGP (critères de correspondance) et pour définir des attributs pour les itinéraires annoncés.

    Si une carte de routage sortante est configurée avec une liste de distribution sortante ou une liste de préfixes, les conditions de la carte d'itinéraire et de la liste doivent être remplies (logique ET).
14. Configurez des publications conditionnelles, qui vous permettent de contrôler l'itinéraire à publier dans le cas où un itinéraire différent existe ou n'existe pas dans le RIB BGP local. Une route qui n'existe pas dans le RIB BGP local peut indiquer un échec d'appairage ou d'accessibilité. Les publications conditionnelles sont utiles dans les cas où vous souhaitez forcer des itinéraires vers un AS en direction d'un autre. Par exemple, lorsque vous disposez de liaisons vers Internet passant par plusieurs ISP et que vous voulez que le trafic soit acheminé vers un fournisseur à la place d'un autre, sauf s'il y a une perte de connectivité avec le fournisseur préféré. Dans la zone de Publication conditionnelle **Exist** :
    - Sélectionnez ou créez une carte d'itinéraire dans **Exist map (carte existante)** existante pour spécifier les critères de correspondance de la publication conditionnelle. Seule la partie Match de la carte d'itinéraire dans ce champ est prise en compte ; la partie Définir est ignorée.
    - **Annoncer la carte (Advertise Map)** : sélectionnez ou créez une carte d'itinéraire pour spécifier les itinéraires à publier si la condition est remplie (les itinéraires de la carte

 ©2024 Palo Alto Networks, Inc.

existante existent dans le RIB BGP local). Seule la partie Match de la carte d'itinéraire dans ce champ est prise en compte ; la partie Définir est ignorée.

15. Dans la zone Publicité conditionnelle **Non-Exist (non existante)** :
    - Sélectionnez ou créez une carte d'itinéraire dans le champ**Non-Exist Map (Carte inexistante)** pour spécifier les critères de correspondance pour lesquels les itinéraires n'existent pas dans le RIB BGP local afin de publier conditionnellement. Seule la partie Match de la carte d'itinéraire dans ce champ est prise en compte ; la partie Définir est ignorée.
    - **Annoncer la carte (Advertise Map**) : sélectionnez ou créez une carte d'itinéraire pour spécifier les itinéraires à publier lorsque les itinéraires de la carte inexistante ne se trouvent pas dans le RIB BGP local. Seule la partie Match de la carte d'itinéraire dans ce champ est prise en compte ; la partie Définir est ignorée.
16. **Annuler la suppression de la carte (Unsuppress Map)**: sélectionnez ou créez une carte d'itinéraire des itinéraires que vous souhaitez annuler, peut-être parce qu'ils ont été résumés et donc supprimés, ou parce qu'ils répondaient à des critères d'amortissement, mais vous souhaitez que des itinéraires spécifiques soient annoncés (non supprimés).
17. (IPv4 AFI uniquement) Sélectionnez **Multidiffusion** pour filtrer les itinéraires de multidiffusion MP-BGP. Sélectionnez **Hériter de la monodiffusion** si vous souhaitez que tous les filtres du SAFI unicast s'appliquent également au SAFI multidiffusion. Sinon, continuez à configurer les champs de filtrage suivants.
18. Pour **la multidiffusion**, **liste de filtres entrants** : spécifiez une liste d'accès au chemin AS ou créez une nouvelle liste d'accès au chemin AS pour spécifier que, lors de la réception d'itinéraires d'homologues, seuls les itinéraires ayant le même chemin AS sont importés à partir du groupe d'homologues ou de l'homologue, c'est-à-dire ajoutés au RIB BGP local.
19. Dans la zone Filtre réseau, **Entrant—Liste de distribution** : Utilisez une liste d'accès (adresse source uniquement, et non adresse de destination) pour filtrer les informations de routage BGP reçues par BGP. Mutuellement exclusif avec la liste de préfixes entrants dans un seul profil de filtrage.
20. **Liste de préfixes** : utilisez une liste de préfixes pour filtrer les informations de routage BGP que BGP reçoit, en fonction d'un préfixe réseau. Mutuellement exclusif avec la liste de distribution entrante dans un seul profil de filtrage.
21. **Carte d'itinéraire entrante** : utilisez une carte d'itinéraire pour avoir encore plus de contrôle sur les itinéraires autorisés dans le RIB BGP local (critères de correspondance) et pour définir des attributs pour les itinéraires (Définir les options). Par exemple, vous pouvez contrôler la préférence d'itinéraire en faisant précéder un AS du chemin AS d'un itinéraire.

    Si une carte d'itinéraire entrante est configurée avec une liste de distribution entrante ou une liste de préfixes, les conditions de la carte d'itinéraire et de la liste doivent être remplies (LOGIQUE ET).
22. **Liste de filtres sortants** : sélectionnez une liste d'accès AS Path ou créez une nouvelle liste d'accès AS Path pour spécifier que seuls les itinéraires avec le même AS Path sont publiés sur un routeur homologue (groupe homologue ou homologue où ce filtre est appliqué).

 ©2024 Palo Alto Networks, Inc.

23. **Sortant** :**Liste de distribution :**utilisez une liste d'accès pour filtrer les informations de routage BGP que BGP publie, en fonction de l'adresse IP de la destination. Mutuellement exclusif avec la liste de préfixes sortants dans un seul profil de filtrage.
24. **Liste de préfixes** : utilisez une liste de préfixes pour filtrer les informations de routage BGP que BGP publie, en fonction d'un préfixe réseau. Mutuellement exclusif avec la liste de distribution sortante dans un seul profil de filtrage.
25. **Carte d'itinéraire sortante** : utilisez une carte d'itinéraire pour avoir encore plus de contrôle sur les itinéraires annoncés par BGP (critères de correspondance) et pour définir des attributs pour les itinéraires annoncés.

    Si une carte de routage sortante est configurée avec une liste de distribution sortante ou une liste de préfixes, les conditions de la carte d'itinéraire et de la liste doivent être remplies (logique ET).
26. Configurez des publications conditionnelles, qui vous permettent de contrôler l'itinéraire à publier dans le cas où un itinéraire différent existe ou n'existe pas dans le RIB BGP local. Une route qui n'existe pas dans le RIB BGP local peut indiquer un échec d'appairage ou d'accessibilité. Les publications conditionnelles sont utiles dans les cas où vous souhaitez forcer des itinéraires vers un AS en direction d'un autre. Par exemple, lorsque vous disposez de liaisons vers Internet passant par plusieurs ISP et que vous voulez que le trafic soit acheminé vers un fournisseur à la place d'un autre, sauf s'il y a une perte de connectivité avec le fournisseur préféré. Dans la zone de Publication conditionnelle **Exist** :
    - Sélectionnez ou créez une carte d'itinéraire dans **Exist map (carte existante)** existante pour spécifier les critères de correspondance de la publication conditionnelle. Seule la partie Match de la carte d'itinéraire dans ce champ est prise en compte ; la partie Définir est ignorée.
    - **Annoncer la carte (Advertise Map**) : sélectionnez ou créez une carte d'itinéraire pour spécifier les itinéraires à publier si la condition est remplie (les itinéraires de la carte existante existent dans le RIB BGP local). Seule la partie Match de la carte d'itinéraire dans ce champ est prise en compte ; la partie Définir est ignorée.
27. Dans la zone Publicité conditionnelle **Non-Exist (non existante)** :
    - Sélectionnez ou créez une carte d'itinéraire dans le champ**Non-Exist Map (Carte inexistante)** pour spécifier les critères de correspondance pour lesquels les itinéraires n'existent pas dans le RIB BGP local afin de publier conditionnellement. Seule la partie Match de la carte d'itinéraire dans ce champ est prise en compte ; la partie Définir est ignorée.
    - **Annoncer la carte (Advertise Map**) : sélectionnez ou créez une carte d'itinéraire pour spécifier les itinéraires à publier lorsque les itinéraires de la carte inexistante ne se trouvent pas dans le RIB BGP local. Seule la partie Match de la carte d'itinéraire dans ce champ est prise en compte ; la partie Définir est ignorée.
28. **Annuler la suppression de la carte (Unsuppress Map)**: sélectionnez ou créez une carte d'itinéraire des itinéraires que vous souhaitez annuler, peut-être parce qu'ils ont été résumés et donc supprimés, ou parce qu'ils répondaient à des critères d'amortissement, mais vous souhaitez que des itinéraires spécifiques soient annoncés (non supprimés).
29. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

Créer des filtres pour le moteur de routage avancé

Le moteur de routage avancé prend en charge les filtres décrits dans cette rubrique. Les listes d'accès, les listes de préfixes et les cartes de routage de redistribution peuvent s'appliquer à BGP, OSPFv2, OSPFv3 et RIPv2. Les listes d'accès et les listes de préfixes peuvent également s'appliquer à la multidiffusion IPv4. Les cartes routières de multidiffusion s'appliquent à la multidiffusion IPv4. Les listes d'accès aux chemins AS, les listes de communautés et les cartes routières BGP s'appliquent uniquement à BGP.

Créez un filtre et référencez le filtre dans un profil ou un autre emplacement approprié pour appliquer facilement et de manière cohérente des paramètres qui contrôlent des éléments tels que l'acceptation de l'itinéraire des homologues vers le RIB local, les publicités d'acheminement vers les homologues, les publicités conditionnelles, la définition d'attributs, l'exportation et l'importation d'itinéraires vers et depuis d'autres routeurs, l'agrégation d'itinéraires et la redistribution d'itinéraires.

- **Listes d'accès** : utilisez une liste d'accès :
  - Pour filtrer les itinéraires réseau en fonction des adresses source IPv4/IPv6 et des adresses de destination IPv4. Pour les listes d'accès IPv4, les adresses source et de destination peuvent être spécifiées par un masque d'adresse et de caractère générique pour exprimer une plage d'adresses. Les listes d'accès IPv6 peuvent spécifier des adresses sources et des sous-réseaux.
  - Dans un profil de filtrage BGP, spécifiez une liste de distribution entrante (liste d'accès) pour contrôler les itinéraires que BGP acceptera à partir d'un groupe d'homologues ou d'un homologue (voisin). Cela signifie que les itinéraires correspondant à une règle de liste de refus d'accès ne sont pas placés dans le RIB BGP local ; les itinéraires correspondant à une règle de liste d'accès aux autorisations sont placés dans le RIB BGP local. Vous appliquez le profil de filtrage BGP à un groupe d'homologues BGP ou à un homologue dans le champ Filtrage IPv4 Unicast ou Filtrage IPv6 Unicast. (Pour ce faire, sélectionnez **Hériter de non**). Les paramètres d'homologue ont priorité sur les paramètres de groupe d'homologues.
  - Dans un profil de filtrage BGP, spécifiez une liste de distribution sortante (liste d'accès) pour contrôler les itinéraires que le pare-feu publie vers son groupe d'homologues ou son homologue, en fonction de votre réseau et de votre déploiement BGP. Appliquez ensuite le profil de filtrage BGP à un groupe d'homologues ou à un homologue BGP dans le champ Filtrage IPv4 Unicast ou Filtrage IPv6 Unicast. (Pour ce faire, sélectionnez **Hériter de non**). Les paramètres d'homologue ont priorité sur les paramètres de groupe d'homologues.
  - En tant que critères de correspondance dans une carte d'itinéraire de redistribution pour spécifier les adresses de destination IPv4 ou IPv6, le tronçon suivant ou la source de routage.
  - Dans une carte d'itinéraire BGP en tant que critères de correspondance pour une adresse IPv4, un tronçon suivant ou une source d'itinéraire, ainsi que pour une adresse IPv6.
  - Dans OSPFv2 et OSPFv3, importer des listes et exporter des listes pour un routeur de frontière de zone (ABR).

 ©2024 Palo Alto Networks, Inc.

- Pour spécifier des autorisations de groupe PIM pour la multidiffusion IPv4.

Une liste d'accès n'est pas destinée à filtrer le trafic utilisateur ou à assurer la sécurité.

Une liste d'accès peut avoir plusieurs règles ; les itinéraires sont évalués par rapport aux règles dans l'ordre séquentiel. Lorsqu'un itinéraire correspond à une règle, l'action de refus ou d'autorisation se produit et l'itinéraire n'est pas évalué par rapport aux règles suivantes.

La vue agrégée affiche toutes les listes d'accès configurées ; vous pouvez mettre en surbrillance une liste d'accès pour la modifier ou la supprimer.

- **Listes de préfixes**: utilisez une liste de préfixes :
  - Pour filtrer les itinéraires réseau ajoutés à un RIB local en fonction du préfixe d'itinéraire et de la longueur du préfixe.
  - Dans un profil de filtrage BGP, spécifiez une liste de préfixes entrants pour contrôler les itinéraires que BGP acceptera à partir d'un groupe d'homologues ou d'un homologue (voisin). Cela signifie que les itinéraires correspondant à une règle de liste de préfixes de refus ne sont pas placés dans le RIB BGP local ; les itinéraires correspondant à une règle de liste de préfixes d'autorisation sont placés dans le RIB BGP local. Appliquez ensuite le profil de filtrage BGP à un groupe d'homologues BGP dans le champ Filtrage IPv4 Unicast ou Filtrage IPv6 Unicast. (Pour ce faire, sélectionnez Hériter de non). Les paramètres d'homologue ont priorité sur les paramètres de groupe d'homologues.
  - Dans un profil de filtrage BGP, spécifiez une liste de préfixes sortants pour contrôler les itinéraires que le pare-feu publie vers son groupe d'homologues ou son homologue, en fonction de votre réseau et de votre déploiement BGP. Appliquez ensuite le profil de filtrage BGP à un groupe d'homologues ou à un homologue BGP dans le champ Filtrage IPv4 Unicast ou Filtrage IPv6 Unicast. (Pour ce faire, sélectionnez Hériter de non). Les paramètres d'homologue ont priorité sur les paramètres de groupe d'homologues.
  - En tant que critères de correspondance dans une carte d'itinéraire de redistribution pour spécifier les adresses de destination IPv4 ou IPv6, le tronçon suivant ou la source de routage.
  - Dans une carte d'itinéraire BGP en tant que critères de correspondance pour une adresse IPv4, un tronçon suivant ou une source d'itinéraire, ainsi que pour une adresse IPv6.
  - Pour un ABR OSPFv2 ou OSPFv3 d'une zone, dans une liste de filtres entrants ou une liste de filtres sortants.
  - Dans une configuration PIM de multidiffusion IPv4 pour spécifier un seuil SPT.
  - Dans une carte d'itinéraire de multidiffusion IPv4.

  Une liste de préfixes peut avoir plusieurs règles ; les itinéraires sont évalués par rapport aux règles dans l'ordre séquentiel. Lorsqu'un itinéraire correspond à une règle, l'action de refus ou d'autorisation se produit et l'itinéraire n'est pas évalué par rapport aux règles suivantes. Une liste de préfixes est flexible en ce sens qu'elle vous permet de configurer un préfixe avec une longueur de préfixe (qui, ensemble, identifient le préfixe) et d'avoir également une plage en spécifiant que la longueur du préfixe soit supérieure, inférieure ou égale à une valeur. Le pare-feu évalue les listes de préfixes plus efficacement que les listes d'accès.
- **Cartes d'itinéraire de redistribution** : utilisez une carte d'itinéraire de redistribution dans un profil de redistribution pour spécifier les routes BGP, OSPFv2, OSPFv3, RIP, connectées ou

 ©2024 Palo Alto Networks, Inc.

statiques (le protocole source) à redistribuer à BGP, OSPFv2, OSPFv3, RIP ou au RIB local (le protocole de destination). Vous pouvez également redistribuer les itinéraires d'hôte BGP aux homologues BGP. Les critères de correspondance peuvent inclure des adresses IPv4 et IPv6 spécifiées par une liste d'accès et une liste de préfixes.

Une carte d'itinéraire de redistribution peut avoir plusieurs entrées ; les itinéraires sont évalués par rapport aux entrées dans l'ordre séquentiel. Lorsqu'un itinéraire correspond à une entrée, il est autorisé ou refusé et l'itinéraire n'est pas évalué par rapport aux entrées suivantes. Si l'action de l'entrée correspondante est Autoriser, le pare-feu définit également les attributs configurés de la carte de routage sur l'itinéraire redistribué.

- **Cartes routières de multidiffusion (Multicast Route Maps**) : créez une carte d'itinéraire de multidiffusion pour filtrer les sources d'une interface IGMP dynamique.

Les filtres suivants s'appliquent uniquement à BGP.

- **Listes d'accès as (AS Path Access Lists**) : créez une liste d'accès AS Path :
  - Pour contrôler l'importation d'itinéraires BGP (dans le RIB BGP local) provenant d'un autre routeur, utilisez-le dans un profil de filtrage BGP, dans la liste des filtres entrants. Par exemple, vous souhaitez importer uniquement des itinéraires qui sont passés par des systèmes autonomes spécifiques.
  - Pour contrôler l'exportation des itinéraires BGP vers un autre routeur, utilisez dans un profil de filtrage BGP, dans la liste des filtres sortants.
  - Pour faire tout ce qu'une carte d'itinéraire BGP peut faire, utilisez une carte d'itinéraire BGP comme critère de correspondance.
  - Pour redistribuer les itinéraires BGP, utilisez dans une carte d'itinéraire de redistribution BGP (AS Path) comme critère de correspondance.

  Une liste d'accès AS Path peut avoir un maximum de 64 règles et se termine par une règle implicite **Autoriser tout** . Utilisez une liste d'accès AS Path pour refuser les systèmes autonomes. Les itinéraires sont évalués par rapport aux règles dans l'ordre séquentiel. Lorsqu'un itinéraire correspond à une règle, l'action de refus ou d'autorisation se produit et l'itinéraire n'est pas évalué par rapport aux règles suivantes.
- **Listes de communauté :**créez une liste de communauté :
  - pour référencer dans une carte d'itinéraire BGP afin de faire correspondre les attributs de communauté BGP des itinéraires que vous souhaitez contrôler d'une manière ou d'une autre. Par exemple, vous pouvez définir un groupe d'itinéraires (qui partagent un attribut de communauté) pour avoir une métrique spécifique ou une préférence locale.
  - Pour référencer dans les actions définies d'une carte d'itinéraire BGP pour supprimer des communautés des itinéraires qui répondent aux critères de correspondance.
  - Pour faire correspondre les communautés BGP dans les itinéraires que vous souhaitez redistribuer à l'aide d'une carte d'itinéraire de redistribution.

  Une liste communautaire peut avoir plusieurs règles ; les itinéraires sont évalués par rapport aux règles dans l'ordre séquentiel. Lorsqu'un itinéraire correspond à une règle, l'action de refus ou d'autorisation se produit et l'itinéraire n'est pas évalué par rapport aux règles suivantes.
- **Cartes d'itinéraires BGP :**créez une carte d'itinéraires BGP :
  - Pour le champ **Route-Map d'origine par défaut** d'un profil AFI BGP , les critères de correspondance définissent quand générer l'itinéraire par défaut (0.0.0.0). Appliquez le profil

 ©2024 Palo Alto Networks, Inc.

AFI BGP à un groupe de pairs ou à un homologue BGP. Les critères de correspondance peuvent être n'importe quel paramètre et s'il existe une correspondance avec un itinéraire BGP existant, l'itinéraire par défaut est créé ; la partie Définir de la carte d'itinéraire n'est pas utilisée. Au lieu de cela, vous pouvez utiliser une carte de routage sortante pour définir les propriétés de l'itinéraire par défaut généré.

- Pour définir (remplacer) les attributs BGP que BGP envoie à un homologue.
- Pour NAT, pour définir l'adresse source et le tronçon suivant IPv4 pour un certain groupe de préfixes que vous annoncez, entrez une adresse IP publique du pool NAT pour remplacer une adresse IP privée.
- Pour redistribuer des itinéraires statiques, connectés ou OSPF dans BGP ; puis référencez la carte d'itinéraire BGP dans un profil de redistribution BGP.
- Dans un profil de filtrage BGP, utilisez une carte d'itinéraire BGP dans **Carte d'itinéraire entrante** ou **Carte d'itinéraire sortant** pour filtrer les itinéraires acceptés (appris) des homologues BGP dans le RIB BGP local (entrant) ou annoncés aux homologues BGP (sortants).
- Pour publier conditionnellement des itinéraires BGP, dans un profil de filtrage BGP, créez une **carte d'existence** qui spécifie que si ces conditions de l'itinéraire existent, publiez l'itinéraire en fonction d'une carte de publicité. Vous pouvez également spécifier que si ces conditions n'existent pas, annoncez l'itinéraire en fonction d'une **carte de publicité inexistante**.
- Dans un profil de filtrage BGP, définissez un tronçon suivant IPv4 pour utiliser une adresse NAT publique plutôt qu'une adresse privée.
- Dans un profil de filtrage BGP, utilisez une carte d'itinéraire BGP pour annuler les itinéraires qui ont été supprimés en raison de l'amortissement ou de l'agrégation d'itinéraires.
- Pour filtrer conditionnellement des itinéraires plus spécifiques, pour un routeur logique, configurez les **itinéraires d'agrégation** BGP et fournissez la **carte de suppression**.
- Pour définir des attributs pour un itinéraire agrégé, pour un routeur logique, configurez BGP **Aggregate Routes** et fournissez la carte **d'attributs**.

Un filtre peut avoir plusieurs règles ; le pare-feu évalue les paquets ou les itinéraires par rapport aux règles d'un filtre dans l'ordre par numéro de séquence (**Seq**) de la règle. Lorsqu'un paquet ou un itinéraire correspond à une règle, l'action de refus ou d'autorisation se produit et le paquet ou l'itinéraire n'est pas évalué par rapport aux règles suivantes.

Tous les filtres, à l'exception des listes d'accès AS Path, se terminent par une règle implicite ***`Deny Any`*** *. Tous les filtres, à l'exception des listes d'accès AS Path, doivent avoir au moins une règle d'****`autorisation`*** *; sinon, tous les itinéraires/paquets examinés sont refusés. Les listes d'accès AS Path se terminent par une règle implicite* ***`Autoriser tout`*** *.*

Sélectionnez un numéro **Seq** configuré pour ouvrir une règle et la modifier. Sélectionnez un champ **Action** dans une règle configurée pour modifier uniquement l'action Autoriser ou Refuser.

Lors de l'ajout d'une règle, laissez suffisamment de numéros de séquence inutilisés entre les règles pour permettre l'insertion de futures règles dans le filtre. Par exemple, utilisez les numéros Seq 10, 20, 30, etc.

 ©2024 Palo Alto Networks, Inc.

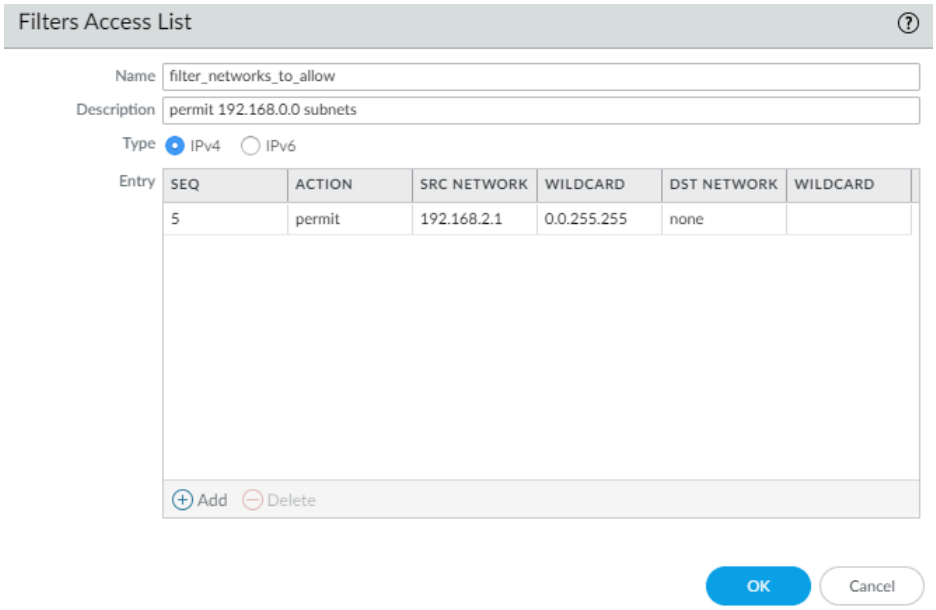
STEP 1 | Créez une liste d'accès pour autoriser ou refuser les adresses IPv4 ou IPv6 où ce filtre est appliqué.

1. Sélectionnez **Network (Réseau)** > **Routing (Routage)** > **Routing Profiles (Profils de routage)** > **Filters (Filtres)**.
2. **Ajoutez** une **liste d'accès aux filtres** par **nom** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.
3. Saisissez une **Description** utile.
4. Sélectionnez la **Type de liste d'accès** : **IPv4** ou **IPv6**.
    1. Pour IPv4, **ajoutez** une **entrée IPv4** et entrez le numéro **Seq** de la règle (la plage est comprise entre 1 et 65 535).
    2. Sélectionnez **Action**: **Refuser** (valeur par défaut) ou **Autoriser**.
    3. Pour **Adresse**, source, il existe trois options : sélectionnez **Adresse** et dans le champ **Adresse** suivant entrez une adresse IPv4. Entrez un masque **générique** pour indiquer une plage. Un zéro (0) dans le masque indique que le bit doit correspondre au bit correspondant dans l'adresse ; un (1) dans le masque indique un bit « ne s'en soucie pas ». Les autres options sont **Any** ou**None**.
    4. Pour **Adresse**, de destination, sélectionnez **Adresse** et, dans le champ **Adresse** suivant entrez une adresse IPv4. Entrez un **caractère générique**. Un zéro (0) dans le masque

 ©2024 Palo Alto Networks, Inc.

indique un bit qui doit correspondre ; un (1) dans le masque indique un morceau « ne s'en soucie pas ». Les autres options sont **Any** ou **None**.

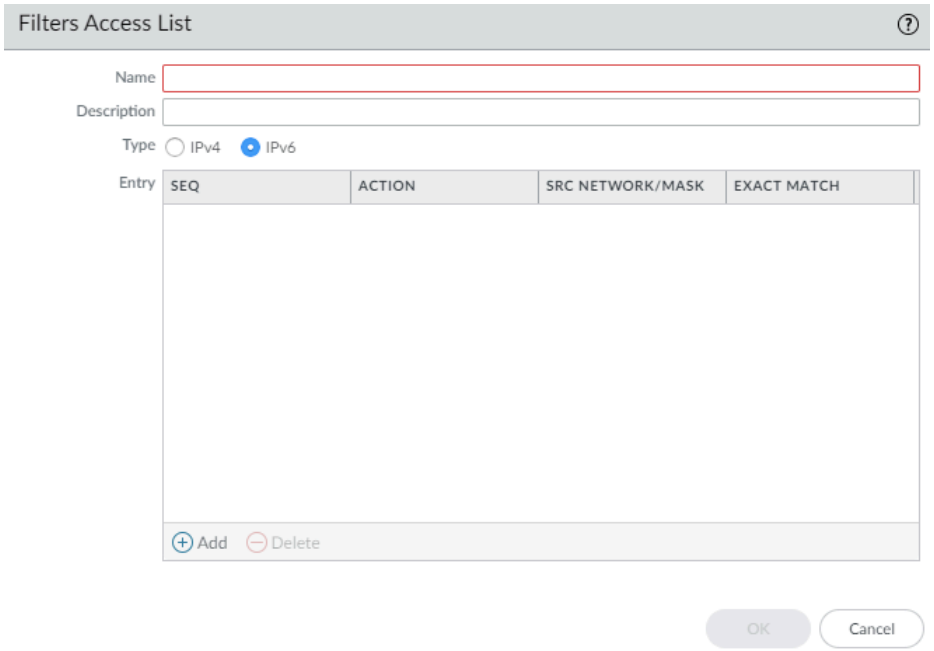
5. Cliquez sur **OK** pour enregistrer l'entrée.



5. Vous pouvez également sélectionner le **type IPv6**.
   1. Pour IPv6, **ajoutez** une **entrée IPv6** et entrez le numéro **Seq** (plage comprise entre 1 et 65 535).
   2. Sélectionnez **Action**: **Refuser** (valeur par défaut) ou **Autoriser**.
   3. Pour **Adresse source**, il existe trois options : sélectionnez **Adresse** et dans le champ **Adresse** suivant entrez une **adresse** IPv6. Vous pouvez éventuellement sélectionner **Correspondance exacte de cette adresse** pour que le pare-feu effectue une comparaison du préfixe et de la longueur du préfixe et qu'ils doivent correspondre exactement ; sinon, le pare-feu détermine la comparaison des correspondances en fonction du fait que l'itinéraire se trouve ou non dans le même sous-réseau que le préfixe configuré. (Si l'adresse source est **Any** ou **None**, vous ne pouvez pas sélectionner **Correspondance exacte de cette adresse**.) Les autres options sont **Any** ou **None**.

©2024 Palo Alto Networks, Inc.

4. Cliquez sur **OK** pour enregistrer l'entrée. Ajoutez éventuellement d'autres entrées.



6. Cliquez sur **OK** pour enregistrer la liste d'accès.

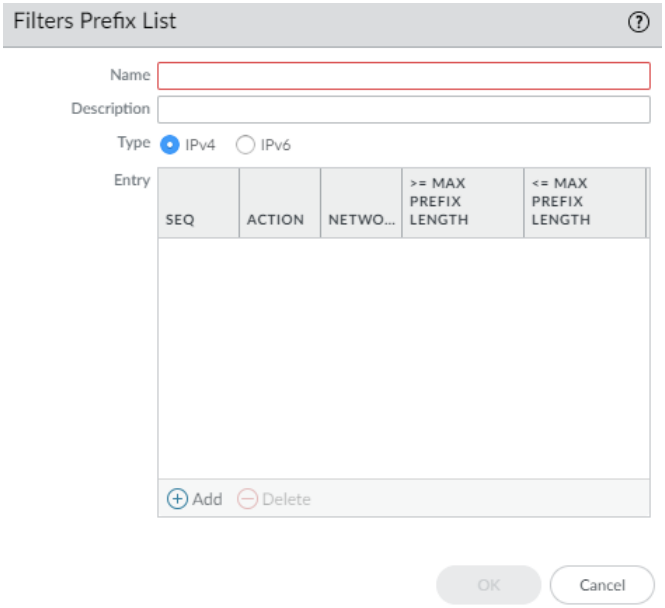
STEP 2 | Créez une liste de préfixes.

1. Sélectionnez **Network (Réseau)** > **Routing (Routage)** > **Routing Profiles (Profils de routage)** > **Filters (Filtres)**.
2. **Ajoutez** une **liste de préfixes de filtres** par **nom** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait

©2024 Palo Alto Networks, Inc.

d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.

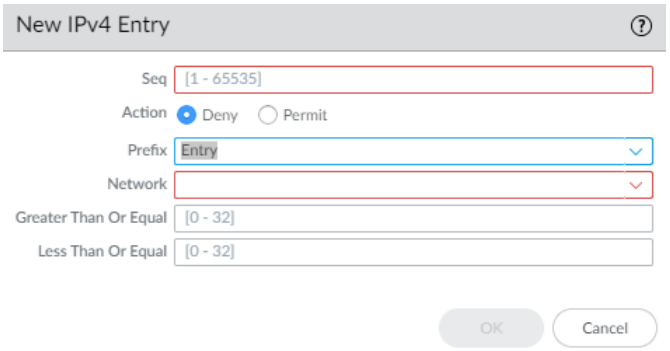
3. Saisissez une **Description** utile.
4. Sélectionnez le **Type** de préfixe de cette règle à filtrer : **IPv4** ou **IPv6**.



1. Pour IPv4, **ajoutez** une **entrée IPv4** et entrez le numéro **Seq** de la règle ; la plage est comprise entre 1 et 65 535.
2. Sélectionnez **Action**: **Refuser** (valeur par défaut) ou **Autoriser**.
3. Pour **Prefix**, il existe trois options ; la valeur par défaut est **None**. Une autre option consiste à sélectionner **Réseau n'importe lequel**. La troisième option consiste à sélectionner **Entrée** et à entrer un préfixe de **réseau** IPv4 avec une barre oblique et une longueur de préfixe de base qui, ensemble, spécifient un réseau, par exemple, 192.168.2.0/24. Vous pouvez éventuellement spécifier que la longueur du préfixe soit **supérieure ou égale** à un nombre (c'est-à-dire au moins aussi grand que la longueur de base que vous avez spécifiée ; la plage est comprise entre 0 et 32). Vous pouvez éventuellement spécifier une limite supérieure à la plage en spécifiant **Inférieur ou égal** à un nombre (c'est-à-dire au moins aussi élevé que la longueur de

©2024 Palo Alto Networks, Inc.

base et au moins aussi élevé que la **longueur supérieure ou égale** si configuré ; la plage est comprise entre 0 et 32).



La comparaison d'un itinéraire à la règle de préfixe (IPv4 ou IPv6) est un processus en deux étapes : 1) Faites d'abord correspondre le préfixe avec le réseau. 2) Faites correspondre la longueur du préfixe à la plage de masques (supérieure ou égale à inférieure ou égale). Par exemple, considérons la règle de liste preflix avec Réseau 192.168.3.0/24 et une longueur de préfixe supérieure ou égale à 26 et inférieure ou égale à 30. Le tableau suivant indique les itinéraires testés et s'ils réussissent ou échouent à la règle. Les itinéraires qui satisfont à la règle sont soumis à l'action configurée (Refuser ou Autoriser).

Exemple d'itinéraire	Résultat
192.168.3.0/28	Pass : la longueur du réseau et du préfixe correspond à la règle.
192.168.2.0/30	Échec : le réseau ne correspond pas à la règle.
192.168.3.0/32	Échec : la longueur du préfixe ne correspond pas à la règle.

Dans le résumé de sortie de la règle, LOU est Unité d'opérateur logique (égale, supérieure ou égale, inférieure ou égale). >= indique une longueur de préfixe supérieure ou égale à la valeur ; c'est la valeur la plus basse d'une plage de la longueur du préfixe. <= indique une longueur de préfixe inférieure ou égale à la valeur ; c'est la valeur la plus élevée d'une plage de la longueur du préfixe.

5. Vous pouvez également **ajouter** une **entrée IPv6** et suivre les étapes similaires à celles d'une règle de préfixe IPv4. La plage de longueur du préfixe IPv6 est **supérieure ou égale** à 0 à 128 et **inférieure ou égale** à 0 à 128.

   Par exemple, considérons la règle de liste de préfixes avec Network 2001:db8:1/48 et une longueur de préfixe supérieure ou égale à 56 et inférieure ou égale à 64. Le tableau suivant indique les itinéraires testés et s'ils réussissent ou échouent à la règle. Les itinéraires qui satisfont à la règle sont soumis à l'action configurée (Refuser ou Autoriser).

Exemple d'itinéraire	Résultat
2001:db8:1/64	Pass : la longueur du réseau et du préfixe correspond à la règle.

©2024 Palo Alto Networks, Inc.

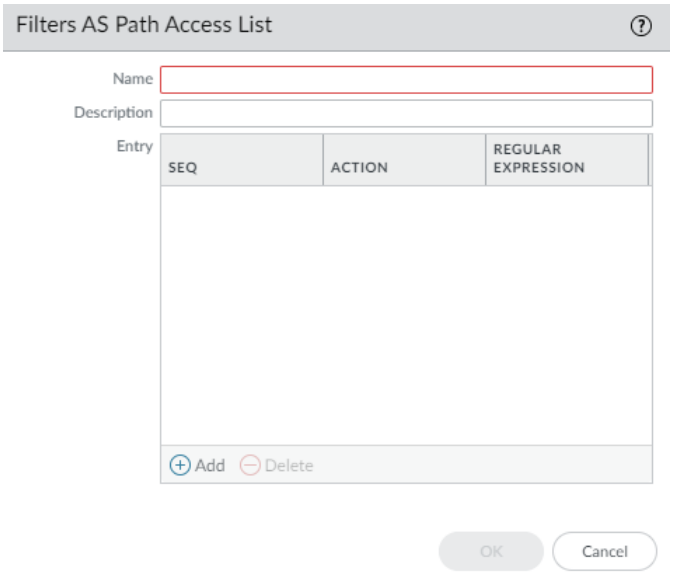
Exemple d'itinéraire	Résultat
2001:db8:2/48	Échec : le réseau ne correspond pas à la règle.
2001:db8:1/65	Échec : la longueur du préfixe ne correspond pas à la règle.

6. Cliquez sur **OK** pour enregistrer l'entrée de préfixe. Ajoutez éventuellement d'autres entrées.
7. Cliquez sur **OK** pour enregistrer la liste des préfixes.

STEP 3 | Créez une liste d'accès as pour BGP.

1. Sélectionnez **Network (Réseau)** > **Routing (Routage)** > **Routing Profiles (Profils de routage)** > **Filters (Filtres)**.
2. **Ajoutez** une **liste AS Path Acess** par **nom** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.
3. Saisissez une **Description** utile.
4. **Ajoutez** une **entrée** et entrez un numéro **Seq** ; la plage est comprise entre 1 et 65 535.
5. Sélectionnez **Action**: **Refuser** (valeur par défaut) ou **Autoriser**.

   *Chaque liste d'accès AS Path se termine par une règle implicite **Autoriser tout** . Utilisez une liste d'accès AS Path pour refuser les systèmes autonomes.*
6. Entrez Aspath **Regex** (expression régulière) au format **`regex1:regex2:regex3`**, où deux points (:) sépare trois valeurs AS. Les caractères autorisés sont 1234567890_^| [,{}()]$*+.? -\. Par exemple, .*65000 dans une instruction Deny exclut les préfixes provenant de AS 65000.

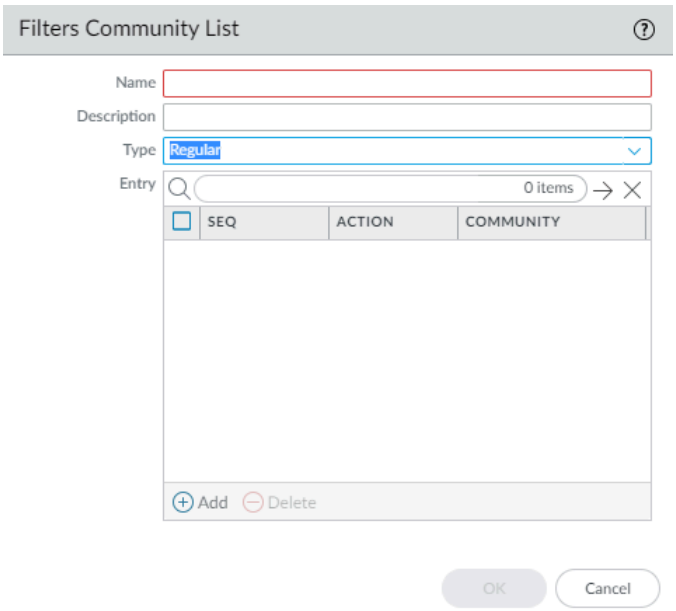


7. Cliquez sur **OK** pour enregistrer l'entrée. Ajoutez éventuellement d'autres entrées; un maximum de 64 entrées sont autorisées dans une liste d'accès AS Path.
8. Cliquez sur **OK** pour enregistrer la liste d'accès AS Path.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Créez une liste de communauté.

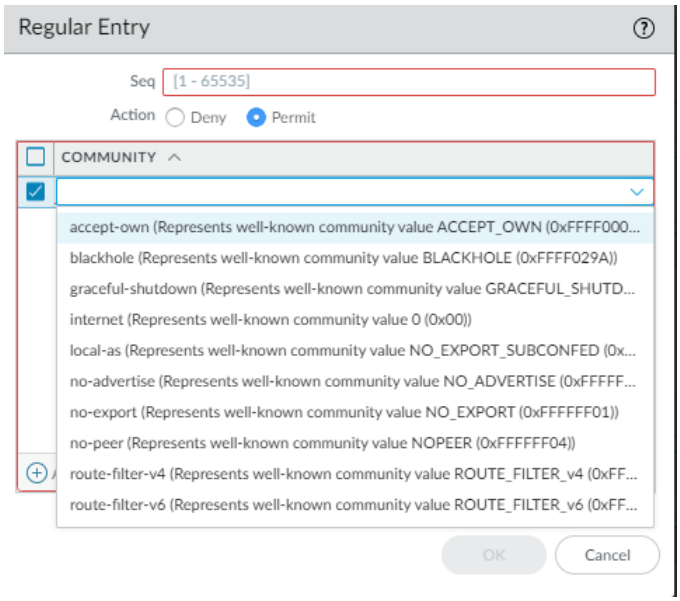
1. Sélectionnez **Network (Réseau)** > **Routing (Routage)** > **Routing Profiles (Profils de routage)** > **Filters (Filtres)**.
2. **Ajoutez** une **liste de communautés de filtres** par **nom** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.
3. Saisissez une **Description** utile.



4. Sélectionnez le **Type** :
   - **Régulier (Regular)** : **ajoutez** un nombre **Seq** (plage comprise entre 1 et 65 535), sélectionnez l'**action** : **Refuser** (valeur par défaut) ou **Autoriser**, et **Ajouter** une ou plusieurs valeurs de communauté, sélectionner une ou plusieurs communautés connues ou entrer une combinaison de valeurs de communauté et de communautés bien connues. Séparez plusieurs communautés avec une barre verticale (|), par exemple, **`6409:10|6520:13|internet`**. Entrez un maximum de 16 communautés dans une entrée **régulière** (règle).
     - Valeur communautaire régulière au format AA:NN où AA est un numéro AS et NN est un numéro de réseau (chacun avec une plage de 0 à 65 535).
     - **accept-own**—Représente la valeur communautaire bien connue ACCEPT-OWN (0xFFFF0001)
     - **blackhole**—Représente la valeur communautaire bien connue BLACKHOLE (0xFFFF029A). Le réseau voisin doit ignorer le trafic destiné au préfixe.
     - **graceful-shutdown**—Représente la valeur communautaire bien connue GRACEFUL_SHUTDOWN (0xFFFF0000)
     - **Internet**—Représente la valeur communautaire bien connue 0 (0x00). Annoncez un préfixe à tous les voisins BGP.

 ©2024 Palo Alto Networks, Inc.

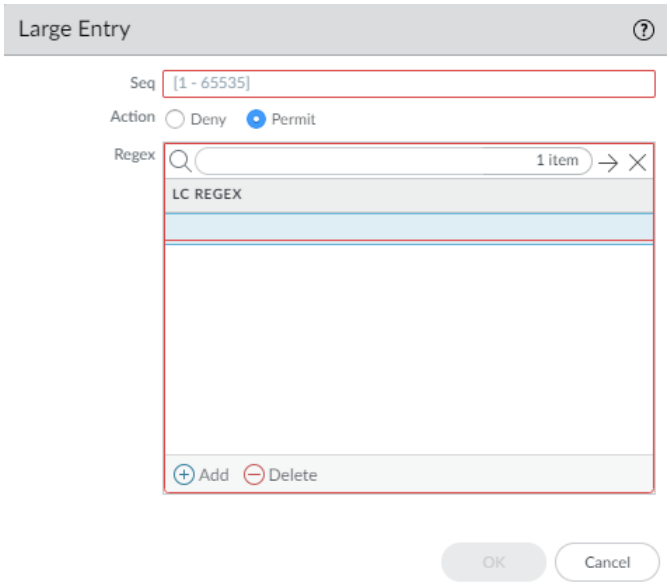
- **local-as**: représente des NO_EXPORT_SUBCONFED de valeur communautaires bien connues (0xFFFFFF03). L'effet est de ne pas annoncer le préfixe en dehors du sous-AS dans une confédération.
- **no-advertise :**représente des NO_ADVERTISE de valeur communautaires bien connues (0xFFFFFF02). L'ajout de cette communauté à un préfixe signifie que l'homologue BGP récepteur placera le préfixe dans sa table de routage BGP, mais ne publiera pas le préfixe auprès d'autres voisins.
- **no-export**: représente la valeur communautaire bien connue NO_EXPORT (0xFFFFFF01). L'ajout de cette communauté à un préfixe signifie que l'homologue BGP récepteur annoncera le préfixe uniquement aux voisins iBGP, et non aux voisins en dehors de l'AS.
- **no-peer**: représente la valeur communautaire bien connue NOPEER (0xFFFFFF04).
- **route-filter-v4**— Représente la valeur communautaire bien connue ROUTE_FILTER_v4 (0xFFFF0003).
- **route-filter-v6**— Représente la valeur communautaire bien connue ROUTE_FILTER_v6 (0xFFFF0005).



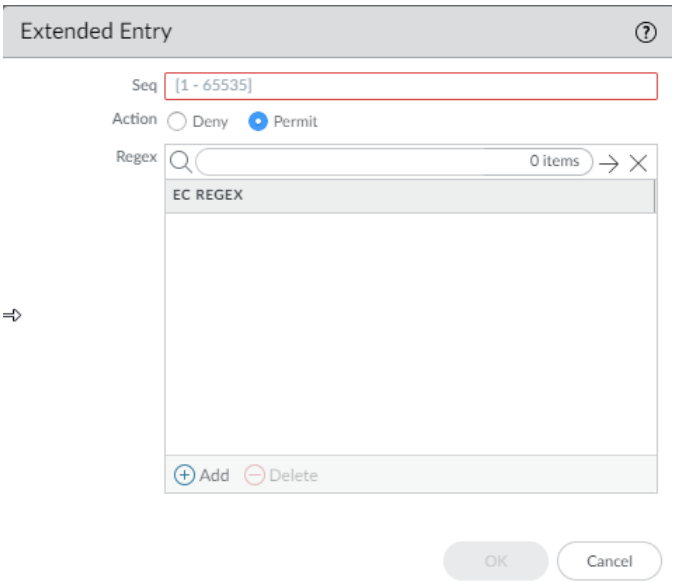
- **Grand (Large)** : **ajoutez** un nombre **Seq** (plage comprise entre 1 et 65 535), sélectionnez l'**action** : **Refuser** (valeur par défaut) ou **Autoriser**, et **Ajouter** une entrée d'expression régulière de grande communauté (LC REGEX). Les caractères autorisés dans une entrée sont 1234567890_^| [,{}()]$*+.? -\. Chaque communauté doit être au

 ©2024 Palo Alto Networks, Inc.

format **regex1:regex2:regex3**; par exemple, **203[1-2]:205[2-5]:206[5-6]**. Entrez un maximum de huit communautés dans une **entrée Large** (règle).



- **Étendu (Extended)** : **ajoutez** un numéro **Seq** (plage comprise entre 1 et 65 535), sélectionnez l'**action** : **Refuser** (valeur par défaut) ou **Autoriser**, et **Ajouter** l'expression régulière de communauté étendue BGP (EC REGEX). Les caractères autorisés sont 1234567890_^| [,{}()]$*+.? -\. Chaque communauté étendue doit être au format **regex1:regex2**; par exemple, **204*[3-8]:205*[4-8]**. Entrez un maximum de huit communautés dans une **entrée étendue** (règle).



5. Cliquez sur **OK** pour enregistrer l'entrée dans la liste des communautés. Vous pouvez éventuellement ajouter d'autres entrées du même type (Regular, Large ou Extended).
6. Cliquez sur **OK** pour enregistrer la liste des communautés.

 ©2024 Palo Alto Networks, Inc.

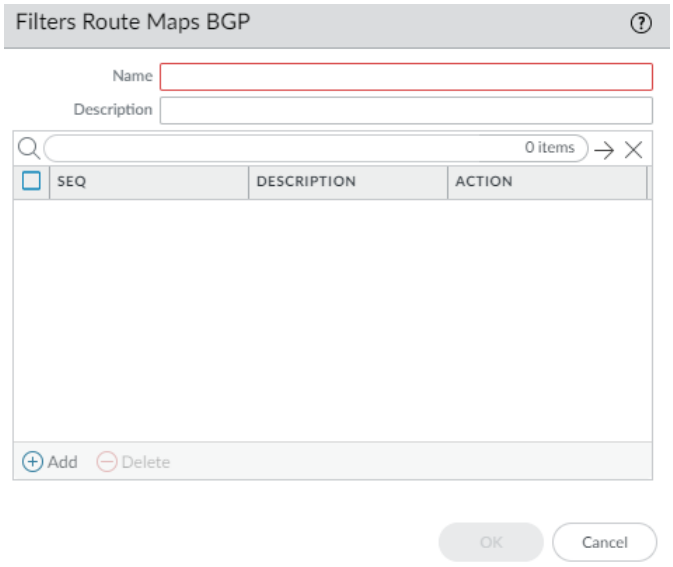
STEP 5 | Créez une carte d'itinéraire BGP.

1. Sélectionnez **Network (Réseau)** > **Routing (Routage)** > **Routing Profiles (Profils de routage)** > **Filters (Filtres)**.
2. **Ajoutez** une **carte d'itinéraires de filtres BGP** par **nom** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou

 ©2024 Palo Alto Networks, Inc.

un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.

3. Entrez une **Description** utile de la carte de l'itinéraire.

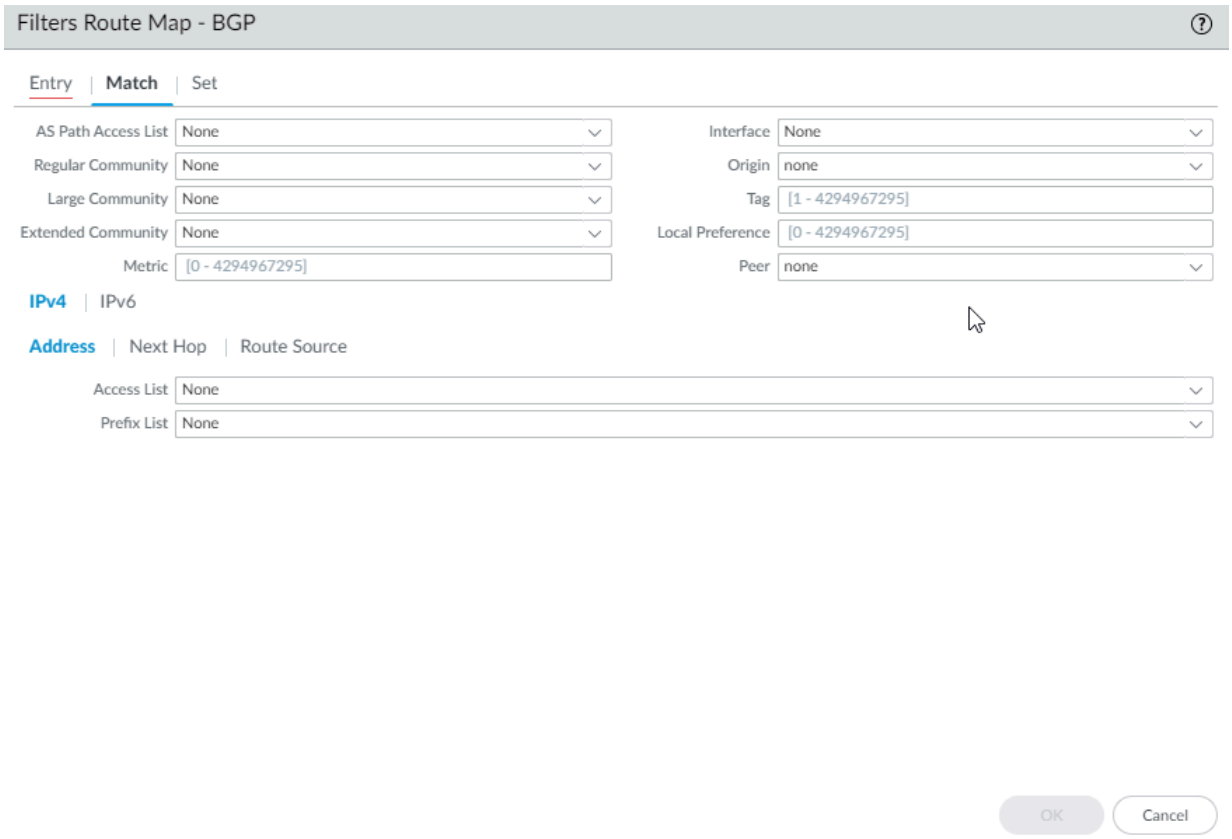


4. **Ajoutez** une carte d'itinéraire et, sous l'onglet **Entrée** attribuez un numéro **Seq** ; la plage est comprise entre 1 et 65 535.

   Attribuez des numéros de séquence séparés de cinq numéros ou plus afin d'avoir des numéros inutilisés pour lesquels insérer des entrées supplémentaires à l'avenir.

5. Entrez une **Description** utile de l'entrée (règle).
6. Pour **Action**, sélectionnez **Refuser** ou **Autoriser**.
7. Sous l'onglet **Correspondance** spécifiez les critères qui déterminent quels itinéraires sont soumis à la fonction qui utilise cette carte d'itinéraire. Plusieurs attributs sont logiquement ANDed, ce qui signifie que tous les critères doivent être remplis.

©2024 Palo Alto Networks, Inc.



- **Liste d'accès as (AS Path Access List)**: sélectionnez une liste de chemins AS. Valeur par défaut : **Aucune**.
- **Communauté régulière :**sélectionnez une liste de communautés. Valeur par défaut : **Aucune**.
- **Grande communauté (Large Community)** : sélectionnez une liste Grande communauté. Valeur par défaut : **Aucune**.
- **Communauté étendue (Extended Community)** : sélectionnez une liste Communauté étendue. Valeur par défaut : **Aucune**.
- **Métrique (Metric)** : entrez une valeur comprise entre 0 et 4 294 967 295.
- **Interface :**sélectionnez une interface locale dans la liste de toutes les interfaces de tous les routeurs logiques. Assurez-vous de choisir une interface qui appartient au routeur logique que vous configurez. Valeur par défaut : **Aucune**. Lors de la validation,

 ©2024 Palo Alto Networks, Inc.

le pare-feu vérifie que l'interface que vous avez choisie appartient au routeur logique que vous configurez.

- **Origine (Origin)** : sélectionnez l'origine de l'itinéraire : **ebgp**, **ibgp**, ou **incomplet**. Valeur par défaut : **Aucune**.
- **Balise (Tag)** : entrez une valeur de balise qui a une signification dans vos réseaux, comprise entre 0 et 4 294 967 295.
- **Préférence locale (Local Preference)** : entrez une valeur comprise entre 0 et 4 294 967 295.
- **Homologue (Peer)** : sélectionnez un nom d'homologue ou **local (routes statiques ou redistribuées).** Valeur par défaut : **Aucune**.

8. Sélectionnez **IPv4** ou **IPv6** pour faire correspondre différents types d'adresses. Si vous sélectionnez **IPv4**:
   - Sous l'onglet **Adresse** sélectionnez une **liste d'accès** pour spécifier les adresses à faire correspondre.
   - Sélectionnez une **liste de préfixes** pour spécifier les adresses à faire correspondre. Il correspond au préfixe reçu d'un homologue ou à un préfixe redistribué au protocole à partir d'un autre protocole.

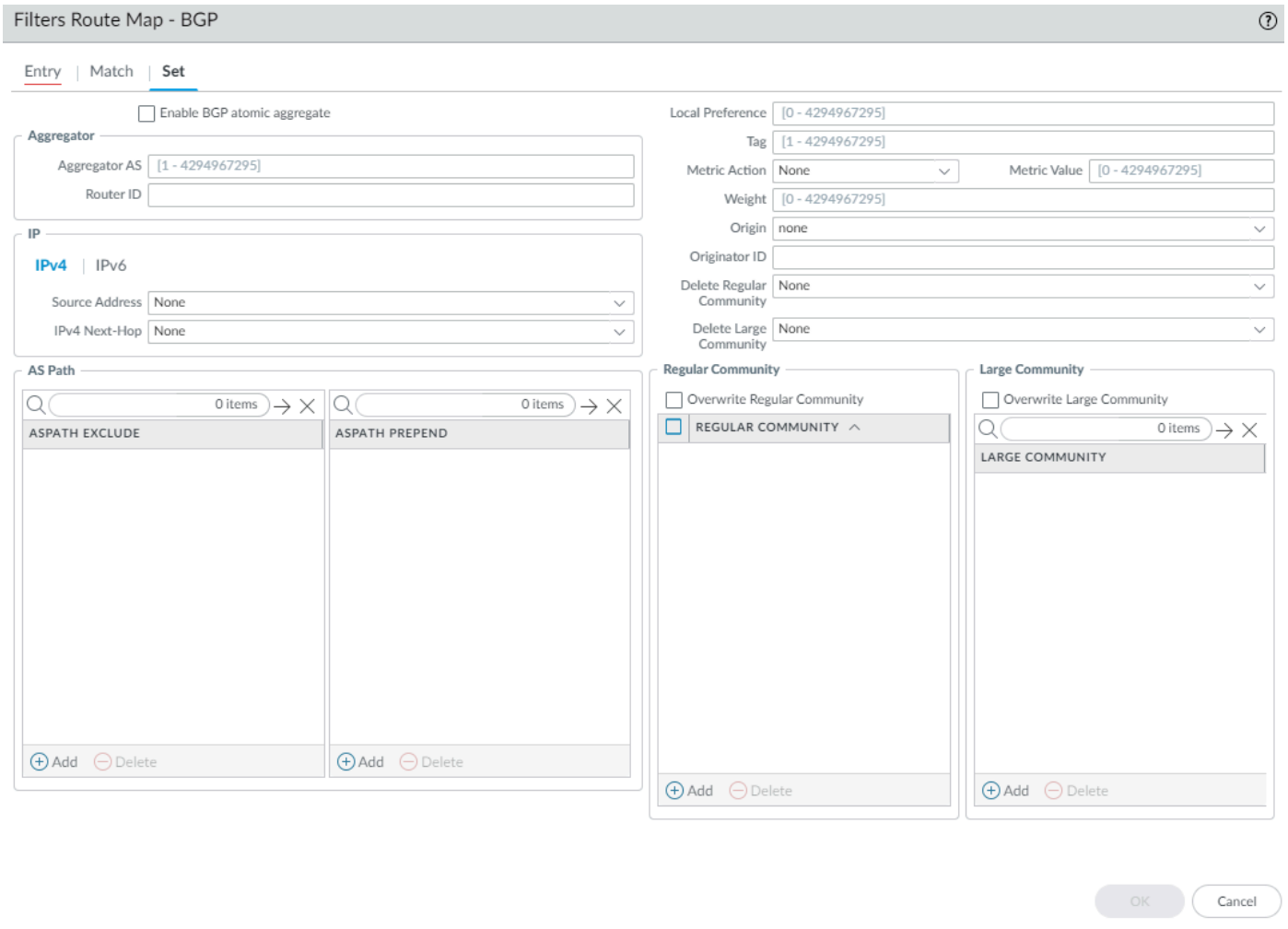
     Si une liste d'accès et une liste de préfixes sont spécifiées, les deux conditions doivent être remplies (LOGIQUE ET).
   - Sous l'onglet **Saut suivant**, sélectionnez une **liste d'accès** pour spécifier les adresses du tronçon suivant à faire correspondre.
   - Sélectionnez une **liste de préfixes** pour spécifier les adresses du saut suivant à faire correspondre.
   - Sous l'onglet **Source d'itinéraire** sélectionnez une **liste d'accès** pour spécifier l'adresse IP source d'un itinéraire à faire correspondre. Par exemple, la liste d'accès peut autoriser un homologue distant avec l'adresse 192.168.2.2 qui annonce un itinéraire vers un certain préfixe. Vous pouvez faire correspondre cette carte d'itinéraire BGP à l'adresse source de l'itinéraire 192.168.2.2, puis peut-être filtrer l'itinéraire en fonction de la correspondance de l'adresse homologue 192.168.2.2 comme source

 ©2024 Palo Alto Networks, Inc.

de l'itinéraire, ou définir un tronçon suivant pour les itinéraires correspondant à cette source d'itinéraire.

- Spécifiez une **liste de préfixes** pour spécifier un ou plusieurs préfixes de réseau source à faire correspondre.

9. Si vous sélectionnez **IPv6**:
   - Sous l'onglet **Adresse** sélectionnez une **liste d'accès** pour spécifier les adresses à faire correspondre.
   - Sélectionnez une **liste de préfixes** pour spécifier les adresses à faire correspondre.
   - Sous l'onglet **Saut suivant**, sélectionnez une **liste d'accès** pour spécifier les adresses du tronçon suivant à faire correspondre.
10. **Définissez** l'un des attributs suivants pour les itinéraires qui répondent aux critères de correspondance :



- **Activer l'agrégat atomique BGP** : marquez l'itinéraire comme un itinéraire moins spécifique car il a été agrégé. ATOMIC_AGGREGATE est un attribut discrétionnaire bien connu qui avertit les locuteurs BGP le long d'un chemin que des informations ont été perdues en raison de l'agrégation d'itinéraires, et par conséquent, le chemin agrégé peut ne pas être le meilleur chemin vers la destination. Lorsque certains routeurs sont agrégés par un agrégateur, l'agrégateur attache son ID de routeur

©2024 Palo Alto Networks, Inc.

à l'itinéraire agrégé dans l'attribut AGGREGATOR-ID et définit ou non l'attribut ATOMIC_AGGREGATE, selon que les informations AS_PATH des routeurs agrégés ont été préservées.

- **Agrégateur AS (Aggregator AS)** : entrez l'agrégateur AS. L'attribut Aggregator inclut le numéro AS et l'adresse IP du routeur à l'origine de l'itinéraire agrégé. L'adresse IP est l'ID de routeur du routeur qui effectue l'agrégation d'itinéraires.
- **ID du routeur** : entrez l'ID du routeur de l'agrégateur (généralement une adresse de bouclage).
- **Préférence locale (Local Preference)** : entrez la préférence locale à laquelle les itinéraires correspondants sont définis ; la plage est comprise entre 0 et 4 294 967 295. Les paquets de mise à jour IBGP ont une préférence locale, qui est annoncée aux pairs IBGP uniquement. Lorsqu'il existe plusieurs itinéraires vers un autre AS, le pare-feu préfère la préférence locale la plus élevée.
- **Balise (Tag)** : définit une balise ; la plage est comprise entre 1 et 4 294 967 295.
- **Action de mesure (Metric Action)** : sélectionnez une action : **définir**, **ajouter**, ou **soustraire**. Vous pouvez définir la valeur de mesure spécifiée, ou ajouter la valeur de mesure spécifiée à la valeur de mesure d'origine de l'itinéraire correspondant, ou soustraire la valeur de mesure spécifiée de la valeur de mesure d'origine de l'itinéraire correspondant ; la valeur par défaut est définie. Sélectionnez l'action d'ajout ou de soustraction pour ajuster une métrique et ainsi hiérarchiser ou déprioriser l'itinéraire correspondant.
- **Valeur de la métrique (Metric Value)** : entrez la valeur de la métrique pour définir les itinéraires correspondants, ajouter ou soustraire de la valeur métrique d'origine ; la plage est comprise entre 0 et 4 294 967 295.
- **Poids (Weight)** : définit un poids (appliqué localement ; non multiplié) ; la plage est comprise entre 0 et 4 294 967 295.
- **Origine (Origin)** : définit l'origine des itinéraires correspondants : **ebgp**, **ibgp**, ou **incomplet** (on ne sait pas comment l'itinéraire a été ajouté au RIB).
- **ID d'origine**: définissez l'adresse IP de l'expéditeur des itinéraires correspondants.
- **Supprimer la communauté régulière (Delete Regular Community)** : sélectionnez une communauté régulière à supprimer. Valeur par défaut : **Aucune**.
- **Supprimer une grande communauté (Delete Large Community)** : sélectionnez une grande communauté à supprimer. Valeur par défaut : **Aucune**.
- Sélectionnez **IPv4** ou **IPv6** comme AFI.
- Sous l'onglet **IPv4** sélectionnez une **adresse** source à définir dans la liste de toutes les adresses sources de tous les routeurs logiques ou sélectionnez **Aucune**. Lors de la validation, le pare-feu vérifie que l'adresse source que vous avez choisie appartient au routeur logique que vous configurez.
- Sélectionnez un **saut suivant IPv4** à définir : **aucun**, **adresse homologue (utiliser l'adresse homologue)**, ou **inchangé**.
- Sous l'onglet **IPv6** sélectionnez **IPv6 Nexthop Prefer Global Address** pour préférer l'adresse de monodiffusion globale aux autres types d'adresses IPv6 (adresse locale de lien, adresse anycast ou adresse de multidiffusion) pour le tronçon suivant. (Par

 ©2024 Palo Alto Networks, Inc.

défaut, les homologues connectés préfèrent une adresse de tronçon suivant locale à une adresse de tronçon suivant globale.)

- Sous l'onglet **IPv6** sélectionnez une **adresse source** à définir dans la liste de toutes les adresses sources de tous les routeurs logiques ou sélectionnez **Aucune**. Lors de la validation, le pare-feu vérifie que l'adresse source que vous avez choisie appartient au routeur logique que vous configurez.
- Sélectionnez un **saut suivant IPv6 à définir** : **aucun** ou **adresse d'homologue (utiliser l'adresse d'homologue).**
- Dans la fenêtre Chemin AS, **Ajoutez** jusqu'à quatre chemins AS à **Exclure** du chemin AS des itinéraires correspondants, peut-être pour supprimer un AS d'une confédération.
- **Ajoutez** jusqu'à quatre chemins AS à **ajouter** au chemin AS de l'itinéraire correspondant (pour rendre l'itinéraire dans une publicité moins souhaitable).
- Dans la fenêtre Communauté régulière, sélectionnez **Remplacer la communauté régulière** pour remplacer la communauté régulière.
- **Ajoutez** une **communauté régulière** pour ajouter une ou plusieurs communautés régulières.
- Dans la fenêtre Grande communauté, sélectionnez **Remplacer une grande communauté** pour remplacer la grande communauté.
- **Ajoutez** une **grande communauté** pour ajouter une ou plusieurs grandes communautés.
- Dans la fenêtre Communauté régulière, sélectionnez **Remplacer la communauté régulière** pour remplacer la communauté régulière.
- **Ajoutez** une **communauté régulière** pour ajouter une ou plusieurs communautés régulières.
- Dans la fenêtre Grande communauté, sélectionnez **Remplacer une grande communauté** pour remplacer la grande communauté.
- **Ajoutez** une **grande communauté** pour ajouter une ou plusieurs grandes communautés.

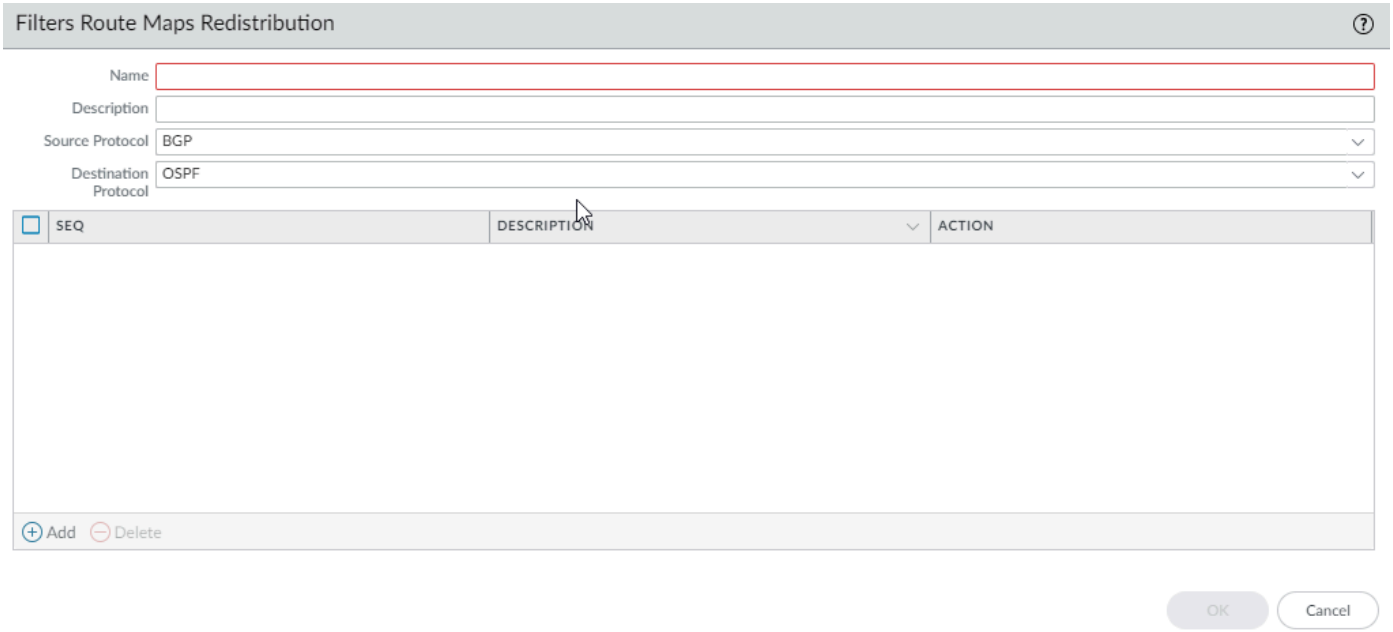
11. Cliquez sur **OK** pour enregistrer l'entrée de la carte d'itinéraires. Ajoutez éventuellement d'autres entrées.
12. Cliquez sur **OK** pour enregistrer la carte d'itinéraire BGP.

STEP 6 | Créez une carte d'itinéraire de redistribution.

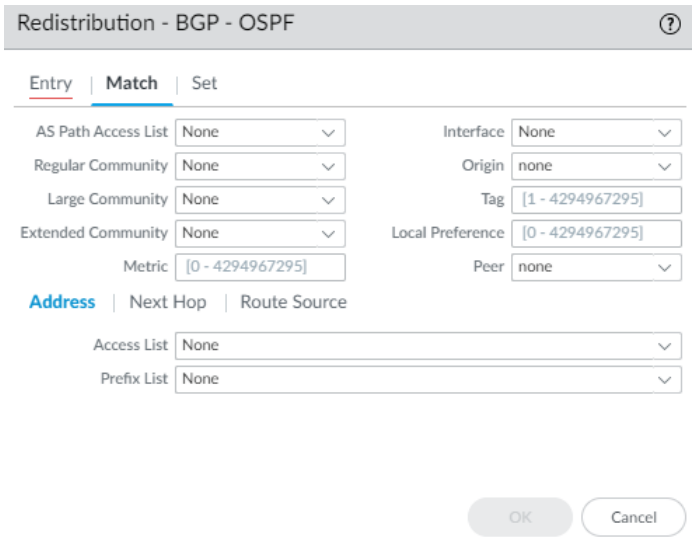
1. Sélectionnez **Network (Réseau)** > **Routing (Routage)** > **Routing Profiles (Profils de routage)** > **Filters (Filtres)**.
2. **Ajoutez** une **redistribution des cartes d'itinéraires de filtres** par **nom** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.
3. Saisissez une **Description** utile.

 ©2024 Palo Alto Networks, Inc.

4. Pour redistribuer à partir d'un **protocole**, source, sélectionnez **BGP**, **OSPF**, **OSPFv3**, **RIP**, ou **Statique connecté**. Le protocole source est l'endroit où les sélections Match s'appliquent.
5. Pour redistribuer les itinéraires vers un **protocole de destination** ou un RIB local, sélectionnez **BGP**, **OSPF**, **OSPFv3**, **RIP**, ou **Rib**. Le protocole de destination est l'endroit où les sélections Set s'appliquent. Les protocoles de destination disponibles dans la liste déroulante dépendent du protocole source sélectionné. (Cette étape montre un exemple de BGP redistribué à OSPF.)

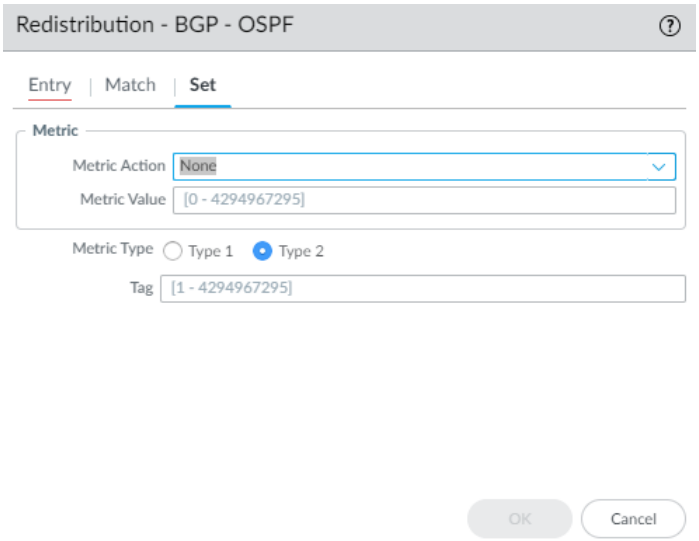


6. **Ajoutez** une **entrée** et entrez le numéro **Seq** (plage comprise entre 1 et 65 535).
7. Saisissez une **Description** utile.
8. Sélectionnez **Action**: **Refuser** ou **permettre**.
9. Sélectionnez l'onglet **Correspondance** pour configurer les critères du protocole source ; cet exemple spécifie les attributs BGP à faire correspondre.



 ©2024 Palo Alto Networks, Inc.

10. Sélectionnez une **liste d'accès au chemin AS** ; la valeur par défaut est **Aucun**.
11. Sélectionnez une **communauté régulière**; la valeur par défaut est **Aucune**.
12. Sélectionnez une **grande communauté**; la valeur par défaut est **Aucune**.
13. Sélectionnez une **communauté étendue**; la valeur par défaut est **Aucune**.
14. Entrez une **métrique**; la plage est comprise entre 0 et 4 294 967 295.
15. Sélectionnez une **interface**; la valeur par défaut est **Aucune**.
16. Sélectionnez l'**origine** de l'itinéraire : **ebgp**, **ibgp**, ou **incomplet**; la valeur par défaut est **aucune**.
17. Entrez une **balise** ; la plage est comprise entre 1 et 4 294 967 295.
18. Entrez une **préférence locale** ; la plage est comprise entre 0 et 4 294 967 295.
19. Sélectionnez un nom d'**homologue** ou **local (itinéraires statiques ou redistribués)**; la valeur par défaut est **aucun**.
20. L'onglet **Adresse** fait référence à l'adresse de destination d'un itinéraire. Sélectionnez une **liste d'accès** pour spécifier les itinéraires dont l'adresse de destination doit correspondre pour être redistribués. Valeur par défaut : **Aucune**.
21. Sélectionnez une **liste de préfixes** pour spécifier les itinéraires dont l'adresse de destination doit correspondre pour être redistribués. Valeur par défaut : **Aucune**.
22. Sélectionnez l'onglet **Définir** pour configurer les actions à effectuer sur les itinéraires correspondant à cette règle, qui seront redistribués au protocole de destination. (Dans cet exemple, le protocole de destination est OSPF.)



23. Sélectionnez l'**action de mesure** pour la règle de redistribution : vous pouvez **définir** la valeur de la mesure, **ajouter** la **valeur de mesure** spécifiée à la valeur de mesure d'origine de l'itinéraire correspondant ou **soustraire** la **valeur de mesure** spécifiée de la valeur de mesure d'origine de l'itinéraire correspondant ; la valeur par défaut est **Aucun**. Sélectionnez l'action d'**ajout** ou de **soustraction** pour ajuster une métrique et ainsi hiérarchiser ou déprioriser l'itinéraire correspondant.

    Par exemple, vous pouvez placer la métrique d'un IGP dans BGP à l'aide de la redistribution. La métrique est dynamique et vous pouvez simplement ajouter à sa valeur plutôt que de la définir sur un nombre absolu.

 ©2024 Palo Alto Networks, Inc.

24. Entrez une **valeur de mesure** à définir, ajouter ou soustraire de la mesure ; la plage est comprise entre 0 et 4 294 967 295.
25. Sélectionnez le **type de mesure** : **Type 1** ou **Type 2** (car cet exemple utilise OSPF comme protocole de destination).
26. Spécifiez une **balise** ; la plage est comprise entre 1 et 4 294 967 295.
27. Cliquez sur **OK** pour enregistrer la règle. Ajoutez éventuellement d'autres règles.
28. Cliquez sur **OK** pour enregistrer la carte d'itinéraire de redistribution.

 ©2024 Palo Alto Networks, Inc.

Configurer OSPFv2 sur un moteur de routage avancé

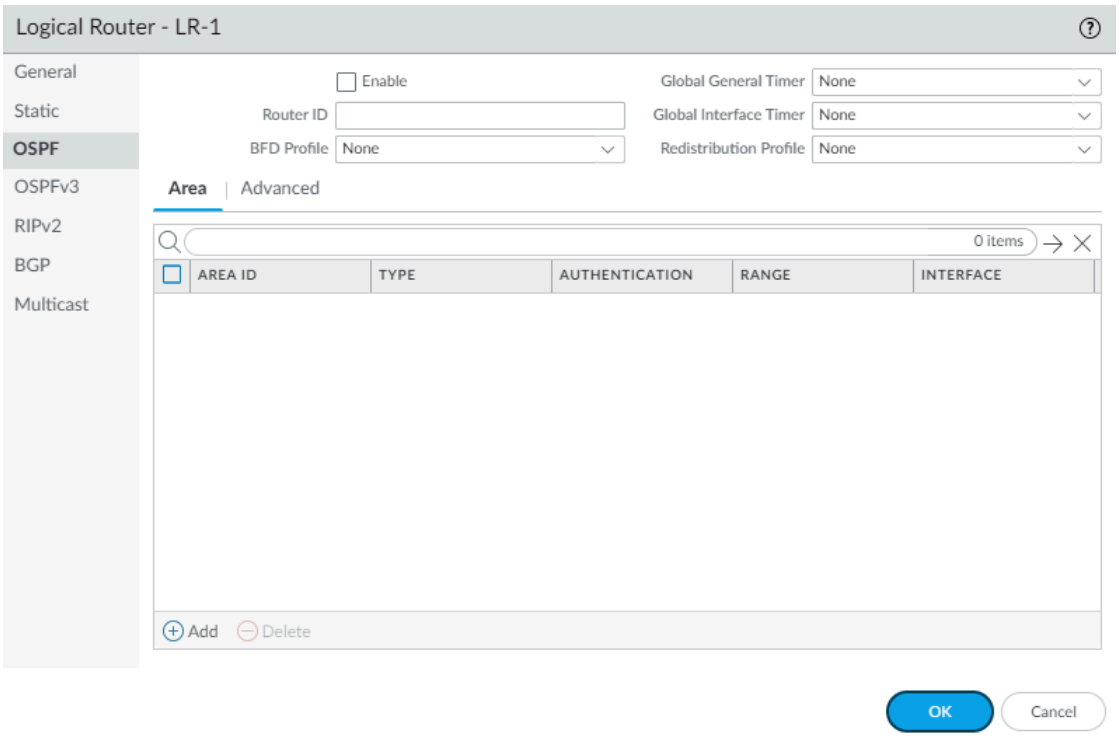
Le moteur de routage avancé prend en charge OSPFv2, qui ne prend en charge que l'adressage IPv4. Avant de configurer OSPFv2, vous devez comprendre Concepts d'OSPF.

Considérez les profils de routage OSPF et les filtres que vous pouvez appliquer à OSPF et ainsi gagner du temps de configuration et maintenir la cohérence. Vous pouvez créer des profils et des filtres à l'avance ou lors de la configuration d'OSPFv2.

STEP 1 | Configurer un routeur logique.

STEP 2 | Activez OSPFv2 et configurez les paramètres généraux.

1. Sélectionnez **Routeurs logiques** > **routage** > **réseau** et sélectionnez un routeur logique.
2. Sélectionnez **OSPF** et **activez** -le.



3. Saisissez l' **ID du routeur** au format d'une adresse IPv4.
4. Si vous souhaitez appliquer BFD à OSPF, sélectionnez un **profil BFD** que vous avez créé, ou sélectionnez le profil **par défaut** , ou créez un nouveau profil BFD. Par défaut **None (disable BFD) (Aucun - BFD désactivé)**.
5. Sélectionnez un profil OSPF **Global General Timer** ou créez-en un nouveau.
6. Sélectionnez un profil **de temporisateur d'interface globale** OSPF ou créez-en un nouveau.
7. Sélectionnez un **profil de redistribution** OSPF ou créez-en un nouveau pour redistribuer les routes statiques IPv4, les routes connectées, les routes RIPv2, les routes BGP IPv4 ou la route par défaut IPv4 vers OSPF.

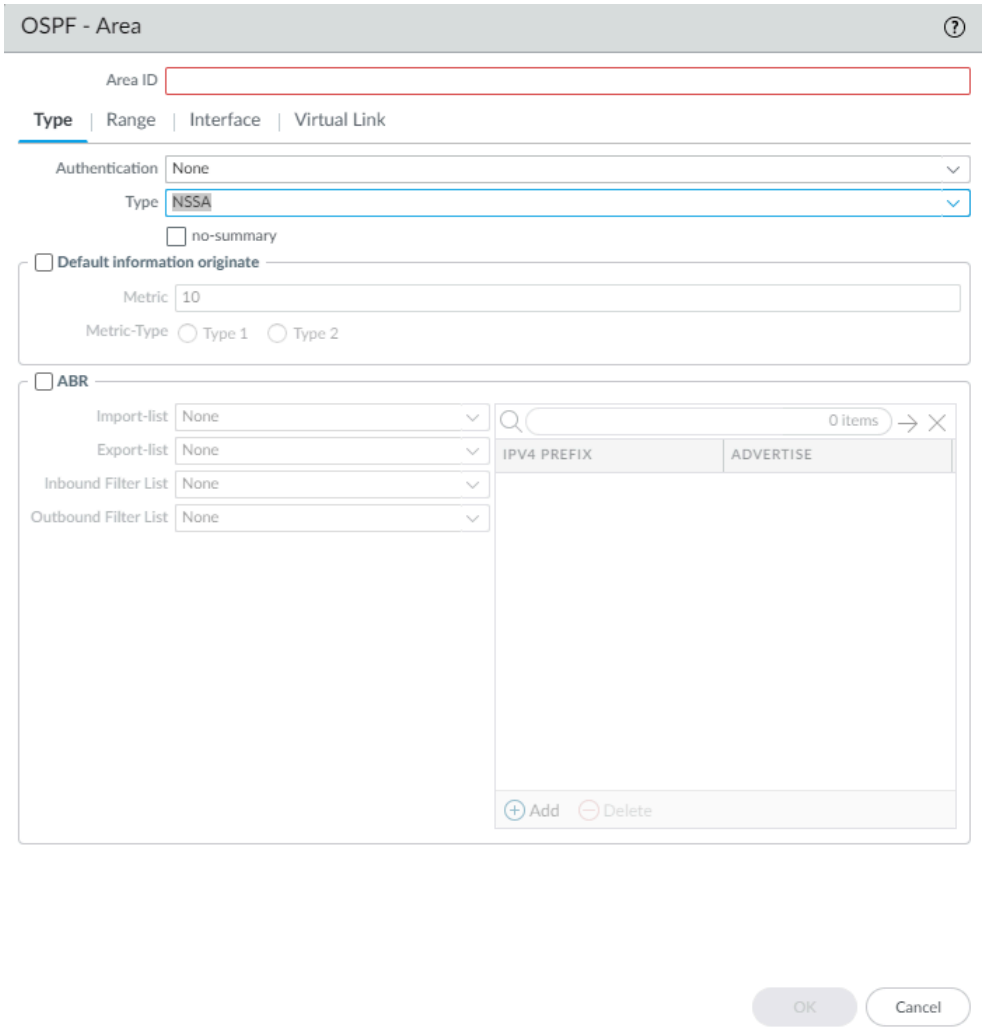
 ©2024 Palo Alto Networks, Inc.

STEP 3 | Créez une zone OSPF et spécifiez les caractéristiques en fonction du type de zone.

1. Sélectionnez **Zone** et **ajoutez** une zone identifiée par son **ID de zone** au format xxxx. Il s'agit de l'identifiant devant faire partie de la même zone et que chaque voisin doit accepter.
2. Sélectionnez l'onglet **Type** et pour **Authentification**, sélectionnez un profil d'authentification ou créez un nouveau profil d'authentification.
3. Sélectionnez le **Type** d'adresse :
   - **Normal**— Il n'y a aucune restriction ; la zone peut porter tous les types de routes (routes intra-zone, routes inter-zone et routes externes).
   - **Stub (Terminale)** : il n'existe aucune sortie issue de la zone. Pour atteindre une destination en dehors de la zone, le trafic doit passer par un routeur frontalier de zone (ABR), qui se connecte à d'autres zones.
   - **NSSA** (Not-So-Stubby-Area) - Les NSSA implémentent une fonctionnalité de stub ou totalement stubby, mais contiennent un routeur de frontière de système autonome (ASBR). Les LSA de type 7 générés par l'ASBR sont convertis en type 5 par les ABR et diffusés dans le reste du domaine OSPF. (Le graphique suivant montre NSSA sélectionné.)
4. (Zones stub et NSSA uniquement) Sélectionnez **no-summary** pour empêcher la zone de recevoir des LSA récapitulatifs de type 3 et ainsi réduire le trafic dans la zone.
5. (Zone NSSA uniquement) Sélectionnez **l'origine des informations par défaut** pour que l'OSPF crée une route par défaut.
   - Saisissez une **mesure** pour la route par défaut ; la plage est de 1 à 16 777 214 ; la valeur par défaut est 10.
   - Sélectionnez le **type de mesure** : **Type 1** ou **Type 2**. Le coût de type E1 est la somme du coût externe plus le coût interne pour atteindre cet itinéraire. Le type E2 n'est que

 ©2024 Palo Alto Networks, Inc.

le coût externe de cet itinéraire. Cela peut être utile lorsque vous souhaitez équilibrer la charge de la même route externe, par exemple.



6. Sélectionnez **ABR** pour filtrer les préfixes entrant ou sortant de la zone, puis configurez les filtres suivants :
   - Sélectionnez une **liste d'importation** ou créez une nouvelle liste d'accès pour filtrer les routes réseau provenant d'un autre routeur dans la zone des LSA, en fonction de l'adresse source IPv4, permettant ou empêchant ainsi l'ajout des routes au RIB global (laissez l'adresse de destination de la liste d'accès vide).
   - Sélectionnez une **liste d'exportation** ou créez une nouvelle liste d'accès pour filtrer les routes réseau qui proviennent de la zone, pour autoriser ou empêcher la publicité des routes vers d'autres zones.
   - Sélectionnez une **liste de filtres entrants** ou créez une nouvelle liste de préfixes pour filtrer les préfixes réseau entrant dans la zone.
   - Sélectionnez une **liste de filtres sortants** ou créez une nouvelle liste de préfixes pour filtrer les préfixes réseau provenant de la zone, afin d'empêcher que les routes ne soient annoncées vers d'autres zones.

©2024 Palo Alto Networks, Inc.

- Si le **type** de zone est **NSSA** et **ABR** est sélectionné, **ajoutez** un **préfixe IPv4** pour résumer un groupe de sous-réseaux externes en un seul LSA de type 7, qui est ensuite traduit en un LSA de type 5 et annoncé à la dorsale lorsque vous sélectionnez **Annoncer**.

STEP 4 | Spécifiez la plage de réseau pour la zone.

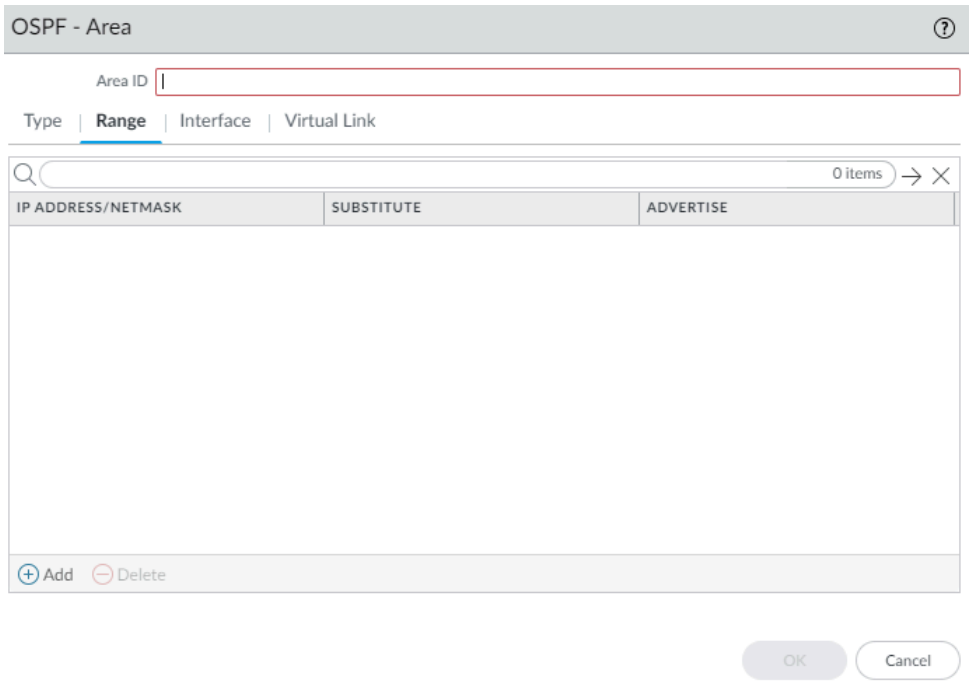
1. Sélectionnez **Plage** et **Ajouter** une **adresse IP/masque de réseau** , qui résume les routes pour la zone. Le résultat est qu'un LSA récapitulatif de type 3 avec des informations de routage correspondant à cette plage est annoncé dans la zone dorsale si cette zone contient au moins un réseau intra-zone (c'est-à-dire décrit avec un routeur ou un réseau LSA) de cette plage.

   Examinez les routes apprises dans la LSDB pour la zone et utilisez cette plage pour résumer les routes, réduisant ainsi le trafic LSA.

2. Entrez une adresse IP/un masque de réseau de **substitution** afin qu'un LSA récapitulatif de type 3 avec cette adresse IP/ce masque de réseau soit annoncé dans la zone de réseau fédérateur si la zone contient au moins un réseau intra-zone à partir de l' **adresse IP/du masque de réseau** spécifié à l'étape précédente.

   Utilisez l'adresse IP/masque de réseau de substitution pour traduire une adresse privée en adresse publique. Une adresse de substitution n'a aucun effet si la publicité est désactivée.

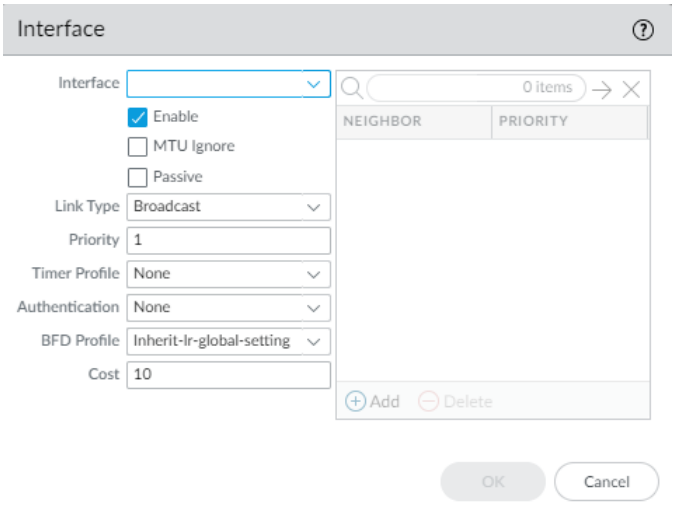
3. Sélectionnez **Publier** pour envoyer des annonces d'état de liens (LSA) qui correspondent au sous-réseau ; par défaut est activé.



 ©2024 Palo Alto Networks, Inc.

STEP 5 | Configurez chaque interface à inclure dans la zone.

1. **Ajoutez** une **interface** en en sélectionnant une et en l' **activant** .
2. Sélectionnez **MTU Ignorer** pour ignorer les incompatibilités d'unité de transmission maximale (MTU) lors de la tentative d'établissement d'une contiguïté (la valeur par défaut est désactivée ; la vérification de correspondance MTU se produit). RFC 2328 définit le MTU de l'interface comme "La taille en octets du plus grand datagramme IP qui peut être envoyé à l'interface associée, sans fragmentation".
3. Sélectionnez **Passif** pour permettre au réseau de l'interface d'être annoncé, mais aucune relation de voisinage n'est établie sur cette interface ; ceci est utile pour les interfaces feuille.



4. Sélectionnez le **type de lien** :
   - **Broadcast (Diffusion)** : tous les voisins accessibles via l'interface soient détectés automatiquement en multidiffusant des messages Hello OSPF, comme par une interface Ethernet.
   - **p2p** (point à point) : découvre automatiquement le voisin.
   - **p2mp** (point-to-multipoint/point-multipoint) : les voisins doivent être définis manuellement. **Ajoutez** l'adresse IP du **voisin** pour tous les voisins qui sont accessibles via cette interface et la **priorité** de chaque voisin à élire le routeur désigné (DR) ou le DR de sauvegarde ; la plage est de 0 à 255 ; la valeur par défaut est 1.
5. Entrez la **priorité** OSPF pour que l'interface soit élue en tant que routeur désigné (DR) ou DR de secours (BDR) ; la plage est de 0 à 255 ; la valeur par défaut est 1. Lorsque la valeur 0 est configurée, le routeur ne sera pas élu en tant que DR ou BDR.
6. Sélectionnez un **profil de minuterie** à appliquer à l'interface ou créez un nouveau profil de minuterie d'interface OSPF. Ce profil de temporisateur d'interface OSPF remplace le temporisateur d'interface global appliqué à OSPF.
7. Sélectionnez un **profil d'authentification** à appliquer à l'interface ou créez un nouveau profil d'authentification d'interface OSPF. Ce profil d'authentification remplace le profil d'authentification appliqué à la zone (sur l'onglet Type).
8. Par défaut, l'interface héritera du profil BFD que vous avez appliqué au routeur logique pour OSPF (**Inherit-lr-global-setting**). Vous pouvez également sélectionner le profil **par**

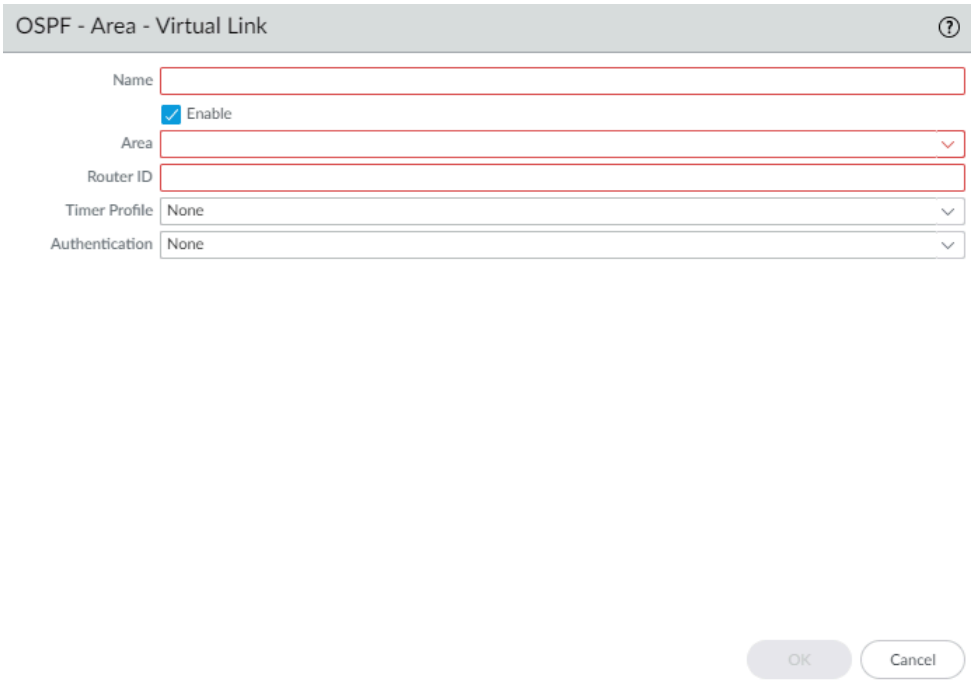
 ©2024 Palo Alto Networks, Inc.

défaut , sélectionner un **profil BFD**différent, créer un nouveau profil BFDou sélectionner **Aucun (Désactiver BFD)** pour désactiver BFD pour l'interface.

9. Entrez un **coût** OSPF pour l'interface, qui influence la sélection de route ; la plage est de 1 à 65,5535 ; la valeur par défaut est 10. Lors de la sélection de l'itinéraire, un itinéraire avec un coût cumulé inférieur (les coûts supplémentaires de chaque interface utilisée) est préféré à un itinéraire avec un coût cumulé plus élevé.
10. Cliquez sur **OK**.

STEP 6 | Si l'ABR n'a pas de lien physique avec la zone dorsale, configurez une liaison virtuelle vers un ABR voisin dans la même zone qui a un lien physique avec la zone dorsale.

1. Sélectionnez **Virtual Link (lien virtuel)**.
2. **Ajouter** un lien virtuel par **Nom**.
3. **Activez** le lien virtuel.



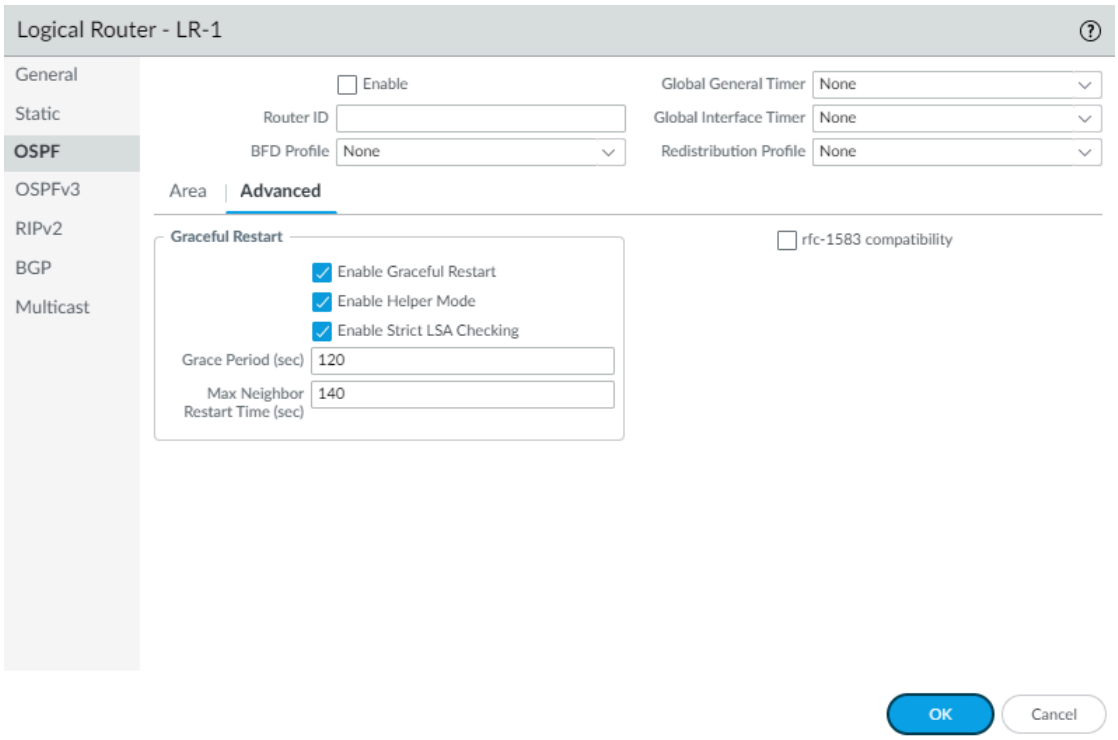
4. Sélectionnez la **zone** de transit où se trouve l'ABR voisin qui a le lien physique avec la zone dorsale.
5. Entrez l'**ID de routeur** de l'ABR voisin à l'extrémité distante de la liaison virtuelle.
6. Sélectionnez un **profil de minuterie** ou créez un nouveau profil de minuterie à appliquer au lien virtuel. Ce profil de minuterie d'interface OSPF remplace le temporisateur d'interface global appliqué à OSPF et le profil de temporisateur d'interface OSPF appliqué à l'interface.
7. Sélectionnez un **profil d'authentification** ou créez un nouveau profil d'authentification à appliquer au lien virtuel. Ce profil d'authentification remplace le profil d'authentification appliqué à la zone (sur l'onglet Type) et le profil d'authentification appliqué à l'interface.
8. Cliquez sur **OK**.

STEP 7 | Cliquez sur **OK** pour enregistrer la zone.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | Configurez le redémarrage progressif OSPF et la compatibilité RFC 1583 pour OSPFv2.

1. Sélectionnez **Réseau** > **Routage** > **Routeurs logiques** et sélectionnez le routeur logique.
2. Sélectionnez **OSPF** > **avancé**.
3. Sélectionnez **compatibilité rfc-1583** pour appliquer la compatibilité avec la RFC 1583, qui autorise un meilleur itinéraire vers un routeur de frontière de système autonome (ASBR) dans la table de routage OSPF. La valeur par défaut est désactivée, ce qui signifie que la table de routage OSPF peut conserver plusieurs chemins intra-AS dans la table de routage, empêchant ainsi les boucles de routage.



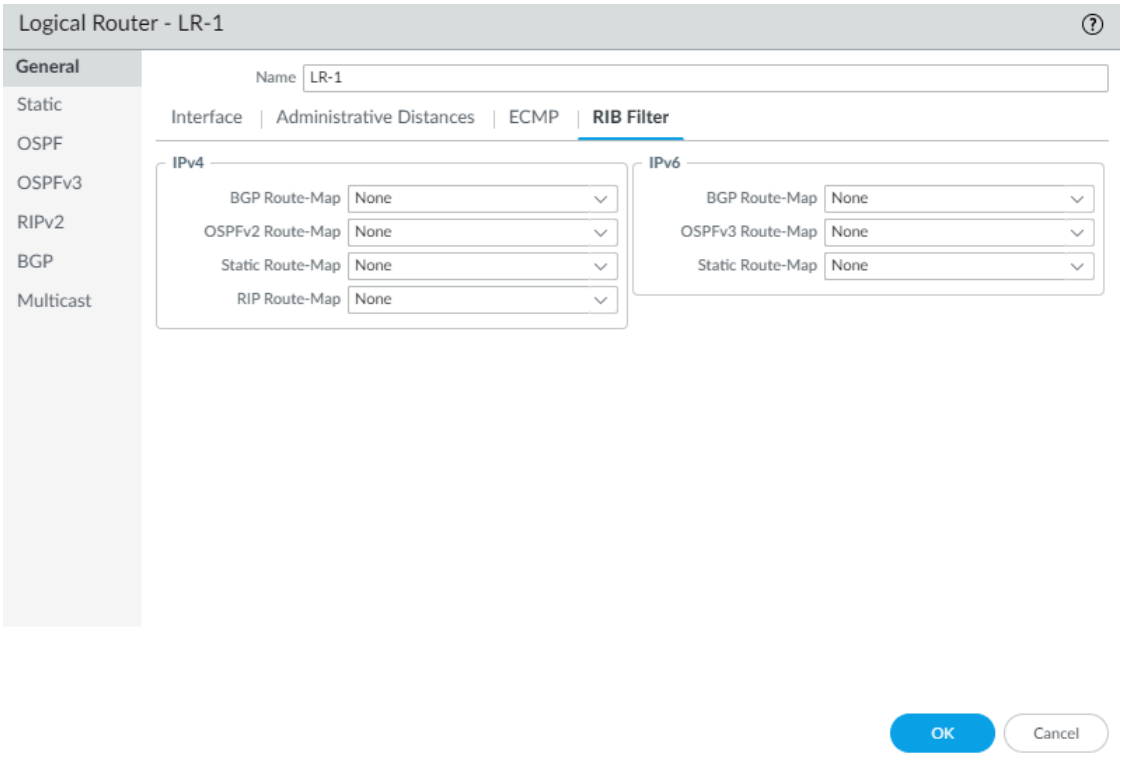
4. **Activez le redémarrage progressif** pour activer le redémarrage progressif OSPF pour le routeur logique. La valeur par défaut est activée.
5. **Activez le mode d'assistance** pour permettre au routeur logique de fonctionner en mode d'assistance Graceful Restart. La valeur par défaut est activée.
6. **Activez la vérification LSA stricte** pour que le routeur d'assistance arrête d'exécuter le mode d'assistance et que le processus de redémarrage progressif s'arrête si une annonce d'état des liens indique un changement de topologie du réseau. La valeur par défaut est activée.
7. Spécifiez la **période de grâce (sec)**— le nombre de secondes pendant lesquelles le routeur logique effectuera un redémarrage progressif si le pare-feu tombe en panne ou devient indisponible ; la plage est de 5 à 1 800 ; la valeur par défaut est 120.
8. Spécifiez le **temps de redémarrage maximal du voisin (sec)** ; la plage est de 5 à 1 800 ; la valeur par défaut est 140.
9. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Configurez le filtrage intra-zone pour déterminer quelles routes OSPFv2 sont placées dans le RIB global.

Vous pouvez apprendre les routes OSPFv2 et les redistribuer, mais ne pas les vouloir dans le RIB global ; vous souhaiterez peut-être autoriser uniquement des routes OSPFv2 spécifiques vers le RIB global.

1. Sélectionnez **Routeurs logiques** > **routage** > **réseau** et sélectionnez un routeur logique.
2. Sélectionnez **Filtre RIB**.
3. Pour filtrer les itinéraires **IPv4** OSPFv2 pour le RIB global, dans la **carte d'itinéraires OSPFv2**, sélectionnez une carte d'itinéraires de redistribution que vous avez créée ou créez une nouvelle carte d'itinéraires de redistribution dans laquelle le protocole source est OSPF et le protocole de destination est RIB.



4. Cliquez sur **OK**.

STEP 10 | (Facultatif) Modifiez les distances administratives par défaut pour les itinéraires OSPF intra-zone, inter-zone et externes au sein d'un routeur logique.

STEP 11 | **Commit** (Valider).

STEP 12 | Affichez les informations de routage avancées pour OSPFv2 et la base de données d'état des liens (LSDB). Le Démarrage rapide de l'interface de ligne de commande PAN-OS répertorie les commandes de la feuille de triche de l'interface de ligne de commande : Networking (Suivant : mise en réseau).

 ©2024 Palo Alto Networks, Inc.

Créer des profils de routage OSPF

Le moteur de routage avancé prend en charge OSPFv2 ; créez les profils suivants à appliquer au protocole, ce qui rend la configuration plus facile et plus cohérente. Les profils peuvent être utilisés sur plusieurs routeurs logiques et systèmes virtuels. Cette rubrique décrit les profils et comment les configurer.

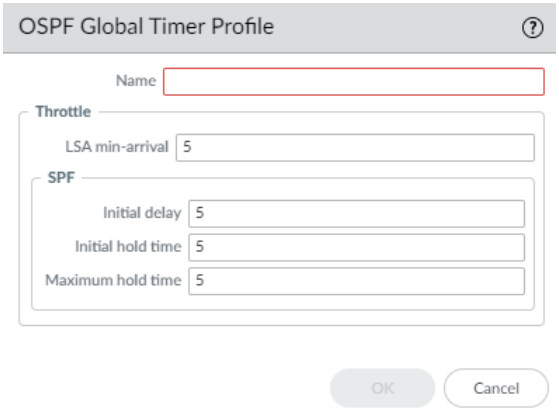
- **Profils de minuterie globale OSPF**— Configurez le temporisateur pour l'arrivée minimum de l'annonce d'état de liaison (LSA) et les temporisateurs SPF (Shortest Path First) pour les zones OSPFv2. Appliquez le profil dans la configuration générale OSPF.
- **Profils d'authentification d'interface OSPF**: spécifiez l'authentification à l'aide d'un mot de passe ou de MD5 ; appliquer de tels profils à une zone OSPF, une interface et/ou une liaison virtuelle.
- **Profils de temporisateur d'interface OSPF**— Configurez les temporisateurs liés aux opérations d'interface, telles que le bonjour OSPF et le redémarrage progressif. Appliquez ces profils à la configuration générale OSPF, à une interface et/ou à une liaison virtuelle.
- **Profils de redistribution OSPF**: spécifiez comment redistribuer les routes statiques IPv4, les routes connectées, les routes IPv4 BGP, les routes RIPv2 et la route par défaut IPv4 vers OSPF. Appliquez le profil dans la configuration générale OSPF.

STEP 1 | Profil de minuterie globale OSPF

1. Sélectionnez **Réseau** > **Routage** > **Profiles de routage** > **OSPF**.
2. **Ajoutez** un **profil de minuterie globale OSPF** par **nom** (un maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.
3. Entrez le **LSA min-arrival**, qui est la durée minimale (en secondes) entre les transmissions de deux instances du même LSA (même ID de routeur publicitaire, même type de LSA et même ID de LSA). Si le même LSA arrive plus tôt que l'intervalle configuré, le LSA est supprimé. La plage est comprise entre 1 et 10 ; la valeur par défaut est 5. L'arrivée min LSA est équivalente à MinLSInterval dans la RFC 2328. Des valeurs inférieures peuvent être utilisées pour réduire les délais de reconvergence en cas de modifications de topologie.
4. Dans la zone SPF, entrez le **délai initial** (en secondes) à partir du moment où le routeur logique reçoit un changement de topologie jusqu'à ce qu'il exécute le calcul du chemin le plus court en premier (SPF) ; la plage est de 0 à 600 ; la valeur par défaut est 5. Des valeurs inférieures permettent une reconvergence OSPF plus rapide. Les routeurs échangeant du trafic avec le pare-feu doivent utiliser la même valeur afin d'optimiser les délais de convergence.
5. Entrez le **temps de maintien initial** (en secondes) entre les calculs SPF consécutifs ; la plage est de 0 à 600 ; la valeur par défaut est 5.

 ©2024 Palo Alto Networks, Inc.

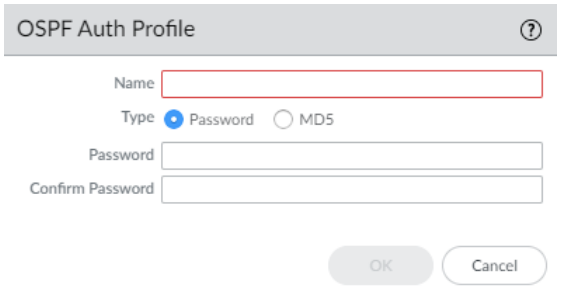
6. Entrez le **temps de maintien maximal** (en secondes), qui est la plus grande valeur à laquelle le temps de maintien se limite jusqu'à ce qu'il reste stable ; la plage est de 0 à 600 ; la valeur par défaut est 5.



7. Cliquez sur **OK**.

STEP 2 | Créez un profil d'authentification d'interface OSPF.

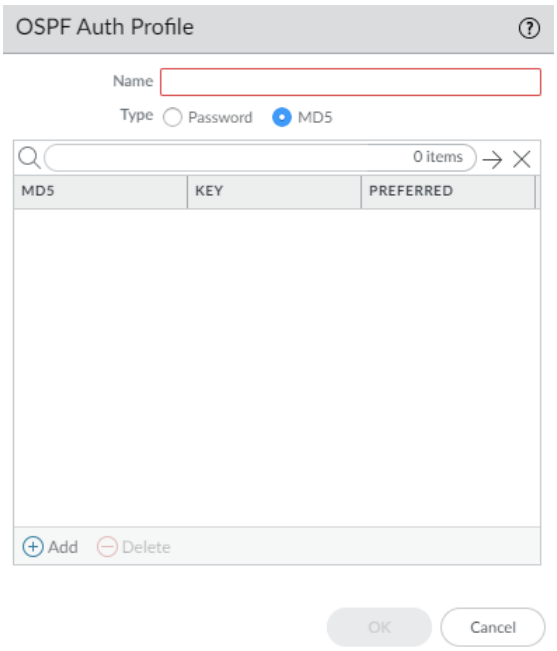
1. Sélectionnez **Réseau** > **Routage** > **Profiles de routage** > **OSPF**.
2. **Ajoutez** un **profil d'authentification OSPF** par **nom** (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.
3. Sélectionnez le type d'authentification : **Mot de passe** ou **MD5**.
   - Si vous choisissez **Mot de passe** , saisissez le **Mot de passe** (huit caractères maximum) et **Confirmez le mot de passe**.



   - Si vous choisissez **MD5**, **ajoutez** un ID de clé MD5 (plage de 0 à 255) et une **clé** (un maximum de 16 caractères alphanumériques). Sélectionnez **Préféré** pour préférer une clé MD5 aux autres touches MD5. Lors de la validation, le pare-feu parcourt la liste des clés de haut en bas et la clé préférée est déplacée en haut de la liste ; la touche

 ©2024 Palo Alto Networks, Inc.

préférée du haut est utilisée. (En d'autres termes, si vous sélectionnez plusieurs clés MD5 préférées, la dernière choisie comme préférée est la clé préférée.)



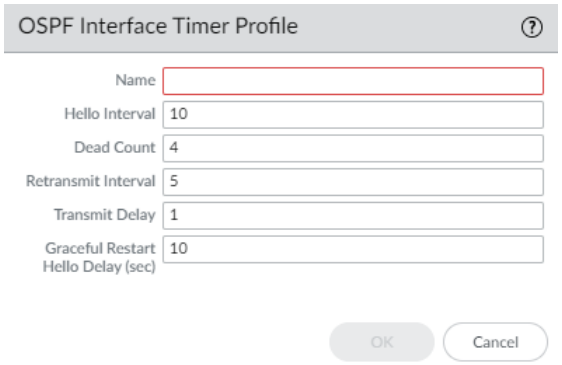
4. Cliquez sur **OK**.

STEP 3 | Créez un profil de minuterie d'interface OSPF.

1. Sélectionnez **Réseau** > **Routage** > **Profiles de routage** > **OSPF**.
2. **Ajoutez** un **profil de minuterie d'interface OSPF** par **nom** (un maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères

 ©2024 Palo Alto Networks, Inc.

alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.

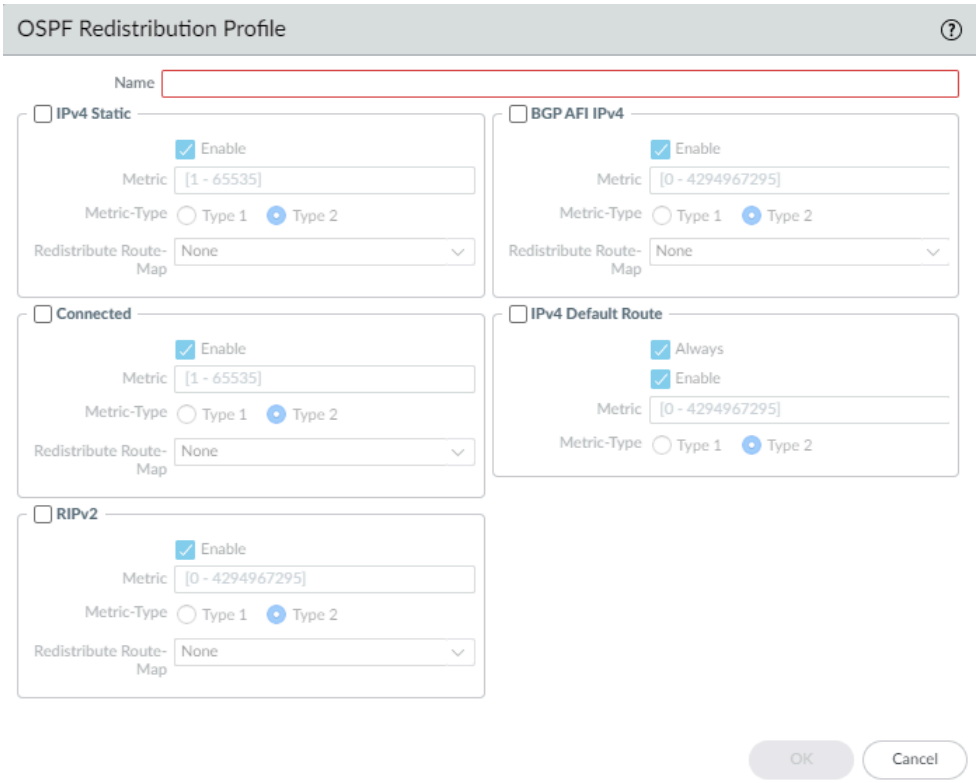


3. Entrez le **Hello Interval**, l'intervalle (en secondes) entre les paquets Hello que le pare-feu envoie à une interface pour maintenir les relations de voisinage ; la plage est de 1 à 3600 ; la valeur par défaut est 10.
4. Entrez le **Dead Counts (Nombre de pertes)** - Nombre de fois que l'intervalle Hello peut se produire pour un voisin sans qu'OSPF ne reçoive un paquet Hello du voisin, avant qu'OSPF ne considère ce voisin comme inactif.
5. Entrez l'**intervalle de retransmission**, le nombre de secondes entre les retransmissions LSA aux Routeurs adjacents ; la plage est de 1 à 1800 ; la valeur par défaut est 5.
6. Entrez le **délai de transmission**, le nombre de secondes nécessaires pour transmettre un paquet de mise à jour de l'état de la liaison sur l'interface. L'âge des annonces d'état de liaison dans le paquet de mise à jour est incrémenté de ce numéro avant d'être transmis ; la plage est comprise entre 1 et 1800; la valeur par défaut est 1.
7. Entrez le **Graceful Restart Hello Delay (sec) (Temporisation de redémarrage en douceur Hello (s))** - S'applique à une interface OSPF lorsque la haute disponibilité active / passive est configurée. La temporisation de redémarrage en douceur Hello est la durée pendant laquelle le pare-feu envoie des paquets LSA à des intervalles de 1 seconde. Pendant cette période, aucun paquet Hello n'est envoyé avant le redémarrage du pare-feu. Lors du redémarrage, le minuteur d'inactivité (qui correspond à l'Intervalle Hello multiplié par le Nombre de pertes) effectue un compte à rebours. Si la valeur du minuteur d'inactivité est trop faible, l'adjacence devient inactive pendant le redémarrage en douceur en raison de la temporisation Hello. Par conséquent, il est recommandé que la valeur du minuteur d'inactivité soit au moins quatre fois celle de la Graceful Restart Hello Delay (Temporisation de redémarrage en douceur Hello). Par exemple, un Intervalle Hello de 10 secondes et un Nombre de pertes de 4 sont égaux à une valeur de minuteur d'inactivité de 40 secondes. Si la Temporisation de redémarrage en douceur Hello est définie sur 10 secondes, la valeur du minuteur d'activité de 40 secondes est suffisante pour que l'adjacence ne devienne pas inactive. La plage est comprise entre 1 et 10 ; la valeur par défaut est 10.
8. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Créez un profil de redistribution OSPF pour spécifier toute combinaison d'itinéraires statiques IPv4, d'itinéraires connectés, d'itinéraires IPv4 BGP, d'itinéraires RIPv2 et d'itinéraire IPv4 par défaut à redistribuer à OSPF.

1. Sélectionnez **Réseau** > **Routage** > **Profiles de routage** > **OSPF**.
2. **Ajoutez** un **profil de redistribution OSPF** par **nom** (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.



3. Sélectionnez **IPv4 statique** pour autoriser la configuration de cette partie du profil.
   - **Activez** la partie IPv4 statique du profil.
   - Saisissez la **mesure** à appliquer aux itinéraires statiques qui sont redistribués dans BGP (plage de 1 à 65 535).
   - Spécifiez le **type de métrique** : **Type 1** (coûts OSPF) ou **Type 2** (par défaut). S'il existe deux itinéraires statiques vers une destination et qu'elles ont le même coût, un itinéraire de type 2 est préférée à un itinéraire de type 1.
   - Sélectionnez une **Redistribute Route-Map** ou créez une nouvelle Redistribute Route Map dont les critères de correspondance contrôlent les itinéraires statiques IPv4 à redistribuer dans OSPF. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué. De même, le Type

 ©2024 Palo Alto Networks, Inc.

de métrique dans la configuration de l'ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.

4. Sélectionnez **Connecté** pour autoriser la configuration de cette partie du profil.
   - **Activez** la partie Connecté du profil.
   - Saisissez la **mesure** à appliquer aux itinéraires connectés qui sont redistribués dans BGP (plage de 1 à 65 535).
   - Spécifiez le **type de métrique** : **Type 1** ou **Type 2** (par défaut). Le coût de type E1 est la somme du coût externe plus le coût interne pour atteindre cet itinéraire. Le type E2 n'est que le coût externe de cet itinéraire. Cela peut être utile lorsque vous souhaitez équilibrer la charge de la même route externe, par exemple.
   - Sélectionnez une **Redistribute Route-Map** ou créez une nouvelle Redistribute Route Map dont les critères de correspondance contrôlent les itinéraires connectés à redistribuer dans OSPF. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué. De même, le Type de métrique dans la configuration de l'ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.
5. Sélectionnez **RIPv2** pour autoriser la configuration de cette partie du profil.
   - **Activez** la partie RIPv2 du profil.
   - Spécifiez la **métrique** à appliquer aux routes RIPv2 redistribuées dans OSPF (la plage est comprise entre 0 et 4 294 967 295).
   - Spécifiez le **type de métrique** : **Type 1** ou **Type 2** (par défaut).
   - Sélectionnez une **Redistribute Route-Map** ou créez une nouvelle Redistribute Route Map dont les critères de correspondance contrôlent les routes RIPv2 à redistribuer dans OSPF. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué. De même, le Type de métrique dans la configuration de l'ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.
6. Sélectionnez **BGP AFI IPv4** pour autoriser la configuration de cette partie du profil.
   - **Activez** la partie BGP AFI IPv4 du profil.
   - Spécifiez la **métrique** à appliquer aux itinéraires BGP redistribués dans OSPF (la plage est comprise entre 0 et 4 294 967 295).
   - Spécifiez le **type de métrique** : **Type 1** ou **Type 2** (par défaut).
   - Sélectionnez une **carte d'itinéraires de redistribution** ou créez une nouvelle carte d'itinéraires de redistribution dont les critères de correspondance contrôlent les itinéraires IPv4 BGP à redistribuer dans OSPF. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué. De même, le Type de métrique dans la configuration de l'ensemble

 ©2024 Palo Alto Networks, Inc.

de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.

7. Sélectionnez **Itinéraire par défaut IPv4** pour autoriser la configuration de cette partie du profil.
   - Sélectionnez **Toujours** pour toujours redistribuer l'itinéraire par défaut IPv4 vers OSPF ; par défaut est activé.
   - **Activez** la partie Itinéraire par défaut IPv4 du profil.
   - Spécifiez la **métrique** à appliquer à la itinéraire par défaut redistribué dans OSPF (la plage est comprise entre 0 et 4 294 967 295).
   - Spécifiez le **type de métrique** : **Type 1** ou **Type 2** (par défaut).
8. Cliquez sur **OK**.

STEP 5 | **Commit** (Valider).

 ©2024 Palo Alto Networks, Inc.

Configurer OSPFv3 sur un moteur de routage avancé

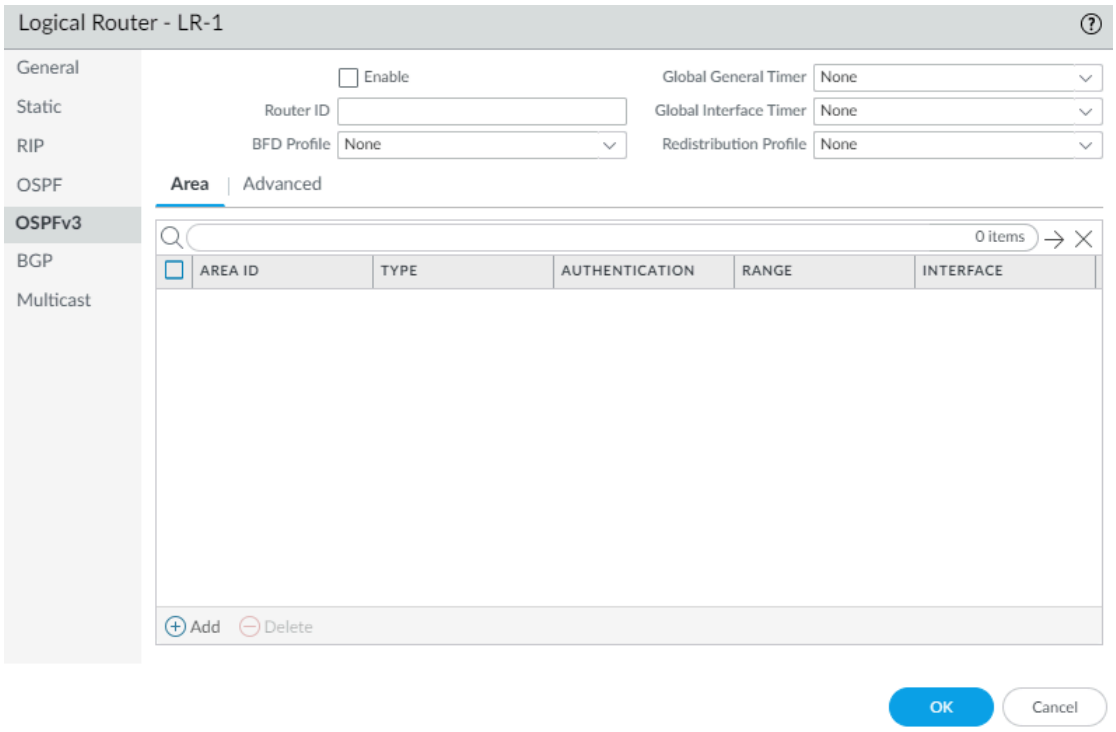
Le moteur de routage avancé prend en charge OSPFv3, qui ne prend en charge que l'adressage IPv6. Avant de configurer OSPFv3, vous devez comprendre Concepts d'OSPF.

Considérez les profils de routage OSPFv3 et les filtres que vous pouvez appliquer à OSPFv3 et ainsi gagner du temps de configuration et maintenir la cohérence. Vous pouvez créer des profils et des filtres à l'avance ou lors de la configuration d'OSPFv3.

STEP 1 | Configurer un routeur logique.

STEP 2 | Configurez les options générales de routage OSPFv3.

1. Sélectionnez **Réseau** > **Routage** > **Routeurs logiques** et sélectionnez le routeur logique.
2. Sélectionnez **OSPFv3** et **activez** -le.



3. Attribuez un **ID de routeur** à OPSFv3 pour le routeur logique, qui est généralement une adresse IPv4 (même si OSPFv3 est destiné à l'adressage IPv6), pour vous assurer que l'ID de routeur est unique.
4. Si vous souhaitez appliquer BFD à OSPFv3, sélectionnez un **profil BFD** que vous avez créé, ou sélectionnez le profil **par défaut** , ou créez un nouveau profil BFD à appliquer à

©2024 Palo Alto Networks, Inc.

toutes les interfaces OSPFv3 appartenant au routeur logique. Par défaut **None (disable BFD) (Aucun - BFD désactivé)**.

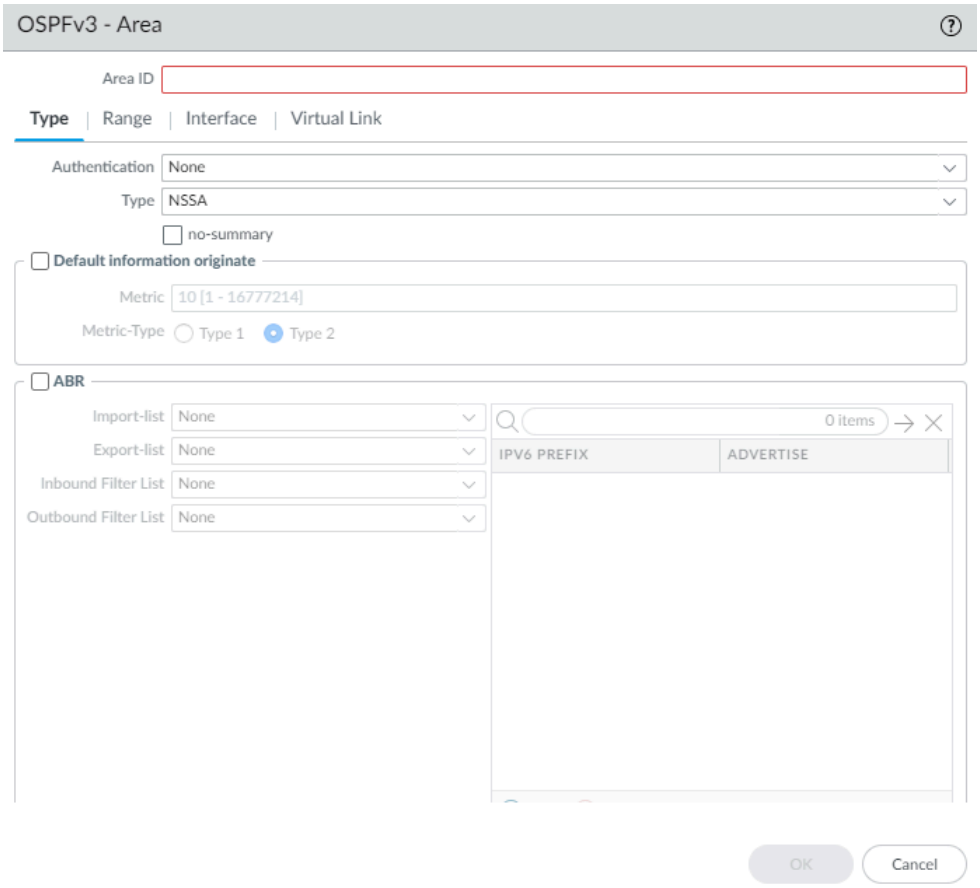
5. Sélectionnez un profil de **temporisateur général global** ou créez-en un nouveau pour définir les temporisateurs de régulation SPF et pour définir l'intervalle minimum entre les instances d'arrivée de la même annonce d'état de liaison (LSA).
6. Sélectionnez un profil **de minuterie d'interface globale** ou créez-en un nouveau pour définir l'intervalle hello, l'intervalle de retransmission et d'autres paramètres.
7. Sélectionnez un **profil de redistribution** ou créez-en un nouveau pour redistribuer les routes statiques IPv6, les routes connectées, les routes BGP IPv6 ou la route par défaut IPv6 vers OSPFv3.
8. Cliquez sur **OK**.

STEP 3 | Créez une zone OSPFv3 et spécifiez les caractéristiques en fonction du type de zone.

1. Sélectionnez **Réseau** > **Routage** > **Routeurs logiques** et sélectionnez le routeur logique.
2. Sélectionnez **Zone** > **OSPFv3** et **ajoutez** une zone par **ID de zone** (une adresse IPv4).
3. Dans l'onglet **Type** , sélectionnez un profil d' **authentification** pour la zone ou créez-en un nouveau.
4. Spécifiez le **Type** de zone :
   - **Normal (Normal)** - Aucune restriction n'est appliquée ; la zone peut accepter tout type d'itinéraire.
   - **Stub (Terminale)** : il n'existe aucune sortie issue de la zone. Pour atteindre une destination en dehors de la zone, le trafic doit passer par un routeur de frontière de zone (ABR), qui se connecte à d'autres zones et à la zone 0.
   - **NSSA** (Not So Stubby Area) : le trafic peut quitter la zone directement, mais uniquement en utilisant des routes non OSPF.
5. (Zones stub et NSSA uniquement) Sélectionnez **no-summary** pour empêcher la zone de recevoir des LSA récapitulatifs de type 3 et ainsi réduire le trafic dans la zone.
6. (Zone NSSA uniquement) Sélectionnez **l'origine des informations par défaut** pour qu'OSPFv3 crée une route par défaut.
   - Saisissez une **mesure** pour la route par défaut ; la plage est de 1 à 16 777 214 ; la valeur par défaut est 10.
   - Sélectionnez le **type de mesure** : **Type 1** ou **Type 2**. Le coût de type E1 est la somme du coût externe plus le coût interne pour atteindre cet itinéraire. Le type E2 n'est que

 ©2024 Palo Alto Networks, Inc.

le coût externe de cet itinéraire. Cela peut être utile lorsque vous souhaitez équilibrer la charge de la même route externe, par exemple.



7. Sélectionnez **ABR** si vous souhaitez configurer les options de filtrage.
8. Sélectionnez une **liste d'importation** ou créez une nouvelle liste d'accès pour filtrer les LSA de type 3 ; s'applique aux chemins annoncés dans la zone spécifiée en tant que LSA récapitulatifs de type 3.
9. Sélectionnez une **liste d'exportation** ou créez une nouvelle liste d'accès pour filtrer les LSA récapitulatifs de type 3 annoncés à d'autres zones provenant de chemins intra-zone à partir de la zone spécifiée.
10. Sélectionnez une **liste de filtres entrants** ou créez une nouvelle liste de préfixes pour filtrer les LSA récapitulatives de type 3 entrant dans la zone.

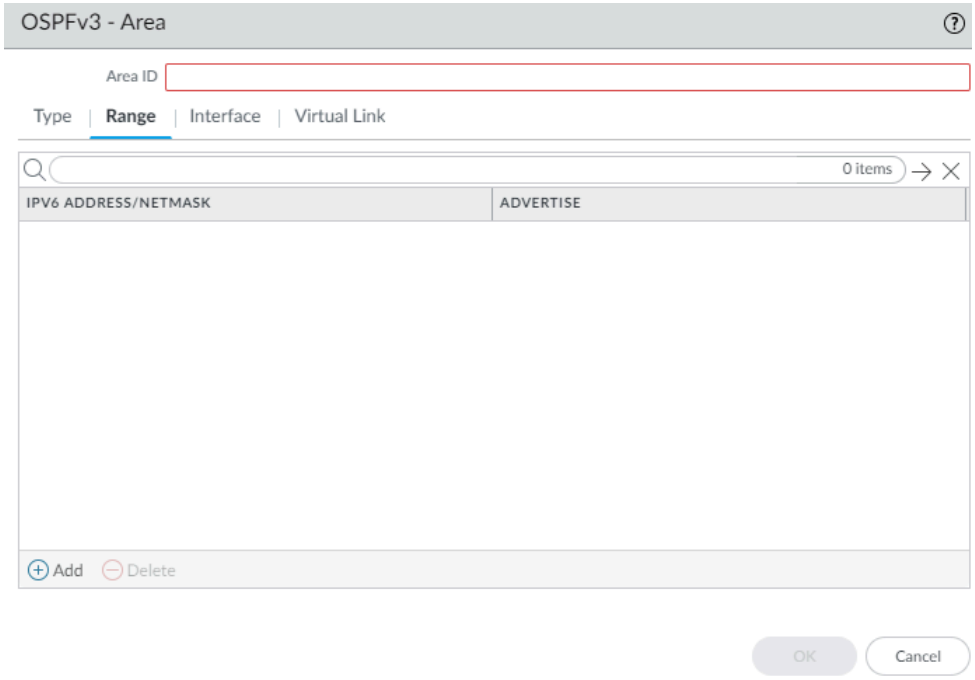
    Si vous appliquez une liste d'accès d'importation et une liste de préfixes entrants, le pare-feu utilise une opération ET (les deux listes doivent être remplies).
11. Sélectionnez une **liste de filtres sortants** ou créez une nouvelle liste de préfixes pour filtrer les LSA récapitulatives de type 3 de la zone.

    Si vous appliquez une liste d'accès d'exportation et une liste de préfixes sortants, le pare-feu utilise une opération ET (les deux listes doivent être remplies).
12. Si le **type** de zone est **NSSA** et **ABR** est sélectionné, **ajoutez** un **préfixe IPv6** pour résumer un groupe de sous-réseaux externes en un seul LSA de type 7, qui est ensuite traduit en un LSA de type 5 et annoncé à la dorsale lorsque vous sélectionnez **Annoncer**.

©2024 Palo Alto Networks, Inc.

STEP 4 | Spécifiez la plage de réseau qu'un LSA de résumé de type 3 annonce à la zone dorsale si la zone contient au moins un réseau intra-zone (c'est-à-dire décrit avec un routeur ou un LSA de réseau) de cette plage.

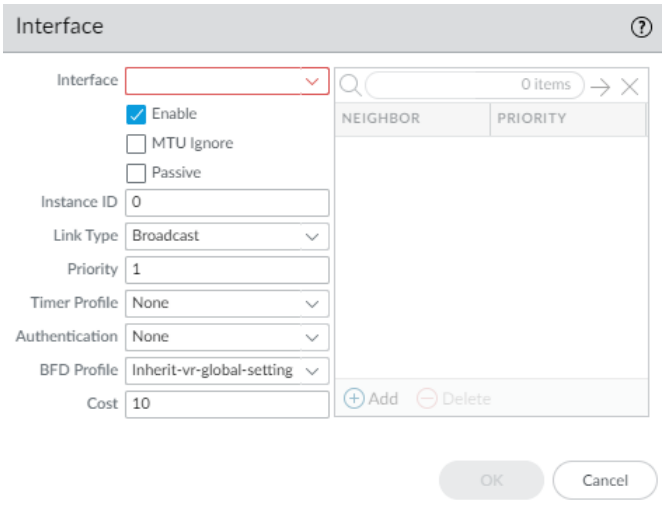
1. Sélectionnez **Plage** et **ajoutez** une **adresse IPv6/masque de réseau** , qui résume les routes pour la zone. Un LSA récapitulatif de type 3 avec des informations d'acheminement qui correspondent à la plage est annoncé dans la zone dorsale si la zone contient au moins un réseau intra-zone de cette plage.
2. Sélectionnez **Publier** pour annoncer les sous-réseaux correspondants dans les LSA à la zone dorsale. Si **Annoncer** est défini sur Non, tous les préfixes intra-zone correspondants qui sont présents dans la zone ne seront pas annoncés dans la zone dorsale.



 ©2024 Palo Alto Networks, Inc.

STEP 5 | Ajoutez des interfaces à la zone.

1. Dans l'onglet **Interface** , **ajoutez** une **interface** en en sélectionnant une.
2. **Activez** l'interface.



3. Sélectionnez **MTU Ignorer** pour ignorer les incompatibilités d'unité de transmission maximale (MTU) lors de la tentative d'établissement d'une contiguïté (la valeur par défaut est désactivée ; la vérification de correspondance MTU se produit).
4. Sélectionnez **Passive** pour empêcher l'envoi de paquets OSPF Hello sur cette interface et ainsi empêcher le routeur logique de créer une contiguïté OSPF avec un voisin ; cependant, l'interface est toujours incluse dans la base de données d'état des liens. Vous pouvez rendre une interface passive, par exemple si elle se connecte à un commutateur, car vous ne souhaitez pas envoyer de paquets Hello là où il n'y a pas de routeur.
5. Conservez l'**ID d'instance** défini sur 0, car une seule instance d'OSPFv3 est autorisée.
6. Sélectionnez le **type de lien** :
   - **Broadcast (Diffusion)** : tous les voisins accessibles via l'interface soient détectés automatiquement en multidiffusant des messages Hello OSPF, comme par une interface Ethernet.
   - **p2p** (point à point) : découvre automatiquement le voisin.
   - **p2mp** (point-to-multipoint/point-multipoint) : les voisins doivent être définis manuellement. **Ajoutez** l'adresse IPv6 du **voisin** pour tous les voisins accessibles via cette interface et la **priorité** de chaque voisin à élire comme routeur désigné (DR) ou DR de secours ; la plage est de 0 à 255 ; la valeur par défaut est 1.
7. Écrivez une **priorité** pour l'interface — la priorité pour que le routeur soit élu en tant que routeur indiqué (DR) ou DR de secours (BDR) ; la plage est de 0 à 255 ; la valeur par

 ©2024 Palo Alto Networks, Inc.

défaut est 1. Lorsque la valeur 0 est configurée, le routeur ne sera pas élu en tant que DR ou BDR.

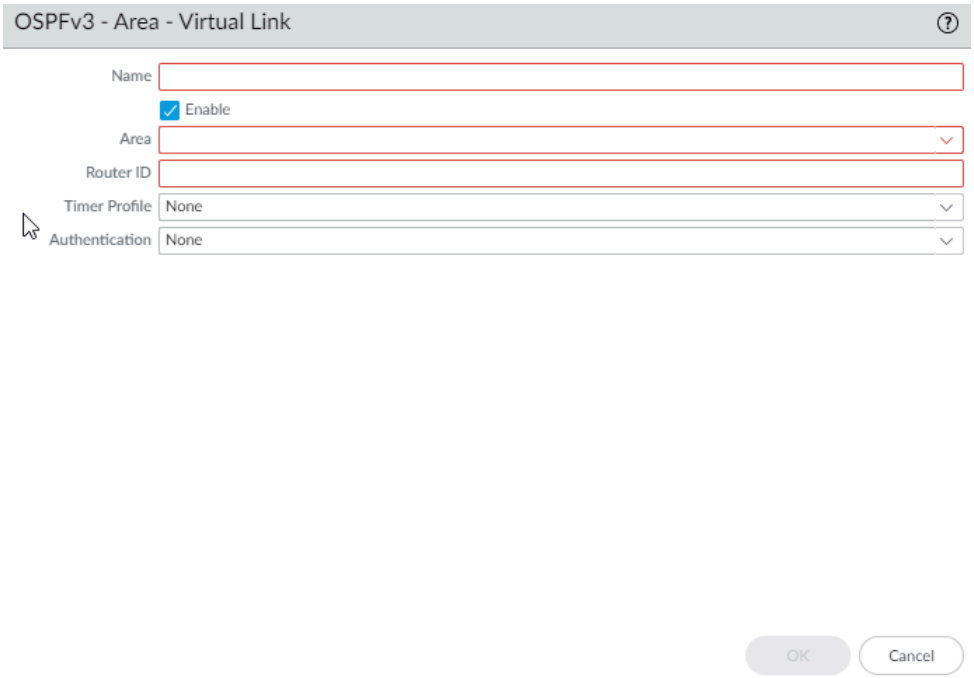
8. Sélectionnez un **profil de minuterie** d'interface OSPFv3 ou créez-en un nouveau à appliquer à l'interface. Ce profil de minuterie d'interface OSPFv3 remplace la minuterie d'interface globale appliquée à OSPFv3.
9. Sélectionnez un **profil d'authentification** d'interface OSPFv3 ou créez-en un nouveau à appliquer à l'interface. Ce profil d'authentification remplace le profil d'authentification appliqué à la zone (sur l'onglet Type).
10. Par défaut, l'interface héritera du profil BFD que vous avez appliqué au routeur logique pour OSPFv3 (**Inherit-vr-global-setting**). Vous pouvez également sélectionner le profil **par défaut** , sélectionner un **profil BFD** que vous avez créé, en créer un nouveauou sélectionner **Aucun (désactiver BFD)** pour remplacer le profil BFD appliqué au niveau OSPFv3.
11. Entrez un **coût** OSPFv3 pour l'interface, qui influence la sélection de l'itinéraire ; la plage est de 1 à 65,5535 ; la valeur par défaut est 10. Lors de la sélection de l'itinéraire, un itinéraire avec un coût cumulé inférieur (les coûts supplémentaires de chaque interface utilisée) est préféré à un itinéraire avec un coût cumulé plus élevé.
12. Cliquez sur **OK** pour enregistrer l'interface.

©2024 Palo Alto Networks, Inc.

STEP 6 | Si l'ABR n'a pas de lien physique avec la zone dorsale, configurez une liaison virtuelle vers un ABR voisin dans la même zone qui a un lien physique avec la zone dorsale.

Les paramètres suivants doivent être définis pour les routeurs de bordure de zone (ABR) et à l'intérieur de la zone du segment principal (0.0.0.0).

1. Sélectionnez **Virtual Link (lien virtuel)**.
2. **Ajouter** un **Lien Virtuel** par **Nom** (31 caractères maximum).
3. **Activez** le lien virtuel.



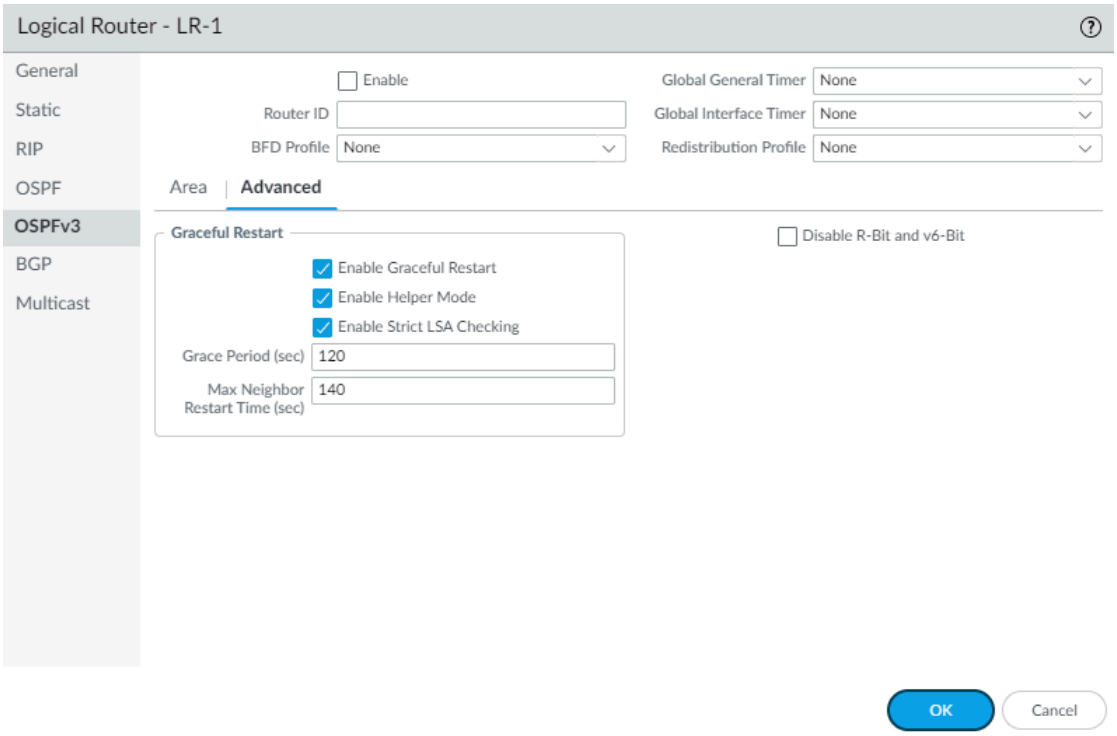
4. Sélectionnez la **zone** de transit où se trouve l'ABR voisin qui a le lien physique avec la zone dorsale.
5. Entrez l'**ID de routeur** de l'ABR voisin à l'extrémité distante de la liaison virtuelle.
6. Sélectionnez un **profil de minuterie** d'interface OSPFv3 ou créez un nouveau profil de minuterie à appliquer au lien virtuel. Ce profil de minuterie d'interface OSPFv3 remplace la minuterie de l'interface globale appliquée à OSPFv3 et le profil de minuterie d'interface OSPFv3 appliqué à l'interface.
7. Sélectionnez un profil d' **authentification** d'interface OSPF ou créez un nouveau profil d'authentification à appliquer au lien virtuel. Ce profil d'authentification remplace le profil d'authentification appliqué à la zone (sur l'onglet Type) et le profil d'authentification appliqué à l'interface.
8. Cliquez sur **OK**.

STEP 7 | Cliquez sur **OK** pour enregistrer la zone.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | Configurez des options OSPFv3 avancées.

1. Sélectionnez **Réseau** > **Routage** > **Routeurs logiques** et sélectionnez le routeur logique.
2. Sélectionnez **OSPFv3** > **Avancé**.
3. **Activer le redémarrage progressif** pour activer le redémarrage progressif pour le routeur logique. La valeur par défaut est activée.
4. **Activez le mode d'assistance** pour permettre au routeur logique de fonctionner en mode d'assistance Graceful Restart. La valeur par défaut est activée.
5. **Activez la vérification LSA stricte** pour que le routeur d'assistance cesse d'exécuter le mode d'assistance et pour que le processus de redémarrage progressif s'arrête si une annonce d'état des liens indique un changement de topologie du réseau. La valeur par défaut est activée.
6. Entrez une **période de grâce (sec)**— le nombre de secondes pendant lesquelles le routeur logique effectuera un redémarrage normal si le pare-feu tombe en panne ou devient indisponible ; la plage est de 5 à 1 800 ; la valeur par défaut est 120.
7. Entrez un **Max Neighbor Restart Time (sec)**— le nombre maximal de secondes de période de grâce que le routeur logique accepte d'un voisin lorsque le routeur logique est en mode d'assistance ; la plage est de 5 à 1 800 ; la valeur par défaut est 140.
8. Sélectionnez **Désactiver R-Bit et v6-Bit** pour effacer le R-bit et V6-bit dans les LSA de routeur envoyés depuis ce routeur logique pour indiquer que le pare-feu n'est pas actif. Lorsqu'il est dans cet état, le pare-feu participe à OSPFv3 mais n'envoie pas de trafic de transit ou de datagrammes IPv6. Dans cet état, le trafic local est transféré au pare-feu. Cela est utile lors de la maintenance sur un réseau à double interface, car le trafic peut être encore atteint lorsqu'il est réacheminé vers le pare-feu. Voir RFC 5340.



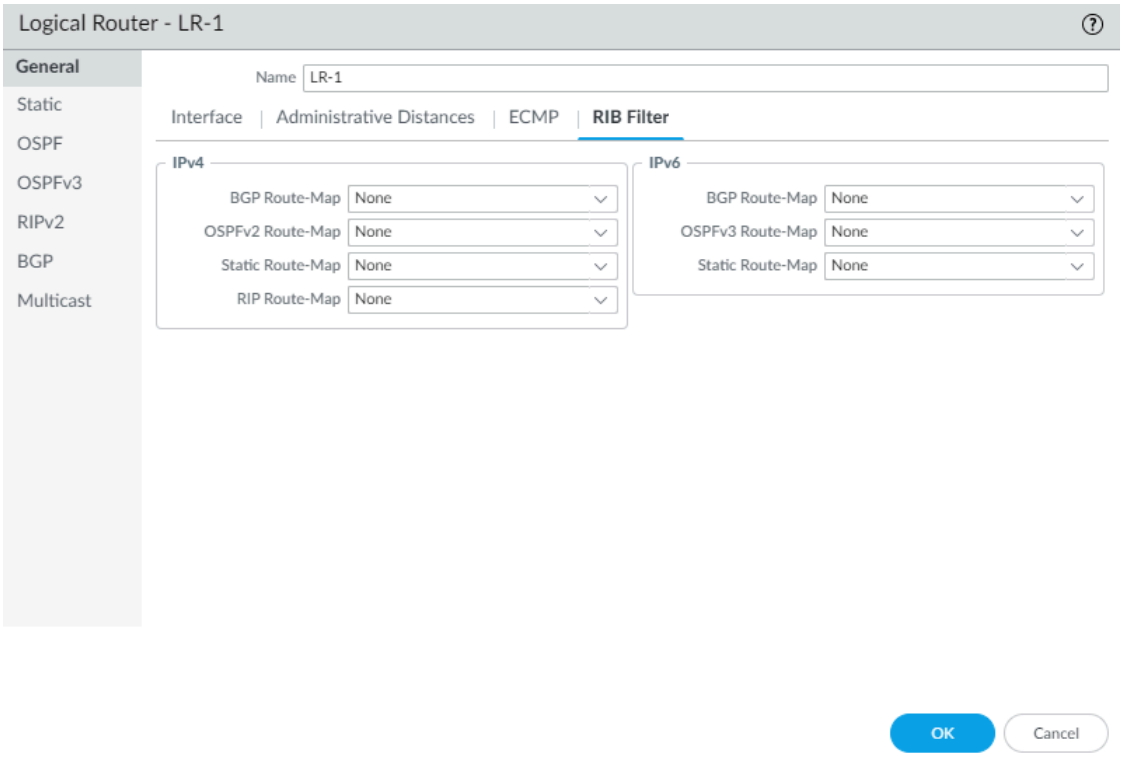
9. Cliquez sur **OK** pour enregistrer les paramètres avancés.

©2024 Palo Alto Networks, Inc.

STEP 9 | Configurez le filtrage intra-zone pour déterminer quelles routes OSPFv3 sont placées dans le RIB global.

Vous pouvez apprendre les routes OSPFv3 et les redistribuer, mais ne pas les vouloir dans le RIB global ; vous souhaiterez peut-être autoriser uniquement des routes OSPFv3 spécifiques vers le RIB global.

1. Sélectionnez **Routeurs logiques** > **routage** > **réseau** et sélectionnez un routeur logique.
2. Sélectionnez **Filtre RIB**.
3. Pour filtrer les itinéraires **IPv6** OSPFv3 pour le RIB global, pour **OSPFv3 Route-Map**, sélectionnez une carte d'itinéraires de redistribution que vous avez créée ou créez une nouvelle carte d'itinéraires de redistribution dans laquelle le protocole source est OSPFv3 et le protocole de destination est RIB.



4. Cliquez sur **OK**.

STEP 10 | (Facultatif) Modifiez les distances administratives par défaut pour les routes intra-zone OSPFv3, inter-zone OSPFv3 et externes OSPFv3 qui se rapportent au routeur logique.

STEP 11 | **Commit** (Valider).

STEP 12 | Affichez les informations de routage avancées pour OSPFv3 et la base de données d'état des liens (LSDB). Le Démarrage rapide de l'interface de ligne de commande PAN-OS répertorie les commandes de la feuille de triche de l'interface de ligne de commande : Networking (Suivant : mise en réseau).

©2024 Palo Alto Networks, Inc.

Créer des profils de routage OSPFv3

Le moteur de routage avancé prend en charge OSPFv3 ; créer des profils de minuteries globales OSPFv3, des profils d'authentification, des profils de minuterie d'interface et des profils de redistribution à appliquer à OSPFv3. Cette rubrique décrit les profils et explique comment les créer. Référencez-les lorsque vous Configurer OSPFv3 sur un moteur de routage avancé.

- **Profils globaux du minuterie OSPFv3** : spécifiez les minuteries pour l'intervalle de publication d'état de liaison (LSA), le délai de calcul SPF, le temps d'attente initial et le temps d'attente maximal qui appliquent toutes les zones OSPFv3. Les paramètres SPF Throttle permettent au protocole de ralentir l'envoi des mises à jour LSA lorsqu'un réseau est instable (en cours de modification de la topologie). Appliquez le profil dans la configuration générale OSPFv3. Le profil est global pour OSPFv3 sur le routeur logique ; vous pouvez en créer plusieurs pour changer facilement les minuteries globales.
- **Profils d'authentification d'interface OSPFv3** : OSPFv3 n'a pas ses propres capacités d'authentification ; il s'appuie sur IPSec pour sécuriser les messages OSPFv3 entre voisins. Appliquez le profil dans l'onglet **Type de zone** > **OSPFv3.**
- **Profils de la minuterie d'interface OSPFv3**: spécifiez les minuteries liées aux opérations d'interface, telles que LE bonjour OSPFv3 et le redémarrage en douceur. Appliquez le profil dans la configuration générale OSPFv3.
- **Profils de redistribution OSPFv3** : redistribuez les itinéraires BGP statiques, connectés ou IPv6 IPv6 ou l'itinéraire par défaut IPv6 dans OSPFv3. Appliquez le profil dans la configuration générale OSPFv3.

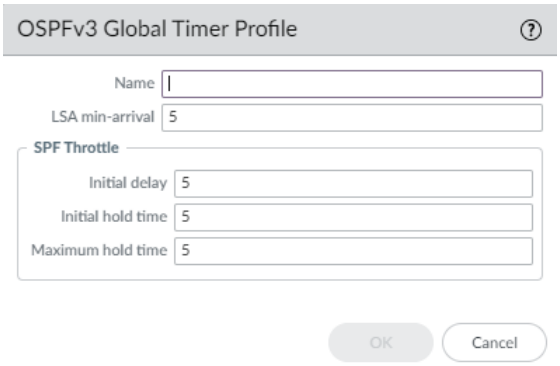
STEP 1 | Créez un profil de minuterie global OSPFv3.

1. Sélectionnez **Réseau** > **Routage** > **Profils de routage** > **OSPFv3**.
2. **Ajoutez** un **profil de minuterie global OSPFv3** par **nom** (un maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.
3. Entrez le **LSA min-arrival** (en secondes), qui est le plus petit intervalle auquel le pare-feu recalcule l'arborescence SPF ; la plage est comprise entre 1 et 10 ; la valeur par défaut est 5. Le pare-feu se recalculerait à un intervalle plus long (moins fréquemment que le paramètre).
4. Dans la zone Throttle SPF, entrez le **délai** initial (en secondes) entre le moment où le routeur logique reçoit un changement de topologie jusqu'à ce qu'il effectue le calcul SPF (Shortest Path First) ; la plage est comprise entre 0 et 600 ; la valeur par défaut est 5.
5. Entrez le **temps d'attente initial** (en secondes) entre les deux premiers calculs SPF consécutifs ; la plage est comprise entre 0 et 600 ; la valeur par défaut est 5. Chaque

 ©2024 Palo Alto Networks, Inc.

temps d'attente suivant est deux fois plus long que le temps d'attente précédent jusqu'à ce que le temps d'attente atteigne le temps d'attente maximal.

6. Entrez le **temps d'attente maximal** (en secondes), qui est la valeur la plus élevée à laquelle le temps d'attente augmente jusqu'à ce qu'il reste stable ; la plage est comprise entre 0 et 600 ; la valeur par défaut est 5.



7. Cliquez sur **OK**.

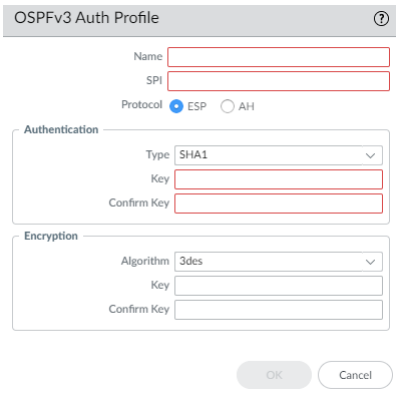
STEP 2 | Créez un profil d'authentification d'interface OSPFv3.

1. Sélectionnez **Réseau** > **Routage** > **Profils de routage** > **OSPFv3**.
2. **Ajoutez** un **profil d'authentification OSPFv3** par **nom** (un maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou

 ©2024 Palo Alto Networks, Inc.

un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.

3. Entrez le **SPI** (Security Policy Index), qui doit correspondre entre les deux extrémités de la contiguïté OSPFv3.
4. Sélectionnez le **Protocol (Protocole)** : **ESP** (Encapsulating Security Payload) (recommandé) ou **AH** (Authentication Header).
5. Sélectionnez le **type** d'authentification :
   - **SHA1** (par défaut) - Sécuriser l'algorithme SHA 1.
   - **Sha256**
   - **SHA384**
   - **SHA512**
   - **MD5**
   - **None**
6. Entrez la **clé** d'authentification à l'aide de 5 sections hexadécimales de 8 caractères hexadécimaux pour un total de 40 caractères hexadécimaux (par exemple, A5DEC4DD155A695A8B983AACEAA5A97C6AECB6D1).
7. **Confirmez la clé** en entrant la même clé.



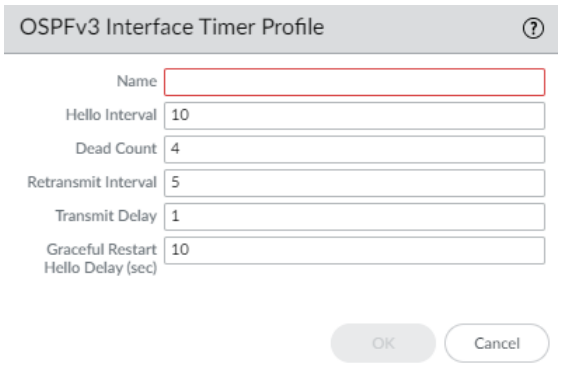
8. (ESP uniquement) Sélectionnez l'**algorithme** de chiffrement:
   - **3des** (par défaut)
   - **aes-128-cbc**
   - **aes-192-cbc**
   - **aes-256-cbc**
   - **zéro**
9. Entrez la **clé** de chiffrement au format hexadécimal ; utilisez le nombre correct de sections en fonction du type de chiffrement ESP :
   - **3des :**utilisez un total de 6 sections hexadécimales dans la clé.
   - **aes-128-cbc :**utilisez un total de 4 sections hexadécimales dans la clé.
   - **aes-192-cbc :**utilisez un total de 6 sections hexadécimales dans la clé.
   - **aes-256-cbc :**utilisez un total de 8 sections hexadécimales dans la clé.
10. **Confirmez la clé** en entrant la même clé.

 ©2024 Palo Alto Networks, Inc.

11. Cliquez sur **OK**.

STEP 3 | Profil de minuterie d'interface OSPFv3

1. Sélectionnez **Réseau** > **Routage** > **Profils de routage** > **OSPFv3**.
2. **Ajoutez** un **profil de minuterie d'interface OSPFv3** par **nom** (un maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.



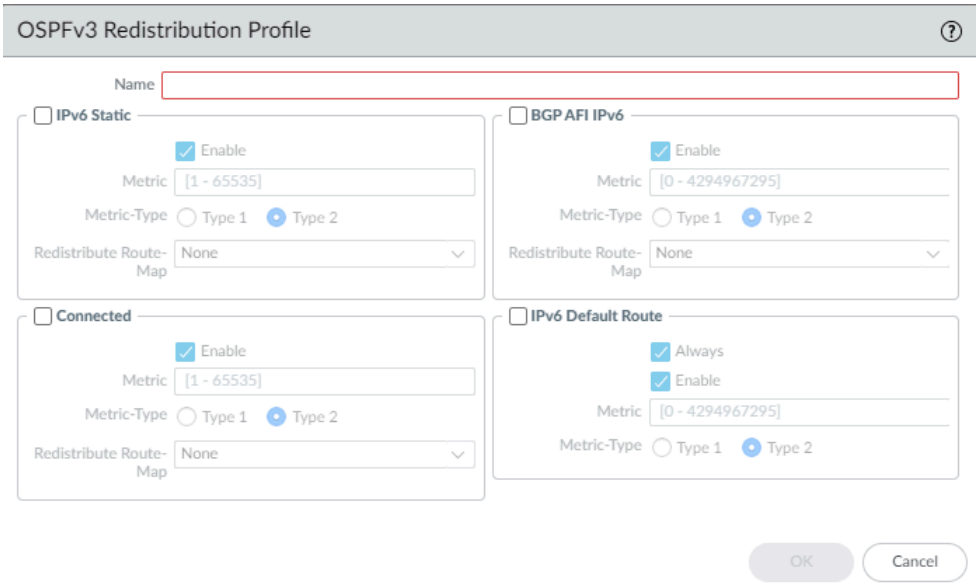
3. Entrez **Hello interval**, l'intervalle (en secondes) auquel OSPFv3 envoie des paquets Hello ; la plage est comprise entre 1 et 3 600 ; la valeur par défaut est 10.
4. Entrez le **Dead Count**, le nombre de fois que l'intervalle Hello peut se produire à partir d'un voisin sans que OSPFv3 reçoive un paquet Hello du voisin, avant que OSPFv3 ne considère ce voisin vers le bas ; la plage est de 3 à 20 ; la valeur par défaut est 4.
5. Entrez **Retransmit interval**, le nombre de secondes pendant lesquelles OSPFv3 attend pour recevoir un ACK pour un LSA d'un voisin avant qu'OSPFv3 ne retransmet le LSA ; la plage est comprise entre 1 et 1 800 ; la valeur par défaut est 5.
6. Entrez **Transmit Delay**, le nombre de secondes pendant lesquelles OSPFv3 retarde la transmission d'un LSA avant d'envoyer le LSA hors d'une interface ; la plage est comprise entre 1 et 1 800 ; la valeur par défaut est 1.
7. Entrez **Graceful Restart Hello Delay (sec)** ; la plage est comprise entre 1 et 10 ; la valeur par défaut est 10. Ce paramètre s'applique à une interface OSPFv3 lorsque la haute disponibilité active/passive est configurée. La temporisation de redémarrage en douceur Hello est la durée pendant laquelle le pare-feu envoie des paquets LSA à des intervalles de 1 seconde. Pendant cette période, aucun paquet Hello n'est envoyé avant le redémarrage du pare-feu. Lors du redémarrage, le minuteur d'inactivité (qui correspond à l'**Intervalle Hello** multiplié par le **Nombre de pertes**) effectue un compte à rebours. Si la valeur du minuteur d'inactivité est trop faible, l'adjacence devient inactive pendant le redémarrage en douceur en raison de la temporisation Hello. Par conséquent, il est recommandé que la valeur du minuteur d'inactivité soit au moins quatre fois celle de la Graceful Restart Hello Delay (Temporisation de redémarrage en douceur Hello). Par exemple, un **Intervalle Hello** de 10 secondes et un **Nombre de pertes** de 4 sont égaux à une valeur de minuteur d'inactivité de 40 secondes. Si la **Graceful Restart Hello Delay** est définie sur 10 secondes, la valeur du minuteur d'activité de 40 secondes est suffisante pour que l'adjacence ne devienne pas inactive (plage de 1 à 10 ; valeur par défaut de 10).

 ©2024 Palo Alto Networks, Inc.

8. Cliquez sur **OK**.

STEP 4 | Créez un profil de redistribution OSPFv3 pour spécifier n'importe quelle combinaison d'itinéraires statiques IPv6, d'itinéraires connectés, d'itinéraires BGP IPv6 et d'itinéraire iPv6 par défaut à redistribuer à OSPFv3.

1. Sélectionnez **Réseau** > **Routage** > **Profils de routage** > **OSPFv3**.
2. **Ajoutez** un **profil de redistribution OSPFv3** par **nom** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.



3. Sélectionnez **IPv6 Statique** pour autoriser la configuration de cette partie du profil.
   - **Activez** la partie de redistribution statique IPv6 du profil.
   - Entrez une **mesure** à appliquer aux routes statiques IPv6 redistribuées à OSPFv3 ; la plage est comprise entre 1 et 65 535.
   - Sélectionnez un **type de mesure** : **Type 1** ou **Type 2**.
   - Sélectionnez une **Redistribute Route-Map (carte d'itinéraires de redistribution)** ou créez une nouvelle carte d'itinéraires de redistribution dont les critères de correspondance contrôlent les itinéraires statiques IPv6 à redistribuer dans OSPFv3. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué. De même, le Type de métrique dans la

 ©2024 Palo Alto Networks, Inc.

configuration de l'ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.

4. Sélectionnez **Connecté** pour autoriser la configuration de cette partie du profil.
   - **Activez** la partie de redistribution d'itinéraire connecté du profil.
   - Entrez une **mesure** à appliquer aux itinéraires connectés redistribués à OSPFv3 ; la plage est comprise entre 1 et 65 535.
   - Sélectionnez un **type de mesure** : **Tapez 1** ou **Type 2**.
   - Sélectionnez une **carte d'itinéraires redistribués** ou créez une nouvelle carte d'itinéraires de redistribution dont les critères de correspondance contrôlent les itinéraires connectés à redistribuer dans OSPFv3. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué. De même, le Type de métrique dans la configuration de l'ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.
5. Sélectionnez **BGP AFI IPv6** pour autoriser la configuration de cette partie du profil.
   - **Activez** la partie de redistribution d'itinéraire BGP AFI IPv6 du profil.
   - Entrez une **mesure** à appliquer aux itinéraires BGP IPv6 redistribuées à OSPFv3 ; la plage est comprise entre 0 et 4 294 967 295.
   - Sélectionnez un **type de mesure** : **Tapez 1** ou **Type 2**.
   - Sélectionnez une **carte d'itinéraires de redistribution** ou créez une nouvelle carte d'itinéraires de redistribution dont les critères de correspondance contrôlent les itinéraires BGP IPv6 à redistribuer dans OSPFv3. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué. De même, le Type de métrique dans la configuration de l'ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.
6. Sélectionnez **Itinéraire par défaut IPv6** pour autoriser la configuration de cette partie du profil.
   - Sélectionnez **Toujours** pour toujours créer et redistribuer l'itinéraire par défaut vers OSPFv3, même s'il n'y a pas d'itinéraire par défaut sur le routeur ; la valeur par défaut est activée. Si **Toujours** n'est pas défini, lorsqu'il n'y a pas d'itinéraire par défaut sur l'ABR, l'itinéraire par défaut n'est pas redistribué.
   - **Activez** la partie de redistribution de l'itinéraire par défaut IPv6 du profil.
   - Entrez une **mesure** à appliquer à l'itinéraire IPv6 par défaut redistribué à OSPFv3 ; la plage est comprise entre 0 et 4 294 967 295.
   - Sélectionnez un **type de mesure** : **Tapez 1** ou **Type 2**.
7. Cliquez sur **OK**.

STEP 5 | **Commit** (Valider).

 ©2024 Palo Alto Networks, Inc.

Configurer RIPv2 sur un moteur de routage avancé

Le moteur de routage avancé prend en charge RIPv2.

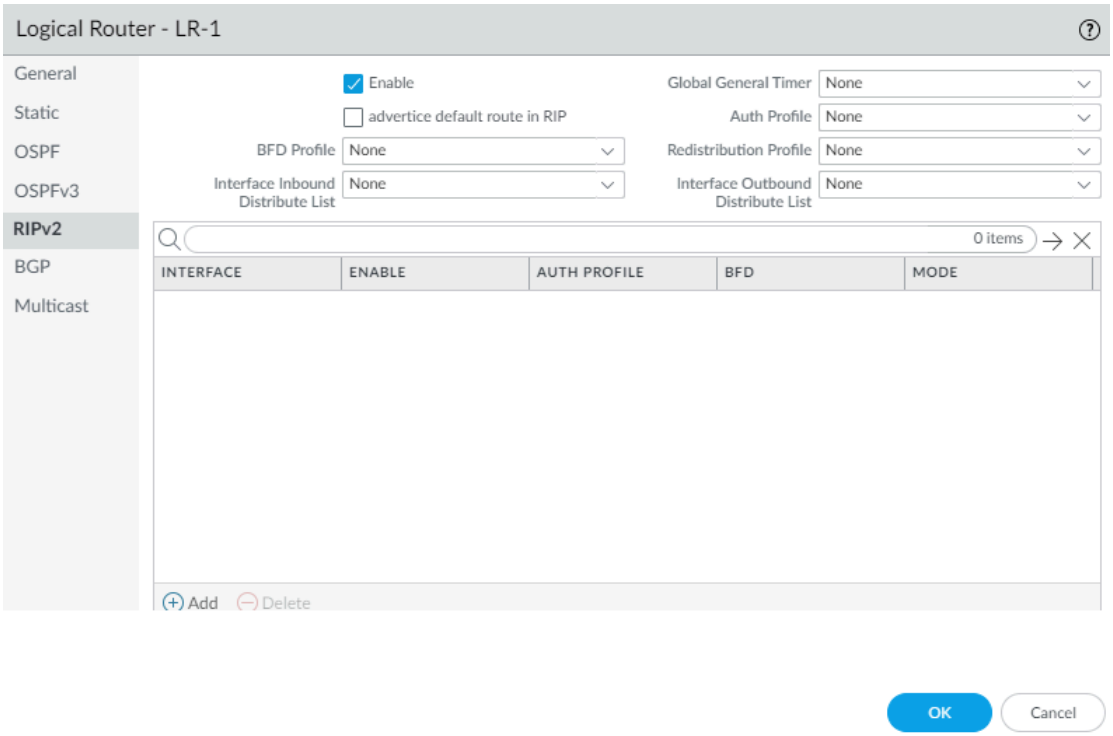
Considérez les profils de routage et les filtres RIPv2 que vous pouvez appliquer à RIPv2 et ainsi gagner du temps de configuration et maintenir la cohérence. Vous pouvez créer des profils et des filtres à l'avance ou lorsque vous configurez RIPv2.

STEP 1 | Configurer un routeur logique.

©2024 Palo Alto Networks, Inc.

STEP 2 | Activez RIPv2 et configurez les paramètres généraux.

1. Sélectionnez **Routeurs logiques** > **routage** > **réseau** et sélectionnez un routeur logique.
2. Sélectionnez **RIPv2** et **activez-le** .

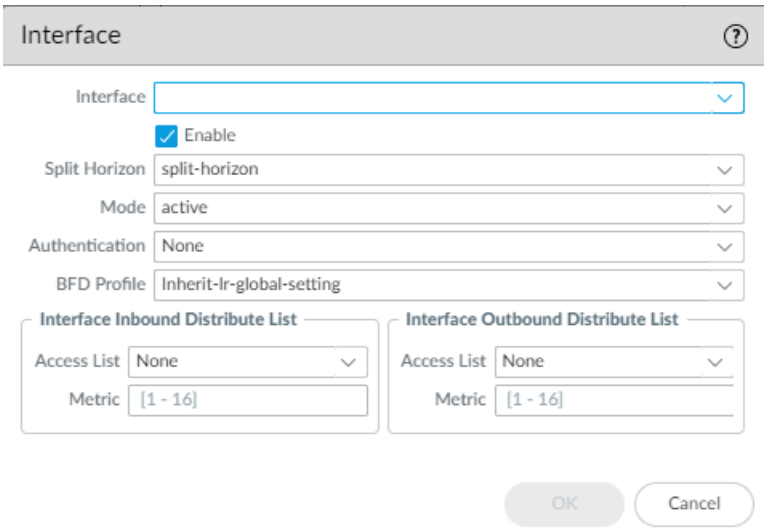


3. Sélectionnez **Publier l'itinéraire par défaut dans RIP** pour publier l'itinéraire par défaut même s'il n'existe pas dans le RIB du moteur de routage.
4. Si vous souhaitez appliquer BFD à RIPv2, sélectionnez un **profil** BFD que vous avez créé, sélectionnez le **profil par défaut** ou créez un nouveau profilBFD. Par défaut **None (disable BFD) (Aucun - BFD désactivé)**.
5. Sélectionnez une **minuterie générale globale** ou créez un nouveau profil de minuterie globale RIPv2.
6. Sélectionnez un **profil d'authentification** ou créez un nouveau profil d'authentification RIPv2.
7. Sélectionnez un **profil de redistribution** ou créez un nouveau profil de redistribution pour redistribuer des itinéraires statiques IPv4, des itinéraires connectés, des itinéraires IPv4 BGP ou des itinéraires OSPFv2 vers RIPv2.
8. Sélectionnez une **liste globale de distribution** entrante pour contrôler les itinéraires entrants acceptés.
9. Sélectionnez une **liste globale de distribution sortante** pour contrôler les itinéraires annoncés aux voisins RIP.

©2024 Palo Alto Networks, Inc.

STEP 3 | Configurez une interface pour RIPv2.

1. **Ajoutez** une **interface** en en sélectionnant une et en l' **activant** .



2. Pour **Split Horizon**, sélectionnez l'une des options suivantes :
   - **split-horizon :**n'annonce pas un itinéraire de retour sur la même interface où il a été reçu.
   - **no-split-horizon :**désactive l'horizon fractionné.
   - **no-split-horizon-with-poison-reverse :**permet à la publicité de revenir sur la même interface où elle a été reçue et définit la métrique pour ces itinéraires sur le maximum autorisé pour RIP, qui est de 16.
3. Sélectionnez le **mode**:
   - **actif :**l'interface annonce les réseaux et envoie des mises à jour RIP.
   - **passif :**l'interface annonce les réseaux, mais n'envoie pas de mises à jour RIP. (Utile s'il n'y a pas de routeurs RIP pour le réseau, et donc aucune raison d'envoyer des mises à jour RIP sur l'interface.)
   - **send-only :**peut être utilisé si le pare-feu est un nœud d'extrémité et que vous souhaitez uniquement publier un préfixe en RIP, mais que vous utilisez des itinéraires statiques ou un itinéraire par défaut pour atteindre des préfixes externes.
4. Sélectionnez un profil d'**authentification** si vous souhaitez remplacer le profil que vous avez appliqué au niveau du routeur logique.
5. Par défaut, l'interface hérite du profil BFD que vous avez appliqué au routeur logique pour RIPv2 (**Inherit-lr-global-setting**). Vous pouvez également sélectionner un autre

©2024 Palo Alto Networks, Inc.

profil BFD,créer un nouveau profil BFD ou sélectionner **Aucun (Désactiver BFD)** pour désactiver BFD pour l'interface.

6. Pour **Interface Inbound Distribute List (Liste de distribution entrante d'interface)**, sélectionnez une **liste d'accès** pour contrôler les itinéraires arrivant à cette interface.
7. Spécifiez la **mesure** appliquée aux itinéraires entrants ; la plage est comprise entre 1 et 16.
8. Pour **Interface Outbound Distribute List (Liste de distribution sortante d'interface)**, sélectionnez une **liste d'accès** pour contrôler les itinéraires annoncés par cette interface aux voisins RIP.
9. Spécifiez la **mesure** à appliquer aux itinéraires annoncés ; la plage est comprise entre 1 et 16.
10. Cliquez sur **OK**.

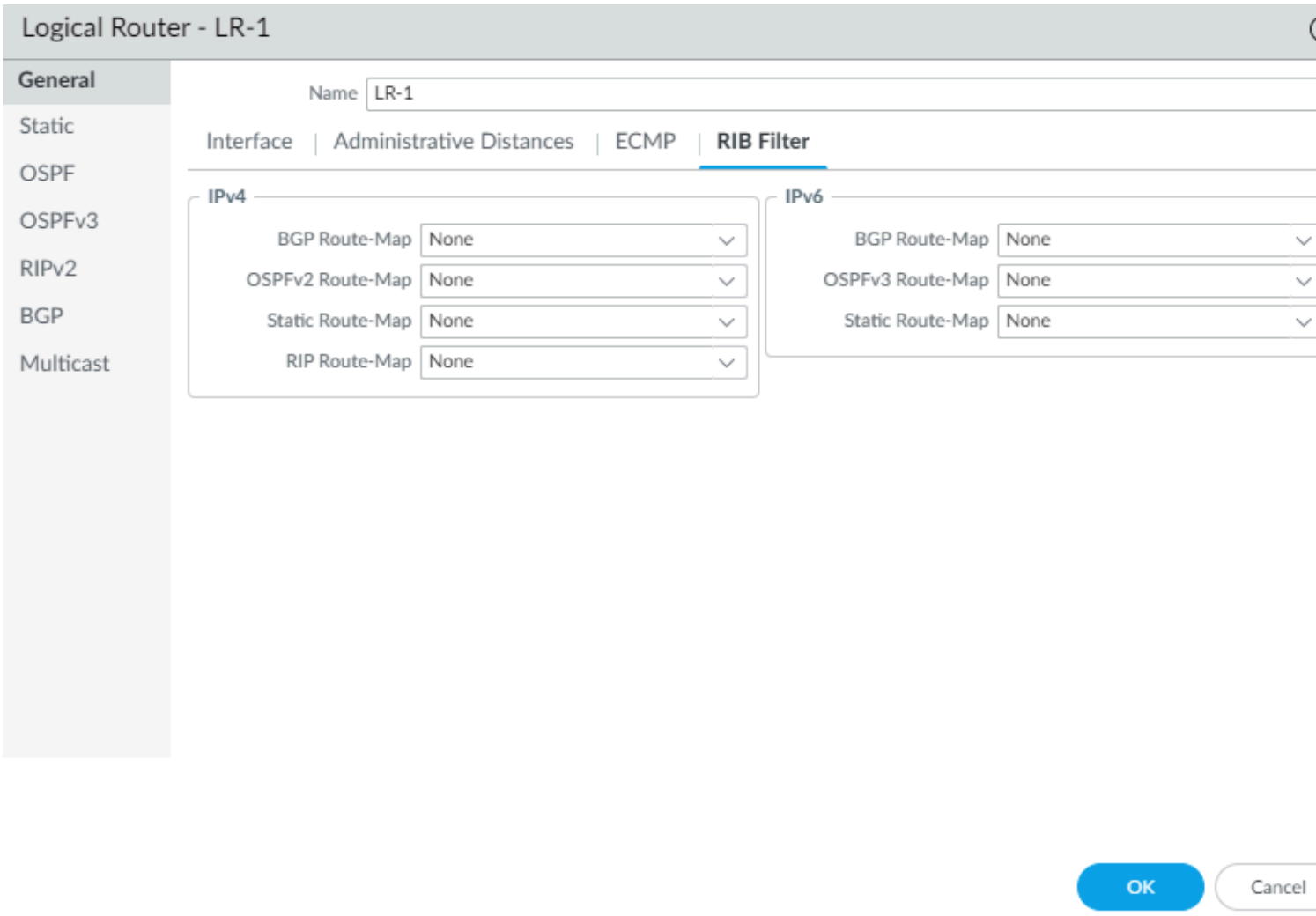
STEP 4 | Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | (Facultatif) Contrôlez les itinéraires RIP placés dans le RIB global.

Vous pouvez apprendre des itinéraires et les redistribuer, mais vous ne les souhaitez pas dans la table de routage locale ou le RIB global du protocole. Vous souhaiterez peut-être ajouter uniquement des itinéraires spécifiques au RIB global.

1. Sélectionnez **Routeurs logiques** > **routage** > **réseau** et sélectionnez un routeur logique.
2. Sélectionnez **Filtre RIB** pour autoriser l'ajout d'itinéraires dans le RIB global ou empêcher l'ajout d'itinéraires à celui-ci.



3. Pour filtrer les itinéraires RIPv2 allant au RIB, dans la zone IPv4, pour **RIP Route-Map, sélectionnez une carte**, d'itinéraire de redistribution ou créez-en une nouvelle.
4. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

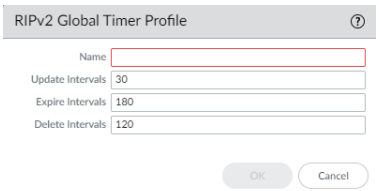
Créer des profils de routage RIPv2

Le moteur de routage avancé prend en charge RIPv2 ; créez les profils suivants à appliquer au protocole. Les profils peuvent être utilisés sur plusieurs routeurs logiques et systèmes virtuels. Cette rubrique décrit les profils et explique comment les configurer.

- **Profils de la minuterie globale RIPv2 :**spécifiez les intervalles de mise à jour, d'expiration et de suppression RIPv2. Appliquez le profil dans la configuration générale RIPv2.
- **Profils d'authentification de l'interface RIPv2** : spécifiez l'authentification RIPv2 à l'aide d'un mot de passe ou md5 ; appliquez le profil dans la configuration générale RIPv2.
- **Profils de redistribution RIPv2** : spécifiez comment redistribuer les itinéraires statiques IPv4, les itinéraires connectés, les itinéraires IPv4 BGP et les itinéraires OSPFv2 vers RIPv2. Appliquez le profil dans la configuration générale RIPv2.

STEP 1 | Créez un profil de minuterie globale RIPv2.

1. Sélectionnez **Réseau** > **Routage** > **Profils de routage** > **RIPv2**.
2. **Ajoutez** un **profil de minuterie globale RIPv2** par **nom** (un maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.



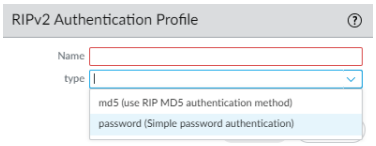
3. Spécifiez **l'intervalle de mise à jour** en secondes, qui correspond à la durée entre les messages de mise à jour planifiées régulièrement ; plage comprise entre 5 et 2 147 483 647 ; la valeur par défaut est 30.
4. Spécifiez **l'intervalle d'expiration** en secondes, qui correspond à la durée pendant laquelle un itinéraire peut se trouver dans la table de routage sans être mis à jour ; la plage est comprise entre 5 et 2 147 483 647 ; la valeur par défaut est 180. Une fois l'intervalle d'expiration atteint, l'itinéraire est toujours inclus dans les messages de mise à jour jusqu'à ce que l'intervalle de suppression soit atteint.
5. Spécifiez **Supprimer l'intervalle** en secondes ; la plage est comprise entre 5 et 2 147 483 647 ; la valeur par défaut est 120. Lorsqu'un itinéraire expiré dans la table de routage atteint l'intervalle de suppression, il est supprimé de la table de routage.
6. Cliquez sur **OK**.

STEP 2 | Créez un profil d'authentification RIPv2

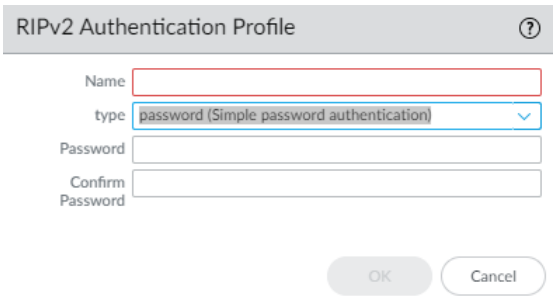
1. Sélectionnez **Réseau** > **Routage** > **Profils de routage** > **RIPv2**.
2. **Ajoutez** un **profil d'authentification RIPv2** par **nom** (un maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou

 ©2024 Palo Alto Networks, Inc.

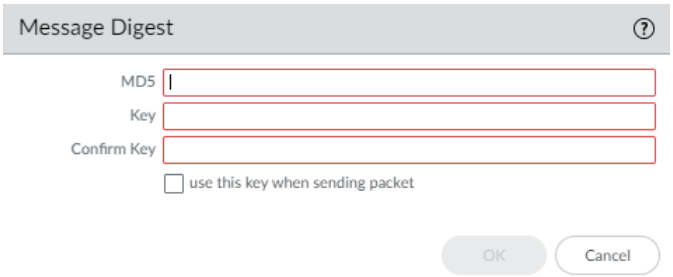
un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.



3. Spécifiez le **type** d'authentification : **md5 (utiliser la méthode d'authentification RIP MD5)** ou **mot de passe (authentification par mot de passe simple)**.
4. Pour **Authentification par mot de passe simple**, entrez le **mot de passe** (un maximum de 16 caractères) et **Confirmer le mot de passe**.



5. Pour **l'authentification RIP MD5** :
   - **Ajoutez** un ID de clé MD5 ; la plage est comprise entre 0 et 255.
   - Entrez la **clé** (un maximum de 16 caractères alphanumériques) et la **clé de confirmation**.
   - Sélectionnez **Utiliser cette clé lors de l'envoi de paquet** pour faire de cette clé la clé préférée.



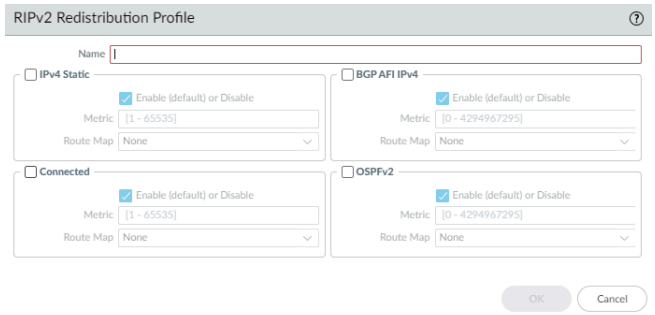
6. Cliquez sur **OK**.

STEP 3 | Créez un profil de redistribution RIPv2 pour spécifier n'importe quelle combinaison d'itinéraires statiques IPv4, d'itinéraires connectés, d'itinéraires IPv4 BGP et d'itinéraires OSPFv2 à redistribuer à RIPv2.

1. Sélectionnez **Réseau** > **Routage** > **Profils de routage** > **RIPv2**.
2. **Ajoutez** un **profil de redistribution RIPv2** par **nom** (un maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou

 ©2024 Palo Alto Networks, Inc.

un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.



3. Sélectionnez **IPv4 statique** pour autoriser la configuration de cette partie du profil.
   - **Activez** la partie de redistribution statique IPv4 du profil.
   - Saisissez la **mesure** à appliquer aux itinéraires statiques qui sont redistribués dans BGP (plage de 1 à 65 535).
   - Sélectionnez une **carte d'itinéraires redistribués** ou créez une nouvelle carte d'itinéraires redistribués dont les critères de correspondance contrôlent les itinéraires statiques IPv4 à redistribuer dans RIPv2. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
4. Sélectionnez **Connecté** pour autoriser la configuration de cette partie du profil.
   - **Activez** la partie de redistribution d'itinéraire connecté du profil.
   - Saisissez la **mesure** à appliquer aux itinéraires connectés qui sont redistribués dans BGP (plage de 1 à 65 535).
   - Sélectionnez une **carte d'itinéraires redistribués** ou créez une nouvelle carte d'itinéraires redistribués. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
5. Sélectionnez **BGP AFI IPv4** pour autoriser la configuration de cette partie du profil.
   - **Activez** la partie de redistribution d'itinéraire IPv4 BGP du profil.
   - Spécifiez la **mesure** à appliquer aux itinéraires BGP redistribuée en RIPv2 (la plage est comprise entre 0 et 4 294 967 295).
   - Sélectionnez une **carte d'itinéraires redistribués** ou créez une nouvelle carte d'itinéraires redistribués. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de

©2024 Palo Alto Networks, Inc.

métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.

6. Sélectionnez **OSPFv2** pour autoriser la configuration de cette partie du profil.
   - **Activez** la partie de redistribution d'itinéraire OSPFv2 du profil.
   - **Activez** la partie de redistribution d'itinéraire par défaut IPv4 du profil.
   - Spécifiez la **mesure** à appliquer à l'itinéraire par défaut redistribué dans RIPv2 (plage comprise entre 0 et 4 294 967 295).
   - Sélectionnez une **carte d'itinéraires redistribués** ou créez une nouvelle carte d'itinéraires redistribués. La valeur par défaut est **Aucun**. Si la configuration de l'ensemble de cartes d'itinéraires inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
7. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

Créer des profils BFD

Sur un moteur de routage avancé, vous pouvez utiliser des profils de détection de transfert bidirectionnel (BFD) pour appliquer facilement les paramètres BFD à un itinéraire statique ou à un protocole de routage. Vous pouvez utiliser le profil par défaut (qui est en lecture seule) ou créer de nouveaux profils BFD.

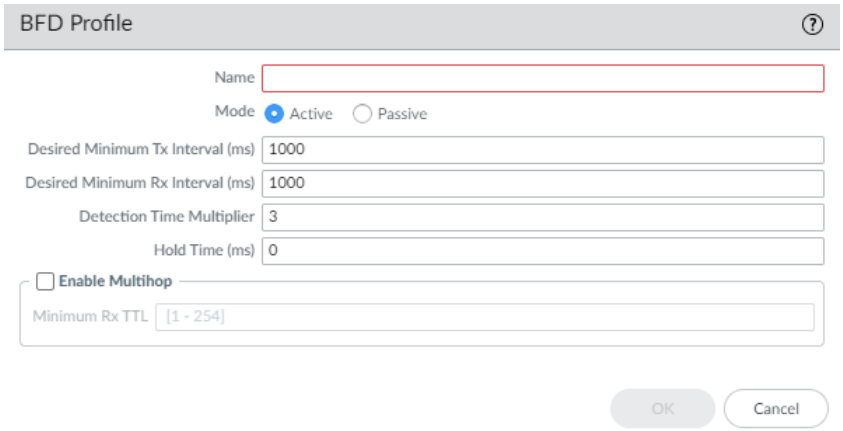
Procédez comme suit avant de créer un profil BFD :

- Configurer un routeur logique.
- Configurez un ou plusieurs itinéraires statiques si vous appliquez la BFD aux itinéraires statiques.
- Configurez un protocole de routage (**BGP**, **OSPF**, **OSPFv3** ou **RIv2P)** si vous appliquez la BFD à un protocole de routage. Par exemple, vous pouvez appliquer un profil BFD lors de la configuration des paramètres BGP généraux.

L'efficacité de votre implémentation BFD repose sur plusieurs facteurs, tels que le volume du trafic, les conditions du réseau, le caractère agressif de vos paramètres BFD et la charge de votre plan de données.

STEP 1 | Sélectionnez **Réseau** > **Routage** > **Profils de routage** > **BFD**.

STEP 2 | **Ajoutez** un profil BFD par **Nom** (63 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique sur le pare-feu. N'utilisez que des lettres, chiffres, traits d'union et traits de soulignement. Aucun point (.) ou espace n'est autorisé.



STEP 3 | Sélectionnez le **Mode (Mode)** sous lequel la BFD fonctionne :

- **Active (Actif)** : la BFD initie l'envoi de paquets de contrôle vers l'homologue (par défaut). Au moins l'un des homologues BFD doit être actif ; ils peuvent être actifs tous les deux.
- **Passive (Passif)** : la BFD attend que l'homologue envoie des paquets de contrôles et réponde comme il se doit.

STEP 4 | Saisissez **Intervalle Tx minimal désiré (en ms)**, Il s'agit de l'intervalle minimal, en millisecondes, auquel vous voulez que le protocole BFD envoie des paquets de contrôles BFD ; vous négociez ainsi l'intervalle de transmission avec l'homologue. La plage des pare-

 ©2024 Palo Alto Networks, Inc.

feux des séries PA-7000, PA-5200 et PA-5450 est de 50 à 10 000 ; la plage pour la série PA-3200 est de 100 à 10 000 ; la plage pour la série VM est de 200 à 10 000. La valeur par défaut est 1 000.

*Si vous disposez de plusieurs protocoles de routage qui utilisent des profils BFD différents sur la même interface, configurez les profils BFD avec le même **Desired Minimum Tx Interval (Intervalle de transmission minimum souhaité)**.*

Sur un pare-feu PA-7000 réglez l'Intervalle Tx minimal désiré sur sur 100 ou une valeur plus grande ; une valeur inférieure à 100 risquerait de causer des battements BFD.

STEP 5 | Saisissez le **Required Minimum Tx Interval (ms) (Intervalle de transmission minimum requis (ms))**. Il s'agit de l'intervalle minimum (en millisecondes) auquel la BFD peut recevoir les paquets de contrôles BFD. La plage des pare-feux des séries PA-7000, PA-5200 et PA-5450 est de 50 à 10 000 ; la plage pour la série PA-3200 est de 100 à 10 000 ; la plage pour la série VM est de 200 à 10 000. La valeur par défaut est 1 000.

Sur un pare-feu de la série PA-7000, définissez l'intervalle Rx minimum souhaité sur 100 ou plus ; une valeur inférieure à 100 risque de provoquer des volets BFD.

STEP 6 | Saisissez le **Detection Time Multiplier (Multiplicateur de délai de détection)**. La plage est comprise entre 2 et 255 ; la valeur par défaut est 3.

Le système local calcule le délai de détection en tant que **Multiplicateur de délai de détection** reçu du système distant multiplié par l'intervalle de transmission du système distant convenu (la valeur la plus élevée entre le **Intervalle de réception minimum requis** et le dernier **Intervalle de transmission minimum souhaité)** reçu. Si la BFD ne reçoit pas de paquet de contrôles BFD de son homologue avant l'expiration du délai de détection, c'est qu'un échec a eu lieu.

Lors de la configuration d'un profil BFD, tenez compte du fait que le pare-feu est un périphérique basé sur une session qui se trouve généralement en périphérie d'un réseau ou d'un centre de données et dont les liaisons peuvent être plus lentes que celles d'un routeur dédié. Par conséquent, il est fort probable que le pare-feu devra disposer d'un intervalle plus long et d'un multiplicateur plus élevé que les paramètres les plus rapides permis. Un délai de détection qui est trop court peut entraîner de fausses détections d'échec liées à la congestion du trafic.

STEP 7 | Saisissez le **Hold Time (ms) (temps d'attente)**, Il s'agit du délai, en millisecondes, entre l'apparition d'une liaison et la transmission des paquets de contrôles BFD par la BFD. Le **Hold Time (Temps d'attente)** ne s'applique qu'au mode **Actif** de la BFD. Si la BFD reçoit des paquets de contrôles BFD pendant le Hold Time (Temps d'attente), ceux-ci sont ignorés. Le paramètre défini par défaut de 0 signifie qu'aucun **Hold Time (Temps d'attente)** n'est utilisé ; le pare-feu envoie et reçoit les paquets de contrôles BFD immédiatement après l'établissement de la liaison.

STEP 8 | Saisissez la **Minimum Rx TTL (TTL de réception minimum)**. Il s'agit du Time-to-Live (Durée de vie ; TTL) minimal (nombre de sauts) que la BFD acceptera (recevra) dans un paquet de

 ©2024 Palo Alto Networks, Inc.

contrôles BFD lorsque le protocole BGP prend en charge la BFD à sauts multiples. La plage est de 1 à 254 ; il n'y a pas de valeur par défaut.

Le pare-feu abandonne le paquet s'il reçoit une TTL inférieure à la **Minimum Rx TTL (TTL de réception minimum)** qui a été configurée. Par exemple, si l'homologue se trouve à cinq sauts et qu'il transmet au pare-feu un paquet BFD ayant une TTL de 100, et que la **Minimum Rx TTL (TTL de réception minimum)** du pare-feu est de 96 ou plus, le pare-feu abandonne le paquet.

STEP 9 | Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

Configurer la multidiffusion IPv4

Le moteur de routage avancé prend en charge la multidiffusion IPv4 pour un routeur logique. Vous devez être familier avec les concepts Multidiffusion IP, IGMP, et PIM.

La multidiffusion IPv4 sur un moteur de routage avancé prend en charge des fonctionnalités non prises en charge sur le moteur de routage hérité :

- Jointure statique IGMP, qui est la possibilité de spécifier un récepteur IGMPv3 ou IGMPv2 statique sur une interface. Le message de jointure PIM correspondant est envoyé en amont.
- La multidiffusion indépendante du protocole (PIM) prend en charge les modes de recherche RPF (Reverse-Path Forwarding) : MRIB uniquement, URIB uniquement et MRIB-then-URIB.

La multidiffusion IPv4 ne prend pas en charge IGMPv1.

Lorsque vous configurez la multidiffusion IPv4, vous Créer des profils de routage multidiffusion devez utiliser des minuteries d'interface PIM et des requêtes d'interface IGMP pour rendre votre configuration plus facile et cohérente. Vous pouvez créer des cartes de routage de multidiffusion pour contrôler les autorisations de groupe PIM.

Vous pouvez également Créer un MRoute IPv4 si vous souhaitez que le trafic de monodiffusion emprunte un itinéraire différent du trafic de multidiffusion.

STEP 1 | Configurer un routeur logique.

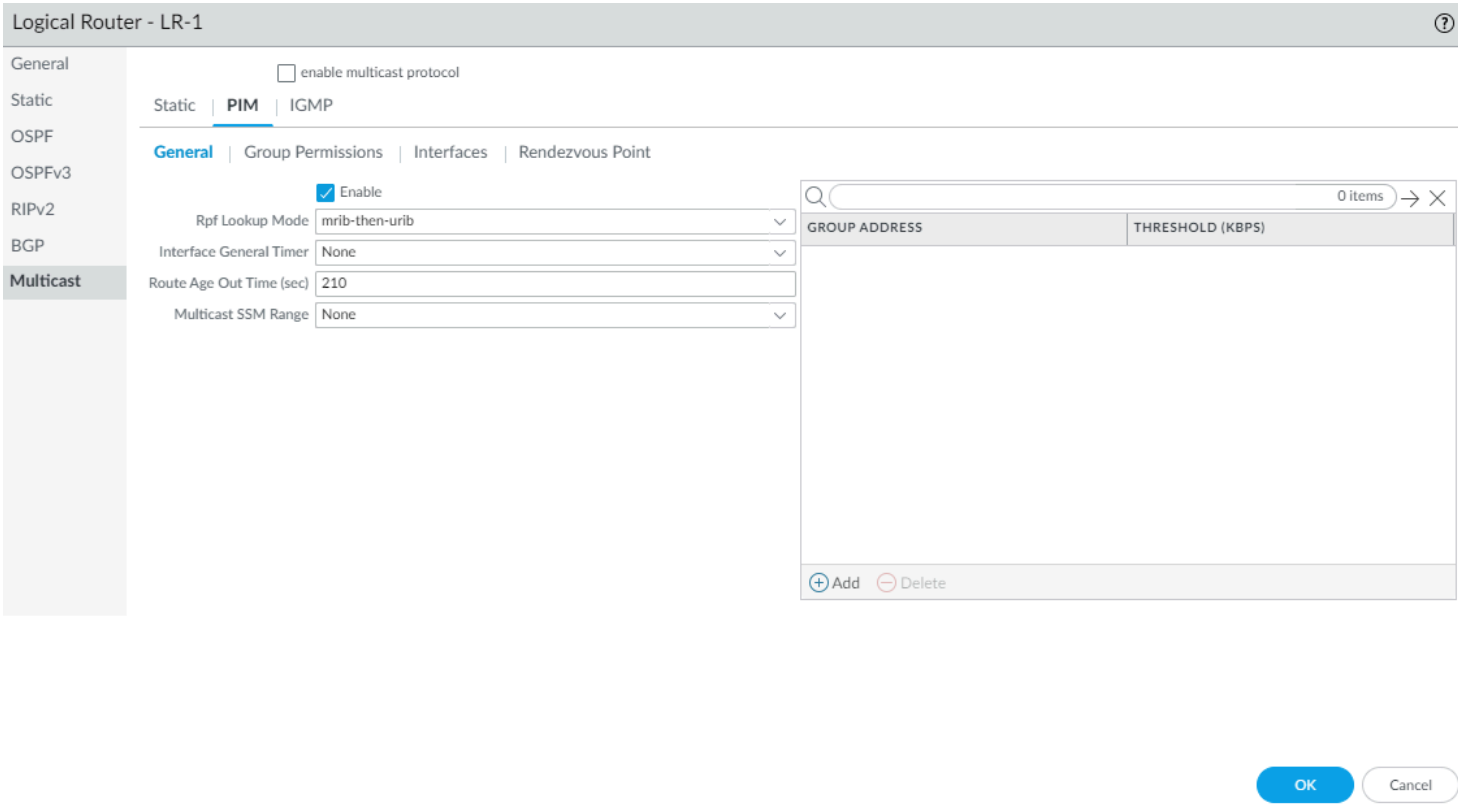
STEP 2 | Sélectionnez **Routeurs logiques** > **routage** > **réseau** et sélectionnez un routeur logique.

STEP 3 | Sélectionnez **Multidiffusion** et **activez le protocole de multidiffusion**.

©2024 Palo Alto Networks, Inc.

STEP 4 | Configurez les paramètres PIM généraux pour le routeur logique.

1. Sélectionnez **PIM** > **Général** et **Activer** PIM.



2. Sélectionnez le **mode de recherche RPF**, qui détermine où le routeur logique cherche à trouver l'interface sortante pour atteindre l'adresse source contenue dans le paquet de multidiffusion. Si l'interface sortante stockée dans le RIB correspond à l'interface sur laquelle le paquet de multidiffusion est arrivé, le routeur logique accepte et transfère le paquet ; sinon, il laisse tomber le paquet.
   - **mrib uniquement :**regardez dans le RIB multidiffusion uniquement.
   - **mrib-then-urib :**regardez d'abord dans le RIB de multidiffusion ; si l'itinéraire n'est pas présent dans le RIB de multidiffusion, regardez dans le RIB de monodiffusion.
   - **urib-only :**regardez dans le RIB unicast uniquement.

   Le **mode de recherche RPF** contrôle également où effectuer la recherche d'itinéraire pour sélectionner l'itinéraire à utiliser pour la jointure PIM.
3. Pour le **minuteur général de l'interface**sélectionnez un **profil de minuteur d'interface PIM** ou créez un nouveau profil de minuteur d'interface PIM IPv4 ; la valeur par défaut est **Aucun**.
4. Spécifiez le **temps d'expiration de l'itinéraire (sec)**: le nombre de secondes pendant lesquelles un itinéraire de multidiffusion reste dans la mRIB après la fin de la session entre un groupe de multidiffusion et une source ; la plage est comprise entre 210 et 7 200 ; la valeur par défaut est 210.
5. Pour configurer la multidiffusion spécifique à la source (SSM), dans **Plage SSM de multidiffusion**, sélectionnez une liste de préfixes (ou créez-en une nouvelle) qui spécifie

©2024 Palo Alto Networks, Inc.

les adresses sources autorisées à fournir le trafic de multidiffusion au récepteur ; la valeur par défaut est **Aucun (pas de liste de préfixes).**

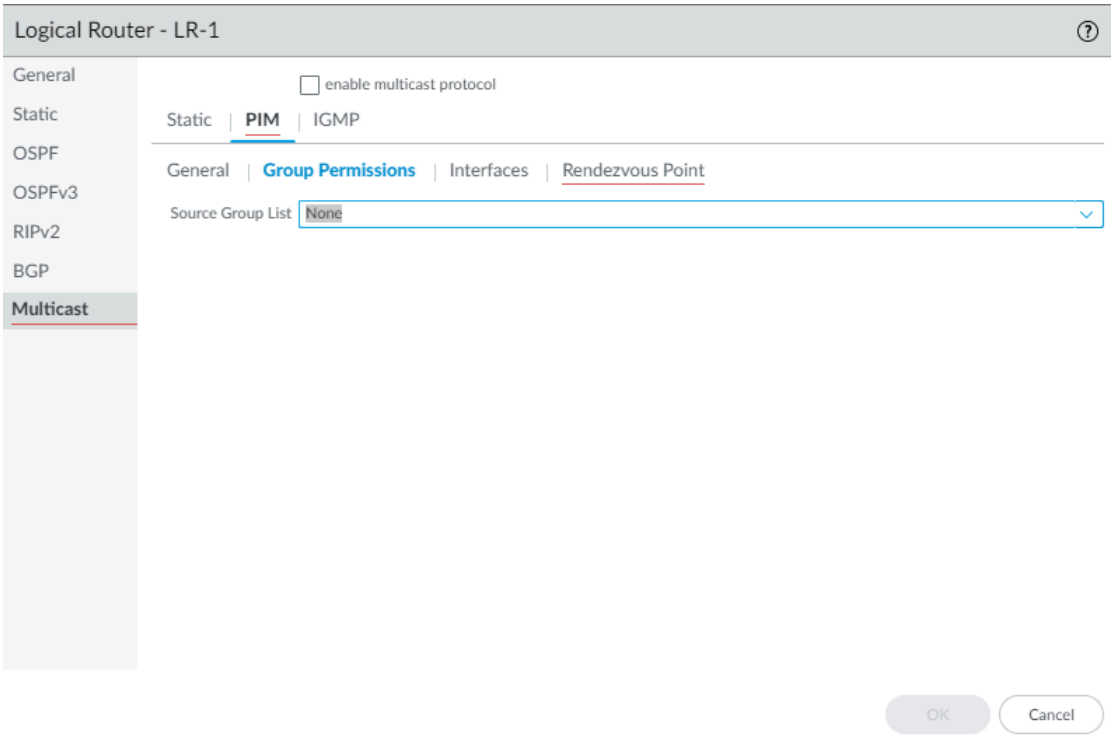
6. Pour configurer le seuil de l'arborescence spt (Shortest-Path Tree) pour un groupe ou un préfixe de multidiffusion, **Ajoutez** une **adresse de groupe** (groupe de multidiffusion ou préfixe pour lequel vous spécifiez l'arborescence de distribution) en sélectionnant une Liste de préfixes ou en en créant une nouvelle.
7. Spécifiez le débit de **seuil** en kilobits par seconde (kbps) ; si le trafic de multidiffusion pour le groupe/préfixe de multidiffusion arrive au routeur logique plus rapidement que ce taux de seuil, le routage vers le groupe/préfixe spécifié passe de l'arborescence partagée (provenant du point de rendez-vous [RP]) à la distribution SPT :
   - **0 (switch on first data packet) (commuter au premier paquet de données)** (par défaut) : la routeur virtuel bascule de l'arborescence partagée à une distribution en arborescence source pour le groupe ou le préfixe lorsque le routeur virtuel reçoit le premier paquet de données du groupe ou du préfixe.
   - Saisissez le nombre total de kilobits provenant des paquets multicast qui peuvent arriver pour le préfixe ou le groupe multicast à toute interface sur une période de temps déterminée, à quel moment le routeur virtuel bascule vers une distribution en arborescence source pour ce groupe ou préfixe multidiffusion.
   - **never (do not switch to spt) (jamais (ne pas basculer vers SPT))** : le routeur virtuel continue d'utiliser l'arborescence partagée pour transférer les paquets vers le groupe ou le préfixe.

STEP 5 | Spécifiez les autorisations de groupe PIM pour contrôler les messages de jointure PIM et les messages d'enregistrement acceptés par le routeur logique et le trafic de multidiffusion que le routeur logique transfère.

1. Sélectionnez **Autorisations de groupe PIM** > **.**
2. Pour contrôler les paquets vers certains groupes de multidiffusion de destination à partir de certaines sources (S, G) afin de transiter le routeur logique, pour **Liste des groupes sources**, sélectionnez une liste d'accès que vous avez créée ou créez-en une nouvelle. La liste d'accès peut être une liste d'accès étendue dans laquelle la source spécifie la

 ©2024 Palo Alto Networks, Inc.

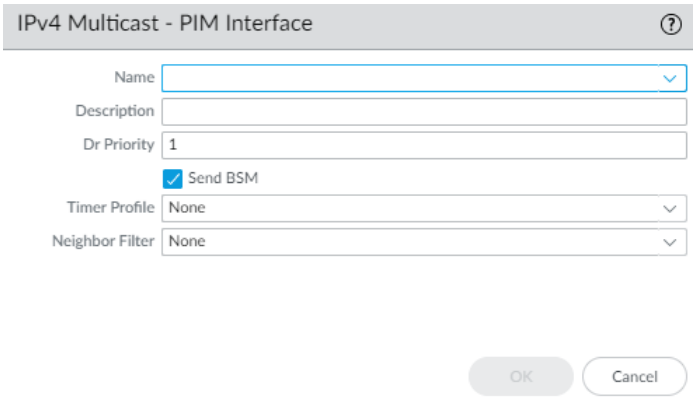
source de multidiffusion et la destination spécifie le groupe de multidiffusion. La valeur par défaut est **Aucun (pas de liste d'accès).**



Lorsque vous modifiez les autorisations de groupe PIM en supprimant ou en modifiant la liste d'accès du groupe source, la nouvelle autorisation n'efface pas rétroactivement les routes de multidiffusion de la table RIB de multidiffusion (mRIB) ou de la table FIB de multidiffusion (mFIB) pour les flux existants. Pour modifier les entrées des flux existants dans le mRIB ou le mFIB, vous devez forcer une entrée Leave ou clear mroute.

STEP 6 | Configurez les caractéristiques PIM d'une interface.

1. Sélectionnez **Interfaces PIM** et **Ajoutez** une interface par **nom**.



2. Entrez une **Description** utile de l'interface.
3. Spécifiez la **priorité DR** (priorité du routeur désigné) de l'interface pour contrôler quel routeur transfère les messages de jointure PIM, les messages de registre PIM et les

 ©2024 Palo Alto Networks, Inc.

messages d'élagage au point de rendez-vous (RP) ; la plage est comprise entre 1 et 4 294 967 295 ; la valeur par défaut est 1. Parmi les périphériques PIM sur un réseau local, si la priorité de reprise après sinistre est configurée, le périphérique ayant la valeur de priorité la plus élevée est élu DR.

4. **Envoyer BSM** pour permettre la propagation des messages Bootstrap (activé par défaut).

   Le Moteur de routage avancé ne peut pas agir en tant que BSR, mais peut envoyer et relayer des messages BSM.

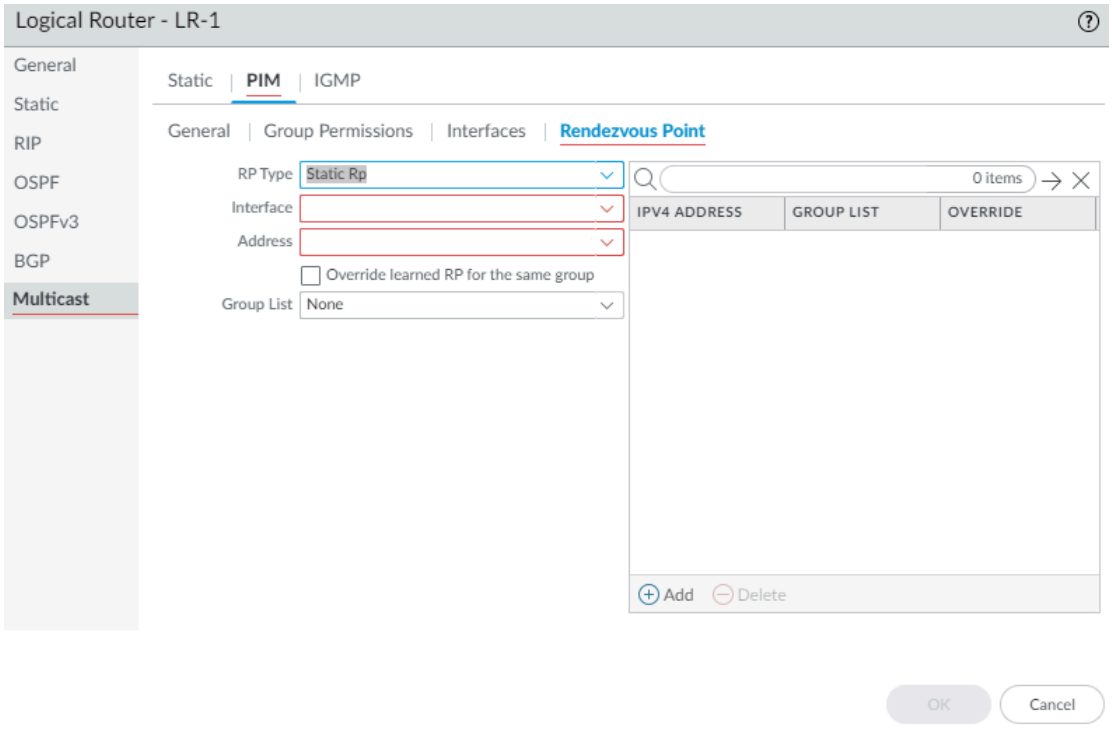
5. Le **profil de minuteur** de l'interface est hérité de la section PIM général, sauf si vous le remplacez en sélectionnant un profil de minuteur d'interface PIM IPv4 ; la valeur par défaut est **Aucun**.
6. Spécifiez un **filtre voisin** à l'aide d'une liste d'accès que vous avez créée ou créez une nouvelle liste d'accès pour spécifier les préfixes des périphériques autorisés ou refusés de devenir des voisins PIM du routeur logique.
7. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | (ASM uniquement) Configurez un point de rendez-vous PIM (RP) pour un environnement de multidiffusion toute source (ASM).

Vous pouvez configurer un RP candidat et un RP statique ; ils ne s'excluent pas mutuellement.

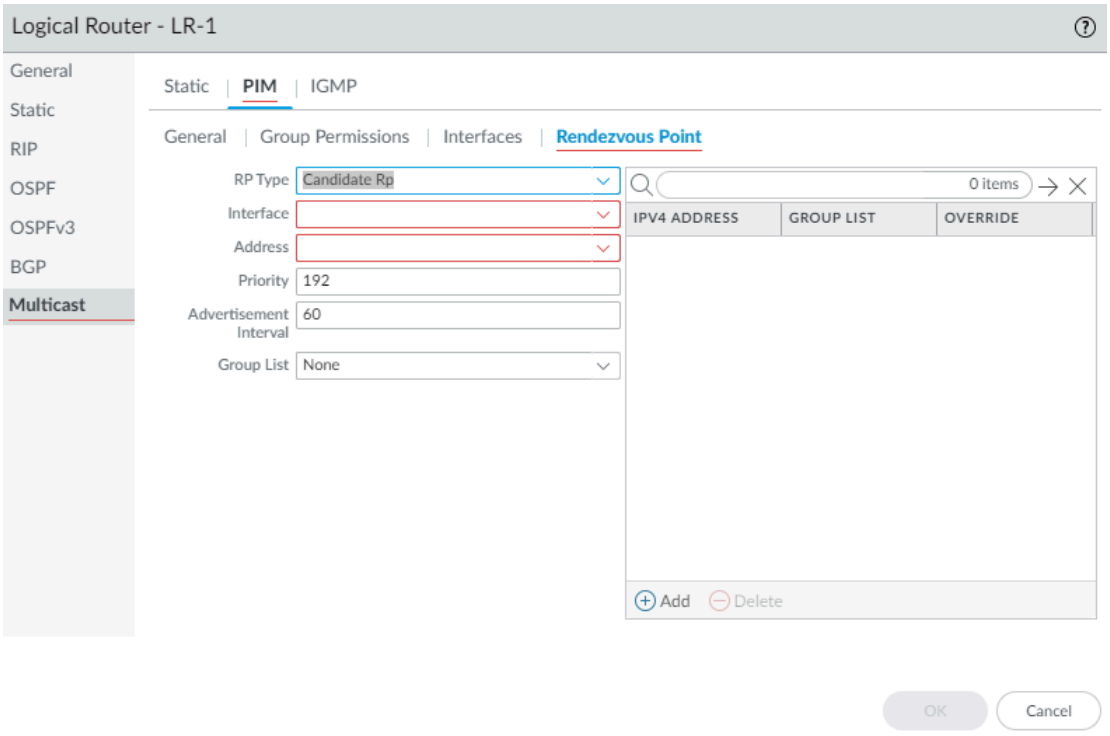
1. Sélectionnez **Point de rendez-vous PIM** > **.**
2. Sélectionnez le **type RP** local : **RP statique** ou **RP candidat** ; la valeur par défaut est **Aucun**.
3. Si vous choisissez **RP statique**, cela établit un mappage statique d'un RP vers des groupes de multidiffusion. Vous devez configurer explicitement le même RP sur les autres routeurs PIM du domaine PIM. Configurez les paramètres suivants :
   - Sélectionnez l'**interface** RP où le RP reçoit et envoie des paquets de multidiffusion. Les types d'interface valides sont les interfaces Layer3 (qui incluent Ethernet, VLAN, loopback, Aggregate Ethernet (AE), tunnel et sous-interfaces).
   - Sélectionnez l'**adresse** de l'interface ; les adresses IP de l'interface que vous avez sélectionnée remplissent la liste.
   - Sélectionnez **Override learned RP for the same group (Écraser le RP appris pour le même groupe)** pour que ce RP agisse en tant que RP au lieu du RP choisi pour les groupes qui figurent dans la liste des groupes.
   - Spécifiez la **liste de groupes** de multidiffusion pour lesquels le RP statique agit en tant que RP en sélectionnant une liste d'accès ou en créant une nouvelle liste d'accès. La valeur par défaut est **Aucun (pas de liste d'accès).**



4. Si vous choisissez **Candidat RP**:

©2024 Palo Alto Networks, Inc.

- Sélectionnez l'**interface** où le RP candidat reçoit et envoie des paquets de multidiffusion. Les types d'interface valides sont les interfaces Layer3 (qui incluent Ethernet, VLAN, loopback, Aggregate Ethernet (AE), tunnel et sous-interfaces).
- Sélectionnez l'**adresse** de l'interface.
- Spécifiez la **priorité** du RP candidat ; la plage est comprise entre 0 et 255 ; la valeur par défaut est 192. Une valeur de priorité inférieure indique une priorité plus élevée.
- Spécifiez l'**intervalle de publication**, la fréquence (en secondes) à laquelle le RP candidat envoie des publicités à d'autres routeurs ; la plage est comprise entre 1 et 26 214 ; la valeur par défaut est 60.
- Pour contrôler les groupes que le RP candidat accepte, sélectionnez une **liste de groupes**, qui est une liste d'accès IPv4 que vous avez créée, ou créez une nouvelle liste d'accès. La valeur par défaut est **Aucun (pas de liste d'accès).** Si aucune liste d'accès n'est appliquée, le routeur logique commence à se présenter comme le RP pour tous les groupes.



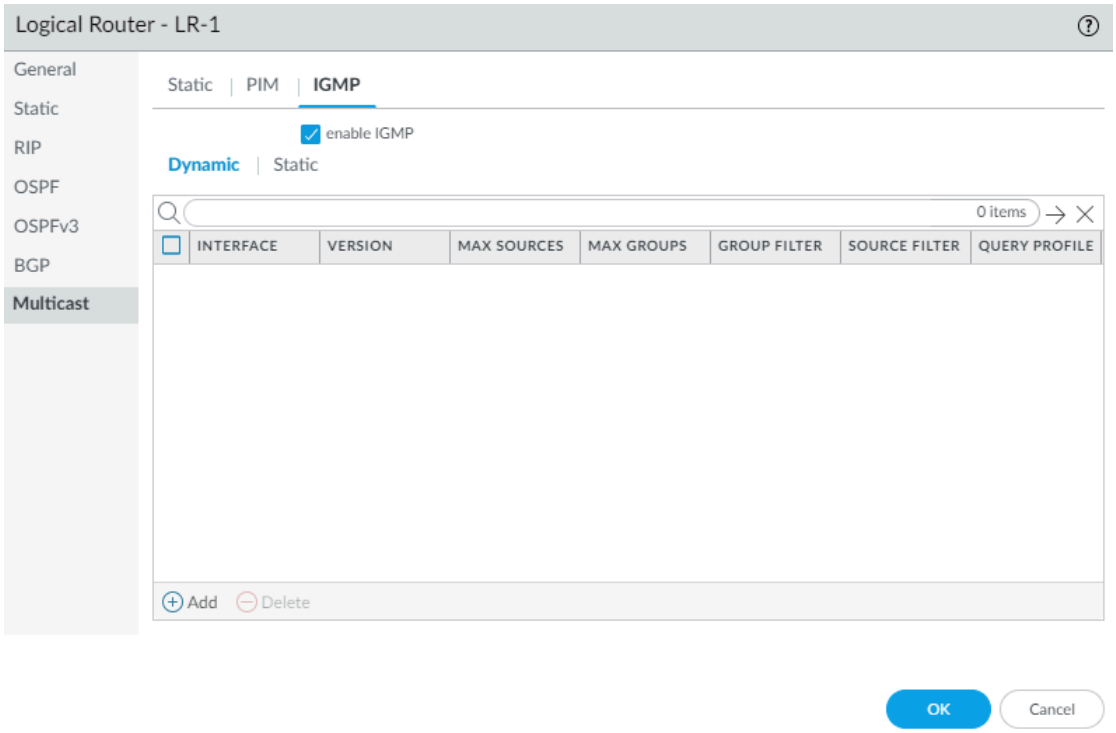
5. **Ajoutez** une **adresse IPv4** du RP distant (externe).
6. Sélectionnez une **liste de groupes** pour spécifier les groupes de multidiffusion pour lesquels le RP distant agit en tant que RP ou créez une nouvelle liste d'accès. La valeur par défaut est **Aucun (pas de liste d'accès).**
7. Sélectionnez **Remplacer** si vous souhaitez que le RP distant que vous avez configuré statiquement serve de RP au lieu d'un RP qui est appris dynamiquement (élu) pour les groupes de la liste des groupes.
8. Cliquez sur **OK**.

STEP 8 | Cliquez sur **OK** pour enregistrer les paramètres PIM.

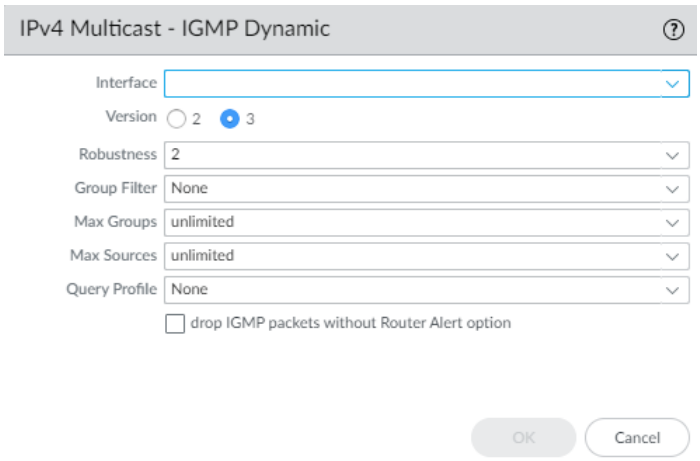
 ©2024 Palo Alto Networks, Inc.

STEP 9 | Configurez IGMP uniquement sur les interfaces qui sont orientées vers un récepteur multidiffusion.

1. Sélectionnez **IGMP** et **activez IGMP**.



2. Pour configurer une interface IGMP dynamique, sélectionnez **Dynamique**.
   1. **Ajoutez** une **interface** en en sélectionnant une dans la liste.



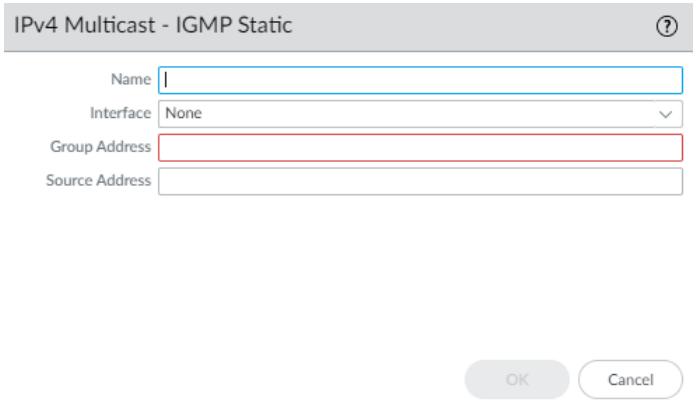
   2. Sélectionnez la **version** IGMP : **2** ou **3**.
   3. Sélectionnez la valeur **Robustesse** dans la plage 1 à 7 ; la valeur par défaut est 2.

 ©2024 Palo Alto Networks, Inc.

*Le (Robustness * QueryInterval) + MaxQueryResponseTime détermine la durée de validité d'un message join sur le routeur logique. Si le routeur logique reçoit un message Leave Group, Robustness * LastMemberQueryInterval est la durée pendant laquelle le routeur logique attend avant de supprimer l'entrée Leave Group. Augmentez la valeur robustesse si le sous-réseau sur lequel se trouve ce routeur logique est susceptible de perdre des paquets. Pour les messages de jointure, une valeur de robustesse de 1 est ignorée. Pour les messages Leave Group, le routeur logique utilise également la valeur Robustness comme nombre de requêtes du dernier membre.*

4. Pour **Filtre de groupe**, sélectionnez une liste d'accès ou créez une nouvelle liste d'accès pour contrôler les sources et les groupes pour lesquels l'interface acceptera les jointures IGMP ; la valeur par défaut est **Aucun (pas de liste d'accès).**
5. Pour **Groupes max**, entrez le nombre maximal de groupes qu'IGMP peut traiter simultanément pour l'interface. La plage est de 1 à 65 535; la valeur par défaut est **illimitée**, ce qui signifie la valeur la plus élevée de la plage.
6. Pour **Max Sources**, entrez le nombre maximal de sources qu'IGMP peut traiter simultanément pour l'interface. La plage est de 1 à 65 535; la valeur par défaut est **illimitée**, ce qui signifie la valeur la plus élevée de la plage.
7. Pour **Profil de requête**, sélectionnez un profil de requête d'interface IGMP que vous avez créé ou créez-en un nouveau à appliquer à l'interface ; la valeur par défaut est **Aucun**.
8. Sélectionnez l'option **Supprimer les paquets IGMP sans alerte de routeur** pour exiger que les paquets IGMPv2 ou IGMPv3 entrants aient l'option, d'alerte de routeur IP, RFC 2113, sinon ils seront supprimés. (La valeur par défaut est désactivée.)
9. Cliquez sur **OK** pour enregistrer l'interface IGMP dynamique.

3. Pour configurer une interface IGMP statique, sélectionnez **Statique**.
   1. **Ajoutez** une interface statique par **Nom**.



   2. Sélectionnez l'**interface** comme interface IGMP statique.
   3. Entrez l'**adresse du groupe de multidiffusion** des membres IGMP statiques.
   4. Entrez l'**adresse source** de l'expéditeur transmettant le trafic de multidiffusion au groupe de multidiffusion (S,G). Le trafic pour cette combinaison (S,G) est autorisé sur l'interface IGMP statique.
   5. Cliquez sur **OK** pour enregistrer l'interface IGMP statique.

 ©2024 Palo Alto Networks, Inc.

STEP 10 | Cliquez sur **OK** pour enregistrer la configuration multidiffusion.

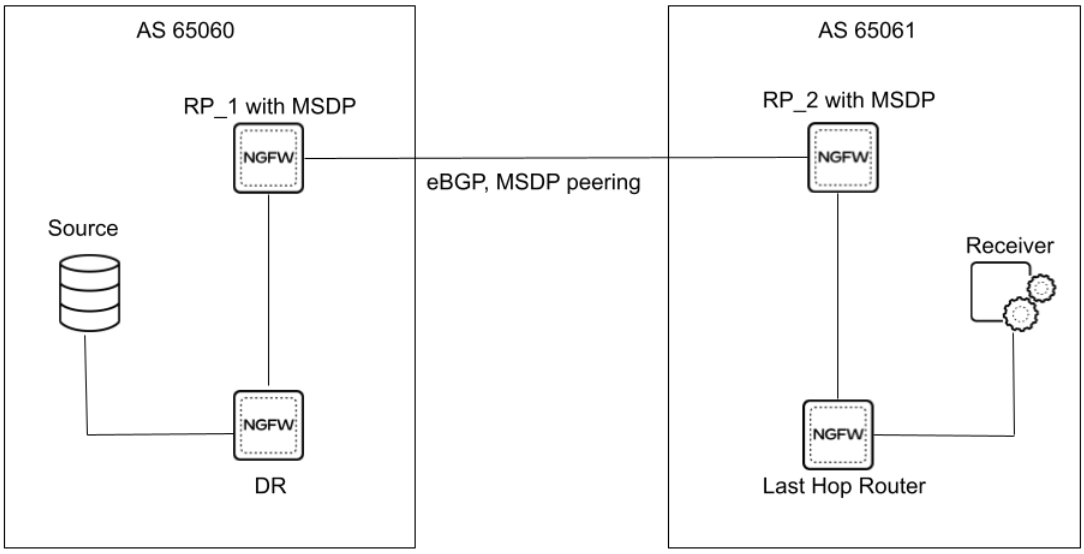
STEP 11 | **Commit** (Valider).

 ©2024 Palo Alto Networks, Inc.

Configurer MSDP

Le mode de routage avancé prend en charge le protocole MSDP (Multicast Source Discovery Protocol) en mode PIM Sparse (PIM-SM). Pare-feux compatibles MSDP dans un pair de domaine avec des périphériques compatibles MDSP dans un domaine différent ou un système autonome. Les pairs échangent des informations de contrôle et découvrent des sources de multidiffusion en dehors de leur propre domaine. MSDP suit les sources actives et les partage avec les pairs configurés. MSDP réduit la complexité de l'interconnexion de plusieurs domaines PIM-SM en permettant aux domaines d'utiliser une arborescence de sources interdomaines.

Dans l'exemple de topologie MSDP, la source et le récepteur multicast sont dans des domaines séparés. Dans chaque domaine multicast se trouve un seul RP pour un groupe multicast donné. En utilisant MSDP, RP_1 informe RP_2 des sources actives pour lesquelles RP_1 agit comme point de rendez-vous. RP_2 est capable de créer l'arbre de multidiffusion à travers la frontière du domaine.



MSDP utilise le port TCP 639 bien connu pour le peering. Le pair avec l'adresse IP supérieure écoute sur le port 639; le pair avec l'adresse IP inférieure tente une connexion active au port 639. Avant de configurer MSDP, familiarisez-vous avec la RFC 3618. La tâche suivante suppose que vous avez déjà configuré la multidiffusion IPv4.

Les types de messages MSDP pris en charge sont:

- **Source Active (SA)** - Contient l'adresse IP du point de rendez-vous d'origine (RP) et une ou plusieurs paires (S,G) annoncées. Peut également contenir un paquet de données encapsulé.
- **Keepalive**—Envoyé pour maintenir la session MSDP active. Si aucun message keepalive ou SA n'est reçu pendant l'intervalle d'attente, la session MSDP est réinitialisée.
- **Notification** — Envoyé si une erreur est détectée.

Les connexions TCP MSDP entre routeurs RP nécessitent un réseau IP unicast sous-jacent. BGP IPv4 unicast doit participer pour confirmer la vérification du reverse-path forwarding (RPF) avec un pair, maintenant ainsi le transfert sans boucle entre les domaines.

 ©2024 Palo Alto Networks, Inc.

Vous pouvez Créer des profils de routage multidiffusion avant la configuration ou pendant le processus de configuration de MSDP.

STEP 1 | Configurer un routeur logique.

STEP 2 | Sélectionnez **Routeurs logiques** > **routage** > **réseau** et sélectionnez un routeur logique.

STEP 3 | Sélectionnez **Multidiffusion** et **activez le protocole de multidiffusion**.

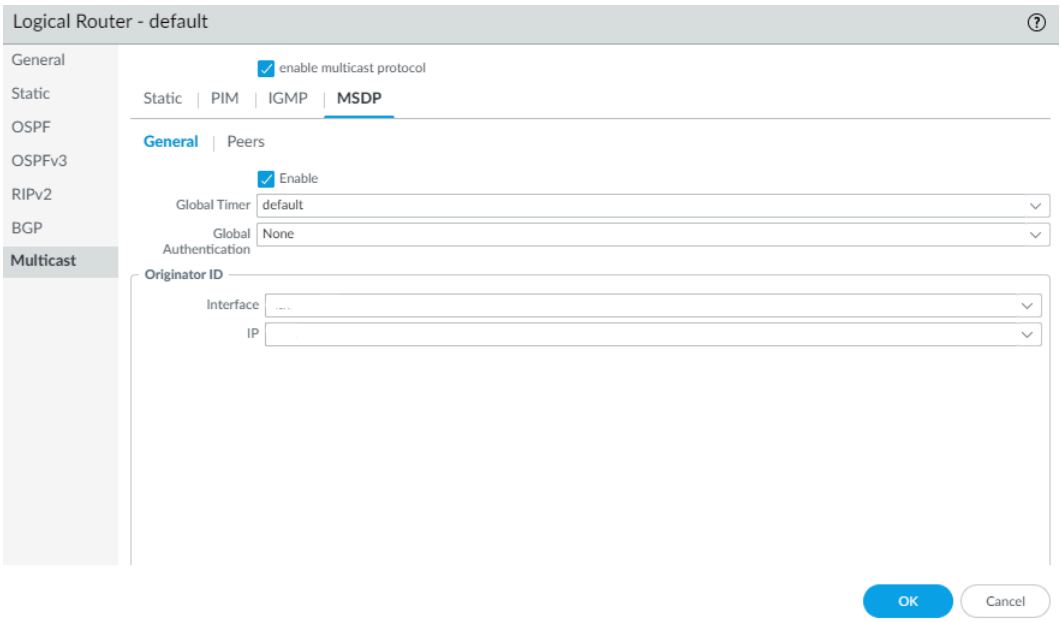
STEP 4 | Sélectionnez **MSDP** > **General** et **Enable (Activer)** MSDP.

STEP 5 | Sélectionnez le profil **Global Timer (Minuterie générale)**, ou sélectionnez le profil **default (par défaut)** (c'est le paramètre par défaut), ou créez un nouveau profil de minuterie. Si vous sélectionnez la valeur **default (par défaut)**, Keep Alive Interval est défini sur 60, Message Timeout est défini sur 75 et Connection Retry Interval est défini sur 30. Si vous sélectionnez **None (Aucun)**, les valeurs par défaut s'appliquent.

STEP 6 | Sélectionnez le profil **Global Authentication (Authentification globale)** ou créez-en un nouveau. Valeur par défaut : **Aucune**.

STEP 7 | Pour l'ID Originator, sélectionnez l'**Interface** que le routeur logique utilise comme interface RP dans les messages Source-Active (SA).

STEP 8 | Sélectionnez ou saisissez l'**adresse IP** (avec la longueur du préfixe) que le routeur logique utilise comme adresse RP dans les messages SA. Si aucune adresse IP Originator n'est configurée, le routeur logique utilise l'adresse PIM RP pour encapsuler le message SA.

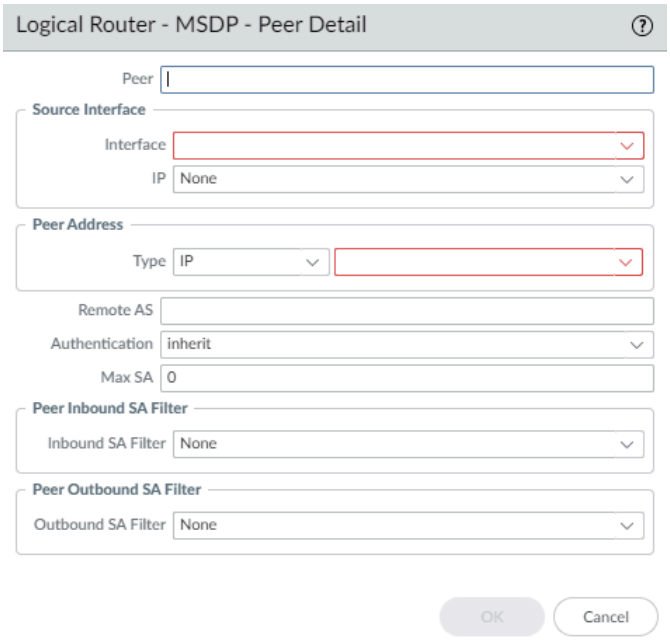


STEP 9 | Cliquez sur **OK**.

STEP 10 | Sélectionnez **Peers (Homologues)** et **Add (ajoutez)** un nom de**Peer (Homologue)** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et peut contenir une combinaison de

 ©2024 Palo Alto Networks, Inc.

caractères alphanumériques, de traits de soulignement, de traits d'union ou de points. Aucun espace n'est autorisé.



STEP 11 | Entrez l'**interface** source utilisée pour établir la connexion MSDP sur TCP avec son homologue MSDP.

STEP 12 | Sélectionnez l'adresse **IP** de l'interface source. Valeur par défaut : **Aucune**.

STEP 13 | Sélectionnez le **Type (Type)** de groupe d'homologues :

- **IP** - (par défaut) et sélectionnez un objet d'adresse ou entrez une adresse IP.
- **FQDN** — Sélectionnez ou saisissez le nom de domaine complet du pair. La liste déroulante affiche tous les noms FQDN configurés comme objets d'adresse.

STEP 14 | Entrez le numéro de système autonome BGP de **Remote as (AS distant)** où se trouve l'homologue MSDP.

STEP 15 | Pour **Anthentication (authentification)**, effectuez l'une des opérations suivantes:

- Sélectionnez un profil d'authentification à appliquer à ce pair, qui remplace le profil d'authentification globale que vous avez appliqué à MSDP sur la page Général.
- **inherit (inherit from global authentication) (hériter (hériter de l'authentification globale))** (par défaut) du profil d'authentification globale.
- Sélectionnez **None (Aucun)** pour désactiver l'authentification à ce pair, qui remplace le profil d'authentification globale.

STEP 16 | Pour **Max SA**, entrez le nombre maximal d'entrées Source-Active (SA) que le cache SA acceptera de ce pair MSDP. La plage est de 0 à 1 024; la valeur par défaut est 0 (illimité). Une fois ce maximum atteint, les nouveaux messages SA de ce pair sont supprimés.

©2024 Palo Alto Networks, Inc.

STEP 17 | Pour **Peer Inbound SA Filter (filtre SA entrant des homologues)**, sélectionnez une liste d'accès ou create a new access list (créez une nouvelle liste d'accès) pour filtrer les messages SA entrants (bloquer les groupes indésirables) de ce pair. Valeur par défaut : **Aucune**.

La liste d'accès peut spécifier des adresses source dans une paire (S,G) à filtrer, ou des adresses destination (groupe) dans une paire (S,G) à filtrer, ou les deux.

STEP 18 | Pour **Peer Outbound SA Filter (filtre SA sortant des homologues)**, sélectionnez une liste d'accès ou create a new access list (créez une nouvelle liste d'accès) pour filtrer les messages SA sortants (bloquer les groupes indésirables) en cours de propagation vers cet homologue. Valeur par défaut : **Aucune**.

La liste d'accès peut spécifier des adresses source dans un (S,G) à filtrer, ou des adresses destination (groupe) dans un (S,G) à filtrer, ou les deux.

STEP 19 | Cliquez sur **OK**.

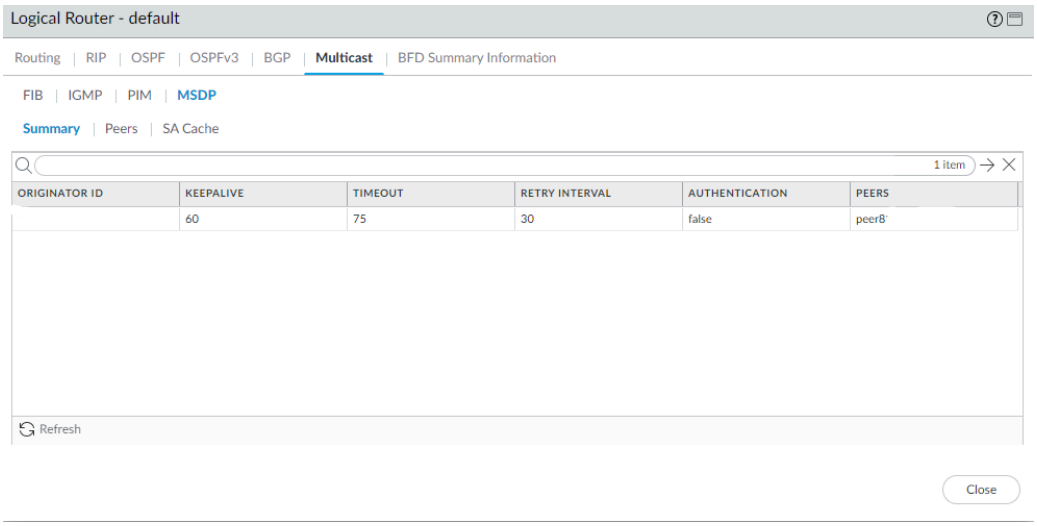
STEP 20 | Create MSDP authentication and timer profiles (Créez des profils d'authentification et de minuterie MSDP) si vous ne l'avez pas encore fait.

STEP 21 | **Commit** (Valider).

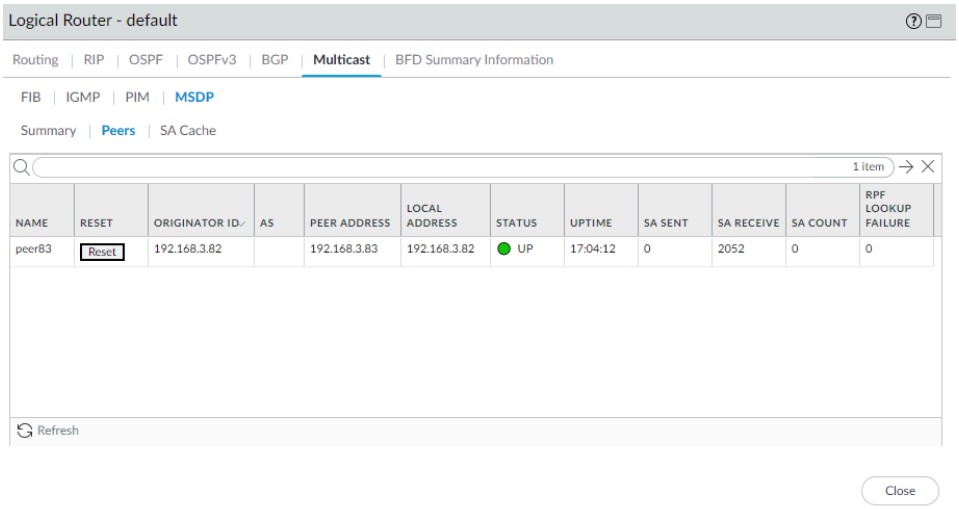
 ©2024 Palo Alto Networks, Inc.

STEP 22 | Voir les informations MSDP.

1. SélectionnezNetwork (Réseau) > Routing (Routage) > Logical Routers (Routeurs logiques) et dans la ligne du routeur logique que vous avez configuré, sélectionnez **More Runtime Stats (Plus de stat d'exécution)**.
2. Sélectionnez **Multicast (Multidiffusion)** > **MSDP** > **Summary (Résumé)** pour voir les informations générales MSDP, telles que l'adresse IP de l'expéditeur, les minuteries, l'authentification et le nom de l'homologue.

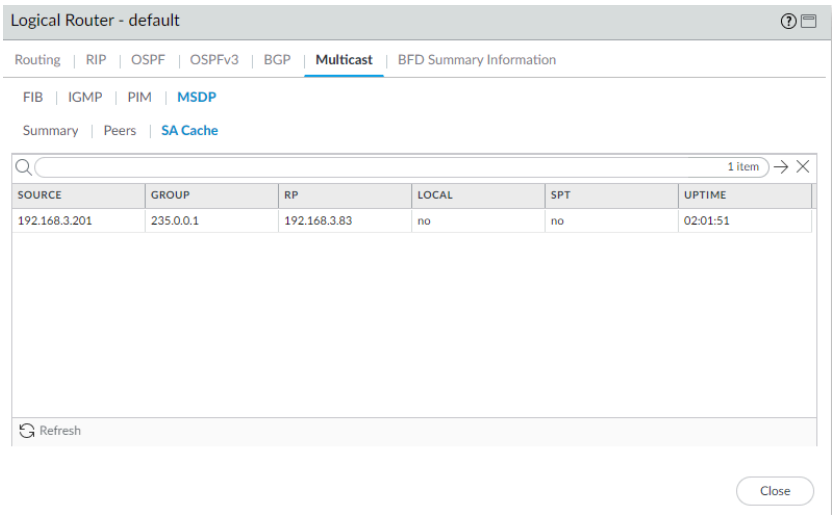


3. Sélectionnez **Pairs (Homologues)** pour afficher des informations sur les pairs MSDP.



4. Sélectionnez **SA Cache** pour afficher les entrées Source-Active dans le cache.

 ©2024 Palo Alto Networks, Inc.



5. **Refresh (Actualiser)** ou **Close (Fermer)** les statistiques d'exécution.

 ©2024 Palo Alto Networks, Inc.

Créer des profils de routage multidiffusion

Sur un moteur de routage avancé, créez les profils de routage suivants à appliquer à une configuration multidiffusion IPv4 :

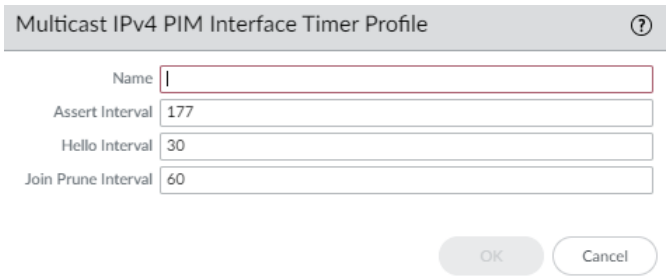
- **Profils de temporisateur d'interface PIM IPv4 multidiffusion**: utilisez l'onglet Général PIM (Temporisateur général d'interface) et l'onglet Interfaces PIM pour remplacer le temporisateur général d'interface.
- **Profils de requête d'interface IGMP IPv4 multidiffusion**: à utiliser dans l'onglet IGMP pour une interface IGMP dynamique.

Créez les profils MSDP (Multicast Source Discovery Protocol) suivants à appliquer à une MSDP configuration (configuration MSDP).

- **MSDP Authentication Profiles (Profils d'authentification MSDP)**: utilisez l'onglet MSDP Général pour appliquer un profil globalement et l'onglet Homologue MSDP pour remplacer le profil d'authentification global. MSDP utilise l'authentification MD5.
- **MSDP Timer Profiles (Profils du minuteur MSDP)** : à utiliser sous l'onglet MSDP Général.

STEP 1 | Profil de minuterie d'interface PIM IPv4 multidiffusion

1. Sélectionnez **Routage** > **réseau** > **Profils** > **Multidiffusion**.
2. **Ajoutez** un **profil de minuterie d'interface PIM IPv4 multidiffusion** par **nom**. (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.
3. Indiquez **Asset Interval (Intervalle d'affirmation)** : nombre de secondes entre les messages d'affirmation PIM que le routeur logique envoie à d'autres routeurs PIM sur le réseau à accès multiple lorsqu'il choisit un porteur PIM (plage de 1 à 65 534 ; la valeur par défaut est 177).
4. Indiquez **Hello Interval (Intervalle Hello)** : nombre de secondes entre les messages Hello PIM que le routeur logique envoie à ses voisins PIM de chaque interface dans le groupe d'interfaces (plage de 1 à 180 ; la valeur par défaut est 30).
5. Indiquez **Join Prune Interval (Intervalle de jointure/élagage)** : nombre de secondes entre les messages de jointure PIM (et entre les messages d'élagage PIM) que le routeur logique envoie en amont vers une source multicast (plage de 60 à 600 ; la valeur par défaut est 60).

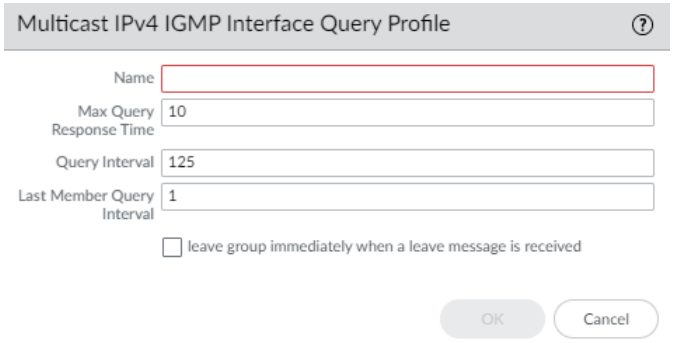


6. Cliquez sur **OK**.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Créer un Profil de requête d'interface IGMP IPv4 multidiffusion

1. Sélectionnez **Routage** > **réseau** > **Profils** > **Multidiffusion**.
2. **Ajoutez** un **profil de requête d'interface IGMP IPv4 multidiffusion** par **nom** (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.
3. Indiquez **Max Query Response Time (sec) (Temps max. de réponse aux requêtes (sec.)** : nombre maximal de secondes dont dispose le récepteur pour répondre à un message de requête d'adhésion IGMP avant que le routeur logique détermine que le récepteur ne souhaite plus recevoir les paquets multidiffusion pour un groupe (la plage est comprise entre 1 et 25 ; la valeur par défaut est 10).
4. Indiquez **Query Interval (Intervalle de requête)** : nombre de secondes entre les messages de requête d'adhésion IGMP que le routeur logique envoie à un récepteur pour déterminer si le récepteur souhaite toujours recevoir les paquets multicast pour un groupe (la plage est comprise entre 1 et 1 800 ; la valeur par défaut est 125).
5. Indiquez **Last Member Query Interval (Dernier intervalle de requête d'un membre)** : nombre de secondes dont dispose un récepteur pour répondre à une requête propre à un groupe que le routeur logique envoie après qu'un récepteur envoie un message d'abandon de groupe (la plage est comprise entre 1 et 25 ; la valeur par défaut est 1).
6. Si vous activez **leave group immediately when a leave message is received (quitter le groupe immédiatement lors de la réception d'un message)**, Lorsqu'il n'y a qu'un seul membre dans un groupe multidiffusion et que le routeur logique reçoit un message d'abandon IGMP pour ce groupe, ce paramètre entraîne la suppression immédiate par le routeur logique de ce groupe et de l'interface de sortie de la multicast routing information base (base d'informations de routage multidiffusion ; mRIB) et de la multicast forwarding information base (base d'informations de transfert multidiffusion ; mFIB) plutôt que d'attendre l'expiration du dernier intervalle de requête d'un membre. L'activation de ce paramètre permet d'économiser des ressources réseau. (La valeur par défaut est désactivée.)



7. Cliquez sur **OK**.

STEP 3 | Profil d'authentification MSDP multidiffusion

1. Sélectionnez **Routage** > **réseau** > **Profils** > **Multidiffusion**.
2. **Add (Ajoutez)** un **Multicast MSDP Authentication Profile (profil d'authentification MSDP de multidiffusion)Name (nom)** (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un

 ©2024 Palo Alto Networks, Inc.

point (.) et peut contenir une combinaison de caractères alphanumériques, de traits de soulignement, de traits d'union ou de point (.). Aucun espace n'est autorisé.

3. Entrez le **Secret (code secret)** (les caractères alphanumériques, !, @, #, % et ^ sont autorisés).
4. **Confirm Secret (Confirmer le code secret)**.
5. Cliquez sur **OK**.

STEP 4 | Créez un profil de minuteur MSDP.

1. Sélectionnez **Routage** > **réseau** > **Profils** > **Multidiffusion**.
2. **Add (Ajoutez)** un **Multicast MSDP Timer Profile (profil du minuteur MSDP de multidiffusion)** par **Name (nom)** (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et peut contenir une combinaison de caractères alphanumériques, de traits de soulignement, de traits d'union ou de points. Aucun espace n'est autorisé.
3. Saisissez **Keep Alive Interval** en secondes ; plage comprise entre 1 et 60 ; la valeur par défaut est 60. Une fois qu'une connexion de transport MSDP est établie avec un homologue, chaque côté de la connexion envoie des messages Keepalive à l'autre côté à cet intervalle pour maintenir la session MSDP active. Si le minuteur expire, l'homologue envoie un message Keepalive et réinitialise le minuteur. Si aucun message Keepalive ou SA n'est reçu pour l'intervalle de délai d'expiration du message, la session MSDP est réinitialisée.
4. Entrez l'intervalle de **Message Timeout (délai d'expiration du message)** en secondes, qui est l'intervalle auquel l'homologue MSDP attend les messages Keepalive d'autres homologues avant de les déclarer. La plage est comprise entre 1 et 75 ; la valeur par défaut est 75.
5. Entrez **Connection Retry Interval (intervalle de nouvelle tentative de connexion)** en secondes, qui est l'intervalle que les homologues attendent après la réinitialisation d'une session d'appairage avant d'essayer de rétablir la session d'homologation. La plage est comprise entre 1 et 60 ; la valeur par défaut est 30.
6. Cliquez sur **OK**.

STEP 5 | **Commit (Validez)** vos modifications.

 ©2024 Palo Alto Networks, Inc.

Créer un MRoute IPv4

Le moteur de routage avancé vous permet de router Configurer la multidiffusion IPv4 pour un routeur logique. Rappelons que PIM vérifie si le pare-feu a reçu les paquets sur la même interface que celle utilisée par le pare-feu pour renvoyer les paquets unicast à la source, en vérifiant le RIB unicast.

Dans une topologie où vous souhaitez que les paquets unicast empruntent une route différente de celle des paquets multicast, vous pouvez configurer un mroute. Une mroute est une route de monodiffusion statique qui pointe vers une source de multidiffusion ; la mroute est stockée dans le RIB de multidiffusion (MRIB). PIM utilise la mroute pour les vérifications RPF, plutôt que d'utiliser la rib unicast pour les vérifications RPF. L'utilisation du PIM par le MRIB ou l'URIB pour la vérification RPF dépend du mode de recherche RPF configuré pour le PIM. Lors des vérifications RPF, le mroute utilisé est celui avec la correspondance de préfixe la plus longue.

Une mroute est utile, par exemple, lorsque certains périphériques le long du chemin ne prennent pas en charge le routage multidiffusion, de sorte qu'un tunnel est utilisé pour connecter des routeurs de multidiffusion.

STEP 1 | Configurer un routeur logique.

STEP 2 | Sélectionnez **Routeurs logiques** > **routage** > **réseau** et sélectionnez un routeur logique.

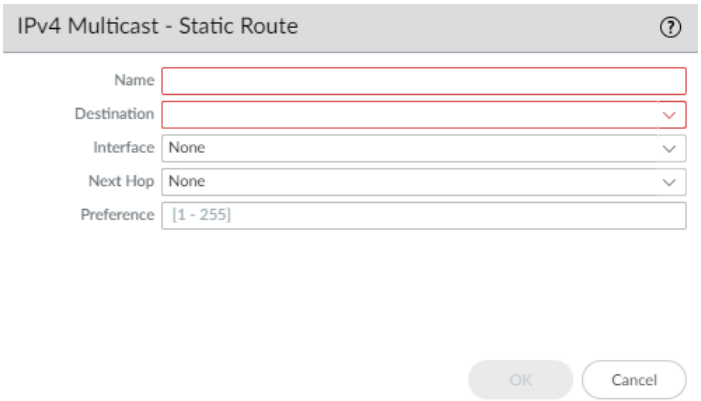
STEP 3 | Sélectionnez **Multidiffusion** et **activez le protocole de multidiffusion**.

STEP 4 | Créez un mroute.

1. Sélectionnez **Statique** et **Ajoutez** un mroute par **nom**. Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et contenir

 ©2024 Palo Alto Networks, Inc.

zéro ou plusieurs caractères alphanumériques, trait de soulignement ou trait d'union. Aucun point (.) ou espace n'est autorisé.



2. Entrez la **Destination** (adresse/masque IPv4 ou objet adresse) du mroute, qui est la source ou le sous-réseau de multidiffusion sur lequel le pare-feu effectue une vérification RPF.
3. Sélectionnez l'**interface** de sortie pour l'itinéraire de monodiffusion vers la source de multidiffusion.
4. Entrez l'adresse IPv4 (ou l'objet adresse) du routeur **Next Hop** vers la source.
5. Entrez une **préférence** pour l'itinéraire ; la plage est comprise entre 1 et 255.
6. Cliquez sur **OK**.

STEP 5 | Cliquez sur **OK**.

STEP 6 | **Commit (Validez)** vos modifications.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Poe

Vous pouvez configurer Power over Ethernet (PoE) sur les interfaces des pare-feu pris en charge pour transférer l'énergie électrique du pare-feu vers un périphérique alimenté connecté (PD). Cela vous permet de répondre aux besoins en énergie des PD tout en continuant à leur transmettre des données à l'aide d'un seul câble Ethernet par port PoE physique.

- Aperçu PoE
- Configurer PoE

Aperçu PoE

Ce tableau répertorie chaque pare-feu Palo Alto Networks® Next-Generation avec ports PoE ainsi que la puissance maximale qu'ils offrent, le budget de puissance total autorisé et les types d'interface qu'ils prennent en charge.

Pare-feu	Ports PoE	Puissance maximale réservée (par port)	Budget PoE total autorisé (tous les ports)	Types d'interfaces pris en charge
PA-415 et PA-445	6, 7, 8 et 9	60W	91W	• Ethernet agrégé (AE) • Haute disponibilité (HA) • Couche 2 • Couche 3 • Tap • Virtual Wire
PA-1410 et PA-1420	9, 10, 11 et 12	90W	151W	

Sélectionnez **Dashboard (Tableau de bord)** > **Widgets** > **System (Système)** > **Interfaces** pour afficher l'état actuel de chaque port. Les ports PoE sont signalés par une icône représentant un éclair. Passer la souris sur une icône de port PoE affiche l'état PoE, l'alimentation allouée, l'alimentation utilisée et d'autres détails configurés.

De même, sélectionnez **Dashboard (Tableau de bord)** > **Widgets** > **System (Système)** > **PoE Power Budget** pour afficher un graphique en anneau qui confirme la puissance disponible sur le pare-feu et vous aide à décider quels PD connecter aux ports PoE.

 ©2024 Palo Alto Networks, Inc.

Configurer PoE

La tâche suivante décrit la procédure de configuration de PoE sur votre pare-feu.

STEP 1 | Assurez-vous que l'appareil que vous souhaitez alimenter est connecté au pare-feu à l'aide d'un câble Ethernet via un port PoE pris en charge sur le pare-feu.

L'utilisation d'un câble Ethernet Cat5 ou Cat6 garantit le transfert de puissance le plus fiable. Un câble Cat3, par exemple, ne pourra transférer que 20W.

STEP 2 | Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et choisissez l'interface que vous avez câblée.

STEP 3 | PoE est actif sur tous les ports PoE par défaut. Dans la fenêtre Interface Ethernet, sélectionner **Advanced (Avancé)** et afficher **PoE Settings (paramètres PoE)** indique que **PoE Enable (activation PoE)** est déjà activée.

Vous pouvez également utiliser la CLI pour activer ou désactiver PoE. Après vous être connecté au pare-feu à l'aide d'un logiciel d'émulation de terminal, entrez ***`configure (configurer)`*** *suivi de* ***`set network interface ethernet ethernet1/9 poe poe-enabled {yes | no}`*** *où « ethernet1/9 » correspond au port PoE que vous souhaitez activer ou désactiver.*

Avant de passer à l'étape suivante, déterminez la puissance maximale prise en charge par l'appareil alimenté (PD) connecté. Cette valeur dépend du type et de la classe du PD.

STEP 4 | Définissez la quantité d'énergie réservée par le port en saisissant une valeur (en watts) pour **PoE Rsvd Pwr**. Cette valeur doit être un nombre compris entre **0** et la puissance maximale

 ©2024 Palo Alto Networks, Inc.

réservée du port telle que définie dans le Aperçu PoE. Un **0** indique qu'aucune alimentation n'est réservée par ce port PoE.

Vous pouvez également utiliser la CLI pour configurer l'alimentation PoE réservée. Entrez ***configure (configurer)*** *suivi de* ***set network interface ethernet1/9 poe poe-rsvd-pwer (définir l'interface réseau ethernet1/9 poe poe-rsvd-pwer)*** *<value>où « ethernet1/9 » correspond au port PoE que vous souhaitez configurer et «<value>» fait référence au nombre de Watts allant de 0 au maximum supporté par l'interface.*

Le total ***PoE Rsvd Pwr*** *de tous vos ports PoE ne doit pas dépasser le budget PoE total autorisé. Si vous dépassez le budget PoE total autorisé, un ou plusieurs appareils alimentés entreront dans l'état* ***Den*** *(alimentation refusée) jusqu'à ce que vous réattribuiez l'alimentation réservée.*

Un port PoE peut également passer à l'état ***Den*** *ou* ***Dis*** *(désactivé) en fonction de la puissance totale allouée actuelle. La puissance totale allouée fait référence à la somme de la puissance réservée de tous les ports PoE ou à la somme de la puissance allouée réelle autorisée par tous les PD. Si la puissance totale réservée est inférieure à la puissance totale allouée réelle, le port PoE passe à l'état* ***Dis*** *ou* ***Den*** *.*

Un port PoE à l'état ***Dis*** *ou* ***Den*** *ne peut pas être résolu en déconnectant et en reconnectant le PD. Utilisez plutôt l'une des méthodes suivantes pour reprendre la détection de l'alimentation sur le PD connecté :*

- *Désactivez PoE sur l'interface en décochant* ***PoE Enable****. Appliquez le paramètre, puis revenez à la même interface et cochez* ***PoE Enable****.*
- *Définissez l'état de liaison du port concerné sur* ***auto*** *ou* ***up****.*
- *Modifiez le* ***PoE Rsvd Pwr*** *du port PoE concerné pour qu'il soit égal ou supérieur à la puissance requise par le PD.*

Si aucun appareil n'est connecté à un port PoE, assurez-vous que ***PoE Enable*** *est décoché ou que la valeur* ***PoE Rsvd Pwr*** *est* ***0*** *pour éviter de consommer une partie du budget PoE.*

STEP 5 | Cliquez sur **OK**.

STEP 6 | **Commit (Validez)** vos modifications.

STEP 7 | Vérifiez l'état des ports PoE en vérifiant l'interface Web du pare-feu ou la CLI.

1. Pour vérifier par l'interface Web du pare-feu, connectez-vous au pare-feu et sélectionnez **Dashboard (tableau de bord)** > **Widgets** > **System (Système)** > **Interfaces**. Passez la souris sur les icônes de port PoE, identifiées par un symbole d'éclair, pour des détails d'interface spécifiques. Sélectionnez **Dashboard (Tableau de bord)** > **Widgets** > **System (Système)** > **PoE Power Budget** pour obtenir des informations sur

 ©2024 Palo Alto Networks, Inc.

l'allocation d'alimentation. Pour afficher les messages d'état et d'autres informations PoE, sélectionnez **Network (Réseau)** > **Interfaces** > **PoE**.

2. Pour vérifier à l'aide de la CLI, entrez **`show poe (afficher poe)`** ou **`show poe detail (afficher les informations poe)`**.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.