paloalto TECHDOCS

Guide de déploiement VM-Series

Version 10.2



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

© 2021-2022 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

February 26, 2022

Table of Contents

À propos du pare-feu VM-Series 15

Déploiements VM-Series 16
VM-Series en haute disponibilité 18
Mise à niveau du pare-feu VM-Series 20
Mise à niveau de la version du logiciel PAN-OS (version autonome) 20
Pour mettre à niveau la version du logiciel PAN-OS (paire HA) 23
Mise à niveau de la version du logiciel PAN-OS avec Panorama 28
Mise à niveau de la version du logiciel PAN-OS (VM-Series pour NSX) 32
Mise à niveau du modèle VM-Series 37
Mise à niveau du modèle VM-Series d'une paire HA 39
Rétrograder un pare-feu VM-Series vers une version antérieure 40
Plug-in VM-Series 42
Configuration du plug-in VM-Series sur le pare-feu 42
Mise à niveau du plug-in VM-Series 43
Activation des trames Jumbo sur le pare-feu VM-Series 46
Adresses MAC attribuées par l'hyperviseur 48
Publication de statistiques PAN-OS personnalisées pour la surveillance 50
Interface utilisée pour accéder aux services externes sur le pare-feu VM-Series 52
Support des pilotes PacketMMAP et DPDK 53
Activation de l'optimisation des performances NUMA sur le VM-Series 55
Activation du ZRAM sur le pare-feu VM-Series 57

Mise sous licence du pare-feu VM-Series 59

Mise sous licence du pare-feu VM-Series 60
Types de licences 60
Licences de vCPU flexibles et de modèle fixe 61
Déploiement de vCPU flexibles et de modèles fixes 64
Création d'un compte de support 65
Format du numéro de série et de l'ID du processeur pour le pare-feu VM-Series 66
API de mise sous licence 67
Gestion de la clé API de mise sous licence 68
Utilisation de l'API de mise sous licence 68
Codes d'erreur de l'API de mise sous licence 72
Installation d'une clé API de licence 73
Utilisation la gestion des licences de pare-feu logiciel basée sur Panorama 74
Crédits NGFW logiciels 79
Limites maximales basées sur le niveau et la mémoire 81
Activer des crédits 92

 ©2023 Palo Alto Networks, Inc.

Création d'un profil de déploiement....93
Gestion d'un profil de déploiement....94
Enregistrement du pare-feu VM-Series (crédits NGFW logiciels)....95
Configuration de Panorama....98
Migration de Panorama vers une licence NGFW logicielle....99
Transfert de crédits....103
Renouvellement de votre licence de crédits NGFW logiciels....105
Désactivation de la licence (crédits NGFW logiciels)....106
Définir le nombre de vCPU sous licence....108
Personnalisation des cœurs de plan de données....109
Migration d'un pare-feu vers une licence VM-Series flexible....110
Modèles VM-Series....115
Configuration système requise pour VM-Series....116
Sursouscription du processeur....118
Le mode VM-50 Lite....119
Types de licences de modèle VM-Series....120
Activation des licences de modèle VM-Series....132
Enregistrement du pare-feu VM-Series....139
Installation d'un certificat de périphérique sur le pare-feu VM-Series....142
Basculer entre les licences BYOL et PAYG....145
Basculer entre les licences de modèle VM-Series....146
Désactivation de la ou des licence(s)....149
Renouveler les paquets de permis de coupe-feu de la série VM....155
Que se passe-t-il à l'expiration des licences ?....158
Licences pour les fournisseurs de services de sécurité cloud (CSSP)....161
Obtention des codes d'autorisation pour les ensembles de licence CSSP....161
Enregistrement du pare-feu VM-Series avec un code d'autorisation CSSP....162
Ajout d'informations sur le client final pour un pare-feu VM-Series enregistré....163

Configuration d'un pare-feu VM-Series sur un serveur ESXi....169

Déploiements pris en charge sur VMware vSphere Hypervisor (ESXi)....170
VM-Series sur système ESXi : configuration système requise et limitations....171
VM-Series sur système ESXi : configuration système requise....171
VM-Series sur système ESXi : limitations....172
Installation d'un pare-feu VM-Series sur VMware vSphere Hypervisor (ESXi)....174
Planification des interfaces pour VM-Series pour ESXi....174
Configuration du pare-feu VM-Series sur un serveur ESXi....176
Configuration initiale sur le VM-Series sur ESXi....178
Ajout d'espace disque supplémentaire au pare-feu VM-Series....180

 ©2023 Palo Alto Networks, Inc.

Utilisation de VMware Tools sur le pare-feu VM-Series sur ESXi et vCloud Air....181
Utilisation de vMotion pour déplacer le pare-feu VM-Series entre les hôtes....183
Utilisation de la CLI du VM-Series pour permuter l'interface de gestion sur ESXi....184
VM Monitoring sur vCenter....185
À propos de VM Monitoring sur VMware vCenter....185
Installation du plug-in Panorama pour VMware vCenter....186
Configurez le plug-in Panorama pour VMware vCenter....187
Résolution des problèmes de déploiement ESXi....191
Résolution des problèmes de base....191
Problèmes d'installation....191
Problèmes de mise sous licence....193
Problèmes de connectivité....194
Réglage des performances de VM-Series pour ESXi....196
Installation du pilote de carte réseau sur ESXi....196
Activation de DPDK sur ESXi....197
Activation de SR-IOV sur ESXi....197
Activation du mode d'accès VLAN (réseau local virtuel) ESXi avec SR-IOV....198
Activation de la prise en charge de files d'attente multiples pour les cartes réseau sur ESXi....200
Réglage des performances du VNF....200

Configuration du pare-feu VM-Series sur vCloud Air....213

À propos du pare-feu VM-Series sur vCloud Air....214
Déploiements pris en charge sur vCloud Air....215
Déploiement du pare-feu VM-Series sur vCloud Air....216

Configuration du pare-feu VM-Series sur VMware NSX-T....223

Configuration du pare-feu VM-Series sur VMware NSX-T (Nord-Sud)....224
Déploiements pris en charge du pare-feu VM-Series sur VMware NSX-T (Nord-Sud)....224
Composants du pare-feu VM-Series sur NSX-T (Nord-Sud)....225
Déploiement du pare-feu VM-Series sur NSX-T (Nord-Sud)....226
Extension de la politique de sécurité du NSX-V au NSX-T....240
Configuration du pare-feu VM-Series sur NSX-T (Est-Ouest)....243
Composants du pare-feu VM-Series sur NSX-T (Est-Ouest)....243
Pare-feu VM-Series sur l'intégration NSX-T (Est-Ouest)....245
Déploiements pris en charge du pare-feu VM-Series sur VMware NSX-T (Est-Ouest)....247
Déploiement du VM-Series à l'aide du flux de travail centré sur les opérations....248

©2023 Palo Alto Networks, Inc.

Déploiement du VM-Series à l'aide du flux de travail centré sur la sécurité..... 266
Suppression d'une définition de service de Panorama..... 298
Migration d'une utilisation de VM-Series sur NSX-T vers un déploiement centré sur la sécurité..... 298
Extension de la politique de sécurité du NSX-V au NSX-T..... 305
Utilisation de la migration sur place pour déplacer votre VM-Series du NSX-V au NSX-T..... 307

Configuration du pare-feu VM-Series sur AWS.....315

À propos du pare-feu VM-Series sur AWS..... 316
Types d'instances AWS EC2..... 316
Pare-feu VM-Series sur AWS GovCloud..... 316
Pare-feu VM-Series sur AWS Chine..... 317
Pare-feu VM-Series sur AWS Outposts..... 317
Terminologie AWS..... 317
Mappage d'interface de gestion pour l'utilisation avec Amazon ELB..... 320
Réglage des performances du pare-feu VM-Series pour AWS..... 322
Déploiements pris en charge sur AWS..... 324
Déploiement du pare-feu VM-Series sur AWS..... 327
Obtention de l'AMI..... 327
Planification de la fiche de travail du pare-feu VM-Series dans AWS VPC..... 331
Lancement du pare-feu VM-Series sur AWS..... 333
Lancement du pare-feu VM-Series sur AWS Outpost..... 342
Création d'une AMI (Image de machine Amazon) personnalisée..... 351
Chiffrement du volume EBS pour le pare-feu VM-Series sur AWS..... 354
Utilisation de la CLI du pare-feu VM-Series pour permuter l'interface de gestion..... 356
Activation de la surveillance CloudWatch sur le pare-feu VM-Series..... 357
Intégration VM-Series avec un équilibreur de charge de passerelle AWS..... 362
Intégration manuelle de VM-Series avec un équilibreur de charge de passerelle..... 365
Groupe de mise à l'échelle automatique VM-Series avec équilibreur de charge AWS Gateway..... 378
Haute disponibilité des pare-feu VM-Series sur AWS..... 394
Vue d'ensemble de la HA dans AWS..... 394
Rôles IAM pour la HA..... 395
Liaisons HA..... 398
Analyse des pulsations et messages Hello..... 399
Priorité et préemption des périphériques..... 399
Minuteurs HA..... 399
Configuration de la HA active/passive dans AWS à l'aide d'un IP secondaire..... 400

 ©2023 Palo Alto Networks, Inc.

Configuration de la HA active/passive dans AWS à l'aide du déplacement d'interface....406
Migration de la HA active/passive dans AWS....410
Cas d'utilisation : Sécurisation des instances EC2 dans le cloud AWS....417
Cas d'utilisation : Utilisation de groupes d'adresses dynamiques pour sécuriser les nouvelles instances EC2 dans VPC....432
Cas d'utilisation : Pare-feu VM-Series en tant que passerelles GlobalProtect sur AWS....436
Composants de l'infrastructure GlobalProtect....437
Déploiement de passerelles GlobalProtect sur AWS....437
Surveillance des ressources sur le AWS....439
Surveillance des ressources AWS avec Plugin AWS sur Panorama....439
Configuration du Plugin AWS pour surveillance de machine virtuelle....439
Mise à l'échelle automatique de pare-feu VM-Series avec le service Amazon ELB....453
Modèles de mise à l'échelle automatique VM-Series pour AWS version 2.0....455
Modèles de mise à l'échelle automatique VM-Series pour AWS version 2.1....492
Liste des attributs surveillés dans AWS VPC....523
Permissions de gestion d'identité et d'accès pour la surveillance dans AWS VPC....525

Configuration du pare-feu VM-Series sur KVM....527

VM-Series sur KVM : configuration système requise et conditions préalables....528
Options d'association du VM-Series sur le réseau....530
Conditions préalables du VM-Series sur KVM....530
Déploiements pris en charge sur KVM....536
Sécurisation du trafic sur un hôte....536
Sécurisation du trafic entre des hôtes Linux....536
Installation du pare-feu VM-Series sur KVM....538
Installation du pare-feu VM-Series à l'aide de Virt-Manager....538
Installation du pare-feu VM-Series à l'aide d'une ISO....545
Utilisation de la CLI du VM-Series pour permuter l'interface de gestion sur KVM....547
Autorisation de l'utilisation d'un contrôleur SCSI....547
Vérification du PCI-ID de commande d'interfaces réseau sur le pare-feu VM-Series....548
Réglage des performances de VM-Series pour KVM....550
Installation de KVM et Open vSwitch sur Ubuntu 16.04.1 LTS....550
Activation d'Open vSwitch sur KVM....550
Intégration d'Open vSwitch avec DPDK....551
Activation de SR-IOV sur KVM....555

©2023 Palo Alto Networks, Inc.

Activation du mode d'accès VLAN (réseau local virtuel) avec SR-IOV 556
Activation de la prise en charge de files d'attente multiples pour les cartes réseau sur KVM 557
Isolation des ressources du processeur dans un nœud NUMA sur KVM 558
Délestage intelligent du trafic 560
Exigences de délestage intelligent du trafic 561
Interfaces intelligentes de délestage du trafic 561
Haute disponibilité 562
Installer le BlueField-2 DPU 565
Installation du pare-feu VM-Series 565
Activer les fonctions virtuelles 565
Vérifiez le système BlueField-2 DPU 567
Installation ou mise à niveau du logiciel BlueField Bootstream 568
Installation ou mise à niveau du package Debian 570
Exécution d'un délestage intelligent du trafic 570
Dépannage BlueField-2 DPU 573
Dépannage PAN-OS 573
Références 576

Configuration du pare-feu VM-Series sur Hyper-V 577

Déploiements pris en charge sur Hyper-V 578
Sécurisation du trafic sur un hôte Hyper-V 578
Sécurisation du trafic entre plusieurs hôtes Hyper-V 578
Configuration système requise sur Hyper-V 580
Services d'intégration Linux 581
Installation du pare-feu VM-Series sur Hyper-V 582
Avant de commencer 582
Réglage des performances du pare-feu VM-Series sur Hyper-V 583
Configuration du pare-feu VM-Series sur un hôte Hyper-V avec Hyper-V Manager 583
Configuration du pare-feu VM-Series sur un hôte Hyper-V avec PowerShell 585
Configuration initiale sur le pare-feu VM-Series 586

Configuration du pare-feu VM-Series sur Azure 591

À propos du pare-feu VM-Series sur Azure 592
Mise en réseau Azure et pare-feu VM-Series 592
Intégration du Centre de sécurité Azure 593
Modèles de pare-feu VM-Series sur Azure 595
Configuration système minimale requise pour le VM-Series sur Azure 596
Prise en charge de la haute disponibilité sur VM-Series sur Azure 597
Autorisations principales de VM-Series sur le service Azure 597

 ©2023 Palo Alto Networks, Inc.

Déploiements pris en charge sur Azure....601
Déploiement du pare-feu VM-Series depuis l'Azure Marketplace (modèle de solution)....602
Déploiement du pare-feu VM-Series depuis l'Azure China Marketplace (modèle de solution)....612
Déploiements orchestrés par Panorama dans Azure....619
Préparation d'un déploiement orchestré....621
Orchestration d'un déploiement de pare-feu VM-Series dans Azure....625
Création d'une image personnalisée VM-Series pour Azure....634
Utilisez les recommandations du Centre de sécurité Azure pour sécuriser vos charges de travail....636
Déployer un pare-feu de série VM en fonction d'une recommandation du Centre de sécurité Azure....636
Connecter un pare-feu de série VM existant à partir du centre de sécurité Azure....638
Utiliser Panorama pour acheminer les journaux au centre de sécurité Azure....639
Déploiement du pare-feu VM-Series dans Azure Stack....643
Activer Azure Application Insights sur le pare-feu VM-Series....647
Surveillance sur Azure....650
À propos de la surveillance sur Azure....650
Configuration du plugin Azure pour la surveillance sur Panorama....650
Attributs surveillés à l'aide du plugin Panorama sur Azure....659
Configuration de la HA active/passive sur Azure....662
Configurer une HA active/passive sur Azure (trafic Nord-Sud et Est-Ouest)....663
Configurer une HA active/passive sur Azure (trafic Est-Ouest uniquement)....677
Utilisation du modèle ARM pour déployer le pare-feu VM-Series....690
Déploiement du modèle VM-Series et Azure Application Gateway....694
Modèle VM-Series et Azure Application Gateway....695
Commencer à utiliser le modèle VM-Series et Azure Appliction Gateway....696
Sécurisation des services Kubernetes dans Azure....705
Comment le plug-in Panorama pour Azure sécurise-t-il les services Kubernetes ?....705
Sécurisation d'un cluster AKS....710

Configuration du pare-feu VM-Series sur OpenStack....721

Déploiement VM-Series dans OpenStack....722
Passerelle de base....722
Chaînage de service et mise à l'échelle de service....722
Composants de VM-Series pour la solution OpenStack....724
Modèle Heat pour un déploiement de passerelle de base....726

 ©2023 Palo Alto Networks, Inc.

Modèles Heat pour le chaînage de service et la mise à l'échelle de service....729
Réseau virtuel....730
Machine virtuelle....730
Modèle de service....731
Instance de service....732
IPAM....732
Politique de service....733
Alarme....734
Installation du pare-feu VM-Series dans un déploiement de passerelle de base....736
Installation du pare-feu VM-Series avec mise à l'échelle ou chaînage de service....739

Configuration du pare-feu VM-Series sur la plateforme Google Cloud....743

À propos du pare-feu VM-Series sur la plateforme Google Cloud....744
Google Cloud Platform et le pare-feu VM-Series....744
Exigences minimales du système pour le pare-feu de série VM....744
Déploiements pris en charge sur la plateforme Google Cloud....746
Passerelle Internet....746
Passerelle de segmentation....747
Hybrid IPSec VPN....747
Configuration du page-feu de la VM-Series (série VM) sur le cloud public de Google....749
Exigences générales....749
Installation du plug-in VM-Series sur Panorama....750
Installation du plug-in Panorama pour GCP....751
Se préparer au déploiement à partir du GCP Marketplace....752
Déploiement du pare-feu VM-Series sur Google Cloud Platform....760
Déployer le pare-feu de la série VM à partir du marché de la plateforme Google Cloud Launcher....760
Échange de l'interface de gestion pour l'équilibrage de la charge de Google Cloud Platform....765
Utilisation de la CLI du pare-feu VM-Series pour permuter l'interface de gestion....766
Activation de la surveillance CloudWatch sur le VM-Series Firewall (pare-feu de la série VM)....767
Permettre la surveillance de la MV pour suivre les changements de VM sur la plateforme de Google Cloud (GCP)....769
Utilisation de groupes d'adresses dynamiques pour sécuriser des instances dans VPC....772
Utiliser des modèles personnalisés ou le CLI de l'infonuagique pour déployer le Pare-feu de la série VM....774
Surveillance VM avec le plugin Panorama pour GCP....776

 ©2023 Palo Alto Networks, Inc.

Configuration de la surveillance VM avec le plugin Panorama pour GCP..... 776
Mise à l'échelle automatique du pare-feu VM-Series sur Google Cloud Platform..... 783
Composants de mise à l'échelle automatique pour Google Cloud Platform..... 783
Déploiement des modèles de mise à l'échelle automatique GCP..... 795

Configuration d'un pare-feu VM-Series sur un réseau Cisco ENCS..... 825

Planification de votre déploiement Cisco ENCS..... 826
Préparation de l'image du pare-feu VM-Series pour Cisco ENCS..... 828
Convertissez un fichier qcow2 à partir de l'interface utilisateur graphique..... 828
Convertissez un fichier qcow2 à partir de l'interface de ligne de commande..... 831
Déploiement du pare-feu VM-Series sur Cisco ENCS..... 834

Configuration du pare-feu VM-Series sur Oracle Cloud Infrastructure..... 837

Types de formes OCI..... 838
Déploiements pris en charge sur OCi..... 839
Préparation à la configuration du pare-feu VM-Series sur OCI..... 841
Déploiement du pare-feu VM-Series à partir du Marketplace Oracle Cloud..... 844
Configuration de la HA active/passive dans OCI..... 849

Configuration du pare-feu VM-Series sur Alibaba Cloud..... 859

Pare-feu VM-Series sur Alibaba Cloud..... 860
Configuration système minimale requise pour le pare-feu VM-Series sur Alibaba Cloud..... 861
Pare-feu VM-Series : configuration logicielle requise..... 861
Recommandations sur les types d'instances Alibaba Cloud pour le pare-feu VM-Series..... 861
CLI Alibaba Cloud..... 861
Préparation au déploiement du pare-feu VM-Series sur Alibaba Cloud..... 862
Choisissez les licences et planifiez les réseaux..... 862
Préparez-vous à utiliser l'interface de ligne de commande Aliyun..... 863
Déploiement du pare-feu VM-Series sur Alibaba Cloud..... 864
Création d'un VPC et configuration des réseaux..... 864
Création et configuration du pare-feu VM-Series..... 867
Sécurisation du trafic nord-sud sur Alibaba Cloud..... 871
Configuration de l'équilibrage de charge sur Alibaba Cloud..... 875

Configuration d'un pare-feu dans Cisco ACI..... 877

Intégration du pare-feu Palo Alto Networks à Cisco ACI..... 878
Modèles de graphique de service..... 879

 ©2023 Palo Alto Networks, Inc.

Déploiements multicontextes 880
Préparation de votre environnement ACI pour l'intégration 881
Intégration du pare-feu à Cisco ACI en mode politique réseau 882
Déploiement du pare-feu pour sécuriser le trafic est-ouest en mode politique réseau 882
Déploiement du pare-feu pour sécuriser le trafic nord-sud en mode politique réseau 900
Surveillance des terminaux dans Cisco ACI 918
Installation du plug-in Panorama pour Cisco ACI 919
Configuration du plug-in Cisco ACI 920
Plug-in Panorama pour le tableau de bord ACI 924

Configuration du pare-feu VM-Series sur Cisco CSP 929
VM-Series sur Cisco CSP : configuration système requise 930
Déploiement du pare-feu VM-Series sur Cisco CSP 931

Surveillance de terminal pour Cisco TrustSec 933
Plug-in Panorama pour Cisco TrustSec 934
Bulk Sync 934
PubSub 935
Installation du plug-in Panorama pour Cisco TrustSec 936
Configuration du plug-in Panorama pour Cisco TrustSec 937
Dépannage du plug-in Panorama pour Cisco TrustSec 945
Commandes d'état du plug-in 945
Commandes de débogage 945
Journaux de débogage 946

Configuration du pare-feu VM-Series sur Nutanix AHV 947
Surveillance VM sur Nutanix 948
À propos de la surveillance VM sur Nutanix 948
Installation du plug-in Panorama pour Nutanix 949
Configuration du plug-in Panorama pour Nutanix 950

Amorçage du pare-feu VM-Series 955
Choix d'une méthode d'amorçage 956
Configurations de base 957
Terminer la configuration 962
Flux d'amorçage du pare-feu VM-Series 963
Ensemble d'amorçage 965
Structure de l'ensemble d'amorçage 965
Livraison de l'ensemble d'amorçage 966
Fichiers de configuration d'amorçage 967

 ©2023 Palo Alto Networks, Inc.

init-cfg.txt 967
bootstrap.xml 967
Génération de la clé d'authentification VM sur Panorama 968
Création du fichier init-cfg.txt 970
Composants du fichier init-cfg.txt 971
Fichier init-cfg.txt modèle 975
Création du fichier bootstrap.xml 977
Préparation des licences pour l'amorçage 978
Préparation de l'ensemble d'amorçage 980
Amorçage du pare-feu VM-Series sur AWS 982
Amorçage du pare-feu VM-Series dans Azure 986
Amorçage du pare-feu VM-Series sur ESXi 989
Amorçage du pare-feu VM-Series sur ESXi avec un fichier ISO 989
Amorçage du pare-feu VM-Series sur ESXi avec un périphérique de stockage de bloc 989
Amorçage du pare-feu VM-Series sur la Google Cloud Platform 991
Amorçage du pare-feu VM-Series sur Hyper-V 993
Amorçage du pare-feu VM-Series sur Hyper-V avec un fichier ISO 993
Amorçage du pare-feu VM-Series sur Hyper-V avec un périphérique de stockage de bloc 994
Amorçage du pare-feu VM-Series sur KVM 996
Amorçage du pare-feu VM-Series sur KVM avec un fichier ISO 996
Amorçage du pare-feu VM-Series sur KVM avec un périphérique de stockage de bloc 997
Vérification d'achèvement de l'amorçage 998
Erreurs d'amorçage 999

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

À propos du pare-feu VM-Series

Le pare-feu VM-Series Palo Alto Networks est la forme virtualisée du pare-feu de dernière génération Palo Alto Networks. Il est destiné à être utilisé dans un environnement de cloud ou virtualisé où il peut protéger et sécuriser le trafic est-ouest et nord-sud.

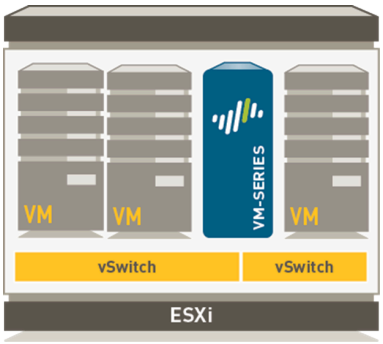
- Déploiements VM-Series
- VM-Series en haute disponibilité
- Mise à niveau du pare-feu VM-Series
- Plug-in VM-Series
- Activation des trames Jumbo sur le pare-feu VM-Series
- Adresses MAC attribuées par l'hyperviseur
- Publication de statistiques PAN-OS personnalisées pour la surveillance
- Interface utilisée pour accéder aux services externes sur le pare-feu VM-Series
- Support des pilotes PacketMMAP et DPDK
- Activation de l'optimisation des performances NUMA sur le VM-Series
- Activation du ZRAM sur le pare-feu VM-Series

Déploiements VM-Series

Le pare-feu VM-Series peut être déployé sur les plates-formes suivantes :

- **VM-Series pour VMware vSphere Hypervisor (ESXi) et vCloud Air**

  Vous pouvez déployer n'importe quel modèle VM-Series en tant que machine virtuelle invitée sur VMware ESXi ; ce qui est idéal pour le cloud ou les réseaux où le format virtuel est requis.

  Pour plus de détails, reportez-vous à la section Configuration d'un pare-feu VM-Series sur un serveur ESXi et Configuration du pare-feu VM-Series sur vCloud Air.

- **Pare-feu VM-Series sur VMware NSX-T**

  Vous pouvez déployer les modèles VM-100, VM-300, VM-500 ou VM-700 dans votre environnement NSX-T.

  Pour plus d'informations, reportez-vous à la section Configuration du pare-feu VM-Series sur VMware NSX-T (Nord-Sud).

- **VM-Series pour AWS (Amazon Web Services)**

  Vous pouvez déployer n'importe quel modèle VM-Series, à l'exception du VM-50, sur des instances EC2 du cloud AWS.

  Pour plus de détails, reportez-vous à la section Configuration du pare-feu VM-Series sur AWS.

- **VM-Series pour Google Cloud Platform**

  Vous pouvez déployer n'importe quel modèle de la série VM, à l'exception du VM-50 et du VM-50 Lite sur les instances de Google Compute Engine. Pour plus d'informations, reportez-vous à la section Configuration du pare-feu VM-Series sur la plateforme Google Cloud.

- **VM-Series pour KVM (Kernel Virtualization Module)**

  Vous pouvez déployer n'importe quel modèle VM-Series sur un serveur Linux exécutant l'hyperviseur KVM. Pour plus de détails, reportez-vous à la section Configuration du pare-feu VM-Series sur KVM.

- **Pare-feu VM-Series pour Microsoft Hyper-V**

  Vous pouvez déployer n'importe quel modèle VM-Series sur un serveur Windows Server 2012 R2 avec le complément de rôle Hyper-V activé ou sur un serveur Hyper-V 2012 R2 autonome. Pour plus de détails, reportez-vous à la section Configuration du pare-feu VM-Series sur Hyper-V.

©2023 Palo Alto Networks, Inc.

- **VM-Series pour Microsoft Azure**

  Vous pouvez déployer n'importe quel modèle de VM-Series, à l'exception du VM-50, sur Azure VNet.

  Pour plus de détails, reportez-vous à la section Configuration du pare-feu VM-Series sur Azure.

©2023 Palo Alto Networks, Inc.

VM-Series en haute disponibilité

La High Availability (haute disponibilité ; HA) est une configuration dans laquelle deux pare-feu sont placés dans un groupe et où leur configuration est synchronisée afin d'éviter tout point de défaillance unique sur votre réseau. Une connexion de pulsation entre les pare-feu homologues garantit un basculement transparent en cas d'arrêt d'un homologue. Le paramétrage des pare-feu dans un cluster composé de deux périphériques fournit une redondance et vous permet d'assurer la continuité de l'activité. Dans une configuration haute disponibilité sur les pare-feu VM-Series, les deux homologues doivent être déployés sur le même type d'hyperviseur, avoir des ressources matérielles identiques (telles que des cœurs de processeur/interfaces réseau) et avoir la même configuration de licences/abonnements. Pour des informations générales sur HA sur les pare-feu Palo Alto Networks, reportez-vous à la section Haute disponibilité.

Les pare-feu VM-Series prennent en charge la haute disponibilité à inspection d'état active/passive ou active/active avec synchronisation de la session et de la configuration. Le déploiement actif/actif est pris en charge dans les déploiements de câble virtuel et de couche 3 sur certains hyperviseurs cloud privés, et il est recommandé uniquement si chaque pare-feu doit posséder ses propres instances de routage et que vous devez compter sur une redondance complète en temps réel des deux pare-feu en tout temps. Pour configurer le pare-feu VM-Series en tant que paire HA, reportez-vous à la section Configuration de la HA active/passive dans AWS et Configuration de la HA active/active.

Si vous déployez le pare-feu VM-Series sur le cloud public, par exemple sur Amazon Web Services (AWS) ou Azure, vous pouvez utiliser la configuration HA active/passive traditionnelle. Reportez-vous aux sections Haute disponibilité des pare-feu VM-Series sur AWS et Configuration de la HA active/passive sur Azure. Sinon, en raison des différences innées dans la manière dont la redondance des ressources ou des régions est intégrée à l'infrastructure cloud par rapport à un centre de données privé, vous pouvez tirer parti des services cloud natifs et créer une architecture résiliente optimisant la disponibilité, reportez-vous à la section

- AWS : Mise à l'échelle automatique de pare-feu VM-Series avec Amazon ELB pour déployer plusieurs pare-feu sur deux ou plusieurs zones de disponibilité au sein d'un VPC.
- Azure : Paramètres du modèle VM-Series et Azure Application Gateway.

Caractéristiques/liaisons prises en charge	ESX	KVM	AWS	NSX V	NSX T (N/S)	Hyper-V	Azure	GCP	OCI
HA active/passive	Oui	Oui	Oui	Non	Oui	Oui	Oui	Non	Oui
HA active/active	Oui	Oui	Non	Non	Non	Oui	Non	Non	Non
HA 1	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui
HA 2 (synchronisation de session et persistance)	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui

©2023 Palo Alto Networks, Inc.

Caractéristiques/liaisons prises en charge	ESX	KVM	AWS	NSX V	NSX T (N/S)	Hyper-V	Azure	GCP	OCI
HA3	Oui	Oui	Non	Non	Non	Oui	Non	Non	Non

La prise en charge de HA1 et HA2 pour VM-Series sur GCP nécessite PAN-OS 10.0x ou version ultérieure et le plug-in VM-Series 2.0.5 ou version ultérieure.

La haute disponibilité pour le pare-feu VM-Series sur NSX-T (E/W) est atteinte grâce à la fonctionnalité NSX-T appelée « contrôle du fonctionnement du service ». Cette fonctionnalité NSX-T vous permet de simuler une haute disponibilité en cas de défaillance de l'instance de service. Lorsqu'il est configuré avec le pare-feu VM-Series, en cas de défaillance d'une instance de service VM-Series, tout le trafic acheminé vers ce pare-feu est redirigé vers une autre instance de pare-feu dans le cluster (pour les déploiements de cluster de service) ou une instance de pare-feu sur un autre hôte (pour les déploiements basés sur un hôte). Consultez Configuration de la définition de service sur Panorama pour le pare-feu VM-Series sur NSX-T (E/W) pour en savoir plus.

©2023 Palo Alto Networks, Inc.

Mise à niveau du pare-feu VM-Series

La mise à niveau de la version du logiciel PAN-OS ou du modèle VM-Series vous permet d'ajouter les dernières fonctionnalités et corrections qui améliorent la sécurité et les performances de vos pare-feu.

La version standard du logiciel PAN-OS se limite à la version normale de PAN-OS qui peut être installée sur tous les pare-feu Palo Alto Networks. Les versions XFR de PAN-OS sont prévues pour les pare-feu VM-Series uniquement et peuvent inclure de nouvelles fonctionnalités et des corrections de bogues pour les pare-feu VM-Series. Si vous installez une image XFR PAN-OS sur les pare-feu VM-Series, les fonctionnalités et les corrections ne seront pas disponibles dans les versions de PAN-OS antérieures à la version logicielle que vous avez installée.

Les images XFR comprennent des fonctionnalités et des corrections spécifiques aux pare-feu VM-Series : si vous mettez à niveau vers une version XFR, vous devez donc continuer avec des versions XFR afin de conserver les fonctionnalités spécifiques à XFR jusqu'à la prochaine version majeure de PAN-OS. Toutes les fonctionnalités et corrections disponibles dans XFR seront déployées de manière cumulative dans la prochaine version majeure de PAN-OS.

- Mise à niveau de la version du logiciel PAN-OS (version autonome)
- Pour mettre à niveau la version du logiciel PAN-OS (paire HA)
- Mise à niveau de la version du logiciel PAN-OS avec Panorama
- Mise à niveau de la version du logiciel PAN-OS (VM-Series pour NSX)
- Mise à niveau du modèle VM-Series
- Mise à niveau du modèle VM-Series d'une paire HA
- Rétrograder un pare-feu VM-Series vers une version antérieure

Pour obtenir des instructions sur l'installation de votre pare-feu VM-Series, reportez-vous à la section Déploiements VM-Series.

Vérifiez la section** Configuration système requise pour VM-Series **pour votre modèle de pare-feu avant la mise à niveau. Si votre pare-feu dispose d'une mémoire de moins de 5,5 Go, la capacité du système (nombre de sessions, règles, zones de sécurité, objets d'adresse, etc.) sur le pare-feu sera limitée à celle du VM-50 Lite.

Mise à niveau de la version du logiciel PAN-OS (version autonome)

Passez en revue les nouvelles fonctionnalités, les problèmes résolus et les problèmes connus, puis utilisez la procédure suivante pour mettre à niveau un pare-feu qui n'est pas dans une configuration HA.

Pour éviter tout impact sur le trafic, procédez à la mise à niveau pendant l'intervalle d'interruption. Assurez-vous que le pare-feu est branché à une source d'alimentation fiable. La perte de courant au cours d'une mise à niveau peut rendre ls pare-feu inutilisable.

©2023 Palo Alto Networks, Inc.

STEP 1 | Vérifiez que suffisamment de ressources matérielles sont disponibles pour le pare-feu VM-Series.

Reportez-vous à la Configuration système requise pour VM-Series pour voir les nouvelles exigences de ressources applicables à chaque modèle VM-Series. Allouez des ressources matérielles supplémentaires avant de poursuivre le processus de mise à niveau. Le processus d'allocation de ressources matérielles supplémentaires diffère selon chaque hyperviseur.

Si le pare-feu VM-Series ne dispose pas des ressources requises pour le modèle, sa capacité par défaut correspond à la capacité associée au VM-50.

STEP 2 | Dans l'interface Web, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que vous disposez de la licence correcte pour le pare-feu VM-Series et qu'elle est activée.

Sur le pare-feu VM-Series version autonome, accédez à **Device (Périphérique)** > **Support** et vérifiez que vous avez activé la licence de support.

STEP 3 | Faites une sauvegarde du fichier de configuration actuel.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**, puis cliquez sur **Export named configuration snapshot (Exporter l'instantané de configuration nommé)**.
2. Sélectionnez le fichier XML contenant la configuration actuelle (par exemple, **running-config.xml**), puis cliquez sur **OK** pour exporter le fichier de configuration.
3. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 4 | Si vous avez activé User-ID, après la mise à niveau, le pare-feu efface les mappages nom d'utilisateur/adresse IP et de groupe, afin que ces champs puissent être complétés avec les attributs depuis les sources User-ID. Pour estimer le temps nécessaire pour que votre environnement complète à nouveau les mappages, exécutez les commandes CLI suivantes sur le pare-feu.

- Pour les mappages nom d'utilisateur/adresse IP :
  - **`show user user-id-agent state all`**
  - **`show user server-monitor state all`**
- Pour les mappages de groupe : **`show user group-mapping statistics`**

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Assurez-vous que le pare-feu exécute la dernière version du contenu.

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mise à jour dynamiques)** et vérifiez les **Applications** ou **Applications and Threats (Applications et menaces)** pour déterminer la mise à jour qui est actuellement installée.
2. Si le pare-feu n'exécute pas la dernière version du contenu requise ou une version supérieure requise pour PAN-OS, cliquez sur **Check Now (Vérifier maintenant)** pour consulter la liste des mises à jour disponibles.
3. Trouvez et **téléchargez** la version du contenu souhaitée.

   Après avoir téléchargé avec succès un fichier de mise à jour du contenu, le lien dans la colonne Action passe de **Télécharger** à **Installer** pour cette version du contenu.
4. **Installez** la mise à jour.

STEP 6 | Mise à niveau du plug-in VM-Series.

1. Avant de procéder à la mise à niveau, consultez les dernières notes de version pour savoir si un nouveau plug-in VM-Series affecte votre environnement.

   Par exemple, supposons qu'une nouvelle version de plug-in VM-Series n'inclue que les fonctionnalités AWS. Pour tirer parti des nouvelles fonctionnalités, vous devez mettre à jour le plug-in sur vos instances de pare-feu VM-Series sur AWS.

   N'installez aucune mise à niveau qui ne s'applique pas à votre environnement.
2. Connectez-vous au pare-feu VM-Series et consultez le tableau de bord pour afficher la version du plug-in.
3. Sélectionnez **Device (Périphérique)** > **Plugins (Plug-ins)** pour savoir la version du plug-in. Utilisez **Check Now** (Vérifier maintenant) pour rechercher des mises à jour.
4. Sélectionnez la version du plug-in et cliquez sur **Install (Installer)** dans la colonne Action pour installer le plug-in.

©2023 Palo Alto Networks, Inc.

STEP 7 | Mettez à jour PAN-OS.

Si votre pare-feu ne possède pas d'accès Internet depuis le port de gestion, vous pouvez télécharger l'image logicielle depuis le portail d'assistance client Palo Alto Networks*, puis le* ***charger*** *manuellement sur votre pare-feu.*

1. Sélectionnez **Device (Périphérique)** > **Software (Logiciel)** et cliquez sur **Check Now (Vérifier maintenant)** pour afficher les dernières mises à jour PAN-OS.
2. Trouvez et **téléchargez** la version du PAN-OS cible.
3. Après avoir téléchargé l'image (ou après avoir chargé l'image pour une mise à niveau manuelle), **installez** l'image.
4. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et cliquez sur **Reboot Device (Redémarrer le périphérique)**.

   Le pare-feu efface alors les mappages User-ID, puis se connecte aux sources User-ID pour remplir à nouveau les mappages.
5. Si vous avez activé User-ID, utilisez les commandes CLI suivantes pour vérifier que le pare-feu a rempli à nouveau les mappages adresse IP/nom d'utilisateur et de groupe avant d'autoriser le trafic.
   - `show user ip-user-mapping all`
   - `show user group list`
6. Si vous mettez à niveau vers une version XFR pour la première fois, répétez cette étape pour mettre à niveau vers la version XFR correspondante.

STEP 8 | Vérifiez que le pare-feu fait passer le trafic.

Sélectionnez **Monitor (Surveiller)** > **Session Browser (Navigateur de session)** et vérifiez que vous voyez de nouvelles sessions.

Pour mettre à niveau la version du logiciel PAN-OS (paire HA)

Utilisez la procédure suivante pour mettre à jour une paire de pare-feu dans une configuration de haute disponibilité (High Availability - HA). Cette procédure s'applique aussi bien aux configurations actives/passives qu'actives/actives.

Pour éviter les temps d'arrêt lors de la mise à niveau des pare-feu qui sont en configuration de disponibilité élevée, mettre à jour un pair HA à la fois : Pour les pare-feu actifs/actifs, l'homologue que vous mettez à niveau en premier n'a pas d'importance (même si cette procédure explique comment mettre à niveau l'homologue secondaire actif en premier, dans un souci de simplicité). Pour les pare-feu actifs / passifs, vous devez d'abord mettre à niveau l'homologue passif, suspendre l'homologue actif (basculement), mettre à jour l'homologue actif, puis ramener cet homologue à un état fonctionnel (retour arrière). Afin d'éviter un basculement lors de la mise à niveau des homologues HA, assurez-vous que la préemption est désactivée avant de poursuivre la mise à niveau. Vous devez uniquement désactiver la préemption sur un homologue de la paire.

 ©2023 Palo Alto Networks, Inc.

Pour éviter tout impact sur le trafic, procédez à la mise à niveau pendant l'intervalle d'interruption. Assurez-vous que les pare-feu sont branchés à une source d'alimentation fiable. La perte de courant au cours d'une mise à niveau peut rendre les pare-feu inutilisables.

STEP 1 | Vérifiez que suffisamment de ressources matérielles sont disponibles pour le pare-feu VM-Series.

Reportez-vous à la Configuration système requise pour VM-Series pour voir les nouvelles exigences de ressources applicables à chaque modèle VM-Series. Allouez des ressources matérielles supplémentaires avant de poursuivre le processus de mise à niveau. Le processus d'allocation de ressources matérielles supplémentaires diffère selon chaque hyperviseur.

Si le pare-feu VM-Series ne dispose pas des ressources requises pour le modèle, sa capacité par défaut correspond à la capacité associée au VM-50.

STEP 2 | Dans l'interface Web, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que vous disposez de la licence correcte pour le pare-feu VM-Series et qu'elle est activée.

Sur le pare-feu VM-Series version autonome, accédez à **Device (Périphérique)** > **Support** et vérifiez que vous avez activé la licence de support.

STEP 3 | Faites une sauvegarde du fichier de configuration actuel.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

Effectuez ces étapes sur chaque pare-feu dans la paire :

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**, puis cliquez sur **Export named configuration snapshot (Exporter l'instantané de configuration nommé)**.
2. Sélectionnez le fichier XML contenant la configuration actuelle (par exemple, **running-config.xml**), puis cliquez sur **OK** pour exporter le fichier de configuration.
3. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 4 | Si vous avez activé User-ID, après la mise à niveau, le pare-feu efface les mappages nom d'utilisateur/adresse IP et de groupe, afin que ces champs puissent être complétés avec les attributs depuis les sources User-ID. Pour estimer le temps nécessaire pour que votre environnement complète à nouveau les mappages, exécutez les commandes CLI suivantes sur le pare-feu.

- Pour les mappages nom d'utilisateur/adresse IP :
  - **`show user user-id-agent state all`**
  - **`show user server-monitor state all`**
- Pour les mappages de groupe : **`show user group-mapping statistics`**

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Assurez-vous que chaque pare-feu dans la paire HA exécute la dernière version du contenu.

Consultez les Release Notes (Notes de publication) pour la version de contenu minimale que vous devez installer pour une version de PAN-OS 10.2. Assurez-vous de suivre les meilleures pratiques pour les mises à jour du contenu de menace et des applications.

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mise à jour dynamiques)** et vérifiez les **Applications** ou **Applications and Threats (Applications et menaces)** pour déterminer la mise à jour qui est actuellement installée.
2. Si les pare-feu n'exécutent pas la dernière version du contenu requise ou une version supérieure requise pour la version logicielle que vous installez, cliquez sur **Check Now (Vérifier maintenant)** pour consulter la liste des mises à jour disponibles.
3. Trouvez et **téléchargez** la version du contenu souhaitée.

   Après avoir téléchargé avec succès un fichier de mise à jour du contenu, le lien dans la colonne Action passe de **Télécharger** à **Installer** pour cette version du contenu.
4. **Installez** la mise à jour. Vous devez installer la mise à jour sur les deux homologues.

STEP 6 | Mise à niveau du plug-in VM-Series.

1. Avant de procéder à la mise à niveau, consultez les dernières notes de version pour savoir si un nouveau plug-in VM-Series affecte votre environnement.

   Par exemple, supposons qu'une nouvelle version de plug-in VM-Series n'inclue que les fonctionnalités AWS. Pour tirer parti des nouvelles fonctionnalités, vous devez mettre à jour le plug-in sur vos instances de pare-feu VM-Series sur AWS.

   N'installez aucune mise à niveau qui ne s'applique pas à votre environnement.
2. Connectez-vous au pare-feu VM-Series et consultez le tableau de bord pour afficher la version du plug-in.
3. Sélectionnez **Device (Périphérique)** > **Plugins (Plug-ins)** pour savoir la version du plug-in. Utilisez **Check Now** (Vérifier maintenant) pour rechercher des mises à jour.
4. Sélectionnez la version du plug-in et cliquez sur **Install (Installer)** dans la colonne Action pour installer le plug-in.

   Lors de l'installation de la fiche sur les pare-feu VM-Series d'une paire HA, installez la fiche sur le pair passif avant le pair actif. Après avoir installé le plug-in sur l'homologue passif, il passera à un état non fonctionnel. L'installation du plug-in sur l'homologue actif renvoie l'homologue passif à un état fonctionnel.

STEP 7 | Désactivez la préemption sur le premier homologue de chaque paire. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans la paire HA, mais assurez-vous que la validation est réussie avant de continuer la mise à niveau.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** et modifiez les **Election Settings (Paramètres de sélection)**.
2. si cette option est activée, désactivez (effacez) le **Preemptive (paramètre préemptif)** et cliquez sur **OK**.
3. **Commit (Validez)** la modification.

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Installez la version du logiciel PAN-OS sur le premier homologue.

Afin de réduire l'interruption dans une configuration active/passive, mettez à niveau l'homologue passif en premier. Pour une configuration active/active, mettez à niveau l'homologue secondaire en premier. Si vous utilisez une configuration active/active, nous vous conseillons en guise de bonne pratique de mettre à niveau les deux homologues lors du même intervalle de maintenance.

Si vous souhaitez vérifier que l'HA fonctionne correctement avant la mise à niveau, mettez à niveau l'homologue actif dans une configuration active/passive en premier afin de vous assurer que le basculement se déroule parfaitement.

1. Pour le premier homologue, sélectionnez **Device (Périphérique)** > **Software (Logiciel)** et cliquez sur **Check Now (Vérifier maintenant)** pour les dernières mises à jour.
2. Trouvez et **téléchargez** la version du PAN-OS cible.

   Si votre pare-feu ne possède pas d'accès Internet depuis le port de gestion, vous pouvez télécharger l'image logicielle depuis le portail d'assistance Palo Alto Networks*, puis le* ***charger*** *manuellement sur votre pare-feu.*
3. Après avoir téléchargé l'image (ou après avoir chargé l'image pour une mise à niveau manuelle), **installez** l'image.
4. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.
5. Une fois que le périphérique a terminé le redémarrage, consultez le widget Haute disponibilité sur le **Dashboard (Tableau de bord)** et vérifiez que le périphérique que vous venez de mettre à jour est toujours l'homologue passif ou actif-secondaire dans la configuration HA.

©2023 Palo Alto Networks, Inc.

STEP 9 | Installez la version du logiciel PAN-OS sur le deuxième homologue.

1. (Configurations actives/passives uniquement) Suspendez l'homologue actif afin que l'HA bascule vers l'homologue que vous venez de mettre à jour.
   1. Pour l'homologue actif, sélectionnez **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**, puis cliquez sur le lien **Suspend local device (Suspendre le périphérique local)**.
   2. Consultez le widget High Availability (haute disponibilité - HA) sur le **Dashboard (Tableau de bord)** et vérifiez que l'état passe à **Passive (Passif)**.
   3. Vérifiez que l'autre homologue est actif et fait passer le trafic (**Monitor (Surveiller)** > **Session Browser (Navigateur de session)**).
2. Pour le deuxième homologue, sélectionnez **Device (Périphérique)** > **Software (Logiciel)** et cliquez sur **Check Now (Vérifier maintenant)** pour les dernières mises à jour.
3. Trouvez et **téléchargez** la version du PAN-OS cible.
4. Une fois que vous avez téléchargé l'image, **installez**-la.
5. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.
6. (Configurations actives/passives uniquement) À partir de la CLI de l'homologue que vous venez de mettre à niveau, exécutez la commande suivante pour rendre le pare-feu de nouveau fonctionnel :

   `request high-availability state functional (demande de fonctionnement d'état de haute disponibilité)`

©2023 Palo Alto Networks, Inc.

STEP 10 | Vérifiez que les deux homologues font passer le trafic comme prévu.

Dans une configuration active/passive, seul l'homologue actif doit faire passer le trafic ; les deux homologues doivent faire passer le trafic dans une configuration active/active.

Exécutez les commandes CLI suivantes pour confirmer la réussite de la mise à niveau :

- (Homologues actifs uniquement) Pour vérifier que les homologues actifs font passer le trafic, exécutez la commande **`show session all (Montrer toutes les sessions)`** command.
- Pour vérifier la synchronisation des sessions, exécutez la **`show high-availability interface ha2`** et assurez-vous que les compteurs d'interface matérielle de la table du processeur augmentent comme suit :
  - Dans une configuration active/passive, seul l'homologue actif affiche les paquets transmis ; l'homologue passif affiche uniquement les paquets reçus.

    Si vous avez activé HA2 keep-alive (Maintien HA2), les compteurs d'interface matérielle sur l'homologue passif affichent à la fois les paquets de transmission et de réception. Cela se produit car HA2 keep-alive (Maintien HA2) est bidirectionnel, ce qui signifie que les deux homologues transmettent des paquets HA2 keep-alive (Maintien HA2).
  - Dans la configuration active/active, les paquets reçus et les paquets transmis s'affichent sur les deux homologues.

STEP 11 | Si vous avez désactivé la préemption avant la mise à niveau, vous pouvez maintenant la réactiver.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** et modifiez les **Election Settings (Paramètres de sélection)**.
2. Sélectionnez **Preemptive (Préemptif)** et cliquez sur **OK**.
3. **Commit (Validez)** la modification.

Mise à niveau de la version du logiciel PAN-OS avec Panorama

Utilisez la procédure suivante pour mettre à niveau les pare-feu que vous gérez avec Panorama. Cette procédure s'applique aux pare-feu autonomes et aux pare-feu déployés dans une configuration à haute disponibilité (HA).

Si Panorama ne parvient pas à se connecter directement au serveur de mises à jour, suivez la procédure pour déployer des mises à jour des pare-feu lorsque Panorama n'est pas connecté à Internet ***afin de pouvoir télécharger manuellement des images dans Panorama, puis les distribuer les images sur le pare-feu.***

Avant de faire la mise-à-jour du pare-feu sur Panorama, vous devez :

- ☐ Assurez-vous que Panorama exécute la même version ou une version ultérieure de PAN-OS que celle utilisée pour la mise à niveau. Vous devez mettre à niveau Panorama et ses Log Collectors (Collecteurs de journaux) vers la version 9.1 avant de mettre à niveau les pare-feu gérés vers cette version. Lorsque vous mettez à niveau les collecteurs de journaux vers la version 9.1, vous devez mettre à niveau tous les collecteurs de journaux en même temps en raison des modifications de l'infrastructure de journalisation.

 ©2023 Palo Alto Networks, Inc.

- Prévoyez un intervalle de maintenance prolongée, qui peut durer six heures, pour la mise à niveau de Panorama vers la version 9.1. Cette version comprend des modifications importantes au niveau de l'infrastructure, ce qui signifie que la mise à niveau de Panorama prendra plus de temps que pour les versions précédentes.
- Assurez-vous que les pare-feu sont branchés à une source d'alimentation fiable. La perte de courant au cours d'une mise à niveau peut rendre les pare-feu inutilisables.

STEP 1 | Après avoir mis Panorama à niveau, validez et appliquez la configuration aux pare-feu que vous prévoyez de mettre à niveau.

STEP 2 | Vérifiez que suffisamment de ressources matérielles sont disponibles pour le pare-feu VM-Series.

Reportez-vous à la Configuration système requise pour VM-Series pour voir les nouvelles exigences de ressources applicables à chaque modèle VM-Series. Allouez des ressources matérielles supplémentaires avant de poursuivre le processus de mise à niveau. Le processus d'allocation de ressources matérielles supplémentaires diffère selon chaque hyperviseur.

Si le pare-feu VM-Series ne dispose pas des ressources requises pour le modèle, sa capacité par défaut correspond à la capacité associée au VM-50.

STEP 3 | Dans l'interface Web, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que vous disposez de la licence correcte pour le pare-feu VM-Series et qu'elle est activée.

Sur le pare-feu VM-Series version autonome, accédez à **Device (Périphérique)** > **Support** et vérifiez que vous avez activé la licence de support.

STEP 4 | Effectuez une copie de sauvegarde du fichier de configuration actuel sur chaque pare-feu géré que vous envisagez de mettre à niveau.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il est recommandé de créer et de stocker une sauvegarde externe avant de procéder à la mise à niveau.

1. À partir de l'interface web de Panorama, sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et cliquez sur **Export Panorama and devices config bundle (Exporter le groupe de configuration des périphériques et de Panorama)** pour générer et exporter la dernière sauvegarde de configuration de Panorama et de chaque appareil géré.
2. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 5 | Mettez à jour la version de contenu sur les pare-feu que vous prévoyez de mettre à niveau.

Consultez les Release Notes (Notes de publication) pour la version de contenu minimale que vous devez installer pour PAN-OS 10.2. Assurez-vous que vous utilisez les meilleures pratiques pour les mises à jour d'applications et de menaces lorsque vous déployez des mises à jour de Panorama et des pare-feu que vous gérez.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Dynamic Updates (Mises à jour dynamiques)** et **Check Now (Vérifiez maintenant)** pour obtenir les dernières mises à jour. Si une mise à jour est disponible, la colonne Action affiche un lien **Download (Télécharger)**.

 ©2023 Palo Alto Networks, Inc.

2. Si elle n'est pas déjà installée, **Download (Téléchargez)** la dernière version du contenu.
3. Cliquez sur **Install (Installer)** et sélectionnez les pare-feu sur lesquels vous voulez installer la mise à jour et cliquez sur **OK**. Si vous mettez à niveau des pare-feu HA, vous devez mettre à jour le contenu des deux homologues.

STEP 6 | (Mises à niveau du pare-feu HA uniquement) Si vous mettez à niveau des pare-feu faisant partie d'une paire haute disponibilité, désactivez la préemption. Vous devez uniquement désactiver ce paramètre sur un pare-feu dans chaque paire haute disponibilité.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** et modifiez les **Election Settings (Paramètres de sélection)**.
2. si cette option est activée, désactivez (effacez) le **Preemptive (paramètre préemptif)** et cliquez sur **OK**.
3. **Commit (Validez)** la modification. Assurez que la validation est un succès avant de procéder à la mise-à-jour.

STEP 7 | Téléchargez l'image de version cible de PAN-OS.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)** et **Check Now (Vérifiez maintenant)** pour obtenir les dernières versions.
2. **Download (Téléchargez)** le(s) fichier(s) spécifique du pare-feu pour la version finale vers laquelle vous effectuez la mise à niveau. Vous devez télécharger un fichier d'installation distinct pour chaque modèle de pare-feu (ou série de pare-feu) que vous avez l'intention de mettre à niveau.

STEP 8 | Installer la mise à jour logicielle PAN-OS sur les pare-feu.

1. Cliquez sur **Install (Installer)** dans la colonne Action correspondant aux modèles de pare-feu que vous souhaitez mettre à niveau.
2. Dans la boîte de dialogue Déployer le fichier logiciel, sélectionnez tous les pare-feu que vous souhaitez mettre à niveau. Pour réduire les temps d'arrêt, sélectionnez uniquement un pair dans chaque paire HA. Pour les paires actives / passives, sélectionnez l'homologue passif; pour les paires actives / actives, sélectionnez l'homologue actif-secondaire.
3. (Mises à niveau des pare-feu HA uniquement) Assurez-vous que le **Group HA Peers (Groupe d'homologues HA)** n'est pas sélectionné.
4. Sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**.
5. Pour débuter la mise à jour, cliquez sur **OK**.
6. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.
7. Après que le pare-feu a terminé le redémarrage, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** et vérifiez que la version du logiciel est 9.1.0 pour les pare-feux que vous avez mis à niveau. Vérifiez également que le statut HA de tous les pare-feu passifs mis à niveau est toujours passif.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | (Mise à niveau des pare-feu HA uniquement) Mettez à niveau le deuxième pair HA dans chaque paire HA.

1. (Mises à niveau active/passive uniquement) Suspendez le périphérique actif dans chaque paire active / passive que vous mettez à niveau.
   1. Basculez le contexte vers le pare-feu actif.
   2. Dans le widget de haute disponibilité sur le **Dashboard (Tableau de bord)**, vérifiez que l'état du pare-feu **Local** est **Active (Actif)** et que le **Peer (Homologue)** est **Passive (Passif)**).
   3. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)** > **Suspend local device (Suspendre le périphérique local)**.
   4. Revenez au widget Haute disponibilité sur le **Dashboard (Tableau de bord)** et vérifiez que **Local** est passé à **Passive (Passif)** et que **Peer (Homologue)** est passé à **Active (Actif)**.
2. Retournez sur Panorama et sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Software (Logiciel)**.
3. Cliquez sur **Install (Installer)** dans la colonne Action correspondant aux modèles de HA que vous souhaitez mettre à niveau.
4. Dans la boîte de dialogue Déployer le fichier logiciel, sélectionnez tous les pare-feu que vous souhaitez mettre à niveau. Cette fois, sélectionnez uniquement les homologues des pare-feu HA que vous venez de mettre à jour.
5. Assurez-vous que le **Group HA Peers (Groupe de paire HA)** n'est pas sélectionné.
6. Sélectionnez **Reboot device after install (Redémarrer le périphérique après l'installation)**.
7. Pour débuter la mise à jour, cliquez sur **OK**.
8. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, sélectionnez **Device (Périphérique)** > **Configuration** > **Operations (Opérations)** et **Reboot Device (Redémarrez le périphérique)**.
9. (Mises à niveau active/passive uniquement) À partir de la CLI de l'homologue que vous venez de mettre à niveau, exécutez la commande suivante pour rendre le pare-feu de nouveau fonctionnel :

   ```
   request high-availability state functional
   ```

STEP 10 | (Mise à niveau PAN-OS XFR uniquement) Mettez à niveau le premier homologue et le deuxième vers PAN-OS XFR en répétant l'étape 8 et l'étape 9.

STEP 11 | Vérifiez la version du logiciel et du contenu qui s'exécute sur chaque pare-feu géré.

1. Sur Panorama, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)**.
2. Localisez les pare-feu et examinez les versions de contenu et logicielles dans le tableau.

   Pour les pare-feu HA, vous pouvez également vérifier que l'état HA de chaque homologue est conforme aux attentes.

©2023 Palo Alto Networks, Inc.

STEP 12 | (Mises à niveau des pare-feu HA uniquement)Si vous avez désactivé la préemption sur l'un de vos pare-feu haute disponibilité avant de procéder à la mise à niveau, modifiez les **Election Settings (Paramètres d'élection)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)**) et réactivez le paramètre **Preemptive (Préemptif)** pour ce pare-feu, puis **Commit (Validez)** le changement.

Mise à niveau de la version du logiciel PAN-OS (VM-Series pour NSX)

Choisissez la méthode de mise à niveau qui convient le mieux à votre déploiement.

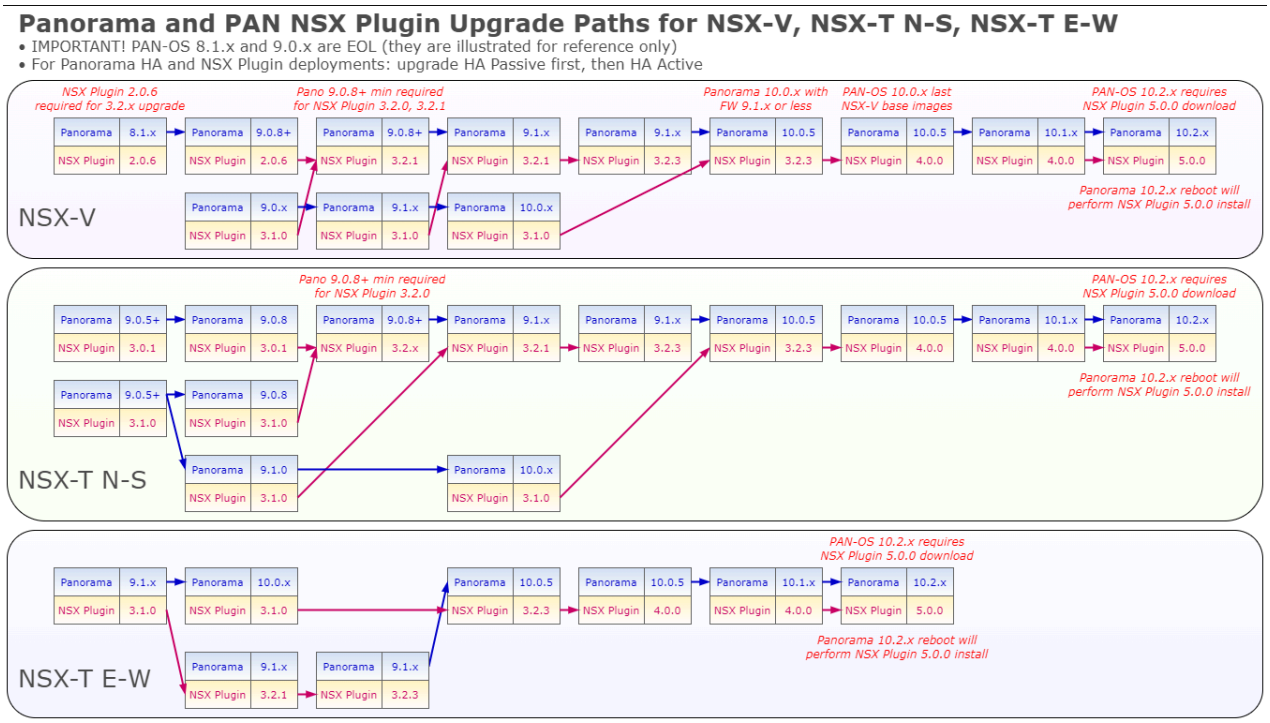
- Upgrade the VM-Series for NSX During a Maintenance Window (Mettre à niveau le VM-Series pour NSX pendant une fenêtre de maintenance) :utilisez cette option pour mettre à niveau le pare-feu VM-Series pendant une fenêtre de maintenance sans modifier l'URL OVF dans la définition de service.
- Upgrade the VM-Series for NSX without disrupting traffic (Mettre à niveau le VM-Series pour NSX sans perturber le trafic) : utilisez cette option pour mettre à niveau le pare-feu VM-Series sans interrompre le service aux VM invitées ou changer l'URL OVF dans la définition du service.

Le graphique suivant montre les combinaisons actuellement prises en charge de Panorama et du plug-in Panorama pour VMware NSX, ainsi que les procédures de mise à niveau que vous devez suivre pour une mise à niveau réussie.

- Chaque case ci-dessous représente une combinaison prise en charge.
- Lorsque vous mettez à niveau le plug-in Panorama pour NSX ou Panorama dans une paire HA, mettez d'abord à niveau l'homologue Panorama passif, puis l'homologue HA actif.

Avant de mettre à niveau votre VM-Series pour le déploiement de VMware NSX, passez en revue les procédures de mise à niveau indiquées ci-dessous pour comprendre les étapes de mise à niveau permettant de parvenir à la combinaison de plug-in et de PAN-OS qui convient le mieux à votre environnement.

 ©2023 Palo Alto Networks, Inc.



Mise à niveau de la VM-series pour le NSX durant une fenêtre de maintenance

Pour le pare-feu VM-Series Édition NSX, utilisez Panorama pour mettre à niveau la version logicielle sur les pare-feu.

STEP 1 | Passez en revue VM-Series pour les procédures de mise à niveau de VMware NSX.

STEP 2 | Allouez des ressources matérielles supplémentaires à votre pare-feu VM-Series.

Vérifiez que suffisamment de ressources matérielles sont disponibles pour le pare-feu VM-Series. Reportez-vous à Configuration système requise pour VM-Series pour voir les nouvelles exigences de ressources pour chaque modèle VM-Series. Allouez des ressources matérielles supplémentaires avant de poursuivre le processus de mise à niveau. Le processus d'attribution de ressources matérielles supplémentaires diffère sur chaque hyperviseur.

©2023 Palo Alto Networks, Inc.

STEP 3 | Effectuez une copie de sauvegarde du fichier de configuration actuel sur chaque pare-feu géré que vous envisagez de mettre à niveau.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il convient d'effectuer une copie de sauvegarde avant de mettre à niveau et de l'enregistrer en externe.

1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Operations (Opérations)**, puis cliquez sur **Export Panorama and devices config bundle (Exporter la solution de configuration des appareils et de Panorama)**. Cette option est utilisée pour générer et exporter manuellement la dernière version de la sauvegarde de configuration de Panorama et celle de chaque périphérique géré.
2. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 4 | Consultez les notes de publication afin de vérifier la version de contenu requise pour la version de PAN-OS.

Les pare-feu dont vous envisagez une mise à niveau doivent exécuter la version de contenu requise pour la version de PAN-OS.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement d'appareils)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Recherchez les dernières mises à jour. Cliquez sur Check Now (Vérifier maintenant) (situé dans le coin inférieur gauche de la fenêtre) pour vérifier les dernières mises à jour. Le lien dans la colonne Action indique si une mise à jour est disponible. Si une version est disponible, le lien **Download (Télécharger)** s'affiche.
3. Cliquez sur **Télécharger (Télécharger)** pour télécharger la version sélectionnée. Une fois le téléchargement terminé, le lien se trouvant dans la colonne **Action** passe de **Télécharger (Télécharger)** à **Install (Installer)**.
4. Cliquez sur **Install (Installer)** et sélectionnez les périphériques sur lesquels vous voulez installer la mise à jour. Une fois l'installation terminée, une coche s'affiche dans la colonne **Currently Installed (Actuellement installé)**.

STEP 5 | Déployez les mises à jour logicielles sur les pare-feu sélectionnés.

*Si vos périphériques sont configurés en HA, veillez à décocher la case **Group HA Peers (Regrouper les homologues HA)** et mettez à niveau un homologue HA à la fois.*

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement d'appareils)** > **Software (Logiciel)**.
2. Recherchez les dernières mises à jour. Cliquez sur **Check Now (Vérifier maintenant)** (situé dans le coin inférieur gauche de la fenêtre) pour vérifier les dernières mises à jour. Le lien dans la colonne **Action** indique si une mise à jour est disponible.
3. Consultez le **File Name (Nom de fichier)** et cliquez sur **Télécharger (Télécharger)**. Vérifiez que les versions de logiciel que vous téléchargez correspondent à celles des modèles de

 ©2023 Palo Alto Networks, Inc.

pare-feu déployés sur votre réseau. Une fois le téléchargement terminé, le lien se trouvant dans la colonne **Action** passe de **Télécharger (Télécharger)** à **Install (Installer)**.

4. Cliquez sur **Install (Installer)** et sélectionnez les périphériques sur lesquels vous voulez installer la version de logiciel.
5. Sélectionnez **Reboot device after install (Redémarrer après l'installation)**, puis cliquez sur **OK**.
6. Si vous disposez de périphériques configurés en HA, décochez la case **Group HA Peers (Regrouper les homologues HA)** et mettez à niveau un homologue HA à la fois.

STEP 6 | Vérifiez la version logicielle et de contenu exécutée sur chaque périphérique géré.

1. Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)**.
2. Localisez le(s) périphérique(s) et examinez les versions de contenu et de logiciel sur le tableau.

Mise à niveau de la VM-series pour le NSX sans perturber le flux

Utilisez la procédure suivante pour mettre à niveau la version PAN-OS des pare-feu de la série VM dans votre environnement VMware NSX. Cette procédure vous permet d'effectuer la mise à niveau PAN-OS sans perturber le trafic en migrant des MV vers différents hôtes ESXi.

STEP 1 | Passez en revue VM-Series pour les procédures de mise à niveau de VMware NSX.

STEP 2 | Effectuez une copie de sauvegarde du fichier de configuration actuel sur chaque pare-feu géré que vous envisagez de mettre à niveau.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il convient d'effectuer une copie de sauvegarde avant de mettre à niveau et de l'enregistrer en externe.

1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Operations (Opérations)**, puis cliquez sur **Export Panorama and devices config bundle (Exporter la solution de configuration des appareils et de Panorama)**. Cette option est utilisée pour générer et exporter manuellement la dernière version de la sauvegarde de configuration de Panorama et celle de chaque périphérique géré.
2. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la mise à niveau.

STEP 3 | Consultez les notes de publication afin de vérifier la version de contenu requise pour la version de PAN-OS.

Les pare-feu dont vous envisagez une mise à niveau doivent exécuter la version de contenu requise pour la version de PAN-OS.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement d'appareils)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Recherchez les dernières mises à jour. Cliquez sur Check Now (Vérifier maintenant) (situé dans le coin inférieur gauche de la fenêtre) pour vérifier les dernières mises à jour. Le

 ©2023 Palo Alto Networks, Inc.

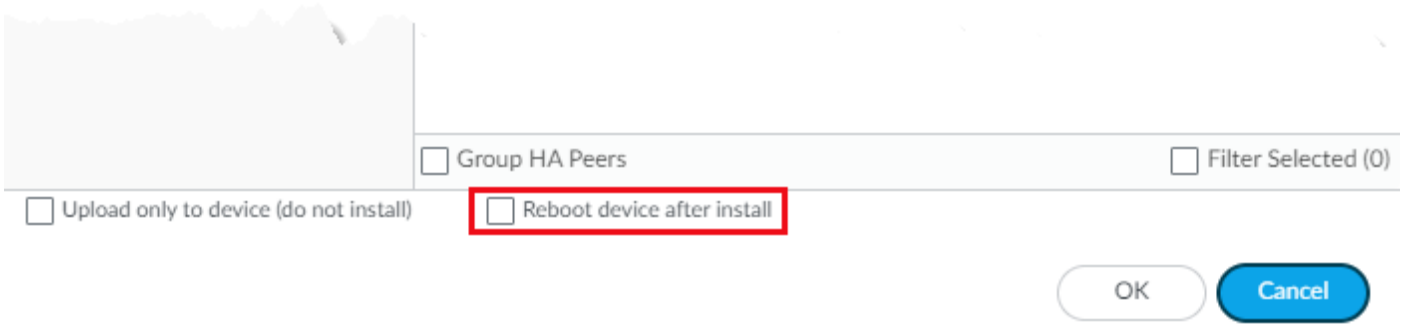
lien dans la colonne Action indique si une mise à jour est disponible. Si une version est disponible, le lien **Download (Télécharger)** s'affiche.

3. Cliquez sur **Télécharger (Télécharger)** pour télécharger la version sélectionnée. Une fois le téléchargement terminé, le lien se trouvant dans la colonne **Action** passe de **Télécharger (Télécharger)** à **Install (Installer)**.
4. Cliquez sur **Install (Installer)** et sélectionnez les périphériques sur lesquels vous voulez installer la mise à jour. Une fois l'installation terminée, une coche s'affiche dans la colonne **Currently Installed (Actuellement installé)**.

STEP 4 | Téléchargez l'image PAN-OS sur tous les pare-feu de la série VM dans l'amas.

1. Connectez-vous à Panorama.
2. Sélectionnez **Panorama** > **Device Deployment (Déploiement d'appareils)** > **Software (Logiciel)**.
3. Cliquez sur **Refresh (Actualiser)** pour afficher la dernière version du logiciel et consultez les **Release Notes (Notes de publication)** pour obtenir la description des modifications de la version et le chemin de migration pour installer le logiciel.
4. Cliquez sur **Download (Télécharger)** pour obtenir le logiciel, puis sur **Install (Installer)**.

   Ne pas redémarrer les pare-feu de la série VM après avoir installé la nouvelle image logicielle.
5. Sélectionnez les appareils gérés à mettre à niveau.
6. Cochez la case **Reboot device after install (Redémarrer le dispositif après l'installation)**



7. Cliquez sur **OK**.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Mettre à niveau le pare-feu de la série VM sur le premier hôte ESXi du groupe.

1. Connectez-vous à vCenter.
2. Sélectionnez **Hosts and Clusters (Hôtes et grappes)**.
3. Cliquez à droite sur l'hôte et sélectionnez **Maintenance Mode (Mode de maintenance)** > **Enter Maintenance Mode (Entrer mode de maintenance)**.
4. Migrer (automatiquement ou manuellement) toutes les MV, sauf le pare-feu de la série VM, hors de l'hôte.
5. Mettez le pare-feu VM-Series hors tension. Cela devrait se faire automatiquement au moment d'entrer en mode maintenance sur l'hôte.
6. (Facultatif) Attribuez des UCT ou une mémoire supplémentaires au pare-feu de la série VM avant de poursuivre le processus de mise à niveau.

   Vérifiez que suffisamment de ressources matérielles sont disponibles pour le pare-feu VM-Series. Reportez-vous à Modèles VM-Series pour voir les nouvelles exigences de ressources pour chaque modèle VM-Series.
7. Clique de droite sur l'hôte et sélectionnez **Maintenance Mode (Mode de maintenance)** > **Enter Maintenance Mode (Entrer mode de maintenance)**. La sortie du mode de maintenance entraîne l'alimentation du NSX ESX Agent Manager (EAM) sur le pare-feu de la série VM. Le pare-feu redémarre avec la nouvelle version PAN-OS.
8. Transférer (automatiquement ou manuellement) toutes les MV à l'hôte initial.

STEP 6 | Répétez ce processus pour chaque pare-feu de série VM sur chaque hôte ESXi.

STEP 7 | Vérifiez la version logicielle et de contenu exécutée sur chaque périphérique géré.

1. Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)**.
2. Localisez le(s) périphérique(s) et examinez les versions de contenu et de logiciel sur le tableau.

Mise à niveau du modèle VM-Series

Le processus de licence du pare-feu VM-Series utilise l'UUID et l'ID de processeur pour générer un numéro de série unique pour chaque pare-feu VM-Series. Par conséquent, lorsque vous générez une licence, celle-ci est mappée à une instance spécifique du pare-feu VM-Series et ne peut être modifiée.

Suivez les instructions de cette section si vous :

- migrez depuis une licence d'évaluation vers une licence de production ;
- mettez à niveau le modèle pour en augmenter la capacité. Par exemple, vous souhaitez effectuer une mise à niveau depuis le modèle VM-100 vers le modèle VM-300.

©2023 Palo Alto Networks, Inc.

- *mettez à niveau la capacité, ce qui redémarre certains processus critiques sur le pare-feu. Une configuration HA est recommandée pour minimiser les interruptions de service. Pour mettre à niveau la capacité sur une paire HA, reportez-vous à la section* Mise à niveau du modèle VM-Series d'une paire HA.
- *dans un déploiement de cloud privé ou public, si votre pare-feu est sous licence avec l'option BYOL, vous devez* désactiver votre VM *avant de modifier le type d'instance ou le type de VM. La mise à niveau du modèle ou de l'instance modifie l'UUID et l'ID du processeur, vous devez donc appliquer la licence lorsque le .*

STEP 1 | Allouez des ressources matérielles supplémentaires à votre pare-feu VM-Series.

Avant d'initier la mise à niveau de capacité, vous devez vérifier que le pare-feu VM-Series dispose de suffisamment de ressources matérielles pour prendre en charge la nouvelle capacité. Le processus d'attribution de ressources matérielles supplémentaires diffère sur chaque hyperviseur.

Pour vérifier la configuration matérielle requise pour votre nouveau modèle VM-Series, reportez-vous à la section Modèles VM-Series.

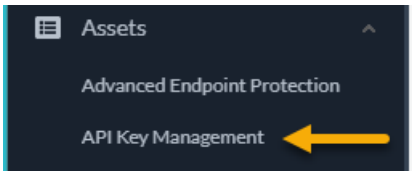
Bien que la mise à niveau de la capacité ne nécessite pas de redémarrage du pare-feu VM-Series, vous devez mettre la machine virtuelle hors tension pour modifier l'allocation matérielle.

STEP 2 | Récupérez la clé API de licence à partir du portail de support client.

1. Ouvrez une session dans le portail de support client.

   Assurez-vous que vous utilisez le même compte que vous avez utilisé pour enregistrer la licence initiale.

2. Dans le menu de gauche, sélectionnez **Assets (Ressources)** > **API Key Management (Gestion de clé API)**.
3. Copiez la clé API.



STEP 3 | Sur le pare-feu, utilisez la CLI pour installer la clé API copiée à l'étape précédente.

```
request license api-key set key <key>
```

STEP 4 | (Si vous avez accès à Internet) Autorisez le pare-feu à **Verify Update Server identity (Vérifier l'identité du serveur de mise à jour)** dans **Device (Périphérique)** > **Setup (Configuration)** > **Service**.

STEP 5 | **Commit (Validez)** vos modifications. Assurez-vous d'avoir un utilisateur configuré au niveau local sur le pare-feu. Les utilisateurs transmis sur Panorama peuvent ne pas être disponibles après la désactivation si la configuration dépasse la limite d'objets PA-VM sans licence.

STEP 6 | Mettez à niveau la capacité.

 ©2023 Palo Alto Networks, Inc.

Sélectionnez **Device (Appareil)** > **Licenses (Licences)** > **Upgrade VM Capacity (Mettre à jour la fonctionnalité VM)**, puis activez vos licences et vos abonnements de l'une des manières suivantes :

- (internet) **Retrieve license keys from license server (Récupérer les clés de licence auprès du serveur de licences)** : utilisez cette option si vous avez activé votre licence sur le portail de support client.
- (internet) **Use an authorization code (Utiliser un code d'autorisation)** : utilisez cette option pour mettre à niveau la capacité de VM-Series à l'aide d'un code d'autorisation pour les licences qui n'ont pas été précédemment activées sur le portail de support. Lorsque vous y êtes invité, saisissez le **Authorization Code (Code d'autorisation)**, puis cliquez sur **OK (OK)**.
- (aucune connexion internet) **Manually upload license key (Charger manuellement la clé de licence)** : utilisez cette option si votre pare-feu ne dispose d'aucune connectivité au portail de support client. Depuis un ordinateur avec accès à Internet, connectez-vous au CSP, téléchargez un fichier de clé de licence, transférez-le sur un ordinateur du même réseau que le pare-feu et téléchargez-le sur le pare-feu.

STEP 7 | Vérifiez que votre pare-feu est correctement mis sous licence.

Sur la page **Device (Périphérique)** > **Licenses (Licences)**, vérifiez que la licence a été activée avec succès.

Mise à niveau du modèle VM-Series d'une paire HA

La mise à niveau du pare-feu VM-Series vous permet d'augmenter la capacité du pare-feu. La capacité est définie en fonction du nombre de sessions, règles, zones de sécurité, objets d'adresse, tunnels IPSec VPN et SSL VPN que le pare-feu VM-Series peut gérer. Le modèle VM-Series fonctionne sous licence. Lorsque vous appliquez la nouvelle licence de capacité sur le pare-feu VM-Series, le numéro de modèle et les fonctionnalités associées y sont implémentés.



Vérifiez la** configuration système requise pour VM-Series **pour votre modèle de pare-feu avant de procéder à la mise à niveau. Si votre pare-feu dispose de moins de 5,5 Go de mémoire, la capacité (nombre de sessions, règles, zones de sécurité, objets d'adresse, etc.) sur le pare-feu sera limitée à celle du VM-50 Lite.

Ce processus est similaire à celui de la mise à niveau d'une paire de pare-feu matériels dans une configuration haute disponibilité. Pendant le processus de mise à niveau de la capacité, la synchronisation de la session se poursuit, si vous l'avez activée. Pour éviter les temps d'arrêt lors de la mise à niveau des pare-feu qui sont en configuration de disponibilité élevée, mettre à jour un pair HA à la fois.

 ©2023 Palo Alto Networks, Inc.

Ne modifiez pas la configuration des pare-feu pendant le processus de mise à niveau. Au cours du processus de mise à niveau, la synchronisation de la configuration est automatiquement désactivée lorsqu'une non-correspondance de capacité est détectée. Elle est ensuite réactivée lorsque les deux homologues HA présentent des licences de capacité correspondantes.

Si les pare-feu de la paire HA présentent des versions logicielles majeures différentes (telles que 9.1 et 9.0) et des capacités différentes, les deux périphériques entreront dans l'état HA suspendu. Par conséquent, il est recommandé de vous assurer que les deux pare-feu exécutent la même version de PAN-OS avant de mettre à niveau la capacité.

STEP 1 | Mettez à niveau la licence de capacité sur le pare-feu passif.

Suivez la procédure de mise à niveau du modèle VM-Series.

Le nouveau modèle VM-Series s'affiche sur le tableau de bord après le redémarrage de certains processus sur cet homologue passif. Cet homologue mis à niveau est maintenant un état non fonctionnel en raison de l'incompatibilité de capacité avec son homologue actif.

Si vous avez activé la synchronisation des sessions, vérifiez que les sessions sont synchronisées entre les homologues HA avant de passer à l'étape suivante. Pour vérifier la synchronisation des sessions, exécutez la **`show high-availability interface ha2`** et assurez-vous que les compteurs d'interface matérielle de la table du processeur augmentent comme suit :

- Dans une configuration active/passive, seul l'homologue actif affiche les paquets transmis et le périphérique passif affiche uniquement les paquets reçus.

  Si vous avez activé HA2 keep-alive (Maintien HA2), les compteurs d'interface matérielle sur l'homologue passif affichent à la fois les paquets de transmission et de réception. Cela se produit car HA2 keep-alive (Maintien HA2) est bidirectionnel, ce qui signifie que les deux homologues transmettent des paquets HA2 keep-alive (Maintien HA2).
- Dans la configuration active/active, les paquets reçus et les paquets transmis s'affichent sur les deux homologues.

STEP 2 | Mettez à niveau la licence de capacité sur le pare-feu actif.

Suivez la procédure pour mettre à niveau le modèle VM-Series.

Le nouveau modèle VM-Series s'affiche sur le tableau de bord après le redémarrage des processus critiques. Le pare-feu passif devient actif et cet homologue (pare-feu précédemment actif) passe de l'état initial à l'homologue passif dans la paire HA.

Rétrograder un pare-feu VM-Series vers une version antérieure

Utilisez le processus suivant pour restaurer la configuration qui était en cours d'exécution avant la mise à niveau vers une autre version de fonctionnalité. Toutes les modifications apportées depuis la mise à niveau seront perdues. Il est donc important de sauvegarder votre configuration actuelle afin de pouvoir restaurer ces modifications lorsque vous reviendrez à la nouvelle version.

Utilisez la procédure suivante pour procéder à la rétrogradation vers une version antérieure.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Faites une sauvegarde du fichier de configuration actuel.

Bien que le pare-feu crée automatiquement une sauvegarde de la configuration, il convient d'effectuer une copie de sauvegarde avant de mettre à niveau et de l'enregistrer en externe.

1. Cliquez sur **Export named configuration snapshot (Exporter l'instantané de configuration nommé)** (**Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opération)**).
2. Sélectionnez le fichier XML contenant la configuration actuelle (par exemple, **running-config.xml**), puis cliquez sur **OK** pour exporter le fichier de configuration.
3. Enregistrez le fichier exporté dans un emplacement externe au pare-feu. Vous pouvez utiliser cette sauvegarde pour restaurer la configuration en cas de problème pendant la rétrogradation.

STEP 2 | Installez l'image de la version de fonctionnalité précédente.

Des versions de sauvegarde automatique sont créées lors de la mise à niveau vers une nouvelle version.

1. Cliquez sur **Check Now (Vérifier maintenant)** (**Device (Périphérique)** > **Software (Logiciel)**) pour vérifier les images disponibles.
2. Localisez l'image vers laquelle vous souhaitez procéder à la rétrogradation. Si l'image n'est pas déjà téléchargée, cliquez sur **Download (Télécharger)** pour la télécharger.
3. Une fois le téléchargement terminé, cliquez sur **Install (Installer)** pour installer l'image.
4. Cliquez sur **Select a Config File for Downgrading (Sélectionner un fichier de configuration pour la rétrogradation)** pour sélectionner le fichier que le pare-feu chargera après le redémarrage du périphérique. Dans la plupart des cas, vous devez sélectionner la configuration qui a été enregistrée automatiquement lors de la mise à niveau à partir de la version vers laquelle vous effectuez maintenant la rétrogradation. Par exemple, si vous exécutez PAN-OS 9.1 et que vous procédez à une rétrogradation vers PAN-OS 9.0.3, sélectionnez `autosave-9.0.3`.
5. Une fois l'installation terminée, redémarrez en utilisant l'une des méthodes suivantes :
   - Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
   - Si vous n'êtes pas invité à redémarrer, accédez à Device Operations (Opérations de périphérique) (**Device (Périphérique)** > **Configuration** > **Operations (Opérations)**) et cliquez sur **Reboot Device (Redémarrer le périphérique)**.

©2023 Palo Alto Networks, Inc.

Plug-in VM-Series

Les pare-feu VM-Series incluent le plug-in VM-Series, une architecture de plug-in intégrée destinée à l'intégration avec des fournisseurs de cloud public ou des hyperviseurs de cloud privé. Le plug-in VM-Series peut être mis à niveau manuellement, indépendamment de PAN-OS, permettant ainsi à Palo Alto Networks® d'accélérer la publication de nouvelles fonctionnalités, correctifs ou intégrations avec de nouveaux fournisseurs de cloud ou hyperviseurs.

Le plug-in VM-Series vous permet de gérer les interactions spécifiques au cloud entre les pare-feu VM-Series et les plates-formes cloud publiques prises en charge : AWS, GCP et Azure. Le plug-in permet la publication de statistiques personnalisées sur des services de surveillance cloud (tels que AWS CloudWatch), l'amorçage, la configuration des informations d'identification de l'utilisateur, la fourniture d'informations depuis des environnements cloud publics et les mises à jour transparentes pour les bibliothèques cloud ou les agents sur PAN-OS.

Le plug-in VM-Series ne gère pas les fonctionnalités communes aux pare-feu VM-Series et aux pare-feu matériels. Par exemple, VM Monitoring ne fait pas partie du plug-in VM-Series, car il s'agit d'une fonctionnalité PAN-OS essentielle qui vous aide à appliquer la politique de manière cohérente sur les charges de travail de votre machine virtuelle à la fois à partir de pare-feu VM-Series et de pare-feu matériels.

Le plug-in VM-Series ne gère pas les Plug-ins Panorama***. Pour connaître la différence entre le plug-in VM-Series et les plug-ins Panorama, reportez-vous à la section*** Plug-in VM-Series et plug-ins Panorama**.**

Le plug-in VM-Series est un composant intégré qui peut être mis à niveau ou rétrogradé, mais pas supprimé. Chaque version de PAN-OS comprend une version du plug-in VM-Series spécifique correspondant à la version du logiciel PAN-OS. Lorsque vous rétrogradez vers une version antérieure du logiciel PAN-OS, la version du plug-in est rétrogradée vers la version compatible avec la version de PAN-OS. Vous pouvez mettre à niveau ou rétrograder le plug-in VM-Series localement sur le pare-feu virtuel ou gérer la version du plug-in de manière centralisée à partir de Panorama.

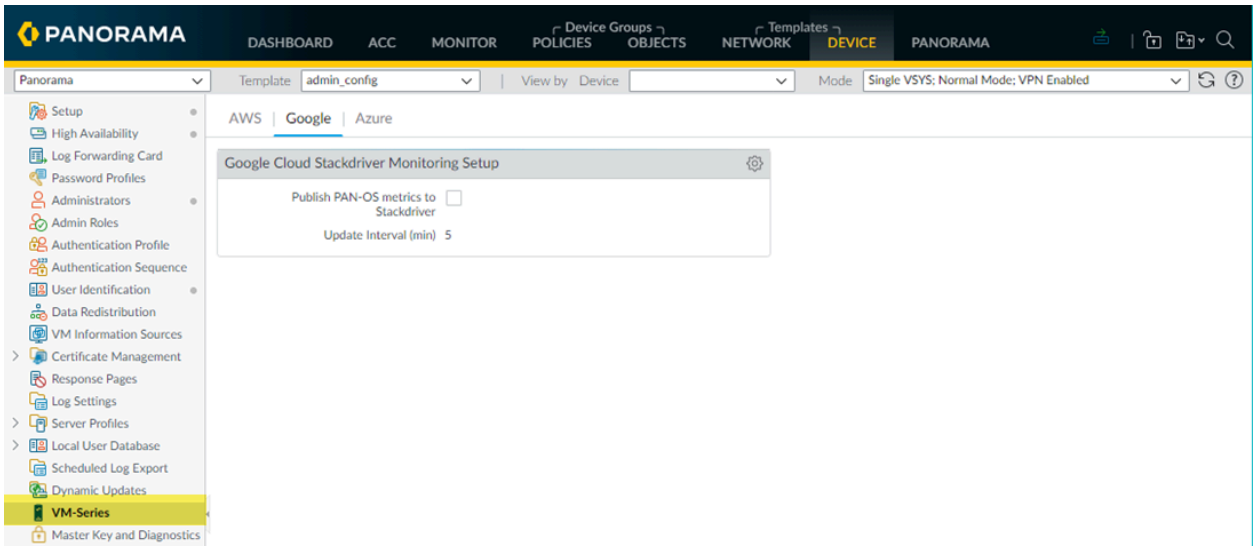
Pour permettre à Panorama de gérer la version du plug-in VM-Series proprement dite, ou des statistiques spécifiques au cloud publiant vos pare-feu gérés, vous devez installer manuellement le plug-in VM-Series sur Panorama, comme indiqué à la section Plug-ins Panorama.

- Configuration du plug-in VM-Series sur le pare-feu
- Mise à niveau du plug-in VM-Series

Configuration du plug-in VM-Series sur le pare-feu

Sélectionnez **Device (Périphérique)** > **VM-Series** pour configurer l'intégration du plug-in pour le fournisseur de cloud sur lequel cette instance du pare-feu VM-Series est déployée.

 ©2023 Palo Alto Networks, Inc.



Si votre pare-feu est déployé sur un hyperviseur ou un cloud sans interface publique (par exemple, VMware ESXi), l'onglet s'appelle VM-Series et affiche un message général.

Mise à niveau du plug-in VM-Series

Lorsqu'une mise à jour de plug-in est publiée indépendamment de PAN-OS, vous pouvez mettre à niveau indépendamment la version du plug-in à partir de votre pare-feu VM-Series (mise à jour du logiciel ou du contenu, par exemple) ou à partir d'un fichier d'amorçage.

Chaque version de plug-in fournit des informations sur la compatibilité PAN-OS et inclut de nouvelles fonctionnalités ou des corrections de bogues pour un ou plusieurs environnements cloud.

STEP 1 | Avant de procéder à la mise à niveau, consultez les dernières notes de version pour savoir si un nouveau plug-in VM-Series affecte votre environnement.

Par exemple, supposons qu'une nouvelle version de plug-in VM-Series n'inclue que les fonctionnalités AWS. Pour tirer parti des nouvelles fonctionnalités, vous devez mettre à jour le plug-in sur vos instances de pare-feu VM-Series sur AWS.

N'installez aucune mise à niveau qui ne s'applique pas à votre environnement.

Le plug-in VM-Series 3.0.0 est pris en charge uniquement dans PAN-OS 10.2.0.

©2023 Palo Alto Networks, Inc.

STEP 2 | Connectez-vous au pare-feu VM-Series et consultez le tableau de bord pour afficher la version du plug-in.

System Mode	panorama
Software Version	10.0.2
Application Version	8335-6370 (10/26/20)
Device Dictionary Version	10-238 (10/30/20)
Time	Mon Nov 2 17:29:10 2020
Uptime	7 days, 0:31:54
Plugin Azure	azure-2.0.3
Plugin Interconnect	interconnect-1.0.2
Plugin SD WAN plugin	sd_wan-1.0.3
Plugin Cisco TrustSec Monitoring Plugin	cisco_trustsec-1.0.2
Plugin VM series	vm_series-2.0.1
Plugin AWS	aws-3.0.0

STEP 3 | Sélectionnez **Panorama** > **Plugins (Plug-ins)** et saisissez **`vm_series`** dans le champ de recherche.

Sélectionnez **Check Now** (Vérifier maintenant) pour afficher les versions disponibles.

STEP 4 | Choisissez la version du plug-in VM-Series et cliquez sur **Download** (Télécharger).

vm_series 1743 / 1600

FILE NAME	VERSION	RELEASE DATE	SIZE	DOWNLOADED	CURRENTLY INSTALLED	ACTIONS	RELEASE NOTE URL
Name: vm_series							
vm_series-1.0.5	1.0.5	Built-in	15M			Download	Release Notes
vm_series-2.0.0	2.0.0	Built-in	9M	✓		Install Delete	
vm_series-2.0.1	2.0.1	Built-in	9M	✓		Install Delete	
vm_series-2.0.2	2.0.2	Built-in	9M	✓	✓	Remove Config Uninstall	

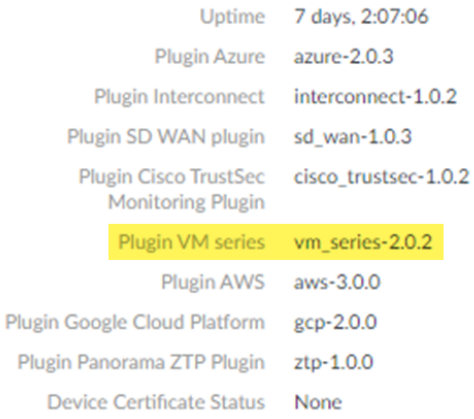
Check Now Upload

STEP 5 | Une fois le téléchargement terminé, cliquez sur **Install** (Installer) dans la colonne **Actions**.

Le pare-feu désinstalle automatiquement la version du plug-in installée précédemment.

©2023 Palo Alto Networks, Inc.

STEP 6 | Consultez le **Dashboard** (Tableau de bord) pour vérifier que la mise à niveau du plug-in a bien été effectuée.



 ©2023 Palo Alto Networks, Inc.

Activation des trames Jumbo sur le pare-feu VM-Series

Par défaut, la taille de l'unité de transmission maximale (MTU) pour les paquets envoyés sur une interface de couche 3 est de 1 500 octets. Cette taille peut être définie manuellement à une taille comprise entre 512 et 1 500 octets par interface. Certaines configurations nécessitent des trames Ethernet avec une valeur MTU supérieure à 1 500 octets. Elles sont appelées trames Jumbo.

Pour utiliser des trames Jumbo sur un pare-feu, vous devez activer spécifiquement les trames Jumbo au niveau global. Lorsqu'elles sont activées, la taille de MTU par défaut de toutes les interfaces de couche 3 est définie à une valeur de 9 192 octets. Cette valeur par défaut peut ensuite être définie sur n'importe quelle valeur comprise entre 512 et 9 216 octets.

Après avoir défini une taille de trame Jumbo globale, elle devient la valeur par défaut de toutes les interfaces de couche 3 qui n'ont pas explicitement eu de valeur MTU définie au niveau de la configuration de l'interface. Cela peut devenir un problème si vous souhaitez uniquement échanger des trames Jumbo sur certaines interfaces. Dans ces situations, vous devez définir la valeur MTU à chaque interface de couche 3 pour lesquelles vous ne souhaitez pas utiliser la valeur par défaut.

La procédure suivante décrit comment activer les trames Jumbo sur un pare-feu, définir la valeur MTU par défaut pour toutes les interfaces de couche 3 et définir une valeur différente pour une interface spécifique.



Les instances de pare-feu VM-Series déployées avec plusieurs nœuds NUMA se présentent en mode MMAP par paquets lorsque la prise en charge des trames jumbo est activée. Vous devez désactiver la prise en charge des trames jumbo pour utiliser DPDK sur une instance de pare-feu VM-Series déployée avec plusieurs nœuds NUMA.

STEP 1 | Activez les trames Jumbo et définissez la valeur MTU globale par défaut.

1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Session** et modifiez la section Session Settings (Paramètres de session).
2. Sélectionnez **Enable Jumbo Frame (Activer la trame Jumbo)**.
3. Entrez une valeur pour **Global MTU (MTU globale)**.

   La valeur par défaut est 9192. La gamme de valeurs acceptables est : 512 à 9 216.
4. Cliquez sur **OK**.

   Un message s'affiche pour vous informer que l'activation ou la désactivation du mode trames Jumbo nécessite un redémarrage et que les interfaces de couche 3 héritent de la valeur **Global MTU (MTU globale)** .
5. Cliquez sur **Yes (Oui)**.

   Un message s'affiche pour vous informer que la prise en charge des trames Jumbo a été activée et vous rappelle qu'un redémarrage du périphérique est requis pour que cette modification soit activée.
6. Cliquez sur **OK**.
7. Cliquez sur **Commit (Valider)**.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Définissez la valeur MTU pour une interface de couche 3 et redémarrez le pare-feu.

La valeur définie pour l'interface remplace la valeur MTU globale.

1. Sélectionnez **Network (Réseau)** > **Interfaces**.
2. Sélectionnez une interface avec **Interface type (Type d'interface)** Layer3 (Couche 3).
3. Sélectionnez **Advanced (Avancé)** > **Other Info (Autres informations)**.
4. Saisissez une valeur pour **MTU**.

   La valeur par défaut est 9192. La gamme de valeurs acceptables est : 512 à 9 216.
5. Cliquez sur **OK**.
6. Cliquez sur **Commit (Valider)**.
7. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Operations (Opérations)** et **Reboot Device (Réamorcer l'appareil)**.

©2023 Palo Alto Networks, Inc.

Adresses MAC attribuées par l'hyperviseur

Par défaut, le pare-feu VM-Series utilise l'adresse MAC attribuée à l'interface physique par l'hôte / l'hyperviseur pour déployer un pare-feu VM-Series avec des interfaces de couche 3. Le pare-feu peut ensuite utiliser l'adresse MAC attribuée à l'hyperviseur dans ses réponses ARP. Cette fonction permet aux commutateurs qui n'apprennent pas les adresses MAC, comme le vSwitch de VMware, de transférer le trafic vers l'interface du dataplane du pare-feu sans que le mode de proximité ne soit activé sur le vSwitch. Dans les situations où ni le mode de proximité ni l'utilisation de l'adresse MAC attribuée par l'hyperviseur n'est activé, l'hôte abandonnera la trame s'il détecte une disparité entre l'adresse MAC de destination d'une interface et l'adresse MAC attribuée par l'hôte.



Il n'existe aucune option permettant d'activer ou de désactiver l'utilisation des adresses MAC attribuées à l'hyperviseur sur AWS et Azure. Elle est activée par défaut pour les deux plates-formes et ne peut pas être désactivée.

Si vous déployez le pare-feu VM-Series dans les modes d'interface de couche 2, câble virtuel ou tap, vous devez activer le mode de proximité sur le commutateur virtuel auquel le pare-feu est connecté. L'utilisation de l'adresse MAC attribuée à l'hyperviseur n'est pertinente que pour les déploiements de couche 3 lorsque le pare-feu est habituellement la passerelle par défaut pour les machines virtuelles invitées.

Lorsque la fonction d'adresse MAC attribuée par l'hyperviseur est activée sur le pare-feu VM-Series, prenez note des exigences suivantes :

- **Adresse IPv6 sur une interface** : dans une configuration HA active/passive (voir VM-Series en haute disponibilité), les interfaces de couche 3 qui utilisent des adresses IPv6 ne doivent pas utiliser l'adresse générée par la méthode EUI-64 en tant qu'identifiant d'interface (ID d'interface). Parce que l'EUI-64 génère l'adresse IPv6 de l'interface à partir de l'adresse MAC constituée de 48 bits de l'interface, l'adresse IP n'est pas statique. Cela se traduit par le changement d'adresse IP de l'homologue HA lorsqu'il y a un changement de matériel hébergeant le pare-feu VM-Series lors du basculement, et entraîne une défaillance de la HA.
- **Location d'une adresse IP** : lorsque l'adresse MAC change, le client DHCP, l'agent relais DHCP et les interfaces PPPoE peuvent libérer l'adresse IP parce que la location de l'adresse IP initiale pourrait prendre fin.
- **Adresse MAC et ARP gratuite** : les pare-feu VM-Series ayant des adresses MAC attribuées par l'hyperviseur dans une configuration à haute disponibilité agissent différemment que les appareils matériels en ce qui a trait aux adresses MAC. Les pare-feu matériels utilisent des adresses MAC flottantes autogénérées entre les périphériques d'une paire HA, et l'adresse MAC unique qui est utilisée sur chacune des interfaces du dataplane (p. ex. eth 1/1) est remplacée par une adresse MAC virtuelle qui est commune aux interfaces du dataplane des deux homologues HA. Lorsque vous activez l'utilisation de l'adresse MAC attribuée par l'hyperviseur sur le pare-feu VM-Series HA, l'adresse MAC virtuelle n'est pas utilisée. L'interface du dataplane de chacun des homologues HA est unique et respecte les spécifications de l'hyperviseur.

  Puisque chaque interface du dataplane possède une adresse MAC unique, lors d'un basculement, le pare-feu VM-Series qui est actif doit envoyer un ARP gratuit afin d'informer les périphériques avoisinants de la combinaison IP-MAC mise à jour. Ainsi, pour activer un basculement en cas de panne, les périphériques de mise en réseau ne doivent pas bloquer ni ignorer les requêtes ARP

 ©2023 Palo Alto Networks, Inc.

gratuites ; au besoin, assurez-vous de désactiver la fonction anti-empoisonnement ARP sur les périphériques interréseau.

Effectuez les étapes suivantes pour configurer le pare-feu VM-Series afin qu'il utilise les adresses MAC de l'interface attribuées par l'hôte ou l'hyperviseur :

STEP 1 | Sélectionnez **Device (Périphérique)** > **Management (Gestion)** > **Setup (Configuration)** > **General Settings (Paramètres généraux)**.

STEP 2 | Cliquez sur l'icône **Edit (Modifier)**.

STEP 3 | Cochez l'option **Use Hypervisor Assigned MAC Address (Utiliser l'adresse MAC attribuée à l'hyperviseur)**.

Lors de la modification de l'adresse MAC, le pare-feu génère un journal système pour enregistrer cette transition, et l'interface génère un ARP gratuit.

STEP 4 | Cliquez sur **OK**.

STEP 5 | Cliquez sur **Commit (Valider)** pour valider la modification apportée au pare-feu. Vous n'avez pas à redémarrer le pare-feu.

 ©2023 Palo Alto Networks, Inc.

Publication de statistiques PAN-OS personnalisées pour la surveillance

Le pare-feu publie en mode natif les métriques suivantes pour surveiller les systèmes du cloud public, tels que AWS® CloudWatch, Azure® Application Insights et Google® Stackdriver. Ces statistiques vous permettent d'évaluer les performances et les modèles d'utilisation du pare-feu afin de pouvoir définir des alarmes et prendre des mesures pour automatiser des événements tels que le lancement ou l'arrêt d'instances des pare-feu VM-Series. Étant donné que ces statistiques sont publiées via des mises à jour de contenu sur le pare-feu, assurez-vous que vous disposez de la version de contenu minimale requise pour activer cette fonctionnalité sur votre pare-feu VM-Series.

Métrique	Description
Dataplane CPU Utilization (%) (Utilisation du processeur du dataplane)	Surveille l'utilisation de l'UC du dataplane et mesure la charge de trafic sur le pare-feu.
Dataplane Packet Buffer Utilization (%) (Utilisation de la mémoire tampon des paquets du dataplane)	Surveille l'utilisation du tampon du dataplane et mesure l'utilisation du tampon. Si vous observez une rafale soudaine dans le trafic, la surveillance de l'utilisation de votre tampon vous permet de vous assurer que le pare-feu n'épuise pas le tampon du dataplane, ce qui entraîne la perte de paquets.
GlobalProtect Gateway Active Tunnels (Tunnels actifs de la passerelle GlobalProtect)	Surveille le nombre de sessions GlobalProtect actives sur un pare-feu déployé en tant que passerelle GlobalProtect. Utilisez cette métrique si vous utilisez ce pare-feu VM-Series en tant que passerelle VPN pour sécuriser les utilisateurs distants. Consultez la fiche technique pour connaître le nombre maximal de tunnels actifs pris en charge pour votre modèle de pare-feu.
GlobalProtect Gateway Tunnel Utilization (%) (Utilisation de tunnels de la passerelle GlobalProtect)	Surveille les tunnels GlobalProtect actifs sur une passerelle et mesure l'utilisation du tunnel. Utilisez cette métrique si vous utilisez ce pare-feu VM-Series en tant que passerelle VPN pour sécuriser les utilisateurs distants.
panSessionConnectionsPerSecond	Surveille le taux d'établissement de nouvelles connexions par seconde.
panSessionThroughputKbps	Surveille le débit en Kbit/s.
panSessionThroughputPps	Surveille le nombre de paquets par seconde.
Sessions actives	Surveille le nombre total de sessions actives sur le pare-feu. Une session active est une session qui se trouve dans la

©2023 Palo Alto Networks, Inc.

Métrique	Description
	table de recherche de flux pour laquelle les paquets seront inspectés et transférés, comme requis par la politique.
Session Utilization (%) (Utilisation des sessions)	Surveille les sessions TCP, UDP, ICMP et SSL actuellement actives et le débit de paquets, le nouveau débit d'établissement de la connexion et le débit du pare-feu pour déterminer l'utilisation de la session.
SSLProxyUtilization (%) (Utilisation du proxy SSL)	Surveille le pourcentage de sessions de proxy de transfert SSL avec les clients pour le déchiffrement SSL/TLS.

Pour publier ces statistiques, voir:

- Activer la surveillance CloudWatch sur le pare-feu VM-Series
- Activer Azure Application Insights sur le pare-feu VM-Series
- Activer Google Stackdriver Monitoring sur le pare-feu VM-Series

©2023 Palo Alto Networks, Inc.

Interface utilisée pour accéder aux services externes sur le pare-feu VM-Series

Pour accéder aux serveurs Palo Alto Networks pour récupérer des licences et des mises à jour logicielles et de contenu, ainsi que pour publier des statistiques PAN-OS personnalisées ou pour récupérer des adresses IP et les mappages de balises pour surveiller des machines virtuelles dans votre déploiement, le pare-feu VM-Series utilise l'interface de gestion, sauf indication contraire décrite ci-dessous. Pour utiliser une interface de plan de données à la place de l'interface de gestion prise en charge, vous devez configurer un itinéraire de service qui spécifie l'interface de plan de données que le pare-feu peut utiliser pour accéder au serveur ou au service.

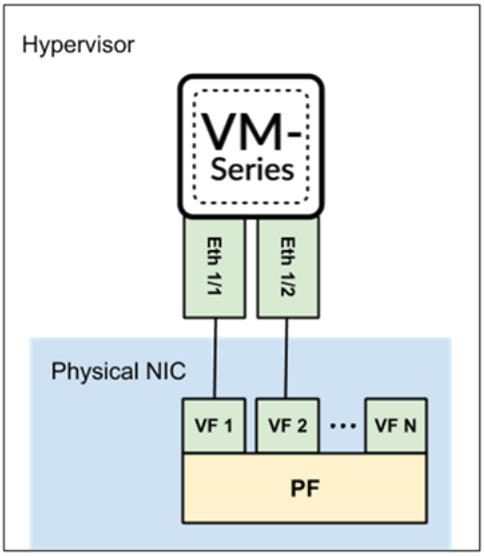
Accès au serveur ou au service	Interface utilisée sur le pare-feu VM-Series
Mise sous licence	Interface de gestion uniquement
Mises à jour logicielles	Interface de gestion ou itinéraire de service
Amorçage à partir d'un emplacement de stockage cloud, tel que le compartiment AWS S3,le service de fichiers de stockage Azure ou le compartiment de stockage Google	Interface de gestion uniquement, y compris lorsque les interfaces sont échangées ***Si votre fichier bootstrap.xml inclut des codes d'autorisation de licence, vous ne pouvez pas utiliser un itinéraire de service. Pour autoriser le pare-feu, l'interface de gestion doit être utilisée.***
Publication des métriques PAN-OS sur un service de surveillance cloud tel qu'AWS CloudWatch, Azure Application Insights ou Google Stackdriver	Interface de gestion uniquement, y compris lorsque les interfaces sont échangées
Surveillance VM	Interface de gestion ou itinéraire de service

©2023 Palo Alto Networks, Inc.

Support des pilotes PacketMMAP et DPDK

La virtualisation d'entrée/sortie à racine unique (SR-IOV, single root input/output virtualization) s'appuie sur la communication entre les pilotes de fonction virtuelle (VF) sur le pare-feu VM-Series et les pilotes de fonction physique (PF) sur l'hôte (l'hyperviseur). L'hôte utilise les pilotes PF pour communiquer avec ses cartes réseau physiques et le pare-feu VM-Series utilise les pilotes VF pour communiquer avec les pilotes PF.

Le schéma suivant fournit une visualisation simple de ce concept.



SR-IOV

Pourquoi utiliser la SR-IOV ? SR-IOV est une technologie d'accélération des paquets qui permet à une machine virtuelle d'accéder directement à des paquets issus de la carte réseau. Au contraire, lors de l'utilisation d'un commutateur virtuel, l'hôte traite les paquets, envoie les paquets par le biais d'un commutateur virtuel, puis la machine virtuelle reçoit ses paquets.

Dans la matrice de compatibilité, PacketMMAP Driver Versions (Versions du pilote PacketMMAP) répertorie la version de l'hôte et la version du pilote natif sur le pare-feu VM-Series. Par exemple, i40e sur l'hôte et, sur le pare-feu, i40e (pour PCI-Pass-Thru) et i40evf (pour SR-IOV).

Pour SR-IOV, supposons une carte réseau qui utilise le pilote PF i40e. L'hôte communique avec la carte réseau par le biais du pilote i40e. Le pare-feu VM-Series peut utiliser son pilote VF (i40evf) pour communiquer directement avec le pilote PF de l'hôte. Cela permet un accès direct au pare-feu VM-Seriesn, ce qui améliore la vitesse de traitement des paquets. Pour garantir la compatibilité, installez une version du pilote PF hôte ultérieure à la version du pilote PF natif.

PCI-Pass-Thru

Pour le pare-feu VM-Series a-t-il des pilotes PF natifs ? Comme indiqué dans Options for Attaching VM-Series on the Network (Options pour lier VM-Series au réseau), lors de l'utilisation de PCI-Pass-Thru, la carte réseau est réservée au pare-feu VM-Series, par conséquent, l'hôte (ou les autres invités sur l'hôte) ne peuvent pas accéder à la carte réseau. Dans une configuration PCI-Pass-Thru, le pare-feu VM-Series utilise son pilote PF natif pour communiquer directement avec la carte réseau hôte.

©2023 Palo Alto Networks, Inc.

Reportez-vous à la liste PacketMMAP Driver Versions (Versions du pilote PacketMMAP) pour déterminer la version du pilote PF à installer sur l'hôte. Installez une version PF ultérieure à la version du pilote PF natif du pare-feu VM-Series.

Reportez-vous à Activation de SR-IOV sur ESXi et Activation de SR-IOV sur KVM pour PCI-Pass-Thru.

DPDK

PAN-OS dispose de deux modes de traitement des paquets – DPDK (par défaut) et MMAP – et chaque mode dispose d'un pilote natif correspondant sur le pare-feu VM-Series. Par exemple, si le pare-feu est en mode DPDK, le pare-feu utilise la version du pilote i40evf DPDK pour communiquer avec le pilote i40e de l'hôte (lorsque la SR-IOV est utilisée). Alternativement, lorsque le pare-feu est en mode PacketMMAP, il utilise une version différente du pilote i40evf pour communiquer avec le pilote i40e de l'hôte.

Vous pouvez activer le mode DPDK sur l'hôte (l'hyperviseur) ou sur l'invité (le pare-feu VM-Series). L'activation des deux offre les meilleurs résultats.

- La compilation d'OVS avec le DPDK contribue à activer le DPDK sur l'hôte.

  Reportez-vous à Configuration d'OVS et de DPDK sur l'hôte.
- Le DPDK VM-Series active le pilote DPDK natif sur le pare-feu VM-Series, de sorte que le DPDK n'a pas besoin d'être activé sur l'hôte, mais il est recommandé pour des performances optimales.

 ©2023 Palo Alto Networks, Inc.

Activation de l'optimisation des performances NUMA sur le VM-Series

Pour améliorer les performances de vos pare-feu VM-Series, vous pouvez activer l'optimisation des performances NUMA (Non-Uniform Memory Access). Lorsque l'optimisation des performances NUMA est activée, le plan de données du pare-feu VM-Series utilise des vCPU attachés au nœud NUMA 0. Le plan de données du pare-feu VM-Series utilise uniquement des vCPU appartenant au nœud NUMA 0. Le plan de gestion VM-Series utilise le noyau 0 et les vCPU restants sur le nœud NUMA 0 peuvent être utilisés par le plan de données VM-Series. Cette fonctionnalité nécessite PAN-OS 10.1.1 ou version ultérieure et le plug-in VM-Series 2.1.1 ou version ultérieure.

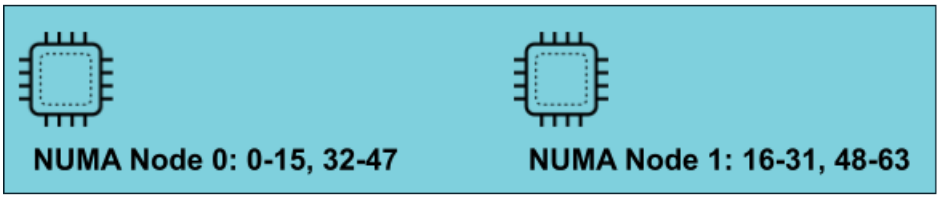
L'optimisation des performances NUMA est désactivée par défaut dans PAN-OS 10.1.

Si vous avez un périphérique qui contient 64 cœurs sur deux nœuds NUMA, lorsque l'optimisation des performances NUMA n'est pas activée, les vCPU de plan de données utilisés par le pare-feu VM-Series peuvent se trouver sur des nœuds différents, ce qui a un impact sur les performances. Par exemple, si votre système est organisé comme dans l'exemple suivant et si vous déployez un pare-feu VM-Series avec 32 cœurs au total avec 24 cœurs de plan de données.

Sans optimisation des performances NUMA, le pare-feu VM-Series utilise les cœurs 1 à 15 sur le nœud 0 et 16 à 24 sur le nœud 1, car il attribue des cœurs dans l'ordre numérique, quel que soit l'emplacement du nœud. Avec l'optimisation NUMA activée, le VM-Series utilise uniquement des cœurs sur le nœud 0, dans ce cas 1 à 15 et 33 à 39, quel que soit l'ordre numérique. Tous les cœurs non utilisés par le plan de données sont affectés au plan de gestion.

Avec l'optimisation des performances NUMA avec des paramètres de base de plan de données personnalisés, les paramètres NUMA sont prioritaires. Par exemple, pour une VM à 64 processeurs avec l'optimisation des performances NUMA activée et le paramètre de base de plan de données 47, les paramètres NUMA sont prioritaires.

Si le nombre de cœurs affectés à votre pare-feu VM-Series dépasse le nombre de vCPU sur le nœud 0, le VM-Series utilise tous les cœurs du nœud 0, mais n'utilise aucun cœur d'autres nœuds. Par exemple, si vous affectez 30 cœurs à votre pare-feu VM-Series mais si le nœud 0 ne comporte que 24 cœurs, le pare-feu VM-Series n'utilisera que les 24 cœurs du nœud 0 pour le plan de données.



STEP 1 | Connectez-vous à la CLI VM-Series.

©2023 Palo Alto Networks, Inc.

STEP 2 | Exécutez la commande suivante.

```
request plugins vm_series numa-perf-optimize enable on
Previous NUMA performance optimization: None
Requested NUMA performance optimization: Activé
Veuillez redémarrer le PA-VM.
```

STEP 3 | Une fois le redémarrage terminé, connectez-vous à la CLI VM-Series et vérifiez que l'optimisation NUMA a été activée.

```
show plugins vm_series numa-perf-optimize
NUMA performance optimization: Activé
```

STEP 4 | Vérifiez le nombre de cœurs du plan de données.

```
show plugins vm_series dp-cores
Current DP cores:31 configured custom DP cores: 47 (Current total cores: 64)
```

STEP 5 | Pour désactiver l'optimisation des performances NUMA, utilisez la commande suivante. Cette commande nécessite le redémarrage du pare-feu VM-Series.

```
request plugins vm_series numa-perf-optimize enable off
```

 ©2023 Palo Alto Networks, Inc.

Activation du ZRAM sur le pare-feu VM-Series

Si votre pare-feu VM-Series rencontre des conditions de mémoire faible ou insuffisante, vous pouvez activer la ZRAM pour améliorer l'utilisation de la mémoire. La ZRAM, également appelée compcache (cache compressée), est un module du noyau Linux permettant de créer un périphérique de blocage compressé en RAM. Lorsqu'elle est activée, la ZRAM est utilisée comme disque d'échange et permet des E/S d'échange plus rapides car elle réside dans la RAM.

Effectuez les étapes suivantes pour activer la ZRAM.

STEP 1 | Connectez-vous à la CLI VM-Series.

STEP 2 | Recherchez la mémoire totale sur la VM à l'aide de la commande CLI suivante.

```
grep pattern “KiB Mem :” mp-log mp-monitor.log
```

```
KiB Mem : 9202656 total, 566504 free, 3475840 used, 5160312 buff/
cache KiB Mem : 9202656 total, 497112 free, 3481944 used, 5223600
 buff/cache KiB Mem : 9202656 total, 511744 free, 3466768 used,
 5224144 buff/cache KiB Mem : 9202656 total, 511668 free, 3466340
 used, 5224648 buff/cache KiB Mem : 9202656 total, 512124 free,
 3465700 used, 5224832 buff/cache KiB Mem : 9202656 total, 511436
 free, 3465976 used, 5225244 buff/cache KiB Mem : 9202656 total,
 510984 free, 3465944 used, 5225728 buff/cache
```

STEP 3 | Convertissez la mémoire totale ci-dessus de Ko en Mo. Par exemple :

9 202 656 / 1024 = 8987 Mo

Notez la valeur totale de la mémoire en Mo. Vous aurez besoin de cette valeur à l'étape suivante.

STEP 4 | Activez la ZRAM à l'aide des deux commandes CLI suivantes.

```
debug software kernelcfg zram-swap enable
```

```
debug software kernelcfg zram-swap modify host-mem-threshold <total-
memory-in-MB>
```

STEP 5 | Redémarrez le pare-feu VM-Series.

STEP 6 | Vérifiez que la ZRAM est activée.

```
debug software kernelcfg zram-swap show config
```

 ©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Mise sous licence du pare-feu VM-Series

Le pare-feu VM-Series prend en charge deux types de licences (BYOL et PayGo) et deux modèles de licences différents : les crédits de pare-feu logiciel de nouvelle génération (NGFW logiciels) pour les configurations flexibles que vous spécifiez avec un profil de déploiement et les configurations fixes du modèle VM-Series. Les deux modèles autorisent également des services de sécurité et d'autres fonctionnalités.

Si vous êtes un partenaire CSSP homologué, consultez la section Licences pour les fournisseurs de services de sécurité cloud (CSSP) pour des informations qui vous concernent.

Consultez les rubriques suivantes pour plus de détails sur la création d'un compte d'assistance et la gestion des licences :

- Mise sous licence du pare-feu VM-Series
- Création d'un compte de support
- Format du numéro de série et de l'ID du processeur pour le pare-feu VM-Series
- API de mise sous licence
- Installation d'une clé API de licence
- Utilisation la gestion des licences de pare-feu logiciel basée sur Panorama
- Crédits NGFW logiciels
- Modèles VM-Series
- Licences pour les fournisseurs de services de sécurité cloud (CSSP)

Mise sous licence du pare-feu VM-Series

Ce chapitre compare les informations de licence suivantes :

- Types de licences : BYOL contre PayGo
- Licences de vCPU flexibles et de modèle fixe : vCPU flexibles par rapport aux modèles fixes
- Déploiement de vCPU flexibles et de modèles fixes : résumé des étapes de déploiement pour les modèles flexibles et fixes.

Types de licences

Palo Alto Networks prend actuellement en charge deux types de licence : Bring Your Own License (BYOL) et PAYG (Pay-As-You-Go, également appelé PayGo).

Type	Description
BYOL	Crédits NGFW logiciels : disponible sur les pare-feu VM-Series exécutant toutes les versions de PAN-OS. Les pare-feu VM-Series exécutant PAN-OS versions 10.0.4 et ultérieures offrent des fonctionnalités avancées et plus de flexibilité. Le coût d'une licence flexible dépend du nombre de vCPU, des services de sécurité que vous avez activés et du fait que vous choisissiez de provisionner Panorama pour gérer le pare-feu ou agir en tant que collecteur de journaux. Voir Crédits NGFW logiciels pour une explication détaillée.
BYOL	Licences VM-Series Model : disponibles pour une utilisation avec toutes les versions de PAN-OS. Le nombre de vCPU est fixé en fonction du modèle VM-Series que vous avez choisi. ***Les vCPU flexibles, disponibles avec PAN-OS 10.0.4 et versions ultérieures, prennent en charge des fonctionnalités avancées et davantage de vCPU.*** Le coût de la licence de capacité est basé sur le modèle VM-Series, la mémoire de l'appareil, les coûts de stockage et les droits d'assistance. Les services de sécurité et un déploiement Panorama pour gérer vos pare-feu sont des coûts supplémentaires. Les types de licence de capacité sont : • **Accord de licence d'entreprise VM-Series (ELA multimodèle)** : un contrat de licence complet d'un ou trois ans pour les pare-feu VM-Series. Une licence individuelle peut inclure un modèle, des services de sécurité, une autorisation de support et une licence de gestion des périphériques en option pour Panorama. L'ELA multi-modèle dispose d'un pool de jetons à partir duquel vous allouez des jetons aux pare-feu VM-Series sous licence. (Il est unique à l'ELA et n'est pas le même que le pool de crédits NGFW logiciels.) • Licence de capacité de modèle perpétuelle VM-Series avec une autorisation de support et/ou un ensemble de services de sécurité 1 ou 2.

©2023 Palo Alto Networks, Inc.

Type	Description
	• Licence de capacité de pare-feu à terme avec un droit de support et votre choix de services de sécurité.
PayGo	Acheté auprès d'un marché de cloud public (tel qu'AWS, Azure ou GCP) ou d'un fournisseur de services de sécurité cloud (CSSP). Disponible sur la version PAN-OS prise en charge par votre fournisseur. Sur les versions PAN-OS antérieures à 9.1.1, PayGo ne prenait en charge que le modèle VM-Series VM-300. Pour PAN-OS 9.1.1 et versions ultérieures, PayGo peut prendre en charge les modèles fixes. Les modèles de VM traditionnels, tels que VM-100, VM-300, VM-500 et VM-700 sont pris en charge.

Licences de vCPU flexibles et de modèle fixe

Quelle est la différence entre les licences NGFW logicielles flexibles vCPU et les licences de modèle fixe VM-Series vCPU ? Elles facturent des choses différentes et les financent différemment. Les tableaux suivants fournissent une comparaison rapide et des liens vers plus de détails.

	vCPU flexibles	Modèle VM-Series (vCPU fixes)
Description	Le coût est basé sur le nombre de vCPU et les services de sécurité que vous avez choisis. Il n'y a aucun coût pour Panorama en dehors des vCPU qu'il consomme. Vous achetez des crédits NGFW logiciels réutilisables qui expirent à la fin d'une durée prédéterminée. Après avoir activé vos crédits, vous pouvez les répartir dans des pools de crédits. Pour utiliser vos crédits, choisissez un profil de crédit et créez un ou plusieurs profils de déploiement. Choisissez votre propre combinaison de composants de pare-feu en tant que plate-forme : vCPU VM-Series, services de sécurité, Panorama virtuel pour la gestion ou la collecte de journaux dédiés, et une autorisation de support. Tous les pare-feu déployés avec un profil sont sous licence avec le même code d'autorisation et vous pouvez les gérer à partir du profil de déploiement.	Le coût est basé sur la licence de capacité du modèle VM-Series, la mémoire du périphérique et le stockage. Panorama et les services de sécurité sont des achats séparés. • Accord de licence d'entreprise VM-Series (ELA multimodèle) : un contrat de licence complet d'un ou trois ans pour les pare-feu VM-Series. L'ELA multi-modèle dispose d'un pool de jetons à partir duquel vous allouez des jetons aux pare-feu VM-Series sous licence. • Licence de capacité de modèle perpétuelle VM-Series avec une autorisation de support et/ou un ensemble de services de sécurité 1 ou 2. • Licence de capacité de pare-feu à terme avec un droit de support et votre choix de services de sécurité.

©2023 Palo Alto Networks, Inc.

	vCPU flexibles	Modèle VM-Series (vCPU fixes)
Activation	Nécessite un e-mail d'activation. L'activation et l'enregistrement se font automatiquement.	Nécessite un e-mail d'activation et une étape d'enregistrement distincte après l'activation.
Services de sécurité	Threat Prevention, sécurité DNS, GlobalProtect, WildFire, filtrage des URL, SD-WAN, DLP et d'autres services dès qu'ils deviennent disponibles. Lorsque vous créez votre profil de déploiement, vous pouvez choisir n'importe quelle combinaison de services de sécurité. Vous pouvez ajouter ou supprimer des services de sécurité de votre profil à tout moment.	**Forfait 1** : Prévention des menaces et autorisation de support premium. **Forfait 2** : Threat Prevention, sécurité DNS, GlobalProtect, WildFire, filtrage des URL, SD-WAN, DLP et autorisation de support premium.
Version de PAN-OS	Jusqu'à 64 vCPU flexibles et options de service avancées pour les pare-feu exécutant 10.0.4 et versions ultérieures.	Vous pouvez déployer un modèle VM-Series (vCPU fixes) sur n'importe quelle version PAN-OS.
Financement	Crédits réutilisables qui vous permettent de consommer des composants de pare-feu en tant que plate-forme. Après avoir acheté des crédits, vous devez les activer en les associant à un compte particulier pour votre organisation. Les crédits activés financent un pool de crédits à partir duquel vous pouvez créer un profil de déploiement. Lorsque les pare-feu sont déployés, les crédits sont consommés. Lorsque les pare-feu sont désactivés, les crédits sont libérés et retournés à votre pool de crédits pour une utilisation ultérieure.	• ELA multi-modèles : jetons. • Licence de capacité de modèle perpétuelle VM-Series avec une autorisation de support et/ou un ensemble de services de sécurité 1 ou 2. Vous déterminez la configuration au moment de l'achat. Vous ne pouvez pas modifier la configuration à moins d'acheter une nouvelle licence. • Licence de capacité de pare-feu à terme avec un droit de support et votre choix de services de sécurité.
Configuration de déploiement	Flexible. Un profil de déploiement peut être modifié à tout moment. Les modifications apportées au profil se propagent à tous les pare-feu qui partagent le code d'autorisation du profil de déploiement.	La capacité du modèle VM-Series ne change pas, mais si vous disposez d'un ELA, vous pouvez ajouter des services de sécurité.

©2023 Palo Alto Networks, Inc.

	vCPU flexibles	Modèle VM-Series (vCPU fixes)
		Les licences perpétuelles et temporaires sont configurées et payées à l'avance et ne changent pas.
Déploiement	Après l'activation du crédit, créez un profil de déploiement pour un environnement ou un cas d'utilisation spécifique (tel que « Protéger mon environnement NSX ») et configurez les processeurs virtuels de pare-feu, les services de sécurité et un Panorama virtuel facultatif. Vous pouvez créer un nombre illimité de profils de déploiement et les personnaliser à tout moment. Vous devez avoir le rôle d'administrateur de crédit sur le portail de support client (s'applique uniquement à la gestion de compte) pour activer et gérer les crédits NGFW logiciels.	Acceptez l'ELA VM-Series. Déployez et configurez le pare-feu VM-Series. Activez le modèle de licence et enregistrez le pare-feu.
Panorama	Lorsque vous créez un profil de déploiement, vous pouvez choisir d'ajouter Panorama pour la gestion ou en tant que collecteur de journaux dédié pour les pare-feu qui utilisent un profil de déploiement. Ce Panorama peut gérer les pare-feu déployés avec le code d'autorisation partagé du profil de déploiement.	Panorama est une dépense distincte. Un Panorama physique ou virtuel peut être utilisé pour la gestion du pare-feu ou pour la collecte de journaux.
Mettre à niveau ou rétrograder	Si le pare-feu VM-Series ou Panorama dispose d'une connexion Internet, les modifications apportées à votre profil de déploiement sont automatiquement appliquées au pare-feu. Si le pare-feu n'a pas de connexion Internet, arrêtez manuellement le pare-feu. Dans Assets (Actifs) > Software NGFW Credits (Crédits NGFW logiciels), modifiez le profil de déploiement, puis dans le CSP, téléchargez les clés de licence et transférez-les sur la VM, obtenez le profil auprès du CSP, transférez-le sur la	Le passage à un autre modèle nécessite un changement de licence et un redémarrage.

©2023 Palo Alto Networks, Inc.

	vCPU flexibles	Modèle VM-Series (vCPU fixes)
	VM, redémarrez la VM et appliquez la licence. Vous n'avez pas besoin de redémarrer le pare-feu dans les deux cas.	

Déploiement de vCPU flexibles et de modèles fixes

Les listes de contrôle suivantes comparent les processus de déploiement des crédits NGFW logiciels et les méthodes de licence de modèle VM-Series.

vCPU flexibles	vCPU fixes (modèle VM-Series)
1. Création d'un compte de support. 2. Activer des crédits. Votre organisation peut avoir plusieurs comptes pour représenter différents centres de coûts. Lors de l'enregistrement, vous associez votre achat de crédit à un compte. 3. Création d'un profil de déploiement. 4. Déployez le pare-feu VM-Series sur Alibaba, AWS, Azure, Cisco ACI, Cisco CSP, Cisco ENCS, ESXi, Google Cloud Platform, Hyper-V, KVM, OpenStack. Oracle Cloud Infrastructure, vCloud Air, NSX-T ou NSX-V 5. Installation d'un certificat de périphérique sur le pare-feu VM-Series (pour les licences de site telles que Cortex Data Lake et Auto Focus.)	1. Création d'un compte de support. 2. Activation des licences de modèle VM-Series. 3. Enregistrement du pare-feu VM-Series. 4. Déployez le pare-feu VM-Series sur Alibaba, AWS, Azure, Cisco ACI, Cisco CSP, Cisco ENCS, ESXi, Google Cloud Platform, Hyper-V, KVM, OpenStack. Oracle Cloud Infrastructure, vCloud Air, NSX-T ou NSX-V. 5. Installation d'un certificat de périphérique sur le pare-feu VM-Series (pour les licences de site telles que Cortex Data Lake et Auto Focus.)

©2023 Palo Alto Networks, Inc.

Création d'un compte de support

Vous avez besoin d'un compte de support pour vous connecter au portail de support client (CSP). Vous devez vous connecter pour activer et gérer les crédits NGFW logiciels, accéder aux mises à jour logicielles ou ouvrir un ticket d'incident auprès du support technique de Palo Alto Networks. Votre compte de support vous permet d'afficher et de gérer toutes les ressources (périphériques, licences et abonnements) que vous avez enregistrées auprès de Palo Alto Networks.

Dans tous les cas, à l'exception des licences d'utilisation qui ne sont offertes que dans AWS, vous avez besoin d'un compte de support pour pouvoir télécharger le module logiciel nécessaire à l'installation du pare-feu VM-Series.

Si vous disposez d'un compte de support existant, vous pouvez télécharger et installer le logiciel de pare-feu VM-Series, puis continuer à enregistrer le pare-feu VM-Series.

STEP 1 | Accédez à https://support.paloaltonetworks.com/UserAccount/PreRegister.

STEP 2 | Saisissez l'adresse e-mail de l'entreprise à associer au compte de support.

STEP 3 | Sélectionnez l'une des options suivantes et remplissez le formulaire d'enregistrement utilisateur :

Pour une licence d'utilisation dans AWS

1. Cliquez sur **Register your Amazon Web Services VM-Series Instance (Enregistrer votre instance du pare-feu VM-Series dans Amazon Web Services)**.
2. Sur la console de gestion AWS, trouvez l'ID d'instance AWS, le Code de produit AWS et la Zone AWS dans laquelle vous avez déployé le pare-feu.
3. Remplissez les autres renseignements.

Pour toutes les autres licences

1. Cliquez sur **Register device using Serial Number or Authorization Code (Enregistrer l'appareil à l'aide du numéro de série ou du code d'autorisation)**.
2. Saisissez le code d'autorisation de capacité et le numéro de commande ou l'ID client.
3. Remplissez les autres renseignements.

STEP 4 | **Submit (Envoyez)** le formulaire. Vous recevrez un e-mail avec un lien pour activer votre compte utilisateur.

Terminez les étapes pour activer le compte. Une fois votre compte vérifié et l'enregistrement terminé, vous pouvez vous connecter au portail de support.

©2023 Palo Alto Networks, Inc.

Format du numéro de série et de l'ID du processeur pour le pare-feu VM-Series

Lorsque vous lancez une instance du pare-feu VM-Series, chaque instance du pare-feu est identifiée de manière unique à l'aide de l'ID du processeur et du numéro de série du pare-feu. Le format de l'ID du processeur et le numéro de série incluent des informations sur l'hyperviseur et le type de licence pour chaque instance du pare-feu VM-Series.

- Avec le modèle de licence basé sur l'utilisation des pare-feu VM-Series, le pare-feu génère au lancement un numéro de série et un ID de processeur, et vous utilisez ces informations pour Enregistrement du modèle basé sur l'utilisation du pare-feu VM-Series pour les clouds publics (sans code d'autorisation).
- Avec le modèle BYOL, vous enregistrez un modèle fixe de pare-feu VM-Series ou un pare-feu VM-Series avec une licence flexible sur le portail de support client (CSP).
  - Pour un pare-feu avec accès direct à Internet, vous pouvez appliquer le code d'autorisation sur le pare-feu pour générer un fichier de licence qui inclut le numéro de série.
  - Pour un pare-feu hors ligne, vous devez utiliser le CSP pour entrer l'ID du processeur, l'UUID et le code d'autorisation afin de générer un fichier de licence qui inclut le numéro de série. Vous pouvez ensuite installer la licence sur le pare-feu.

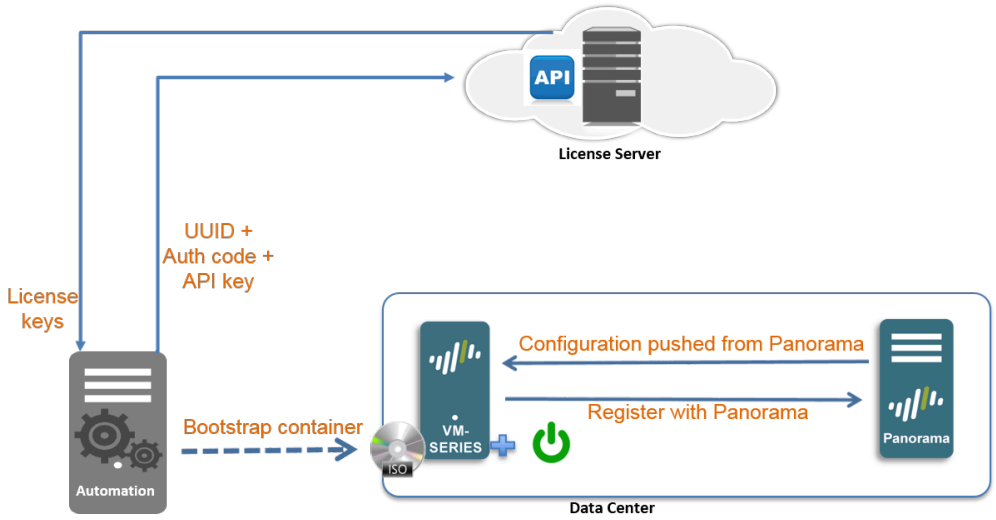
Type de licence	Numéro de série	ID de processeur
BYOL	15 caractères, tous numériques Exemple : 0071 **51** 345678909	<Hypervisor>:<ActualCPUID> Exemple : **ESX**:12345678
PAYG	15 caractères, alphanumériques Exemple : **4** DE0YTAYOGMYYTN	<Hypervisor>:<Instance-ID>:<CloudProductCode>:<CloudRegion> Exemple : **AWSMP**:1234567890abcdef0: 6kxdw3bbmdeda 3o6i1ggqt4km:us-west1

©2023 Palo Alto Networks, Inc.

API de mise sous licence

Utilisez l'API de mise sous licence pour enregistrer des codes d'autorisation, récupérer des licences attachées à un code d'autorisation, renouveler des licences ou désactiver toutes les licences sur un pare-feu VM-Series. De plus, l'API de mise sous licence vous permet d'attribuer des licences aux pare-feu qui n'ont pas d'accès Internet direct et ne peuvent pas atteindre le serveur de licences de Palo Alto Networks. Vous pouvez gérer les licences manuellement ou automatiser les licences avec un script personnalisé ou un service d'orchestration.

Vous pouvez également utiliser le plug-in de licence de pare-feu logiciel Panorama pour les tâches de mise sous licence, y compris les mises sous licence hors ligne. Le plug-in nécessite Panorama 10.0.0 ou version ultérieure avec le plug-in VM-Series 2.0.4 ou version ultérieure, et vos pare-feu VM-Series gérés doivent exécuter PAN-OS 9.1.0 ou version ultérieure et le plug-in VM-Series 2.0.4 ou version ultérieure ; le pare-feu VM-Series pour Azure nécessite le plug-in VM-Series 2.0.8.



Pour les licences basées sur des modèles, l'API vous permet de voir les détails d'un code d'autorisation afin que vous puissiez suivre le nombre de licences inutilisées associées à un code d'autorisation ou un ensemble de codes d'autorisation qui vous permettent de mettre sous licence plusieurs instances du pare-feu. Un ensemble de codes d'autorisation inclut le modèle VM-Series, les abonnements et le support dans un format unique et facile à commander ; vous pouvez utiliser cet ensemble plusieurs fois pour mettre sous licence les pare-feu VM-Series au fur et à mesure que vous les déployez.

Pour utiliser l'API, chaque compte de support reçoit une clé unique. Chaque API appelle une requête POST et la requête doit inclure la clé de l'API pour authentifier la requête sur le serveur de mise sous licence. Après l'authentification, le serveur de mise sous licence envoie la réponse au format json (application de type contenu/json).

- Gestion de la clé API de mise sous licence
- Utilisation de l'API de mise sous licence
- Codes d'erreur de l'API de mise sous licence
- Installation d'une clé API de licence

©2023 Palo Alto Networks, Inc.

Gestion de la clé API de mise sous licence

Pour obtenir la clé API requise pour utiliser l'API de mise sous licence, votre compte doit disposer de privilèges de super utilisateur sur le portail de support. La même clé est utilisée pour activer et désactiver la licence.

La date d'expiration de la clé d'API est la même date que celle du dernier abonnement de votre compte de support. Si vous renouvelez vos abonnements actuels et que vous devez redéfinir la date d'expiration de la clé API, vous pouvez régénérer une clé (et remplacer la clé existante par cette nouvelle clé où que vous l'ayez utilisée) ou contacter le support de Palo Alto Networks pour obtenir de l'aide avec l'extension de la durée de validité de votre clé API existante.

STEP 1 | Obtenez votre clé API de mise sous licence.

1. Connectez-vous au portail de support de Palo Alto Networks avec un compte qui dispose des privilèges de super utilisateur.
2. Sélectionnez **Assets (Ressources)** > **API Key Management (Gestion des clés API)**.
3. Cliquez sur **Enable (Activer)** pour afficher votre clé et copiez-la pour l'utiliser. Une fois que vous générez une clé, celle-ci est activée jusqu'à ce que vous la régénériez ou la désactiviez.

STEP 2 | Régénérez ou révoquez la clé de l'API.

1. Vous pouvez générer une nouvelle clé de l'API ou révoquer l'utilisation de la clé.
   - Cliquez sur **Regenerate (Régénérer)** pour générer une nouvelle clé. Si vous pensez qu'une clé API peut être compromise, vous pouvez générer une nouvelle clé. La régénération invalide automatiquement l'ancienne clé.
   - Sélectionnez **Disable (Désactiver)** si vous prévoyez de ne plus utiliser la clé. La désactivation de la clé de l'API la révoque.

Utilisation de l'API de mise sous licence

L'URI de base pour accéder à l'API de licence est https://api.paloaltonetworks.com/api/license. En fonction de la tâche que vous souhaitez effectuer, par exemple activer des licences, désactiver des licences ou suivre l'utilisation de la licence, l'URL change.

Une requête API doit utiliser la méthode HTTP POST, et vous devez inclure la clé API dans l'en-tête de requête HTTP apikey et transmettre les paramètres de la requête sous forme de données de formulaire codées en URL avec l'`application de type contenu /x-www-form-urlencoded`.

La version de l'API est facultative et peut inclure les valeurs suivantes : 0 ou 1. Si spécifiée, elle doit être incluse dans l'en-tête de requête HTTP `version`. La version actuelle de l'API est 1. Si vous ne spécifiez pas de version ou si vous spécifiez la version 0, la requête utilise la version actuelle de l'API.

Toutes les réponses de l'API sont représentées en json.

Avant de commencer, procurez-vous votre clé API de mise sous licence et copiez-la sur votre lecteur local. Cela est requis avant de pouvoir effectuer l'une des tâches suivantes :

- Activation des licences
- Désactivation des licences

 ©2023 Palo Alto Networks, Inc.

- Suivi de l'utilisation de licence

Activation des licences

En-tête : apikey

Paramètres : `uuid`, `cpuid`, `authCode`, `memory`, `serialNumber` et `vCPU`

URL : **`https://api.paloaltonetworks.com/api/license/activate`**

Les paramètres uuid, cpuid, authCode et serialNumber s'appliquent à toutes les licences VM-Series, quelle que soit la version de PAN-OS.

Les paramètres facultatifs `memory` et `vCPU` s'appliquent uniquement aux vCPU flexibles (PAN-OS 10.0.4 et versions ultérieures).

- Pour l'activation initiale de la licence, fournissez les paramètres dans la requête d'API. Par exemple :

```
curl -i -H
 "apikey:a103e3065360acc5e01666fb9335964fcfe668100666db6f3ff43d4544de0###"
 --data-urlencode cpuid=AWS:57060500FFFBE### --data-urlencode
 uuid=EC2278FF-F0CB-45E2-343B-E97984BAC### --data-urlencode
 authCode=D3521### --data-urlencode vcpu=4 --data-urlencode
 memory=8388608 https://api.paloaltonetworks.com/api/license/
activate
```

- Si vous n'avez pas enregistré les clés de licence ou si vous avez rencontré des problèmes de connexion réseau lors de l'activation initiale de la licence, vous pouvez récupérer la ou les licences d'un pare-feu que vous avez précédemment activé.

  Dans la requête d'API, fournissez le `cpuid` et l'`uuid`, ou fournissez le `serialNumber` du pare-feu.

Exemple de requête pour activation de licence initale en utilisant Curl :

```
curl -i -H "apikey:$APIKEY" --data-urlencode cpuid=51060400FFFBAB1F
 --data-urlencode uuid=564D0E5F-3F22-5FAD-DA58-47352C6229FF --data-
urlencode authCode=I7115398 https://api.paloaltonetworks.com/api/
license/activate
```

Exemple de réponse de l'API :

```
[{"lfidField":"13365773","partidField":"PAN-SVC-PREM-
VM-300","featureFi--eld": "Premium","feature_descField":"24
 x 7 phone support; advanced replacement
 hardware service","keyField":"m4iZEL1t3n6Oa
+6ll1L7itDZTphYw48N1AMOZXutDgExC5f5pOA52+Qg1jmAxanB
\nKOyat4FJI4k2hWiBYz9cONuKoiaNOtAGhJvAuZmYgqAZejKueWrTzCuLrwxI/iEw
\nkRGR3cYG+j6o84RitR937m2iOk2v9o8RSfLVilgX28nqmcO8LcAnTqbrRWdFtwVk
\nluz47AUMXauuqwpMipouQYjk0ZL7fTHHslhyL7yFjCyxBoYXOt3JiqQ0OCDdBdDI
\n91RkVPylEwTKgSXm3xpzbmC2ciUR5b235gyqdyW8eQXKvaThuR8YyHr1Pdw/lAjs
\npyyIVFa6FufPacfB2RHApQ==\n","auth_codeField":"","errmsgField":null,
 "typeField":"SUP","regDateField":"2016-06-03T08:18:41","startDateField":"5/29/
 "vm_capacityField":null,"uuidField":null,"cpuidField":null,"mac_baseField":nul
 "mac_countField":null,"drrField":null,"expirationField":"8/29/2016
 12:00:00 AM","PropertyChanged":null},
```

 ©2023 Palo Alto Networks, Inc.

```
{"lfidField":"13365774","partidField":"PAN-VM-300-TP",
 "featureField":"Threat Prevention","feature_descField":"Threat
 Prevention","keyField":"NqaXoaFG+9qj0t9Vu7FBMizDArj
+pmFaQEd6I2OqfBfAibXrvuoFKeXX/K2yXtrl\n2qJhNq3kwXBDxn181z3nrUOsQd/
eW68dyp4jb1MfAwEM8mlnCyLhDRM3EE+umS4b\ndZBRH5AQjPoaON7xZ46VMFovOR
+asOUJXTptS/Eu1bLAI7PBp3+nm04dYTF9O50O
\ndey1jmGoiBZ9wBkesvukg3dVZ7gxppDvz14+wekYEJqPfM0NZyxsC5dnoxg9pciF
\ncFelhnTYlma1lXrCqjJcFdniHRwO0RE9CIKWe0g2HGo1uo2eq1XMxL9mE5t025im
\nblMnhL06smrCdtXmb4jjtg==\n","auth_codeField":"",
 "errmsgField":null,"typeField":"SUB","regDateField":"2016-06-03T08:18:41",
 "startDateField":"5/29/2016","vm_capacityField":null,"uuidField":null,
 "cpuidField":null,"mac_baseField":null,"mac_countField":null,"drrField":null,
 "expirationField":"8/29/2016 12:00:00
 AM","PropertyChanged":null} ...<truncated>
```

L'élément eature_Field dans la réponse indique le type de clé qui suit dans le champ keyField. Copiez chaque clé dans un fichier texte et enregistrez-le avec l'extension .key. Parce que la clé est au format json, elle n'a pas de sauts de ligne. Assurez-vous de la convertir en sauts de ligne si cela est nécessaire pour votre analyseur. Assurez-vous de nommer chaque clé de manière appropriée et de l'enregistrer dans le dossier / license de l'ensemble d'amorçage. Par exemple, incluez le code d'autorisation avec le type de clé pour la nommer I3306691_1pa-vm.key (pour la clé de licence de capacité), I3306691_1threat.key (pour la clé de licence de Threat Prevention), I3306691_1wildfire.key (pour la clé de licence d'abonnement à WildFire).

Exemple de requête API pour récupérer des licences précédemment activées à l'aide de Curl :

```
curl -i -H "apikey:$APIKEY" --data-urlencode
 serialNumber=007200006142 https://api.paloaltonetworks.com/api/
license/activate
```

Exemple de réponse de l'API :

```
[{"lfidField":"13365773","partidField":"PAN-SVC-PREM-
VM-300","featureField": "Premium","feature_descField":"24
 x 7 phone support; advanced replacement
 hardware service","keyField":"m4iZEL1t3n6Oa
+6ll1L7itDZTphYw48N1AMOZXutDgExC5f5pOA52+Qg1jmAxanB
\nKOyat4FJI4k2hWiBYz9cONuKoiaNOtAGhJvAuZmYgqAZejKueWrTzCuLrwxI/iEw
\nkRGR3cYG+j6o84RitR937m2iOk2v9o8RSfLVilgX28nqmcO8LcAnTqbrRWdFtwVk
\nluz47AUMXauuqwpMipouQYjk0ZL7fTHHslhyL7yFjCyxBoYXOt3JiqQ0OCDdBdDI
\n91RkVPylEwTKgSXm3xpzbmC2ciUR5b235gyqdyW8eQXKvaThuR8YyHr1Pdw/lAjs
\npyyIVFa6FufPacfB2RHApQ==\n","auth_codeField":"","errmsgField":null,
 "typeField":"SUP","regDateField":"2016-06-03T08:18:41","startDateField":"5/29/
 "vm_capacityField":null,"uuidField":null,"cpuidField":null,"mac_baseField":nul
 "mac_countField":null,"drrField":null, "expirationField":"8/29/2016
 12:00:00 AM","PropertyChanged":null},
{"lfidField":"13365774","partidField":"PAN-VM-300-TP",
 "featureField":"Threat Prevention","feature_descField":
 "Threat Prevention","keyField": "NqaXoaFG
+9qj0t9Vu7FBMizDArj+pmFaQEd6I2OqfBfAibXrvuoFKeXX/K2yXtrl
\n2qJhNq3kwXBDxn181z3nrUOsQd/eW68dyp4jb1MfAwEM8mlnCyLhDRM3EE+umS4b
\ndZBRH5AQjPoaON7xZ46VMFovOR+asOUJXTptS/Eu1bLAI7PBp3+nm04dYTF9O50O
\ndey1jmGoiBZ9wBkesvukg3dVZ7gxppDvz14+wekYEJqPfM0NZyxsC5dnoxg9pciF
```


©2023 Palo Alto Networks, Inc.

```
\ncFelhnTYlma1lXrCqjJcFdniHRwO0RE9CIKWe0g2HGo1uo2eq1XMxL9mE5t025im
\nblMnhL06smrCdtXmb4jjtg==
\n","auth_codeField":"","errmsgField":null,"typeField":"SUB",
 "regDateField":"2016-06-03T08:18:41","startDateField":"5/29/2016","vm_capacity
 "mac_countField":null,"drrField":null,"expirationField":"8/29/2016
 12:00:00 AM","PropertyChanged":null} ...<truncated>
```


Désactivation des licences

URL : **`https://api.paloaltonetworks.com/api/license/deactivate`**

Paramètres : encryptedToken.

Pour désactiver les licences sur un pare-feu qui ne dispose pas d'un accès direct à Internet, vous devez générer le fichier de jeton de licence en local sur le pare-feu, puis utiliser ce fichier jeton dans la requête API. Pour plus de détails sur la génération du fichier de jeton de licence, reportez-vous à la section Désactivation de VM ou Désactivation de la licence (crédits NGFW logiciels) et Désactivation d'un abonnement ou d'une licence de fonctionnalité à l'aide de l'interface de ligne de commande (CLI).

En-tête : apikey

Requête : https://api.paloaltonetworks.com/api/license/deactivate?encryptedtoken@<token>

Exemple de requête API pour la désactivation de licence en utilisant Curl :

```
curl -i -H "apikey:$APIKEY" --data-urlencode
 encryptedtoken@dact_lic.05022016.100036.tok https://
api.paloaltonetworks.com/api/license/deactivate
```

Exemple de réponse de l'API :


```
[{"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
 "successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nu
 {"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
 "successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nu
 {"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
 "successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nu
 {"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
 "successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nu
 {"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
 "successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nu
 {"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
 "successField":"Y","errorField":null,"isBundleField":null,
 "PropertyChanged":null}]$
```


Suivi de l'utilisation de licence

URL : **`https://api.paloaltonetworks.com/api/license/get`**

Paramètres : authCode

En-tête : apikey

Requête : https://api.paloaltonetworks.com/api/license/get?authCode=<authcode>

 ©2023 Palo Alto Networks, Inc.

Exemple de requête API pour le suivi d'utilisation de licence en utilisant Curl :

```
curl -i -H "apikey:$APIKEY" --data-urlencode authcode=I9875031
 https://api.paloaltonetworks.com/api/license/get
```

Exemple de réponse de l'API :

```
HTTP/1.1 200 OK Date: Thu, 05 May 2016 20:07:16 GMT Content-Length:
 182
 {"AuthCode":"I9875031","UsedCount":4,"TotalVMCount":10,"UsedDeviceDetails":
[{"UUID":"420006BD-113D-081B-F500-2E7811BE80C
 9","CPUID":"D7060200FFFBAB1F","SerialNumber":"007200006142"}]}.....
```

Codes d'erreur de l'API de mise sous licence

Les codes d'erreur HTTP que le serveur de mise sous licence renvoie sont les suivants :

- 200 Réussite
- 400 Erreur
- 401 Clé API invalide
- 500 Erreur du serveur

©2023 Palo Alto Networks, Inc.

Installation d'une clé API de licence

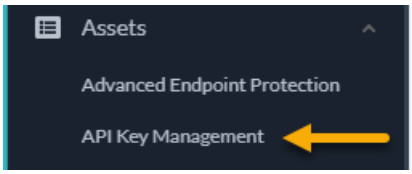
La clé API de licence peut être utilisée pour activer, modifier ou désactiver une licence. Cette procédure s'applique à un pare-feu VM-Series ou à un déploiement Panorama.

Vous devez disposer des **privilèges de super utilisateur** pour récupérer la clé API de licence à partir du portail de support client et utiliser la CLI pour installer la clé sur le pare-feu ou Panorama.

Lorsque vous installez une clé API de licence sur Panorama, Panorama envoie la clé API à ses périphériques gérés. Si une clé API est installée sur le périphérique géré, Panorama remplace l'ancienne clé API par la nouvelle.

STEP 1 | Récupérez la clé API de licence à partir du portail de support client.

1. Ouvrez une session dans le portail de support client.
2. Sélectionnez **Assets (Actifs)** > **Licensing API (API de mise sous licence)**.
3. Copiez la clé API.



STEP 2 | Utilisez la CLI pour installer la clé API copiée à l'étape précédente. Collez la clé dans la requête :

```
request license api-key set key <key>
```

STEP 3 | (facultatif) Pour remplacer une clé API de désactivation de licence, utilisez la commande CLI suivante afin de supprimer une clé API installée.

```
request license api-key delete
```

Si vous supprimez la clé API, vous devez installer une autre clé de désactivation de licence avant de pouvoir désactiver des licences.

 ©2023 Palo Alto Networks, Inc.

Utilisation la gestion des licences de pare-feu logiciel basée sur Panorama

Le plug-in de licence de pare-feu logiciel Panorama vous permet d'attribuer automatiquement une licence à un pare-feu VM-Series lorsqu'il se connecte à Panorama. Si vos pare-feu VM-Series sont situés dans le périmètre de votre déploiement et n'ont pas de connectivité au serveur de licences Palo Alto Networks, le plug-in de licence de pare-feu logiciel simplifie le processus d'activation de licence en utilisant Panorama pour octroyer une licence au pare-feu VM-Series.

De plus, le plug-in de licence de pare-feu logiciel simplifie l'activation et la désactivation de la licence des pare-feu VM-Series dans les environnements qui utilisent la mise à l'échelle automatique et l'automatisation pour déployer et supprimer des pare-feu afin de répondre aux changements dans le cloud.

Les licences Pay-As-You-Go (PAYG) ne sont pas prises en charge pour une utilisation avec ce plug-in.

N'utilisez pas le plug-in de licence de pare-feu logiciel pour obtenir une licence de pare-feu VM-Series pour VMware NSX. Le plug-in Panorama pour VMware NSX autorise automatiquement les pare-feu VM-Series déployés dans NSX et NSX-T

.

De plus, n'utilisez pas ce plug-in pour autoriser les pare-feu déployés dans des groupes d'appareils qui incluent des instances du pare-feu VM-Series déployé dans NSX-T.

Pour installer le plug-in de licence de pare-feu logiciel Panorama, vous devez utiliser Panorama 10.0.0 ou version ultérieure et le plug-in VM-Series 2.0.4 ou version ultérieure. Vos pare-feu VM-Series doivent exécuter PAN-OS 9.1.0 ou une version ultérieure.

Le pare-feu VM-Series pour Azure nécessite le plug-in VM-Series 2.0.8 ou version ultérieure.

Si vous avez un appareil Panorama autonome ou deux appareils Panorama installés dans une paire HA avec plusieurs plug-ins installés, les plug-ins peuvent ne pas recevoir les informations des indicateurs d'adresse IP mises à jour si un ou plusieurs des plug-ins ne sont pas configurés. Cela se produit, car Panorama ne transfère pas les informations des indicateurs d'adresse IP aux plug-ins non configurés. De plus, ce problème peut se présenter si un ou plusieurs plug-ins Panorama ne se trouvent pas dans l'état Registered (Enregistré) ou Success (Réussite) (l'état positif diffère sur chaque plug-in). Assurez-vous que vos plug-ins se trouvent dans l'état positif avant de continuer ou d'exécuter les commandes décrites ci-dessous.

Si vous rencontrez ce problème, il existe deux solutions alternatives :

- Désinstallez le ou les plug-ins non configurés. Il est déconseillé d'installer un plug-in que vous n'envisagez pas de configurer dans l'immédiat

 ©2023 Palo Alto Networks, Inc.

- Vous pouvez utiliser les commandes suivantes pour contourner ce problème. Exécutez la commande suivante pour chaque plug-in non configuré sur chaque instance de Panorama afin que Panorama n'attende pas pour envoyer des mises à jour. Dans le cas contraire, vos pare-feu risquent de perdre certaines informations des indicateurs d'adresse IP.

  `request plugins dau plugin-name <plugin-name> unblock-device-push yes`

  Vous pouvez annuler cette commande en exécutant :

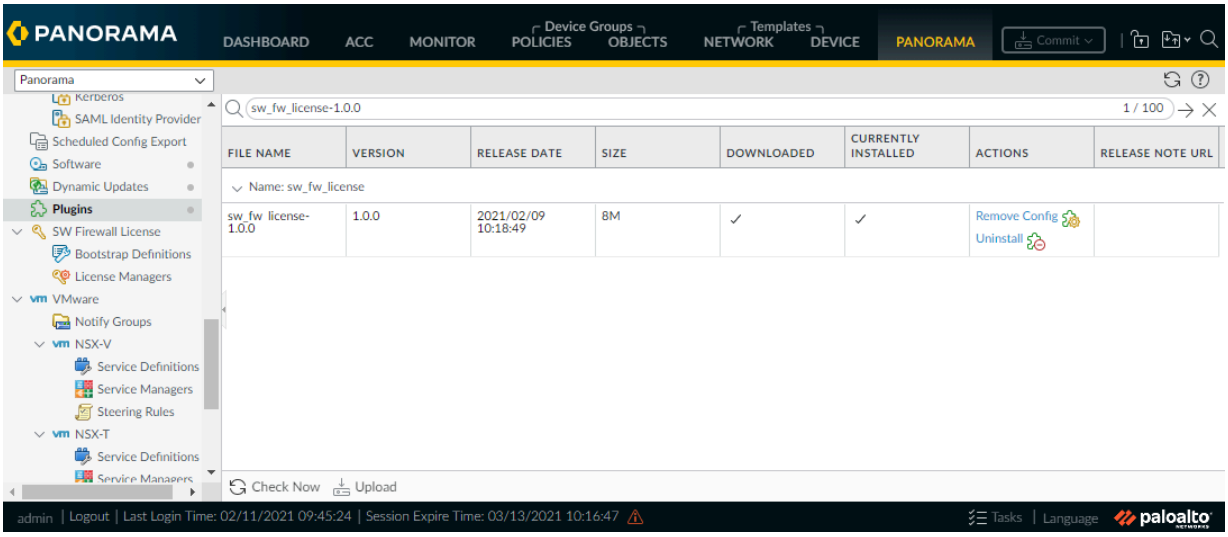
  `request plugins dau plugin-name <plugin-name> unblock-device-push no`

Les commandes décrites ne sont pas persistantes lors des redémarrages et doivent être réutilisées pour tout redémarrage ultérieur. Pour Panorama en paire HA, les commandes doivent être exécutées sur chaque Panorama.

STEP 1 | Installez le plug-in de licence de pare-feu logiciel pour Panorama.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Plugins**.
3. Cliquez sur **Check Now** (Vérifier maintenant) pour obtenir la liste des plug-ins disponibles.
4. Recherchez sw_fw_license pour localiser le plug-in.
5. Sélectionnez **Download** (Télécharger) et **Install** (Installer) pour installer le plug-in de licence logicielle.

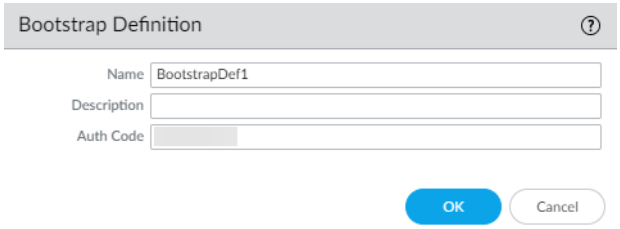
Une fois l'installation réussie, Panorama s'actualise et le plug-in de licence logicielle s'affiche sur l'onglet **Panorama**.



 ©2023 Palo Alto Networks, Inc.

STEP 2 | Configurez une définition d'amorçage.

1. Sélectionnez **Panorama** > **SW Firewall License** > **Bootstrap Definitions**.
2. Cliquez sur **Add (Ajouter)**.
3. Entrez un **Name** (Nom) descriptif pour identifier la définition d'amorçage.
4. (Facultatif) Saisissez une **Description** de la définition d'amorçage.
5. Entrez l'**Auth Code** (Code d'autorisation) que Panorama utilisera pour mettre sous licence le pare-feu VM-Series lorsqu'il se connectera à Panorama.
6. Cliquez sur **OK**.



STEP 3 | Configurez un gestionnaire de licences.

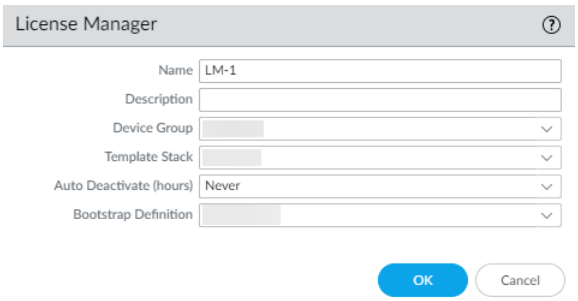
1. Sélectionnez **Panorama** > **SW Firewall License** > **License Managers**.
2. Cliquez sur **Add (Ajouter)**.
3. Saisissez un **Name** (Nom) descriptif pour identifier le gestionnaire de licences.
4. (Facultatif) Saisissez une **Description** du gestionnaire de licences.
5. Sélectionnez un **Device Group (Groupe d'appareils)** dans la liste déroulante. Lorsqu'un pare-feu VM-Series amorcé à l'aide du gestionnaire de licences se connecte à Panorama, il est placé dans le groupe d'appareils spécifié.
6. Sélectionnez une **Template Stack** (Pile de modèles) dans la liste déroulante. Lorsqu'un pare-feu VM-Series amorcé à l'aide du gestionnaire de licences se connecte à Panorama, il est placé dans la pile de modèles spécifiée.
7. Dans le champ **Auto Deactivate** (Désactivation automatique), spécifiez la durée, en heures, pendant laquelle Panorama doit attendre avant de désactiver la licence d'un pare-feu VM-Series déconnecté. Lorsque vous sélectionnez **Never** (Jamais), Panorama ne désactive pas

 ©2023 Palo Alto Networks, Inc.

un pare-feu VM-Series déconnecté. La désactivation automatique est définie sur Never (Jamais) par défaut. Vous pouvez régler l'heure de désactivation, en heures, de 1 à 24.

> ***Lors d'un intervalle de désactivation automatique, le plug-in peut désactiver la licence des pare-feu VM-Series arrêtés qui sont gérés par le même gestionnaire de licences des pare-feu qui se désactivent comme prévu.***

8. Sélectionnez une **Bootstrap Definition** (Définition d'amorçage) dans la liste déroulante. La définition d'amorçage sélectionnée spécifie le code d'autorisation utilisé par Panorama pour octroyer une licence aux pare-feu VM-Series associés au gestionnaire de licences.
9. Cliquez sur **OK**.
10. **Commit (Validez)** vos modifications.



STEP 4 | (Facultatif) Créez un fichier **`init-cfg.txt`** pour amorcer le pare-feu VM-Series. Après avoir configuré un gestionnaire de licences, vous pouvez copier et coller les paramètres d'amorçage générés par Panorama lors du déploiement de vos pare-feu VM-Series. Selon votre déploiement, les paramètres affichés peuvent être un sous-ensemble de ceux affichés dans l'image ci-dessous. Par exemple, si votre appareil Panorama est déployé dans un cloud public, les paramètres d'amorçage n'incluront pas l'adresse IP publique de Panorama. Dans ce cas, vous devez saisir manuellement l'adresse IP publique dans le fichier **`init-cfg.txt`**. Panorama générera toujours la clé d'autorisation et **`plugin-op-commands=panorama-licensing-mode-on`** à utiliser dans votre fichier **`init-cfg.tx`**t.

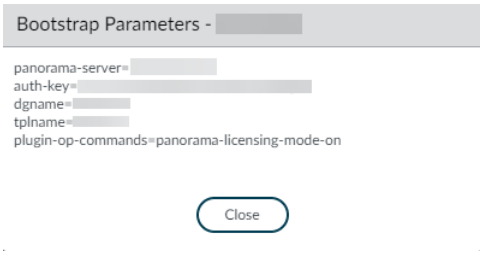
La clé d'autorisation affichée ici est générée par Panorama et utilisée pour authentifier la connexion du pare-feu VM-Series à Panorama. De plus, cette clé d'autorisation est utilisée à la place de la clé d'autorisation VM que vous pouvez générer sur Panorama et ajouter à votre fichier init-cfg.txt.

> ***Si vous utilisez la clé d'autorisation affichée ici dans votre fichier init-cfg.txt, n'utilisez pas de clé d'autorisation de machine virtuelle générée manuellement.***

1. Sélectionnez **Panorama** > **SW Firewall License** > **License Managers**.
2. Dans la colonne Action d'un gestionnaire de licences donné, cliquez sur **Show Bootstrap Parameters** (Afficher les paramètres d'amorçage).
3. Copiez les informations affichées et collez-les dans un éditeur de texte pour créer un fichier **`init-cfg.txt`** pour l'amorçage.

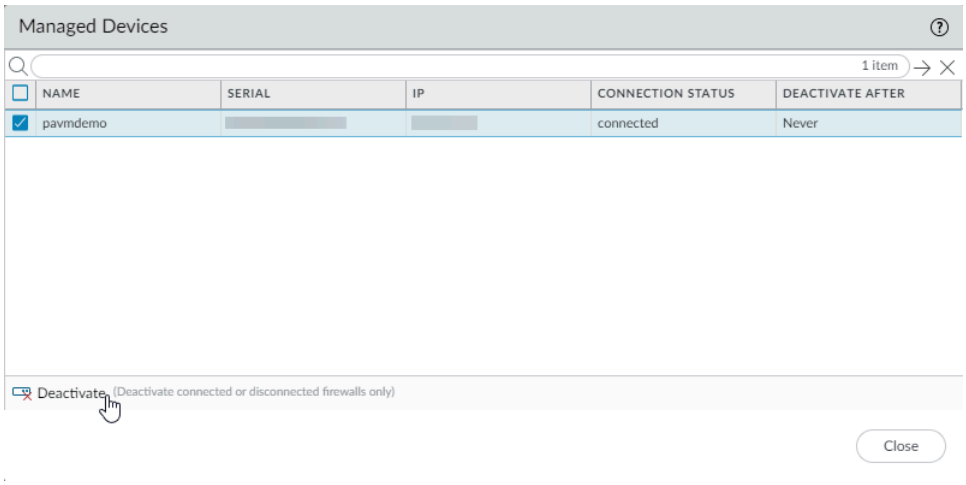
 ©2023 Palo Alto Networks, Inc.

4. Cliquez sur **Close** (Fermer) lorsque vous avez terminé.



STEP 5 | (Facultatif) Affichez et désactivez un pare-feu VM-Series géré. Dans la boîte de dialogue **Show Devices** (Afficher les périphériques), vous pouvez afficher les appareils associés à un gestionnaire de licences donné. Vous pouvez afficher le nom, le numéro de série, l'adresse IP de gestion, l'état de la connexion et le temps que Panorama attend pour désactiver un pare-feu déconnecté. De plus, vous pouvez désactiver manuellement la licence du pare-feu géré VM-Series.

1. Sélectionnez **Panorama** > **SW Firewall License** > **License Managers**.
2. Dans la colonne Action d'un gestionnaire de licence donné, cliquez sur **Show Devices** (Afficher les périphériques).
3. Pour désactiver manuellement un pare-feu géré VM-Series connecté ou déconnecté (mais pas encore désactivé), sélectionnez un ou plusieurs pare-feu VM-Series répertoriés et cliquez sur **Deactivate** (Désactiver).



STEP 6 | (Facultatif) Vérifiez que Panorama a terminé les appels d'API nécessaires pour autoriser les pare-feu connectés.

1. Connectez-vous à l'interface de ligne de commande Panorama.
2. Exécutez la commande suivante.

   ```
   show plugins sw_fw_license panorama-api-requests
   ```

 ©2023 Palo Alto Networks, Inc.

Crédits NGFW logiciels

Les crédits NGFW logiciels peuvent être utilisés pour financer des NGFW logiciels (VM-Series et CN-Series), des services de sécurité fournis par le cloud (CDSS) ou des appareils virtuels Panorama dans des réseaux avec ou sans accès Internet (réseaux air gap, par exemple).

Vous créez un profil de déploiement pour configurer un ou plusieurs pare-feu en fonction de la version PAN-OS, du nombre de vCPU par pare-feu, du nombre total de pare-feu pris en charge par le profil de déploiement, de la gestion Panorama ou de la collecte de journaux, et des services de sécurité. Toutes les VM créées avec un profil de déploiement partagent le même code d'autorisation.

- vCPU fixes : compatibles avec toutes les versions PAN-OS. Basés sur Modèles VM-Series et des ensembles de services de sécurité. La modification du modèle ou des options de service nécessite l'utilisation d'une nouvelle licence.
- vCpU flexibles : sélectionnez un nombre flexible de vCPU et procédez à une sélection flexible de services de sécurité. Vous pouvez modifier le profil de déploiement pour ajouter ou diminuer le nombre de vCPU, ajouter de nouveaux services dès qu'ils deviennent disponibles ou supprimer des services. Le nombre maximal de vCPU pour un profil de déploiement est de 64.

Les crédits NGFW logiciels sont basés sur une durée spécifique. Ces durées peuvent être définies entre 1 et 5 ans. Les crédits alloués et non alloués expirent à la fin de la durée convenue. Vous pouvez acheter des crédits supplémentaires pour un pool de crédits, mais la date d'expiration doit être identique à celle du pool cible. Utilisez le Software NGFW Credit Estimator (Estimateur de crédits NGFW logiciels) pour calculer et obtenir des crédits pour votre profil de déploiement.

Si vous disposez d'une connexion Internet au serveur de licences et que vous cessez d'utiliser un pare-feu, un service de sécurité ou un déploiement Panorama, les crédits alloués à cette ressource sont remboursés dans le pool de crédits et peuvent être réaffectés à une nouvelle ressource.

Si vous n'avez pas de connexion Internet et que vous ne pouvez pas vous connecter au serveur de mises à jour Palo Alto Networks (par exemple, vous êtes dans un réseau air gap), vous pouvez gérer le pare-feu VM-Series localement à partir de son interface utilisateur ou de Panorama. Votre administrateur doit ensuite se connecter au portail de support client pour retourner le jeton de licence, afin que les fonds puissent être réutilisés.

Utilisez le tableau **Supported Hypervisor (Hyperviseur pris en charge)** ci-dessous et les tableaux **Total vCPU on Dataplane (Nombre total de vCPU sur le plan de données)** qui suivent pour vous veiller à allouer les ressources matérielles nécessaires pour le nombre de vCPU que vous avez choisi.

Niveau	Mémoire
Niveau 1	4,5 Go, 5 Go, 5 Go, 5,5 Go, 6 Go, 6,5 Go, 7 Go, 8 Go
Niveau 2	9 Go, 10 Go, 12 Go, 14 Go, 16 Go, 18 Go
Niveau 3	20 Go, 24 Go, 28 Go, 32 Go, 36 Go, 40 Go, 44 Go, 48 Go, 52 Go, 56 Go, 60 Go, 64 Go
Niveau 4	128 Go

©2023 Palo Alto Networks, Inc.

Profil de mémoire	Hyperviseurs pris en charge	Disque dur minimum
Niveau 1 (4,5 Go, 5 Go, 5,5 Go, 6 Go de mémoire)	ESXi, Hyper-V, KVM	• Avec 4,5 Go de mémoire : 32 Go (60 Go au démarrage) • 60 Go
Niveau 1	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, Cisco ENCS, NSX-T	60 Go
Niveau 2	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, Cisco ENCS, NSX-T	60 Go
Niveau 3	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, NSX-T	60 Go
Niveau 4	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, NSX-T	60 Go

Pour tous les profils de mémoire répertoriés ci-dessus, le nombre minimum de vCPU s'élève à 2.

Le niveau 1 nécessite au moins 32 Go d'espace disque. Toutefois, étant donné que l'image de base VM-Series est commune à toutes les combinaisons de vCPU, vous devez allouer 60 Go d'espace disque jusqu'à la mise sous licence d'un pare-feu VM-Series avec 4,5 Go de mémoire.

Pour obtenir les meilleures performances, tous les cœurs requis doivent être disponibles sur un seul socket de processeur.

Par défaut, les vCPU du plan de gestion et du plan de données sont affectés dans un rapport de un à trois, sauf si vous affectez quatre vCPU ou moins. En outre, le nombre maximal de vCPU du plan de données est lié à la mémoire allouée, comme décrit dans les tableaux ci-dessous. Par exemple, si vous affectez 16 vCPU à un pare-feu VM-Series, 4 vCPU sont alloués au plan de gestion et 12 au plan de données. Si vous avez 20 vCPU et 20 Go de mémoire dans un pare-feu VM-Series, 12 vCPU sont alloués au plan de données et le reste est affecté au plan de gestion.

Vous pouvez également utiliser la CLI du pare-feu VM-Series pour Personnalisation des cœurs de plan de données. Cela vous permet de spécifier le nombre de vCPU affectés au plan de données sur votre pare-feu VM-Series.

©2023 Palo Alto Networks, Inc.

Niveau 1	4,5 Go	5 Go	5,5 Go	6 Go	6,5 Go	7 Go	8 Go
vCPU du plan de données par défaut	1	1	1	1	2	2	2

Niveau 2	9 Go	10 Go	12 Go	14 Go	16 Go	18 Go	20 Go
vCPU du plan de données par défaut	4	4	4	4	12	12	12

Niveau 3	20 Go	24 Go	28 Go	32 Go	36 Go	40 Go	44 Go	48 Go	52 Go	56 Go	64 Go
vCPU du plan de données par défaut	12	12	12	12	12	12	12	12	12	24	47

Niveau 4	121 - 128 Go
vCPU du plan de données par défaut	47

Passez aux tâches NGFW logicielles :

- Limites maximales basées sur le niveau et la mémoire
- Activer des crédits
- Création d'un profil de déploiement
- Gestion d'un profil de déploiement
- Enregistrement du pare-feu VM-Series (crédits NGFW logiciels)
- Configuration de Panorama
- Migration de Panorama vers une licence NGFW logicielle
- Transfert de crédits
- Renouvellement de votre licence de crédits NGFW logiciels
- Désactivation de la licence (crédits NGFW logiciels)
- Définir le nombre de vCPU sous licence
- Personnalisation des cœurs de plan de données
- Migration d'un pare-feu vers une licence VM-Series flexible

Limites maximales basées sur le niveau et la mémoire

Les tables suivantes indiquent le nombre maximal d'objets ou de ressources particuliers qu'un seul déploiement de pare-feu VM-Series peut créer, stocker, gérer ou avec lesquels il peut interagir en fonction de la mémoire ou du niveau alloué(e). Ces limites s'appliquent aux pare-feu VM-Series utilisant des licences financées par des crédits NGFW logiciels.

©2023 Palo Alto Networks, Inc.

Pour la mise à l'échelle de la mémoire, les incréments de mémoire sont regroupés en quatre niveaux qui représentent la capacité de configuration du pare-feu VM-Series. Quelle que soit la quantité de mémoire que vous affectez à une instance de pare-feu VM-Series, le niveau dans lequel se situe la quantité de mémoire détermine la limite des valeurs non liées aux sessions, telles que les règles de sécurité, les objets d'adresse, les profils de sécurité, etc.

Le profil de mémoire et le nombre total de vCPU déterminent le nombre de cœurs automatiquement attribués au plan de gestion et au plan de données. En outre, vous avez la possibilité de personnaliser la distribution des cœurs du plan de données.

Si vous utilisez des crédits NGFW logiciels pour la mise sous licence, vous pouvez choisir un profil de mémoire qui répond à vos exigences pour une ou plusieurs des ressources suivantes :

• Affectation d'adresse • App-ID • EDL • Client VPN GlobalProtect • VPN sans client GlobalProtect • Haute disponibilité	• Interfaces • VPN IPSec • Transfert L2 • Multicast • NAT • Objets (adresses et services)	• Politiques • QoS • Routage • Profils de sécurité • Zones de sécurité • Sessions	• Décryptage SSL • Filtrage d'URL • User-id • Routeurs virtuels • Systèmes virtuels • Câbles virtuels

Sessions

Niveau 1	4,5 Go	5 Go	5,5 Go	6 Go	6,5 Go	7 Go	8 Go
Nombre maximal de sessions (IPv4 ou IPv6)	25 000	40 000	50 000	100 000	200 000	300 000	500 000
Nombre maximal de vCPU du plan de données par défaut	1	1	1	1	2	2	2

Niveau 2	9 Go	10 Go	12 Go	14 Go	16 Go	18 Go	20 Go
Nombre maximal de sessions (IPv4 ou IPv6)	600 000	800 000	1 000 000	1 200 000	1 800 000	2 000 000	2 800 000
Nombre maximal de vCPU du plan	4	4	4	4	12	12	12

©2023 Palo Alto Networks, Inc.

Niveau 2	9 Go	10 Go	12 Go	14 Go	16 Go	18 Go	20 Go
de données par défaut							

Niveau 3	24 Go	28 Go	32 Go	36 Go	40 Go	44 Go
Nombre maximal de sessions (IPv4 ou IPv6)	3 600 000	4 400 000	5 200 000	6 000 000	6 800 000	6 800 000
Nombre maximal de vCPU du plan de données par défaut	12	12	12	12	12	12

Niveau 3 (suite)	48 Go	52 Go	56 Go	64 Go
Nombre maximal de sessions (IPv4 ou IPv6)	7 600 000	8 400 000	9 200 000	10 000 000
Nombre maximal de vCPU du plan de données par défaut	12	12	24	47

Niveau 4	121 - 128 Go
Nombre maximal de sessions (IPv4 ou IPv6)	14 000 000
Nombre maximal de vCPU du plan de données par défaut	47

Politiques

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Règles de sécurité	1 500	10,000	20,000	65 000
Planifications des règles de sécurité	256	256	256	256
Règles NAT	3000	8 000	15 000	16 000
Règles de décryptage	1 000	1 000	2 000	5 000
Règles de remplacement d'application	1 000	1 000	2 000	4 000

©2023 Palo Alto Networks, Inc.

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Règles d'inspection du contenu du tunnel	100	500	2 000	8 500
Règles SD-WAN	100	300	300	1 000
Règles de transfert basées sur les politiques	100	500	2 000	2 000
Règles du portail captif	1 000	1 000	2 000	8 000
Règles de protection DoS	1 000	1 000	1 000	2 000

Zones de sécurité

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Zones de sécurité max.	40	200	200	17 000

Objets (adresses et services)

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Objets d'adresse	10,000	20,000	40 000	160 000
Groupes d'adresses	1 000	2 500	4 000	80 000
Membres par groupe d'adresses	2 500	2 500	2 500	2 500
Objets de service	2 000	2 000	5 000	12 000
Groupes de services	500	250	500	6 000
Membres par groupe de service	500	500	500	2 500
Objets d'adresse FQDN	2 000	2 000	2 000	6 144
Adresses IP DAG max.* (capacité à l'échelle du système)	2 500	300 000	300 500	500 000
Étiquettes par adresse IP	32	32	32	64

* Débit du pare-feu mesuré avec les fonctionnalités App-ID et User-ID activées à l'aide des transactions AppMix.

©2023 Palo Alto Networks, Inc.

Profils de sécurité

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Profils de sécurité	375	750	750	750

App-ID

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Signatures d'ID d'application personnalisés	6 000	6 000	6 000	6 000
ID d'application personnalisés partagés	512	512	512	512
ID d'application personnalisés (spécifique au système virtuel)	6416	6416	6416	6416

User-id

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Mappages IP-utilisateur (plan de gestion)	524 288	524 288	524 288	524 288
Mappages IP-Utilisateur (plan de données)	64 000	512 000	512 000	512 000
Groupes actifs et uniques utilisés dans la politique (agrégat de groupes LDAP, groupes d'API XML et groupe d'utilisateurs dynamiques).*	1 000	10,000	10,000	10,000
Nombre d'agents d'identification utilisateur	100	100	100	100
Serveurs surveillés pour l'ID utilisateur	100	100	100	100
Agents Terminal Server	400	2 000	2 500	2 500
Étiquettes par utilisateur* (PAN-OS 9.1.x et versions ultérieures)	32	32	32	32

*Débit du pare-feu mesuré avec les fonctionnalités App-ID et User-ID activées à l'aide des transactions AppMix.

©2023 Palo Alto Networks, Inc.

Décryptage SSL

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Nombre maximal de certificats entrants SSL	1 000	1 000	1 000	4 000
Cache de certificat SSL (proxy de transfert)	128	4 000	8 000	32 000
Nombre maximal de sessions de décryptage simultanées	6400	50 000	100 000	2 000 000
Miroir de port SSL	Oui	Oui	Oui	Oui
Agent de décryptage SSL	Non	Non	Oui	Oui
Pris en charge par HSM	Oui	Oui	Oui	Oui

Filtrage d'URL

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Nombre total d'entrées pour la liste verte, la liste de blocage et les catégories personnalisées	25 000	25 000	100 000	100 000
Nombre maximal de catégories personnalisées	2849	2849	2849	2849
Catégories personnalisées maximales (spécifiques au système virtuel)	500	500	500	500
Taille du cache du plan de données pour le filtrage des URL	90 000	90 000	250 000	250 000
Taille du cache dynamique du plan de gestion	100 000	100 000	600 000	900 000

EDL

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Nombre maximal de listes personnalisées	30	30	30	30

©2023 Palo Alto Networks, Inc.

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Nombre maximal d'adresses IP par système	50 000	50 000	50 000	150 000
Nombre maximal de domaines DNS par système	50 000	2 000 000	2 000 000	4 000 000
Nombre maximal d'URL par système	50 000	100 000	100 000	250 000
Intervalle de vérification le plus court (minutes)	5	5	5	5

Interfaces

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Gestion – hors bande	ND	ND	ND	ND
Gestion – Haute disponibilité 10/100/1000	ND	ND	ND	ND
Gestion – Haute disponibilité 40 Gbit/s	ND	ND	ND	ND
Gestion – Haute disponibilité 10 Gbit/s	ND	ND	ND	ND
Trafic – 10/100/1000	ND	ND	ND	ND
Trafic – 100/1000/10 000	ND	ND	ND	ND
Trafic – 1 Gbit/s SFP	ND	ND	ND	ND
Trafic – 10 Gbit/s SFP+	ND	ND	ND	ND
Trafic – 40/100 Gbit/s QSFP+/QSFP28	ND	ND	ND	ND
Étiquettes 802.1q par périphérique	4094	4094	4094	4094
Étiquettes 802.1q par interface physique	4094	4094	4094	4094
Nombre maximal d'Interfaces (logiques et physiques)	2048	4096	4096	4096
Nombre maximal d'interfaces agrégées	ND	ND	ND	ND
Nombre maximal d'interfaces virtuelles SD-WAN	300	1 000	1 000	1 000

©2023 Palo Alto Networks, Inc.

Routeurs virtuels

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Routeurs virtuels	3	20	125	225

Câbles virtuels

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Câbles virtuels	12	12	12	12

Systèmes virtuels

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Systèmes virtuels de base	1	1	1	1
Systèmes virtuels max. Des licences supplémentaires sont requises pour les capacités du système virtuel supérieures à la capacité du système virtuel de base	ND	ND	ND	ND

Routage

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Dimensions de la table de transfert IPv4* (Entrées partagées entre les Virtual Routers)	5 000	32 000	100 000	À ajouter
Dimensions de la table de transfert IPv6* (Entrées partagées entre les Virtual Routers)	5 000	32 000	100 000	À ajouter
Dimensions totales de la table de transfert du système	5 000	32 000	100 000	À ajouter
32 000	50	50	50	À ajouter
Nombre maximal d'homologues de routage (dépendant du protocole)	500	1 000	1 000	À ajouter

©2023 Palo Alto Networks, Inc.

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Entrées statiques – Proxy DNS	1024	1024	1024	À ajouter
Sessions de détection de transfert bidirectionnel (BFD)	128	1024	1024	À ajouter

*Débit du pare-feu mesuré avec les fonctionnalités App-ID et User-ID activées à l'aide des transactions AppMix.

Transfert L2

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Dimensions de la table ARP par périphérique	2 500	32 000	128 000	132 000
Dimensions de la table de voisinage IPv6	2 500	32 000	128 000	132 000
Dimensions de la table MAC par périphérique	2 500	32 000	128 000	132 000
Nombre maximal d'entrées ARP par domaine de diffusion	2 500	32 000	128 000	132 000
Nombre maximal d'entrées MAC par domaine de diffusion	2 500	32 000	128 000	132 000

NAT

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Capacité totale des règles NAT	3000	8 000	8 000	À ajouter
Nombre maximal de règles NAT (statiques)* (La configuration des règles NAT statiques à pleine capacité nécessite qu'aucun autre type de règle NAT ne soit utilisé.)	3000	8 000	8 000	À ajouter
Nombre maximal de règles NAT (DIP)* (La configuration des règles DIP NAT à pleine capacité nécessite qu'aucun autre type de règle NAT ne soit utilisé.)	2 000	8 000	8 000	À ajouter

©2023 Palo Alto Networks, Inc.

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Nombre maximal de règles NAT (DIPP)	400	2 000	2 000	À ajouter
Nombre maximal d'adresses IP traduites (DIP)	128 000	160 000	160 000	À ajouter
Nombre maximal d'adresses IP traduites (DIPP)* (La capacité IP traduite DIPP est proportionnelle à la valeur de dépassement d'abonnement du pool DIPP. La capacité indiquée ici est basée sur une valeur de dépassement d'abonnement de 1x.)	400	2 000	2 000	À ajouter
Dépassement d'abonnement de pool DIPP par défaut* (Réutilisation de l'IP source et du port source entre les sessions simultanées)	2	8	8	À ajouter

*Débit du pare-feu mesuré avec les fonctionnalités App-ID et User-ID activées à l'aide des transactions AppMix.

Affectation d'adresse

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Serveurs DHCP	3	20	125	À ajouter
Relais DHCP* (La capacité maximale représente le nombre total de serveurs DHCP et de relais DHCP combinés)	500	500	500	À ajouter
Nombre maximal d'adresses attribuées	64 000	64 000	64 000	À ajouter

*Débit du pare-feu mesuré avec les fonctionnalités App-ID et User-ID activées à l'aide des transactions AppMix.

Haute disponibilité

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Périphériques pris en charge	2	2	2	2

©2023 Palo Alto Networks, Inc.

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Adresses virtuelles max.	128	32	128	À ajouter

QoS

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Nombre de politiques QoS	500	2 000	4 000	À ajouter
Interfaces physiques prenant en charge la QoS	6	12	12	12
Nœuds de texte clair par interface physique	31	63	63	63
Marquage DSCP par politique	Oui	Oui	Oui	Oui
Sous-interfaces prises en charge	ND	ND	ND	ND

VPN IPSec

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Nombre maximal d'homologues IKE	1 000	1 000	2 000	À ajouter
Site à site (avec ID de proxy)	1 000	4 000	8 000	À ajouter
Tunnels IPSec SD-WAN	1 000	1 000	2 000	À ajouter

Client VPN GlobalProtect

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Nombre maximal de tunnels (SSL, IPSec et IKE avec XAUTH)	500	6 000	12 000	À ajouter

VPN sans client GlobalProtect

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Nombre maximal de tunnels SSL	100	1 200	2 500	25 000

©2023 Palo Alto Networks, Inc.

Multicast

Fonctionnalité	Niveau 1	Niveau 2	Niveau 3	Niveau 4
Réplication (interfaces de sortie)	100	100	100	À ajouter
Itinéraires	2 000	4 000	4 000	À ajouter

Activer des crédits

Au sein de votre organisation, vous pouvez créer de nombreux comptes ayant chacun un objectif différent. Pendant l'activation, vous ne pouvez choisir qu'un seul compte par pool de crédits par défaut. Une fois que le pool de crédits est actif, les utilisateurs qui se voient attribuer le rôle d'administrateur de crédits peuvent allouer des crédits pour les déploiements, et même transférer des crédits vers d'autres pools.

Si vous avez un compte CSP existant et que vous êtes un super utilisateur ou un administrateur, le système ajoute automatiquement le rôle d'administrateur de crédits à votre profil. Si vous n'avez pas de compte existant, le CSP crée automatiquement un compte pour vous et ajoute le rôle d'administrateur de crédits à votre profil.

Vous (l'acheteur) recevez un e-mail détaillant l'abonnement, l'ID du pool de crédits, la date de début et de fin de l'abonnement, le montant des crédits achetés et la description du pool de crédits par défaut (voir « pools de crédits par défaut » dans Mise sous licence du pare-feu VM-Series).

Conservez cet e-mail pour référence ultérieure.

STEP 1 | Dans l'e-mail, cliquez sur **Start Activation** (Démarrer l'activation) pour afficher vos pools de crédits disponibles.

STEP 2 | Sélectionnez le pool de crédits que vous souhaitez activer. Vous pouvez utiliser le champ de recherche pour filtrer votre liste de comptes par numéro ou par nom.

Si vous avez acheté plusieurs pools de crédit (voir Crédits NGFW logiciels), ceux-ci sont automatiquement sélectionnés. Les coches représentent les liens d'activation pour les crédits d'intégration.

Vous êtes invité à vous authentifier ou à vous connecter.

*Si vous désélectionnez un pool de crédits, un rappel s'affiche pour indiquer que si vous souhaitez activer ces crédits, vous devez revenir à l'e-mail et cliquer sur le lien **Start Activation** (Démarrer l'activation).*

STEP 3 | Sélectionnez **Start Activation** (Démarrer l'activation).

STEP 4 | Sélectionnez le compte d'assistance (vous pouvez effectuer une recherche par numéro de compte ou par nom).

STEP 5 | Sélectionnez le pool de crédits par défaut.

©2023 Palo Alto Networks, Inc.

STEP 6 | Sélectionnez **Deposit Credits** (Déposer des crédits).

Un message indique que le dépôt a réussi.

STEP 7 | (facultatif) S'il s'agit de votre première activation de crédit, la boîte de dialogue **Create Deployment Profile (Créer un profil de déploiement)** s'affiche.

Passez à la section Création d'un profil de déploiement.

Création d'un profil de déploiement

Pour créer un profil de déploiement, vous devez disposer d'un compte de portail de service client et d'un accès à un pool de crédits activé.

Avant de commencer, estimez le nombre de pare-feu qui utiliseront la configuration dans le profil de déploiement. Vous n'avez pas besoin de déployer tous les pare-feu à la fois.

STEP 1 | Si vous disposez déjà d'un pool de crédits, connectez-vous au compte et, dans le tableau de bord, sélectionnez **Assets (Ressources)** > **Software NGFW Credits (Crédits NGFW logiciels)** > **Create Deployment Profile (Créer un profil de déploiement)**.

Si vous venez d'activer un pool de crédits, le formulaire **Create Deployment Profile (Créer un profil de déploiement)** s'affiche.

1. Sélectionnez le type de pare-feu VM-Series.
2. Sélectionnez la version de PAN-OS.
   - **Modèles fixes** (Modèles VM-Series)
   - **vCPU flexibles (PAN-OS 10.0.4 et versions ultérieures)**
3. Cliquez sur **Next (Suivant)**.

STEP 2 | Profil VM-Series.

1. **Nom du profil**.

   Nommez le profil.
2. **Nombre de pare-feu**.

   Entrez le nombre de pare-feu déployés par ce profil, à condition de disposer de crédits suffisants. Vous n'avez pas besoin de les déployer tous en même temps.
3. **Firewall Model (Modèle de pare-feu)** :

   Choisissez un modèle VM-Series.

   vCPU/pare-feu planifié (PAN-OS 10.0.4 ou version ultérieure).

   Entrez le nombre de vCPU par pare-feu.

   Cas d'utilisation de sécurité : Choisissez un cas d'utilisation.
4. **Personnaliser les abonnements**.

   Après avoir sélectionné un cas d'utilisation, vous pouvez ajouter ou supprimer des services de sécurité.
5. (facultatif) **Utilisez des crédits pour activer VM Panorama**.

   Choisissez le(s) cas d'utilisation Panorama : gestion et/ou collecteur de journaux.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | (facultatif) Survolez le point d'interrogation après **Protect more, save more (Protégez plus, économisez plus)** pour voir comment votre allocation de crédit affecte l'épargne.

STEP 4 | Cliquez sur **Calculate Estimated Cost** (Calculer le coût estimé) pour afficher le total des crédits et le nombre de crédits disponibles avant le déploiement.

(facultatif) Passez le curseur de la souris sur le point d'interrogation suivant l'estimation pour afficher la répartition des crédits pour chaque élément.

STEP 5 | **Créez le profil de déploiement**.

Vous devrez peut-être attendre plusieurs secondes pour que le profil apparaisse dans la liste de l'onglet **Current Deployment Profiles (Profils de déploiement actuels)**. Avant la fin de l'allocation, la colonne **Credits Consumed/Allocated (Crédits consommés/alloués)** affiche 0 et **Update Pending (Mise à jour en attente)**. Faites défiler vers le bas et accédez à la dernière page pour trouver votre profil.

Pour afficher votre profil de déploiement ultérieurement, cliquez sur le bouton **Details (Détails)** sur le pool de crédits parent et sélectionnez **Current Deployment Profiles (Profils de déploiement actuels)**.

- Notez le code d'authentification de votre profil tout à droite ; les codes d'authentification de crédit NGFW logiciel commencent par un D.
- La colonne **Credits Consumed/Allocated (Crédits consommés/alloués)** affiche 0 et **Update Pending (Mise à jour en attente)** avant la fin de l'allocation.
- L'onglet **Audit Trail (Piste d'audit)** affiche **Credit Transactions (Opérations de crédit)** et les **profils de déploiement** que vous gérez. Vous pouvez également rechercher un profil par heure dans cet onglet.

  Utilisez la recherche pour localiser votre profil et développez la ligne pour afficher la configuration que vous avez spécifiée lors de la création du profil.

Gestion d'un profil de déploiement

Après avoir créé votre profil de déploiement, vous pouvez le modifier, le copier ou le supprimer.

- Modifier un profil de déploiement
- Cloner un profil de déploiement
- Suppression d'un profil de déploiement

Modifier un profil de déploiement

STEP 1 | Sélectionnez **Assets (Ressources)** > **Software NGFW Credits (Crédits NGFW logiciels)** et cliquez sur le bouton **Details (Détails)** du pool de crédits que vous avez utilisé afin de créer votre profil.

STEP 2 | Sélectionnez l'onglet **Current Deployment Profiles (Profils de déploiement actuels)**.

STEP 3 | Tout à droite, sélectionnez les points de suspension verticaux (More Options [Plus d'options]) et sélectionnez **Edit Profile (Modifier le profil)**.

STEP 4 | Apportez vos modifications et sélectionnez **Update Deployment Profile** (Mettre à jour le profil de déploiement).

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Sélectionnez l'onglet **Audit Trail (Piste d'audit)** et utilisez la recherche pour localiser votre profil.

Utilisez la recherche pour localiser votre profil et développez la ligne pour afficher la configuration que vous avez spécifiée lors de la création du profil.

Cloner un profil de déploiement

STEP 1 | Sélectionnez **Assets (Ressources)** > **Software NGFW Credits (Crédits NGFW logiciels)** et cliquez sur le bouton **Details (Détails)** du pool de crédits que vous avez utilisé afin de créer votre profil.

STEP 2 | Tout à droite, sélectionnez les points de suspension verticaux (More Options [Plus d'options]) et sélectionnez **Clone Profile** (Cloner le profil).

STEP 3 | Modifiez le nom du profil, apportez d'autres modifications, puis sélectionnez **Create Deployment Profile** (Créer un profil de déploiement).

STEP 4 | Sélectionnez l'onglet **Audit Trail (Piste d'audit)** et utilisez la recherche pour localiser votre profil.

Développez la ligne pour afficher la configuration que vous avez clonée. Il s'agit d'une nouvelle configuration avec un nom de profil et un code d'autorisation différents.

Suppression d'un profil de déploiement

Avant de supprimer un profil de déploiement, vous devez Désactivation de la licence (crédits NGFW logiciels) sur n'importe quel pare-feu utilisant le profil de déploiement, puis désactiver la VM.

STEP 1 | Sélectionnez **Assets (Ressources)** > **Software NGFW Credits (Crédits NGFW logiciels)** et cliquez sur le bouton **Details (Détails)** du pool de crédits que vous avez utilisé afin de créer votre profil.

STEP 2 | Tout à droite, sélectionnez les points de suspension verticaux (More Options [Plus d'options]) et sélectionnez **Delete (Supprimer)**.

Enregistrement du pare-feu VM-Series (crédits NGFW logiciels)

L'enregistrement nécessite l'accès au portail de support client de Palo Alto Networks (le CSP) et un compte de support. Créez-en un si nécessaire.

Lors de l'activation, un administrateur active un pool de crédits et les crédits sont déposés. Lorsque quelqu'un crée un profil de déploiement, un code d'autorisation est créé. Effectuez l'une des procédures suivantes pour lancer l'enregistrement.

- Le périphérique peut accéder au CSP
- Le périphérique ne peut pas accéder au CSP

 ©2023 Palo Alto Networks, Inc.

- **Procédez comme suit si le pare-feu est capable de se connecter au CSP :**
  1. Connectez-vous au CSP avec les informations d'identification de votre compte.
  2. Sélectionnez **Assets (Ressources)** > **Software NFGW Credits (Crédits NFGW logiciels)**.

     Localisez votre pool de crédits et affichez **Details (Détails)**.
  3. Affichez les **Current Deployment Profiles (Profils de déploiement actuels)** et choisissez (ou créez) un profil.

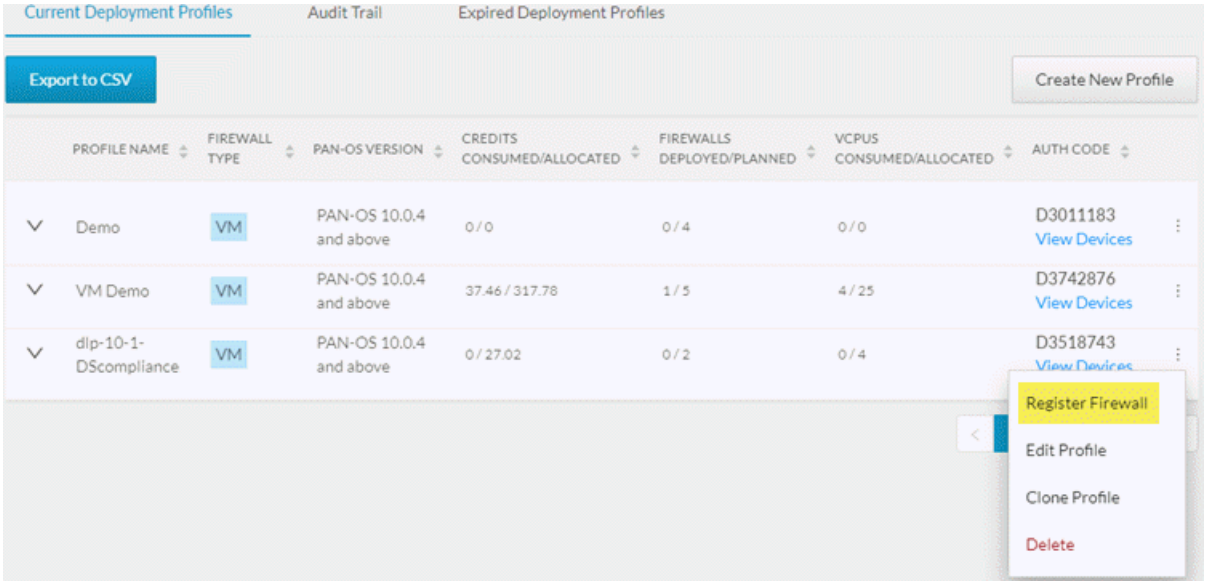
     Vous utiliserez le code d'autorisation de ce profil pour obtenir une licence pour tout pare-feu que vous créez avec celui-ci. Un code d'autorisation pour une licence de pare-feu flexible commence par la lettre D.
  4. Connectez-vous à l'interface Web du pare-feu VM-Series.
  5. Vérifiez la configuration du serveur de mises à jour de Palo Alto Networks.
     1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Services**.
     2. Confirmez que **Update Server (Serveur de mise à jour)** est défini sur `updates.paloaltonetworks.com`.
     3. Confirmez que **Verify Update Server Identity (Vérifier la mise à jour de l'identité du serveur)** est sélectionné.
  6. Sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.
     1. Sélectionnez le lien **Activate feature using authorization code (Activer la fonctionnalité à l'aide du code d'autorisation)**.
     2. Saisissez le code d'autorisation VM-Series à partir du profil de déploiement.
     3. Cliquez sur **OK** pour confirmer la mise à niveau de la licence. Le pare-feu contacte le serveur de mises à jour de Palo Alto Networks et utilise les jetons requis pour votre pare-feu en fonction du modèle VM-Series.
  7. Vérifiez que le **Dashboard (Tableau de bord)** affiche un numéro de série valide et que la licence **PA-VM** apparaît dans l'onglet **Device (Périphérique)** > **Licenses (Licences)**.
  8. Vérifiez que votre pare-feu est enregistré sur le CSP :
     - Sélectionnez **Assets (Ressources)** > **Software NFGW Credits (Crédits NFGW logiciels)**.
     - Colonne Auth Code (Code d'autorisation), **View Devices (Afficher les périphériques)** et recherchez le numéro de série de votre déploiement.
     - Dans le pool de crédits, les crédits consommés, les pare-feu déployés et les vCPU consommés doivent être incrémentés afin de refléter votre déploiement.

 ©2023 Palo Alto Networks, Inc.

- **Procédez comme suit si le pare-feu ne parvient *pas* à se connecter au CSP** :

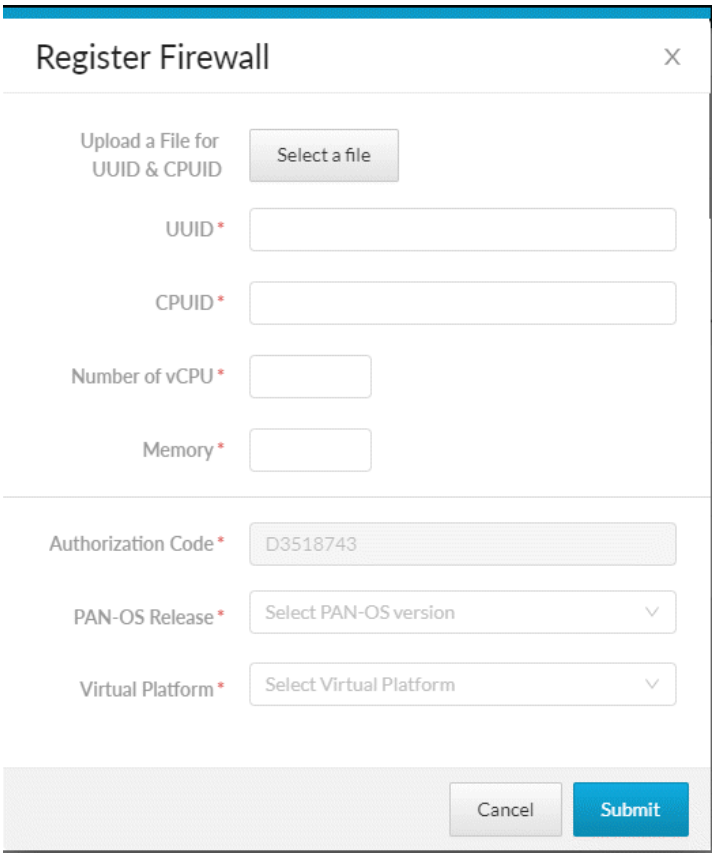
  Ce flux de travail ajoute votre pare-feu à la base de données de support. Le pare-feu ne pouvant pas se connecter au serveur de licences, vous devez transmettre manuellement les licences du CSP au pare-feu.

  1. Connectez-vous au CSP avec les informations d'identification de votre compte.
  2. Sélectionnez le nouveau profil et les points de suspension verticaux (More Option [Plus d'options]) et **Register Firewall (Enregistrer le pare-feu)**.



  Le formulaire d'enregistrement du périphérique s'ouvre. Saisissez les informations de votre pare-feu et cliquez sur **Submit (Envoyer)** :

 ©2023 Palo Alto Networks, Inc.



Cela associe le pare-feu au profil et à son code d'autorisation et attribue un numéro de série.

3. Cliquez sur **View Devices (Afficher les périphériques)** pour afficher les pare-feu associés dans **Software NGFW Devices (Périphériques NGFW logiciels)**.

   Dans la colonne **License (Licence)**, téléchargez chaque clé de licence vers un emplacement à partir duquel vous pouvez transférer les fichiers en toute sécurité vers le pare-feu.

4. Connectez-vous au pare-feu et sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.

   Les clés de licence doivent être installées via l'interface Web. Le pare-feu ne prend pas en charge l'installation de clé de licence via SCP ou FTP.

   - Cliquez sur **Manually Upload License (Charger manuellement la licence)**.
   - Vérifiez que le tableau de bord affiche un numéro de série valide et que la licence **PA-VM** apparaît dans l'onglet **Device (Périphérique)** > **Licenses (Licences)**.

Configuration de Panorama

Cette option n'est visible que si vous avez sélectionné Panorama lors de la création du profil de déploiement. Vous pouvez modifier le profil, le cas échéant.

STEP 1 | Sélectionnez **Assets (Ressources)** > **Software NGFW Credits (Crédits NGFW logiciels)** et cliquez sur le bouton **Details (Détails)** du pool de crédits que vous avez utilisé afin de créer votre profil.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Tout à droite, sélectionnez les points de suspension verticaux (More Options [Plus d'options]), puis **Provision Panorama (Configuration du Panorama)** et **Provision (Configurer)**. Vous voyez la liste des pare-feu configurés pour le profil de déploiement actuel.

Cela a pour effet de créer un Panorama, d'attribuer un numéro de série et le type de modèle PAN-PRA-1000-CP, et d'enregistrer le Panorama en tant que ressource. Le Panorama que vous venez de configurer est le dernier Panorama répertorié. Notez que le code d'autorisation commence par F (il n'est donc pas identique à celui du profil de déploiement), mais la date d'expiration est la même que le pool de crédits de votre profil.

Copiez le numéro de série.

STEP 3 | Dans le profil de déploiement, appuyez sur **View Devices (Afficher les périphériques)** et sélectionnez **Panorama** sur la page des périphériques NGFW logiciels. Tous les Panoramas NGFW logiciels s'affichent alors.

Effectuez une recherche **Search By (Rechercher par)** par numéro de série en utilisant le numéro de série que vous avez copié.

Vous pouvez également sélectionner **Assets (Ressources)** > **Software NGFW Devices (Périphériques NGFW logiciels)** et effectuez une recherche **Search By (Rechercher par)** par numéro de série avec le numéro de série que vous avez copié.

Migration de Panorama vers une licence NGFW logicielle

Vous pouvez migrer la licence VM-ELA ou la licence Panorama virtuelle perpétuelle vers une licence de pare-feu nouvelle génération logicielle (NGFW logicielle).

- Migration d'un panorama avec accès au CSP
- Migration d'une paire HA Panorama pouvant accéder au CSP
- Migration d'un Panorama autonome ne pouvant pas accéder au CSP vers une licence flexible
- Migration d'une paire HA ne pouvant pas accéder au CSP vers une licence flexible

Migration d'un panorama avec accès au CSP

Effectuez la procédure suivante pour migrer votre licence VM-ELA ou Panorama virtuelle perpétuelle vers une licence NGFW logicielle. Cette migration vous permet de déplacer vos périphériques Panorama existants vers la licence NGFW logicielle sans interruption tout en conservant votre numéro de série existant. Étant donné que votre numéro de série reste identique, vos journaux et politiques existantes sont conservés.

STEP 1 | Sélectionnez **Assets (Actifs)** > **Software NGFW Credits (Crédits NGFW logiciels)** et cliquez sur le lien **Details (Détails)** du pool de crédits que vous avez utilisé afin de créer votre profil.

STEP 2 | Tout à droite, sélectionnez les points de suspension verticaux (More Options [Plus d'options]), puis **Provision Panorama (Configuration du Panorama)** et cliquez sur **Migrate Existing (Migrer les périphériques existants)**.

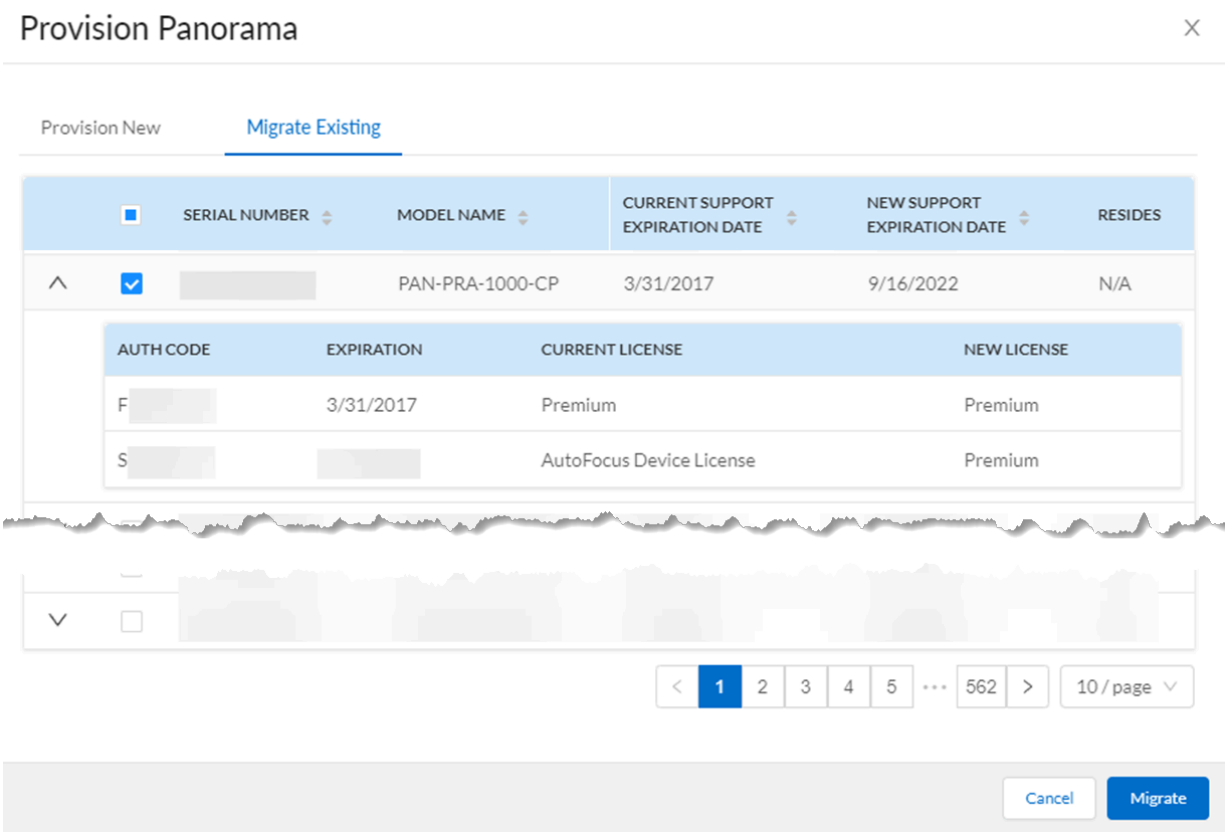
Le CSP affiche tous les périphériques Panorama virtuels associés à votre compte.

STEP 3 | Cochez la case de chaque Panorama virtuel à migrer.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Cliquez sur **Migrate (Migrer)**.

Vérifiez que la **Current Support Expiration Date (Date d'expiration du support actuel)** a été mise à jour. En outre, vous pouvez développer chaque ligne pour afficher les licences individuelles appliquées au Panorama sélectionné.



Migration d'une paire HA Panorama pouvant accéder au CSP

Effectuez la procédure suivante pour migrer une paire HA avec des licences VM-ELA ou perpétuelles vers une licence NGFW logicielle. Cette migration vous permet de déplacer vos périphériques Panorama existants vers la licence NGFW logicielle sans interruption tout en conservant votre numéro de série existant. Étant donné que vos numéros de série restent identiques, vos journaux et politiques existantes sont conservés.

STEP 1 | Sélectionnez **Assets (Actifs)** > **Software NGFW Credits (Crédits NGFW logiciels)** et cliquez sur le lien **Details (Détails)** du pool de crédits que vous avez utilisé afin de créer votre profil.

©2023 Palo Alto Networks, Inc.

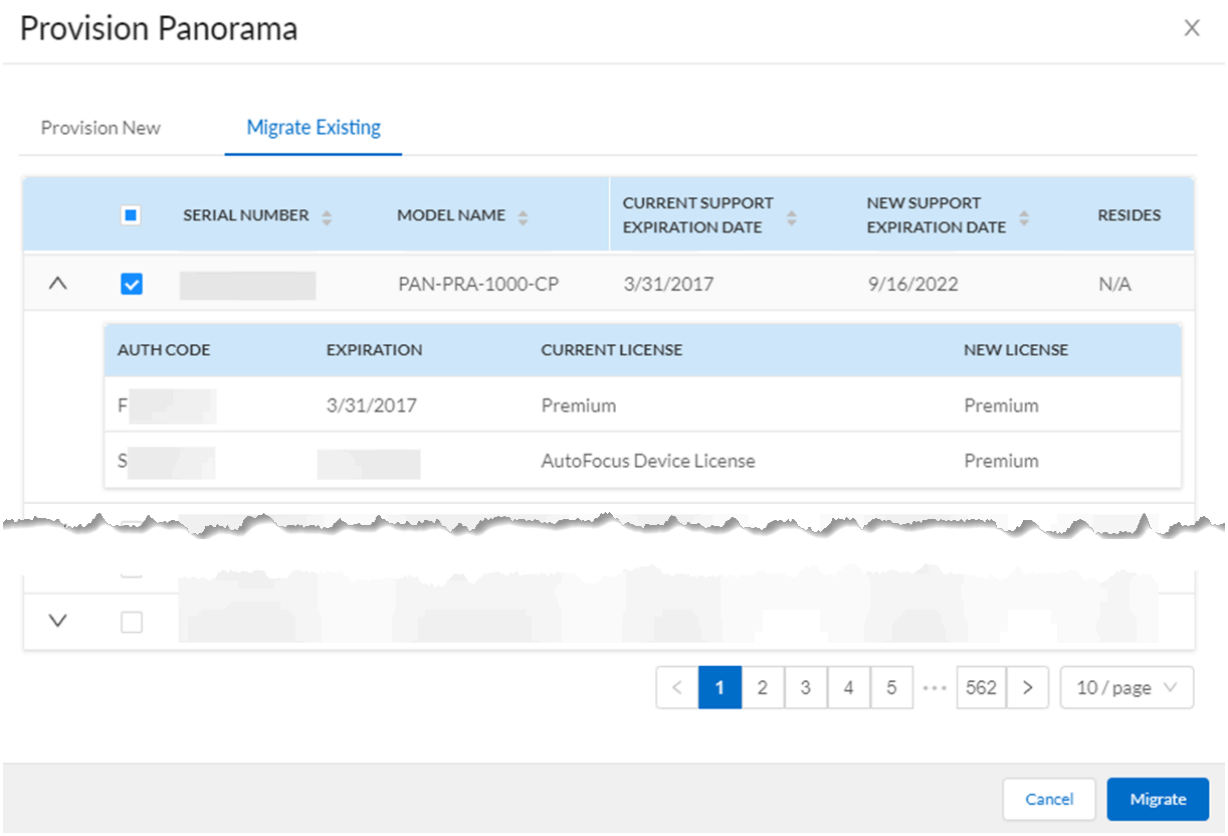
STEP 2 | Tout à droite, sélectionnez les points de suspension verticaux (More Options [Plus d'options]), puis **Provision Panorama (Configuration du Panorama)** et cliquez sur **Migrate Existing (Migrer les périphériques existants)**.

Le CSP affiche tous les périphériques Panorama virtuels associés à votre compte.

STEP 3 | Cochez la case de chaque Panorama virtuel à migrer.

STEP 4 | Sélectionnez **Migrate (Migrer)**.

Vérifiez que la **Current Support Expiration Date (Date d'expiration du support actuel)** a été mise à jour. En outre, vous pouvez développer chaque ligne pour afficher les licences individuelles appliquées au Panorama sélectionné.



Migration d'un Panorama autonome ne pouvant pas accéder au CSP vers une licence flexible

Effectuez la procédure suivante pour migrer votre licence VM-ELA ou Panorama virtuelle perpétuelle vers une licence NGFW logicielle, même si votre Panorama ne peut pas accéder au CSP. La migration

 ©2023 Palo Alto Networks, Inc.

sans le CSP nécessite un changement de numéro de série, mais elle permet à vos périphériques Panorama de migrer vers des licences NGFW logicielles et de conserver vos politiques existantes.

La version minimale pour le support de Panorama est 8.1. Si vous devez mettre à niveau PAN-OS, faites-le avant de commencer le processus de migration. Si vous souhaitez gérer des pare-feu qui utilisent des vCPU flexibles et des services avancés, la version de PAN-OS doit correspondre à la version 10.0.4 ou à une version ultérieure.

STEP 1 | Sur votre Panorama, effectuez une mise à niveau si nécessaire et notez le numéro de série et la date d'expiration du support actuel.

STEP 2 | Dans le CSP, sélectionnez **Assets (Actifs)** > **Software NGFW Credits (Crédits NGFW logiciels)** et cliquez sur le lien **Details (Détails)** sur un pool de crédits. Sélectionnez un profil de déploiement ou créez-en un.

STEP 3 | Tout à droite, sélectionnez les points de suspension verticaux (More Options [Plus d'options]), puis **Provision Panorama (Configuration du Panorama)** et sélectionnez **Migrate Existing (Migrer les périphériques existants)**.

Le CSP affiche tous les périphériques Panorama virtuels associés à votre compte.

STEP 4 | Cochez la case de chaque Panorama virtuel à migrer et sélectionnez **Migrate (Migrer)**.

STEP 5 | Dans Panorama, remplacez le numéro de série par le numéro de série du Panorama que vous avez configuré dans le CSP. Attendez une minute, puis actualisez la page.

STEP 6 | Dans le CSP, sélectionnez votre Panorama configuré et téléchargez toutes les licences (licence de support, licence de gestion et Panorama en tant que gestionnaire de journaux si votre profil de déploiement l'inclut).

Transmettez les licences en toute sécurité à votre Panorama.

STEP 7 | Téléchargez toutes les licences NGFW logicielles.

STEP 8 | Vérifiez que la **Current Support Expiration Date (Date d'expiration du support actuel)** a été mise à jour. En outre, vous pouvez développer chaque ligne pour afficher la licence de support et/ou la licence de journalisation appliquée au Panorama sélectionné.

Migration d'une paire HA ne pouvant pas accéder au CSP vers une licence flexible

Utilisez cette procédure lorsque votre paire HA ne peut pas communiquer avec le CSP. Cette procédure lance un basculement.

STEP 1 | Sélectionnez **Assets (Actifs)** > **Software NGFW Credits (Crédits NGFW logiciels)** et cliquez sur le bouton **Details (Détails)** sur un pool de crédits.

STEP 2 | Tout à droite, sélectionnez les points de suspension verticaux (More Options [Plus d'options]), puis **Provision Panorama (Configuration du Panorama)**.

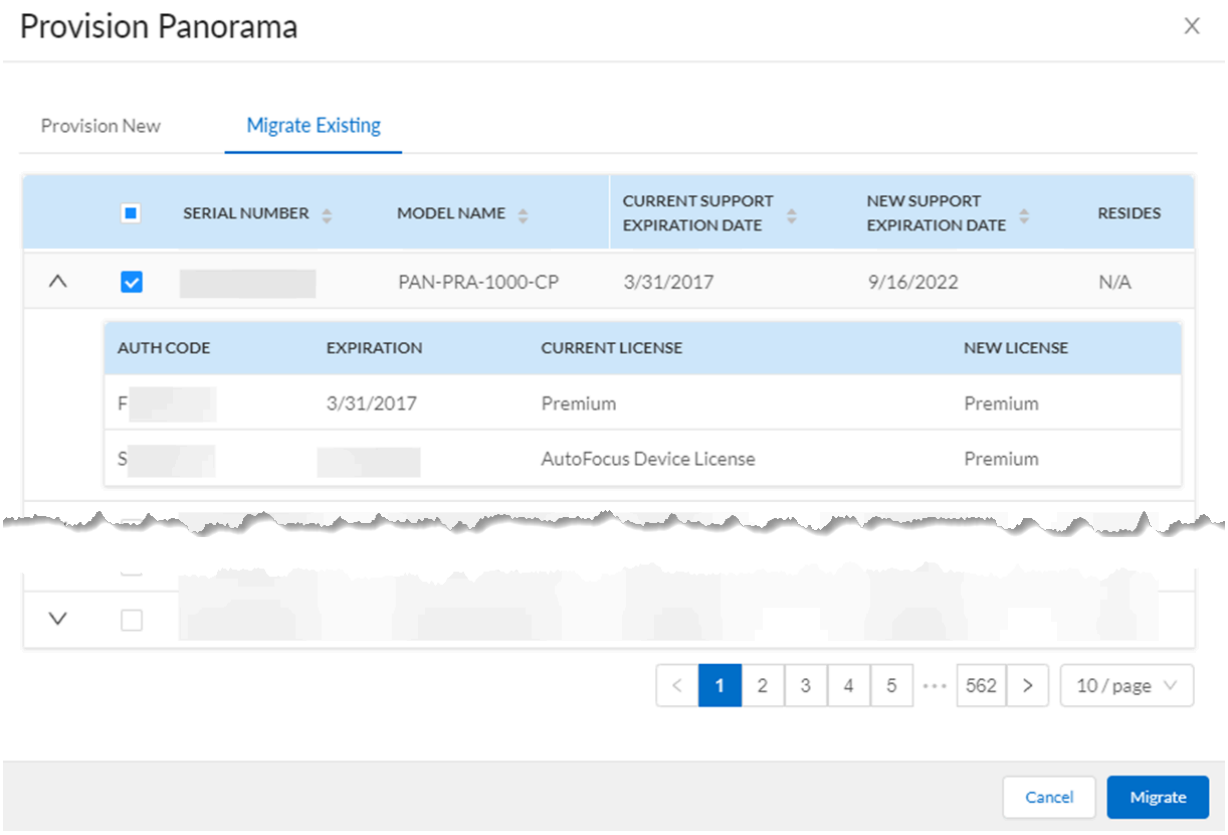
Le CSP affiche tous les périphériques Panorama virtuels associés à votre compte de support.

©2023 Palo Alto Networks, Inc.

STEP 3 | Sélectionnez **Provision New (Nouvelle configuration)**, cochez la case de chaque Panorama virtuel à migrer, puis sélectionnez **Migrate (Migrer)**.

Les Panoramas migrés sont affichés en tant que Software NGFW Devices (Périphériques NGFW logiciels).

STEP 4 | Vérifiez que la **Current Support Expiration Date (Date d'expiration du support actuel)** a été mise à jour. En outre, vous pouvez développer chaque ligne pour afficher les licences individuelles appliquées au Panorama sélectionné.



Transfert de crédits

À partir du portail de support client (CSP), transférez des crédits vers un pool de crédits du même compte ou vers un pool de crédits d'un autre compte auquel vous pouvez accéder.

- Compte CSP différent
- Pool différent dans ce compte

©2023 Palo Alto Networks, Inc.

Compte CSP différent

STEP 1 | Connectez-vous à votre compte CSP.

STEP 2 | Sélectionnez **Assets** > **Software NGFW Credits**.

- Identifiez le pool de crédits source et notez l'ID du pool de crédits.
- Identifiez le pool de crédits de destination et notez l'ID du pool de crédits.

  Si la destination se trouve dans un autre compte, sélectionnez-le dans la liste déroulante **Current Account** (Compte courant) en haut à gauche et sélectionnez **Assets** > **Software NGFW Credits**. Recherchez la destination et notez le type de crédit et l'ID du pool de crédits.

STEP 3 | Accédez au pool de crédits source et cliquez sur **Transfer Credits** (Transférer des crédits) en bas à gauche.

STEP 4 | Choisissez un autre compte CSP.

1. **Transfer to** (Transférer vers) — Choisissez un nom de compte.
2. **As credit type** (Comme type de crédit) — Choisissez un type de crédit. À ce stade, le type de source et de destination doit être le même.
3. **Credit Pool ID#** (N° ID pool de crédits) — Choisissez un numéro d'identification de pool de crédits.

   Si le compte de destination n'a pas de pool de crédits du type choisi, le CSP vous invite à créer un pool de crédits.
4. **Amount to Transfer** (Montant à transférer) — Entrez le montant à transférer.

STEP 5 | Sélectionnez **Update Credits** (Mettre à jour les crédits).

Vous devrez peut-être attendre un peu ou actualiser votre écran pour voir le changement.

STEP 6 | Pour afficher les transactions de crédit pour un pool, sélectionnez **Details** (Détails), puis **Audit Trail** (Piste d'audit).

Pool différent dans ce compte

STEP 1 | Connectez-vous à votre compte CSP.

STEP 2 | Sélectionnez **Assets** > **Software NGFW Credits**.

- Identifiez le pool de crédits de destination et notez l'ID du pool de crédits.
- S'il n'existe pas de pool de crédits de destination du type que vous spécifiez, vous êtes invité à créer un nouveau pool de crédits.

STEP 3 | Accédez au pool de crédits source et sélectionnez **Transfer Credits** (Transférer des crédits) en bas à gauche.

©2023 Palo Alto Networks, Inc.

STEP 4 | Sélectionnez **Different Pool in this Account** (Pool différent dans ce compte).

1. **New credit type** (Nouveau type de crédit) — Choisissez un type de crédit. À ce stade, le type de source et de destination doit être le même.
2. **Credit Pool ID#** (N° ID pool de crédits) — Choisissez un numéro d'identification de pool de crédits.

   Si le compte de destination n'a pas de pool de crédits du type choisi, le CSP vous invite à créer un pool de crédits.
3. **Amount to Transfer** (Montant à transférer) — Entrez le montant à transférer.

STEP 5 | Sélectionnez **Update Credits** (Mettre à jour les crédits).

Vous devrez peut-être attendre un peu ou actualiser votre écran pour voir le changement.

STEP 6 | Pour afficher les transactions de crédit pour un pool, sélectionnez **Details** (Détails), puis **Audit Trail** (Piste d'audit).

Renouvellement de votre licence de crédits NGFW logiciels

Lorsqu'un profil de déploiement expire, il passe de l'onglet Current Deployment Profiles (Profils de déploiement actuels) à l'onglet Renew Profiles (Renouveler les profils). Dans l'onglet Renew Profiles (Renouveler les profils), vous pouvez renouveler rapidement vos profils de déploiement à partir du portail de support client de Palo Alto Networks sans interrompre les opérations de votre pare-feu VM-Series. Une fois qu'un profil de déploiement expire et passe à l'onglet Renew Profiles (Renouveler les profils), vous disposez de 30 jours pour renouveler le profil. Tous les profils de déploiement non renouvelés dans les 30 jours expirent et passent à l'onglet Expired Deployment Profile (Profil de déploiement expiré). Pour plus d'informations, reportez-vous à la section Que se passe-t-il à l'expiration des licences ?.

Après le renouvellement, vous remarquerez peut-être des changements entre vos profils de déploiement précédents. Les pools de crédits NGFW Prisma et NGFW virtuels s'appellent désormais pools de crédits NGFW logiciels. En outre, le nombre de crédits dans votre pool peut changer après le renouvellement en raison de modifications apportées au modèle de tarification du produit.

STEP 1 | Connectez-vous au portail de support client de Palo Alto Networks.

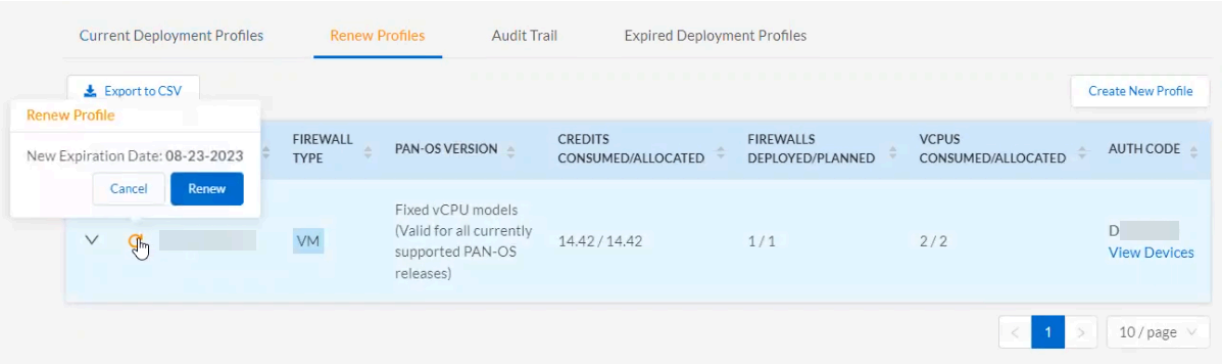
STEP 2 | Sélectionnez **Assests (Ressources)** > **Software NGFW Credits (Crédits NGFW logiciels)**.

STEP 3 | Recherchez le profil de déploiement à renouveler et cliquez sur **Details (Détails)**.

STEP 4 | Sélectionnez **Renew Profiles (Renouveler les profils)**.

 ©2023 Palo Alto Networks, Inc.

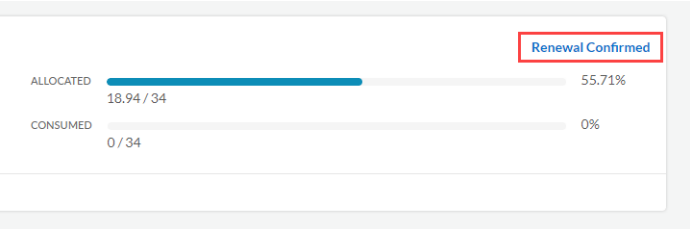
STEP 5 | Cliquez sur l'icône Renouveler, puis sur **Renew (Renouveler)** pour confirmer.



STEP 6 | Vérifiez que votre profil de déploiement a été renouvelé avec succès.

1. Cliquez sur **Current Deployment Profiles (Profils de déploiement actuels)**.
2. Confirmez que le profil de déploiement renouvelé est affiché.

   De plus, vous pouvez revenir au tableau de bord Software NGFW (NGFW logiciel) pour afficher votre pool de crédits. Une fois le renouvellement réussi, le pool de crédits affiche **(Renewal Confirmed) Renouvellement confirmé**. Ce message reste jusqu'à la fin de la date d'expiration de vos crédits NGFW logiciels renouvelés.



Désactivation de la licence (crédits NGFW logiciels)

Vous devez désactiver toutes les licences du CSP **avant** de supprimer un pare-feu (ou la VM hébergeant le pare-feu) ou les crédits de licence ne peuvent pas revenir à votre pool de crédits.

Lorsque vous avez un accès Internet au serveur de licences, la désactivation du pare-feu sur le CSP supprime automatiquement les licences et les crédits restants sont renvoyés au profil de déploiement. Après avoir désactivé la licence, vous devez supprimer le pare-feu ou il continuera à consommer des crédits.

Si vous n'avez pas accès à Internet, vous devez exporter le jeton de licence à partir du pare-feu. Ensuite, dans le CSP, démarrez la désactivation et téléchargez le jeton (ou collez-le dans le texte du jeton) pour terminer la désactivation.

- Accès à internet
- Aucun accès à Internet

©2023 Palo Alto Networks, Inc.

- Aucun accès à Internet – gestion de Panorama

- Accès direct à Internet.
  1. Sélectionnez **Assets (Ressources)** > **Software NGFW Credits (Crédits NGFW logiciels)** et cliquez sur le bouton **Details (Détails)** du pool de crédits que vous avez utilisé pour créer votre profil de déploiement.
  2. Localisez votre profil de déploiement et, tout à droite, sélectionnez les points de suspension verticaux (More Options [Plus d'options]) et sélectionnez **Deactivate Firewall (Désactiver le pare-feu)**.
  3. Cochez le pare-feu que vous souhaitez désactiver, puis sélectionnez **Deactivate Firewall (Désactiver le pare-feu)**.

- Aucun accès à Internet.
  1. Connectez-vous à l'interface Web du pare-feu et sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.
  2. Dans la section License Management (Gestion des licences), sélectionnez **Deactivate VM (Désactiver VM)**.

     Vérifiez la liste des licences et des autorisations à désactiver sur le pare-feu.
  3. Sélectionnez **Complete Manually (Terminer manuellement)** pour démarrer la désactivation.

     Cliquez sur le lien **Export license token (Exporter le jeton de licence)** pour enregistrer le fichier de jeton sur le client. Un nom de fichier de jeton ressemble à ceci : `20150128_1307_dact_lic.01282015.130737.tok`

     À ce stade, la licence a été désactivée sur le pare-feu, mais les crédits n'ont pas été renvoyés au pool de crédits.
  4. Utilisez le fichier de jeton pour enregistrer les modifications auprès du serveur de mise sous licence :

     1. Connectez-vous au site Web d'assistance client de Palo Alto Networks.
     2. Sélectionnez **Assets** > **VM-Series Auth-Codes** > **Deactivate License(s) (Désactivation des licences)**.

     Dans le formulaire Deactivate Licenses (Désactiver les licences), collez le texte du jeton ou copiez le jeton sur un ordinateur doté d'un accès à Internet et téléchargez le fichier du jeton dans le CSP pour terminer la suppression de la licence.
  5. Supprimer la VM

 ©2023 Palo Alto Networks, Inc.

- Aucun accès à Internet – gestion de Panorama
  1. Connectez-vous à Panorama et sélectionnez **Panorama** > **Device Deployment (Déploiement de périphérique)** > **Licenses (Licences)**.
  2. **Cliquez sur Deactivate VMs (Désactiver VM)**, puis sélectionnez le pare-feu VM-Series que vous souhaitez désactiver.
  3. Sélectionnez **Complete Manually (Terminer manuellement)** pour exporter le fichier de jeton.
  4. Cliquez sur le lien **Export license token (Exporter le jeton de licence)** pour enregistrer le fichier de jeton. Un nom de fichier de jeton ressemble à ceci : 20150128_1307_dact_lic.01282015.130737.tok

     Si l'exportation réussit, un message d'achèvement s'affiche et le pare-feu redémarre automatiquement.
  5. Utilisez le fichier de jeton pour enregistrer les modifications auprès du serveur de mise sous licence.

     1. Connectez-vous au site Web d'assistance client de Palo Alto Networks.
     2. Sélectionnez **Assets** > **VM-Series Auth-Codes** > **Deactivate License(s) (Désactivation des licences)**.

     Dans le formulaire Deactivate Licenses (Désactiver les licences), collez le texte du jeton ou copiez le jeton sur un ordinateur doté d'un accès à Internet et téléchargez le fichier du jeton dans le CSP pour terminer la suppression de la licence.
  6. (facultatif) Retirez le pare-feu VM-Series désactivé des périphériques gérés dans Panorama.

     Au lieu de supprimer les pare-feu désactivés, vous pouvez créer un groupe d'appareils distinct et les lui affecter.

     1. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)**.
     2. Sélectionnez le pare-feu que vous avez désactivé et cliquez sur **Delete (Supprimer)**.

Définir le nombre de vCPU sous licence

Vous pouvez spécifier le nombre de vCPU sous licence lors de l'utilisation de crédits NGFW logiciels au lieu de mettre sous licence tous les vCPU disponibles sur l'instance de calcul de votre choix. Cela vous permet d'utiliser une plus grande instance de calcul sans consommer plus de crédits NGFW logiciels que nécessaire.

Cette fonctionnalité nécessite le plug-in VM-Series 2.1.4 ou version ultérieure.

Vous pouvez spécifier le nombre de vCPU à mettre sous licence à l'aide d'une commande opérationnelle du plug-in d'amorçage ou de la CLI du pare-feu VM-Series.

 ©2023 Palo Alto Networks, Inc.

- Pour définir le nombre de cœurs lors de l'amorçage d'un pare-feu VM-Series, ajoutez la commande suivante à votre fichier init-cfg.txt.

  plugin-op-commands=set-cores:<number-of-cores>

  Par exemple :

  plugin-op-commands=set-cores:4
- Pour définir le nombre de cœurs sur un pare-feu VM-Series qui a déjà été déployé, utilisez la commande CLI suivante.

  request plugins vm_series set-cores cores <number-of-cores>

  Par exemple :

  request plugins vm_series set-cores cores 16

  Vous devez redémarrer le pare-feu VM-Series pour que cette modification prenne effet.

Personnalisation des cœurs de plan de données

Comme mentionné dans Crédits NGFW logiciels, lorsqu'un pare-feu est déployé à l'aide de crédits NGFW logiciels, le profil de mémoire et le nombre total de vCPU déterminent le nombre de cœurs automatiquement attribués au plan de gestion et au plan de données. Les configurations par défaut fonctionnent bien dans la plupart des cas.

Personnaliser les cœurs du plan de données est une fonctionnalité facultative qui vous permet de personnaliser le nombre de cœurs du plan de données de deux manières :

- Lors du déploiement initial, utilisez le paramètre d'amorçage du fichier **init-cfg.txt** **plugin-op-commands=set-dp-cores:<#-cores>**. Reportez-vous à la section Composants du fichier init-cfg.txt.
- À partir d'un pare-feu déployé, à l'aide de la commande CLI VM-Series **request plugins vm_series dp-cores <#-cores>**. Cette procédure est décrite ci-dessous.

En règle générale, vous augmentez le nombre de cœurs de plan de données (ce qui diminue le nombre de cœurs de plan de gestion) pour améliorer les performances. La personnalisation des cœurs du plan de données ne nécessite pas de modification du profil de déploiement ou de crédits supplémentaires, car le nombre total de vCPU reste le même.

- La personnalisation des cœurs du plan de données est prise en charge sur les pare-feu exécutant PAN-OS 10.1 ou version ultérieure sous licence avec un pool de crédits NGFW logiciels pour la version 10.0.4 et les versions ultérieures.
- La personnalisation des cœurs du plan de données n'est pas prise en charge pour :
  - NSX-T
  - Délestage intelligent du trafic

Suivez ces étapes pour personnaliser les cœurs du plan de données sur le pare-feu VM-Series.

STEP 1 | Connectez-vous au pare-feu VM-Series et affichez le nombre de cœurs.

```
admin@PA-VM(active)>show plugins vm_series dp-cores
Device current DP cores: 13 (Total cores: 18)
```

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Modifiez le nombre de cœurs de plan de données.

> *Notez que vous devez disposer d'au moins un cœur de plan de gestion et que le fait d'avoir trop peu de cœurs affecte les performances.*

Dans cet exemple, nous augmentons les plans de données à 14.

```
admin@PA-VM(active)>request plugins vm_series dp-cores 14
Device current DP cores: 14 (Total cores: 18)
```

STEP 3 | Redémarrez le pare-feu VM-Series.

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)** et cliquez sur **Reboot Device (Redémarrer le périphérique)**.

STEP 4 | Utilisez **`show plugins vm_series dp-cores`** pour vérifier que le nombre de cœurs du plan de données a changé.

Migration d'un pare-feu vers une licence VM-Series flexible

Vous pouvez procéder à la migration de votre licence de pare-feu VM-Series perpétuelle ou ELA vers une licence de pare-feu VM-Series flexible (financée à l'aide de crédits NGFW logiciels). À partir de Panorama, vous pouvez faire passer la licence sur un pare-feu individuel ou sur plusieurs pare-feu simultanément à partir de Panorama.

Utilisez cette procédure pour migrer d'une licence d'évaluation vers un code d'autorisation de pool de crédits non lié à l'évaluation sans interruption.

Effectuez l'une des procédures suivantes pour procéder à la migration de vos licences.

- Pare-feu autonome avec accès au CSP
- Pare-feu autonome sans accès au CSP
- Pare-feu gérés par Panorama avec accès au CSP
- Pare-feu gérés par Panorama sans accès au CSP
- Le pare-feu géré par Panorama et Panorama n'ont pas accès au CSP
- Vérification de la migration

Pare-feu autonome avec accès au CSP

Ce processus n'interrompt pas le trafic qui traverse le pare-feu.

STEP 1 | Connectez-vous à l'interface Web du pare-feu VM-Series.

STEP 2 | Vérifiez la configuration du serveur de mises à jour de Palo Alto Networks.

1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Services**.
2. Confirmez que **Update Server (Serveur de mise à jour)** est défini sur `updates.paloaltonetworks.com`.
3. Confirmez que **Verify Update Server Identity (Vérifier la mise à jour de l'identité du serveur)** est sélectionné.

©2023 Palo Alto Networks, Inc.

STEP 3 | Connectez-vous au CSP et Création d'un profil de déploiement. Si la licence dont vous souhaitez effectuer la migration concerne un pare-feu VM-Series avec une licence ELA ou perpétuelle, vous devez choisir **Fixed Models (Modèles fixes)** et utiliser le même modèle VM-Series et le même nombre de vCPU lorsque vous créez le profil de déploiement SW NGFW pour la licence flexible.

Vous utiliserez le code d'autorisation de ce profil. Un code d'autorisation pour une licence de pare-feu flexible commence par la lettre D, comme indiqué ci-dessous.

STEP 4 | Sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.

Si le modèle VM-Series actuel et le modèle VM-Series vers lequel vous effectuez la migration sont différents, sélectionnez le lien **Upgrade VM Capacity (Mettre à niveau la capacité de la VM)**.

Si le modèle VM-Series est le même avant et après la migration, sélectionnez le lien **Activate feature using authorization code (Activer la fonctionnalité à l'aide du code d'autorisation)**.

STEP 5 | Entrez le code d'autorisation VM-Series à partir du nouveau profil de déploiement.

STEP 6 | Cliquez sur **OK** pour confirmer la mise à niveau de la licence. Le pare-feu contacte le serveur de mises à jour de Palo Alto Networks et utilise les jetons requis pour votre pare-feu en fonction du modèle VM-Series.

STEP 7 | (Facultatif) Vérification de la migration.

STEP 8 | Répétez ce processus pour chaque pare-feu VM-Series de votre déploiement.

Pare-feu autonome sans accès au CSP

Procédez à la migration d'une licence sur un pare-feu sans accès direct au CSP.

STEP 1 | Si nécessaire, installez la clé API de licence sur votre pare-feu VM-Series.

STEP 2 | Utilisez la CLI pour utiliser le mode manuel afin de désactiver la licence de modèle fixe.

STEP 3 | Désactivez la VM du pare-feu. à l'aide de la procédure manuelle, et connectez-vous au CSP et utilisez le fichier de jeton pour désactiver la VM.

STEP 4 | Dans le CSP, Création d'un profil de déploiement avec le même modèle VM-Series, le même nombre de vCPU et les mêmes abonnements de sécurité que l'ancienne licence de modèle fixe. Vous utiliserez le code d'autorisation de ce profil.

STEP 5 | Sélectionnez le nouveau profil, cliquez sur les points de suspension verticaux et sélectionnez **Register Firewall (Enregistrer le pare-feu)**.

1. Entrez les informations de la VM et du pare-feu et sélectionnez **Submit (Envoyer)**. Cela associe le pare-feu au profil et à son code d'autorisation et attribue un numéro de série.
2. Cliquez sur **View Devices (Afficher les périphériques)** pour afficher les périphériques associés dans **Software NGFW Devices (Périphériques NGFW logiciels)**.
3. Dans la colonne **License (Licence)**, téléchargez les clés de licence vers un emplacement à partir duquel vous pouvez transférer les fichiers en toute sécurité vers la machine hôte.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Dans le pare-feu, sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.

Les clés de licence doivent être installées via l'interface Web. Le pare-feu ne prend pas en charge l'installation de clé de licence via SCP ou FTP.

STEP 7 | Cliquez sur **Manually Upload License (Charger manuellement la licence)** et saisissez les clés de licences.

STEP 8 | Vérifiez que le **Dashboard (Tableau de bord)** affiche un numéro de série valide et que la licence **PA-VM** apparaît dans l'onglet **Device (Périphérique)** > **Licenses (Licences)**.

STEP 9 | (facultatif) Vérification de la migration.

Pare-feu gérés par Panorama avec accès au CSP

Procédez à la migration d'une licence fixe vers une licence flexible sur les pare-feu gérés par Panorama.

STEP 1 | Avant de commencer, assurez-vous d'installer une clé API de licence sur le pare-feu.

STEP 2 | Connectez-vous à l'interface Web Panorama.

STEP 3 | Vérifiez la configuration du serveur de mises à jour de Palo Alto Networks pour les pare-feu.

1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Services**.
2. Confirmez que **Update Server (Serveur de mise à jour)** est défini sur `updates.paloaltonetworks.com`.
3. Confirmez que **Verify Update Server Identity (Vérifier la mise à jour de l'identité du serveur)** est sélectionné.

STEP 4 | Création d'un profil de déploiement pour la nouvelle licence si vous ne l'avez pas déjà fait. Ce profil est requis pour générer le nouveau code d'autorisation pour le Panorama migré.

STEP 5 | Récupérez le code d'autorisation VM-Series. Un code d'autorisation de pare-feu pour une licence flexible commence par la lettre F, comme indiqué ci-dessous.

STEP 6 | Appliquez le nouveau code d'autorisation.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Licenses (Licences)** et **Activate (Activer)**.
2. Saisissez votre code d'autorisation VM-Series.
3. Utilisez les Filters (Filtres) pour sélectionner les pare-feu gérés à mettre sous licence.
4. Saisissez votre code d'autorisation dans la colonne **Auth Code** (Code d'autorisation) pour chaque pare-feu.
5. **Activez** pour confirmer la mise à niveau de la licence. Panorama contacte le serveur de mises à jour de Palo Alto Networks et utilise les jetons requis pour vos pare-feu en fonction du modèle VM-Series, des vCPU et des services que vous avez choisis.

STEP 7 | (facultatif) o.

 ©2023 Palo Alto Networks, Inc.

Pare-feu gérés par Panorama sans accès au CSP

Procédez à la migration d'un pare-feu VM-Series géré par Panorama qui ne peut pas accéder au CSP.

STEP 1 | Avant de commencer, assurez-vous d'installer une clé API de licence sur le pare-feu.

STEP 2 | **Panorama, aucun accès à Internet** : procédez à la migration des licences sur des pare-feu gérés par Panorama hors ligne.

STEP 3 | Désactivez la VM de Panorama. à l'aide de la procédure manuelle, et connectez-vous au CSP et utilisez le fichier de jeton pour désactiver la VM.

STEP 4 | Dans le CSP, Création d'un profil de déploiement avec le même modèle VM-Series, le même nombre de vCPU, les mêmes abonnements de sécurité et Panorama comme licence de modèle fixe. Vous utiliserez le code d'autorisation de ce profil.

STEP 5 | Sélectionnez le nouveau profil, cliquez sur les points de suspension verticaux et sélectionnez **Register Firewall (Enregistrer le pare-feu)**.

1. Entrez les informations de la VM et du pare-feu et sélectionnez **Submit (Envoyer)**. Cela associe le pare-feu au profil et à son code d'autorisation et attribue un numéro de série.
2. Cliquez sur **View Devices (Afficher les périphériques)** pour afficher les périphériques associés dans **Software NGFW Devices (Périphériques NGFW logiciels)**.
3. Dans la colonne **License (Licence)**, téléchargez les clés de licence vers un emplacement à partir duquel vous pouvez transférer les fichiers en toute sécurité vers la machine hôte.

STEP 6 | Appliquez le nouveau code d'autorisation.

1. Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Licenses (Licences)** et cliquez sur **Activate (Activer)**.
2. Utilisez les Filters (Filtres) pour sélectionner les pare-feu gérés à mettre sous licence.
3. Entrez votre code d'autorisation à partir de votre profil de déploiement dans la colonne **Auth Code (Code d'autorisation)** pour chaque pare-feu.
4. Cliquez sur **Activate (Activer)** pour confirmer la mise à niveau de la licence. Panorama contacte le serveur de mises à jour de Palo Alto Networks et utilise les jetons requis pour vos pare-feu en fonction du modèle VM-Series, des vCPU et des services que vous avez choisis.

STEP 7 | (facultatif) Vérification de la migration.

Le pare-feu géré par Panorama et Panorama n'ont pas accès au CSP

Lorsque Panorama et un pare-feu géré ne peuvent pas accéder au CSP, procédez à la migration d'une licence sur le pare-feu géré.

STEP 1 | Si nécessaire, installez la clé API de licence sur votre pare-feu VM-Series.

STEP 2 | Utilisez la CLI pour utiliser le mode manuel afin de désactiver la licence de modèle fixe.

STEP 3 | Désactivez la VM du pare-feu. à l'aide de la procédure manuelle, et connectez-vous au CSP et utilisez le fichier de jeton pour désactiver la VM.

©2023 Palo Alto Networks, Inc.

STEP 4 | Dans le CSP, Création d'un profil de déploiement avec le même modèle VM-Series, le même nombre de vCPU et les mêmes abonnements de sécurité que l'ancienne licence de modèle fixe. Vous utiliserez le code d'autorisation de ce profil.

STEP 5 | Sélectionnez le nouveau profil, cliquez sur les points de suspension verticaux et sélectionnez **Register Firewall (Enregistrer le pare-feu)**.

1. Entrez les informations de la VM et du pare-feu et sélectionnez **Submit (Envoyer)**. Cela associe le pare-feu au profil et à son code d'autorisation et attribue un numéro de série.
2. Cliquez sur **View Devices (Afficher les périphériques)** pour afficher les périphériques associés dans **Software NGFW Devices (Périphériques NGFW logiciels)**.
3. Dans la colonne **License (Licence)**, téléchargez les clés de licence vers un emplacement à partir duquel vous pouvez transférer les fichiers en toute sécurité vers la machine hôte.

STEP 6 | Dans le pare-feu, sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.

Les clés de licence doivent être installées via l'interface Web. Le pare-feu ne prend pas en charge l'installation de clé de licence via SCP ou FTP.

STEP 7 | Cliquez sur **Manually Upload License (Charger manuellement la licence)** et saisissez les clés de licences.

STEP 8 | Vérifiez que le **Dashboard (Tableau de bord)** affiche un numéro de série valide et que la licence **PA-VM** apparaît dans l'onglet **Device (Périphérique)** > **Licenses (Licences)**.

STEP 9 | (facultatif) Vérification de la migration.

Vérification de la migration

Vérifiez que votre migration de licence a été effectuée avec succès.

STEP 1 | Sur le périphérique, vérifiez que la licence a bien été mise à jour en vérifiant la date d'expiration de la licence.

STEP 2 | Vérifiez que tous les abonnements activés dans votre profil de déploiement sont appliqués à votre périphérique.

STEP 3 | Sur le CSP, vérifiez que le nombre attendu de crédits alloués et de crédits consommés correspond à votre pool de crédits.

STEP 4 | Sur le CSP, vérifiez que les jetons associés ou la quantité de licences ont été renvoyés à votre code d'autorisation précédent.

 ©2023 Palo Alto Networks, Inc.

Modèles VM-Series

Le pare-feu VM-Series est disponible dans les modèles à vCPU fixe suivants : VM-50, VM-100, VM-200, VM-300, VM-500, VM-700 et VM-1000-HV. Ces modèles sont disponibles pour toutes les versions PAN-OS prises en charge, sauf indication contraire ci-dessous. Le module logiciel (fichier ***.xva***, ***.ova*** ou ***.vhdx***) utilisé pour déployer le pare-feu VM-Series est commun à tous les modèles.

Vous pouvez migrer votre ELA de modèle fixe ou votre licence perpétuelle vers une licence flexible et conserver le modèle fixe ou remplacer la licence par une licence vCPU flexible. Voir Mise sous licence du pare-feu VM-Series pour comparer les méthodes de mise sous licence.

- Tous les modèles peuvent être déployés en tant que machines virtuelles invitées sur VMware ESXi et vCloud Air, KVM, Microsoft Hyper-V, Cisco ACI, Cisco ENCS et Cisco CSP.
- Dans les environnements de cloud public (Amazon Web Services, Azure, Google Cloud Platform, Oracle Cloud Infrastructure, Alibaba Cloud), tous les modèles sauf VM-50 sont pris en charge.
- Pour VMware NSX, seuls les pare-feu VM-100, VM-200, VM-300, VM-500 et VM-1000-HV sont pris en charge.

Lorsque vous appliquez la licence sur le pare-feu VM-Series, le numéro de modèle et les fonctionnalités associées y sont implémentés. La capacité est définie en fonction du nombre de sessions, règles, zones de sécurité, objets d'adresse, tunnels IPSec VPN et SSL VPN que le pare-feu VM-Series peut gérer. Pour vous assurer que vous achetez le bon modèle pour vos besoins réseau, utilisez le tableau suivant pour comprendre la capacité maximale de chaque modèle et les différences de capacité par modèle :

Modèle	Sessions	Règles de sécurité	Adresses IP dynamiques	Zones de sécurité	Tunnels VPN IPSec	Tunnels VPN SSL
VM-50	50 000	• 250 • 200 en mode simplifié	1 000	15	• 250 • 25 en mode simplifié	• 250 • 25 en mode simplifié
VM-100 VM-200	250 000	1 500	2 500	40	1 000	500
VM-300 VM-1000-HV	800 000	10,000	100 000	40	2 000	2 000
VM-500	2 000 000	10,000	100 000	200	4 000	6 000
VM-700	10 000 000	20,000	100 000	200	8 000	12 000

©2023 Palo Alto Networks, Inc.

Pour plus d'informations sur les plates-formes sur lesquelles vous pouvez déployer le pare-feu VM-Series, reportez-vous à la section Déploiements VM-Series. Pour plus d'informations sur les modèles de pare-feu VM-Series, consultez l'outil de comparaison de pare-feu Palo Alto Networks. Vous pouvez également consulter des informations générales à propos du pare-feu VM-Series.

- Configuration système requise pour VM-Series
- Sursouscription du processeur
- Le mode VM-50 Lite
- Types de licences de modèle VM-Series
- Activation des licences de modèle VM-Series
- Enregistrement du pare-feu VM-Series
- Installation d'un certificat de périphérique sur le pare-feu VM-Series
- Basculer entre les licences BYOL et PAYG
- Basculer entre les licences de modèle VM-Series
- Désactivation de la ou des licence(s)
- Renouveler les paquets de permis de coupe-feu de la série VM

Configuration système requise pour VM-Series

Chaque instance du pare-feu VM-Series nécessite une allocation de ressources minimale (nombre de processeurs, mémoire et espace disque) sur son serveur hôte. Utilisez le tableau ci-dessous pour vérifier que vous allouez les ressources matérielles nécessaires à votre modèle VM-Series ou à votre profil de mémoire.

PAN-OS 10.2 ajoute des fonctionnalités et des capacités supplémentaires et nécessite donc un peu plus de mémoire. Pour fournir la même échelle de session qu'une version antérieure à PAN-OS 10.2, vous devez augmenter l'allocation de mémoire minimale. Dans le cas où vous n'augmentez pas la mémoire minimale des configurations antérieures à PAN-OS 10.2, l'échelle de session maximale est réduite.

Modèle Series	Hyperviseurs pris en charge	vCPU pris en charge	Mémoire minimum	Mémoire minimum avec GTP activé	Disque dur minimu	Nombre maximal de sessions (héritées)	Session mise à l'échelle dans PAN-OS 10.2*	Mémoire recommand pour le nombre de sessions héritées
VM-50	ESXi, Hyper-V, KVM	2	• 5,5 Go • 4,5 Go en mode Lite	• 6 Go • 5 Go en mode Lite	32 Go (60 Go au démarrage)	• 65 000 • 50 000 en mode Lite	• 50 000 • 25 000 en mode Lite	• 6 Go • 5,5 Go
VM-100	AWS, Azure, ESXi, Google Cloud Platform,	2	6,5 Go	7,5 Go	60 Go	250 000	200 000	7 Go

©2023 Palo Alto Networks, Inc.

Modèle Series	Hyperviseurs pris en charge	vCPU pris en charge	Mémoire minimum	Mémoire minimum avec GTP activé	Disque dur minimu	Nombre maximal de sessions (héritées)	Session mise à l'échelle dans PAN-OS 10.2*	Mémoire recommand pour le nombre de sessions héritées
	Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, Cisco ENCS, NSX-T (VM-100) *La VM-100 sur Azure nécessite 4 vCPU.*							
VM-300	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, Cisco ENCS, NSX-T (VM-300)	2, 4	9 Go (min) 11 Go (recommandé)	10 Go	60 Go	800 000	600 000	10 Go
VM-500	AWS, Azure, Cisco ACI, Cisco CSP, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, NSX-T	2, 4, 8	16 Go	20 Go	60 Go	2 000 000	1 800 000	18 Go
VM-700	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, NSX-T	2, 4, 8, 16	56 Go	64 Go	60 Go	10 000 000	10 000 000	56 Go

©2023 Palo Alto Networks, Inc.

* Pare-feux VM-Series de modèle fixe avec des licences financées par des crédits NGFW logiciels.

** Dans PAN-OS 10.2, 9 Go peuvent être insuffisants selon l'ensemble de fonctionnalités ou la combinaison d'ensembles de fonctionnalités (comme GTP ou les fonctionnalités hautes performances) utilisés sur le pare-feu. Si vous rencontrez des problèmes liés aux ressources mémoire, augmentez la mémoire à 11 Go pour répondre aux besoins en mémoire supplémentaires de certaines fonctionnalités ou combinaisons de fonctionnalités.

Vous pouvez activer le mode simplifié sur le VM-50. Le mode simplifié est un mode de fonctionnement alternatif pour les environnements où les ressources sont limitées. Pour plus d'informations, consultez Mode VM-50 Lite.

Pour obtenir les meilleures performances, tous les cœurs nécessaires doivent être disponibles sur un seul socket de processeur.

Pour fonctionner, le pare-feu VM-50 nécessite au moins 32 Go d'espace disque. Toutefois, étant donné que l'image de base VM-Series est commune à tous les modèles, vous devez allouer 60 Go d'espace disque jusqu'à la mise sous licence du VM-50.

Le nombre de vCPU assignés au plan de gestion et ceux assignés au dataplane diffèrent en fonction du nombre total de vCPU assignés au pare-feu VM-Series. Si vous assignés plus de vCPU que ceux officiellement pris en charge par la licence, tous les vCPU supplémentaires sont assignés au plan de gestion.

Total des vCPU	vCPU du plan de gestion	vCPU Dataplane du dataplane
2	1	1
4	2	2
8	2	6
16	4	12

Sursouscription du processeur

Le pare-feu VM-Series prend en charge la sursouscription du processeur sur tous les modèles. La sursouscription du processeur vous permet de déployer une densité plus élevée de pare-feu VM-Series sur les hyperviseurs s'exécutant sur l'architecture x86. Vous pouvez déployer deux (2:1) à cinq (5:1) pare-feu VM-Series par allocation de processeur requise. Lorsque vous planifiez votre déploiement, utilisez la formule suivante pour calculer le nombre de pare-feu VM-Series que votre matériel peut prendre en charge.

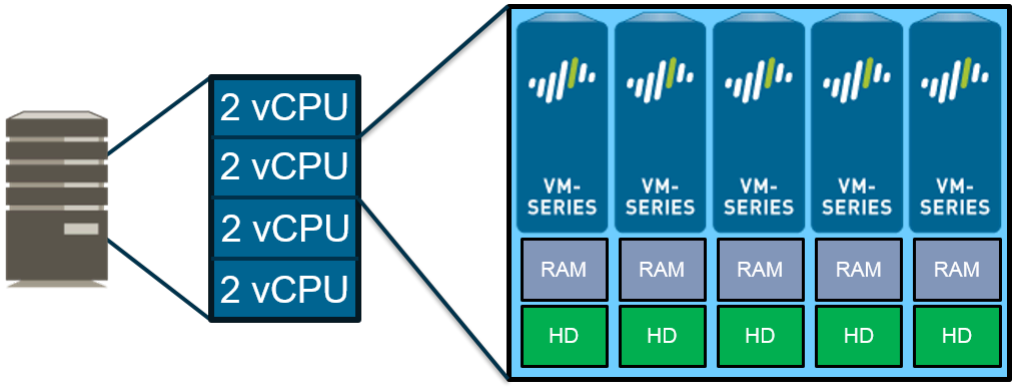
(Nombre total de processeurs x rapport de sursouscription)/processeurs par pare-feu = nombre total de pare-feu VM-Series

Par exemple, avec un rapport de 5:1, une machine hôte dotée de 16 processeurs physiques et d'au moins 180 Go de mémoire (40 × 4,5 Go) peut prendre en charge jusqu'à 40 instances sur le VM-50. Chaque VM-50 nécessite deux processeurs virtuels, et cinq VM-50 peuvent être associées à chaque paire de processeurs virtuels.

©2023 Palo Alto Networks, Inc.

(16 processeurs x 5)/2 = 40 pare-feu VM-50

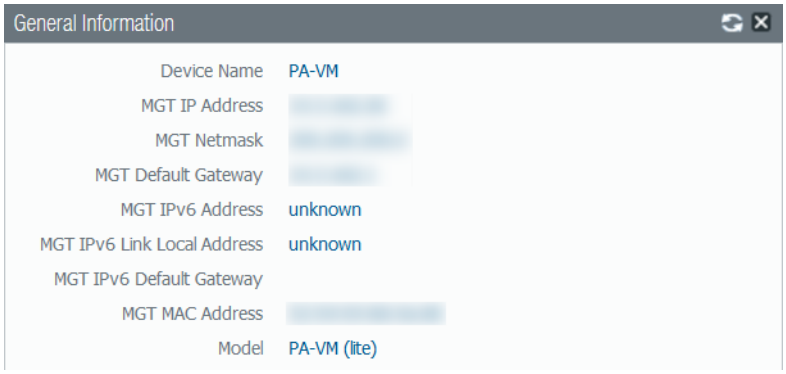
Au-delà de répondre à la Configuration système requise pour VM-Series minimum, aucune configuration supplémentaire n'est requise pour profiter de la sursouscription. Déployez les pare-feu VM-Series normalement et le dépassement d'abonnement des ressources se produit automatiquement. Lors de la planification de votre déploiement, tenez compte des autres fonctions, telles que les commutateurs virtuels et les machines invitées sur l'hôte qui requièrent leurs propres ressources matérielles.



Le mode VM-50 Lite

Le standard VM-50, bien que le plus petit modèle de la série VM, nécessite plus de ressources que celles disponibles dans certains environnements. Le mode VM-50 Lite fournit une alternative pour les environnements où les ressources matérielles sont limitées. Le VM-50 Lite nécessite 4,5 Go de mémoire au lieu des 5,5 Go requis par le VM-50 standard. Le VM-50 Lite utilise la même licence que le VM-50 standard, mais est en mode Lite lorsque qu'il reçoit 4,5 Go de mémoire vive (RAM).

- *Dans les déploiements de haute disponibilité, les deux pare-feu VM-série doivent être autorisés en tant que VM-50 Lite pour éviter les problèmes de non-concordance de capacité. Dans le cas d'une non-concordance de licence de capacité, le VM-50 (non-Lite) est considéré comme ayant une capacité supérieure; le VM-50 devient non fonctionnel tandis que le VM-50 Lite demeure fonctionnel.*
- *Le VM-50 Lite ne prend pas en charge les trames Jumbo ; le VM-50 et le VM-50 Lite ne prennent pas en charge WildFire inline ML.*



 ©2023 Palo Alto Networks, Inc.

Types de licences de modèle VM-Series

Les licences et abonnements suivants sont disponibles pour le pare-feu VM-Series :

- **Licence de capacité** : il faut détenir une licence de base, que l'on nomme également une ***licence de capacité,*** pour activer le numéro de modèle (VM-50, VM-100, VM-200, VM300, VM-500, VM-700 ou VM-1000-HV) du pare-feu VM-Series ainsi que ses fonctionnalités associées. Les licences de capacité sont incluses dans un ensemble et peuvent être perpétuelles ou basées sur des conditions :
  - **Licence perpétuelle** : une licence sans date d'expiration, qui vous permet d'utiliser le pare-feu VM-Series à la capacité sous licence et pour une durée illimitée. Les licences perpétuelles sont offertes pour la licence de capacité VM-Series uniquement.
  - **Licence de durée limitée** : une licence de durée limitée vous permet d'utiliser le pare-feu VM-Series pendant une période de temps donnée. Elle comporte une date d'expiration ; vous serez donc invité à renouveler la licence avant qu'elle n'expire. Les licences de durée limitée sont offertes pour les licences de capacité, les autorisations de support et les abonnements.
- **ELA VM-Series** : pour les entreprises à croissance élevée, l'accord de licence d'entreprise VM-Series (ELA VM-Series) offre une option de licence à prix fixe qui permet le déploiement illimité de pare-feu VM-Series avec BYOL. Le ELA est offert dans le cadre d'ententes d'une durée d'un an et de trois ans, sans véritable conclusion à la fin du mandat.

  Il existe deux types d'ELA VM-Series :

  - Si vous avez acheté l'ELA VM-Series avant le 4 décembre 2018, vous disposez de l'ELA VM-Series hérité, qui vous permet de choisir un modèle VM-Series unique dans n'importe quel environnement cloud public ou hyperviseur pris en charge. Avec cet ELA, vous recevez un seul code d'autorisation de licence pour la capacité, le support et les abonnements GlobalProtect, PAN-DB URL Filtering, Threat Prevention, WildFire pour chaque instance de pare-feu VM-Series. Vous bénéficiez également de déploiements illimités de l'appareil virtuel Panorama inclus avec une licence de gestion d'appareils pour 1 000 pare-feu sur chacun d'eux.

    Palo Alto Networks a commencé à éliminer progressivement l'ELA VM-Series hérité le 16 avril 2019. Les clients disposant de licences Entreprise existants seront informés par leur représentant du support technique lors de la migration de leur compte vers l'ELA multimodèle. Les jetons de licence seront distribués conformément à votre contrat d'abonnement au pare-feu VM-Series. Aucune action supplémentaire n'est nécessaire pour la poursuite du fonctionnement de vos pare-feu. Si vous souhaitez procéder à la Gestion des jetons de licence ELA VM-Series, vous devez désigner un administrateur ELA. Seul un rôle de super utilisateur sur le Portail assistance clientèle (CSP) de Palo Alto Networks peut affecter un administrateur ELA.
  - L'Accord de licence d'entreprise VM-Series (ELA multimodèle) que vous avez acheté après le 4 décembre 2018 (en tant que nouvel achat ou en tant que rachat de l'ELA VM-Series hérité) est appelé l'ELA VM-Series multimodèle, qui inclut la plupart des modèles du portefeuille de pare-feu VM-Series avec les abonnements GlobalProtect, PAN-DB URL Filtering, Threat Prevention, WildFire et des autorisations de support. Vous bénéficiez également de déploiements illimités de l'appareil virtuel Panorama avec une licence de gestion d'appareils pour 1 000 pare-feu sur chacun d'eux.

©2023 Palo Alto Networks, Inc.

Licences de pare-feu VM-Series pour les clouds publics

La stratégie de licence de pare-feu VM-Series est la même pour AWS, Azure et Google Cloud Platform. Il existe différents types de licences (voir Types de licence - Pare-feu VM-Series), ainsi que les méthodes de licence Bring Your Own License (Apportez votre propre licence) et Pay-as-you-go (Paiement au fur et à mesure) :

- **Bring Your Own License (BYOL)** : une licence achetée auprès d'un partenaire, d'un revendeur ou directement auprès de Palo Alto Networks. Apportez votre propre licence prend en charge les licences de capacité individuelles, les licences de support et les offres groupées d'abonnements.
  - Pour les licences BYOL individuelles, vous devez appliquer le code d'autorisation après avoir déployé le pare-feu VM-Series.
  - Un ensemble de licences BYOL possède un seul code d'autorisation que vous pouvez inclure dans le module d'amorçage (reportez-vous à la section Amorçage du pare-feu VM-Series). Tous les abonnements inclus dans l'ensemble sont sous licence lorsque le pare-feu est lancé.

  Une licence BYOL pour le pare-feu VM-Series sur OCI GovCloud nécessite PAN-OS 10.1.2 ou une version ultérieure pour les modes FIPS et non FIPS.

- **Pay-as-you-go (PAYG) (Paiement au fur et à mesure)** : également appelé ***licence basée sur l'utilisation*** ou ***pay-per-use***. Les licences PAYG peuvent être achetées auprès de votre fournisseur Cloud :
  - AWS : Achetez à partir de l'AWS Marketplace. Prend en charge les options PAYG à l'heure et annuelle.
  - Azure : Achetez à partir de l'Azure Marketplace. Prend en charge l'option PAYG à l'horaire.
  - Google Cloud Platform : Achetez à partir de Google Cloud Platform Marketplace. Google Cloud Platform prend en charge l'option PAYG par minute.
  - Infrastructure Cloud Oracle : (PAN-OS 10.0.3 ou version ultérieure) Achetez à partir de l'Oracle Cloud Marketplace.

  La licence PAYG de VM-Series sur OCI ne prend pas en charge la VM-100.

  Avec les licences basées sur l'utilisation, le pare-feu est pré-licencié et prêt à l'emploi dès que vous le déployez ; vous ne recevez pas de code d'autorisation. Lorsque vous arrêtez ou arrêtez le pare-feu de votre console Cloud, les licences PAYG sont suspendues ou terminées.

  Une licence PAYG applique une licence de capacité VM-Series en fonction du matériel alloué à l'instance. L'instance PAYG vérifie le nombre de ressources matérielles disponibles pour l'instance et applique la plus grande licence de capacité de pare-feu VM-Series autorisée pour les ressources disponibles. Par exemple, si l'instance possède 2 vCPU et 16 Go de mémoire, une licence VM-100 est appliquée en fonction du nombre de vCPU. Si l'instance possède 16 vCPU et 16 Go de mémoire, une licence VM-500 est toutefois appliquée en fonction de la mémoire.

©2023 Palo Alto Networks, Inc.

Pour en savoir plus sur les exigences en matière de ressources des modèles VM-Series, voir Configuration système requise pour VM-Series.

La rétrogradation de PAN-OS n'est pas prise en charge sur une instance de pare-feu PAYG qui était initialement déployée en exécutant PAN-OS 9.1.2. Les instances de pare-feu déployées avant la version 9.1.2 de PAN-OS peuvent être rétrogradées vers d'anciennes versions de PAN-OS.

Les licences PAYG sont regroupées comme suit :

Caractéristiques de la licence	Forfait 1	Forfait 2	Forfait 3
Licence de capacité de pare-feu VM-Series	VM-100, VM-300, VM-500, VM-700	VM-100, VM-300, VM-500, VM-700	VM-100, VM-300, VM-500, VM-700
Assistance premium	✓	✓	✓
Prévention des menaces (AV, IPS et prévention contre les logiciels malveillants)	✓	✓	
GlobalProtect		✓	✓
Filtrage des données PAN-DB		✓	
WildFire		✓	✓
Sécurité DNS		✓	✓
URL Filtering avancé			✓
Advanced Threat Prevention (Prévention avancée des menaces)			✓

Lorsque vous utilisez la CLI du pare-feu VM-Series pour afficher votre licence PAYG appliquée, la commande ***show system info*** *affiche une valeur différente de celle de la sortie affichée pour la commande* ***request license info****. Pour les versions PAN-OS 9.1.1 et antérieures, la commande* ***request license info*** *affiche toujours le modèle en tant que VM-300, quel que soit le modèle VM-Series qui a été appliqué.*

Vous ne pouvez pas passer d'une licence PAYG à une BYOL. Pour passer de PAYG à BYOL, contactez votre revendeur ou représentant commercial Palo Alto Networks pour acheter une licence BYOL et obtenir un code d'autorisation BYOL que vous pouvez utiliser pour attribuer une licence à votre pare-feu. Si vous avez déployé votre pare-feu et que vous souhaitez changer de licence, reportez-vous à la section Basculer entre les licences BYOL et PAYG.

©2023 Palo Alto Networks, Inc.

Si vous possédez une copie d'évaluation du pare-feu VM-Series et que vous souhaitez la convertir en copie sous licence (achetée) pour le même type de licence (BYOL à BYOL), vous pouvez désactiver la licence d'évaluation et activer la licence achetée à la place. Reportez-vous à la section Mise à niveau du pare-feu VM-Series *pour des instructions.*

Accord de licence d'entreprise VM-Series (ELA multimodèle)

L'accord de licence d'entreprise VM-Series(ELA VM-Series) est un accord de licence complet d'un ou trois ans vous permettant d'acheter des pare-feu VM-Series, ainsi que des abonnements GlobalProtect, PAN-DB URL Filtering, Threat Prevention, WildFire et DNS Security. Il comprend également une autorisation de support et une licence de gestion d'appareils pour Panorama. L'ELA VM-Series multimodèle fournit une gestion simplifiée des licences avec un contrat unique qui vous permet de déployer n'importe quel modèle de pare-feu VM-Series qui répond aux besoins de sécurité de votre entreprise.

Lorsque vous achetez l'ELA VM-Series multimodèle, vous devez prévoir le nombre de pare-feu dont vous aurez besoin sur la durée de votre abonnement. En fonction de vos prévisions et d'une allocation supplémentaire adaptée à votre croissance future, votre compte sur le Portail assistance clientèle (CSP) est crédité d'un pool de jetons de licence qui vous permet de déployer n'importe quel modèle de pare-feu VM-Series. En fonction du modèle de pare-feu et du nombre de pare-feu que vous déployez, un nombre spécifique de jetons est déduit de votre pool de jetons de licence disponible. Les jetons déduits de votre compte sont calculés en fonction de la valeur de chaque modèle de pare-feu :

- VM-50—10 jetons
- VM-100—25 jetons
- VM-300—50 jetons
- VM-500—140 jetons
- VM-700—300 jetons

Avec l'ELA VM-Series, il n'y a aucun ajustement dû à la fin du délai, ce qui signifie que vous ne serez pas facturé de manière rétroactive, même si vous déployez plus de pare-feu que vos prévisions initiales. Ainsi, afin d'équilibrer flexibilité et responsabilité, les conditions d'utilisation de l'ELA de VM-Series incluent une période limitée et illimitée qui explique comment vous pouvez utiliser des jetons et déployer des pare-feu selon les besoins. Pour plus de détails, reportez-vous à la section Conditions générales des ELA. Les pare-feu VM-Series que vous déployez avec l'ELA VM-Series ne possèdent pas de licence perpétuelle. À l'expiration de ce délai, vous devez renouveler l'accord pour prolonger l'autorisation de support et obtenir un accès continu aux mises à jour logicielles et de contenu sur les pare-feu.

Avec le rôle d'administrateur ELA sur le CSP, vous pouvez transférer ou scinder les jetons de licence entre d'autres administrateurs appartenant à différents services et disposant de leur propre compte CSP. Ce partage permet aux autres administrateurs de votre entreprise de déployer le pare-feu VM-Series à la demande, à condition qu'ils disposent de jetons disponibles sur leurs comptes CSP respectifs. Reportez-vous à la section Gestion des jetons de licence ELA VM-Series pour inviter d'autres administrateurs à partager des jetons ELA et à déployer tout modèle de pare-feu VM-Series répondant aux besoins de sécurité de votre entreprise. Vous pouvez également réclamer des jetons pour supprimer des comptes CSP à partir de l'ELA VM-Series si vous souhaitez redistribuer les jetons en fonction de l'évolution des besoins de l'organisation.

©2023 Palo Alto Networks, Inc.

Regarder les vidéos ELA multi-modèles VM-Series

- Gestion des jetons de licence ELA VM-Series
- Acceptation de l'ELA VM-Series

Gestion des jetons de licence ELA VM-Series

La section Accord de licence d'entreprise VM-Series (ELA multimodèle) (ELA VM-Series) vous offre la possibilité d'avoir un contrat unique que vous pouvez partager avec d'autres administrateurs de votre entreprise. Vous devez disposer du rôle super utilisateur sur le Portail assistance clientèle (CSP) de Palo Alto Networks pour activer l'ELA. Après l'activation du code d'autorisation ELA, vous héritez du rôle d'administrateur ELA sur le CSP.

Avec le rôle d'administrateur ELA, vous pouvez gérer le pool de jetons de licence disponible pour déployer les pare-feu et les abonnements VM-Series inclus dans l'accord. Vous pouvez inviter d'autres administrateurs à partager les jetons ELA VM-Series, attribuer les modèles et le nombre d'instances de pare-feu VM-Series disponibles pour chaque administrateur, ainsi que supprimer des comptes CSP de votre ELA VM-Series. Selon ce que vous allouez à chaque bénéficiaire, ils reçoivent un nombre spécifique de jetons qu'ils peuvent ensuite utiliser pour déployer des pare-feu VM-Series.

Les achats et les octrois supplémentaires n'augmentent pas directement le nombre de pare-feu VM-Series disponibles dans un compte CSP ; à la place, les jetons de licence ELA sont ajoutés au pool de jetons ELA VM-Series. Les jetons de licence ELA peuvent ensuite être attribués par l'administrateur ELA à un compte CSP donné pour augmenter le nombre de pare-feu VM-Series disponibles.

STEP 1 | (Clients ELA VM-Series hérités uniquement) Désignez un administrateur ELA pour gérer les jetons.

Les clients de licences d'entreprise existants qui ont migré vers l'ELA multimodèle doivent désigner un administrateur ELA pour gérer les jetons de licence ELA VM-Series. Lors de la conversion, aucune autre action n'est nécessaire pour la poursuite du fonctionnement de vos pare-feu. Toutefois, vous ne pourrez pas (ré)attribuer des jetons pour le déploiement de pare-feu tant qu'un administrateur ELA n'aura pas été affecté. Seul un administrateur ayant un rôle de super utilisateur sur le CSP peut désigner un administrateur ELA qui, à son tour, peut gérer des jetons ou octroyer des jetons à d'autres administrateurs.

1. Connectez-vous au CSP de Palo Alto Networks.
2. Sélectionnez **Members (Membres)** > **Manage Users (Gérer les utilisateurs)**.
3. Cliquez sur l'icône en forme de crayon dans la colonne **Actions** pour modifier l'utilisateur auquel vous souhaitez attribuer le rôle d'administrateur ELA.
4. Sélectionnez **ELA Administrator** (Administrateur ELA), puis cliquez sur la coche pour ajouter le nouveau rôle à l'utilisateur sélectionné.
5. Passez à l'étape 3.

©2023 Palo Alto Networks, Inc.

STEP 2 | Activez le code d'autorisation ELA.

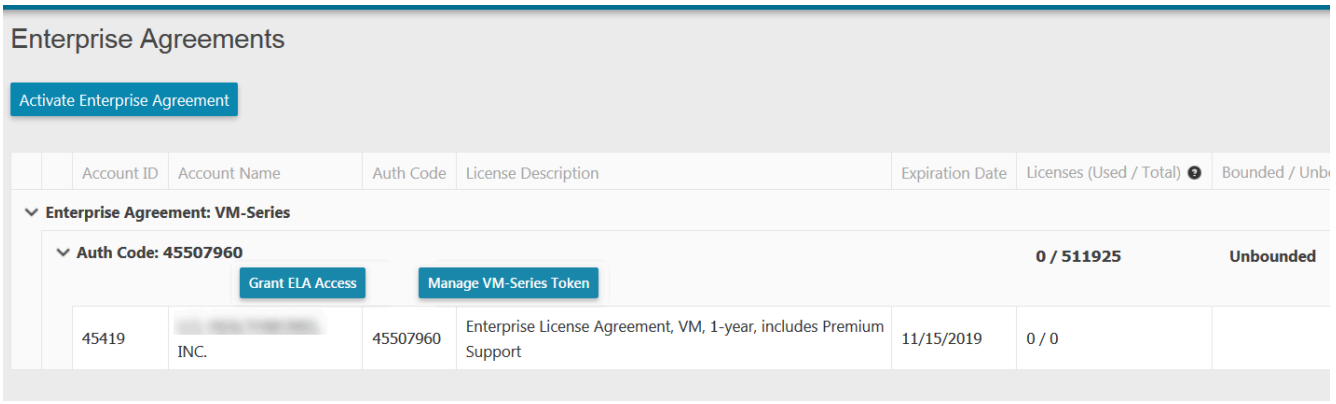
L'utilisateur administrateur qui active l'ELA hérite du rôles de super utilisateur et d'administrateur ELA sur le CSP et peut gérer les jetons ou octroyer les jetons à d'autres administrateurs.

1. Connectez-vous au CSP de Palo Alto Networks.
2. Sélectionnez **Assets (Actifs)** > **Enterprise Agreements (Accords d'entreprise)** > **Activate Enterprise Agreement (Activer un accord d'entreprise)**.
3. Saisissez le **Authorization code** (Code d'autorisation) puis cliquez sur **Agree and Submit** (Accepter et envoyer) pour accepter et envoyer le CLUF.

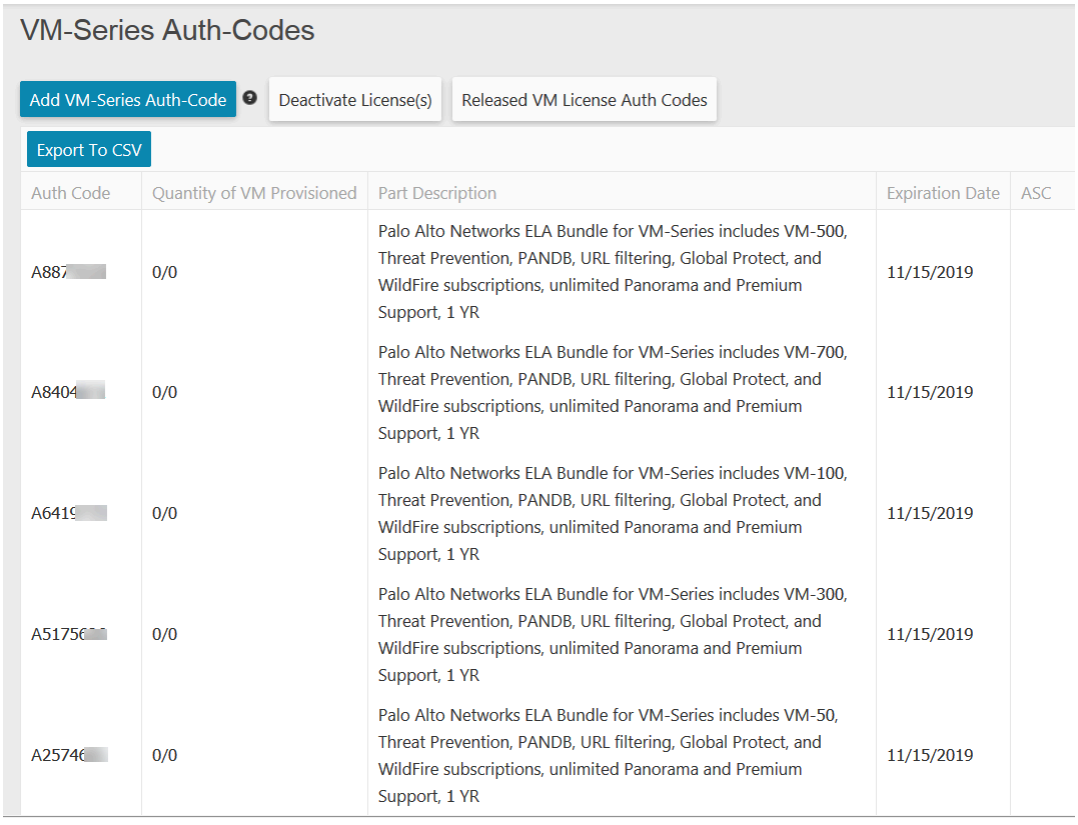
   Vérifiez que le code d'autorisation est enregistré sur votre compte sous Enterprise Agreements: VM-Series (Accords d'entreprise : VM-Series). La page affiche l'Auth Code (Code d'autorisation), l'Account ID (ID de compte), l'Account Name (Nom de compte), la License Description (Description de la licence), l'Expiration Date (Date d'expiration), le nombre de Licenses (Used/Total) (Licences [utilisées/totales]) dont vous disposez et le

©2023 Palo Alto Networks, Inc.

nombre de licences que vous pouvez déployez au cours de la période limitée et illimitée de l'accord.



4. Sélectionnez **Assets (Actifs)** > **VM-Series Auth-Codes (Codes d'autorisation VM-Series)** pour afficher les codes d'autorisation permettant de déployer chaque modèle de pare-feu VM-Series et les abonnements associés inclus avec l'ELA.

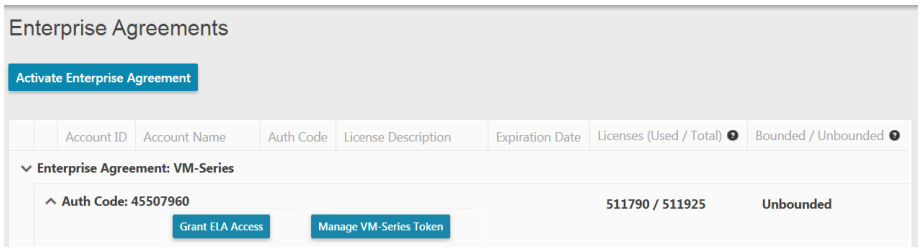


STEP 3 | Octroyez l'accès ELA à d'autres administrateurs de votre entreprise.

Cette fonctionnalité vous permet de partager l'ELA VM-Series avec d'autres administrateurs de votre entreprise ou de votre service afin qu'ils puissent déployer des pare-feu VM-Series à la

©2023 Palo Alto Networks, Inc.

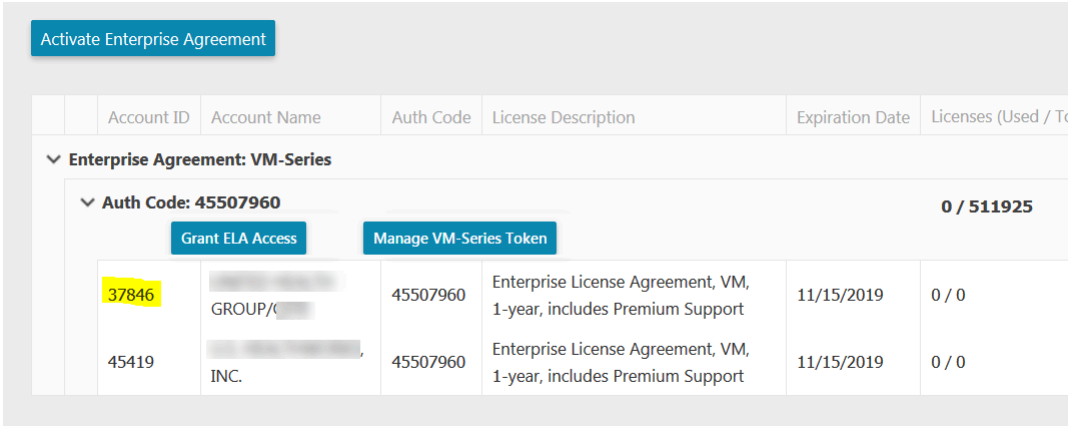
demande. En tant qu'administrateur ELA, vous pouvez octroyer l'accès à d'autres utilisateurs qui sont enregistrés avec une adresse électronique sur le CSP.



1. Sur **Assets (Actifs)** > **Enterprise Agreements (Accords d'entreprise)**, sélectionnez **Grant ELA Access (Octroyer un accès ELA)**.
2. Saisissez la **Destination Email** address (Adresse électronique de destination) de l'administrateur que vous souhaitez inviter.

   L'adresse électronique de destination que vous avez indiquée ci-dessus doit être un utilisateur enregistré sur le CSP avec un rôle de super utilisateur afin de pouvoir se connecter et accepter l'octroi. Si l'adresse électronique n'est pas enregistrée sur le CSP, vous devez d'abord créer un nouveau compte pour l'utilisateur sur **Members (Membres)** > **Create New User (Créer un nouvel utilisateur)**.
3. Sélectionnez **Notify User** (Notifier l'utilisateur) pour déclencher un e-mail de notification envoyé à l'adresse électronique que vous avez entrée.

   Le destinataire doit se connecter au CSP pour procéder à l'Acceptation de l'ELA VM-Series. Une fois que le destinataire a accepté l'octroi, l'Account ID (ID du compte) est disponible dans **Assets (Actifs)** > **Enterprise Agreements (Accords d'entreprise)** comme indiqué dans la capture d'écran suivante.



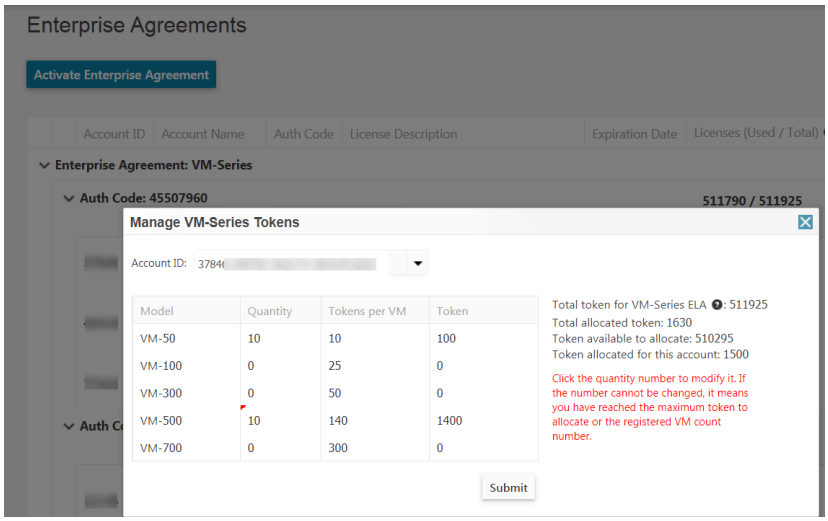
STEP 4 | Attribuez des jetons pour le déploiement des pare-feu.

1. Sélectionnez **Assets (Actifs)** > **Enterprise Agreements (Accords d'entreprise)** > **Manage VM-Series Tokens (Gérer les jetons VM-Series)**.

   Pour chaque ID de compte, vous pouvez spécifier le nombre de pare-feu que vous souhaitez attribuer par modèle. Sur la base du nombre et du modèle de pare-feu, le

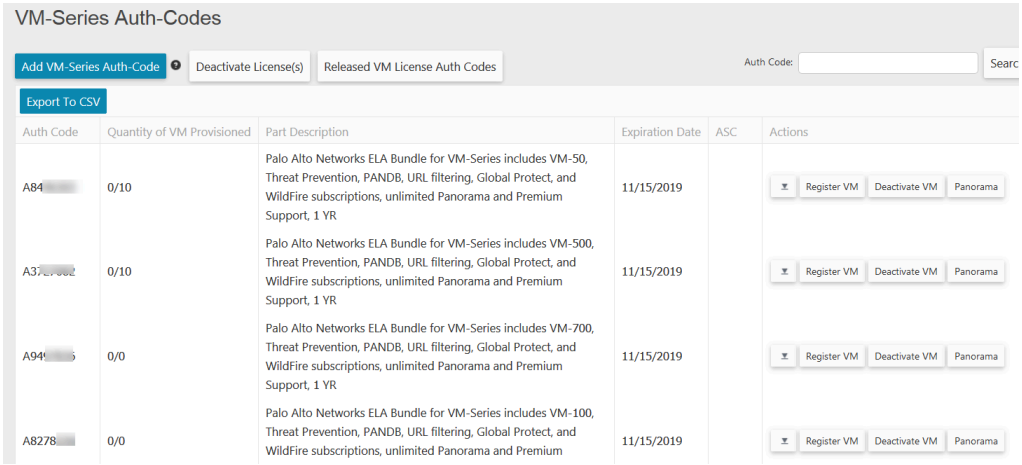
©2023 Palo Alto Networks, Inc.

nombre de jetons est automatiquement calculé et disponible pour utilisation. Dans cet exemple, vous autorisez 10 instances de VM-50 et de VM-500 chacun.



2. Vérifiez que le nombre exact d'instances de pare-feu est déposé sur le compte.

   Sélectionnez **Assets (Actifs)** > **VM-Series Auth-Code (Code d'autorisation VM-Series)** pour confirmer les codes d'autorisation que vous avez attribués. Dans cet exemple, le compte peut configurer 10 instances de VM-50 et de VM-500 chacun. Lorsque les destinataires déploient des pare-feu, le nombre de jetons est déduit du pool disponible total. Vous pouvez afficher le nombre d'instances de pare-feu qu'ils ont configurées sous forme de ratio par rapport à la quantité totale que vous leur avez attribuée. Au fur et à mesure de l'évolution de vos besoins en matière de sécurité, vous avez la possibilité d'attribuer davantage de ressources et de permettre l'accès à un autre modèle de pare-feu VM-Series, tant que des jetons sont disponibles.



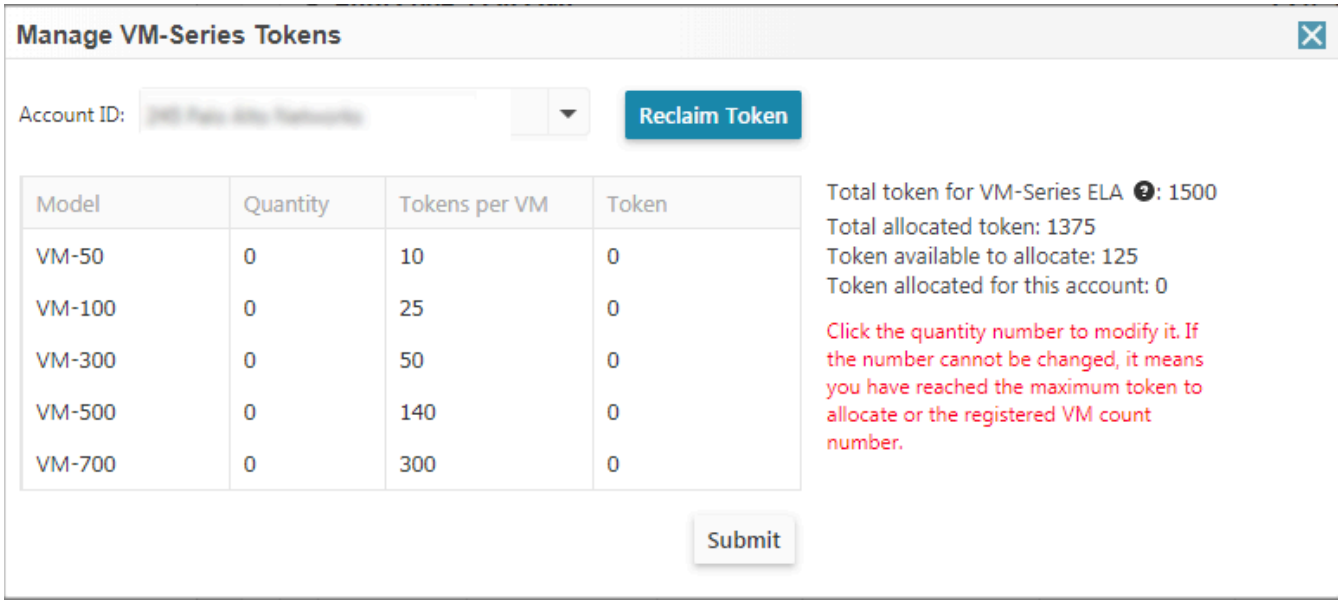
 ©2023 Palo Alto Networks, Inc.

STEP 5 | Supprimez un compte CSP de l'ELA VM-Series pour réclamer des jetons.

Vous ne pouvez pas réclamer une partie des jetons attribués à un compte CSP. En réclamant des jetons, vous supprimez l'intégralité du compte CSP de l'ELA de VM-Series et réattribuez tous les jetons associés au pool de jetons.

1. Vérifiez que tous les jetons associés au compte CSP que vous souhaitez supprimer ne sont pas utilisés par les pare-feu VM-Series. Désactivez les pare-feu VM-Series si nécessaire pour fournir des jetons à supprimer.
2. Sélectionnez **Assets (Actifs)** > **Enterprise Agreements (Accords d'entreprise) > Manage VM-Series Token (Gérer le jeton VM-Series)**.

   Sélectionnez l'Account ID (ID du compte) duquel vous souhaitez réclamer les jetons et cliquez sur **Reclaim Token** (Réclamer le jeton). Si des jetons peuvent être réclamés, vous recevrez une confirmation de la suppression réussie.



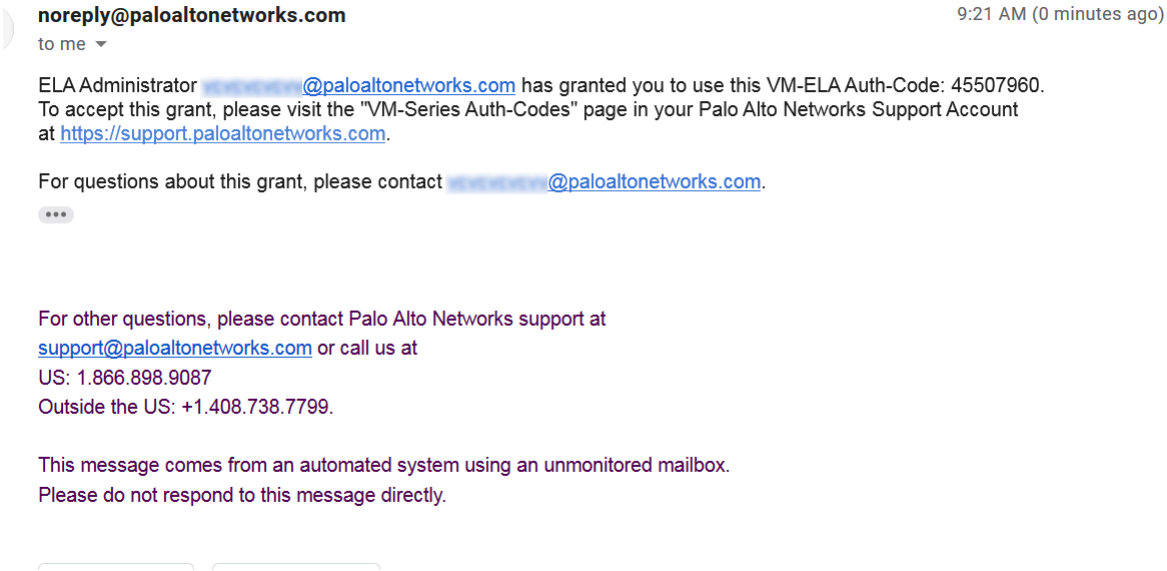
Acceptation de l'ELA VM-Series

Si votre entreprise a acheté un ELA VM-Series, votre administrateur ELA peut vous inviter à partager le contrat et le pool de jetons de licence afin que vous ayez accès aux codes d'autorisation de pare-feu VM-Series qui vous permettent de déployer des pare-feu VM-Series à la demande. Lorsque vous recevez un octroi d'accès à l'ELA VM-Series, vous recevez une notification par e-mail incluant un lien permettant de vous connecter au Portail assistance clientèle (CSP) de Palo Alto Networks et vous devez accepter les conditions d'utilisation. Une fois que vous avez accepté les conditions d'utilisation de l'ELA, l'administrateur ELA peut attribuer les modèles de pare-feu VM-Series et le nombre que vous êtes autorisé à utiliser : le nombre correspondant de jetons ELA VM-Series est déposé sur votre compte.

©2023 Palo Alto Networks, Inc.

STEP 1 | Vérifiez votre boîte de messagerie pour la notification d'octroi.

La notification comprend l'adresse électronique de l'administrateur ELA qui vous a invité à partager l'ELA VM-Series.



STEP 2 | Acceptez l'octroi.

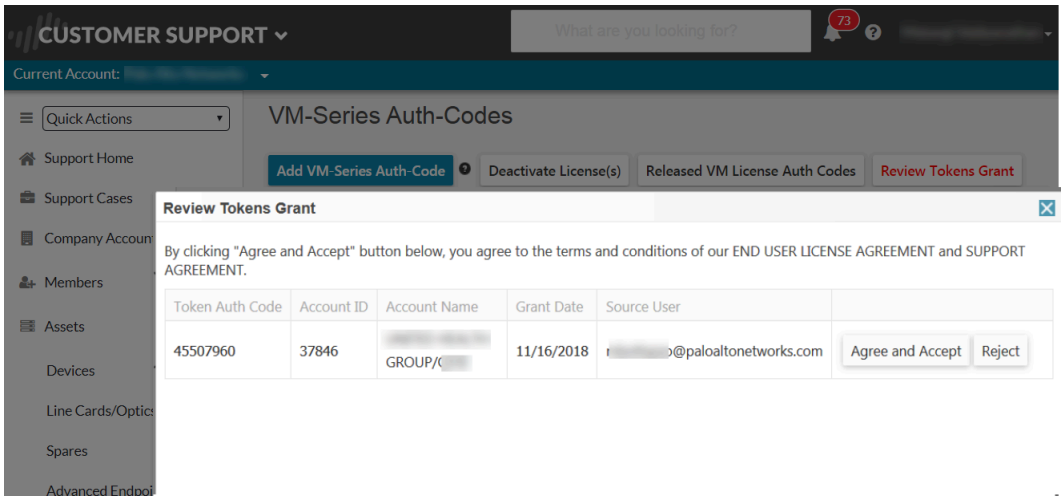
Vous devez examiner les conditions et accepter le CLUF et le contrat de support avant que l'administrateur ELA puisse allouer des jetons vous permettant de déployer des pare-feu VM-Series.

1. Connectez-vous au CSP de Palo Alto.
2. Sélectionnez **VM-Series Auth Codes** (Codes d'autorisation VM-Series) pour **Review Tokens Grant** (Examiner l'octroi de jetons).

   Vous devez accepter le CLUF et l'accord de support pour accepter l'octroi. Si vous le refusez, l'administrateur ELA qui vous a donné l'octroi reçoit une notification par e-mail l'informant de votre refus. Assurez-vous d'informer l'administrateur ELA que vous avez

©2023 Palo Alto Networks, Inc.

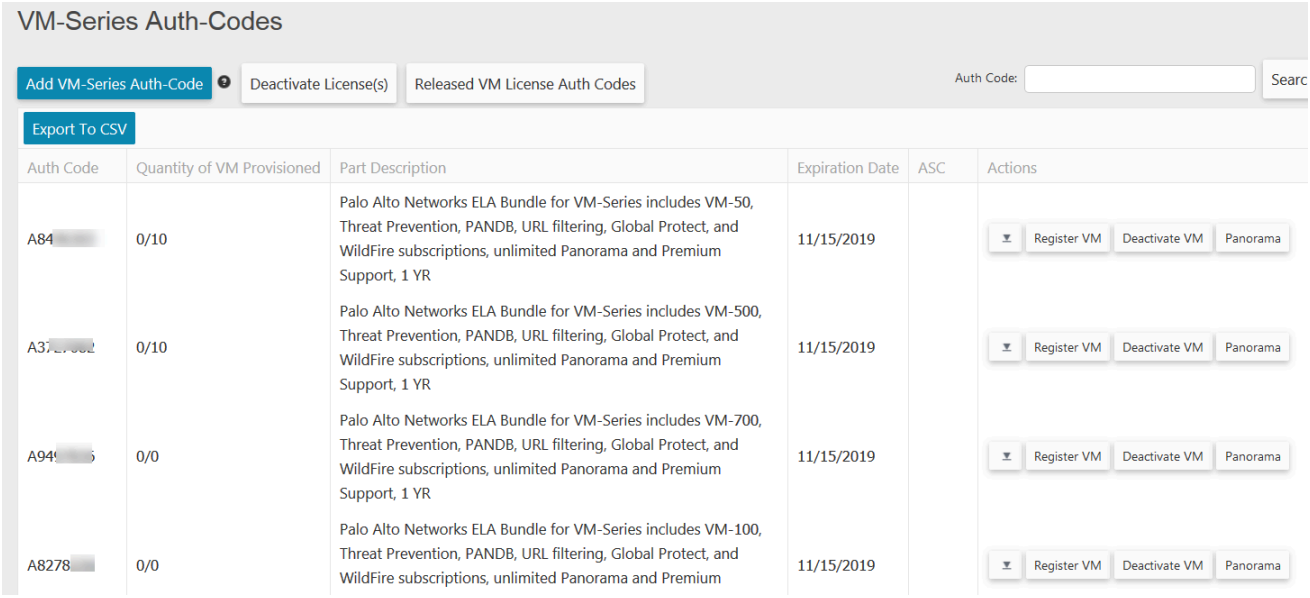
accepté l'octroi afin qu'il puisse attribuer les modèles de pare-feu VM-Series et la quantité que vous pouvez déployer.



Si vous appartenez à plusieurs comptes sur le CSP et acceptez accidentellement l'octroi sur le mauvais compte, vous devez demander à l'administrateur ELA de vous renvoyer l'octroi. Ne commencez pas à utiliser le code d'autorisation pour configurer des pare-feu avant d'accepter l'octroi dans le compte approprié.

STEP 3 | Vérifiez les modèles VM-Series et le nombre qui vous sont alloués.

Une fois que l'administrateur ELA a attribué les modèles de pare-feu VM-Series et le nombre d'instances que vous pouvez configurer, vous pouvez sélectionner **Assets (Actifs)** > **VM-Series Auth Codes (Codes d'autorisation VM-Series)** pour voir les modèles et le nombre de chaque modèle qui vous sont attribués. Par exemple, l'octroi dans la capture d'écran suivante affiche les codes d'autorisation qui vous permettent de déployer 10 instances de VM-50 et de VM-500 chacun.



Lorsque vous déployez des pare-feu et les enregistrez sur le CSP, le nombre de pare-feu configurés est augmenté. La **Quantity of VM Provisioned** (Nombre de machines virtuelles

 ©2023 Palo Alto Networks, Inc.

configurées) affiche le rapport entre le nombre de machines virtuelles configurées et le nombre total disponible pour chaque modèle.

Activation des licences de modèle VM-Series

Pour activer la licence sur votre pare-feu VM-Series, vous devez d'abord le déployer, puis effectuer la configuration initiale. Pour déployer le pare-feu, reportez-vous à la section Déploiements VM-Series.

Suivez les instructions de cette section pour tous les modèles BYOL, y compris AWS, Azure et Google Public Cloud. Pour les licences basées sur l'utilisation dans les clouds publics, vous n'avez pas besoin d'activer la licence. Vous devez enregistrer le modèle basé sur l'utilisation du pare-feu VM-Series pour les clouds publics (sans de code d'autorisation) afin d'activer votre autorisation de support premium.

Pour les modèles basés sur l'utilisation du pare-feu VM-Series dans AWS Marketplace, les instances avec des ID d'instance AWS courts et longs sont prises en charge.

Tant que vous n'activez pas la licence sur le pare-feu' VM-Series, celui-ci ne dispose d'aucun numéro de série, les adresses' MAC des interfaces du dataplane ne sont pas uniques et seul un nombre minimum de sessions est pris en charge. Comme les adresses' MAC ne sont pas uniques tant que le pare-peu n'est pas mis sous licence, pour éviter les problèmes causés par le chevauchement des adresses' MAC, assurez-vous de ne pas disposer de plusieurs pare-feu VM-Series qui ne sont pas sans licence.

Lors de l'activation de la licence, le serveur de licence utilise l'UUID et l'ID de processeur de la machine virtuelle pour générer un numéro de série unique pour le pare-feu' VM-Series. Le code d'autorisation de capacité relatif au numéro de série est utilisé pour valider votre éligibilité.

*L'onglet **License (Licence)** du pare-feu VM-Series affiche un fichier de licence VM-300 standard pour tous les modèles de licences. Pour trouver les informations sur votre modèle de licence spécifique, affichez les informations système dans l'interface utilisateur ou utilisez la CLI pour affiche les **`informations système`**.*

Si vous devez supprimer ou redéployer un pare-feu VM-Series que vous avez mis sous licence, n'oubliez pas de procéder à la Désactivation des licences sur le pare-feu. La désactivation de la licence vous permet de transférer les licences actives vers une nouvelle instance du pare-feu VM-Series sans obtenir d'aide du support technique.

- Activation de la licence pour le pare-feu VM-Series (version autonome)
- Activation de la licence pour le pare-feu VM-Series pour VMware NSX
- Résoudre les problèmes d'activation de licence

Activation de la licence pour le pare-feu VM-Series (version autonome)

Si vous n'avez pas choisi d'utiliser le flux d'amorçage à l'aide d'un forfait d'abonnement, vous devez déployer le pare-feu VM-Series et terminer la configuration initiale avant de pouvoir activer la licence sur votre pare-feu VM-Series.

- Accès Internet direct
- Aucun accès à Internet

 ©2023 Palo Alto Networks, Inc.

- Accès Internet direct

  Pour activer la licence, le pare-feu doit être configuré avec une adresse IP, un masque réseau, une passerelle par défaut et une adresse IP de serveur DNS.

  Le pare-feu doit avoir une configuration DNS valide et disposer d'une connectivité réseau pour accéder au serveur de licences Palo Alto Networks.

  1. Sélectionnez **Device (Périphérique)** > **Licenses** et sélectionnez le lien **Retrieve license keys from license server (Récupérer les clés de licence du serveur de licences)**.
  2. Le pare-feu se connecte alors au serveur de mise à jour (updates.paloaltonetworks.com), télécharge la licence et redémarre automatiquement.
  3. Reconnectez-vous à l'interface Web et vérifiez que le **Dashboard (Tableau de bord)** affiche un numéro de série valide. Si le terme **Unknown (Inconnu)** s'affiche, cela signifie que le périphérique n'est pas sous licence.
  4. Dans **Device (Périphérique)** > **Licenses (Licences)**, vérifiez que la licence **PA-VM** a été ajoutée au périphérique.

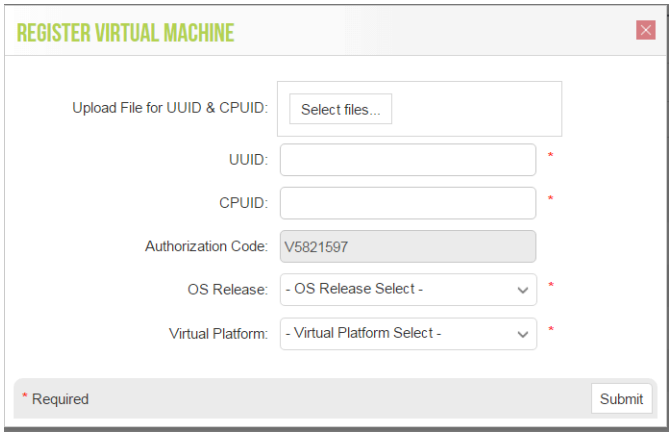
     Si vous voyez un message d'erreur, consultez la section Résoudre les problèmes d'activation de licence.

- Aucun accès à Internet

  1. Sélectionnez **Device (Appareil)** > **Licenses (Licences)**, puis cliquez sur le lien **Activate Feature using Auth Code (Activer la fonctionnalité à l'aide du code d'autorisation)**.
  2. Cliquez sur **Download Authorization File (Télécharger le fichier d'autorisation)**, puis téléchargez le fichier **authorizationfile.txt** sur la machine cliente.
  3. Copiez le fichier **authorizationfile.txt** sur un ordinateur qui a accès à Internet, puis connectez-vous au portail de support. Cliquez sur le lien **My VM-Series Auth-Codes (Mes codes d'autorisation VM-Series)**, puis sélectionnez le code d'autorisation applicable dans la liste et cliquez sur le lien **Register VM (Enregistrer la machine virtuelle)**.
  4. Dans l'onglet **Register Virtual Machine (Enregistrer la machine virtuelle)**, chargez le fichier d'autorisation. Sélectionnez la version de PAN-OS et l'hyperviseur sur lequel vous avez

 ©2023 Palo Alto Networks, Inc.

déployé le pare-feu pour terminer le processus d'enregistrement. Le numéro de série de votre pare-feu VM-Series est associé à vos enregistrements de compte.



5. Sélectionnez **Assets (Actifs)** > **My Devices (Mes appareils)**, puis recherchez l'appareil VM-Series récemment enregistré et cliquez sur le lien **PA-VM**. La clé de licence' VM-Series est alors téléchargée sur la machine cliente.
6. Copiez la clé de licence sur la machine qui peut accéder à l'interface Web du pare-feu VM-Series, puis sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.

   Les clés de licence doivent être installées via l'interface Web. Le pare-feu ne prend pas en charge l'installation de clé de licence via SCP ou FTP.
7. Cliquez sur le lien **Manually Upload License (Charger manuellement la licence)** et saisissez la clé de licence. Lorsque la licence de capacité est activée sur le pare-feu, un redémarrage se produit.
8. Connectez-vous au périphérique et vérifiez que le **Dashboard (Tableau de bord)** affiche un numéro de licence valide et que la licence **PA-VM** apparaît dans l'onglet **Device (Périphérique)** > **Licenses (Licences)**.

Activation de la licence pour le pare-feu VM-Series pour VMware NSX

Panorama sert de point de gestion central des pare-feu VM-Series pour VMware NSX et le processus d'activation de la licence est automatisé lorsque Panorama possède un accès direct à Internet. Panorama se connecte au serveur de mise à jour Palo Alto Networks pour récupérer les licences, et lorsqu'un nouveau pare-feu VM-Series pour NSX est déployé, il communique avec Panorama pour obtenir la licence. Si Panorama n'est pas connecté à Internet, vous devez mettre sous licence manuellement chaque instance du pare-feu VM-Series afin que le pare-feu puisse se connecter à Panorama.

Pour cette solution intégrée, le code d'autorisation (PAN-VM-1000-HV-SUB-BND-NSX2, par exemple) inclut les licences d'abonnements de Threat Prevention, de URL Filtering et WildFire, ainsi qu'un support premium pour la période demandée.

Pour pouvoir activer la licence, vous devez avoir effectué les tâches suivantes :

- Enregistrer le code d'autorisation dans le compte de support. Si vous n'avez pas enregistré le code d'autorisation, le serveur de licences ne parviendra pas à créer une licence.

©2023 Palo Alto Networks, Inc.

- Saisir le code d'autorisation dans la définition de service sur Panorama. Sur Panorama, sélectionnez **VMware Service Manager** pour ajouter le **Authorization Code (Code d'autorisation)** à la **VMware Service Definition (Définition de service VMware)**.

  Si vous avez acheté un code d'autorisation d'évaluation, vous pouvez activer sous licence jusqu'à 5 pare-feu VM-Series avec la licence de capacité VM-1000-HV pour une période de 30 ou 60 jours. Cette solution vous permettant de déployer un pare-feu VM-Series par hôte ESXi, le cluster ESXi peut inclure 5 hôtes ESXi maximum avec une licence d'évaluation.

Le processus suivant d'activation des licences est manuel. Si vous disposez d'un script personnalisé ou d'un service d'orchestration, vous pouvez utiliser l'API de mise sous licence pour automatiser le processus de récupération des licences pour les pare-feu VM-Series.

- Activer des licences sur les pare-feu VM-Series sur NSX lorsque Panorama dispose d'un accès Internet
- Activer des licences sur les pare-feu VM-Series sur NSX lorsque Panorama n'a pas d'accès Internet
- Résoudre les problèmes d'activation de licence

Activer des licences sur les pare-feu VM-Series sur NSX lorsque Panorama dispose d'un accès Internet

Effectuez la procédure suivante pour activer le pare-feu VM-Series pour NSX lorsque Panorama dispose d'un accès à Internet.

STEP 1 | Vérifiez que le pare-feu VM-Series est connecté à Panorama.

1. Connectez-vous à Panorama.
2. Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)** et vérifiez que le pare-feu apparaît comme étant Connected (Connecté).

STEP 2 | Vérifiez que chaque pare-feu est mis sous licence.

Sélectionnez **Panorama** > **Device Deployment (Déploiement de périphériques)** > **Licenses (Licences)** et vérifiez que Panorama a associé le code d'autorisation et appliqué les licences à chaque pare-feu.

Si vous ne voyez pas les licences, cliquez sur **Refresh (Actualiser)**. Sélectionnez les pare-feu VM-Series pour lesquels vous souhaitez récupérer des licences d'abonnement, puis cliquez sur **OK**.

Activer des licences sur les pare-feu VM-Series sur NSX lorsque Panorama n'a pas d'accès Internet

Effectuez la procédure suivante pour activer le pare-feu VM-Series pour NSX lorsque Panorama n'a pas accès à Internet.

STEP 1 | Repérez l'ID du processeur et l'UUID du pare-feu VM-Series.

1. Sur le serveur vCenter, obtenez l'adresse IP du pare-feu.
2. Connectez-vous à l'interface Web et sélectionnez **Dashboard (Tableau de bord)**.
3. Obtenez l'**ID du processeur** et l'**UUID** pour le pare-feu à partir du widget Informations générales.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Activez le code d'autorisation et générez les clés de licence.

1. Connectez-vous au site Web d'assistance client de Palo Alto Networks avec vos identifiants de compte. Si vous devez créer un nouveau compte, reportez-vous à la section Création d'un compte de support.
2. Sélectionnez **Assets (Actifs)** > **VM-Series Auth Codes (Codes d'autorisation VM-Series)** et cliquez sur **Add VM-Series Auth Codes (Ajouter des codes d'autorisation VM-Series)** pour saisir le code d'autorisation.
3. Sélectionnez **Register VM (Enregistrer VM)** dans la ligne qui correspond au code d'autorisation que vous venez d'enregistrer, saisissez l'ID du processeur et l'UUID du pare-feu et cliquez sur **Submit (Envoyer)**. Le portail génèrera un numéro de série pour le pare-feu.
4. Sélectionnez **Assets (Actifs)** > **Devices (Appareils)** et recherchez le numéro de série.
5. Cliquez sur le lien dans la colonne Actions pour télécharger chaque clé en local sur votre ordinateur portable. En plus de la clé de licence d'abonnement, vous devez obtenir la licence de capacité et les clés de licence de support.

STEP 3 | Chargez les clés dans la base de données.

1. Connectez-vous à l'interface Web du pare-feu.
2. Sélectionnez **Device (Appareil)** > **Licenses (Licences)**, puis **Manually upload license key (Charger manuellement une clé de licence)**.
3. Cliquez sur **Browse (Parcourir)** pour sélectionner une clé et cliquez sur **OK** pour installer la licence sur le pare-feu.

   Installez d'abord le fichier de clé de licence de capacité (pa-vm.key). Lorsque vous appliquez la clé de licence de capacité, le pare-feu VM-Series redémarre. Au redémarrage, le pare-feu disposera d'un numéro de série que vous pourrez utiliser pour enregistrer le pare-feu comme périphérique géré sur Panorama.
4. Répétez le processus pour installer chaque clé sur le pare-feu.
5. Sélectionnez **Dashboard (Tableau de bord)** et vérifiez que vous pouvez voir le **Serial # (N° de série)** dans le widget Informations générales.

STEP 4 | Ajoutez le numéro de série du pare-feu sur Panorama.

Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** et cliquez sur **Add (Ajouter)** pour saisir le numéro de série pour le pare-feu VM-Series édition NSX. Le pare-feu devrait à présent pouvoir se connecter à Panorama afin d'obtenir sa configuration et ses règles de politique.

Résoudre les problèmes d'activation de licence

Certains des problèmes les plus courants liés à l'activation de votre licence sont traités dans cette section.

 ©2023 Palo Alto Networks, Inc.

- L'octroi d'une licence PA-VM sans mémoire suffisante provoque une erreur semblable à la suivante :

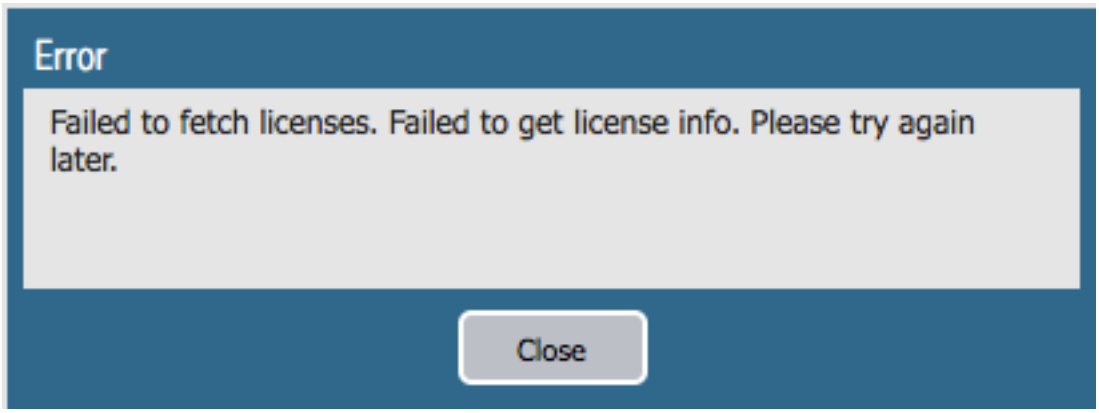
```
Server error : failed key check : Resource check failed. Memory
 needed: 6.5GB, allocated memory: 4.8GB
```

  Pour résoudre ce problème, provisionnez la mémoire supplémentaire dont la licence a besoin et récupérez la licence avec la commande **`request license fetch`**.

  Si vous utilisez une autre commande, elle échouera avec l'erreur suivante :

```
Server error : failed to fetch license: Cannot apply a provisioning
 license feature to an already provisioned device.
```

- Si vous voyez une erreur qui indique **Failed to fetch licenses (Impossible d'extraire les licences). Failed to get license info (Impossible d'obtenir les informations de licence), Please try again later (Veuillez réessayer plus tard)**, ou si un message d'erreur de communication générique s'affiche.

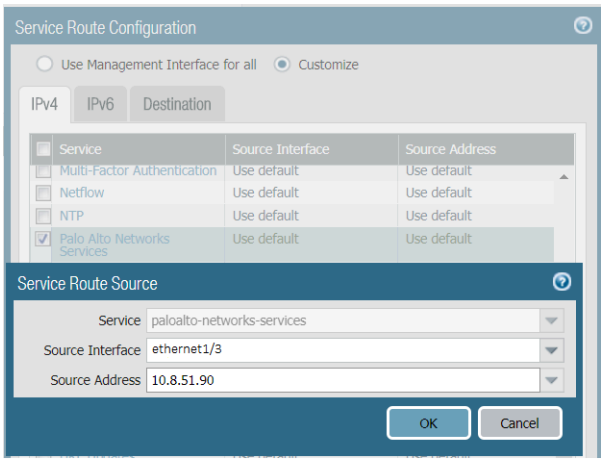


  Vérifiez les éléments suivants :

  - Le pare-feu peut-il acheminer le trafic vers le serveur Palo Alto Networks à l'aide d'un itinéraire de service ? Par défaut, le pare-feu utilise l'interface de gestion pour accéder au serveur. Si

 ©2023 Palo Alto Networks, Inc.

vous envisagez d'utiliser une interface du dataplane, assurez-vous que vous avez configuré un itinéraire de service.



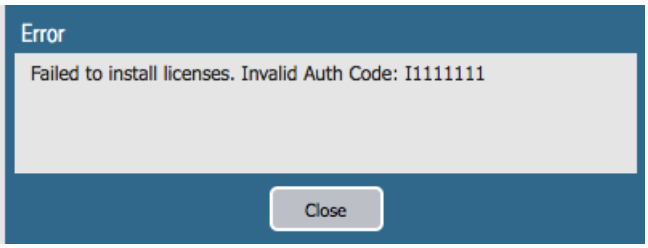
- Le routage sur Internet fonctionne-t-il ? SSH dans le pare-feu et ping sur une adresse IP accessible au public telle que 4.2.2.2. Veillez à utiliser l'option source si vous utilisez une interface du dataplane. Par exemple : ping count 3 source 10.0.1.1 hôte 4.2.2.2.
- Le DNS est-il correctement configuré ? SSH dans le pare-feu et envoyez une requête ping sur un nom DNS tel que google.com. Par exemple :

```
warby@warbylan> ping count 3 source 10.0.1.1 host google.com
PING google.com (216.58.195.78) from 10.0.1.1 : 56(84) bytes of data.
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=1 ttl=55 time=11.6 ms
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=2 ttl=55 time=11.9 ms
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=3 ttl=55 time=11.5 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 11.586/11.721/11.975/0.200 ms
```


©2023 Palo Alto Networks, Inc.

- Si vous voyez une erreur indiquant Invalid Auth Code (Code d'authentification invalide) :



  Vérifiez les éléments suivants :

  - Vous avez correctement entré le code d'autorisation.
  - Vous avez enregistré le code d'autorisation sur votre compte sur le portail de support.
  - Votre code d'autorisation n'a pas atteint la capacité d'approvisionnement maximale pour les pare-feu VM-Series.
    - Pour les licences héritées, connectez-vous au CSP et sélectionnez **Assets** > **VM-Series Auth-Codes**.
    - Pour les crédits NGFW logiciels, si vous connaissez le profil de déploiement, connectez-vous au CSP et sélectionnez **Assets** > **Software NGFW Credits**, recherchez votre profil, puis cliquez sur **Details** (Détails).

      Vous pouvez également sélectionner **Assets** > **Software NGFW Devices** et effectuer une recherche par code d'autorisation.

Enregistrement du pare-feu VM-Series

Lorsque vous achetez un pare-feu VM-Series, vous recevez un e-mail qui inclut un code d'autorisation pour une licence de capacité pour le modèle VM-Series, un code d'autorisation pour le support, ainsi qu'un ou plusieurs codes d'autorisation pour les licences d'abonnement. Pour utiliser les codes d'autorisation, vous devez les enregistrer dans le compte de support sur le site Web d'assistance client de Palo Alto Networks. Dans le cas d'une solution NSX intégrée à VMware, l'e-mail contient un code d'autorisation unique qui regroupe la licence de capacité pour une ou plusieurs instances du modèle VM-Series, l'autorisation de support, et une ou plusieurs licence(s) d'abonnement.

Pour les licences basées sur l'utilisation dans les clouds publics (AWS, Azure ou Google Cloud Platform), vous ne recevez pas de code d'autorisation. Toutefois, pour activer votre autorisation au support premium avec Palo Alto Networks, vous devez créer un compte de support et enregistrer le pare-feu VM-Series sur le site Web d'assistance client de Palo Alto Networks.

Suivez les instructions de cette section pour enregistrer le code d'autorisation de capacité ou le pare-feu dans votre compte de support :

- Enregistrement du pare-feu VM-Series (crédits NGFW logiciels)
- Enregistrement du pare-feu VM-Series (avec code d'autorisation)
- Enregistrement du modèle basé sur l'utilisation du pare-feu VM-Series pour les clouds publics (sans code d'autorisation)

 ©2023 Palo Alto Networks, Inc.

Enregistrement du pare-feu VM-Series (avec code d'autorisation)

Suivez la procédure suivante pour enregistrer votre pare-feu VM-Series avec un code d'authentification.

STEP 1 | Connectez-vous au site Web d'assistance client de Palo Alto Networks avec vos identifiants de compte. Si nécessaire, créez un compte de support.

STEP 2 | Sélectionnez **Assets (Ressources)** > **VM-Series Auth-Codes (Codes d'authentification VM-Series)** > **Add VM-Series Auth-Code (Ajouter un code d'autorisation VM-Series)**.

STEP 3 | Dans le champ **Add VM-Series Auth-Code (Ajouter un code d'authentification VM-Series)**, saisissez le code d'authentification de capacité reçu par e-mail, puis cliquez sur la coche tout à droite pour enregistrer vos données. La page affiche alors la liste des codes d'autorisation enregistrés dans votre compte de support.

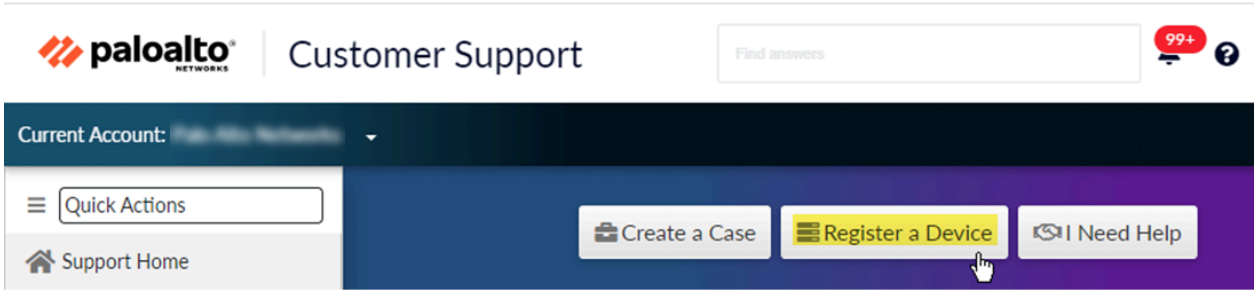
Vous pouvez suivre le nombre de pare-feu VM-Series déployés et le nombre de licences encore disponibles pouvant être utilisées par rapport à chaque code d'autorisation. Lorsque toutes les licences disponibles sont utilisées, le code d'autorisation ne s'affiche pas sur la page VM-Series Auth-Codes (Codes d'autorisation VM-Series). Pour afficher toutes les ressources déployées, sélectionnez **Assets (Ressources)** > **Devices (Périphériques)**.

Enregistrement du modèle basé sur l'utilisation du pare-feu VM-Series pour les clouds publics (sans code d'autorisation)

Pour enregistrer des pare-feu basés sur l'utilisation sur le portail de support client (CSP) de Palo Alto Networks, vous pouvez utiliser l'enregistrement automatique ou l'enregistrement manuel. L'enregistrement automatique des pare-feu basés sur l'utilisation vous permet d'enregistrer de manière transparente votre pare-feu dès que vous le lancez et d'accéder aux autorisations de licence de site associées à votre compte CSP. Pour plus d'informations, reportez-vous à la section Installation d'un certificat de périphérique sur le pare-feu VM-Series.

Utilisez le flux de travail suivant pour enregistrer manuellement vos pare-feu VM-Series. Avant de commencer le processus d'enregistrement manuel, connectez-vous au pare-feu VM-Series et notez le numéro de série et l'ID du processeur (l'UUID est facultatif) à partir du tableau de bord.

STEP 1 | Connectez-vous sur le site Internet de support client de Palo Alto Networks et cliquez sur **Assets (Ressources)** > **Devices (Périphériques)** > **Register New Devices (Enregistrer de nouveaux périphériques)**.

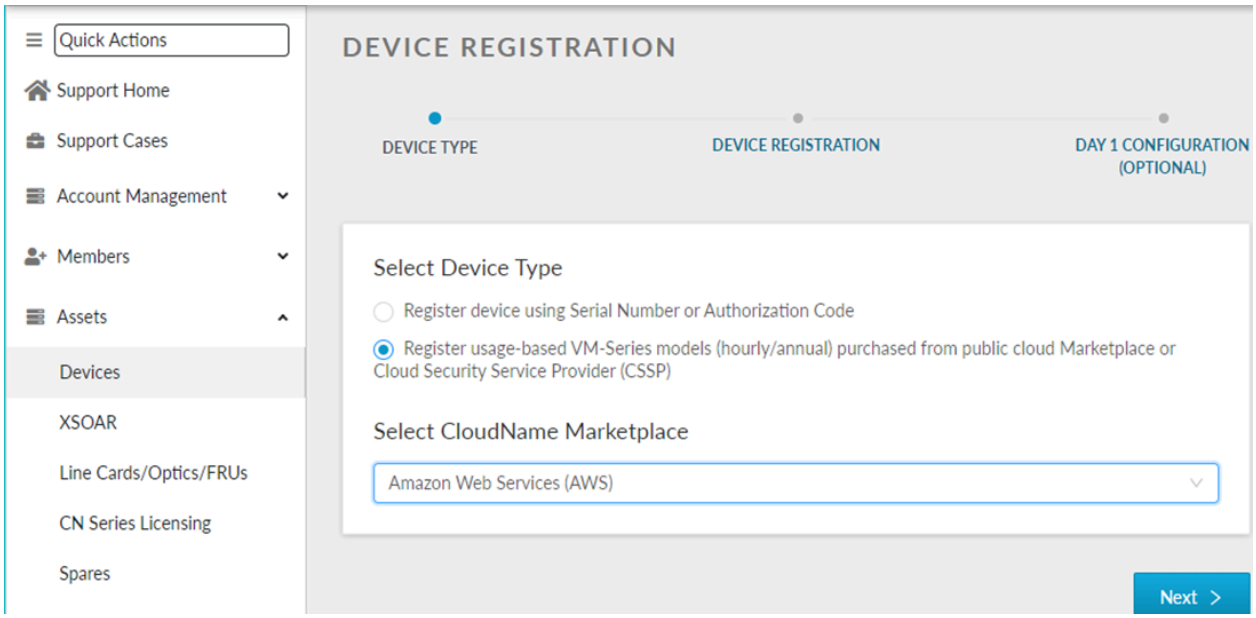


1. Sélectionnez **Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace or Cloud Security Service Provider (CSSP) (Enregistrement des modèles VM-Series basés sur l'utilisation [horaire/annuelle] achetés dans le**

 ©2023 Palo Alto Networks, Inc.

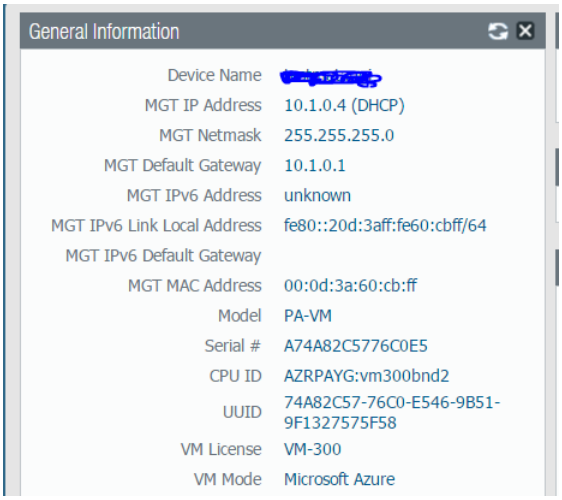
Marketplace du cloud public ou auprès du fournisseur de services de sécurité cloud [CSSP]).

2. Sélectionnez votre fournisseur **Cloud Marketplace (Marketplace du cloud)** et cliquez sur **Next (Suivant)**.



STEP 2 | Entrez le **Serial # (N° de série)**, le **CPU ID** et l'**UUID** du pare-feu VM-Series.

Par exemple, dans le tableau de bord du pare-feu VM-Series sur votre VM, vous verrez les informations suivantes.



*Si vous prévoyez d'utiliser le pare-feu hors ligne, cochez la case **Offline (Hors ligne)** et entrez la version de PAN-OS que vous prévoyez d'utiliser.*

STEP 3 | Cliquez sur **Agree and Submit (Accepter et envoyer)** pour accepter le CLUF et enregistrer le pare-feu.

STEP 4 | Vérifiez que les détails des licences que vous avez achetées sont affichés sur la page **Assets (Ressources)** du CSP.

 ©2023 Palo Alto Networks, Inc.

Installation d'un certificat de périphérique sur le pare-feu VM-Series

Le pare-feu nécessite un certificat de périphérique pour récupérer les droits de licence de site et accéder de manière sécurisée à des services cloud tels que WildFire, AutoFocus et Cortex Data Lake. Il existe deux méthodes pour appliquer une licence de site à votre pare-feu VM-Series : un mot de passe à usage unique et un PIN d'enregistrement automatique. Chaque mot de passe ou PIN est généré sur le portail de support client (CSP) et est unique à votre compte de support Palo Alto Networks. La méthode que vous utilisez dépend du type de licence utilisé pour déployer votre pare-feu et si vos pare-feu sont gérés par Panorama.

- Mot de passe à usage unique : pour les pare-feu VM-Series qui ont déjà été enregistrés auprès du serveur de licences Palo Alto Networks, vous devez générer un One-Time Password (mot de passe à usage unique - OTP) sur le portail de support client et l'appliquer à votre pare-feu VM-Series. Utilisez cette méthode pour les pare-feu VM-Series avec une licence BYOL ou ELA dans les déploiements à petite échelle non gérés et les pare-feu VM-Series déployés manuellement et gérés par Panorama.
- PIN d'enregistrement : cette méthode vous permet d'appliquer une licence de site à votre pare-feu VM-Series lors du démarrage initial. Utilisez cette méthode pour les pare-feu VM-Series avec des licences basées sur l'utilisation (PAYG) que vous amorcez au lancement ou avec tout type de déploiement automatisé, quel que soit le type de licence. Le code PIN d'enregistrement automatique vous permet d'enregistrer automatiquement vos pare-feu basés sur l'utilisation au lancement auprès du CSP et de récupérer les licences de site.

Pour le pare-feu VM-Series sur NSX-T, vous pouvez ajouter le code PIN d'enregistrement automatique à votre configuration de définition de service afin que le certificat de périphérique soit récupéré par le pare-feu lors du démarrage initial. Consultez la configuration de définition de service pour NSX-T (Nord-Sud) et NSX-T (Est-Ouest) pour obtenir plus d'informations. Si vous mettez à niveau des pare-feu précédemment déployés vers la version PAN-OS qui prend en charge les certificats de périphérique, vous pouvez appliquer un certificat de périphérique à ces pare-feu individuellement en utilisant un mot de passe à usage unique.

Les mots de passe à usage unique et les PIN d'enregistrement automatique doivent être utilisés avant leur expiration. Sinon, vous devez retourner sur le CSP pour en générer un nouveau.

- Activez les pare-feu pour qu'ils récupèrent automatiquement les licences de site au lancement.

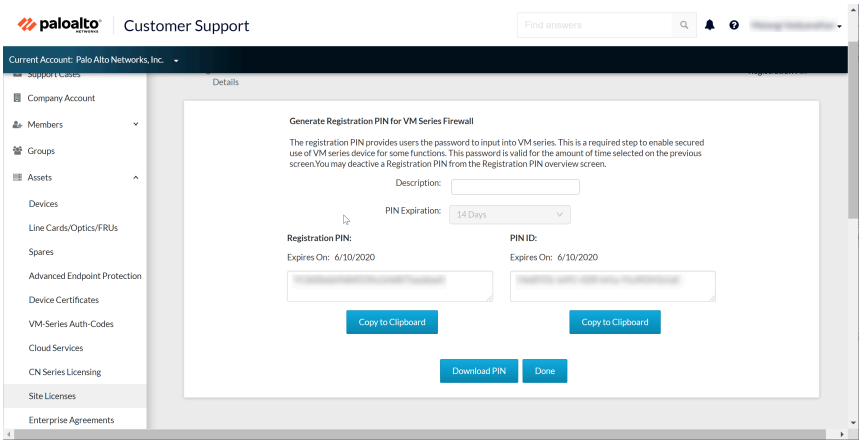
  Le pare-feu a besoin du certificat de périphérique pour obtenir les droits de licence de site et accéder de manière sécurisée aux services cloud. Pour récupérer les licences de site au lancement du pare-feu, vous devez inclure, dans l'ensemble d'amorçage, le code d'authentification dans le dossier /license, ajouter l'ID et la valeur du PIN d'enregistrement automatique dans le fichier init-cfg.txt et le placer dans le dossier /config. L'ajout de l'ID et de la valeur du PIN d'enregistrement automatique permet également l'enregistrement automatique du PAYG ou des instances basées sur l'utilisation sur le pare-feu VM-Series.

  1. Connectez-vous au portail de support client (CSP).

 ©2023 Palo Alto Networks, Inc.

2. Générez le PIN d'enregistrement VM-Series.

   Sélectionnez **Assets (Ressources)** > **Device Certificates (Certificats de périphériques)** > **Generate Registration PIN (Générer un PIN d'enregistrement)**. Enregistrez l'ID et la valeur du PIN. Veillez à lancer le pare-feu avant l'expiration du PIN.

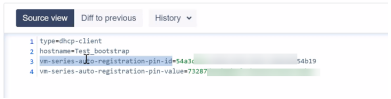


3. Ajoutez l'ID et la valeur du PIN d'enregistrement dans le fichier init-cfg.txt file.

   Outre les paramètres requis, vous devez inclure :

   ```
   vm-series-auto-registration-pin-id=
   ```

   ```
   vm-series-auto-registration-pin-value=
   ```



4. Connectez-vous au pare-feu et vérifiez que vous pouvez voir la licence de site sur le pare-feu.

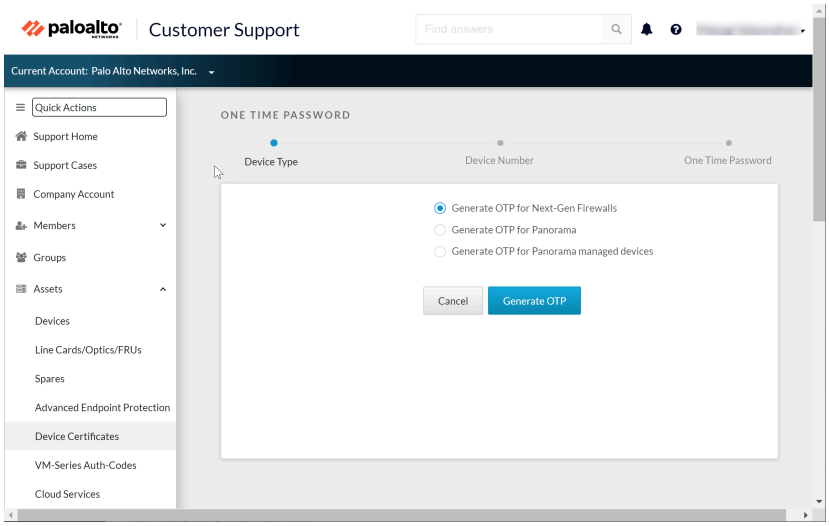
©2023 Palo Alto Networks, Inc.

- Générez le mot de passe à usage unique (OTP) et récupérez manuellement le certificat de périphérique sur le pare-feu.

  Le pare-feu a besoin de ce certificat de périphérique pour obtenir les droits de licence de site et accéder de manière sécurisée aux services cloud.

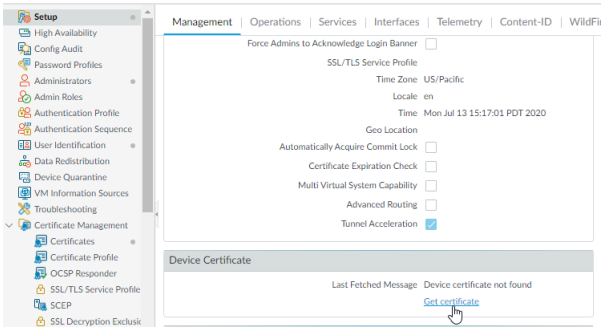
  1. Ouvrez une session dans le portail de support client.

     Enregistrez votre pare-feu VM-Series, si vous ne l'avez pas encore fait.
  2. Sélectionnez **Assets (Ressources)** > **Device Certificates (Certificats de périphériques)** > **Generate OTP (Générer un OTP)**.



  3. Sélectionnez votre pare-feu dans la liste pour **Generate OTP (Générer un OTP)**.
  4. Connectez-vous au pare-feu et récupérez le certificat de périphérique.

     Sélectionnez **Setup (Configuration)** > **Management (Gestion)** > **Device Certificate (Certificat de périphérique)** et **Get Certificate (Obtenir un certificat)**.



  5. Vérifiez que le certificat de périphérique est récupéré et que vous pouvez voir la licence de site sur le pare-feu.

- Si vous utilisez Panorama pour gérer le pare-feu VM-Series, reportez-vous à la section Installer le certificat de périphérique sur un pare-feu géré.

©2023 Palo Alto Networks, Inc.

Basculer entre les licences BYOL et PAYG

Le pare-feu VM-Series ne peut pas passer de l'option de licence BYOL à l'option PAYG, et vice-versa. Si vous avez déjà déployé et configuré un pare-feu VM-Series avec l'option PAYG ou BYOL dans AWS, Azure ou Google Cloud Platform et que vous souhaitez maintenant passer à l'autre option, suivez les instructions ci-dessous pour enregistrer et exporter la configuration sur un pare-feu existant, déployez un nouveau pare-feu, puis restaurez la configuration sur le nouveau pare-feu.

STEP 1 | Enregistrez une sauvegarde du fichier de configuration actuelle et stockez-la sur un serveur externe.

1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Operations (Opérations)** et **Export named configuration snapshot (Exporter l'instantané de configuration nommé)**.
2. Sélectionnez le fichier XML contenant la configuration actuelle (par exemple, running-config.xml), puis cliquez sur **OK** pour exporter le fichier de configuration.
3. Enregistrez le fichier exporté dans un emplacement externe au pare-feu.

STEP 2 | Déployez un nouveau pare-feu et enregistrez ou activez la licence, selon le cas.

Pour une nouvelle instance PAYG :

1. Dans AWS, Azure ou Google Cloud Platform Marketplace, sélectionnez l'image logicielle du regroupement de licences PAYG que vous souhaitez déployer.
2. Déployez un nouveau pare-feu VM-Series dans le cloud public AWS, Azure ou Google. Voir Configurer le pare-feu VM-Series sur AWS, Configurer le pare-feu VM-Series sur Azure ou Configurer le pare-feu VM-Series sur Google Cloud Platform.
3. Enregistrement modèle basé sur l'utilisation du pare-feu VM-Series pour les clouds publics (sans code d'autorisation).

Pour une nouvelle instance BYOL :

1. Contactez votre représentant commercial ou revendeur pour acheter une licence BYOL et obtenir un code d'autorisation BYOL que vous pouvez utiliser pour obtenir une licence pour votre pare-feu.
2. Enregistrez le pare-feu VM-Series (avec code d'autorisation).
3. Déployez un nouveau pare-feu VM-Series sur le cloud public Azure ou AWS. Voir Configurer le pare-feu VM-Series sur AWS, Configurer le pare-feu VM-Series sur Azure ou Configurer le pare-feu VM-Series sur Google Cloud Platform.
4. Activez la licence pour le pare-feu VM-Series (version autonome).

©2023 Palo Alto Networks, Inc.

STEP 3 | Sur le pare-feu nouvellement déployé, restaurez la configuration que vous avez exportée.

1. Accédez à l'interface Web du pare-feu nouvellement déployé.
2. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Operations (Opérations)**, **Import named configuration snapshot (Importez l'instantané de configuration)**, Browse (Parcourir) jusqu'au fichier de configuration sur l'hôte externe, puis cliquez sur **OK**.
3. Cliquez sur **Load named configuration snapshot (Charger l'instantané de la configuration)**, sélectionnez le **Name (Nom)** du fichier de configuration que vous venez d'importer et cliquez sur **OK**.
4. Cliquez sur **Commit (Valider)** pour remplacer la configuration active avec l'instantané que vous venez d'importer.
5. Avant de supprimer le pare-feu ou de désactiver les licences sur le pare-feu remplacé, vérifiez que la configuration du nouveau pare-feu correspond au pare-feu que vous remplacez.

Basculer entre les licences de modèle VM-Series

Vous pouvez changer la licence de votre pare-feu VM-Series actuellement déployé avec l'option BYOL. Par exemple, vous pouvez passer d'un forfait d'abonnement à un contrat de licence d'entreprise (ELA) et vice versa, sans perturber le trafic passant par le pare-feu. Vous pouvez faire passer la licence sur un pare-feu individuel ou sur plusieurs pare-feu simultanément à partir de Panorama.

N'utilisez pas cette procédure pour basculer des licences ELA ou perpétuelles entre PAYG et BYOL. Pour plus d'informations, reportez-vous à la section Basculer entre les licences BYOL et PAYG.

Effectuez l'une des procédures suivantes pour effectuer l'une des modifications de licence suivantes :

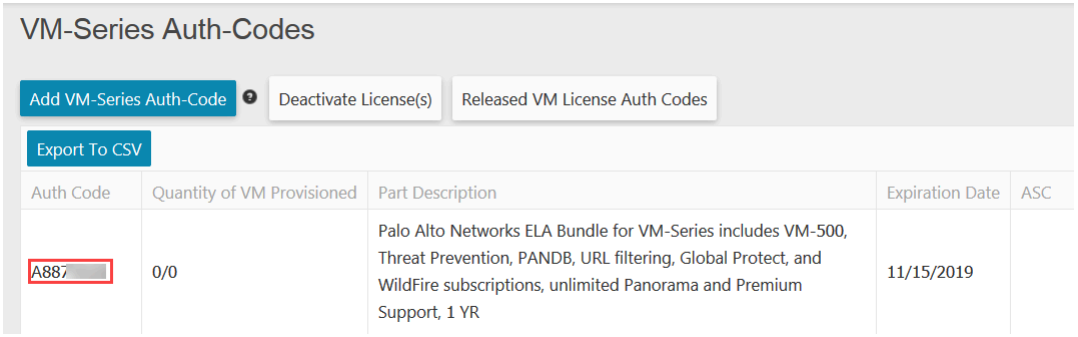
- Forfait d'abonnement 1 vers forfait d'abonnement 2
- Forfait d'abonnement 1 ou 2 vers un ELA
- Licence de capacité vers un forfait d'abonnement ou ELA

Avant de passer à une licence ELA, vous devez allouer un nombre suffisant de jetons pour soutenir le nombre de pare-feu VM-Series actuellement déployés. Reportez-vous à la section Accord de licence d'entreprise VM-Series (ELA multimodèle) pour plus d'informations sur les jetons requis pour chaque modèle VM-Series.

©2023 Palo Alto Networks, Inc.

- Modifiez une licence sur un pare-feu autonome.
  1. Enregistrez votre code d'autorisation.
     - Pour un forfait d'abonnement, procédez à l'enregistrement de votre nouveau code d'autorisation.
     - Pour un ELA, activez le code d'autorisation ELA.

     N'utilisez pas le code d'autorisation ELA pour activer des pare-feu individuels VM-Series. Après avoir enregistré votre ELA, utilisez les codes d'autorisation de modèle VM-Series pour activer les pare-feu individuels. Vous pouvez trouver ces codes d'autorisation sur le portail de support client dans ***Assets (Ressources) > VM-Series Auth-Codes (Codes d'autorisation VM-Series).***
  2. Connectez-vous à l'interface Web du pare-feu VM-Series.
  3. Vérifiez la configuration du serveur de mises à jour de Palo Alto Networks.
     1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Services**.
     2. Confirmez que **Update Server** (Serveur de mise à jour) est défini sur updates.paloaltonetworks.com.
     3. Confirmez que **Update Server Identity** (Mettre à jour l'identité du serveur) est sélectionné.
  4. Appliquez un code d'autorisation VM-Series. Un code d'autorisation de pare-feu pour une ELA commence par la lettre A, comme indiqué ci-dessous.

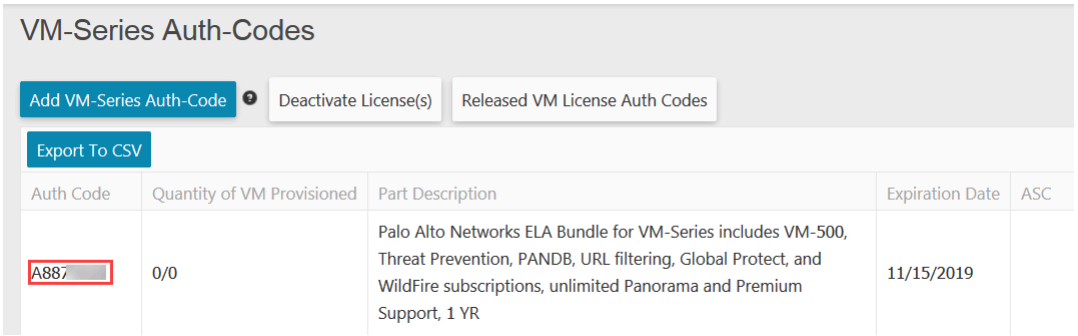
     

     1. Sélectionnez **Device (Appareil)** > **Licenses (Licences)**, puis cliquez sur le lien **Activate feature using authorization code (Activer la fonctionnalité à l'aide du code d'autorisation)**.
     2. Saisissez votre code d'autorisation VM-Series.
     3. Cliquez sur **OK** pour confirmer la mise à niveau de la licence. Le pare-feu contacte le serveur de mises à jour de Palo Alto Networks et utilise les jetons requis pour votre pare-feu en fonction du modèle VM-Series.
     4. Vérifiez que la licence a bien été mise à jour en vérifiant la Expiration Date (date d'expiration) de la licence.
  5. Répétez ce processus pour chaque pare-feu VM-Series de votre déploiement.

©2023 Palo Alto Networks, Inc.

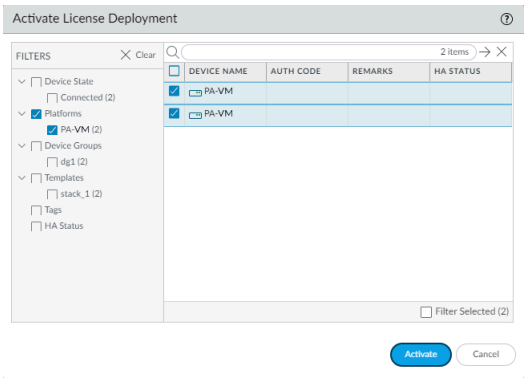
- Modifiez les licences sur les pare-feu gérés à l'aide de Panorama.
  1. Enregistrez votre code d'autorisation.
     - Pour un forfait d'abonnement, procédez à l'enregistrement de votre nouveau code d'autorisation.
     - Pour un ELA, activez le code d'autorisation ELA.

     N'utilisez pas le code d'autorisation ELA pour activer des pare-feu individuels VM-Series. Après avoir enregistré votre ELA, utilisez les codes d'autorisation de modèle VM-Series pour activer les pare-feu individuels. Vous pouvez trouver ces codes d'autorisation sur le portail de support client dans ***Assets (Ressources) > VM-Series Auth-Codes (Codes d'autorisation VM-Series).***
  2. Connectez-vous à l'interface Web Panorama.
  3. Vérifiez la configuration du serveur de mises à jour de Palo Alto Networks pour les pare-feu.
     1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Services**.
     2. Confirmez que **Update Server** (Serveur de mise à jour) est défini sur updates.paloaltonetworks.com.
     3. Confirmez que **Update Server Identity** (Mettre à jour l'identité du serveur) est sélectionné.
  4. Appliquez un code d'autorisation VM-Series. Un code d'autorisation de pare-feu pour une ELA commence par la lettre A, comme indiqué ci-dessous.

     1. Sélectionnez **Panorama** > **Device Deployment (Déploiement d'appareils)** > **Licenses (Licences)** et cliquez sur **Activate (Activer)**.
     2. Saisissez votre code d'autorisation VM-Series.
     3. Utilisez les Filters (Filtres) pour sélectionner les pare-feu gérés à mettre sous licence.
     4. Saisissez votre code d'autorisation dans la colonne **Auth Code** (Code d'autorisation) pour chaque pare-feu.
     5. Cliquez sur **Activate (Activer)** pour confirmer la mise à niveau de la licence. Panorama contacte le serveur de mises à jour Palo Alto Networks et utilise les jetons requis pour vos pare-feu en fonction du modèle VM-Series.

 ©2023 Palo Alto Networks, Inc.



6. Vérifiez que la licence a bien été mise à jour en vérifiant la Expiration Date (date d'expiration) de la licence.

Désactivation de la ou des licence(s)

Le processus de désactivation des licences vous permet d'autogérer les licences. Si vous voulez retirer un ou plusieurs licences ou abonnements attribués à un pare-feu (pare-feu matériel ou VM-Series) ou si vous voulez désactiver le pare-feu VM-Series et désaffecter des licences et abonnements actifs, commencez le processus de désactivation sur le pare-feu ou Panorama (pas sur le site Web d'assistance client de Palo Alto Networks).

Pour désactiver une licence, vous devez installer une clé API de désactivation de licence et activer la vérification de l'identité du serveur de mise à jour (activée par défaut). PAN-OS utilise cette clé API de désactivation pour s'authentifier avec toutes les mises à jour des services de licence. La clé API de désactivation n'est pas nécessaire pour la désactivation manuelle de licence lorsqu'il n'y a pas de connectivité entre le pare-feu et le serveur de licences.

Si le pare-feu ou Panorama a accès à Internet et qu'il peut communiquer avec les serveurs de licences de Palo Alto Networks, le processus de retrait de la licence se termine automatiquement d'un clic de bouton. Si le pare-feu ou Panorama n'a pas accès à Internet, vous devez effectuer le processus manuellement en deux étapes. À la première étape, à partir du pare-feu ou de Panorama, vous devez générer un fichier de jeton de licence qui contient des renseignements sur les clés désactivées et l'exporter. À la deuxième étape, lorsque vous êtes connecté au site Web d'assistance client de Palo Alto Networks, chargez le fichier jeton pour dissocier les clés de licence du pare-feu.

- Désactivation d'un abonnement ou d'une licence de fonctionnalité à l'aide de l'interface de ligne de commande (CLI)
- Désactivation de VM

Désactivation d'un abonnement ou d'une licence de fonctionnalité à l'aide de l'interface de ligne de commande (CLI)

Si vous avez installé une licence ou un abonnement sur un pare-feu et devez la réattribuer à un autre pare-feu, vous pouvez désactiver la licence individuelle et réutiliser le même code d'autorisation sur un autre pare-feu sans obtenir d'aide du support technique. Cette capacité est uniquement prise en charge dans la CLI et est prise en charge sur les périphériques physiques et virtuels exécutant PAN-OS. Cette procédure est généralement utilisée avec les licences perpétuelles ou ELA à modèle fixe.

- Accès Internet (mode automatique)
- Aucun accès à Internet (mode manuel)

 ©2023 Palo Alto Networks, Inc.

Accès Internet (mode automatique)

STEP 1 | Connectez-vous à la CLI sur le pare-feu.

STEP 2 | Affichez le nom de la clé de licence correspondant à la caractéristique que vous souhaitez désactiver.

```
demander une licence désactive les fonctionnalités clés
```

STEP 3 | Désactivez la licence ou l'abonnement.

Utilisez le mode automatique pour supprimer la clé de licence.

```
request license deactivate key features <name> mode auto
```

Le nom est le nom complet du fichier de clé de licence. Par exemple :

```
admin@vmPAN2> request license deactivate key features <name>
```

```
WildFire_License_2015_01_28_I5820573.key mode auto007200002599
 WildFire License Success Successfully removed license keys
```

Aucun accès à Internet (mode manuel)

Utilisez le mode manuel pour supprimer la clé de licence et générer un jeton de licence pour une licence basée sur un modèle. Cette procédure suppose que vous avez installé la clé API de licence sur votre pare-feu.

STEP 1 | Connectez-vous à la CLI sur le pare-feu.

STEP 2 | Affichez le nom de la clé de licence correspondant à la caractéristique que vous souhaitez désactiver.

```
demander une licence désactive les fonctionnalités clés
```

STEP 3 | Désactivez la licence manuellement depuis la ligne de commande.

```
request license deactivate key features <name> mode manual
```

Par exemple :

```
admin@PA-VM> request license deactivate key features
```

```
PAN_DB_URL_Filtering_2015_01_28_I6134084.key mode manual
 Successfully removed license keys dact_lic.01282015.100502.tok
```

Le fichier de jeton utilise le format `dact_lic.timestamp.tok`, où l'horodatage est présenté au format `jmmaaaa.hms`.

STEP 4 | Vérifiez que le fichier de jeton a été généré.

```
show -token-files
```

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Exportez le fichier de jeton.

Entrez cette commande sur une seule ligne :

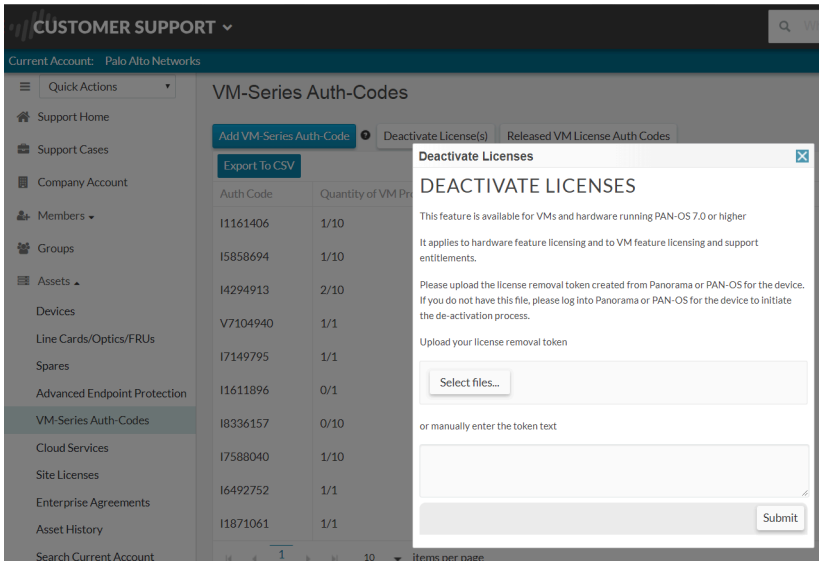
```
scp export license-token-file to <username@serverIP>
from <token_filename>
```

Par exemple :

```
scp export license-token-file to admin@10.1.10.55:/tmp/ from
dact_lic.01282015.100502.tok
```

STEP 6 | Connectez-vous au portail de support client de Palo Alto Networks.

1. Cliquez sur le lien **Deactivate License(s) (Désactiver licence(s))** qui se trouve à l'onglet **Assets (Ressources)**.
2. Sélectionnez **Assets (Ressources)** > **VM-Series Auth-Codes (Codes d'authenfication VM-Series)** et sélectionnez **Deactivate License(s) (Désactivation des licences)**.
3. Téléchargez le fichier de jeton pour terminer la désactivation.



Désactivation de VM

Lorsque vous n'avez plus besoin d'une instance du pare-feu VM-Series, vous pouvez libérer toutes les licences actives (licences d'abonnement, licences de capacité basées sur le modèle et autorisations de support), à partir de l'interface Web, de la CLI ou de l'API XML sur le pare-feu ou sur Panorama. Les licences sont recréditées sur votre compte et vous pouvez utiliser les mêmes codes d'autorisation sur une autre instance d'un pare-feu VM-Series.

Lors de la désactivation d'une VM, toutes les licences et les autorisations sont retirées et le pare-feu VM-Series se retrouve sans licences ; le pare-feu n'a plus de numéro de série et peut uniquement prendre en charge un nombre restreint de sessions. Étant donné que la configuration du pare-feu n'est pas touchée, vous pouvez de nouveau appliquer un ensemble de licences et rétablir toutes les fonctions du pare-feu, au besoin.

©2023 Palo Alto Networks, Inc.

*Assurez-vous de désactiver les licences **avant** de supprimer le pare-feu VM-Series. Si vous supprimez le pare-feu avant d'avoir désactivé les licences, deux options s'offrent à vous :*

***Géré par Panorama** : désactivez la licence de Panorama.*

***Non géré par Panorama** :contactez le support client de Palo Alto Networks pour obtenir de l'aide à la désactivation.*

- Désactivez la VM du pare-feu.
- Désactivez la VM de Panorama.

Désactivez la VM du pare-feu.

Effectuez la procédure suivante pour désactiver la licence VM du pare-feu.

STEP 1 | Connectez-vous à l'interface Web et sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.

STEP 2 | Dans la section License Management (Gestion des licences), sélectionnez **Deactivate VM (Désactiver VM)**.

Vous ne pouvez voir cette option que sur une VM. Elle n'est pas disponible sur un pare-feu physique.

STEP 3 | Vérifiez la liste des licences et des autorisations à désactiver sur le pare-feu.

STEP 4 | Pour procéder à la désactivation de VM, sélectionnez l'une des options suivantes :

- (Accès Internet au serveur de mise sous license de Palo Alto Networks) Sélectionnez **Continue (Continuer)**.

  Vous êtes invité à redémarrer le pare-feu ; au redémarrage, les licences sont désactivées.
- (Pas d'Internet) : sélectionnez **Complete Manually (Terminer manuellement)**.

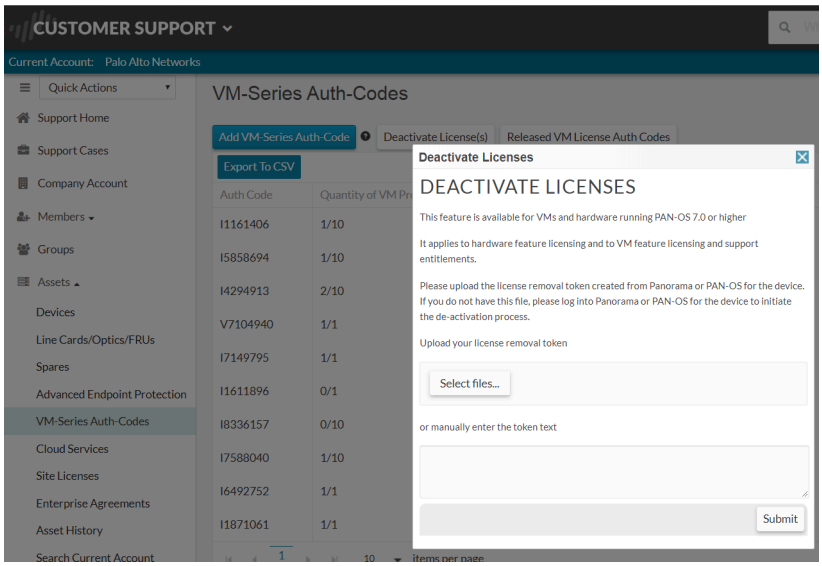
  Cliquez sur le lien **Export license token (Exporter le jeton de licence)** pour enregistrer le fichier de jeton sur votre ordinateur local. Voici un exemple de nom de fichier de jeton : 20150128_1307_dact_lic.01282015.130737.tok

  Vous êtes invité à redémarrer le pare-feu ; au redémarrage, les licences sont désactivées.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | (Processus manuel – pas d'Internet) Utilisez le fichier de jeton pour enregistrer les modifications auprès du serveur de mise sous licence :

1. Connectez-vous au site Web d'assistance client de Palo Alto Networks.
2. Sélectionnez **Assets** > **VM-Series Auth-Codes** > **Deactivate License(s) (Désactivation des licences)**.
3. Lorsque vous êtes connectés au site Web d'assistance client de Palo Alto Networks, chargez le fichier jeton pour terminer la désactivation.



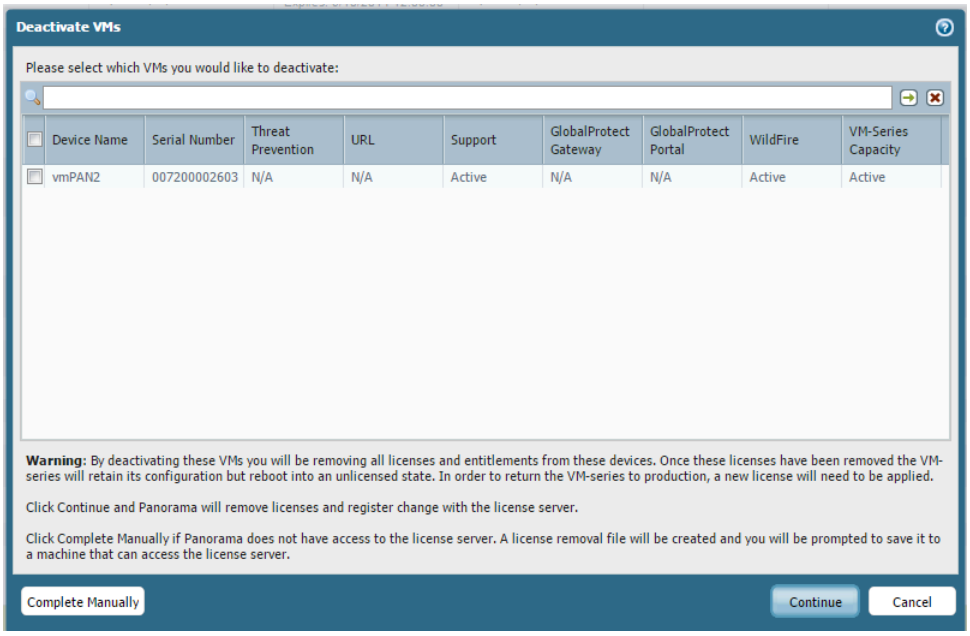
Désactivez la VM de Panorama.

Effectuez la procédure suivante pour désactiver une licence VM de Panorama.

STEP 1 | Connectez-vous à Panorama et sélectionnez **Panorama** > **Device Deployment (Déploiement de périphérique)** > **Licenses (Licences)**.

©2023 Palo Alto Networks, Inc.

STEP 2 | Cliquez sur **Deactivate VMs (Désactiver VM)**, puis sélectionnez le pare-feu VM-Series que vous souhaitez désactiver.



STEP 3 | Pour désactiver la VM, sélectionnez l'une des options suivantes :

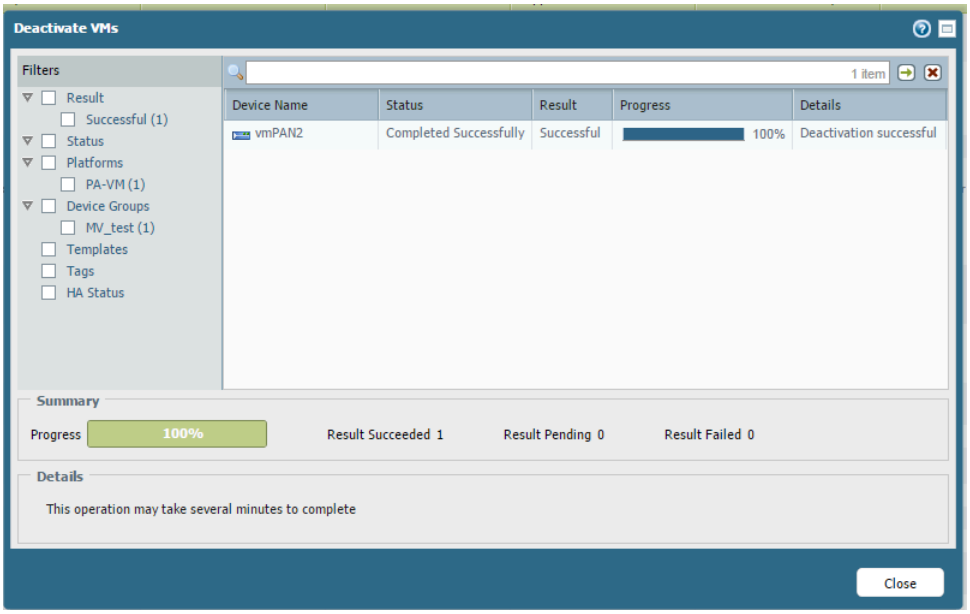
- **Continue (Continuer)** : si Panorama peut communiquer directement avec les serveurs de licences de Palo Alto Networks et enregistrer les modifications. Pour vérifier que les licences ont été désactivées sur le pare-feu, cliquez sur **Refresh on Panorama (Actualiser dans Panorama)** > **Device Deployment (Déploiement de périphériques)** > **Licenses (Licences)**. Le pare-feu redémarre automatiquement.

 ©2023 Palo Alto Networks, Inc.

- **Terminer manuellement** : si Panorama n'a pas accès à Internet, Panorama génère un fichier de jeton.

  Cliquez sur le lien **Export license token (Exporter le jeton de licence)** pour enregistrer le fichier de jeton sur votre ordinateur local. Voici un exemple de nom de fichier de jeton : 20150128_1307_dact_lic.01282015.130737.tok

  Un message confirmant que l'exportation a été effectuée avec succès s'affiche à l'écran, et le pare-feu redémarre automatiquement.



STEP 4 | (Processus manuel uniquement – pas d'Internet) Utilisez le fichier de jeton pour enregistrer les modifications auprès du serveur de mise sous licence.

1. Connectez-vous au site Web d'assistance client de Palo Alto Networks.
2. Sélectionnez **Assets** > **VM-Series Auth-Codes** > **Deactivate License(s) (Désactivation des licences)**.
3. Téléchargez le fichier de jeton pour terminer la désactivation.

STEP 5 | Retirez le pare-feu VM-Series désactivé des périphériques gérés dans Panorama.

1. Sélectionnez **Panorama** > **Managed Devices (Appareils gérés)**.
2. Dans la liste des périphériques gérés, sélectionnez le pare-feu que vous avez désactivé, puis cliquez sur **Supprimer**.

Plutôt que de supprimer les pare-feu, vous pouvez également décider de créer un groupe de périphériques distinct et d'affecter les pare-feu VM-Series qui ont été désactivés à ce groupe de périphériques.

Renouveler les paquets de permis de coupe-feu de la série VM

Lorsque vos licences de lot de pare-feu de série VM doivent être renouvelées, vous pouvez ouvrir une session dans le Portail de soutien à la clientèle de Palo Alto Networks et ajuster la quantité de licence pour répondre à vos besoins de déploiement. Au moment du renouvellement, vous pouvez

©2023 Palo Alto Networks, Inc.

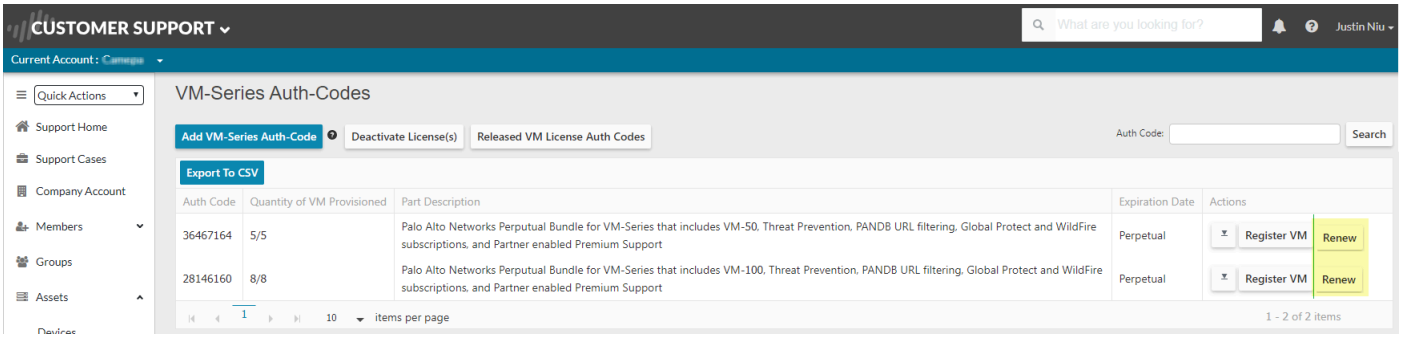
examiner vos tendances d'utilisation et établir vos besoins futurs en choisissant parmi les options suivantes :

- **Renew**—Vous pouvez choisir de renouveler toutes les licences telles quelles, ou d'augmenter ou de diminuer la quantité autorisée. Si vous réduisez le nombre de licences dont vous avez besoin, vous devez choisir d'obtenir un forfait de base pour les pare-feu que vous ne renouvelez pas, sinon vous perdrez la portion que vous ne renouvelez pas. Si vous augmentez la quantité de permis, l'ajout est ajouté à votre code d'autorisation existant.
- **Changement au forfait de base**—Si vous avez un forfait de série VM 1 ou un forfait 2 qui comprend des abonnements, vous pouvez passer à un forfait de base qui comprend une licence de capacité perpétuelle et un droit de soutien. Lorsque vous passez à la liasse de base, vous conservez le modèle VM-Series de pare-feu que vous aviez déjà acheté. Tous les pare-feu qui sont actuellement déployés et qui sont associés au code d'autorisation existant continueront de fonctionner, et le droit de soutien aura une nouvelle date d'expiration. Pour tout coupe-feu non programmé, vous recevrez un nouveau code d'auteur que vous pourrez utiliser pour déployer de nouvelles instances.
- **Confiscation**—Renoncez aux licences dont vous n'avez plus besoin. Si vous avez déployé les pare-feu que vous ne voulez pas renouveler, vous devez sélectionner le numéro de série des instances pour lesquelles vous voulez interrompre le renouvellement. Vous pouvez continuer d'utiliser ces instances de pare-feu avec les versions logicielles et de contenu qui sont actuellement installées, mais vos abonnements et vos droits de soutien ne sont plus valides. Et pour perdre la licence des pare-feu VM-Series que vous n'avez pas configurée, il vous suffit de sélectionner la quantité que vous souhaitez perdre.

STEP 1 | Connectez-vous au Portail assistance clientèle de Palo Alto Networks avec vos identifiants de compte.

STEP 2 | Sélectionner **Assets** > **VM-Series Auth-Codes** et trouver le code d'auteur que vous souhaitez renouveler.

L'option **Renew (Renouveler)** s'affiche pour les codes d'autorisation admissibles au renouvellement.

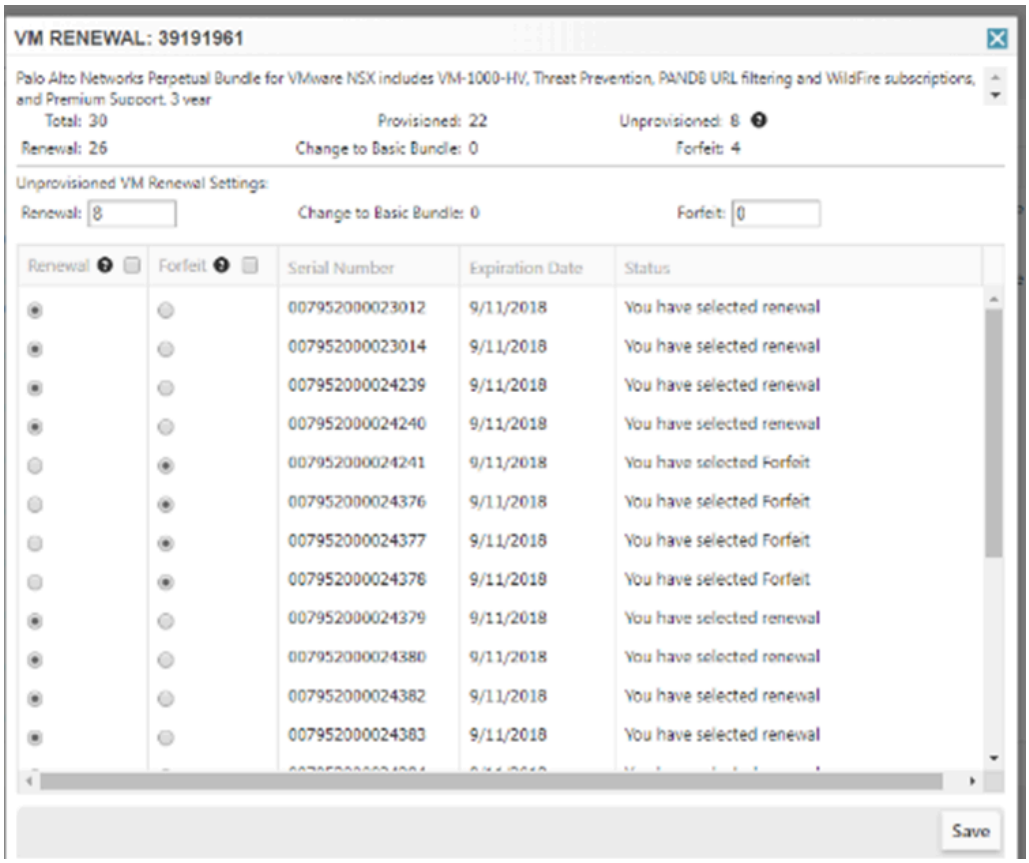


STEP 3 | Cliquez sur le lien **Renew** pour sélectionner les numéros de série à **Renew**, **Change to Basic Bundle**, ou **Forfeit**.

Si vous avez configuré le pare-feu, sélectionnez l'option appropriée dans la ligne correspondant au Serial Number (Numéro de série). Si vous avez des instances non configurées du pare-feu,

 ©2023 Palo Alto Networks, Inc.

sélectionnez la quantité pour chaque option de renouvellement choisie dans **Unprovisioned VM Renewal Settings (Paramètres de renouvellement de VM non configurés)**.



STEP 4 | Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

Vous recevrez à l'écran une confirmation que vos modifications sont soumises pour le traitement. Après avoir soumis vos modifications, si vous sélectionnez à nouveau l'option Renew (Renouveler), vous pouvez afficher l'état de votre requête par rapport à chaque numéro de série. Si le processus de renouvellement a commencé et que vous devez effectuer des révisions supplémentaires, vous ne pourrez pas enregistrer les modifications. Pour obtenir de l'aide, vous pouvez contacter l'équipe des renouvellements à l'adresse renewals@paloaltonetworks.com.

©2023 Palo Alto Networks, Inc.

Que se passe-t-il à l'expiration des licences ?

Grâce aux abonnements et aux licences de pare-feu VM-Series Palo Alto Networks, le pare-feu bénéficie de fonctionnalités accrues et/ou d'un accès à un service fourni par le cloud de Palo Alto Networks. Lorsqu'une licence est dans les 30 jours suivant son expiration, un message d'avertissement s'affiche quotidiennement dans le journal système jusqu'à ce que l'abonnement soit renouvelé ou expire. Lorsque la licence arrive à expiration, certains abonnements continuent de fonctionner de façon limitée, et d'autres cessent complètement de fonctionner. Vous découvrirez ici ce qui se produit lors de l'expiration de chaque abonnement.

Le moment précis de l'expiration de la licence est au début du jour suivant à 00h00 (GMT). Par exemple, si votre licence doit se terminer le 1/20, vous aurez des fonctionnalités pour le reste de la journée. Au début de la nouvelle journée le 21/01 à 00h00 (GMT), la licence expirera. Toutes les fonctions liées aux licences fonctionnent à l'heure GMT (Greenwich Mean Time), quel que soit le fuseau horaire configuré sur le pare-feu.

Licence	Comportement à l'expiration
VM-Series	**Vous pouvez tout de même :** Vous pouvez continuer à configurer et à utiliser le ou les pare-feux que vous avez déployés avant l'expiration de la licence sans modifier la capacité de la session. Le ou les pare-feux ne redémarreront pas automatiquement et causeront une interruption du trafic. Cependant, si le pare-feu redémarre pour une raison quelconque, celui-ci entre dans un état « sans licence ». Sans licence, le nombre de sessions prises en charge est limité à 1 200. Aucune autre fonctionnalité ou option de configuration du plan de gestion n'est restreinte.
Threat Prevention	Des alertes indiquant que la licence est expirée apparaissent dans le journal système. **Vous pouvez tout de même :** • Utilisez les signatures qui ont été installées au moment où la licence a expiré, sauf si vous installez une nouvelle mise à jour du contenu des applications uniquement, soit manuellement, soit dans le cadre d'un programme automatique. Si vous le faites, la mise à jour supprimera vos signatures de menace existantes et vous ne serez plus protégé contre celles-ci. • Utiliser et modifier les App-ID™ et les signatures de menaces personnalisés. **Vous ne pouvez plus :** • Installer de nouvelles signatures.

©2023 Palo Alto Networks, Inc.

Licence	Comportement à l'expiration
	• Retourner à des versions antérieures des signatures.
Sécurité DNS	**Vous pouvez tout de même :** • Utiliser les signatures DNS locales et vous détenez une licence de prévention des menaces. **Vous ne pouvez plus :** • Obtenir de nouvelles signatures DNS.
Filtrage d'URL avancé / Filtrage d'URL	**Vous pouvez tout de même :** • Appliquer la politique au moyen des catégories d'URL personnalisées. • Appliquer la politique au moyen des catégories PAN-DB qui se trouvaient dans votre mémoire tampon local lors de l'expiration de la licence. **Vous ne pouvez plus :** • Obtenir les mises à jour des catégories PAN-DB mises en mémoire tampon. • Connectez-vous à la base de données de filtrage d'URL PAN-DB. • Obtenir les catégories PAN-DB des URL qui ne sont pas en mémoire tampon. • Analysez les demandes d'URL en temps réel à l'aide du filtrage d'URL avancé.
WildFire	**Vous pouvez tout de même :** • Transmettre des PE à des fins d'analyse. • Obtenir les mises à jour des signatures aux 24 à 48 heures, si vous détenez un abonnement Prévention des menaces actif. **Vous ne pouvez plus :** • Obtenez des mises à jour aux cinq minutes grâce aux clouds WildFire publics et privés. • Transférez des types de fichiers avancés, comme les fichiers APK, Flash, PDF, Microsoft Office, applets Java, fichiers Java (.jar et .class), ainsi que les liens d'e-mail HTTP/HTTPS contenus dans les messages électroniques SMTP et POP3. • Utilise l'API WildFire. • Utilisez l'appareil WildFire pour héberger un cloud WildFire privé ou un cloud WildFire hybride.
AutoFocus	**Vous pouvez tout de même :**

©2023 Palo Alto Networks, Inc.

Licence	Comportement à l'expiration
	• Utiliser une liste dynamique externe avec des données AutoFocus pour une période de grâce de trois mois. **Vous ne pouvez plus :** • Accéder au portail AutoFocus. • Consulter le récapitulatif des données de renseignements d'AutoFocus du journal de surveillance ou des artefacts ACC.
Cortex Data Lake	**Vous pouvez tout de même :** • Stocker les données des journaux pour une période de grâce de 30 jours, après quoi ils sont supprimés. • Transférer les journaux au lac de données Cortex jusqu'à la fin de la période de grâce de 30 jours.
GlobalProtect	**Vous pouvez tout de même :** • Utiliser l'application pour les terminaux exécutant Windows et macOS. • Configurer des passerelles internes uniques ou multiples. **Vous ne pouvez plus :** • Accéder à l'application Linux OS et à l'application mobile pour iOS, Android, Chrome OS et les applications UWP de Windows 10. • Utiliser IPv6 pour les passerelles externes. • Exécuter des vérifications HIP. • Utiliser le VPN sans client. • Appliquez la segmentation des tunnels en fonction du domaine de destination, du processus client ou de l'application de diffusion vidéo en continu.
Assistance	**Vous ne pouvez plus :** • Recevoir les mises à jour logicielles. • Télécharger les images de VM. • Recevoir l'aide du soutien technique.

©2023 Palo Alto Networks, Inc.

Licences pour les fournisseurs de services de sécurité cloud (CSSP)

Le programme de partenaires CSSP de Palo Alto Networks permet aux fournisseurs de services de fournir une sécurité en tant que service ou en tant qu'application hébergée à leurs clients finaux. Les offres de licence que Palo Alto Networks fournit aux partenaires autorisés du fournisseur de services Cloud Security (CSSP) sont différentes des offres destinées aux utilisateurs professionnels.

Pour les partenaires CSSP, Palo Alto Networks prend en charge un modèle basé sur l'utilisation pour les pare-feu VM-Series regroupés avec les abonnements et le support. Les partenaires CSSP peuvent combiner une licence de capacité à durée déterminée pour les modèles VM-Series avec un choix de licences d'abonnement pour la prévention des menaces, le filtrage des URL, AutoFocus, GlobalProtect et WildFire, et les autorisations de support qui permettent d'accéder au support technique et aux mises à jour logicielles. Si vous envisagez de déployer les pare-feu dans une configuration haute disponibilité, vous pouvez acheter l'option haute disponibilité rentable.

- Obtention des codes d'autorisation pour les ensembles de licence CSSP
- Enregistrement du pare-feu VM-Series avec un code d'autorisation CSSP
- Ajout d'informations sur le client final pour un pare-feu VM-Series enregistré

Obtention des codes d'autorisation pour les ensembles de licence CSSP

Pour devenir partenaire CSSP, vous devez vous inscrire au programme des partenaires CSSP de Palo Alto Networks. Pour plus d'informations sur l'inscription au programme CSSP, contactez votre directeur commercial Palo Alto Networks. Si vous êtes inscrit, le portail de support Palo Alto Network fournit des outils qui vous permettent de sélectionner un ensemble de licences, de suivre l'utilisation des licences et d'appliquer les droits de licence.

Un ensemble de licence est une combinaison des options suivantes :

- Conditions d'utilisation : les options de paiement à l'utilisation sont les suivantes : horaire, mensuel, 1 an et 3 ans.
- Modèle de pare-feu VM-Series : les modèles VM-100, VM-200, VM-300 et VM-1000-HV qui vous donnent le numéro de modèle et les capacités associés à chaque modèle.
- Forfait d'abonnement : les trois options sont base, forfait 1 et forfait 2. L'option de base n'inclut aucun abonnement. Le forfait 1 présente la licence Threat Prevention qui inclut IPS, AV, la prévention contre les logiciels malveillants. Le forfait 2 dispose des licences Threat Prevention (notamment IPS, AV, prévention contre les logiciels malveillants), DNS Security, GlobalProtect, WildFire et PAN-DB URL Filtering.
- Niveau de support : support premium ou support en ligne arrière.
- Pare-feu redondants : l'option est soit haute disponibilité (HA) ou sans HA. Cette option est rentable si vous prévoyez de déployer une paire de pare-feu redondants.

L'offre PAN-VM-300-SP-PREM-BND1-YU, par exemple, est un forfait d'un an qui inclut le VM-300 avec un support premium et le forfait d'abonnement 1. Chaque ensemble prend en charge jusqu'à 10 000 instances du pare-feu VM-Series.

©2023 Palo Alto Networks, Inc.

Après avoir sélectionné votre ensemble de licence, vous recevez un e-mail avec votre code d'autorisation.Le processus d'exécution peut prendre jusqu'à 48 heures.

STEP 1 | Connectez-vous au site Web d'assistance client de Palo Alto Networks avec vos identifiants de compte. Si vous devez créer un nouveau compte, reportez-vous à la section Création d'un compte de support.

STEP 2 | Sélectionnez **CSSP** > **Order History (Historique des commandes)** pour consulter la liste des codes d'autorisation enregistrés dans votre compte de support.

Lorsque vous déployez des pare-feu, vous devez enregistrer chaque instance du pare-feu avec un code d'autorisation.

Enregistrement du pare-feu VM-Series avec un code d'autorisation CSSP

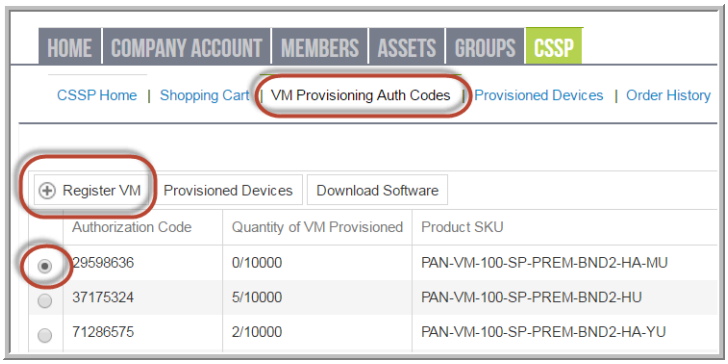
Pour activer la licence sur votre pare-feu VM-Series, vous devez d'abord le déployer, puis effectuer la configuration initiale. En tant que partenaire CSSP, vous pouvez choisir parmi les options suivantes pour enregistrer un pare-feu :

- API : utilisez l'API de licence si vous avez un script personnalisé ou un service d'orchestration. Avec cette option, le pare-feu n'a pas besoin d'un accès direct à Internet.
- Amorçage : utilisez cette option pour configurer automatiquement le pare-feu et le mettre sous licence au premier démarrage. Reportez-vous à la section Amorçage du pare-feu VM-Series.
- Interface Web du pare-feu : vous pouvez activer la licence pour le pare-feu VM-Series (version autonome) en utilisant l'interface Web du pare-feu. Ce flux de travail est valide pour les pare-feu avec ou sans accès à Internet.
- Portail de support client : utilisez cette option pour enregistrer manuellement le pare-feu sur le portail de support client de Palo Alto Networks, comme illustré ci-dessous.

STEP 1 | Connectez-vous au site Web d'assistance client de Palo Alto Networks avec vos identifiants de compte. Si vous devez créer un nouveau compte, reportez-vous à la section Création d'un compte de support.

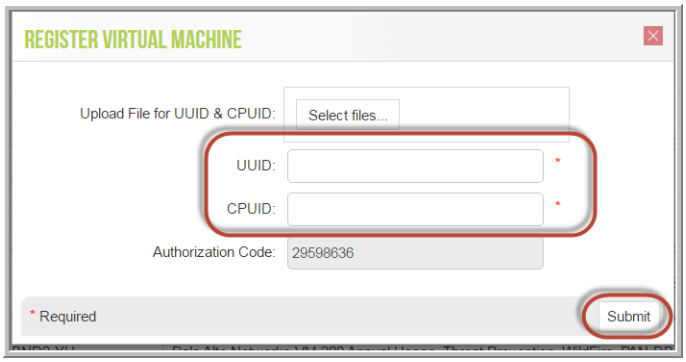
STEP 2 | Sélectionnez **CSSP** > **Order History (Historique des commandes)** pour consulter la liste des codes d'autorisation enregistrés dans votre compte de support.

STEP 3 | Sélectionnez **CSSP** > **VM Provisioning Auth Codes (Codes d'autorisation de provisionnement VM)**, sélectionnez un **Authorization Code (Code d'autorisation)** et cliquez sur **Register VM (Enregistrer la machine virtuelle)**.



 ©2023 Palo Alto Networks, Inc.

STEP 4 | Entrez l'**UUID** et le **CPUID** de l'instance VM et cliquez sur **Submit (Envoyer)**. Le portail génèrera un numéro de série pour le pare-feu.



Vous pouvez suivre le nombre de pare-feu VM-Series déployés et le nombre de licences encore disponibles pouvant être utilisées par rapport à chaque code d'autorisation. Pour afficher le nombre total de pare-feu enregistrés en fonction d'un code d'autorisation spécifique, sélectionnez ***CSSP > VM Provisioning Auth Codes (Codes d'autorisation de provisionnement VM)****, puis sélectionnez un* ***Authorization Code (Code d'autorisation)*** *et cliquez sur* ***Provisioned Devices (Appareils provisionnés)****.*

Ajout d'informations sur le client final pour un pare-feu VM-Series enregistré

Pour les détenteurs de licence CSSP, après avoir enregistré le pare-feu, vous pouvez utiliser le portail de support de Palo Alto Networks ou l'API de mise sous licence pour lier le numéro de série du pare-feu VM-Series au client pour lequel vous avez provisionné le pare-feu.

- Ajout d'informations sur le client final pour un pare-feu VM-Series enregistré (portail de support client). Le portail de support s'authentifie avec le nom d'utilisateur et le mot de passe.
- Ajout d'informations sur le client final pour un pare-feu VM-Series enregistré (API). L'API s'authentifie à l'aide de la clé API de mise sous licence.

Ajout d'informations sur le client final pour un pare-feu VM-Series enregistré (portail de support client)

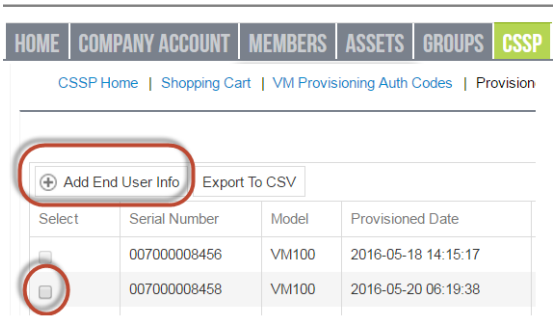
Effectuez la procédure suivante pour ajouter des informations sur le client final pour un pare-feu enregistré via le Portail assistance clientèle.

STEP 1 | Connectez-vous au site Web d'assistance client de Palo Alto Networks avec vos identifiants de compte.

STEP 2 | Sélectionnez **CSSP** > **Provisioned Devices (Périphériques provisionnés)**.

©2023 Palo Alto Networks, Inc.

STEP 3 | Sélectionnez le **Serial Number (Numéro de série)** et cliquez sur **Add End User Info (Ajouter des informations sur l'utilisateur final)**.

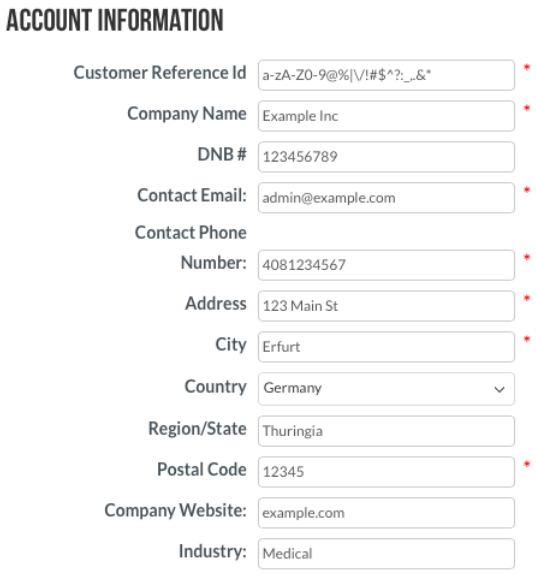


 ©2023 Palo Alto Networks, Inc.

STEP 4 | Saisissez les **Account Information (Informations sur le compte)** pour le client comme suit.

- Customer Reference Id (ID de référence du client) : requis
- Company Name (Nom de l'entreprise) : requis
- DNB # (N° DNB) : numéro du système de numérotation universel des données (DUNS)
- Contact Email (E-mail de contact) : requis, adresse e-mail de l'utilisateur final
- Contact Phone Number (Numéro de téléphone de contact) : numéro de téléphone de l'utilisateur final
- Address (Adresse) : requis, adresse de l'utilisateur final
- Country (Pays) : requis, code pays à deux lettres ISO
- City (Ville) : requis, nom de la ville de l'utilisateur final
- Region/State (Région/État) : requis ; pour les États-Unis et le Canada, vous devez entrer un code de subdivision à deux lettres ISO ; pour tous les autres pays, toute chaîne de texte est valide
- Postal Code (Code postal) : requis, code postal de l'utilisateur final
- Company Website (Site Web de l'entreprise) : URL du site Web de l'utilisateur final
- Industry (Secteur) : secteur d'activité de l'utilisateur final, tel que la mise en réseau ou la consultation

Cliquez sur **Submit (Envoyer)** pour enregistrer les détails.



*Après avoir ajouté des informations de compte, vous pouvez trouver tous les pare-feu enregistrés auprès d'un client. Dans **Search Existing End User (Rechercher un utilisateur final existant)**, entrez l'ID ou le nom du client et cliquez sur **Search (Rechercher)** pour trouver tous les pare-feu provisionnés pour le client.*

Ajout d'informations sur le client final pour un pare-feu VM-Series enregistré (API)

L'URL pour accéder à l'API est https://api.paloaltonetworks.com/api/license/ReportEndUserInfo.

 ©2023 Palo Alto Networks, Inc.

Une demande d'API doit utiliser la méthode HTTP POST et vous devez inclure les en-têtes des requêtes HTTP qui incluent la clé API et spécifier le type de contenu en tant que JSON. Les réponses de l'API sont au format JSON.

STEP 1 | Obtenez votre clé API de mise sous licence.

STEP 2 | Utilisez l'API ReportEndUserInfo pour ajouter des informations sur l'utilisateur final pour un pare-feu VM-Series enregistré auprès d'un CSSP.

URL : **`https://api.paloaltonetworks.com/api/license/ReportEndUserInfo`**

En-têtes :

- Content-Type : application/json
- apiKey : *clé API*

Paramètres :

- `SerialNumbers` : requis, fournissez au moins un numéro de série de pare-feu valide
- `CustomerReferenceId` : requis
- `CompanyName` : requis, nom de l'entreprise de l'utilisateur final
- `DnBNumber` : numéro du système de numérotation universel des données (DUNS)
- `PhoneNumber` : numéro de téléphone de l'utilisateur final
- `EndUserContactEmail` : requis, adresse e-mail de l'utilisateur final
- `Address` : requis, adresse de l'utilisateur final
- `Country` : requis, code pays à deux lettres ISO
- `City` : requis, nom de la ville de l'utilisateur final
- `Region/State` : requis ; pour les États-Unis et le Canada, vous devez entrer un code de subdivision à deux lettres ISO ; pour tous les autres pays, toute chaîne alpha est valide
- `PostalCode` : requis, code postal de l'utilisateur final
- `Industry` : secteur d'activité de l'utilisateur final, tel que la mise en réseau ou la consultation
- `WebSite` : URL du site Web de l'utilisateur final
- `CreatedBy` : système ou personne soumettant cette information

Exemple de demande d'ajout d'informations sur l'utilisateur final pour un pare-feu VM-Series enregistré à l'aide de Curl :

```
curl -X POST "http://api.paloaltonetworks.com/api/license/
ReportEndUserInfo" \-H "Content-Type: application/json" \-
H "apikey: your_key_here" \--data-raw '{ "SerialNumbers":
 ["0001A101234"], "CustomerAccountId": 12345, "CompanyName":
 "ExampleInc", "DnBNumber": "123456789", "Address": "123 Main St",
 "City": "Sunnydale", "Region": "CA", "State": "CA", "Country":
 "US", "PostalCode": "12345", "Industry": "Medical", "PhoneNumber":
```

 ©2023 Palo Alto Networks, Inc.

```
 "4081234567", "WebSite": "example.com", "EndUserContactEmail":
 "admin@example.com", "CreatedBy": "Jane Doe"}'
```

Exemple de réponse de l'API :

```
"{"Message": "End User Information Updated Successfully"}"
```

Si vous recevez une erreur, consultez la section Codes d'erreur de l'API de mise sous licence.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

Configuration d'un pare-feu VM-Series sur un serveur ESXi

Le pare-feu VM-Series est distribué au format Open Virtualization Alliance (OVA), devenu la norme en matière de configuration en package et de déploiement de machines virtuelles. Vous pouvez installer cette solution sur tout appareil x86 capable d'exécuter VMware ESXi.

Afin de déployer un pare-feu VM-Series, vous devez maîtriser VMware et vSphere, y compris la mise en réseau vSphere, l'installation et la configuration de l'hôte ESXi et le déploiement de la machine virtuelle invitée.

Si vous souhaitez automatiser le processus de déploiement d'un pare-feu VM-Series, vous pouvez créer un modèle standard or comportant la configuration optimale et les politiques, et utiliser l'API vSphere et l'API XML PAN-OS pour déployer rapidement de nouveaux pare-feu VM-Series sur votre réseau.

Pour plus d'informations, reportez-vous aux rubriques suivantes :

- Déploiements pris en charge sur VMware vSphere Hypervisor (ESXi)
- VM-Series sur système ESXi : configuration système requise et limitations
- Installation d'un pare-feu VM-Series sur VMware vSphere Hypervisor (ESXi)
- VM Monitoring sur vCenter
- Résolution des problèmes de déploiement ESXi
- Réglage des performances de VM-Series pour ESXi

Déploiements pris en charge sur VMware vSphere Hypervisor (ESXi)

Vous pouvez déployer une ou plusieurs instances du pare-feu VM-Series sur le serveur ESXi. Positionnez le pare-feu VM-Series sur le réseau en fonction de votre topologie. Choisissez parmi les options suivantes (pour les environnements n'utilisant pas VMware NSX) :

- **Un pare-feu VM-Series par hôte ESXi** : chaque serveur de machine virtuelle sur l'hôte ESXi passe par le pare-feu avant de quitter l'hôte pour le réseau physique. Les serveurs de machine virtuelle sont reliés au pare-feu via des commutateurs virtuels standard. Les serveurs invités n'ont aucune autre connectivité réseau. Par conséquent, le pare-feu a la visibilité et le contrôle sur tout le trafic quittant l'hôte ESXi. Une variante de ce cas pratique est d'exiger également que tout le trafic passe par le pare-feu, y compris le trafic de serveur à serveur (trafic est-ouest) sur le même hôte ESXi.
- **Un pare-feu VM-Series par réseau virtuel** : déployez un pare-feu VM-Series pour chaque réseau virtuel. Si vous avez conçu votre réseau de telle manière qu'un ou plusieurs hôtes ESXi disposent d'un groupe de machines virtuelles appartenant au réseau interne, d'un groupe appartenant au réseau externe et d'autres au réseau DMZ, vous pouvez déployer un pare-feu VM-Series pour protéger les serveurs de chaque groupe. Si un groupe ou un réseau virtuel ne partage aucun commutateur virtuel ou groupe de ports avec les autres réseaux virtuels, il est complètement isolé de tous les autres réseaux virtuels sur ou entre les hôtes. Comme il n'existe aucun autre chemin d'accès virtuel ou physique aux autres réseaux, les serveurs de chaque réseau virtuel doivent utiliser le pare-feu pour communiquer avec les autres réseaux. Le pare-feu a la visibilité et le contrôle sur tout le trafic laissant le commutateur virtuel (standard ou distribué) attaché à chaque réseau virtuel.
- **Environnement hybride** : les hôtes physiques et virtuels sont utilisés. Le pare-feu VM-Series peut remplacer un appareil de pare-feu physique dans un emplacement d'agrégation traditionnel. Un environnement hybride offre les avantages d'une plate-forme de serveur commune pour tous les périphériques et supprime les dépendances de mise à niveau matérielle et logicielle.

Poursuivez en vous reportant aux sections VM-Series sur système ESXi : configuration système requise et limitations et Installation d'un pare-feu VM-Series sur VMware vSphere Hypervisor (ESXi).

 ©2023 Palo Alto Networks, Inc.

VM-Series sur système ESXi : configuration système requise et limitations

Cette section décrit la configuration requise et les limitations du pare-feu VM-Series sur VMware vSphere Hypervisor (ESXi). Pour déployer le pare-feu VM-Series, reportez-vous à la section Installation d'un pare-feu VM-Series sur VMware vSphere Hypervisor (ESXi).

- VM-Series sur système ESXi : configuration système requise
- VM-Series sur système ESXi : limitations

VM-Series sur système ESXi : configuration système requise

Vous pouvez créer et déployer plusieurs instances du pare-feu VM-Series sur un serveur ESXi. Comme chaque instance du pare-feu requiert une allocation minimum des ressources (nombre de processeurs, mémoire et espace disque) sur le serveur ESXi, assurez-vous de vous conformer aux spécifications ci-dessous pour obtenir des performances optimales.

Le pare-feu VM-Series possède les exigences suivantes :

- Le processeur de l'hôte doit être un processeur x86 Intel ou AMD avec extension de virtualisation.
- Consultez la matrice de compatibilité pour connaître les versions de ESXi prises en charge. La prise en charge de la version vmx repose sur l'OVA que vous utilisez pour déployer le pare-feu VM-Series. Vous ne pouvez pas modifier cette version. La mise à niveau ou la rétrogradation de la version du logiciel VM-Series ne modifie pas la version de vmx activée au lancement.
- Reportez-vous à la section Configuration système requise pour VM-Series pour la configuration matérielle minimale requise pour votre modèle VM-Series.
- Au moins deux interfaces de réseau (CNRV). Un vmNIC dédié pour l'interface de gestion et l'autre pour l'interface de données. Il est possible d'ajouter jusqu'à huit vmNIC supplémentaires pour le trafic de données. Pour des interfaces supplémentaires, utilisez VGT (VLAN Guest Tagging) sur le serveur ESXi ou configurez des sous-interfaces sur le pare-feu.

  Les adresses MAC attribuées à l'hyperviseur sont activées par défaut. vSphere attribue une adresse MAC vmNIC unique à chaque interface du dataplane du pare-feu VM-Series. Si vous désactivez les adresses MAC affectées à l'hyperviseur, le pare-feu VM-Series attribue à chaque interface une adresse MAC à partir de son propre pool. Dans la mesure où les adresses MAC de chaque interface diffèrent, vous devez activer le mode de proximité sur le groupe de ports du commutateur virtuel auquel les interfaces du dataplane du pare-feu sont attachées. Cela permet au pare-feu de recevoir des trames (référez-vous à Provisionner le pare-feu VM-Series sur un serveur ESX). Si le mode de proximité ni l'adresse MAC attribuée par l'hyperviseur n'est activé, le pare-feu ne recevra aucun trafic. Cela est dû au fait que vSphere ne transfère pas les trames à une machine virtuelle lorsque l'adresse MAC de destination de l'image et l'adresse MAC vmNIC ne correspondent pas.
- Le kit de développement du dataplane (DPDK) est activé par défaut sur les pare-feu VM-Series sur ESXi. Pour plus d'informations sur DPDK, reportez-vous à la section Activation de DPDK sur ESXi.

©2023 Palo Alto Networks, Inc.

- Pour optimiser les performances du pare-feu VM-Series, vous pouvez apporter les modifications suivantes à l'hôte avant de déployer le pare-feu VM-Series. Reportez-vous à la section Réglage des performances de VM-Series pour ESXi pour plus d'informations.
  - **Activez DPDK**. DPDK permet à l'hôte de traiter les paquets plus rapidement en contournant le noyau Linux. Au lieu de cela, les interactions avec la carte réseau sont effectuées à l'aide des pilotes et des bibliothèques DPDK.
  - **Activez SR-IOV**. La virtualisation d'E/S racine unique (SR-IOV) permet à un périphérique physique PCIe unique sous un port racine unique d'apparaître comme plusieurs périphériques physiques distincts de l'hyperviseur ou de l'invité.

    Ne configurez pas un vSwitch sur le port physique sur lequel vous activez SR-IOV. Pour communiquer avec l'hôte ou d'autres machines virtuelles sur le réseau, le pare-feu VM-Series doit avoir un accès exclusif au port physique et aux fonctions virtuelles associées (VF) sur cette interface.
  - **Activez la prise en charge de files d'attente multiples pour les cartes d'interface réseau**. Les files d'attente multiples permettent aux performances du réseau d'évoluer avec le nombre de processeurs virtuels et permet le traitement parallèle des paquets en créant plusieurs files d'attente TX et RX.

VM-Series sur système ESXi : limitations

Les fonctionnalités du pare-feu VM-Series sont similaires à celles des pare-feu matériels Palo Alto Networks, mais avec les limitations suivantes :

- N'utilisez pas la fonction d'instantanés sur le pare-feu VM-Series sur ESXi. Les instantanés peuvent avoir un impact sur les performances et entraîner une perte de paquets intermittente et incohérente. Consultez la recommandation de VMware relative aux meilleures pratiques pour l'utilisation des instantanés.

  Si vous avez besoin de copies de sauvegarde de configuration, utilisez Panorama ou depuis le pare-feu utilisez **Export named configuration snapshot (Exporter l'instantané de configuration nommé)** (Device (Périphérique) > Configuration > Operations (Opérations)). En utilisant **Export named configuration snapshot (Exporter l'instantané de configuration nommé)** vous exportez la configuration active (`running-config.xml`) du pare-feu et vous pouvez l'enregistrer dans un emplacement réseau.
- Des cœurs de processeurs dédiés sont recommandés.
- La surveillance de la liaison HA n'est pas prise en charge sur les pare-feu VM-Series sur ESXi. Utilisez la surveillance des chemins pour vérifier la connexion à une adresse IP cible ou à l'adresse IP de saut suivant.
- Jusqu'à 10 ports peuvent être configurés ; il s'agit d'une limitation VMware. Un port est utilisé pour le trafic de gestion et jusqu'à 9 peuvent être utilisés pour le trafic de données.
- Seul le pilote vmxnet3 est pris en charge.
- Les systèmes virtuels ne sont pas pris en charge.
- Le vMotion du pare-feu VM-Series est pris en charge sur vSphere 6.5, 6.7 et 7.0 si les hôtes ESXi ont une configuration de processeur homogène. PAN-OS 9.1.6 et version ultérieure est nécessaire pour Utilisation de vMotion pour déplacer le pare-feu VM-Series entre les hôtes installé sur vSphere 6.5 ou 6.7.

 ©2023 Palo Alto Networks, Inc.

- Le mode de proximité et de fausse transmission doit être activé sur les groupes de ports vSwitch ESXi connectés aux interfaces de couche 2 et vwire sur le pare-feu VM-Series.
- Pour utiliser des périphériques PCI avec le pare-feu VM-Series sur ESXi, les E/S mappées en mémoire (MMIO) doivent être inférieures à 4 Go. Vous pouvez désactiver les MMIO supérieures à 4 Go dans le BIOS de votre serveur. Il s'agit d'une limitation propre à ESXi.
- Lors de l'utilisation d'ESXi 7.0, les interfaces n'apparaissent pas lorsque l'on associe des VF à des machines virtuelles avec relais de périphérique PCI.

©2023 Palo Alto Networks, Inc.

Installation d'un pare-feu VM-Series sur VMware vSphere Hypervisor (ESXi)

Pour installer un pare-feu VM-Series vous devez avoir accès au modèle OVA (Open Virtualization Alliance). Utilisez le code d'autorisation contenu dans l'e-mail de confirmation de commande que vous avez reçu pour enregistrer votre pare-feu VM-Series et téléchargez le modèle OVA. Le modèle OVA est une archive zip qui contient trois types de fichiers :

- .mf: Fichier manifeste MF contenant les condensés SHA-1 des fichiers individuels du package
- .ovf: Fichier descripteur OVF contenant toutes les métadonnées du package et de son contenu
- .vmdk: Fichier image du disque virtuel qui contient la version virtualisée du pare-feu.

Exécutez les tâches suivantes pour installer et configurer le pare-feu VM-Series sur ESXi.

- Planification des interfaces pour VM-Series pour ESXi
- Configuration du pare-feu VM-Series sur un serveur ESXi
- Configuration initiale sur le VM-Series sur ESXi
- (Facultatif) Ajout d'espace disque supplémentaire au pare-feu VM-Series
- Utilisation de VMware Tools sur le pare-feu VM-Series sur ESXi et vCloud Air
- Utilisation de vMotion pour déplacer le pare-feu VM-Series entre les hôtes
- Utilisation de la CLI du VM-Series pour permuter l'interface de gestion sur ESXi

Planification des interfaces pour VM-Series pour ESXi

En planifiant le mappage des vNIC (cartes réseau virtuelles) et des interfaces du pare-feu VM-Series, vous pouvez éviter les redémarrages et les problèmes de configuration. Le tableau suivant décrit le mappage par défaut entre les vNIC VMware et les interfaces VM-Series lorsque les 10 vNIC sont activées sur ESXi.

vNIC VMware	Interfaces VM-Series
1	Ethernet 1/0 (mgmt)
2	Ethernet 1/1 (eth1)
3	Ethernet 1/2 (eth2)
4	Ethernet 1/3 (eth3)
5	Ethernet 1/4 (eth4)
6	Ethernet 1/5 (eth5)
7	Ethernet 1/6 (eth6)

©2023 Palo Alto Networks, Inc.

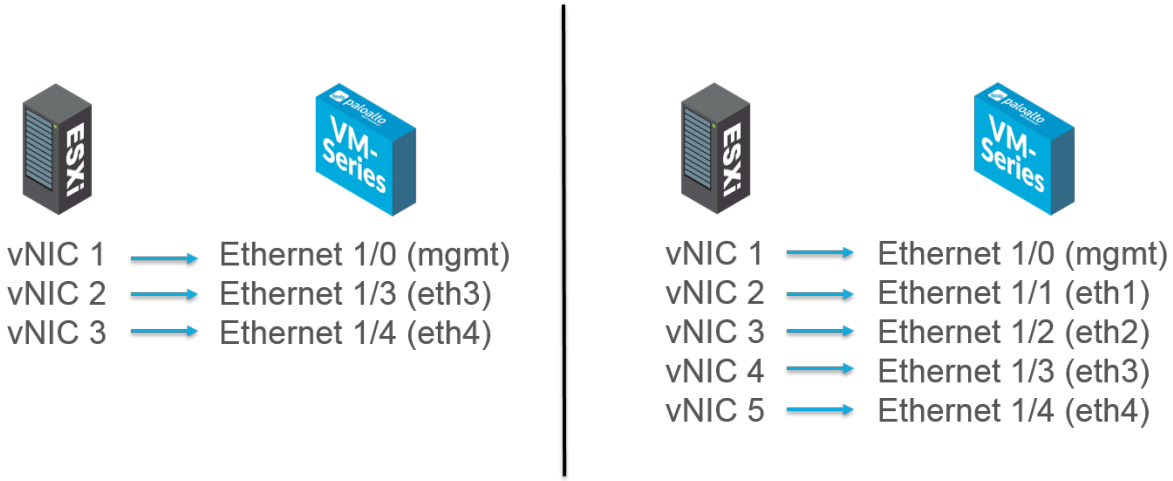
vNIC VMware	Interfaces VM-Series
8	Ethernet 1/7 (eth7)
9	Ethernet 1/8 (eth8)
10	Ethernet 1/9 (eth9)

Le mappage sur le pare-feu VM-Series reste le même, quels que soient les vNIC que vous ajoutez sur ESXi. Les interfaces que vous activez sur le pare-feu prennent toujours la prochaine version de vNIC disponible sur ESXi.

Dans le diagramme suivant, eth3 et eth4 sur le pare-feu VM-Series sont associés aux cartes vNIC 2 et 3 sur ESXi, et eth1 et eth2 sont non mappés, comme indiqué à gauche.

Si vous souhaitez ajouter deux interfaces supplémentaires tout en conservant le mappage actuel, activez les vNIC 4 et 5 et redémarrez le pare-feu. Le mappage vNIC existant est conservé car vous avez ajouté les interfaces après l'interface de dernier mappage.

Si vous activez eth1 et eth2 sur le pare-feu VM-Series, les interfaces se réordonnent comme indiqué sur la droite, ce qui entraîne une non-concordance de mappage affectant le trafic.



Pour éviter les problèmes tels que ceux décrits dans l'exemple précédent, vous pouvez effectuer les opérations suivantes :

- Lorsque vous configurez votre hôte ESXi pour la première fois, activez tous les neuf vNIC au-delà du premier. L'ajout des neuf cartes vNIC en tant qu'espaces réservés avant la mise sous tension du pare-feu VM-Series vous permet d'utiliser toutes les interfaces de VM-Series, quel que soit leur ordre.
- Si toutes les cartes vNIC sont actives, l'ajout d'interfaces supplémentaires ne nécessite plus de redémarrage. Parce que chaque vNIC sur ESXi requiert que vous choisissiez un réseau, vous pouvez créer un groupe de ports vide en tant qu'espace réservé réseau.
- Ne supprimez pas les vNIC de pare-feu VM-Series pour éviter les incompatibilités de mappage.

©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur un serveur ESXi

Suivez ces instructions pour déployer le pare-feu VM-Series sur un serveur ESXi (autonome). Pour déployer le pare-feu de l'édition NSX VM-Series, consultez Configuration du pare-feu VM-Series sur VMware NSX-T.

STEP 1 | Téléchargez le fichier OVA.

Enregistrez votre pare-feu VM-Series et obtenez le fichier OVA sur le site Internet d'assistance client de Palo Alto Networks.

Le fichier OVA contient les fichier d'installation de base. Une fois l'installation de base terminée, vous devez télécharger et installer la dernière version de PAN-OS à partir du portail d'assistance. Cela garantit que vous disposez des derniers correctifs implémentés depuis la création de l'image de base. Pour obtenir des instructions, reportez-vous à la section Mise à niveau de la version du logiciel PAN-OS (version autonome)*.*

STEP 2 | Avant de déployer le fichier OVA, configurez les commutateurs standard virtuels et les commutateurs distribués virtuels dont vous avez besoin pour le pare-feu VM-Series.

Si vous déployez le pare-feu VM-Series avec des interfaces de couche 3, votre pare-feu utilisera les adresses MAC attribuées par l'hyperviseur *par défaut. Si vous choisissez de désactiver l'adresse MAC assignée à l'hyperviseur, ou si vous déployez le pare-feu avec la couche 2, le fil virtuel ou les interfaces d'écoute, vous devez configurer (configurer à* ***Accepter****) tout commutateur virtuel fixé au coupe-feu de la série VM pour permettre les modes suivants : mode simple, changements d'adresse MAC et messages transmis forgés.*

Configurer un commutateur standard virtuel ou un commutateur réparti virtuel pour recevoir les cadres du pare-feu de la série VM.

Commutateur virtuel standard

1. Rendez-vous à **Home (Page d'accueil)** > **Hosts and Clusters (Hôtes et clusters)** et sélectionnez un hôte.
2. Cliquez sur l'onglet **Configure (Configurer)** et voir **Virtual Switches**. Pour chaque pare-feu de série VM relié à un commutateur virtuel, cliquez sur **Properties (Propriétés)**.
3. Sélectionnez un groupe de ports correspondant à un commutateur virtuel et cliquez sur **Edit Settings (Modifier les paramètres)**. Dans les propriétés vSwitch, cliquez sur l'onglet **Security (Sécurité)**, définissez **Promiscuous Mode (Mode de proximité), MAC Address Changes (Modifications d'adresse MAC)** et **Forged Transmits (Fausses transmissions)** sur **Accept (Accepter)**, puis cliquez **OK**. Cette modification se propage à tous les groupes de ports sur le commutateur virtuel.

Commutateur virtuel distribué

1. Sélectionnez **Home (Page d'accueil)** > **Networking (Mise en réseau)**. Sélectionnez votre commutateur réparti virtuel et mettez en surbrillance le **Distributed Port Group (groupe de ports distribués)** que vous voulez modifier.
2. Cliquez sur **Edit Settings (Modifier les paramètres)**, sélectionnez **Policies (Politiques)** > **Sécurité (Security)**, définissez **Promiscuous (Mode de proximité), MAC Address Changes**

©2023 Palo Alto Networks, Inc.

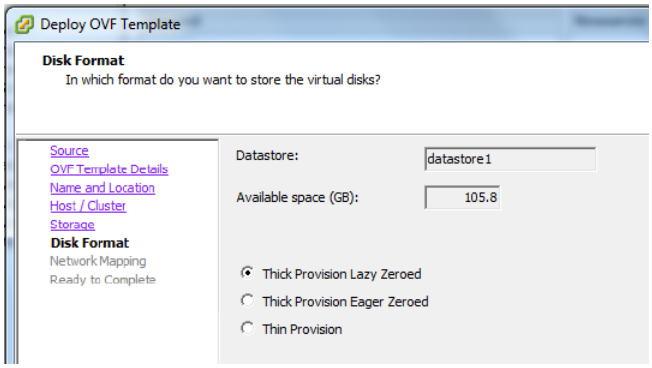
(Modifications d'adresse MAC) et **Forged Transmits (Fausses transmissions)** sur **Accepter (Accept)**, puis cliquez **OK**.

STEP 3 | Déployez l'OVA.

Si vous ajoutez des interfaces supplémentaires (vmNIC) au pare-feu VM-Series, vous devez redémarrer (car de nouvelles interfaces sont détectées pendant le cycle de démarrage). Pour réduire le besoin de redémarrer le pare-feu, activez les interfaces lors du déploiement initial ou lors d'une fenêtre de maintenance.

*Pour voir la progression de l'installation, surveillez la liste **Recent Tasks (Tâches récentes)**.*

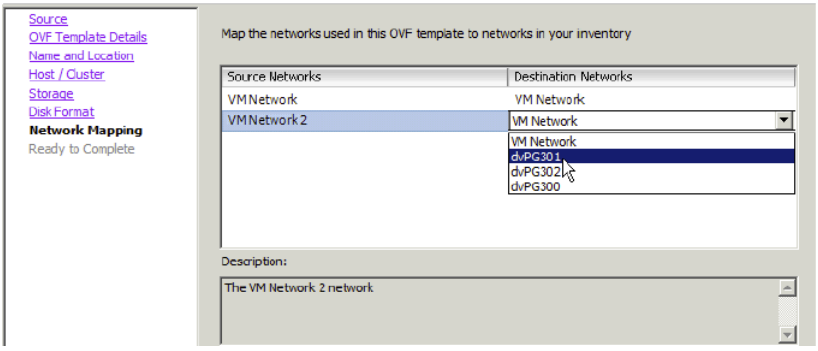
1. Connectez-vous à vCenter à l'aide du client vSphere. Il est également possible d'accéder directement à l'hôte ESXi cible, si besoin.
2. À partir du client Web vSphere, allez à **Hosts and Clusters**, cliquez à droite sur votre hôte et sélectionnez **Deploy OVF Template**.
3. Accédez au fichier OVA que vous avez téléchargé précédemment. Sélectionnez le fichier, puis cliquez sur **Next (Suivant)**. Vérifiez les détails du modèle, puis cliquez sur **Next (Suivant)**.
4. Donnez un nom à l'instance du pare-feu VM-Series et, dans la fenêtre **Inventory Location (Emplacement d'inventaire)**, sélectionnez un centre de données et un dossier, puis cliquez sur **Next (Suivant)**
5. Sélectionnez un hôte ESXi pour le pare-feu VM-Series et cliquez sur **Next (Suivant)**.
6. Sélectionnez le magasin de données à utiliser pour le pare-feu VM-Series et cliquez sur **Next (Suivant)**.
7. Conservez les paramètres par défaut pour le provisionnement du magasin de données et cliquez sur **Next (Suivant)**. L'option par défaut est **Thick Provision Lazy Zeroed (Allocation statique avec mise à zéro tardive)**.



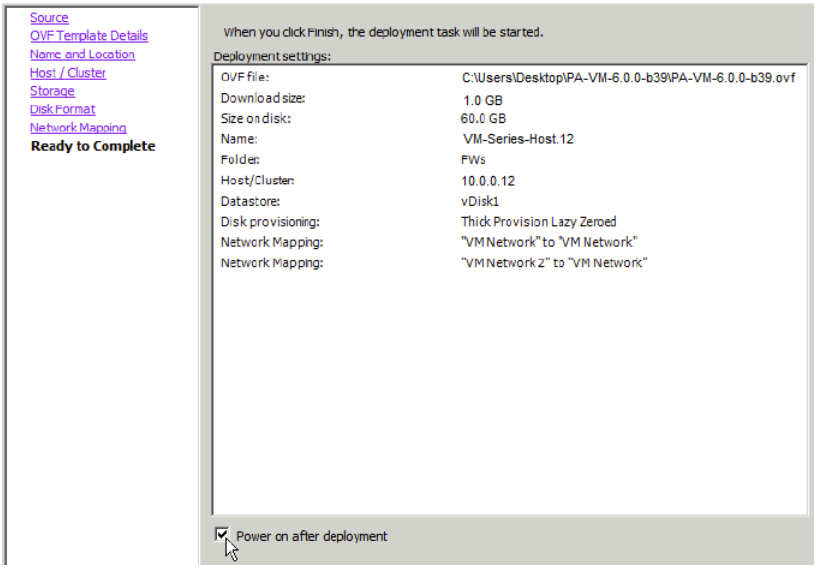
8. Sélectionnez les réseaux à utiliser pour les deux premières vmNIC. Le premier vmNIC est utilisé pour l'interface de gestion et le second vmNIC pour le premier port de données.

 ©2023 Palo Alto Networks, Inc.

Vérifiez que les **Source Networks (Réseaux sources)** sont mappés aux bons **Destination Networks (Réseaux de destination)**.



9. Vérifiez les détails, cochez la case **Power on after deployment (Mise sous tension après le déploiement)**, puis cliquez sur **Next (Suivant)**.



10. Une fois le déploiement terminé, cliquez sur l'onglet **Summary (Récapitulatif)** pour afficher le statut actuel.

Configuration initiale sur le VM-Series sur ESXi

Utilisez la console d'appareil virtuel sur le serveur ESXi pour configurer l'accès réseau au pare-feu VM-Series. Par défaut, le pare-feu VM-Series utilise DHCP pour obtenir une adresse IP pour l'interface de gestion, mais vous pouvez également attribuer une adresse IP statique. Une fois la configuration initiale terminée, accédez à l'interface Web pour effectuer d'autres tâches de configuration. Si vous utilisez Panorama pour la gestion centralisée, reportez-vous au Guide de l'administrateur Panorama pour plus d'informations sur la gestion du périphérique à l'aide de Panorama.

Si vous utilisez l'amorçage pour effectuer la configuration de votre pare-feu VM-Series sur ESXi, reportez-vous à la section Amorçage du pare-feu VM-Series sur ESXi.

Pour plus d'informations sur l'amorçage, reportez-vous à la section Amorçage du pare-feu VM-Series.

 ©2023 Palo Alto Networks, Inc.

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

- Adresse IP du port MGT
- netmask
- Passerelle par défaut
- Adresse IP du serveur DNS

STEP 2 | Accédez à la console du pare-feu VM-Series.

1. Cliquez sur l'onglet **Console** sur le serveur ESXi pour le pare-feu VM-Series, ou faites un clic droit dur le pare-feu VM-Series et sélectionnez **Open Console (Ouvrir la console)**.
2. Appuyez sur Entrée pour accéder à l'écran de connexion.
3. Saisissez le nom d'utilisateur/mot de passe (admin/admin) par défaut pour vous connecter.
4. Entrer **`configurer`** pour passer en mode de configuration.

STEP 3 | Configurez les paramètres d'accès réseau pour l'interface de gestion.

Entrez les commandes suivantes :

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> netmask <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

STEP 4 | Validez vos modifications et quittez le mode Configuration.

Saisissez **`commit`**.

Saisissez **`exit`**.

STEP 5 | Vérifiez l'accès réseau aux services externes nécessaire à la gestion de pare-feu, notamment au serveur de mise à jour Palo Alto Networks.

1. Utilisez l'utilitaire Ping pour vérifier la connectivité réseau au serveur Palo Alto Networks Update, comme illustré dans l'exemple suivant. Vérifiez que la résolution DNS se produit et que la réponse inclut l'adresse IP du serveur de mise à jour (le serveur de mise à jour ne répond pas aux requêtes ping.) Après avoir vérifié la résolution DNS, appuyez sur Ctrl + C pour arrêter la requête ping.

```
admin@PA-220 > ping host updates.paloaltonetworks.com
```

```
PING updates.paloaltonetworks.com (10.101.16.13) 56(84)
 bytes of data. From 192.168.1.1 icmp_seq=1 Destination Host
 Unreachable From 192.168.1.1 icmp_seq=2 Destination Host
 Unreachable From 192.168.1.1 icmp_seq=3 Destination Host
 Unreachable From 192.168.1.1 icmp_seq=4 Destination Host
 Unreachable
```

2. Utilisez la commande CLI suivante pour récupérer des informations sur le droit de prise en charge du pare-feu à partir du serveur de mise à jour de Palo Alto Networks : request

 ©2023 Palo Alto Networks, Inc.

support check. Si vous disposez de la connectivité, le serveur de mise à jour répond avec le statut de support de votre pare-feu.

STEP 6 | Appliquez le code d'autorisation de capacité et récupérez une licence avant de commencer à tester le pare-feu VM-Series.

Un pare-feu VM-Series sans licence peut traiter jusqu'à 1 230 sessions simultanées environ. Selon l'environnement, la limite de session peut être atteinte très rapidement, ce qui entraîne des résultats imprévisibles.

Ajout d'espace disque supplémentaire au pare-feu VM-Series

Le pare-feu VM-Series nécessite un disque virtuel de 60 Go, dont 21 Go sont utilisés pour la journalisation, par défaut.

- Pour les déploiements de grande envergure, utilisez Panorama pour regrouper les données de tous les pare-feu de nouvelle génération et assurer la visibilité de tout le trafic sur votre réseau. Panorama fournit une journalisation et des rapports centralisés.
- Dans les déploiements plus petits dans lesquels vous n'utilisez pas Panorama, vous pouvez ajouter un nouveau disque virtuel pour augmenter la capacité de stockage des journaux. Le nouveau disque virtuel peut prendre en charge 60 Go à 2 To de capacité de stockage pour les journaux. Cette tâche est décrite ci-dessous.

> ***Lorsque le dispositif virtuel est configuré pour utiliser un disque virtuel, le pare-feu VM-Series ne stocke plus les journaux. Si l'appareil perd la connectivité au disque virtuel, les journaux peuvent être perdus pendant l'intervalle d'échec. Si nécessaire, placez le disque virtuel nouvellement créé sur une banque de données qui fournit la redondance RAID. RAID 10 offre les meilleures performances d'écriture pour des applications avec des besoins de journalisation importants.***

STEP 1 | Mettez le pare-feu VM-Series hors tension.

STEP 2 | Sur le serveur ESXi, ajoutez le disque virtuel au pare-feu.

1. Sélectionnez le pare-feu VM-Series sur le serveur ESXi.
2. Cliquez sur **Edit Settings (Modifier les paramètres)**.
3. Cliquez sur **Add (Ajouter)** pour lancer l'assistant Ajout de matériel et sélectionnez les options suivantes lorsque vous y êtes invité :
    1. Sélectionnez **Hard Disk (Disque dur)** comme type de matériel.
    2. Sélectionnez **Create a new virtual disk (Créer un disque virtuel)**.
    3. Sélectionnez **SCSI** en tant que type de disque virtuel.
    4. Sélectionnez le format de disque « **Thick provisioning** ».
    5. Dans le champ d'emplacement, sélectionnez **Store with the virtual machine option (Enregistrer avec l'option de machine virtuelle)**. Le magasin de données n'a pas à résider sur le serveur ESXi.
    6. Vérifiez que la configuration est correcte, puis cliquez sur **Finish (Terminer)** pour quitter l'assistant. Le nouveau disque est ajouté à la liste des périphériques de l'appareil virtuel.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Mettez le pare-feu sous tension.

La mise sous tension du pare-feu initialise le disque virtuel pour la première utilisation. La durée du processus d'initialisation varie en fonction de la taille du nouveau disque virtuel.

Lorsque le nouveau disque virtuel est initialisé et prêt, PAN-OS déplace tous les journaux du disque existant vers le nouveau disque virtuel. Les nouvelles entrées de journal sont maintenant écrites sur ce nouveau disque virtuel.

PAN-OS génère également une entrée de journal système qui enregistre le nouveau disque.

Si vous réutilisez un disque virtuel précédemment utilisé pour stocker des journaux PAN-OS, tous les journaux du disque existant sont remplacés.

STEP 4 | Vérifiez la taille du nouveau disque virtuel.

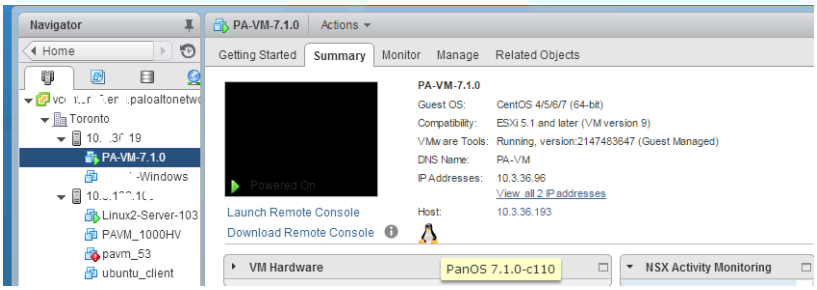
1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Management (Gestion)**.
2. Dans la section Paramètres de journalisation et création de rapport, vérifiez que la capacité de capacité de **Log Storage (Stockage de journal)** affiche correctement la nouvelle capacité de disque.

Utilisation de VMware Tools sur le pare-feu VM-Series sur ESXi et vCloud Air

L'utilitaire VMware Tools améliore la gestion du pare-feu VM-Series à partir du serveur vCenter et de vCloud Director. VMware Tools est fourni avec l'image logicielle du pare-feu VM-Series et toutes les mises à jour sont disponibles avec une nouvelle image OVF. Vous ne pouvez pas installer ou mettre à niveau manuellement VMware Tools à l'aide du serveur vCenter ou de vCloud Director.

- Consultez la ou les adresses IP sur l'interface de gestion et la version du logiciel sur le pare-feu et Panorama.

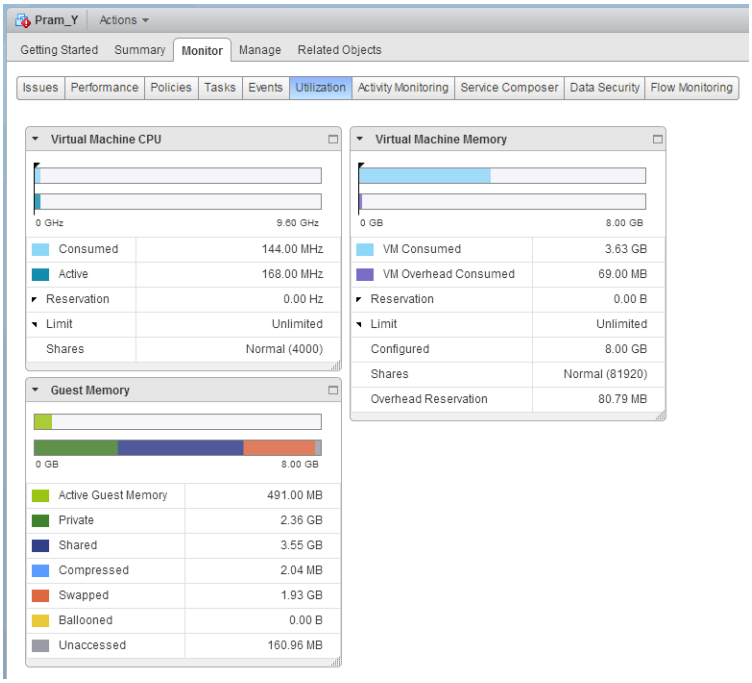
  Dans la section Hôtes et Cluster sur le serveur vCenter, sélectionnez le pare-feu ou Panorama et affichez l'onglet **Summary (Récapitulatif)** pour obtenir des informations sur les adresse IP attribuées à l'interface de gestion et sur la version du logiciel actuellement installée.



 ©2023 Palo Alto Networks, Inc.

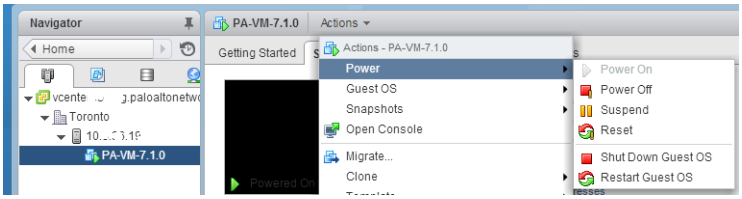
- Affichez les mesures d'utilisation des ressources sur le disque dur, la mémoire et le processeur. Utilisez ces mesures pour activer des alarmes sur le serveur vCenter.

  Dans la section Hosts and Cluster (Hôtes et cluster) sur le serveur vCenter, sélectionnez le pare-feu ou Panorama et affichez l'onglet **Monitor (Surveillance)** > **Utilization (Utilisation)** pour obtenir des informations sur l'utilisation du disque dur, de la mémoire et du processeur.



- Arrêtez ou redémarrez facilement le pare-feu et Panorama à partir du serveur vCenter.

  Dans la section Hosts and Cluster (Hôtes et cluster) sur le serveur vCenter, sélectionnez le pare-feu ou Panorama et la liste déroulante **Actions** > **Power (Alimentation)**.



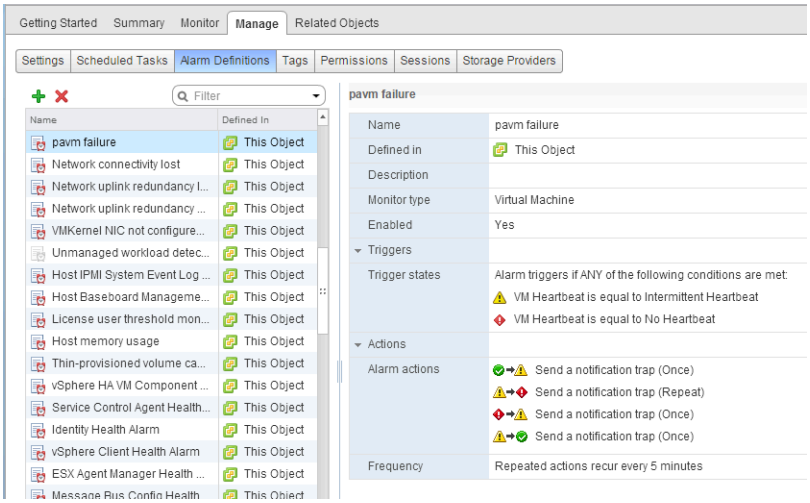
- Créez des définitions d'alarmes pour les événements pour lesquels vous voulez être averti ou pour lesquels vous voulez spécifier une action automatisée.

  Reportez-vous à la documentation VMware pour plus d'informations sur la création des définitions d'alarme.

  Dans la section Hôtes et Cluster sur le serveur vCenter, sélectionnez le pare-feu ou Panorama et sélectionnez **Manage (Gestion)** > **Alarm Definitions (Définitions d'alarme)** pour ajouter un nouveau déclencheur et spécifier une action lorsqu'un seuil est atteint. Par exemple, le manque de pulsations pendant une durée spécifiée, ou lorsque l'utilisation des ressources de mémoire

©2023 Palo Alto Networks, Inc.

dépasse un seuil. La capture d'écran suivante vous montre comment utiliser les notifications pour la surveillance de pulsation sur le pare-feu ou Panorama.



Utilisation de vMotion pour déplacer le pare-feu VM-Series entre les hôtes

Pour maintenir le flux de trafic lorsque vous utilisez vMotion pour déplacer votre pare-feu VM-Series sur VMware ESXientre les hôtes ESXI avec des configurations de processeur homogènes, vous devez utiliser la CLI PAN-OS pour interrompre la surveillance des pulsations du pare-feu VM-Series pendant vMotion. Vous pouvez spécifier la durée, en minutes, pendant laquelle la surveillance des pulsations est interrompue. La surveillance peut être interrompue pendant une durée jusqu'à 60 minutes. Lorsque l'intervalle d'interruption expire ou lorsque vous choisissez d'y mettre fin, la surveillance des pulsations reprend.

Le vMotion du pare-feu VM-Series est pris en charge sur vSphere 6.5, 6.7 et 7.0 si les hôtes ESXi ont une configuration de processeur homogène.

Ces commandes ne sont pas requises lorsque vous utilisez vMotion si vous exécutez vSphere version 7.0 ou ultérieure.

STEP 1 | Connectez-vous à la CLI du pare-feu VM-Series.

STEP 2 | Réglez l'intervalle d'interruption de la surveillance des pulsations à l'aide de la commande suivante. L'interruption commence dès que la commande est exécutée. Si vMotion dure plus longtemps qu'attendu, vous pouvez réexécuter cette commande pour définir un nouvel intervalle plus long qui démarre lorsque la commande est exécutée une nouvelle fois.

```
request system heartbeat-pause set interval <pause-time-in-minutes>
```

Vous pouvez afficher la durée restante dans l'intervalle de pause à l'aide de la commande suivante.

```
request system heartbeat-pause show interval
```


©2023 Palo Alto Networks, Inc.

STEP 3 | (Facultatif) Si vous terminez vMotion avant la fin de l'intervalle d'interruption, vous pouvez mettre fin à l'interruption en réglant l'intervalle sur zéro (0).

```
request system heartbeat-pause set interval 0
```

Utilisation de la CLI du VM-Series pour permuter l'interface de gestion sur ESXi

Par défaut, le pare-feu VM-Series affecte la première interface (eth0) comme interface de gestion. Toutefois, dans certains déploiements, la première interface doit être pré-mappée à une adresse IP publique. Par conséquent, l'interface de gestion doit être affectée à une interface différente. L'attribution d'une adresse IP publique à l'interface de gestion constitue un risque de sécurité.

Cette procédure nécessite le plug-in VM-Series 2.0.7 ou version ultérieure.

Vous pouvez également activer l'échange d'interface de gestion dans le cadre de Composants du fichier init-cfg.txt *pendant l'amorçage.*

STEP 1 | Connectez-vous à la CLI du pare-feu VM-Series et saisissez la commande suivante :

```
set system setting mgmt-interface-swap enable yes
```

STEP 2 | Confirmez que vous voulez permuter l'interface et utiliser l'interface du dataplane eth1 comme interface de gestion.

STEP 3 | Redémarrez le pare-feu pour que la permutation prenne effet. Utilisez la commande suivante :

```
request restart system
```

STEP 4 | Vérifiez que les interfaces ont été permutées. Utilisez la commande suivante :

```
debug show vm-series interfaces all Phoenix_interface   Base-
OS_port   Base-OS_MAC        PCI-ID         Driver mgt(interface-
swap) eth0   0e:53:96:91:ef:29   0000:00:04.0   ixgbevf Ethernet1/1
          eth1    0e:4d:84:5f:7f:4d       0000:00:03.0   ixgbevf
```


©2023 Palo Alto Networks, Inc.

VM Monitoring sur vCenter

Installez et configurez le plug-in Panorama pour VMware vCenter afin de récupérer les adresses IP des invités dans votre environnement vCenter et d'utiliser ces informations pour créer une politique à l'aide de groupes d'adresses dynamiques.

Le plugin Panorama pour VMware vCenter ne prend pas en charge les serveurs proxy.

- À propos de VM Monitoring sur VMware vCenter
- Installation du plug-in Panorama pour VMware vCenter
- Configurez le plug-in Panorama pour VMware vCenter

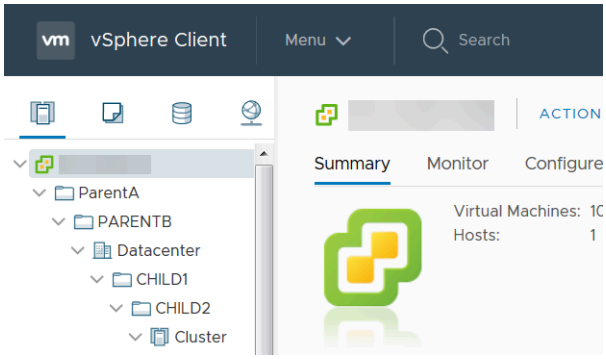
À propos de VM Monitoring sur VMware vCenter

Le plug-in Panorama pour VMware vCenter vous donne les outils pour créer une politique pour votre environnement vCenter en utilisant les Groupes d'adresses dynamiques. Les groupes d'adresses dynamiques vous permettent de créer une politique qui s'adapte automatiquement aux modifications de votre environnement telles que l'ajout ou la suppression d'invités. Le plug-in VMware vCenter surveille les modifications dans votre environnement vCenter et partage ces informations avec Panorama.

Le plug-in traite les informations qu'il reçoit de vCenter et les convertit en un ensemble d'étiquettes sur Panorama que vous pouvez utiliser comme critères de correspondance pour attribuer une adresse IP à des groupes d'adresses dynamiques. Chaque étiquette comporte un préfixe qui décrit la hiérarchie au-dessus de la VM.

Dans cet exemple, chaque étiquette dans Panorama commence par le préfixe indiqué ci-dessous. Chaque étiquette inclut le nom vCenter, le nom du centre de données et le nom du cluster ; si vous avez des dossiers dans votre hiérarchie vCenter, les étiquettes incluront les noms des dossiers. L'ordre des objets dans l'étiquette correspond à l'ordre dans la hiérarchie vCenter.

vcenter.<vcenter-name>_ParentA_ParentB_Datacenter_CHILD1_CHILD2_Cluster_<tag>



Le plug-in Panorama pour VMware vCenter ne prend pas en charge les étiquettes associées aux vApp ou les pools de ressources.

Les étiquettes sont affichées dans Panorama dans les formats suivants :

©2023 Palo Alto Networks, Inc.

- **vcenter.**<vcenter-name>_<datacenter-name>_<cluster-name>_vmname.<vm-name>— cette étiquette mappe les adresses IP des Virtual Machines (machines virtuelles – VM) en fonction du nom de la VM.
- **vcenter.**<vcenter-name>_<datacenter-name>_<cluster-name>_guestos.<guest-os>— cette étiquette mappe les adresses IP des Virtual Machines (machines virtuelles – VM) en fonction du système d'exploitation invité.
- **vcenter.**<vcenter-name>_<datacenter-name>_<cluster-name>_annotation.<annotation>— cette étiquette mappe les adresses IP des Virtual Machines (machines virtuelles – VM) en fonction des annotations.
- **vcenter.**<vcenter-name>_<datacenter-name>_<cluster-name>_vlanId.<vlan-ID>— cette étiquette mappe les adresses IP des Virtual Machines (machines virtuelles – VM) en fonction de l'ID de VLAN.
- **vcenter.**<vcenter-name>_<datacenter-name>_<cluster-name>_host-ip.<host-ip>— cette étiquette mappe les adresses IP des Virtual Machines (machines virtuelles – VM) en fonction de l'adresse IP de l'hôte.
- **vcenter.**<vcenter-name>_<datacenter-name>_<cluster-name>_<tag-category>.<user-defined-tag>— cette étiquette mappe les adresses IP des Virtual Machines (machines virtuelles – VM) en fonction des étiquettes définies par l'utilisateur créées dans vCenter.

> ***Le plug-in prend en charge un maximum de 16 étiquettes définies par l'utilisateur par machine virtuelle. Si le nombre d'étiquettes définies par l'utilisateur est supérieur à 16, celles-ci ne sont pas traitées.***

Le plug-in Panorama pour vCenter ne peut pas traiter les étiquettes de plus de 128 caractères. Cela inclut des lettres, des chiffres et des caractères spéciaux. L'espace dans les noms d'objets vCenter est remplacé par des barres obliques. De plus, Panorama ne prend pas en charge les caractères spéciaux non-ASCII ou les caractères spéciaux suivants —**'<>&"** dans les annotations et noms de machine virtuelle vCenter. Panorama abandonne les étiquettes comprenant des caractères non pris en charge.

Pour récupérer les informations de mappage d'adresse IP à étiquette des terminaux, vous devez configurer une définition de surveillance pour chaque vCenter de votre environnement virtuel. La définition de surveillance spécifie le nom d'utilisateur et le mot de passe permettant à Panorama de se connecter à vCenter. Elle spécifie également les groupes d'appareils et les groupes de notification correspondants contenant les pare-feu auxquels Panorama envoie les étiquettes. Une fois que vous avez configuré la définition de surveillance et que le plug-in Panorama pour VMware vCenter a récupéré les étiquettes, vous pouvez créer des DAG et ajouter les étiquettes en tant que critères de correspondance.

Installation du plug-in Panorama pour VMware vCenter

Pour démarrer avec la surveillance des terminaux sur vCenter, téléchargez et installez le plug-in Panorama for VMware vCenter.

Si vous avez une configuration d'HA de Panorama, répétez ce processus d'installation sur chaque pair de Panorama. Lors de l'installation de la fiche sur les Panoramas d'une paire HA, installez la fiche sur le pair passif avant le pair actif. Après avoir installé le plug-in sur l'homologue passif, il passera à un état non fonctionnel. L'installation du plug-in sur l'homologue actif renvoie l'homologue passif à un état fonctionnel.

 ©2023 Palo Alto Networks, Inc.

Si vous avez un appareil Panorama autonome ou deux appareils Panorama installés dans une paire HA avec plusieurs plug-ins installés, les plug-ins peuvent ne pas recevoir les informations des indicateurs d'adresse IP mises à jour si un ou plusieurs des plug-ins ne sont pas configurés. Cela se produit, car Panorama ne transfère pas les informations des indicateurs d'adresse IP aux plug-ins non configurés. De plus, ce problème peut se présenter si un ou plusieurs plug-ins Panorama ne se trouvent pas dans l'état Registered (Enregistré) ou Success (Réussite) (l'état positif diffère sur chaque plug-in). Assurez-vous que vos plug-ins se trouvent dans l'état positif avant de continuer ou d'exécuter les commandes décrites ci-dessous.

Si vous rencontrez ce problème, il existe deux solutions alternatives :

- Désinstallez le ou les plug-ins non configurés. Il est déconseillé d'installer un plug-in que vous n'envisagez pas de configurer dans l'immédiat
- Vous pouvez utiliser les commandes suivantes pour contourner ce problème. Exécutez la commande suivante pour chaque plug-in non configuré sur chaque instance de Panorama afin que Panorama n'attende pas pour envoyer des mises à jour. Dans le cas contraire, vos pare-feu risquent de perdre certaines informations des indicateurs d'adresse IP.

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  Vous pouvez annuler cette commande en exécutant :

  request plugins dau plugin-name <plugin-name> unblock-device-push no

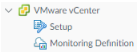
Les commandes décrites ne sont pas persistantes lors des redémarrages et doivent être réutilisées pour tout redémarrage ultérieur. Pour Panorama en paire HA, les commandes doivent être exécutées sur chaque Panorama.

STEP 1 | Sélectionnez **Panorama** > **Plugins**.

STEP 2 | Sélectionnez **Upload (Télécharger)** et cliquez sur **Browse (Parcourir)** pour localiser le fichier du plug-in.

STEP 3 | Cliquez sur **OK** pour terminé le téléchargement.

STEP 4 | Sélectionnez la version du plug-in et cliquez sur **Install (Installer)** dans la colonne Action pour installer le plug-in. Panorama vous alertera lorsque l'installation est terminée.



Configurez le plug-in Panorama pour VMware vCenter

Après avoir installé le plug-in, effectuez la procédure suivante pour établir une connexion entre Panorama et vCenter.

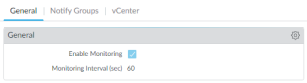
Pour que le plug-in puisse surveiller les machines virtuelles dans votre environnement vCenter, vous devez installer des outils VMware (VMware tools). Dans vCenter, les adresses IP des machines virtuelles ne sont pas récupérables de manière externe. Elles ne sont visibles que via les outils VMware (VMware tools). De plus, des autorisations natives en lecture seule sont requises pour que le plug-in récupère les informations d'adresse IP de vCenter.

STEP 1 | Connectez-vous à l'interface Web Panorama.

 ©2023 Palo Alto Networks, Inc.

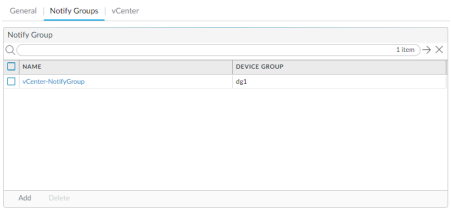
STEP 2 | Activez la surveillance et définissez l'intervalle de surveillance.

1. Sélectionnez **Panorama** > **VMware vCenter** > **Setup (Configuration)** > **General (Général)**.
2. Sélectionnez **Enable Monitoring** (Activer la surveillance). Cela active la surveillance de tous les vCenter de votre déploiement.
3. Définissez le **Monitoring Interval** (Intervalle de surveillance) en secondes. L'intervalle de surveillance correspond à la fréquence à laquelle Panorama récupère les informations réseau mises à jour à partir de vCenter. La valeur par défaut est de 60 secondes et possède une plage allant de 60 à 84 600 secondes.



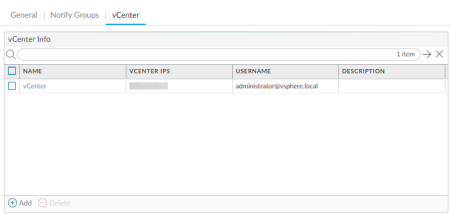
STEP 3 | Créez un groupe de notification.

1. Sélectionnez **Panorama** > **VMware vCenter** > **Setup (Configuration)** > **Notify Groups (Groupes de notification)**.
2. Cliquez sur **Add (Ajouter)**.
3. Saisissez un **Name** (Nom) descriptif pour votre groupe de notification.
4. Sélectionnez les groupes d'appareils dans votre déploiement de vCenter.



STEP 4 | Ajoutez des informations sur vCenter. Le plug-in Panorama pour VMware vCenter prend en charge jusqu'à 16 instances de vCenter.

1. Sélectionnez **Panorama** > **VMware vCenter** > **Setup (Configuration)** > **vCenter**.
2. Saisissez un **Name** (Nom) descriptif pour votre vCenter.
3. Saisissez l'adresse IP ou le FQDN pour vCenter et le port, le cas échéant.
4. Saisissez votre nom d'utilisateur vCenter.
5. Saisissez et confirmez votre mot de passe vCenter.
6. Cliquez sur **Validate (Valider)** pour vérifier que Panorama peut se connecter à vCenter à l'aide des identifiants de connexion que vous avez saisis.
7. Cliquez sur **OK**.



 ©2023 Palo Alto Networks, Inc.

STEP 5 | Configurez jusqu'à 16 définitions de surveillance.

Une instance vCenter peut être attribuée à une seule définition de surveillance.

1. Sélectionnez **Panorama** > **VMware vCenter** > **Monitoring Definition (Définition de surveillance)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name** (Nom) descriptif et éventuellement une Description pour identifier le vCenter pour lequel vous utilisez cette définition.
3. Sélectionnez le **vCenter** et **Notify Group** (Groupe de notification).
4. Cliquez sur **OK**.



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

STEP 7 | Vérifiez que vous pouvez visualiser l'information VM sur Panorama et définir les critères d'appariement pour les groupes d'adresses dynamiques.

Vous devez utiliser l'opérateur OR si vous appliquez plusieurs étiquettes dans les critères de correspondance. Utiliser l'opérateur AND ne fonctionne pas.

Certaines extensions de navigateur peuvent bloquer les appels API entre Panorama et vCenter, ce qui empêche Panorama de recevoir les critères de correspondance. Si Panorama n'affiche aucun critère de correspondance et que vous utilisez des extensions de navigateur, désactivez ces extensions et cliquez sur Synchronize Dynamic Objects (Synchroniser des objets dynamiques) pour renseigner les étiquettes disponibles dans Panorama.

STEP 8 | Vérifiez que les adresses de vos machines virtuelles sont ajoutées aux DAG.

1. Sélectionnez **Panorama** > **Objects (Objets)** > **Address Groups (Groupes d'adresses)**.
2. Cliquez sur **More** (Plus) dans la colonne Addresses (Adresses) d'un DAG.

   Panorama affiche une liste des adresses IP ajoutées à ce DAG en fonction des critères de correspondance que vous avez spécifiés.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Utilisez des groupes d'adresses dynamiques dans une politique.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Cliquez sur **Add (Ajouter)** et saisissez un **Name (nom)** et une **Description (description)** pour identifier la politique.
3. Ajoutez la **Source Zone (Zone source)** pour indiquer la zone d'où provient le trafic.
4. Ajoutez la **Destination Zone (Zone de destination)** dans laquelle se termine le trafic.
5. Pour **Destination Address (Adresse de destination)**, sélectionnez le groupe d'adresses dynamiques que vous venez de créer.
6. Indiquez l'action (**Allow (Autoriser)** ou **Deny (Refuser)**) pour le trafic, puis associez éventuellement les profils de sécurité par défaut à la règle.
7. Répétez les étapes 1 à 6 pour créer une autre règle de politique.
8. Cliquez sur **Commit (Valider)**.

STEP 10 | Vous pouvez mettre à jour les objets dynamiques à partir de vCenter à tout moment en synchronisant les objets dynamiques. La synchronisation des objets dynamiques vous permet de conserver le contexte des modifications dans l'environnement virtuel et vous permet d'activer des applications grâce à la mise à jour automatique des groupes d'adresses dynamiques utilisés dans les règles de politique.

1. Sélectionnez **Panorama** > **vCenter** > **Monitoring Definition (Définition de surveillance)**.
2. Cliquez sur **Synchronize Dynamic Objects** (Synchroniser les objets dynamiques).

STEP 11 | Si un pare-feu de votre déploiement vCenter redémarre ou se déconnecte de Panorama, ce pare-feu n'est plus synchronisé avec le plug-in Panorama pour vCenter et ne reçoit aucune mise à jour. Une fois le pare-feu reconnecté à Panorama, vous devez synchroniser manuellement Panorama et le pare-feu.

1. Connectez-vous à la CLI Panorama.
2. Exécutez la commande suivante.

   ```
   admin@Panorama> request plugins vmware_vcenter sync
   ```

 ©2023 Palo Alto Networks, Inc.

Résolution des problèmes de déploiement ESXi

La plupart des étapes de dépannage pour le pare-feu VM-Series sont similaires à celles des versions matérielles de PAN-OS. En cas de problème, consultez les compteurs de l'interface, les fichiers journaux du système, et si nécessaire, utilisez le débogage pour créer des captures.

Les sections suivantes décrivent comment résoudre les problèmes les plus courants :

- Résolution des problèmes de base
- Problèmes d'installation
- Problèmes de mise sous licence
- Problèmes de connectivité

Résolution des problèmes de base



Recommandation pour les outils de résolution des problèmes réseau

Il est recommandé de disposer d'un poste de résolution des problèmes distinct pour capturer le trafic ou injecter des paquets de test dans l'environnement virtuel. Il peut être utile de créer un nouveau système d'exploitation de toutes pièces à l'aide des outils de résolution des problèmes courants installés, tels que tcpdump, nmap, hping, traceroute, iperf, tcpedit, netcat, etc. Cette machine peut alors être mise hors tension et convertie en un modèle. Chaque fois que les outils sont nécessaires, le client de résolution des problèmes (la machine virtuelle) peut être rapidement déployé sur le(s) commutateur(s) virtuel(s) en question et utilisé pour isoler les problèmes de mise en réseau. Une fois le test terminé, l'instance peut simplement être supprimée et le modèle utilisé à nouveau la prochaine fois qu'il est requis.

En cas de problèmes de performances du pare-feu, commencez par consulter le **Dashboard (Tableau de bord)** depuis l'interface Web du pare-feu. Pour afficher les alertes ou créer un dossier de support technique ou un fichier de vidage des statistiques, sélectionnez **Device (Périphérique)** > **Support**.

Pour obtenir des informations sur le client vSphere, sélectionnez **Home (Accueil)** > **Inventory (Inventaire)** > **VMs and Templates (Machines virtuelles et modèles)**, puis sélectionnez l'instance du pare-feu VM-Series et cliquez sur l'onglet **Summary (Récapitulatif)**. Sous **Resources (Ressources)**, consultez les statistiques relatives à la consommation de mémoire, de la capacité processeur et de stockage. Pour obtenir l'historique des ressources, cliquez sur l'onglet **Performance** et contrôlez la consommation des ressources.

Problèmes d'installation

- Problèmes de déploiement du modèle OVA
- Pourquoi le pare-feu démarre-t-il en mode maintenance ?
- Pourquoi dois-je modifier le fichier image de base pour la licence VM-1000-HV ?

©2023 Palo Alto Networks, Inc.

Problèmes de déploiement du modèle OVA

- La série VM est livrée sous forme d'archive zip au format Open Virtualization Alliance (OVA) qui se développe en trois fichiers.

  Si vous rencontrez des problèmes à déployer l'image OVA, assurez-vous que les trois fichiers sont décompressés et accessibles. Si nécessaire, téléchargez et extrayez à nouveau l'image OVA.
- Le disque virtuel de l'image OVA est de presque 1GB. Il doit être présent sur l'ordinateur exécutant le client vSphere ou être accessible en tant que lien (URL) pour l'image OVA.
  - Assurez-vous que la connexion réseau entre l'ordinateur client vSphere et l'hôte ESXi cible a une faible latence et une bande passante suffisante. Si la connexion est mauvaise, le déploiement OVA peut prendre des heures ou bien expirer et échouer.

    Vous pouvez réduire ce problème si vous hébergez l'image sur un périphérique dans le même réseau que l'hôte ESXi.
  - Tous les pare-feu du chemin doivent autoriser les ports TCP 902 et 443 du client vSphere vers les hôtes ESXi.
- La version ESX 6.5.0a 4887370 vous limite à 2 cœurs de processeur (CPU) par socket. Si vous déployez un VM-300, VM-500 ou VM-700 auquel vous souhaitez allouer plus de 2 vCPU par socket, pour une solution de contournement, reportez-vous à la base de connaissances VMware: https://kb.vmware.com/s/article/53354

Pourquoi le pare-feu démarre-t-il en mode maintenance ?

Si vous avez acheté la licence VM-1000-HV et que vous déployez le pare-feu VM-Series en mode autonome sur un serveur VMware ESXi, vous devez allouer la quantité de mémoire minimum nécessaire à votre modèle VM-Series.

Pour éviter le démarrage en mode maintenance, vous devez soit modifier le fichier image de base (voir How do I modify the base image file for the VM-1000-HV license? Comment modifier le fichier image de base de la licence VM-1000-HV?)), ou bien modifier les paramètres sur l'hôte ESXi ou le serveur vCenter avant vous d'allumer le pare-feu VM-Series.

De plus, vérifiez que l'interface est à VMXnet3. Régler le type d'interface dans n'importe quel autre format entraînera le démarrage du pare-feu en mode maintenance.

Pourquoi dois-je modifier le fichier image de base pour la licence VM-1000-HV ?

Si vous avez acheté la licence VM-1000-HV et déployez le pare-feu VM-Series en mode autonome sur un serveur VMware ESXi, suivez ces instructions pour modifier les attributs suivants définis dans le fichier image de base (.ova ou .xva) du pare-feu VM-Series.

Important : La modification des valeurs autres que celles répertoriées ci-dessous invalidera le fichier image de base.

STEP 1 | Ouvrez le fichier image de base, par exemple 7.0.0, à l'aide d'un outil d'édition de texte tel que le Bloc-Notes.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Recherchez 4096, modifiez la mémoire allouée et définissez-la sur 5012 (c'est-à-dire 5 Go) et suivez les instructions suivantes :

```
<Item> <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
 <rasd:Description>Memory Size</rasd:Description>
 <rasd:ElementName>4096MB of memory</rasd:ElementName>
 <rasd:InstanceID>2</rasd:InstanceID> <rasd:ResourceType>4</
rasd:ResourceType> <rasd:VirtualQuantity>4096</
rasd:VirtualQuantity> <Item> <rasd:AllocationUnits>byte
 * 2^20</rasd:AllocationUnits> <rasd:Description>Memory
 Size</rasd:Description> <rasd:ElementName>5120MB
 of memory</rasd:ElementName> <rasd:InstanceID>2</
rasd:InstanceID> <rasd:ResourceType>5</rasd:ResourceType>
 <rasd:VirtualQuantity>5120</rasd:VirtualQuantity>
```

STEP 3 | Modifiez le nombre de cœurs de processeurs virtuels alloués (de 2 à 4 ou 8, comme souhaité) pour votre déploiement :

```
<Item> <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
 <rasd:Description>Number of Virtual CPUs</rasd:Description>
 <rasd:ElementName>2 virtual CPU(s)</rasd:ElementName>
 <rasd:InstanceID>1</rasd:InstanceID> <rasd:ResourceType>3</
rasd:ResourceType> <rasd:VirtualQuantity>2</rasd:VirtualQuantity>
 <vmw:CoresPerSocket ova:required="false">2</vmw:CoresPerSocket>
 </Item> <Item> <rasd:AllocationUnits>hertz * 10^6</
rasd:AllocationUnits> <rasd:Description>Number of Virtual
 CPUs</rasd:Description> <rasd:ElementName>4 virtual CPU(s)</
rasd:ElementName> <rasd:InstanceID>1</rasd:InstanceID>
 <rasd:ResourceType>3</rasd:ResourceType> <rasd:VirtualQuantity>4</
rasd:VirtualQuantity> <vmw:CoresPerSocket ova:required="false">2</
vmw:CoresPerSocket> </Item>
```

Vous pouvez également déployer le pare-feu et, avant de mettre le pare-feu VM-Series sous tension, modifier directement l'allocation de mémoire et de CPU virtuelle sur l'hôte ESXi ou le serveur vCenter.

Problèmes de mise sous licence

- Pourquoi ne puis-je pas appliquer la licence de fonctionnalité ou de support ?
- Pourquoi mon pare-feu VM-Series cloné ne dispose pas d'une licence valide ?
- Déplacer le pare-feu VM-Series invalide-t-il la licence ?

Pourquoi ne puis-je pas appliquer la licence de fonctionnalité ou de support ?

Avez-vous appliqué le code d'autorisation de capacité au pare-feu VM-Series ? Avant d'activer la licence de fonctionnalité ou de support, vous devez appliquer le code d'autorisation de capacité de manière à ce que le périphérique puisse obtenir un numéro de série. Ce numéro de série est requis pour activer les autres licences sur le pare-feu VM-Series.

©2023 Palo Alto Networks, Inc.

Pourquoi mon pare-feu VM-Series cloné ne dispose pas d'une licence valide ?

VMware affecte un UUID unique à chaque machine virtuelle, y compris le pare-feu VM-Series. Par conséquent, lorsqu'un pare-feu VM-Series est cloné, un nouvel UUID lui est affecté. Comme le numéro de série et la licence pour chaque instance du pare-feu VM-Series sont associés à l'UUID, le clonage d'un pare-feu VM-Series sous licence donne lieu à un nouveau pare-feu disposant d'une licence non valide. Vous avez besoin d'un nouveau code d'autorisation pou activer la licence sur le pare-feu qui vient d'être déployé. Vous devez appliquer le code d'autorisation de capacité et une nouvelle licence de support afin d'obtenir des fonctionnalités, un support et des mises à jour logicielles complets sur le pare-feu VM-Series.

Déplacer le pare-feu VM-Series invalide-t-il la licence ?

Si vous déplacez manuellement le pare-feu VM-Series entre deux hôtes, veillez à sélectionner l'option **This guest was moved (Cet invité a été déplacé)** pour éviter l'invalidation de la licence.

Problèmes de connectivité

- Pourquoi le pare-feu VM-Series ne reçoit aucun trafic réseau ?

Pourquoi le pare-feu VM-Series ne reçoit aucun trafic réseau ?

Sur le pare-feu VM-Series, vérifiez les journaux de trafic (**Monitor (Surveillance)** > **Logs (Journaux)**). Si les journaux sont vides, utilisez la commande de la CLI suivante pour afficher les paquets sur les interfaces du pare-feu VM-Series :

```
show counter global filter delta yes Global counters:
 Elapsed time since last sampling: 594.544 seconds
 ------------------------------------------------------------------------------
 Total counters shown: 0
 ------------------------------------------------------------------------------
```

Dans l'environnement vSphere, recherchez les problèmes suivants :

- Vérifiez les groupes de ports et assurez-vous que le pare-feu et la/les machine(s) virtuelle(s) se trouvent sur le bon groupe de ports.

  Vérifiez que les interfaces sont correctement mappées.

  Carte réseau 1 = gestion

  Carte réseau 2 = Ethernet 1/1

  Carte réseau 3 = Ethernet 1/2

  Pour chaque machine virtuelle, accédez aux paramètres et vérifiez que l'interface est mappée au bon groupe de ports.

 ©2023 Palo Alto Networks, Inc.

- Vérifiez que le mode de proximité est activé pour chaque groupe de ports ou pour le commutateur, ou que vous avez configuré le pare-feu pour les adresses MAC attribuées par l'hyperviseur.

  Comme les adresses MAC PAN-OS sont différentes des adresses MAC VMNIC affectées par vSphere, le groupe de ports (ou vSwitch) doit être en mode de proximité si l'option d'utiliser l'adresse MAC attribuée par l'hyperviseur n'est pas activée.

  - Vérifiez les paramètres VLAN sur vSphere.

    L'utilisation du paramètre VLAN pour le groupe de ports vSphere vise deux objectifs : déterminer les groupes de ports qui partagent un domaine de couche 2 et si les ports de liaison montante sont marqués (802.1Q).

  - Vérifiez les paramètres de port du commutateur physique.

    Si un ID de réseau local virtuel est spécifié sur un groupe de port doté de ports de liaison montante, vSphere utilise 802.1Q pour marquer les trames sortantes. L'étiquette doit correspondre à la configuration sur le commutateur physique, sinon le trafic ne passe pas.

    Vérifiez les statistiques de port si vous utilisez des commutateurs distribués (vDS) ; les commutateurs standard ne fournissent aucune statistique de port.

 ©2023 Palo Alto Networks, Inc.

Réglage des performances de VM-Series pour ESXi

Le pare-feu VM-Series pour ESXi est un appareil haute performance, mais il peut nécessiter un réglage de l'hyperviseur pour obtenir les meilleurs résultats. Cette section décrit quelques bonnes pratiques et recommandations pour faciliter les meilleures performances du pare-feu VM-Series. Pour de meilleures performances, ESXi 6.0.0.0 ou version ultérieure est recommandé.

- Installation du pilote de carte réseau sur ESXi
- Activation de DPDK sur ESXi
- Activation de SR-IOV sur ESXi
- Activation du mode d'accès VLAN (réseau local virtuel) ESXi avec SR-IOV
- Activation de la prise en charge de files d'attente multiples pour les cartes réseau sur ESXi
- Réglage des performances du VNF

Installation du pilote de carte réseau sur ESXi

Pour de meilleures performances, utilisez SR-IOV avec des interfaces réseau Intel 10 Go, ce qui nécessite le pilote ixgbe 4.4.1 pour prendre en charge les files d'attente multiples pour chaque interface.

STEP 1 | Obtenez une liste d'interfaces réseau sur l'hôte ESXi.

1. Connectez-vous à la CLI de l'hôte ESXi.
2. Utilisez la commande suivante pour renvoyer une liste d'interfaces réseau :

```
$ esxcli network nic list
```

STEP 2 | Déterminez la version du pilote pour une interface particulière.

Vous pouvez utiliser soit **ethtool** ou **esxcli** pour déterminer la version du pilote actuellement installée. L'exemple suivant utilise vNIC4 et renvoie la version de pilote 3.21.6.

- ethtool—**ethtool -l *<nic-name>***

```
$ ethtool -I vNIC4 driver: ixgbe version: 3.21.6iov firmware-
version: 0x80000389 bus-info: 0000:04:00.0
```

- esxcli—**esxcli network nic get -n *<nic-name>***

```
$ esxcli network nic get -n vNIC4 Advertised Auto Negotiation:
 true Advertised Link Modes: Auto Negotiation: true Cable Type:
 Current Message Level: 7 Driver Info: Bus Info: 0000:04:00.0
 Driver: ixgbe Firmware Version: 0x80000389 Version: 3.21.6iov
 Link Detected: false Link Status: Down Name: vNIC4 PHYAddress:
 0 Pause Autonegotiate: true Pause RX: true Pause TX: true
 Supported Ports: FIBRE Supports Auto Negotiation: true Supports
 Pause: true Supports Wakeon: false Transceiver: external Wakeon:
 None
```


©2023 Palo Alto Networks, Inc.

STEP 3 | Installez le nouveau pilote.

1. Téléchargez le pilote 4.4.1 depuis le site web de VMware. Ouvrez le contenu dans un répertoire local et trouvez les fichiers . zip ou . vib pour votre conducteur.
2. Créez un nouveau dossier dans votre magasin de données hôte ESXi.
3. Copiez le fichier local . zip ou .vib que vous avez extrait dans le nouveau dossier de votre magasin de données hôte ESXi.
4. Activez le mode maintenance sur l'hôte ESXi.
5. Utilisez l'une des commandes suivantes pour installer le nouveau pilote en utilisant -d pour les fichiers . zip ou -v pour les fichiers .vib.

   - **`$ esxcli software vib install -d <path to driver .zip file>`**
   - **`$ esxcli software vib install -v <path to driver .vib file>`**

   Vous devez préciser le chemin absolu vers le fichier . zip ou .vib. Par exemple :

   ```
   $ esxcli software vib install -d "/vmfs/volumes/
   Datastore/DirectoryName/DriverName.zip"
   ```

6. Vérifier l'installation de la VIB.

   ```
   $ esxcli software vib list
   ```

7. Redémarrer l'hôte ESXi.

Activation de DPDK sur ESXi

Le kit de développement du plan de données (DPDK) améliore les performances de VM-Series en augmentant la vitesse de traitement des paquets de cartes d'interface réseau (NIC). Dans le pare-feu VM-Series, DPDK est activé par défaut sur ESXi.

Pour tirer parti de DPDK, vous devez utiliser une carte réseau avec l'un des pilotes DPDK pris en charge mentionnés dans les versions de pilotes DPDK :

Si vous désactivez DPDK, la carte d'interface réseau utilise PacketMMAP au lieu de DPDK. Vous pouvez désactiver la DPDK en utilisant la commande **`set system setting dpdk-pkt-io off`**.

Consultez la matrice de compatibilité pour la prise en charge de l'hyperviseur ESXi et la prise en charge des pilotes PacketMMAP et DPDK par la version de PAN-OS.

Activation de SR-IOV sur ESXi

La virtualisation d'E/S racine unique (SR-IOV) permet à un périphérique physique PCIe unique sous un port racine unique d'apparaître comme plusieurs périphériques physiques distincts de l'hyperviseur ou de l'invité. Activez SR-IOV en activant les périphériques à fonction virtuelle sur la carte d'interface réseau SR-IOV et en modifiant les paramètres d'invité dans vCenter.

 ©2023 Palo Alto Networks, Inc.

SR-IOV sur VM-Series pour ESXi nécessite l'un des pilotes de carte réseau Intel mentionnés dans les versions de pilotes PacketMMAP. Consultez la matrice de compatibilité pour la prise en charge des pilotes SR-IOV et DPDK par la version de PAN-OS.

Il y a deux façons d'activer SR-IOV sur ESXi.

- **SR-IOV passthrough (Relais SR-IOV)** : dans cette méthode, vous activez les périphériques à fonction virtuelle sur la carte réseau SR-IOV et modifiez les paramètres d'invité dans vCenter, en ajoutant l'interface VF SR-IOV comme adaptateur de type relais SR-IOV. Reportez-vous à la section Attribuer une fonction virtuelle en tant qu'adaptateur de type relais SR-IOV à une machine virtuelle.

  Cette méthode, qui est privilégiée pour PAN-OS 8.1.2 et les versions ultérieures, vous permet d'ajouter le PF SR-IOV à un vSwitch ou un DvSwitch.
- **PCI Adaptor (Adaptateur PCI)** : cette méthode était nécessaire pour les versions PAN-OS 8.0 à 8.1.1. Vous pouvez consulter le flux de travail de l'adaptateur PCI dans Activer SR-IOV sur ESXi dans le guide de déploiement 8.1.

  La méthode PCI Adaptor (Adaptateur PCI) présente une limitation : vous ne pouvez pas configurer un vSwitch sur le port physique sur lequel vous activez SR-IOV. Le pare-feu VM-Series doit avoir un accès exclusif au port physique et aux fonctions virtuelles associées (VF) sur cette interface pour pouvoir communiquer avec l'hôte ou d'autres machines virtuelles sur le réseau. Reportez-vous à la section Ajouter un périphérique PCI dans le client Web vSphere..

Activation du mode d'accès VLAN (réseau local virtuel) ESXi avec SR-IOV

Les pare-feu VM-Series sur ESXi peuvent fonctionner en mode d'accès VLAN pour prendre en charge les cas d'utilisation où il est déployé comme une fonction de réseau virtuel (VNF) qui offre la sécurité en tant que service dans un environnement de centre de données/cloud à plusieurs locataires. En mode d'accès VLAN, chaque VNF dispose d'interfaces de réseau virtuel (VNI) dédiées pour chaque réseau et envoie et reçoit des paquets vers/depuis les fonctions virtuelles (VF) SR-IOV sans étiquettes VLAN. Vous devez activer cette capacité sur les fonctions physiques et virtuelles de l'hyperviseur hôte. Lorsque vous activez ensuite le mode d'accès VLAN sur le pare-feu VM-Series, ce dernier peut envoyer et recevoir du trafic sans étiquettes VLAN à travers toutes ses interfaces de plan de données. De plus, si vous configurez des politiques QoS, le pare-feu peut appliquer la QoS sur l'interface d'accès et fournir un traitement différencié du trafic dans un déploiement multi-tenant.

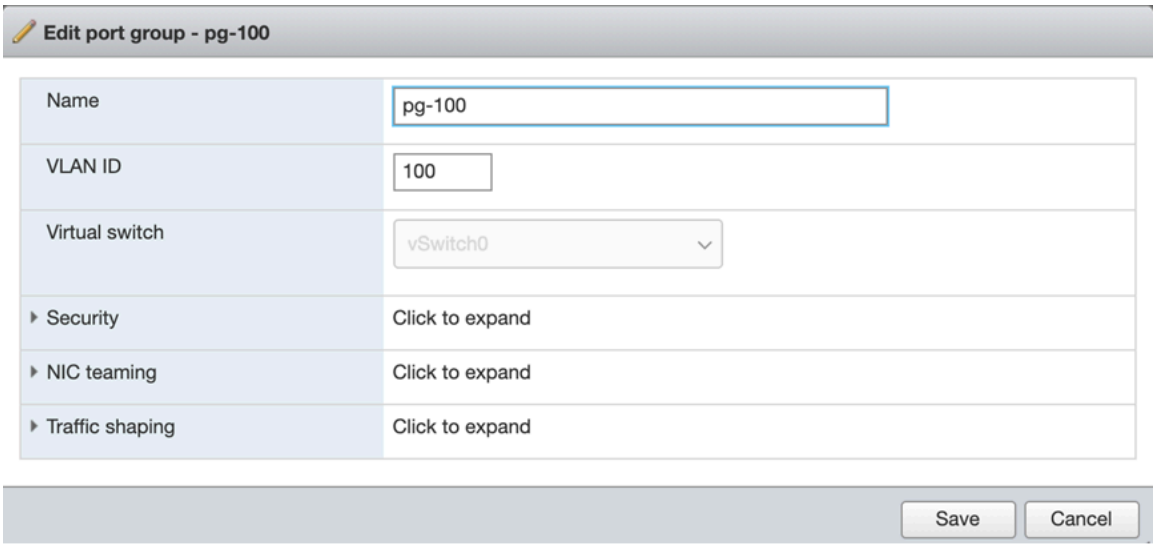


Par défaut, le pare-feu VM-Series sur ESXi fonctionne en mode VLAN tronc (trunk).

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Sur le système hôte, configurez la fonction physique et virtuelle pour fonctionner en mode d'accès VLAN.

1. Cliquez sur **Networking (Mise en réseau)** dans l'inventaire du client hôte VMware et cliquez sur **Port groups (Groupes de ports)**.
2. Dans la liste que vous souhaitez modifier, cliquez avec le bouton droit sur le groupe de ports et sélectionnez **Edit settings (Modifier les paramètres)**. Entrez un nouveau **Name (Nom)** de groupe de ports. Entrez une nouvelle valeur pour le **VLAN ID (ID VLAN)**.



Pour obtenir les meilleures performances du pare-feu VM-Series, veillez à :

- *Activer l'épinglage du processeur (CPU Pinning).*
- *Désactiver la protection contre les relectures, si vous avez configuré des tunnels IPSec.*

  *Sur l'interface web du pare-feu, sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**, choisissez un tunnel IPSec, puis cliquez sur **General (Général)**, sélectionnez **Show Advanced Options (Afficher les options avancées)** et décochez **Enable Replay Protection (Activer la protection contre les relectures).***

STEP 2 | Accédez à la CLI sur le pare-feu VM-Series.

STEP 3 | Activez le mode d'accès VLAN.

```
request plugins vm-series vlan-mode access-mode on
```

on active le mode d'accès VLAN. Pour utiliser le mode VLAN tronc, saisissez **request plugins vm-series vlan-mode access-mode off**.

STEP 4 | Redémarrez le pare-feu.

```
request restart system
```

STEP 5 | Vérifiez la configuration du mode VLAN.

```
show plugins vm-series vlan-mode
```

 ©2023 Palo Alto Networks, Inc.

Activation de la prise en charge de files d'attente multiples pour les cartes réseau sur ESXi

Les files d'attente multiples permettent aux performances du réseau d'évoluer avec le nombre de processeurs virtuels et permet le traitement parallèle des paquets en créant plusieurs files d'attente TX et RX. Modifiez le fichier .vmx ou accédez aux paramètres avancés pour activer les files d'attente multiples.

STEP 1 | Activez les files d'attente multiples.

1. Ouvrez le fichier .vmx.
2. Ajoutez le paramètre suivant :

```
ethernetX.pnicFeatures = "4"
```

STEP 2 | Activez la mise à l'échelle côté réception (RSS).

1. Connectez-vous à la CLI de l'hôte ESXi.
2. Exécutez la commande suivante :

```
$ vmkload_mod -u ixgbe $ vmkload_mod ixgbe RSS="4,4,4,4,4,4"
```

STEP 3 | Pour des performances optimales, allouez des threads de processeur supplémentaires par périphérique Ethernet/vSwitch. Cela est limité par la quantité de ressources du processeur disponibles sur l'hôte ESXi.

1. Ouvrez le fichier .vmx.
2. Ajoutez le paramètre suivant :

```
ethernetX.ctxPerDev = "1"
```

Réglage des performances du VNF

Cette rubrique fournit des indications sur le réglage du VNF pour les déploiements VM-Series. Elle sert de référence pour vous permettre de choisir certains des réglages de paramètres pour un déploiement VM-Series. Avant de tenter le réglage, vous devez vous familiariser avec les étapes d'installation du pare-feu VM-Series sur l'hyperviseur VMware vSphere (ESXi), y compris la manière de configurer les paramètres de réglage et les attributs.

Il est possible que ces indications ne s'appliquent pas aux déploiements VM-Series sur des environnements de boîte blanche ou de boîte grise ciblant les cas d'utilisation SD-WAN, MSSP ou CSSP.

Le VM-Series est un appareil haute performance disponible dans plusieurs facteurs de forme selon la taille, l'empreinte de l'hyperviseur et l'emplacement du déploiement dans un cloud privé ou public.

Les modifications de la configuration au niveau global et au niveau de l'hôte affectent les autres VM qui s'exécutent sur le même hôte. Vous devez prendre en considération les compromis et choisir avec soin les paramètres qui conviennent le mieux à votre déploiement.

 ©2023 Palo Alto Networks, Inc.

- Paramètres de réglage ESXi
- Cas pratiques
- Références

Paramètres de réglage ESXi

Pour obtenir les meilleurs résultats de performance sur VM-Series, vous pouvez régler les paramètres E/S matériels, de l'hyperviseur et du réseau.

Les paramètres mentionnés ici ne s'appliquent pas à tous les modèles de déploiement.

- Paramètres BIOS
- Paramètres physiques
- Paramètres d'interface réseau virtuelle
- Considérations sur NUMA et les ressources

Paramètres BIOS

Cette section recommande les paramètres de gestion de l'alimentation, d'hyperthreading et d'Intel VT-D du BIOS susceptibles d'améliorer les performances du pare-feu VM-Series, et propose un exemple de configuration du BIOS en conclusion.

- Gestion de l'alimentation
- Hyperthreading
- Intel Virtualization Technology for Directed I/O
- Exemple de configuration du BIOS

Gestion de l'alimentation

Pour les applications sensibles à la latence, toute forme de gestion de l'alimentation ajoute de la latence au chemin où un système inactif (dans l'un des différents modes d'économie d'énergie) répond à un événement externe. VMware recommande de régler le paramètre de gestion de l'alimentation du BIOS sur « static high performance » (performance élevée statique) (aucune gestion de l'alimentation contrôlée par le système d'exploitation), ce qui désactive toute forme de gestion active de l'alimentation. Les serveurs de classe Intel Nehalem et les processeurs ultérieurs (Intel Xeon 55x et ultérieurs) proposent deux options de gestion de l'alimentation : C-states et Intel Turbo Boost.

Le fait de laisser les C-states activés peut augmenter la latence de la mémoire et n'est donc pas recommandé pour les charges de travail à faible latence. Même le C-state amélioré, appelé C1E, introduit des latences plus longues pour faire passer les processeurs de l'état inactif à la pleine puissance. VMware recommande de désactiver le C1E dans le BIOS pour réduire encore les latences.

- Pour HP, définissez le mode de régulation de l'alimentation en mode élevé statique et désactivez le processeur QPI, la prise en charge du C-state et la prise en charge du C1E.
- Pour Dell, réglez la mode de gestion de l'alimentation, l'alimentation du processeur et la gestion des performances sur les performances maximales.

Les P-states sont un autre paramètre à prendre en compte. Pour des considérations purement axées sur les performances, désactivez les paramètres de P-state dans le BIOS.

 ©2023 Palo Alto Networks, Inc.

Intel Turbo Boost peut entraîner des variations de performances au fil du temps. Pour des performances constantes et déterministes, désactivez Turbo Boost.

Hyperthreading

Si le matériel et le BIOS prennent en charge l'hyperthreading, ESXi active automatiquement l'hyperthreading sur les hôtes. Pour des performances optimales des pare-feu VM-series, désactivez l'hyperthreading sur les hôtes ESXi.

Si l'environnement de déploiement justifie l'activation de l'hyperthreading, assurez-vous que toutes les ressources du processeur pour le pare-feu VM-Series sont réservées pour le même nœud de NUMA/Socket qui a accès aux périphériques PCI.

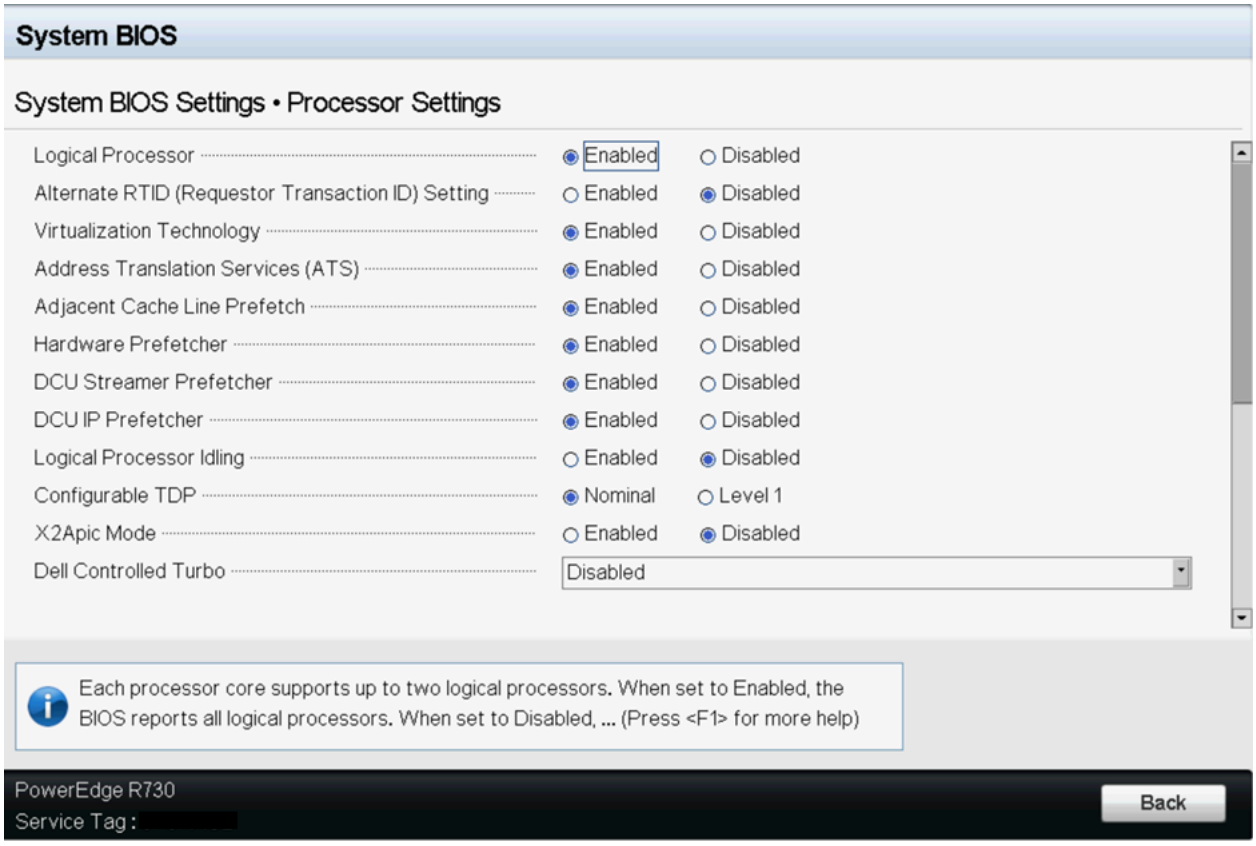
En règle générale, configurez la VM PA comme une VM NUMA unique. Pour plus d'informations, reportez-vous à la section Considérations sur NUMA et les ressources.

Intel Virtualization Technology for Directed I/O

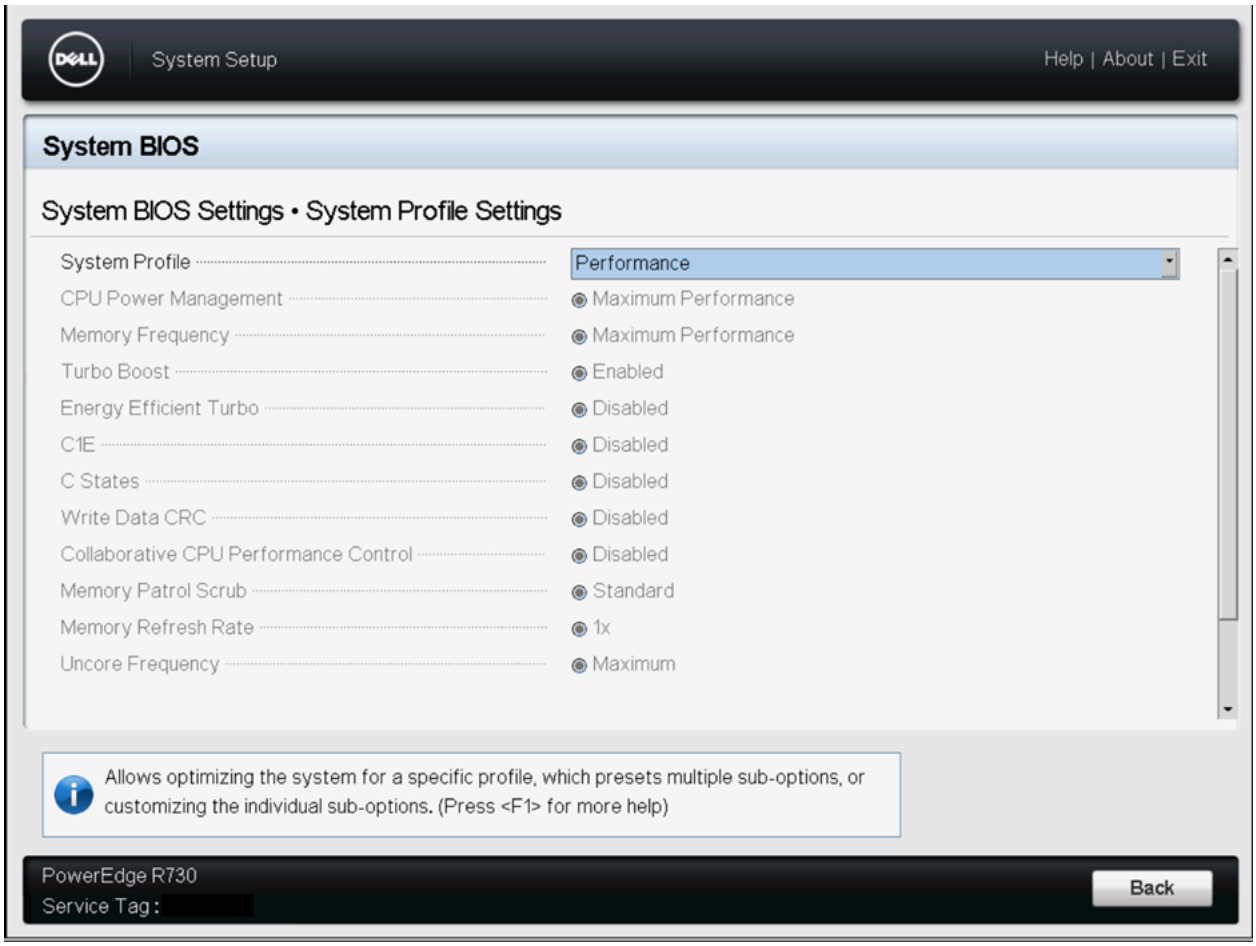
Intel Virtualization Technology for Directed I/O (Intel VT-D) permet d'affecter une carte LAN à un système invité, ce qui permet d'augmenter les performances du réseau au-delà de celles d'une carte LAN émulée. Activez cette fonctionnalité dans le BIOS. Si vous comptez tirer profit de SR-IOV pour les performances (recommandé), activez le paramètre BIOS SRI-OV.

Exemple de configuration du BIOS

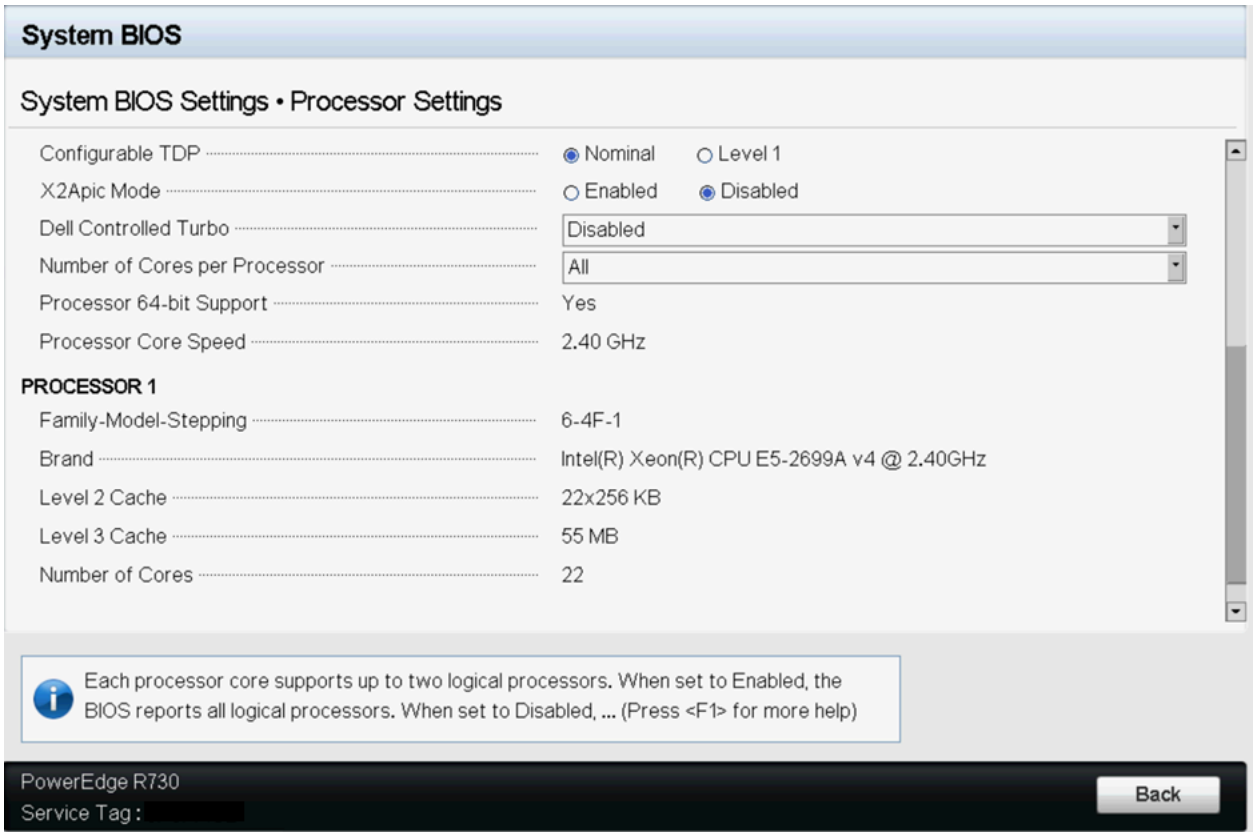
Les captures d'écran qui suivent montrent les paramètres de profil du système et les paramètres du processeur pour un BIOS Dell.



 ©2023 Palo Alto Networks, Inc.



 ©2023 Palo Alto Networks, Inc.



Paramètres physiques

La plupart des interfaces réseau (NIC) 1GbE ou 10GbE prennent en charge une fonctionnalité appelée modération des interruptions ou limitation des interruptions, qui fusionne les interruptions de l'interface réseau vers l'hôte, de manière à éviter que l'hôte ne soit submergé et n'utilise tous ses cycles de processeur pour traiter les interruptions. Cependant, pour les charges de travail sensibles à la latence, la durée pendant laquelle l'interface réseau reporte la livraison d'une interruption pour un paquet reçu ou un paquet correctement envoyé sur le câble est la durée qui augmente la latence de la charge de travail. Pour des performances optimales sur PA-VM, désactivez la modération des interruptions. Par exemple, désactivez la modération des interruptions de l'interface réseau physique sur l'hôte ESXi en procédant comme suit :

```
# esxcli system module parameters set -m ixgbe -p
 "InterruptThrottleRate=0"
```

- File d'attente de transmission
- Couplage de file d'attente

File d'attente de transmission

La couche physique de la pNIC montante ESXi maintient également une file d'attente Tx logicielle des paquets mis en file d'attente pour la transmission, qui contient 500 paquets par défaut. Si la charge de travail est intensive en E/S avec des pics importants de paquets transmis, cette file d'attente peut déborder et des paquets peuvent être lâchés dans la couche montante. La taille de la file d'attente Tx peut être augmentée jusqu'à 10 000 paquets à l'aide de la commande ESXi suivante :

©2023 Palo Alto Networks, Inc.

```
# esxcli system settings advanced set -i 10000 -o /Net/
MaxNetifTxQueueLen
```

En fonction de l'interface réseau physique et de la version spécifique du pilote ESXi utilisé sur l'hôte ESXi, il arrive que des paquets soient lâchés dans le pilote de la pNIC parce que l'anneau de transmission sur la pNIC est trop petit et est plein. La plupart des pilotes de pNIC vous permettent d'augmenter la taille de l'année de transmission à l'aide de la commande suivante :

```
# ethtool -G vmnic0 tx 4096
```

Cette commande augmente la taille de l'année Tx à 4 096 entrées. La taille maximale que vous pouvez définir pour un pilote de pNIC spécifique, ainsi que la taille d'anneau Tx actuelle effective, peuvent être déterminées à l'aide de la commande suivante :

```
# ethtool -g vmnic0
```

```
Ring parameters for vmnic0: Pre-set maximums: RX: 4096 RX Mini: 0 RX
 Jumbo: 0 TX: 4096 Current hardware settings: RX: 512 RX Mini: 0 RX
 Jumbo: 0 TX: 4096
```

Couplage de file d'attente

Certains pilotes de pNIC, comme l'ixgbe d'Intel et le bnx2x de Broadcom, prennent également en charge le « couplage de file d'attente », qui indique à la couche montante ESXi que le thread de réception (NetPoll) traitera également l'achèvement des paquets transmis sur une file d'attente de transmission couplée. Pour certaines charges de travail comportant beaucoup de transmissions, cela peut entraîner des retards de traitement des achèvements de transmissions, ce qui fait que l'anneau de transmission pour la vNIC n'a pas suffisamment d'espace pour transmettre des paquets supplémentaires, et force le pilote de vNIC dans le système d'exploitation invité à lâcher des paquets.

La désactivation du couplage de file d'attente pour toutes les pNIC sur un hôte ESXi crée un thread distinct pour le traitement des achèvements de transmission pNIC. Par conséquent, les achèvements sont traités rapidement, ce qui libère de l'espace dans l'anneau de transmission de la vNIC pour transmettre des paquets supplémentaires.

La commande ESXi pour désactiver le couplage de file d'attente est la suivante :

```
# esxcli system settings advanced set -o /Net/
NetNetqRxQueueFeatPairEnable -i 0
```

Pour que celle-ci prenne effet, vous devez redémarrer l'hôte ESXi.

Si PCI-Pass-Thru sur VM-700 est utilisé sur un hôte dédié, aucun réglage de performance de l'interface réseau / du pilote de l'interface réseau n'est nécessaire. Cependant, ce mode de déploiement n'est pas courant.

©2023 Palo Alto Networks, Inc.

Paramètres d'interface réseau virtuelle

Si possible, utilisez SR-IOV pour des performances améliorées, comme expliqué dans les rubriques suivantes :

- SR-IOV
- VMXNET3/vSwitch et fusion des interruptions virtuelles
- Activer la prise en charge des files d'attente multiples sur Intel x710/x520

SR-IOV

- La modification des paramètres de module pour un pilote SR-IOV nécessite de redémarrer l'hôte ESXi.
- Désactivez la modération des interruptions de l'interface réseau physique sur l'hôte ESXi en procédant comme suit :

```
# esxcli system module parameters set -m ixgbe -p
 "InterruptThrottleRate=0“
```

- Si vous activez la prise en charge des files d'attente multiples, vous devez également activer la mise à l'échelle côté réception (RSS) pour le pilote.
  - Pour activer la RSS, définissez la valeur du port sur 4.
  - Spécifiez les ports à l'aide d'une chaîne séparée par des virgules.

  Exemple : définissez 3 interfaces réseau avec 2 ports chacune.

```
$ vmkload_mod -u ixgbe esxcli system module parameters set -m ixgbe
 -p RSS=”4,4,4,4,4,4”
```

```
$ vmkload_mod ixgbe RSS=”4,4,4,4,4,4”
```

  Exemple : définissez une RSS pour un port unique :

```
$ vmkload_mod -u ixgbe esxcli system module parameters set -m ixgbe
 -p RSS=”0,4,0,0,0,0”
```

VMXNET3/vSwitch et fusion des interruptions virtuelles

Par défaut, VMXNET3 prend en charge un algorithme de fusion des interruptions (pour les mêmes raisons que les interfaces réseau physiques mettent en œuvre la modération des interruptions). Pour éviter que le système hôte soit inondé de trop nombreuses interruptions, les paquets sont collectés et une seule interruption est générée pour plusieurs paquets. C'est ce que l'on appelle la fusion des interruptions.

La fusion des interruptions se réfère au volume de trafic reçu par un réseau, ou à la durée écoulée après que le trafic a été reçu, avant que vous appliquez un interruption. Les interruptions trop précoces ou trop fréquentes entraînent des performances médiocres du système, car le noyau arrête (ou « interrompt ») une tâche en cours pour traiter la demande d'interruption du matériel. Une interruption trop tardive peut entraîner une perte de trafic si le trafic n'est pas retiré de l'interface

 ©2023 Palo Alto Networks, Inc.

réseau suffisamment tôt – du trafic supplémentaire arrive, écrasant le trafic précédent qui attend toujours d'être reçu dans le noyau. Pour désactiver cette fonctionnalité à l'aide du client Web vSphere, accédez à **VM Settings (Paramètres VM)** > **Options** > **Advanced General (Général avancé)** > **Configuration Parameters (Paramètres de configuration)**et ajoutez une entrée pour **`ethernetX.coalescingScheme`** avec la valeur **`désactivé`**.

Pour désactiver la fusion des interruptions virtuelles pour toutes les interfaces réseau virtuelles sur l'hôte (ce qui affecte toutes les VM, pas uniquement celles qui sont sensibles à la latence), définissez l'option de performances réseau avancée. Accédez à **Configuration** > **Advanced Settings (Paramètres avancés)** > **Net (Réseau)** et définissez **`CoalesceDefaultOn`** sur **`0`** (désactivé).

Activer la prise en charge des files d'attente multiples sur Intel x710/x520

Utilisez ESXi version 6.0.0 ou ultérieure, avec une version du pilote ixgbe avec prise en charge des files d'attente multiples. Voir Versions du pilote SR-IOV dans la matrice de compatibilité. Modifiez le fichier `.vmx` ou accédez aux **Advanced Settings (Paramètres avancés)** pour activer la prise en charge des files d'attente :

```
ethernetX.pnicFeatures = “4”
```

Pour définir l'affinité multicœur de manière à ce que vSwitch puisse dépasser 300 000 PPS, définissez :

```
ethernetX.pnicFeatures = "4" ethernetX.ctxPerDev = "1"
```

Le paramètre **`ethernetX.ctxPerDev = “1”`** fonctionne comme un indicateur binaire (définissez sur 1 pour activer). L'indicateur binaire ajoute un thread de processeur pour gérer le trafic uniquement depuis le port **`ethernetX`**. Cela permet d'améliorer les performances de planification du trafic.

Considérations sur NUMA et les ressources

NUMA signifie Non-Uniform Memory Access (accès mémoire non uniforme). Les processeurs multicœurs ont des conceptions complexes. Pour gérer les problèmes de performances de ces systèmes, vous devez connaître toutes les nuances relatives au NUMA et à l'épinglage de processeur. Aspects essentiels à prendre en compte :

- Sur quels cœurs nos threads s'exécutent-ils ? (si l'hyperthreading est activé, vérifiez Hyperthreading)
- Sur quels cœurs nos vCPU s'exécutent-ils ? (affinité)
- Dans quel socket NUMA la carte d'interface réseau physique est-elle installée ?
- Où la mémoire a-t-elle été allouée ? (effets NUMA)

  Les threads qui s'exécutent sur un socket voient un seul espace de mémoire unifié – ils peuvent donc lire/écrire dans une mémoire locale des autres sockets.
- La mémoire est-elle partagée entre différents sockets sur un nœud ?

©2023 Palo Alto Networks, Inc.

- Cela prend plus de temps pour accéder à la mémoire sur différents sockets que pour accéder à la mémoire locale.

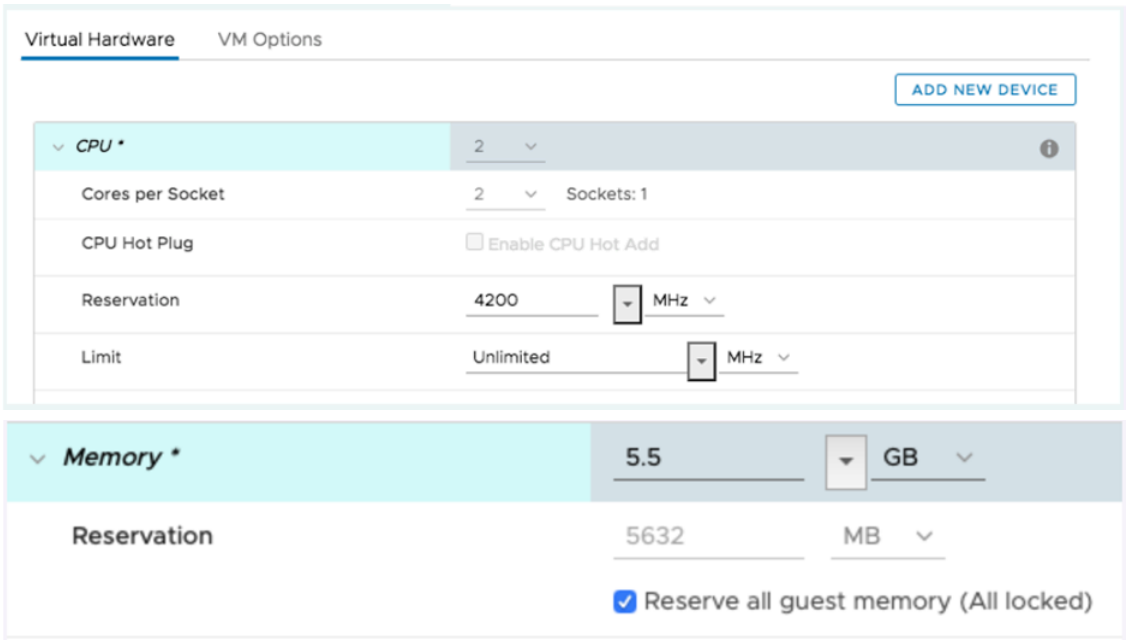
  Les effets NUMA se produisent lorsque les threads accèdent de manière excessive à la mémoire sur un domaine NUMA différent. Pour éviter les problèmes entre plusieurs NUMA, évitez le Quick Path Interconnect (QPi) entre la communication du socket 0 et le socket 1.

Pour les VM sensibles à la latence comme la PA-VM, VMware vous recommande de ne pas surcharger les vCPU par rapport au nombre de processeurs physiques sur l'hôte ESXi. Par exemple, si l'hôte comporte 8 cœurs de processeur, limitez le nombre de vCPU pour votre VM à 7. Ceci garantit que le planificateur ESXi VMkernel a une chance accrue de placer les vCPU sur des pCPU qui ne gèreront pas d'autres contextes de planification, comme les vCPU issus d'autres VM ou les mondes d'assistance ESXi. Il est recommandé de s'assurer que le nombre de vCPU que vous allouez à la VM ne dépasse pas le nombre de processus ou de threads actifs consommant des processeurs dans la VM.

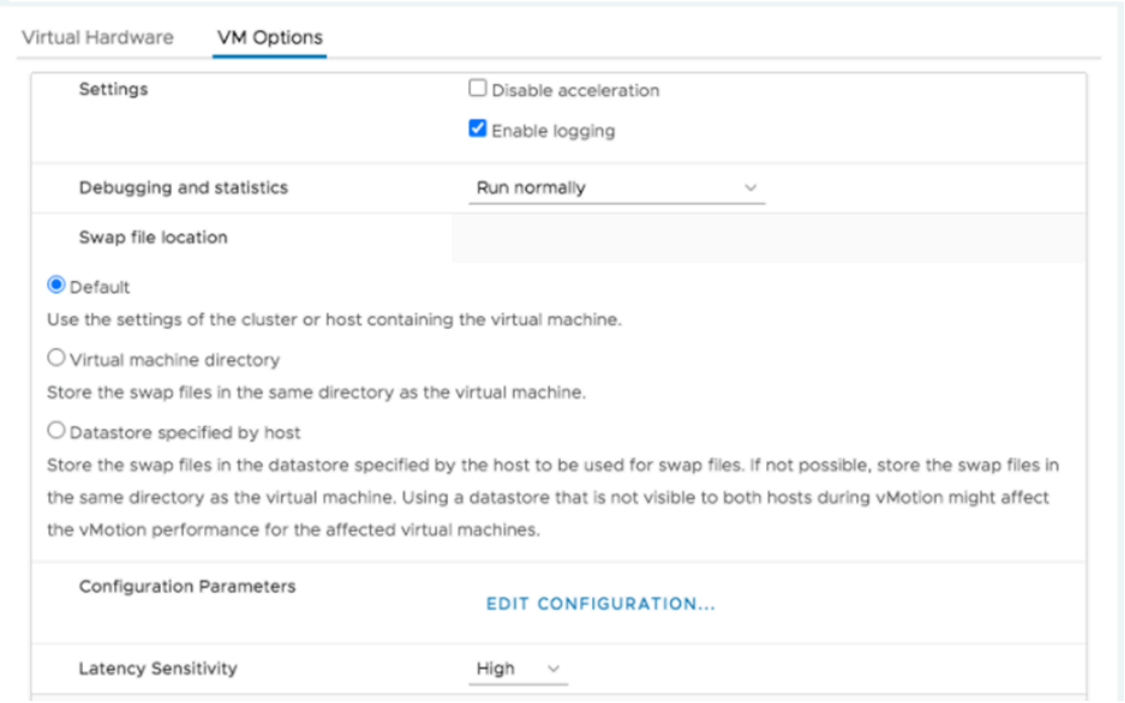
Pour des performances optimales, tous les vCPU doivent être planifiés sur le même nœud NUMA et la totalité de la mémoire de VM doit correspondre et être allouée à partir de la mémoire physique locale associée à ce nœud NUMA. Il est possible de modifier cette configuration à l'aide du paramètre de VM **`numa.nodeAffinity=0, 1, …`**, où 0, 1, etc. correspondent aux numéros de sockets.

Pour vous assurer que la VM bénéficie d'un accès exclusif aux ressources du processeur, définissez Latency Sensibility (Sensibilité à la latence) sur High (Élevée). Pour que le nouveau paramètre prenne effet, la réservation du processeur VM doit être réglée au maximum, la mémoire doit être réservée et la limite du processeur doit être définie comme illimitée.

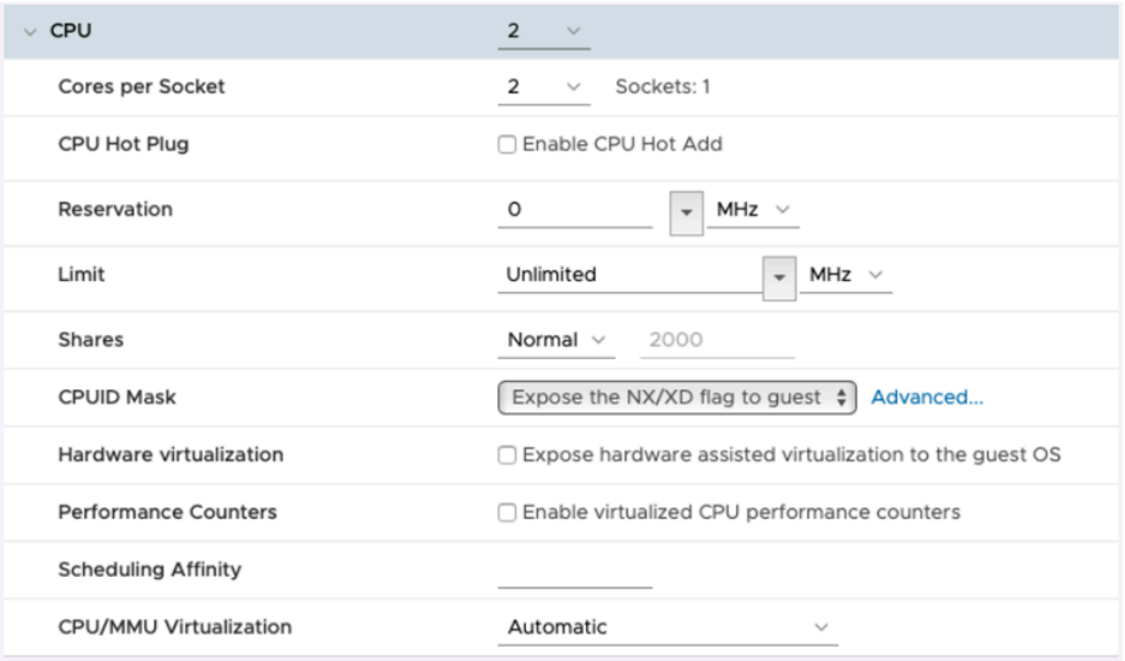
- Dans les versions plus récentes, utilisez le client Web vSphere pour définir l'option de sensibilité à la latence de la VM sur High (Élevée) (la valeur par défaut est Normal [Normale]).
- Dans les versions antérieures, définissez **`sched.cpu.latencySensitivity`** sur High (Élevée).



 ©2023 Palo Alto Networks, Inc.



En outre, les vCPU de VM peuvent être épinglés pour héberger des cœurs de processeur à l'aide du réglage de VM **Host Affinity (Affinité de l'hôte)**, de manière à ce qu'ils ne soient jamais planifiés sur des cœurs différents. Gardez la NUMA et l'hyperthreading à l'esprit lorsque vous utilisez l'affinité de l'hôte. Évitez de définir l'affinité de l'hôte si le système est surchargé. Pour plus de détails, voir Potential Issues with CPU Affinity (Problèmes potentiels liés à l'affinité du processeur).



Après avoir appliqué les paramètres de réglage, utilisez esxtop ou les graphiques de processeur pour vérifier CPU Ready (%RDY) et Co Stop (%CSTP) pour la VM. Les deux valeurs doivent être proches de 0 % pour garantir un accès exclusif aux ressources du processeur. Vous pouvez également utiliser esxtop pour vérifier l'utilisation de NUMA et vous assurer que les ressources de la mémoire pour

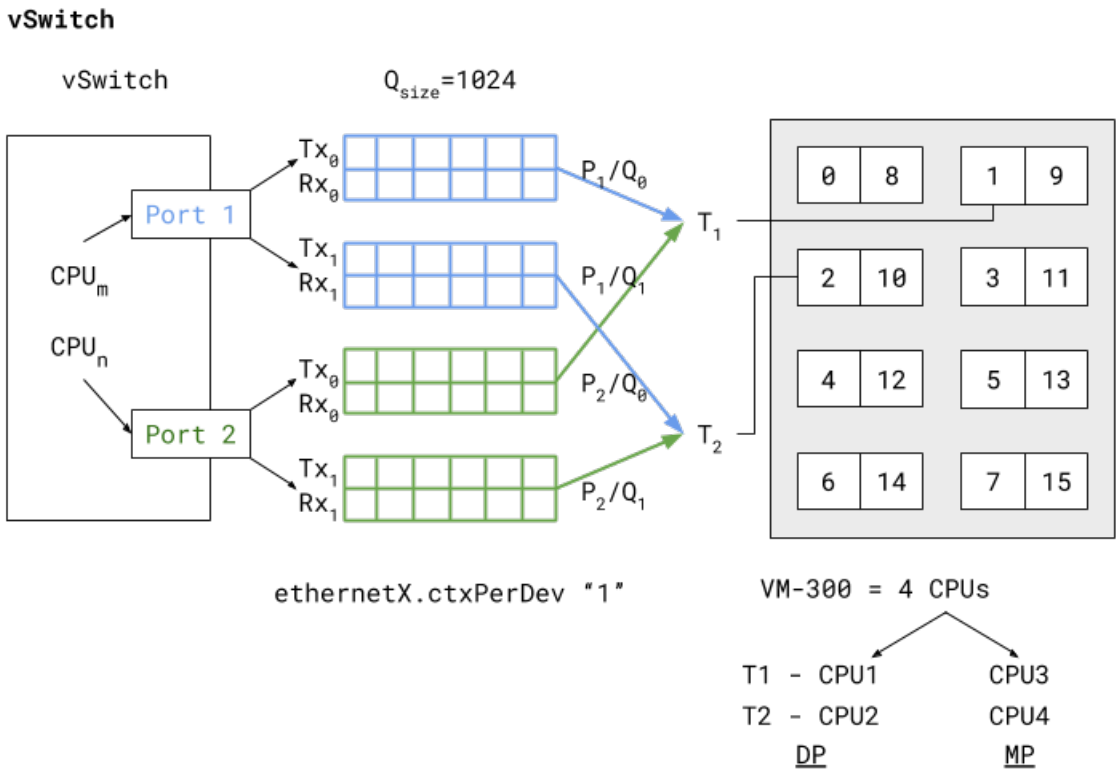
 ©2023 Palo Alto Networks, Inc.

la VM ne sont pas réparties entre les nœuds NUMA. Pour plus de détails, voir Interprétation des statistiques esxtop.

Cas pratiques

Cas pratique 1 ; déploiement de vSwitch

La figure ci-dessous montre un déploiement de PA-VM sur un hôte ESXi où les ports de données « Port 1 » et « Port 2 » sont liés à eth1 et eth2 de la PA-VM. Chaque port héberge deux paires de file d'attente (par exemple, Tx0/Rx0 et Tx1/Rx1) ou a l'option de file d'attente multiple activée.



L'activation de la file d'attente multiple et du RSS pour les paquets d'équilibrage de charge envoyés vers / reçus à partir de plusieurs files d'attente améliore les performances de traitement. Selon la logique interne du mappage du vCPU vers le port / la file d'attente (dans cas), les paquets qui arrivent et sont envoyés depuis P1/Q0 et P2/Q0 sont traités par la tâche T1 du plan de données qui s'exécute sur (c'est-à-dire, qui est épinglée à) vCPU1. La tâche T2 du plan de données suit une association similaire, comme illustré sur le schéma de déploiement de vSwitch.

Les deux tâches du plan de données s'exécutent sur vCPU1 et vCPU2 et il s'agit de processeurs non frères et sœurs (ce qui signifie qu'ils ne partagent pas le même cœur en cas d'hyperthreading). Cela signifie que même lorsque l'hyperthreading est activé, la tâche affectée peut être épinglée à différents cœurs pour des performances élevées. Ces vCPU de tâche de plan de données appartiennent également tous au même nœud (ou socket) NUMA pour éviter les problèmes de performances liées au NUMA.

Il est possible de résoudre deux autres goulots d'étranglement des performances en augmentant la taille des files d'attente et en dédiant un vCPU ou un thread aux ports qui planifient le trafic vers et depuis ces ports. Augmenter la taille des files d'attente (Qsize) permet de gérer les pics soudains et importants de trafic et d'empêcher les pertes de paquets lors d'un trafic en rafales. L'ajout d'un thread CPU dédié (**`ethernetX.ctxPerDev = 1`**) au traitement des paquets au niveau du port

 ©2023 Palo Alto Networks, Inc.

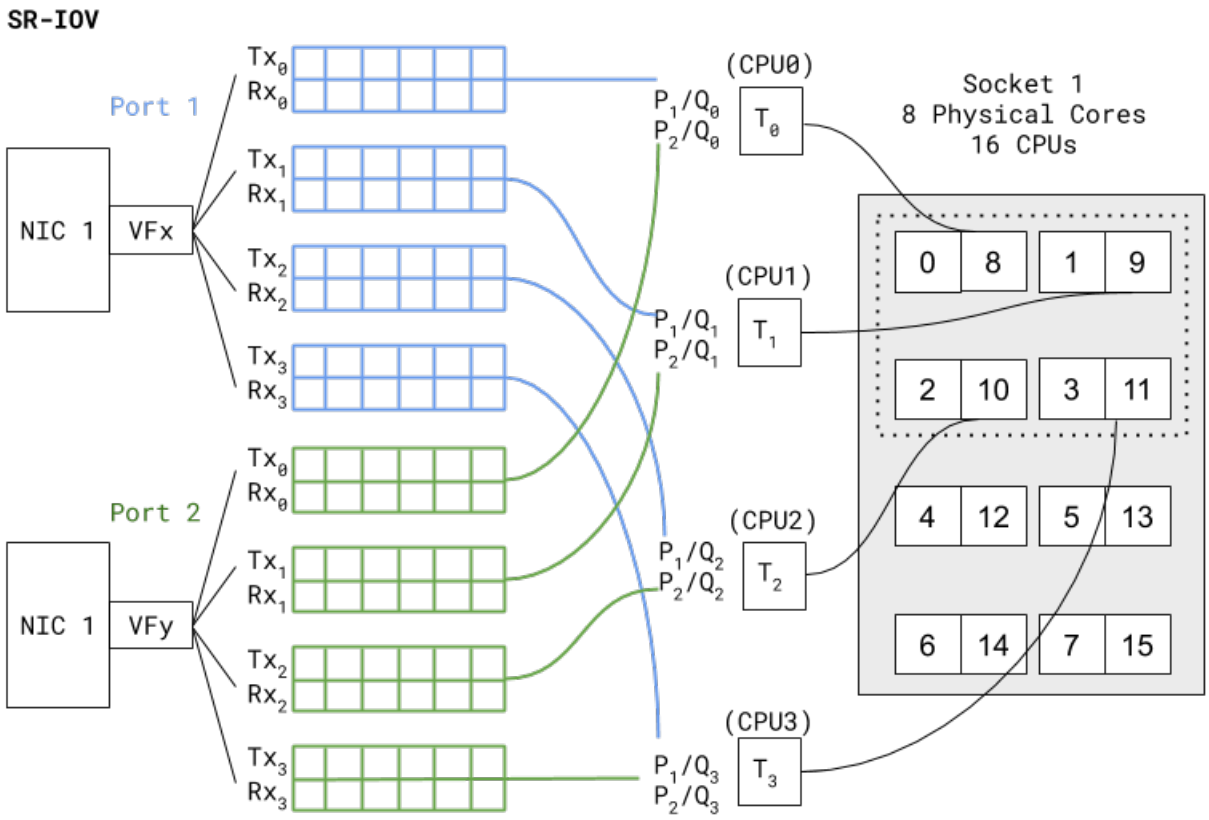
permet de traiter le trafic à un rythme plus élevé, ce qui augmente le débit du trafic pour atteindre un débit linéaire.

La technique de traitement des paquets PA-VM détermine également les performances. Elle peut être configurée comme DPDK ou PacketMMAP. DPDK utilise un pilote de mode de sondage (en fonction du type de pilote) pour sonder de manière constante pour détecter les paquets reçus dans les files d'attente. Ceci permet d'améliorer les performances de débit. En fonction de la période de sondage, la latence est observée par les paquets. Si le sondage est continu (sondage actif d'un paramètre à partir de la CLI PANOS), l'utilisation du vCPU pour les tâches du plan de données sera de 100 % mais délivrer les meilleures performances. Au niveau interne, le logiciel utilise une durée de sondage d'une milliseconde pour éviter d'utiliser inutilement les ressources du processeur.

De son côté, PacketMMAP affiche des performances moindres que DPDK mais fonctionne avec n'importe quels pilotes au niveau du réseau. Pour DPDK, le pilote vSwitch doit prendre en charge DPDK. PacketMMAP fonctionne avec des interruptions qui surviennent lorsqu'un paquet est reçu par le port et placé dans la file d'attente de réception. Cela signifie que pour tous les paquets, ou groupes de paquets, les interruptions surviennent et les paquets sont retirés de la file d'attente de réception pour être traités. Cela entraîne une latence plus faible lors du traitement des paquets, mais un débit réduit, car les interruptions doivent être traitées à chaque fois, ce qui entraîne une surcharge plus élevée du processeur. En règle générale, PacketMMAP aura une latence de traitement des paquets plus faible que DPDK (sans modification de sondage actif).

Cas pratique 2 : Déploiement de SR-IOV

Le schéma de SR-IOV ci-dessous montre un déploiement PAVM similaire au cas pratique de vSwitch, mais en mode SR-IOV.



 ©2023 Palo Alto Networks, Inc.

Dans SR-IOV, le port de l'interface réseau physique compatible (se manifeste sous la forme d'une fonction physique) est en fait découpé en plusieurs interfaces (se manifeste sous la forme de fonctions virtuelles). La figure ci-dessus montre que le NIC1 Port1 comporte une VF appelée VFX qui est associée comme l'une des interfaces de plan de données PAVM – eth1, par exemple. Une association similaire est créée pour Port2 VF vers PAVM eth2. La chaîne de traitement des paquets est similaire à celle du déploiement dans l'environnement vSwitch. La seule différence tient au fait que les pilotes SR-IOV VF doivent être compatibles avec ceux qui sont utilisés dans PAN-OS. De même, étant donné qu'il n'y a aucun vSwitch interne (dans l'hôte) qui commute le trafic, il n'est pas nécessaire de définir un thread dédié pour planifier le trafic depuis un port (autrement dit, **`ethernetX.ctxPerDev = 1`** n'est pas nécessaire avec ce réglage). Les interfaces avec SR-IOV et DPDK offriront des performances de traitement des paquets plus élevées que le cas pratique de vSwitch.

Références

- Réglage de VMware vCloud NFV pour des charges de travail intensives en données
- Meilleures pratiques pour le réglage des performances des charges de travail Telco et NFV dans vSphere
- Problèmes potentiels liés à l'affinité du processeur
- Interprétation des statistiques esxtop

 ©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur vCloud Air

Le pare-feu VM-Series peut être déployé dans un centre de données virtuel (vDC) sur vCloud Air via le portail vCloud Air, à partir du portail vCloud Director ou via l'API vCloud Air.

- À propos du pare-feu VM-Series sur vCloud Air
- Déploiements pris en charge sur vCloud Air
- Déploiement du pare-feu VM-Series sur vCloud Air

À propos du pare-feu VM-Series sur vCloud Air

Vous pouvez déployer le pare-feu VM-Series dans un centre de données virtuel (vDC) sur VMWare vCloud Air via le portail vCloud Air ou à partir du portail vCloud Director. Et pour gérer de façon centralisée tous vos pare-feu physiques et VM-Series, vous pouvez utiliser un Panorama existant ou déployer un nouveau Panorama sur le site ou sur vCloud Air.

Le pare-feu VM-Series sur vCloud Air nécessite les éléments suivants :

- La version ESXi de l'image logicielle, un fichier Open Virtualization Alliance (OVA), depuis le site Web d'assistance client de Palo Alto Networks. Actuellement, vCloud Air Marketplace n'héberge pas l'image logicielle.

  Insérez l'image logicielle du pare-feu VM-Series dans un vApp afin de déployer ce dernier efficacement. Un vApp est un contenant pour les appareils virtuels préconfigurés (machines virtuelles et images de systèmes d'exploitation) qui est géré comme un seul objet. Par exemple, si votre vApp englobe un ensemble d'applications multiniveaux ainsi que le pare-feu VM-Series, chaque fois que vous déployez le vApp, le pare-feu VM-Series sécurise automatiquement le serveur Web et le serveur de base de données qui sont déployés en même temps que le vApp.
- Les licences et les abonnements de type « Bring Your Own License » (BYOL) peuvent être achetés auprès des partenaires, des revendeurs ou directement de Palo Alto Networks ; les licences d'utilisation ne sont pas offertes pour les pare-feu VM-Series déployés dans vCloud Air.
- En raison des contraintes de sécurité de vCloud Air, la meilleure façon de déployer le pare-feu VM-Series sur vCloud Air se fait via des interfaces de couche 3, et l'utilisation de l'adresse MAC attribuée par l'hyperviseur doit être activée sur les interfaces. Si vous n'activez pas l'utilisation de l'adresse MAC attribuée par l'hyperviseur, le vSwitch VMWare ne peut transférer le trafic vers les interfaces du plan de données sur le pare-feu VM-Series car le vSwitch sur vCloud Air ne prend pas en charge le mode de proximité ou les fausses transmissions MAC. Le pare-feu VM-Series ne peut être déployé avec des interfaces robinet, de couche 2 ou de câble virtuel.

Le pare-feu VM-Series peut être déployé sur vCloud Air en configuration haute disponibilité active/passive. Toutefois, le pare-feu VM-Series sur vCloud Air ne prend pas en charge les capacités de surveillance VM des machines virtuelles qui sont hébergées sur vCloud Air.

Pour tout savoir de vCloud Air, reportez-vous à la documentation qui porte sur VMware vCloud Air.

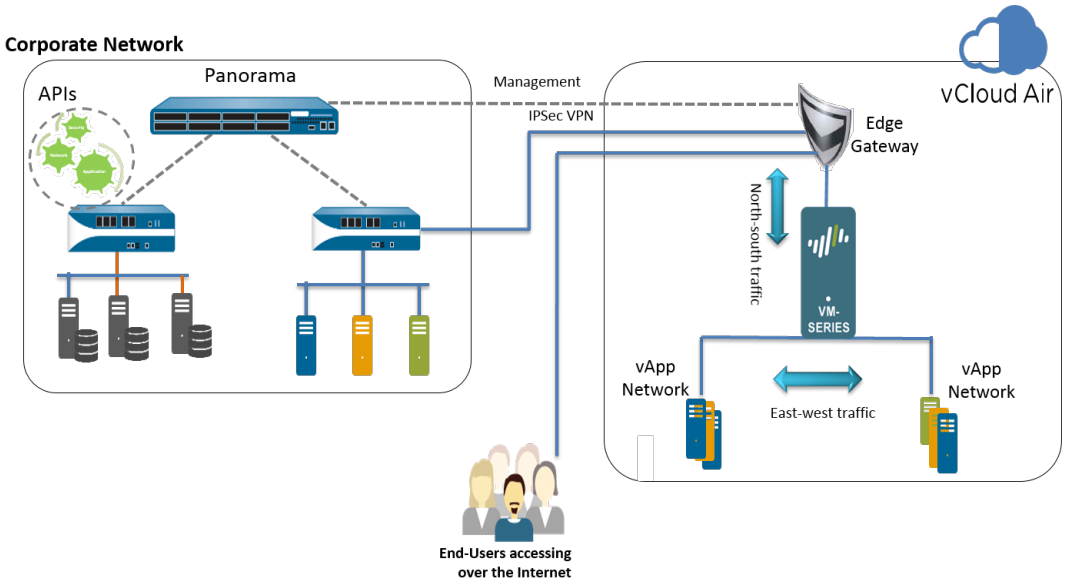
©2023 Palo Alto Networks, Inc.

Déploiements pris en charge sur vCloud Air

Afin d'activer des applications en toute sécurité, bloquez les menaces connues et inconnues. de plus, pour suivre l'évolution de votre environnement, vous pouvez déployer le pare-feu VM-Series sur vCloud Air avec des interfaces de couche 3 comme suit :

- **Sécuriser le périmètre du centre de données virtuel** : déployez le pare-feu VM-Series en tant que machine virtuelle qui connecte les réseaux isolés et routés sur vCloud Air. Dans ce déploiement, le pare-feu sécurise tout le trafic nord-sud qui passe par l'infrastructure sur vCloud Air.
- **Configurer un cloud hybride** : faites passer votre centre de données et votre cloud privé au vCloud Air et utilisez une connexion VPN pour permettre la communication entre le réseau d'entreprise et le centre de données. Dans ce déploiement, le pare-feu VM-Series utilise IPSec pour crypter le trafic et sécuriser l'accès au cloud.
- **Sécuriser le trafic entre les sous-réseaux d'application dans le vDC** : pour accroître la sécurité, segmentez votre réseau et isolez le trafic en créant des niveaux d'application, puis déployez le pare-feu VM-Series pour vous protéger contre les menaces latérales entre les sous-réseaux et les niveaux d'application.

L'illustration suivante combine les trois scénarios et inclut Panorama. Panorama rationalise les mises à jour de politique, centralise la gestion des politiques et met à votre disposition des journaux et des rapports centralisés.



 ©2023 Palo Alto Networks, Inc.

Déploiement du pare-feu VM-Series sur vCloud Air

Utilisez les instructions présentées dans cette section pour déployer votre pare-feu VM-Series sur un centre de données virtuel vDC géré sur demande ou dédié. Cette procédure suppose que vous avez configuré votre vDC, notamment les passerelles nécessaires pour laisser entrer et sortir le trafic du vDC, ainsi que les réseaux requis pour le routage du trafic de gestion et du trafic de données via le vDC.

STEP 1 | Téléchargez l'image OVA VM-Series depuis le site Web d'assistance client de Palo Alto Networks ; le vCloud Air Marketplace n'héberge pas l'image logicielle pour l'instant.

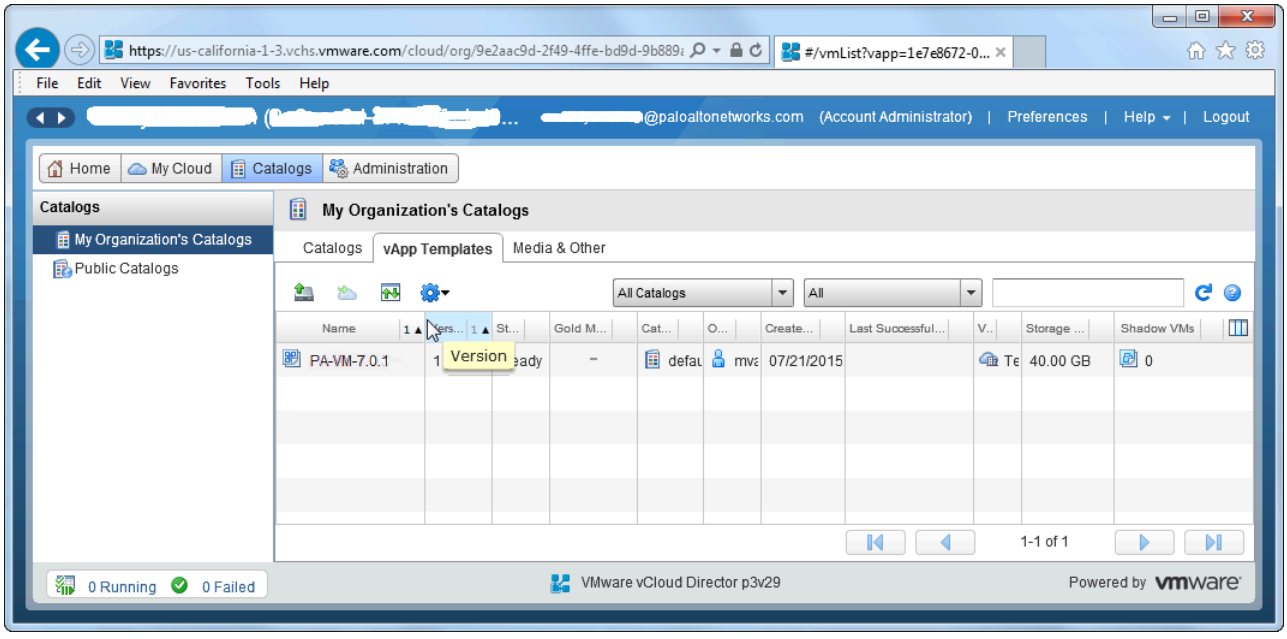
1. Accédez à www.paloaltonetworks.com/services/support.html.
2. Filtrez par **PAN-OS for VM-Series Base Images (Images de base PAN-OS pour VM-Series)** et téléchargez l'image OVA. Par exemple, PA-VM-ESX-9.1.0.ova.

STEP 2 | Effectuez l'extraction du fichier Open Virtualization Format (OVF) depuis l'image OVA et importez le fichier OVF dans votre catalogue vCloud Air.

Lors de l'extraction des fichiers de l'image OVA, assurez-vous de placer tous les fichiers (.mf, .ovf et .vmdk) dans le même dossier.

Pour les instructions sur l'extraction du fichier OVF depuis l'image OVA, reportez-vous à la documentation VMware : https://www.vmware.com/support/developer/ovf/#sthash.WUp55ZyE.dpuf

Lorsque vous importez le fichier OVF, l'image logicielle pour le pare-feu VM-Series est indiquée dans **My Organization's Catalogs (Catalogues de mon organisation)**.



©2023 Palo Alto Networks, Inc.

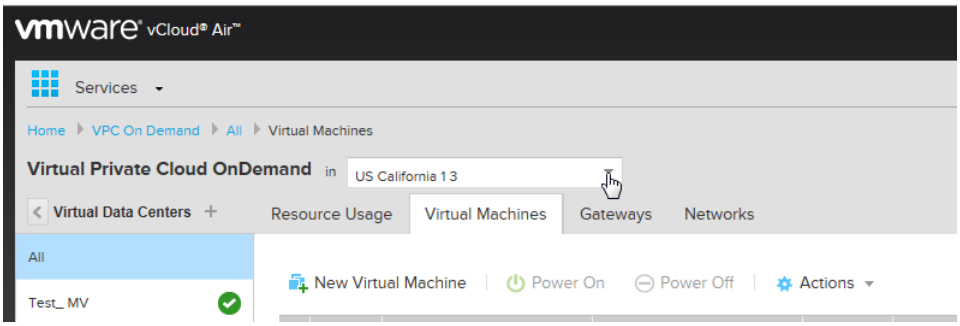
STEP 3 | Choisissez votre flux de travail.

Un vApp est un regroupement de modèles applicables aux appareils virtuel préconfigurés qui contiennent des machines virtuelles et d'images de systèmes d'exploitation.

- Si vous voulez créer un nouveau vDC et un nouveau vApp qui inclut le pare-feu VM-Series, reportez-vous à l'étape 4.
- Si vous avez déjà déployé un vDC et avez un vApp et que vous aimeriez ajouter le pare-feu VM-Series au vApp pour sécuriser le trafic, reportez-vous à l'étape 5

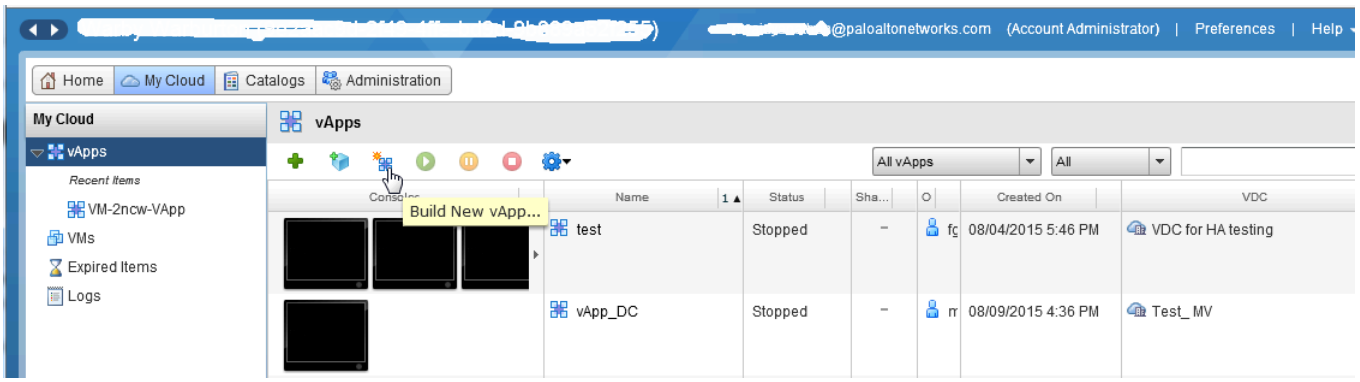
STEP 4 | Créez un vDC et un vApp qui comprend le pare-feu VM-Series.

1. Connectez-vous à vCloud Air.
2. Sélectionnez **VPC OnDemand (VPC sur demande)** et sélectionnez l'emplacement où vous souhaitez déployer le pare-feu VM-Series.



3. Sélectionnez **Virtual Data Centers (Centres de données virtuels)**, puis cliquez sur **+** pour ajouter un nouveau centre de données virtuel.
4. Sélectionnez le vDC, cliquez sur le bouton de droite, puis sélectionnez **Gérer les catalogues dans vCloud Director**. Vous serez rédigé vers l'interface Web de vCloud Director.
5. Créez un nouveau vApp qui contient une ou plusieurs machines virtuelles, dont le pare-feu VM-Series :

   1. Sélectionnez **My Cloud (Mon cloud)** > **vApps**, puis cliquez sur **Build New vApp (Créer un nouveau vApp)**.



   2. Sélectionnez **Name and Location (Nom et emplacement)**, puis sélectionnez le **Virtual Datacenter (Centre de données virtuel)** dans lequel le vApp doit s'exécuter. Par défaut,

 ©2023 Palo Alto Networks, Inc.

les **Leases (Locations)** n'expirent jamais en ce qui a trait à l'exécution et au stockage, et le vApp ne s'arrête pas automatiquement.

3. **Add Virtual Machines (Ajoutez des machines virtuelles)**. Pour ajouter l'image du pare-feu VM-Series à partir de la liste déroulante **Look in: (Regarder dans :)**, sélectionnez **My Organization's Catalogs (Catalogues de mon organisation)**, puis sélectionnez l'image et cliquez sur **Add (Ajouter)**. Cliquez sur **Next (Suivant)**.
4. Configurez les **Resources (Ressources)** afin de préciser les politiques de stockage relatives aux machines virtuelles, une fois qu'elles sont déployées. Le pare-feu VM-Series utilise l'option **Standard**.
5. Configurez les **Virtual Machines (Machines virtuelles)**. Nommez chacune des machines virtuelles et sélectionnez le réseau auquel vous souhaitez qu'elles se connectent. Vous devez connecter le NIC 0 (pour l'accès de gestion) au réseau routé par défaut ; NIC 1 est utilisé pour le trafic de données. Vous pouvez ajouter d'autres NIC ultérieurement.
6. Vérifiez les paramètres et cliquez sur **Finish (Terminer)**.
7. Passez à l'étape 6.

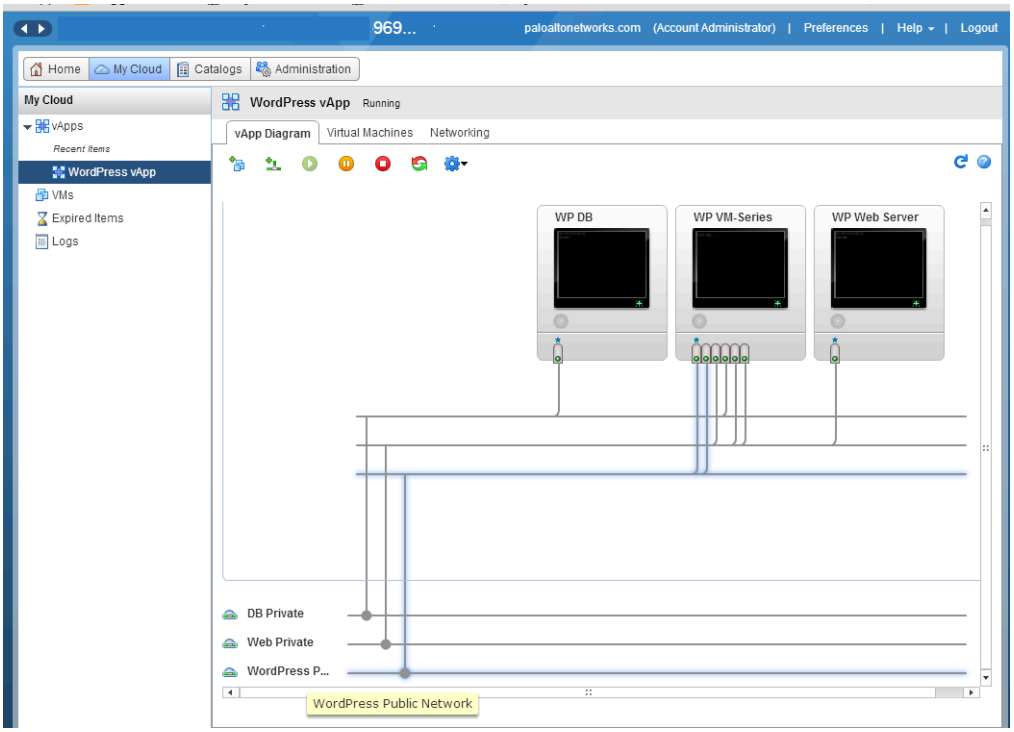
STEP 5 | Ajoutez un pare-feu VM-Series à un vApp.

1. Connectez-vous à vCloud Air.
2. Sélectionnez votre **Virtual Data Center (Centre de données virtuel)** existant dans le panneau de gauche, cliquez sur le bouton droit de la souris, puis sélectionnez **Manage Catalogs in vCloud Director (Gérer les catalogues dans vCloud Director)**. Vous serez rédigé vers l'interface Web de vCloud Director.
3. Sélectionnez **My Cloud (Mon cloud)** > **vApps**, puis cliquez sur le **Name (Nom)** du vApp dans lequel vous souhaitez ajouter le pare-feu VM-Series.
4. Ouvrez le vApp (double-cliquez sur le nom), sélectionnez **Virtual Machines (Machines virtuelles)**, puis cliquez sur ✚ afin d'ajouter une machine virtuelle.
   1. Dans la liste déroulante **Look in: (Regarder dans :)**, sélectionnez **My Organization's Catalogs (Catalogues de mon organisation)**, puis sélectionnez l'image du pare-feu VM-Series et cliquez sur **Add (Ajouter)**. Cliquez sur **Next (Suivant)**.
   2. Cliquez sur **Next (Suivant)** pour omettre la **Configure Resources (Configuration des ressources)**. Le pare-feu VM-Series utilise l'option **Standard** et vous ne pouvez modifier la politique de stockage.
   3. Saisissez un **Name (Nom)** pour le pare-feu et pour l'accès de gestion (**NIC 0**) puis sélectionnez le réseau routé par défaut et l'**IP Mode (Mode IP)**, soit statique ou DHCP. Vous pouvez configurer le NIC 1 et ajouter d'autres NIC à l'étape 6. Cliquez sur **Next (Suivant)**.
   4. Vérifiez le moyen de connexion de ce vApp au vDC : adresse de passerelle et masque de réseau pour les machines virtuelles dans ce vApp.
   5. Vérifiez que vous avez ajouté le pare-feu VM-Series et cliquez sur **Terminer**.
   6. Passez à l'étape 6.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Connectez la ou les interfaces de données du pare-feu VM-Series a un réseau isolé ou routé, selon les exigences de votre déploiement.

1. Dans vCloud Director, sélectionnez **My Cloud (My cloud)** > **vApps**, puis sélectionnez le vApp que vous venez de créer ou de modifier.
2. Sélectionnez **Virtual Machines (Machines virtuelles)**, puis sélectionnez le pare-feu VM-Series. Ensuite, cliquez sur le bouton de droite et sélectionnez **Properties (Propriétés)**.
3. Sélectionnez **Hardware (Matériel)**, puis faites défiler jusqu'à la section NIC et sélectionnez **NIC 1**.
4. Associez l'interface de réseau du plan de données à un réseau vApp ou à un réseau VDC d'entreprise en fonction de vos exigences de connectivité pour le trafic de données vers le pare-feu VM-Series. Pour créer un nouveau réseau :
   1. Dans la liste déroulante Network (Réseau), cliquez sur **Add Network (Ajouter réseau)**.
   2. Sélectionnez le **Network Type (Type de réseau)**, puis nommez-le et cliquez sur **OK**.
   3. Vérifiez que le nouveau réseau est associé à l'interface.
5. Pour ajouter d'autres NIC au pare-feu, cliquez sur **Add (Ajouter)** et répétez l'étape 4 décrite ci-dessus. Vous pouvez associer un maximum de sept interfaces du dataplane au pare-feu VM-Series.
6. Vérifiez que l'interface de gestion du pare-feu VM-Series est associée au sous-réseau routé par défaut sur le vDC et qu'au moins une interface du dataplane est connectée à un réseau routé ou isolé.
   1. Sélectionnez **My Cloud (Mon cloud)** > **vApps** puis double-cliquez sur le **Name (Nom)** du vApp que vous venez de modifier.
   2. Vérifiez la connectivité du réseau dans le **vApp Diagram (Diagramme vApp)**.

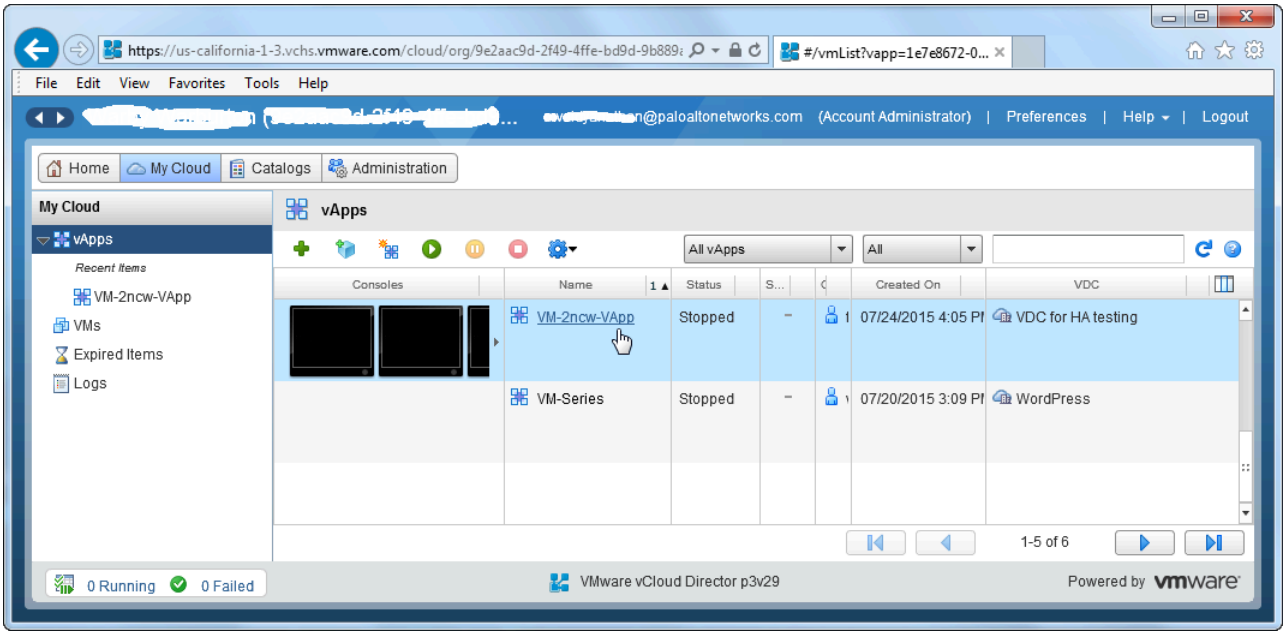


 ©2023 Palo Alto Networks, Inc.

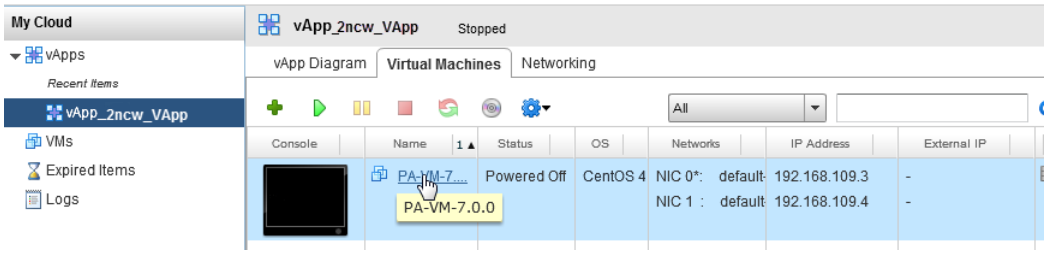
STEP 7 | (Facultatif) Modifiez les ressources matérielles allouées au pare-feu VM-Series.

Cette étape n'est obligatoire que si vous devez allouer plus de processeurs, de mémoires, ou de disques durs au pare-feu.

1. Sélectionnez **My Cloud (Mon cloud)** > **vApps** puis double-cliquez sur le **Name (Nom)** du vApp que vous venez de déployer.



2. Sélectionnez **Virtual Machine (Machine virtuelle)**, puis sur le **Name (Nom)** du pare-feu VM-Series pour accéder aux propriétés de la machine virtuelle.



3. Ajoutez des ressources **Hardware (Matérielles)** supplémentaires au pare-feu VM-Series :
   - Reportez-vous à la section Configuration système requise pour VM-Series pour les exigences minimales de vCPU, de mémoire et de disque pour votre modèle VM-Series.
   - NIC : une interface de gestion et un maximum de sept interfaces du dataplane.

STEP 8 | Mettez le pare-feu VM-Series sous tension.

STEP 9 | Configurez une adresse IP pour l'interface de gestion de pare-feu VM-Series.

Réalisez la configuration initiale sur le VM-Series sur ESXi.

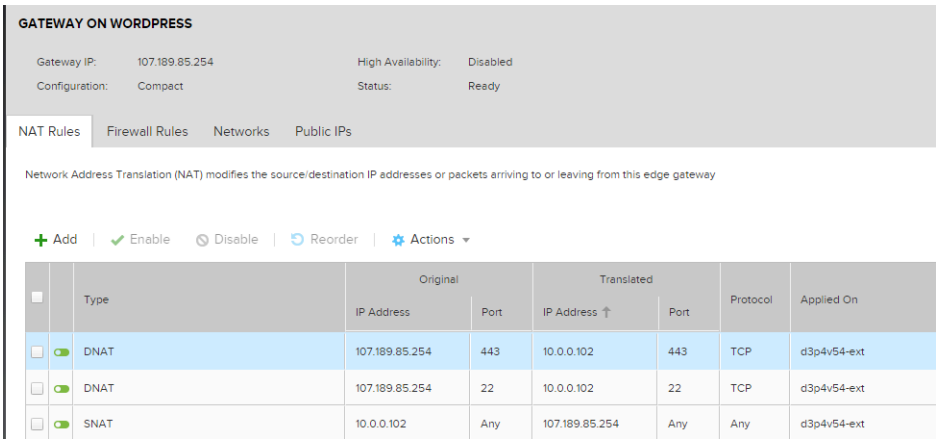
Le pare-feu VM-Series sur vCloud Air prend en charge VMware Tools et vous pouvez utiliser VMware Tools sur le pare-feu VM-Series sur ESXi et vCloud Air pour afficher l'adresse IP de gestion du pare-feu VM-Series.

©2023 Palo Alto Networks, Inc.

STEP 10 | Définissez des règles NAT sur la passerelle vCloud Air Edge afin d'activer l'accès Internet pour le pare-feu VM-Series.

1. Sélectionnez **Virtual Data Centers (Centres de données virtuels)** > **Gateways (Passerelles)**, puis sélectionnez la passerelle et double-cliquez pour ajouter les **NAT Rules (Règles NAT)**.
2. Créez deux règles DNAT. Une règle pour permettre l'accès SSH et une règle pour autoriser l'accès HTTPS à l'adresse IP du port de gestion sur le pare-feu VM-Series.
3. Créez une règle SNAT pour la traduction de l'adresse IP de source interne qui s'applique à tout le trafic provenant du port de gestion sur le pare-feu VM-Series vers une adresse IP externe.

> ***Pour envoyer et recevoir sur le pare-feu le trafic en provenant des interfaces du dataplane, vous devez créer d'autres règles DNAT et SNAT sur la passerelle vCloud Air Edge.***



STEP 11 | Connectez-vous à l'interface Web du pare-feu.

Dans cet exemple, l'URL de l'interface Web est : https://107.189.85.254

La règle NAT sur la passerelle de périmètre traduit l'adresse IP externe et le port 107.189.85.254:443 en adresse IP privée et en port 10.0.0.102:443.

STEP 12 | Ajoutez un ou plusieurs codes d'autorisation pour activer les licences sur le pare-feu.

Activez la licence.

STEP 13 | Configurez le pare-feu VM-Series de façon à utiliser l'adresse MAC attribuée par l'hyperviseur.

Adresses MAC attribuées par l'hyperviseur

 ©2023 Palo Alto Networks, Inc.

STEP 14 | Configurez les interfaces du dataplane en tant qu'interfaces de couche 3.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
2. Cliquez sur la liaison **ethernet 1/1** et configurez comme suit :
   - **Interface Type (Type d'interface) : Layer3 (Couche 3)**
   - Sélectionnez l'onglet **Config (Configuration)**, affectez l'interface au routeur par défaut.
   - Dans l'onglet **Config (Configuration)**, sélectionnez **New Zone (Nouvelle zone)** dans la liste déroulante **Security Zone (Zone de sécurité)**. Définissez une nouvelle zone, Non approuvée par exemple, puis cliquez sur **OK**.
   - Sélectionnez **IPv4**, puis affectez une adresse IP statique.
   - Dans **Advanced (Avancé)** > **Other Info (Autres informations)**, développez la liste **Management Profile (Profil de gestion)**, puis sélectionnez **New Management Profile (Nouveau profil de gestion)**.
   - Saisissez un **Name (Nom)** pour le profil, tel que allow_ping, sélectionnez Ping dans la liste des services autorisés, puis cliquez sur **OK**.
   - Pour enregistrer la configuration de l'interface, cliquez sur **OK**.
3. Répétez l'opération pour chaque interface supplémentaire.
4. Cliquez sur **Commit (Valider)** pour enregistrer les modifications.

 ©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur VMware NSX-T

Le pare-feu VM-Series peut être déployé sur VMware NSX-T pour sécuriser le trafic Nord-Sud et Est-Ouest.

- Configuration du pare-feu VM-Series sur VMware NSX-T (Nord-Sud)
- Configuration du pare-feu VM-Series sur NSX-T (Est-Ouest)

Configuration du pare-feu VM-Series sur VMware NSX-T (Nord-Sud)

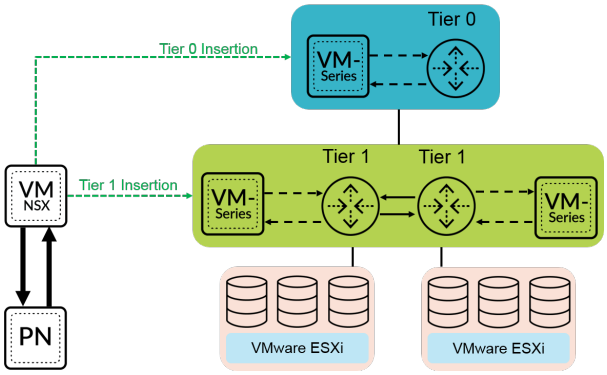
Le pare-feu VM-Series sur VMware NSX-T intègre les pare-feu nouvelle génération de Palo Alto et Panorama avec des serveurs hôtes ESXi pour offrir une visibilité complète et une activation sécurisée des applications de tout le trafic nord-sud dans votre centre de données défini par logiciel NSX-T.

Les rubriques suivantes fournissent des informations sur le pare-feu VM-Series sur VMware NSX-T :

- Déploiements pris en charge du pare-feu VM-Series sur VMware NSX-T (Nord-Sud)
- Composants du pare-feu VM-Series sur NSX-T (Nord-Sud)
- Déploiement du pare-feu VM-Series sur NSX-T (Nord-Sud)
- Extension de la politique de sécurité du NSX-V au NSX-T

Déploiements pris en charge du pare-feu VM-Series sur VMware NSX-T (Nord-Sud)

Vous pouvez déployer une ou plusieurs instances du pare-feu VM-Series en tant que service partenaire dans votre centre de données VMware NSX-T. Associez un pare-feu VM-Series à un routeur logique de niveau 0 ou 1 pour protéger le trafic nord-sud. Vous pouvez déployer le pare-feu VM-Series en tant qu'instance de service autonome ou en deux pare-feu dans une paire HA (haute disponibilité). Panorama gère la connexion avec NSX-T Manager et les pare-feu VM-Series déployés dans votre centre de données défini par logiciel NSX-T.



- Insertion de niveau 0 : l'insertion de niveau 0 déploie un pare-feu VM-Series sur un routeur logique de niveau 0 qui traite le trafic entre les réseaux logiques et physiques. Lorsque vous déployez le pare-feu VM-Series avec une insertion de niveau 0, NSX-T Manager utilise les informations de déploiement que vous avez configurées sur Panorama pour associer un pare-feu à un routeur logique de niveau 0 en mode Câble virtuel.
- Insertion de niveau 1 : l'insertion de niveau 1 déploie un pare-feu VM-Series sur un routeur logique de niveau 1 qui fournit des connexions de liaison descendante aux segments et une connexion de liaison montante aux routeurs logiques de niveau 0. NSX-T Manager associe des pare-feu VM-Series déployés avec des insertions de niveau 1 à un routeur logique de niveau 1 en mode Câble virtuel.

©2023 Palo Alto Networks, Inc.

Après avoir déployé le pare-feu, vous configurez des règles de redirection du trafic qui envoient du trafic au pare-feu VM-Series lors de la traversée d'un routeur de niveau 0 ou 1. Les règles de politique de sécurité que vous configurez sur Panorama sont transférées vers les pare-feu gérés VM-Series, puis appliquées au trafic traversant le pare-feu.

Composants du pare-feu VM-Series sur NSX-T (Nord-Sud)

Les tableaux suivants indiquent les composants de cette solution conjointe Palo Alto Networks et VMware NSX-T.

Composants VMware	
vCenter/ESXi	Le serveur vCenter est l'outil de gestion centralisée de la suite vSphere. ESXi est un hyperviseur qui permet la virtualisation informatique. Reportez-vous à la matrice de compatibilité VMware pour la compatibilité de vCenter avec votre version de NSX-T.
NSX-T Manager	Le centre de données VMware NSX-T 2.4.0 et versions ultérieures doit être installé et enregistré sur le serveur vCenter. Le NSX-T Manager et requis pour déployer le pare-feu VM-Series sur les hôtes ESXi au sein d'un cluster ESXi.

Composants Palo Alto Networks	
PAN-OS	L'image de base VM-Series (PA-VM-NST-9.1.zip) est requise pour le déploiement du pare-feu VM-Series sur NSX-T. La configuration système minimale requise pour le déploiement du pare-feu VM-Series pour NSX sur le serveur ESXi dépend de votre modèle VM-Series. Reportez-vous à la section Modèles VM-Series pour obtenir la configuration matérielle minimale requise pour votre modèle VM-Series.
Panorama Panorama doit exécuter la même version ou une version ultérieure que les pare-feu qu'il doit gérer.	Le pare-feu VM-Series sur NSX-T nécessite Panorama 9.1 ou version ultérieure. Panorama est l'outil de gestion centralisée pour les pare-feu de dernière génération Palo Alto Networks. Dans cette solution, Panorama fonctionne avec le NSX-T Manager pour déployer, mettre sous licence et gérer de manière centralisée la configuration et les politiques sur le pare-feu VM-Series pour NSX-T.

©2023 Palo Alto Networks, Inc.

Composants Palo Alto Networks	
	Panorama doit pouvoir se connecter au NSX-T Manager, aux pare-feu VM-Series et au serveur de mise à jour Palo Alto Networks. Reportez-vous à la section Guide de l'administrateur Panorama pour plus d'informations sur le déploiement de votre appareil Panorama.
Plug-in Panorama pour VMware NSX	3.0.0 ou version ultérieure
Plug-in VM-Series	1.0.6 ou version ultérieure
Modèles de pare-feu VM-Series	Les modèles VM-100, VM-300, VM-500 et VM-700 prennent en charge NSX-T.

Déploiement du pare-feu VM-Series sur NSX-T (Nord-Sud)

Effectuez les tâches suivantes pour sécuriser le trafic nord-sud dans votre environnement NSX-T avec le pare-feu VM-Series.

La procédure suivante se réfère à NSX-T Manager 3.0

.

- Installation du plug-in Panorama pour VMware NSX
- Autorisation de la communication entre NSX-T Manager et Panorama
- Création de piles de modèles et de groupes de périphériques sur Panorama
- Configuration de la définition de service sur Panorama
- Déploiement du pare-feu VM-Series
- Redirection du trafic vers le pare-feu VM-Series
- Application de la politique de sécurité au pare-feu VM-Series sur NSX-T
- Utilisation de vMotion pour déplacer le pare-feu VM-Series entre les hôtes

Installation du plug-in Panorama pour VMware NSX

Téléchargez et installez le plug-in Panorama pour VMware NSX. Reportez-vous à la matrice de compatibilité avant d'installer ou de mettre à jour votre plug-in.

Si vous avez une configuration d'HA de Panorama, répétez ce processus d'installation sur chaque pair de Panorama. Lors de l'installation du plug-in sur les homologues HA Panorama, installez le plug-in sur le pair passif avant le pair actif. Après avoir installé le plug-in sur l'homologue passif, il passera à un état non fonctionnel. L'installation du plug-in sur l'homologue actif renvoie l'homologue passif à un état fonctionnel.

Si vous avez un appareil Panorama autonome ou deux appareils Panorama installés dans une paire HA avec plusieurs plug-ins installés, les plug-ins peuvent ne pas recevoir les informations des indicateurs d'adresse IP mises à jour si un ou plusieurs des plug-ins ne sont pas configurés. Cela

 ©2023 Palo Alto Networks, Inc.

se produit, car Panorama ne transfère pas les informations des indicateurs d'adresse IP aux plug-ins non configurés. De plus, ce problème peut se présenter si un ou plusieurs plug-ins Panorama ne se trouvent pas dans l'état Registered (Enregistré) ou Success (Réussite) (l'état positif diffère sur chaque plug-in). Assurez-vous que vos plug-ins se trouvent dans l'état positif avant de continuer ou d'exécuter les commandes décrites ci-dessous.

Si vous rencontrez ce problème, il existe deux solutions alternatives :

- Désinstallez le ou les plug-ins non configurés. Il est déconseillé d'installer un plug-in que vous n'envisagez pas de configurer dans l'immédiat
- Vous pouvez utiliser les commandes suivantes pour contourner ce problème. Exécutez la commande suivante pour chaque plug-in non configuré sur chaque instance de Panorama afin que Panorama n'attende pas pour envoyer des mises à jour. Dans le cas contraire, vos pare-feu risquent de perdre certaines informations des indicateurs d'adresse IP.

  ```
  request plugins dau plugin-name <plugin-name> unblock-device-push yes
  ```

  Vous pouvez annuler cette commande en exécutant :

  ```
  request plugins dau plugin-name <plugin-name> unblock-device-push no
  ```

Les commandes décrites ne sont pas persistantes lors des redémarrages et doivent être réutilisées pour tout redémarrage ultérieur. Pour Panorama en paire HA, les commandes doivent être exécutées sur chaque Panorama.

STEP 1 | Sélectionnez **Panorama** > **Plugins**. Reportez-vous à la matrice de compatibilité avant d'installer ou de mettre à jour votre plug-in.

STEP 2 | Sélectionnez **Check Now (Vérifiez maintenant)**pour récupérer la liste des mises à jour disponibles.

STEP 3 | Sélectionnez **Download (Télécharger)** dans la colonne Action pour installer le plug-in (module d'extension).

STEP 4 | Sélectionnez la version du plug-in et cliquez sur **Install (Installer)** dans la colonne Action pour installer le plug-in. Panorama vous alertera lorsque l'installation est terminée.

Autorisation de la communication entre NSX-T Manager et Panorama

Effectuez la procédure suivante pour activer la communication entre Panorama et NSX-T Manager. Vous pouvez connecter votre Panorama à un maximum de 16 NSX-T Managers. Si vous connectez votre Panorama à plusieurs NSX-T Managers, vous devez planifier soigneusement la hiérarchie des groupes de périphériques et les piles de modèles, et examiner leur interaction avec les autres composants nécessaires au déploiement. Les définitions de service font référence aux groupes de périphériques et aux piles de modèles, et transmettent ces informations aux pare-feu des clusters ESXi associés.

STEP 1 | (Facultatif) Ignorez les paramètres du serveur proxy, configurés sur Panorama sous **Panorama** > **Setup (Configuration)** > **Services** > **Proxy Server (Serveur proxy)** pour la communication entre Panorama et NSX-T Manager. Cette commande permet à Panorama de communiquer directement avec NSX-T Manager tout en maintenant la communication par proxy pour d'autres services.

1. Connectez-vous à la CLI Panorama.

 ©2023 Palo Alto Networks, Inc.

2. Exécutez la commande suivante pour activer ou désactiver le contournement du proxy.

   ```
   admin@Panorama> request plugins vmware_nsx proxy bypass {yes | no}
   ```

   Sélectionnez **yes** (oui) pour activer le contournement du proxy et **no** (non) pour désactiver le contournement du proxy. La valeur par défaut est **no** (non).

STEP 2 | Connectez-vous à l'interface Web Panorama.

À l'aide d'une connexion sécurisée (https) fournie par un navigateur Web, connectez-vous avec l'adresse IP et le mot de passe que vous avez affectés lors de la configuration initiale (https://<*adresse IP*>).

STEP 3 | Configurez l'accès au NSX-T Manager. Répétez cette procédure pour chaque NSX-T Manager auquel vous allez connecter Panorama.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Managers (Gestionnaires de service)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name** (Nom) descriptif pour votre NSX-T Manager.
3. (Facultatif) Ajoutez une **Description** pour NSX-T Manager.
4. Saisissez le **NSX Manager URL (URL NSX Manager)** (adresse IP ou FQDN du cluster NSX-T Manager) qui permet d'accéder au NSX-T Manager.
5. Saisissez les informations d'identification de **NSX Manager Login** (Connexion NSX Manager) (nom d'utilisateur et mot de passe) de manière à ce que Panorama puisse s'authentifier auprès du NSX-T Manager.
6. Cliquez sur **OK**.

Si vous changez votre mot de passe de connexion au NSX-T Manager, assurez-vous de le mettre immédiatement à jour sur Panorama. Un mot de passe incorrect rompt la connexion entre Panorama et NSX-T Manager.

STEP 4 | Validez vos modifications sur Panorama.

Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

STEP 5 | Vérifiez l'état de la connexion sur Panorama.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Managers (Gestionnaires de service)**.
2. Vérifiez le message dans la colonne **Status** (État).

   Lorsque la connexion a réussi, l'état affiché est : **Registered (Enregistré)**. Cela indique que Panorama et le NSX-T Manager sont synchronisés.

   Lorsque la connexion a échoué, l'état affiché peut être :

   - **No connection** (aucune connexion) : impossible d'atteindre/établir une connexion réseau au NSX-T Manager.
   - **Invalid Credentials** (informations d'identification invalides) : les informations d'identification d'accès (nom d'utilisateur et/ou mot de passe) sont incorrectes.
   - **Out of sync (Désynchronisé)** : les paramètres de configuration définis sur Panorama sont différents de ceux définis sur le NSX-V Manager. Cliquez sur le lien pour connaître

 ©2023 Palo Alto Networks, Inc.

les détails de la raison de l'échec. Par exemple, NSX-T Manager peut disposer d'une définition de service ayant le même nom que celui qui est défini sur Panorama. Pour corriger l'erreur, utilisez le nom de la définition de service qui est indiqué dans le message d'erreur afin de valider la définition de service sur le NSX-T Manager. Jusqu'à ce que la configuration sur Panorama et le NSX-T Manager soient synchronisées, vous ne pouvez ajouter aucune nouvelle définition de service sur Panorama.

- **Connection Disabled** (connexion désactivée) : la connexion entre Panorama et le NSX-T Manager a été désactivée manuellement.

Création de piles de modèles et de groupes de périphériques sur Panorama

Pour gérer les pare-feu VM-Series sur NSX-T à l'aide de Panorama, ils doivent appartenir à un groupe de périphériques et une pile de modèles. Les groupes de périphériques vous permettent de regrouper les pare-feu qui nécessitent des politiques et des objets similaires comme unités logiques ; la configuration est définie à l'aide des onglets **Objects (Objets)** et **Policies (Politiques)** sur Panorama. Utilisez les piles de modèles pour configurer les paramètres requis pour le fonctionnement des pare-feu VM-Series sur le réseau. La configuration est définie à l'aide des onglets **Device** (Appareil) et **Network** (Réseau) sur Panorama. Chaque pile de modèles utilisée dans votre configuration NSX-T doit être associée à une définition de service.

Les pare-feu déployés dans NSX-T ont deux zones par défaut et deux interfaces configurées en mode câble virtuel (virtual-wire). Ethernet1/1 fait partie de la zone **south (sud)**, alors qu'ethernet1/2 fait partie de la zone **north (nord)**. Pour pousser les règles de politique de Panorama vers les pare-feu gérés, vous devez configurer des zones et des interfaces qui correspondent à celles sur le pare-feu dans la pile de modèles correspondante sur Panorama.

STEP 1 | Ajoutez un groupe de périphériques ou une hiérarchie de groupe de périphériques.

1. Sélectionnez **Panorama** > **Device Groups (Groupes d'appareils)**, puis cliquez sur **Add (Ajouter)**. Vous pouvez aussi créer une hiérarchie de groupe de périphériques.
2. Entrez un **Name (Nom)** unique et une **Description** pour identifier le groupe de périphériques.
3. Cliquez sur **OK**.
4. Cliquez sur **Commit (Valider)**, puis sélectionnez **Panorama** en tant que **Commit Type (Type de validation)** pour enregistrer les modifications de la configuration en cours sur Panorama.

STEP 2 | Ajoutez un modèle.

1. Sélectionnez **Panorama** > **Templates (Modèles)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** unique et une **Description** pour identifier le modèle.
3. Cliquez sur **OK**.
4. Cliquez sur **Commit (Valider)**, puis sélectionnez **Panorama** en tant que **Commit Type (Type de validation)** pour enregistrer les modifications de la configuration en cours sur Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Créez une pile de modèle.

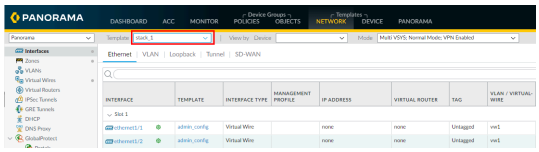
1. Sélectionnez **Panorama** > **Templates (Modèles)**, puis cliquez sur **Add Stack (Ajouter une pile)**.
2. Saisissez un **Name (Nom)** unique et une **Description** pour identifier le modèle.
3. Cliquez sur **Add (Ajouter)** pour ajouter le modèle que vous avez créé précédemment.
4. Cliquez sur **OK**.
5. Cliquez sur **Commit (Valider)**, puis sélectionnez **Commit to Panorama (Valider sur Panorama)**pour enregistrer les modifications de la configuration en cours sur Panorama.

STEP 4 | Configurez le câble virtuel, les interfaces et les zones. Assurez-vous de sélectionner le modèle approprié dans la liste déroulante affichée ci-dessous. Les objets que vous créez doivent répondre aux critères suivants :

Si vous modifiez le câble virtuel par défaut ou les noms des zones, le câble virtuel et les zones sur Panorama doivent correspondre aux noms utilisés sur le pare-feu.

- Utilisez **ethernet1/1** et **ethernet1/2**.
- L'objet câble virtuel est nommé **vw1**.
- La première zone est nommée **south (sud)**. Saisissez **virtual-wire** et elle inclut **ethernet1/1**.
- La deuxième zone est nommée **north (nord)**. Saisissez **virtual-wire** et elle inclut **ethernet1/2**.

Répétez ce processus pour chaque modèle de votre déploiement.



STEP 5 | Cliquez sur **Commit (Valider)**, puis sélectionnez **Panorama** en tant que **Commit Type (Type de validation)** pour enregistrer les modifications de la configuration en cours sur Panorama.

STEP 6 | Mettez à jour les informations de serveur DNS et NTP de votre pile de modèles. Vous devez effectuer cette étape si vous utilisez des certificats d'appareil dans votre déploiement. Cela est nécessaire pour garantir que les pare-feu déployés dans votre environnement NSX-T disposent des informations DNS correctes nécessaires pour atteindre le serveur de certificats de périphérique.

1. Vérifiez que vous avez spécifié la pile de modèles correcte dans la liste déroulante **Template (Modèle)**.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** et cliquez sur l'icône **Edit (Modifier)**.
3. Dans l'onglet Services, saisissez l'adresse IP du **Primary DNS Server (Serveur DNS principal)** et du **Secondary DNS Server (Serveur DNS secondaire)**.
4. Sous l'onglet NTP, entrez l'adresse IP du **serveur NTP**.
5. Cliquez sur **OK**.
6. **Validez** vos modifications sur Panorama.

 ©2023 Palo Alto Networks, Inc.

Configuration de la définition de service sur Panorama

Une définition de service spécifie la configuration pour les pare-feu VM-Series installés dans votre environnement de centre de données NSX-T. La définition de service doit inclure le groupe de périphériques, une pile de modèles et une URL OVF.

STEP 1 | Ajoutez une nouvelle définition de service.

Vous pouvez créer jusqu'à 32 définitions de service sur Panorama.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Definitions (Définitions de service)**.
2. Sélectionnez **Add (Ajouter)** pour créer une nouvelle définition de service.
3. Saisissez un **Name** (Nom) descriptif pour votre définition de service.
4. (Facultatif) Ajoutez une **Description** qui identifie la fonction ou le but des pare-feu VM-Series qui seront déployés en utilisant cette définition de service.

STEP 2 | Associez un groupe de périphériques et un modèle pour la définition de service.

Assurez-vous de procéder à la Création de piles de modèles et de groupes de périphériques sur Panorama.

Comme les pare-feu déployés dans cette solution sont gérés de manière centralisée à partir de Panorama, vous devez spécifier le **Device Group (Groupe de périphériques)** et le **Template (Modèle)** auquel les pare-feu appartiennent. Tous les pare-feu qui sont déployés en utilisant cette définition de service appartiennent au modèle et au groupe de périphériques spécifiés.

1. Sélectionnez le groupe d'appareils ou la hiérarchie de groupe d'appareils dans le menu déroulant **Device Group** (Groupe d'appareils).
2. Sélectionnez la pile de modèles dans le menu déroulant **Template** (Modèle).

Vous ne pouvez pas réutiliser un modèle ou un groupe de périphériques attribués à une définition de service dans une autre définition de service.

©2023 Palo Alto Networks, Inc.

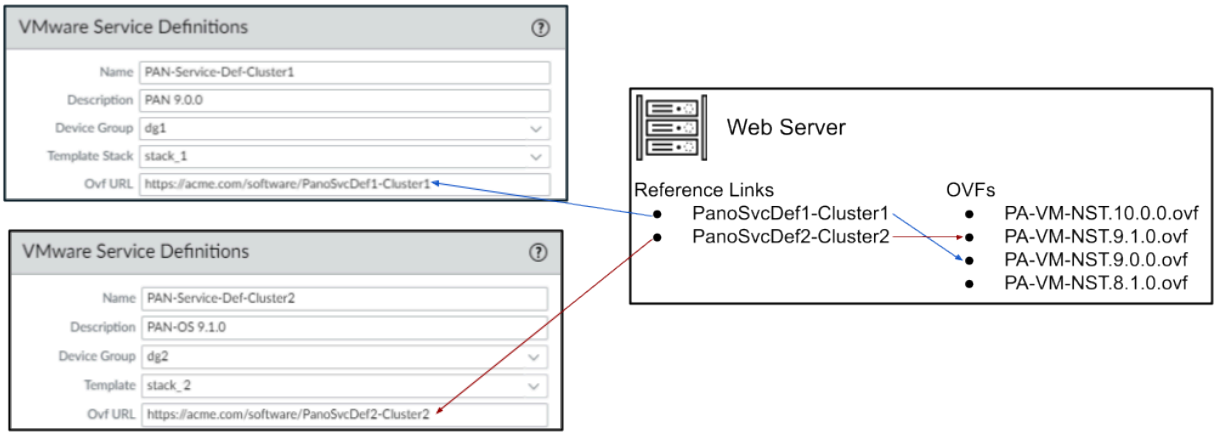
STEP 3 | Spécifiez l'emplacement du fichier OVF.

Téléchargez le fichier zip, puis décompressez-le pour extraire puis enregistrer les fichiers .ovf, mf et .vmdk dans le même répertoire. Les fichiers ovf et vmdk sont utilisés pour déployer chaque instance du pare-feu.

Si nécessaire, modifiez les paramètres de sécurité sur le serveur pour pouvoir télécharger les types de fichiers. Par exemple, sur le serveur IIS, modifiez la configuration des types Mime ; sur un serveur Apache, modifiez le fichier .htaccess.

Ne modifiez pas le chemin OVF de la définition du service Panorama après un déploiement réussi du service NSX des pare-feu VM-Series. La modification du chemin OVF, après un déploiement réussi du pare-feu VM-Series, peut entraîner un état d'échec du déploiement du service NSX. Vous pouvez résoudre cet échec dans NSX-T Manager, mais cela peut entraîner le redéploiement de tous les pare-feu VM-Series.

Il est recommandé d'utiliser un nom de chemin OVF qui évolue et vous permette de modifier l'image de base sans affecter vos pare-feu déployés. Au lieu d'un chemin tel que **https://acme.com/software/PA-VM-NST.9.1.0.ovf**, utilisez quelque chose comme **https://acme.com/software/PanoSvcDef1-Cluster1.ovf**. L'utilisation d'une référence de chemin statique éliminera tout besoin futur de modifier le chemin OVF. Il est recommandé de créer un chemin pour chaque définition de service Panorama (cluster vSphere) dans votre déploiement et de modifier les références des images de base PAN-OS sur le serveur Web si nécessaire.



Dans **OVF URL** (URL OVF), ajoutez l'emplacement du serveur Web qui héberge le fichier ovf. Les protocoles http et https sont tous les deux pris en charge.

Panorama doit avoir une connexion réseau avec le serveur web pour récupérer le fichier OVF.

Vous pouvez utiliser la même version ovf ou des versions différentes entre les définitions de service. L'utilisation de versions ovf différentes entre les définitions de service vous permet de varier la version de PAN-OS sur les pare-feu VM-Series dans différents clusters ESXi.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Sélectionnez **North South (Nord-Sud)** comme **Insertion Type (Type d'insertion)** pour votre pare-feu.

STEP 5 | Pour récupérer automatiquement un certificat de périphérique lorsque le pare-feu VM-Series est déployé par NSX Manager, configurez le certificat de périphérique.

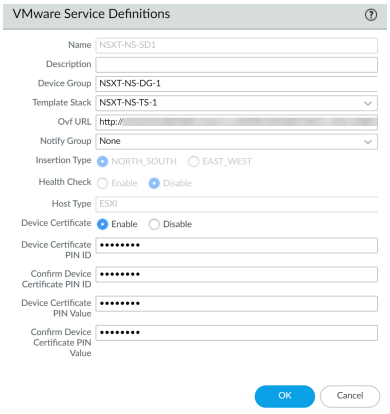
Activez cette option pour appliquer un certificat de périphérique aux pare-feu VM-Series nouvellement déployés. N'utilisez cette option que lorsque vous déployez le pare-feu en utilisant une image de base OVF qui prend en charge les certificats de périphériques. Panorama transmet les informations du certificat de périphérique à NSX Manager dans le cadre de la définition du service. Lorsqu'un nouveau pare-feu est déployé dans NSX, le certificat de périphérique est installé sur le pare-feu au démarrage.

Pour obtenir la liste des OVF qui prennent en charge les certificats de périphériques pour le pare-feu VM-Series sur VMware NSX, consultez Palo Alto Networks Compatibility Matrix (Matrice de compatibilité des réseaux Palo Alto).

Si votre OVF prend en charge un certificat de périphérique, vous devez activer les certificats de périphériques, que vous utilisiez ou non un certificat de périphérique. Si votre OVF ne prend pas en charge un certificat de périphérique, désactivez cette option.

1. Si vous ne l'avez pas encore fait, connectez-vous au portail de support client et générez un PIN d'enregistrement et un ID de PIN.
2. Sous **Device Certificate (Certificat de périphérique)**, cliquez sur **Enable (Activer)**.
3. Copiez l'ID de PIN et saisissez-le dans le champ **Device Certificate PIN ID (ID du PIN du certificat de périphérique)**.
4. Saisissez à nouveau l'ID de PIN dans le champ **Confirm Device Certificate PIN ID (Confirmer l'ID du PIN du certificat de périphérique)**.
5. Copiez la valeur du PIN et saisissez-la dans le champ **Device Certificate PIN Value (Valeur du PIN du certificat de périphérique)**.
6. Saisissez à nouveau la valeur du PIN dans le champ **Confirm Device Certificate PIN Value (Confirmer la valeur du PIN du certificat de périphérique)**.

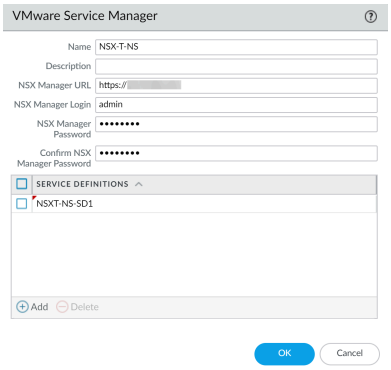
STEP 6 | Cliquez sur **OK** pour enregistrer la définition de service.



 ©2023 Palo Alto Networks, Inc.

STEP 7 | Associez la définition de service au gestionnaire de services.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Manager (Gestionnaire de services)** et cliquez sur le lien du nom du gestionnaire de services.
2. Sous Service Definitions (Définitions de service), cliquez sur **Add (Ajouter)** et sélectionnez votre définition de service dans la liste déroulante.
3. Cliquez sur **OK**.

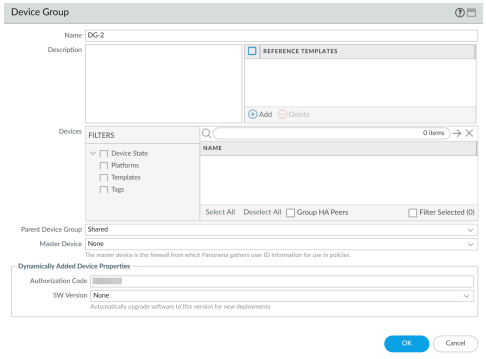


STEP 8 | Ajoutez le code d'autorisation pour mettre sous licence les pare-feu.

1. Sélectionnez **Panorama** > **Device Groups (Groupes d'appareils)** et choisissez le groupe d'appareils que vous avez associé à la définition de service que vous venez de créer.
2. Sous **Dynamically Added Device Properties (Propriétés du périphérique ajouté dynamiquement)**, ajoutez le code d'autorisation que vous avez reçu avec votre e-mail de confirmation de commande et, en option, sélectionnez None (Aucune) dans la liste déroulante **SW Version** (Version du logiciel).

   Lorsqu'un nouveau pare-feu est déployé sur NSX-T, il est automatiquement ajouté au groupe de périphériques, mis sous licence avec le code d'autorisation que vous avez fourni, et mis à niveau vers la version du logiciel PAN-OS que vous avez indiquée.

   Sur le portail de support, vous pouvez consulter le nombre de pare-feu que vous êtes autorisé à déployer et le nombre de licences qui ont été utilisées par rapport au nombre total de licences activées par votre code d'autorisation.



STEP 9 | **Commit to Panorama (Validez sur Panorama)**.

©2023 Palo Alto Networks, Inc.

STEP 10 | Sur le gestionnaire NSX-T, vérifiez que la définition de service est disponible.

Sélectionnez **System (Système)** > **Service Deployments (Déploiements de services)** > **Catalog (Catalogue)**. La définition de service est répertoriée en tant que service sur le NSX-T Manager.

Déploiement du pare-feu VM-Series

Une fois la configuration terminée sur Panorama, effectuez la procédure suivante pour lancer le pare-feu VM-Series dans votre centre de données NSX-T.

Lors du déploiement du pare-feu VM-Series sur NSX-T en haute disponibilité (HA), les deux pare-feu sont déployés sur le même groupe d'appareils et la même pile de modèles.

STEP 1 | Connectez-vous à NSX-T Manager.

STEP 2 | Sélectionnez **System (Système)** > **Service Deployments (Déploiements de services)** > **Deployment (Déploiement)**.

STEP 3 | Sélectionnez votre définition de service dans la liste déroulante **Partner Service (Service partenaire)**.

STEP 4 | Cliquez sur **Deploy Service (Déployer le service)**.

STEP 5 | Saisissez un **Service Deployment Name (Nom de déploiement de service)** descriptif pour votre pare-feu VM-Series.

STEP 6 | Sélectionnez un routeur de niveau 0 ou de niveau 1 sous **Attachment Points (Points d'attache)**. NSX-T Manager connecte le pare-feu VM-Series au routeur sélectionné et redirige le trafic passant par ce routeur vers le pare-feu VM-Series pour inspection. Vous devez sélectionner un routeur sans insertion de service.

STEP 7 | Sélectionnez un **Compute Manager (Gestionnaire de calcul)**. Le gestionnaire de calcul est le serveur vCenter qui gère votre centre de données.

STEP 8 | Sélectionnez un **Cluster**. Vous pouvez déployer le pare-feu VM-Series sur n'importe quel cluster qui n'inclut pas de nœuds de transport de périphérie.

STEP 9 | Sélectionnez un **Datastore (Magasin de données)**.

STEP 10 | Configurez les paramètres de votre réseau.

1. Cliquez sur **Edit Details (Modifier les détails)** dans la colonne **Networks** (Réseaux).
2. Sélectionnez le **Primary Interface Network (Réseau d'interface principale)**.
3. Saisissez la **Primary Interface IP (IP de l'interface principale)**.
4. Saisissez la **Primary Gateway Address (Adresse de la passerelle principale)**.
5. Saisissez le **Primary Subnet Mask (Masque de sous-réseau principal)**.
6. Cliquez sur **Save (Enregistrer)**.

STEP 11 | NSX-T Manager préremplit la **Deployment Specification (Spécification de déploiement)** et le **Deployment Template (Modèle de déploiement)** en fonction du service partenaire que vous avez sélectionné.

 ©2023 Palo Alto Networks, Inc.

STEP 12 | Définissez la **Failure Policy** (Politique d'échec) sur Allow (Autoriser) ou Block (Bloquer). La politique d'échec définit la manière dont NSX-T Manager gère le trafic dirigé vers le pare-feu VM-Series si celui-ci devient indisponible.

STEP 13 | Sélectionnez le **Deployment Mode** (Mode de déploiement) pour votre pare-feu VM-Series : Standalone (Autonome) ou High Availability (Haute disponibilité). Si vous disposez d'un cluster de nœuds de périphérie et que vous sélectionnez High Availability (Haute disponibilité), NSX-T Manager déploiera un pare-feu VM-Series supplémentaire sur le nœud de périphérie en attente en plus du pare-feu déployé sur le nœud de périphérie actif.

STEP 14 | Cliquez sur **Save (Enregistrer)** pour déployer le pare-feu VM-Series.

STEP 15 | Vérifiez que vos pare-feu sont connectés à Panorama.

1. Connectez-vous à Panorama.
2. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**.
3. Vérifiez que vos pare-feu sont répertoriés sous le bon groupe de périphériques et que le **Device State (État du déploiement)** affiche **Connected (Connecté)**.

   Le Device Name (Nom de périphérique) du pare-feu VM-Series s'affiche sur Panorama en tant que **PA-VM:<nsx.clusterid>** pour le déploiement de NSX-T (N-S) et en tant que **PA-VM:<nsx.servicevmid>** pour le déploiement de NSX-T (E-W).

Redirection du trafic vers le pare-feu VM-Series

Effectuez la procédure suivante pour diriger le trafic vers votre pare-feu VM-Series. Pour le trafic Nord-Sud, les règles de redirection sont sans état par défaut et ne peuvent pas être modifiées. En outre, NSX-T crée automatiquement une règle réflexive correspondante pour le trafic de retour.

Lorsque vous déployez le pare-feu VM-Series pour NSX-T nord-sud en mode HA, vous devez créer une règle de redirection du trafic pour les deux homologues HA. De plus, vous devez créer la règle de redirection pour l'homologue actif en premier et l'homologue passif en second.

La règle réflexive n'apparaît pas dans l'interface Web NSX-T.

STEP 1 | Connectez-vous à NSX-T Manager.

STEP 2 | Vérifiez que vous êtes en mode **Policy (Politique)**.

STEP 3 | Sélectionnez **Security (Sécurité)** > **North South Security (Sécurité nord-sud)** > **Network Introspection (N-S) (Introspection réseau [N-S])**.

STEP 4 | Cliquez sur **Add Policy (Ajouter une politique)**.

STEP 5 | Saisissez un **nom** descriptif pour votre politique.

STEP 6 | Sélectionnez une instance de service de pare-feu VM-Series dans le menu déroulant **Redirect To (Rediriger vers)**. NSX-T Manager remplira automatiquement le champ **Applied To (Appliqué à)** en fonction de l'instance de service que vous sélectionnez.

STEP 7 | Sélectionnez votre politique nouvellement créée.

 ©2023 Palo Alto Networks, Inc.

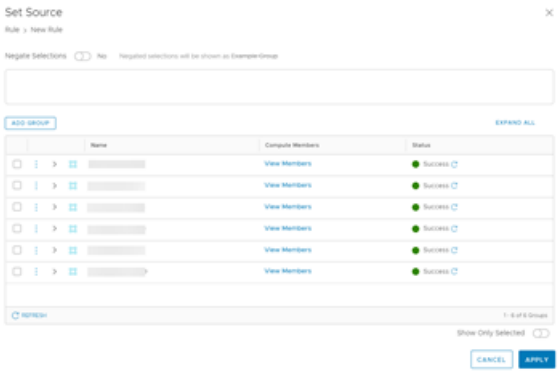
STEP 8 | Cliquez sur **Add rule** (Ajouter une règle).

> *Si votre environnement NSX-T comporte des nœuds de périphérie en HA actif-passif, vous devez créer une règle de redirection pour chaque nœud de périphérie. NSX-T n'applique pas automatiquement de règle de redirection au nœud en veille en cas de basculement.*

STEP 9 | Cliquez sur le champ **Name** (Nom) et saisissez un nom descriptif pour la règle.

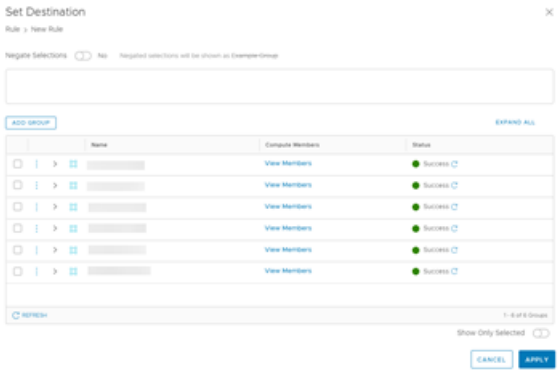
STEP 10 | La source est définie par défaut sur Any (Tout). Effectuez les étapes suivantes pour spécifier une source différente.

1. Cliquez sur le bouton d'édition dans la colonne **Source**.
2. Sélectionnez le ou les groupes à définir comme Source ou cliquez sur Add Group (Ajouter un groupe) pour créer un nouveau groupe.
3. Cliquez sur **Apply (Appliquer)**.



STEP 11 | La destination est définie par défaut sur Any (Tout). Effectuez les étapes suivantes pour spécifier une destination différente.

1. Cliquez sur le bouton d'édition dans la colonne **Destination**.
2. Sélectionnez le ou les groupes à définir comme Destination ou cliquez sur Add Group (Ajouter un groupe) pour créer un nouveau groupe.
3. Cliquez sur **Apply (Appliquer)**.



 ©2023 Palo Alto Networks, Inc.

STEP 12 | Par défaut, Any (Tout) service est redirigé vers le pare-feu. Effectuez les étapes suivantes pour spécifier certains services et protocoles.

1. Cliquez sur le bouton d'édition dans la colonne **Services**.
2. Sélectionnez le ou les groupes à définir comme Service ou cliquez sur Add Service (Ajouter un service) pour créer un nouveau service.
3. Cliquez sur **Apply (Appliquer)**.

STEP 13 | Sélectionnez **Redirect** (Rediriger) dans la liste déroulante **Action** pour envoyer le trafic vers votre pare-feu VM-Series.

STEP 14 | **Enable (Activez)** la règle. NSX-T Manager publie la règle de redirection que vous venez de créer et crée automatiquement une règle réflexive pour le trafic de retour. La règle réflexive n'apparaît pas dans l'interface Web NSX-T Manager.



STEP 15 | Si vos pare-feu VM-Series sont déployés en mode HA, créez une autre règle pour l'homologue HA passif.

Si le trafic de retour n'est pas dirigé vers le pare-feu VM-Series, configurez manuellement une règle de redirection pour le trafic de retour.

Application de la politique de sécurité au pare-feu VM-Series sur NSX-T

Maintenant que vous avez déployé le pare-feu VM-Series et créé les règles de redirection du trafic pour envoyer le trafic au pare-feu, vous pouvez utiliser Panorama pour gérer de manière centralisée les règles de politique de sécurité sur le pare-feu VM-Series.

STEP 1 | Connectez-vous à Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Créez des règles de politique de sécurité.

Par défaut, le pare-feu crée une règle qui autorise la détection de transmission bidirectionnelle (BFD). Ne créez pas de règle qui bloque BFD. Si la BFD est bloquée, NSX-T pense que le pare-feu est indisponible.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Prerules (Pré-règles)**.
2. Sélectionnez le **Device Group (Groupe d'appareils)** que vous avez créé pour gérer les pare-feu VM-Series sur NSX-T dans Création de piles de modèles et de groupes de périphériques sur Panorama.
3. Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** et une **Description** pour identifier la règle. Dans cet exemple, la règle de sécurité autorise tout le trafic entre les serveurs Web frontaux et les serveurs d'applications.
4. Sélectionnez la **Source Zone (Zone source)** et la **Destination Zone (Zone de destination)**.
5. Pour **Source Address (Adresse source)** et **Destination Address (Adresse de destination)**, sélectionnez ou saisissez une adresse, un groupe d'adresses statiques ou une région.

   Le pare-feu VM-Series sur NSX-T ne prend pas en charge les groupes d'adresses dynamiques pour le trafic nord-sud.
6. Sélectionnez l'**Application** à autoriser. Dans cet exemple, un **Application Group (Groupe d'applications)** est créé ; il s'agit d'un groupe statique d'applications spécifiques.
   1. Cliquez sur **Add (Ajouter)** et sélectionnez **New Application Group (Nouveau groupe d'applications)**.
   2. Cliquez sur **Add (Ajouter)** pour sélectionner l'application que vous souhaitez inclure dans le groupe.
   3. Cliquez sur **OK** pour créer le groupe d'applications.
7. Spécifiez l'action (**Allow (Autoriser)** ou **Deny (Refuser)**) pour le trafic, puis associez éventuellement les profils de sécurité par défaut pour l'antivirus, l'antispyware et la protection contre les vulnérabilités sous Profils.
8. Cliquez sur **Valider** et sélectionnez **Commit to Panorama (Valider sur Panorama)**. Cliquez sur **OK**.

STEP 3 | Appliquez les politiques aux pare-feu VM-Series sur NSX-T.

1. Cliquez sur **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** > **Edit Selections (Modifier les sélections)**.
2. Sélectionnez le groupe de périphériques et cliquez sur **OK**.
3. Sélectionnez **Force Template Values (Forcer les valeurs du modèle)**. Par défaut, Panorama ne remplace pas les objets sur le pare-feu par des objets sur Panorama ayant le même nom. Vous devez sélectionner Force Template Values (Forcer les valeurs du modèle) pour appliquer la politique aux pare-feu gérés.
4. Cliquez sur **Yes (Oui)** pour confirmer que vous souhaitez forcer les valeurs du modèle.
5. Cliquez sur **OK**.
6. Vérifiez que la validation a réussi.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | (Facultatif) Utilisez un modèle pour appliquer une configuration de périphérique et réseau de base, notamment à un serveur DNS, NTP, Syslog ou à une bannière de connexion.

Pour plus d'informations sur l'utilisation des modèles, reportez-vous au Guide de l'administrateur Panorama.

Utilisation de vMotion pour déplacer le pare-feu VM-Series entre les hôtes

Pour maintenir le flux de trafic lorsque vous utilisez vMotion pour déplacer votre pare-feu VM-Series entre les hôtes ESXI avec des configurations de processeur homogènes dans VMware NSX-T, vous devez utiliser la CLI PAN-OS pour interrompre la surveillance des pulsations du pare-feu VM-Series pendant vMotion. Vous pouvez spécifier la durée, en minutes, pendant laquelle la surveillance des pulsations est interrompue. La surveillance peut être interrompue pendant une durée jusqu'à 60 minutes. Lorsque l'intervalle d'interruption expire ou lorsque vous choisissez d'y mettre fin, la surveillance des pulsations reprend.

Le vMotion du pare-feu VM-Series est pris en charge sur vSphere 6.5, 6.7 et 7.0 si les hôtes ESXi ont une configuration de processeur homogène.

Cette procédure n'est pas requise lorsque vous utilisez vMotion pour déplacer le pare-feu VM-Series si vous exécutez vSphere version 7.0 ou ultérieure.

STEP 1 | Connectez-vous à la CLI du pare-feu VM-Series.

STEP 2 | Réglez l'intervalle d'interruption de la surveillance des pulsations à l'aide de la commande suivante. L'interruption commence dès que la commande est exécutée. Si vMotion dure plus longtemps qu'attendu, vous pouvez réexécuter cette commande pour définir un nouvel intervalle plus long qui démarre lorsque la commande est exécutée une nouvelle fois.

```
request system heartbeat-pause set interval <pause-time-in-minutes>
```

Vous pouvez afficher la durée restante dans l'intervalle de pause à l'aide de la commande suivante.

```
request system heartbeat-pause show interval
```

STEP 3 | (Facultatif) Si vous terminez vMotion avant la fin de l'intervalle d'interruption, vous pouvez mettre fin à l'interruption en réglant l'intervalle sur zéro (0).

```
request system heartbeat-pause set interval 0
```

Extension de la politique de sécurité du NSX-V au NSX-T

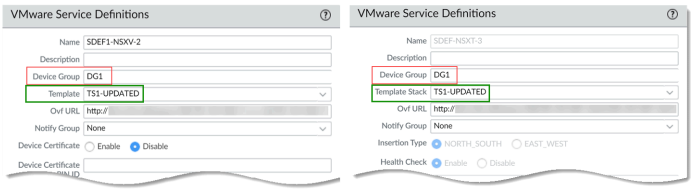
Si vous passez d'un déploiement NSX-V à un déploiement NSX-T ou si vous combinez un déploiement NSX-T avec un déploiement NSX-V, vous pouvez étendre votre politique de sécurité existante du NSX-V au NSX-T sans avoir à recréer les règles de la politique. Pour ce faire, vous pouvez exploiter vos groupes d'appareils existants et les partager entre les définitions de service NSX-V et NSX-T. Après avoir migré votre politique vers le NSX-T, vous pouvez continuer à utiliser VM-Series pour le NSX-V ou supprimer votre déploiement NSX-V.

STEP 1 | Installation du plug-in Panorama pour VMware NSX 3.2.0 ou version ultérieure. Consultez les notes de version du plugin Panorama pour VMware NSX 3.2.0 avant la mise à niveau.

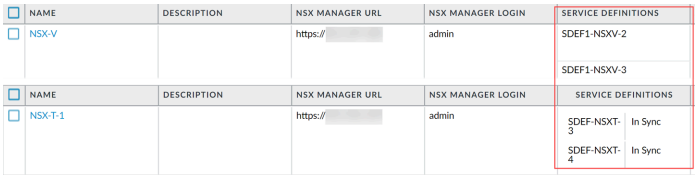
STEP 2 | Configurez une définition de service NSX-T pour chaque définition de service NSX-V dans votre déploiement. Ne créez pas de nouveaux groupes d'appareils, mais utilisez plutôt vos

 ©2023 Palo Alto Networks, Inc.

groupes d'appareils NSX-V existants. L'utilisation des groupes d'appareils existants vous permet d'appliquer les mêmes règles de sécurité que celles utilisées sur NSX-V aux pare-feu VM-Series déployés sur NSX-T. Si votre politique fait référence à une zone particulière, ajoutez la même pile de modèles de votre définition de service NSX-V à votre définition de service NSX-T. En outre, si votre groupe d'appareils référence un modèle particulier, assurez-vous de sélectionner la pile de modèles qui inclut le modèle référencé dans le groupe d'appareils.



STEP 3 | Configurez un gestionnaire de service NSX-T et associez les définitions de service NSX-T au gestionnaire de service.



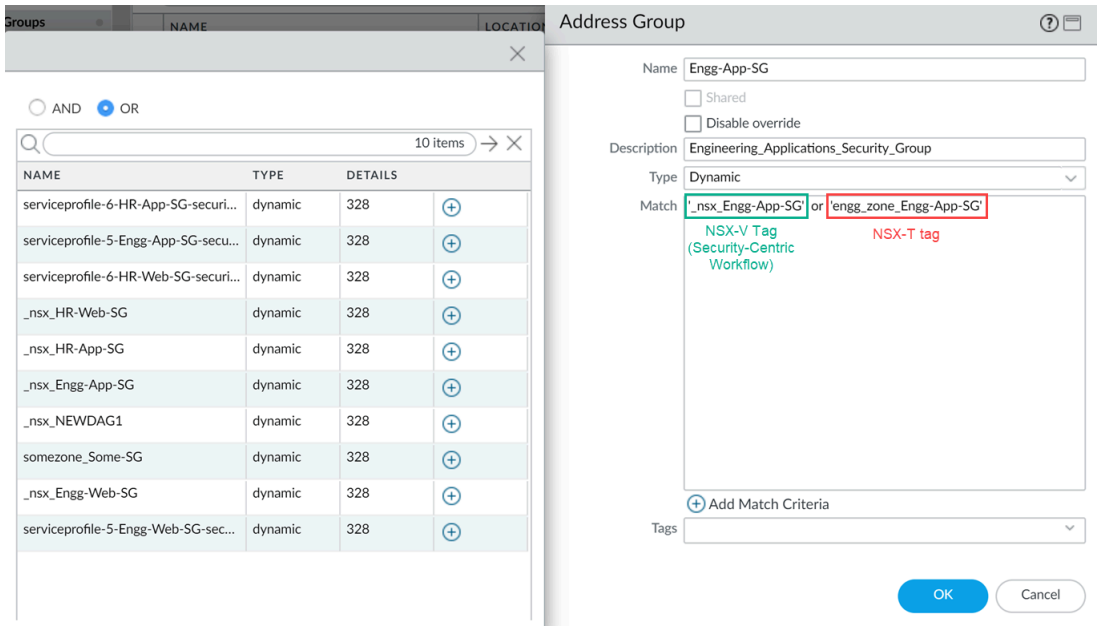
STEP 4 | Préparez votre environnement NSX-T et déployez le pare-feu VM-Series. Vous devez créer vos groupes de sécurité, vos chaînes de services et votre politique de redirection du trafic avant de lancer le pare-feu VM-Series.

- Déploiement du pare-feu VM-Series sur NSX-T (Nord-Sud)
- Déploiement du VM-Series à l'aide du flux de travail centré sur les opérations

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Ajoutez les étiquettes NSX-T à vos groupes d'adresses dynamiques existants.

1. Sélectionnez **Panorama** > **Objects (Objets)** > **Address Groups (Groupes d'adresses)**.
2. Cliquez sur le nom d'un groupe d'adresses dynamiques NSX-V existant.
3. Cliquez sur **Add Match Criteria (Ajouter des critères de correspondance)** pour afficher les étiquettes NSX-V et NSX-T.
4. Ajoutez l'étiquette NSX-T aux groupes d'adresses dynamiques. Veillez à utiliser l'opérateur **OR (OU)** entre les étiquettes.
5. Lorsque vous avez ajouté toutes les étiquettes nécessaires, cliquez sur **OK**.
6. **Commit (Validez)** vos modifications.



STEP 6 | Une fois que les charges de travail de votre VM ont migré avec succès du NSX-V au NSX-T, vous pouvez supprimer les étiquettes NSX-V de vos groupes d'adresses dynamiques si vous prévoyez de ne plus utiliser le NSX-V. Toutes les étiquettes NSX-V et les adresses IP correspondantes sont désenregistrées une fois que l'ensemble de la configuration liée au NSX-V est retiré du plugin Panorama pour NSX et que la configuration du pare-feu de VM-Series est retirée du gestionnaire NSX-V.

 ©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur NSX-T (Est-Ouest)

Le pare-feu VM-Series sur VMware NSX-T intègre les pare-feu nouvelle génération de Palo Alto et Panorama avec des serveurs hôtes ESXi pour offrir une visibilité complète et une activation sécurisée des applications de tout le trafic est-ouest dans votre centre de données défini par logiciel NSX-T.

- Composants du pare-feu VM-Series sur NSX-T (Est-Ouest)
- Pare-feu VM-Series sur l'intégration NSX-T (Est-Ouest)
- Déploiements pris en charge du pare-feu VM-Series sur VMware NSX-T (Est-Ouest)
- Déploiement du VM-Series à l'aide du flux de travail centré sur les opérations
- Déploiement du VM-Series à l'aide du flux de travail centré sur la sécurité
- Suppression d'une définition de service de Panorama
- Migration d'une utilisation de VM-Series sur NSX-T vers un déploiement centré sur la sécurité
- Extension de la politique de sécurité du NSX-V au NSX-T
- Utilisation de la migration sur place pour déplacer votre VM-Series du NSX-V au NSX-T

Composants du pare-feu VM-Series sur NSX-T (Est-Ouest)

Les tableaux suivants indiquent les composants de cette solution conjointe Palo Alto Networks et VMware NSX-T (Est-Ouest).

Composants VMware	
vCenter/ESXi	Le serveur vCenter est l'outil de gestion centralisée de la suite vSphere. ESXi est un hyperviseur qui permet la virtualisation informatique. Reportez-vous à la matrice de compatibilité VMware pour la compatibilité de vCenter avec votre version de NSX-T.
NSX-T Manager	Le centre de données VMware NSX-T 2.5.0 et versions ultérieures doit être installé et enregistré sur le serveur vCenter. Le NSX-T Manager et requis pour déployer le pare-feu VM-Series sur les hôtes ESXi au sein d'un cluster ESXi.

Composants Palo Alto Networks	
PAN-OS	PAN-OS 10.1.x et versions ultérieures.

©2023 Palo Alto Networks, Inc.

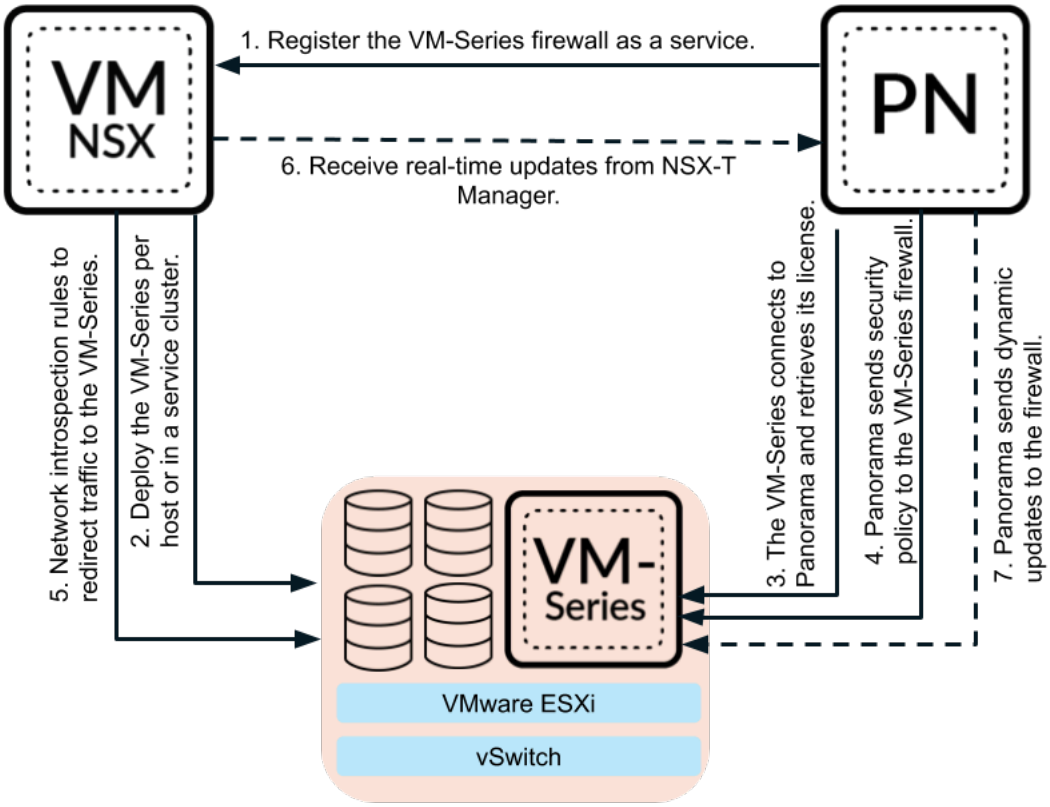
Composants Palo Alto Networks	
	L'image de base VM-Series (PA-VM-NST-10.1.0zip par exemple) est requise pour le déploiement du pare-feu VM-Series sur NSX-T. La configuration système minimale requise pour le déploiement du pare-feu VM-Series pour NSX sur le serveur ESXi dépend de votre modèle VM-Series. Reportez-vous à la section Modèles VM-Series pour obtenir la configuration matérielle minimale requise pour votre modèle VM-Series.
Panorama Panorama doit exécuter la même version ou une version ultérieure que les pare-feu qu'il doit gérer.	Le pare-feu VM-Series sur NSX-T nécessite Panorama 10.1.0 ou version ultérieure pour les pare-feu exécutant la version 10.1.0 Panorama est l'outil de gestion centralisée pour les pare-feu de dernière génération Palo Alto Networks. Dans cette solution, Panorama fonctionne avec le NSX-T Manager pour déployer, mettre sous licence et gérer de manière centralisée la configuration et les politiques sur le pare-feu VM-Series pour NSX-T. Panorama doit pouvoir se connecter au NSX-T Manager, aux pare-feu VM-Series et au serveur de mise à jour Palo Alto Networks. Reportez-vous à la section Guide de l'administrateur Panorama 10.2 pour plus d'informations sur le déploiement de votre appareil Panorama.
Plug-in Panorama pour VMware NSX	3.1.0 ou version ultérieure 4.0.0 ou version ultérieure pour le flux de travail centré sur la sécurité
Plug-in VM-Series	1.0.8 ou version ultérieure
Modèles de pare-feu VM-Series	Les modèles VM-100, VM-300, VM-500 et VM-700 prennent en charge NSX-T.

©2023 Palo Alto Networks, Inc.

Composants Palo Alto Networks	
	Avant de déployer la pare-feu VM-Series sur NSX-T, assurez-vous de disposer de ressources matérielles suffisantes pour prendre en charge le nombre de pare-feu VM-Series dans le modèle de déploiement que vous avez choisi (cluster de services ou par hôte). Ce point est essentiel lorsque vous déployez des pare-feu volumineux tels que le VM-700.

Pare-feu VM-Series sur l'intégration NSX-T (Est-Ouest)

NSX-T Manager, vCenter, Panorama et le pare-feu VM-Series fonctionnent ensemble pour répondre aux problèmes de sécurité de votre centre de données NSX-T.



1. **Enregistrez le pare-feu VM-Series en tant que service** : utilisez Panorama pour vous connecter à votre VMware NSX-T Manager. Panorama communique avec NSX-T Manager à l'aide de l'API NSX-T et établit une communication bidirectionnelle. Sur Panorama, configurez le gestionnaire de

 ©2023 Palo Alto Networks, Inc.

service en saisissant l'adresse IP, le nom d'utilisateur et le mot de passe de NSX-T Manager pour lancer la communication.

Une fois la communication établie avec NSX-T Manager, configurez la définition du service. La définition du service comprend l'emplacement de l'image de base du pare-feu VM-Series, le code d'autorisation nécessaire pour mettre le pare-feu VM-Series sous licence, ainsi que les groupes de périphériques et la pile de modèles à laquelle appartiendra le pare-feu.

NSX Manager utilise également cette connexion pour envoyer des mises à jour concernant les modifications de l'environnement NSX-T avec Panorama.

2. **Déployez le pare-feu VM-Series par hôte dans un cluster de service** : NSX-T Manager utilise les informations transmises par Panorama dans la définition du service afin de déployer le pare-feu VM-Series. Choisissez un endroit où le pare-feu VM-Series sera déployé (dans un cluster de service ou sur chaque hôte ESXi) et comment NSX-T fournit une adresse IP de gestion au pare-feu VM-Series (DHCP ou IP statique). Lorsque le pare-feu démarre, l'API de NSX-T Manager se connecte au pare-feu VM-Series à l'hyperviseur de manière à ce qu'il puisse recevoir le trafic de vSwitch.
3. **Le VM-Series se connecte à Panorama** : le pare-feu VM-Series se connecte ensuite à Panorama pour obtenir sa licence. Panorama obtient la licence depuis le serveur de mises à jour Palo Alto Networks et l'envoie au pare-feu. Lorsque le pare-feu obtient sa licence, il redémarre et se restaure avec un numéro de série.

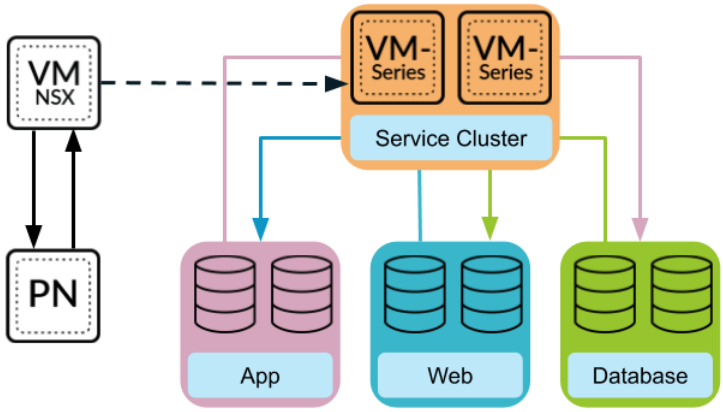
   Si Panorama ne possède pas d'accès à Internet, il ne peut pas récupérer des licences et les transmettre au pare-feu. Vous devez donc mettre chaque pare-feu sous licence manuellement. Si le pare-feu VM-Series ne possède pas d'accès à Internet, vous devez ajouter manuellement les numéros de série à Panorama pour les enregistrer en tant que périphériques gérés. Panorama pourra alors transmettre les piles de modèles, les groupes de périphériques et les autres informations de configuration. Pour plus d'informations, consultez Activation de la licence pour le pare-feu VM-Series pour VMware NSX.
4. **Panorama envoie la politique de sécurité au pare-feu VM-Series** : lorsque le pare-feu se reconnecte à Panorama, il est ajouté au groupe de périphériques et à la pile de modèles définis dans la définition du service, et Panorama transmet la politique de sécurité appropriée à ce pare-feu. Le pare-feu peut désormais sécuriser le trafic dans votre centre de données NSX-T.
5. **Création de règles d'introspection du réseau pour rediriger le trafic vers le pare-feu VM-Series** : créez une chaîne de service sur NSX-T Manager et des règles d'introspection du réseau qui redirigent le trafic dans votre centre de données NSX-T.
6. **Envoi de mises à jour en temps réel de NSX-T Manager** : NSX-T Manager envoie des mises à jour en temps réel des modifications effectuées dans l'environnement virtuel à Panorama. Ces mises à jour comprennent des modifications au niveau de l'adhésion à des groupes et des adresses IP des machines virtuelles en groupes qui envoient le trafic au pare-feu VM-Series.
7. **Panorama envoie des mises à jour dynamiques** : à mesure que Panorama reçoit des mises à jour par NSX-T Manager, il envoie ces mises à jour depuis ses pare-feu gérés VM-Series. Panorama place des machines virtuelles dans des groupes d'adresses dynamiques en se basant sur des critères que vous déterminez, et transmet les informations d'adhésion aux groupes d'adresses dynamiques aux pare-feu. Les pare-feu peuvent alors appliquer la politique de sécurité appropriée au trafic depuis et vers les machines virtuelles dans votre centre de données NSX-T.

©2023 Palo Alto Networks, Inc.

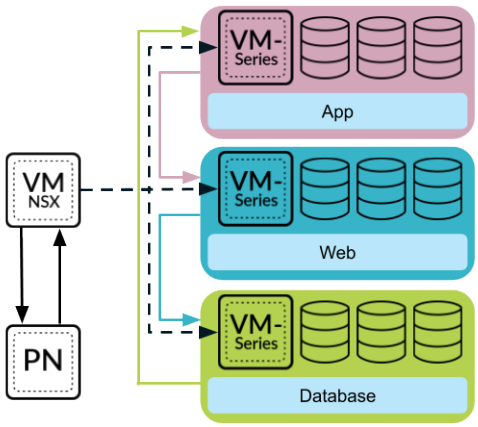
Déploiements pris en charge du pare-feu VM-Series sur VMware NSX-T (Est-Ouest)

Vous pouvez déployer une ou plusieurs instances du pare-feu VM-Series en tant que service partenaire dans votre centre de données VMware NSX-T pour sécuriser le trafic est-ouest et effectuer une microsegmentation. Pour configurer le pare-feu VM-Series afin d'effectuer une microsegmentation, vous pouvez déployer les pare-feu dans un cluster de services ou par hôte.

- **Cluster de services** : dans le cas d'un déploiement par clusters, tous les pare-feu VM-Series sont installés sur un seul cluster. Le trafic entre les VM et les groupes est redirigé vers le cluster VM-Series pour une inspection et une mise en œuvre des politiques avant de poursuivre vers sa destination. Lorsque vous configurez un déploiement par clusters, vous pouvez préciser un hôte particulier au sein du cluster, ou sélectionner **Any (Tout)** et laisser NSX-T choisir un hôte.



- **Basé sur un hôte** : dans le cas d'un déploiement par hôte, une instance du pare-feu VM-Series est installée sur chaque hôte dans le cluster ESXi. Le trafic entre les invités sur le même hôte est inspecté par le pare-feu local et ne doit donc pas quitter l'hôte pour une inspection. Le trafic quittant l'hôte est inspecté par le pare-feu avant d'atteindre le vSwitch.



Après avoir déployé le pare-feu, vous configurez des règles de redirection du trafic qui envoient du trafic au pare-feu VM-Series. Les règles de politique de sécurité que vous configurez sur Panorama sont transférées vers les pare-feu gérés VM-Series, puis appliquées au trafic traversant le pare-feu.

Pour déployer votre pare-feu VM-Series sur VMware NSX-T, vous disposez de deux possibilités de flux de travail : un déploiement centré sur les opérations et un déploiement centré sur la sécurité.

©2023 Palo Alto Networks, Inc.

- Centré sur les opérations : dans un flux de travail centré sur les opérations, certaines parties de la procédure de déploiement sont effectuées sur Panorama et le reste est effectué sur NSX-T Manager. Sur Panorama, vous devez d'abord activer la communication entre Panorama et NSX-T Manager, configurer la définition du service et lancer le pare-feu VM-Series. Ensuite, vous devez vous connecter à NSX-T Manager pour poursuivre la configuration en créant des chaînes de services et des règles de redirection. Pour terminer votre déploiement VM-Series, vous devez revenir à Panorama pour créer une politique de sécurité.
- Centré sur la sécurité : dans un flux de travail centré sur la sécurité, vous pouvez utiliser Panorama comme un tableau de bord unique pour contrôler et gérer les opérations de sécurité. Vous terminez l'intégralité du flux de travail de déploiement à partir de Panorama. Le plug-in Panorama pour VMware NSX transmet la configuration à NSX-T Manager, qui crée des chaînes de services et des règles de redirection.

Il est recommandé de sélectionner un flux de travail de déploiement pour votre déploiement VM-Series sur NSX-T pour plus de facilité d'utilisation. Cependant, le pare-feu VM-Series pour VMware NSX-T prend en charge l'utilisation des deux flux de travail sur le même plug-in.

Déploiement du VM-Series à l'aide du flux de travail centré sur les opérations

Effectuez les tâches suivantes pour déployer le pare-feu VM-Series afin de sécuriser le trafic Est-Ouest dans votre centre de données NSX-T.

- Installation du plug-in Panorama pour VMware NSX
- Autorisation de la communication entre NSX-T Manager et Panorama
- Création de piles de modèles et de groupes de périphériques sur Panorama
- Configuration de la définition de service sur Panorama
- Lancement du pare-feu VM-Series sur NSX-T (Est-Ouest)
- Ajout d'une chaîne de service
- Redirection du trafic vers le pare-feu VM-Series
- Application des politiques de sécurité au pare-feu VM-Series sur NSX-T (Est-Ouest)
- Utilisation de vMotion pour déplacer le pare-feu VM-Series entre les hôtes

Installation du plug-in Panorama pour VMware NSX

Téléchargez et installez le plug-in Panorama pour VMware NSX. Reportez-vous à la matrice de compatibilité avant d'installer ou de mettre à jour votre plug-in.

Si vous avez une configuration d'HA de Panorama, répétez ce processus d'installation sur chaque pair de Panorama. Lors de l'installation du plug-in sur les homologues HA Panorama, installez le plug-in sur le pair passif avant le pair actif. Après avoir installé le plug-in sur l'homologue passif, il passera à un état non fonctionnel. L'installation du plug-in sur l'homologue actif renvoie l'homologue passif à un état fonctionnel.

Si vous avez un appareil Panorama autonome ou deux appareils Panorama installés dans une paire HA avec plusieurs plug-ins installés, les plug-ins peuvent ne pas recevoir les informations des indicateurs d'adresse IP mises à jour si un ou plusieurs des plug-ins ne sont pas configurés. Cela se produit, car Panorama ne transfère pas les informations des indicateurs d'adresse IP aux plug-

 ©2023 Palo Alto Networks, Inc.

ins non configurés. De plus, ce problème peut se présenter si un ou plusieurs plug-ins Panorama ne se trouvent pas dans l'état Registered (Enregistré) ou Success (Réussite) (l'état positif diffère sur chaque plug-in). Assurez-vous que vos plug-ins se trouvent dans l'état positif avant de continuer ou d'exécuter les commandes décrites ci-dessous.

Si vous rencontrez ce problème, il existe deux solutions alternatives :

- Désinstallez le ou les plug-ins non configurés. Il est déconseillé d'installer un plug-in que vous n'envisagez pas de configurer dans l'immédiat
- Vous pouvez utiliser les commandes suivantes pour contourner ce problème. Exécutez la commande suivante pour chaque plug-in non configuré sur chaque instance de Panorama afin que Panorama n'attende pas pour envoyer des mises à jour. Dans le cas contraire, vos pare-feu risquent de perdre certaines informations des indicateurs d'adresse IP.

  `request plugins dau plugin-name <plugin-name> unblock-device-push yes`

  Vous pouvez annuler cette commande en exécutant :

  `request plugins dau plugin-name <plugin-name> unblock-device-push no`

Les commandes décrites ne sont pas persistantes lors des redémarrages et doivent être réutilisées pour tout redémarrage ultérieur. Pour Panorama en paire HA, les commandes doivent être exécutées sur chaque Panorama.

STEP 1 | Sélectionnez **Panorama** > **Plugins (Plug-ins)**.

STEP 2 | Sélectionnez **Check Now (Vérifiez maintenant)**pour récupérer la liste des mises à jour disponibles.

STEP 3 | Sélectionnez **Download (Télécharger)** dans la colonne Action pour installer le plug-in (module d'extension).

STEP 4 | Sélectionnez la version du plug-in et cliquez sur **Install (Installer)** dans la colonne Action pour installer le plug-in. Panorama vous alertera lorsque l'installation est terminée.

Autorisation de la communication entre NSX-T Manager et Panorama

Effectuez la procédure suivante pour activer la communication entre Panorama et NSX-T Manager. Vous pouvez connecter votre Panorama à un maximum de 16 NSX-T Managers. Si vous connectez votre Panorama à plusieurs NSX-T Managers, vous devez planifier soigneusement la hiérarchie des groupes de périphériques et les piles de modèles, et examiner leur interaction avec les autres composants nécessaires au déploiement. Les définitions de service font référence aux groupes de périphériques et aux piles de modèles, et transmettent ces informations aux pare-feu des clusters ESXi associés.

STEP 1 | (Facultatif) Ignorez les paramètres du serveur proxy, configurés sur Panorama sous **Panorama** > **Setup (Configuration)** > **Services** > **Proxy Server (Serveur proxy)** pour la communication entre Panorama et NSX-T Manager. Cette commande permet à Panorama de communiquer directement avec NSX-T Manager tout en maintenant la communication par proxy pour d'autres services.

1. Connectez-vous à la CLI Panorama.

 ©2023 Palo Alto Networks, Inc.

2. Exécutez la commande suivante pour activer ou désactiver le contournement du proxy.

   ```
   admin@Panorama> request plugins vmware_nsx proxy bypass {yes | no}
   ```

   Sélectionnez **yes** (oui) pour activer le contournement du proxy et **no** (non) pour désactiver le contournement du proxy. La valeur par défaut est **no** (non).

STEP 2 | Connectez-vous à l'interface Web Panorama.

À l'aide d'une connexion sécurisée (https) fournie par un navigateur Web, connectez-vous avec l'adresse IP et le mot de passe que vous avez affectés lors de la configuration initiale (https://<*adresse IP*>).

STEP 3 | Configurez l'accès au NSX-T Manager. Répétez cette procédure pour chaque NSX-T Manager auquel vous allez connecter Panorama.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Managers (Gestionnaires de service)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name** (Nom) descriptif pour votre NSX-T Manager.
3. (Facultatif) Ajoutez une **Description** pour NSX-T Manager.
4. Saisissez le **NSX Manager URL (URL NSX Manager)** (adresse IP ou FQDN du cluster NSX-T Manager) qui permet d'accéder au NSX-T Manager.
5. Saisissez les informations d'identification de **NSX Manager Login** (Connexion NSX Manager) (nom d'utilisateur et mot de passe) de manière à ce que Panorama puisse s'authentifier auprès du NSX-T Manager.
6. Cliquez sur **OK**.

Si vous changez votre mot de passe de connexion au NSX-T Manager, assurez-vous de le mettre immédiatement à jour sur Panorama. Un mot de passe incorrect rompt la connexion entre Panorama et NSX-T Manager.

STEP 4 | Validez vos modifications sur Panorama.

Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

STEP 5 | Vérifiez l'état de la connexion sur Panorama.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Managers (Gestionnaires de service)**.
2. Vérifiez le message dans la colonne **Status** (État).

   Lorsque la connexion a réussi, l'état affiché est : **Registered (Enregistré)**. Cela indique que Panorama et le NSX-T Manager sont synchronisés.

   Lorsque la connexion a échoué, l'état affiché peut être :

   - **No connection** (aucune connexion) : impossible d'atteindre/établir une connexion réseau au NSX-T Manager.
   - **Invalid Credentials** (informations d'identification invalides) : les informations d'identification d'accès (nom d'utilisateur et/ou mot de passe) sont incorrectes.
   - **Out of sync (Désynchronisé)** : les paramètres de configuration définis sur Panorama sont différents de ceux définis sur le NSX-V Manager. Cliquez sur le lien pour connaître

 ©2023 Palo Alto Networks, Inc.

les détails de la raison de l'échec. Par exemple, NSX-T Manager peut disposer d'une définition de service ayant le même nom que celui qui est défini sur Panorama. Pour corriger l'erreur, utilisez le nom de la définition de service qui est indiqué dans le message d'erreur afin de valider la définition de service sur le NSX-T Manager. Jusqu'à ce que la configuration sur Panorama et le NSX-T Manager soient synchronisées, vous ne pouvez ajouter aucune nouvelle définition de service sur Panorama.

- **Connection Disabled** (connexion désactivée) : la connexion entre Panorama et le NSX-T Manager a été désactivée manuellement.

Création de piles de modèles et de groupes de périphériques sur Panorama

Pour gérer les pare-feu VM-Series pour NSX-T à l'aide de Panorama, ils doivent appartenir à un groupe de périphériques et à un modèle membre d'une pile de modèles. Les groupes de périphériques vous permettent de regrouper les pare-feu qui nécessitent des politiques et des objets similaires comme unités logiques ; la configuration est définie à l'aide des onglets **Objects (Objets)** et **Policies (Politiques)** sur Panorama. Les modèles sont utilisés pour configurer les paramètres requis pour le fonctionnement et l'association des pare-feu VM-Series sur le réseau. La configuration est définie à l'aide des onglets **Device (Périphérique)** et **Network (Réseau)** du Panorama. Chaque pile de modèle contenant des zones utilisées dans votre configuration NSX-T sur Panorama doit être associé à une définition de service ; vous devez au minimum créer une zone dans la pile de modèles afin que le NSX-T Manager puisse rediriger le trafic vers le pare-feu VM-Series.

Panorama peut prendre en charge les déploiements de NSX-T Nord-Sud et NSX-T Est-Ouest en même temps. Il est recommandé de configurer de manière distincte les groupes de périphériques, les piles de modèles, et les définitions de services pour NSX-T Nord-Sud et NSX-T Est-Ouest.

STEP 1 | Ajoutez un groupe de périphériques ou une hiérarchie de groupe de périphériques.

1. Sélectionnez **Panorama** > **Device Groups (Groupes d'appareils)**, puis cliquez sur **Add (Ajouter)**. Vous pouvez aussi créer une hiérarchie de groupe de périphériques.
2. Entrez un **Name (Nom)** unique et une **Description** pour identifier le groupe de périphériques.
3. Cliquez sur **OK**.
4. Cliquez sur **Commit (Valider)**, puis sélectionnez **Panorama** en tant que **Commit Type (Type de validation)** pour enregistrer les modifications de la configuration en cours sur Panorama.

STEP 2 | Ajoutez un modèle.

1. Sélectionnez **Panorama** > **Templates (Modèles)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** unique et une **Description** pour identifier le modèle.
3. Cliquez sur **OK**.
4. Cliquez sur **Commit (Valider)**, puis sélectionnez **Panorama** en tant que **Commit Type (Type de validation)** pour enregistrer les modifications de la configuration en cours sur Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Créez une pile de modèle.

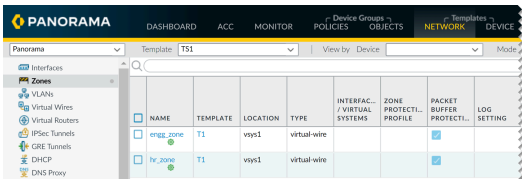
1. Sélectionnez **Panorama** > **Templates (Modèles)**, puis cliquez sur **Add Stack (Ajouter une pile)**.
2. Saisissez un **Name (Nom)** unique et une **Description** pour identifier le modèle.
3. Cliquez sur **OK**.
4. Cliquez sur **Commit (Valider)**, puis sélectionnez **Commit to Panorama (Valider sur Panorama)**pour enregistrer les modifications de la configuration en cours sur Panorama.

STEP 4 | Créez la ou les zones pour chaque modèle.

Chaque zone est associée à un profil de service sur NSX-T Manager. Pour se qualifier, une zone doit être du type de câble virtuel et un modèle doit être associé à une définition de service.

Vous pouvez ajouter jusqu'à 32 zones dans chaque modèle.

1. Sélectionnez **Network (Réseau)** > **Zones**.
2. Sélectionnez le modèle correct dans le menu déroulant **Template** (Modèle).
3. Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** de zone.
4. Définissez le **Type** sur **Virtual Wire (Câble virtuel)**.
5. Cliquez sur **OK**.
6. Vérifiez que les zones sont associées au bon modèle.



7. Cliquez sur **Commit (Valider)**, puis sélectionnez **Panorama** en tant que **Commit Type (Type de validation)** pour enregistrer les modifications de la configuration en cours sur Panorama.

   Panorama crée un profil de service correspondant sur NSX-T Manager pour chaque zone qualifiée lors de la validation.

STEP 5 | Mettez à jour les informations de serveur DNS et NTP de votre pile de modèles. Vous devez effectuer cette étape si vous utilisez des certificats d'appareil dans votre déploiement. Cela est nécessaire pour garantir que les pare-feu déployés dans votre environnement NSX-T disposent des informations DNS correctes nécessaires pour atteindre le serveur de certificats de périphérique.

1. Vérifiez que vous avez spécifié la pile de modèles correcte dans la liste déroulante **Template (Modèle)**.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** et cliquez sur l'icône **Edit (Modifier)**.
3. Dans l'onglet Services, saisissez l'adresse IP du **Primary DNS Server (Serveur DNS principal)** et du **Secondary DNS Server (Serveur DNS secondaire)**.
4. Sous l'onglet NTP, entrez l'adresse IP du **serveur NTP**.
5. Cliquez sur **OK**.
6. **Validez** vos modifications sur Panorama.

 ©2023 Palo Alto Networks, Inc.

Configuration de la définition de service sur Panorama

Une définition de service spécifie la configuration pour les pare-feu VM-Series installés dans votre environnement de centre de données NSX-T. La définition de service doit inclure le groupe de périphériques, une pile de modèles et une URL OVF.

STEP 1 | (Facultatif) Configurez un groupe de notification

Créez un groupe de notification en spécifiant des groupes de périphériques devant être notifiés des modifications apportées à l'environnement virtuel. Les pare-feu des groupes de périphériques spécifiés reçoivent une mise à jour en temps réel des groupes de sécurité et des adresses IP des VM invitées. Les pare-feu utilisent cette mise à jour pour déterminer la liste la plus récente des membres qui constituent les groupes d'adresses dynamiques référencés dans la politique

1. Sélectionnez **Panorama** > **VMware** > **Notify Group (Groupe de notification)** et cliquez sur **Add (Ajouter)**.
2. Donnez au groupe de notification un **Name (Nom)** descriptif.
3. Cochez les cases de tous les groupes de périphériques qui doivent être notifiés des modifications apportées à l'environnement virtuel. Si un groupe de périphériques n'a aucune case à cocher disponible, cela signifie que le groupe de périphériques est automatiquement inclus parce qu'il fait partie d'une hiérarchie de groupe de périphériques.
4. Cliquez sur **OK**.

STEP 2 | Ajoutez une nouvelle définition de service.

Vous pouvez créer jusqu'à 32 définitions de service sur Panorama.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Definitions (Définitions de service)**.
2. Sélectionnez **Add (Ajouter)** pour créer une nouvelle définition de service.
3. Saisissez un **Name** (Nom) descriptif pour votre définition de service.
4. (Facultatif) Ajoutez une **Description** qui identifie la fonction ou le but des pare-feu VM-Series qui seront déployés en utilisant cette définition de service.

STEP 3 | Associez un groupe de périphériques et un modèle pour la définition de service.

Assurez-vous de procéder à la Création de piles de modèles et de groupes de périphériques sur Panorama.

Comme les pare-feu déployés dans cette solution sont gérés de manière centralisée à partir de Panorama, vous devez spécifier le **Device Group (Groupe de périphériques)** et le **Template (Modèle)** auquel les pare-feu appartiennent. Tous les pare-feu qui sont déployés en utilisant cette définition de service appartiennent au modèle et au groupe de périphériques spécifiés.

1. Sélectionnez le groupe d'appareils ou la hiérarchie de groupe d'appareils dans le menu déroulant **Device Group** (Groupe d'appareils).
2. Sélectionnez la pile de modèles dans le menu déroulant **Template** (Modèle).

Vous ne pouvez pas réutiliser un modèle ou un groupe de périphériques attribués à une définition de service dans une autre définition de service.

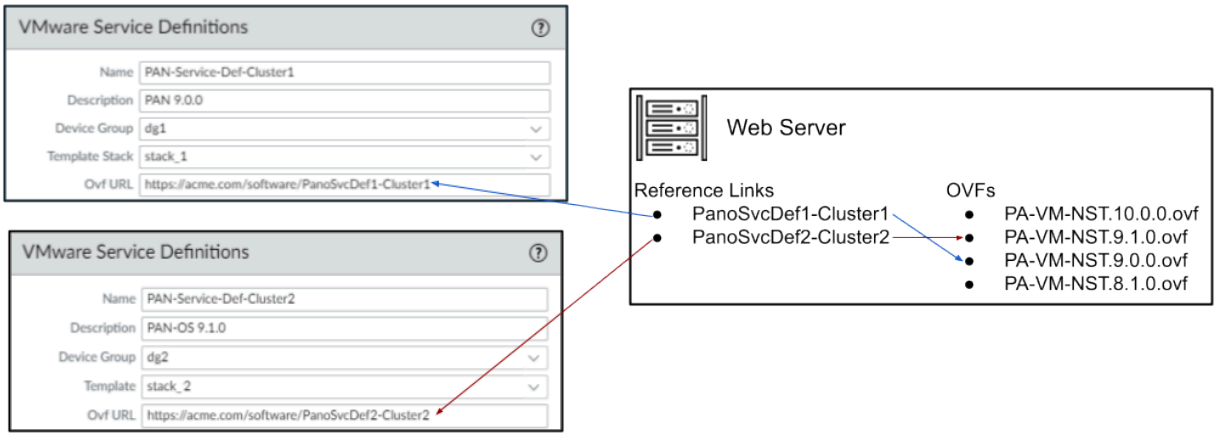
 ©2023 Palo Alto Networks, Inc.

STEP 4 | Spécifiez l'emplacement du fichier OVF.

Téléchargez le fichier zip, puis décompressez-le pour extraire puis enregistrer les fichiers .ovf, mf et .vmdk dans le même répertoire. Les fichiers ovf et vmdk sont utilisés pour déployer chaque instance du pare-feu.

> *Ne modifiez pas le chemin OVF de la définition du service Panorama après un déploiement réussi du service NSX des pare-feu VM-Series. La modification du chemin OVF, après un déploiement réussi du pare-feu VM-Series, peut entraîner un état d'échec du déploiement du service NSX. Vous pouvez résoudre cet échec dans NSX-T Manager, mais cela peut entraîner le redéploiement de tous les pare-feu VM-Series.*

Il est recommandé d'utiliser un nom de chemin OVF qui évolue et vous permette de modifier l'image de base sans affecter vos pare-feu déployés. Au lieu d'un chemin tel que **https://acme.com/software/PA-VM-NST.9.1.0.ovf**, utilisez quelque chose comme **https://acme.com/software/PanoSvcDef1-Cluster1.ovf**. L'utilisation d'une référence de chemin statique éliminera tout besoin futur de modifier le chemin OVF. Il est recommandé de créer un chemin pour chaque définition de service Panorama (cluster vSphere) dans votre déploiement et de modifier les références des images de base PAN-OS sur le serveur Web si nécessaire.



Dans **OVF URL** (URL OVF), ajoutez l'emplacement du serveur Web qui héberge le fichier ovf. Les protocoles http et https sont tous les deux pris en charge.

Vous pouvez utiliser la même version ovf ou des versions différentes entre les définitions de service. L'utilisation de versions ovf différentes entre les définitions de service vous permet de varier la version de PAN-OS sur les pare-feu VM-Series dans différents clusters ESXi.

STEP 5 | (Facultatif) Sélectionnez un **Notify Group (Groupe de notification).**

STEP 6 | Sélectionnez **East West (Est-Ouest)** comme **Insertion Type (Type d'insertion)** pour votre pare-feu.

STEP 7 | (Facultatif) **Activez Health Check (Contrôle de fonctionnement)**. Le contrôle de fonctionnement est activé par défaut dans le plug-in Panorama pour VMware NSX 3.2.0 et versions ultérieures. Dans les anciennes versions du plugin, le contrôle de fonctionnement est

©2023 Palo Alto Networks, Inc.

désactivé par défaut. Aussi appelé contrôle de fonctionnement du service, cette fonctionnalité NSX-T vous permet de simuler une haute disponibilité en cas de défaillance de l'instance de service. Lorsqu'il est configuré avec le pare-feu VM-Series, en cas de défaillance d'une instance de service VM-Series, tout le trafic acheminé vers ce pare-feu est redirigé vers une autre instance de pare-feu dans le cluster (pour les déploiements de cluster de service) ou une instance de pare-feu sur un autre hôte (pour les déploiements basés sur un hôte).

Vous ne pouvez pas désactiver ou activer le contrôle de fonctionnement dans une définition de service après avoir validé et déployé les pare-feu VM-Series dans NSX-T. Si vous essayez de valider une modification dans la configuration du contrôle de fonctionnement, vous recevez un échec de validation. Pour modifier ceci, vous devez supprimer et recréer votre définition de service et redéployer vos pare-feu VM-Series.

STEP 8 | Pour récupérer automatiquement un certificat de périphérique lorsque le pare-feu VM-Series est déployé par NSX Manager, configurez le certificat de périphérique.

Activez cette option pour appliquer un certificat de périphérique aux pare-feu VM-Series nouvellement déployés. N'utilisez cette option que lorsque vous déployez le pare-feu en utilisant une image de base OVF qui prend en charge les certificats de périphériques. Panorama transmet les informations du certificat de périphérique à NSX Manager dans le cadre de la définition du service. Lorsqu'un nouveau pare-feu est déployé dans NSX, le certificat de périphérique est installé sur le pare-feu au démarrage.

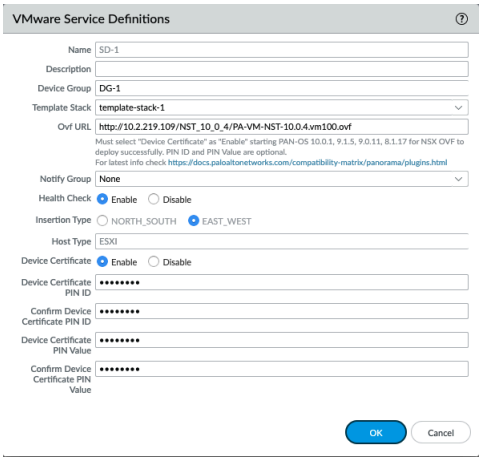
Pour obtenir la liste des OVF qui prennent en charge les certificats de périphériques pour le pare-feu VM-Series sur VMware NSX, consultez Palo Alto Networks Compatibility Matrix (Matrice de compatibilité des réseaux Palo Alto).

Si votre OVF prend en charge un certificat de périphérique, vous devez **activer** les certificats de périphériques, que vous utilisiez ou non un certificat de périphérique. Si votre OVF ne prend pas en charge un certificat de périphérique, désactivez cette option.

1. Si vous ne l'avez pas encore fait, connectez-vous au portail de support client et générez un PIN d'enregistrement et un ID de PIN.
2. Sous **Device Certificate (Certificat de périphérique)**, cliquez sur **Enable (Activer)**.
3. Copiez l'ID de PIN et saisissez-le dans le champ **Device Certificate PIN ID (ID du PIN du certificat de périphérique)**.
4. Saisissez à nouveau l'ID de PIN dans le champ **Confirm Device Certificate PIN ID (Confirmer l'ID du PIN du certificat de périphérique)**.
5. Copiez la valeur du PIN et saisissez-la dans le champ **Device Certificate PIN Value (Valeur du PIN du certificat de périphérique)**.
6. Saisissez à nouveau la valeur du PIN dans le champ **Confirm Device Certificate PIN Value (Confirmer la valeur du PIN du certificat de périphérique)**.

©2023 Palo Alto Networks, Inc.

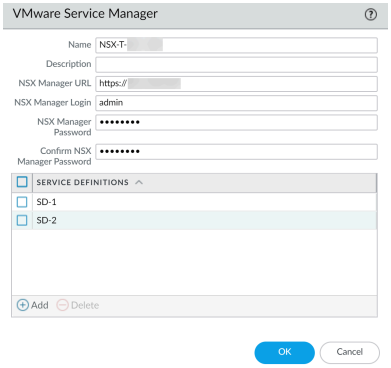
STEP 9 | Cliquez sur **OK** pour enregistrer la définition de service.



STEP 10 | Associez la définition de service au gestionnaire de services.

> *Vous ne pouvez pas utiliser une définition de service dans plus d'un gestionnaire de services.*

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Manager (Gestionnaire de services)** et cliquez sur le lien du nom du gestionnaire de services.
2. Sous Service Definitions (Définitions de service), cliquez sur **Add (Ajouter)** et sélectionnez votre définition de service dans la liste déroulante.
3. Cliquez sur **OK**.



STEP 11 | Ajoutez le code d'autorisation pour mettre sous licence les pare-feu.

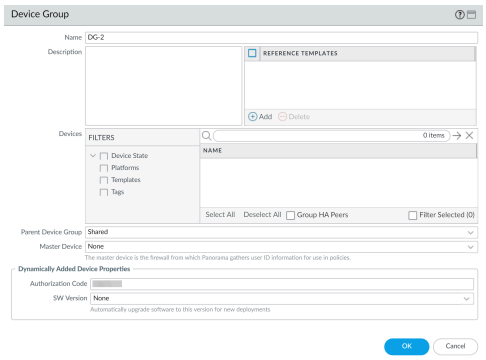
1. Sélectionnez **Panorama** > **Device Groups (Groupes d'appareils)** et choisissez le groupe d'appareils que vous avez associé à la définition de service que vous venez de créer.
2. Sous **Dynamically Added Device Properties (Propriétés du périphérique ajouté dynamiquement)**, ajoutez le code d'autorisation que vous avez reçu avec votre e-mail

 ©2023 Palo Alto Networks, Inc.

de confirmation de commande et, en option, sélectionnez None (Aucune) dans la liste déroulante **SW Version** (Version du logiciel).

Lorsqu'un nouveau pare-feu est déployé sur NSX-T, il est automatiquement ajouté au groupe de périphériques, mis sous licence avec le code d'autorisation que vous avez fourni, et mis à niveau vers la version du logiciel PAN-OS que vous avez indiquée.

Sur le portail de support, vous pouvez consulter le nombre de pare-feu que vous êtes autorisé à déployer et le nombre de licences qui ont été utilisées par rapport au nombre total de licences activées par votre code d'autorisation.



STEP 12 | **Commit to Panorama (Validez sur Panorama)**.

STEP 13 | Sur le gestionnaire NSX-T, vérifiez que la définition de service est disponible.

Sélectionnez **System (Système)** > **Service Deployments (Déploiements de services)** > **Catalog (Catalogue)**. La définition de service est répertoriée en tant que service sur le NSX-T Manager.

Lancement du pare-feu VM-Series sur NSX-T (Est-Ouest)

Effectuez la procédure suivante pour déployer le pare-feu VM-Series en tant que service dans votre environnement NSX-T. Les champs **Deployment Specification (Spécification de déploiement)** et **Deployment Template (Modèle de déploiement)** sont automatiquement remplis avec des informations provenant de Panorama dans le cadre de la définition du service.

Ne modifiez aucun paramètre sous Deployment Attributes (Attributs de déploiement). Ces valeurs sont importées depuis Panorama et leur modification entraîne l'échec du déploiement.

STEP 1 | Connectez-vous à NSX-T Manager.

STEP 2 | Sélectionnez **System (Système)** > **Service Deployments (Déploiements de services)** > **Deployment (Déploiement)**.

STEP 3 | Sélectionnez votre définition de service dans la liste déroulante **Partner Service (Service partenaire)**.

STEP 4 | Cliquez sur **Deploy Service (Déployer le service)**.

STEP 5 | Saisissez un **Name (Nom)** descriptif pour votre déploiement de service.

STEP 6 | Sélectionnez le **Compute Manager (Gestionnaire de calcul)** (vCenter).

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Sélectionnez un **Deployment Type (Type de déploiement)** : **Clustered (En cluster)** ou **Host Based (Basé sur l'hôte)**.

STEP 8 | Si vous avez sélectionné **Clustered (En cluster)** comme **Deployment Type (Type de déploiement)**, saisissez le **Clustered Deployment Count (Nombre de déploiements en cluster)** pour spécifier le nombre d'instances de pare-feu VM-Series à déployer sur le cluster.

STEP 9 | Sélectionnez un **Host (Hôte)** si vous lancez VM-Series dans un déploiement en cluster. Sélectionnez un hôte particulier dans la liste déroulante **Host (Hôte)** ou sélectionnez **Any (Indifférent)** pour permettre à NSX-T Manager de choisir l'hôte. Cette option est grisée dans les déploiements **Per Host (Par hôte)**.

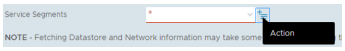
STEP 10 | Sélectionnez un **Data Store (Magasin de données)** comme référentiel pour le pare-feu VM-Series. Dans un déploiement en cluster, sélectionnez un magasin de données partagé si vous choisissez **Any (Indifférent)** pour l'hôte ou sélectionnez un magasin de données local si vous avez spécifié un hôte particulier.

STEP 11 | Configurez les paramètres **Networks (Réseaux)**.

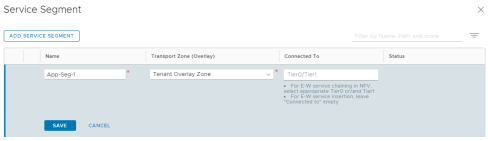
1. Dans la colonne Networks (Réseaux), cliquez sur **Set (Définir)**.
2. Sélectionnez le **Network (Réseau)** pour **eth0 - Management Nic (Carte réseau de gestion)**.
3. Sélectionnez le **Network Type (Type de réseau)** : pool d'adresses IP statiques ou DHCP. Si vous choisissez Static IP Pool (Pool d'adresses IP), sélectionnez un **IP Pool (Pool d'adresses IP)**.
4. Cochez **eth1 - Data-1 Nic**.
5. Cliquez sur **Save (Enregistrer)**.

STEP 12 | Sélectionnez ou configurez un **Service Segment (Segment de service)**. Pour configurer un segment de service, suivez la procédure suivante.

1. Cliquez sur **Action** dans la colonne **Service Segments (Segments de service)**.



2. Cliquez sur **Add Service Segment (Ajouter un segment de service)**.
3. Saisissez un **Name (Nom)** descriptif.
4. Sélectionnez une **Transport Zone (Overlay) (Zone de transport (Superposition))**.
5. Cliquez sur **Save (Enregistrer)**et **Close (Fermer)**.



STEP 13 | Sélectionnez le **Cluster** dans lequel le service sera déployé. Vous devez sélectionner un cluster avec **NSX Configuration (Configuration NSX)**.

STEP 14 | Cliquez sur **Save (Enregistrer)**.

 ©2023 Palo Alto Networks, Inc.

STEP 15 | Assurez-vous que vos pare-feu ont été déployés avec succès.

1. Sélectionnez **System (Système)** > **Service Deployments (Déploiements de services)** > **Service Instances (Instances de services)**.
2. Vérifiez que vos pare-feu sont répertoriés et que le **Deployment Status (État du déploiement)** affiche **Up (Haut)**.

STEP 16 | Vérifiez que vos pare-feu sont connectés à Panorama.

1. Connectez-vous à Panorama.
2. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**.
3. Vérifiez que vos pare-feu sont répertoriés sous le bon groupe de périphériques et que le **Device State (État du déploiement)** affiche **Connected (Connecté)**.

   Le Device Name (Nom de périphérique) du pare-feu VM-Series s'affiche sur Panorama en tant que **PA-VM:<nsx.clusterid>** pour le déploiement de NSX-T (N-S) et en tant que **PA-VM:<nsx.servicevmid>** pour le déploiement de NSX-T (E-W).

Ajout d'une chaîne de service

Une chaîne de service est un groupe de services configurés selon une séquence logique. Lorsque le trafic est redirigé vers la chaîne de service, il passe dans chaque service selon l'ordre que vous avez configuré.

STEP 1 | Sélectionnez **Security (Sécurité)** > **Network Introspection Settings (Paramètres d'introspection réseau)** > **Service Chains (Chaînes de service)** > **Add Chain (Ajouter une chaîne)**.

STEP 2 | Indiquez un **Name (Nom)** et une **Description** (facultatif) pour votre chaîne de services.

STEP 3 | Sélectionnez le **Service Segment (Segment de service)** que vous avez appliqué lorsque vous avez déployé le pare-feu VM-Series.

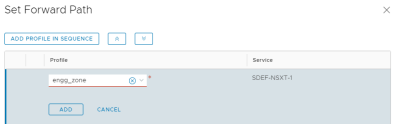
 ©2023 Palo Alto Networks, Inc.

STEP 4 | Configurez le chemin à suivre. La chaîne de service est une séquence logique de profils de services, le trafic passe donc d'un service à l'autre selon l'ordre que vous avez défini comme chemin à suivre.

1. Sélectionnez **Set Forward Path (Configurer le chemin à suivre)** > **Add Profile in Sequence (Ajouter un profil à la séquence)**.
2. Sélectionnez un profil de service. La colonne service est remplie automatiquement en fonction du profil de service que vous sélectionnez.
3. Cliquez sur **Add (Ajouter)**.
4. (Facultatif) Si vous disposez d'autres profils de service partenaires dans votre environnement NSX-T, cliquez sur **Add Profile in Sequence (Ajouter un profil à la séquence)** pour les ajouter à cette chaîne de service.

   Vous ne pouvez sélectionner qu'un seul profil de service par définition de service.

5. Cliquez sur **Save (Enregistrer)** lorsque vous avez fini d'ajouter des profils de service.



STEP 5 | Dans la colonne Reverse Path (Chemin inverse), cochez **Inverse ForwardPath (Inverser le chemin à suivre)** pour que le trafic de retour suive la chaîne de service en ordre inverse.

STEP 6 | (Facultatif) Si d'autres profils de service partenaires sont sélectionnées, définissez un chemin inverse.

Vous devez sélectionner le même profil de service VM-Series défini dans le chemin à suivre.

1. Sélectionnez **Set Reverse Path (Configurer le chemin inverse)** > **Add Profile in Sequence (Ajouter un profil à la séquence)**.
2. Sélectionnez un profil de service. La colonne service est remplie automatiquement en fonction du profil de service que vous sélectionnez.
3. Cliquez sur **Add (Ajouter)**.
4. (Facultatif) Si vous disposez d'autres profils de service dans votre environnement NSX-T, cliquez sur **Add Profile in Sequence (Ajouter un profil à la séquence)** pour les ajouter à cette chaîne de service.
5. Cliquez sur **Save (Enregistrer)** lorsque vous avez fini d'ajouter des profils de service.

STEP 7 | Définissez la **Failure Policy (Politique d'échec)** : **Allow (Autoriser)** ou **Block (Bloquer)**. Cela définit l'action prise par NSX-T en cas d'échec d'un profil de service.

STEP 8 | Cliquez sur **Save (Enregistrer)**.

Redirection du trafic vers le pare-feu VM-Series

Configurez les règles de politique pour diriger le trafic des machines virtuelles ou des groupes de machines virtuelles vers le pare-feu VM-Series.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Sélectionnez **Security (Sécurité)** > **Network Introspection (E-W) (Introspection réseau)** > **Rules (Règles)** > **Add Policy (Ajouter une politique)**.

STEP 2 | Cliquez sur **New Policy (Nouvelle politique)** pour donner un nom descriptif à votre politique.

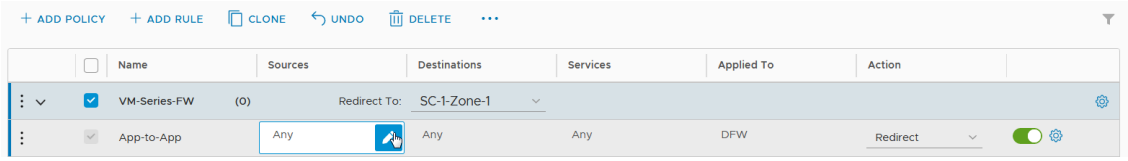
STEP 3 | Sélectionnez votre chaîne de service dans le menu déroulant **Redirect To (Rediriger vers)**.

STEP 4 | Sélectionnez la politique et cliquez sur **Add Rule (Ajouter une règle)**.

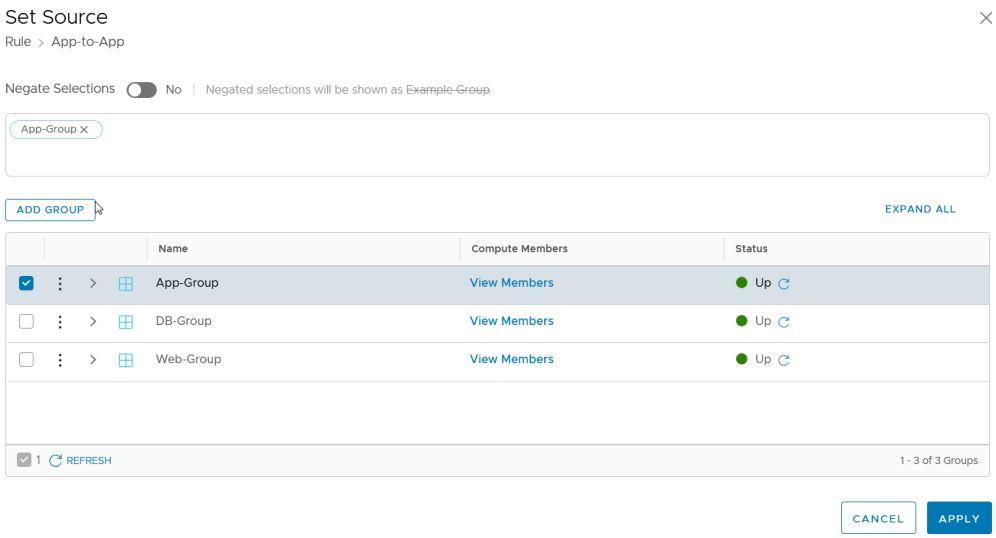
STEP 5 | Cliquez sur **New Rule (Nouvelle règle)** pour donner un nom descriptif à votre règle.

STEP 6 | Sélectionnez une source.

1. Cliquez sur l'icône en forme de crayon dans la colonne source pour choisir un groupe source de machines virtuelles.



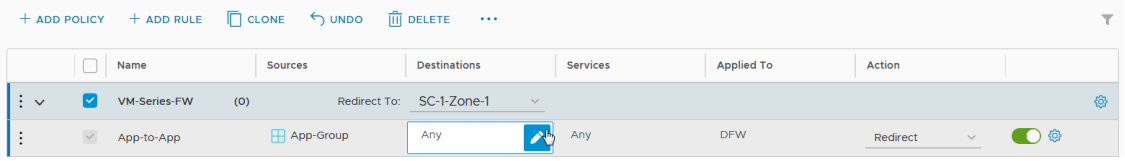
2. Cochez le ou les groupes source.
3. Cliquez sur **Apply (Appliquer)**.



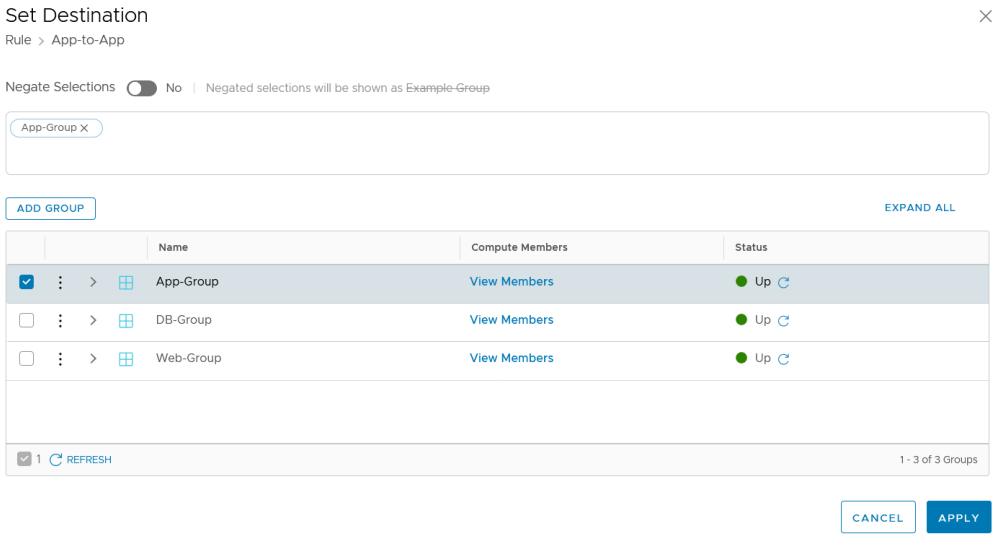
 ©2023 Palo Alto Networks, Inc.

STEP 7 | Sélectionnez une **Destination**.

1. Cliquez sur l'icône en forme de crayon dans la colonne de destination pour choisir un groupe source de machines virtuelles.



2. Cochez le ou les groupes de destination.
3. Cliquez sur **Apply (Appliquer)**.



STEP 8 | (Facultatif) Sélectionnez les**Services** auxquels la règle sera appliquée.

STEP 9 | Choisissez l'un des éléments suivants dans le champ **Applied To (Appliqué à)** :

- Sélectionnez **DFW** pour appliquer la règle à toutes les cartes d'interface réseau (NIC) virtuelles connectées au commutateur logique.
- Sélectionnez **Groups (Groupes)** pour appliquer la règle aux cartes d'interface réseau (NIC) virtuelles des machines virtuelles membres du ou des groupes spécifiés.

STEP 10 | Sélectionnez l'**Action** : **Redirect (Rediriger)** ou **Do Not Redirect (Ne pas rediriger)**.

STEP 11 | Cliquez sur **Publish** (Publier).

STEP 12 | Répétez ce processus pour créer une politique ou des règles supplémentaires.

Application des politiques de sécurité au pare-feu VM-Series sur NSX-T (Est-Ouest)

Maintenant que vous avez créé les règles de redirection dans NSX-T Manager, vous pouvez désormais utiliser Panorama pour administrer les politiques de manière centralisée sur les pare-feu VM-Series.

Pour gérer une politique centralisée, associez le groupe d'adresses dynamiques comme adresse source ou de destination à la politique de sécurité et appliquez-le aux pare-feu ; ces derniers peuvent récupérer de manière dynamique les adresses IP des machines virtuelles de chaque groupe

 ©2023 Palo Alto Networks, Inc.

de sécurité afin d'appliquer la conformité du trafic depuis ou vers les machines virtuelles du groupe spécifié.

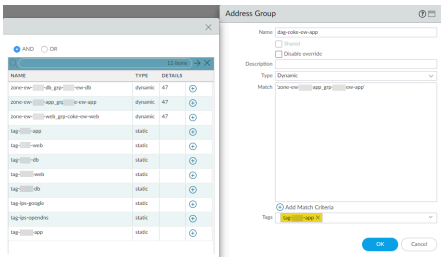
STEP 1 | Connectez-vous à Panorama.

STEP 2 | Créez des groupes d'adresses dynamiques.

1. Sélectionnez **Objects (Objets)** > **Address Groups (Groupes d'adresses)**.
2. Sélectionnez le groupe de périphériques que vous avez créé pour gérer votre VM-Series sur le pare-feu NSX-T dans la liste déroulante **Device Group (Groupe de périphériques)**.
3. Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** et une **Description** pour le groupe d'adresses dynamiques.
4. Définissez le **Type (type)** sur **Dynamic (Dynamique)**.
5. Ajoutez des critères de correspondance à votre groupe d'adresses dynamique.

   Certaines extensions de navigateur peuvent bloquer les appels API entre Panorama et NSX-T, ce qui empêche Panorama de recevoir les critères de correspondance. Si Panorama n'affiche aucun critère de correspondance et que vous utilisez des extensions de navigateur, désactivez ces extensions et cliquez sur Synchronize Dynamic Objects (Synchroniser des objets dynamiques) pour renseigner les étiquettes disponibles dans Panorama.
6. Cliquez sur **Add Match Criteria (Ajouter des critères de correspondance)**.
7. Sélectionnez l'opérateur **And (Et)** ou **Or (Ou)** et cliquez sur l'icône plus (+) à côté du nom du groupe de sécurité pour l'ajouter au groupe d'adresses dynamiques.

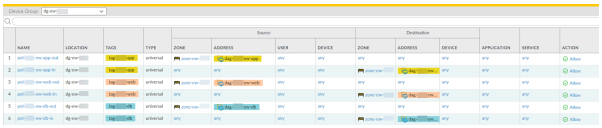
   Les groupes de sécurité qui s'affichent dans la boîte de dialogue de critères de correspondance sont dérivés des groupes que vous avez définis dans NSX-T Manager. Seuls les groupes référencés dans les politiques de sécurité et dont le trafic est redirigé vers le pare-feu VM-Series sont disponibles ici.



8. Cliquez sur **OK**.
9. Répétez ces étapes pour créer le nombre approprié de groupes d'adresses dynamiques requis pour votre déploiement.
10. **Commit (Validez)** vos modifications.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Créez des règles de politique de sécurité.



1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Prerules (Pré-règles)**.
2. Sélectionnez le **Device Group (Groupe d'appareils)** que vous avez créé pour gérer les pare-feu VM-Series sur NSX-T dans Création de piles de modèles et de groupes de périphériques sur Panorama.
3. Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** et une **Description** pour identifier la règle. Dans cet exemple, la règle de sécurité autorise tout le trafic entre les serveurs Web frontaux et les serveurs d'applications.
4. Sélectionnez la **Source Zone (Zone source)** et la **Destination Zone (Zone de destination)**. Le nom de la zone doit être le même dans les deux colonnes.
5. Sous **Source Address (Adresse source)** et **Destination Address (Adresse de destination)**, sélectionnez ou saisissez une adresse, un groupe d'adresses ou une région. Dans cet exemple, un groupe d'adresses est sélectionné. Il s'agit du groupe d'adresses dynamiques créé précédemment.
6. Sélectionnez l'**Application** à autoriser. Dans cet exemple, un **Application Group (Groupe d'applications)** est créé ; il s'agit d'un groupe statique d'applications spécifiques.
   1. Cliquez sur **Add (Ajouter)** et sélectionnez **New Application Group (Nouveau groupe d'applications)**.
   2. Cliquez sur **Add (Ajouter)** pour sélectionner l'application que vous souhaitez inclure dans le groupe.
   3. Cliquez sur **OK** pour créer le groupe d'applications.
7. Spécifiez l'action (**Allow (Autoriser)** ou **Deny (Refuser)**) pour le trafic, puis associez éventuellement les profils de sécurité par défaut pour l'antivirus, l'antispyware et la protection contre les vulnérabilités sous Profils.
8. Surveillance MV Répète les étapes ci-dessus pour créer les règles de politique pertinentes. Le plugiciel AWS sur Panorama.
9. Cliquez sur **Valider** et sélectionnez le type de validation **Panorama**. Cliquez sur **OK**.

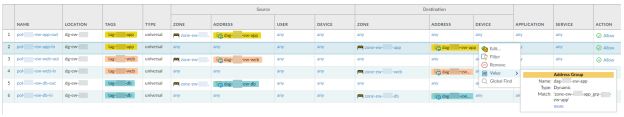
STEP 4 | Appliquez les politiques aux pare-feu VM-Series pour NSX-T.

1. Cliquez sur **Commit (Valider)** et sélectionnez le type de validation **Device Groups (Groupes de périphériques)**.
2. Sélectionnez le groupe de périphériques, c'est-à-dire le groupe de périphériques NSX-T dans cet exemple, puis cliquez sur **OK**.
3. Vérifiez que la validation a réussi.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Assurez-vous que les membres du groupe d'adresses dynamiques sont renseignés sur le pare-feu VM-Series.

1. À partir de Panorama, changez de contexte de périphérique pour lancer l'interface Web d'un pare-feu sur lequel vous avez appliqué des politiques.
2. Sur le pare-feu VM-Series, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et sélectionnez une règle.
3. Cliquez sur la flèche déroulante en regard du lien du groupe d'adresses et sélectionnez **Inspect (Inspecter)**. Vous pouvez également vérifier que les critères de correspondance sont corrects.



4. Cliquez sur le lien **more (Plus)** et vérifiez que la liste des adresses IP enregistrées s'affiche.

   La politique est appliquée à toutes les adresses IP qui appartiennent à ce groupe d'adresses et s'affichent ici.

STEP 6 | (Facultatif) Utilisez un modèle pour appliquer une configuration de périphérique et réseau de base, notamment à un serveur DNS, NTP, Syslog ou à une bannière de connexion.

Pour plus d'informations sur l'utilisation des modèles, reportez-vous au Guide de l'administrateur Panorama.

STEP 7 | Créez un profil de protection de zone et associez-le à une zone.

Un profil de protection de zone offre une protection contre les attaques par inondation et a la capacité de vous protéger contre le balayage de ports et les attaques par commutation de paquets. Il vous permet de sécuriser le trafic dans un niveau et entre les niveaux entre les machines virtuelles au sein de votre centre de données et le trafic provenant d'Internet qui est destiné aux machines virtuelles (charges de travail) dans votre centre de données.

1. Sélectionnez votre **Template (Modèle)**.
2. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)** pour ajouter et configurer un nouveau profil.
3. Sélectionnez **Network (Réseau)** > **Zones**, puis la zone par défaut répertoriée et le profil dans la liste déroulante **Zone Protection Profile (Profil de protection de zone)**.

STEP 8 | Créez un profil de protection DoS (déni de service) et associez-le à la règle de Protection contre les attaques par déni de service.

1. Sélectionnez votre **Groupe de périphériques**.
2. Sélectionnez **Objects (Objet)** > **Security Profiles (Profils de sécurité)** > **DoS Protection (Protection contre les attaques par déni de service)** pour ajouter et configurer un nouveau profil.
   - Un profil classifié permet la création d'un seuil qui s'applique à une seule adresse IP source. Par exemple, vous pouvez configurer le nombre de sessions maximum pour une adresse IP correspondant à la politique, et puis bloquer l'adresse IP unique une fois que le seuil est atteint.

 ©2023 Palo Alto Networks, Inc.

- Un profil agrégé permet la création d'un nombre maximal de sessions pour tous les paquets qui sont conformes à la politique. Le seuil s'applique au nombre de nouvelles sessions pour toutes les adresses IP combinées. Une fois le seuil atteint, tout le trafic qui correspond à la politique est affecté.

3. Créez une nouvelle règle de politique de protection contre les attaques par déni de service dans **Policy (Politique)** > **DoS Protection (Protection contre les attaques par déni de service)**, puis associez-y le nouveau profil.

Utilisation de vMotion pour déplacer le pare-feu VM-Series entre les hôtes

Pour maintenir le flux de trafic lorsque vous utilisez vMotion pour déplacer votre pare-feu VM-Series entre les hôtes ESXI avec des configurations de processeur homogènes dans VMware NSX-T, vous devez utiliser la CLI PAN-OS pour interrompre la surveillance des pulsations du pare-feu VM-Series pendant vMotion. Vous pouvez spécifier la durée, en minutes, pendant laquelle la surveillance des pulsations est interrompue. La surveillance peut être interrompue pendant une durée jusqu'à 60 minutes. Lorsque l'intervalle d'interruption expire ou lorsque vous choisissez d'y mettre fin, la surveillance des pulsations reprend.

Le vMotion du pare-feu VM-Series est pris en charge sur vSphere 6.5, 6.7 et 7.0 si les hôtes ESXi ont une configuration de processeur homogène.

Cette procédure n'est pas requise lorsque vous utilisez vMotion pour déplacer le pare-feu VM-Series si vous exécutez vSphere version 7.0 ou ultérieure.

STEP 1 | Connectez-vous à la CLI du pare-feu VM-Series.

STEP 2 | Réglez l'intervalle d'interruption de la surveillance des pulsations à l'aide de la commande suivante. L'interruption commence dès que la commande est exécutée. Si vMotion dure plus longtemps qu'attendu, vous pouvez réexécuter cette commande pour définir un nouvel intervalle plus long qui démarre lorsque la commande est exécutée une nouvelle fois.

```
request system heartbeat-pause set interval <pause-time-in-minutes>
```

Vous pouvez afficher la durée restante dans l'intervalle de pause à l'aide de la commande suivante.

```
request system heartbeat-pause show interval
```

STEP 3 | (Facultatif) Si vous terminez vMotion avant la fin de l'intervalle d'interruption, vous pouvez mettre fin à l'interruption en réglant l'intervalle sur zéro (0).

```
request system heartbeat-pause set interval 0
```

Déploiement du VM-Series à l'aide du flux de travail centré sur la sécurité

Vous pouvez utiliser le flux de travail centré sur la sécurité pour contrôler et gérer votre pare-feu VM-Series pour NSX-T à partir de Panorama. Vous n'avez pas besoin d'accéder à NSX-T Manager pour créer des chaînes de service et des règles de redirection ; toutefois, le déploiement du service doit toujours être créé sur NSX-T Manager.

- Installation du plug-in Panorama pour VMware NSX
- Autorisation de la communication entre NSX-T Manager et Panorama

 ©2023 Palo Alto Networks, Inc.

- Création de piles de modèles et de groupes de périphériques sur Panorama
- Configuration de la définition de service sur Panorama
- Lancement du pare-feu VM-Series sur NSX-T (Est-Ouest)
- Création de groupes d'adresses dynamiques
- Création de politiques de sécurité
- Création de critères d'adhésion à un Dynamic Address Group (groupe d'adresses dynamiques)
- Génération d'une politique de redirection
- Génération de règles de redirection

Installation du plug-in Panorama pour VMware NSX

Téléchargez et installez le plug-in Panorama pour VMware NSX. Reportez-vous à la matrice de compatibilité avant d'installer ou de mettre à jour votre plug-in.

Le flux de travail de déploiement centré sur la sécurité nécessite le plug-in Panorama pour VMware NSX 4.0.0. En outre, vous devez effectuer une mise à niveau vers le plug-in 4.0.0 à partir du plug-in Panorama pour VMware NSX 3.2.x

Si vous avez une configuration d'HA de Panorama, répétez ce processus d'installation sur chaque pair de Panorama. Lors de l'installation du plug-in sur les homologues HA Panorama, installez le plug-in sur le pair passif avant le pair actif. Après avoir installé le plug-in sur l'homologue passif, il passera à un état non fonctionnel. L'installation du plug-in sur l'homologue actif renvoie l'homologue passif à un état fonctionnel.

Si vous avez un appareil Panorama autonome ou deux appareils Panorama installés dans une paire HA avec plusieurs plug-ins installés, les plug-ins peuvent ne pas recevoir les informations des indicateurs d'adresse IP mises à jour si un ou plusieurs des plug-ins ne sont pas configurés. Cela se produit, car Panorama ne transfère pas les informations des indicateurs d'adresse IP aux plug-ins non configurés. De plus, ce problème peut se présenter si un ou plusieurs plug-ins Panorama ne se trouvent pas dans l'état Registered (Enregistré) ou Success (Réussite) (l'état positif diffère sur chaque plug-in). Assurez-vous que vos plug-ins se trouvent dans l'état positif avant de continuer ou d'exécuter les commandes décrites ci-dessous.

Si vous rencontrez ce problème, il existe deux solutions alternatives :

- Désinstallez le ou les plug-ins non configurés. Il est déconseillé d'installer un plug-in que vous n'envisagez pas de configurer dans l'immédiat
- Vous pouvez utiliser les commandes suivantes pour contourner ce problème. Exécutez la commande suivante pour chaque plug-in non configuré sur chaque instance de Panorama afin que Panorama n'attende pas pour envoyer des mises à jour. Dans le cas contraire, vos pare-feu risquent de perdre certaines informations des indicateurs d'adresse IP.

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  Vous pouvez annuler cette commande en exécutant :

  request plugins dau plugin-name <plugin-name> unblock-device-push no

Les commandes décrites ne sont pas persistantes lors des redémarrages et doivent être réutilisées pour tout redémarrage ultérieur. Pour Panorama en paire HA, les commandes doivent être exécutées sur chaque Panorama.

©2023 Palo Alto Networks, Inc.

STEP 1 | Sélectionnez **Panorama** > **Plugins (Plug-ins)**.

STEP 2 | Sélectionnez **Check Now (Vérifiez maintenant)**pour récupérer la liste des mises à jour disponibles.

STEP 3 | Sélectionnez **Download (Télécharger)** dans la colonne Action pour installer le plug-in (module d'extension).

STEP 4 | Sélectionnez la version du plug-in et cliquez sur **Install (Installer)** dans la colonne Action pour installer le plug-in. Panorama vous alertera lorsque l'installation est terminée.

Autorisation de la communication entre NSX-T Manager et Panorama

Effectuez la procédure suivante pour activer la communication entre Panorama et NSX-T Manager. Vous pouvez connecter votre Panorama à un maximum de 16 NSX-T Managers. Si vous connectez votre Panorama à plusieurs NSX-T Managers, vous devez planifier soigneusement la hiérarchie des groupes de périphériques et les piles de modèles, et examiner leur interaction avec les autres composants nécessaires au déploiement. Les définitions de service font référence aux groupes de périphériques et aux piles de modèles, et transmettent ces informations aux pare-feu des clusters ESXi associés.

STEP 1 | (Facultatif) Ignorez les paramètres du serveur proxy, configurés sur Panorama sous **Panorama** > **Setup (Configuration)** > **Services** > **Proxy Server (Serveur proxy)** pour la communication entre Panorama et NSX-T Manager.

Cette commande permet à Panorama de communiquer directement avec NSX-T Manager tout en maintenant la communication par proxy pour d'autres services.

1. Connectez-vous à la CLI Panorama.
2. Exécutez la commande suivante pour activer ou désactiver le contournement du proxy.

   ```
   admin@Panorama> request plugins vmware_nsx proxy bypass {yes | no}
   ```

   Sélectionnez **yes** (oui) pour activer le contournement du proxy et **no** (non) pour désactiver le contournement du proxy. La valeur par défaut est **no** (non).

STEP 2 | Connectez-vous à l'interface Web Panorama.

À l'aide d'une connexion sécurisée (https) fournie par un navigateur Web, connectez-vous avec l'adresse IP et le mot de passe que vous avez affectés lors de la configuration initiale (https://<*adresse IP*>).

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configurez l'accès au NSX-T Manager.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Managers (Gestionnaires de service)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name** (Nom) descriptif pour votre NSX-T Manager.
3. (Facultatif) Ajoutez une **Description** pour NSX-T Manager.
4. Saisissez le **NSX Manager URL (URL NSX Manager)** (adresse IP ou FQDN du cluster NSX-T Manager) qui permet d'accéder au NSX-T Manager.
5. Saisissez les informations d'identification de **NSX Manager Login** (Connexion NSX Manager) (nom d'utilisateur et mot de passe) de manière à ce que Panorama puisse s'authentifier auprès du NSX-T Manager.
6. Cliquez sur **OK**.
7. Répétez cette procédure pour chaque NSX-T Manager auquel vous allez connecter Panorama.



Si vous changez votre mot de passe de connexion au NSX-T Manager, assurez-vous de le mettre immédiatement à jour sur Panorama. Un mot de passe incorrect rompt la connexion entre Panorama et NSX-T Manager.

STEP 4 | Validez vos modifications sur Panorama.

Sélectionnez **Commit (Valider)** et **Commit to Panorama (Validez sur Panorama)**.

STEP 5 | Vérifiez l'état de la connexion sur Panorama.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Managers (Gestionnaires de service)**.
2. Vérifiez le message dans la colonne **Status** (État).

   Lorsque la connexion a réussi, l'état affiché est : **Registered (Enregistré)**. Cela indique que Panorama et le NSX-T Manager sont synchronisés.

   Lorsque la connexion a échoué, l'état affiché peut être :

   - **No connection** (aucune connexion) : impossible d'atteindre/établir une connexion réseau au NSX-T Manager.
   - **Invalid Credentials** (informations d'identification invalides) : les informations d'identification d'accès (nom d'utilisateur et/ou mot de passe) sont incorrectes.
   - **Out of sync (Désynchronisé)** : les paramètres de configuration définis sur Panorama sont différents de ceux définis sur le NSX-V Manager. Cliquez sur le lien pour connaître les détails de la raison de l'échec. Par exemple, NSX-T Manager peut disposer d'une définition de service ayant le même nom que celui qui est défini sur Panorama. Pour corriger l'erreur, utilisez le nom de la définition de service qui est indiqué dans le message d'erreur afin de valider la définition de service sur le NSX-T Manager. Jusqu'à ce que la configuration sur Panorama et le NSX-T Manager soient synchronisées, vous ne pouvez ajouter aucune nouvelle définition de service sur Panorama.
   - **Connection Disabled** (connexion désactivée) : la connexion entre Panorama et le NSX-T Manager a été désactivée manuellement.

 ©2023 Palo Alto Networks, Inc.

Création de piles de modèles et de groupes de périphériques sur Panorama

Pour gérer les pare-feu VM-Series pour NSX-T à l'aide de Panorama, ils doivent appartenir à un groupe de périphériques et à un modèle membre d'une pile de modèles. Les groupes de périphériques vous permettent de regrouper les pare-feu qui nécessitent des politiques et des objets similaires comme unités logiques ; la configuration est définie à l'aide des onglets **Objects (Objets)** et **Policies (Politiques)** sur Panorama. Les modèles sont utilisés pour configurer les paramètres requis pour le fonctionnement et l'association des pare-feu VM-Series sur le réseau. La configuration est définie à l'aide des onglets **Device (Périphérique)** et **Network (Réseau)** du Panorama. Chaque pile de modèle contenant des zones utilisées dans votre configuration NSX-T sur Panorama doit être associé à une définition de service que vous créerez ultérieurement ; vous devez au minimum créer une zone dans la pile de modèles afin que le NSX-T Manager puisse rediriger le trafic vers le pare-feu VM-Series. Plus tard, vous associerez un groupe d'appareils et un modèle à votre déploiement NSX-T pour créer une définition de service.

Panorama peut prendre en charge les déploiements de NSX-T Nord-Sud et NSX-T Est-Ouest en même temps. Vous devez configurer de manière distincte les groupes de périphériques, les piles de modèles, et les définitions de services pour NSX-T Nord-Sud et NSX-T Est-Ouest.

STEP 1 | Ajoutez un groupe de périphériques ou une hiérarchie de groupe de périphériques.

1. Sélectionnez **Panorama** > **Device Groups (Groupes d'appareils)**, puis cliquez sur **Add (Ajouter)**. Vous pouvez aussi créer une hiérarchie de groupe de périphériques.
2. Entrez un **Name (Nom)** unique et une **Description** pour identifier le groupe de périphériques.
3. Cliquez sur **OK**.
4. Cliquez sur **Commit (Valider)**, puis sélectionnez **Panorama** en tant que **Commit Type (Type de validation)** pour enregistrer les modifications de la configuration en cours sur Panorama.

STEP 2 | Ajoutez un modèle.

1. Sélectionnez **Panorama** > **Templates (Modèles)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** unique et une **Description** pour identifier le modèle.
3. Cliquez sur **OK**.
4. Cliquez sur **Commit (Valider)**, puis sélectionnez **Panorama** en tant que **Commit Type (Type de validation)** pour enregistrer les modifications de la configuration en cours sur Panorama.

STEP 3 | Créez une pile de modèles et ajoutez votre modèle nouvellement créé.

1. Sélectionnez **Panorama** > **Templates (Modèles)**, puis cliquez sur **Add Stack (Ajouter une pile)**.
2. Saisissez un **Name (Nom)** unique et une **Description** pour identifier la pile de modèle.
3. Dans **Templates (Modèles)**, cliquez sur **Add (Ajouter)** et sélectionnez le modèle que vous avez créé à l'étape 2 dans la liste déroulante.
4. Cliquez sur **OK**.
5. Cliquez sur **Commit (Valider)**, puis sélectionnez **Commit to Panorama (Valider sur Panorama)**pour enregistrer les modifications de la configuration en cours sur Panorama.

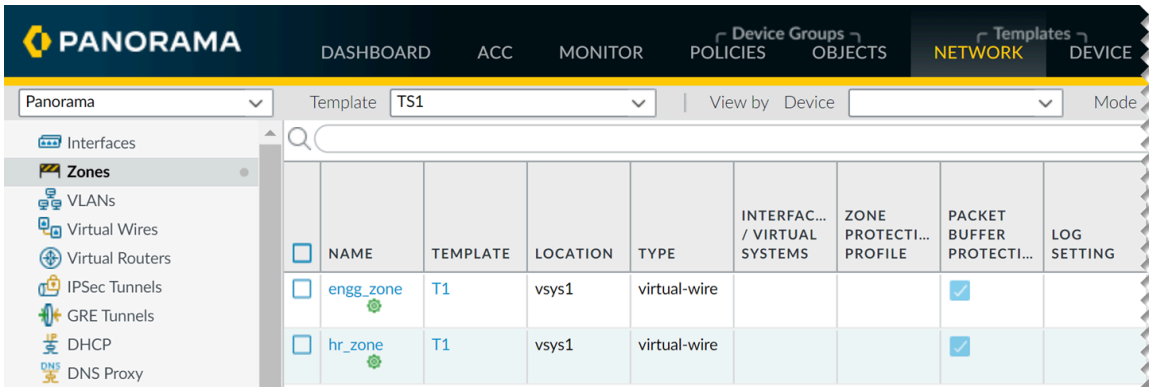
 ©2023 Palo Alto Networks, Inc.

STEP 4 | Créez la ou les zones pour chaque modèle.

Le plug-in Panorama pour VMware NSX mappe chaque zone à un profil de service sur NSX-T Manager. Pour être admissible, une zone doit être du type câble virtuel et faire partie d'un modèle que vous associerez à une définition de service ; voir Configuration de la définition de service sur Panorama pour plus d'informations. Dans la plupart des cas d'utilisation, une seule zone suffit. Toutefois, vous devez créer plusieurs zones pour une location multiple.

Vous pouvez ajouter jusqu'à 32 zones dans chaque modèle.

1. Sélectionnez **Network (Réseau)** > **Zones**.
2. Sélectionnez le modèle correct dans le menu déroulant **Template** (Modèle).
3. Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** de zone.
4. Définissez le **Type** sur **Virtual Wire (Câble virtuel)**.
5. Cliquez sur **OK**.
6. Vérifiez que les zones sont associées au bon modèle.



7. Cliquez sur **Commit (Valider)**, puis sélectionnez **Panorama** en tant que **Commit Type (Type de validation)** pour enregistrer les modifications de la configuration en cours sur Panorama.

STEP 5 | Mettez à jour les informations de serveur DNS et NTP de votre pile de modèles. Vous devez effectuer cette étape si vous utilisez des certificats d'appareil dans votre déploiement. Cela est nécessaire pour garantir que les pare-feu déployés dans votre environnement NSX-T disposent des informations DNS correctes nécessaires pour atteindre le serveur de certificats de périphérique.

1. Vérifiez que vous avez spécifié la pile de modèles correcte dans la liste déroulante **Template (Modèle)**.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** et cliquez sur l'icône **Edit (Modifier)**.
3. Dans l'onglet Services, saisissez l'adresse IP du **Primary DNS Server (Serveur DNS principal)** et du **Secondary DNS Server (Serveur DNS secondaire)**.
4. Sous l'onglet NTP, entrez l'adresse IP du **serveur NTP**.
5. Cliquez sur **OK**.
6. **Validez** vos modifications sur Panorama.

 ©2023 Palo Alto Networks, Inc.

Configuration de la définition de service sur Panorama

Une définition de service vous permet d'enregistrer le pare-feu VM-Series en tant que service de sécurité partenaire sur NSX-T Manager. La définition de service doit inclure le groupe de périphériques, une pile de modèles et une URL OVF.

STEP 1 | (Facultatif) Configurez un groupe de notification

Créez un groupe de notification en spécifiant des groupes de périphériques devant être notifiés des modifications apportées à l'environnement virtuel. Les pare-feu des groupes de périphériques spécifiés reçoivent une mise à jour en temps réel des groupes de sécurité et des adresses IP des VM invitées. Les pare-feu utilisent cette mise à jour pour déterminer la liste la plus récente des membres qui constituent les groupes d'adresses dynamiques référencés dans la politique.

1. Sélectionnez **Panorama** > **VMware** > **Notify Group (Groupe de notification)** et cliquez sur **Add (Ajouter)**.
2. Donnez au groupe de notification un **Name (Nom)** descriptif.
3. Cochez les cases de tous les groupes de périphériques qui doivent être notifiés des modifications apportées à l'environnement virtuel. Si un groupe de périphériques n'a aucune case à cocher disponible, cela signifie que le groupe de périphériques est automatiquement inclus parce qu'il fait partie d'une hiérarchie de groupe de périphériques.
4. Cliquez sur **OK**.

STEP 2 | Ajoutez une nouvelle définition de service.

Vous pouvez créer jusqu'à 32 définitions de service sur Panorama.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Definitions (Définitions de service)**.
2. Sélectionnez **Add (Ajouter)** pour créer une nouvelle définition de service.
3. Saisissez un **Name** (Nom) descriptif pour votre définition de service.
4. (Facultatif) Ajoutez une **Description** qui identifie la fonction ou le but des pare-feu VM-Series qui seront déployés en utilisant cette définition de service.

STEP 3 | Associez un groupe de périphériques et un modèle pour la définition de service.

Assurez-vous de procéder à la Création de piles de modèles et de groupes de périphériques sur Panorama.

Comme les pare-feu déployés dans cette solution sont gérés de manière centralisée à partir de Panorama, vous devez spécifier le **Device Group (Groupe de périphériques)** et le **Template (Modèle)** auquel les pare-feu appartiennent. Tous les pare-feu qui sont déployés en utilisant cette définition de service appartiennent au modèle et au groupe de périphériques spécifiés.

1. Sélectionnez le groupe d'appareils ou la hiérarchie de groupe d'appareils dans le menu déroulant **Device Group** (Groupe d'appareils).
2. Sélectionnez la pile de modèles dans le menu déroulant **Template** (Modèle).

Vous ne pouvez pas réutiliser un modèle ou un groupe de périphériques attribués à une définition de service dans une autre définition de service.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Spécifiez l'emplacement du fichier OVF.

Téléchargez le fichier zip, puis décompressez-le pour extraire puis enregistrer les fichiers .ovf, mf et .vmdk dans le même répertoire. Les fichiers ovf et vmdk sont utilisés pour déployer chaque instance du pare-feu.

Ne modifiez pas le chemin OVF de la définition du service Panorama après un déploiement réussi du service NSX des pare-feu VM-Series. La modification du chemin OVF, après un déploiement réussi du pare-feu VM-Series, peut entraîner un état d'échec du déploiement du service NSX. Vous pouvez résoudre cet échec dans NSX-T Manager, mais cela peut entraîner le redéploiement de tous les pare-feu VM-Series.

Dans **OVF URL** (URL OVF), ajoutez l'emplacement du serveur Web qui héberge le fichier ovf. Les protocoles http et https sont tous les deux pris en charge.

Vous pouvez utiliser la même version ovf ou des versions différentes entre les définitions de service. L'utilisation de versions ovf différentes entre les définitions de service vous permet de varier la version de PAN-OS sur les pare-feu VM-Series dans différents clusters ESXi.

STEP 5 | (Facultatif) Sélectionnez un **Notify Group (Groupe de notification).**

STEP 6 | Sélectionnez **East West (Est-Ouest)** comme **Insertion Type (Type d'insertion)** pour votre pare-feu.

STEP 7 | (Facultatif) **Activez Health Check (Contrôle de fonctionnement)**.

Le contrôle de fonctionnement est activé par défaut. Aussi appelé contrôle de fonctionnement du service, cette fonctionnalité NSX-T vous permet de simuler une haute disponibilité en cas de défaillance de l'instance de service. Lorsqu'il est configuré avec le pare-feu VM-Series, en cas de défaillance d'une instance de service VM-Series, tout le trafic acheminé vers ce pare-feu est redirigé vers une autre instance de pare-feu dans le cluster (pour les déploiements de cluster de service) ou une instance de pare-feu sur un autre hôte (pour les déploiements basés sur un hôte).

Vous ne pouvez pas désactiver ou activer le contrôle de fonctionnement dans une définition de service après avoir validé et déployé les pare-feu VM-Series dans NSX-T. Si vous essayez de valider une modification dans la configuration du contrôle de fonctionnement, vous recevez un échec de validation. Pour modifier ceci, vous devez supprimer et recréer votre définition de service et redéployer vos pare-feu VM-Series.

STEP 8 | Pour récupérer automatiquement un certificat de périphérique lorsque le pare-feu VM-Series est déployé par NSX Manager, configurez le certificat de périphérique.

Activez cette option pour appliquer un certificat de périphérique aux pare-feu VM-Series nouvellement déployés. N'utilisez cette option que lorsque vous déployez le pare-feu en utilisant une image de base OVF qui prend en charge les certificats de périphériques. Panorama transmet les informations du certificat de périphérique à NSX Manager dans le cadre de la définition du

 ©2023 Palo Alto Networks, Inc.

service. Lorsqu'un nouveau pare-feu est déployé dans NSX, le certificat de périphérique est installé sur le pare-feu au démarrage.

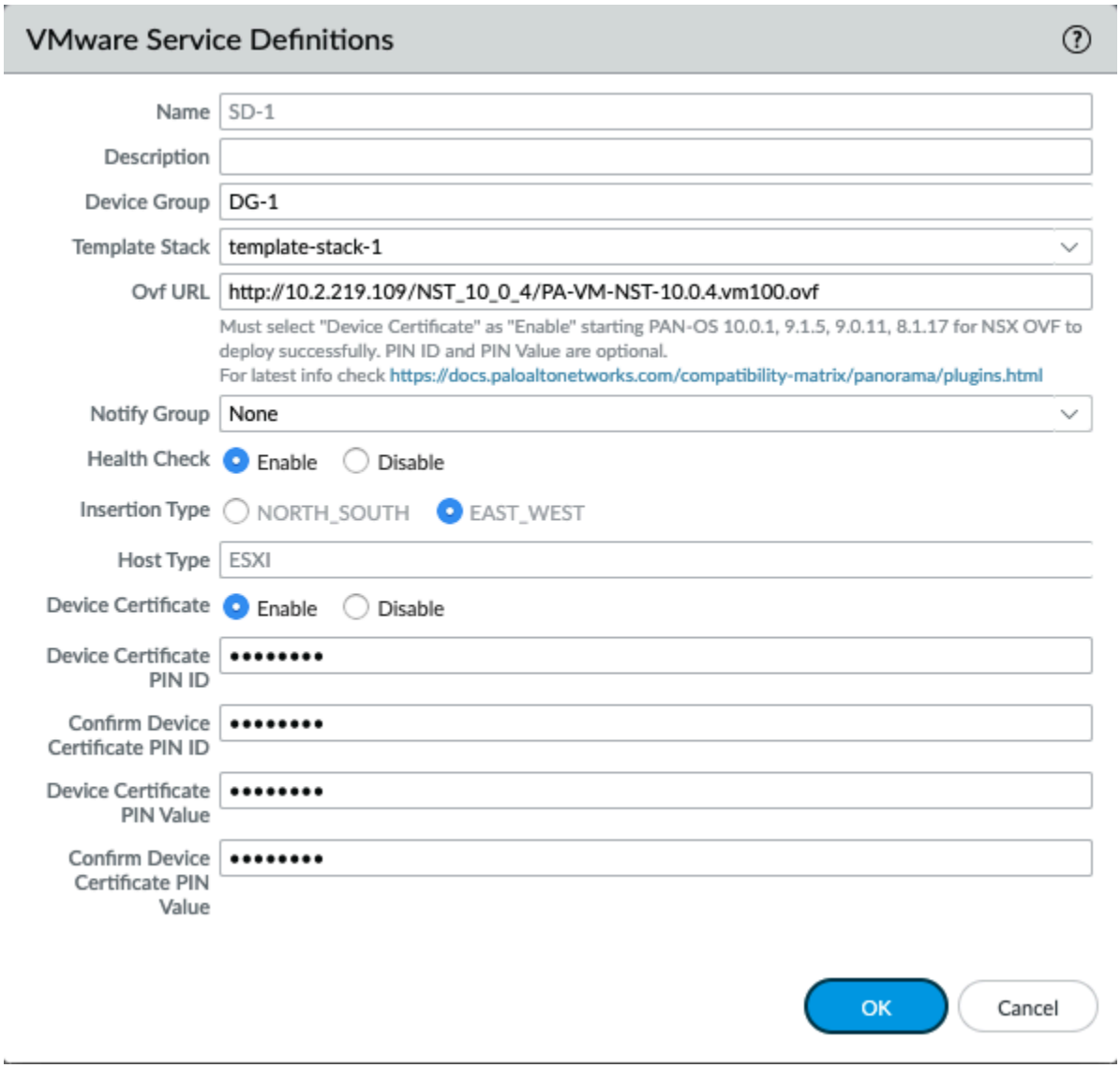
Pour obtenir la liste des OVF qui prennent en charge les certificats de périphériques pour le pare-feu VM-Series sur VMware NSX, consultez Palo Alto Networks Compatibility Matrix (Matrice de compatibilité des réseaux Palo Alto).

Si votre OVF prend en charge un certificat de périphérique, vous devez activer les certificats de périphériques, que vous utilisiez ou non un certificat de périphérique. Si votre OVF ne prend pas en charge un certificat de périphérique, désactivez cette option.

1. Si vous ne l'avez pas encore fait, connectez-vous au portail de support client et générez un PIN d'enregistrement et un ID de PIN.
2. Sous **Device Certificate (Certificat de périphérique)**, cliquez sur **Enable (Activer)**.
3. Copiez l'ID de PIN et saisissez-le dans le champ **Device Certificate PIN ID (ID du PIN du certificat de périphérique)**.
4. Saisissez à nouveau l'ID de PIN dans le champ **Confirm Device Certificate PIN ID (Confirmer l'ID du PIN du certificat de périphérique)**.
5. Copiez la valeur du PIN et saisissez-la dans le champ **Device Certificate PIN Value (Valeur du PIN du certificat de périphérique)**.
6. Saisissez à nouveau la valeur du PIN dans le champ **Confirm Device Certificate PIN Value (Confirmer la valeur du PIN du certificat de périphérique)**.

©2023 Palo Alto Networks, Inc.

STEP 9 | Cliquez sur **OK** pour enregistrer la définition de service.

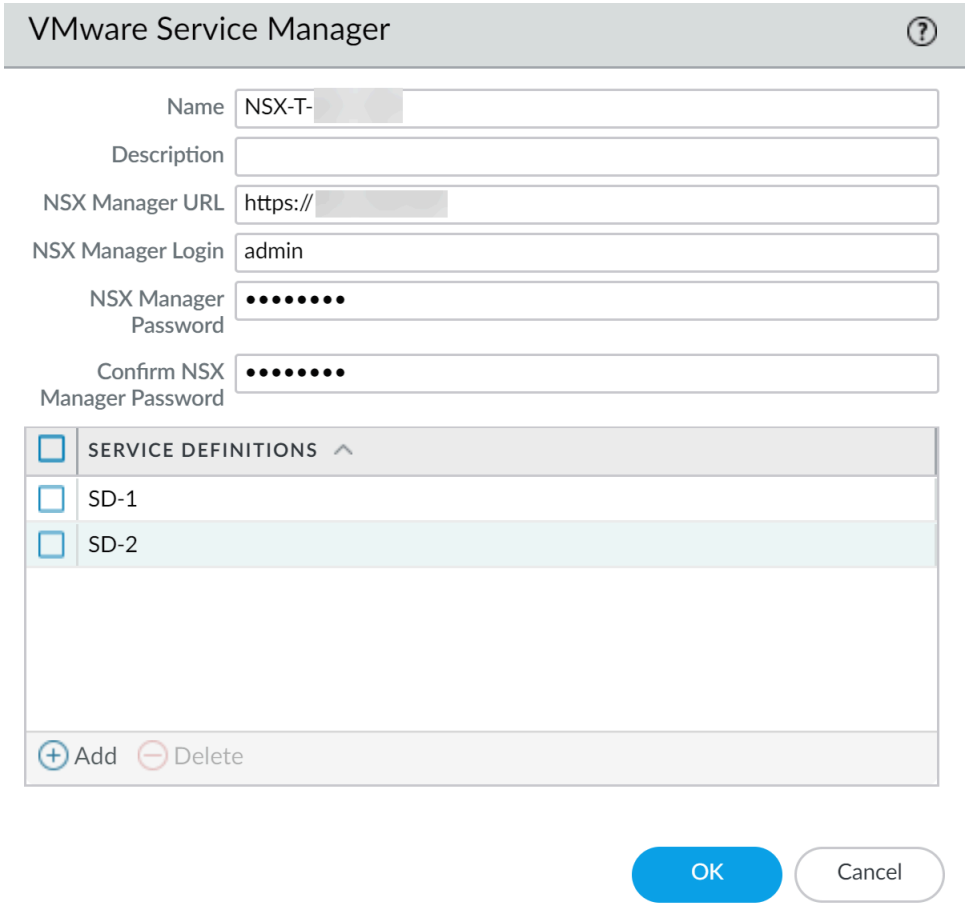


 ©2023 Palo Alto Networks, Inc.

STEP 10 | Associez la définition de service au gestionnaire de services.

Vous ne pouvez pas utiliser une définition de service dans plus d'un gestionnaire de services.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Manager (Gestionnaire de services)** et cliquez sur le lien du nom du gestionnaire de services.
2. Sous Service Definitions (Définitions de service), cliquez sur **Add (Ajouter)** et sélectionnez votre définition de service dans la liste déroulante.
3. Cliquez sur **OK**.



STEP 11 | Ajoutez le code d'autorisation pour mettre sous licence les pare-feu.

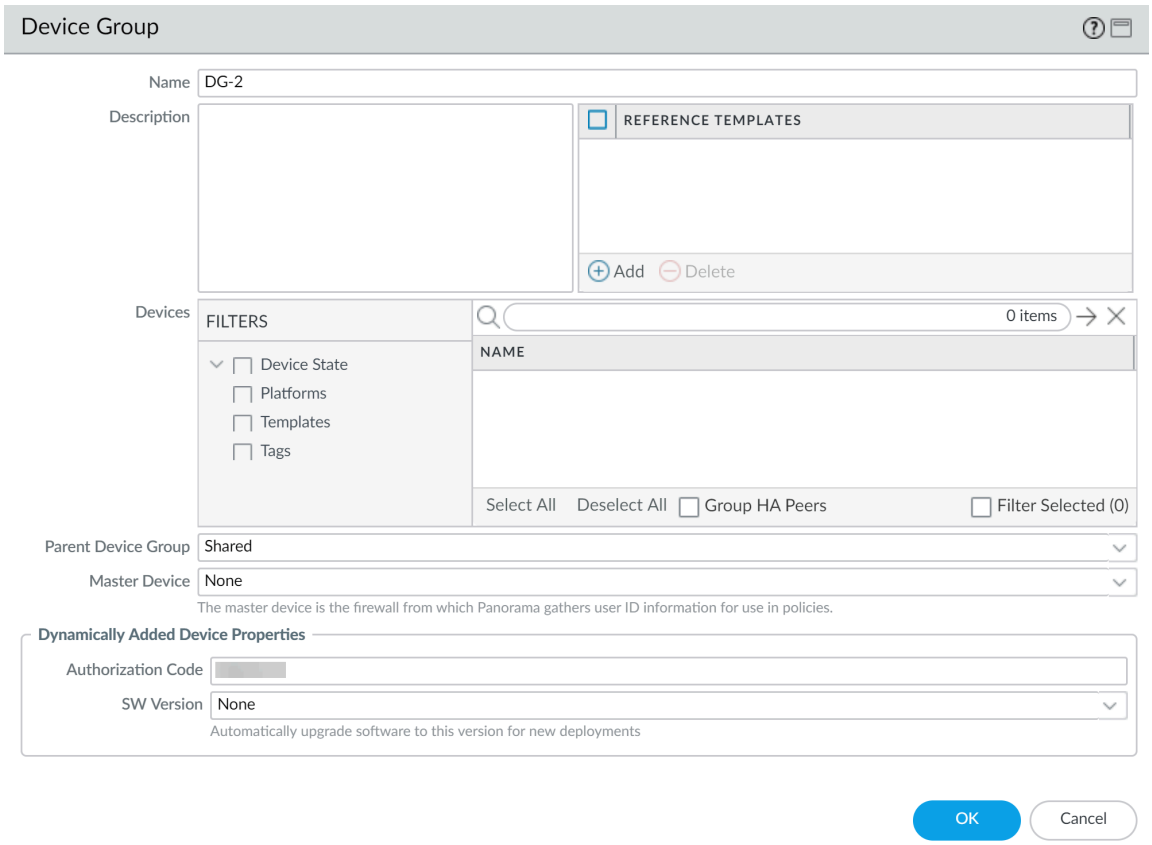
1. Sélectionnez **Panorama** > **Device Groups (Groupes d'appareils)** et choisissez le groupe d'appareils que vous avez associé à la définition de service que vous venez de créer.
2. Sous **Dynamically Added Device Properties (Propriétés du périphérique ajouté dynamiquement)**, ajoutez le code d'autorisation que vous avez reçu avec votre e-mail

©2023 Palo Alto Networks, Inc.

de confirmation de commande et, en option, sélectionnez None (Aucune) dans la liste déroulante **SW Version** (Version du logiciel).

Lorsqu'un nouveau pare-feu est déployé sur NSX-T, il est automatiquement ajouté au groupe de périphériques, mis sous licence avec le code d'autorisation que vous avez fourni, et mis à niveau vers la version du logiciel PAN-OS que vous avez indiquée.

Sur le portail de support, vous pouvez consulter le nombre de pare-feu que vous êtes autorisé à déployer et le nombre de licences qui ont été utilisées par rapport au nombre total de licences activées par votre code d'autorisation.



STEP 12 | **Commit to Panorama (Validez sur Panorama)**.

STEP 13 | Sur le gestionnaire NSX-T, vérifiez que la définition de service est disponible.

Sélectionnez **System (Système)** > **Service Deployments (Déploiements de services)** > **Catalog (Catalogue)**. La définition de service est répertoriée en tant que service sur le NSX-T Manager.

©2023 Palo Alto Networks, Inc.

Lancement du pare-feu VM-Series sur NSX-T (Est-Ouest)

Effectuez la procédure suivante pour déployer le pare-feu VM-Series en tant que service dans votre environnement NSX-T. Les champs **Deployment Specification (Spécification de déploiement)** et **Deployment Template (Modèle de déploiement)** sont automatiquement remplis avec des informations provenant de Panorama dans le cadre de la définition du service.

Ne modifiez aucun paramètre sous Deployment Attributes (Attributs de déploiement). Ces valeurs sont importées depuis Panorama et leur modification entraîne l'échec du déploiement.

STEP 1 | Connectez-vous à NSX-T Manager.

STEP 2 | Sélectionnez **System (Système)** > **Service Deployments (Déploiements de services)** > **Deployment (Déploiement)**.

STEP 3 | Sélectionnez votre définition de service dans la liste déroulante **Partner Service (Service partenaire)**.

STEP 4 | Cliquez sur **Deploy Service (Déployer le service)**.

STEP 5 | Saisissez un **Name (Nom)** descriptif pour votre déploiement de service.

STEP 6 | Sélectionnez le **Compute Manager (Gestionnaire de calcul)** (vCenter).

STEP 7 | Sélectionnez un **Deployment Type (Type de déploiement)** : **Clustered (En cluster)** ou **Host Based (Basé sur l'hôte)**.

STEP 8 | Si vous avez sélectionné **Clustered (En cluster)** comme **Deployment Type (Type de déploiement)**, saisissez le **Clustered Deployment Count (Nombre de déploiements en cluster)** pour spécifier le nombre d'instances de pare-feu VM-Series à déployer sur le cluster.

STEP 9 | Sélectionnez un **Host (Hôte)** si vous lancez VM-Series dans un déploiement en cluster. Sélectionnez un hôte particulier dans la liste déroulante **Host (Hôte)** ou sélectionnez **Any (Indifférent)** pour permettre à NSX-T Manager de choisir l'hôte. Cette option est grisée dans les déploiements **Host Based (Basés sur l'hôte)**.

STEP 10 | Sélectionnez un **Data Store (Magasin de données)** comme référentiel pour le pare-feu VM-Series. Dans un déploiement en cluster, sélectionnez un magasin de données partagé si vous choisissez **Any (Indifférent)** pour l'hôte ou sélectionnez un magasin de données local si vous avez spécifié un hôte particulier.

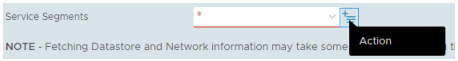
©2023 Palo Alto Networks, Inc.

STEP 11 | Configurez les paramètres **Networks (Réseaux)**.

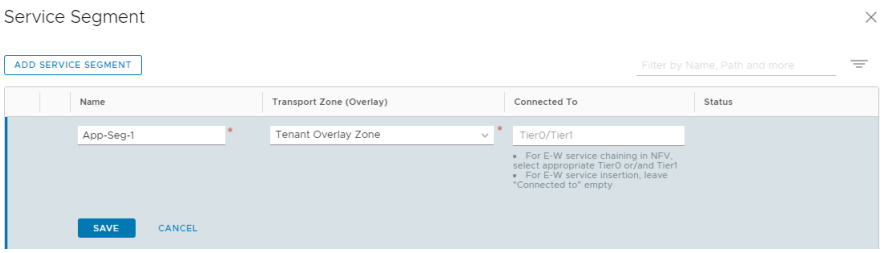
1. Dans la colonne Networks (Réseaux), cliquez sur **Set (Définir)**.
2. Sélectionnez le **Network (Réseau)** pour **eth0 - Management Nic (Carte réseau de gestion)**.
3. Sélectionnez le **Network Type (Type de réseau)** : pool d'adresses IP statiques ou DHCP. Si vous choisissez Static IP Pool (Pool d'adresses IP), sélectionnez un **IP Pool (Pool d'adresses IP)**.
4. Cochez **eth1 - Data-1 Nic**.
5. Vérifiez que les deux interfaces sont cochées.
6. Cliquez sur **Save (Enregistrer)**.

STEP 12 | Sélectionnez ou configurez un **Service Segment (Segment de service)**. Pour configurer un segment de service, suivez la procédure suivante.

1. Cliquez sur **Action** dans la colonne **Service Segments (Segments de service)**.



2. Cliquez sur **Add Service Segment (Ajouter un segment de service)**.
3. Saisissez un **Name (Nom)** descriptif.
4. Sélectionnez une **Transport Zone (Overlay) (Zone de transport (Superposition))**.
5. Cliquez sur **Save (Enregistrer)**et **Close (Fermer)**.



STEP 13 | Sélectionnez le **Cluster** dans lequel le service sera déployé. Vous devez sélectionner un cluster avec **NSX Configuration (Configuration NSX)**.

STEP 14 | Cliquez sur **Save (Enregistrer)**.

STEP 15 | Assurez-vous que vos pare-feu ont été déployés avec succès.

1. Sélectionnez **System (Système)** > **Service Deployments (Déploiements de services)** > **Service Instances (Instances de services)**.
2. Vérifiez que vos pare-feu sont répertoriés et que le **Deployment Status (État du déploiement)** affiche **Up (Haut)**.

©2023 Palo Alto Networks, Inc.

STEP 16 | Vérifiez que vos pare-feu sont connectés à Panorama.

1. Connectez-vous à Panorama.
2. Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**.
3. Vérifiez que vos pare-feu sont répertoriés sous le bon groupe de périphériques et que le **Device State (État du déploiement)** affiche **Connected (Connecté)**.

   Le Device Name (Nom de périphérique) du pare-feu VM-Series s'affiche sur Panorama en tant que **PA-VM:<nsx.clusterid>** pour le déploiement de NSX-T (N-S) et en tant que **PA-VM:<nsx.servicevmid>** pour le déploiement de NSX-T (E-W).

Création de groupes d'adresses dynamiques

Un groupe de sécurité est un conteneur logique qui regroupe des invités sur plusieurs hôtes ESXi d'un cluster. Lorsque vous créez un groupe d'adresses dynamiques répondant aux critères appropriés et que vous validez vos modifications, un groupe de sécurité correspondant est créé sur le NSX-T Manager. La création de groupes de sécurité est nécessaire pour la gestion et la sécurisation des invités.

Pour qu'un Dynamic Address Group (groupe d'adresses dynamiques) devienne un groupe de sécurité sur NSX-T, vous devez ajouter des critères de correspondance dans le groupe d'adresses dynamiques au format suivant : **'_nsxt_<dynamic-address-group-name>'**. Le nom d'adresse dynamique ajouté dans les critères de correspondance doit correspondre exactement au nom du groupe d'adresses dynamiques. Par exemple, un groupe d'adresses dynamique appelé **applications** doit inclure des critères de correspondance **'_nsxt_applications'**. En outre, vous devez inclure le groupe d'adresses dynamiques dans un groupe d'appareils dans une définition de service, qui fait partie d'un gestionnaire de services et qui est validée.

Chaque groupe de sécurité créé à partir d'un Dynamic Address Group (groupe d'adresses dynamiques) suit le format suivant : **<service-def-name>_<dynamic-address-group-name>**. Par exemple, **ServiceDef1_applications**.

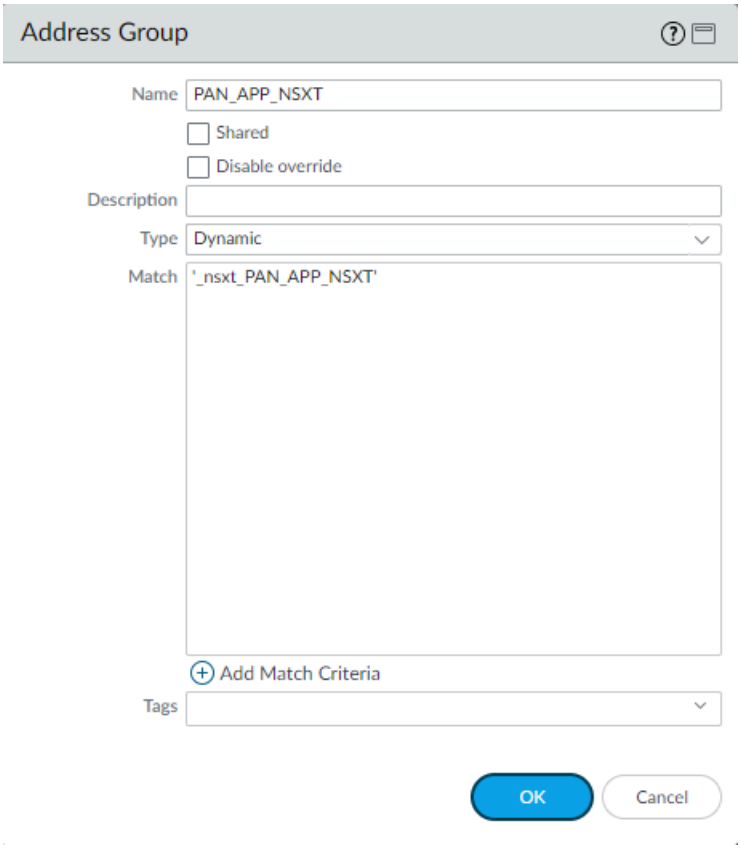
Chaque groupe d'adresses dynamiques que vous créez doit avoir un nom unique sur chaque groupe d'appareils configuré sur votre Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Configurez un groupe d'adresses dynamiques pour chaque groupe de sécurité requis pour votre déploiement.

1. Sélectionnez **Objects (Objets)** > **Address Groups (Groupes d'adresses)**.
2. Vérifiez que vous configurez les groupes d'adresses dynamiques dans un groupe d'appareils associé à une définition de service NSX-T.
3. Cliquez sur **Add (Ajouter)** et saisissez un **Name (nom)** et une **Description** pour identifier le groupe d'adresses.
4. Définissez le **Type (type)** sur **Dynamic (Dynamique)**.
5. Définissez les critères de correspondance.

   Pour que le groupe d'adresses dynamiques devienne un groupe de sécurité dans NSX-T Manager, la chaîne de critères de correspondance doit être placée entre guillemets simples avec le préfixe _nsxt_ suivi du nom exact du groupe d'adresses. Par exemple, ***'_nsxt_PAN_APP_NSX'***.
6. Répétez ce processus pour chaque groupe de sécurité dont vous avez besoin.



STEP 2 | **Commit (Validez)** vos modifications.

Création de politiques de sécurité

Créez des règles de politique de sécurité qui seront utilisées pour générer automatiquement des règles de redirection utilisées dans la politique de redirection.

Lorsque vous Génération de règles de redirection, vous aurez la possibilité de générer des règles de redirection basées sur des règles « avant », des règles « après » ou toutes les règles. Si vous

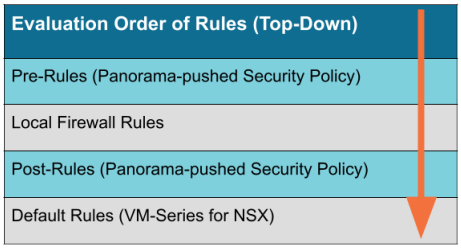
 ©2023 Palo Alto Networks, Inc.

sélectionnez All (Tout), le plug-in VMware pour NSX crée une règle de redirection pour chaque sécurité applicable dans les règles pré et post. Cela peut entraîner la création de règles de redirection inutiles et rendre la gestion des règles plus difficile. Pour aider à séparer facilement vos règles de redirection de vos règles de sécurité, vous pouvez créer vos règles de redirection en tant que post-règles et vos règles de sécurité en tant que pré-règles.

Pour générer automatiquement une règle de redirection basée sur une règle de sécurité créée sur Panorama, la règle de sécurité doit répondre aux critères suivants :

- appartient à un groupe de périphériques parent ou enfant enregistré auprès d'un gestionnaire de services NSX-T ;
- est une politique intra-zone et n'inclut qu'une seule zone ;
- n'inclut pas de groupe d'adresses statiques, de plage d'adresses IP ou de masque de réseau configuré pour la règle.

Lorsque vous décidez où définir vos règles de redirection NSX-T dans Panorama (base de pré-règles ou de post-règles), tenez compte du nombre de règles de politique de sécurité et de règles de redirection NSX-T que vous allez créer sur Panorama et de l'ordre dans lequel les règles sont appliquées au trafic. Les pré-règles sont appliquées au trafic avant les post-règles.



- Pré-règles : vous pouvez utiliser la base de pré-règles Panorama pour définir vos règles de redirection NSX-T et les règles de politique de sécurité du pare-feu VM-Series. Si vous définissez les règles de sécurité et les règles de redirection dans la même base de règles, vous devez considérer l'ordre des règles de sécurité par rapport aux règles de redirection. Lorsque vous disposez d'une grande base de règles qui inclut à la fois des règles de redirection et des règles de politique de sécurité, il peut devenir difficile de gérer les deux types de règles à mesure que vous évoluez.
- Post-règles : séparer vos règles de politique de sécurité utilisées pour l'inspection et l'application des règles de sécurité utilisées pour générer des règles de redirection NSX-T peut vous aider à faire évoluer le déploiement avec un grand nombre de règles. Lorsque vous générez automatiquement vos règles de redirection, le plugin génère une règle de redirection pour chaque règle de la base de règles spécifiée qui répond aux critères nécessaires. Par conséquent, en séparant les deux types de règles, vous pouvez empêcher la génération involontaire de règles de redirection superflues. L'utilisation de la base de post-règles pour les règles de redirection est recommandée ; en particulier dans les déploiements avec de grandes quantités de règles de politique de sécurité.

Les groupes d'adresses dynamiques source et de destination que vous spécifiez dans la règle de sécurité. Lorsque vous générez automatiquement une règle de redirection, l'endroit où la règle est appliquée (pare-feu distribué NSX-T ou groupe de sécurité) dépend de la source et de la destination que vous avez spécifiées lors de la configuration de la règle de sécurité. Si vous en avez sélectionné une pour la source ou la destination, NSX-T Manager applique la règle de redirection au pare-feu distribué. Si vous sélectionnez un groupe d'adresses dynamiques pour la source et la destination, la

 ©2023 Palo Alto Networks, Inc.

redirection est appliquée aux VM invitées dans ces groupes de sécurité. Si vous créez manuellement des règles de redirection, vous pouvez spécifier le ou les groupes de sécurité auxquels la règle de redirection est appliquée.

Assurez-vous que votre politique de sécurité utilisée pour définir les règles de redirection n'inclut pas de groupes d'adresses dynamiques configurés dans le cadre d'un flux de travail de déploiement centré sur les opérations. Si vous le faites, la source et la destination des règles de redirection seront transmises à NSX-T Manager en tant que source-any et destination-any. Cela peut avoir un impact sur le trafic dans votre environnement NSX-T.

Si vous désactivez une règle de sécurité que vous utiliserez pour générer automatiquement une règle de redirection, la règle de redirection sera également désactivée.

- Utilisation de la pré-règlementation pour définir les règles de redirection NSX-T
- Utilisation de la post-règlementation pour définir les règles de redirection NSX-T
- Application des politiques de sécurité au pare-feu VM-Series sur NSX-T (Est-Ouest)

Utilisation de la pré-règlementation pour définir les règles de redirection NSX-T

La procédure suivante décrit comment créer les règles de politique de sécurité qui seront utilisées pour générer des règles de redirection NSX-T et comment créer la politique de sécurité que Panorama poussera vers le pare-feu VM-Series pour l'inspection et l'application du trafic.

N'appliquez **pas** les politiques de redirection du trafic, à moins que vous ne compreniez le fonctionnement des règles sur le NSX-V Manager, ainsi que sur le pare-feu VM-Series et Panorama. La politique par défaut sur le pare-feu VM-Series est définie sur ***deny all (refuser tout)*** ; cela signifie que tout le trafic redirigé vers le pare-feu VM-Series est abandonné.

Créez des règles de politique de sécurité dans le groupe de périphériques associé. Pour chaque règle de sécurité, définissez le Rule Type (Type de règle) sur Intrazone, sélectionnez une zone dans le modèle associé, puis sélectionnez les groupes d'adresses dynamiques en tant que source et destination. La création d'une politique de sécurité admissible dans Panorama facilite la création d'une règle de redirection correspondante sur NSX-T Manager lors de la génération des règles de redirection et de la validation dans Panorama.

STEP 1 | Dans Panorama, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Pré-règles)**.

STEP 2 | Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** et une **Description** pour votre règle de politique de sécurité.

STEP 3 | Vérifiez que vous configurez les politiques de sécurité dans un groupe d'appareils associé à une définition de service NSX-T.

STEP 4 | Définissez le Rule Type (Type de règle) sur **intrazone (Périphériques avec PAN-OS 6.1 ou version ultérieure)**.

STEP 5 | Dans l'onglet Source, définissez la zone source sur la zone à partir du modèle associé à la définition de service. Sélectionnez ensuite un groupe d'adresses dynamiques (groupe de sécurité NSX-T) que vous avez créé précédemment en tant que Source Address (Adresse source). N'ajoutez pas de groupes d'adresses statiques, de plages d'adresses IP ou de masques de réseau en tant qu'adresse source.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Dans l'onglet Destination, Panorama ne vous permet pas de définir une zone de destination, car vous avez défini le type de règle sur intrazone. Sélectionnez ensuite un groupe d'adresses dynamiques (groupe de sécurité NSX-T) que vous avez créé précédemment en tant que Destination Address (Adresse de destination). N'ajoutez pas de groupes d'adresses statiques, de plages d'adresses IP ou de masques de réseau en tant qu'adresse de destination.

STEP 7 | Cliquez sur **OK**.

STEP 8 | Répétez les étapes 1 à 7 pour chaque règle de politique dont vous avez besoin.

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

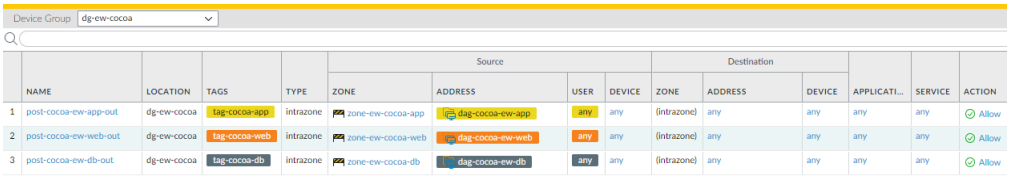
STEP 10 | Application des politiques de sécurité au pare-feu VM-Series sur NSX-T (Est-Ouest).

Utilisation de la post-règlementation pour définir les règles de redirection NSX-T

Créez des règles de politique de sécurité dans la post-réglementation pour définir les règles de redirection NSX-T.

STEP 1 | Créez des règles de politique de sécurité.

1. Dans Panorama, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Post Rules (Post-règles)**.
2. Vérifiez que vous configurez les règles de politique de sécurité dans un groupe d'appareils associé à une définition de service NSX-T.
3. Cliquez sur le nom d'une règle de politique de sécurité à modifier.
4. Définissez le Rule Type (Type de règle) sur **intrazone (Périphériques avec PAN-OS 6.1 ou version ultérieure)**.
5. Dans l'onglet Source, définissez la zone source sur la zone à partir du modèle associé à la définition de service. Sélectionnez ensuite un groupe d'adresses dynamique que vous avez créé précédemment en tant qu'adresse source. N'ajoutez pas de groupes d'adresses statiques, de plages d'adresses IP ou de masques de réseau en tant qu'adresse source.
6. Dans l'onglet Destination, Panorama ne vous permet pas de définir une zone de destination, car vous avez défini le type de règle sur intrazone. Sélectionnez ensuite un groupe d'adresses dynamiques que vous avez créé précédemment en tant qu'adresse de destination. N'ajoutez pas de groupes d'adresses statiques, de plages d'adresses IP ou de masques de réseau en tant qu'adresse de destination.
7. Cliquez sur **OK**.
8. Répétez les étapes 1 à 7 pour chaque règle de politique dont vous avez besoin.



STEP 2 | **Validez** vos modifications sur Panorama.

STEP 3 | Appliquez les règles de politique de sécurité au pare-feu VM-Series NSX-T EW SEC Centric.

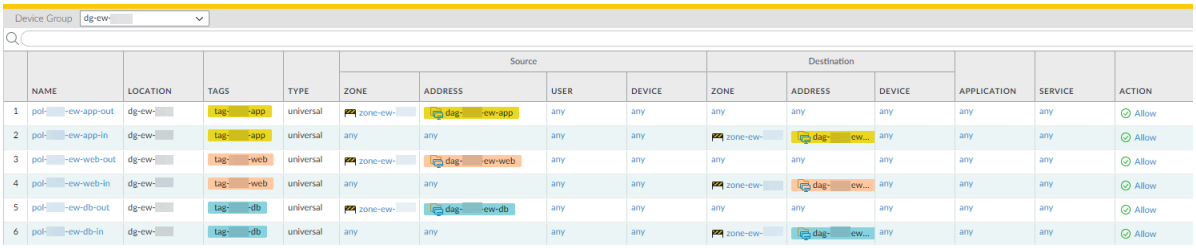
 ©2023 Palo Alto Networks, Inc.

Application des politiques de sécurité au pare-feu VM-Series sur NSX-T (Est-Ouest)

Maintenant que vous avez défini les règles de redirection, vous pouvez désormais utiliser Panorama pour administrer les politiques de manière centralisée sur les pare-feu VM-Series.

Pour gérer une politique centralisée, associez le groupe d'adresses dynamiques comme adresse source ou de destination à la politique de sécurité et appliquez-le aux pare-feu ; ces derniers peuvent récupérer de manière dynamique les adresses IP des machines virtuelles de chaque groupe de sécurité afin d'appliquer la conformité du trafic depuis ou vers les machines virtuelles du groupe spécifié.

STEP 1 | Créez des règles de politique de sécurité.



1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Prerules (Pré-règles)**.
2. Sélectionnez le **Device Group (Groupe d'appareils)** que vous avez créé pour gérer les pare-feu VM-Series sur NSX-T dans Création de piles de modèles et de groupes de périphériques sur Panorama.
3. Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** et une **Description** pour identifier la règle. Dans cet exemple, la règle de sécurité autorise tout le trafic entre les serveurs Web frontaux et les serveurs d'applications.
4. Sélectionnez la **Source Zone (Zone source)** et la **Destination Zone (Zone de destination)**. Le nom de la zone doit être le même dans les deux colonnes.
5. Sous **Source Address (Adresse source)** et **Destination Address (Adresse de destination)**, sélectionnez ou saisissez une adresse, un groupe d'adresses ou une région. Dans cet exemple, un groupe d'adresses est sélectionné. Il s'agit du groupe d'adresses dynamiques créé précédemment.
6. Sélectionnez l'**Application** à autoriser. Dans cet exemple, un **Application Group (Groupe d'applications)** est créé ; il s'agit d'un groupe statique d'applications spécifiques.
   1. Cliquez sur **Add (Ajouter)** et sélectionnez **New Application Group (Nouveau groupe d'applications)**.
   2. Cliquez sur **Add (Ajouter)** pour sélectionner l'application que vous souhaitez inclure dans le groupe.
   3. Cliquez sur **OK** pour créer le groupe d'applications.
7. Spécifiez l'action (**Allow (Autoriser)** ou **Deny (Refuser)**) pour le trafic, puis associez éventuellement les profils de sécurité par défaut pour l'antivirus, l'antispyware et la protection contre les vulnérabilités sous Profils.
8. Surveillance MV Répète les étapes ci-dessus pour créer les règles de politique pertinentes. Le plugiciel AWS sur Panorama.
9. Cliquez sur **Valider** et sélectionnez le type de validation **Panorama**. Cliquez sur **OK**.

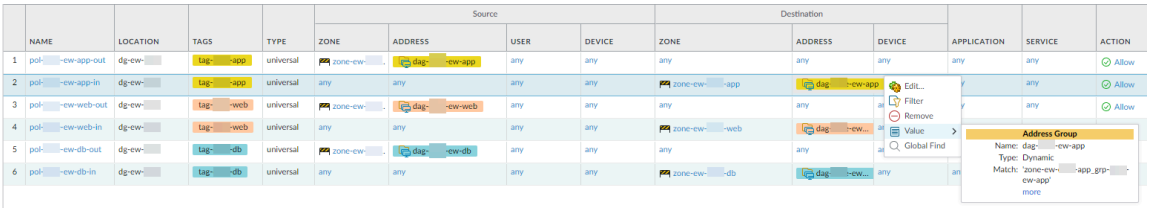
©2023 Palo Alto Networks, Inc.

STEP 2 | Appliquez les politiques aux pare-feu VM-Series pour NSX-T.

1. Cliquez sur **Commit (Valider)** et sélectionnez le type de validation **Device Groups (Groupes de périphériques)**.
2. Sélectionnez le groupe de périphériques, c'est-à-dire le groupe de périphériques NSX-T dans cet exemple, puis cliquez sur **OK**.
3. Vérifiez que la validation a réussi.

STEP 3 | Assurez-vous que les membres du groupe d'adresses dynamiques sont renseignés sur le pare-feu VM-Series.

1. À partir de Panorama, changez de contexte de périphérique pour lancer l'interface Web d'un pare-feu sur lequel vous avez appliqué des politiques.
2. Sur le pare-feu VM-Series, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et sélectionnez une règle.
3. Cliquez sur la flèche déroulante en regard du lien du groupe d'adresses et sélectionnez **Inspect (Inspecter)**. Vous pouvez également vérifier que les critères de correspondance sont corrects.



4. Cliquez sur le lien **more (Plus)** et vérifiez que la liste des adresses IP enregistrées s'affiche.

   La politique est appliquée à toutes les adresses IP qui appartiennent à ce groupe d'adresses et s'affichent ici.

STEP 4 | (Facultatif) Utilisez un modèle pour appliquer une configuration de périphérique et réseau de base, notamment à un serveur DNS, NTP, Syslog ou à une bannière de connexion.

Pour plus d'informations sur l'utilisation des modèles, reportez-vous au Guide de l'administrateur Panorama.

STEP 5 | Créez un profil de protection de zone et associez-le à une zone.

Un profil de protection de zone offre une protection contre les attaques par inondation et a la capacité de vous protéger contre le balayage de ports et les attaques par commutation de paquets. Il vous permet de sécuriser le trafic dans un niveau et entre les niveaux entre les machines virtuelles au sein de votre centre de données et le trafic provenant d'Internet qui est destiné aux machines virtuelles (charges de travail) dans votre centre de données.

1. Sélectionnez votre **Template (Modèle)**.
2. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)** pour ajouter et configurer un nouveau profil.
3. Sélectionnez **Network (Réseau)** > **Zones**, puis la zone par défaut répertoriée et le profil dans la liste déroulante **Zone Protection Profile (Profil de protection de zone)**.

©2023 Palo Alto Networks, Inc.

STEP 6 | Créez un profil de protection DoS (déni de service) et associez-le à la règle de Protection contre les attaques par déni de service.

1. Sélectionnez votre **Groupe de périphériques**.
2. Sélectionnez **Objects (Objet)** > **Security Profiles (Profils de sécurité)** > **DoS Protection (Protection contre les attaques par déni de service)** pour ajouter et configurer un nouveau profil.
   - Un profil classifié permet la création d'un seuil qui s'applique à une seule adresse IP source. Par exemple, vous pouvez configurer le nombre de sessions maximum pour une adresse IP correspondant à la politique, et puis bloquer l'adresse IP unique une fois que le seuil est atteint.
   - Un profil agrégé permet la création d'un nombre maximal de sessions pour tous les paquets qui sont conformes à la politique. Le seuil s'applique au nombre de nouvelles sessions pour toutes les adresses IP combinées. Une fois le seuil atteint, tout le trafic qui correspond à la politique est affecté.
3. Créez une nouvelle règle de politique de protection contre les attaques par déni de service dans **Policy (Politique)** > **DoS Protection (Protection contre les attaques par déni de service)**, puis associez-y le nouveau profil.

Création de critères d'adhésion à un Dynamic Address Group (groupe d'adresses dynamiques)

Dans NSX-T, vous pouvez configurer les critères d'adhésion pour vos machines virtuelles et votre ensemble d'adresses IP appartenant à un groupe de sécurité NSX-T (groupe d'adresses dynamiques) dans le plug-in Panorama pour NSX. Pour chaque groupe d'adresses dynamiques, vous devez spécifier une définition de service et définir jusqu'à cinq critères de correspondance et chaque critère comprend jusqu'à cinq règles de correspondance.



Vous créez ce critère d'adhésion sur le plug-in, puis vous le transférez vers NSX-T Manager. Cependant, cela n'applique pas les critères d'appartenance aux machines virtuelles invitées dans votre déploiement. Vous devez définir et appliquer des données d'appartenance, telles que des balises, à vos VM invitées dans NSX-T Manager.

Les règles selon lesquelles le plug-in Panorama pour NSX-T identifie et classe les VM se fondent sur deux types d'appartenance : VM ou ensemble IP. Les clés et opérateurs utilisables avec chaque type de membre sont répertoriés dans le tableau ci-dessous.

Type de membre	Clé	Opérateur
Ensemble IP	Étiquette	Est égal à
Machine virtuelle	• Étiquette • Nom • Nom du système d'exploitation • Nom de l'ordinateur	• Est égal à • Contient • Commence par • Se termine par • Non égaux (non applicable avec la clé Étiquette)

 ©2023 Palo Alto Networks, Inc.

*Les modifications de critères d'adhésion ne doivent être effectués que sur Panorama ; n'apportez pas de modifications sur NSX-T Manager. Si vous apportez des modifications sur NSX-T Manager, le plug-in Panorama pour VMware NSX affiche la définition de service comme désynchronisée. Vous devez cliquer sur le lien **Out-of-Sync (Désynchronisé)** pour voir la raison spécifique de l'état de désynchronisation. Si une modification des critères d'adhésion en est la cause, effectuez une synchronisation de configuration en cliquant sur **NSX-T Config-Sync (Sync Config NSX-T)**.*

STEP 1 | Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Membership Criteria (Critères d'appartenance)** > **Add (Ajouter)**.

Pour ajouter ou modifier des critères d'appartenance pour une définition de service, avec au moins un groupe d'adresses dynamiques, vous pouvez cliquer sur le nom de la définition de service au lieu de cliquer sur **Add (Ajouter)**.

STEP 2 | Dans **Name (Nom)**, sélectionnez une définition de service pour les critères d'adhésion. La définition de service sélectionnée doit avoir le type d'insertion Est_Ouest et être utilisée dans le cadre d'un déploiement centré sur la sécurité.

STEP 3 | Cliquez sur **Add (Ajouter)** pour spécifier un groupe d'adresses dynamique.

STEP 4 | Sélectionnez un **groupe d'adresses dynamiques** dans la liste déroulante. La liste déroulante répertorie les groupes d'adresses dynamiques associés à la définition de service spécifiée.

L'interface utilisateur du plug-in affiche les groupes d'adresses dynamiques et statiques configurés sur Panorama. Veillez à ne pas sélectionner accidentellement un groupe d'adresses statiques lors de la configuration des critères d'appartenance.

STEP 5 | Cliquez sur **Add (Ajouter)** pour définir les critères associés au groupe d'adresses dynamiques choisi.

STEP 6 | Saisissez un nom descriptif pour les **critères**.

STEP 7 | Cliquez sur **Add (Ajouter)** pour définir une règle.

STEP 8 | Définissez une règle. Vous pouvez créer jusqu'à cinq règles.

1. Saisissez un nom descriptif pour la règle.
2. Sélectionnez le **type de membre** : Virtual Machine ou ensemble d'adresses IP.
3. Sélectionnez la **clé** : étiquette, nom, nom du système d'exploitation, nom de l'ordinateur.
4. Sélectionnez l'**opérateur** : égal, contient, commence par, se termine par, différent de.
5. Entrez la **valeur**.

   Si la clé est définie sur Tag (Étiquette), la valeur est l'étiquette. L'interface utilisateur du plug-in ne répertorie pas les balises, vous devez donc utiliser la CLI Panorama (avec NSX-T Manager 3.0.0. et versions ultérieures).

   ```
   request plugins vmware_nsx nsx_t nsxt-tags service-definition <SD_name>
   ```

6. (Facultatif) Saisissez la **portée**. La portée est applicable uniquement avec la clé **Tag (Étiquette)**. La portée est une valeur facultative appliquée à une étiquette d'objet dans NSX-T. La portée est définie sur NSX-T Manager. Par exemple, si vous étiquetez des

 ©2023 Palo Alto Networks, Inc.

Virtual Machines en fonction du système d'exploitation, vous pouvez créer des étiquettes pour Windows, Linux et MacOS, puis définir la portée de chaque balise sur OS (Système d'exploitation).

Pour afficher les étiquettes et la portée, utilisez la CLI Panorama (avec NSX-T Manager 3.0.0 et versions ultérieures).

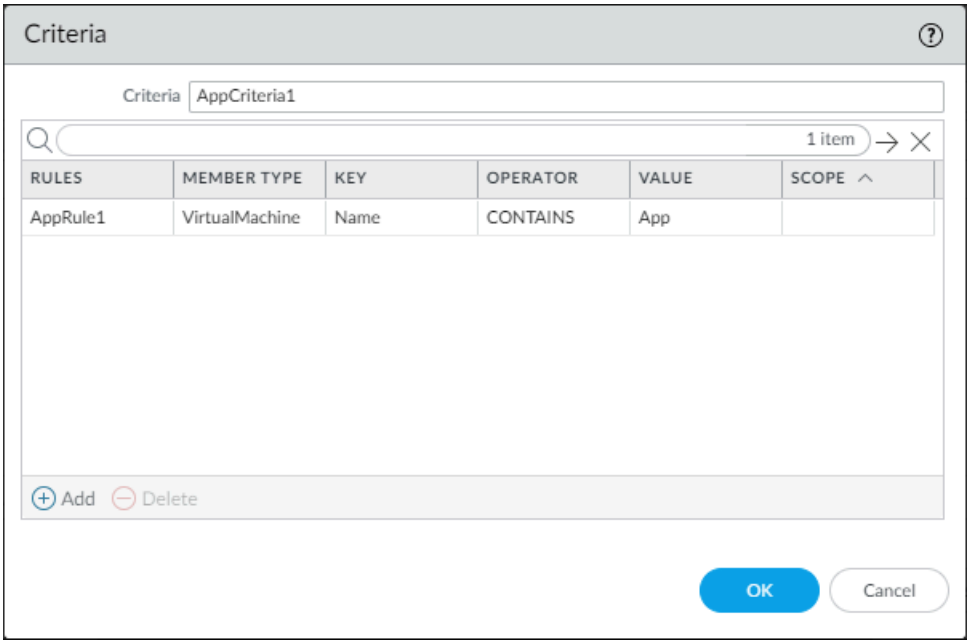
Exécutez la commande suivante pour afficher la liste des étiquettes.

```
request plugins vmware_nsx nsx_t nsxt-tags service-definition <SD_name>
```

Exécutez la commande suivante pour afficher la portée associée à l'étiquette spécifiée.

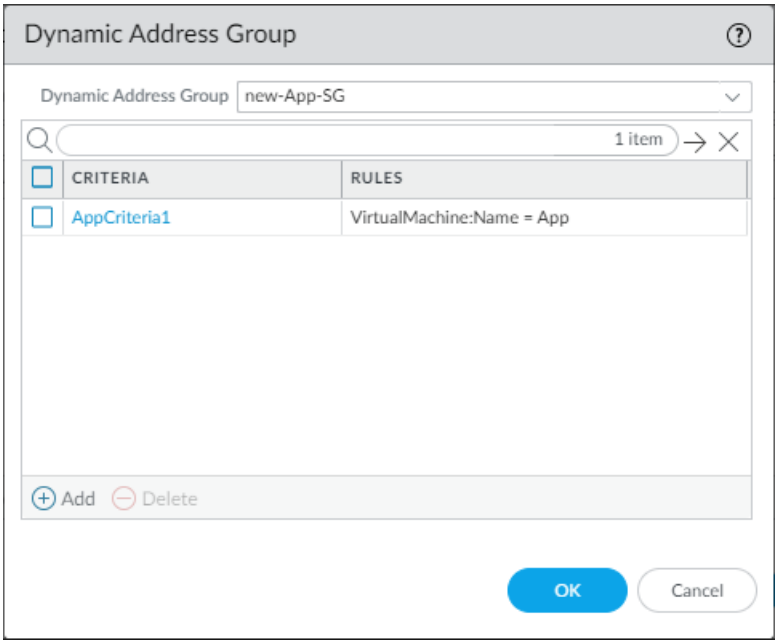
```
request plugins vmware_nsx nsx_t nsxt-scope tag <tag_value> service-definition <SD-name>
```

7. Cliquez sur **OK**.
8. (Facultatif) Cliquez sur **Add (Ajouter)** pour créer des règles supplémentaires (jusqu'à cinq au total).

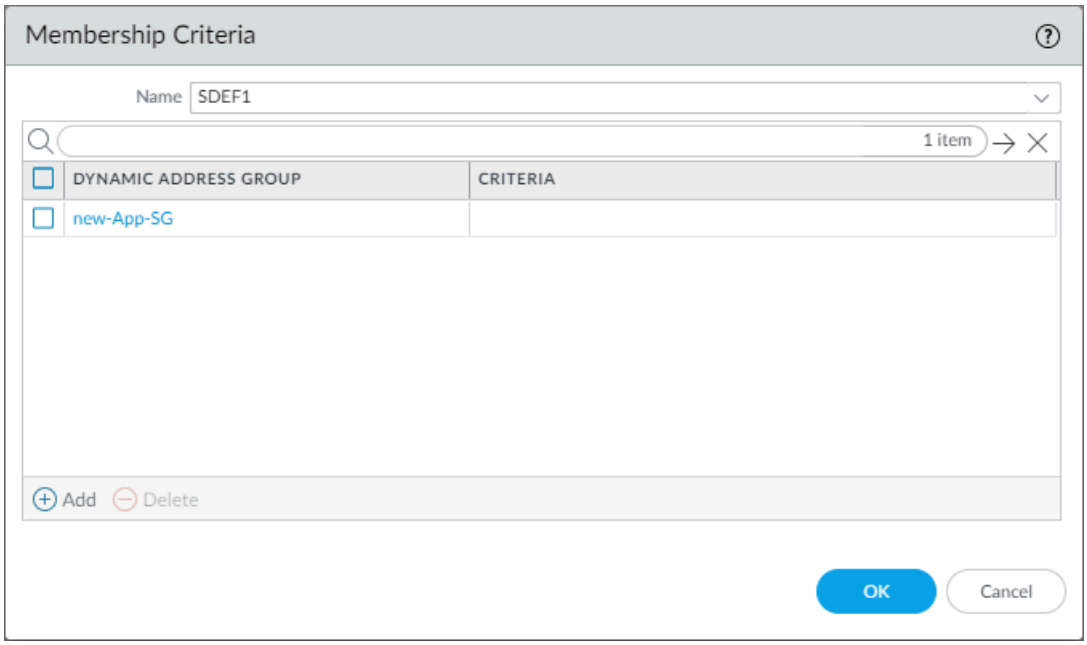


 ©2023 Palo Alto Networks, Inc.

STEP 9 | Dans la fenêtre Dynamic Address Group (Groupe d'adresses dynamiques), cliquez sur **OK** pour terminer ou sur **Add (Ajouter)** pour créer des critères (jusqu'à cinq au total) et des règles supplémentaires.



STEP 10 | Dans la fenêtre Membership Criteria (Critères d'appartenance), cliquez sur **OK** pour terminer ou sur **Add (Ajouter)** pour spécifier des groupes d'adresses dynamiques supplémentaires.



Génération d'une politique de redirection

La politique de redirection est utilisée par NSX-T pour définir la chaîne de service vers laquelle le trafic sera dirigé. Vous pouvez créer une politique de redirection manuellement ou générer automatiquement une politique de redirection.

 ©2023 Palo Alto Networks, Inc.

Lorsque vous générez automatiquement une politique de redirection, le plug-in Panorama pour VMware NSX-T crée une politique de redirection pour chaque gestionnaire de services spécifié et les définitions de service associées. Par défaut, TCP strict est désactivé et la politique d'échec est définie sur Autoriser. La politique générée automatiquement utilise le format de dénomination **auto_<service-def-name>_<zone-name>_steering_policy**.

Lorsque TCP Strict est activé, le pare-feu applique l'exigence de l'établissement de la connexion en trois étapes. Si le pare-feu capte le trafic en cours de session (par exemple, en raison d'un trafic asymétrique) et ne détecte pas d'établissement de connexion en trois étapes, la session est interrompue. Reportez-vous à la documentation de VMware NSX-T pour plus d'informations.

La politique d'échec définit ce qu'il advient du trafic si le pare-feu tombe en panne. Si vous sélectionnez Allow (Autoriser), le trafic continue vers sa destination. Si vous sélectionnez Block (Bloquer), le trafic est supprimé.

En outre, vous avez la possibilité de sélectionner tous vos gestionnaires de services au lieu de sélectionner des gestionnaires de services spécifiques. Il n'est pas recommandé de choisir **All (Tout)** si l'un de vos gestionnaires de services contient des définitions de service centrées sur les opérations. Le plug-in créera une politique de redirection pour chaque zone associée aux définitions de service centrées sur l'opération, puis la transmettra à NSX-T Manager. Si vous choisissez **All (Tout)**, vérifiez que le gestionnaire de services que vous sélectionnez lorsque vous générez automatiquement la politique de redirection inclut uniquement des définitions de service centrées sur la sécurité.

Si vous générez automatiquement une politique de redirection, vous devez également générer automatiquement des règles de direction. Et si vous créez manuellement une politique de redirection, vous devez également créer manuellement des règles de redirection.

- Génération automatique d'une politique de redirection
- Création manuelle d'une politique de redirection

*Les modifications de politique de redirection ne doivent être effectuées que sur Panorama ; n'apportez pas de modifications sur NSX-T Manager. Si vous apportez des modifications sur NSX-T Manager, le plug-in Panorama pour VMware NSX affiche la définition de service comme désynchronisée. Vous devez cliquer sur le lien **Out-of-Sync (Désynchronisé)** pour voir la raison spécifique de l'état de désynchronisation. Si une modification de politique de redirection en est la cause, effectuez une synchronisation de configuration en cliquant sur **NSX-T Config-Sync (Sync Config NSX-T)**.*

Génération automatique d'une politique de redirection

Utilisez la procédure suivante pour générer automatiquement une politique de redirection.

*Les étapes suivantes permettent de spécifier des gestionnaires de services au lieu de sélectionner **All (Tous)**.*

STEP 1 | Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspection réseau)** > **Policy (Politique)**.

STEP 2 | Cliquez sur **Auto Generate (Générer automatiquement)**.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Pour **Service Managers (Gestionnaires de services)**, choisissez **Select (Sélectionner)**.

*Si vous sélectionnez **All (Tous)** au lieu de sélectionner des gestionnaires de services spécifiques, le plug-in générera une politique de redirection pour chaque définition de service associée à chaque gestionnaire de service dans votre configuration. En outre, assurez-vous que le gestionnaire de services que vous avez sélectionné inclut des définitions de service centrées sur la sécurité.*

STEP 4 | Cliquez sur **Add (Ajouter)** pour sélectionner le gestionnaire de services.

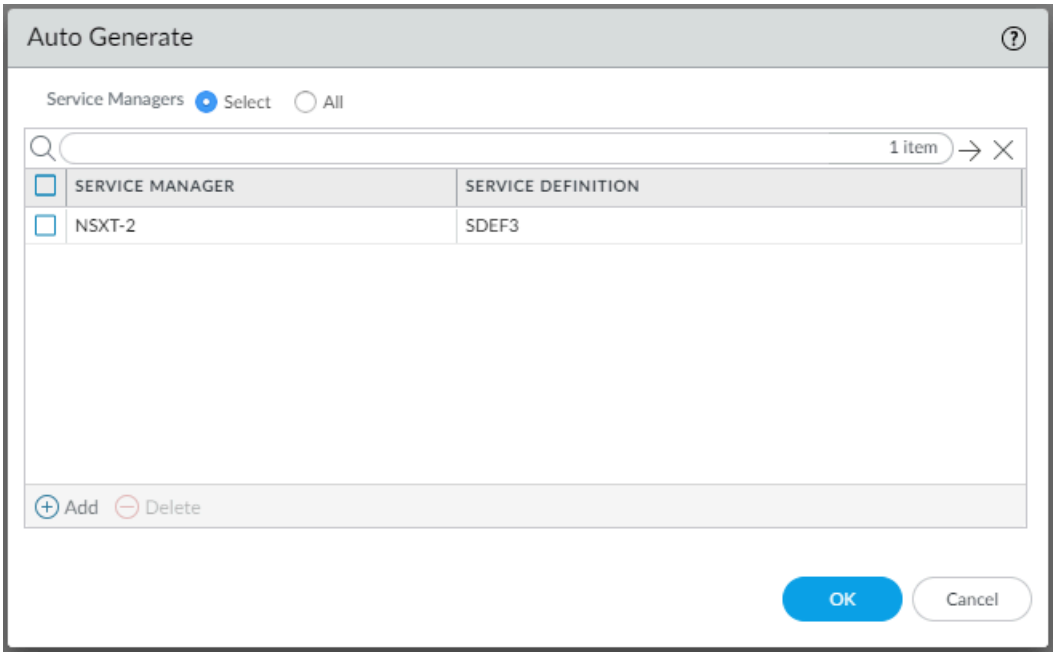
STEP 5 | Sélectionnez un **Service Manager (Gestionnaire de services)** dans la liste déroulante.

STEP 6 | Cliquez sur **Add (Ajouter)** pour sélectionner les définitions de services.

STEP 7 | Sélectionnez la définition de service dans la liste déroulante.

STEP 8 | Cliquez sur **OK**, puis cliquez à nouveau sur **OK**.

STEP 9 | **Validez** vos modifications sur Panorama.



Création manuelle d'une politique de redirection

Utilisez la procédure suivante pour créer manuellement une politique de redirection.

STEP 1 | Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspection réseau)** > **Policy (Politique)**.

STEP 2 | Cliquez sur **Add (Ajouter)**.

STEP 3 | Entrez un **Name (Nom)** descriptif pour votre politique de redirection.

Le nom de la politique de redirection ne peut pas inclure d'espaces.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Sélectionnez une **Service Definition (Définition de service)** dans la liste déroulante.

STEP 5 | Sélectionnez une **Service Chain (Chaîne de service)** dans la liste déroulante.

STEP 6 | (Facultatif) Activez **TCP Strict**. Cette option est désactivée par défaut.

STEP 7 | Choisissez la **Failure Policy (Politique d'échec)** : **Allow (Autoriser)** ou **Block (Bloquer)**. Allow (Autoriser) est le réglage par défaut.

STEP 8 | Cliquez sur **OK**.

STEP 9 | **Validez** vos modifications sur Panorama.



Génération de règles de redirection

Les règles de redirection sont définies dans la politique de redirection. Une règle définit la source et la destination du trafic, les services d'introspection, les objets NSX-T auxquels la règle s'applique et la politique de redirection du trafic. Vous pouvez créer des règles de redirection manuellement ou générer des règles de redirection automatiquement.

Vous devez générer ou créer une politique de redirection avant de générer ou de créer des règles de redirection.

Pour générer automatiquement une règle de redirection basée sur une règle de sécurité créée sur Panorama, la règle de sécurité doit répondre aux critères suivants :

- appartient à un groupe de périphériques parent ou enfant enregistré auprès d'un gestionnaire de services NSX-T ;
- est une politique intra-zone et n'inclut qu'une seule zone ;
- n'inclut pas de groupe d'adresses statiques, de plage d'adresses IP ou de masque de réseau configuré pour la règle.

Les règles de redirection générées automatiquement utilisent le format de dénomination **auto_<device-group-name>_<device-group-rule-name>**.

Par défaut, les règles de redirection générées automatiquement sont configurées sans qu'un service NSX ne soit spécifié. En outre, le sens du trafic NSX est défini sur in-out (entrée-sortie), la journalisation est désactivée, le protocole IP est ipv4-ipv6 et l'action est définie sur redirect (rediriger). Après avoir généré automatiquement des règles, vous pouvez mettre à jour la redirection pour modifier les valeurs par défaut.

 ©2023 Palo Alto Networks, Inc.

En outre, vous avez la possibilité de sélectionner tous vos gestionnaires de services au lieu de sélectionner des gestionnaires de services spécifiques. Choisir **All (Tout)** n'est pas recommandé.

Si vous générez automatiquement une politique de redirection, vous devez également générer automatiquement des règles de direction. Et si vous créez manuellement une politique de redirection, vous devez également créer manuellement des règles de redirection.

- Génération automatique de règles de redirection
- Création manuelle de règles de redirection

*Les modifications de règles de redirection ne doivent être effectuées que sur Panorama ; n'apportez pas de modifications sur NSX-T Manager. Si vous apportez des modifications sur NSX-T Manager, le plug-in Panorama pour VMware NSX affiche la définition de service comme désynchronisée. Vous devez cliquer sur le lien **Out-of-Sync (Désynchronisé)** pour voir la raison spécifique de l'état de désynchronisation. Si une modification de règles de redirection en est la cause, effectuez une synchronisation de configuration en cliquant sur **NSX-T Config-Sync (Sync Config NSX-T)**.*

Génération automatique de règles de redirection

Utilisez la procédure suivante pour générer automatiquement des règles de redirection.

Lorsque vous générez automatiquement une règle de redirection, l'endroit où la règle est appliquée (pare-feu distribué NSX-T ou groupe de sécurité) dépend de la source et de la destination que vous avez spécifiées lors de la configuration de la règle de sécurité. Si vous avez sélectionné **Any (N'importe laquelle)** pour la source ou la destination, NSX-T Manager applique la règle de redirection au pare-feu distribué. Si vous sélectionnez un groupe d'adresses dynamiques pour la source et la destination, la redirection est appliquée aux VM invitées dans ces groupes de sécurité.

Si vous apportez des modifications à la configuration d'un groupe de périphériques qui fait également partie de la configuration de la règle de redirection, par exemple les groupes d'adresses source et de destination qui correspondent au paramètre Applied To (Appliqué à) dans une règle de redirection, vous devez générer automatiquement la règle de redirection pour que les modifications prennent effet.

*Les étapes suivantes permettent de spécifier des gestionnaires de services au lieu de sélectionner **All (Tous)**.*

STEP 1 | Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspection réseau)** > **Rule (Règle)**.

STEP 2 | Cliquez sur **Auto Generate (Générer automatiquement)**.

STEP 3 | Sélectionnez le type de règles de sécurité dans la liste déroulante : **All (Tous)**, **Pre Rulebase (Base de règles « avant »)** uniquement ou **Post Rulebase (Base de règles « après »)**

 ©2023 Palo Alto Networks, Inc.

uniquement. Les règles de sécurité sont extraites des définitions de service spécifiées dans les étapes suivantes.

Si vous régénérez les règles de redirection, toutes les règles actuelles sont supprimées et de nouvelles règles sont créées en fonction de la base de règles sélectionnée. Si vous avez créé à l'origine des règles de redirection à l'aide de la base de règles « avant », puis régénérez les règles de redirection à l'aide de la base de règles « après », seules les règles de redirection de la base de règles « après » sont conservées.

STEP 4 | Pour **Type**, choisissez **Select (Sélectionner)**.

STEP 5 | Cliquez sur **Add (Ajouter)** pour spécifier le(s) **Service Manager(s) (Gestionnaire[s] de services)** et la ou les **Service Definition(s) (Définition[s] de service)**.

STEP 6 | Sélectionnez un **Service Manager (Gestionnaire de services)** dans la liste déroulante.

STEP 7 | Cliquez sur **Add (Ajouter)** pour sélectionner la ou les définition(s) de service(s).

STEP 8 | Cliquez sur **OK**.

STEP 9 | Cliquez sur **OK** pour terminer ou sur **Add Ajouter)** pour spécifier des gestionnaires de services et des définitions de services supplémentaires.

STEP 10 | (Facultatif) Cliquez sur une règle générée automatiquement pour modifier les options par défaut suivantes.

Si vous régénérez les règles de redirection, toutes les modifications que vous avez apportées à une règle de redirection précédemment générée seront remplacées.

- Activez la **journalisation** NSX-T.
- Cliquez sur **Add (Ajouter)** pour spécifier les **NSX Services (Services NSX)**, tels que Active Directory Server, HTTPS, DNS, etc.
- **Désactivez** la règle. Si vous désactivez une règle de redirection, mais si la règle de sécurité correspondante est activée (**Device Group [Groupe d'appareils]** > **Policies [Politiques]** > **Security [Sécurité]**), la règle de redirection sera également activée.
- **Applied to (Appliqué à)** vous permet de modifier l'emplacement d'application de la règle de redirection :**DFW** ou **Security Group (Groupe de sécurité)**.

STEP 11 | Nettoyez les règles de redirection indésirables ou incorrectes.

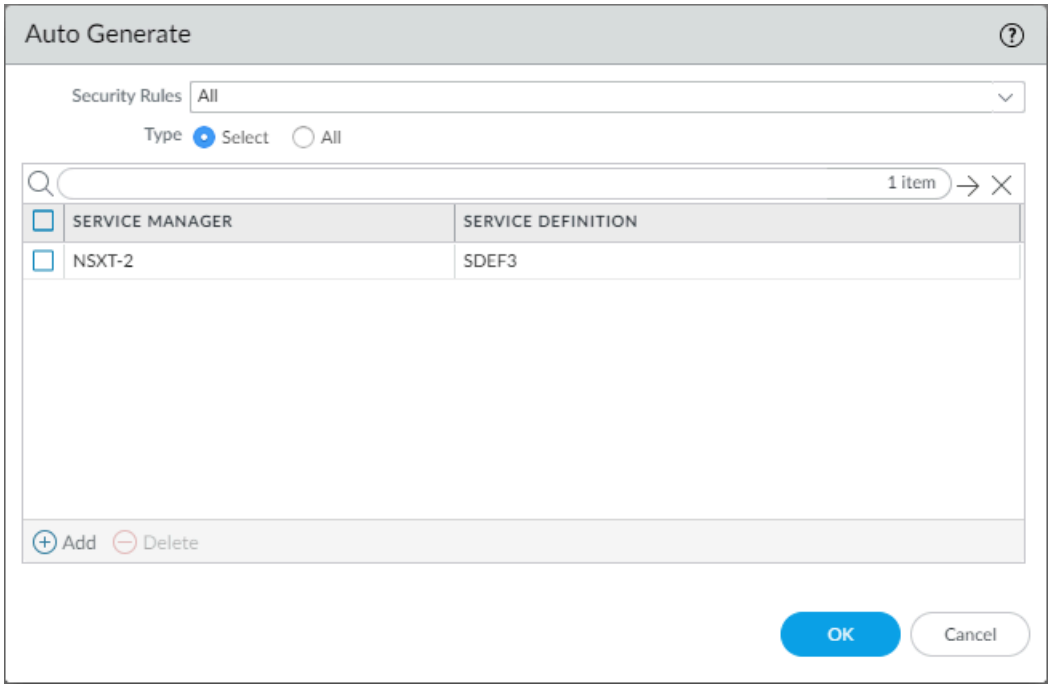
Si, par exemple, votre groupe d'appareils contient des règles de sécurité dans la même base de règles que vos règles de redirection NSX-T, le plug-in génère des règles de sécurité basées sur ces règles de sécurité non NSX-T. Étant donné que ces règles ne font pas référence à un groupe d'adresses dynamiques NSX-T, la source et la destination de ces règles seront définies sur Any (N'importe laquelle) Any (N'importe laquelle) dans NSX-T Manager. Cette condition peut avoir un impact sur la façon dont NSX-T Manager dirige le trafic. Pour éviter cela, vous devez supprimer manuellement les règles de redirection incorrectes.

1. Sélectionnez les règles de redirection incorrectes.
2. Cliquez sur **Delete (Supprimer)**.

 ©2023 Palo Alto Networks, Inc.

3. Cliquez sur **Yes (Oui)** pour confirmer la suppression.

STEP 12 | **Validez** votre configuration pour la transmettre à NSX-T Manager.



Création manuelle de règles de redirection

Utilisez la procédure suivante pour créer manuellement des règles de redirection.

STEP 1 | Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspection réseau)** > **Rule (Règle)**.

STEP 2 | Cliquez sur **Add (Ajouter)**.

STEP 3 | Entrez un **Name (Nom)** descriptif pour la règle de redirection.

Le nom de la règle de redirection ne peut pas inclure d'espaces.

STEP 4 | Sélectionnez une **Steering Policy (Politique de redirection)** dans la liste déroulante.

STEP 5 | Sélectionnez un **Device Group (Groupe d'appareils)** dans la liste déroulante.

STEP 6 | Sélectionnez une **Security Rule (Règle de sécurité)** dans la liste déroulante.

La liste déroulante Security Rule (Règle de sécurité) affiche les règles de toutes les règles de sécurité sur tous les groupes d'appareils de la définition de service. Assurez-vous de sélectionner la règle de sécurité appropriée.

STEP 7 | Spécifiez l'**Action** : **Redirect (Rediriger)** ou **Do Not Redirect (Ne pas rediriger)**.

STEP 8 | (Facultatif) Activez la **journalisation** NSX-T.

©2023 Palo Alto Networks, Inc.

STEP 9 | Spécifiez le **protocole IP** : **ipv4-ipv6**, **ipv4** ou **ipv6**.

STEP 10 | Spécifiez la **direction du trafic NSX** : **in-out (entrée-sortie)**, **in (entrée)** ou **out (sortie)**.

STEP 11 | (Facultatif) Cliquez sur Add (Ajouter) pour spécifier les **NSX Services (Services NSX)**, tels que Active Directory Server, HTTPS, DNS, etc.

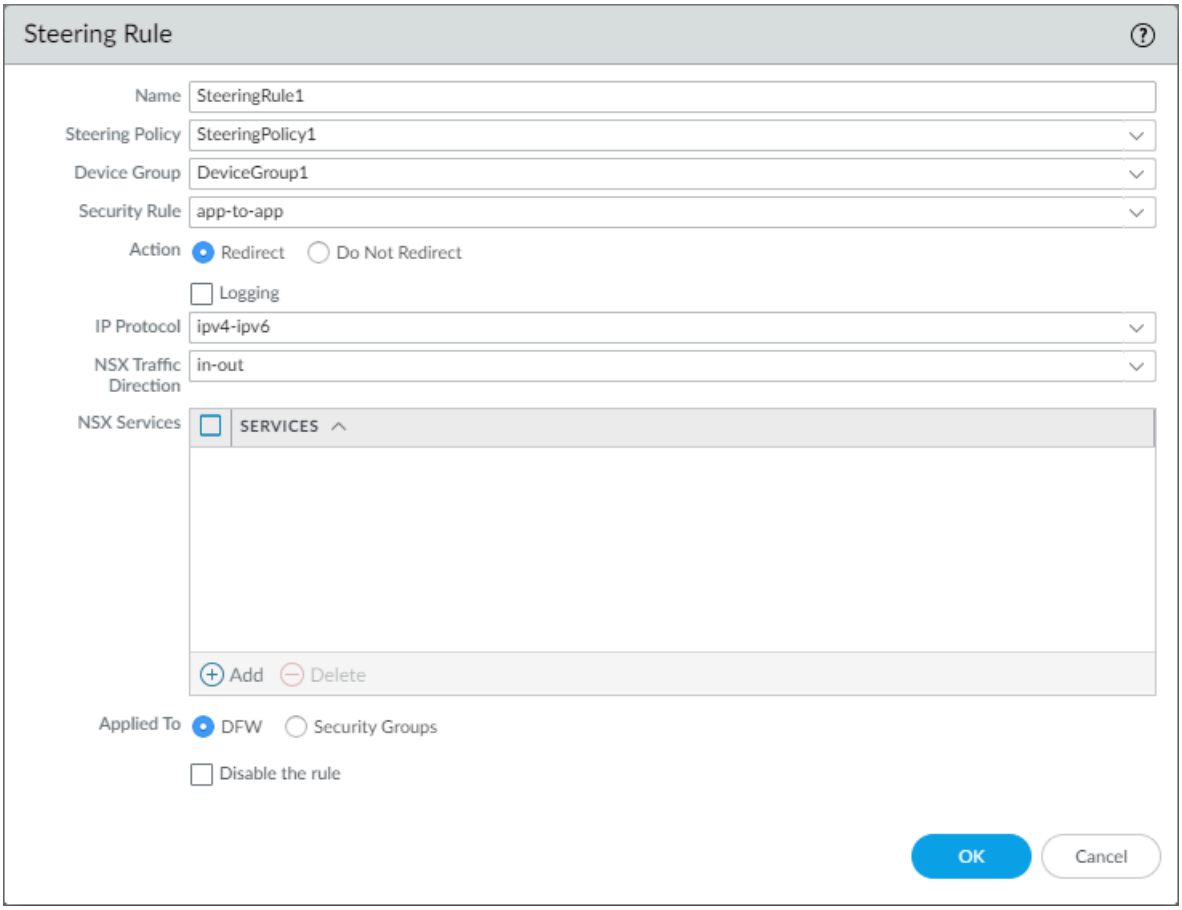
Les services ALG suivants ne sont pas pris en charge : FTP, TFTP, ORACLE_TNS, SUN_RPC_TCP, SUN_RPC_UDP, MS_RPC_TCP, MS_RPC_UDP, NBNS_BROADCAST, NBDG_BROADCAST.

STEP 12 | **Applied To (Appliqué à)** : **DFW** ou **Security Groups (Groupes de sécurité)**. Vous pouvez sélectionner un ou plusieurs groupes de sécurité. Les groupes de sécurité sont créés à partir de groupes d'adresses dynamiques configurés sur Panorama. Les noms des groupes de sécurité sont mis en forme comme suit **<servicedefinition>_<dynamic-address-group>**. Si vous sélectionnez DFW, la règle de redirection s'applique à toutes les VM invitées, quelle que soit leur appartenance de sécurité.

STEP 13 | (Facultatif) Désactivez la règle.

STEP 14 | Cliquez sur **OK**.

STEP 15 | **Validez** votre configuration pour la transmettre à NSX-T Manager.



 ©2023 Palo Alto Networks, Inc.

Suppression d'une définition de service de Panorama

Effectuez la procédure suivante pour supprimer une définition de service de votre configuration NSX-T sur Panorama.

STEP 1 | Connectez-vous à Panorama.

STEP 2 | Pour un déploiement centré sur la sécurité, supprimez les règles de redirection et la politique de redirection associées à la définition de service à supprimer.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspection réseau)** > **Rules (Règles)**.
2. Sélectionnez les règles de redirection à supprimer.
3. Cliquez sur **Delete (Supprimer)**.
4. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspection réseau)** > **Policy (Politique)**.
5. Sélectionnez la politique de redirection à supprimer.
6. Cliquez sur **Delete (Supprimer)**.

STEP 3 | **Commit (Validez)** vos modifications.

STEP 4 | Supprimez les pare-feu VM-Series déployés dans NSX-T qui sont associés à la définition de service à supprimer.

STEP 5 | Supprimez les critères d'appartenance associés à la définition de service.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Membership Criteria (Critères d'appartenance)**.
2. Sélectionnez les critères à supprimer.
3. Cliquez sur **Delete (Supprimer)**.

STEP 6 | Dissociez la définition de service du gestionnaire de services auquel elle est associée.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Service Managers (Gestionnaires de service)**.
2. Cliquez sur le nom du gestionnaire de service.
3. Sélectionnez la définition de service.
4. Cliquez sur **Delete (Supprimer)**.
5. Cliquez sur **OK**.

STEP 7 | **Validez** vos modifications sur Panorama.

Migration d'une utilisation de VM-Series sur NSX-T vers un déploiement centré sur la sécurité

Utilisez la procédure suivante pour migrer votre déploiement NSX-T centré sur les opérations vers un déploiement NSX-T centré sur la sécurité.

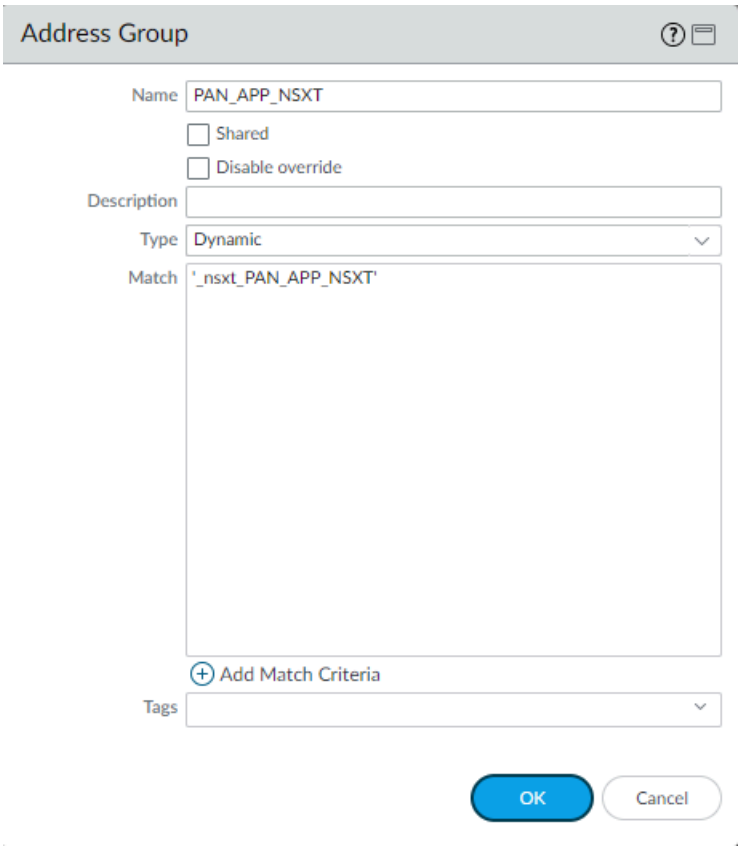
STEP 1 | Connectez-vous à Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Modifiez les critères de correspondance de vos groupes d'adresses dynamiques pour suivre le format requis pour un déploiement centré sur la sécurité.

1. Sélectionnez **Objects (Objets)** > **Address Groups (Groupes d'adresses)**.
2. Vérifiez que vous configurez les groupes d'adresses dynamiques dans un groupe d'appareils associé à une définition de service NSX-T.
3. Cliquez sur le nom d'un groupe d'adresses dynamiques NSX-T créé précédemment.
4. Modifiez les critères de correspondance.

   Pour que le groupe d'adresses dynamiques devienne un groupe de sécurité dans NSX-T Manager, la chaîne de critères de correspondance doit être placée entre guillemets simples avec le préfixe _nsxt_ suivi du nom exact du groupe d'adresses. Par exemple, ***'_nsxt_PAN_APP_NSX'***.
5. Répétez ce processus pour chaque groupe de sécurité dont vous avez besoin.



 ©2023 Palo Alto Networks, Inc.

STEP 3 | Définissez les règles de sécurité comme des règles de pilotage NSX-T sur intra-zone.

1. Dans Panorama, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Pré-règles)**.
2. Vérifiez que vous configurez les politiques de sécurité dans un groupe d'appareils associé à une définition de service NSX-T.
3. Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** et une **Description** pour votre règle de politique de sécurité.
4. Définissez le Rule Type (Type de règle) sur **intrazone (Périphériques avec PAN-OS 6.1 ou version ultérieure)**.
5. Dans l'onglet Source, définissez la zone source sur la zone à partir du modèle associé à la définition de service. Sélectionnez ensuite un groupe d'adresses dynamique que vous avez créé précédemment en tant qu'adresse source. N'ajoutez pas de groupes d'adresses statiques, de plages d'adresses IP ou de masques de réseau en tant qu'adresse source.
6. Dans l'onglet Destination, Panorama ne vous permet pas de définir une zone de destination, car vous avez défini le type de règle sur intrazone. Sélectionnez ensuite un groupe d'adresses dynamiques que vous avez créé précédemment en tant qu'adresse de destination. N'ajoutez pas de groupes d'adresses statiques, de plages d'adresses IP ou de masques de réseau en tant qu'adresse de destination.
7. Cliquez sur **OK**.
8. Répétez les étapes 1 à 7 pour chaque règle de politique dont vous avez besoin.
9. **Commit (Validez)** vos modifications.

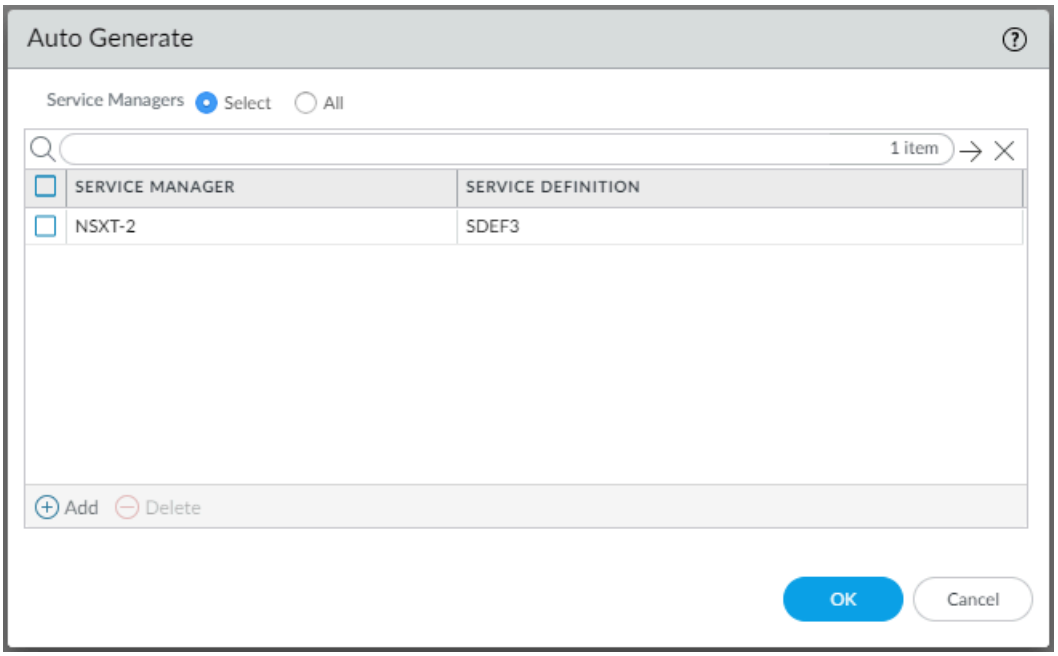
©2023 Palo Alto Networks, Inc.

STEP 4 | Générez automatiquement une nouvelle politique de redirection.

Les étapes suivantes permettent de spécifier des gestionnaires de services au lieu de sélectionner **All (Tous)**.

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspection réseau)** > **Policy (Politique)**.
2. Cliquez sur **Auto Generate (Générer automatiquement)**.
3. Pour **Service Managers (Gestionnaires de services)**, choisissez **Select (Sélectionner)**.

   *Si vous sélectionnez **All (Tous)** au lieu de sélectionner des gestionnaires de services spécifiques, le plug-in générera une politique de redirection pour chaque définition de service associée à chaque gestionnaire de service dans votre configuration.*
4. Cliquez sur **Add (Ajouter)** pour sélectionner le gestionnaire de services.
5. Sélectionnez un **Service Manager (Gestionnaire de services)** dans la liste déroulante.
6. Cliquez sur **Add (Ajouter)** pour sélectionner les définitions de services.
7. Sélectionnez la définition de service dans la liste déroulante.
8. Cliquez sur **OK**, puis cliquez à nouveau sur **OK**.



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

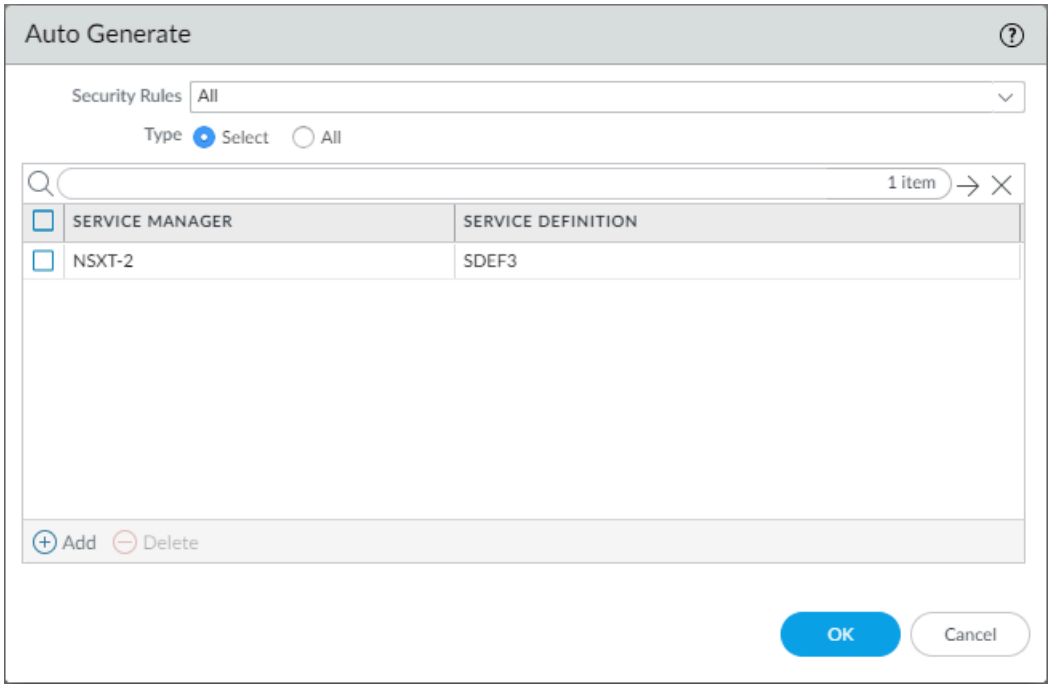
©2023 Palo Alto Networks, Inc.

STEP 5 | Générez automatiquement de nouvelles règles de redirection.

Si vous générez automatiquement une politique de redirection, vous devez également générer automatiquement des règles de direction. Et si vous créez manuellement une politique de redirection, vous devez également créer manuellement des règles de redirection.

*Les étapes suivantes permettent de spécifier des gestionnaires de services au lieu de sélectionner **All (Tous)**.*

1. Sélectionnez **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspection réseau)** > **Rule (Règle)**.
2. Cliquez sur **Auto Generate (Générer automatiquement)**.
3. Sélectionnez le type de règles de sécurité dans la liste déroulante : **All (Tous)**, **Pre Rulebase (Base de règles « avant »)** uniquement ou **Post Rulebase (Base de règles « après »)** uniquement. Les règles de sécurité sont extraites des définitions de service spécifiées dans les étapes suivantes.
4. Pour **Type**, choisissez **Select (Sélectionner)**.
5. Cliquez sur Add (Ajouter) pour spécifier le(s) **Service Manager(s) (Gestionnaire[s] de services)** et la ou les **Service Definition(s) (Définition[s] de service)**.
6. Sélectionnez un **Service Manager (Gestionnaire de services)** dans la liste déroulante.
7. Cliquez sur **Add (Ajouter)** pour sélectionner la ou les définition(s) de service(s).
8. Cliquez sur **OK**.
9. Cliquez sur **OK** pour terminer ou sur **Add Ajouter)** pour spécifier des gestionnaires de services et des définitions de services supplémentaires.
10. (Facultatif) Cliquez sur une règle générée automatiquement pour modifier les options par défaut.



STEP 6 | Création de critères d'adhésion à un Dynamic Address Group (groupe d'adresses dynamiques).

©2023 Palo Alto Networks, Inc.

STEP 7 | **Validez** vos modifications sur Panorama.

STEP 8 | Supprimez les règles de redirection centrées sur les opérations de NSX-T Manager.

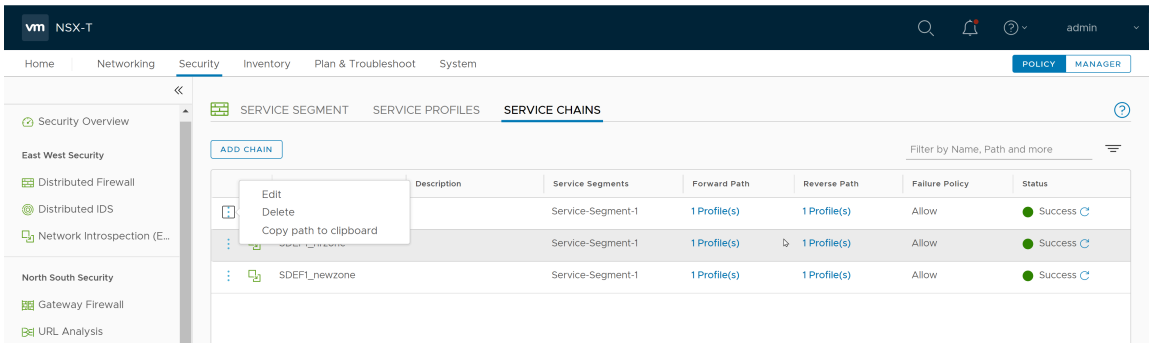
1. Connectez-vous à NSX-T Manager.
2. Sélectionnez **Security (Sécurité)** > **Network Introspection (E-W) (Introspection réseau [E-O])** > **Rules (Règles)**.
3. Sélectionnez chaque règle de redirection centrée sur les opérations.
4. Cliquez sur **Delete (Supprimer)**.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Supprimez la chaîne de services centrée sur les opérations de NSX-T Manager.

1. Connectez-vous à NSX-T Manager.
2. Sélectionnez **Security (Sécurité)** > **Network Introspection Settings (Paramètres d'introspection réseau)** > **Service Chains (Chaînes de service)**.
3. Cliquez sur les ellipses verticales.
4. Cliquez sur **Delete (Supprimer)**.

©2023 Palo Alto Networks, Inc.



Extension de la politique de sécurité du NSX-V au NSX-T

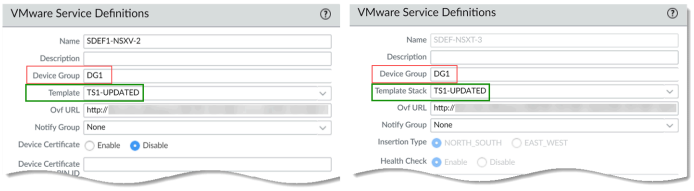
Si vous passez d'un déploiement NSX-V à un déploiement NSX-T ou si vous combinez un déploiement NSX-T avec un déploiement NSX-V, vous pouvez étendre votre politique de sécurité existante du NSX-V au NSX-T sans avoir à recréer les règles de la politique. Pour ce faire, vous

©2023 Palo Alto Networks, Inc.

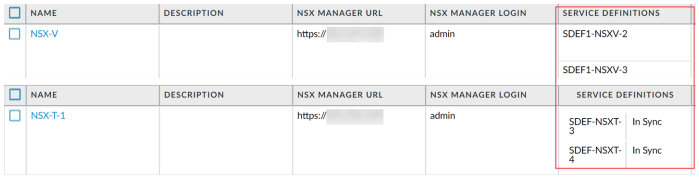
pouvez exploiter vos groupes d'appareils existants et les partager entre les définitions de service NSX-V et NSX-T. Après avoir migré votre politique vers le NSX-T, vous pouvez continuer à utiliser VM-Series pour le NSX-V ou supprimer votre déploiement NSX-V.

STEP 1 | Installation du plug-in Panorama pour VMware NSX 3.2.0 ou version ultérieure. Consultez les notes de version du plugin Panorama pour VMware NSX 3.2.0 avant la mise à niveau.

STEP 2 | Configurez une définition de service NSX-T pour chaque définition de service NSX-V dans votre déploiement. Ne créez pas de nouveaux groupes d'appareils, mais utilisez plutôt vos groupes d'appareils NSX-V existants. L'utilisation des groupes d'appareils existants vous permet d'appliquer les mêmes règles de sécurité que celles utilisées sur NSX-V aux pare-feu VM-Series déployés sur NSX-T. Si votre politique fait référence à une zone particulière, ajoutez la même pile de modèles de votre définition de service NSX-V à votre définition de service NSX-T. En outre, si votre groupe d'appareils référence un modèle particulier, assurez-vous de sélectionner la pile de modèles qui inclut le modèle référencé dans le groupe d'appareils.



STEP 3 | Configurez un gestionnaire de service NSX-T et associez les définitions de service NSX-T au gestionnaire de service.



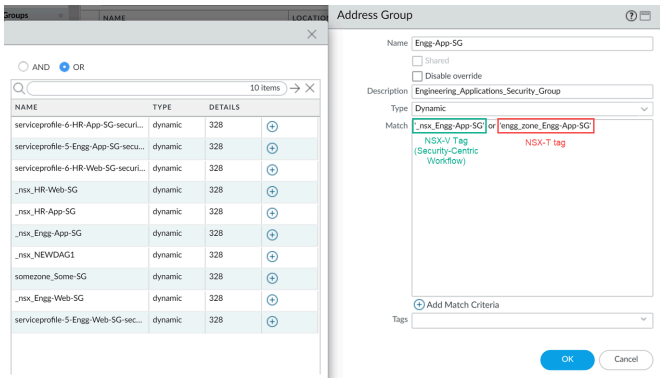
STEP 4 | Préparez votre environnement NSX-T et déployez le pare-feu VM-Series. Vous devez créer vos groupes de sécurité, vos chaînes de services et votre politique de redirection du trafic avant de lancer le pare-feu VM-Series.

- Déploiement du pare-feu VM-Series sur NSX-T (Nord-Sud)
- Déploiement du VM-Series à l'aide du flux de travail centré sur les opérations

©2023 Palo Alto Networks, Inc.

STEP 5 | Ajoutez les étiquettes NSX-T à vos groupes d'adresses dynamiques existants.

1. Sélectionnez **Panorama** > **Objects (Objets)** > **Address Groups (Groupes d'adresses)**.
2. Cliquez sur le nom d'un groupe d'adresses dynamiques NSX-V existant.
3. Cliquez sur **Add Match Criteria (Ajouter des critères de correspondance)** pour afficher les étiquettes NSX-V et NSX-T.
4. Ajoutez l'étiquette NSX-T aux groupes d'adresses dynamiques. Veillez à utiliser l'opérateur **OR (OU)** entre les étiquettes.
5. Lorsque vous avez ajouté toutes les étiquettes nécessaires, cliquez sur **OK**.
6. **Commit (Validez)** vos modifications.



STEP 6 | Une fois que les charges de travail de votre VM ont migré avec succès du NSX-V au NSX-T, vous pouvez supprimer les étiquettes NSX-V de vos groupes d'adresses dynamiques si vous prévoyez de ne plus utiliser le NSX-V. Toutes les étiquettes NSX-V et les adresses IP correspondantes sont désenregistrées une fois que l'ensemble de la configuration liée au NSX-V est retiré du plugin Panorama pour NSX et que la configuration du pare-feu de VM-Series est retirée du gestionnaire NSX-V.

Utilisation de la migration sur place pour déplacer votre VM-Series du NSX-V au NSX-T

Suivez la procédure suivante pour migrer la configuration de votre pare-feu VM-Series du NSX-V au NSX-T. En migrant votre configuration, vous pouvez réutiliser les politiques et groupes d'adresses dynamiques déjà configurés sur Panorama. Cette procédure se réfère aux informations et aux processus publiés dans la documentation VMware ainsi qu'aux étapes spécifiques à PAN.

Cette procédure ne prend en charge que les déploiements NSX-V centrés sur les opérations. Un déploiement signifie que vos règles de politique pour rediriger le trafic vers le pare-feu VM-Series ont été créées dans NSX-V Manager, et non dans Panorama.

Cette procédure nécessite NSX-T Manager 3.1.0 ou une version ultérieure.

Il est recommandé de prévoir une interruption de la sécurité pendant la réalisation de cette migration.

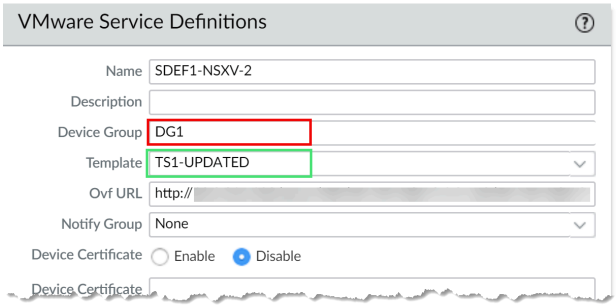
STEP 1 | Préparez vos environnements NSX-V et NSX-T pour la migration en suivant les étapes décrites par VMware.

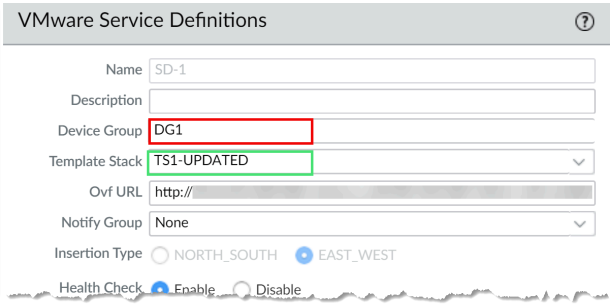
 ©2023 Palo Alto Networks, Inc.

STEP 2 | Installation du plug-in Panorama pour VMware NSX 3.2.0 ou version ultérieure. Consultez les notes de version du plugin Panorama pour VMware NSX 3.2.0 avant la mise à niveau.

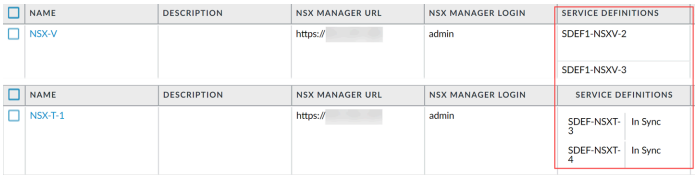
STEP 3 | Autorisation de la communication entre NSX-T Manager et Panorama.

STEP 4 | Configurez une définition de service NSX-T pour chaque définition de service NSX-V dans votre déploiement. **Ne créez pas de nouveaux groupes d'appareils**, mais utilisez plutôt vos groupes d'appareils NSX-V existants. L'utilisation des groupes d'appareils existants vous permet d'appliquer les mêmes règles de sécurité que celles utilisées sur NSX-V aux pare-feu VM-Series déployés sur NSX-T. Si votre politique fait référence à une zone particulière, ajoutez la même pile de modèles de votre définition de service NSX-V à votre définition de service NSX-T. En outre, si votre groupe d'appareils référence un modèle particulier, assurez-vous de sélectionner la pile de modèles qui inclut le modèle référencé dans le groupe d'appareils.





STEP 5 | Configurez un gestionnaire de service NSX-T et associez les définitions de service NSX-T au gestionnaire de service.



STEP 6 | Vérifiez que votre configuration NSX-T est présente dans NSX-T Manager.

1. Connectez-vous à NSX-T Manager.
2. Sélectionnez **System (Système)** > **Service Deployments (Déploiements de services)** > **Catalog (Catalogue)**.
3. Vérifiez que votre définition de service NSX-T figure est répertoriée.
4. Sélectionnez **Security (Sécurité)** > **Network Introspection Settings (Paramètres d'introspection réseau)** > **Service Profiles (Profils de service)**.
5. Vérifiez que vos zones associées à votre modèle NSX-T sont répertoriées.

STEP 7 | Si vous ne l'avez pas encore fait, ajoutez un gestionnaire de calcul dans NSX-T Manager. Après avoir vérifié que l'état d'enregistrement et l'état de connexion sont actifs, continuez ci-dessous.

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Importez la configuration NSX-V dans NSX-T.

STEP 9 | Désinstallez l'instance de service de NSX-V.



Cette étape entraînera une perturbation du trafic.

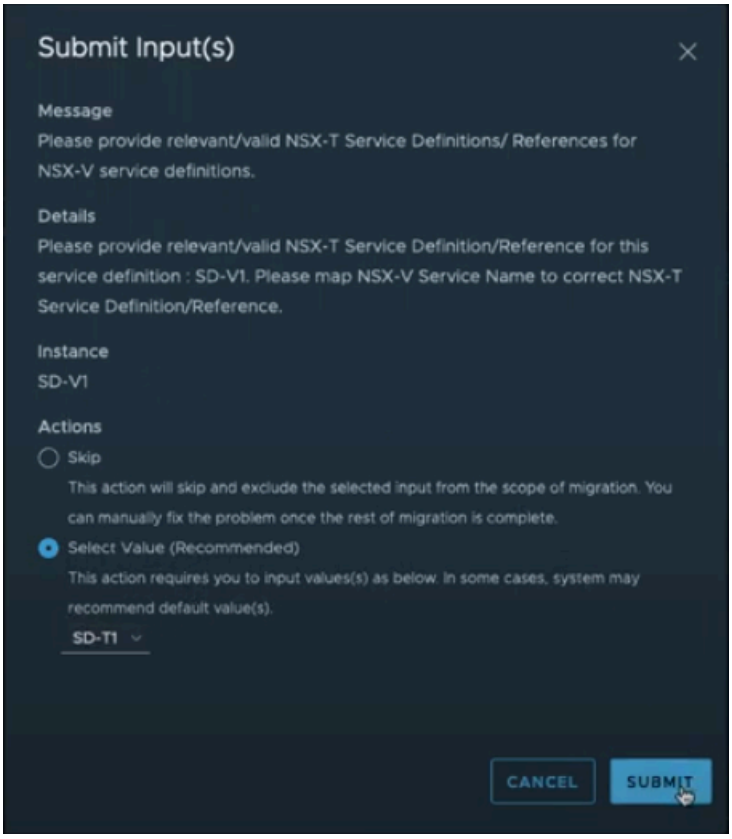
1. Connectez-vous à votre client vSphere.
2. Sélectionnez **Installation and Upgrade (Installation et mise à jour)** > **Service Deployment (Déploiement de service)**.
3. Sélectionnez votre déploiement de service.
4. Cliquez sur **Delete (Supprimer)**.
5. Cliquez sur **Delete (Supprimer)** pour confirmer.

STEP 10 | Résolvez les problèmes de configuration sur NSX-T Manager. Lors de la résolution des problèmes de configuration, vous devez prendre des mesures spécifiques pour migrer votre

 ©2023 Palo Alto Networks, Inc.

configuration de pare-feu VM-Series. Dans la plupart des cas, vous pouvez accepter les recommandations présentées par NSX-T Manager.

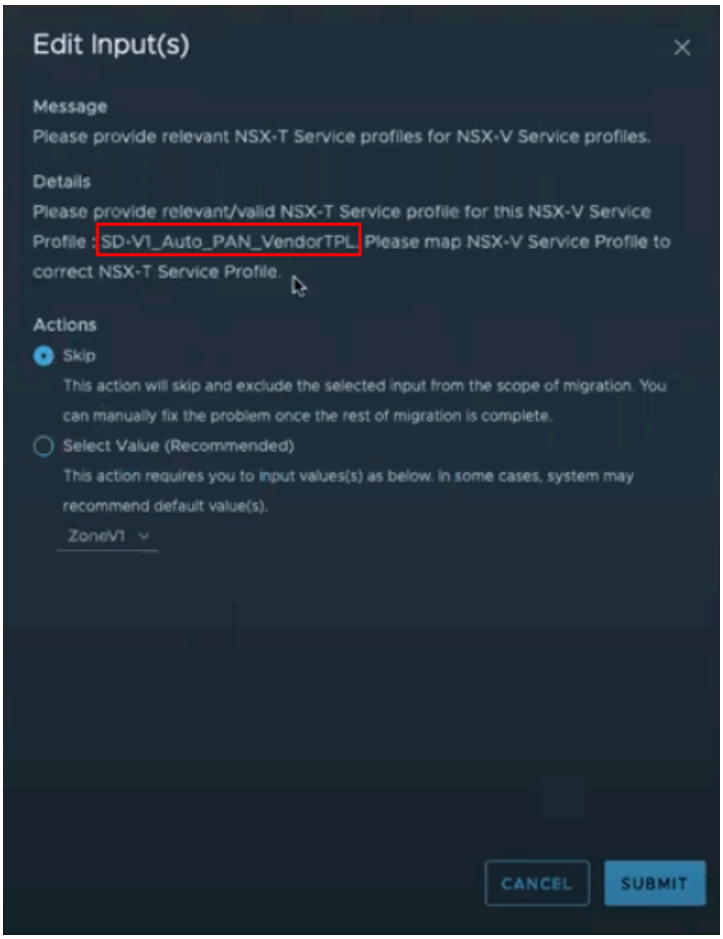
1. Lors de la résolution de la configuration de l'insertion de service, vérifiez que vous avez sélectionné la bonne définition de service que vous avez précédemment configurée sur Panorama pour VM-Series sur NSX-T.



2. Poursuivez la résolution de la configuration restante.
3. Avant de passer à **Migrate Configuration (Configurer la migration)**, il vous sera demandé de fournir une zone de transport pour l'insertion de service.
4. Mappez les profils de service sur NSX-V aux profils de service correspondants sur NSX-T.

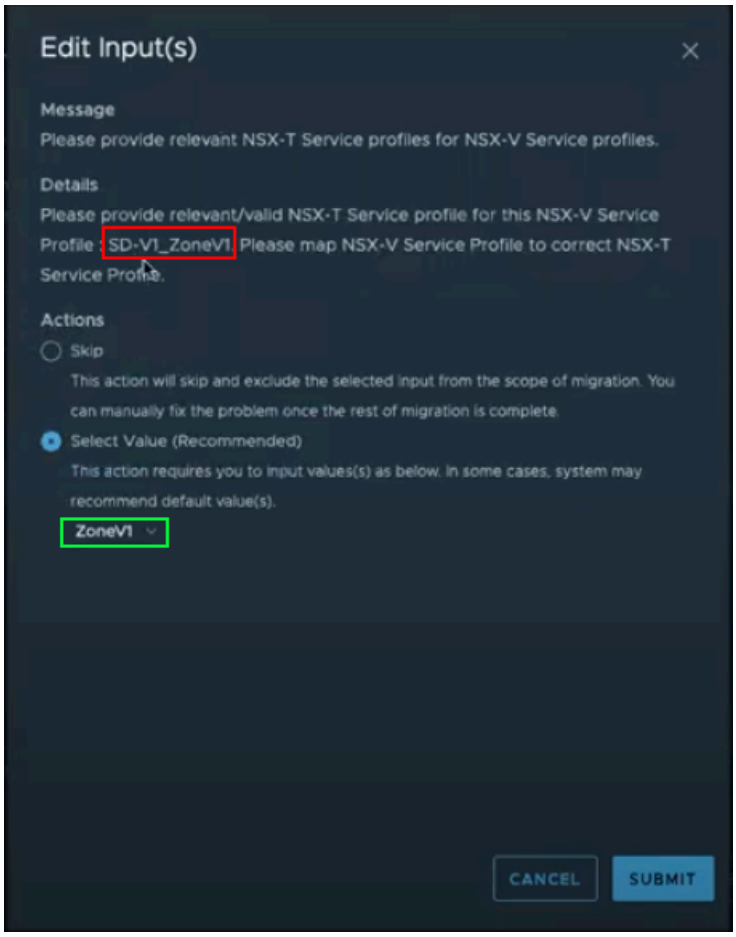
   1. Auto_PAN_VendorTPL peut être sauté.

 ©2023 Palo Alto Networks, Inc.



2. Mappez le profil de service NSX-T au profil de service NSX-V correspondant.

 ©2023 Palo Alto Networks, Inc.



STEP 11 | Migrez la configuration.

STEP 12 | Vérifiez que votre configuration a été migrée avec succès.

1. Sélectionnez **Inventory (Inventaire)** > **Groups (Groupes)** pour vérifier que vos ensembles d'IP et vos groupes de sécurité sont présents. Vous pouvez cliquer sur le nom du groupe de sécurité pour voir que les adresses IP correctes font partie du groupe de sécurité.
2. Sélectionnez **Security (Sécurité)** > **Network Introspection Settings (Paramètres d'introspection réseau)** > **Service Segment (Segment de service)** pour confirmer qu'un segment de service a été créé.
3. Sélectionnez **Security (Sécurité)** > **Network Introspection Settings (Paramètres d'introspection réseau)** > **Service Chains (Chaînes de service)** pour confirmer qu'une chaîne de service a été créée. Cliquez sur le lien Profiles (Profils) dans les colonnes Forward Path (Chemin avant) et Reverse Path (Chemin inverse) pour afficher votre profil de service.
4. Sélectionnez **Security (Sécurité)** > **Network Introspection (E-W) (Introspection réseau [E-O])** pour confirmer qu'une règle de redirection du trafic a été créée pour diriger le trafic vers le profil de service du pare-feu VM-Series.

STEP 13 | Le cas échéant, modifiez et migrez les périphéries.

STEP 14 | Configurez et migrez vos hôtes.

 ©2023 Palo Alto Networks, Inc.

STEP 15 | Ajoutez les étiquettes NSX-T à vos groupes d'adresses dynamiques existants.

1. Sélectionnez **Panorama** > **Objects (Objets)** > **Address Groups (Groupes d'adresses)**.
2. Cliquez sur le nom d'un groupe d'adresses dynamiques NSX-V existant.
3. Cliquez sur **Add Match Criteria (Ajouter des critères de correspondance)** pour afficher les étiquettes NSX-V et NSX-T.
4. Ajoutez l'étiquette NSX-T aux groupes d'adresses dynamiques. Si vous choisissez de ne pas supprimer les étiquettes NSX-V, veillez à utiliser l'opérateur **OR (OU)** entre les étiquettes.
5. Lorsque vous avez ajouté toutes les étiquettes nécessaires, cliquez sur **OK**.
6. **Commit (Validez)** vos modifications.

STEP 16 | Lancement du pare-feu VM-Series sur NSX-T (Est-Ouest). Vous n'avez pas besoin de créer un nouveau segment de service ; sélectionnez plutôt le segment de service créé lors de la migration.

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur AWS

Le pare-feu VM-Series peut être déployé dans le cloud Amazon Web Services (AWS) public et AWS GovCloud. Il peut ensuite être configuré pour sécuriser l'accès aux applications déployées sur des instances EC2 et placées dans un Virtual Private Cloud (VPC) sur AWS.

- À propos du pare-feu VM-Series sur AWS
- Déploiements pris en charge sur AWS
- Déploiement du pare-feu VM-Series sur AWS
- Intégration VM-Series avec un équilibreur de charge de passerelle AWS
- Haute disponibilité des pare-feu VM-Series sur AWS
- Cas d'utilisation : Sécurisation des instances EC2 dans le cloud AWS
- Cas d'utilisation : Utilisation de groupes d'adresses dynamiques pour sécuriser les nouvelles instances EC2 dans VPC
- Cas d'utilisation : Pare-feu VM-Series en tant que passerelles GlobalProtect sur AWS
- Surveillance VM sur le AWS
- Mise à l'échelle automatique de pare-feu VM-Series avec le service Amazon ELB
- Liste des attributs surveillés dans AWS VPC

À propos du pare-feu VM-Series sur AWS

L'AWS (Amazon Web Service) est un service de cloud public qui vous permet d'exécuter vos applications sur une infrastructure partagée gérée par Amazon. Ces applications peuvent être déployées sur une capacité informatique évolutive ou des instances EC2 dans différentes régions de l'AWS et accessibles aux utilisateurs sur Internet.

Pour garantir la cohérence de la mise en réseau et la simplicité de gestion des instances EC2, Amazon propose le VPC (Virtual Private Cloud). Un VPC est réparti à partir du cloud public AWS et est affecté à un bloc CIDR à partir de l'espace réseau privé (RFC 1918). Dans un VPC, vous pouvez fractionner des sous-réseaux public/privé en fonction de vos besoins et déployer les applications sur les instances EC2 de ces sous-réseaux. Ensuite, pour autoriser l'accès aux applications du VPC, vous pouvez déployer le pare-feu VM-Series sur une instance EC2. Le pare-feu VM-Series peut alors être configuré pour sécuriser le trafic depuis et vers les instances EC2 du VPC.

Le pare-feu VM-Series est disponible à la fois dans le cloud AWS public et sur AWS GovCloud. Le pare-feu VM-Series dans AWS public et AWS GovCloud prend en charge le modèle Bring Your Own License (BYOL) et le modèle de mise sous licence horaire basé sur l'utilisation Pay-As-You-Go (PAYG), disponible depuis AWS Marketplace. Pour plus d'informations sur la licence, voir Licences de pare-feu VM-Series pour les clouds publics.

- Types d'instances AWS EC2
- Pare-feu VM-Series sur AWS GovCloud
- Pare-feu VM-Series sur AWS Chine
- Pare-feu VM-Series sur AWS Outposts
- Terminologie AWS
- Mappage d'interface de gestion pour l'utilisation avec Amazon ELB
- Réglage des performances du pare-feu VM-Series pour AWS

Types d'instances AWS EC2

Pour les types d'instance pris en charge, consultez les modèles VM-Series sur les instances EC2.

Vous pouvez déployer le pare-feu VM-Series sur une taille d'instance AWS avec plus de ressources que la Configuration système requise pour VM-Series minimum. Si vous choisissez une taille d'instance plus grande pour le modèle de pare-feu VM-Series, bien que le pare-feu utilise uniquement les cœurs vCPU et la mémoire maximum indiqués dans le tableau, elle bénéficiera des performances réseau plus rapides fournies par AWS. Si vous souhaitez modifier le type d'instance sur votre pare-feu VM-Series sous licence avec l'option BYOL, vous devez désactiver la VM avant de basculer le type d'instance, pour vous assurer que votre licence est valide. Reportez-vous à Mise à niveau du modèle VM-Series pour savoir pourquoi.

Pour savoir comment dimensionner le pare-feu VM-Series sur AWS, reportez-vous à cet article.

Pare-feu VM-Series sur AWS GovCloud

AWS GovCloud est une région AWS isolée qui satisfait les exigences réglementaires et de conformité des agences gouvernementales et des clients des États-Unis.

©2023 Palo Alto Networks, Inc.

Pour sécuriser vos charges de travail qui contiennent toutes les catégories de données d'informations contrôlées non classées (Controlled Unclassified Information ; CUI) et de données orientées gouvernement disponibles au public dans la région AWS GovCloud (US), le pare-feu VM-Series offre les mêmes fonctionnalités de sécurité robustes dans le cloud public AWS standard et sur AWS GovCloud. Le pare-feu VM-Series sur AWS GovCloud et le cloud public AWS standard prennent en charge les mêmes fonctionnalités.

Reportez-vous aux sections AMI sur l'AWS GovCloud à Déploiement du pare-feu VM-Series sur AWS.

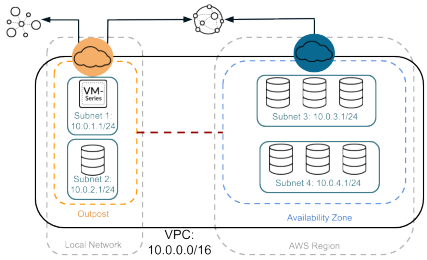
Pare-feu VM-Series sur AWS Chine

Le pare-feu VM-Series est disponible avec l'option BYOL sur la région AWS Chine Marketplace, et est disponible dans la région AWS Chine (Pékin) et la région AWS Chine (Ningxia). Vous devez disposer d'un compte AWS Chine distinct de votre compte AWS global pour accéder à cette image et utiliser les ressources AWS sur AWS Chine.

Assurez-vous de revoir la configuration système requise pour VM-Series avant de procéder au lancement du pare-feu VM-Series sur AWS.

Pare-feu VM-Series sur AWS Outposts

Afin d'offrir le même niveau de sécurité aux charges de travail situées sur site que celles situées dans le cloud AWS, vous pouvez installer le pare-feu VM-Series sur AWS sur un rack AWS Outposts sur votre site. Utilisez les AMI BYOL AWS Marketplace pour votre région AWS pour déployer les instances de pare-feu VM-Series dans vos sous-réseaux AWS Outposts.



Reportez-vous à Enregistrement du pare-feu VM-Series (avec code d'autorisation) pour créer un compte de support et enregistrer le pare-feu VM-Series sur le site Web de support client de Palo Alto Networks afin d'activer votre autorisation au support avec Palo Alto Networks.

Terminologie AWS

Ce document part du principe que vous maîtrisez la mise en réseau et la configuration du VPC AWS. Afin de fournir un contexte pour les termes utilisés dans cette section, voici un bref rappel des termes AWS (certaines définitions proviennent directement du glossaire AWS) auxquels ce document fait référence.

Terme	Description
EC2	Elastic Compute Cloud

©2023 Palo Alto Networks, Inc.

Terme	Description
	Un service Web vous permettant de lancer et de gérer des instances de serveur Linux/UNIX et Windows dans des centres de données d'Amazon.
AMI	Amazon Machine Image Fournit les informations nécessaires au lancement d'une instance ; il s'agit d'un serveur virtuel dans le cloud. L'AMI VM-Series est une image machine cryptée incluant le système d'exploitation nécessaire à l'instanciation du pare-feu VM-Series sur une instance EC2.
ELB	Équilibrage de charge élastique ELB est un service Web Amazon qui vous aide à améliorer la disponibilité et l'évolutivité de vos applications en dirigeant le trafic sur plusieurs instances Elastic Compute Cloud (EC2). ELB détecte les instances EC2 malsaines et redirige le trafic vers les instances saines jusqu'au rétablissement des instances malsaines. ELB peut envoyer le trafic uniquement vers l'interface principale de la prochaine instance EC2 à charge équilibrée au prochain saut. Ainsi, pour utiliser ELB avec un pare-feu VM-Series sur AWS, le pare-feu doit être capable d'utiliser l'interface principale pour le trafic du dataplane.
ENI	Elastic Network Interface Interface réseau supplémentaire pouvant être associée à une instance EC2. Les ENI peuvent inclure une adresse IP privée principale, une ou plusieurs adresse(s) IP privée(s) secondaire(s), une adresse IP publique, une adresse IP élastique (facultative), une adresse MAC, une adhésion à des groupes de sécurité spécifiés, une description et un indicateur de vérification de source/destination.
Types d'adresses IP des instances EC2	Une instance EC2 peut comporter différents types d'adresses IP. • Adresse IP publique : adresse IP pouvant être acheminée sur Internet. • Adresse IP privée : adresse IP dans la plage d'adresses IP privées tel que défini dans RFC 1918. Vous pouvez choisir d'attribuer manuellement une adresse IP ou d'attribuer automatiquement une adresse IP dans la plage du bloc CIDR pour le sous-réseau dans lequel vous lancez l'instance EC2. Si vous attribuez manuellement une adresse IP, Amazon réserve les quatre (4) premières adresses IP et la dernière (1) adresse IP dans chaque sous-réseau à des fins de mise en réseau IP. • Adresse IP élastique (EIP) : adresse IP statique que vous avez allouée dans Amazon EC2 ou Amazon VPC, puis associée à une instance. Les adresses IP élastiques sont liées à votre compte, et non à une instance spécifique. Elles sont élastiques, car vous pouvez facilement

©2023 Palo Alto Networks, Inc.

Terme	Description
	les allouer, les attacher, les détacher et les libérer à mesure que vos besoins changent. Une instance dans un sous-réseau public peut comporter une adresse IP privée, une adresse IP publique et une adresse IP élastique (EIP). Une instance dans un sous-réseau privé comportera une adresse IP privée et, éventuellement, une EIP.
Type d'instance	Caractéristiques techniques définies par Amazon stipulant la mémoire, le processeur, la capacité de stockage et le coût horaire d'une instance. Certains types d'instances sont conçus pour des applications standard alors que d'autres sont conçus pour des applications utilisant le processeur, la mémoire, etc., de manière intensive.
VPC	Virtual Private Cloud Réseau élastique alimenté par des services d'infrastructure, de plate-forme et d'application qui partagent une sécurité et une interconnexion communes.
IGW	Passerelle Internet fournie par Amazon. Connecte un réseau à Internet. Vous pouvez acheminer du trafic d'adresses IP en dehors de votre VPC vers la passerelle Internet.
Rôle IAM	Identity and Access Management (Gestion de l'identité et des accès) Nécessaire à l'activation de la haute disponibilité des pare-feu VM-Series sur AWS. Le rôle IAM définit les ressources et les actions de l'API que l'application peut utiliser après avoir assumé le rôle. Lors du basculement, le rôle IAM permet au pare-feu VM-Series de transmettre des demandes sécurisées de l'API en vue de faire passer les interfaces du plan de données de l'homologue actif à l'homologue passif. Un rôle IAM est également requis pour la surveillance VM. Reportez-vous à la Liste des attributs surveillés dans AWS VPC.
Sous-réseaux	Segment de la plage d'adresses IP d'un VPC auquel des instances EC2 peuvent être liées. Les instances EC2 sont regroupées par sous-réseaux en fonction de vos besoins de sécurité et opérationnels. Il existe deux types de sous-réseaux : • Sous-réseau privé : les instances EC2 de ce sous-réseau ne peuvent pas accéder à Internet. • Sous-réseau public : la passerelle Internet est liée au sous-réseau public, et les instances EC2 de ce sous-réseau peuvent accéder à Internet.

©2023 Palo Alto Networks, Inc.

Terme	Description
Groupes de sécurité	Un groupe de sécurité est lié à une ENI et spécifie la liste de protocoles, de ports et de plages d'adresses IP autorisées pour établir des connexions entrantes/sortantes sur l'interface. ***Dans AWS VPC, les groupes de sécurité et les ACL réseau contrôlent le trafic entrant et sortant. Les groupes de sécurité régulent l'accès à l'instance EC2, tandis que les ACL réseau régulent l'accès au sous-réseau. Étant donné que vous déployez le pare-feu VM-Series, définissez des règles plus strictes dans vos groupes de sécurité et ACL réseau, et autorisez le pare-feu à activer des applications en toute sécurité dans le VPC.***
Tables de routage	Ensemble de règles de routage contrôlant le trafic sortant d'un sous-réseau associé à la table de routage. Un sous-réseau ne peut être associé qu'à une seule table de routage.
Paire de clés	Ensemble d'informations d'identification de sécurité utilisé pour prouver votre identité de manière électronique. La paire de clés comporte une clé privée et une clé publique. Lorsque vous lancez le pare-feu VM-Series, générez une paire de clés ou sélectionnez-en une existante pour le pare-feu VM-Series. La clé privée est requise pour accéder au pare-feu en mode maintenance.
CloudWatch	Amazon CloudWatch est un service de surveillance qui vous permet de collecter et de suivre les statistiques des pare-feu VM-Series sur AWS. Lorsqu'ils sont activés, les pare-feu utilisent les API AWS pour publier des métriques PAN-OS natives dans CloudWatch.

Mappage d'interface de gestion pour l'utilisation avec Amazon ELB

Par défaut, l'interface réseau élastique (ENI) eth0 se mappe vers l'interface MGT sur le pare-feu et l'ENI eth1 se mappe vers ethernet 1/1 sur le pare-feu. Puisque l'ELB peut envoyer le trafic uniquement vers l'interface principale de l'instance EC2 à charge équilibrée au prochain saut, le pare-feu VM-Series doit être capable d'utiliser l'interface principale pour le trafic du dataplane.

Le pare-feu peut recevoir le trafic du dataplane sur l'interface principale dans les scénarios suivants où le pare-feu VM-Series se trouve derrière le service Amazon ELB (pour un diagramme de topologie, reportez-vous à la section Mise à l'échelle automatique de pare-feu VM-Series avec le service Amazon ELB) :

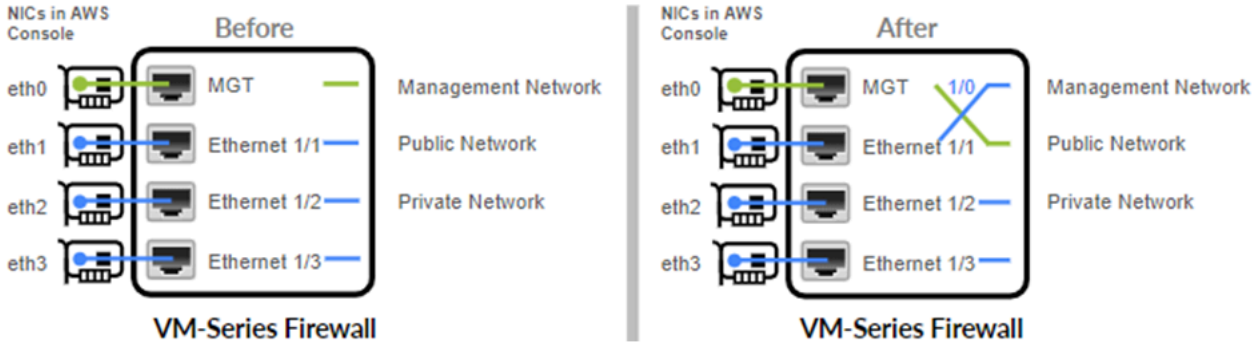
- Le pare-feu VM-Series sécurise le trafic sortant directement vers Internet sans devoir utiliser un lien VPN ou un lien de connexion directe en retour vers le réseau d'entreprise.

 ©2023 Palo Alto Networks, Inc.

- Le pare-feu VM-Series sécurise une application Web lorsqu'il y a exactement un serveur de backend, comme un serveur Web, pour chaque pare-feu. Les pare-feu VM-Series et les serveurs Web peuvent évoluer de manière linéaire, par paires, derrière ELB.

  À l'heure actuelle, pour les cas d'utilisation qui nécessitent un déploiement ELB de type sandwich pour faire évoluer les pare-feu et les instances EC2 de couche d'application, la permutation de l'interface de gestion ne vous permet pas de déployer de manière transparente la solution ELB. La possibilité de permuter l'interface de gestion résout en partie seulement l'intégration avec ELB.

Pour permettre au pare-feu d'envoyer e de recevoir le trafic du dataplane sur eth0 au lieu d'eth1, vous devez permuter les ENI au sein du pare-feu de sorte que l'ENI eth0 se mappe vers ethernet 1/1 et l'ENI eth1 se mappe vers l'interface MGT sur le pare-feu comme illustré ci-dessous.



Permutez l'interface de gestion avant de configurer le pare-feu ou de définir les règles de politique.

La permutation du mappage des interfaces permet à ELB de distribuer et de diriger le trafic vers les instances saines du pare-feu VM-Series situées dans des zones de disponibilité identiques ou différentes sur AWS pour une plus grande capacité et tolérance aux pannes.

La permutation d'interface n'est requise que lorsque le pare-feu VM-Series est situé derrière le service Amazon ELB. Si vous souhaitez déployer les pare-feu VM-Series dans une configuration traditionnelle à haute disponibilité, vous n'avez pas besoin de configurer la permutation d'interface décrite dans cette section. Passez à la section Haute disponibilité des pare-feu VM-Series sur AWS.

Pour permuter les interfaces, les options suivantes s'offrent à vous :

- **Au lancement** —Lorsque vous lancez le pare-feu, vous pouvez soit saisir la commande **`mgmt-interface-swap=enable`** dans le champ **User data (Données utilisateur)** sur la console de gestion AWS (reportez-vous à la section Launch the VM-Series Firewall on AWS) ou la CLI ou vous pouvez inclure la nouvelle commande opérationnelle **`mgmt-interface-swap`** dans la configuration d'amorçage.

©2023 Palo Alto Networks, Inc.

- **Après le lancement** —Après avoir lancé le pare-feu, Utiliser la CLI du Pare-feu de la série VM pour échanger l'interface de gestion (**régler le système mgmt-interface-swap et activer la commande opérationnelle « yes »**) sur le pare-feu.

  - *Pour éviter un comportement imprévisible de la part du pare-feu, choisissez une méthode pour spécifier uniformément le paramètre de permutation d'interface (dans la configuration d'amorçage, depuis la CLI sur le pare-feu, ou en utilisant le champ **User data (Données utilisateur)** d'Amazon EC2 sur la console AWS).*
  - *Assurez-vous de disposer de l'accès à la console WAS (console de gestion ou CLI) pour consulter l'adresse IP de l'interface eth1. Vérifiez également que les règles du groupe de sécurité AWS autorisent les connexions (HTTPS et SSH) à la nouvelle interface de gestion.*
  - *Si vous avez configuré le pare-feu ou défini des règles de politique avant la permutation d'interface, vérifiez si des changements d'adresse IP pour eth0 ou eth1 ont un impact sur les règles de politique.*

Réglage des performances du pare-feu VM-Series pour AWS

Les configurations suivantes affectent les performances :

- Les versions PAN-OS 9.0.3 et antérieures prennent en charge les types d'instance AWS C5 et M5, qui prennent en charge Elastic Network Adapter pour le mode SR-IOV par défaut. Pour en savoir plus, consultez Elastic Network Adapter – High Performance Network Interface for Amazon EC2 (Elastic Network Adapter – Interface réseau hautes performances pour Amazon EC2).
- Les versions PAN-OS 9.0.4 et ultérieures prennent en charge DPDK pour les types d'instance C5 et M5 par défaut. Lorsque le pare-feu est en mode DPDK, il utilise des pilotes DPDK. Pour obtenir la liste des pilotes pris en charge, consultez PacketMMAP and PDK Drivers on VM-Series Firewalls (Pilotes PacketMMAP et PDK sur les pare-feu VM-Series) et les notes de version officielles de DPDK.
- Pour bénéficier de l'encapsulation IETF RFC 8926 (Geneve) et d'un débit amélioré, effectuez une mise à niveau vers PAN-OS 10.0.2 ou une version ultérieure, et reportez-vous à VM-Series Integration with AWS Gateway Load Balancer (Intégration VM-Series avec l'équilibreur de charge de passerelle AWS).

Utilisez la CLI VM-Series pour afficher vos paramètres DPDK ou activer les E/S compressées.

Affichage de la configuration DPDK sur votre pare-feu

STEP 1 | Connectez-vous à la CLI du pare-feu VM-Series.

STEP 2 | Affichez votre configuration DPDK. Si DPDK est activé, la sortie est la suivante :

```
> show system setting dpdk-pkt-io on
```

```
Device current Packet IO mode: DPDK Device DPDK Packet IO capable:
 yes Device default Packet IO mode: DPDK
```

 ©2023 Palo Alto Networks, Inc.

Activation des E/S compressées DPDK

STEP 1 | Connectez-vous à la CLI du pare-feu VM-Series.

STEP 2 | Activez DPDK :

```
> set system setting dpdk-pkt-io on
```

STEP 3 | Redémarrez le périphérique.

Sur le pare-feu, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**, et sélectionnez **Reboot Device (Réamorcer le périphérique)**.

©2023 Palo Alto Networks, Inc.

Déploiements pris en charge sur AWS

Le pare-feu VM-Series sécurise le trafic entrant et sortant vers et depuis des instances EC2 du Virtual Private Cloud (VPC) AWS. Le VPC AWS ne prenant en charge qu'un réseau IP (capacités de mise en réseau de couche 3), le pare-feu VM-Series ne peut être déployé qu'avec des interfaces de couche 3.

- Déployez le pare-feu VM-Series pour sécuriser les instances EC2 hébergées dans le Virtual Private Cloud (VPC) AWS.

  Si vous hébergez vos applications dans le cloud AWS, déployez le pare-feu VM-Series pour protéger et activer en toute sécurité des applications destinées aux utilisateurs ayant accès à ces applications sur Internet. Par exemple, le diagramme suivant illustre le pare-feu VM-Series déployé dans le sous-réseau du périmètre auquel la passerelle Internet est liée. La ou les application(s) sont(est) déployée(s) dans le sous-réseau privé, qui ne dispose pas d'un accès direct à Internet.

  Lorsque les utilisateurs doivent accéder aux applications du sous-réseau privé, le pare-feu reçoit la requête et la dirige vers l'application appropriée après vérification de la politique de sécurité et exécution de la règle NAT de destination. Sur le chemin de retour, le pare-feu reçoit le trafic, applique la politique de sécurité et utilise la règle NAT source pour distribuer le contenu à l'utilisateur. Reportez-vous à la section Cas d'utilisation : Sécurisation des instances EC2 dans le cloud AWS.

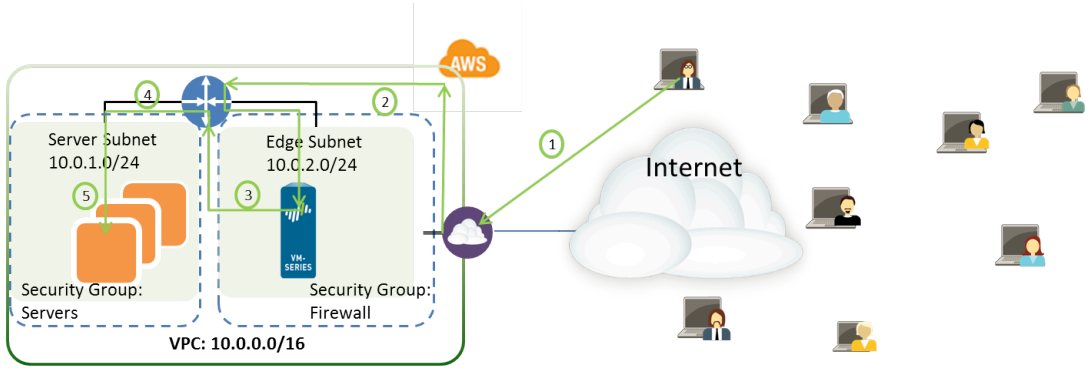


Figure 1: VM-Series pour instances EC2

- Déployez le pare-feu VM-Series pour l'accès VPN entre le réseau d'entreprise et les instances EC2 du Virtual Private Cloud (VPC) AWS.

  Pour connecter votre réseau d'entreprise aux applications déployées dans le cloud AWS, vous pouvez configurer le pare-feu en tant que point de terminaison d'un tunnel VPN IPSec. Ce tunnel VPN permet aux utilisateurs de votre réseau d'accéder en toute sécurité aux applications du cloud.

  Pour une gestion centralisée, une mise en œuvre cohérente des politiques sur l'ensemble du réseau, et la journalisation et la génération de rapports centralisées, vous pouvez également déployer Panorama dans votre réseau d'entreprise. Si vous devez configurer un accès VPN à plusieurs VPC, l'utilisation de Panorama vous permet de regrouper les pare-feu par région et de les gérer facilement.

©2023 Palo Alto Networks, Inc.

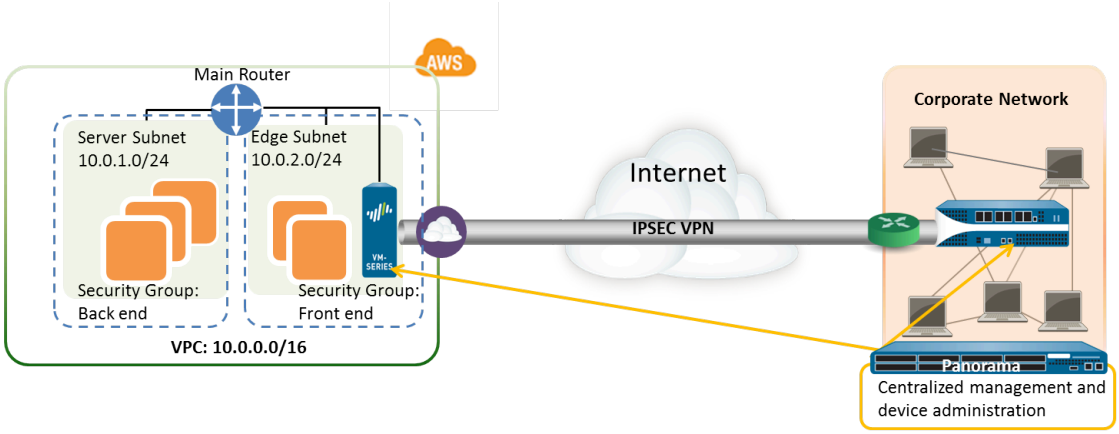


Figure 2: VM-Series pour accès VPN

- Déployez le pare-feu VM-Series en tant que passerelle GlobalProtect pour sécuriser l'accès d'utilisateurs distants à partir d'ordinateurs portables. L'agent GlobalProtect sur l'ordinateur portable se connecte à la passerelle et, en fonction de la requête, la passerelle établit une connexion VPN au réseau d'entreprise ou achemine la requête sur Internet. Pour garantir la conformité de la sécurité des utilisateurs de périphériques mobiles (utilisant l'application GlobalProtect), la passerelle GlobalProtect est combinée au Gestionnaire de sécurité mobile GlobalProtect. Le Gestionnaire de sécurité mobile GlobalProtect garantit que les périphériques mobiles sont gérés et configurés avec les paramètres de périphériques et informations de compte permettant d'utiliser les applications et réseaux d'entreprise.

  Dans chacun des cas pratiques présentés ci-dessus, vous pouvez déployer le pare-feu VM-Series sous forme de paire haute disponibilité (HA) active/passive. Pour obtenir des renseignements sur la configuration de la HA sur le pare-feu VM-Series, reportez-vous à la section Cas d'utilisation : Utilisation de groupes d'adresses dynamiques pour sécuriser les nouvelles instances EC2 dans VPC.

- Déployez le pare-feu VM-Series avec le service Amazon Elastic Load Balancing (ELB), de sorte que le pare-feu puisse recevoir le trafic du dataplane sur l'interface principale dans les scénarios suivants où le pare-feu VM-Series se trouve derrière l'Amazon ELB:

  - Le pare-feu VM-Series sécurise le trafic sortant directement vers Internet sans devoir utiliser un lien VPN ou un lien de connexion directe en retour vers le réseau d'entreprise.
  - Le pare-feu VM-Series sécurise une application Web lorsqu'il y a exactement un serveur dorsal, comme un serveur Web, pour chaque pare-feu. Les pare-feu VM-Series et les serveurs Web peuvent évoluer de manière linéaire, par paires, derrière ELB.

  Si vous souhaitez faire une Mise à l'échelle automatique des pare-feu VM-Series avec le service Amazon ELB, utilisez le modèle CloudFormation disponible dans le référentiel GitHub pour déployer le VM-Series dans une topologie sandwich ELB avec un ELB classique Internet et un équilibreur de charge classique interne ou un équilibreur de charge d'application interne (ELB interne).

 ©2023 Palo Alto Networks, Inc.

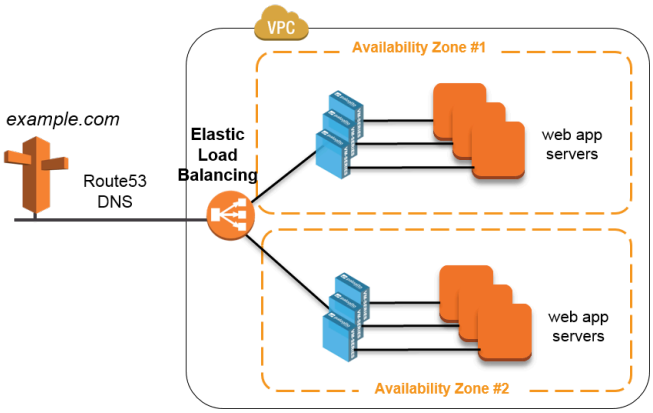


Figure 3: VM-Series avec ELB

Vous ne pouvez pas configurer le pare-feu pour envoyer et recevoir le trafic du dataplane sur eth0 lorsque le pare-feu est face à ELB. Le pare-feu VM-Series doit être placé derrière l'Amazon ELB.

Vous pouvez soit utiliser la CLI du pare-feu VM-Series pour permuter l'interface de gestion *ou l'activer à l'amorçage. Pour plus de détails, reportez-vous à la section* Mappage d'interface de gestion pour l'utilisation avec Amazon ELB.

Si vous souhaitez déployer une topologie sandwich d'équilibreur de charge, reportez-vous à Mise à l'échelle automatique de pare-feu VM-Series avec le service Amazon ELB.

En plus des liens ci-dessus qui sont couverts par la politique de support officielle de Palo Alto Networks, Palo Alto Networks fournit des modèles pris en charge par la communauté dans le référentiel GitHub de Palo Alto Networks *qui vous permettent d'explorer les solutions disponibles pour l'automatisation du cloud et la mise à l'échelle sur AWS. Reportez-vous à la section* VPC de transit AWS *pour un déploiement de VPC d'abonnement et de hub qui vous permet de sécuriser le trafic entre les VPC, entre un VPC et une ressource cloud sur site/hybride et le trafic sortant vers Internet.*

©2023 Palo Alto Networks, Inc.

Déploiement du pare-feu VM-Series sur AWS

- Obtention de l'AMI
- Planification de la fiche de travail du pare-feu VM-Series dans AWS VPC
- Lancement du pare-feu VM-Series sur AWS
- Lancement du pare-feu VM-Series sur AWS Outpost
- Création d'une AMI (Image de machine Amazon) personnalisée
- Chiffrement du volume EBS pour le pare-feu VM-Series sur AWS
- Utilisation de la CLI du pare-feu VM-Series pour permuter l'interface de gestion
- Activation de la surveillance CloudWatch sur le pare-feu VM-Series

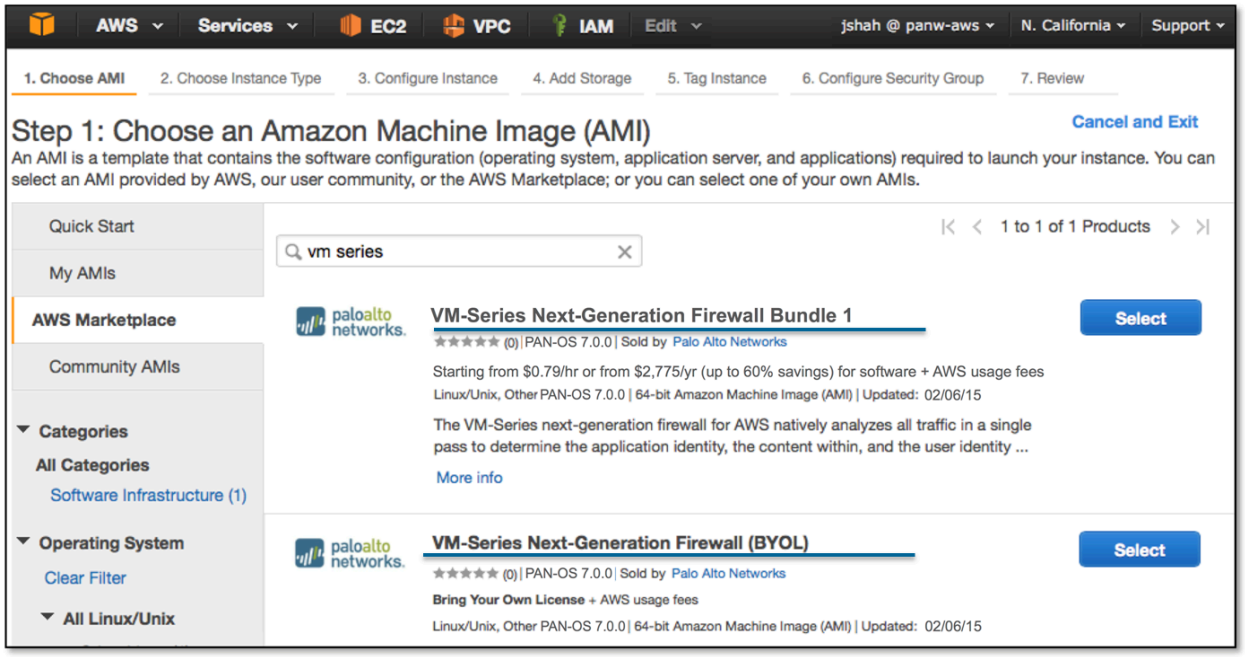
Obtention de l'AMI

Obtenez l'image de la machine Amazon pour le nuage public AWS et le GovCloud AWS à partir du marché respectif.

- AMI dans le cloud AWS public
- AMI sur l'AWS GovCloud
- Obtention de l'ID AMI (Image de machine Amazon) du pare-feu VM-Series

AMI dans le cloud AWS public

L'AMI pour le pare-feu VM-Series est disponible dans l'AWS Marketplace avec l'option Bring Your Own License (BYOL) et l'option de forfait basé sur l'utilisation.



Pour acheter des licences BYOL, contactez votre ingénieur ou revendeur Palo Alto Networks Systems.

©2023 Palo Alto Networks, Inc.

AMI sur l'AWS GovCloud

Le modèle Apportez votre propre licence (BYOL) et le modèle fondé sur l'utilisation du pare-feu de la série VM sont disponibles sur le AWS GovCloud Marketplace.

Avec un compte GovCloud, vous pouvez chercher Palo Alto Networks et trouver les AMIs pour le pare-feu de la série VM sur le Marketplace. Assurez-vous de consulter les Types d'instances EC2 pris en charge avant de lancer le pare-feu. Pour plus de détails, reportez-vous à la section Lancement du pare-feu VM-Series sur AWS.

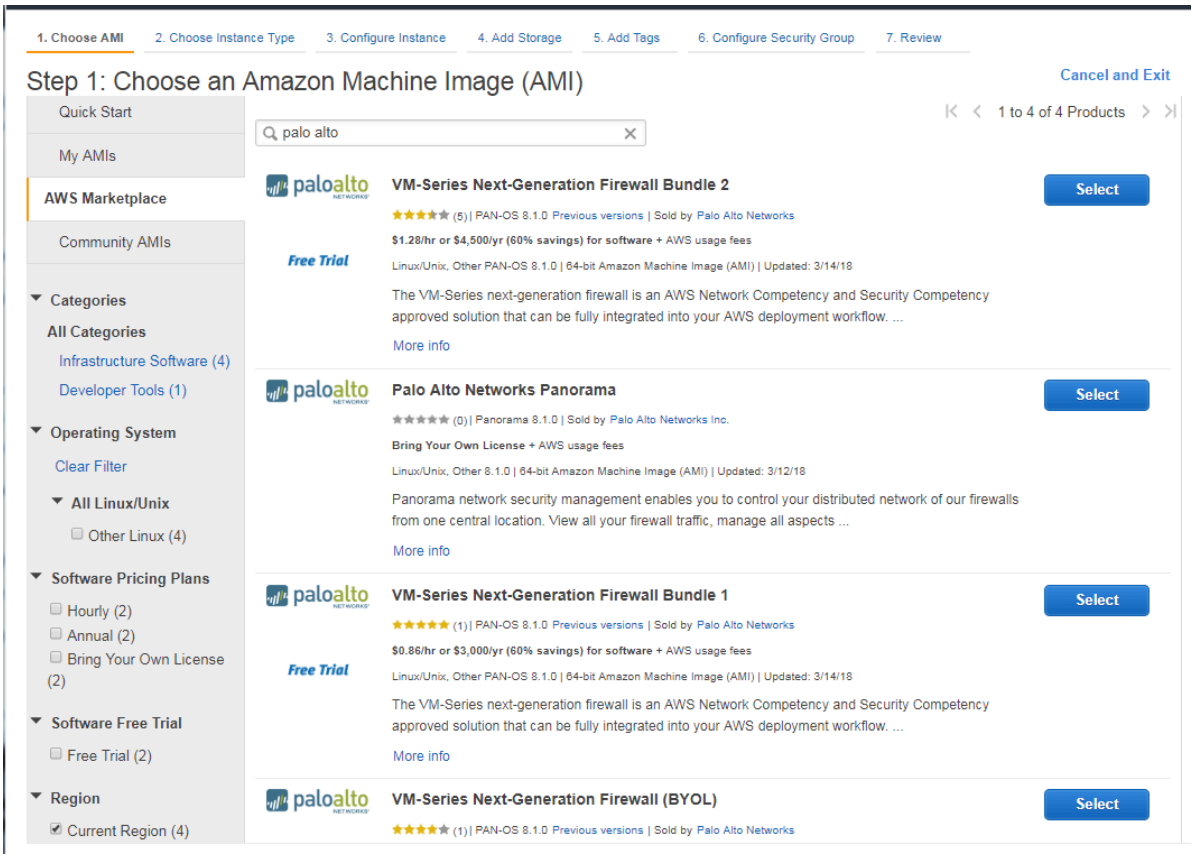


Table 1: Configuration système requise et limitations pour VM-Series sur AWS

Exigences	Détails
Types d'instances EC2	Le type d'instance EC2 que vous sélectionnez doit répondre à la Configuration système requise pour VM-Series pour le modèle de pare-feu VM-Series. Si vous déployez le pare-feu VM-Series sur un type d'instance EC2 non conforme à cette configuration requise, le pare-feu démarrera en mode maintenance.

©2023 Palo Alto Networks, Inc.

Exigences	Détails
	Pour prendre en charge la surveillance VM et une disponibilité élevée sur AWS, le pare-feu VM-Series doit être capable d'atteindre directement les terminaux de service API AWS sans aucun serveur proxy entre l'interface de gestion du pare-feu et les terminaux API AWS (comme ec2.us-west-2.amazonaws.com).
Elastic Block Storage (EBS) Amazon	Le pare-feu VM-Series doit utiliser le volume Elastic Block Storage (EBS) Amazon pour le stockage. L'optimisation EBS offre une meilleure pile de configuration et une capacité supplémentaire dédiée aux E/S EBS Amazon.
Mise en réseau	L'AWS ne prenant en charge que les capacités de mise en réseau de couche 3, le pare-feu VM-Series ne peut être déployé qu'avec des interfaces de couche 3. Les interfaces de couche 2, Virtual Wire, VLAN et sous-interfaces ne sont pas prises en charge sur le pare-feu VM-Series déployé dans le VPC AWS.
Interfaces	Prise en charge d'un total de huit interfaces (si disponibles) : une interface de gestion et un maximum de sept ENI (Elastic Network Interface) pour le trafic de données. Le pare-feu VM-Series ne prend pas l'association à chaud d'ENI. Pour détecter l'ajout ou la suppression d'une ENI, vous devez redémarrer le pare-feu. *Le type d'instance EC2 choisi détermine le nombre total d'ENI que vous pouvez activer. Par exemple, le type c3.8xlarge prend en charge huit (8) ENI.*
Autorisation de support et licences	Pour le modèle licence Bring Your Own Licence, un compte de support et une licence VM-Series valide sont requis pour obtenir le fichier image de machine (AMI) Amazon qui est nécessaire pour installer le pare-feu VM-Series dans AWS VPC. Les licences requises pour le pare-feu VM-Series (licence de capacité, licence de support et abonnements de prévention contre les menaces, de filtrage des URL et WildFire, etc.) doivent être achetées auprès de Palo Alto Networks. Pour acheter les licences pour votre déploiement, contactez votre représentant commercial. Reportez-vous à la section Licences de pare-feu VM-Series pour les clouds publics.. En ce qui a trait à la licence d'utilisation, il est possible d'acheter des forfaits horaires ou annuels, qui sont facturés directement à AWS. Vous devez toutefois enregistrer votre autorisation de support auprès de Palo Alto Networks. Pour plus de détails, voir Enregistrement modèle basé sur l'utilisation du pare-feu VM-Series pour les clouds publics (sans code d'autorisation).

©2023 Palo Alto Networks, Inc.

Obtention de l'ID AMI (Image de machine Amazon) du pare-feu VM-Series

Utilisez les instructions suivantes pour rechercher l'ID AMI du pare-feu VM-Series correspondant à la version de PAN-OS, au type de licence et à la région AWS dans laquelle vous souhaitez lancer le pare-feu VM-Series.

STEP 1 | Installez la CLI AWS sur le client que vous utilisez pour récupérer l'ID AMI et connectez-vous avec vos informations d'identification AWS.

Consultez la documentation AWS pour connaître les instructions relatives à l'installation de la CLI.

STEP 2 | Recherchez l'ID AMI avec la commande CLI suivante.

```
aws ec2 describe-images --filters "Name=product-
code,Values=<license-type-value>" Name=name,Values=PA-VM-AWS*<PAN-
OS-version>*  --region <region> --output json
```

Vous devez remplacer la valeur entre les chevrons <> par les informations pertinentes comme indiqué ci-dessous :

- Utilisez le code produit VM-Series pour chaque type de licence. Les valeurs sont les suivantes :
  - Paquet 1 :

    ```
    e9yfvyj3uag5uo5j2hjikv74n
    ```

  - Paquet 2 :

    ```
    hd44w1chf26uv4p52cdynb2o
    ```

  - BYOL :

    ```
    6njl1pau431dv1qxipg63mvah
    ```

- Utilisez la version de PAN-OS : 10.0. S'il existe plusieurs versions de fonctionnalités dans une version de PAN-OS, tous les ID AMI sont répertoriés pour vous. Par exemple, dans la version 9.0.x, vous verrez une liste des ID AMI pour les versions de PAN-OS 9.0, 9.0.3.xfr, 9.0.5.xfr et 9.0.6 et vous pourrez utiliser l'ID AMI pour la version de PAN-OS dont vous avez besoin.
- Obtenez les détails de la région AWS sur le site :https://docs.aws.amazon.com/general/latest/gr/rande.html.

Par exemple : Pour trouver l'AMI-ID pour le paquet 1 VM-Series pour PAN-OS 10.0.0 dans la région US California (Californie aux États-Unis), la commande CLI est la suivante :

```
 aws ec2 describe-images --filters "Name=product-
code,Values=e9yfvyj3uag5uo5j2hjikv74n" "Name=name,Values=PA-VM-
AWS*10.0*"  --region us-west-1 --output json
```

La sortie est :

```
{ "ProductCodes": [ { "ProductCodeId":
"e9yfvyj3uag5uo5j2hjikv74n", "ProductCodeType": "marketplace" } ],
"VirtualizationType": "hvm", "Hypervisor": "xen",
```

 ©2023 Palo Alto Networks, Inc.

```
 "ImageOwnerAlias": "aws-marketplace", "EnaSupport": true,
 "SriovNetSupport": "simple", "ImageId": "ami-06f7a63d7481d0ded",
 "State": "available", "BlockDeviceMappings": [ { "DeviceName":
 "/dev/xvda", "Ebs": { "SnapshotId": "snap-0009036179b39824b",
 "DeleteOnTermination": false, "VolumeType": "gp2",
 "VolumeSize": 60, "Encrypted": false } } ], "Architecture":
 "x86_64", "ImageLocation": "aws-marketplace/PA-
VM-AWS-10.0.0-f1260463-68e1-4bfb-bf2e-075c2664c1d7-
ami-06f7a63d7481d0ded.1", "RootDeviceType": "ebs", "OwnerId":
 "679593333241", "RootDeviceName": "/dev/xvda", "CreationDate":
 "2020-07-20T12:45:22.000Z", "Public": true, "ImageType":
 "machine", "Name": "PA-VM-AWS-10.0.0-f1260463-68e1-4bfb-
bf2e-075c2664c1d7-ami-06f7a63d7481d0ded.1" }
```

Vous pouvez également effectuer une sortie sous forme de tableau. Par exemple, pour voir l'image AMI pour BYOL pour PAN-OS 10.0.2 :

```
aws ec2 describe-images --filters "Name=product-
code,Values=6njl1pau431dv1qxipg63mvah" "Name=name,Values=PA-VM-
AWS*10.0.2*" --region us-west-1 --output table --query "Images[*].
{Name:Name,AMI:ImageId,State:State}"
```

```
-----------------------------------------------------------------------------
 DescribeImages |+----------------------
+-----------------------------------------------------------------------------
+-------------+| AMI | Name | State |+----------------------
+-----------------------------------------------------------------------------
+-------------+| ami-037b90bd9b630f594| PA-VM-
AWS-10.0.2-7064e142-2859-40a4-ab62-8b0996b842e9-
ami-07a0e94019f2a2001.4 | available |+----------------------
+-----------------------------------------------------------------------------
+-------------+
```

Planification de la fiche de travail du pare-feu VM-Series dans AWS VPC

Pour simplifier le déploiement, planifiez les sous-réseaux du VPC et les instances EC2 que vous souhaitez déployer dans chaque sous-réseau. Avant de commencer, consultez le tableau ci-dessous pour disposer des informations réseau nécessaires au déploiement et à l'insertion du pare-feu VM-Series dans le flux de trafic du VPC :

Élément de configuration	Valeur
CIDR VPC	
Groupes de sécurité	
Sous-réseau (public) CIDR	
Sous-réseau (privé) CIDR	

©2023 Palo Alto Networks, Inc.

Élément de configuration	Valeur
Sous-réseau (public) Table de routage	
Sous-réseau (privé) Table de routage	
Groupes de sécurité • Règles d'accès de gestion au pare-feu (eth0/0) • Règles d'accès aux interfaces du dataplane du pare-feu • Règles d'accès aux interfaces affectées aux serveurs d'applications	
Pare-feu VM-Series derrière ELB	
EC2 Instance 1 (pare-feu VM-Series) *Une EIP n'est requise que pour l'interface du dataplane liée au sous-réseau public.*	Sous-réseau : Type d'instance : IP de l'interface de gestion : EIP de l'interface de gestion : Interface du dataplane eth1/1 • IP privée : • EIP (si nécessaire) : • Groupe de sécurité : Interface du dataplane eth1/2 • IP privée : • EIP (si nécessaire) : • Groupe de sécurité :
EC2 Instance 2 (application à sécuriser) Répétez ces valeurs pour les autres applications déployées.	Sous-réseau : Type d'instance : IP de l'interface de gestion : Passerelle par défaut : Interface du dataplane 1 • IP privée :

©2023 Palo Alto Networks, Inc.

Élément de configuration	Valeur
Configuration pour la HA	Si vous déployez les pare-feu VM-Series dans une configuration à haute disponibilité (active/passive), vous devez faire ce qui suit : • Créez un rôle IAM et affectez le rôle au pare-feu VM-Series lors du déploiement de l'instance. Reportez-vous à la section Rôles IAM pour la HA. • Déployez les homologues HA dans la même zone de disponibilité AWS. • Le pare-feu actif de la paire HA doit avoir au moins trois ENI, soit deux interfaces du plan de données et une interface de gestion. Le pare-feu passif de la paire HA doit avoir une ENI de gestion et une ENI qui agit en tant qu'interface du plan de données ; vous configurerez l'interface du plan de données en tant qu'interface HA2. ***N'associez pas d'interfaces du plan de données supplémentaires au pare-feu passif de la paire HA. Lors du basculement, les interfaces du plan de données du pare-feu qui était précédemment actif sont déplacées (dissociées et puis associées) vers le pare-feu qui est désormais actif (précédemment passif).***

Lancement du pare-feu VM-Series sur AWS

Si vous n'avez pas encore enregistré dans votre compte de support le code d'autorisation de capacité contenu dans l'e-mail de confirmation de commande que vous avez reçu, reportez-vous à la section Enregistrement du pare-feu VM-Series. Après l'enregistrement, déployez le pare-feu VM-Series à l'aide d'une AMI publiée sur le Marketplace ou procédez à la Création d'une AMI (Image de machine Amazon) personnalisée dans le VPC AWS comme suit :

STEP 1 | Accédez à la console AWS.

Connectez-vous à la console AWS et sélectionnez l'EC2 Dashboard (Tableau de bord EC2).

©2023 Palo Alto Networks, Inc.

STEP 2 | Configurez le VPC en fonction de vos besoins réseau.

Que vous lanciez le pare-feu VM-Series dans un VPC existant ou que vous créiez un nouveau VPC, le pare-feu VM-Series doit être en mesure de recevoir le trafic des instances EC2 et d'établir des communications entrantes et sortantes entre le VPC et Internet.

Reportez-vous à la documentation d'AWS VPC pour obtenir des instructions sur la création d'un VPC et sur sa configuration pour l'accès.

Pour un exemple avec un flux de travail complet, reportez-vous à la section Cas d'utilisation : Sécurisation des instances EC2 dans le cloud AWS.

1. Créez un nouveau VPC ou utilisez un VPC existant. Reportez-vous à la documentation d'AWS sur le Démarrage.
2. Vérifiez que les composants réseau et de sécurité sont définis de manière appropriée.
   - Activez la communication avec Internet. Le VPC par défaut inclut une passerelle Internet et si vous installez le pare-feu VM-Series dans le sous-réseau par défaut, il a accès à Internet.
   - Créez des sous-réseaux. Les sous-réseaux sont des segments de la plage d'adresses IP affectée au VPC dans lequel vous lancez les instances EC2. Le pare-feu VM-Series doit appartenir au sous-réseau public pour pouvoir être configuré pour l'accès à Internet.
   - Si nécessaire, créez des groupes de sécurité pour gérer le trafic entrant et sortant des instances EC2/sous-réseaux.
   - Ajoutez des itinéraires à la table de routage pour un sous-réseau privé afin de vous assurer que le trafic peut être acheminé entre des sous-réseaux et des groupes de sécurité du VPC, le cas échéant.
3. Si vous souhaitez déployer une paire de pare-feu WM-Series en haute disponibilité vous devez définir les Rôles IAM pour la HA avant de pouvoir procéder à la Configuration de la HA active/passive dans AWS.
4. (Facultatif) Si vous utilisez l'amorçage pour effectuer la configuration de votre pare-feu VM-Series, reportez-vous à la section Amorçage du pare-feu VM-Series dans AWS. Pour plus d'informations sur l'amorçage, reportez-vous aux sections Amorçage du pare-feu VM-Series et Choix d'une méthode d'amorçage.

STEP 3 | Lancez le pare-feu VM-Series.

Bien que vous puissiez ajouter d'autres interfaces réseau (ENI) au pare-feu VM-Series lors de son lancement, AWS libère l'adresse IP publique automatiquement attribuée à l'interface de gestion lors du redémarrage du pare-feu. Par conséquent, afin d'assurer la connectivité à l'interface de gestion, vous devez affecter une adresse IP élastique à l'interface de gestion avant d'associer d'autres interfaces au pare-feu.

Si vous souhaitez conserver les adresses EIP, vous pouvez affecter une adresse EIP à l'interface eth 1/1 et utiliser cette interface pour le trafic de gestion et le trafic de données. Pour restreindre

 ©2023 Palo Alto Networks, Inc.

les services autorisés sur l'interface ou limiter les adresses IP qui peuvent se connecter à l'interface eth 1/1, associez un profil de gestion à l'interface.

1. Sur le tableau de bord EC2, cliquez sur **Launch Instance (Lancer l'instance)**.
2. Sélectionnez l'AMI VM-Series. Pour obtenir l'AMI, reportez-vous à la section Obtention de l'AMI.
3. Lancez le pare-feu VM-Series sur une instance EC2.
    1. Choisissez le **EC2 instance type (Type d'instance EC2)** pour allouer les ressources nécessaires au pare-feu, puis cliquez sur **Next (Suivant)**. Reportez-vous à la section VM-Series sur système SDX : configuration système requise pour connaître les exigences de ressources.
    2. Sélectionnez le VPC.
    3. Sélectionnez le sous-réseau public auquel l'interface de gestion du pare-feu VM-Series sera liée.
    4. Sélectionnez **Automatically assign a public IP address (Affecter automatiquement une adresse IP publique)**. Cela vous permet d'obtenir une adresse IP accessible publiquement pour l'interface de gestion du pare-feu VM-Series.

        Vous pouvez lier une adresse IP élastique à l'interface de gestion ultérieurement. Contrairement à l'adresse IP publique qui est dissociée du pare-feu lorsque l'instance est fermée, l'adresse IP élastique est persistante et peut être reliée à une nouvelle instance (ou de remplacement) du pare-feu VM-Series sans reconfigurer l'adresse IP si vous devez y faire référence.
    5. Sélectionnez **Launch as an EBS-optimized instance (Lancer en tant qu'instance optimisée EBS)**.

 ©2023 Palo Alto Networks, Inc.

6. Ajoutez une autre interface réseau pour les déploiements avec ELB afin de pouvoir permuter les interfaces de gestion et de données sur le pare-feu. La permutation des interfaces exige un minimum de deux ENI (eth0 et eth1).

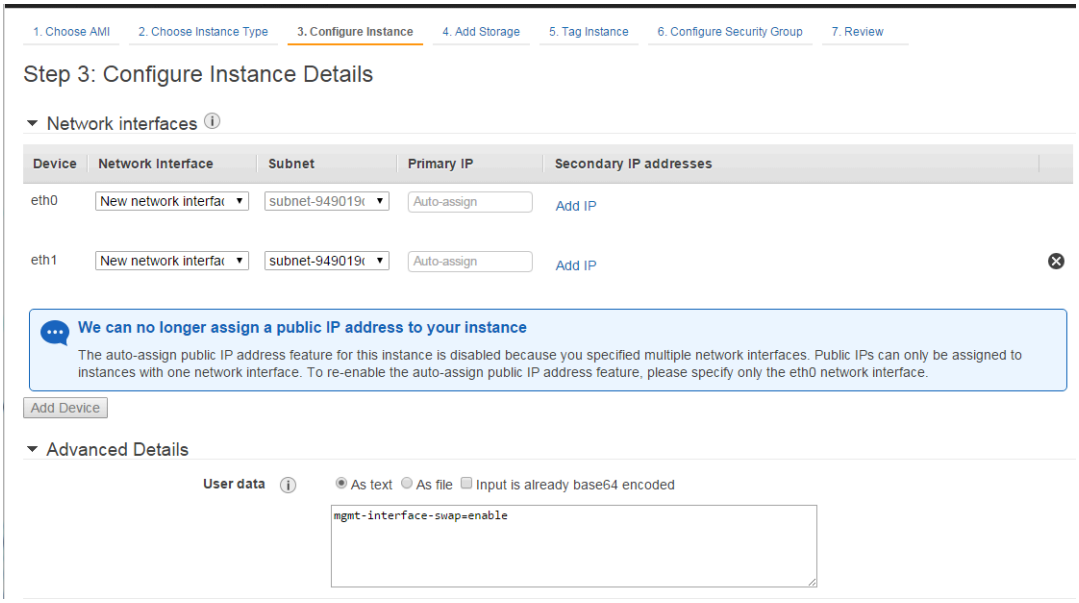
   - Développez la section Interfaces réseau et cliquez sur **Add Device (Ajouter périphérique)** pour ajouter une autre interface réseau.

     Assurez-vous que votre VPC possède plus d'un sous-réseau afin de pouvoir ajouter des ENI supplémentaires au lancement.

     Si vous lancez le pare-feu avec une seule ENI :

     - *La commande de permutation d'interface entraînera le démarrage du pare-feu en mode maintenance.*
     - *Vous devez redémarrer le pare-feu lorsque vous ajoutez la deuxième ENI.*

   - Développez la section Advanced Details (Détails avancés) et, dans le champ **Données utilisateur**, saisissez le texte **`mgmt-interface-swap=enable`** pour effectuer la permutation d'interface durant le lancement.



   Bootstrap Package (Ensemble d'amorçage) : si vous amorcez le pare-feu avec l'ensemble d'amorçage, vous pouvez également saisir un point-virgule comme séparateur après **`mgmt-interface-swap=enable`**, puis saisir **`vmseries-bootstrap-aws-s3bucket=<bucketname>`**.

   User Data (Données utilisateur) : si vous amorcez avec des données utilisateur, saisissez un point virgule comme séparateur après **`mgmt-interface-swap=enable`** et saisissez des paires clé-valeur supplémentaires selon Saisir une configuration de base en tant que données utilisateur (clouds publics).

   AWS Secret (Secret AWS) : si vous amorcez avec un secret AWS, saisissez un point virgule comme séparateur après **`mgmt-interface-swap=enable`** et saisissez le nom secret comme une paire clé-valeur, comme décrit à l'étape 3 de Amorçage du pare-feu VM-Series sur AWS. Par exemple :

©2023 Palo Alto Networks, Inc.

7. Acceptez les paramètres de **Storage (Stockage)** par défaut. Le pare-feu utilise le type de volume SSD (gp2).

   Cette paire de clés est requise lorsque vous accédez pour la première fois au pare-feu. Elle est également nécessaire pour accéder au pare-feu en mode maintenance.

8. (Facultatif) **Tagging (Étiquetage)**. Ajoutez une ou plusieurs étiquettes pour créer vos propres métadonnées afin d'identifier et de grouper le pare-feu VM-Series. Par exemple, ajoutez une étiquette **Name (Nom)** avec une **Value (Valeur)** qui vous aide à vous souvenir que les interfaces ENI ont été permutées sur ce pare-feu VM-Series.
9. Sélectionnez un **Security Group (Groupe de sécurité)** existant ou créez-en un nouveau. Ce groupe de sécurité vise à limiter l'accès à l'interface de gestion du pare-feu. Vous devriez envisager d'au moins permettre l'accès https et ssh pour l'interface de gestion.
10. Lorsque vous y êtes invité, sélectionnez l'option **SSD** adaptée à votre configuration.
11. Sélectionnez **Review and Launch (Vérifier et lancer)**. Vérifiez que vos sélections sont correctes, puis cliquez sur **Launch (Lancer)**.
12. Sélectionnez une paire de clés existante ou créez-en une, et acceptez l'avis de non-responsabilité de la clé.
13. Téléchargez et enregistrez la clé privée dans un emplacement sûr ; l'extension de fichier est `.pem`. Vous ne pouvez pas régénérer cette clé en cas de perte.

    Le lancement du pare-feu VM-Series prend 5 à 7 minutes. Vous pouvez voir la progression sur le tableau de bord EC2. Une fois le processus terminé, le pare-feu VM-Series s'affiche sur la page **Instances** du tableau de bord EC2.

©2023 Palo Alto Networks, Inc.

STEP 4 | Configurez un nouveau mot de passe administratif pour le pare-feu.

Sur la CLI du pare-feu VM-Series, vous devez configurer un mot de passe d'administration unique avant de pouvoir accéder à l'interface Web du pare-feu. Pour vous connecter à la CLI, vous avez besoin de la clé privée que vous avez utilisée pour lancer le pare-feu.

1. Utilisez l'adresse IP publique vers SSH dans l'interface de ligne de commande (CLI) du pare-feu VM-Series. Vous aurez besoin de la clé privée utilisée ou créée dans 3 ci-dessus pour accéder à la CLI.

   Si vous avez ajouté une ENI supplémentaire pour prendre en charge les déploiements avec ELB, vous devez d'abord créer et affecter une adresse IP élastique à l'ENI pour accéder à la CLI (voir 6).

   Si vous utilisez PuTTY pour l'accès SSH, vous devez convertir le format .pem au format .ppk. Consultez https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html
2. Saisissez la commande suivante pour vous connecter au pare-feu :

   ssh-i <*private_key.pem*> admin@<*public-ip_address*>
3. Configurez un nouveau mot de passe à l'aide de la commande suivante, et suivez les invites affichées à l'écran :

   configure

   set mgt-config users admin password
4. Si votre licence de type BYOL doit être activée, définissez l'adresse IP du serveur DNS pour que le pare-feu puisse accéder au serveur de licences de Palo Alto Networks. Saisissez la commande suivante pour établir l'adresse IP du serveur DNS :

   set deviceconfig system dns-setting servers primary <*ip_address*>
5. Validez vos modifications à l'aide de la commande suivante :

   commit
6. Fermez la session SSH.

STEP 5 | Arrêtez le pare-feu VM-Series.

1. Sur le tableau de bord EC2, sélectionnez **Instances**.
2. Dans la liste, sélectionnez le pare-feu VM-Series, puis cliquez sur **Actions** > **Stop (Arrêter)**.

STEP 6 | Créez une adresse IP élastique (EIP) et affectez-la à l'ENI utilisée pour l'accès de gestion au pare-feu, puis redémarrez le pare-feu VM-Series.

1. Sélectionnez **Elastic IPs (IP élastiques)**, puis cliquez sur **Allocate New Address (Allouer une nouvelle adresse)**.
2. Sélectionnez **EC2-VPC**, puis cliquez sur **Yes, Allocate (Oui, allouer)**.
3. Sélectionnez la nouvelle EIP allouée, puis cliquez sur **Associate Address (Associer l'adresse)**.
4. Sélectionnez l'**Interface réseau** et l'**Adresse IP privée** associée à l'interface de gestion, puis cliquez sur **Oui, associer**.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Créez la ou les interface(s) réseau virtuel et associez-les(la) au pare-feu VM-Series. Les interfaces réseau virtuel sont appelées des interfaces réseau élastiques (ENI) dans AWS, et servent d'interfaces réseau du dataplane sur le pare-feu. Ces interfaces sont utilisées pour la gestion du trafic de données depuis/vers le pare-feu.

Vous aurez besoin d'au moins deux ENI qui autorisent le trafic entrant et sortant vers le pare-feu et depuis ce dernier. Vous pouvez ajouter jusqu'à sept ENI pour gérer le trafic de données sur le pare-feu VM-Series. Vérifiez le type de votre instance EC2 pour connaître le nombre maximum qu'il peut prendre en charge.

1. Sur le tableau de bord EC2, sélectionnez **Network Interfaces (Interfaces réseau)**, puis cliquez sur **Create Network Interface (Créer une interface réseau)**.
2. Donnez un nom descriptif à l'interface.
3. Sélectionnez le sous-réseau. Utilisez l'ID de sous-réseau pour vérifier que vous avez sélectionné le bon sous-réseau. Vous ne pouvez lier qu'une seule ENI à une instance d'un même sous-réseau.
4. Saisissez l'adresse **Private IP (IP privée)** pour l'affecter à l'interface ou sélectionnez **Auto-assign (Affectation automatique)** pour affecter automatiquement une adresse IP parmi les adresses IP disponibles du sous-réseau sélectionné.
5. Sélectionnez le **Security group (Groupe de sécurité)** contrôlant l'accès à l'interface réseau du dataplane.
6. Cliquez sur **Yes, Create (Oui, créer)**.



7. Pour associer l'ENI au pare-feu VM-Series, sélectionnez l'interface que vous venez de créer, puis cliquez sur **Attach (Associer)**.



8. Sélectionnez l'**Instance ID (ID d'instance)** du pare-feu VM-Series, puis cliquez sur **Attach (Associer)**.
9. Répétez les étapes ci-dessus pour créer et associer au moins une ENI supplémentaire au pare-feu.

 ©2023 Palo Alto Networks, Inc.

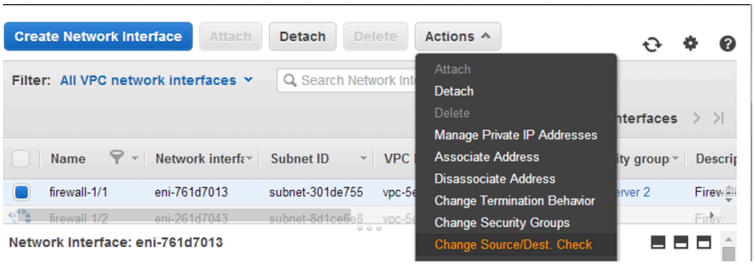
STEP 8 | (Non nécessaire pour la licence d'utilisation) Activez les licences sur le pare-feu VM-Series.

> ***Cette tâche n'est pas exécutée sur la console de gestion AWS. Accédez au portail de support de Palo Alto Networks et l'interface Web du pare-feu VM-Series est nécessaire pour l'activation de la licence.***

Reportez-vous à la section Activation de la licence.

STEP 9 | Désactivez la vérification de la source/destination sur chaque interface réseau du dataplane du pare-feu. La désactivation de cette option permet à l'interface de gérer le trafic réseau non destiné à l'adresse IP affectée à l'interface réseau.

1. Sur le tableau de bord EC2, sélectionnez l'interface réseau, eth1/1 par exemple, dans l'onglet **Network Interfaces** (Interfaces réseau).
2. Dans la liste déroulante **Action**, sélectionnez **Change Source/Dest. (Modifier la source/dest.) Check (Vérifier)** .



3. Cliquez sur **Disabled (Désactivé)** et **Save (Enregistrez)** vos modifications.
4. Répétez les étapes 1 à 3 pour chaque interface du dataplane du pare-feu.

STEP 10 | Configurez les interfaces réseau du plan de données en tant qu'interfaces de couche 3 sur le pare-feu.

Pour un exemple de configuration, reportez-vous aux étapes 14 à 17 dans Cas d'utilisation : Sécurisation des instances EC2 dans le cloud AWS.

> ***Sur les serveurs d'applications du VPC, définissez l'interface réseau du dataplane du pare-feu en tant que passerelle par défaut.***

1. Dans votre navigateur Web, connectez-vous de manière sécurisée (https) à l'aide de l'adresse EIP et du mot de passe que vous avez attribués lors de la configuration initiale

©2023 Palo Alto Networks, Inc.

(https://<Elastic_IP address>). Un avertissement de certificat s'affiche ; ne vous en préoccupez pas. Continuez vers la page Web.

2. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
3. Cliquez sur la liaison **ethernet 1/1** et configurez comme suit :
   - **Interface Type (Type d'interface)** : **Layer3 (Couche 3)**
   - Dans l'onglet **Config (Configuration)**, affectez l'interface au routeur par défaut.
   - Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Définissez une nouvelle zone, VM_Series_Non approuvée par exemple, puis cliquez sur **OK**.
   - Dans l'onglet **IPv4**, sélectionnez **Static (Statique)** ou **DHCP Client (Client DHCP)**.

     Si vous utilisez l'option **Static (Statique)**, cliquez sur **Add (Ajouter)** dans la section IP, puis saisissez l'adresse IP et le masque réseau pour l'interface, par exemple, 10.0.0.10/24.

     Assurez-vous que l'adresse IP correspond à l'adresse IP ENI que vous avez affectée précédemment.

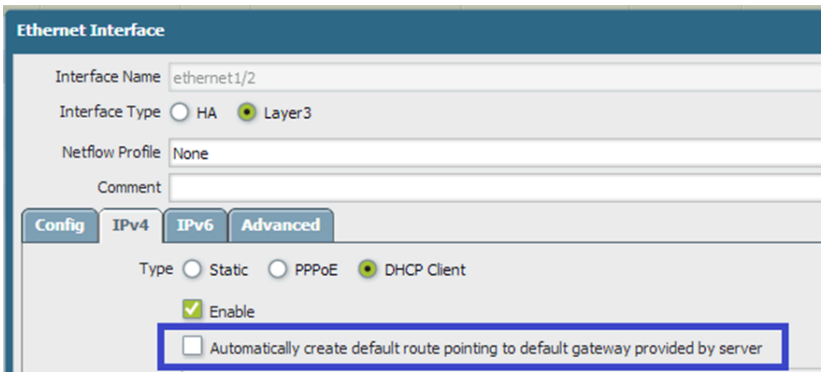
     Si vous utilisez DHCP, sélectionnez **DHCP Client (Client DHCP)** ; l'adresse IP privée que vous avez affectée à l'ENI dans la console de gestion AWS est automatiquement acquise.
4. Cliquez sur le lien pour **ethernet 1/2** et configurez-le comme suit :
   - **Interface Type (Type d'interface)** : **Layer3 (Couche 3)**
   - Zone de sécurité : VM_Series_Approuvée
   - **Adresse IP** : sélectionnez le bouton radio **Static** (Statique) ou **DHCP Client** (Client DHCP).

     Pour l'option Statique, cliquez sur **Add (Ajouter)** dans la section IP, puis saisissez l'adresse IP et le masque réseau pour l'interface. Assurez-vous que l'adresse IP correspond à l'adresse IP ENI associée que vous avez affectée précédemment.
5. Cliquez sur **Commit (Valider)**. Vérifiez que la liaison des interfaces est active.



*Pour l'option DHCP, décochez la case **Automatically create default route to default gateway provided by server** (Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur). Pour une interface associée au sous-réseau privé du VPC, la désactivation de cette option garantit que le trafic géré par cette interface n'est pas dirigé directement vers la passerelle Internet sur le VPC.*

 ©2023 Palo Alto Networks, Inc.



STEP 11 | Créez des règles NAT pour autoriser le trafic entrant et sortant des serveurs déployés dans le VPC.

1. Sélectionnez **Policies (Politiques)** > **NAT** sur l'interface Web du pare-feu.
2. Créez une règle NAT pour autoriser le trafic entre l'interface réseau du dataplane sur le pare-feu et l'interface serveur Web dans le VPC.
3. Créez une règle NAT pour autoriser l'accès sortant pour le trafic entre le serveur Web et Internet.

STEP 12 | Créez des politiques de sécurité pour autoriser/refuser le trafic vers les/des serveurs déployés dans le VPC.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** sur l'interface Web du pare-feu.
2. Cliquez sur **Add (Ajouter)**, puis spécifiez les zones, applications et options de journalisation que vous souhaitez exécuter afin de limiter et d'auditer le trafic traversant le réseau.

STEP 13 | Cliquez sur Commit (Valider) pour valider les modifications apportées au pare-feu.

Cliquez sur **Commit (Valider)**.

STEP 14 | Vérifiez que le pare-feu VM-Series sécurise le trafic et que les règles NAT sont appliquées.

1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)** sur l'interface Web du pare-feu.
2. Consultez les journaux pour vérifier que les applications sur le réseau sont conformes aux politiques de sécurité que vous avez mises en œuvre.

Lancement du pare-feu VM-Series sur AWS Outpost

Suivez cette procédure pour déployer le pare-feu VM-Series sur un rack AWS Outpost. Si vous n'avez pas encore enregistré dans votre compte de support le code d'autorisation de capacité contenu dans l'e-mail de confirmation de commande que vous avez reçu, reportez-vous à la section Enregistrement du pare-feu VM-Series.

STEP 1 | Accédez à la console AWS Outpost.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Étendez votre VPC pour inclure votre rack AWS Outpost.

Le pare-feu VM-Series doit être en mesure de recevoir le trafic des instances EC2 et d'établir des communications entrantes et sortantes entre le VPC et Internet.

Reportez-vous à la documentation d'AWS Outpost pour obtenir des instructions sur la connexion de votre Outpost à votre VPC.

1. Vérifiez que les composants réseau et de sécurité sont définis de manière appropriée.
   - Activez la communication avec Internet. L'Outpost nécessite une passerelle locale pour se connecter à votre réseau local (LAN) et à Internet.
   - Créez un sous-réseau Outpost.
   - Si nécessaire, créez des groupes de sécurité pour gérer le trafic entrant et sortant des instances EC2/sous-réseaux.
   - Ajoutez des itinéraires à la table de routage pour un sous-réseau privé afin de vous assurer que le trafic peut être acheminé entre des sous-réseaux et des groupes de sécurité du VPC, le cas échéant.
2. Si vous souhaitez déployer une paire de pare-feu WM-Series en mode HA (haute disponibilité),vous devez définir les Rôles IAM pour la HA avant de pouvoir procéder à Haute disponibilité des pare-feu VM-Series sur AWS.
3. (Facultatif) Si vous utilisez l'amorçage pour effectuer la configuration de votre pare-feu VM-Series, reportez-vous à la section Amorçage du pare-feu VM-Series sur AWS. Pour plus d'informations sur l'amorçage, reportez-vous à la section Amorçage du pare-feu VM-Series.

STEP 3 | Lancez le pare-feu VM-Series.

Bien que vous puissiez ajouter d'autres interfaces réseau (ENI) au pare-feu VM-Series lors de son lancement, AWS libère l'adresse IP publique automatiquement attribuée à l'interface de gestion lors du redémarrage du pare-feu. Par conséquent, afin d'assurer la connectivité à l'interface de gestion, vous devez affecter une adresse IP élastique à l'interface de gestion avant d'associer d'autres interfaces au pare-feu.

Si vous souhaitez conserver les adresses EIP, vous pouvez affecter une adresse EIP à l'interface eth 1/1 et utiliser cette interface pour le trafic de gestion et le trafic de données. Pour restreindre les services autorisés sur l'interface ou limiter les adresses IP qui peuvent se connecter à l'interface eth 1/1, associez un profil de gestion à l'interface.

1. Sur le tableau de bord EC2, cliquez sur **Launch Instance (Lancer l'instance)**.
2. Sélectionnez l'AMI VM-Series. Pour obtenir l'AMI, reportez-vous à la section Obtention de l'AMI.
3. Lancez le pare-feu VM-Series sur une instance EC2.
   1. Choisissez le **EC2 instance type (Type d'instance EC2)** pour allouer les ressources nécessaires au pare-feu, puis cliquez sur **Next (Suivant)**. Reportez-vous à la section VM-Series sur système SDX : configuration système requise pour connaître les exigences de ressources.
   2. Sélectionnez le VPC.
   3. Sélectionnez le sous-réseau public sur Outpost auquel l'interface de gestion du pare-feu VM-Series sera liée.

©2023 Palo Alto Networks, Inc.

4. Sélectionnez **Automatically assign a public IP address (Affecter automatiquement une adresse IP publique)**. Cela vous permet d'obtenir une adresse IP accessible publiquement pour l'interface de gestion du pare-feu VM-Series.

   Vous pouvez lier une adresse IP élastique à l'interface de gestion ultérieurement. Contrairement à l'adresse IP publique qui est dissociée du pare-feu lorsque l'instance est fermée, l'adresse IP élastique est persistante et peut être reliée à une nouvelle instance (ou de remplacement) du pare-feu VM-Series sans reconfigurer l'adresse IP si vous devez y faire référence.
5. Sélectionnez **Launch as an EBS-optimized instance (Lancer en tant qu'instance optimisée EBS)**.

©2023 Palo Alto Networks, Inc.

6. Ajoutez une autre interface réseau pour les déploiements avec ELB afin de pouvoir permuter les interfaces de gestion et de données sur le pare-feu. La permutation des interfaces exige un minimum de deux ENI (eth0 et eth1).

   - Développez la section Interfaces réseau et cliquez sur **Add Device (Ajouter périphérique)** pour ajouter une autre interface réseau.

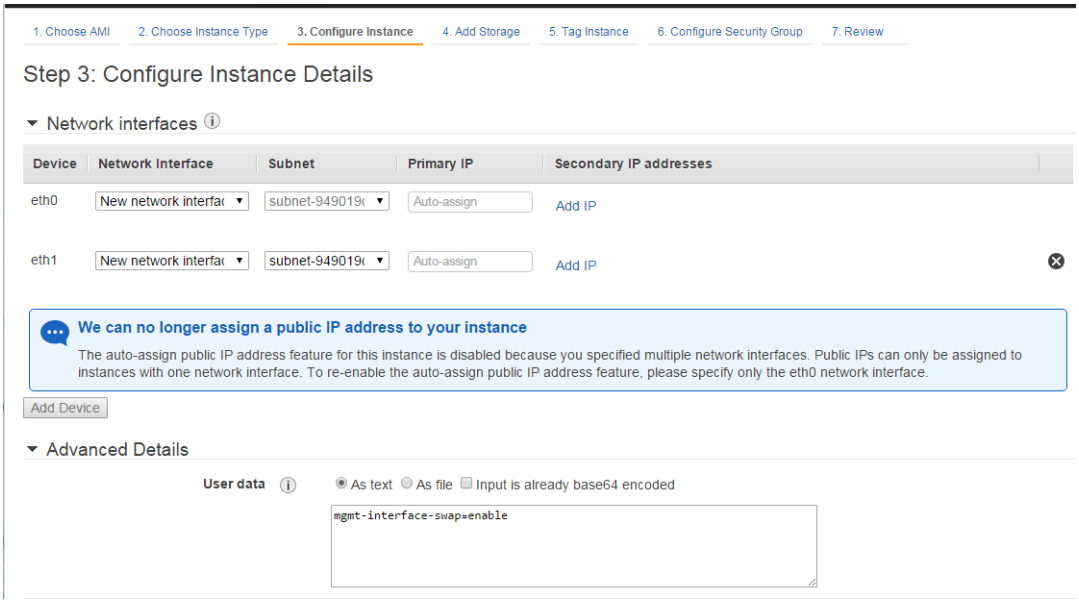
     Assurez-vous que votre VPC possède plus d'un sous-réseau afin de pouvoir ajouter des ENI supplémentaires au lancement.

     Si vous lancez le pare-feu avec une seule ENI :

     - *La commande de permutation d'interface entraînera le démarrage du pare-feu en mode maintenance.*
     - *Vous devez redémarrer le pare-feu lorsque vous ajoutez la deuxième ENI.*

   - Développez la section Détails avancés et dans le champ Données utilisateur saisissez le texte **`mgmt-interface-swap=enable`** pour effectuer la permutation d'interface durant le lancement.

     *Si vous amorcez le pare-feu, vous pouvez également saisir **`vmseries-bootstrap-aws-s3bucket=<bucketname>`** avec une virgule comme séparateur après **`mgmt-interface-swap=enable`**.*



7. Acceptez les paramètres de **Storage (Stockage)** par défaut. Le pare-feu utilise le type de volume SSD (gp2)

   Cette paire de clés est requise lorsque vous accédez pour la première fois au pare-feu. Elle est également nécessaire pour accéder au pare-feu en mode maintenance.

8. (Facultatif) **Tagging (Étiquetage)**. Ajoutez une ou plusieurs étiquettes pour créer vos propres métadonnées afin d'identifier et de grouper le pare-feu VM-Series. Par exemple,

 ©2023 Palo Alto Networks, Inc.

ajoutez une étiquette **Name (Nom)** avec une **Value (Valeur)** qui vous aide à vous souvenir que les interfaces ENI ont été permutées sur ce pare-feu VM-Series.

9. Sélectionnez un **Security Group (Groupe de sécurité)** existant ou créez-en un nouveau. Ce groupe de sécurité vise à limiter l'accès à l'interface de gestion du pare-feu. Vous devriez envisager d'au moins permettre l'accès https et ssh pour l'interface de gestion.
10. Lorsque vous y êtes invité, sélectionnez l'option **SSD** adaptée à votre configuration.
11. Sélectionnez **Review and Launch (Vérifier et lancer)**. Vérifiez que vos sélections sont correctes, puis cliquez sur **Launch (Lancer)**.
12. Sélectionnez une paire de clés existante ou créez-en une, et acceptez l'avis de non-responsabilité de la clé.
13. Téléchargez et enregistrez la clé privée dans un emplacement sûr ; l'extension de fichier est `.pem`. Vous ne pouvez pas régénérer cette clé en cas de perte.

    Le lancement du pare-feu VM-Series prend 5 à 7 minutes. Vous pouvez voir la progression sur le tableau de bord EC2. Une fois le processus terminé, le pare-feu VM-Series s'affiche sur la page **Instances** du tableau de bord EC2.

©2023 Palo Alto Networks, Inc.

STEP 4 | Configurez un nouveau mot de passe administratif pour le pare-feu.

Sur la CLI du pare-feu VM-Series, vous devez configurer un mot de passe d'administration unique avant de pouvoir accéder à l'interface Web du pare-feu. Pour vous connecter à la CLI, vous avez besoin de la clé privée que vous avez utilisée pour lancer le pare-feu.

1. Utilisez l'adresse IP publique vers SSH dans l'interface de ligne de commande (CLI) du pare-feu VM-Series. Vous aurez besoin de la clé privée utilisée ou créée dans 3 ci-dessus pour accéder à la CLI.

   Si vous avez ajouté une ENI supplémentaire pour prendre en charge les déploiements avec ELB, vous devez d'abord créer et affecter une adresse IP élastique à l'ENI pour accéder à la CLI (voir 6).

   Si vous utilisez PuTTY pour l'accès SSH, vous devez convertir le format .pem au format .ppk. Consultez https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html
2. Saisissez la commande suivante pour vous connecter au pare-feu :

   ssh-i <*private_key.pem*> admin@<*public-ip_address*>
3. Configurez un nouveau mot de passe à l'aide de la commande suivante, et suivez les invites affichées à l'écran :

   configure

   set mgt-config users admin password
4. Si votre licence de type BYOL doit être activée, définissez l'adresse IP du serveur DNS pour que le pare-feu puisse accéder au serveur de licences de Palo Alto Networks. Saisissez la commande suivante pour établir l'adresse IP du serveur DNS :

   set deviceconfig system dns-setting servers primary <*ip_address*>
5. Validez vos modifications à l'aide de la commande suivante :

   commit
6. Fermez la session SSH.

STEP 5 | Arrêtez le pare-feu VM-Series.

1. Sur le tableau de bord EC2, sélectionnez **Instances**.
2. Dans la liste, sélectionnez le pare-feu VM-Series, puis cliquez sur **Actions** > **Stop (Arrêter)**.

STEP 6 | Créez une adresse IP élastique (EIP) et affectez-la à l'ENI utilisée pour l'accès de gestion au pare-feu, puis redémarrez le pare-feu VM-Series.

1. Sélectionnez **Elastic IPs (IP élastiques)**, puis cliquez sur **Allocate New Address (Allouer une nouvelle adresse)**.
2. Sélectionnez **EC2-VPC**, puis cliquez sur **Yes, Allocate (Oui, allouer)**.
3. Sélectionnez la nouvelle EIP allouée, puis cliquez sur **Associate Address (Associer l'adresse)**.
4. Sélectionnez l'**Interface réseau** et l'**Adresse IP privée** associée à l'interface de gestion, puis cliquez sur **Oui, associer**.

 ©2023 Palo Alto Networks, Inc.

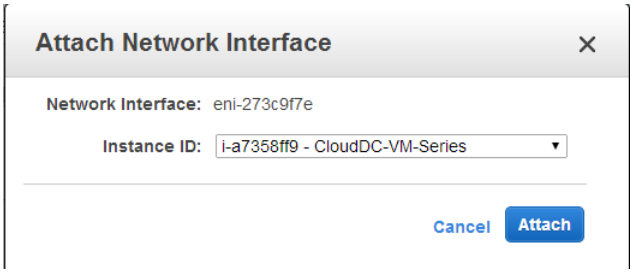
STEP 7 | Créez la ou les interface(s) réseau virtuel et associez-les(la) au pare-feu VM-Series. Les interfaces réseau virtuel sont appelées des interfaces réseau élastiques (ENI) dans AWS, et servent d'interfaces réseau du dataplane sur le pare-feu. Ces interfaces sont utilisées pour la gestion du trafic de données depuis/vers le pare-feu.

Vous aurez besoin d'au moins deux ENI qui autorisent le trafic entrant et sortant vers le pare-feu et depuis ce dernier. Vous pouvez ajouter jusqu'à sept ENI pour gérer le trafic de données sur le pare-feu VM-Series. Vérifiez le type de votre instance EC2 pour connaître le nombre maximum qu'il peut prendre en charge.

1. Sur le tableau de bord EC2, sélectionnez **Network Interfaces (Interfaces réseau)**, puis cliquez sur **Create Network Interface (Créer une interface réseau)**.
2. Donnez un nom descriptif à l'interface.
3. Sélectionnez le sous-réseau. Utilisez l'ID de sous-réseau pour vérifier que vous avez sélectionné le bon sous-réseau. Vous ne pouvez lier qu'une seule ENI à une instance d'un même sous-réseau.
4. Saisissez l'adresse **Private IP (IP privée)** pour l'affecter à l'interface ou sélectionnez **Auto-assign (Affectation automatique)** pour affecter automatiquement une adresse IP parmi les adresses IP disponibles du sous-réseau sélectionné.
5. Sélectionnez le **Security group (Groupe de sécurité)** contrôlant l'accès à l'interface réseau du dataplane.
6. Cliquez sur **Yes, Create (Oui, créer)**.



7. Pour associer l'ENI au pare-feu VM-Series, sélectionnez l'interface que vous venez de créer, puis cliquez sur **Attach (Associer)**.



8. Sélectionnez l'**Instance ID (ID d'instance)** du pare-feu VM-Series, puis cliquez sur **Attach (Associer)**.
9. Répétez les étapes ci-dessus pour créer et associer au moins une ENI supplémentaire au pare-feu.

 ©2023 Palo Alto Networks, Inc.

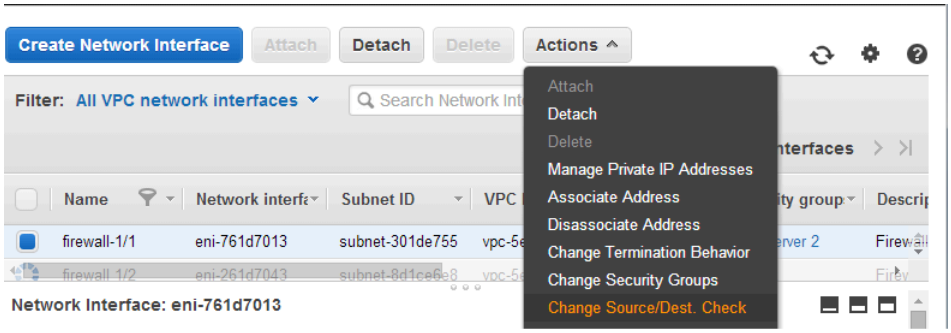
STEP 8 | (Non nécessaire pour la licence d'utilisation) Activez les licences sur le pare-feu VM-Series.

> ***Cette tâche n'est pas exécutée sur la console de gestion AWS. Accédez au portail de support de Palo Alto Networks et l'interface Web du pare-feu VM-Series est nécessaire pour l'activation de la licence.***

Reportez-vous à la section Activation de la licence.

STEP 9 | Désactivez la vérification de la source/destination sur chaque interface réseau du dataplane du pare-feu. La désactivation de cette option permet à l'interface de gérer le trafic réseau non destiné à l'adresse IP affectée à l'interface réseau.

1. Sur le tableau de bord EC2, sélectionnez l'interface réseau, eth1/1 par exemple, dans l'onglet **Network Interfaces** (Interfaces réseau).
2. Dans la liste déroulante **Action**, sélectionnez **Change Source/Dest. (Modifier la source/dest.) Check (Vérifier)** .



3. Cliquez sur **Disabled (Désactivé)** et **Save (Enregistrez)** vos modifications.
4. Répétez les étapes 1 à 3 pour chaque interface du dataplane du pare-feu.

STEP 10 | Configurez les interfaces réseau du plan de données en tant qu'interfaces de couche 3 sur le pare-feu.

Pour un exemple de configuration, reportez-vous aux étapes 14 à 17 dans Cas d'utilisation : Sécurisation des instances EC2 dans le cloud AWS.

> ***Sur les serveurs d'applications du VPC, définissez l'interface réseau du dataplane du pare-feu en tant que passerelle par défaut.***

1. Dans votre navigateur Web, connectez-vous de manière sécurisée (https) à l'aide de l'adresse EIP et du mot de passe que vous avez attribués lors de la configuration initiale

 ©2023 Palo Alto Networks, Inc.

(https://<Elastic_IP address>). Un avertissement de certificat s'affiche ; ne vous en préoccupez pas. Continuez vers la page Web.

2. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
3. Cliquez sur la liaison **ethernet 1/1** et configurez comme suit :
   - **Interface Type (Type d'interface)** : **Layer3 (Couche 3)**
   - Dans l'onglet **Config (Configuration)**, affectez l'interface au routeur par défaut.
   - Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Définissez une nouvelle zone, VM_Series_Non approuvée par exemple, puis cliquez sur **OK**.
   - Dans l'onglet **IPv4**, sélectionnez **Static (Statique)** ou **DHCP Client (Client DHCP)**.

     Si vous utilisez l'option **Static (Statique)**, cliquez sur **Add (Ajouter)** dans la section IP, puis saisissez l'adresse IP et le masque réseau pour l'interface, par exemple, 10.0.0.10/24.

     Assurez-vous que l'adresse IP correspond à l'adresse IP ENI que vous avez affectée précédemment.

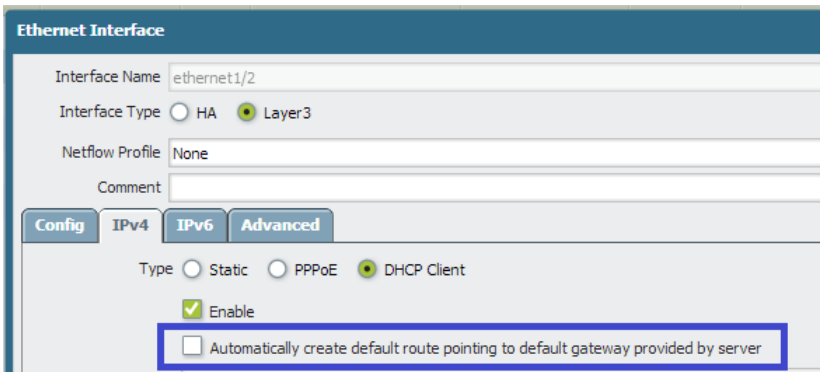
     Si vous utilisez DHCP, sélectionnez **DHCP Client (Client DHCP)** ; l'adresse IP privée que vous avez affectée à l'ENI dans la console de gestion AWS est automatiquement acquise.
4. Cliquez sur le lien pour **ethernet 1/2** et configurez-le comme suit :
   - **Interface Type (Type d'interface)** : **Layer3 (Couche 3)**
   - Zone de sécurité : VM_Series_Approuvée
   - **Adresse IP** : sélectionnez le bouton radio **Static** (Statique) ou **DHCP Client** (Client DHCP).

     Pour l'option Statique, cliquez sur **Add (Ajouter)** dans la section IP, puis saisissez l'adresse IP et le masque réseau pour l'interface. Assurez-vous que l'adresse IP correspond à l'adresse IP ENI associée que vous avez affectée précédemment.
5. Cliquez sur **Commit (Valider)**. Vérifiez que la liaison des interfaces est active.



*Pour l'option DHCP, décochez la case **Automatically create default route to default gateway provided by server** (Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur). Pour une interface associée au sous-réseau privé du VPC, la désactivation de cette option garantit que le trafic géré par cette interface n'est pas dirigé directement vers la passerelle Internet sur le VPC.*

 ©2023 Palo Alto Networks, Inc.



STEP 11 | Créez des règles NAT pour autoriser le trafic entrant et sortant des serveurs déployés dans le VPC.

1. Sélectionnez **Policies (Politiques)** > **NAT** sur l'interface Web du pare-feu.
2. Créez une règle NAT pour autoriser le trafic entre l'interface réseau du dataplane sur le pare-feu et l'interface serveur Web dans le VPC.
3. Créez une règle NAT pour autoriser l'accès sortant pour le trafic entre le serveur Web et Internet.

STEP 12 | Créez des politiques de sécurité pour autoriser/refuser le trafic vers les/des serveurs déployés dans le VPC.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** sur l'interface Web du pare-feu.
2. Cliquez sur **Add (Ajouter)**, puis spécifiez les zones, applications et options de journalisation que vous souhaitez exécuter afin de limiter et d'auditer le trafic traversant le réseau.

STEP 13 | Cliquez sur Commit (Valider) pour valider les modifications apportées au pare-feu.

Cliquez sur **Commit (Valider)**.

STEP 14 | Vérifiez que le pare-feu VM-Series sécurise le trafic et que les règles NAT sont appliquées.

1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)** sur l'interface Web du pare-feu.
2. Consultez les journaux pour vérifier que les applications sur le réseau sont conformes aux politiques de sécurité que vous avez mises en œuvre.

Création d'une AMI (Image de machine Amazon) personnalisée

Une AMI personnalisée VM-Series vous offre la cohérence et la flexibilité nécessaires pour déployer un pare-feu VM-Series avec la version de PAN-OS que vous souhaitez utiliser sur votre réseau au lieu de se limiter à l'utilisation d'une AMI publiée sur l'AWS public Marketplace ou sur l'AWS GovCloud Marketplace. L'utilisation d'une AMI personnalisée accélère le processus de déploiement d'un pare-feu avec la version de PAN-OS de votre choix, car elle réduit le temps nécessaire à la configuration du pare-feu avec une AMI publiée sur l'AWS public ou l'AWS GovCloud Marketplace, puis effectue des mises à niveau logicielles vers la version PAN-OS que vous avez qualifiée ou que vous souhaitez utiliser sur votre réseau. De plus, vous pouvez ensuite utiliser l'AMI personnalisée dans les modèles CloudFormation de pare-feu VM-Series de mise à l'échelle automatique ou dans tout autre modèle que vous avez créé.

©2023 Palo Alto Networks, Inc.

Vous pouvez créer une AMI personnalisée avec les licences BYOL, Bundle 1 (Forfait 1) ou Bundle 2 (Forfait 2). Le processus de création d'une AMI personnalisée nécessite que vous supprimiez toute la configuration du pare-feu et que vous restauriez les paramètres d'usine. Par conséquent, dans ce flux de travail, vous lancerez une nouvelle instance du pare-feu à partir de l'AWS Marketplace au lieu d'utiliser un pare-feu existant entièrement configuré.



Lorsque vous créez une AMI personnalisée avec une version BYOL du pare-feu, vous devez d'abord activer la licence sur le pare-feu afin de pouvoir accéder aux mises à jour logicielles PAN-OS et les télécharger pour mettre à niveau votre pare-feu, puis désactiver la licence sur le pare-feu avant de restaurer le pare-feu aux paramètres d'usine par défaut et créer l'AMI personnalisée. Si vous ne désactivez pas la licence, vous perdez la licence que vous avez appliquée sur cette instance de pare-feu.

STEP 1 | Lancez le pare-feu VM-Series depuis le Marketplace.

Reportez-vous à la section 3

STEP 2 | (Uniquement pour BYOL) Activez la licence.

STEP 3 | Installez les mises à jour logicielles et mettez à niveau le pare-feu avec la version de PAN-OS que vous prévoyez d'utiliser.

STEP 4 | (Uniquement pour BYOL) Désactivez la licence.

STEP 5 | Effectuez une réinitialisation des données privées.

Une réinitialisation des données privées supprime tous les journaux et restaure la configuration par défaut.

Les disques système ne sont pas effacés, de sorte que les mises à jour du contenu de l'étape 4 sont intactes.

1. Accédez à la CLI du pare-feu.
2. Supprimez tous les journaux et restaurez la configuration par défaut.

```
request system private-data-reset
```

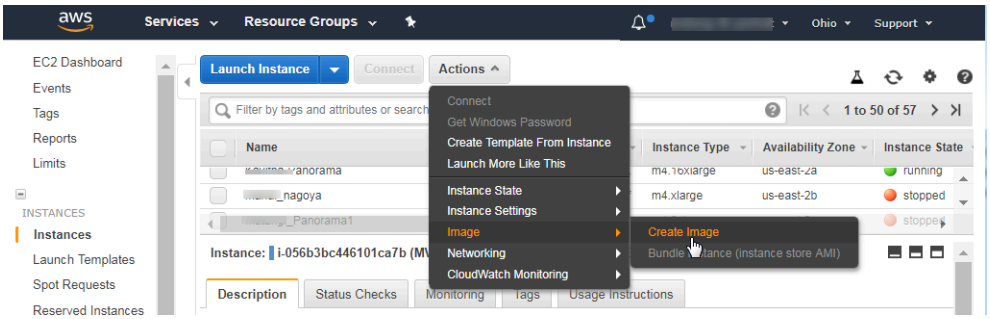
Appuyez sur **y** pour confirmer.

Le pare-feu redémarre pour initialiser la configuration par défaut.

 ©2023 Palo Alto Networks, Inc.

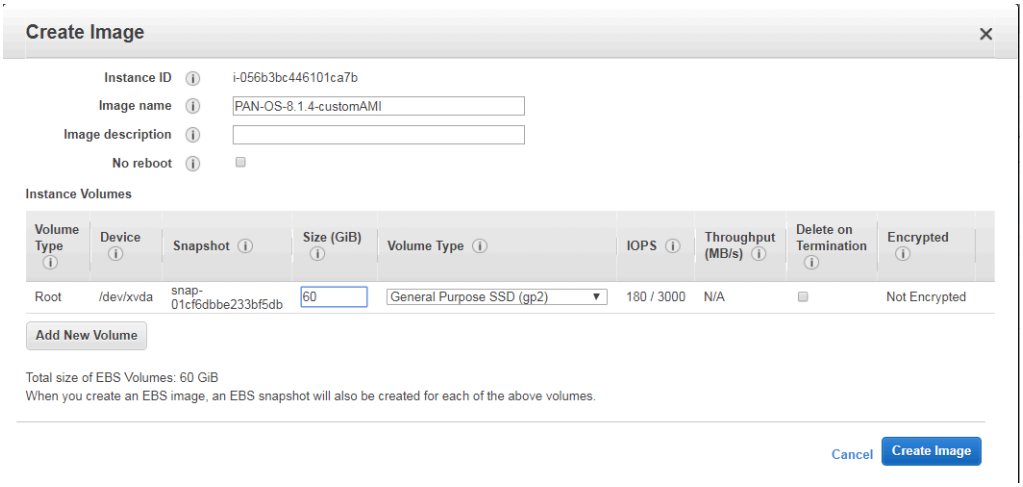
STEP 6 | Créez l'AMI personnalisée.

1. Connectez-vous à la console AWS et sélectionnez l'EC2 Dashboard (Tableau de bord EC2).
2. Cliquez sur **Stop** (Arrêter) pour arrêter le pare-feu VM-Series.
3. Sélectionnez l'instance de pare-feu VM-Series, puis cliquez sur **Image** > **Create Image (Créer une image)**.



4. Saisissez un nom d'image personnalisée, puis cliquez sur **Create Image** (Créer une image).

   L'espace disque requis de 60 Go est la configuration minimale requise.



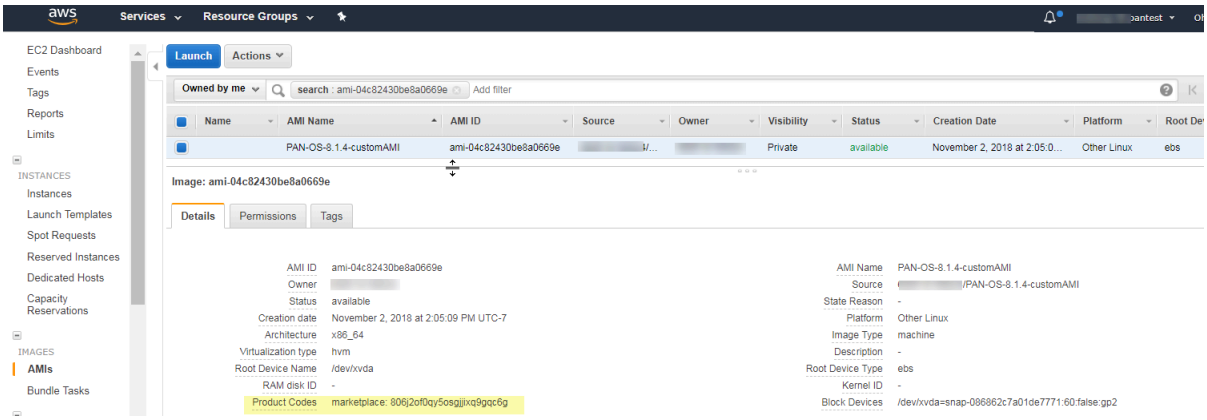
5. Vérifiez que l'AMI personnalisée est créée et que le code produit est correct.

   1. Sur l'EC2 Dashboard (Tableau de bord EC2), sélectionnez **AMI**.

   2. Sélectionnez l'AMI que vous venez de créer. Selon que vous avez sélectionné une AMI avec les options de licence BYOL, Bundle 1 (Forfait 1) ou Bundle 2 (Forfait 2), vous devez voir l'un des **Product Codes** (Codes produit) suivants dans les Details (Détails) :

   - BYOL : 6njl1pau431dv1qxipg63mvah
   - Forfait 1 : 6kxdw3bbmdeda3o6i1ggqt4km
   - Bundle 2—806j2of0qy5osgjjixq9gqc6g

©2023 Palo Alto Networks, Inc.



STEP 7 | Chiffrement du volume EBS pour le pare-feu VM-Series sur AWS.

Si vous envisagez d'utiliser l'AMI personnalisée avec le chiffrement EBS pour un déploiement de Mise à l'échelle automatique de pare-feu VM-Series avec le service Amazon ELB, vous devez utiliser la clé principale par défaut de votre compte AWS.

STEP 8 | Configurez le mot de passe administrateur sur le pare-feu.

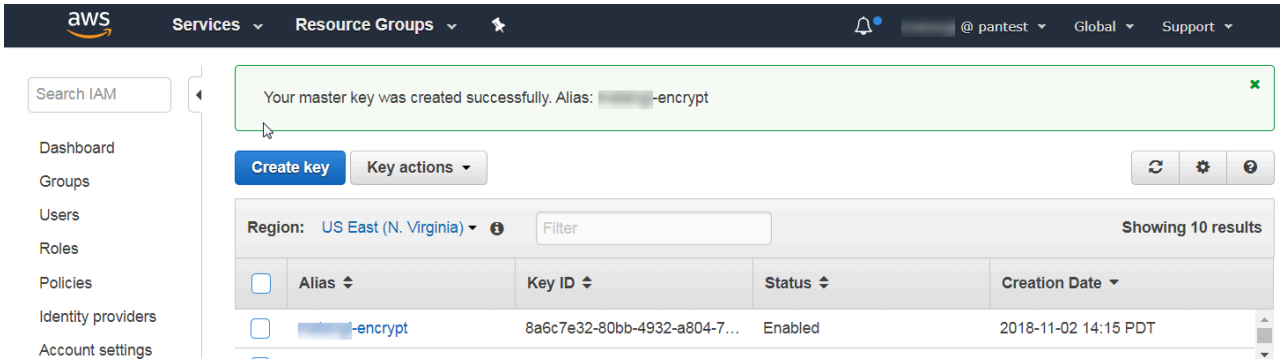
Reportez-vous à la section 4

Chiffrement du volume EBS pour le pare-feu VM-Series sur AWS

Le chiffrement EBS est disponible pour tous les Types d'instances AWS EC2 sur lesquels vous pouvez déployer le pare-feu VM-Series. Pour stocker en toute sécurité des données sur le pare-feu VM-Series sur AWS, vous devez d'abord créer une copie d'une AMI publiée sur l'AWS public ou sur GovCloud Marketplace, ou utiliser une AMI personnalisée, puis chiffrer le volume EBS avec une clé principale client (CMK) sur l'AWS KMS (Key Management Service). Vous pouvez utiliser la clé principale par défaut pour votre compte AWS ou toute clé CMK que vous avez précédemment créée à l'aide de l'AWS KMS (Key Management Service). EBS et KMS interagissent pour assurer la sécurité des données.

STEP 1 | Créez une clé de chiffrement sur AWS ou ignorez cette étape si vous souhaitez utiliser la clé principale par défaut pour votre compte.

Vous utiliserez cette clé pour chiffrer le volume EBS sur le pare-feu. Notez que la clé est spécifique à la région.

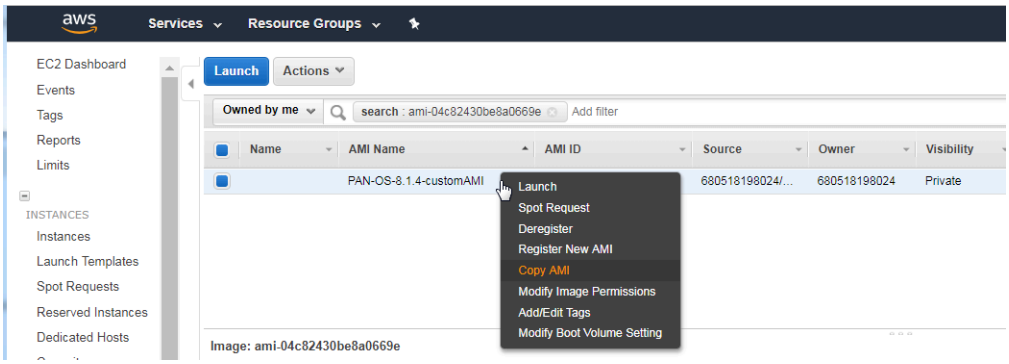


 ©2023 Palo Alto Networks, Inc.

STEP 2 | Utilisez la clé pour chiffrer le volume EBS sur le pare-feu.

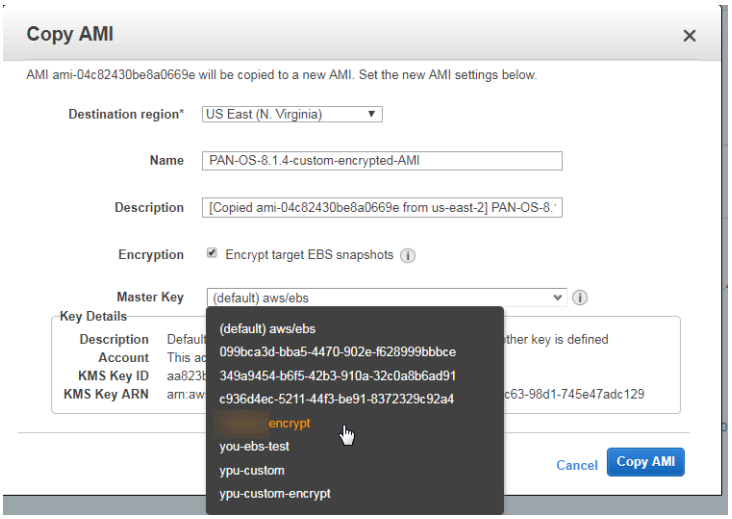
Vous devez créer une copie de l'AMI que vous souhaitez chiffrer. Vous pouvez copier une AMI publiée sur l'AWS public ou sur GovCloud Marketplace, ou utiliser une AMI personnalisée (Création d'une AMI (Image de machine Amazon) personnalisée).

1. Dans l'EC2 Dashboard (Tableau de bord EC2), sélectionnez l'AMI et **Copy AMI** (Copier l'AMI).



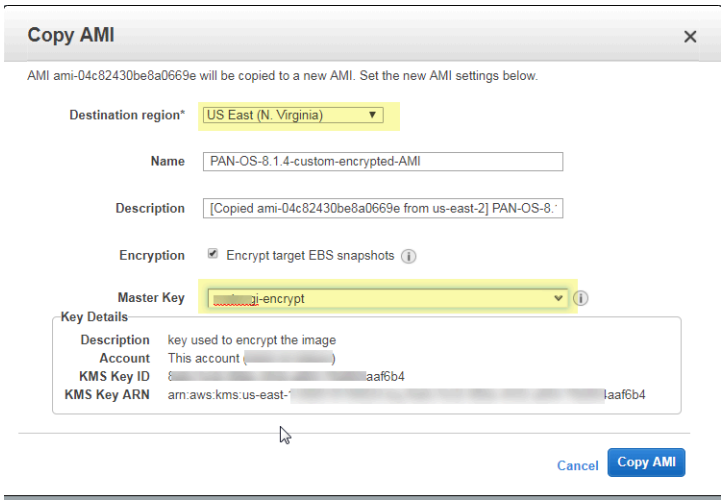
2. Définissez les détails de l'AMI.

   Assurez-vous de cocher la case **Encrypt target EBS snapshots (Chiffrer les instantanés EBS cibles)**.

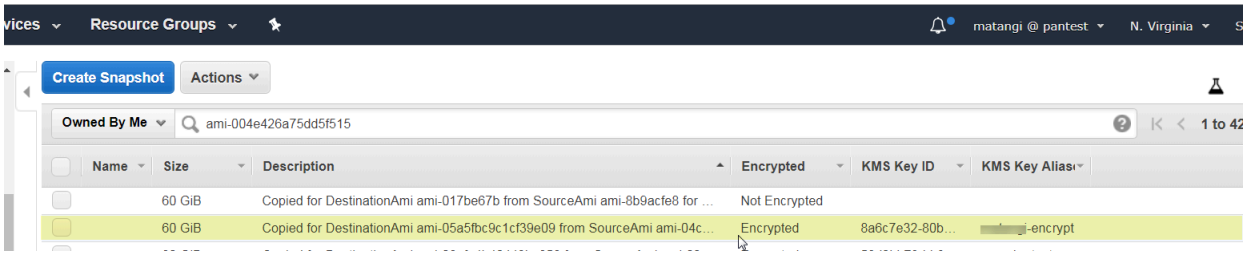


3. Sélectionnez la clé de chiffrement et **Copy AMI** (Copier l'AMI) pour créer un instantané EBS chiffré.

 ©2023 Palo Alto Networks, Inc.



4. Sélectionnez **EC2 Dashboard (Tableau de bord EC2)** > **Snapshots (Instantanés)** pour vérifier que l'instantané EBS est chiffré avec la clé que vous avez sélectionnée ci-dessus.



Utilisation de la CLI du pare-feu VM-Series pour permuter l'interface de gestion

Si vous n'avez pas permuté l'interface de gestion (MGT) avec l'interface du dataplane (ethernet 1/1) lors du déploiement du pare-feu, vous pouvez utiliser la CLI pour permettre au pare-feu de recevoir le trafic du dataplane sur l'interface principale après le lancement du pare-feu.

STEP 1 | Suivez les étapes 1 à 7 dans Lancement du pare-feu VM-Series sur AWS.

> ***Avant de continuer, vérifiez que le pare-feu possède au moins deux ENI (eth0 et eth1). Si vous lancez le pare-feu avec une seule ENI, la commande de permutation d'interface provoquera l'amorçage du pare-feu en mode maintenance.***

STEP 2 | Sur le tableau de bord EC2, consultez l'adresse IP de l'interface eth1 et vérifiez que les règles du groupe de sécurité AWS autorisent les connexions (HTTPS et SSH) à la nouvelle interface de gestion (eth1).

STEP 3 | Connectez-vous à la CLI du pare-feu VM-Series et saisissez la commande suivante :

```
set system setting mgmt-interface-swap enable yes
```

STEP 4 | Confirmez que vous voulez permuter l'interface et utiliser l'interface du dataplane eth1 comme interface de gestion.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Redémarrez le pare-feu pour que la permutation prenne effet. Utilisez la commande suivante :

```
request restart system
```

STEP 6 | Vérifiez que les interfaces ont été permutées. Utilisez la commande suivante :

```
debug show vm-series interfaces all Phoenix_interface   Base-
OS_port   Base-OS_MAC        PCI-ID         Driver mgt(interface-
swap) eth0   0e:53:96:91:ef:29   0000:00:04.0   ixgbevf Ethernet1/1
           eth1    0e:4d:84:5f:7f:4d       0000:00:03.0   ixgbevf
```

Activation de la surveillance CloudWatch sur le pare-feu VM-Series

Le pare-feu VM-Series sur AWS peut publier des métriques PAN-OS natives dans AWS CloudWatch que vous pouvez utiliser pour surveiller les pare-feu. Ces métriques vous permettent d'évaluer les performances et les modèles d'utilisation que vous pouvez utiliser pour entreprendre des actions pour le lancement ou l'arrêt des instances des pare-feu VM-Series.

Les pare-feu utilisent les APIs AWS pour publier les métriques dans un ***espace de noms***, qui est l'endroit sur AWS où les métriques sont collectées à un intervalle de temps spécifié. Lorsque vous configurez les pare-feu pour publier des métriques dans AWS CloudWatch, il existe deux espaces de noms dans lesquels vous pouvez afficher les métriques : l'espace de noms principal collecte et regroupe les métriques sélectionnées pour toutes les instances configurées pour utiliser l'espace de noms, et l'espace de noms secondaire qui est automatiquement créé avec le suffixe `_dimensions` vous permet de filtrer les métriques en utilisant le nom d'hôte et les métadonnées (ou ***dimensions***) de l'ID d'instance AWS et d'obtenir une visibilité sur l'utilisation et les performances de chaque pare-feu VM-Series.

Vous pouvez surveiller la métrique dans CloudWatch ou créer des règles de mise à l'échelle automatique pour déclencher des alarmes et entreprendre une action pour déployer manuellement une nouvelle instance lorsque la métrique surveillée atteint la valeur de seuil indiquée. Reportez-vous à la documentation AWS CloudWatch et Groupes de mise à l'échelle automatique (ASG) qui porte sur les meilleures pratiques pour définir les conditions d'alarme pour une action de mise à l'échelle (augmentation ou diminution).

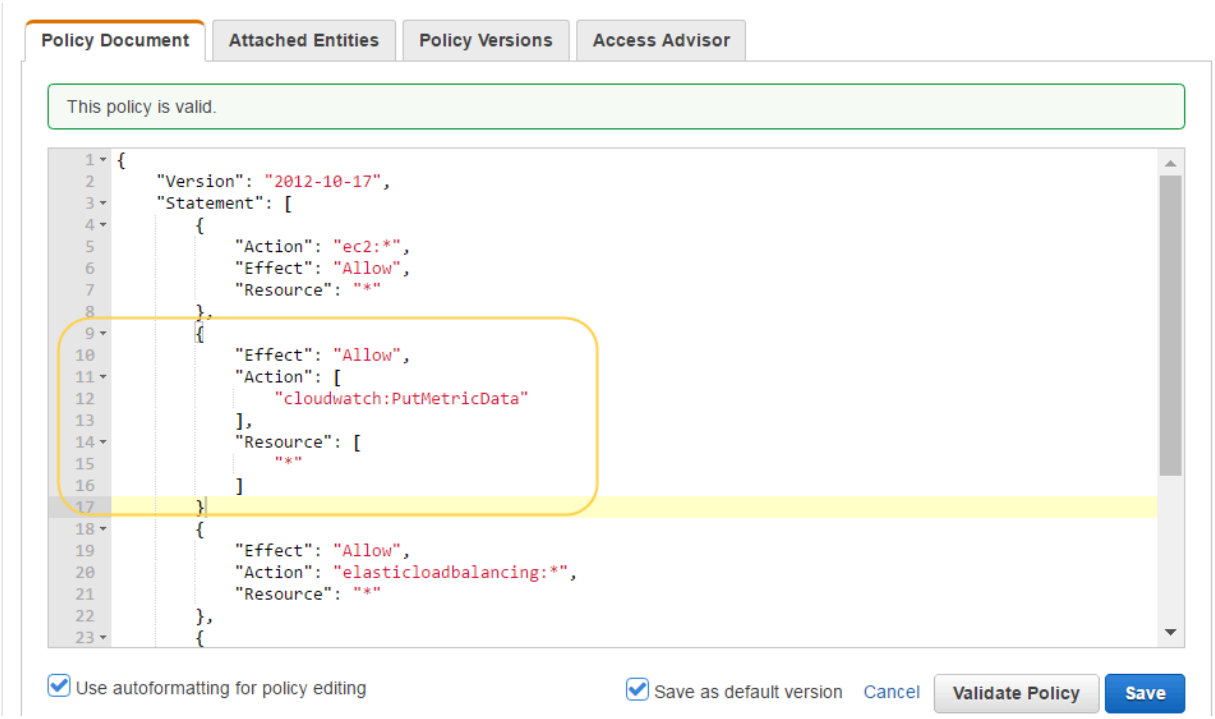
Pour obtenir une description des statistiques PAN-OS que vous pouvez publier sur CloudWatch, consultez la rubrique Statistiques PAN-OS personnalisées publiées pour la surveillance.

©2023 Palo Alto Networks, Inc.

STEP 1 | Affectez les autorisations appropriées au rôle d'utilisateur Identity and Access Management (IAM) AWS que vous utilisez pour déployer le pare-feu VM-Series sur AWS.

Que vous lanciez une nouvelle instance du pare-feu VM-Series ou que mettiez à niveau un pare-feu VM-Series existant sur AWS, le rôle IAM associé à votre instance doit disposer des autorisations nécessaires pour publier des métriques sur CloudWatch.

1. Sur la console AWS, sélectionnez IAM.
2. Modifiez le rôle IAM afin d'accorder les autorisations suivantes :



Vous pouvez copier et coller les autorisations ici :

```
 { "Version": "2012-10-17", "Statement": [ { "Effect":
"Allow", "Action": [ "cloudwatch:PutMetricData" ],
"Resource": [ "*" ] } ] }
```

STEP 2 | Activez CloudWatch sur le pare-feu VM-Series sur AWS.

1. Connectez-vous à l'interface Web sur le pare-feu VM-Series
2. Sélectionnez **Device (Appareil)** > **VM-Series**.
3. Dans AWS CloudWatch Setup (Configuration d'AWS CloudWatch), cliquez sur **Edit (Modifier)** ( ) et sélectionnez **Enable CloudWatch Monitoring (Activer la surveillance CloudWatch)**.

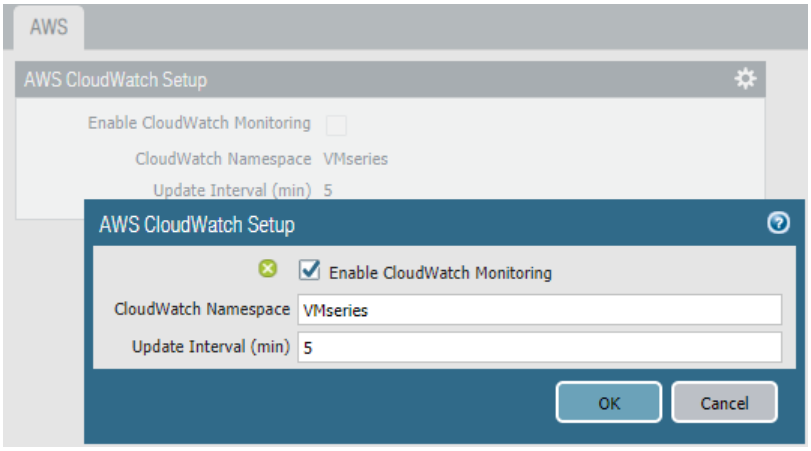
   1. Saisissez le **CloudWatch Namespace (Espace de noms CloudWatch)** auquel le pare-feu peut publier des métriques. L'espace de nommage ne peut pas commencer avec le **AWS**.

      Les métriques agrégées pour tous les pare-feu VM-Series dans une paire HA ou un déploiement à mise à l'échelle automatique sont publiées dans l'espace de noms que vous avez saisi ci-dessus. L'espace de noms avec le suffixe `_dimensions` qui est automatiquement créé vous permet de filtrer et de visualiser les métriques pour un

©2023 Palo Alto Networks, Inc.

pare-feu VM-Series spécifique en utilisant le nom d'hôte ou les métadonnées d'ID d'instance AWS attachées au pare-feu.

2. Modifiez l'**Update Interval (Intervalle de mise à jour)** à une valeur comprise entre 1 et 60 minutes. Il s'agit de la fréquence à laquelle le pare-feu publie les métriques dans CloudWatch. La valeur par défaut est de 5 minutes.



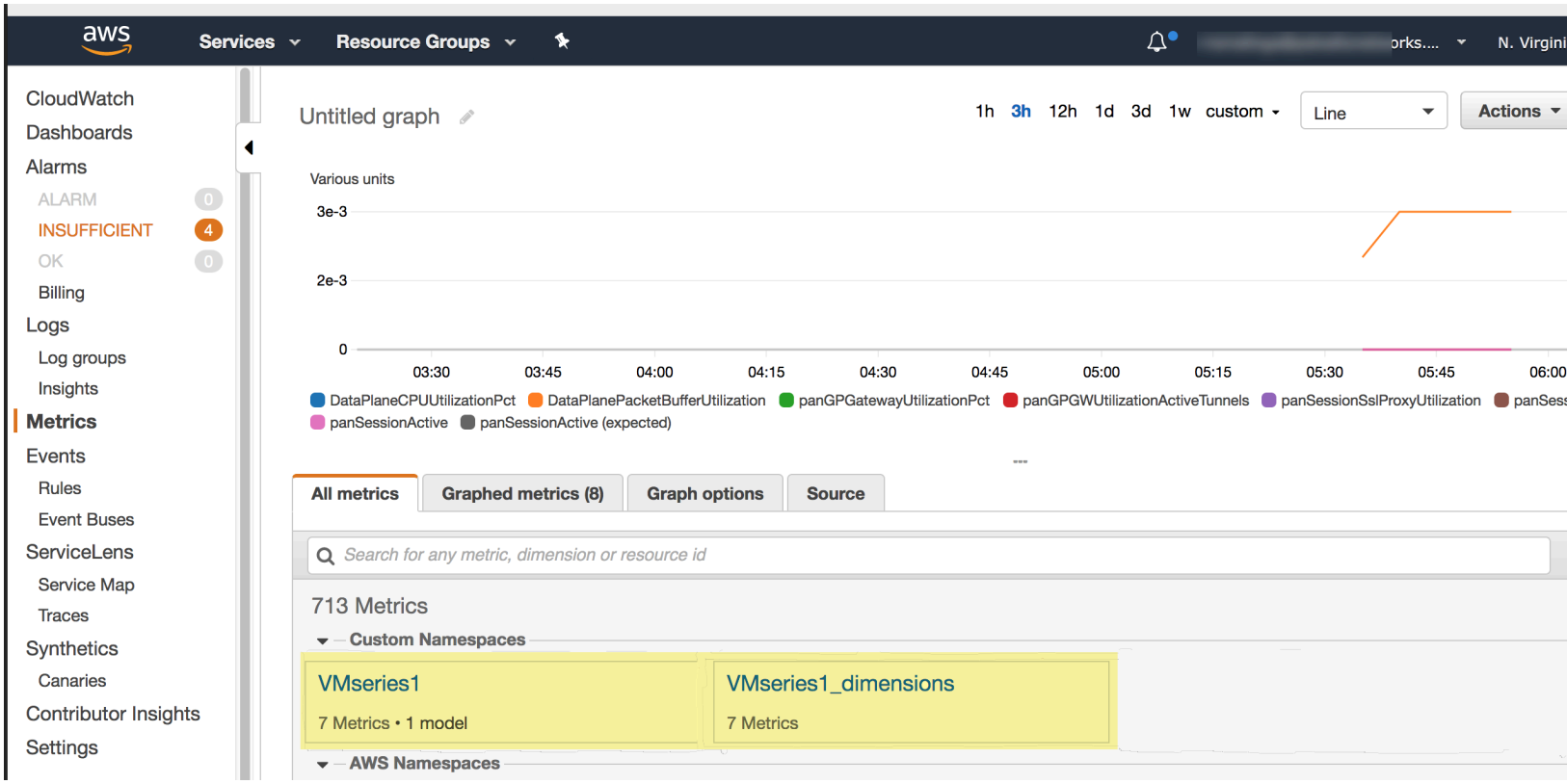
4. **Commit (Validez)** les modifications.

   Tant que le pare-feu ne commence pas à publier des métriques sur CloudWatch, vous ne pouvez pas configurer d'alarmes pour les métriques PAN-OS.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Vérifiez que vous pouvez voir les métriques sur CloudWatch.

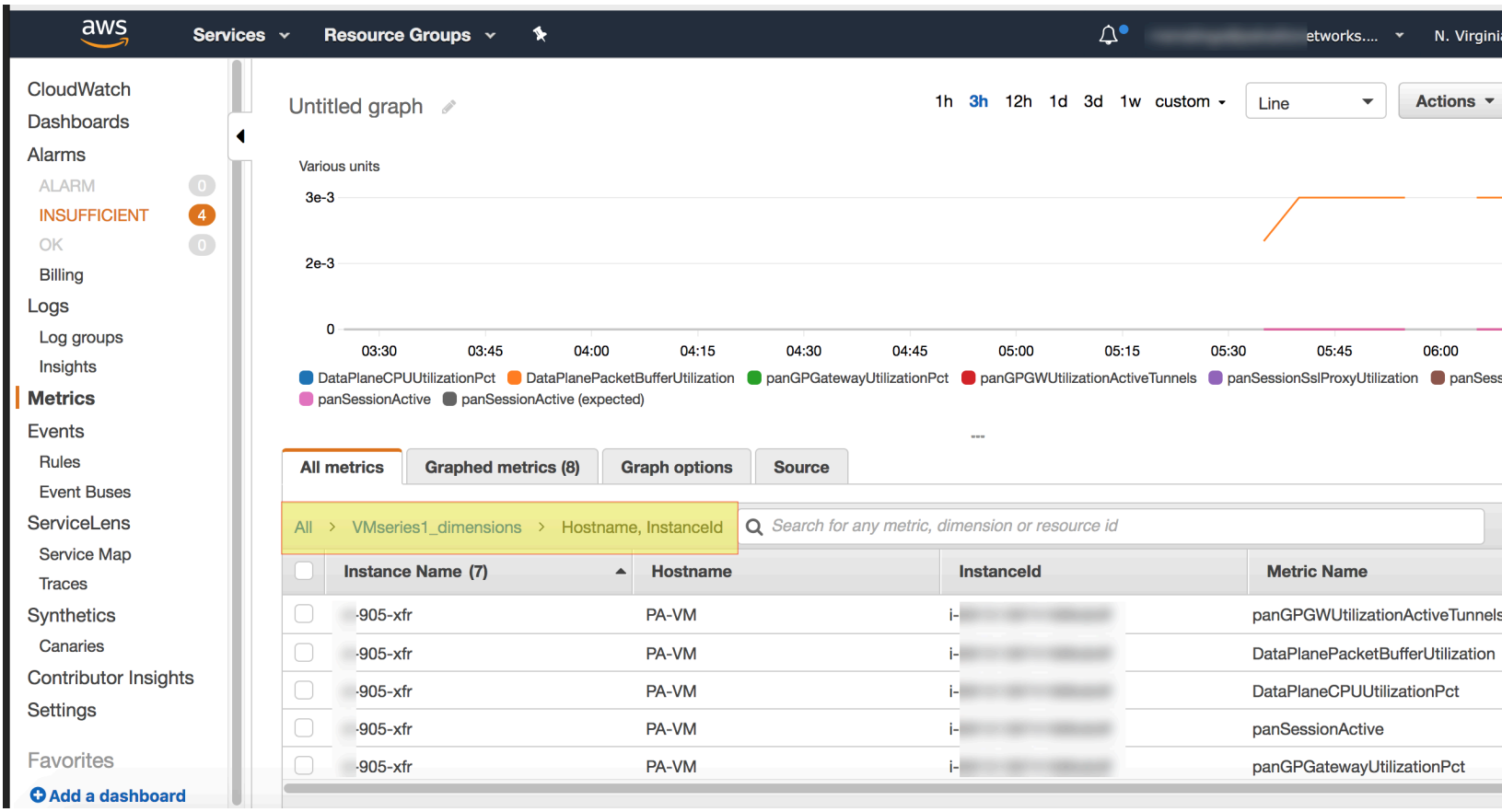
1. Sur la console AWS, sélectionnez **CloudWatch** > **Metrics (Métriques)** pour afficher les métriques CloudWatch par catégorie.
2. Dans la liste déroulante Custom Metrics (Métriques personnalisées), sélectionnez l'espace de noms.



3. Vérifiez que vous pouvez voir les métriques de PAN-OS dans la liste d'affichage.

   Pour filtrer par nom d'hôte ou ID d'instance AWS d'un pare-feu spécifique, sélectionnez `_dimensions`.

 ©2023 Palo Alto Networks, Inc.



STEP 4 | Configurez les alarmes et l'action pour les métriques PAN-OS sur CloudWatch.

Reportez-vous à la documentation d'AWS suivante : http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html

Un pare-feu VM-Series avec configuration d'amorçage prendra environ 7 à 9 minutes pour être disponible pour le service. Voici donc quelques exemples sur la façon de définir les alarmes qui déclenchent la mise à l'échelle automatique du pare-feu VM-Series :

- Si vous avez déployé 2 instances des pare-feu VM-Series en tant que passerelles Global Protect qui sécurisent les utilisateurs distants, utilisez la métrique GlobalProtect Gateway Active Tunnels (Tunnels actifs). Vous pouvez configurer une alarme lorsque le nombre de tunnels actifs est supérieur à 300 pendant 15 minutes. Vous pouvez déployer 2 nouvelles instances du pare-feu VM-Series qui sont amorcées et configurées pour servir de passerelles Global Protect.
- Si vous utilisez le pare-feu pour sécuriser vos charges de travail dans AWS, utilisez la métrique Session Utilization (Utilisation des sessions) pour mettre à l'échelle (augmenter ou diminuer) le pare-feu en fonction de l'utilisation des ressources. Vous pouvez configurer une alarme lorsque cette métrique est supérieure à 60 % pendant 15 minutes, afin de déployer une instance du pare-feu de l'instance VM-Series. Et inversement, si l'utilisation des sessions est inférieure à 50 % pendant 30 minutes, fermez une instance du pare-feu VM-Series.

©2023 Palo Alto Networks, Inc.

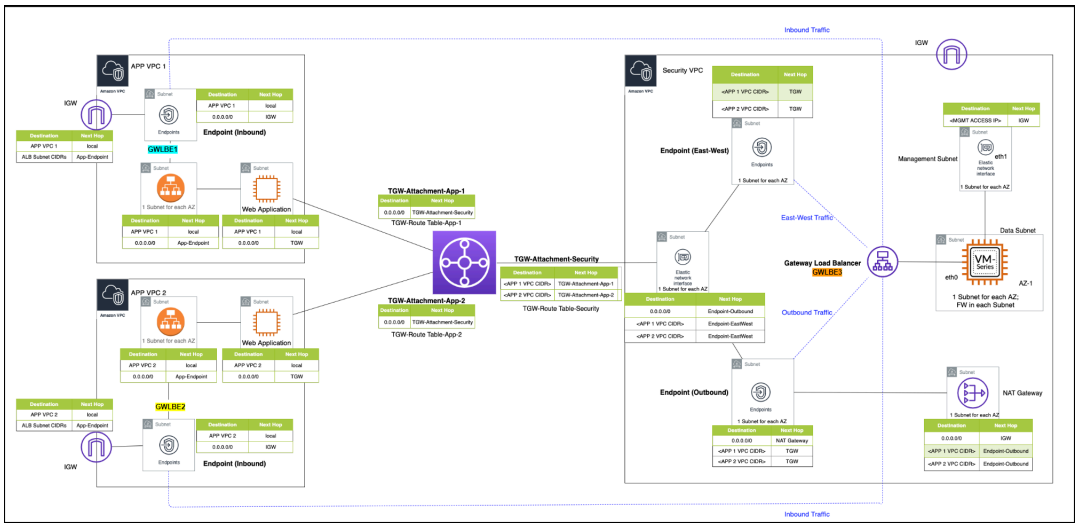
Intégration VM-Series avec un équilibreur de charge de passerelle AWS

L'équilibreur de charge de passerelle AWS (GWLB) est un service géré AWS qui vous permet de déployer une pile de pare-feu VM-Series et de fonctionner de manière évolutive horizontalement et tolérante aux pannes. Vous pouvez ensuite exposer le GWLB AWS avec la pile de pare-feu en tant que service de terminal VPC pour l'inspection du trafic et la prévention des menaces. En créant des terminaux d'équilibreur de charge de passerelle (GWLBE) pour le service de terminal VPC, vous pouvez facilement insérer une pile de pare-feu VM-Series de mise à l'échelle automatique dans les chemins de trafic sortant, est-ouest et entrant de vos applications. Les pare-feu VM-Series et le GWLB utilisent l'encapsulation GENEVE pour garder les en-têtes de paquets de trafic et la charge utile intacts, ce qui permet d'offrir une visibilité complète de l'identité de la source à vos applications.

Le pare-feu VM-Series** prend en charge le décryptage **lorsqu'il est déployé derrière un GWLB pour les cas d'utilisation avants et entrants, y compris TLS1.2 et TLS1.3 utilisant les chiffrements DHE/ECDHE.

Le déploiement du pare-feu VM-Series derrière un GWLB nécessite que vous configuriez la** passerelle de transit AWS**.

L'image ci-dessous décrit comment l'intégration du GWLB avec VM-Series simplifie vos environnements de passerelle de transit AWS (TGW). Vous associez un VPC de sécurité centralisé à votre passerelle de transit. Le VPC de sécurité centralisé comprend un GWLB pour mettre à l'échelle et équilibrer la charge du trafic à travers la pile de pare-feu VM-Series.



Pour que le pare-feu VM-Series puisse inspecter le trafic qui est acheminé entre les attachements de VPC, vous devez activer le mode appareil sur l'attachement de VPC de la passerelle de transit pour le VPC de sécurité contenant le pare-feu VM-Series. Vous pouvez activer le mode appareil à l'aide de la commande :

```
modify-transit-gateway-vpc-attachment --transit-gateway-attachment-id
 <value> --options ApplianceModeSupport=enable
```


©2023 Palo Alto Networks, Inc.

Pour plus d'instructions, reportez-vous à l'activation du mode appareil.

Cela garantit que le trafic bidirectionnel est acheminé de manière symétrique : le trafic de requête et de réponse est dirigé vers le même terminal de passerelle dans le VPC du pare-feu et le GWLB maintiendra la persistance vers le même pare-feu VM-Series pour l'inspection avant de continuer vers la bonne destination.

Lorsqu'il est déployé avec un GWLB, vous pouvez utiliser le pare-feu VM-Series pour protéger les éléments suivants :

- Trafic entrant : trafic provenant de l'extérieur du VPC et destiné aux ressources de votre VPC d'application, telles que les serveurs Web. Les pare-feu VM-Series empêchent les logiciels malveillants et les vulnérabilités de pénétrer sur le réseau dans le trafic autorisé par les groupes de sécurité AWS.
- Trafic sortant : trafic provenant des VPC d'application et destiné à des ressources externes sur Internet. Les pare-feu VM-Series protègent les flux de trafic sortant en s'assurant que les charges de travail des VPC d'application se connectent aux services autorisés (tels que Windows Update) et aux catégories d'URL autorisées, et en empêchant l'exfiltration de données sensibles. En outre, les profils de sécurité VM-Series empêchent les logiciels malveillants et les vulnérabilités de pénétrer sur le réseau dans le trafic de retour.
- Trafic est-ouest : dans un environnement de passerelle de transit, le trafic est-ouest désigne le trafic inter-VPC, tel que le trafic entre les charges de travail source et destination dans deux VPC d'application différents. Les pare-feu VM-Series protègent les flux de trafic est-ouest contre la propagation de logiciels malveillants.

Pour protéger le trafic entrant vers vos VPC d'application :

1. Créez des terminaux GWLBE (GWLBE1 et GWLBE2 dans la figure ci-dessus) ayant des sous-réseaux distincts associés dans vos VPC en étoile. Assurez-vous de disposer de sous-réseaux distincts pour les terminaux GWLB, ALB et l'attachement de la passerelle d'application et de transit dans le VPC d'application.
2. Ajoutez des tables de routage dans le VPC d'application (en plus de l'itinéraire local du VPC) comme suit :
    1. Table de routage avec association périphérique de l'IGW : ajoutez un itinéraire destiné à ALB avec le GWLBE comme cible.
    2. Table de routage avec association du sous-réseau ALB : ajoutez un itinéraire destiné à 0.0.0.0/0 avec le GWLBE comme cible.
    3. Table de routage avec association du sous-réseau GWLBE : ajoutez un itinéraire destiné à 0.0.0.0/0 avec l'IGW comme cible.

Une fois ces itinéraires en place, le trafic entrant arrivant à l'IGW du VPC est acheminé vers le GWLBE. Le GWLBE transfère le trafic au GWLB qui, à son tour, envoie le trafic au pare-feu VM-Series dans le VPC de sécurité pour inspection. Le pare-feu renvoie le trafic de requête au GWLBE du VPC d'application, qui transfère ensuite le trafic à l'application via ALB. Le trafic de réponse à cette requête est envoyé par ALB vers le GWLBE d'application qui envoie ensuite le trafic au GWLB. Le GWLB envoie à son tour le trafic au pare-feu VM-Series. Après avoir inspecté le trafic de réponse, le pare-feu renvoie le trafic de réponse au GWLBE qui, à son tour, envoie le trafic à l'IGW.

Pour protéger le trafic sortant des VPC d'application :

 ©2023 Palo Alto Networks, Inc.

1. Créez un GWLBE (GWLBE3 dans la figure ci-dessus) dans le VPC de pare-feu centralisé. Assurez-vous de disposer de sous-réseaux distincts pour le terminal GWLB, l'attachement de la passerelle de transit et la passerelle NAT dans le VPC de sécurité.
2. Créez une passerelle NAT dans le VPC de sécurité.
3. Ajoutez des tables de routage comme suit :
    1. Table de routage avec association du sous-réseau d'application :ajoutez un itinéraire destiné à 0.0.0.0/0 avec la TGW comme cible. Cela s'ajoute à l'itinéraire local du VPC.
    2. Tables de routage dans le VPC de sécurité :
        - Table de routage avec association du sous-réseau d'attachement de TGW : en plus de l'itinéraire local du VPC, ajoutez un itinéraire destiné à 0.0.0.0/0 avec le GWLBE3 comme cible.
        - Table de routage avec association du sous-réseau GWLBE : en plus de l'itinéraire local du VPC, ajoutez un itinéraire destiné à 0.0.0.0/0 avec la passerelle NAT comme cible. Ajoutez un itinéraire destiné aux CIDR du VPC d'application avec la TGW comme cible.
        - Table de routage avec association du sous-réseau de passerelle NAT : en plus de l'itinéraire local du VPC, ajoutez un itinéraire destiné à 0.0.0.0/0 avec l'IGW comme cible. Ajoutez un itinéraire destiné aux CIDR du VPC d'application avec le GWLBE3 comme cible.
    3. Ajoutez des tables de routage de passerelle de transit comme suit :
        - Table de routage avec association de l'attachement de TGW de VPC App1-1 : ajoutez un itinéraire destiné à 0.0.0.0/0 avec l'attachement de TGW du VPC de sécurité comme ID d'attachement.
        - Table de routage avec association de l'attachement de TGW de VPC App2-2 : ajoutez un itinéraire destiné à 0.0.0.0/0 avec l'attachement de TGW du VPC de sécurité comme ID d'attachement.
        - Table de routage avec association de l'attachement de TGW de VPC de sécurité : (a) Ajoutez un itinéraire destiné au CIDR de VPC App-1 avec l'attachement de TGW de VPC d'Application-1 comme ID d'attachement. (b) Ajoutez un itinéraire destiné au CIDR de VPC App-2 avec l'attachement de TGW de VPC d'Application-2 comme ID d'attachement.

Une fois cette configuration en place, le trafic sortant initié par l'Application(App1) est envoyé à la TGW et la TGW le transfère au sous-réseau du VPC de sécurité. Le trafic est ensuite acheminé vers le GWLBE de sécurité (GWLBE3) qui envoie le trafic au pare-feu VM-Series pour inspection via le GWLB. Le pare-feu VM-Series renvoie le trafic au GWLBE3 après inspection et le GWLBE3 transfère le trafic à la passerelle NAT qui envoie le trafic via l'IGW. De même, le trafic de réponse passe par la passerelle NAT vers le GWLBE3, le pare-feu VM-Series et la TGW, après quoi il est réacheminé vers l'application.

Le trafic Est-Ouest est également géré avec les itinéraires et la configuration décrits dans les étapes ci-dessus. Lorsque le trafic est envoyé de l'App1 à l'App2, le trafic passe par la TGW qui achemine le trafic vers le GWLBE3. Le GWLBE3 transfère le trafic au pare-feu VM-Series via le GWLB. Le pare-feu VM-Series renvoie le paquet au GWLBE3 après inspection. Le GWLBE3 transfère ensuite le paquet à l'App2 via la TGW. Le trafic de réponse de l'App-2 à l'App-1 empruntera le chemin inverse.



Il est recommandé que tous les sous-réseaux se trouvent dans la même zone de disponibilité pour éviter des frais de trafic interzone.

 ©2023 Palo Alto Networks, Inc.

Intégration manuelle de VM-Series avec un équilibreur de charge de passerelle

Consultez les rubriques suivantes pour intégrer manuellement le pare-feu VM-Series avec un équilibreur de charge de passerelle AWS.

- Possibilité d'intégration VM-Series avec un équilibreur de charge de passerelle
- Intégration manuelle VM-Series avec un équilibreur de charge de passerelle
- (Facultatif) Association d'un terminal VPC à une interface VM-Series
- (Facultatif) Activation du routage de superposition pour le VM-Series sur AWS

Possibilité d'intégration VM-Series avec un équilibreur de charge de passerelle

Lors de l'intégration du pare-feu VM-Series à un équilibreur de charge de passerelle (GWLB), vous devez d'abord activer le pare-feu VM-Series pour qu'il traite correctement le trafic redirigé vers le pare-feu par les terminaux GWLB. Vous pouvez activer cette fonctionnalité en utilisant la CLI du pare-feu VM-Series, par le biais de l'ensemble d'amorçage VM-Series ou via le champ de données utilisateur de la console AWS.

Le déploiement du pare-feu VM-Series avec un GWLB nécessite :

- PAN-OS 10.0.2 ou version ultérieure
- Plugin VM-Series 2.0.2 ou version ultérieure
- Panorama 10.0.2 ou version ultérieure si vous utilisez Panorama pour gérer vos pare-feu

Le tableau ci-dessous énumère les commandes nécessaires pour permettre l'inspection du trafic du GWLB avec un terminal VPC. Les commandes d'opération peuvent être utilisées dans le fichier init-cfg.txt d'amorçage ou dans le champ de données utilisateur de la console AWS.

Paramètre d'amorçage	Commande de la CLI	Description
op-command-modes=mgmt-interface-swap	op-command-modes=mgmt-interface-swap ***Cette commande exige que le pare-feu redémarre avant de prendre effet.***	Permute eth0 et eth1. GWLB par défaut, envoie le trafic uniquement à Eth0 de ses instances cibles. En permutant, Eth0 devient l'interface de données et eth1 devient l'interface de gestion.
plugin-op-commands=aws-gwlb-inspect:enable	request plugins vm_series aws gwlb inspect enable <yes/no>	Permet au pare-feu VM-Series de traiter le trafic traversant un GWLB.

Intégration manuelle VM-Series avec un équilibreur de charge de passerelle

Suivez la procédure suivante pour intégrer manuellement votre pare-feu VM-Series sur AWS avec un équilibreur de charge de passerelle (GWLB).

©2023 Palo Alto Networks, Inc.

Si vous associez des terminaux VPC à une interface ou à des sous-interfaces via des données utilisateur pendant l'amorçage et que votre fichier bootstrap.xml n'inclut pas la configuration de l'interface, vous pouvez configurer les interfaces après le démarrage du pare-feu.

STEP 1 | Définissez le VPC de sécurité. Reportez-vous à la documentation d'AWS pour plus d'informations sur la création de votre VPC de sécurité.

- Créez deux sous-réseaux :un pour la gestion et un pour les données.
- Créez deux groupes de sécurité : un pour la gestion du pare-feu et un pour les données.
- Les groupes de sécurité du sous-réseau de gestion doivent autoriser https et ssh pour l'accès à la gestion.
- Assurez-vous que le ou les groupes de sécurité de votre VPC de données autorisent les paquets encapsulés GENEVE (port UDP 6081).
- Si votre déploiement comprend une passerelle de transit et du trafic qui se déplacera entre les VPC, vous devez activer le mode appareil sur l'attachement de sécurité VPC.

Le groupe cible du GWLB ne peut pas utiliser HTTP pour les contrôles de santé car le pare-feu VM-Series ne permet pas l'accès avec un protocole non sécurisé. Utilisez plutôt un autre protocole tel que HTTPS ou TCP.

STEP 2 | Lancez le pare-feu VM-Series.

1. Sur le tableau de bord EC2, cliquez sur **Launch Instance (Lancer l'instance)**.
2. Sélectionnez l'AMI VM-Series Palo Alto. Pour obtenir l'AMI, reportez-vous à la section Obtention de l'AMI.
3. Lancez le pare-feu VM-Series sur une instance EC2.
   1. Choisissez le **EC2 instance type (Type d'instance EC2)** pour allouer les ressources nécessaires au pare-feu, puis cliquez sur **Next (Suivant)**. Reportez-vous à la section Configuration système requise pour VM-Series pour connaître les exigences en matière de ressources.
   2. Sélectionnez le VPC de sécurité.
   3. Sélectionnez le sous-réseau de données à associer à eth0.

©2023 Palo Alto Networks, Inc.

4. Ajoutez une autre interface réseau pour que eth1 agisse comme interface de gestion après la permutation d'interface. La permutation des interfaces exige un minimum de deux ENI (eth0 et eth1).

   - Développez la section Network Interfaces (Interfaces réseau) et cliquez sur **Add Device (Ajouter un périphérique)** pour ajouter une autre interface réseau et configurer le sous-réseau Management (Gestion) pour cette interface.

     Assurez-vous que votre VPC possède plus d'un sous-réseau afin de pouvoir ajouter des ENI supplémentaires au lancement.

     Si vous lancez le pare-feu avec une seule ENI :

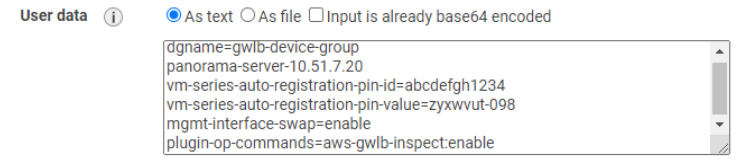
     - *La commande de permutation d'interface entraînera le démarrage du pare-feu en mode maintenance.*
     - *Vous devez redémarrer le pare-feu lorsque vous ajoutez la deuxième ENI.*

   - Développez la section Advanced Details (Détails avancés) et, dans le champ **Données utilisateur**, saisissez le texte pour effectuer la permutation d'interface durant le lancement.

     `mgmt-interface-swap=enable`

     `plugin-op-commands=aws-gwlb-inspect:enable`

     Si vous définissez le type de cible sur l'adresse IP d'une interface spécifique du pare-feu VM-Series, il n'est pas nécessaire d'activer la permutation de l'interface de gestion.



5. Acceptez les paramètres de **Storage (Stockage)** par défaut. Le pare-feu utilise le type de volume SSD (gp2).
6. Lorsque vous y êtes invité, sélectionnez l'option **SSD** adaptée à votre configuration.
7. (Facultatif) **Tagging (Étiquetage)**. Ajoutez une ou plusieurs étiquettes pour créer vos propres métadonnées afin d'identifier et de grouper le pare-feu VM-Series. Par exemple,

©2023 Palo Alto Networks, Inc.

ajoutez une étiquette **Name (Nom)** avec une **Value (Valeur)** qui vous aide à vous souvenir que les interfaces ENI ont été permutées sur ce pare-feu VM-Series.

8. Sélectionnez le **Security Group (Groupe de sécurité)** de données pour eth0 (interface de données). Autorisez le trafic sur le port UDP 6081.

   Si vous activez les contrôles de santé au niveau du pare-feu, vous ne pouvez pas utiliser HTTP. Utilisez plutôt un autre protocole tel que HTTPS ou TCP.

9. Sélectionnez **Review and Launch (Vérifier et lancer)**. Vérifiez que vos sélections sont correctes, puis cliquez sur **Launch (Lancer)**.

10. Sélectionnez une paire de clés existante ou créez-en une, et acceptez l'avis de non-responsabilité de la clé.

    Cette paire de clés est requise lorsque vous accédez pour la première fois au pare-feu. Elle est également nécessaire pour accéder au pare-feu en mode maintenance.

11. Téléchargez et enregistrez la clé privée dans un emplacement sûr ; l'extension de fichier est `.pem`. Vous ne pouvez pas régénérer cette clé en cas de perte.

    Le lancement du pare-feu VM-Series prend 5 à 7 minutes. Vous pouvez voir la progression sur le tableau de bord EC2. Une fois le processus terminé, le pare-feu VM-Series s'affiche sur la page **Instances** du tableau de bord EC2.

STEP 3 | Associez le groupe de sécurité de gestion à eth1 (interface de gestion). Autorisez ssh et https. Reportez-vous à la documentation d'AWS pour plus d'informations.

STEP 4 | Créez une adresse IP élastique (EIP) et affectez-la à l'ENI utilisée pour l'accès de gestion (eth1) au pare-feu.

1. Sélectionnez **Elastic IPs (IP élastiques)**, puis cliquez sur **Allocate New Address (Allouer une nouvelle adresse)**.
2. Sélectionnez **EC2-VPC**, puis cliquez sur **Yes, Allocate (Oui, allouer)**.
3. Sélectionnez la nouvelle EIP allouée, puis cliquez sur **Associate Address (Associer l'adresse)**.
4. Sélectionnez l'**Interface réseau** et l'**Adresse IP privée** associée à l'interface de gestion, puis cliquez sur **Oui, associer**.

©2023 Palo Alto Networks, Inc.

STEP 5 | Configurez un nouveau mot de passe administratif pour le pare-feu.

Sur la CLI du pare-feu VM-Series, vous devez configurer un mot de passe d'administration unique avant de pouvoir accéder à l'interface Web du pare-feu. Pour vous connecter à la CLI, vous avez besoin de la clé privée que vous avez utilisée pour lancer le pare-feu.

1. Utilisez l'EIP vers SSH dans l'interface de ligne de commande (CLI) du pare-feu VM-Series. Vous aurez besoin de la clé privée utilisée ou créée ci-dessus et utilisant le nom d'utilisateur **admin** pour accéder à la CLI.

   Si vous utilisez PuTTY pour l'accès SSH, vous devez convertir le format .pem au format .ppk. Consultez https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html
2. Saisissez la commande suivante pour vous connecter au pare-feu :

   ssh-i *<private_key.pem>* admin@*<public-ip_address>*
3. Configurez un nouveau mot de passe à l'aide de la commande suivante, et suivez les invites affichées à l'écran :

   configure

   set mgt-config users admin password
4. Si votre licence de type BYOL doit être activée, définissez l'adresse IP du serveur DNS pour que le pare-feu puisse accéder au serveur de licences de Palo Alto Networks. Saisissez la commande suivante pour établir l'adresse IP du serveur DNS :

   set deviceconfig system dns-setting servers primary *<ip_address>*
5. Validez vos modifications à l'aide de la commande suivante :

   commit
6. Fermez la session SSH.

STEP 6 | Configurez l'interface réseau du plan de données en tant qu'interface de couche 3 sur le pare-feu.

Sur les serveurs d'applications du VPC, définissez l'interface réseau du dataplane du pare-feu en tant que passerelle par défaut.

1. Dans votre navigateur Web, connectez-vous de manière sécurisée (https) à l'aide de l'adresse EIP et du mot de passe que vous avez attribués lors de la configuration initiale

 ©2023 Palo Alto Networks, Inc.

(https://<Elastic_IP address>). Un avertissement de certificat s'affiche ; ne vous en préoccupez pas. Continuez vers la page Web.

2. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
3. Cliquez sur la liaison **ethernet 1/1** et configurez comme suit :
   - **Interface Type (Type d'interface)** : **Layer3 (Couche 3)**
   - Dans l'onglet **Config (Configuration)**, affectez l'interface au routeur virtuel par défaut.
   - Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Définissez une nouvelle zone et laissez les champs restants avec des valeurs par défaut, puis cliquez sur **OK**.
   - Dans l'onglet **IPv4**, sélectionnez **DHCP Client (Client DHCP)**.

     Si vous utilisez DHCP, sélectionnez **DHCP Client (Client DHCP)** ; l'adresse IP privée que vous avez affectée à l'ENI dans la console de gestion AWS est automatiquement acquise.
   - Dans l'onglet Advanced (Avancé), créez un profil de gestion pour activer le service HTTP dans le cadre de la création de profil de gestion et autoriser les sondes de contrôle de santé à partir de GWLB.
4. Cliquez sur **Commit (Valider)**. Vérifiez que l'état de liaison de l'interface est actif.

STEP 7 | Créer des politiques de sécurité pour autoriser/refuser le trafic.

Comme VM-Series traite le trafic comme intra-zone lorsqu'il est intégré à un GWLB, une règle intra-zone par défaut autorise tout le trafic. Il est recommandé de remplacer la règle intra-zone par défaut par une action de refus pour le trafic qui ne correspond à aucune autre règle de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** sur l'interface Web du pare-feu.
2. Cliquez sur **Add (Ajouter)**, puis spécifiez les zones de sécurité, applications et options de journalisation que vous souhaitez exécuter afin de limiter et d'auditer le trafic traversant le réseau.

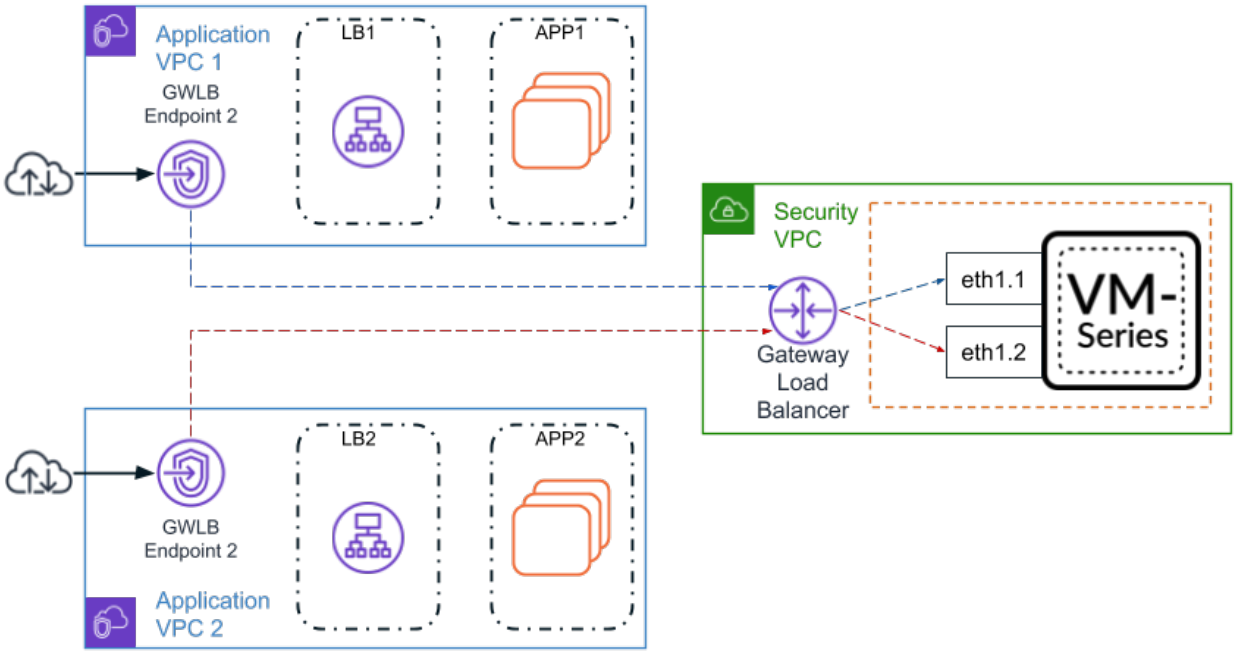
STEP 8 | Cliquez sur **Commit (Valider)** pour valider les modifications apportées au pare-feu.

Association d'un terminal VPC à une interface VM-Series

Vous pouvez associer un ou plusieurs terminaux VPC à une interface ou une sous-interface du pare-feu VM-Series. Vous pouvez assurer une application cohérente des politiques en associant tous les terminaux d'un même VPC à la même sous-interface sur le pare-feu. Ou, si votre déploiement comporte des VPC dont les adresses IP se superposent, vous pouvez associer les points terminaux de différents VPC à différentes sous-interfaces pour une application différenciée des politiques.

L'association d'un VPC à une interface ou une sous-interface n'est pas obligatoire pour intégrer le pare-feu VM-Series à un GWLB.

©2023 Palo Alto Networks, Inc.



Vous pouvez configurer des interfaces et associer un VPC à des interfaces de pare-feu en utilisant les méthodes suivantes :

- Ajoutez la configuration de l'interface dans votre fichier **`bootstrap.xml`** et les commandes d'association dans le fichier **`init-cfg.txt`** ou les données utilisateur AWS.
- Après avoir déployé le pare-feu, configurez manuellement vos interfaces et utilisez le CLI du pare-feu pour associer vos VPC aux interfaces.

Vous pouvez associer plusieurs terminaux VPC à une seule interface sur le pare-feu VM-Series. Cependant, vous devez associer chaque terminal VPC individuellement. Par exemple, pour associer le terminal VPC 1 et le terminal VPC 2 à la sous-interface ethernet1/1.2, vous devez exécuter la commande d'association séparément pour chaque terminal VPC.

Le tableau ci-dessous décrit les commandes utilisées pour associer un VPC à une interface. Vous pouvez inclure la commande operation dans votre fichier **`init-cfg.txt`** ou dans les données utilisateur AWS.

Paramètre d'amorçage	Commande de la CLI	Description
plugin-op-commands= aws-gwlb-associate-vpce:<vpce-id>@ethernet<subinterface>	request plugins vm_series aws gwlb associate vpc-endpoint <vpce-id> interface <subinterface>	Associe un terminal VPC à une interface ou une sous-interface sur le pare-feu. L'interface spécifiée est affectée à une zone de sécurité.
—	request plugins vm_series aws gwlb disassociate vpc-endpoint <vpce-id> interface <subinterface>	Dissocie un terminal VPC à une interface ou une sous-interface sur le pare-feu. L'interface spécifiée

©2023 Palo Alto Networks, Inc.

Paramètre d'amorçage	Commande de la CLI	Description
		est affectée à une zone de sécurité.
—	show plugins vm_series aws gwlb	Affiche l'état de fonctionnement du pare-feu en ce qui concerne le déploiement de votre GWLB. Il n'affiche pas la configuration du pare-feu. Par exemple, si vous configurez une association à une interface qui n'existe pas, cette association est configurée mais ne fait pas partie de l'état de fonctionnement. Par conséquent, elle n'est pas affichée.

Lorsque vous associez un terminal VPC en utilisant le fichier d'amorçage init-cfg.txt ou les données utilisateur AWS, vous pouvez lister plusieurs interfaces ou sous-interfaces ensemble. Toutes les commandes doivent être sur une seule ligne dans une liste séparée par des virgules et sans espace, comme le montre l'exemple suivant.

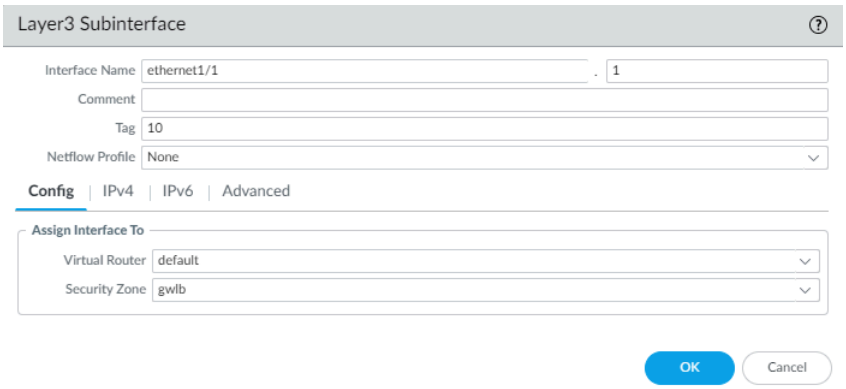
```
plugin-op-commands=aws-gwlb-inspect:enable,aws-gwlb-associate-
vpce:vpce-0913731043b5c0ebc@ethernet1/1.1,aws-gwlb-associate-
vpce:vpce-08207ccb4cb23a1de@ethernet1/1.1,aws-gwlb-associate-
vpce:vpce-07b66cca88821d6e1@ethernet1/1.2,aws-gwlb-associate-
vpce:vpce-0a9a583fdb928492b@ethernet1/1.3
```

Si vous utilisez des sous-interfaces pour séparer le trafic, créez une sous-interface pour chaque VPC et associez-la à un VPC.

©2023 Palo Alto Networks, Inc.

STEP 1 | Configurez la sous-interface.

1. Connectez-vous à l'interface Web du pare-feu.
2. Sélectionnez **Network (Réseau)** > **Interface**.
3. Choisissez **ethernet1/1** et cliquez sur **Add Subinterface (Ajouter une sous-interface)**.
4. Saisissez un suffixe numérique (1 à 9 999) pour identifier la sous-interface.
5. Saisissez une **étiquette VLAN** (1 à 4 094) de la sous-interface. Ce champ est obligatoire mais le VLAN n'est pas utilisé.
6. Sélectionnez **Virtual Router (routeur virtuel – VR)** comme valeur par défaut.
7. Sélectionnez une **Security Zone (Zone de sécurité)**.
8. Dans l'onglet **IPv4**, définissez le **Type** sur **DHCP Client (Client DHCP)**.
9. Cliquez sur **OK**.
10. Répétez cette commande pour chaque terminal VPC.



STEP 2 | Associez l'interface à un terminal VPC.

1. Connectez-vous au CLI du pare-feu.
2. Exécutez la commande suivante :

   request plugins vm_series aws gwlb associate vpc-endpoint <vpce-id> interface <subinterface>

   Par exemple :

   request plugins vm_series aws gwlb associate vpc-endpoint vpce-02c4e6g8ha97h7e39 interface ethernet1/1.4

   Vous pouvez localiser l'identifiant du terminal VPC dans la console AWS.

3. Répétez cette commande pour chaque association d'interface et terminal VPC.

STEP 3 | Vérifiez votre interface avec les associations de terminaux VPC.

show plugins vm_series aws gwlb

```
GWLB enabled: True Overlay Routing: False
 ------------------------------------------------------------ VPC
 endpoint Interface
 ------------------------------------------------------------
```

 ©2023 Palo Alto Networks, Inc.

```
vpce-0aeb1a919bd4ae609 ethernet1/1.1 vpce-0294375bfe413f04a
ethernet1/1.2
```

STEP 4 | Si nécessaire, vous pouvez utiliser la commande suivante pour dissocier un terminal VPC d'une interface.

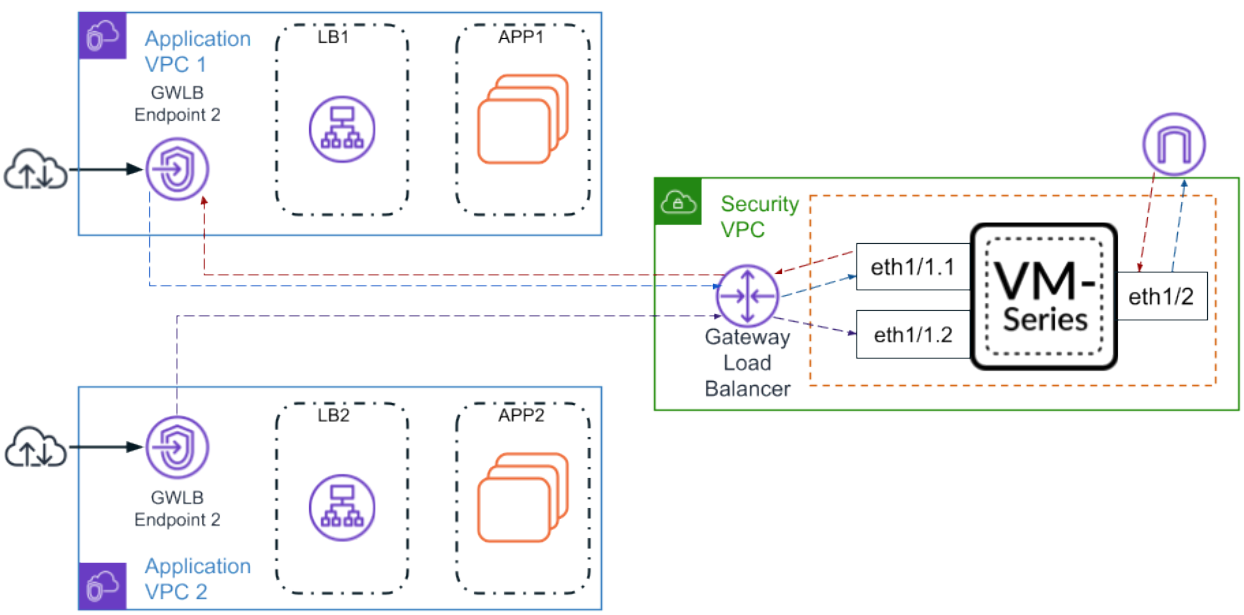
```
request plugins vm_series aws gwlb disassociate vpc-endpoint <vpce-
id> interface <subinterface>
```

Activation du routage de superposition pour le VM-Series sur AWS

Le routage de superposition nécessite PAN-OS 10.0.5 ou une version ultérieure.

En utilisant le routage de superposition dans votre intégration de pare-feu VM-Series, l'AWS GWLB vous permet d'utiliser une politique à deux zones pour inspecter le trafic sortant de votre environnement AWS. Cela permet aux paquets de quitter le pare-feu VM-Series via une interface différente de celle par laquelle ils sont entrés.

Lorsque le routage de superposition est configuré, le pare-feu est capable d'effectuer une recherche d'itinéraire de couche 3 dans l'en-tête interne d'un paquet. Si la destination est la même que l'interface d'entrée, le paquet sera dirigé normalement. Tous les futurs paquets de la session sont traités comme vwire ; comme si le routage de superposition n'était pas activé. Si le paquet va vers une destination sortante, le pare-feu désencapsule le paquet et le transmet à la passerelle IGW ou NAT. Lorsque le paquet revient, le pare-feu réapplique l'encapsulation.



Utilisez la procédure suivante pour activer le routage de superposition.

STEP 1 | Avant de commencer, assurez-vous de créer des sous-réseaux différents pour les interfaces approuvées et non approuvées.

©2023 Palo Alto Networks, Inc.

STEP 2 | Intégration manuelle VM-Series avec un équilibreur de charge de passerelle.

STEP 3 | (Facultatif) Association d'un terminal VPC à une interface VM-Series.

STEP 4 | Utilisez la commande CLI de routage de superposition. Cette commande CLI n'est pas requise si vous avez inclus la commande opérationnelle de routage de superposition dans les données utilisateur AWS ou dans le fichier d'amorçage init-cfg.txt.

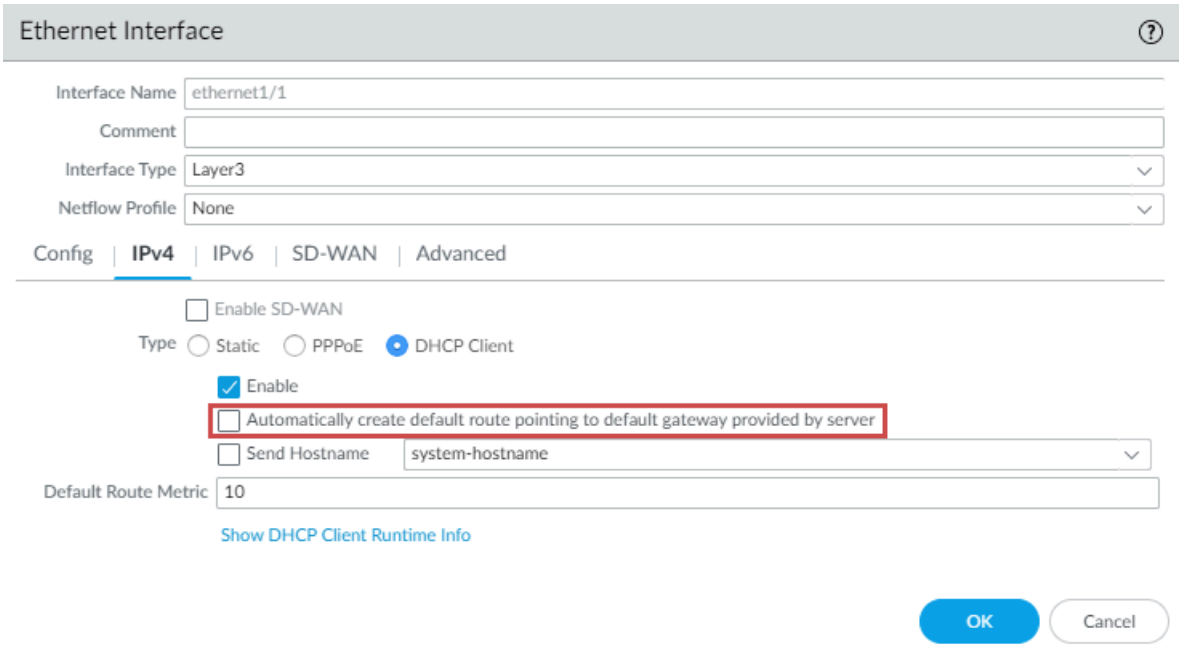
1. Connectez-vous à l'interface de ligne de commande du pare-feu.
2. Exécutez la commande suivante.

```
request plugins vm_series aws gwlb overlay-routing enable yes
```

STEP 5 | Connectez-vous à l'interface Web du pare-feu.

STEP 6 | Désactivez **Automatically create default route pointing to default gateway provided by server (Créer automatiquement une route par défaut pointant en direction de la passerelle par défaut fournie par le serveur)** sur l'interface (d'entrée) approuvée.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
2. Cliquez sur votre interface approuvée puis sur l'onglet IPv4.
3. Désélectionnez **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)**.
4. Cliquez sur OK.



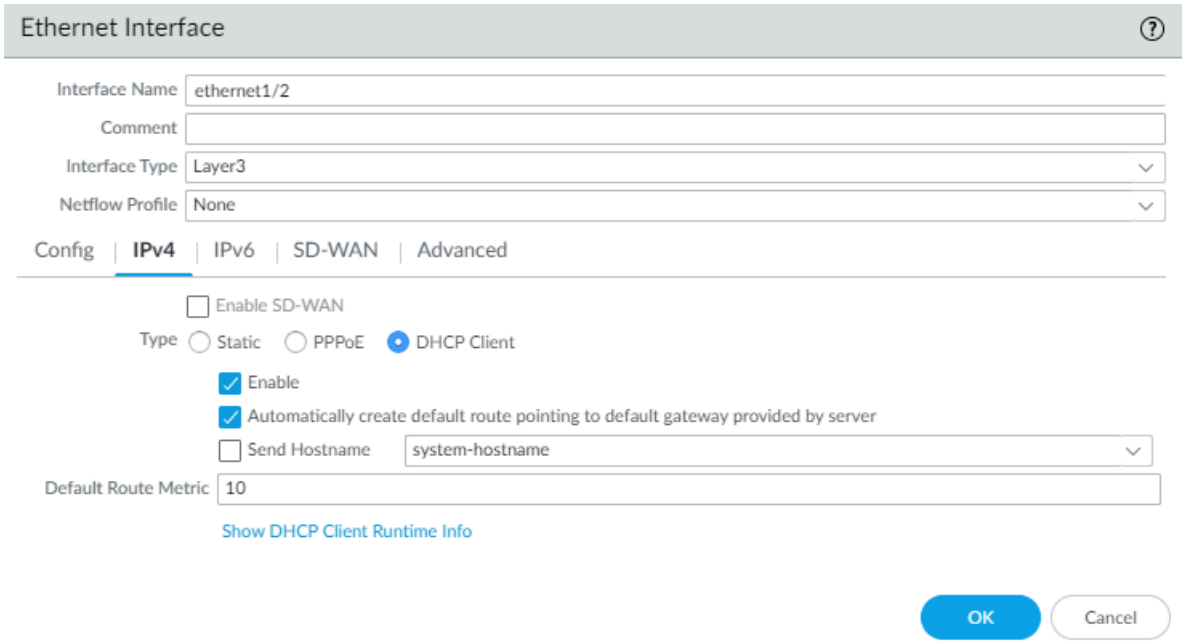
STEP 7 | Configurez l'interface Ethernet 1/2.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
2. Sélectionnez **Interface Type (Type d'interface)** – **Layer 3 (De couche 3)**.
3. Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Cette zone constituera votre zone

 ©2023 Palo Alto Networks, Inc.

non approuvée et dirigera le trafic sortant hors de votre VPC de sécurité. Définissez la nouvelle zone, par exemple VM-Series-non approuvée, puis cliquez sur **OK**.

4. Dans l'onglet **IPv4**, sélectionnez **DHCP Client (Client DHCP)**.
5. Sélectionnez **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)**.
6. Cliquez sur **OK**.

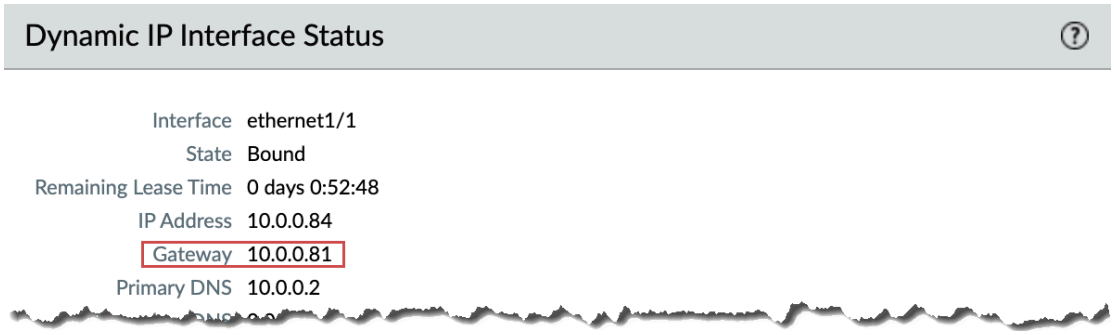


STEP 8 | Configurez un routeur virtuel.

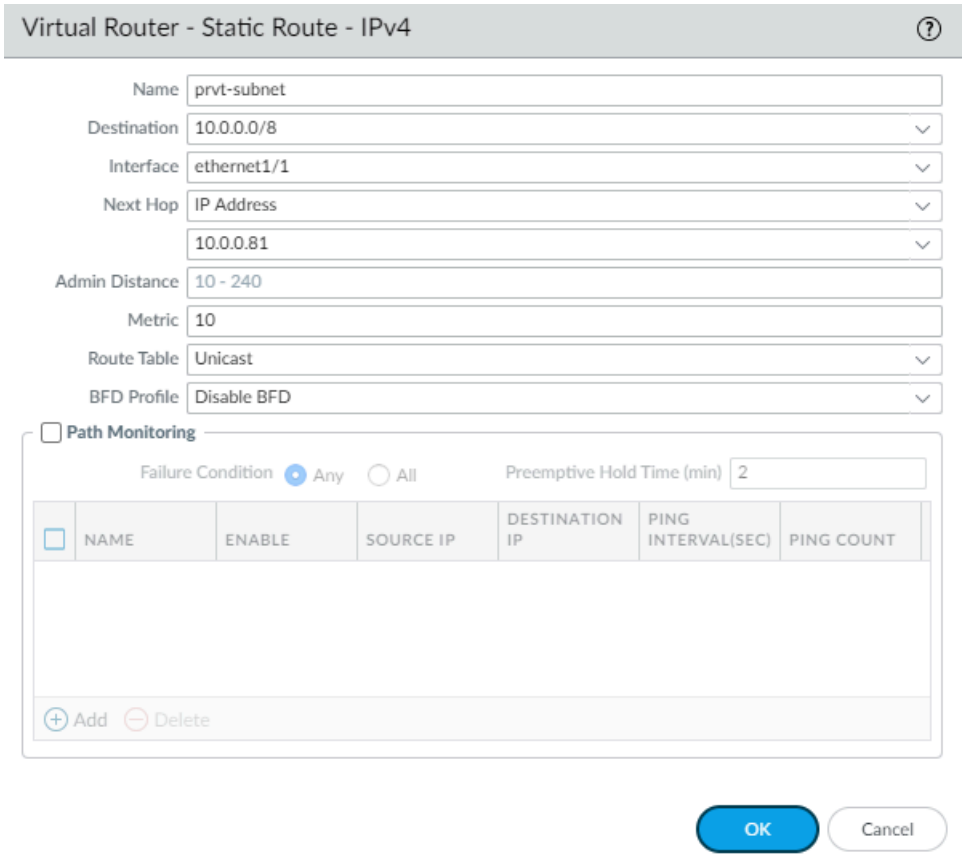
1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** > **Add (Ajouter)**.
2. Donnez un **Name (Nom)** descriptif au routeur virtuel.
3. Dans **Interfaces**, cliquez sur **Add (Ajouter)** Ethernet1/1, toutes les sous-interfaces sous Ethernet1/1, et Ethernet1/2.
4. Cliquez sur **Static Routes (Routes statiques)** > **Add (Ajouter)**.
   1. Saisissez un nom descriptif pour la route statique.
   2. Comme **Destination**, saisissez l'adresse IP privée du sous-réseau VPC de l'application.
   3. Sélectionnez l'interface (d'entrée) approuvée dans la liste déroulante **Interface**.
   4. Pour **Next Hop (Saut suivant)**, sélectionnez IP Address (Adresse IP) et entrez l'adresse IP de la passerelle de l'interface approuvée. Vous pouvez trouver l'adresse IP de la

©2023 Palo Alto Networks, Inc.

passerelle dans **Network (Réseau)** > **Interfaces** > **Ethernet** > **Dynamic-DHCP Client (Client DHCP dynamique)**.



5. Cliquez sur **OK**.



5. Assurez-vous que les itinéraires statiques peuvent atteindre tous les VPC d'application de votre déploiement. Vous pouvez soit créer quelques grands itinéraires agrégés (couvrant toute la RFC1918), soit des routes spécifiques au VPC d'application. Si vous utilisez des

 ©2023 Palo Alto Networks, Inc.

sous-interfaces, vous n'avez pas besoin de rediriger vers la sous-interface. Le contrôle de sortie recherche uniquement l'interface correspondante au lieu de la sous-interface correspondante.

6. Cliquez sur **OK**.

STEP 9 | Créez une politique NAT pour le trafic sortant Ethernet1/2.

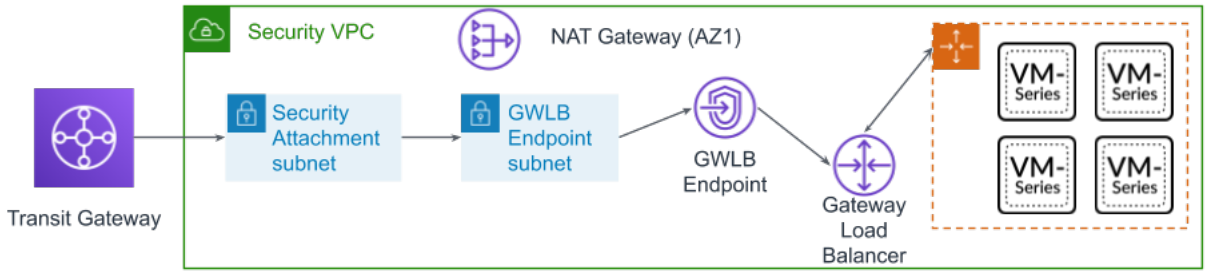
1. Sélectionnez **Policies (Politiques)** > **NAT** > **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** descriptif pour la règle de politique NAT.
3. Sélectionnez **ipv4** dans la liste déroulante **NAT Type (Type de NAT)**.
4. Dans l'onglet **Original Packet (Paquet d'origine)**, définissez la **Source Zone (Zone source)** sur n'importe laquelle et la **Destination Zone (Zone de destination)** sur votre zone (de sortie) non approuvée.
5. Dans l'onglet **Translated Packet (Paquet traduit)**, définissez les paramètres suivants.
   - Translation Type (Type de traduction) : port et IP dynamiques
   - Type d'adresse : Adresse de l'interface
   - Interface : Sélectionnez votre port (de sortie) non approuvé dans la liste déroulante.
   - IP address: None
6. Cliquez sur **OK**.

STEP 10 | **Commit (Validez)** vos modifications.

Groupe de mise à l'échelle automatique VM-Series avec équilibreur de charge AWS Gateway

Les modèles de mise à l'échelle automatique pour AWS de Palo Alto Networks vous permettent d'intégrer et de configurer les pare-feu VM-Series avec un GWLB pour protéger les applications déployées dans AWS. Les modèles exploitent les fonctionnalités d'évolutivité AWS pour mettre indépendamment et automatiquement à l'échelle les pare-feu VM-Series déployés dans AWS afin de répondre aux augmentations soudaines de la demande de ressources de charges de travail d'applications.

*Ces modèles sont **pris en charge par la communauté.***



Cette solution fournit un modèle VPC de sécurité et un modèle d'application. Le modèle VPC de sécurité déploie le groupe de mise à l'échelle automatique du pare-feu VM-Series, un GWLBE, le sous-réseau GWLBE, le sous-réseau d'attachement de sécurité et une passerelle NAT pour chaque

 ©2023 Palo Alto Networks, Inc.

zone de disponibilité. Téléchargez les modèles CloudFormation depuis le répertoire GitHub de Palo Alto Networks.

Le modèle de mise à l'échelle automatique VM-Series pour l'intégration à un GWLB AWS comprend les blocs de construction suivants :

Bloc de construction	Description
Composants PAN	• Panorama exécutant la version 10.0.2 ou ultérieure • PAN-OS 10.0.2 ou version ultérieure • Plug-in VM-Series version 2.0.2 ou ultérieure installée sur Panorama
Modèle de pare-feu (Modèle pris en charge par la communauté)	En fonction du nombre de zones de disponibilité que vous choisissez, `firewall-new-vpc-v3.0.template` déploie les éléments suivants : *Le modèle prend en charge un maximum de quatre zones de disponibilité.* • Sous-réseaux pour la gestion de Lambda, attachements de passerelle de transit, terminaux GWLB et passerelles NAT, ainsi que les sous-réseaux approuvés. • Tables de routage pour chaque sous-réseau • Attachements de passerelle de transit et tables de routage • Passerelles NAT et Internet • Un groupe de mise à l'échelle automatique avec un pare-feu VM-Series par zone de disponibilité. • Un GWLB et un terminal GWLB pour chaque zone de disponibilité. Le CIDR VPC pour le modèle de pare-feu doit être supérieur à /23. En raison des nombreuses variations dans un environnement de production qui comprend, sans toutefois s'y limiter, plusieurs composants spécifiques comme des sous-réseaux, des zones de disponibilité, des tables de routage et des groupes de sécurité. Vous devez déployer `firewall-new-vpc-v3.0.template` dans un nouveau VPC. *Le modèle de mise à l'échelle automatique VM-Series pour AWS ne déploie pas de passerelle de transit ou Panorama. Vous devez déployer une passerelle de transit et Panorama avant de démarrer firewall-new-vpc-v3.0.template.*
Modèle d'application (Modèle pris en	En fonction du nombre de zones de disponibilité que vous choisissez, `panw-aws-app-v3.0.template` déploie les éléments suivants : *Le modèle prend en charge un maximum de quatre zones de disponibilité.*

©2023 Palo Alto Networks, Inc.

Bloc de construction	Description
charge par la communauté)	• sous-réseaux pour Lambda, attachements de passerelle de transit, terminaux GWLB, équilibreurs de charge d'application ; • tables de routage pour chaque sous-réseau, ainsi qu'une table de routage entrant associée à la passerelle Internet pour orienter le trafic entrant vers le terminal GWLB ; • un équilibreur de charge d'application ; • une passerelle Internet ; • un groupe de mise à l'échelle automatique avec une instance Ubuntu par zone de disponibilité. Le CIDR VPC pour le modèle d'application doit être supérieur à /23.  ***Le modèle d'application est destiné à être utilisé comme exemple pour valider le modèle de sécurité.***
Fonctions Lambda	AWS Lambda fournit une automatisation robuste, dirigée par les événements, sans devoir recourir à un logiciel d'orchestration complexe. En plus de déployer les composants décrits dans les lignes ci-dessus, le `firewall-new-vpc-v3.0.template` exécute les fonctions suivantes : • Ajoute ou supprime une interface (ENI) lorsqu'une interface est lancée ou résiliée. • Supprime toutes les ressources associées lorsque vous supprimez une pile ou résiliez une instance. • Supprime un pare-feu en tant que périphérique géré Panorama lorsqu'il y a un événement de mise à l'échelle. • Désactive la licence lorsqu'un événement de mise à l'échelle entraîne une résiliation du pare-feu. • Surveille la passerelle de transit de manière périodique pour détecter la présence de nouveaux attachements ou détachements, et met à jour les tables de routage conformément au VPC de sécurité.
Fichiers d'amorçage Le fichier bootstrap.xml fourni dans le référentiel GitHub est fourni uniquement pour les tests et l'évaluation. Pour un	Cette solution nécessite le fichier init-cfg.txt et le fichier bootstrap.xml afin que le pare-feu VM-Series dispose de la configuration de base pour la gestion du trafic. • Le fichier `init-cfg.txt` inclut la commande opérationnelle mgmt-interface-swap pour permettre au pare-feu de recevoir le trafic du plan de données sur son interface principale (eth0). Cette solution de mise à l'échelle automatique nécessite l'échange des interfaces du plan de données et de gestion pour permettre au GWLB de transférer le trafic Web vers le niveau de mise à l'échelle automatique des pare-feu VM-Series. • Le fichier `bootstrap.xml` active la connectivité de base pour les interfaces réseau du pare-feu et permet au pare-feu de se connecter à

 ©2023 Palo Alto Networks, Inc.

Bloc de construction	Description
déploiement de production, vous devez modifier les informations d'identification d'exemple dans le fichier bootstrap.xml avant le lancement.	l'espace de noms AWS CloudWatch correspondant au nom de la pile que vous entrez lorsque vous lancez le modèle.

Si vous avez besoin de supprimer ces modèles d'AWS, supprimez toujours le modèle d'application en premier. Le fait de tenter de supprimer le modèle de pare-feu entraîne l'échec de la suppression.

- Avant le lancement des modèles
- Lancement du modèle de pare-feu
- Lancement du modèle d'application

Avant le lancement des modèles

Avant de lancer les modèles pour intégrer un groupe de mise à l'échelle automatique de pare-feu VM-Series avec un GWLB AWS, vous devez suivre la procédure suivante.

STEP 1 | Assurez-vous que vous disposez des éléments suivants avant de commencer.

- Obtenez le code d'autorisation pour un forfait prenant en charge le nombre de pare-feu pouvant être requis pour votre déploiement. Vous devez enregistrer ce code d'autorisation dans un fichier texte nommé **`authcodes`** (sans extension) et mettre le fichier **`authcodes`** dans le dossier **`/license`** de l'ensemble d'amorçage.
- Téléchargez les fichiers requis pour lancer le modèle d'équilibreur de charge de la passerelle VM-Series à partir du référentiel GitHub.

©2023 Palo Alto Networks, Inc.

- Créez une passerelle de transit. Cette passerelle de transit relie vos VPC de sécurité et d'application.
  - Notez l'ID de la passerelle de transit ; vous en aurez besoin plus tard lors du déploiement du modèle.
  - Vous devez ajouter un itinéraire 0.0.0.0/0 à la table de routage de la pièce jointe de la demande pointant vers la pièce jointe de sécurité afin de protéger le trafic est-ouest et sortant.
  - Assurez-vous que **l'association de la table de routage par défaut** et **la propagation de la table d'itinéraires par défaut** sont désactivées.
- Le CIDR VPC recommandé pour le pare-feu et les modèles d'application doit être supérieur à /23.



Le groupe cible de la passerelle GWLB ne peut pas utiliser HTTP pour les contrôles de santé car le pare-feu VM-Series ne permet pas l'accès avec un protocole non sécurisé. Utilisez plutôt HTTPS ou TCP.

STEP 2 | Déployez Panorama sous la version 10.0.2 et configurez ce qui suit.

Panorama doit autoriser les adresses IP publiques de AWS. Le pare-feu VM-Series accède à Panorama en utilisant l'adresse IP externe de la passerelle NAT créée par le modèle.

STEP 3 | Téléchargez et installez le plug-in VM-Series sur Panorama.

1. Sélectionnez **Panorama** > **Plugins (Plug-ins)** et utilisez **Check Now (Vérifier maintenant)** pour chercher de nouveaux paquets de plug-ins. Le nom du plug-in VM-Series est `vm_series`.
2. Consultez les notes de version du plug-in pour déterminer la version qui vous procure des mises à niveaux qui vous sont utiles.
3. Sélectionnez une version du plug-in et cliquez sur **Download (Télécharge)** dans la colonne Action.
4. Dans la colonne Action, cliquez sur **Install (Installer)**. Panorama vous alerte lorsque l'installation est terminée.
5. Pour afficher le plug-in, sélectionnez **Device (Périphérique)** > **VM-Series**.

©2023 Palo Alto Networks, Inc.

STEP 4 | Configurez le modèle.

1. Connectez-vous à l'interface Web Panorama.
2. Sélectionnez **Panorama** > **Templates (Modèles)** puis cliquez sur **Add (Ajouter)**.
   1. Saisissez un **Name (Nom)** descriptif.
   2. Cliquez sur **OK**.
3. Configurez le Virtual Router (routeur virtuel - VR).
   1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**.
   2. Assurez-vous que vous avez sélectionné le modèle que vous avez créé ci-dessus dans la liste déroulante **Modèle**.
   3. Cliquez sur **Add (Ajouter)**.
   4. Nommez le routeur virtuel en utilisant le format suivant : VR-<tempstackname>.
   5. Activez l'ECMP sur le routeur virtuel.
   6. Cliquez sur **OK**.
4. Configurez l'interface et créez la zone.
   1. Sélectionnez **Network (Réseau)** > **Interfaces** puis cliquez sur **Add Interface (Ajouter une interface)**.
   2. Sélectionnez **Slot 1 (Logement 1)**, puis sélectionnez le nom de l'interface (par exemple, ethernet 1/1).
   3. Définissez **Interface Type (Type d'interface)** sur Couche 3.
   4. Dans l'onglet **Config (Configuration)**, sélectionnez **New Zone (Nouvelle zone)** dans la liste déroulante **Security Zone (Zone de sécurité)**. Dans la boîte de dialogue Zone

©2023 Palo Alto Networks, Inc.

(Zone), donnez un **Name (Nom)** à la nouvelle zone, par exemple : Internet, puis cliquez sur **OK (OK)**.

5. Dans la liste déroulante **Virtual Router (routeur virtuel - VR)**, sélectionnez le routeur virtuel que vous avez créé ci-dessus.
6. Sélectionnez **IPv4** et cliquez sur **DHCP Client (Client DHCP)**.
7. Cliquez sur **OK**.

5. Créez un profil de gestion qui autorise HTTPS sur l'interface créée ci-dessus pour prendre en charge les vérifications de l'état.
   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.*
6. 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 Interface **Management Profile (Profil de gestion d'interface)** que vous venez de configurer.
   3. Cliquez sur **OK**.
7. Configurez le serveur DNS et le temps de d'actualisation du FQDN.
   1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Services** et cliquez sur l'icône Edit (Modifier).
   2. Configurez le **serveur DNS principal** sur 169.254.169.253. Il s'agit de l'adresse DNS de AWS.
   3. Configurez le **temps minimum d'actualisation du FQDN** à 60 secondes.
   4. Cliquez sur **OK**.
8. **Commit (Validez)** vos modifications. Cela est nécessaire avant de passer à l'étape suivante.
9. Créez un administrateur.
   1. Sélectionnez **Device (Périphérique)** > **Administrators (Administrateurs).**
   2. Saisissez **`pandemo`** comme **Name (Nom)**.
   3. Configurez le **Password (Mot de passe)** sur **`demopassword`** et **Confirm (Confirmer)**.
   4. Cliquez sur **OK**.
10. **Commit (Validez)** vos modifications.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Configurez une pile de modèles et ajoutez le modèle à la pile de modèles.

1. Sélectionnez **Panorama** > **Templates (Modèles)** et cliquez sur **Add Stack (Ajouter une pile)**.
2. Entrez un **Name (Nom)** unique pour identifier la pile.
3. Cliquez sur **Add (Ajouter)** et sélectionnez le modèle.
4. Cliquez sur **OK** pour sauvegarder la pile de modèle.

STEP 6 | Créez le **Device Group (Groupe d'appareils)**.

1. Sélectionnez **Panorama** > **Device Groups (Groupe d'appareils)**.
2. Cliquez sur **Add (Ajouter)**.
3. Saisissez un **Name (Nom)** descriptif.
4. Cliquez sur **OK**.
5. Ajoutez une règle « avant » autorisant toute sécurité.
    1. Assurez-vous que vous avez sélectionné le groupe d'appareils que vous avez créé ci-dessus dans la liste déroulante **Groupe d'appareils**.
    2. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules (Règles « avant »)** et cliquez sur **Add (Ajouter)**.
    3. Saisissez un **Name (Nom)** descriptif.
    4. Sous **Source**, **User (Utilisateur)**, **Destination**, **Application**, et **Service/URL Category (Service/Catégorie URL)**, sélectionnez n'importe laquelle.
    5. Sous **Actions**, sélectionnez **Allow (Autoriser)**.
    6. Cliquez sur **OK**.
6. **Commit (Validez)** vos modifications.

STEP 7 | Ajoutez la clé API de désactivation de licence pour le pare-feu à Panorama.

1. Ouvrez une session dans le portail de support client.
2. Sélectionnez **Assets (Ressources)** > **API Key Management (Gestion des clés API)**.
3. Copiez la clé API.
4. Utilisez la CLI pour installer la clé API copiée à l'étape précédente.

    `request license api-key set key <key>`

STEP 8 | Après le déploiement de Panorama, vous devez ouvrir les ports suivants comme décrit ci-dessous sur le groupe de sécurité Panorama dans AWS.

- **Port 443 (HTTPS)** : lors du déploiement initial du modèle de pare-feu, laissez HTTPS ouvert pour que Lambda puisse se connecter à Panorama.

  Lorsque vous sécurisez le port 443, vous spécifiez une plage d'adresse IP à partir de laquelle vous autoriserez les connexions, ainsi que les EIP attribués aux passerelles NAT. Le nombre de passerelles NAT dans votre déploiement dépend du nombre de zones de disponibilité que vous configurez. Pour rechercher les EIP des passerelles NAT dans AWS, accédez à **VPC** >

 ©2023 Palo Alto Networks, Inc.

NAT Gateways (Passerelles NAT). Notez les informations EIP pour le groupe de sécurité pour HTTPS.

De plus, pour permettre à Panorama de publier la licence du pare-feu après la suppression de la pile, vous devez autoriser le trafic de la plage CIDR de la région où vous avez déployé le modèle de pare-feu. Vous pouvez trouver le CIDR pour votre région sur ce lien.

- **Port 3978** : le port 3978 doit pouvoir recevoir du trafic à partir de n'importe quelle adresse IP.

Lancement du modèle de pare-feu

Ce flux de travail décrit comment déployer le modèle de pare-feu.

STEP 1 | Modifiez le fichier **`init-cfg.txt`** et chargez-le dans le dossier **`/config`**.

Comme vous utilisez Panorama pour amorcer les pare-feu VM-Series, votre fichier **`init-cfg.txt`** doit être modifié comme suit. Aucun fichier **`bootstrap.xml`** n'est nécessaire.

Assurez-vous d'utiliser les noms de groupes d'appareils et de modèles que vous avez créés ci-dessus dans le fichier init-cfg.txt.

```
type=dhcp-client ip-address= default-gateway= netmask=
 ipv6-address= ipv6-default-gateway= hostname= vm-auth-key=
 panorama-server= panorama-server-2= tplname= dgname= dhcp-
send-hostname=yes dhcp-send-client-id=yes dhcp-accept-server-
hostname=yesdhcp-accept-server-domain=yes plugin-op-commands=aws-
gwlb-inspect:enable
```

Votre fichier init-cfg.txt doit inclure **`plugin-op-commands=aws-gwlb-inspect:enable`**. Cela est nécessaire lors de l'intégration du pare-feu VM-Series avec un GWLB.

Vous devez ajouter le PIN d'enregistrement automatique du certificat de périphérique au fichier init-cfg.txt pour installer automatiquement un certificat de périphérique lorsque votre instance de pare-feu VM-Series est déployée.

STEP 2 | Ajoutez le code d'autorisation de licence au dossier **`/license`** de l'ensemble d'amorçage.

1. Utilisez un éditeur de texte pour créer un nouveau fichier texte nommé **`authcodes`** (sans extension).
2. Ajoutez le code d'autorisation de vos licences BYOL à ce fichier, puis enregistrez-le. Le code d'autorisation doit représenter un forfait et prendre en charge le nombre de pare-feu pouvant être requis pour votre déploiement. Si vous utilisez des codes d'autorisation individuels au lieu d'un forfait, le pare-feu ne récupère que la clé de licence pour le premier code d'autorisation inclus dans le fichier.

STEP 3 | Chargez le code Lambda pour le modèle de pare-feu (**`panw-aws.zip`**) et le modèle d'application (**`app.zip`**) dans un compartiment S3. Vous pouvez utiliser le même compartiment S3 que celui que vous avez utilisé pour l'amorçage.

Si la pile d'applications est gérée par un compte différent du pare-feu, utilisez le compte d'application pour créer un autre compartiment s3 dans la même région AWS que le modèle de pare-feu et copiez le fichier **`app.zip`** dans ce compartiment s3.

©2023 Palo Alto Networks, Inc.

STEP 4 | Sélectionnez l'interface de pare-feu.

1. Dans la console de gestion AWS, sélectionnez **CloudFormation** > **Create Stack (Créer une pile)**.
2. Sélectionnez **Upload (Télécharger)** pour télécharger le dernier modèle de pare-feu à partir du Git repository (Référentiel Git) pour choisir le modèle de pare-feu afin de déployer les ressources lancées par le modèle. Cliquez sur Open (Ouvrir) et Next (Suivant).
3. Spécifiez le Stack name (Nom de la pile). Le nom de la pile vous permet d'identifier de manière unique toutes les ressources déployées à l'aide de ce modèle.

STEP 5 | Saisissez un **Name (Nom)** descriptif pour votre pile. Le nom doit contenir 28 caractères maximum.

STEP 6 | Configurez les paramètres pour le VPC.

1. Saisissez le nombre de zones de disponibilité et sélectionnez la région dans le menu déroulant des zones de disponibilité.
2. Recherchez l'ID AMI pour le pare-feu VM-Series et saisissez-le. Assurez-vous que l'ID AMI correspond à la région AWS, à la version de PAN-OS et à l'option de licence BYOL ou PAYG que vous avez choisi d'utiliser. Pour plus d'informations, reportez-vous à la section Obtenir les ID des images de machine Amazon.
3. Sélectionnez la **Key pair** (Paire de clés) EC2 (à partir de la liste déroulante) pour lancer le pare-feu. Pour vous connecter aux pare-feu, vous devez fournir le nom de cette paire de clés et la clé privée qui lui est associée.
4. Sélectionnez **Yes** (Oui) si vous souhaitez **Enable Debug Log** (Activer le journal de débogage). L'activation du journal de débogage génère des journaux plus détaillés qui aident à résoudre les problèmes liés au déploiement. Ces journaux sont générés à l'aide du nom de la pile et sont enregistrés dans AWS CloudWatch.

Par défaut, le modèle utilise l'utilisation du processeur comme paramètre de mise à l'échelle pour les pare-feu VM-Series. Les statistiques PAN-OS personnalisées sont automatiquement publiées dans l'espace de noms CloudWatch qui correspond au nom de la pile que vous avez spécifié précédemment.

STEP 7 | Indiquez le nom du ou des compartiments Amazon S3.

1. Entrez le nom du compartiment S3 qui contient l'ensemble d'amorçage.

   Si le compartiment d'amorçage n'est pas configuré correctement ou si vous entrez un nom de compartiment incorrect, le processus d'amorçage échoue et vous ne pouvez pas vous connecter au pare-feu. Les vérifications de l'état pour les équilibreurs de charge échouent également.
2. Saisissez le nom du S3 bucket (Compartiment S3) qui contient le fichier panw-aws.zip. Comme mentionné précédemment, vous pouvez utiliser un compartiment S3 pour le code Lambda ou Bootstrap (Amorçage).

STEP 8 | Spécifiez les clés permettant d'activer l'accès API au pare-feu et à Panorama.

1. Entrez la clé que le pare-feu doit utiliser pour authentifier les appels d'API. La clé par défaut est basée sur l'exemple de fichier et ne doit être utilisée que pour les tests et l'évaluation. Pour un déploiement de production, vous devez créer une connexion PAN-OS distincte uniquement pour l'appel d'API et générer une clé associée.

 ©2023 Palo Alto Networks, Inc.

2. Saisissez l'API Key (Clé API) pour permettre à AWS Lambda de passer des appels API à Panorama. Pour un déploiement de production, vous devez créer une connexion distincte uniquement pour l'appel d'API et générer une clé associée.

STEP 9 | Ajoutez votre ou vos numéros de compte AWS. Vous devez fournir le numéro de compte utilisé pour déployer tout VPC qui est connecté à votre GWLB. Ajoutez ces valeurs sous forme de liste séparée par des virgules. Vous pouvez ajouter des numéros de compte supplémentaires après avoir déployé le modèle.

Pour trouver votre numéro de compte, cliquez sur votre nom d'utilisateur AWS en haut à droite de la console AWS et sélectionnez **My Security Credentials (Mes informations d'identification de sécurité)**.

STEP 10 | Saisissez l'ID de la passerelle de transit. L'ID de la passerelle de transit est nécessaire pour sécuriser le trafic est-ouest et sortant. Si vous ne saisissez pas d'ID de passerelle de transit, le modèle suppose que seul le trafic entrant doit être inspecté par les pare-feu intégrés au GWLB.

STEP 11 | Saisissez le CIDR pour le VPC de sécurité.

STEP 12 | Passez en revue les paramètres du modèle et lancez le modèle.

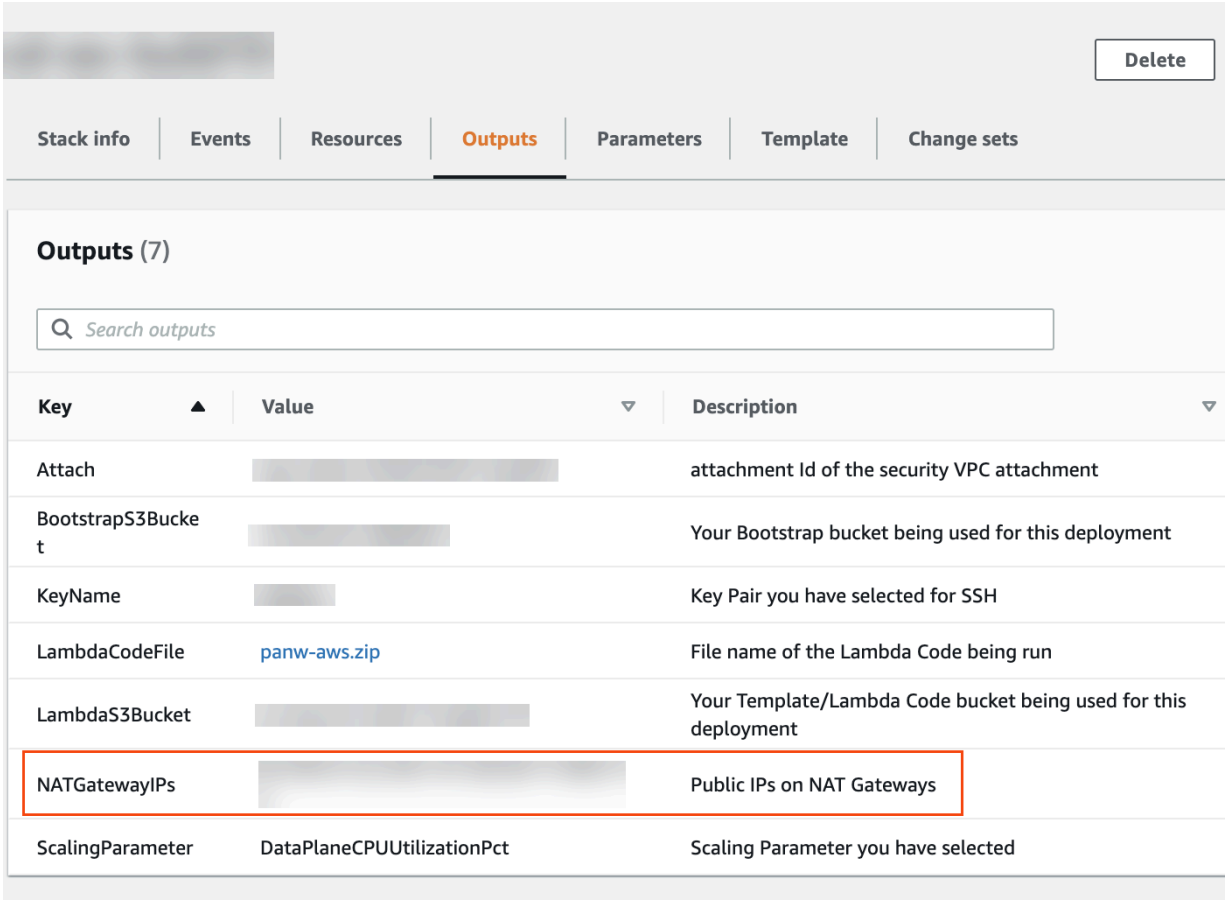
1. Sélectionnez **I acknowledge that this template might cause AWS CloudFormation to create IAM resources (Je reconnais que ce modèle peut entraîner la création de ressources IAM par AWS CloudFormation)**.
2. Cliquez sur **Create (Créer)** pour lancer le modèle. L'événement CREATE_IN_PROGRESS s'affiche.
3. En cas de déploiement réussi, le statut est mis à jour et passe à CREATE_COMPLETE.

STEP 13 | Vérifiez que le modèle a lancé toutes les ressources requises.

STEP 14 | Créez des règles autorisant les adresses IP de la passerelle NAT sur le groupe de sécurité où votre appareil Panorama est déployé. Ceci est nécessaire pour permettre à vos pare-feu de se

 ©2023 Palo Alto Networks, Inc.

connecter à Panorama. Vous pouvez trouver la liste des adresses IP de la passerelle NAT dans la sortie de la pile de sécurité CFT.



 ©2023 Palo Alto Networks, Inc.

1. Accédez à la console AWS VPC.
2. Sélectionnez **Security Groups (Groupes de sécurité)** dans le volet de navigation.
3. Sélectionnez la sécurité où Panorama est déployé.
4. Sélectionnez **Actions** > **Edit Inbound Rules (Modifier les règles entrantes)** > **Add rule (Ajouter une règle)**.
5. Ajoutez des règles autorisant les adresses IP de passerelle NAT pour la règle TCP personnalisée pour la plage de ports 3978.
6. Cliquez sur **Save rules (Enregistrer les règles)**.

Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0
Custom TCP Rule	TCP	3978	
Custom TCP Rule	TCP	3978	
Custom TCP Rule	TCP	3978	

Lancement du modèle d'application

Suivez la procédure suivante pour lancer le modèle d'application.

STEP 1 | Créez un compartiment S3 à partir duquel vous lancerez le modèle d'application.

- S'il s'agit d'un déploiement entre comptes, créez un nouveau compartiment.
- S'il existe un compte, vous pouvez créer un nouveau compartiment ou utiliser le compartiment S3 que vous avez créé précédemment (vous pouvez utiliser un compartiment pour tout).

STEP 2 | Chargez le fichier app.zip dans le compartiment S3.

STEP 3 | Sélectionnez le modèle de lancement d'application que vous souhaitez lancer.

1. Dans la console de gestion AWS, sélectionnez **CloudFormation** > **CreateStack**
2. Sélectionnez Upload a template to Amazon S3 (Charger un modèle sur Amazon S3) pour choisir le modèle d'application permettant de déployer les ressources que le modèle lance dans le même VPC que les pare-feu ou dans un VPC différent. Cliquez sur **Open (Ouvrir)** et **Next (Suivant)**.
3. Spécifiez le Stack name (Nom de la pile). Le nom de la pile vous permet d'identifier de manière unique toutes les ressources déployées à l'aide de ce modèle.

©2023 Palo Alto Networks, Inc.

STEP 4 | Sélectionnez les Availability Zones (Zones de disponibilité) (AZ) que votre configuration va couvrir dans Select list of AZ (Sélectionner une liste d'AZ).

STEP 5 | Saisissez un **VPC Name (Nom de VPC)** descriptif.

STEP 6 | Configurez les paramètres pour Lambda.

1. Saisissez le S3 Bucket Name (Nom du compartiment S3) où est stocké app.zip.
2. Saisissez le nom du Zip File Name (Nom du fichier zip).

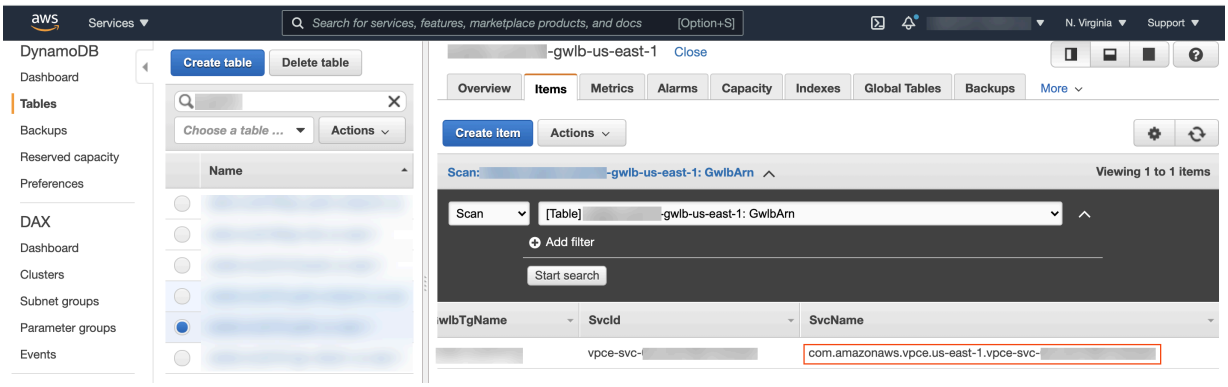
STEP 7 | Sélectionnez le type d'instance EC2 pour le serveur Web Ubuntu lancé par ce modèle.

STEP 8 | Saisissez votre paire de clés EC2 Amazon.

©2023 Palo Alto Networks, Inc.

STEP 9 | Saisissez le nom de la configuration de service (Service Name) pour le terminal GWLB dans le VPC de sécurité.

1. Sélectionnez **DynamoDB** dans le menu déroulant **Services** de la console AWS.
2. Sélectionnez **Tables** et localisez la table de votre VPC de sécurité. Le nom de la table sera <stack name>-gwlb-<region>. Par exemple, cft-deployment-gwlb-us-east-1.
3. Cliquez sur l'onglet Items (Éléments) et copiez le nom du service.
4. Collez le nom du service dans les paramètres de configuration du modèle de l'application.



 ©2023 Palo Alto Networks, Inc.

STEP 10 | Saisissez l'ID de la passerelle de transit. Il s'agit de la même passerelle de transit que vous avez créée avant de déployer le modèle de pare-feu.

STEP 11 | Passez en revue les paramètres du modèle et lancez le modèle.

STEP 12 | Une fois que l'application a été déployée, vous devez ajouter un itinéraire à la table de routage de la passerelle de transit pour permettre l'inspection du trafic est-ouest et sortant.

1. Connectez-vous à la console de VPC AWS.
2. Sélectionnez **Transit Gateway Route Tables (Tables de routage de passerelle de transit)** et choisissez votre table de routage de passerelle de transit. Cette table de routage est créée par le modèle et s'appelle**<app-stack-name>-<region>-PANWAppAttRt**.
3. Sélectionnez **Routes (Itinéraires)** et cliquez sur **Create static route (Créer un itinéraire statique)**.
4. Saisissez 0.0.0.0/0 dans le champ **CIDR**.
5. Dans la liste déroulante **Choose attachment (Choisir un attachement)**, sélectionnez l'attachement de VPC du pare-feu VM-Series.
6. Cliquez sur **Create static route (Créer un itinéraire statique)**.

STEP 13 | (Facultatif) Créez un hôte bastion (également appelé jump box) pour accéder au serveur Web créé par le modèle d'application.

1. Créez un sous-réseau orienté vers le public dans votre VPC d'application.
2. Ajoutez un itinéraire vers ce sous-réseau à partir de votre adresse IP vers la passerelle Internet.
3. Créez une nouvelle instance EC2 dans le sous-réseau public avec une adresse IP publique.
4. Créez un groupe de sécurité pour cette instance EC2 qui autorise le SSH à partir de votre adresse IP.

©2023 Palo Alto Networks, Inc.

Haute disponibilité des pare-feu VM-Series sur AWS

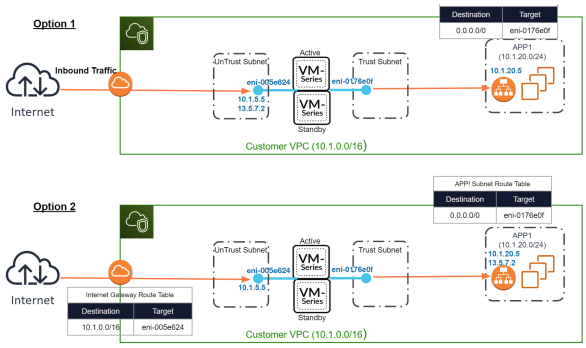
Le pare-feu VM-Series sur AWS prend en charge la HA active/passive uniquement. S'il est déployé avec Amazon Elastic Load Balancing (ELB), il ne prend pas en charge la HA (dans ce cas, ELB fournit les capacités de basculement).

- Vue d'ensemble de la HA dans AWS
- Rôles IAM pour la HA
- Liaisons HA
- Analyse des pulsations et messages Hello
- Priorité et préemption des périphériques
- Minuteurs HA
- Configuration de la HA active/passive dans AWS à l'aide d'un IP secondaire
- Configuration de la HA active/passive dans AWS à l'aide du déplacement d'interface
- Migration de la HA active/passive dans AWS

Vue d'ensemble de la HA dans AWS

Pour assurer la redondance, vous pouvez déployer les pare-feu VM-Series sous forme de configuration haute disponibilité (HA) active/passive dans AWS. L'homologue actif synchronise continuellement les informations de configuration et de session avec l'homologue passif ayant la même configuration. Une connexion de pulsation entre les deux périphériques garantit un basculement dans l'éventualité où le périphérique actif tombe en panne. Il y a deux options pour le déploiement du pare-feu VM-Series sur AWS dans HA – déplacer l'adresse IP secondaire et déplacer l'interface du plan de données (ENI).

Pour vous assurer que tout le trafic vers vos applications Internet passent par le pare-feu, vous avez deux options. Vous pouvez soit configurer l'adresse IP publique de l'application sur l'interface non approuvée (E1/2 dans l'illustration ci-dessus) du pare-feu VM-Series, soit configurer le routage d'entrée AWS. La fonction de routage d'entrée AWS vous permet d'associer des tables de routage à la passerelle Internet AWS et d'ajouter des règles de routage pour rediriger le trafic de l'application à travers le pare-feu VM-Series. Cette redirection garantit que tout le trafic Internet passe par le pare-feu sans avoir à reconfigurer les terminaisons des applications.

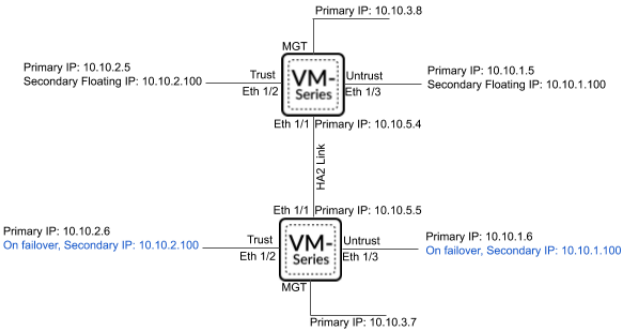


©2023 Palo Alto Networks, Inc.

Déplacer l'adresse IP secondaire

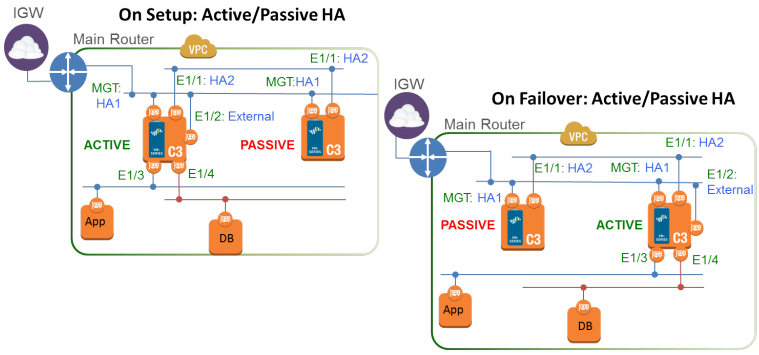
Lorsque l'homologue actif tombe en panne, l'homologue passif détecte cette défaillance et devient actif. Il déclenche également des appels d'API vers l'infrastructure AWS pour déplacer les adresses IP secondaires configurées depuis les interfaces de plan de données de l'homologue défaillant vers lui-même. En outre, AWS met à jour les tables de routage pour s'assurer que le trafic est dirigé vers l'instance de pare-feu active. Ces deux opérations permettent de s'assurer que les sessions de trafic entrant et sortant sont rétablies après le basculement. Cette option vous permet de tirer profit de DPDK pour améliorer les performances des instances de votre pare-feu VM-Series et offre une meilleure durée de basculement que le HA de déplacement d'interface, tout en prenant en charge l'ensemble des fonctionnalités fournies par le déplacement d'interface.

La HA de déplacement d'IP secondaire nécessite le plugin VM-Series 2.0.1 ou une version ultérieure.



Déplacement d'interface du plan de données

Lorsque l'homologue actif tombe en panne, l'homologue passif détecte la défaillance et devient actif. Il déclenche également des appels d'API vers l'infrastructure AWS pour déplacer toutes les interfaces de plan de données (ENI) de l'homologue défaillant vers lui-même.



Rôles IAM pour la HA

AWS exige que toutes les requêtes de l'API reçoivent une signature cryptographique à l'aide d'authentifiants émis par ces derniers. Afin d'activer les permissions API pour les pare-feu VM-Series qui seront déployés en tant que paire HA, vous devez créer une politique et associer cette politique à un rôle dans le service de gestion de l'identité et des accès (Identity and Access Management ; IAM) d'AWS. Le rôle doit être associé aux pare-feu VM-Series lors du lancement. La politique donne

©2023 Palo Alto Networks, Inc.

à l'IAM les permissions de rôle pour initier les actions de l'API afin de déplacer des interfaces ou des adresses IP secondaires entre l'homologue actif et l'homologue passif lorsqu'un basculement est déclenché.

Pour les instructions détaillées sur la création d'une politique, reportez-vous à la documentation AWS sur la Création de politiques gérées par le client. Pour obtenir des instructions détaillées sur la création d'un rôle IAM, la détermination des comptes ou des services AWS qui peuvent assumer le rôle et la détermination des actions et des ressources API que l'application peut utiliser après avoir assumé le rôle, reportez-vous à la documentation d'AWS qui porte sur les rôles IAM dans Amazon EC2.

La politique IAM, qui est configurée dans la console AWS, doit disposer des permissions pour les actions et ressources suivantes (au minimum) :

Les actions, autorisations et ressources IAM suivantes sont nécessaires pour activer le mode HA. Pour activer la surveillance AWS Cloudwatch, consultez Activation de la surveillance CloudWatch sur le pare-feu VM-Series

pour l'action IAM requise.

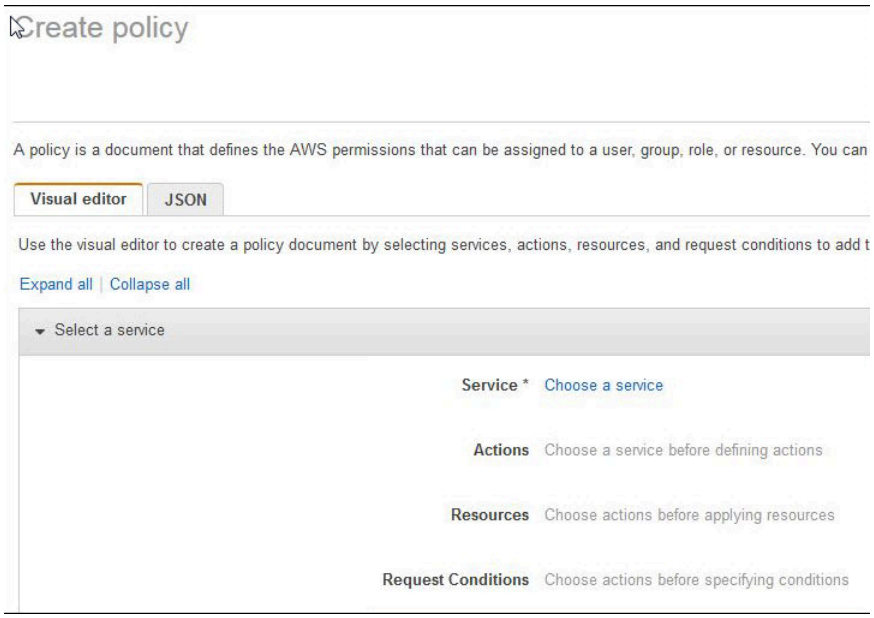
Action, autorisation ou ressource IAM	Description	Déplacer l'interface	Déplacer l'adresse IP secondaire
AttachNetworkInterface	Pour l'autorisation d'associer une ENI à une instance.	✓	✓
DescribeNetworkInterfaces	Pour télécharger les paramètres de l'ENI afin d'associer une interface à une instance.	✓	✓
DetachNetworkInterface	Pour l'autorisation de dissocier l'ENI de l'instance EC2.	✓	✓
DescribeInstances	Pour l'autorisation d'obtenir des informations sur les instances EC2 sur le VPC.	✓	✓
AssociateAddress	Pour les autorisations de déplacer des adresses IP publiques associées aux adresses IP primaires des interfaces passives vers les interfaces actives.		✓
AssignPrivateIpAddresses	Pour les autorisations d'attribuer des adresses IP secondaires et des adresses IP publiques associées aux interfaces sur l'homologue passif.		✓
DescribeRouteTables	Pour l'autorisation de récupérer toutes les tables de routage		✓

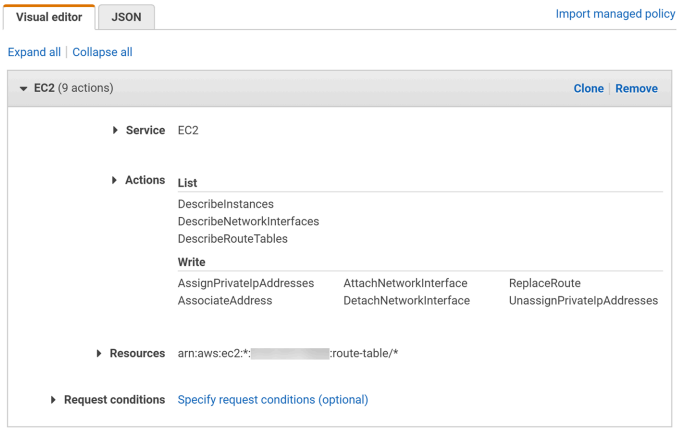
©2023 Palo Alto Networks, Inc.

Action, autorisation ou ressource IAM	Description	Déplacer l'interface	Déplacer l'adresse IP secondaire
	associées aux instances du pare-feu VM-Series.		
ReplaceRoute	Pour les autorisations de mettre à jour des entrées de la table de routage AWS.		✓
GetPolicyVersion	Pour l'autorisation de récupérer les informations sur la version de la politique AWS.		✓
GetPolicy	Pour l'autorisation de récupérer les informations sur la politique AWS.		✓
ListAttachedRolePolicies	Pour l'autorisation de récupérer la liste de toutes les politiques gérées associées à un rôle IAM spécifié.		✓
ListRolePolicies	Pour l'autorisation de récupérer une liste des noms des politiques en ligne intégrées dans un rôle IAM spécifié.		✓
GetRolePolicy	Pour l'autorisation de récupérer une politique en ligne spécifique intégrée dans un rôle IAM spécifié.		✓
policy	Pour l'autorisation d'accéder à la politique IAM Amazon Resource Name (ARN).		✓
role	Pour l'autorisation d'accéder aux rôles IAM ARN.		✓
route-table	Pour l'autorisation d'accéder à la table de routage Amazon Resource Name (ARN) afin de la mettre à jour lors du basculement.		✓
Caractère générique (*)	Dans le champ ARN, utilisez* comme caractère générique.	✓	✓

Les captures d'écran suivantes présentent les paramètres de gestion d'accès pour le rôle IAM décrit ci-dessus pour la HA d'IP secondaire :

 ©2023 Palo Alto Networks, Inc.





Les autorisations minimales dont vous avez besoin pour une HA de déplacement d'interface sont les suivantes : **{"Version": "2012-10-17","Statement": [{"Sid": "VisualEditor0","Effect": "Allow","Action": ["ec2:AttachNetworkInterface","ec2:DetachNetworkInterface","ec2:DescribeInstance "*"}]}**

Les autorisations minimales dont vous avez besoin pour une HA de déplacement d'IP secondaire sont les suivantes : {"Version": "2012-10-17","Statement": [{"Sid": "VisualEditor0","Effect": "Allow","Action": ["ec2:AttachNetworkInterface","ec2:DetachNetworkInterface","ec2:DescribeInstances","ec2:DescribeNetworkInterfa "ec2:AssignPrivateIpAddresses","ec2:AssociateAddress","ec2:DescribeRouteTables"],"Resource": "*"} {"Sid": "VisualEditor1","Effect": "Allow","Action": "ec2:ReplaceRoute", "Resource": "arn:aws:ec2:*:*:route-table/*"}]}

Liaisons HA

Les périphériques d'une paire HA utilisent des liaisons HA pour synchroniser les données et gérer les informations d'état. Sur AWS, le pare-feu VM-Series utilise les ports suivants :

 ©2023 Palo Alto Networks, Inc.

- **Liaison de contrôle**—La liaison HA1 permet d'échanger des messages Hello, des pulsations et des informations d'état HA, ainsi que des synchronisations de panneaux de gestion pour le routage et des informations sur l'ID d'un utilisateur. Cette liaison permet également de synchroniser des modifications de configuration apportées au périphérique actif ou passif avec son homologue.

  Le port de gestion est utilisé pour la liaison HA1. Les ports TCP 28769 et 28260 pour les communications en texte clair ; le port 28 pour les communications cryptées (SSH sur TCP).
- **Liaison de données**—La liaison HA2 permet de synchroniser des sessions, des tables de transfert, des associations de sécurité IPSec et des tables ARP entre des périphériques d'une paire HA. Le flux de données de la liaison HA2 est toujours unidirectionnel (sauf pour la persistance HA2), du périphérique actif vers le périphérique passif.

  Ethernet1/1 doit être attribué comme liaison HA2. Cela est nécessaire pour déployer le pare-feu VM-Series sur AWS en mode HA. La liaison de données HA peut être configurée pour utiliser IP (numéro de protocole 99) ou UDP (port 29281) comme protocole de transport.

Dans AWS, le pare-feu VM-Series ne prend pas en charge les liens de secours pour HA1 ou HA2.

Analyse des pulsations et messages Hello

Les pare-feu utilisent les messages hello et les pulsations pour vérifier que le périphérique homologue est réactif et opérationnel. Les messages Hello sont envoyés par un homologue à un autre à un ***intervalle Hello*** configuré afin de vérifier l'état du périphérique. La pulsation est une requête ping ICMP envoyée à l'homologue HA sur la liaison de contrôle et l'homologue y répond pour indiquer que les périphériques sont connectés et réactifs. Pour plus d'informations sur les minuteurs HA qui déclenchent un basculement, reportez-vous à la section Minuteurs HA. (Les minuteurs HA des pare-feu VM-Series sont identiques à ceux des pare-feu PA-5200 Series.)

Priorité et préemption des périphériques

Les périphériques d'une paire HA peuvent être assignés à une valeur ***Priorité du périphérique*** afin d'indiquer une préférence pour laquelle un périphérique doit assumer un rôle actif et gérer le trafic lors d'un basculement. Si vous devez utiliser un périphérique spécifique dans la paire HA pour la sécurisation active du trafic, vous devez activer le comportement préemptif sur les deux pare-feu et assigner une valeur de priorité pour chaque périphérique. Le périphérique affichant la valeur numérique la plus basse et, par conséquent, la ***priorité la plus élevée***, est désigné comme étant actif et gère l'ensemble du trafic sur le réseau. L'autre périphérique est dans un état passif et synchronise les informations de configuration et d'état avec le périphérique actif afin d'être prêt à passer en état actif en cas d'échec.

Par défaut, la préemption est désactivée sur les pare-feu et doit être activée sur les deux périphériques. Lorsqu'il est activé, le comportement préemptif autorise le pare-feu affichant la ***priorité la plus élevée*** (valeur numérique la plus basse) à reprendre en état actif après avoir récupéré d'un échec. En cas de préemption, l'événement est consigné dans les journaux système.

La préemption n'est pas recommandée pour la HA dans le pare-feu VM-Series sur AWS.

Minuteurs HA

Les minuteurs haute disponibilité (HA) permettent de détecter une défaillance du pare-feu et de déclencher un basculement. Pour réduire la complexité de configuration des minuteurs HA, vous

 ©2023 Palo Alto Networks, Inc.

pouvez sélectionner l'un des trois profils suivants : **Recommended (Recommandé)**, **Aggressive (Agressif)** et **Advanced (Avancé)**. Ces profils renseignent automatiquement les valeurs optimales des minuteurs HA pour une plate-forme de pare-feu spécifique afin de permettre un déploiement HA accéléré.

Utilisez le profil **Recommended (Recommandé)** si vous souhaitez des paramètres de minuteur de basculement types ou le profil **Aggressive (Agressif)** si vous préférez des paramètres de minuteur de basculement plus rapides. Le profil **Advanced (Avancé)** vous permet de personnaliser les valeurs des minuteurs pour répondre à vos besoins en matière de réseau.

Minuteur HA sur les pare-feu VM-Series sur AWS	Valeurs par défaut pour les profils recommandé ou agressif
Délai de maintien de promotion	2000/500 ms
Intervalle Hello	8000/8000 ms
Intervalle de pulsation	2000/1000 ms
Nombre maximal de battements	3/3
Délai de maintien de préemption	1/1 min
Temps d'attente actif après l'échec de la surveillance	0/0 ms
Temps d'attente actif principal supplémentaire	500/500 ms

Configuration de la HA active/passive dans AWS à l'aide d'un IP secondaire

Effectuez la procédure suivante pour déployer les nouveaux pare-feu VM-Series en tant que paire HA avec des adresses IP secondaires.

STEP 1 | Avant de déployer les pare-feu VM-Series pour votre homologue HA, assurez-vous de ce qui suit :

- Reportez-vous à la fiche de planification VPC pour vous assurer que votre VPC est préparé pour le pare-feu VM-Series.
- La HA de déplacement d'IP secondaire nécessite le plugin VM-Series 2.0.1 ou une version ultérieure.
- Déployez les deux homologues HA dans la même zone de disponibilité AWS.

  À partir du plugin VM-Series 2.0.3, vous pouvez déployer les homologues HA dans différentes zones de disponibilité. Cependant, lors d'un événement de basculement HA, les tables de

 ©2023 Palo Alto Networks, Inc.

routage sont mises à jour mais l'IP secondaire n'est pas déplacé. Ce type de déploiement n'est pas recommandé.

- Créez un rôle IAM et affectez le rôle aux pare-feu VM-Series lors du déploiement des instances.
- Les pare-feu actifs et passifs doivent avoir au moins quatre interfaces chacun : une interface de gestion, une interface HA2, une interface non approuvée et une interface approuvée. En outre, les interfaces approuvée et non approuvée du pare-feu actif doivent se voir attribuer une adresse IP secondaire.

  L'interface de gestion doit être utilisée comme interface HA1.
- Vérifiez que les composants réseau et de sécurité sont définis de manière appropriée.
  - Activez la communication avec Internet. Le VPC par défaut inclut une passerelle Internet et si vous installez le pare-feu VM-Series dans le sous-réseau par défaut, il a accès à Internet.
  - Créez des sous-réseaux. Les sous-réseaux sont des segments de la plage d'adresses IP affectée au VPC dans lequel vous lancez les instances EC2. Le pare-feu VM-Series doit appartenir au sous-réseau public pour pouvoir être configuré pour l'accès à Internet.
  - Créez un groupe de sécurité des données qui comprend les interfaces de données du pare-feu. De plus, configurez la sécurité pour autoriser tout le trafic (0.0.0.0/0), afin que la sécurité soit renforcée par les pare-feu. Ceci est nécessaire pour maintenir les sessions existantes pendant le basculement.
  - Ajoutez des itinéraires à la table de routage pour un sous-réseau privé afin de vous assurer que le trafic peut être acheminé entre des sous-réseaux et des groupes de sécurité du VPC, le cas échéant.
- Si vous amorcez le pare-feu, créez le compartiment S3 nécessaire contenant les fichiers d'amorçage requis.

©2023 Palo Alto Networks, Inc.

STEP 2 | Déploiement du pare-feu VM-Series sur AWS.

1. Si votre pare-feu VM-Series n'a pas le plugin VM-Series 2.0.1 ou supérieur installé, mettez le plugin à niveau avant de continuer.
2. Configurez ethernet 1/1 comme interface HA2 sur chaque homologue HA.
   1. Ouvrez la console EC2 Amazon.
   2. Sélectionnez Network Interface (Interface réseau), puis choisissez et sélectionnez votre interface réseau.
   3. Sélectionnez **Actions** > **Manage IP Addresses (Gérer les adresses IP).**
   4. Laissez le champ vide pour permettre à AWS d'attribuer une adresse IP de manière dynamique ou saisissez une adresse IP dans la plage du sous-réseau pour le pare-feu VM-Series.
   5. Cliquez sur **Yes (Oui)** et sur **Update (Mettre à jour)**.
   6. Sélectionnez **Actions** > **Change Source/Dest (Changer Source/Dest). Check (Modifier la vérification de la source/destination)** et sélectionnez **Disable (Désactiver)**.
   7. Répétez ce processus sur le deuxième (à être passif) homologue HA.
3. Ajoutez une adresse IP secondaire à vos interfaces de plan de données sur le premier (à être actif) homologue HA.
   1. Sélectionnez **Network Interface (Interface réseau)**, puis choisissez et sélectionnez votre interface réseau.
   2. Sélectionnez **Actions** > **Manage IP Addresses (Gérer les adresses IP)** > **IPv4 Addresses (Adresses IPv4)** > **Assign new IP (Attribuer une nouvelle IP)**.
   3. Laissez le champ vide pour permettre à AWS d'attribuer une adresse IP de manière dynamique ou saisissez une adresse IP dans la plage du sous-réseau pour le pare-feu VM-Series.
   4. Cliquez sur **Yes (Oui)** et sur **Update (Mettre à jour)**.
4. Associez une adresse IP élastique (publique) secondaire à l'interface non approuvée de l'homologue actif.
   1. Sélectionnez **Elastic IPs (IP élastiques)** puis choisissez et sélectionnez l'adresse IP élastique à associer.
   2. Sélectionnez **Actions** > **Associate Elastic IP (Associer une IP élastique)**.
   3. Sous **Resource Type (Type de ressource)**, sélectionnez **Network Interface (Interface réseau)**.
   4. Choisissez l'interface réseau à laquelle associer l'adresse IP élastique.
   5. Cliquez sur **Associate (Associer)**.
5. Pour l'inspection du trafic sortant, ajoutez une entrée à la table de routage du sous-réseau qui définit le prochain saut comme l'interface approuvée du pare-feu.
   1. Sélectionnez **VPC** > **Route Tables (Tables de routage)**.
   2. Choisissez votre table de routage de sous-réseau.
   3. Sélectionnez **Actions** > **Edit routes (Modifier routes)** > **Add route (Ajouter route)**.
   4. Saisissez l'adresse IP ou le bloc CIDR de **Destination**.
   5. Pour **Target (Cibler)**, entrez dans l'interface réseau de l'interface approuvée du pare-feu.

 ©2023 Palo Alto Networks, Inc.

6. Cliquez sur **Save routes (Enregistrer routes)**.

6. Pour utiliser le routage des entrées AWS, créez une table de routage et associez-y la passerelle Internet. Ensuite, ajoutez une entrée avec le prochain saut défini comme l'interface non approuvée du pare-feu actif.
   1. Sélectionnez **Route Tables (Tables de routage)** > **Create Route Table (Créer une table de routage)**.
   2. (En option) Saisissez une **Name tag (Étiquette de nom)** descriptive pour votre table de routage.
   3. Cliquez sur **Create (Créer)**.
   4. Cliquez sur votre table de routage et sélectionnez **Actions** > **Edit edge associations (Modifier les associations périphériques)**.
   5. Sélectionnez **Internet gateways (Passerelles Internet)** et choisissez votre passerelle Internet VPC.
   6. Cliquez sur **Save (Enregistrer)**.
   7. Cliquez sur votre table de routage et sélectionnez **Actions** > **Edit routes (Modifier les routes)**.
   8. Pour **Target (Cible)**, sélectionnez **Network Interface (Interface réseau)** et choisissez l'interface non approuvée du pare-feu actif.
   9. Cliquez sur **Save routes (Enregistrer routes)**.

STEP 3 | Configurez les interfaces sur le pare-feu. Vous devez configurer la liaison de données HA2 et au moins deux interfaces Couche 3 pour vos interfaces non approuvée (Untrust) et approuvée (Trust). Terminez ce flux de travail sur le premier homologue HA puis répétez ces étapes sur le second homologue HA.

1. Connectez-vous à l'interface Web du pare-feu.
2. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**, puis cliquez sur votre interface non approuvée. Dans cet exemple, l'interface HA2 est 1/1, l'interface approuvée (Trust) est ethernet 1/2 et l'interface non approuvée (Untrust) est ethernet 1/3.
3. Cliquez sur la liaison **ethernet 1/1** et configurez comme suit :
   - **Interface Type (Type d'interface)** : **HA**
4. Cliquez sur le lien pour **ethernet 1/2** et configurez-le comme suit :
   - **Interface Type (Type d'interface)** : **Layer3 (Couche 3)**
   - Dans l'onglet **Config (Configuration)**, affectez l'interface au routeur par défaut.
   - Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Définissez une nouvelle zone, trust-zone par exemple, puis cliquez sur **OK**.
   - Dans l'onglet **IPv4**, sélectionnez **DHCP Client (Client DHCP)**.
   - Cochez **Enable (Activer)**.
   - Sur l'interface non approuvée, cochez **Automatically create default route pointing to default gateway provided by server (Créer automatiquement un itinéraire par défaut**

 ©2023 Palo Alto Networks, Inc.

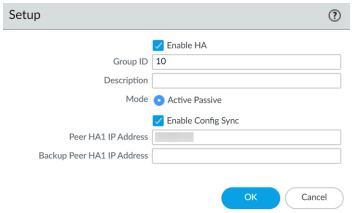
en direction de la passerelle par défaut fournie par le serveur). Cette option indique au pare-feu de créer une route statique vers une passerelle par défaut.

- Répétez ces étapes pour ethernet 1/3.

5. Répétez les étapes ci-dessus pour l'homologue passif.

STEP 4 | Activez HA.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**.
2. Modifiez les paramètres de configuration.
3. Saisissez l'adresse IP privée de l'homologue passif dans le champ **Peer HA1 IP address (Adresse IP de l'homologue HA1)**.
4. Cliquez sur **OK**.



5. Modifiez **Election Settings (Paramètres de sélection)** pour spécifier qu'un pare-feu particulier est l'homologue actif. Entrez une valeur numérique inférieure de **Device Priority (Priorité de périphérique)** sur le pare-feu actif. Si les deux pare-feu affichent une valeur de priorité du périphérique identique, le pare-feu disposant de la valeur MAC la plus basse sur le contrôle HA1 devient le pare-feu actif.

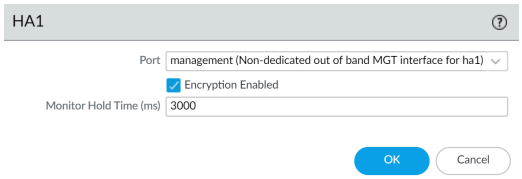
   L'activation de la préemption n'est pas recommandée.

6. Cliquez sur **OK**.
7. **Commit (Validez)** vos modifications.
8. Répétez les étapes ci-dessus pour l'homologue passif.

©2023 Palo Alto Networks, Inc.

STEP 5 | Configurez la liaison de contrôle (HA1) pour qu'elle utilise le port de gestion.

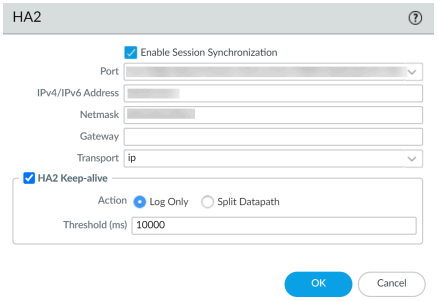
1. Sélectionnez **Device (Appareil)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la section Control Link (HA1) (Liaison de contrôle (HA1)).



2. (Facultatif) Sélectionnez **Encryption Enabled (Cryptage activé)** pour sécuriser la communication HA entre les homologues. Pour activer le cryptage, vous devez exporter la clé HA d'un périphérique et l'importer dans le périphérique homologue.
   1. Sélectionnez **Device (Appareil)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**.
   2. Sélectionnez **Export HD key (Exporter la clé HD)**. Enregistrez la clé HA sur un emplacement réseau auquel le périphérique homologue peut accéder.
   3. Dans l'appareil homologue, allez dans **Device (Appareil)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** et sélectionnez **Import HA key (Importer la clé HA)** pour accéder à l'emplacement dans lequel vous avez sauvegardé la clé et l'importer dans l'appareil homologue.

STEP 6 | Configurez la liaison de données (HA2) pour qu'elle utilise ethernet1/1.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la section Liaison de données (HA2).
2. Sélectionnez le **Port** ethernet1/1.
3. Saisissez l'adresse IP d'ethernet1/1. Cette adresse IP doit être identique à celle qui a été affectée à l'ENI sur le tableau de bord EC2.
4. Saisissez le **Netmask (Masque de réseau)**.
5. Saisissez une adresse IP de **Gateway (Passerelle)** si les interfaces HA1 se trouvent sur des sous-réseaux distincts.
6. Sélectionnez **IP** ou **UDP** comme **Transport (Protocole de transport)**. Utilisez **IP** si vous avez besoin d'un protocole de transport de couche 3 (numéro de protocole IP 99). Utilisez **UDP** si vous voulez que le pare-feu calcule la somme de contrôle sur l'ensemble du paquet et non sur l'en-tête comme c'est le cas avec l'option IP (port UDP n° 29281).



7. (Facultatif) Modifiez le **Threshold** (Seuil) des paquets de **HA2 Keep-alive** (Persistance HA2). Par défaut, la **HA2 Keep-alive (Persistance HA2)** est activée à des fins de surveillance de la liaison de données HA2 entre les homologues. En cas d'échec, si ce seuil (établi

 ©2023 Palo Alto Networks, Inc.

par défaut à 10000 ms) est dépassé, l'action définie se produira. Un message critique du journal système est généré en cas d'échec de la persistance HA2.

> *Vous pouvez configurer l'option **HA2 Keep-alive (Persistance HA2)** sur les deux périphériques ou sur un seul périphérique de la paire HA. Si vous activez cette option sur un seul périphérique, il sera le seul à envoyer des messages de persistance.*

STEP 7 | Une fois la HA configurée sur les deux pare-feu, vérifiez que les pare-feu sont appariés en mode HA active/passive.

1. Accédez au **Dashboard (Tableau de bord)** sur les deux pare-feu et affichez le widget High Availability (Haute disponibilité).
2. Sur l'homologue HA actif, cliquez sur **Sync to peer (Synchroniser à l'homologue)**.
3. Vérifiez que les pare-feu sont appariés et synchronisés.
   - Sur le pare-feu passif : l'état du pare-feu local doit afficher **Passive (Passif)** et la **Running Config (Configuration en cours)** doit être Synchronized (Synchronisée).
   - Sur le pare-feu actif : l'état du pare-feu local doit afficher **Active (Actif)** et la **Running Config (Configuration en cours)** doit être Synchronized (Synchronisée).
4. Depuis l'interface de ligne de commande (CLI) du pare-feu, exécutez les commandes suivante :
   - Pour vérifier l'état de préparation du basculement :

     ```
     show plugins vm_series aws ha state
     ```
   - Pour afficher le mappage d'IP secondaire :

     ```
     show plugins vm_series aws ha ips
     ```

Configuration de la HA active/passive dans AWS à l'aide du déplacement d'interface

Effectuez la procédure suivante pour configurer la HA active-passive en utilisant le mode de déplacement de l'interface.

STEP 1 | Assurez-vous que vous avez suivi les prérequis.

Pour le déploiement d'une paire de pare-feu VM-Series dans une configuration à HA dans le cloud AWS, vous devez vous assurer de faire ce qui suit :

- Sélectionnez le rôle IAM que vous avez créé lors du lancement du pare-feu VM-Series sur une instance EC2 ; vous ne pouvez affecter le rôle à une instance qui est en cours d'exécution. Reportez-vous à Rôles IAM pour la HA.

  Pour obtenir des instructions détaillées sur la création d'un rôle IAM, la détermination des comptes ou des services AWS qui peuvent assumer le rôle et la détermination des actions et

 ©2023 Palo Alto Networks, Inc.

des ressources API que l'application peut utiliser après avoir assumé le rôle, reportez-vous à la documentation d'AWS.

- DPDK n'est pas pris en charge par le pare-feu VM-Series sur AWS dans un déploiement HA à déplacement d'interface. Si vous avez le plugin VM-Series 2.0.1 ou plus récent sur votre pare-feu, vous devez désactiver DPDK.

  La désactivation de DPDK nécessite le redémarrage du pare-feu. Si vous utilisez l'amorçage pour déployer le pare-feu VM-Series, vous pouvez éviter de redémarrer le pare-feu en désactivant DPDK dans le fichier initi-cfg.txt, en utilisant **`op-cmd-dpdk-pkt-io=off`**. Pour plus d'informations, reportez-vous à la section Amorçage du pare-feu VM-Series sur AWS.
- Le pare-feu actif dans la paire HA doit avoir au moins trois ENI : deux interfaces de plan de données et une interface de gestion.

  Le pare-feu passif de la paire HA doit avoir une ENI pour la gestion et une ENI qui fonctionne comme interface de plan de données ; vous allez configurer l'interface du plan de données en tant qu'interface HA2.

  N'attachez pas d'interfaces de plan de données supplémentaires au pare-feu passif dans la paire HA. Lors du basculement, les interfaces du plan de données du pare-feu qui était précédemment actif sont déplacées (dissociées et puis associées) vers le pare-feu qui est désormais actif (précédemment passif).
- Les homologues HA doivent être déployés dans la même zone de disponibilité AWS.

STEP 2 | Lancez le pare-feu VM-Series sur AWS.

STEP 3 | (plugin VM-Series 2.0.1 ou supérieur) Désactivez DPDK sur les pare-feu actifs et passifs. DPDK est activé par défaut et le mode HA de déplacement d'interface ne supporte pas DPDK, vous devez donc le désactiver ; en activant Packet MMAP (Paquet MMAP).

1. Connectez-vous à la CLI du pare-feu passif.
2. Désactivez DPDK à l'aide de la commande suivante. L'exécution de cette commande redémarre le pare-feu.

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

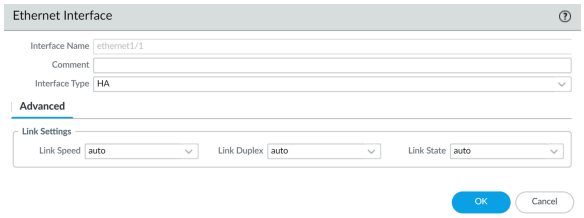
STEP 4 | Activez HA.

1. Sélectionnez **Device (Appareil)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la section Setup (Configuration).
2. Sélectionnez **Enable HD (Activer la HD)**.

©2023 Palo Alto Networks, Inc.

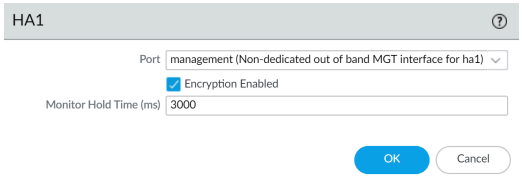
STEP 5 | Configurez ethernet 1/1 en tant qu'interface HA. Cette interface doit servir à la communication HA2.

1. Sélectionnez **Network (Réseau)** > **Interfaces**.
2. Confirmez que la liaison est activée sur ethernet1/1.
3. Cliquez sur la liaison de ethernet1/1 et définissez l'**Interface Type (Type d'interface)** sur HA.



STEP 6 | Configurez la liaison de contrôle (HA1) pour qu'elle utilise le port de gestion.

1. Sélectionnez **Device (Appareil)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la section Control Link (HA1) (Liaison de contrôle (HA1)).



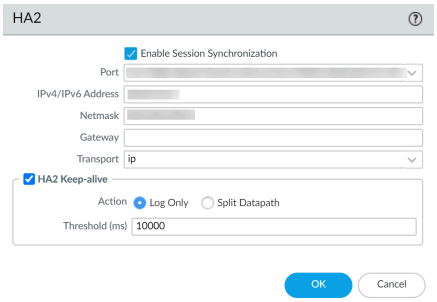
2. (Facultatif) Sélectionnez **Encryption Enabled (Cryptage activé)** pour sécuriser la communication HA entre les homologues. Pour activer le cryptage, vous devez exporter la clé HA d'un périphérique et l'importer dans le périphérique homologue.
   1. Sélectionnez **Device (Appareil)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**.
   2. Sélectionnez **Export HD key (Exporter la clé HD)**. Enregistrez la clé HA sur un emplacement réseau auquel le périphérique homologue peut accéder.
   3. Dans l'appareil homologue, allez dans **Device (Appareil)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** et sélectionnez **Import HA key (Importer la clé HA)** pour accéder à l'emplacement dans lequel vous avez sauvegardé la clé et l'importer dans l'appareil homologue.

STEP 7 | Configurez la liaison de données (HA2) pour qu'elle utilise ethernet1/1.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la section Liaison de données (HA2).
2. Sélectionnez le **Port** ethernet1/1.
3. Saisissez l'adresse IP d'ethernet1/1. Cette adresse IP doit être identique à celle qui a été affectée à l'ENI sur le tableau de bord EC2.
4. Saisissez le **Netmask (Masque de réseau)**.
5. Saisissez une adresse IP de **Gateway (Passerelle)** si les interfaces HA1 se trouvent sur des sous-réseaux distincts.
6. Sélectionnez **IP** ou **UDP** comme **Transport (Protocole de transport)**. Utilisez **IP** si vous avez besoin d'un protocole de transport de couche 3 (numéro de protocole IP 99). Utilisez

 ©2023 Palo Alto Networks, Inc.

UDP si vous voulez que le pare-feu calcule la somme de contrôle sur l'ensemble du paquet et non sur l'en-tête comme c'est le cas avec l'option IP (port UDP n° 29281).



7. (Facultatif) Modifiez le **Threshold** (Seuil) des paquets de **HA2 Keep-alive** (Persistance HA2). Par défaut, la **HA2 Keep-alive (Persistance HA2)** est activée à des fins de surveillance de la liaison de données HA2 entre les homologues. En cas d'échec, si ce seuil (établi par défaut à 10000 ms) est dépassé, l'action définie se produira. Un message critique du journal système est généré en cas d'échec de la persistance HA2.

   *Vous pouvez configurer l'option **HA2 Keep-alive (Persistance HA2)** sur les deux périphériques ou sur un seul périphérique de la paire HA. Si vous activez cette option sur un seul périphérique, il sera le seul à envoyer des messages de persistance.*

STEP 8 | Définissez la priorité des périphériques et activez la préemption.

Utilisez ce paramètre si vous voulez vous assurer qu'un périphérique donné est le périphérique actif privilégié. Pour plus d'informations, reportez-vous à la section Priorité et préemption des périphériques.

1. Sélectionnez **Device (Appareil)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la section Election Settings (Paramètres de sélection).
2. Définissez la valeur numérique dans **Device Priority (Priorité du périphérique)**. Veillez à définir une valeur numérique inférieure sur le périphérique auquel vous voulez assigner une priorité supérieure.

   Si les deux pare-feu affichent une valeur de priorité de périphérique identique, le pare-feu disposant de l'adresse MAC la plus basse sur la liaison de contrôle HA1 va devenir le périphérique actif.
3. Sélectionnez **Preemptive (Préemptif)**.

   Vous devez activer l'option Préemptif sur le périphérique actif et passif.
4. Modifiez les minuteurs de basculement. Par défaut, le profil de minuteur HA est défini sur **Recommended (Recommandé)** et est adapté à la plupart des déploiements HA.

STEP 9 | (Facultatif) Modifiez le temps d'attente avant le déclenchement d'un basculement.

1. Sélectionnez **Device (Appareil)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la section Active/Passive Settings (Paramètres actif/passif).
2. Modifiez le **Monitor fail hold up time (Temps d'attente actif après l'échec de la surveillance)** à une valeur entre 1 et 60 minutes ; la valeur par défaut est établie à 1 minute. Il s'agit de l'intervalle de temps pendant laquelle le pare-feu demeurera actif

 ©2023 Palo Alto Networks, Inc.

en cas d'échec d'une liaison. Utilisez ce paramètre pour empêcher que le battement occasionnel de périphériques à proximité ne déclenche un basculement HA.

STEP 10 | Configurez l'adresse IP de l'homologue HA.

1. Sélectionnez **Device (Appareil)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la section Setup (Configuration).
2. Saisissez l'adresse IP du port HA1 sur l'homologue. Il s'agit de l'adresse IP qui a été affectée à l'interface de gestion (ethernet 0/0), laquelle constitue également la liaison HA1 qui se trouve sur l'autre pare-feu.
3. Définissez le numéro du **Group ID (ID de groupe)** sur une valeur entre 1 et 63. On ne peut laisser ce champ vide, bien que cette valeur ne soit pas utilisée sur le pare-feu WM-Series dans AWS.

STEP 11 | Configurez l'autre homologue.

Répétez les étapes 3 à 9 sur l'homologue HA.

STEP 12 | Une fois les deux périphériques configurés, vérifiez qu'ils sont appariés en mode actif/passif HA.

1. Accédez au **Dashboard (Tableau de bord)** sur les deux périphériques et affichez le widget **High Availability (Haute disponibilité)**.
2. Sur le périphérique actif, cliquez sur le lien **Sync to peer (Synchroniser avec l'homologue)**.
3. Vérifiez que les périphériques sont appariés et synchronisés comme indiqué ci-dessous :
   - Sur le périphérique passif : l'état du périphérique local doit afficher **passive (passif)** et la configuration est **synchronized (synchronisée)**.
   - Sur le périphérique actif : l'état du périphérique local doit afficher **active (actif)** et la configuration est **synchronized (synchronisée)**.

STEP 13 | Vérifiez que le basculement se fait correctement.

1. Vérifiez le mode HA.
   ```
   show plugins vm_series aws ha failover-mode
   ```
2. Vérifiez que le mode packet IO est réglé sur le mode packet MMAP.
   ```
   show system setting dpdk-pkt-io
   ```
3. Éteignez l'homologue HA actif.
   1. Sur le tableau de bord EC2, sélectionnez **Instances**.
   2. Dans la liste, sélectionnez le pare-feu VM-Series, puis cliquez sur **Actions** > **Stop (Arrêter)**.
4. Vérifiez que l'homologue passif assume le rôle de son homologue actif et que les interfaces du plan de données se sont déplacées vers l'homologue HA qui est désormais actif.

Migration de la HA active/passive dans AWS

Les deux modes de haute disponibilité sont pris en charge, ce qui vous permet de migrer entre chaque mode si votre déploiement l'exige. Le mode de déplacement d'interface ne prenant pas en charge DPDK, vous devez le désactiver sur le pare-feu VM-Series avant de terminer la migration.

 ©2023 Palo Alto Networks, Inc.

Pour désactiver DPDK, vous devez redémarrer le pare-feu VM-Series, ce qui aura un impact sur toutes les sessions de trafic sur le pare-feu actif.

- Migration de la HA active/passive dans AWS à l'aide d'un IP secondaire
- Migration de la HA active/passive dans AWS à l'aide du mode de déplacement d'interface

Migration de la HA active/passive dans AWS à l'aide d'un IP secondaire

Suivez la procédure suivante pour migrer votre paire HA de pare-feu VM-Series existante de la HA de déplacement d'interface à la HA d'IP secondaire.

La HA de déplacement d'IP secondaire nécessite le plugin VM-Series 2.0.1 ou une version ultérieure.

STEP 1 | Mise à niveau du plug-in VM-Series sur l'homologue HA passif, puis sur l'homologue actif.

STEP 2 | Créez une adresse IP secondaire pour toutes les interfaces de données sur l'homologue actif.

1. Connectez-vous à la console EC2 AWS.
2. Sélectionnez **Network Interface (Interface réseau)**, puis choisissez et sélectionnez votre interface réseau.
3. Sélectionnez **Actions** > **Manage IP Addresses (Gérer les adresses IP)** > **IPv4 Addresses (Adresses IPv4)** > **Assign new IP (Attribuer une nouvelle IP)**.
4. Laissez le champ vide pour permettre à AWS d'attribuer une adresse IP de manière dynamique ou saisissez une adresse IP dans la plage du sous-réseau pour le pare-feu VM-Series.
5. Cliquez sur **Yes (Oui)** et sur **Update (Mettre à jour)**.

STEP 3 | Associez une adresse IP élastique (publique) secondaire à l'interface non approuvée de l'homologue actif.

1. Connectez-vous à la console EC2 AWS.
2. Sélectionnez **Elastic IPs (IP élastiques)** puis choisissez et sélectionnez l'adresse IP élastique à associer.
3. Sélectionnez **Actions** > **Associate Elastic IP (Associer une IP élastique)**.
4. Sous **Resource Type (Type de ressource)**, sélectionnez **Network Interface (Interface réseau)**.
5. Choisissez l'interface réseau à laquelle associer l'adresse IP élastique.
6. Cliquez sur **Associate (Associer)**.

©2023 Palo Alto Networks, Inc.

STEP 4 | Créez une table de routage pointant le sous-réseau contenant l'interface approuvée.

1. Sélectionnez **Route Tables (Tables de routage)** > **Create Route Table (Créer une table de routage)**.
2. (En option) Saisissez une **Name tag (Étiquette de nom)** descriptive pour votre table de routage.
3. Sélectionnez votre **VPC**.
4. Cliquez sur **Create (Créer)**.
5. Sélectionnez **Subnet Associations (Associations de sous-réseau)** > **Edit subnet associations (Modifier les associations de sous-réseau)**.
6. Cochez la case **Associate (Associer)** pour le sous-réseau contenant l'interface approuvée.
7. Cliquez sur **Save (Enregistrer)**.

STEP 5 | Mettez à jour les rôles IAM avec les actions et les autorisations supplémentaires requises pour migrer vers l'HA de déplacement d'IP secondaire.

Action, autorisation ou ressource IAM	Description
AssociateAddress	Pour les autorisations de déplacer des adresses IP publiques associées aux adresses IP primaires des interfaces passives vers les interfaces actives.
AssignPrivateIpAddresses	Pour les autorisations de déplacer des adresses IP secondaires et des adresses IP publiques associées des interfaces passives vers les interfaces actives.
UnassignPrivateIpAddress	Pour les autorisations de désattribuer des adresses IP secondaires et des adresses IP publiques associées des interfaces sur l'homologue actif.
DescribeRouteTables	Pour l'autorisation de récupérer toutes les tables de routage associées aux instances du pare-feu VM-Series.
ReplaceRoute	Pour l'autorisation de mettre à jour des entrées de la table de routage AWS.
GetPolicyVersion	Pour l'autorisation de récupérer les informations sur la version de la politique AWS.
GetPolicy	Pour l'autorisation de récupérer les informations sur la politique AWS.
ListAttachedRolePolicies	Pour l'autorisation de récupérer la liste de toutes les politiques gérées associées à un rôle IAM spécifié.
ListRolePolicies	Pour l'autorisation de récupérer une liste des noms des politiques en ligne intégrées dans un rôle IAM spécifié.

©2023 Palo Alto Networks, Inc.

Action, autorisation ou ressource IAM	Description
GetRolePolicy	Pour l'autorisation de récupérer une politique en ligne spécifique intégrée dans un rôle IAM spécifié.
policy	Pour l'autorisation d'accéder à la politique IAM Amazon Resource Name (ARN).
role	Pour l'autorisation d'accéder aux rôles IAM ARN.
route-table	Pour l'autorisation d'accéder à la table de routage ARN.
Caractère générique (*)	Dans le champ ARN, utilisez* comme caractère générique.

STEP 6 | Créez de nouvelles interfaces (ENI) sur le pare-feu passif dans le même sous-réseau que les interfaces de données du pare-feu actif.

N'attribuez pas d'adresses IP secondaires à ces nouvelles interfaces.

1. Ouvrez la console EC2 Amazon.
2. Sélectionnez **Network Interfaces (Interfaces réseau)** > **Create Network Interfaces (Créer des interfaces réseau)**.
3. Saisissez un **Name (Nom)** descriptif pour votre nouvelle interface.
4. Sous **Subnet (Sous-réseau)**, sélectionnez le sous-réseau de l'interface non approuvée du pare-feu actif.
5. Sous **Private IP (IP privée)**, laissez le champ vide pour permettre à AWS d'attribuer une adresse IP de manière dynamique ou saisissez une adresse IP dans la plage du sous-réseau pour l'interface non approuvée du pare-feu actif.
6. Sous **Security groups (Groupes de sécurité)**, sélectionnez un ou plusieurs groupes de sécurité.
7. Sélectionnez **Yes (Oui)** et **Create (Créer)**.
8. Sélectionnez **Actions** > **Change Source/Dest. Check (Modifier la vérification de la source/destination)** et sélectionnez **Disable (Désactiver)**.
9. Répétez ces étapes pour le sous-réseau de l'interface approuvée du pare-feu actif.

STEP 7 | Associez les nouvelles ENI à l'instance du pare-feu passif. Vous devez associer ces ENI au pare-feu passif dans le bon ordre, car la méthode HA d'IP secondaire est basée sur l'index d'interface réseau attribué par AWS. Par exemple, si eth1/2 sur le pare-feu actif fait partie du sous-réseau A et que eth1/3 fait partie du sous-réseau B, alors vous devez associer l'interface qui fait partie du sous-réseau A et l'interface qui fait partie du sous-réseau B. Dans cet exemple, AWS a attribué une valeur d'index de 2 à eth1/2 et une valeur de 3 à eth1/3. Cette indexation doit être maintenue pour que le basculement se fasse avec succès.

1. Pour associer les ENI créées ci-dessus, sélectionnez l'interface non approuvée que vous avez créée et cliquez sur **Attach (Associer)**.

©2023 Palo Alto Networks, Inc.

2. Sélectionnez l'ID d'instance du pare-feu passif, puis cliquez sur **Attach (Associer)**.
3. Répétez ces étapes pour l'interface approuvée.

STEP 8 | Connectez-vous au pare-feu passif et configurez les interfaces pour obtenir leurs adresses IP via DHCP.

1. Connectez-vous à l'interface Web du pare-feu VM-Series passif.
2. Sélectionnez **Network (Réseau)** > **Interfaces**.
3. Cliquez sur la première interface de données.
4. Sélectionnez **IPv4**.
5. Sélectionnez **DHCP Client (Client DHCP)**.
6. Sur l'interface non approuvée uniquement, sélectionnez **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)**.
7. Cliquez sur OK.
8. Répétez ce processus pour chaque interface de données.

STEP 9 | Si vous avez configuré des politiques NAT sur le pare-feu VM-Series qui référencent les adresses IP privées des interfaces de données, ces politiques doivent être mises à jour pour référencer les adresses IP secondaires nouvellement attribuées à la place.

1. Accédez à l'interface Web du pare-feu VM-Series actif.
2. Sélectionnez **Policies (Politiques)** > **NAT**.
3. Cliquez sur la règle de politique NAT à modifier, puis sur **Translated Packet (Paquet traduit)**.
4. Sous **Translated Address (Adresse traduite)**, cliquez sur Add (Ajouter) et saisissez l'adresse IP secondaire créée dans AWS.
5. Supprimez l'adresse IP principale.
6. Cliquez sur **OK**.
7. Répétez ces étapes si nécessaire.
8. **Commit (Validez)** vos modifications.

STEP 10 | Activez le mode de basculement HA d'IP secondaire.

1. Accédez à la CLI du pare-feu VM-Series sur l'homologue actif.
2. Exécutez la commande suivante.

   ```
   request plugins vm_series aws ha failover-mode secondary-ip
   ```
3. Validez vos modifications.
4. Confirmez votre mode HA en exécutant la commande suivante.

   ```
   show plugins vm_series aws ha failover-mode
   ```
5. Répétez cette commande sur l'homologue passif.

 ©2023 Palo Alto Networks, Inc.

STEP 11 | Une fois la HA configurée sur les deux pare-feu, vérifiez que les pare-feu sont appariés en mode HA active/passive.

1. Accédez au **Dashboard (Tableau de bord)** sur les deux pare-feu et affichez le widget High Availability (Haute disponibilité).
2. Sur l'homologue HA actif, cliquez sur **Sync to peer (Synchroniser à l'homologue)**.
3. Vérifiez que les pare-feu sont appariés et synchronisés.
   - Sur le pare-feu passif : l'état du pare-feu local doit afficher **Passive (Passif)** et la **Running Config (Configuration en cours)** doit être Synchronized (Synchronisée).
   - Sur le pare-feu actif : l'état du pare-feu local doit afficher **Active (Actif)** et la **Running Config (Configuration en cours)** doit être Synchronized (Synchronisée).
4. Depuis l'interface de ligne de commande (CLI) du pare-feu, exécutez les commandes suivante :
   - Pour vérifier l'état de préparation du basculement :

     ```
     show plugins vm_series aws ha state
     ```
   - Pour afficher le mappage d'IP secondaire :

     ```
     show plugins vm_series aws ha ips
     ```

Migration de la HA active/passive dans AWS à l'aide du mode de déplacement d'interface

Suivez la procédure suivante pour migrer votre paire HA de pare-feu VM-Series existante de la HA d'IP secondaire à la HA d'interface mobile.

STEP 1 | Désactivez la prise en charge de DPDK sur l'homologue HA passif. Le mode HA de déplacement d'interface-ne prend pas en charge DPDK. Vous devez donc le désactiver, en activant Packet MMAP (Paquet MMAP).

1. Connectez-vous à la CLI du pare-feu passif.
2. Désactivez DPDK à l'aide de la commande suivante. L'exécution de cette commande redémarre le pare-feu.

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

STEP 2 | Désactivez la prise en charge de DPDK sur l'homologue HA actif.

1. Connectez-vous à la CLI du pare-feu actif.
2. Désactivez DPDK à l'aide de la commande suivante. L'exécution de cette commande redémarre le pare-feu.

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

   Le redémarrage du pare-feu aura un impact sur le trafic.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Passez du mode HA sur l'homologue actif du mode d'IP secondaire au mode de déplacement d'interface.

1. Accédez à la CLI du pare-feu VM-Series sur l'homologue actif.
2. Exécutez la commande suivante.

   ```
   request plugins vm_series aws ha failover-mode interface-move
   ```
3. Validez vos modifications.
4. Confirmez votre mode HA en exécutant la commande suivante.

   ```
   show plugins vm_series aws ha failover-mode
   ```
5. Répétez cette commande sur l'homologue passif.

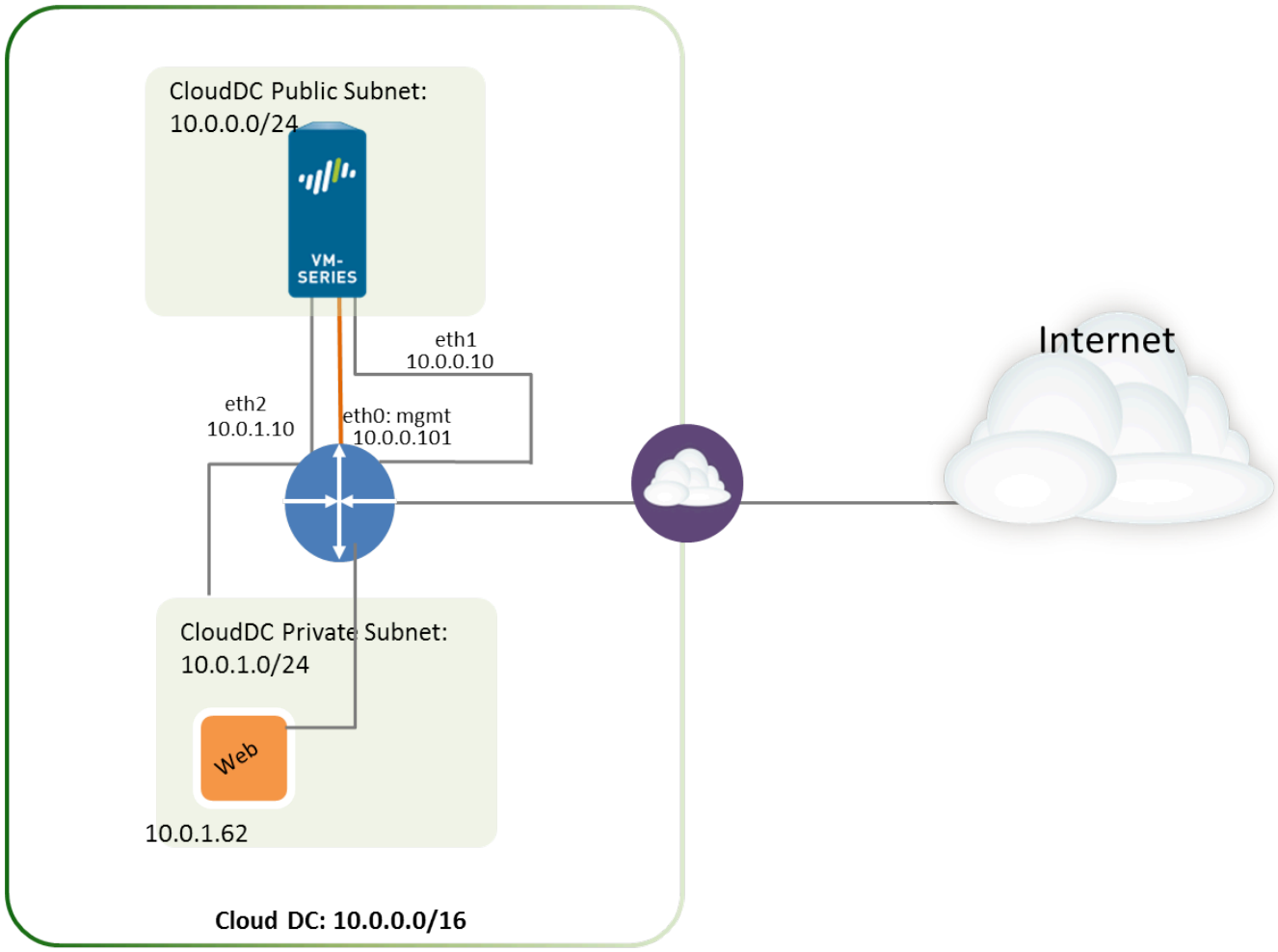
STEP 4 | Supprimez les interfaces de données de l'instance de pare-feu passif.

1. Connectez-vous à la console EC2 AWS.
2. Sélectionnez **Network Interfaces (Interfaces réseau)**.
3. Sélectionnez une interface de données sur l'instance de pare-feu passif et cliquez sur **Delete (Supprimer)**.
4. Dans la fenêtre **Delete Network Interface (Supprimer l'interface réseau)**, cliquez sur **Yes, Delete (Oui, supprimer)**.
5. Répétez ce processus pour chaque interface de données sur l'instance de pare-feu passif.

©2023 Palo Alto Networks, Inc.

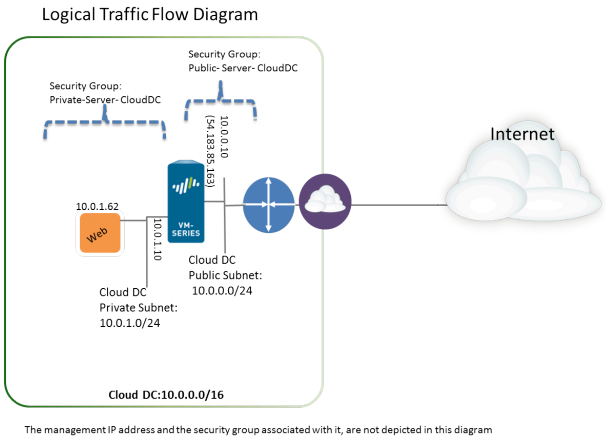
Cas d'utilisation : Sécurisation des instances EC2 dans le cloud AWS

Dans cet exemple, le VPC est déployé dans le réseau 10.0.0.0/16 avec deux sous-réseaux /24 : 10.0.0.0/24 et 10.0.1.0/24. Le pare-feu VM-Series sera lancé dans le sous-réseau 10.0.0.0/24 auquel la passerelle Internet est liée. Le sous-réseau 10.0.1.0/24 est un sous-réseau privé qui hébergera les instances EC2 devant être sécurisées par le pare-feu VM-Series. Tout serveur sur ce sous-réseau privé utilise NAT pour une adresse IP acheminable (il s'agit d'une adresse IP élastique) afin d'accéder à Internet. Utilisez la Planification de la fiche de travail du pare-feu VM-Series dans AWS VPC pour planifier la conception de votre VPC. Grâce à l'enregistrement de plages de sous-réseaux, d'interfaces réseau et des adresses IP associées des instances EC2, et de groupes de sécurité, le processus de configuration sera simplifié et plus fiable.



L'image suivante illustre le flux de trafic logique vers/depuis le serveur Web et Internet. Le trafic vers/depuis le serveur Web est envoyé à l'interface de données du pare-feu VM-Series associé au sous-réseau privé. Le pare-feu applique une politique et des processus de trafic entrant/sortant depuis/vers la passerelle Internet du VPC. L'image illustre également les groupes de sécurité auxquels les interfaces de données sont associées.

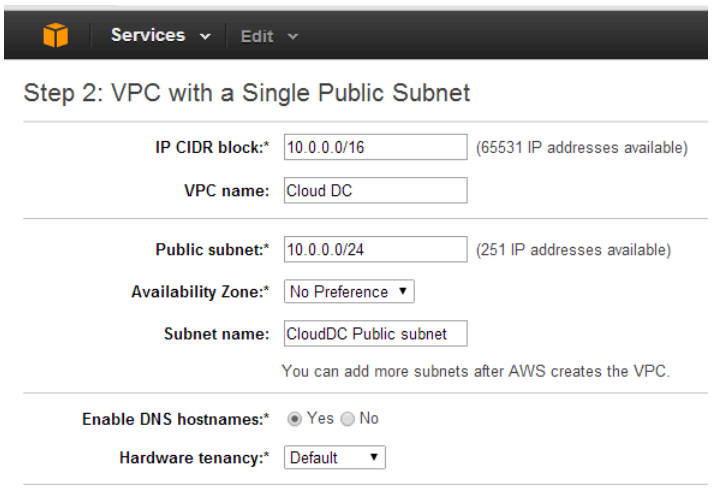
©2023 Palo Alto Networks, Inc.



STEP 1 | Créez un nouveau VPC avec un sous-réseau public (ou sélectionnez un VPC existant).

1. Connectez-vous à la console AWS et sélectionnez le tableau de bord **VPC**.
2. Vérifiez que vous avez sélectionné la zone géographique appropriée (région AWS). Le VPC sera déployé dans la région sélectionnée.
3. Sélectionnez **Start VPC Wizard (Démarrer l'assistant VPC)**, puis **VPC with a Single Public Subnet (VPC avec un seul sous-réseau public)**.

   Dans cet exemple, le bloc CIDR IP du VPC est 10.0.0.0/16, le nom du VPC est Cloud DC, le sous-réseau public est 10.0.0.0/24, et le nom du sous-réseau est Cloud DC Public. Vous créerez un sous-réseau privé après la création du VPC.



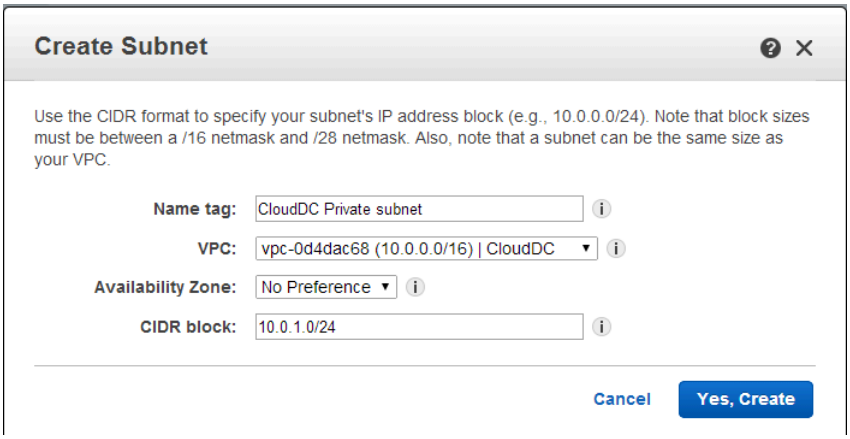
4. Cliquez sur **Create VPC (Créer un VPC)**.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Créez un sous-réseau privé.

Sélectionnez **Subnets (Sous-réseaux)**, puis cliquez sur **Create a Subnet (Créer un sous-réseau)**. Fournissez les informations.

Dans cet exemple, le **Name tag (Nom d'étiquette)** du sous-réseau est Web/DB Server Subnet. Il est créé dans le VPC Cloud Datacenter et affecté au bloc CIDR 10.0.1.0/24.



 ©2023 Palo Alto Networks, Inc.

STEP 3 | Créez une nouvelle table de routage pour chaque sous-réseau.

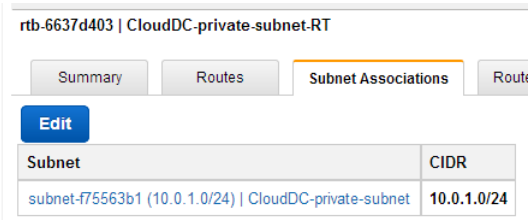
Bien qu'une table de routage principale soit automatiquement créée sur le VPC, nous recommandons de créer de nouvelles tables de routage plutôt que de modifier la table de routage par défaut.

Pour diriger le trafic sortant de chaque sous-réseau, vous ajouterez des itinéraires à la table de routage associée à chaque sous-réseau, ultérieurement dans ce flux de travail.

1. Sélectionnez **Route Tables (Tables de routage)** > **Create Route Table (Créer une table de routage)**.
2. Ajoutez un **Name (Nom)**, CloudDC-public-subnet-RT par exemple, sélectionnez le **VPC** que vous avez créé à l'étape 1, puis cliquez sur **Yes, Create (Oui, créer)**.
3. Sélectionnez la table de routage, cliquez sur **Subnet Associations (Associations de sous-réseau)**, puis sélectionnez le sous-réseau public.



4. Sélectionnez **Create Route Table (Créer une table de routage)**.
5. Ajoutez un **Name (Nom)**, CloudDC-private-subnet-RT par exemple, sélectionnez le **VPC** que vous avez créé à l'étape 1, puis cliquez sur **Yes, Create (Oui, créer)**.
6. Sélectionnez la table de routage, cliquez sur **Subnet Associations (Associations de sous-réseau)**, puis sélectionnez le sous-réseau privé.



STEP 4 | Créez des groupes de sécurité pour limiter l'accès Internet entrant/sortant aux instances EC2 dans le VPC.

Par défaut, AWS interdit la communication entre des interfaces n'appartenant pas au même groupe de sécurité.

Sélectionnez **Security Groups (Groupes de sécurité)**, puis cliquez sur le bouton **Create Security Group (Créer un groupe de sécurité)**. Dans cet exemple, nous créons trois groupes de sécurité avec les règles d'accès entrant suivantes :

- CloudDC-Management qui spécifie les protocoles et adresses IP source pouvant se connecter à l'interface de gestion du pare-feu VM-Series. Vous avez besoin, au minimum, de SSH et

 ©2023 Palo Alto Networks, Inc.

HTTPS. Dans cet exemple, nous activons SSH, ICMP, HTTP et HTTPS sur les interfaces associées à ce groupe de sécurité.

L'interface de gestion (eth 0/0) du pare-feu VM-Series sera affectée à CloudDC-management-sg.

- Public-Server-CloudDC qui spécifie les adresses IP source pouvant se connecter via HTTP, FTP, SSH dans le VPC. Ce groupe autorise le trafic entre le réseau externe et le pare-feu.

  L'interface du dataplane eth 1/1 du pare-feu VM-Series sera affectée à Public-Server-CloudDC.

- Private-Server-CloudDC qui dispose d'un accès très limité. Il permet uniquement aux autres instances EC2 du même sous-réseau de communiquer entre elles et avec le pare-feu VM-Series.

  L'interface du dataplane eth1/2 du pare-feu VM-Series et l'application du sous-réseau privés seront associées à ce groupe de sécurité.

  Les captures d'écran suivantes illustrent les groupes de sécurité qui correspondent au présent cas d'utilisation.

Name tag	Group ID	Group Name	VPC	Description
CloudDC-private-subnet-sg	sg-6c32c409	Private-Server-CloudDC	vpc-0d4dac68 (10.0.0.0/16) |...	For Private Servers to comm...
CloudDC-public-subnet-sg	sg-6832c40d	Public-Server-CloudDC	vpc-0d4dac68 (10.0.0.0/16) |...	External Traffic to VM-Series
CloudDC-management-sg	sg-9735c3f2	CloudDC-Managment	vpc-0d4dac68 (10.0.0.0/16) |...	CloudDC-Management
	sg-1035c375	default	vpc-0d4dac68 (10.0.0.0/16) |...	default VPC security group

STEP 5 | Déployez le pare-feu VM-Series.

Seule l'interface réseau principale qui servira d'interface de gestion sera associée et configurée pour le pare-feu lors du premier lancement. Les interfaces réseau nécessaires pour la gestion du trafic de données seront ajoutées à l'étape 6.

Reportez-vous à l'étape 3 dans Lancement du pare-feu VM-Series sur AWS.

©2023 Palo Alto Networks, Inc.

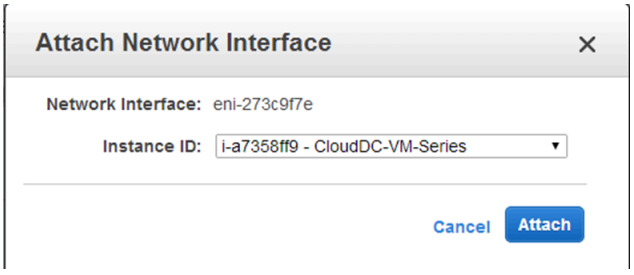
STEP 6 | Créez et associez la ou les interface(s) réseau virtuel, également appelée(s) ENI (Elastic Network Interface), au pare-feu VM-Series. Ces ENI sont utilisées pour la gestion du trafic de données depuis/vers le pare-feu.

1. Sur le tableau de bord EC2, sélectionnez **Network Interfaces (Interfaces réseau)**, puis cliquez sur **Create Network Interface (Créer une interface réseau)**.
2. Donnez un nom descriptif à l'interface.
3. Sélectionnez le sous-réseau. Utilisez l'ID de sous-réseau pour vérifier que vous avez sélectionné le bon sous-réseau. Vous ne pouvez lier qu'une seule ENI à une instance d'un même sous-réseau.
4. Saisissez l'adresse **Private IP (IP privée)** que vous souhaitez affecter à l'interface ou sélectionnez **Auto-assign (Affectation automatique)** pour affecter automatiquement une adresse IP parmi les adresses IP disponibles du sous-réseau sélectionné.
5. Sélectionnez le **Security group (Groupe de sécurité)** contrôlant l'accès à l'interface réseau.
6. Cliquez sur **Yes, Create (Oui, créer)**.

   Dans cet exemple, nous créons deux interfaces avec la configuration suivante :

Name	Network interfa	Subnet ID	VPC ID	Zone	Security group	Description	Instance ID
CloudDC-VM-Series-Untrust	eni-bcf355e5	subnet-ef5563a9	vpc-0d4dac68	us-west-1a	Public-Server-...	CloudDC-VM-Series-untrust	i-a7358ff9
CloudDC-VM-Series-Trust	eni-abf355f2	subnet-f75563b1	vpc-0d4dac68	us-west-1a	Private-Server-...	CloudDC-VM-Series-Trust	i-a7358ff9

   - Pour Eth1/1 (VM-Series-Untrust)
     - Sous-réseau : 10.0.0.0/24
     - IP privée : 10.0.0.10
     - Groupe de sécurité : Public-Server-CloudDC
   - Pour Eth1/2 (VM-Series-Trust)
     - Sous-réseau : 10.0.1.0/24
     - IP privée : 10.0.1.10
     - Groupe de sécurité : Private-Server-CloudDC
7. Pour associer l'ENI au pare-feu VM-Series, sélectionnez l'interface que vous venez de créer, puis cliquez sur **Attach (Associer)**.



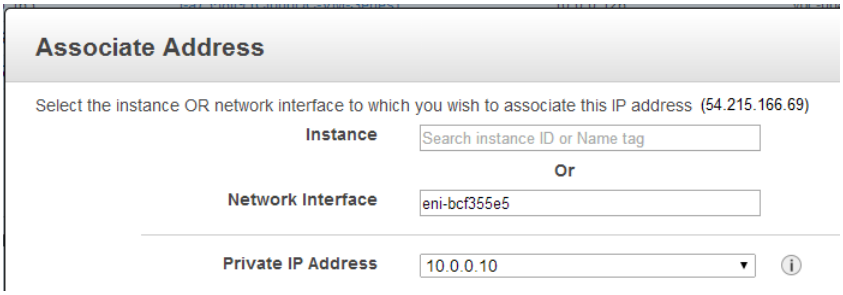
8. Sélectionnez l'**Instance ID (ID d'instance)** du pare-feu VM-Series, puis cliquez sur **Attach (Associer)**.
9. Répétez les étapes 7 et 8 pour associer l'autre interface réseau.

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Créez une adresse IP élastique et associez-la à l'interface réseau du dataplane du pare-feu qui doit disposer d'un accès direct à Internet.

Dans cet exemple, une EIP est affectée à VM-Series_Non approuvée. L'EIP associée à l'interface est l'adresse IP accessible du serveur Web dans le sous-réseau privé.

1. Sélectionnez **Elastic IPs (IP élastiques)**, puis cliquez sur **Allocate New Address (Allouer une nouvelle adresse)**.
2. Sélectionnez **EC2-VPC**, puis cliquez sur **Yes, Allocate (Oui, allouer)**.
3. Sélectionnez la nouvelle EIP allouée, puis cliquez sur **Associate Address (Associer l'adresse)**.
4. Sélectionnez la **Network Interface (Interface réseau)** et la **Private IP address (Adresse IP privée)** associée à l'interface, puis cliquez sur **es, Allocate (Oui, allouer)**.



Dans cet exemple, la configuration est la suivante :

Address	Instance	Private IP Address	Scope	Public DNS
54.183.85.163	i-a7358ff9 (CloudDC-VM-Series)	10.0.0.126	vpc-0d4dac68	ec2-54-183-85-163.us-west-...
54.215.166.69	i-a7358ff9 (CloudDC-VM-Series)	10.0.0.10	vpc-0d4dac68	ec2-54-215-166-69.us-west-...

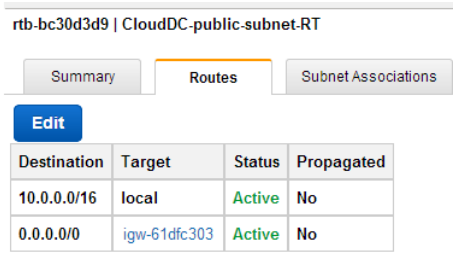
STEP 8 | Désactivez la vérification de la source/destination sur chaque interface réseau associée au pare-feu VM-Series. La désactivation de cet attribut permet à l'interface de gérer le trafic réseau non destiné à son adresse IP.

1. Sélectionnez l'interface réseau dans l'onglet **Network Interfaces (Interfaces réseau)**.
2. Dans la liste déroulante **Action**, sélectionnez **Change Source/Dest. (Modifier la source/dest.) Check (Vérifier)** .
3. Cliquez sur **Disabled (Désactivé)** et **Save (Enregistrez)** vos modifications.
4. Répétez les étapes 1 à 3 pour d'autres interfaces réseau, firewall-1/2 dans cet exemple.

©2023 Palo Alto Networks, Inc.

STEP 9 | Dans la table de routage associée au sous-réseau public (de l'étape 3), ajoutez un itinéraire par défaut vers la passerelle Internet pour le VPC.

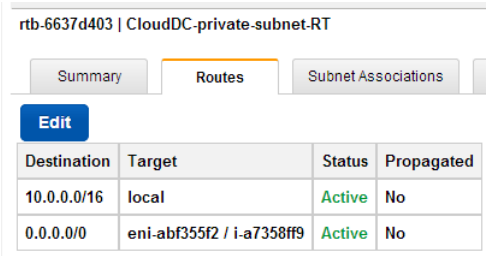
1. Dans le tableau de bord VPC, sélectionnez **Route Tables (Tables de routage)** et recherchez la table de routage associée au sous-réseau public.
2. Sélectionnez la table de routage, **Routes (Itinéraires)**, puis cliquez sur **Edit (Modifier)**.
3. Ajoutez un itinéraire pour transférer des paquets de ce sous-réseau à la passerelle Internet. Dans cet exemple, 0.0.0.0/0 indique que l'ensemble du trafic depuis/vers ce sous-réseau utilisera la passerelle Internet associée au VPC.



STEP 10 | Dans la table de routage associée au sous-réseau privé, ajoutez un itinéraire par défaut pour envoyer du trafic au pare-feu VM-Series.

L'ajout de cet itinéraire permet le transfert de trafic depuis les instances EC2 de ce sous-réseau privé vers le pare-feu VM-Series.

1. Dans le tableau de bord VPC, sélectionnez **Route Tables (Tables de routage)** et recherchez la table de routage associée au sous-réseau privé.
2. Sélectionnez la table de routage, **Routes (Itinéraires)**, puis cliquez sur **Edit (Modifier)**.
3. Ajoutez un itinéraire pour transférer des paquets de ce sous-réseau à l'interface réseau du pare-feu VM-Series résidant sur le même sous-réseau. Dans cet exemple, 0.0.0.0/0 indique que l'ensemble du trafic depuis/vers ce sous-réseau utilisera eni-abf355f2 (ethernet 1/2, à savoir CloudDC-VM-Series-Approuvée) sur le pare-feu VM-Series.



Pour chaque serveur Web ou de base de données déployé sur l'instance EC2 dans le sous-réseau privé, vous devez définir un itinéraire par défaut vers l'adresse IP du pare-feu VM-Series afin que le pare-feu soit la passerelle par défaut du serveur.

Effectuez les étapes 11 à 16 sur le pare-feu VM-Series.

©2023 Palo Alto Networks, Inc.

STEP 11 | Configurez un nouveau mot de passe administratif pour le pare-feu.

> ***Un outil SSH tel que PuTTY est nécessaire pour accéder à la CLI sur le pare-feu et modifier le mot de passe administratif par défaut. Vous ne pouvez pas accéder à l'interface Web tant que n'avez pas activé SSH et modifié le mot de passe par défaut.***

1. Utilisez l'adresse IP publique, que vous avez configurée sur le pare-feu, vers SSH dans l'interface de ligne de commande (CLI) du pare-feu VM-Series.

   Vous aurez besoin de la clé privée que vous avez utilisée ou créée dans Lancement du pare-feu VM-Series sur AWS, aux étapes 3-12, pour accéder à la CLI.
2. Saisissez la commande suivante pour vous connecter au pare-feu :

   ssh-i *<private_key_name>* admin@*<public-ip_address>*
3. Configurez un nouveau mot de passe à l'aide de la commande suivante, et suivez les invites affichées à l'écran :

   configure
   set mgt-config users admin password
   commit
4. Fermez la session SSH.

STEP 12 | Accédez à l'interface Web du pare-feu VM-Series.

Ouvrez un navigateur Web et saisissez l'EIP de l'interface de gestion. Par exemple : https://54.183.85.163

STEP 13 | Activez les licences sur le pare-feu VM-Series. Cette étape n'est nécessaire que pour la licence BYOL ; les licences ayant une tarification fondée sur l'utilisation sont automatiquement activées.

Reportez-vous à la section Activation de la licence.

©2023 Palo Alto Networks, Inc.

STEP 14 | Sur le pare-feu VM-Series, configurez les interfaces réseau du dataplane sur pare-feu en tant qu'interfaces de couche 3.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
2. Cliquez sur la liaison **ethernet 1/1** et configurez comme suit :
   - **Interface Type (Type d'interface)** : **Layer3 (Couche 3)**
   - Sélectionnez l'onglet **Config (Configuration)**, affectez l'interface au routeur par défaut.
   - Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez New Zone (Nouvelle zone). Définissez une nouvelle zone, Non approuvée par exemple, puis cliquez sur OK.
   - Sélectionnez IPv4, sélectionnez **DHCP Client (Client DHCP)** ; l'adresse IP privée que vous avez affectée à l'interface réseau dans la console de gestion AWS est automatiquement acquise.
   - Dans l'onglet **Advanced (Avancé)** > **Other Info (Autres informations)**, développez la liste Profil de gestion, puis sélectionnez **New Management Profile (Nouveau profil de gestion)**.
   - Saisissez un **Name (Nom)** pour le profil, tel que allow_ping, sélectionnez **Ping** dans la liste des services autorisés, puis cliquez sur **OK**.
   - Pour enregistrer la configuration de l'interface, cliquez sur **OK**.
3. Cliquez sur le lien pour **ethernet 1/2** et configurez-le comme suit :
   - **Interface Type (Type d'interface)** : **Layer3 (Couche 3)**
   - Sélectionnez l'onglet **Config (Configuration)**, affectez l'interface au routeur par défaut.
   - Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Définissez une nouvelle zone, Approuvée par exemple, puis cliquez sur **OK**.
   - Sélectionnez **IPv4**, puis **Client DHCP**.
   - Dans l'onglet **IPv4**, décochez la case **Automatically create default route to default gateway provided by server (Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur)**. Pour une interface associée au sous-réseau privé du VPC, la désactivation de cette option garantit que le trafic géré par cette interface n'est pas dirigé directement vers la passerelle Internet (IGW) sur le VPC.
   - Dans l'onglet **Advanced (Avancé)** > **Other Info (Autres informations)**, développez la liste Profil de gestion, puis sélectionnez le profil allow_ping créé précédemment.
   - Cliquez sur **OK** pour enregistrer la configuration de l'interface.
4. Cliquez sur **Commit (Valider)** pour enregistrer les modifications. Vérifiez que la liaison de l'interface est active . Si la liaison n'est pas activée, redémarrez le pare-feu.

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Security Zone
ethernet1/1	Layer3	allow_ping		Dynamic-DHCP Client	default	untrust
ethernet1/2	Layer3	allow_ping		Dynamic-DHCP Client	default	trust

©2023 Palo Alto Networks, Inc.

STEP 15 | Sur le pare-feu VM-Series, créez des règles NAT de destination et source pour autoriser le trafic entrant/sortant vers/depuis les applications déployées dans le VPC.

1. Sélectionnez **Policies (Politiques)** > **NAT**.
2. Créez une règle NAT de destination qui redirige trafic entre le pare-feu et le serveur Web.
   1. Cliquez sur **Add (Ajouter)** et saisissez un nom pour la règle. Par exemple, NAT2WebServer.
   2. Dans l'onglet **Original Packet (Paquet d'origine)**, effectuez les sélections suivantes :
      - **Source Zone (Zone source)** : non approuvée (d'où provient le trafic)
      - **Destination Zone (Zone de destination)** : non approuvée (la zone de l'interface du dataplane du pare-feu à laquelle l'EIP du serveur Web est associée)
      - **Source Address (Adresse source)** : indifférent
      - **Destination Address (Adresse de destination)** : 10.0.0.10
      - Dans l'onglet **Translated Packet (Paquet traduit)**, cochez la case Destination Address Translation (Traduction de l'adresse de destination), puis définissez la **Translated**

©2023 Palo Alto Networks, Inc.

Address (Adresse traduite) sur 10.0.1.62, à savoir l'adresse IP privée du serveur Web.

3. Cliquez sur **OK**.

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT2WebServer	none	untrust	untrust	any	any	10.0.0.10	any	none	address: 10.0.1.62

3. Créez une règle NAT source pour autoriser l'accès sortant pour le trafic entre le serveur Web et Internet.
   1. Cliquez sur **Add (Ajouter)** et saisissez un nom pour la règle. Par exemple, NAT2External.
   2. Dans l'onglet **Original Packet (Paquet d'origine)**, effectuez les sélections suivantes :
      - **Zone source** : approuvée (d'où provient le trafic)
      - **Destination Zone (Zone de destination)** : non approuvée (la zone de l'interface du dataplane du pare-feu à laquelle l'EIP du serveur Web est associée)
      - **Source Address (Adresse source)** : indifférent
      - **Destination Address (Adresse de destination)** : indifférent
   3. Dans l'onglet **Translated Packet (Paquet traduit)**, effectuez les sélections suivantes dans la section Traduction de l'adresse source :
      - **Translation Type (Type de traduction)** : port et IP dynamiques
      - **Address Type (Type d'adresse)** : adresse traduite
      - **Translated Address (Adresse traduite)** : 10.0.0.10 (l'interface du dataplane du pare-feu dans la zone non approuvée)
   4. Cliquez sur **OK**.

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT2WebServer	none	untrust	untrust	any	any	10.0.0.10	any	none	address: 10.0.1.62
2	NAT2External	none	trust	untrust	any	any	any	any	dynamic-ip-and-port 10.0.0.10	none

4. Cliquez sur **Commit (Valider)** pour enregistrer les politiques NAT.

STEP 16 | Sur le pare-feu VM-Series, créez des politiques de sécurité pour gérer le trafic.

Plutôt que de saisir une adresse IP statique pour le serveur Web, utilisez un groupe d'adresses dynamiques. Les groupes d'adresses dynamiques vous permettent de créer une règle qui s'adapte automatiquement aux changements. Vous ne devez donc pas mettre à jour la politique lorsque vous lancez d'autres serveurs Web dans le sous-réseau. Pour plus d'informations, reportez-vous à la section Cas d'utilisation : Utilisation de groupes d'adresses dynamiques pour sécuriser les nouvelles instances EC2 dans VPC.

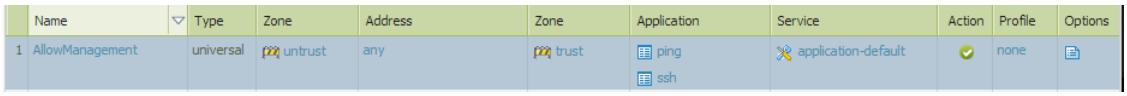
1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.

   Dans cet exemple, nous avons quatre règles. Une règle qui autorise l'accès de gestion au trafic du pare-feu, une règle autorisant le trafic entrant vers le serveur Web, une troisième

 ©2023 Palo Alto Networks, Inc.

règle autorisant l'accès Internet au serveur Web, et dans la dernière règle, nous modifions une règle intrazone prédéfinie par défaut pour journaliser l'ensemble du trafic refusé.

2. Créez une règle pour autoriser l'accès de gestion au pare-feu.
   1. Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** pour la règle. Vérifiez que le **Rule Type (Type de règle)** est universel.
   2. Dans l'onglet **Source**, ajoutez Non approuvée en tant que **Source Zone (Zone source)**.
   3. Dans l'onglet **Destination**, ajoutez Approuvée en tant que **Destination Zone (Zone de destination)**.
   4. Dans l'onglet **Applications**, **Add (Ajoutez)** ping et ssh.
   5. Dans l'onglet **Actions**, définissez la valeur **Action** sur Autoriser.
   6. Cliquez sur **OK**.



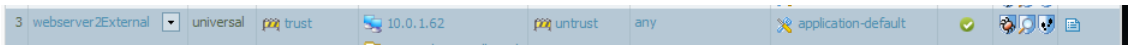
3. Créez une règle pour autoriser le trafic entrant vers le serveur Web.
   1. Cliquez sur **Add (Ajouter)**, saisissez un **Name (Nom)** pour la règle et vérifiez que le **Rule Type (Type de règle)** est universel.
   2. Dans l'onglet **Source**, ajoutez Non approuvée en tant que **Source Zone (Zone source)**.
   3. Dans l'onglet **Destination**, ajoutez Approuvée en tant que **Destination Zone (Zone de destination)**.
   4. Dans l'onglet **Applications**, **Add (Ajoutez)** Navigation Web.
   5. Dans l'onglet **Service/URL Category (Catégorie de service/d'URL)**, vérifiez que le service est défini sur application-default (Par défaut de l'application).
   6. Dans l'onglet **Actions**, définissez la valeur **Action** sur Autoriser.
   7. Dans la section Paramètres de profil de l'onglet **Actions**, sélectionnez **Profiles (Profils)**, puis associez les profils par défaut pour l'antivirus, l'antispyware et la protection contre les vulnérabilités.
   8. Cliquez sur **OK**.



4. Créez une règle pour autoriser l'accès Internet au serveur Web.
   1. Cliquez sur **Add (Ajouter)**, saisissez un **Name (Nom)** pour la règle et vérifiez que le Rule Type (Type de règle) est universel.
   2. Dans l'onglet **Source**, ajoutez Approuvée en tant que **Source Zone (Zone source)**.
   3. Dans la section Adresse source de l'onglet **Source**, ajoutez 10.0.1.62, l'adresse IP du serveur Web.
   4. Dans l'onglet **Destination**, ajoutez Non approuvée en tant que **Destination Zone (Zone de destination)**.
   5. Dans l'onglet **Service/URL Category (Catégorie de service/d'URL)**, vérifiez que le service est défini sur **application-default (Par défaut de l'application)**.
   6. Dans l'onglet **Actions**, définissez la valeur **Action** sur Autoriser.

 ©2023 Palo Alto Networks, Inc.

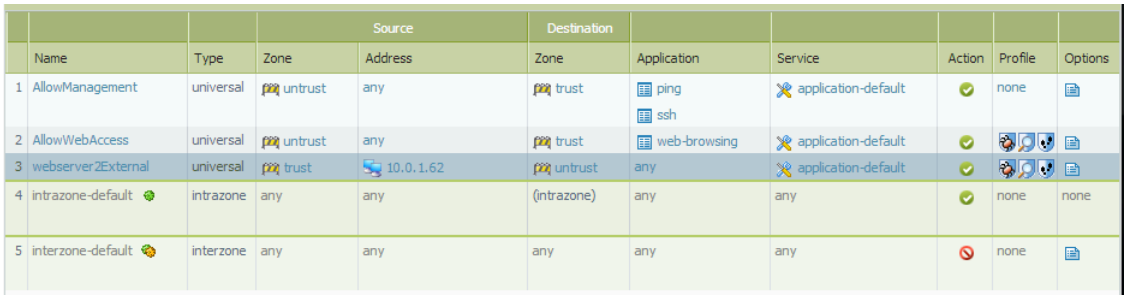
7. Dans la section Paramètres de profil de l'onglet **Actions**, sélectionnez **Profiles (Profils)**, puis associez les profils par défaut pour l'antivirus, l'antispyware et la protection contre les vulnérabilités.
8. Cliquez sur **OK**.



5. Modifiez la règle d'interzone par défaut pour journaliser l'ensemble du trafic refusé. Cette règle d'interzone prédéfinie est évaluée lorsqu'aucune autre règle n'est explicitement définie pour faire correspondre le trafic entre différentes zones.
   1. Sélectionnez la règle **interzone-default (Interzone par défaut)**, puis cliquez sur **Override (Remplacer)**.
   2. Dans l'onglet **Actions**, sélectionnez **Log at session end (Journaliser en fin de session)**.
   3. Cliquez sur **OK**.



6. Passez en revue toutes les règles de sécurité définies sur le pare-feu.
7. Cliquez sur **Commit (Valider)** pour enregistrer les politiques.

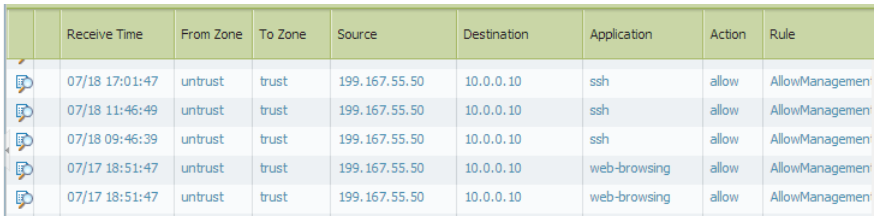


 ©2023 Palo Alto Networks, Inc.

STEP 17 | Vérifiez que le pare-feu VM-Series sécurise le trafic.

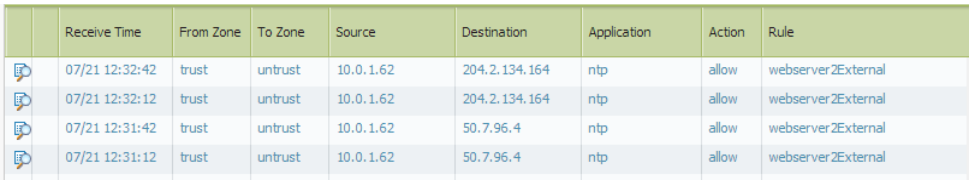
1. Ouvrez un navigateur Web et saisissez l'adresse IP du serveur Web.
2. Connectez-vous à l'interface Web du pare-feu VM-Series et vérifiez que les logs de trafic pour les sessions apparaissent dans **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**.

   - Trafic entrant dans le serveur Web (qui arrive au niveau de l'instance EC2 dans AWS VPC) :



Receive Time	From Zone	To Zone	Source	Destination	Application	Action	Rule
07/18 17:01:47	untrust	trust	199.167.55.50	10.0.0.10	ssh	allow	AllowManagemen
07/18 11:46:49	untrust	trust	199.167.55.50	10.0.0.10	ssh	allow	AllowManagemen
07/18 09:46:39	untrust	trust	199.167.55.50	10.0.0.10	ssh	allow	AllowManagemen
07/17 18:51:47	untrust	trust	199.167.55.50	10.0.0.10	web-browsing	allow	AllowManagemen
07/17 18:51:47	untrust	trust	199.167.55.50	10.0.0.10	web-browsing	allow	AllowManagemen

   - Trafic sortant du serveur Web (instance EC2 dans AWS VPC) :



Receive Time	From Zone	To Zone	Source	Destination	Application	Action	Rule
07/21 12:32:42	trust	untrust	10.0.1.62	204.2.134.164	ntp	allow	webserver2External
07/21 12:32:12	trust	untrust	10.0.1.62	204.2.134.164	ntp	allow	webserver2External
07/21 12:31:42	trust	untrust	10.0.1.62	50.7.96.4	ntp	allow	webserver2External
07/21 12:31:12	trust	untrust	10.0.1.62	50.7.96.4	ntp	allow	webserver2External

Le déploiement du pare-feu VM-Series en tant que passerelle de cloud est terminé !

©2023 Palo Alto Networks, Inc.

Cas d'utilisation : Utilisation de groupes d'adresses dynamiques pour sécuriser les nouvelles instances EC2 dans VPC

Dans un environnement dynamique tel qu'AWS-VPC dans lequel vous lancez de nouvelles instances EC2 à la demande, la surcharge administrative de gestion de la politique de sécurité peut être fastidieuse. L'utilisation de groupes d'adresses dynamiques dans une politique de sécurité vous apporte de la flexibilité et évite une interruption de service ou des failles de protection.

Dans cet exemple, vous pouvez utiliser la source d'information VM sur le pare-feu pour surveiller un VPC et utiliser les groupes d'adresses dynamiques dans la politique de sécurité pour découvrir et sécuriser les instances EC2. Lorsque vous développez des instances EC2, le groupe d'adresses dynamiques regroupe toutes les adresses IP de toutes les instances correspondant aux critères définis d'appartenance au groupe, puis la politique de sécurité est appliquée au groupe. La politique de sécurité dans cet exemple autorise l'accès Internet à tous les membres du groupe.

Au lieu d'utiliser VM Information Source sur le pare-feu, vous pouvez choisir d'utiliser Panorama comme point central pour communiquer avec vos VPC. À l'aide du plugiciel AWS sur Panorama, vous pouvez extraire la cartographie de l'adresse IP à l'étiquette et enregistrer l'information sur les pare-feux gérés pour lesquels vous configurez l'avis. Pour plus de détails sur cette option, voir Surveillance VM avec le plugin AWS sur Panorama.

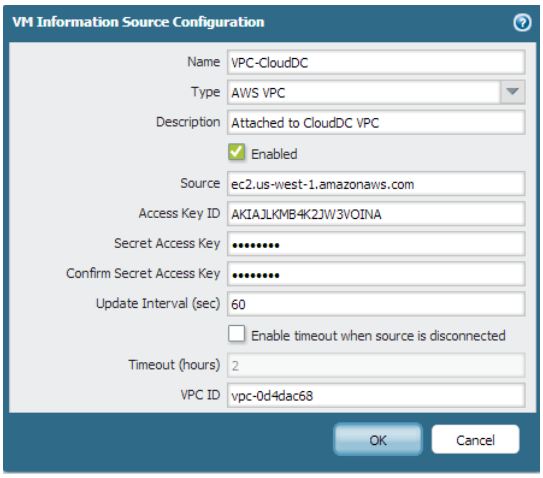
Le flux de travail de la section suivante suppose que vous avez créé l'AWS VPC et déployé le pare-feu VM-Series et des applications sur des instances EC2. Pour obtenir des instructions sur la configuration du VPC pour le pare-feu VM-Series, reportez-vous à la section Cas d'utilisation : Sécurisation des instances EC2 dans le cloud AWS.

STEP 1 | Configurez le pare-feu pour qu'il surveille le VPC.

1. Sélectionnez **Device (Appareil)** > **VM Information Sources (Sources d'informations de machine virtuelle)**.
2. Cliquez sur **Add (Ajouter)** et saisissez les informations suivantes :
   1. Un **Name (Nom)** pour identifier le VPC que vous souhaitez surveiller. Par exemple, VPC-CloudDC.
   2. Définissez le **Type** sur AMS VPC.
   3. Dans **Source**, saisissez l'URI du VPC. La syntaxe est **`ec2.<your_region>.amazonaws.com`**
   4. Ajoutez les informations d'identification nécessaires au pare-feu pour signer numériquement les appels de l'API aux services AWS. Vous avez besoin des éléments suivants :
      - **Access Key ID (ID de clé d'accès)** : Saisissez la chaîne de texte alphanumérique qui identifie de manière unique l'utilisateur qui possède ou est autorisé à accéder au compte AWS.
      - **Secret Access Key (Clé d'accès secrète)** : Saisissez et confirmez le mot de passe.
   5. (**Facultatif**) Modifiez l'**Update interval (Intervalle de mise à jour)** sur une valeur entre 5 et 600 secondes. Par défaut, le pare-feu effectue des recherches toutes

 ©2023 Palo Alto Networks, Inc.

les 5 secondes. Les appels API sont mis en file d'attente et récupérés toutes les 60 secondes. Par conséquent, les mises à jour peuvent prendre 60 secondes plus l'intervalle d'interrogation donné.



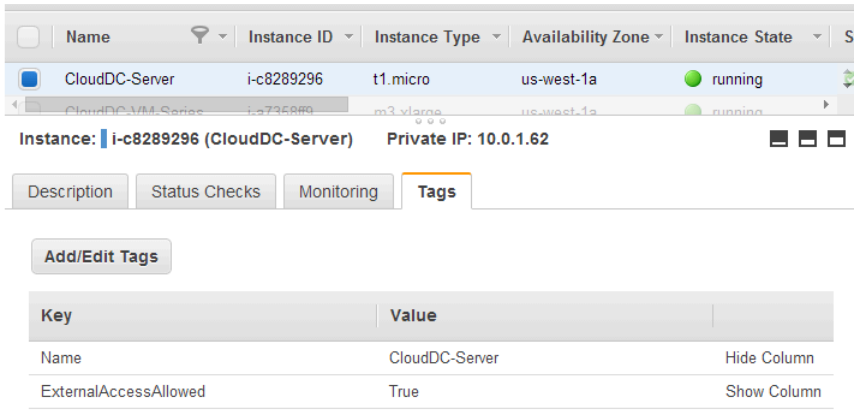
6. Saisissez l'**VPC ID (ID VPC)** affiché sur le tableau de bord VPC dans la console de gestion AWS.
7. Cliquez sur **OK** et sur **Commit (Valider)** pour enregistrer les modifications.
8. Vérifiez que le **Status (État)** de connexion affiché est connecté.

STEP 2 | Étiquetez les instances EC2 dans le VPC.

Pour obtenir la liste des étiquettes que le pare-feu VM-Series peut surveiller, reportez-vous à la Liste des attributs surveillés dans AWS VPC.

Une étiquette est une paire nom-valeur. Vous pouvez étiqueter les instances EC2 sur le tableau de bord EC2 dans la console de gestion AWS ou à l'aide de l'API AWS ou de la CLI AWS.

Dans cet exemple, nous utilisons le tableau de bord EC2 pour ajouter l'étiquette :

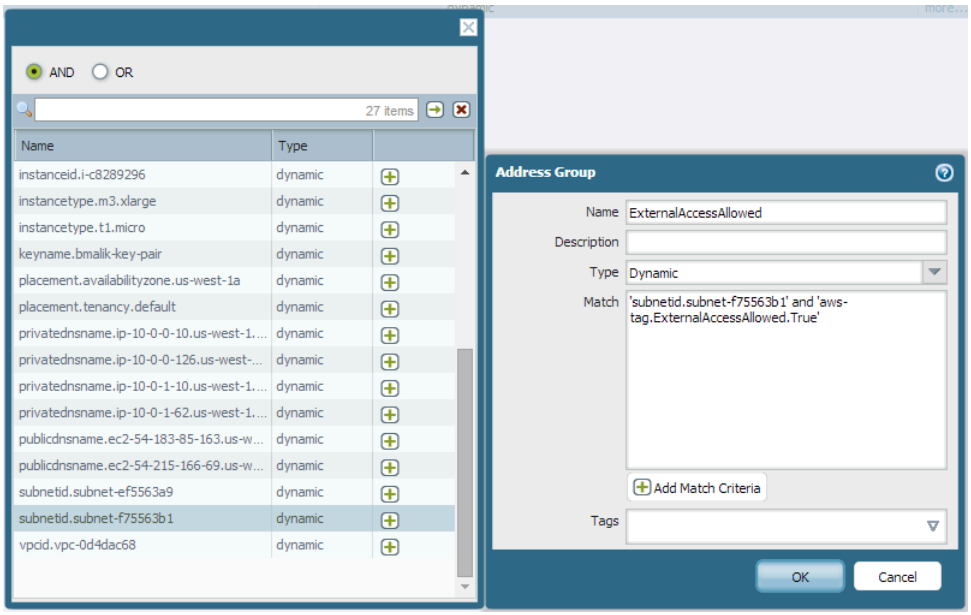


 ©2023 Palo Alto Networks, Inc.

STEP 3 | Créez un groupe d'adresses dynamiques sur le pare-feu.

Consultez le didacticiel pour avoir une vue d'ensemble de la fonction.

1. Sélectionnez **Object (Objet)** > **Address Groups (Groupes d'adresses)**.
2. Cliquez sur **Add (Ajouter)** et saisissez un **Name (nom)** et une **Description (description)** pour identifier le groupe d'adresses.
3. Définissez le **Type (type)** sur **Dynamic (Dynamique)**.
4. Définissez les critères de correspondance.
   1. Cliquez sur **Add Match Criteria (Ajouter un critère de correspondance)**, puis sélectionnez l'opérateur **And (Et)**.
   2. Sélectionnez les attributs de filtrage ou de correspondance. Dans cet exemple, nous sélectionnons l'étiquette ExternalAccessAllowed que vous venez de créer et l'ID de sous-réseau pour le sous-réseau privé du VPC.



5. Cliquez sur **OK**.
6. Cliquez sur **Commit (Valider)**.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Utilisez le groupe d'adresses dynamiques dans une politique de sécurité.

Pour créer une règle pour autoriser l'accès Internet à tout serveur Web appartenant au groupe d'adresses dynamiques nommé ExternalServerAccess.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Cliquez sur **Add (Ajouter)**, saisissez un **Name (Nom)** pour la règle et vérifiez que le **Rule Type (Type de règle)** est universel.
3. Dans l'onglet **Source**, ajoutez Approuvée en tant que **Source Zone (Zone source)**.
4. Dans la section Adresse source de l'onglet **Source**, **ajoutez** le groupe ExternalServerAccess que vous venez de créer.
5. Dans l'onglet **Destination**, ajoutez Non approuvée en tant que **Destination Zone (Zone de destination)**.
6. Dans l'onglet **Service/URL Category (Catégorie de service/d'URL)**, vérifiez que le service est défini sur **application-default (Par défaut de l'application)**.
7. Dans l'onglet **Actions**, définissez la valeur **Action** sur Autoriser.
8. Dans la section Paramètres de profil de l'onglet **Actions**, sélectionnez **Profiles (Profils)**, puis associez les profils par défaut pour l'antivirus, l'antispyware et la protection contre les vulnérabilités.
9. Cliquez sur **OK**.

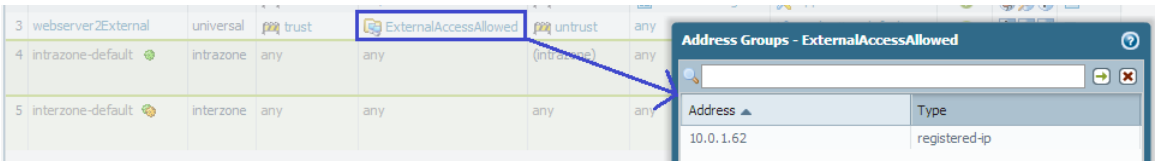


10. Cliquez sur **Commit (Valider)**.

STEP 5 | Vérifiez que les membres du groupe d'adresses dynamiques sont renseignés sur le pare-feu.

La politique est appliquée à toutes les adresses IP qui appartiennent à ce groupe d'adresses et s'affichent ici.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis choisissez la règle.
2. Cliquez sur la flèche déroulante en regard du lien du groupe d'adresses et sélectionnez **Inspect (Inspecter)**. Vous pouvez également vérifier que les critères de correspondance sont corrects.
3. Cliquez sur le lien **more (Plus)** et vérifiez que la liste des adresses IP enregistrées s'affiche.



 ©2023 Palo Alto Networks, Inc.

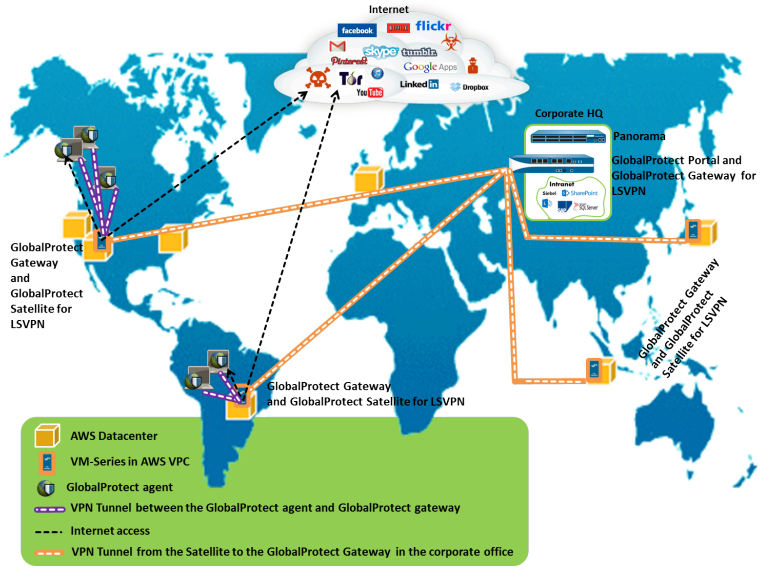
Cas d'utilisation : Pare-feu VM-Series en tant que passerelles GlobalProtect sur AWS

La protection des utilisateurs mobiles contre les menaces et les applications à risques est généralement une combinaison complexe de distribution et de configuration de la sécurité et de l'infrastructure informatique, de réponse aux besoins de bande passante et de disponibilité à divers endroits du globe, et de maîtrise du budget.

Le pare-feu VM-Series sur AWS combine la sécurité et la logistique informatique nécessaires pour protéger de manière homogène et fiable les périphériques utilisés par les utilisateurs mobiles dans des régions où vous n'êtes pas présent. En déployant le pare-feu VM-Series dans le cloud AWS, vous pouvez déployer rapidement et facilement des passerelles GlobalProtect™ dans n'importe quelle région sans les coûts ou la logistique informatique généralement liés à la configuration de cette infrastructure avec vos propres ressources.

Pour réduire la latence, sélectionnez les régions AWS les plus proches de vos utilisateurs, déployez les pare-feu VM-Series sur des instances EC2 et configurez les pare-feu en tant que passerelles GlobalProtect. Grâce à cette solution, les passerelles GlobalProtect du cloud AWS appliquent la politique de sécurité du trafic Internet. Il n'est donc pas nécessaire d'acheminer ce trafic vers le réseau d'entreprise. De plus, pour l'accès aux ressources sur le réseau d'entreprise, les pare-feu VM-Series sur AWS utilisent la fonctionnalité LSVPN afin d'établir des tunnels IPSec de retour vers le pare-feu sur le réseau d'entreprise.

Pour simplifier le déploiement et la gestion centralisée de cette infrastructure distribuée, utilisez Panorama pour configurer les composants GlobalProtect inclus dans cette solution. Facultativement, pour s'assurer que les périphériques mobiles, tels que les smartphones et les tablettes, peuvent être utilisés en toute sécurité sur votre réseau, utilisez un Gestionnaire de périphérique mobile pour configurer et gérer les périphériques mobiles.



- Composants de l'infrastructure GlobalProtect
- Déploiement de passerelles GlobalProtect sur AWS

©2023 Palo Alto Networks, Inc.

Composants de l'infrastructure GlobalProtect

Pour bloquer les applications à risques et protéger les utilisateurs mobiles contre les logiciels malveillants, vous devez configurer l'infrastructure GlobalProtect qui inclut le portail GlobalProtect, la passerelle GlobalProtect et l'application GlobalProtect. De plus, pour l'accès aux ressources d'entreprise, vous devez configurer une connexion VPN IPSec entre les pare-feu VM-Series sur AWS et le pare-feu du siège social à l'aide de LSVPN (un déploiement VPN en étoile).

- L'agent/application GlobalProtect est installé sur chaque système utilisateur final qui est autorisé à accéder aux applications/ressources d'entreprise. L'agent se connecte tout d'abord au portail pour obtenir des informations sur les passerelles, puis établit une connexion VPN sécurisée avec la passerelle GlobalProtect la plus proche. La connexion VPN entre le système utilisateur final et la passerelle garantit la confidentialité des données.
- Le portail GlobalProtect fournit les fonctions de gestion de l'infrastructure GlobalProtect. Chaque système utilisateur final qui fait partie du réseau GlobalProtect reçoit des informations de configuration du portail, notamment des informations sur les passerelles disponibles, ainsi que les certificats clients pouvant être requis pour se connecter aux passerelles GlobalProtect. Dans ce cas d'utilisation, le portail GlobalProtect est un pare-feu matériel déployé dans le siège social.
- La passerelle GlobalProtect fournit la mise en œuvre de prévention contre les menaces et de politique mobile en fonction des applications, utilisateurs, contenus, périphériques et états de périphérique. Dans ce cas d'utilisation, les pare-feu VM-Series sur AWS servent de passerelles GlobalProtect. La passerelle GlobalProtect analyse chaque requête client à la recherche de logiciels malveillants ou autres menaces et, si la politique le permet, envoie la requête à Internet ou au réseau d'entreprise via le tunnel IPSec (à la passerelle LSVPN).
- Pour LSVPN, vous devez configurer le portail GlobalProtect, la passerelle GlobalProtect pour LSVPN (concentrateur) et les satellites GlobalProtect (branches).

  Dans ce cas d'utilisation, le seul pare-feu matériel du bureau est déployé en tant que portail GlobalProtect et passerelle LSVPN. Les pare-feu VM-Series sur AWS sont configurés pour servir de satellites GlobalProtect. Les satellites GlobalProtect et la passerelle sont configurés pour établir un tunnel IPSec qui se termine sur la passerelle. Lorsqu'un utilisateur mobile demande une application ou une ressource résidant sur le réseau d'entreprise, le pare-feu VM-Series achemine la requête via le tunnel IPSec.

Déploiement de passerelles GlobalProtect sur AWS

Pour protéger les utilisateurs mobiles, en plus de déployer et de configurer les passerelles GlobalProtect sur AWS, vous devez configurer les autres composants nécessaires à cette solution intégrée. Le tableau suivant inclut le flux de travail recommandé :

1. Déployez le ou les pare-feu VM-Series sur AWS.

   Reportez-vous à la section Configuration du pare-feu VM-Series sur AWS.

©2023 Palo Alto Networks, Inc.

- Configurez le pare-feu au niveau du siège social.

  Dans ce cas pratique, le pare-feu est configuré en tant que portail GlobalProtect et passerelle LSVPN.

  - Configuration du portail GlobalProtect.
  - Configuration du portail GlobalProtect pour LSVPN.
  - Configuration du portail pour l'authentification de satellites LSVPN.
  - Configuration de la passerelle GlobalProtect pour LSVPN.

- Définissez un modèle sur Panorama pour configurer les pare-feu VM-Series sur AWS en tant que passerelles GlobalProtect et satellites LSVPN.

  Pour gérer facilement ce déploiement distribué, utilisez Panorama pour configurer les pare-feu sur AWS.

  - Création de modèles sur Panorama.

  Utilisez ensuite les liens ci-dessous pour définir la configuration dans les modèles.

  - Configuration du pare-feu en tant que passerelle GlobalProtect.
  - Préparation du satellite pour l'association au LSVPN.

- Créez des groupes de périphériques sur Panorama pour définir les politiques d'accès réseau et les règles d'accès Internet, et appliquez-les aux pare-feu sur AWS.

  Reportez-vous à la section Création de groupes de périphériques.

- Appliquez les modèles et les groupes de périphériques aux pare-feu sur AWS, puis vérifiez que les pare-feu sont configurés correctement.

- Déployez le logiciel client GlobalProtect.

  Sur chaque système utilisateur final, l'agent ou l'application GlobalProtect doit se connecter à la passerelle GlobalProtect.

  Reportez-vous à la section Déploiement du logiciel client GlobalProtect.

 ©2023 Palo Alto Networks, Inc.

Surveillance des ressources sur le AWS

Lorsque vous déployez ou arrêtez des ressources dans le cloud public AWS, vous pouvez utiliser le plug-in Panorama pour AWS ou les sources d'information sur les ressources AWS sur le pare-feu pour appliquer de façon uniforme les règles de politique de sécurité sur ces charges de travail. Reportez-vous à la Matrice de compatibilité pour plus d'informations sur la version du plug-in Panorama.

Le plug-in Panorama pour AWS est conçu pour l'évolution et vous permet de surveiller jusqu'à 1 000 VPC AWS sur le cloud public AWS. Avec ce plug-in, vous utilisez Panorama comme point d'ancrage pour interroger vos comptes AWS pour les tags, puis distribuez les métadonnées (association IP vers tags) à de nombreux pare-feu dans un groupe de périphériques. Étant donné que Panorama communique avec vos comptes AWS pour récupérer des informations sur les ressources AWS, vous pouvez rationaliser le nombre d'appels API effectués dans l'environnement cloud. Lorsque vous utilisez Panorama et le plugin AWS, vous pouvez centraliser l'extraction des étiquettes et la gestion des politiques de sécurité pour assurer l'uniformité des politiques pour les architectures hybrides et d'origine infonuagique. Voir Surveillance des ressources AWS avec Plugin AWS sur Panorama.

Si vous n'avez pas de Panorama ou que vous avez un déploiement plus simple et que vous devez surveiller 10 VPC ou moins, vous pouvez utiliser la source d'information VM sur le pare-feu (matériel ou pare-feu de série VM) pour surveiller vos charges de travail AWS. Vous pouvez utiliser les métadonnées, que le pare-feu extrait, dans les groupes d'adresses dynamiques et les consulter dans les politiques de sécurité pour sécuriser vos charges de travail de MV lorsqu'elles tournent vers le haut ou vers le bas et que les adresses IP changent fréquemment. Reportez-vous à la section Cas d'utilisation : Utilisation de Dynamic Address Groups (groupes d'adresses dynamiques) pour sécuriser les nouvelles instances EC2 dans le VPC.

Surveillance des ressources AWS avec Plugin AWS sur Panorama

Lorsque vous déployez ou éteignez des ressources dans le nuage public AWS, vous devez mettre à jour de façon synchrone la politique de sécurité sur vos pare-feu Palo Alto NetworksMD afin de sécuriser ces instances EC2. Pour activer cette fonction à partir de Panorama, vous devez installer le plugin AWS sur Panorama et activer la communication API entre Panorama et vos VPC AWS. Panorama peut ensuite recueillir un ensemble prédéfini d'attributs (ou d'éléments de métadonnées) comme étiquettes pour vos ressources AWS et enregistrer l'information dans vos pare-feu Palo Alto NetworksMD. Lorsque vous faites référence à ces étiquettes dans les groupes d'adresses dynamiques et que vous les faites correspondre à des règles de politique de sécurité, vous pouvez continuellement appliquer la politique sur l'ensemble des ressources déployées au sein de vos comptes AWS.

- Configuration du Plugin AWS pour surveillance sur Panorama
- Liste des attributs surveillés dans AWS VPC

Configuration du Plugin AWS pour surveillance de machine virtuelle

Pour trouver toutes les charges de travail des machines virtuelles que votre organisation a déployées dans le nuage public AWS, vous devez installer la fiche AWS sur Panorama et configurer les ***définitions de surveillance*** qui permettent à Panorama d'authentifier vos VPC AWS et d'extraire l'information VM sur les charges de travail. Panorama récupère l'adresse IP des MV qui fonctionnent

 ©2023 Palo Alto Networks, Inc.

— adresse IP publique et adresses IP privées primaires et secondaires — et les étiquettes connexes. Pour une liste des éléments de métadonnées pris en charge par Panorama, consultez Liste des attributs surveillés dans AWS VPC.

Après que Panorama a détecté les attributs, pour déplacer l'information de la machine virtuelle de Panorama vers les pare-feu, vous devez ajouter les coupe-feu (matériel ou série VM) comme dispositifs gérés sur Panorama, et regrouper les pare-feu en un ou plusieurs groupes d'appareils. Vous pouvez ensuite préciser les groupes d'appareils qui font partie du ***groupe de notification***, qui est un élément de configuration dans une définition de surveillance, que Panorama utilise pour enregistrer la cartographie de l'adresse IP à l'étiquette qu'il extrait du AWS.

Enfin, pour assurer l'application uniforme des politiques de sécurité dans l'ensemble des cas EC2, vous devez établir des Dynamic Address Groups et les renvoyer dans des règles stratégiques qui permettent ou refusent le trafic aux adresses IP des VMs. Pour simplifier votre configuration et gérer vos politiques et objets de façon centralisée à partir de Panorama, vous pouvez définir les groupes d'adresses dynamiques et les règles de politique de sécurité sur Panorama et les déplacer vers les pare-feu plutôt que de gérer les groupes d'adresses dynamiques et les règles de politique de sécurité localement sur chaque pare-feu.

Le plug-in AWS version 2.0 sert à surveiller les instances EC2 pour un maximum de 1 000 VPC sur le cloud public AWS, AWS GovCloud et AWS China. Cependant, étant donné que Panorama ne peut pas être déployé sur AWS China, le rôle IAM ne prend pas en charge les profils d'instance sur AWS China. À la place, vous devez fournir les informations d'identification AWS.

- Liste de vérification de planification pour la surveillance de la VM sur AWS
- Autorisations et rôles IAM pour Panorama
- Installation ou mise à niveau du plug-in AWS
- Configurer le Plugin AWS pour surveillance de machine virtuelle

Liste de vérification de planification pour la surveillance de la VM sur AWS

Pour que Panorama puisse interagir avec les API de AWS et recueillir des renseignements sur vos instances EC2, vous devez créer un rôle de IAM et attribuer les politiques qui accordent les autorisations nécessaires pour authentifier le AWS et accéder aux instances EC2 dans votre VPC. Vous pouvez ajouter 100 rôles IAM pour gérer jusqu'à 1 000 VPC sur Panorama.

- ☐ Rassemblez le ID du VPC.
- ☐ Tag your EC2 instances on AWS. Vous pouvez étiqueter (définir une paire nom-valeur) les instances EC2 sur le tableau de bord EC2 dans la console de gestion AWS ou à l'aide de l'API AWS ou de la CLI AWS. Voir La liste des attributs surveillés dans AWS VPC. pour la liste des attributs pris en charge.
- ☐ Vérifiez s'il y a des adresses IP en double dans les VPC pour lesquelles vous activerez la surveillance. Si vous avez des adresses IP en double dans les CPV des SSFE, les métadonnées seront annexées ou échangées, ce qui pourrait entraîner des résultats inattendus en matière d'application de la politique.

Les adresses IP en double sont écrites sur le fichier plugin_aws_ret.log. Vous pouvez accéder à ce dernier depuis la CLI sur Panorama.

©2023 Palo Alto Networks, Inc.

- Passer en revue les exigences pour Panorama et les pare-feu gérés :
  - Configuration système minimale requise : appareil virtuel Panorama ou appareil matériel Panorama.

<table>
<tr><th colspan="5">Configuration minimale requise pour Panorama</th></tr>
<tr><td rowspan="4">Ressources systèmes</td><td>Mémoire</td><td>Processeurs</td><td>Nombre de VPC surveillés</td><td>Nombre d’étiquettes enregistrées</td></tr>
<tr><td>16 Go</td><td>4</td><td>1-100</td><td rowspan="3">Panorama 9.1 ou version ultérieure avec plug-in version 2.0 a été testé pour récupérer 10 000 adresses IP avec 13 étiquettes chacune, ou 5 000 adresses IP avec 25 étiquettes chacune, et pour les enregistrer dans les pare-feu inclus dans un groupe de périphériques.La longueur des étiquettes de chaque instance EC2, valeur et nom inclus, est considérée être de 64 octets par étiquette. Par exemple, l’étiquette de nom de l’instance EC2 est aws.ec2.tag.Name.prod-web-app-4523-lvss6j.</td></tr>
<tr><td>32 Go</td><td>8</td><td>100-500</td></tr>
<tr><td>64 Go</td><td>16</td><td>500-1000</td></tr>
<tr><td>Version du système d’exploitation Panorama</td><td colspan="4">9.1 ou ultérieure</td></tr>
<tr><td>Version du plug-in AWS</td><td colspan="4">2.0.0 ou ultérieure</td></tr>
<tr><td>Licences</td><td colspan="4">Licence d’assistance active et une licence de gestion de périphériques sur Panorama pour la gestion des pare-feu.

Les pare-feu nouvelle génération doivent également avoir une licence d’assistance valide.</td></tr>
<tr><td>Rôles et autorisations pour récupérer les métadonnées des instances EC2</td><td colspan="4">Reportez-vous à la section Autorisations et rôles IAM pour Panorama</td></tr>
</table>

  - Vous devez ajouter les pare-feu comme dispositifs gérés sur Panorama et créer des groupes d’appareils de façon à pouvoir configurer Panorama pour aviser ces groupes à l’aide de l’information VM qu’il récupère. Les groupes d’appareils peuvent inclure des pare-feu de série VM ou des systèmes virtuels sur les pare-feu matériels.

©2023 Palo Alto Networks, Inc.

- Si vos appareils Panorama sont en configuration de disponibilité élevée, vous devez installer manuellement la même version du plugin AWS sur les deux appareils Panorama. De plus, si vous utilisez des profils d'instance, vous devez attacher le même profil d'instance aux deux pairs Panorama.

  Vous configurez le plugin AWS sur le poste de Panorama actif seulement. Sur l'engagement, la configuration est synchronisée avec le pair passif Panorama. Seuls les pairs actifs Panorama sondent les comptes AWS que vous avez configurés pour la surveillance VM.

- Configurez les informations d'identification et les autorisations dont Panorama a besoin pour signer numériquement les appels API aux services AWS.

  Vous pouvez choisir de fournir les informations d'identification à long terme (l'ID de clé d'accès et la clé d'accès secrète) permettant d'accéder aux ressources de chaque compte AWS ou de configurer un rôle Assume sur AWS pour autoriser l'accès à des ressources AWS définies dans le même compte AWS ou dans plusieurs comptes. Avec un rôle Assume, vous devez configurer une relation de confiance et définir les autorisations lors de la création du rôle lui-même. Cela est particulièrement utile dans un déploiement dans plusieurs comptes où le compte interrogateur ne dispose pas des autorisations nécessaires pour voir ou gérer les données du compte interrogé. Pour que le plug-in Panorama s'authentifie avec succès sur le VPC et récupère les étiquettes, vous devez configurer le rôle Assume pour qu'il utilise l'API STS (Security Token Service) AWS sur n'importe quel service AWS. Et un utilisateur du compte interrogateur doit disposer des autorisations STS pour interroger le rôle Assume et obtenir les informations d'identification de sécurité temporaires permettant d'accéder aux ressources. Si votre Panorama est déployé sur AWS, vous pouvez choisir d'utiliser un profil d'instance au lieu de devoir fournir les informations d'identification AWS pour le rôle IAM. Le profil d'instance comprend les informations sur le rôle et les informations d'identification associées dont Panorama a besoin pour signer numériquement les appels API aux services AWS. Pour plus d'informations, reportez-vous à la section Autorisations et rôles IAM pour Panorama.

Autorisations et rôles IAM pour Panorama

Grâce au plug-in version 2.0, vous pouvez utiliser des rôles IAM ou des profils d'instance pour autoriser Panorama à authentifier et à récupérer des métadonnées sur les ressources déployées dans vos comptes AWS.

- Si votre Panorama n'est pas déployé sur AWS, deux options se présentent à vous. Vous pouvez soit fournir les informations d'identification IAM à long terme pour les comptes AWS que vous souhaitez surveiller, soit configurer un rôle Assume sur AWS pour autoriser l'accès à des ressources AWS définies dans le même compte AWS ou dans plusieurs comptes. Il est recommandé d'utiliser un rôle Assume, car cette option est la plus sécurisée.
- Si votre Panorama est déployé sur AWS, en plus des deux options indiquées ci-dessus, vous pouvez également ajouter un profil d'instance permettant au rôle IAM d'être transmis à l'instance EC2. Vous pouvez utiliser un profil d'instance hébergeant Panorama et toutes vos ressources surveillées dans le même compte ou un profil d'instance avec rôle Assume pour accéder à plusieurs comptes si votre Panorama et vos ressources surveillées sont déployés sur différents comptes AWS. Si vous utilisez un profil d'instance, vous ne devez pas saisir vos informations d'identification AWS dans Panorama.

 ©2023 Palo Alto Networks, Inc.

Option 1 : rôle IAM avec informations d'identification à long terme	
Autorisations et rôles requis	Les informations d'identification AWS associées au compte AWS possédant les instances VPC/EC2 que vous souhaitez surveiller. Le format JSON pour les autorisations minimales associées au rôle IAM avec les informations d'identification à long terme est le suivant : `{ "Path": "/", "UserName": "panorama_vm_programmatic", "UserId": "AIDAIZXXXXCR5JPII4XYZ", "Arn": "arn:aws:iam::412383210500:user/ panorama_vm_programmatic", "CreateDate": "2018-07-06T19:14:31Z", "GroupList": [], "AttachedManagedPolicies": [{ "PolicyName": "ReadOnlyAccess", "PolicyArn": "arn:aws:iam::aws:policy/ReadOnlyAccess" }] },`
Entrées sur Panorama	Renseignez les champs **Access Key ID (ID de clé d'accès)** et **Secret Access Key (Clé d'accès secrète)** pour l'utilisateur dans **Panorama** > **Plugins** > **AWS** > **Setup (Configuration)** > **IAM Role (Rôle IAM)**.
Option 2 : rôle IAM avec rôle Assume	
Autorisations et rôles requis	Bien que vous puissiez utiliser cette option pour surveiller les VPC d'un ou de plusieurs comptes, il est recommandé de l'utiliser pour autoriser l'accès à plusieurs comptes en adoptant un rôle vous permettant d'accéder à des ressources auxquelles vous pourriez accéder en temps normal. Pour adopter un rôle d'un autre compte, votre compte AWS doit être approuvé par ce rôle et être défini comme une entité approuvée dans sa politique d'approbation. En outre, tout utilisateur souhaitant accéder à un rôle dans un autre compte doit disposer d'une politique avec accès STS (service d'émission de jeton de sécurité) spécifiant l'ARN de rôle. **Sur le compte 1 que vous souhaitez surveiller :** • Créez un rôle IAM avec les autorisations requises. Pour la surveillance VM, vous avez besoin d'AmazonEC2ReadOnlyAccess. • Copiez l'ARN de rôle. • Créez un utilisateur et ajoutez l'ID du compte 2 en tant qu'entité approuvée. Ceci donne au compte 2 les autorisations requises pour utiliser ce rôle afin d'accéder aux ressources du compte 1. **Sur le compte 2 requérant un accès au compte 1 :** • Attachez la politique suivante avec des autorisations STS et modifiez l'ARN de rôle pour qu'il corresponde à celui que vous avez créé sur le compte 1. `{ "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource":"arn:aws:iam::012347211234:role/ PAN-OS-assume-role" } }`

©2023 Palo Alto Networks, Inc.

Entrées sur Panorama	• Renseignez les champs **Access Key ID (ID de clé d'accès)** et **Secret Access Key (Clé d'accès secrète)** pour l'utilisateur sur le compte 2 dans **Panorama** > **Plugins** > **AWS** > **Setup (Configuration)** > **IAM Role (Rôle IAM)**. • Saisissez le **Role ARN (ARN de rôle)** pour le compte AWS 1 que vous souhaitez surveiller dans **Panorama** > **Plugins** > **AWS** > **Monitoring Definitions (Définitions de surveillance)**.
Option 3 : profil d'instance	
Autorisations et rôles requis	Uniquement si Panorama est déployé en tant qu'instance EC2 sur AWS *Notez que si vous utilisez la console de gestion AWS pour créer un rôle IAM, la console crée automatiquement un profil d'instance portant le même nom que le rôle. Dès lors, si vous lancez votre Panorama (instance EC2) avec un rôle IAM, le profil d'instance du même nom est associé au rôle.* Si Panorama et les ressources que vous souhaitez surveiller se trouvent sur un seul et même compte AWS. Créez un rôle IAM avec AmazonEC2ReadOnlyAccess.
Entrées sur Panorama	Sélectionnez l'option **Instance Profile (Profil d'instance)** dans **Panorama** > **Plugins** > **AWS** > **Setup (Configuration)** > **IAM Role (Rôle IAM)**.
Option 4 : profil d'instance avec rôle Assume	
Autorisations et rôles requis	Utilisez un profil d'instance avec rôle Assume si Panorama et les ressources que vous souhaitez surveiller se trouvent sur plusieurs comptes AWS. Pour Panorama HA, assurez-vous de bien attacher le même profil d'instance aux deux pairs Panorama. **Sur le compte 1, où vos instances EC2 sont déployées :** • Créez un rôle IAM. • Ajoutez à ce rôle l'ID du compte AWS (compte 2) sur lequel votre Panorama est déployé en tant qu'entité approuvée. • Joignez les politiques JSON, comme décrit ci-dessus pour la surveillance VM. • Copiez l'ARN de rôle. Panorama a besoin de ce rôle pour récupérer les métadonnées de vos instances EC2 sur les clusters EKS. **Sur le compte 2, où votre Panorama est déployé :** • Créez un rôle IAM et joignez-y la politique JSON (avec la politique STS et l'ARN de ressource provenant du compte 1). • Pour chaque compte AWS supplémentaire que vous souhaitez surveiller, copiez la même politique STS et modifiez l'ARN de rôle.

©2023 Palo Alto Networks, Inc.

Entrées sur Panorama	• Sélectionnez l'option **Instance Profile (Profil d'instance)** dans **Panorama** > **Plugins** > **AWS** > **Setup (Configuration)** > **IAM Role (Rôle IAM)**. • Saisissez le **Role ARN (ARN de rôle)** pour le compte AWS que vous souhaitez surveiller dans **Panorama** > **Plugins** > **AWS** > **Monitoring Definitions (Définitions de surveillance)**. Par exemple, le compte 1 dans cet exemple.

Installation ou mise à niveau du plug-in AWS

Pour commencer à surveiller vos instances EC2 sur AWS, reportez-vous à la Matrice de compatibilité pour connaître le plug-in Panorama pour AWS et les versions du plug-in VM-Seriesnécessaires pour prendre en charge la surveillance VM.

Pour mettre à niveau un plug-in Panorama pour AWS de la version 1.0.1 à la version 2.0.x, vous devez d'abord effectuer une mise à niveau vers les versions des plug-ins Panorama et VM-Series requises pour la version 2.0.x, puis procéder à l'installation conformément aux instructions ci-dessous.

Vous ne pourrez plus revenir à la version 1.0 après avoir installé la version 2.0 du plug-in AWS.

Si vous avez une configuration HA de Panorama, répétez le processus d'installation / de mise à niveau sur chaque pair Panorama.

Installez ou désinstallez des plug-ins pendant une fenêtre planifiée.

Si vous disposez actuellement d'un plug-in Panorama pour n'importe quelle plateforme cloud, l'installation (ou la désinstallation) d'un plug-in supplémentaire nécessite un redémarrage de Panorama pour valider les modifications.

Si vous avez un appareil Panorama autonome ou deux appareils Panorama installés dans une paire HA avec plusieurs plug-ins installés, les plug-ins peuvent ne pas recevoir les informations des indicateurs d'adresse IP mises à jour si un ou plusieurs des plug-ins ne sont pas configurés. Cela se produit, car Panorama ne transfère pas les informations des indicateurs d'adresse IP aux plug-ins non configurés. De plus, ce problème peut se présenter si un ou plusieurs plug-ins Panorama ne se trouvent pas dans l'état Registered (Enregistré) ou Success (Réussite) (l'état positif diffère sur chaque plug-in). Assurez-vous que vos plug-ins se trouvent dans l'état positif avant de continuer ou d'exécuter les commandes décrites ci-dessous.

Si vous rencontrez ce problème, il existe deux solutions alternatives :

- Désinstallez le ou les plug-ins non configurés. Il est déconseillé d'installer un plug-in que vous n'envisagez pas de configurer dans l'immédiat
- Vous pouvez utiliser les commandes suivantes pour contourner ce problème. Exécutez la commande suivante pour chaque plug-in non configuré sur chaque instance de Panorama afin

©2023 Palo Alto Networks, Inc.

que Panorama n'attende pas pour envoyer des mises à jour. Dans le cas contraire, vos pare-feu risquent de perdre certaines informations des indicateurs d'adresse IP.

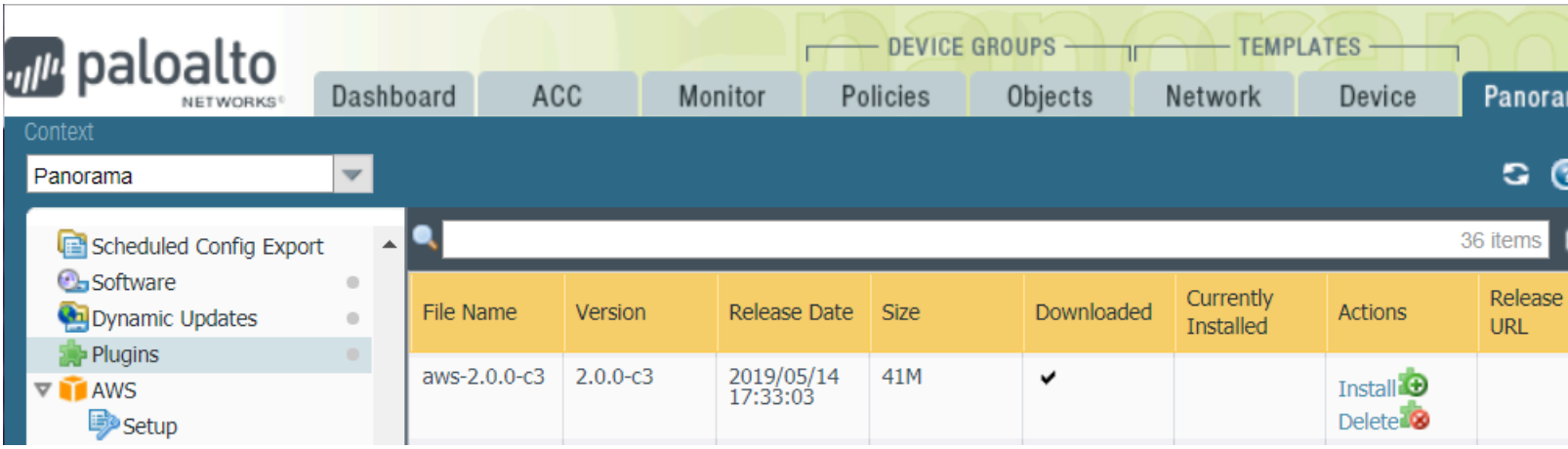
```
request plugins dau plugin-name <plugin-name> unblock-device-push yes
```

Vous pouvez annuler cette commande en exécutant :

```
request plugins dau plugin-name <plugin-name> unblock-device-push no
```

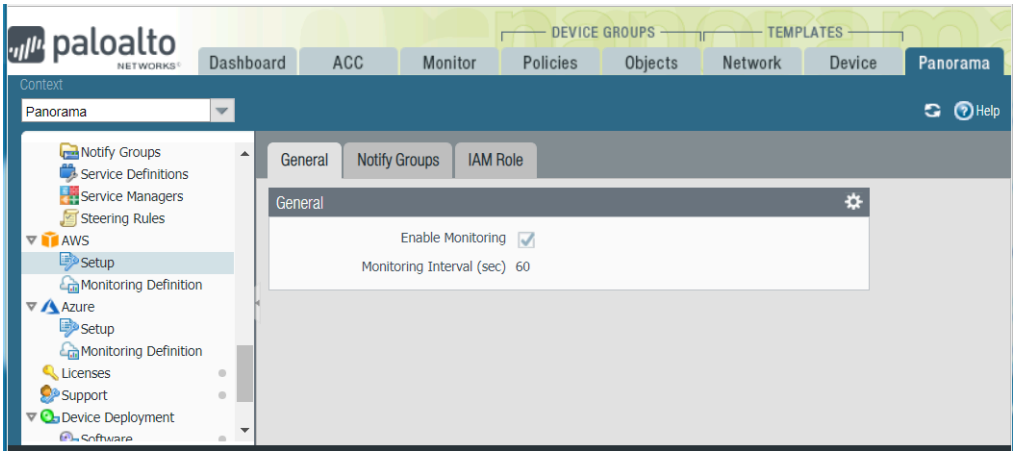
Les commandes décrites ne sont pas persistantes lors des redémarrages et doivent être réutilisées pour tout redémarrage ultérieur. Pour Panorama en paire HA, les commandes doivent être exécutées sur chaque Panorama.

STEP 1 | Connectez-vous à l'interface web Panorama, sélectionnez **Panorama** > **Plugins** et cliquez sur **Check Now (Vérifier maintenant)** pour obtenir la version du plug-in **AWS** prenant en charge la surveillance VM.



STEP 2 | **Téléchargez et installez** le plug-in.

Une fois l'installation réussie, Panorama s'actualise et le plug-in AWS s'affiche sur l'onglet **Panorama** > **Plugins (Plug-ins)**.



*Sur le **Dashboard (Tableau de bord)** Panorama, le widget General Information (Informations générales) vous permet de vérifier la version installée du plug-in Panorama pour AWS.*

©2023 Palo Alto Networks, Inc.

STEP 3 | (Panorama en HA) **Valider** > **Valider sur Panorama**.

Si votre Panorama est en HA, validez les modifications sur la configuration Panorama pour vous assurer que les étiquettes sont enregistrées sur le pair Panorama en cas de basculement.

Configurer le Plugin AWS pour surveillance de machine virtuelle

Pour commencer à surveiller les machines virtuelles dans votre déploiement de nuage public AWS, après avoir Install the AWS Plugin (installé la fiche AWS) vous devez créer une définition de surveillance. Cette définition précise le rôle de l'AIM qui est autorisé à accéder aux instances EC2 dans le VPC des AWS que vous voulez surveiller et le groupe de notification qui comprend les pare-feu vers lesquels Panorama devrait pousser toutes les correspondances IP-address-tag qu'il récupère. Pour appliquer la politique, vous devez ensuite créer des groupes d'adresses dynamiques et les consulter dans la politique sur la sécurité. Les groupes d'adresses dynamiques vous permettent de filtrer les étiquettes sur lesquelles vous voulez vous aligner, de sorte que le pare-feu puisse enregistrer les adresses IP publiques et privées sur chaque étiquette, puis permettre ou refuser l'accès à la charge de travail en fonction des règles de politique que vous définissez.

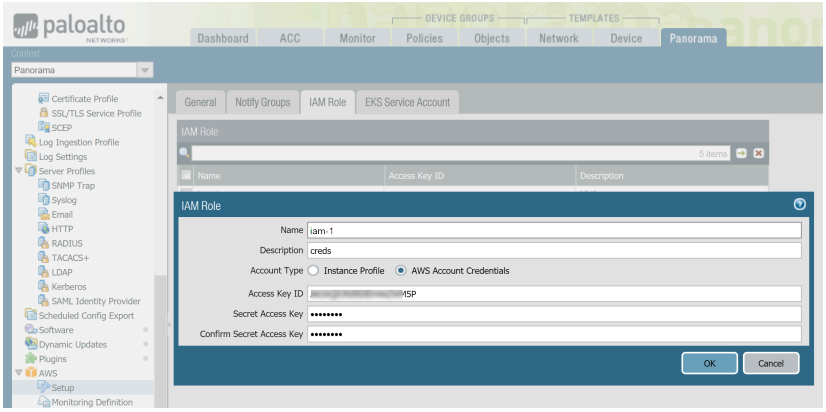
STEP 1 | Connectez-vous à l'interface Web Panorama.

STEP 2 | Configurez les objets suivants pour l'activation de VM Monitoring sur AWS.

- Ajoutez un nouveau rôle.

  Un rôle IAM est une entité qui vous permet de déléguer l'accès afin que Panorama puisse présenter des requêtes de service en votre nom aux ressources AWS (machines virtuelles qui sont déployées comme instances EC2).

  1. Sélectionnez **Panorama** > **Plugins (Plug-ins)** > **AWS** > **Setup (Configuration)** > **IAM Role (Rôle IAM)** > **Add (Ajouter)**.



  2. Donnez un **Name** (Nom) et s'il y a lieu, une **Description** pour indiquer le rôle IAM.
  3. Comme Account Type (Type de compte), sélectionnez **Instance Profile (Profil d'instance)** ou **AWS Account Credentials (Informations d'identification de compte AWS)**. Si votre Panorama est déployé sur AWS, vous pouvez soit y associer un profil d'instance avec les autorisations adéquates, soit ajouter les informations d'identification associées au rôle IAM

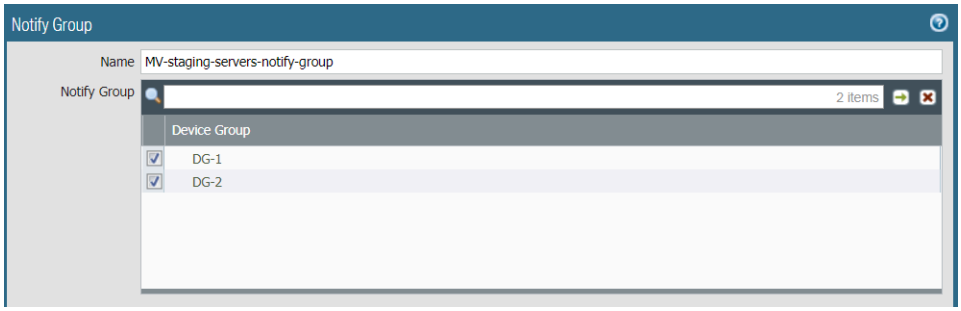
©2023 Palo Alto Networks, Inc.

sur Panorama. Si votre Panorama n'est pas déployé sur AWS, vous devez saisir localement les informations d'identification pour le rôle IAM sur Panorama.

4. (Uniquement pour les informations d'identification de compte AWS) Saisissez la **Secret Access Key (Clé d'accès secrète)** et saisissez-la à nouveau pour la confirmer, puis cliquez sur **OK**.

- Ajoutez un groupe de notification.

1. Sélectionnez **Panorama** > **Plugins** > **AWS** > **Setup (Configuration)** > **Notify Groups (Groupes de notification)** > **Add (Ajouter)**.



2. Saisissez un **Name** (Nom) pour identifier le groupe de pare-feu vers lequel Panorama envoie les informations sur les machines virtuelles qu'il récupère.
3. Sélectionnez les **Device Groups (groupes d'appareils)**, qui sont un groupe de pare-feu ou de systèmes virtuels, vers lesquels Panorama poussera l'information de MV (carte IP d'adresse à étiquette) qu'il extrait de vos VPC AWS. Les pare-feu utilisent cette mise à jour pour déterminer la liste la plus récente des membres qui constituent les groupes d'adresses dynamiques référencés dans la politique. Si vous utilisez le plug-in Panorama pour Azure et AWS, vous pouvez cibler le même pare-feu ou système virtuel avec des étiquettes des deux environnements.

   Réfléchissez soigneusement à vos groupes d'appareils.

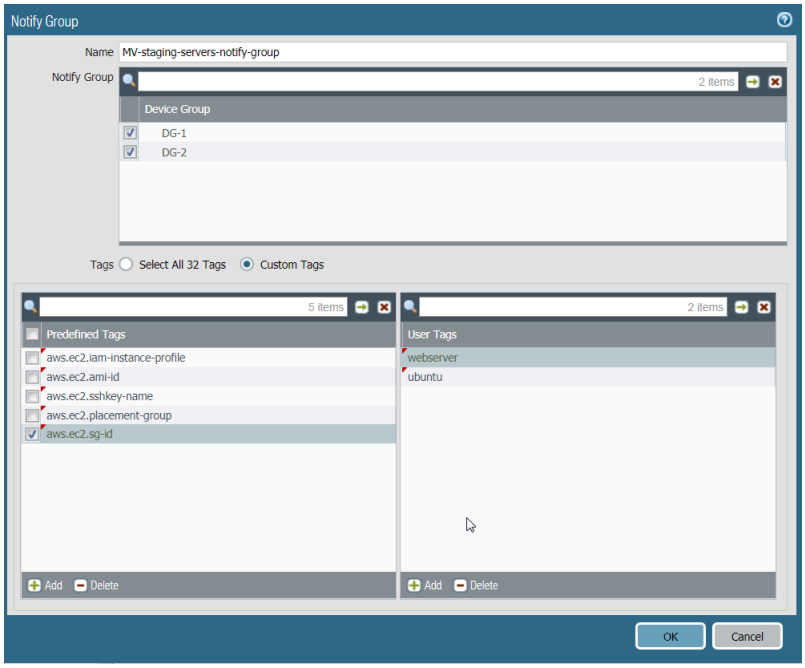
   - *Étant donné qu'une définition de surveillance ne peut inclure qu'un seul groupe d'avis, assurez-vous de sélectionner tous les groupes d'appareils pertinents au sein de votre groupe d'avis. Si vous voulez désenregistrer les étiquettes que Panorama a envoyées à un pare-feu inclus dans un groupe de notification, vous devez supprimer la Monitoring Definition (Définition de surveillance).*
   - *Pour enregistrer des étiquettes à tous les systèmes virtuels sur un pare-feu activé pour plusieurs systèmes virtuels, vous devez ajouter chaque système virtuel à un groupe de dispositifs distinct sur Panorama et attribuer les groupes de dispositifs au groupe de notification. Si vous attribuez tous les systèmes virtuels à un seul groupe de périphériques, Panorama enregistrera les étiquettes dans un seul système virtuel du pare-feu.*

4. Sélectionnez les étiquettes que vous souhaitez récupérer à partir des VPC AWS.

   Vous pouvez **Select All 32 Tags** (Sélectionner les 32 étiquettes) (par défaut) ou choisir les **Custom Tags** (Étiquettes personnalisées) que vous voulez récupérer pour vos instances. Avec l'option Custom Tags (Étiquettes personnalisées), vous pouvez cliquer sur **Add (Ajouter)** pour ajouter les étiquettes prédéfinies et les étiquettes définies par l'utilisateur que vous souhaitez utiliser comme critères de correspondance dans la politique de sécurité. Si vous surveillez un grand nombre d'instances EC2, la réduction du nombre d'étiquettes

 ©2023 Palo Alto Networks, Inc.

récupérées garantit une utilisation plus efficace du processeur et de la capacité mémoire sur votre Panorama. Reportez-vous à la section Liste de vérification de planification pour la surveillance de la VM sur AWS pour obtenir des lignes directrices.



- Vérifier que la surveillance est activée sur le plugin. Ce réglage doit être activé pour que Panorama communique avec le nuage public AWS pour la surveillance VM.

  La case à cocher **Enable Monitoring (Activer la surveillance)** se trouve sur **Panorama** > **Plugins** > **AWS** > **Setup (Configuration)** > **General (Général)**.

STEP 3 | Créez une **Monitoring Definition (Définition de surveillance)** pour chaque VPC que vous souhaitez surveiller.

Lorsque vous ajoutez une nouvelle définition de surveillance, elle est activée par défaut.

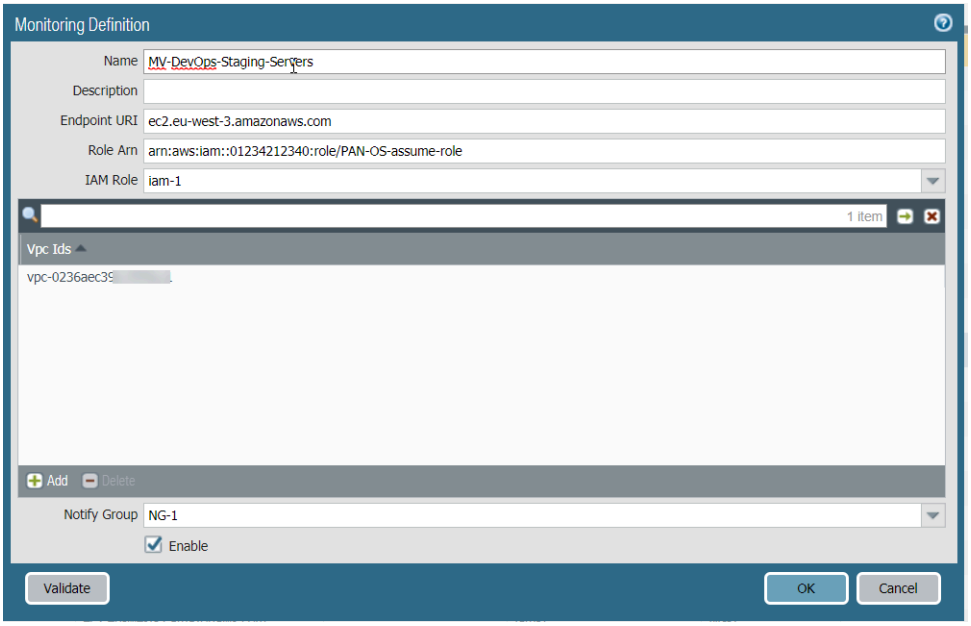
- Sélectionnez **Panorama** > **Plugins** > **AWS** > **Monitoring Definition (Définition de surveillance)** pour **Add (Ajouter)** une nouvelle définition.
- Entrez un **Name (Nom)** et une **Description** pour identifier le VPC du AWS pour lequel vous utilisez cette définition.
- Saisissez l'**Endpoint URI** (URI de terminal). La syntaxe est ec2.<your_region>.amazonaws.com ;

  Pour AWS China, il s'agit de ec2.<your region>.amazonaws.com.cn.
- (Facultatif) Saisissez le **Role ARN** (ARN de rôle) si vous avez configuré des rôles IAM et de chaînage de rôles avec des informations d'identification temporaires disposant des autorisations nécessaires pour utiliser l'API STS AWS pour accéder aux ressources AWS

 ©2023 Palo Alto Networks, Inc.

avec le même compte ou plusieurs comptes. L'ARN de rôle doit appartenir au VPC que vous souhaitez surveiller.

- Sélectionnez le **IAM Role** (Rôle IAM), **Add (Ajouter)** pour ajouter le **VPC ID (ID de VPC)** à partir du VPC Dashboard (Tableau de bord VPC) sur la console de gestion AWS et **Notify Group (Groupe de notification)**.



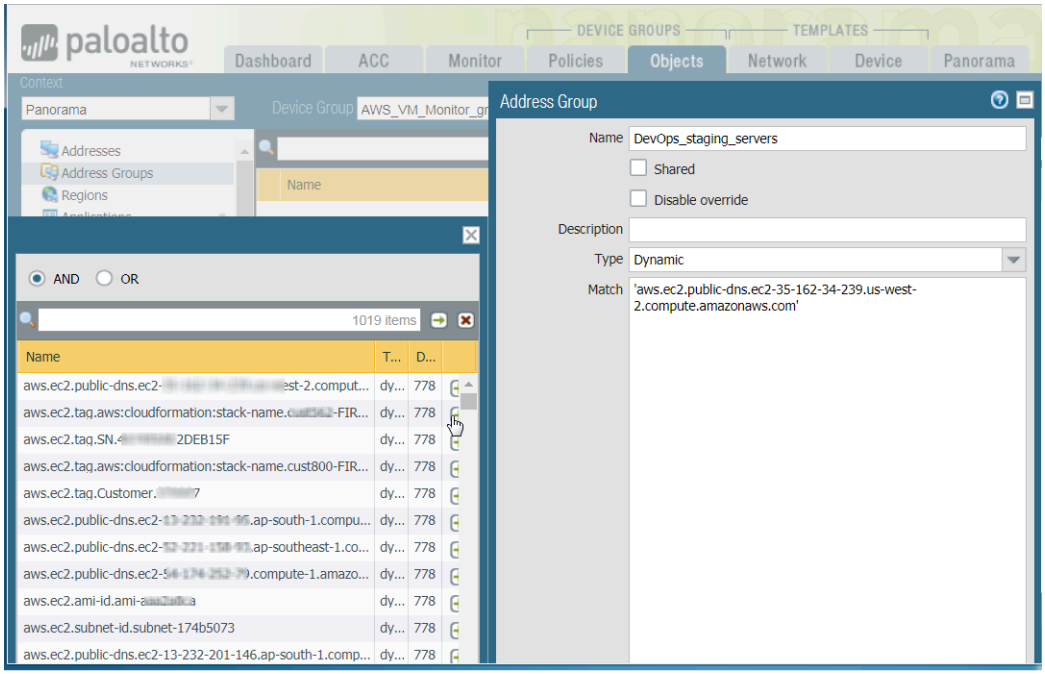
STEP 4 | **Engagez** les changements sur Panorama.

Assurez-vous que l'état de la définition de surveillance s'affiche comme « Succès ». S'il échoue, vérifiez que vous avez saisi l'AWS VPC ID (ID de VPC AWS) avec exactitude et que vous avez fourni les bonnes clés et les bons ID pour autoriser l'accès.

*Cliquez sur **Validate (Valider)** pour vérifier que Panorama peut s'authentifier à l'aide du rôle IAM et des clés et pour communiquer avec les VPC AWS que vous avez indiqués ci-dessus.*

©2023 Palo Alto Networks, Inc.

STEP 5 | Vérifiez que vous pouvez visualiser l'information VM sur Panorama et définir les critères d'appariement pour les groupes d'adresses dynamiques.



Sur le basculement HA, le Panorama nouvellement actif tente de se reconnecter au cloud AWS et de récupérer les étiquettes pour toutes les définitions de la surveillance. Si Panorama ne parvient pas à se reconnecter avec l'une des définitions de surveillance que vous avez configurées et activées, Panorama génère un message de journal système

```
Unable to process accounts after HA switch-over; user-intervention required.
```

Si cela se produit, vous devez vous connecter à Panorama et vérifier les définitions de surveillance pour corriger les informations d'identification non valides ou supprimer les comptes non valides. Bien que Panorama soit déconnecté du cloud AWS, toutes les étiquettes qui ont été récupérées pour les définitions de surveillance avant le basculement sont conservées et les pare-feu peuvent continuer d'appliquer la politique sur cette liste d'adresses IP. Panorama ne supprime toutes les étiquettes associées aux comptes que lorsque vous supprimez une définition de surveillance. Comme pratique exemplaire, pour surveiller ce problème, vous pouvez configurer log forwarding to an HTTPS destination (un journal orienté action vers une destination HTTPS) *à partir de Panorama afin de pouvoir prendre des mesures immédiatement.*

©2023 Palo Alto Networks, Inc.

STEP 6 | Sachez où trouver les journaux liés au plug-in AWS sur Panorama à des fins de dépannage.

- Utilisez la commande CLI **`less plugins-log`** pour afficher une liste de tous les journaux disponibles.

  plugin_aws_ret.log affiche les journaux liés à la récupération de l'adresses IP et des étiquettes.

  plugin_aws_proc.log affiche des journaux liés au traitement de l'adresse IP et des étiquettes.

  plugin_aws.log affiche des journaux liés à la configuration et aux démons du plug-in AWS.

Utilisez la commande **`show plugins aws vm-mon-status`** pour afficher l'état des définitions de surveillance.

```
admin@Panorama> show plugins aws vm-mon-status Mon-
Def Name VPC Status Last Updated Time Error Msg
 ------------------------------------------------------------------------------
 MD-Ins-Prof-ARN vpc-07986b091 Success 2019-12-02T10:24:56.007000
 MD-gov vpc-7ea1cf1a Success 2019-12-02T10:24:56.008000 MD-IAM-ARN
 vpc-025a83c123 Success 2019-12-02T10:24:56.012000
```

 ©2023 Palo Alto Networks, Inc.

Mise à l'échelle automatique de pare-feu VM-Series avec le service Amazon ELB

Les modèles de mise à l'échelle automatique pour AWS de Palo Alto Networks vous permettent de configurer et de déployer des pare-feu VM-Series pour protéger les applications déployées dans AWS. Les modèles exploitent les fonctionnalités d'évolutivité AWS pour mettre indépendamment et automatiquement à l'échelle les pare-feu VM-Series déployés dans AWS afin de répondre aux augmentations soudaines de la demande de ressources de charges de travail d'applications.

- Les fonctionnalités d'automatisation de VM-Series incluent l'API PAN-OS et l'amorçage (en utilisant un fichier d'amorçage pour la version 2.0 et Panorama pour la version 2.1).
- La technologie d'automatisation AWS inclut des modèles et des scripts CloudFormation pour des services AWS tels que Lambda, des groupes de mise à l'échelle automatique (ASG), Elastic Load Balancing (ELB), S3 et SNS.

Les modèles sont disponibles sur le référentiel GitHub pour la mise à l'échelle automatique des pare-feu VM-Series dans AWS de Palo Alto Networks :

- La version 2.0 fournit un modèle de pare-feu et un modèle d'application. Ces modèles et les scripts de prise en charge déploient des pare-feu VM-Series, un pare-feu Internet, un pare-feu interne et des ASG d'applications dans un seul Virtual Private Cloud (cloud privé virtuel – VPC) ou plusieurs VPC.

  Dans la version 2.0, Palo Alto Networks prend en charge le modèle de pare-feu et le modèle d'application est pris en charge par la communauté. Reportez-vous à la section Modèle de mise à l'échelle automatique VM-Series pour AWS version 2.0 pour obtenir des détails sur le déploiement.
- La version 2.1 ajoute également la prise en charge du déploiement dans un seul VPC et d'une topologie d'équilibreur de charge en sandwich qui vous permet de déployer les pare-feu VM-Series dans un VPC frontal et les applications principales dans un ou plusieurs VPC d'applications connectés par l'appariement VPC ou AWS PrivateLink.

  Dans la version 2.1, vous pouvez implémenter des équilibreurs de charge d'application (ALB) et des équilibreurs de charge réseau (NLB) dans les VPC. La version 2.1 inclut deux modèles de pare-feu et cinq modèles d'application. Reportez-vous à la section Modèles de mise à l'échelle automatique VM-Series pour AWS version 2.1 pour obtenir des détails sur le déploiement.

Si vous avez un déploiement de modèle existant, il n'y a aucune procédure de migration.

Le tableau suivant compare certaines fonctionnalités de haut niveau de chaque version de modèle.

Fonctionnalités/exigences	Version 2.0	Version 2.1
Panorama exécutant PAN-OS version 9.0.1 ou ultérieure en mode Panorama.	(Facultatif) Si vous choisissez d'utiliser Panorama, vous devez configurer l'appariement VPC entre le VPC de pare-feu VM-Series et les VPC	(Obligatoire) Déployez les modèles de la version 2.1.

©2023 Palo Alto Networks, Inc.

Fonctionnalités/exigences	Version 2.0	Version 2.1
Panorama avec une configuration High Availability (haute disponibilité – HA) n'est pas pris en charge.	d'application. Le trafic soumis à l'appariement traverse l'Internet public.	*Sur Panorama, vous devez installer manuellement le plug-in VM-Series pour permettre aux pare-feu VM-Series de publier des statistiques PAN-OS pour une mise à l'échelle automatique.*
Bootstrapping	Le fichier de configuration **`bootstrap.xml`** dans un compartiment S3.	Un fichier **`init-cfg.txt`** pour Panorama.
Exemple de compartiment S3 Palo Alto Networks	Utilisez votre propre compartiment S3 ou utilisez l'exemple dans panw-aws-autoscale-v20-us-west-2.	Utilisez votre propre compartiment S3 pour le déploiement.
VPC unique ou VPC distincts (en étoile)	Oui	Oui
Nouveau VPC	Oui	Oui
VPC existant (brown field)	Non	Oui
Zones de disponibilité par VPC	2	2-4
Équilibreur de charge externe	ALB seulement	ALB ou NLB
Équilibreur de charge interne	NLB seulement	ALB ou NLB
Connexion AWS PrivateLink au VPC de pare-feu VM-	Non	Oui

©2023 Palo Alto Networks, Inc.

Fonctionnalités/exigences	Version 2.0	Version 2.1
Series et aux serveurs principaux.		

Pour plus d'informations sur les modèles, reportez-vous à la section :

- Modèles de mise à l'échelle automatique VM-Series pour AWS version 2.0
- Modèles de mise à l'échelle automatique VM-Series pour AWS version 2.1

Modèles de mise à l'échelle automatique VM-Series pour AWS version 2.0

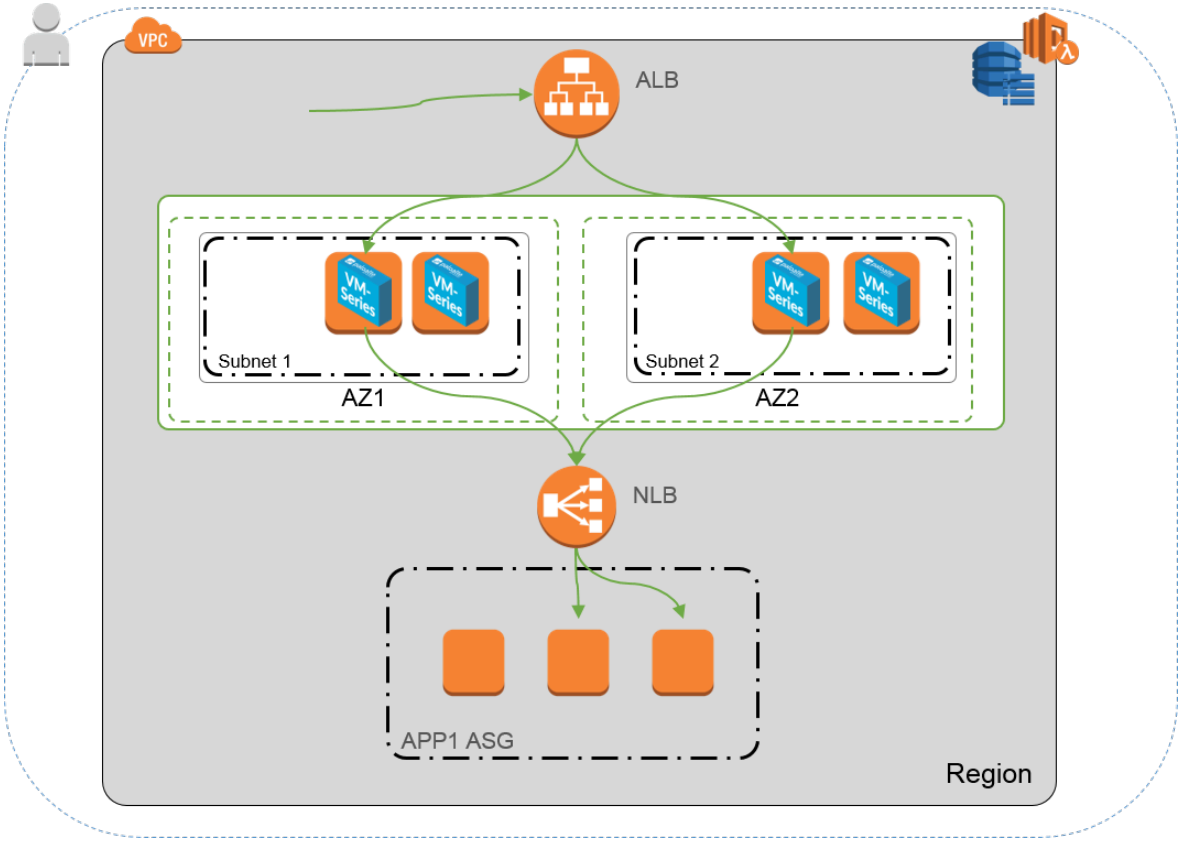
Pour vous aider à gérer l'augmentation de l'évolution des applications, la version 2.0 du modèle mise à l'échelle automatique de pare-feu VM-Series fournit une architecture en étoile qui simplifie le déploiement. Cette version de la solution fournit deux modèles qui prennent en charge un déploiement mono et multi-VPC à la fois dans un même compte AWS et dans plusieurs comptes AWS.

- **Modèle de pare-feu** : le modèle de pare-feu déploie un équilibreur de charge d'application (ALB) et des pare-feu VM-Series dans des groupes de mise à l'échelle automatique sur deux zones de disponibilité (AZ). Cet ALB Internet distribue le trafic entrant dans le VPC à travers un pool de

©2023 Palo Alto Networks, Inc.

pare-feu VM-Series. Les pare-feu VM-Series publient automatiquement des métriques PAN-OS personnalisées qui permettent la mise à l'échelle automatique.

Palo Alto Networks prend officiellement en charge le modèle de pare-feu et, avec une autorisation de support valide, vous pouvez demander l'assistance du support technique de Palo Alto Networks.



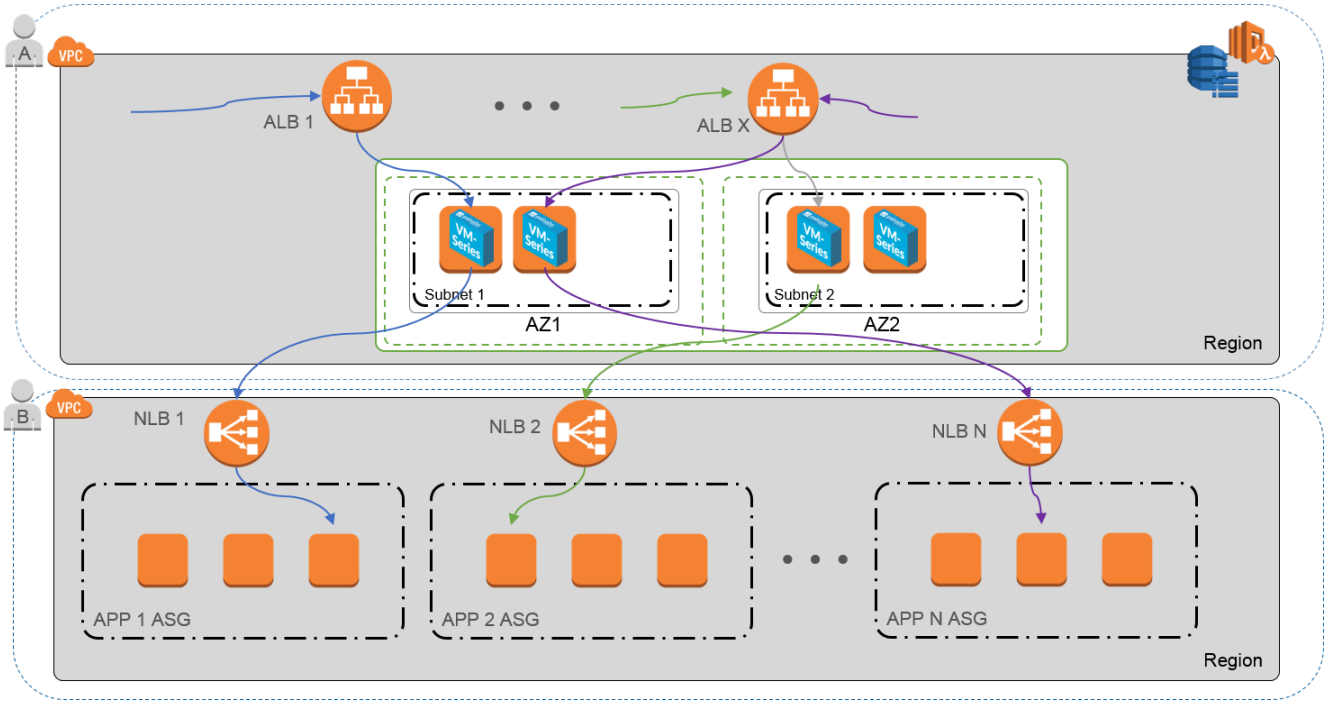
Le modèle d'application suivant déploie l'équilibreur de charge réseau illustré dans l'image précédente.

- **Modèle d'application** : le modèle d'application déploie un équilibreur de charge réseau (NLB) et un groupe de mise à l'échelle automatique (ASG) avec un serveur Web dans chaque zone de disponibilité (AZ).

  Le modèle d'application est pris en charge par la communauté. Ce modèle est fourni à titre d'exemple pour vous aider à démarrer avec une application Web de base. Pour un environnement de production, utilisez votre propre modèle d'application ou personnalisez ce modèle pour répondre à vos besoins.

Ces modèles vous permettent de déployer une topologie sandwich d'équilibreur de charge avec un ALB connecté à Internet et un NLB interne. L'ALB est accessible depuis Internet et distribue le trafic entrant dans le VPC à travers un pool de pare-feu VM-Series. Les pare-feu acheminent ensuite le trafic à l'aide de la politique NAT vers les NLB, qui distribuent le trafic vers un niveau de mise à l'échelle automatique des serveurs Web ou d'application. Les pare-feu VM-Series sont autorisés à publier des métriques PAN-OS personnalisées sur AWS CloudWatch où vous pouvez surveiller la santé et la charge de ressources sur les pare-feu VM-Series, puis utiliser ces informations pour déclencher des événements de mise à l'échelle automatique dans les ASG appropriés des pare-feu.

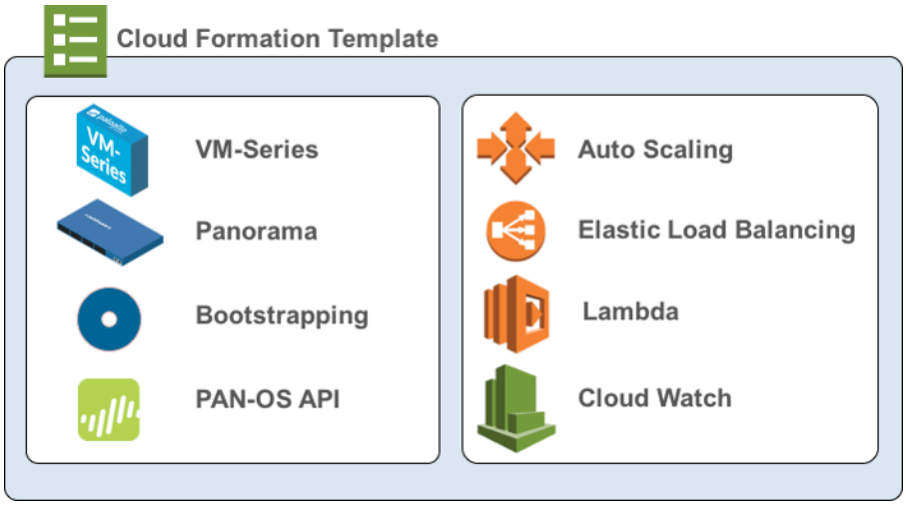
©2023 Palo Alto Networks, Inc.



- Quels sont les composants déployés par le modèle de mise à l'échelle automatique de VM-Series pour AWS (v2.0) ?
- Comment le modèle de mise à l'échelle automatique de VM-Series pour AWS (v2.0) active-t-il la mise à l'échelle dynamique ?
- Planification du modèle de mise à l'échelle automatique de VM-Series pour AWS (v2.0)
- Personnalisation du modèle de pare-feu avant le lancement (v2.0)
- Lancement du modèle de mise à l'échelle automatique de VM-Series pour AWS (v2.0)
- Personnalisation du fichier bootstrap.xml (v2.0)
- Mise à jour de la pile avec le modèle de mise à l'échelle automatique VM-Series pour AWS (v2.0)
- Modification du compte administrateur et mise à jour de la pile

©2023 Palo Alto Networks, Inc.

Quels sont les composants déployés par le modèle de mise à l'échelle automatique de VM-Series pour AWS (v2.0) ?



Le modèle de mise à l'échelle automatique VM-Series pour AWS comprend les blocs de construction suivants :

Bloc de construction	Description
Modèle de pare-feu (Modèle officiellement pris en charge par Palo Alto Networks)	Le modèle `firewall-v2.0.template` déploie un nouveau VPC avec des sous-réseaux, des tables de routage, une passerelle NAT AWS, deux zones de disponibilité (AZ) et des groupes de sécurité requis pour le routage du trafic entre ces AZ. Ce modèle de version 2.0 déploie également un ALB externe, ainsi qu'un ASG avec un pare-feu VM-Series dans chaque AZ. En raison des nombreuses variations dans un environnement de production qui comprend, sans toutefois s'y limiter, plusieurs composants spécifiques comme des sous-réseaux, des zones de disponibilité, des tables de routage et des groupes de sécurité. Vous devez déployer le modèle `firewall-v2.0.template` dans un nouveau VPC. *Le modèle de mise à l'échelle automatique VM-Series pour AWS ne déploie pas Panorama, et Panorama est facultatif. Panorama facilite la gestion des politiques et la visibilité centrale. Si vous souhaitez utiliser Panorama pour gérer les pare-feu VM-Series déployées par la solution, vous pouvez utiliser une application M-Series ou une application virtuelle Panorama dans votre réseau d'entreprise, ou vous pouvez utiliser une application virtuelle Panorama sur AWS.* Cette solution inclut une passerelle NAT AWS utilisée par les pare-feu pour lancer des requêtes sortantes afin de récupérer les mises à jour, se connecter à Panorama et publier des métriques dans AWS CloudWatch.

©2023 Palo Alto Networks, Inc.

Bloc de construction	Description
Modèle d'application (Modèle pris en charge par la communauté)	Le modèle d'application déploie un NLB et un ASG avec un serveur Web dans chaque AZ. Étant donné que le NLB possède une adresse IP unique pour chaque AZ et que la règle de politique NAT sur les pare-feu doit faire référence à une adresse IP unique, il existe un groupe de contrôle d'accès pour chacune des deux AZ. Tous les pare-feu d'un ASG possèdent une configuration identique. La version 2.0 de la solution de mise à l'échelle automatique comprend deux modèles d'application : • Le `panw_aws_nlb-v2.0.template` vous permet de déployer les ressources de modèle d'application au sein du même VPC que celui dans lequel vous avez déployé le modèle de pare-feu (même compte AWS). • Le modèle `panw_aws_nlb_vpcv-2.0.template` vous permet de déployer les ressources du modèle d'application dans un VPC distinct en utilisant le même compte AWS ou plusieurs comptes AWS.
Fonctions Lambda	AWS Lambda fournit une automatisation robuste, dirigée par les événements, sans devoir recourir à un logiciel d'orchestration complexe. Dans le modèle `firewall-v2.0.template`, AWS Lambda surveille un service SQS (Simple Queue Service) pour en savoir plus sur les NLB qui sont publiés dans la file d'attente. Lorsque la fonction Lambda détecte un nouvel NLB, elle crée une nouvelle règle de politique NAT et l'applique aux pare-feu VM-Series dans l'ASG. Les pare-feu ont une règle de politique NAT pour chaque application et utilisent la règle de politique NAT (qui mappe le port à l'adresse IP du NLB) pour transférer le trafic vers le NLB devant les serveurs Web d'application. *Vous devez créer la règle de politique de sécurité pour autoriser ou refuser le trafic d'application pour votre déploiement. L'exemple de fichier `bootstrap.xml` n'inclut aucune règle de politique de sécurité. Utilisez Panorama pour gérer de manière centralisée vos pare-feu et simplifier la création de règles de politique de sécurité.* Il y a également d'autres fonctions : • Ajoute ou supprime une interface (ENI) lorsqu'une interface est lancée ou résiliée. • Supprime toutes les ressources associées lorsque vous supprimez une pile ou résiliez une instance. • Supprime un pare-feu en tant que périphérique géré Panorama lorsqu'il y a un événement de mise à l'échelle. • Désactive la licence BYOL lorsqu'un événement de mise à l'échelle entraîne une résiliation du pare-feu.

©2023 Palo Alto Networks, Inc.

Bloc de construction	Description
	Pour en savoir plus sur les fonctions lambda, consultez **http://paloaltonetworks-aws-autoscale-2-0.readthedocs.io/en/latest/**
Fichiers d'amorçage Le fichier bootstrap.xml fourni dans le référentiel GitHub est fourni uniquement pour les tests et l'évaluation. Pour un déploiement de production, vous devez modifier les informations d'identification d'exemple dans le fichier bootstrap.xml avant le lancement.	Cette solution nécessite le fichier init-cfg.txt et le fichier bootstrap.xml afin que le pare-feu VM-Series dispose de la configuration de base pour la gestion du trafic. • Le fichier **`init-cfg.txt`** inclut la commande opérationnelle mgmt-interface-swap pour permettre au pare-feu de recevoir le trafic du plan de données sur son interface principale (eth0). Cette solution de mise à l'échelle automatique nécessite l'échange des interfaces du plan de données et de gestion pour permettre à l'ALB de transférer le trafic Web vers le niveau de mise à l'échelle automatique des pare-feu VM-Series. Pour plus de détails, reportez-vous à la section Mappage d'interface de gestion pour l'utilisation avec Amazon ELB. • Le fichier **`bootstrap.xml`** active la connectivité de base pour les interfaces réseau du pare-feu et permet au pare-feu de se connecter à l'espace de noms AWS CloudWatch correspondant au nom de la pile que vous entrez lorsque vous lancez le modèle.

Pour déployer la solution, reportez-vous à la section Lancement du modèle de mise à l'échelle automatique de VM-Series pour AWS (v2.0).

Comment le modèle de mise à l'échelle automatique VM-Series pour AWS (v2.0 et v2.1) active-t-il la mise à l'échelle dynamique ?

Le pare-feu VM-Series réalise une mise à l'échelle (augmentation et diminution) en utilisant les pare-feu VM-Series qui sont déployés à l'aide des modèles de mise à l'échelle automatique selon les métriques PAN-OS personnalisées. Les pare-feu VM-Series publient de manière native ces métriques sur la console Amazon CloudWatch et, en fonction des métriques que vous choisissez pour les paramètres de mise à l'échelle, vous pouvez définir des alarmes et des politiques CloudWatch pour déployer ou arrêter dynamiquement les instances permettant de gérer le trafic d'applications dans votre déploiement AWS.

Les pare-feu publient les métriques sur AWS CloudWatch toutes les cinq minutes (par défaut). Lorsqu'une métrique surveillée atteint le seuil configuré pour l'intervalle de temps défini, CloudWatch déclenche une alarme et un événement de mise à l'échelle automatique.

Lorsque l'événement de mise à l'échelle automatique déclenche le déploiement d'un nouveau pare-feu, la nouvelle instance s'amorce au démarrage et une fonction AWS Lambda configure le pare-feu avec des règles de politique NAT. Une règle de politique NAT est créée pour chaque application et la règle référence les adresses IP de chaque équilibreur de charge réseau dans votre déploiement. Lorsque l'équilibreur de charge d'application reçoit une requête, il la transmet au pare-feu sur le port TCP affecté. Le pare-feu inspecte alors le trafic et le transmet à l'équilibreur de charge réseau correspondant, qui à son tour transmet la requête à un serveur Web de son groupe cible.

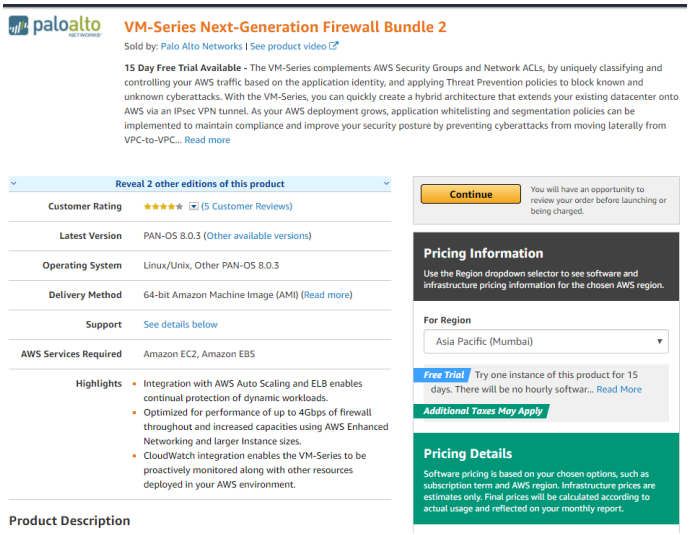
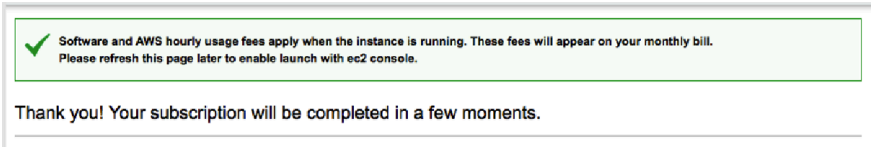
 ©2023 Palo Alto Networks, Inc.

Planification du modèle de mise à l'échelle automatique VM-Series pour AWS (v2.0 et v2.1)

Les éléments de cette liste de contrôle sont des actions et des choix que vous devez effectuer pour mettre en œuvre cette solution.

Planification de la liste de contrôle pour les modèles v2.0 et v2.1	
❑ Vérifiez les conditions requises pour le déploiement du modèle de mise à l'échelle automatique VM-Series.	Le modèle de mise à l'échelle automatique nécessite AWS Lambda et S3 Signature versions 2 ou 4, et peut déployer des pare-feu VM-Series exécutant les versions de PAN-OS prises en charge. Vous devez consulter la liste des régions prises en charge et les ID AMI, à fournir en tant qu'entrée dans le modèle de pare-feu.
❑ Affectez les autorisations appropriées au rôle d'utilisateur IAM.	L'utilisateur qui déploie le modèle de mise à l'échelle automatique VM-Series doit disposer de privilèges administratifs ou disposer des autorisations répertoriées dans iam-policy.json pour lancer cette solution avec succès. Copiez et collez les autorisations de ce fichier dans une nouvelle politique IAM, puis associez la politique à un rôle IAM nouveau ou existant. Pour un déploiement entre comptes, afin d'accéder aux ressources d'un compte AWS différent, le rôle IAM de l'utilisateur qui déploie le modèle d'application doit disposer d'autorisations d'accès SQS complètes et d'une relation d'approbation l'autorisant l'écriture dans la file d'attente SQS au modèle de pare-feu.
❑ Recueillez les détails requis pour un déploiement entre comptes.	Pour un déploiement où le modèle de pare-feu et le modèle d'application se trouvent dans des comptes différents, le compte qui héberge les ressources du modèle de pare-feu est le compte d'approbation, et les autres comptes AWS qui contiennent les ressources du modèle d'application sont les comptes approuvés. Pour lancer le modèle d'application dans un déploiement entre comptes, vous devez disposer des informations suivantes : • Nom de ressource Amazon (ARN) de rôle entre comptes du compte dans lequel vous déployez le modèle d'application. • ID externe, que vous avez défini lors de la création du rôle IAM qui accorde un accès SQS complet au compte d'approbation. • Le numéro de compte à 10 chiffres pour chaque compte AWS dans lequel vous envisagez de lancer le modèle d'application. Étant donné que le compte hébergeant les ressources du modèle de pare-feu sert de compte d'approbation et qu'il possède les ressources nécessaires aux utilisateurs du modèle d'application, vous devez répertorier le numéro de compte de chaque compte approuvé pouvant accéder aux ressources du pare-feu.

©2023 Palo Alto Networks, Inc.

Planification de la liste de contrôle pour les modèles v2.0 et v2.1	
❑ Création d'un compte de support sur le portail de support de Palo Alto Networks, si vous n'en avez pas déjà un.	Vous pouvez opter pour les licences BYOL ou PAYG. • Pour BYOL, vous devez enregistrer un code d'autorisation auprès de votre compte de support Palo Alto Networks avant de lancer le modèle de mise à l'échelle VM-Series, et ajouter le code d'autorisation au dossier `/license` avec le nom de fichier authcodes dans l'ensemble d'amorçage. Reportez-vous à la section Lancement du modèle de mise à l'échelle automatique VM-Series pour AWS (v2.0) ou Lancement du modèle de pare-feu (v2.1) pour plus de détails. • Pour PAYG, vous devez enregistrer les pare-feu VM-Series pour activer votre autorisation de support.
❑ (Pour PAYG uniquement) Passez en revue et acceptez le Contrat de Licence Utilisateur Final (CLUF). Cela est requis, si vous lancez un pare-feu VM-Series dans un compte AWS pour la première fois.	Dans AWS Marketplace, recherchez Palo Alto Networks et sélectionnez le forfait que vous prévoyez d'utiliser. Les pare-feu VM-Series ne se déploieront pas si vous n'avez pas accepté le CLUF pour le forfait que vous prévoyez d'utiliser. • Recherchez **VM-Series Next Generation Firewall Bundle 2 (Forfait de pare-feu nouvelle génération VM-Series 2), par exemple**.  • Cliquez sur **Continue (Continuer)** et sélectionnez **Manual Launch (Lancement manuel)**. Passez en revue le contrat et cliquez sur **Accept Software Terms (Accepter les conditions du logiciel)** pour accepter le CLUF.  Vous pouvez maintenant fermer le navigateur.

©2023 Palo Alto Networks, Inc.

Planification de la liste de contrôle pour les modèles v2.0 et v2.1	
❑ Décidez si vous envisagez d'utiliser les compartiments S3 publics ou votre compartiment S3 privé pour AWS Lambda, les scripts Python et les modèles.	Palo Alto Networks fournit des compartiments S3 publics dans toutes les régions AWS incluses dans la liste des régions prises en charge. Ces compartiments S3 incluent tous les modèles, le code AWS Lambda et les fichiers d'amorçage dont vous avez besoin. ***Palo Alto Networks recommande d'utiliser les fichiers d'amorçage dans le compartiment public S3 uniquement pour évaluer cette solution. Pour un déploiement de production, vous devez créer un compartiment S3 privé pour l'ensemble d'amorçage.*** La convention de dénomination pour le compartiment S3 est `panw-aws-autoscale-v20-<region_name>`. Par exemple, le compartiment dans la région AWS Oregon est panw-aws-autoscale-v20-us-west-2. Pour utiliser votre compartiment S3 privé, vous devez télécharger et copier les modèles, le code AWS Lambda et les fichiers d'amorçage dans votre compartiment S3 privé. Vous pouvez placer tous les fichiers requis pour le modèle de pare-feu et le modèle d'application dans un compartiment S3, ou les placer dans des compartiments S3 distincts.

❑ Téléchargez les modèles, le code AWS Lambda et les fichiers d'amorçage.	• Obtenez les fichiers pour le déploiement du modèle de pare-feu (équilibreur de charge d'application et pare-feu VM-Series) depuis le référentiel GitHub.
	
	Ne combinez pas les fichiers entre différentes versions de modèles de mise à l'échelle automatique VM-Series.
	
	• Modèles et code lambda :
	  • panw-aws.zip
	  • firewall-v2.X.template
	• Fichiers d'amorçage :
	  • init-cfg.txt
	  • bootstrap.xml
	  Le fichier bootstrap.xml fourni avec cette solution est conçu pour vous aider à démarrer et n'est fourni que pour les tests et l'évaluation. Pour un déploiement de production, vous devez modifier le fichier bootstrap.xml avant le lancement.
	• iam-policy : l'utilisateur qui déploie le modèle de mise à l'échelle automatique VM-Series doit disposer des privilèges

©2023 Palo Alto Networks, Inc.

Planification de la liste de contrôle pour les modèles v2.0 et v2.1	

	d'administration ou des autorisations répertoriées dans ce fichier pour lancer cette solution avec succès.
	
	Le modèle de pare-feu est pris en charge par le support technique de Palo Alto Networks.
	
	• Obtenez les fichiers pour le déploiement de l'équilibrage de la charge réseau et des serveurs Web à partir des versions 2.0 ou 2.1 du référentiel GitHub.
	  • Modèles :
	  • pan_aws_nlb-2.X.template : utilisez ce modèle pour déployer les ressources de modèle d'application au sein du même VPC que celui dans lequel vous avez déployé le modèle de pare-feu (même compte AWS).
	  • pan_aws_nlb_vpc-2.X.template : utilisez ce modèle pour déployer les ressources du modèle d'application dans un autre VPC. Ce modèle vous permet de déployer les ressources dans le même compte AWS ou dans un autre compte AWS, à condition que vous disposiez des autorisations appropriées pour prendre en charge un déploiement entre comptes.
	  • pan_nlb_lambda.template : crée un équilibreur de charge AWS Network, qui multiplexe le trafic pour enregistrer les serveurs web de back-end mis à l'échelle.
	  • Code Lambda et scripts Python.

❑ Personnalisez le fichier bootstrap.xml pour votre environnement de production.	Pour vous assurer que votre environnement de production est sécurisé, vous devez personnaliser le fichier bootstrap.xml avec un nom d'utilisateur et un mot de passe administratifs uniques pour les déploiements de production. Le nom d'utilisateur et le mot de passe par défaut sont pandemo/demopassword. Vous pouvez également utiliser cette opportunité pour créer une configuration de pare-feu optimale avec des interfaces, des zones et des règles de politique de sécurité qui répondent aux besoins de sécurité de votre application.
❑ Décidez si vous souhaitez utiliser Panorama pour la journalisation centralisée, la création de rapports et la gestion des pare-feu.	Panorama est une option pour faciliter l'administration, et constitue la meilleure pratique pour gérer les pare-feu. Il n'est pas nécessaire de gérer le niveau de mise à l'échelle automatique des pare-feu VM-Series déployés dans cette solution. Si vous souhaitez utiliser Panorama, vous pouvez utiliser un dispositif virtuel Panorama sur AWS ou utiliser un dispositif M-Series ou un dispositif virtuel Panorama dans votre réseau d'entreprise. ***Le Panorama doit être en mode Panorama et non en mode Gestion uniquement.***

©2023 Palo Alto Networks, Inc.

Planification de la liste de contrôle pour les modèles v2.0 et v2.1	
	Pour enregistrer correctement les pare-feu avec Panorama, vous devez recueillir les informations suivantes : • Clé d'API pour Panorama : afin qu'AWS Lambda puisse faire des requêtes d'API à Panorama, vous devez fournir une clé API lorsque vous lancez le modèle de mise à l'échelle automatique VM-Series. En guise de meilleure pratique, dans un déploiement de production, créez un compte administrateur distinct uniquement pour l'appel d'API et générez une clé API associée. • Adresse IP de panorama : vous devez inclure l'adresse IP dans le fichier de configuration (init-cfg.txt). Les pare-feu doivent pouvoir accéder à cette adresse IP à partir du VPC. Pour assurer une connexion sécurisée, utilisez un lien de connexion directe ou un tunnel IPSec. • Clé d'authentification de la machine virtuelle : permet à Panorama d'authentifier les pare-feu afin de pouvoir ajouter chaque pare-feu en tant que périphérique géré. Vous devez inclure cette clé dans le fichier de configuration (init-cfg.txt). La clé d'authentification VM est requise pour la durée de vie du déploiement. Sans clé valide dans la requête de connexion, le pare-feu VM-Series ne pourra pas s'enregistrer auprès de Panorama. Pour en savoir plus sur la clé, consultez Génération de la clé d'authentification VM sur Panorama. • Nom de la pile de modèles et nom du groupe de périphériques auquel attribuer les pare-feu : vous devez d'abord ajouter un modèle et l'affecter à une pile de modèles, créer un groupe de périphériques sur Panorama, puis inclure le nom de la pile de modèles et le nom du groupe de périphériques dans le fichier de configuration (init-cfg.txt). ***Afin de réduire les coûts et les limites de mise à l'échelle des adresses IP élastiques, les pare-feu n'ont pas d'adresse IP publique. Si vous n'utilisez pas Panorama pour gérer les pare-feu, vous devez déployer un serveur de saut (un hôte bastion avec une adresse EIP) qui se connecte au sous-réseau non approuvé dans le VPC pour activer l'accès SSH et/ou HTTPS aux pare-feu VM-Series. Par défaut, cette solution inclut une passerelle NAT AWS utilisée par les pare-feu pour lancer des requêtes sortantes afin de récupérer les mises à jour, se connecter à Panorama et publier des métriques dans AWS CloudWatch.***
Commencez.	Lancement du modèle de mise à l'échelle automatique de VM-Series pour AWS (v2.0).

©2023 Palo Alto Networks, Inc.

Personnalisation du modèle de pare-feu avant le lancement (v2.0 et v2.1)

Pour simplifier le flux de travail de déploiement, le pare-feu affiche un ensemble limité de paramètres pour lesquels vous devez fournir des entrées lors du lancement du modèle. Si vous souhaitez afficher et personnaliser d'autres options incluses dans le modèle, vous pouvez utiliser un outil de modification de texte tel que Notepad ou Visual Studio Code pour spécifier les valeurs que vous préférez avant le lancement du modèle de mise à l'échelle automatique VM-Series pour AWS v2.0 ou 2.1.

Utilisez le tableau suivant pour consulter la liste des paramètres que vous êtes autorisé à personnaliser pour votre déploiement du modèle de pare-feu à mise à l'échelle automatique pour AWS. La modification des paramètres de cette liste fait partie de la politique de support officielle de Palo Alto Networks via les options de support que vous avez achetées.

Paramètre	Description	Valeur par défaut
CIDR Block for the VPC (Bloc CIDR pour le VPC)	L'espace d'adressage IP que vous souhaitez utiliser pour le VPC. ***Les sous-réseaux que vous modifiez ci-dessous doivent appartenir à ce bloc VPC CIDR et être uniques.***	192.168.0.0/16
Management Subnet CIDR Block (Bloc CIDR de sous-réseau de gestion)	Liste délimitée par des virgules de blocs CIDR pour le sous-réseau de gestion des pare-feu.	192.168.0.0/24, 192.168.10.0/24
Untrust Subnet CIDR Block (Bloc de sous-réseau CIDR non approuvé)	Liste délimitée par des virgules de blocs CIDR pour le sous-réseau non approuvé.	192.168.1.0/24, 192.168.11.0/24
Trust Subnet CIDR Block (Bloc de sous-réseau CIDR approuvé)	Liste délimitée par des virgules de blocs CIDR pour le sous-réseau approuvé.	192.168.2.0/24, 192.168.12.0/24
NAT Gateway Subnet CIDR Block (Bloc CIDR de sous-réseau de passerelle NAT)	Liste délimitée par des virgules de blocs CIDR pour la passerelle NAT AWS.	192.168.100.0/24, 192.168.101.0/24
Lambda Subnet CIDR Block (Bloc CIDR sous-réseau Lambda)	Liste délimitée par des virgules de blocs CIDR pour les fonctions Lambda.	192.168.200.0/24, 192.168.201.0/24
Firewall Instance size (Taille de l'instance de pare-feu)	Les types d'instances AWS et la taille que vous souhaitez pour les pare-feu VM-Series dans votre déploiement.	M4.xlarge
Choose your Scaling Parameter (Choisissez	Le modèle publie toutes les mesures suivantes dans AWS CloudWatch :	Dataplane CPU Utilization (Utilisation

©2023 Palo Alto Networks, Inc.

Paramètre	Description	Valeur par défaut
votre paramètre de mise à l'échelle) ***Vous n'avez pas besoin de modifier le modèle pour le paramètre de mise à l'échelle. Vous pouvez définir les alarmes AWS CloudWatch sur la console AWS pour une ou plusieurs métriques PAN-OS personnalisées sur lesquelles vous souhaitez déclencher la mise à l'échelle automatique.***	• CPU—DataPlane CPU Utilization (Utilisation du processeur du plan de données) • AS—Active Sessions (Sessions actives) • SU—Session Utilization (Utilisation de session) • SSPU—SSL Proxy Utilization (Utilisation du proxy SSL) • GPU—GlobalProtect Gateway Utilization (Utilisation de la passerelle GlobalProtect) • GPAT—GlobalProtect Gateway Utilization ActiveTunnels (Tunnels actifs d'utilisation de la passerelle GlobalProtect) • DPB—Dataplane Packet Buffer Utilization (Utilisation de la mémoire tampon des paquets du plan de données)	du processeur du dataplane)
Choose time in seconds for Scaling Period (Choisissez le temps en secondes pour la période de mise à l'échelle)	La durée en secondes pendant laquelle la statistique moyenne est appliquée. Elle doit être un multiple de 60.	900
Maximum VM-Series Instances (Nombre maximum d'instances VM-Series)	Nombre maximum de pare-feu VM-Series dans le groupe de mise à l'échelle automatique.	3
Minimum VM-Series Instances (Nombre minimum d'instances VM-Series)	Nombre minimum de pare-feu VM-Series dans le groupe de mise à l'échelle automatique.	1
ScaleDown threshold value in percentage/value (Valeur du seuil de descente en	Valeur à laquelle un événement de diminution (mise à l'échelle) est déclenché.	20

©2023 Palo Alto Networks, Inc.

Paramètre	Description	Valeur par défaut
puissance en pourcentage/valeur)		
ScaleUp threshold value in percentage/value (Valeur du seuil de montée en puissance en pourcentage/valeur)	Valeur à laquelle l'événement d'augmentation (mise à l'échelle) est déclenché.	80

Lancement du modèle de mise à l'échelle automatique de VM-Series pour AWS (v2.0)

Vous pouvez choisir de déployer le modèle de pare-feu dans un VPC et l'exemple de modèle d'application dans le même VPC que celui dans lequel vous avez déployé les pare-feu, ou dans un VPC différent.

Si les applications que vous souhaitez sécuriser appartiennent à un compte AWS distinct, l'exemple de modèle d'application inclut la prise en charge des déploiements entre comptes. La solution prend en charge une architecture en étoile permettant de déployer le modèle de pare-feu dans un compte AWS et de l'utiliser comme concentrateur pour sécuriser vos applications (branches) appartenant au même ou à différents comptes AWS.

- Lancement du modèle de pare-feu VM-Series
- Lancement du modèle d'application
- (Requis uniquement si vous déployez plusieurs équilibreurs de charge internes) Activation du trafic vers le service ELB (v2.0 et v2.1)

Lancement du modèle de pare-feu VM-Series

Ce flux de travail vous indique comment déployer l'équilibreur de charge de l'application et les pare-feu VM-Series à l'aide du modèle de pare-feu.

Ce modèle de pare-feu inclut une passerelle NAT AWS utilisée par les pare-feu pour lancer des requêtes sortantes afin de récupérer les mises à jour, se connecter à Panorama et publier des métriques dans AWS CloudWatch. Si vous n'utilisez pas Panorama pour gérer les pare-feu, vous devez déployer un serveur de saut (un hôte bastion avec une adresse EIP) qui se connecte au sous-réseau non approuvé dans le VPC pour activer l'accès SSH et/ou HTTPS aux pare-feu VM-Series. Ce serveur de saut est requis car l'interface de gestion des pare-feu VM-Series possède uniquement une adresse IP privée.

©2023 Palo Alto Networks, Inc.

STEP 1 | Examinez la liste de contrôle pour la Planification du modèle de mise à l'échelle automatique VM-Series pour AWS (v2.0).

Assurez-vous que vous avez effectué les tâches suivantes :

- (Pour PAYG uniquement) Passez en revue et acceptez le CLUF pour le forfait PAYG que vous prévoyez d'utiliser.
- (Pour BYOL uniquement) Obtenez le code d'autorisation. Vous devez entrer ce code d'autorisation dans le dossier /license de l'ensemble d'amorçage.
- Téléchargez les fichiers requis pour lancer le modèle de mise à l'échelle automatique VM-Series à partir du référentiel GitHub.

STEP 2 | Modifiez le fichier init-cfg.txt. Vous devez ajouter le PIN d'enregistrement automatique du certificat de périphérique au fichier init-cfg.txt pour installer automatiquement un certificat de périphérique lorsque votre instance de pare-feu VM-Series est déployée.

vm-series-auto-registration-id=

vm-series-auto-registration-pin-value=

Pour plus de détails, lisez les sections sur le processus d'amorçage et le fichier le init-cfg.txt .

Si vous utilisez Panorama pour gérer les pare-feu, effectuez les tâches suivantes :

1. Génération de la clé d'authentification VM sur Panorama. Les pare-feu doivent inclure une clé valide dans la requête de connexion à Panorama. Définissez la durée de vie de la clé sur 8 760 heures (1 an).
2. Ouvrez le fichier init-cfg.txt avec un éditeur de texte, tel que le Bloc-notes. Assurez-vous que vous ne modifiez pas le format, car cela entraîne un échec du déploiement du modèle

 ©2023 Palo Alto Networks, Inc.

de mise à l'échelle VM-Series. Ajoutez les informations suivantes en tant que paires nom-valeur :

- Adresses IP pour le Panorama principal et éventuellement un Panorama secondaire. Entrez :

  panorama-server=

  panorama-server-2=
- Spécifiez le nom de la pile de modèles et le groupe de périphériques auxquels vous voulez attribuer le pare-feu. Entrez :

  tplname=

  dgname=
- Clé d'authentification VM. Entrez :

  vm-auth-key=

3. Vérifiez que vous n'avez pas supprimé la commande pour la permutation de l'interface de gestion (mgmt) et de l'interface du dataplane (ethernet 1/1) sur le pare-feu VM-Series sur AWS. Par exemple, le fichier doit inclure des paires nom-valeur comme indiqué ici :

   op-command-modes=mgmt-interface-swap

   vm-auth-key=755036225328715

   panorama-server=10.5.107.20

   panorama-server-2=10.5.107.21

   tplname=FINANCE_TG4

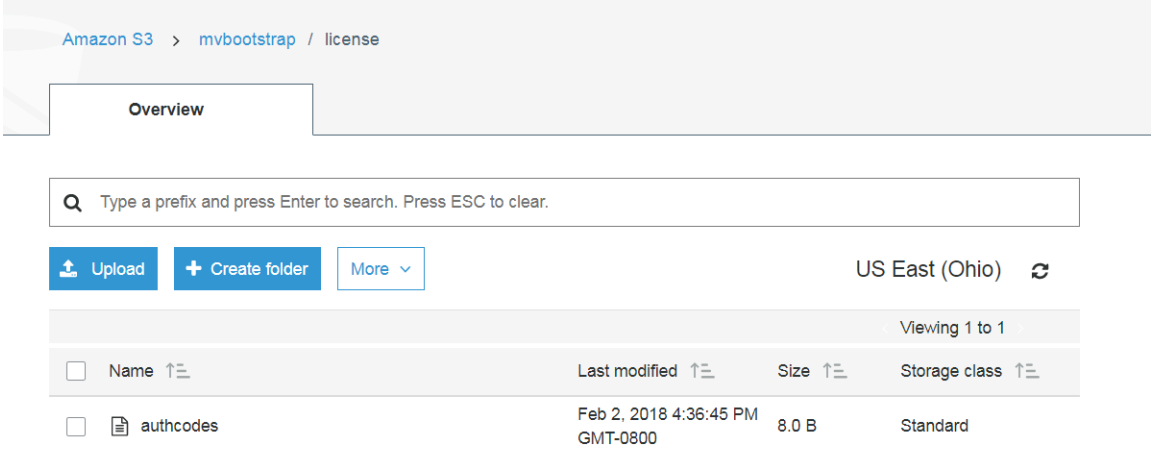
   dgname=finance_dg
4. Enregistrez et fermez le fichier.

STEP 3 | (Pour BYOL uniquement) Ajoutez le code d'autorisation de licence au dossier /license de l'ensemble d'amorçage. Pour plus d'informations, consultez Préparation de l'ensemble d'amorçage.

1. Créez un nouveau fichier .txt avec un éditeur de texte, tel que Notepad.
2. Ajoutez le code d'authentification pour vos licences BYOL à ce fichier, ensuite enregistrez le fichier avec authcodes (sans écrire l'extension de fichier) et téléchargez-le dans le dossier / license. Le code d'autorisation doit prendre en charge le nombre de pare-feu pouvant être requis pour votre déploiement. Vous devez utiliser un ensemble de codes d'authentification au lieu de codes individuels de sorte que le pare-feu puisse extraire simultanément toutes les clés de licence associées au pare-feu. Si vous utilisez des codes d'authentification

 ©2023 Palo Alto Networks, Inc.

individuels au lieu d'un ensemble, le pare-feu ne récupère que la clé de licence pour le premier code d'authentification inclus dans le fichier.



STEP 4 | Modifiez les informations d'identification par défaut pour le compte administrateur du pare-feu VM-Series défini dans le fichier bootstrap.xml.

Requis pour l'utilisation du modèle de mise à l'échelle automatique VM-Series dans un environnement de production.

Le fichier bootstrap.xml dans le référentiel GitHub est fourni uniquement pour les tests et l'évaluation. Pour un déploiement de production, vous devez personnaliser le fichier Bootstrap.xml (v2.0) avant le lancement.

STEP 5 | Préparez les compartiments Amazon Simple Storage (S3) pour lancer le modèle de mise à l'échelle automatique VM-Series dans un environnement de production.

Assurez-vous de créer les compartiments S3 dans la même région que celle dans laquelle vous prévoyez de déployer le modèle. Les fichiers d'amorçage hébergés dans le compartiment public S3 sont fournis uniquement pour vous faciliter l'évaluation du modèle.

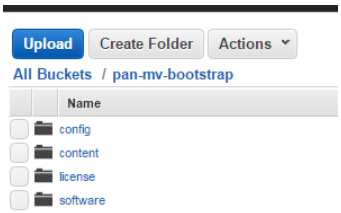
1. Créez un nouveau compartiment S3 pour les fichiers d'amorçage.
   1. Connectez-vous à la console de gestion AWS et sélectionnez la console S3.
   2. Cliquez sur **Create Bucket (Créer un compartiment)**.
   3. Saisissez un **Bucket Name (Nom de compartiment)** et une **Region (Région)** puis cliquez sur **Create (Créer)**. Le compartiment doit être au niveau racine S3. Si vous imbriquez le

©2023 Palo Alto Networks, Inc.

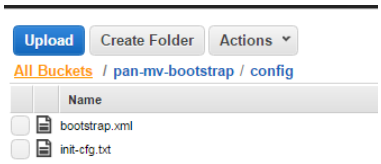
compartiment, l'amorçage échoue car vous ne pouvez pas spécifier de chemin d'accès à l'emplacement des fichiers d'amorçage.

2. Chargez les fichiers d'amorçage dans le compartiment S3. Les dossiers d'amorçage doivent être dans le dossier racine du compartiment S3.

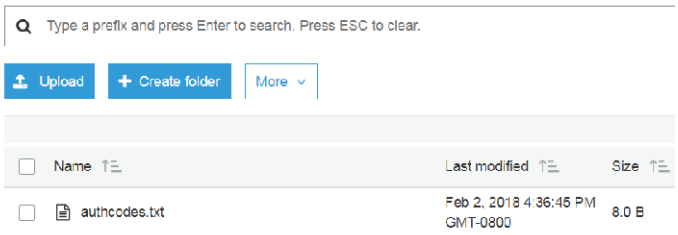
   1. Cliquez sur le nom du compartiment, puis sur **Create folder (Créer un dossier)**.
   2. Créez la structure de dossier suivante pour l'amorçage.



   3. Cliquez sur le lien pour ouvrir le dossier **config**.
   4. Sélectionnez **Actions** > **Upload (Charger)** et **Add Files (Ajouter des fichiers)**, recherchez le fichier init-cfg.txt et le fichier bootstrap.xml, puis cliquez sur **Open (Ouvrir)**.
   5. Cliquez sur **Start Upload (Commencer le chargement)** pour ajouter les fichiers au dossier config. Le dossier ne peut contenir que deux fichiers : init-cfg.txt et bootstrap.xml.



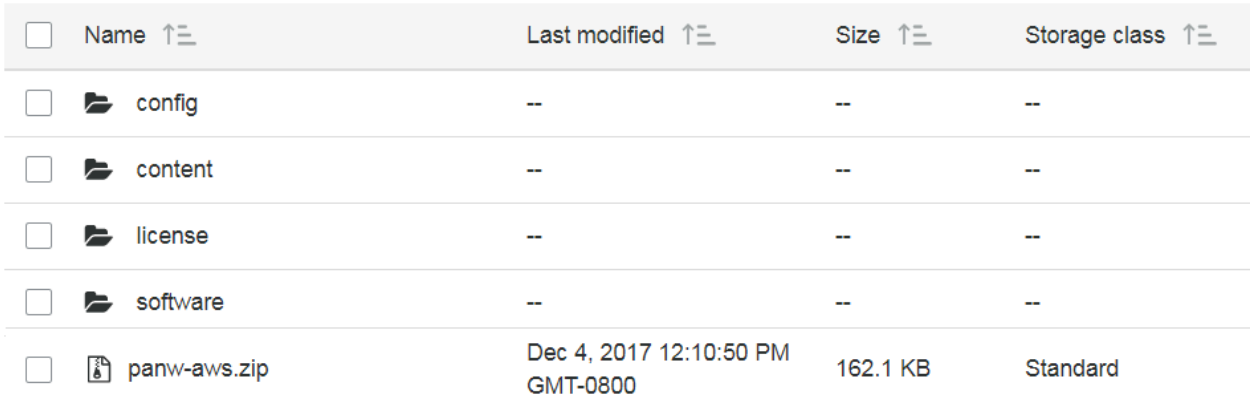
   6. (Pour BYOL uniquement) Cliquez sur le lien pour ouvrir le dossier **license** et chargez le fichier txt avec le code d'autorisation requis pour la mise sous licence des pare-feu VM-Series.



3. Chargez le code AWS Lambda (fichier panw-aws.zip) dans un compartiment S3. Dans cet exemple, le code AWS Lambda se trouve dans le même compartiment S3 que l'ensemble d'amorçage.

   1. Cliquez sur le nom du compartiment.
   2. Cliquez sur **Add Files (Ajouter des fichiers)** pour sélectionner le fichier panw-aws.zip, puis cliquez sur **Open (Ouvrir)**.
   3. Cliquez sur **Start Upload (Commencer le chargement)** pour ajouter le fichier zip au compartiment S3.

©2023 Palo Alto Networks, Inc.



Name	Last modified	Size	Storage class
config	--	--	--
content	--	--	--
license	--	--	--
software	--	--	--
panw-aws.zip	Dec 4, 2017 12:10:50 PM GMT-0800	162.1 KB	Standard

STEP 6 | Sélectionnez l'interface de pare-feu.

Si vous devez personnaliser le modèle de pare-feu avant le lancement (v2.0), faites-le maintenant et sélectionnez le modèle modifié.

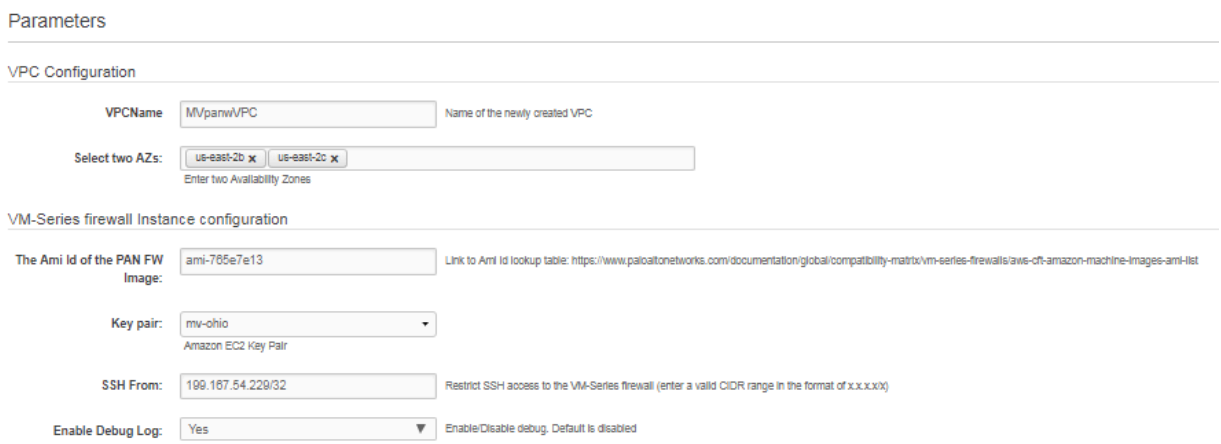
1. Dans la console de gestion AWS, sélectionnez **CloudFormation** > **Create Stack (Créer une pile)**.
2. Sélectionnez **Upload a template to Amazon S3 (Charger un modèle sur Amazon S3)**, choisissez le firewall-v2.0.template, puis cliquez sur **Open (Ouvrir)** et **Next (Suivant)**.
3. Spécifiez le **Stack name (Nom de la pile)**. Le nom de la pile vous permet d'identifier de manière unique toutes les ressources déployées par ce modèle.

STEP 7 | Configurez les paramètres pour le VPC.

1. Entrez les paramètres pour la **VPC Configuration (Configuration VPC)** comme suit :
   1. Saisissez un **VPCName** (Nom de VPC).
   2. Sélectionnez les deux zones de disponibilité incluses dans votre installation dans **Select two AZs (Sélectionner deux AZ)**.

©2023 Palo Alto Networks, Inc.

STEP 8 | Sélectionnez vos préférences pour le pare-feu VM-Series.

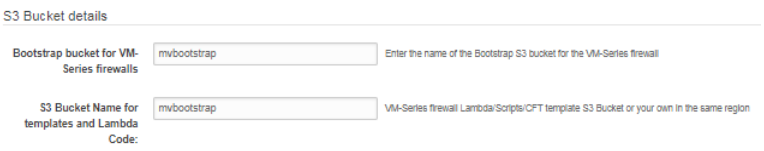


1. Recherchez l'ID AMI pour le pare-feu VM-Series et entrez-le. Assurez-vous que l'ID AMI correspond à la région AWS, à la version de PAN-OS et à l'option de licence BYOL ou PAYG que vous avez choisi d'utiliser.
2. Sélectionnez la **Key pair (Paire de clés)** de l'EC2 (à partir de la liste déroulante) pour lancer le pare-feu. Pour vous connecter aux pare-feu, vous devez fournir le nom de cette paire de clés et la clé privée qui lui est associée.
3. Limitez l'accès SSH à l'interface de gestion du pare-feu. Assurez-vous de fournir un bloc CIDR qui correspond à votre réseau ou vos adresses IP de gestion dédiées. Ne définissez pas une plage de réseau source autorisée plus grande que nécessaire et ne configurez jamais la source autorisée comme 0.0.0.0/0. Vérifiez votre adresse IP avant de la configurer sur le modèle pour vous assurer de ne pas rester bloqué.
4. Sélectionnez **Yes (Oui)** si vous souhaitez **Enable Debug Log (Activer le journal de débogage)**. L'activation du journal de débogage génère des journaux plus détaillés qui aident à résoudre les problèmes liés au déploiement. Ces journaux sont générés à l'aide du nom de la pile et sont enregistrés dans AWS CloudWatch.

Par défaut, le modèle utilise l'utilisation du processeur comme paramètre de mise à l'échelle pour les pare-feu VM-Series. Les métriques PAN-OS personnalisées sont automatiquement publiées dans l'espace de noms CloudWatch qui correspond au nom de la pile que vous avez spécifié précédemment.

STEP 9 | Indiquez le nom du ou des compartiments Amazon S3.

Vous pouvez utiliser un compartiment S3 pour l'ensemble d'amorçage et le fichier zip.



1. Entrez le nom du compartiment S3 qui contient l'ensemble d'amorçage.

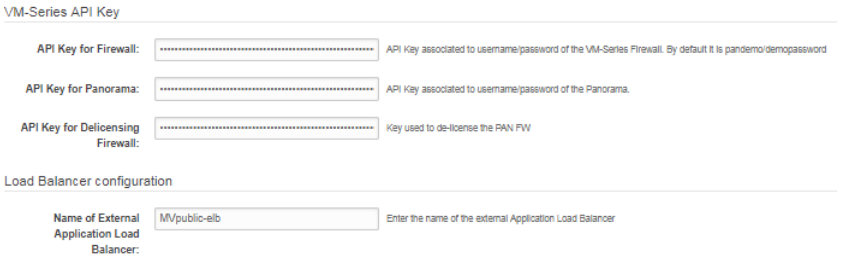
   Si le compartiment d'amorçage n'est pas configuré correctement ou si vous entrez un nom de compartiment incorrect, le processus d'amorçage échoue et vous ne pouvez pas vous

 ©2023 Palo Alto Networks, Inc.

connecter au pare-feu. Les vérifications de l'état pour les équilibreurs de charge échouent également.

2. Saisissez le nom du S3 bucket (Compartiment S3) qui contient le fichier panw-aws.zip.

STEP 10 | Spécifiez les clés permettant d'activer l'accès API au pare-feu et à Panorama.



1. Entrez la clé que le pare-feu doit utiliser pour authentifier les appels d'API. La clé par défaut est basée sur l'exemple de fichier bootstrap.xml et ne doit être utilisée que pour les tests et l'évaluation. Pour un déploiement de production, vous devez créer une connexion PAN-OS distincte uniquement pour l'appel d'API et générer une clé associée.
2. Entrez la clé API pour permettre à AWS Lambda de passer des appels d'API à Panorama, si vous utilisez Panorama pour la gestion centralisée. Pour un déploiement de production, vous devez créer une connexion distincte uniquement pour l'appel d'API et générer une clé associée.
3. Copiez et collez la clé API de désactivation de licence pour votre compte. Cette clé est requise pour correctement désactiver les licences sur vos pare-feu lorsqu'un événement de mise à l'échelle se produit. Pour obtenir cette clé :
   1. Ouvrez une session dans le portail de support client.
   2. Sélectionnez **Assets (Ressources)** > **API Key Management (Gestion des clés API)**.
   3. Copiez la clé API.

STEP 11 | Entrez le nom de l'équilibreur de charge de l'application.

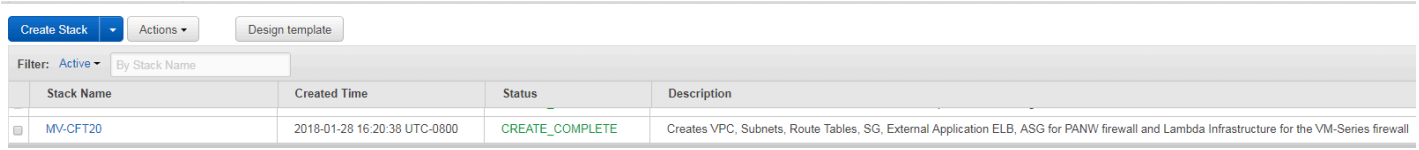
STEP 12 | (Facultatif) Appliquez des étiquettes pour identifier les ressources associées au modèle de mise à l'échelle automatique VM-Series.

Ajoutez une paire nom-valeur pour identifier et classer les ressources dans cette pile.

 ©2023 Palo Alto Networks, Inc.

STEP 13 | Passez en revue les paramètres du modèle et lancez le modèle.

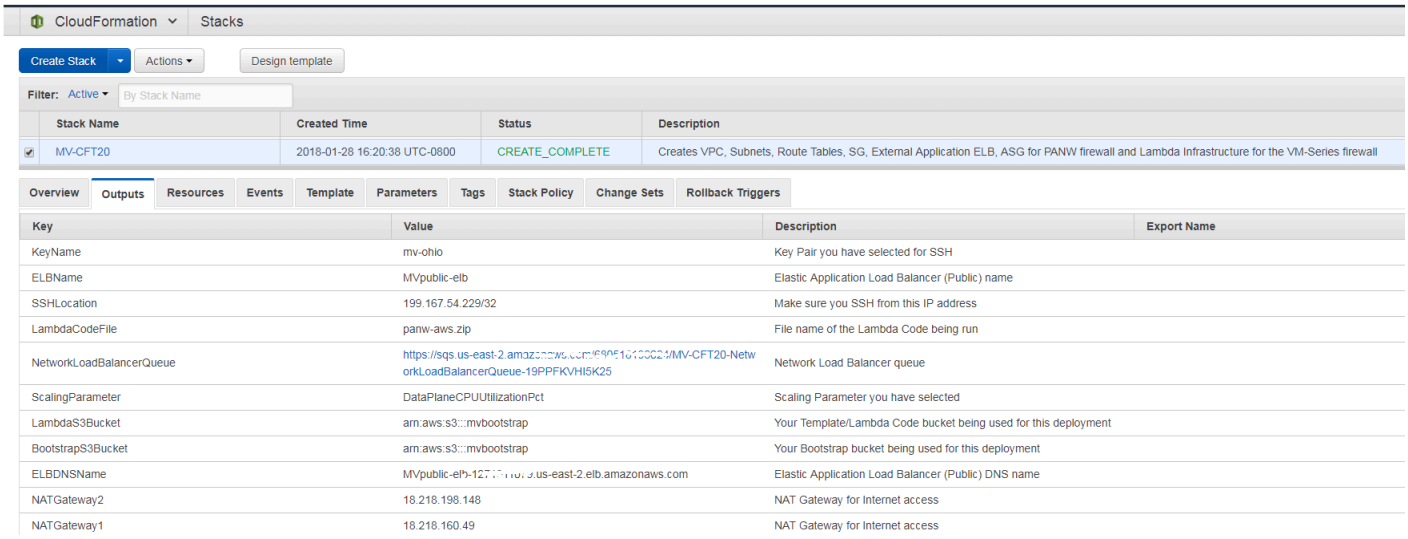
1. Sélectionnez **I acknowledge that this template might cause AWS CloudFormation to create IAM resources (Je reconnais que ce modèle peut entraîner la création de ressources IAM par AWS CloudFormation)**.
2. Cliquez sur **Create (Créer)** pour lancer le modèle. L'événement CREATE_IN_PROGRESS s'affiche.
3. En cas de déploiement réussi, le statut est mis à jour et passe à CREATE_COMPLETE.



À moins que vous ne personnalisiez le modèle, le modèle de mise à l'échelle automatique VM-Series lance un ASG qui inclut un pare-feu VM-Series dans chaque AZ, derrière l'équilibreur de charge de l'application.

STEP 14 | Vérifiez que le modèle a lancé toutes les ressources requises.

1. Sur la console de gestion AWS, sélectionnez le nom de la pile pour afficher l'**Output (Sortie)** pour la liste des ressources.



2. Sur le tableau de bord EC2, sélectionnez **Auto Scaling Groups (Groupes de mise à l'échelle automatique)**. Vérifiez que dans chaque AZ, vous avez un ASG pour les pare-feu

 ©2023 Palo Alto Networks, Inc.

VM-Series avec un pare-feu dans chaque ASG. Le préfixe du nom de l'ASG inclut le nom de la pile.

3. Connectez-vous au pare-feu VM-Series. Vous devez déployer un serveur de saut ou utiliser Panorama pour accéder à l'interface Web du pare-feu.

- ***Cela peut prendre jusqu'à 20 minutes pour que les pare-feu démarrent et soient disponibles pour gérer le trafic.***
- ***Lorsque vous avez terminé les tests ou un déploiement de production, la seule façon de garantir l'arrêt des charges consiste à supprimer complètement la pile. L'arrêt d'instances ou la modification du maximum d'ASG à 0 n'est pas suffisant.***

STEP 15 | Enregistrez les informations suivantes. Vous devez fournir ces valeurs en tant qu'entrées lors du déploiement du modèle d'application.

- Les adresses IP de la passerelle NAT dans chaque AZ. Vous avez besoin de cette adresse IP pour restreindre l'accès HTTP aux serveurs Web si vous déployez l'application dans un autre VPC. La spécification de cette adresse IP garantit que le pare-feu sécurise l'accès à vos applications dans un VPC différent et que personne ne peut contourner le pare-feu pour accéder directement au serveur Web. Le modèle d'application de l'échantillon (panw_aws_nlb_vpc-2.0.template) affiche une erreur de validation de modèle si vous ne saisissez pas les adresses IP de passerelle NAT; Vous devez entrer les adresses IP sous la forme d'une liste séparée par des virgules.
- URL SQS de l'équilibreur de charge réseau. Une fonction AWS Lambda dans la pile de pare-feu surveille cette file d'attente pour connaître les équilibreurs de charge de réseau que vous déployez et créer des règles de politique NAT (une par application) sur les pare-feu VM-Series permettant aux pare-feu d'envoyer du trafic à l'adresse IP de l'équilibreur de charge de réseau.

Lancement du modèle d'application

Le modèle d'application vous permet de compléter la topologie sandwich et est fourni afin que vous puissiez évaluer la solution de mise à l'échelle automatique. Ce modèle d'application déploie un équilibreur de charge réseau et une paire de serveurs Web derrière le groupe de mise à l'échelle automatique des pare-feu VM-Series, que vous avez déployé à l'aide du modèle de pare-feu. Les serveurs Web de ce modèle disposent d'une adresse IP publique pour un accès sortant direct afin de récupérer les mises à jour logicielles. Utilisez ce modèle pour évaluer la solution, mais créez votre propre modèle à déployer en production. Pour un modèle personnalisé, assurez-vous d'activer la messagerie SQS entre le modèle d'application et le modèle de pare-feu.

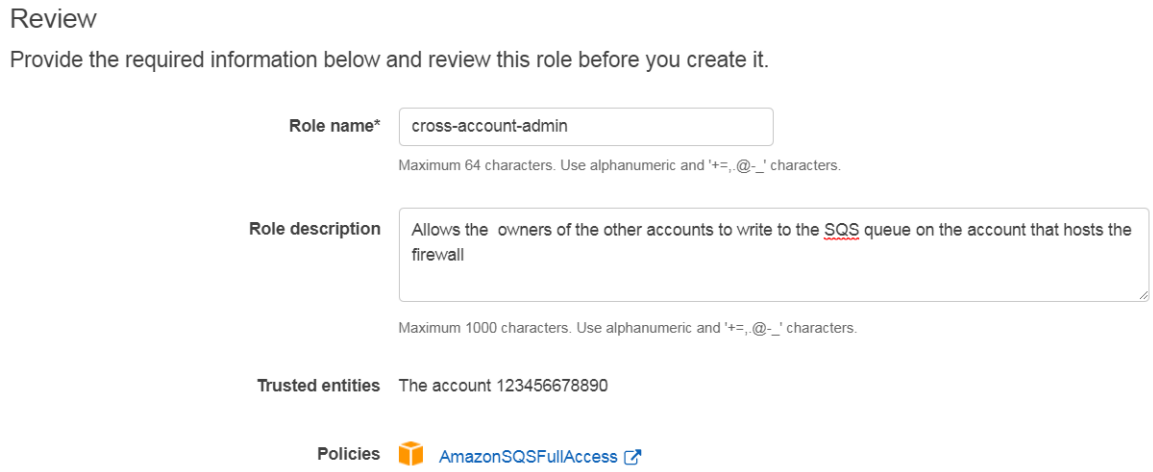
Lors du lancement du modèle d'application, vous devez sélectionner le modèle selon que vous souhaitez déployer le modèle d'application dans le même VPC (panw_aws_nlb-2.0.template) dans lequel vous avez déployé le modèle de pare-feu ou dans un VPC distinct (panw_aws_nlb_vpc-2.0.template). Pour un VPC distinct, le modèle fournit des prises en charge pour les déploiements entre comptes. Un déploiement entre comptes nécessite la création d'un rôle IAM et l'activation des autorisations et de la relation d'approbation entre le compte AWS d'approbation et le compte AWS approuvé, et les informations de compte sont requises en entrée lors du lancement du modèle.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | (Requis uniquement pour un déploiement entre comptes.) Créez le rôle IAM. Reportez-vous à la documentation d'AWS.

Ce rôle accorde l'accès à un utilisateur appartenant à un autre compte AWS. Cet utilisateur nécessite des autorisations pour accéder à la ressource SQS (Service de file d'attente simple) dans le modèle de pare-feu. Le pare-feu utilise cette file d'attente pour en savoir plus sur chaque équilibreur de charge réseau que vous déployez afin de pouvoir créer une politique NAT pour envoyer du trafic aux serveurs Web qui se trouvent derrière l'équilibreur de charge réseau.

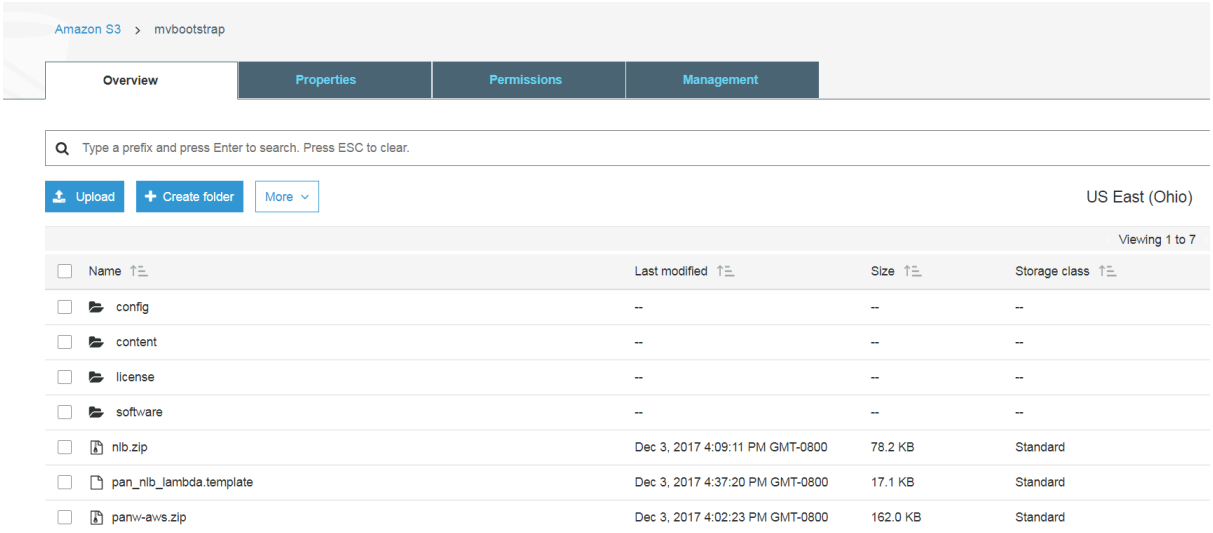
- Pour **Account ID (ID du compte)**, saisissez l'ID de compte AWS du compte dans lequel vous déployez le modèle d'application. La spécification de cet ID de compte vous permet d'accorder l'accès aux ressources de votre compte hébergeant les ressources du modèle de pare-feu.
- Sélectionnez **Require external ID (Exiger un ID externe)** et entrez une valeur qui est un secret partagé. La spécification d'un ID externe permet à l'utilisateur d'assumer le rôle uniquement si la requête contient la valeur correcte.
- Choisissez **Permissions (Autorisations)** pour autoriser l'**Amazon SQS Full Access (Accès complet à Amazon SQS)**.



 ©2023 Palo Alto Networks, Inc.

STEP 2 | Utilisez le compartiment public S3 de Palo Alto Networks ou préparez votre compartiment privé (S3) pour lancer le modèle d'application.

1. Créer un fichier zip avec tous les fichiers dans le référentiel GitHub, à l'exception des trois fichiers .template, nommés nlb.zip dans la capture d'écran ci-dessous.
2. Téléchargez le fichier zip dans le compartiment S3 que vous avez créé précédemment ou dans un nouveau compartiment.



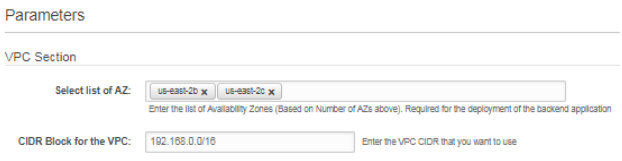
3. Copiez le modèle pan_nlb_lambda dans le même compartiment que celui dans lequel vous avez copié le fichier nlb.zip.

STEP 3 | Sélectionnez le modèle d'application à lancer.

1. Dans la console de gestion AWS, sélectionnez **CloudFormation** > **Create Stack (Créer une pile)**.
2. Sélectionnez **Upload a template to Amazon S3 (Charger un modèle sur Amazon S3)** pour choisir le module panw_aws_nlb-2.0.template afin de déployer les ressources que le modèle lance dans le même VPC que les pare-feu, ou le module panw_aws_nlb_vpc-2.0.template pour déployer les ressources dans un VPC différent. Cliquez sur **Open (Ouvrir)** et **Next (Suivant)**.
3. Spécifiez le **Stack name (Nom de la pile)**. Le nom de la pile vous permet d'identifier de manière unique toutes les ressources déployées à l'aide de ce modèle.

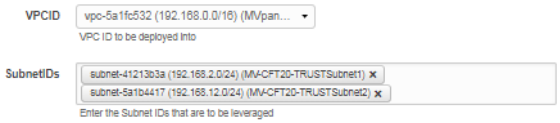
STEP 4 | Configurez les paramètres pour le VPC et l'équilibreur de charge réseau.

1. Sélectionnez les deux Availability Zones (Zones de disponibilité) que votre configuration va couvrir dans **Select list of AZ** (Sélectionner une liste d'AZ). Si vous effectuez un déploiement dans le même VPC, veillez à sélectionner les mêmes Availability Zones (Zones de disponibilité) que celles que vous avez sélectionnées pour le modèle de pare-feu.
2. Entrez un **CIDR Block for the VPC (Bloc CIDR pour le VPC)**. Le CIDR par défaut est 192.168.0.0/16.



 ©2023 Palo Alto Networks, Inc.

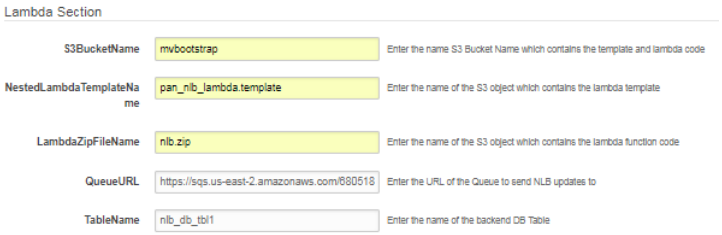
3. (Uniquement si vous utilisez panw_aws_nlb-2.0.template pour déployer les applications dans le même VPC.)



   Sélectionnez le **VPC ID (ID VPC)** et les **Subnet IDs (ID de sous-réseau)** associés au sous-réseau approuvé sur les pare-feu dans chaque AZ. L'équilibreur de charge réseau est associé au sous-réseau approuvé sur les pare-feu, afin de compléter la topologie sandwich de l'équilibreur de charge.

4. Entrez un nom pour l'équilibreur de charge réseau.

STEP 5 | Configurez les paramètres pour AWS Lambda.



1. Entrez le nom du compartiment S3 où sont stockés nlb.zip et pan_nlb_lambda.template.
2. Saisissez le nom du fichier pan_nlb_lambda.template et le nom du fichier zip.
3. Collez l'URL SQS que vous avez copiée précédemment.
4. Entrez un **TableName (Nom de la table)** unique. Cette table stocke un mappage du port et de l'adresse IP pour les applications associées à l'équilibreur de charge réseau dans votre déploiement.

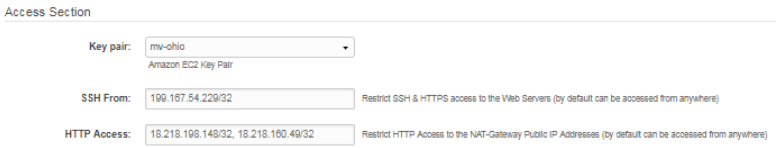
   Lorsque vous supprimez la pile d'applications, cette table est supprimée. Par conséquent, si plusieurs instances de l'équilibreur de charge réseau écrivent dans la même table et que la table est supprimée, les règles NAT sur les pare-feu ne fonctionnent pas correctement et le trafic d'application peut être transféré de manière incorrecte vers le mauvais équilibreur de charge réseau/port.

STEP 6 | Modifiez le type d'instance EC2 du serveur Web pour répondre à vos besoins de déploiement.

STEP 7 | Sélectionnez la **Paire de clés** de l'EC2 (à partir de la liste déroulante) pour lancer les serveurs Web. Pour vous connecter aux serveurs Web, vous devez fournir le nom de la paire de clés et la clé privée associée.

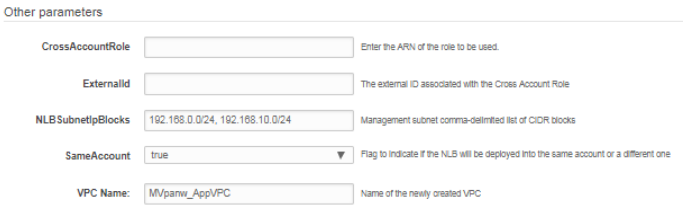
©2023 Palo Alto Networks, Inc.

STEP 8 | (Uniquement si vous utilisez panw_aws_nlb_vpc-2.0.template.) Verrouillez l'accès aux serveurs Web.



1. Limitez l'accès **SSH From (SSH depuis)** aux serveurs Web. Seules les adresses IP répertoriées ici peuvent se connecter aux serveurs Web.
2. Limitez l'accès HTTP aux serveurs Web. Saisissiez les adresses IP publiques de la passerelle NAT à partir de la sortie du modèle de pare-feu et assurez-vous de séparer les adresses IP par des virgules. La saisie de l'adresse IP de la passerelle NAT vous permet de garantir que l'ensemble du trafic Web vers les serveurs d'applications est sécurisé par les pare-feu VM-Series.

STEP 9 | (Uniquement si vous utilisez panw_aws_nlb_vpc-2.0.template.) Configurez les autres paramètres pour lancer la pile de modèles d'application dans un VPC différent.



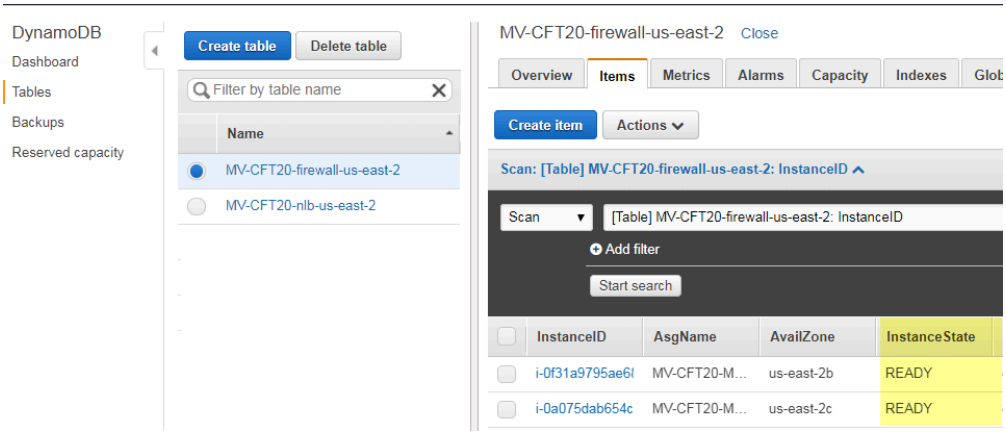
1. Sélectionnez **true (vrai)** pour SameAccount (Même compte) si vous déployez ce modèle d'application dans le même compte AWS que le modèle de pare-feu et laissez le rôle entre comptes et l'ID externe vides ; sélectionnez **false (faux)** pour un déploiement entre comptes.

   Pour un déploiement entre comptes, entrez le numéro de ressource Amazon (ARN) pour le **CrossAccountRole (Rôle entre comptes)** et **ExternalId (ID externe)** que vous avez défini à l'étape (Requis uniquement pour un déploiement entre comptes.) Créez le rôle IAM. Reportez-vous à la documentation d'AWS.Vous pouvez obtenir l'ARN depuis **Soutien** > **Support Center (Centre de support)** sur la console de gestion AWS.
2. Entrer le **VPC Name (Nom du VPC)** dans lequel vous souhaitez déployer les ressources du modèle d'application.
3. Facultatif Changer les **NLBSubnetIPBlocks (Blocs IP de sous-réseau NLB)** pour le sous-réseau de gestion de l'équilibreur de charge réseau.

STEP 10 | Passez en revue les paramètres du modèle et lancez le modèle.

©2023 Palo Alto Networks, Inc.

STEP 11 | Vérifiez que l'équilibreur de charge réseau est déployé et dans un état prêt.



STEP 12 | Obtenez le **DNS name (Nom de DNS)** pour l'équilibreur de charge de l'application, et entrez-le dans un navigateur Web.

Par exemple : http://MVpublic-elb-123456789.us-east-2.elb.amazonaws.com/

Lorsque la page Web s'affiche, vous avez lancé avec succès le modèle de mise à l'échelle automatique.

STEP 13 | Vérifiez que chaque pare-feu possède une règle de politique NAT pour l'adresse IP de chaque équilibreur de charge réseau.

Lorsque vous déployez le modèle d'application pour lancer une autre instance d'un équilibreur de charge réseau et d'une paire de serveurs Web, le pare-feu prend connaissance du port attribué à l'instance d'équilibreur de charge réseau suivante et crée une autre règle de politique NAT. Ainsi, si vous déployez le modèle d'application trois fois, le pare-feu dispose de trois règles de politique NAT pour les ports 81, 82 et 83.



STEP 14 | Si vous avez lancé le modèle d'application plusieurs fois, vous devez activer le trafic vers le service ELB.

Activation du trafic vers le service ELB (v2.0 et v2.1)

Si vous ajoutez un deuxième équilibreur de charge interne (ILB) ou un équilibreur de charge supplémentaire dans votre déploiement, vous devez effectuer une configuration supplémentaire pour que l'équilibreur de charge interne, les groupes de mise à l'échelle automatique des pare-feu VM-Series et les serveurs Web soient en bon état et que le trafic soit équilibré en charge entre toutes vos ressources AWS.

Dans v2.0, ILB ne peut être qu'un équilibreur de charge de réseau. Dans v2.1, l'ILB peut être un équilibreur de charge d'application ou un équilibreur de charge de réseau.

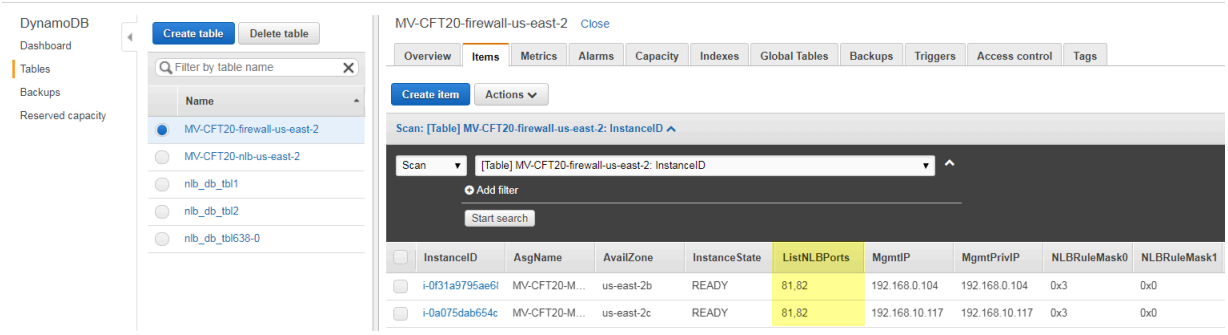
©2023 Palo Alto Networks, Inc.

STEP 1 | Sur la console de gestion AWS, vérifiez les ports alloués pour chaque équilibreur de réseau sur la table DynamoDB.

Lorsque vous lancez un nouvel équilibreur de charge interne, le modèle d'application doit envoyer un message SQS à l'URL SQS que vous avez fournie en tant qu'entrée lorsque vous avez lancé le modèle. La fonction AWS Lambda du modèle de pare-feu surveille le SQS et ajoute le mappage de port à la table DynamoDB pour le modèle de pare-feu. À partir du port 81, le port attribué pour chaque équilibreur de charge interne supplémentaire déployé augmente de 1. Ainsi, le deuxième équilibreur de charge interne utilise le port 82 et le troisième port utilise le port 83.

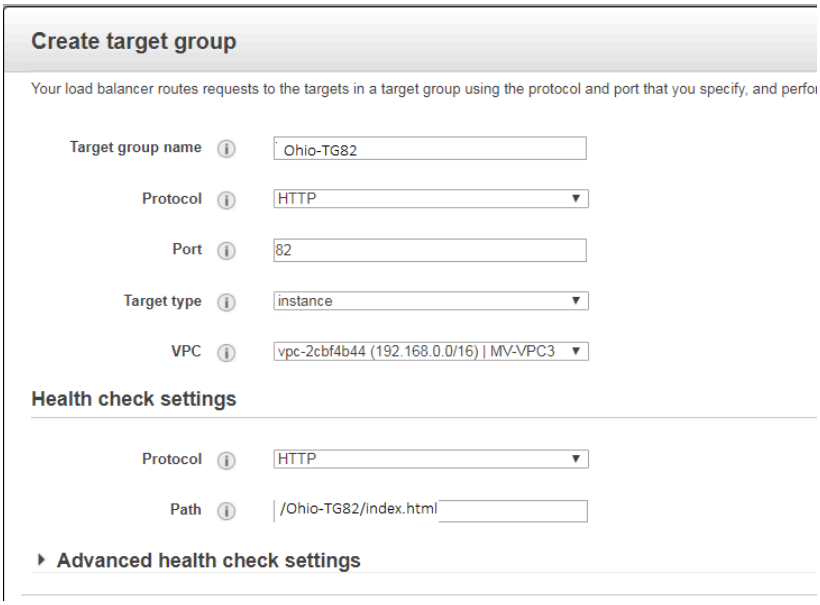
1. Sélectionnez le service **DynamoDB** sur la console de gestion AWS.
2. Sélectionnez **Tables** et cliquez sur la table correspondant au nom de la pile pour votre modèle de pare-feu. Par exemple, MV-CFT20-firewall-us-east-2.

   Dans la liste Items (Éléments), affichez les ports utilisés par les équilibreurs de charge internes qui publient sur le SQS associé au modèle de pare-feu.



STEP 2 | Créez un groupe cible. L'équilibreur de charge interne envoie des requêtes aux cibles enregistrées à l'aide du port et du protocole que vous spécifiez pour les serveurs du groupe cible.

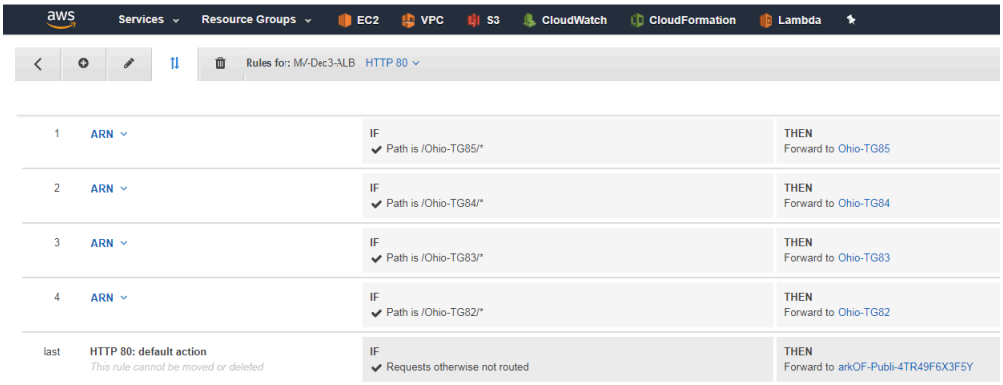
Lorsque vous ajoutez un nouveau groupe cible, utilisez les informations sur le port que vous avez vérifiées dans la table DynamoDB.



 ©2023 Palo Alto Networks, Inc.

STEP 3 | Procédez à la Modification des règles de l'écouteur sur l'équilibreur de charge interne pour acheminer les requêtes vers les serveurs Web cibles.

1. Sur la console de gestion AWS, sélectionnez **Load Balancers** (Équilibreurs de charge) dans la section Load Balancing (Équilibrage de charge), puis l'équilibreur de charge interne correspondant au nom de la pile.
2. Sélectionnez **View/edit rules (Afficher/modifier les règles)** pour modifier les règles de l'écouteur.
3. Sélectionnez **Insert rule (Insérer une règle)** et ajoutez une route basée sur l'itinéraire pour transférer le trafic vers le groupe cible que vous avez défini ci-dessus comme suit :



STEP 4 | Associez le groupe cible aux deux groupes de mise à l'échelle automatique des pare-feu VM-Series.

1. Sélectionnez **Auto Scaling Groups (Groupes de mise à l'échelle automatique)** dans la section Auto Scaling (Mise à l'échelle) et sélectionnez un groupe de mise à l'échelle automatique correspondant au nom de la pile.
2. Sélectionnez **Details (Détails)** > **Edit (Modifier)** et le nouveau groupe cible depuis le menu déroulant **Target Groups (Groupes cibles)**.



STEP 5 | Connectez-vous à chaque serveur Web déployé par le modèle d'application, créez un nouveau répertoire avec le nom du groupe cible et copiez le fichier index.html dans le répertoire. Tant

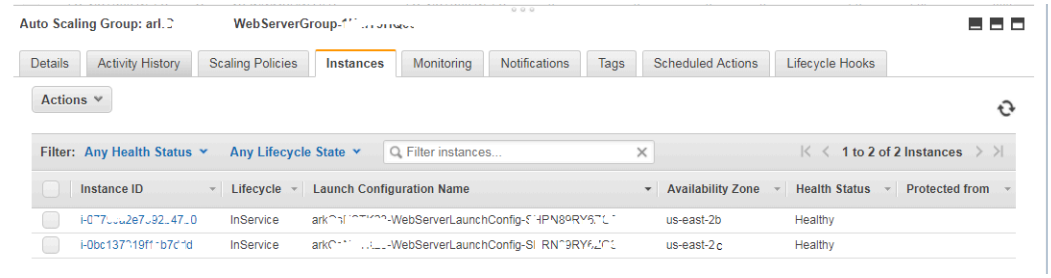
 ©2023 Palo Alto Networks, Inc.

que vous n'avez pas configuré le chemin d'accès au fichier index.html, le bilan de santé de ce serveur Web est incorrect.

```
sudo su
cd/var/www/html
mkdir <target-groupname>
cp index.html <target-groupname>
```

STEP 6 | Vérifiez l'état de santé des serveurs Web.

Sélectionnez **Auto Scaling Groups (Groupes de mise à l'échelle automatique)** et utilisez le nom de la pile d'application pour trouver le groupe de mise à l'échelle automatique du serveur Web afin de vérifier que les serveurs Web génèrent des rapports sains.



Personnalisation du fichier bootstrap.xml (v2.0)

Le fichier bootstrap.xml fourni dans le référentiel GitHub utilise un nom d'utilisateur et un mot de passe par défaut pour l'administrateur du pare-feu. Avant de déployer le modèle Auto Scaling VM-Series dans un environnement de production, vous devez au minimum créer un nom d'utilisateur et un mot de passe uniques pour le compte administrateur sur le pare-feu VM-Series. Éventuellement, vous pouvez entièrement configurer le pare-feu avec des zones, des règles de politique, des profils de sécurité et exporter un instantané de configuration principale. Vous pouvez ensuite utiliser cet instantané de configuration en tant que fichier bootstrap.xml pour votre environnement de production.

Vous avez deux façons de personnaliser le fichier bootstrap.xml pour une utilisation dans un environnement de production :

- **Option 1** : lancez un pare-feu VM-Series sur AWS à l'aide des fichiers d'amorçage fournis dans le référentiel GitHub, modifiez la configuration du pare-feu et exportez la configuration pour créer un nouveau fichier bootstrap.xml pour le modèle de mise à l'échelle automatique VM-Series. Reportez-vous à la section Utilisation des fichiers d'amorçage GitHub en tant que valeurs initiales.
- **Option 2** : lancez un nouveau pare-feu VM-Series sur AWS sans utiliser les fichiers d'amorçage, ajoutez une règle de politique NAT pour garantir que le pare-feu VM-Series traite correctement le trafic et exportez la configuration pour créer un nouveau fichier bootstrap.xml pour le modèle de mise à l'échelle automatique de VM-Series. Reportez-vous à la section Création d'un nouveau fichier Bootstrap à partir de rien.

Si vous avez déployé le modèle et devez maintenant modifier les informations d'identification de l'utilisateur administratif ou ajouter un nouvel utilisateur administratif et mettre à jour la pile de modèles, reportez-vous à la section Modification du compte administrateur et mise à jour de la pile.

©2023 Palo Alto Networks, Inc.

Création d'un nouveau fichier Bootstrap à partir de rien

Lancez un nouveau pare-feu VM-Series sur AWS à l'aide de l'AMI pour une version PAN-OS prise en charge (voir la matrice de compatibilité pour les plug-ins Panorama), sans utiliser le fichier bootstrap.xml et exportez la configuration pour créer un nouveau fichier bootstrap.xml à utiliser avec la machine virtuelle, modèle de mise à l'échelle (Auto Scaling) 2.0.

STEP 1 | Déployez le pare-feu VM-Series sur AWS (aucun amorçage requis) et utilisez l'adresse IP publique vers SSH dans l'interface de ligne de commande (CLI) du pare-feu VM-Series. Vous devrez configurer un nouveau mot de passe administratif pour le pare-feu.

STEP 2 | Connectez-vous à l'interface Web du pare-feu.

STEP 3 | (Facultatif) Configurez le pare-feu. Vous pouvez configurer les interfaces du dataplane, les zones et les règles de politique.

STEP 4 | Cliquez sur **Commit (Valider)** pour valider les modifications apportées au pare-feu.

STEP 5 | Exportez le fichier de configuration et nommez-le **`bootstrap.xml`**. (**Device (Appareil)** > **Setup (Configuration)** > **Operation (Opération)** > **Export named configuration snapshot (Exporter l'instantané de configuration nommé)**).

STEP 6 | Téléchargez le fichier bootstrap.xml à partir du référentiel GitHub, ouvrez-le avec un outil d'édition de texte et copiez les lignes 353 à 356. Ces lignes définissent l'espace de noms AWS CloudWatch dans lequel le pare-feu publie les métriques PAN-OS personnalisées requises pour que la mise à l'échelle automatique des pare-feu.

STEP 7 | Modifiez le fichier de configuration que vous avez exporté précédemment pour inclure les informations AWS CloudWatch.

Recherchez **`</management>`** et collez les lignes 353 à 356 après **`</management>`**.

```
352         </management>
353         <aws-cloudwatch>
354           <enabled>yes</enabled>
355           <name>autoscale-default-panw-asg-name</name>
356         </aws-cloudwatch>
357       </setting>
```


©2023 Palo Alto Networks, Inc.

STEP 8 | Supprimez la configuration de l'interface de gestion.

1. Recherchez **</service>** et supprimez l'adresse IP, le masque réseau et la passerelle par défaut qui suivent.
2. Recherchez **</type>** et supprimez l'adresse IP, le masque réseau, la passerelle par défaut et la clé publique qui suivent.

```
      </service>
      <ip-address>192.168.10.16</ip-address>
      <netmask>255.255.255.0</netmask>
      <default-gateway>192.168.10.1</default-gateway>
      <hostname>PA-VM</hostname>
    </system>
    <setting>
      <config>
        <rematch>yes</rematch>
      </config>
      <management>
        <hostname-type-in-syslog>FQDN</hostname-type-in-syslog>
        <initcfg>
          <type>
            <dhcp-client>
              <send-hostname>yes</send-hostname>
              <send-client-id>no</send-client-id>
              <accept-dhcp-hostname>no</accept-dhcp-hostname>
              <accept-dhcp-domain>no</accept-dhcp-domain>
            </dhcp-client>
          </type>
          <ip-address>192.168.10.16</ip-address>
          <netmask>255.255.255.0</netmask>
          <default-gateway>192.168.10.1</default-gateway>
          <public-key>c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCQVFDQTRCSjJwZFBSZlh0TjF2SDVqWW5GRUdYTVdvTmZlaU1FcCtBSlZRaVU4c2hEMHBmSUtOVTVSeHdGRFd4OVZZckRRRFVrLzQ5VDdkeThXcXorcXZ1em44dlFpamY1RDI
          VEeHB2WXk3ZWtiam1IallYdTVXUFR4MnZSaXdiMmVzcS91K3FXbm9hSlQ1cXdjU2srbHRxN0prVjlGcC9HSy9jQkRDT0FqOVhmSHMvWi8xQ0VZRk9uZ0UrNTd5L2VwSjFFWWtxZXlLczZuRTBvbWxRajBHSmNhb1FMcUlqZDZmQW5Dcm93dEZ4Y3c3YWVTF
        </initcfg>
      </management>
```

STEP 9 | Enregistrez le fichier. Vous pouvez maintenant poursuivre avec Lancement du modèle de mise à l'échelle automatique de VM-Series pour AWS (v2.0).

Utilisation des fichiers d'amorçage GitHub en tant que valeurs initiales

Lancez un pare-feu VM-Series sur AWS à partir d'AWS Marketplace à l'aide des fichiers d'amorçage fournis dans le référentiel GitHub. Modifiez la configuration du pare-feu pour votre environnement de production. Ensuite, exportez la configuration pour créer un nouveau fichier bootstrap.xml que vous pouvez maintenant utiliser pour le modèle de mise à l'échelle automatique VM-Series.

STEP 1 | Pour lancer le pare-feu, reportez-vous à la section Amorçage du pare-feu VM-Series sur AWS.

STEP 2 | Ajoutez une interface réseau élastique (ENI) et associez-lui une adresse IP élastique (EIP), de sorte que vous puissiez accéder à l'interface Web sur le pare-feu VM-Series. Reportez-vous à la section Lancement du pare-feu VM-Series sur AWS pour obtenir plus de détails.

STEP 3 | Utilisez l'adresse EIP pour vous connecter à l'interface Web du pare-feu avec admin comme nom d'utilisateur et mot de passe.

STEP 4 | Ajoutez un mot de passe sécurisé pour le compte d'administrateur (**Device (Périphérique)** > **Local User Database (Base de données utilisateur locale)** > **Users (Utilisateurs)**).

STEP 5 | (Facultatif) Configurez le pare-feu pour sécuriser votre environnement de production.

STEP 6 | Cliquez sur **Commit (Valider)** pour valider les modifications apportées au pare-feu.

STEP 7 | Générez une nouvelle clé API pour le compte administrateur. Copiez cette nouvelle clé dans un nouveau fichier. Vous devrez entrer cette clé API lorsque vous lancerez le modèle de mise à l'échelle automatique VM-Series. Les services AWS utilisent la clé API pour déployer le pare-feu et publier des métriques pour la mise à l'échelle automatique.

©2023 Palo Alto Networks, Inc.

STEP 8 | Exportez le fichier de configuration et sauvegardez le sous **`bootstrap.xml`**. (**Device (Appareil)** > **Setup (Configuration)** > **Operation (Opération)** > **Export named configuration snapshot (Exporter l'instantané de configuration nommé)**).

STEP 9 | Ouvrez le fichier bootstrap.xml avec un outil d'édition de texte et supprimez la configuration de l'interface de gestion.

```
        </service>
        <ip-address>192.168.10.16</ip-address>
        <netmask>255.255.255.0</netmask>
        <default-gateway>192.168.10.1</default-gateway>
        <hostname>PA-VM</hostname>
      </system>
      <setting>
        <config>
          <rematch>yes</rematch>
        </config>
        <management>
          <hostname-type-in-syslog>FQDN</hostname-type-in-syslog>
          <initcfg>
            <type>
              <dhcp-client>
                <send-hostname>yes</send-hostname>
                <send-client-id>no</send-client-id>
                <accept-dhcp-hostname>no</accept-dhcp-hostname>
                <accept-dhcp-domain>no</accept-dhcp-domain>
              </dhcp-client>
            </type>
            <ip-address>192.168.10.16</ip-address>
            <netmask>255.255.255.0</netmask>
            <default-gateway>192.168.10.1</default-gateway>
            <public-key>c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCQVFDQTRC5jJwZFBSZlh0TjF2SDVqWW5GRUdYTVdvTmZlaU1FcCtBSlZRaVU4c2hEMHBmSUtOVTVSeHdGRFd4OVZZckRRRFVrLzQ5VDdkeThXcXorcXZ1em44dlFpamY1RDJ4dldEaHFWQ3
            VEeHB2WXk3ZWtiam1IallYdTVXUFR4MnZSaXdiMmVzcS91K3FXbm9hSlQ1cXdjU2srbHRxN0prVjlGcC9HSy9jQkRDT0FqOVhmSHMvWi8xQ0VZRk9uZ0UrNTd5L2VwSjFFWWtxZXllczZuRTBvbWxRajBHSmNhb1FMcUlqZDZmQW5Dcm93dEZ4Y3c3YWVTRnhZdDdXUlFY
          </initcfg>
        </management>
```

STEP 10 | (Requis si vous avez exporté une configuration PAN-OS 8.0) Assurez-vous que le paramètre permettant de valider les serveurs Palo Alto Networks est désactivé. Recherchez **`<server-verification>no</server-verification>.`**

STEP 11 | Si le contrôle est **`yes`**, changez-le pour **`no`**.

STEP 12 | Enregistrez le fichier. Vous pouvez maintenant poursuivre avec Lancement du modèle de mise à l'échelle automatique de VM-Series pour AWS (v2.0).

Messagerie SQS entre le modèle d'application et le modèle de pare-feu

Pour que les pare-feu VM-Series déployés à l'aide de firewall-v2.0.template puissent détecter et envoyer du trafic vers les équilibreurs de charge réseau auxquels vous souhaitez distribuer automatiquement le trafic entrant, le modèle de pare-feu inclut une fonction lambda qui surveille un service de file d'attente simple (SQS) pour les messages. Le message permet à la fonction lambda de se familiariser avec un nouvel équilibreur de charge réseau, puis de créer automatiquement une règle de politique NAT sur le pare-feu pour envoyer le trafic à l'adresse IP de l'équilibreur de charge réseau. Pour acheminer le trafic correctement dans l'infrastructure AWS, le message doit également inclure des informations de base sur le DNS, l'ID VPC et l'AZ à laquelle appartient l'équilibreur de charge réseau.

Si vous créez votre propre modèle d'application, vous devez configurer votre modèle d'application pour publier deux types de messages dans l'URL SQS que le modèle de pare-feu du modèle de mise à l'échelle automatique VM-Series version 2.0 utilise pour se familiariser avec les équilibreurs de charge réseau auxquels il doit répartir le trafic dans votre environnement :

- Message ADD-NLB qui informe les pare-feu lorsqu'un nouvel équilibreur de charge réseau est disponible.
- Message DEL-NLB qui informe les pare-feu lorsqu'un équilibreur de charge réseau a été arrêté et n'est plus disponible.

©2023 Palo Alto Networks, Inc.

Les exemples suivants de chaque type de message incluent des exemples de valeurs. Vous devez modifier ce message avec des valeurs correspondant à votre déploiement.

Message ADD-NLB

```
msg_add_nlb= { 'MSG-TYPE': 'ADD-NLB', 'AVAIL-ZONES': [{'NLB-
IP':'192.168.2.101', 'ZONE-NAME':'us-east-2a', 'SUBNET-ID':
 'subnet-2a566243'}, {'NLB-IP':'192.168.12.101', 'ZONE-NAME':'us-
east-2b', 'SUBNET-ID': 'subnet-2a566243 '}], 'DNS-NAME':
 'publicelb1-2119989486.us-east-2.elb.amazonaws.com', 'VPC-ID':
 'vpc-42ba9f2b', 'NLB-NAME': 'publicelb1' }
```

DEL-NLB Message

```
msg_del_nlb= { 'MSG-TYPE': 'DEL-NLB', 'DNS-NAME':
 'publicelb1-2119989486.us-east-2.elb.amazonaws.com', }
```

Reportez-vous à la documentation d'AWS pour plus d'informations sur l'envoi d'un message à une file d'attente Amazon SQS, ou consultez **describe_nlb_dns.py** dans l'exemple de package de modèle d'application pour voir comment le modèle d'application construit les messages.

Mise à jour de la pile avec le modèle de mise à l'échelle automatique VM-Series pour AWS (v2.0)

Une mise à jour de la pile vous permet de modifier les ressources déployées par le modèle de mise à l'échelle automatique VM-Series (firewall-v2.0.template). Au lieu de supprimer votre déploiement existant et de redéployer la solution, utilisez la mise à jour de la pile pour modifier les paramètres suivants :

- Licence : passez de BYOL à PAYG et vice versa ou passez d'un forfait PAYG à un autre.
- Autres ressources de la pile : modifiez les paramètres de configuration du lancement, tels que l'ID AMI (Image de machine Amazon), le type d'instance AWS, ou la paire de clés pour vos groupes de mise à l'échelle automatique. Vous pouvez également mettre à jour la clé API associée au compte utilisateur administratif sur le pare-feu.



La modification de l'ID AMI vous permet de déployer de nouvelles instances des pare-feu VM-Series avec une version différente de PAN-OS.

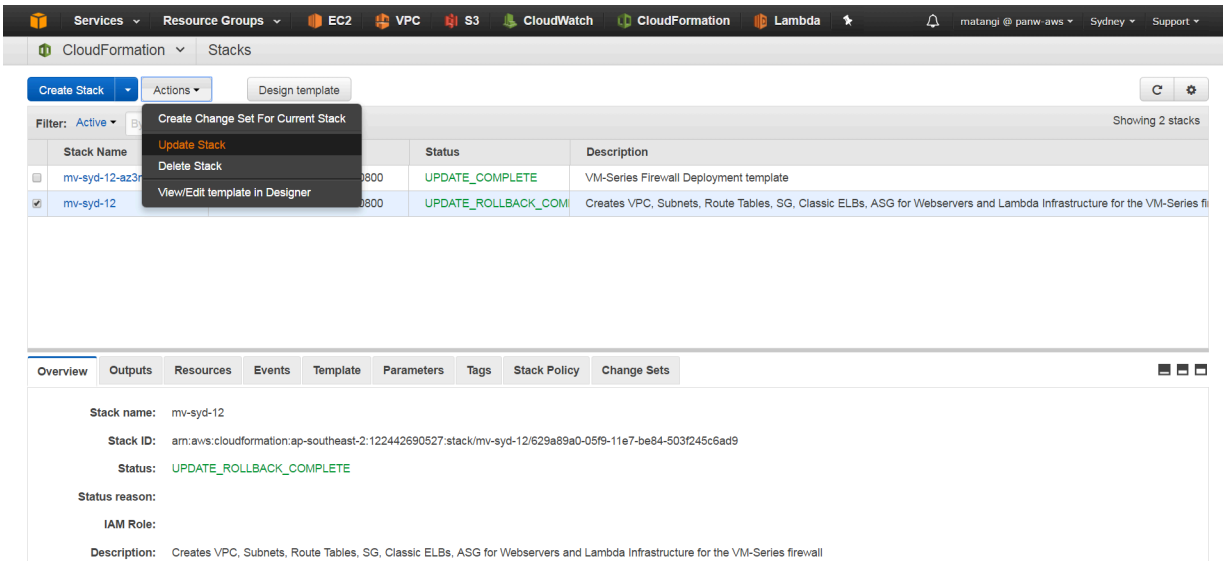
Lorsque vous déployez le modèle de mise à l'échelle automatique VM-Series, les groupes de mise à l'échelle automatique et la configuration de lancement sont automatiquement créés pour vous. La configuration de lancement est un modèle utilisé par un groupe de mise à l'échelle automatique pour lancer l'instance EC2. Elle spécifie des paramètres tels que l'ID AMI, le type d'instance et la paire de clés de votre groupe de mise à l'échelle automatique. Pour lancer les pare-feu VM-Series avec vos paramètres mis à jour, vous devez d'abord mettre à jour la pile, puis supprimer les groupes de mise à l'échelle automatique existants dans chaque AZ. Pour éviter toute interruption de service, supprimez d'abord le groupe de mise à l'échelle automatique dans un AZ et attendez le lancement des nouvelles instances de pare-feu avec les paramètres de pile mis à jour. Ensuite, vérifiez que les pare-feu ont hérité des mises à jour que vous avez effectuées avant de procéder aux modifications dans l'autre AZ.

©2023 Palo Alto Networks, Inc.

Pour les applications critiques, effectuez une mise à jour de la pile pendant une fenêtre de maintenance.

Vous pouvez mettre à jour la pile directement ou créer des ensembles de modifications. Le flux de travail dans ce document vous guide à travers la mise à jour manuelle de la pile.

STEP 1 | Dans la console AWS CloudFormation, sélectionnez la pile parente que vous souhaitez mettre à jour et choisissez **Actions** > **Update Stack (Mettre à jour la pile)**.



STEP 2 | Modifiez les ressources que vous souhaitez mettre à jour.

- Version de PAN-OS : pour modifier la version de PAN-OS, recherchez l'ID AMI pour la version que vous voulez utiliser et entrez l'ID.
- Option de licence : passez de BYOL à PAYG ou entre des forfaits PAYG 1 et 2.

Si vous passez à BYOL, assurez-vous d'inclure le code d'authentification dans l'ensemble d'amorçage (voir les étapes 3 et 5).

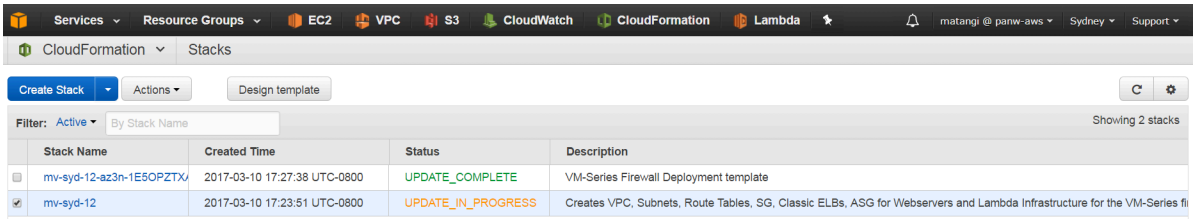
Si vous basculez entre les versions 1 et 2 du forfait PAYG, recherchez l'ID AMI pour le pare-feu VM-Series.

- Autres ressources de la pile : vous pouvez modifier l'ID de l'AMI, le type d'instance, le groupe de sécurité, la paire de clés pour les ressources de la pile ou la clé API associée au compte utilisateur administratif sur le pare-feu.

Si vous créez un nouveau compte administrateur ou modifiez les informations d'identification de l'administrateur existant sur le pare-feu, afin de mettre à jour cette pile et de déployer de nouveaux pare-feu avec la clé API mise à jour, vous devez suivre le flux de travail dans la section Modification du compte administrateur et mise à jour de la pile.

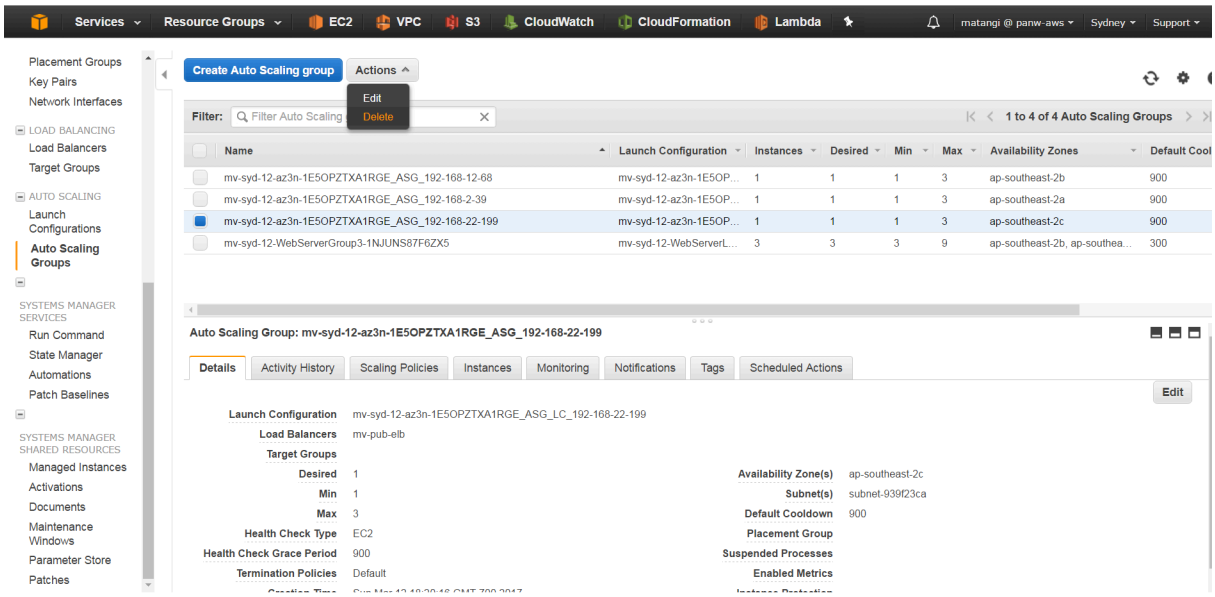
©2023 Palo Alto Networks, Inc.

STEP 3 | Acceptez les notifications et passez en revue les modifications, puis cliquez sur **Update (Mettre à jour)** pour lancer la mise à jour de la pile.



STEP 4 | Sur l'**EC2 dashboard (Tableau de bord EC2)** > **Auto Scaling Groups (Groupes de mise à l'échelle automatique)**, choisissez une AZ dans laquelle supprimer l'ASG.

La suppression d'un ASG déclenche automatiquement le processus de redéploiement d'un nouvel ASG. Les pare-feu du nouvel ASG utilisent la configuration de la pile mise à jour.



STEP 5 | Vérifiez que les paramètres mis à jour sont utilisés pour lancer les pare-feu VM-Series dans le nouvel ASG.

Utilisez un processus de lancement progressif, où vous testez le nouvel ASG en profondeur et vous vous assurez que les pare-feu gèrent correctement le trafic. Ensuite, attendez une heure avant de passer au ASG suivant.

STEP 6 | Répétez les étapes 4 et 5 pour remplacer l'ASG dans l'autre AZ.

Modification du compte administrateur et mise à jour de la pile (v2.0)

Si vous avez déjà déployé le modèle et souhaitez maintenant modifier le mot de passe du compte administrateur ou créer un nouveau compte utilisateur administrateur sur le pare-feu VM-Series, vous devez générer une nouvelle clé API et mettre à jour la pile de modèles avec la nouvelle clé API pour le compte utilisateur administrateur. Pour que les nouvelles instances de pare-feu soient configurées avec le compte utilisateur administrateur mis à jour, vous devez exporter la configuration du pare-feu et la renommer en bootstrap.xml, puis la charger dans le dossier bootstrap S3 que le modèle de mise à l'échelle automatique VM-Series utilise.

©2023 Palo Alto Networks, Inc.

STEP 1 | Connectez-vous à l'interface Web du pare-feu et modifiez les informations d'identification d'un utilisateur administrateur existant, ou créez un nouveau compte.

STEP 2 | Générez la clé API.

STEP 3 | Exportez la configuration en cours d'exécution et renommez-la en bootstrap.xml.

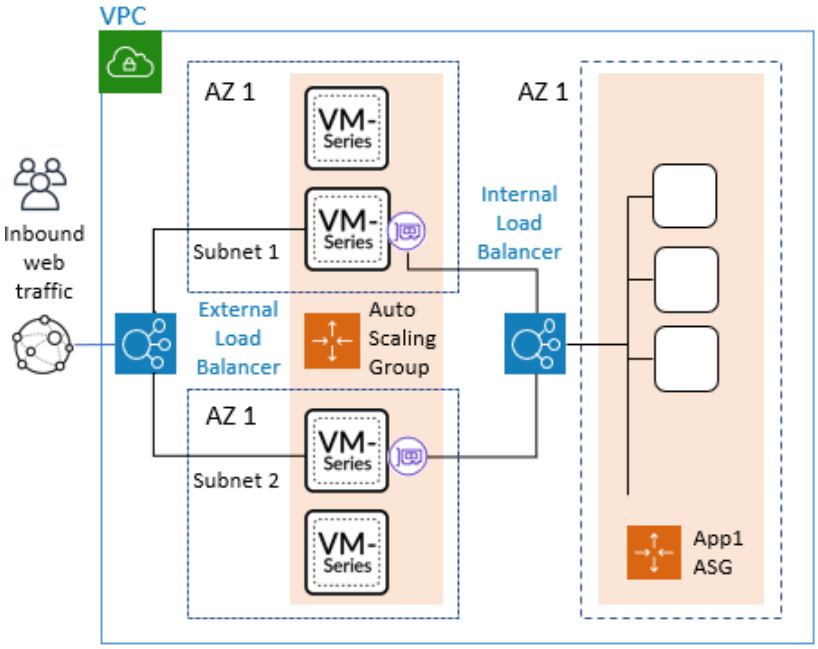
STEP 4 | Chargez ce fichier bootstrap.xml dans le dossier d'amorçage S3 ; reportez-vous à la section Personnalisation du fichier bootstrap.xml (v2.0).

STEP 5 | Mettez à jour la clé API dans la pile pour vous assurer que les pare-feu nouvellement lancés auront le compte d'administrateur mis à jour.

Reportez-vous à la section Mise à jour de la pile avec le modèle de mise à l'échelle automatique VM-Series pour AWS (v2.0).

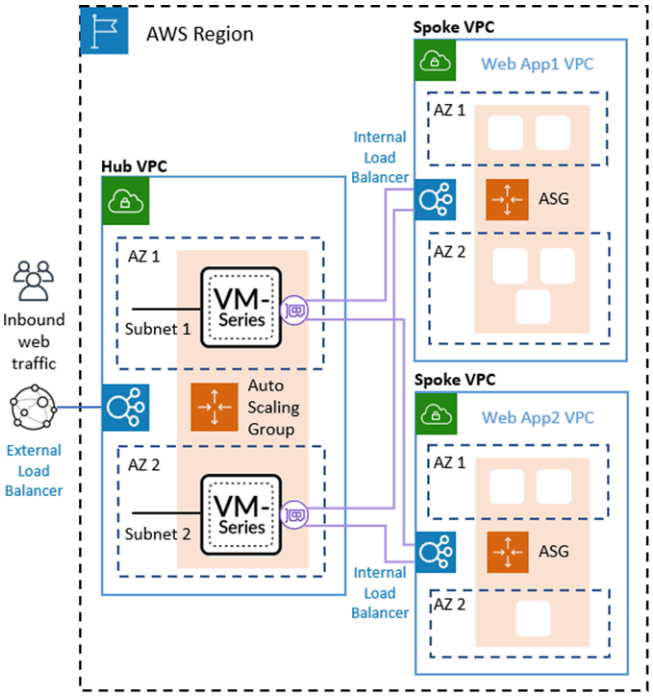
Modèles de mise à l'échelle automatique VM-Series pour AWS version 2.1

Les modèles de mise à l'échelle automatique VM-Series vous permettent de déployer un seul groupe de mise à l'échelle automatique (ASG) de pare-feu VM-Series pour sécuriser le trafic entrant d'Internet vers les charges de travail de vos applications sur AWS. Vous pouvez déployer l'ASG de pare-feu VM-Series et les charges de travail des applications dans un seul VPC, comme indiqué ci-dessous.



Vous pouvez également déployer l'ASG de pare-feu dans un VPC centralisé et les charges de travail de vos applications dans des VPC distincts au sein de la même région, formant ainsi une architecture en étoile, comme indiqué ci-dessous.

©2023 Palo Alto Networks, Inc.



Grâce à l'architecture en étoile, vous pouvez rationaliser la fourniture de sécurité et de connectivité centralisées pour les déploiements AWS avec de nombreuses applications, VPC ou comptes. Cette architecture peut augmenter l'agilité. Les administrateurs de la sécurité de votre réseau gèrent le VPC de pare-feu et les administrateurs ou développeurs d'applications DevOps peuvent gérer les VPC de l'application.

Assurez-vous que les VPC d'applications connectés au VPC de pare-feu ne disposent pas d'une passerelle Internet (IGW) et utilisez un service de surveillance continue et de conformité à la sécurité, tel que Prisma Public Cloud.

Vous pouvez utiliser un seul compte AWS ou plusieurs comptes AWS pour surveiller et sécuriser le trafic entre les VPC et Internet. La centralisation des pare-feu dans un seul VPC peut réduire les coûts des déploiements avec plusieurs VPC et/ou plusieurs comptes.

Pour plus de flexibilité dans la sécurisation de vos charges de travail d'application, la version 2.1 vous permet de déployer un équilibreur de charge d'application ou un équilibreur de charge de réseau pour l'équilibreur de charge externe situé en face de votre ASG de pare-feu VM-Series et l'équilibreur de charge interne situé en face de vos charges de travail d'application.

Lorsqu'un équilibreur de charge d'application est situé en face des charges de travail d'application, vous pouvez connecter le VPC de pare-feu au VPC d'application à l'aide de l'appariement VPC. Lorsqu'un NLB est situé en face des charges de travail d'application, vous pouvez utiliser l'appariement VPC ou un AWS Private Link pour connecter les VPC de pare-feu et d'application, comme résumé ci-dessous :

Équilibreur de charge VPC de pare-feu(externe)	Équilibreur de charge VPC d'application (interne)	Méthode de connexion
ALB	NLB	AWS Private Link

©2023 Palo Alto Networks, Inc.

Équilibreur de charge VPC de pare-feu(externe)	Équilibreur de charge VPC d'application (interne)	Méthode de connexion
NLB	NLB	AWS Private Link
NLB	ALB	Appariement VPC
ALB	ALB	Appariement VPC

Si vous effectuez un déploiement dans un seul VPC, vous pouvez utiliser toutes les combinaisons d'équilibrage de charge du tableau précédent.

Vous pouvez déployer les modèles dans les deux cas d'utilisation greenfield (VPC et applications nouveaux) et brownfield (VPC et applications existants).

Modèle	Nouveau	Existant
Pare-feu	firewall-new-vpc-v2.1.template panw-aws-same-vpc-v2.1.template	firewall-existing-vpc-v2.1.template panw-aws-same-vpc-v2.1.template
Application	panw-aws-nlb-new-vpc-v2.1.template panw-aws-alb-new-vpc-v2.1.template	panw-aws-alb-existing-vpc-v2.1.template panw-aws-nlb-existing-vpc-v2.1.template

Quels sont les composants déployés par le modèle de mise à l'échelle automatique VM-Series pour AWS (v2.1) ?

Le modèle de mise à l'échelle automatique VM-Series pour AWS comprend les blocs de construction suivants.

- Modèles de pare-feu VM-Series
- Modèles d'application
- Fonctions Lambda
- Panorama
- Fichiers d'amorçage

Modèles de pare-feu VM-Series

Les modèles de pare-feu déploient un équilibreur de charge externe Internet et des pare-feu VM-Series au sein d'un groupe de mise à l'échelle automatique couvrant au moins deux zones de disponibilité (AZ). L'équilibreur de charge externe répartit le trafic VPC entrant sur le pool de pare-feu VM-Series. Il peut s'agir d'un équilibreur de charge d'application (ALB) ou d'un équilibreur de charge de réseau (NLB). Les pare-feu VM-Series publient automatiquement des métriques PAN-OS personnalisées qui permettent la mise à l'échelle automatique.

©2023 Palo Alto Networks, Inc.

Modèle	Description
firewall-new-vpc-v2.1.template	Déploie une pile de pare-feu avec deux à quatre zones de disponibilité dans un nouveau VPC.
firewall-existing-vpc-v2.1.template	Déploie une pile de pare-feu avec deux à quatre zones de disponibilité dans un VPC existant. Pour déployer dans un VPC existant, vous devez saisir : • l'ID de VPC • l'ID de passerelle Internet. Il s'agit d'une passerelle existante. • les listes CIDR de sous-réseau des sous-réseaux de gestion, non approuvés, approuvés, de passerelle NAT et Lambda. Le modèle utilise les CIDR pour créer ces sous-réseaux. Si vous choisissez de créer un nouvel ELB, le modèle connecte l'ASG de pare-feu au pool principal d'ELB. Si vous utilisez un ELB existant, vous devez connecter manuellement l'ASG de pare-feu au pool d'équilibreurs de charge existant.

Reportez-vous à la section Personnalisation du modèle de pare-feu avant le lancement (v2.0 et v2.1) pour plus d'informations sur ces paramètres.

Modèles d'application

Le modèle d'application déploie un équilibreur de charge interne (ILB) et un groupe de mise à l'échelle automatique avec un serveur Web dans chaque zone de disponibilité (AZ).

Modèle	Description
panw-aws-same-vpc-v2.1.template	Déployez l'application dans le même VPC que le VPC de pare-feu. Vous pouvez choisir un équilibreur de charge de réseau ou d'application.
panw-aws-alb-new-vpc-v2.1.template	Déployez l'application dans un nouveau VPC, en utilisant ALB comme équilibreur de charge interne et l'appariement VPC entre le VPC de pare-feu et le VPC d'application. Ce modèle prend en charge les déploiements sur un compte et sur plusieurs comptes. Vous devez fournir les paramètres suivants : • l'ID de compte Hub • l'ID de VPC Hub pour l'appariement VPC • les CIDR de sous-réseau approuvé VPC Hub. Le modèle les utilise pour la création de la

 ©2023 Palo Alto Networks, Inc.

Modèle	Description
	table de routage après l'établissement de l'appariement VPC, à raison d'un CIDR par zone de disponibilité. • StsAssumeRoleARN (sortie du modèle Hub pour l'accès SQS)
panw-aws-nlb-new-vpc-v2.1.template	Déployez l'application dans un nouveau VPC, en utilisant NLB comme équilibreur de charge interne et les interfaces/services des terminaux NLB pour la communication entre le VPC de pare-feu et le VPC d'application. Vous devez fournir ces paramètres. • ID de compte Hub • StsAssumeRoleARN (sortie du modèle Hub pour l'accès SQS)
panw-aws-alb-existing-vpc-v2.1.template	Déployez ALB dans un VPC d'application existant. Vous devez fournir l'ID de VPC pour votre application et un ID de sous-réseau existant. Ce modèle déploie l'équilibreur de charge dans le VPC d'application et établit les ressources lambda. Vous devez détacher votre charge de travail cible de tout équilibreur de charge existant et la connecter au nouvel équilibreur de charge.
panw-aws-nlb-existing-vpc-v2.1.template	Déployez NLB dans un VPC d'application existant. Déployez l'application dans un nouveau VPC, en utilisant NLB comme équilibreur de charge interne et les interfaces/services des terminaux NLB pour la communication entre le VPC de pare-feu et le VPC d'application.

Fonctions Lambda

AWS Lambda fournit une automatisation robuste, dirigée par les événements, sans devoir recourir à un logiciel d'orchestration complexe. AWS Lambda surveille un service SQS (service de file d'attente simple) pour en savoir plus sur les équilibreurs de charge (ALB ou NLB) qui sont publiés dans la file d'attente. Lorsque la fonction Lambda détecte un nouvel équilibreur de charge, elle crée une nouvelle règle de politique NAT et l'applique aux pare-feu VM-Series dans l'ASG. Les pare-feu ont une règle de politique NAT pour chaque application et utilisent la règle de politique NAT (qui mappe le port à l'adresse IP de l'équilibreur de charge) pour transférer le trafic vers l'équilibreur de charge devant les serveurs Web d'application.

Les fonctions Lambda suppriment également tous les éléments de configuration que Lambda a ajoutés au groupe d'appareils et à la pile de modèles dans Panorama. Cela inclut la règle NAT, l'objet

 ©2023 Palo Alto Networks, Inc.

d'adresse et les itinéraires statiques qui ont été transférés vers le pare-feu VM-Series. La fonction Lambda prend également en charge la suppression des licences.

Pour en savoir plus sur les fonctions Lambda, reportez-vous à la section **Documentation sur la mise à l'échelle automatique AWS de Palo Alto Networks**.

Panorama

Vous devez avoir le serveur de gestion Panorama en mode Panorama pour configurer la mise à l'échelle automatique v2.1.

Le serveur de gestion Panorama assure la surveillance et la gestion centralisées de plusieurs pare-feu nouvelle génération de Palo Alto Networks à partir d'un seul emplacement. Panorama vous permet de superviser toutes les applications, les utilisateurs et le contenu passant par votre réseau et d'utiliser les informations obtenues pour créer des politiques de mise en œuvre d'applications permettant de protéger et de contrôler le réseau. Si vous ne connaissez pas bien Panorama, veuillez consulter le Guide de l'administrateur Panorama.

Les pare-feu gérés sont amorcés avec un fichier `init-config.txt`. Un exemple de fichier est inclus dans le référentiel GitHub afin que vous puissiez copier la configuration à partir de la pile de modèles et du groupe d'appareils lorsque vous les créez dans votre Panorama existant.

Les zones approuvée et non approuvée créées dans Panorama doivent être toutes en minuscules.

Dans Panorama, vous devez configurer vos interfaces réseau à l'aide de DHCP.

- Seul eth1/1 doit créer automatiquement des zones approuvée et non approuvée d'itinéraires par défaut.
- Les zones de politique de sécurité sont nommées `approuvée` et `non approuvée`.

  Tous les noms de zone doivent être en minuscules

- Les modèles configurent un compte administrateur nommé `pandemo` et le mot de passe `demopassword`.
- Créez un routeur virtuel avec la convention de dénomination VR-<*TemplateStackName* Sur l'onglet ECMP du routeur virtuel, activez l'ECMP.
- Pour définir l'adresse du serveur DNS sur Panorama, sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Services**. Définissez le **Primary DNS Server** (Serveur DNS principal) sur 169.254.169.253, le **Secondary DNS Server** (Serveur DNS secondaire) sur 8.8.8.8 et le **FQDN Refresh Time (sec)** (Fréquence d'actualisation FQDN (s)) sur 60. Panorama a besoin de l'adresse IP du serveur DNS AWS pour résoudre le FQDN de l'équilibreur de charge interne sur AWS. La fréquence d'actualisation du FQDN correspond à l'intervalle auquel Panorama valide les équilibreurs de charge internes récemment détectés.

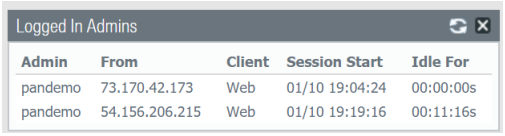
Une fois le modèle d'application lancé, Lambda renseigne les éléments suivants dans Panorama :

- Politique NAT
- Objet d'adresse pour l'équilibreur de charge dans le modèle d'application
- Itinéraires statiques dans le routeur virtuel
- Objet de service Tcp81

©2023 Palo Alto Networks, Inc.

Le modèle de pare-feu v2.1 inclut une passerelle NAT AWS utilisée par les pare-feu pour lancer des requêtes sortantes afin de récupérer les mises à jour, se connecter à Panorama et publier des statistiques dans AWS CloudWatch. Les adresses IP Elastic sont également associées aux passerelles NAT pour chaque zone.

Vous devez disposer des ressources Panorama suivantes pour utiliser les modèles de mise à l'échelle automatique pour AWS.

Clé API Panorama	Vous avez besoin d'une clé API Panorama pour authentifier l'API. Lambda utilise votre clé API pour configurer automatiquement les options de groupes d'appareils et de modèles. Pour générer la clé API, reportez-vous à la section Obtention de votre clé API.
Clé de désactivation de licence Panorama	Le modèle nécessite une clé API de désactivation de licence et l'activation de « Verify Update Server Identity » (Vérifier l'identité du serveur de mise à jour) pour désactiver les clés de licence à partir de Panorama. La clé de désactivation de licence doit être obtenue à partir du portail de support client de Palo Alto (CSP), comme décrit à la section Installation d'une clé API de licence.
Clé d'authentification de machine virtuelle Panorama	Vous avez besoin d'une clé d'authentification de machine virtuelle pour permettre aux pare-feu amorcés de se connecter à Panorama et de recevoir leur configuration d'amorçage. Reportez-vous à la section Génération de la clé d'authentification VM sur Panorama.
Accès à l'interface de gestion Panorama	• **Port 443 (HTTPS)** : lors du déploiement initial du modèle de pare-feu, laissez HTTPS ouvert pour que Lambda puisse se connecter à Panorama. Attendez de recevoir la confirmation de connexion suivante dans Panorama :  Logged In Admins Admin From Client Session Start Idle For pandemo 73.170.42.173 Web 01/10 19:04:24 00:00:00s pandemo 54.156.206.215 Web 01/10 19:19:16 00:11:16s Lorsque vous sécurisez le port 443, vous spécifiez une plage d'adresse IP à partir de laquelle vous autoriserez les connexions, ainsi que les EIP attribués aux passerelles NAT. Il existe deux passerelles NAT et les EIP qui leur sont associés. Pour rechercher les EIP des passerelles NAT dans AWS, accédez à **VPC** > **NAT Gateways (Passerelles NAT)**. Notez les informations EIP pour le groupe de sécurité pour HTTPS. • **Port 3978** : le port 3978 doit pouvoir recevoir du trafic à partir de n'importe quelle adresse IP.

Fichiers d'amorçage

Le référentiel de mise à l'échelle automatique GitHub comprend un fichier `init-cfg.txt` pour que le pare-feu VM-Series dispose de la configuration de base pour :

 ©2023 Palo Alto Networks, Inc.

- Effectuer la permutation d'interface pour que le trafic `non approuvé` du pare-feu VM-Series utilise l'ENI AWS pour eth0.
- Communiquer avec Panorama pour la configuration des modèles et des groupes d'appareils.

Le référentiel GitHub de mise à l'échelle automatique dispose de la configuration de base pour commencer. Cette solution de mise à l'échelle automatique nécessite la permutation des interfaces du dataplane et de gestion pour permettre à l'équilibreur de charge de transférer le trafic Web vers le niveau de mise à l'échelle automatique des pare-feu VM-Series. Pour en savoir plus sur le mappage d'interface de gestion avec Amazon ELB comme indiqué à Mappage d'interface de gestion pour l'utilisation avec Amazon ELB.

Planifiez de déployer les modèles de mise à l'échelle automatique VM-Series pour AWS (v2.1)

Avant de commencer le déploiement, examinez les ressources suivantes.

- Reportez-vous à la section Mise à l'échelle automatique de pare-feu VM-Series avec le service Amazon ELB pour obtenir un aperçu des fonctionnalités de modèles et de la planification des comptes.
- Personnalisation du modèle de pare-feu avant le lancement (v2.0 et v2.1). Les paramètres de base de cette rubrique s'appliquent à toutes les versions de modèles.
- Comment le modèle de mise à l'échelle automatique VM-Series pour AWS (v2.0 et v2.1) active-t-il la mise à l'échelle dynamique ?

  Ces concepts s'appliquent à toutes les versions de modèles.

Lancement du modèle de pare-feu (v2.1)

Vous pouvez choisir de déployer les modèles d'application et pare-feu dans le même VPC ou dans des VPC distincts.

Les modèles prennent en charge une architecture en étoile dans laquelle vous pouvez déployer le modèle de pare-feu dans un compte AWS et l'utiliser comme hub pour sécuriser les applications (en étoile) appartenant au même ou à différents comptes AWS.

Ce flux de travail vous indique comment déployer l'équilibreur de charge externe et les pare-feu VM-Series à l'aide du modèle de pare-feu. La clé vm-auth-key doit être configurée sur Panorama avant de lancer ce modèle.

STEP 1 | Examinez les listes de contrôle des sections Planifiez de déployer les modèles de mise à l'échelle automatique VM-Series pour AWS (v2.1) et Planification du modèle de mise à l'échelle automatique VM-Series pour AWS (v2.0 et v2.1).

Vérifiez que vous avez effectué les tâches suivantes :

- (Pour PAYG uniquement) Passez en revue et acceptez le CLUF pour le forfait PAYG que vous prévoyez d'utiliser.
- (Pour BYOL uniquement) Obtenez le code d'autorisation pour un forfait prenant en charge le nombre de pare-feu pouvant être requis pour votre déploiement. Vous devez enregistrer ce

 ©2023 Palo Alto Networks, Inc.

code d'autorisation dans un fichier texte nommé **`authcodes`** (sans extension) et mettre le fichier **`authcodes`** dans le dossier **`/license`** de l'ensemble d'amorçage.



Si vous utilisez des codes d'autorisation individuels au lieu d'un forfait, le pare-feu ne récupère que la clé de licence pour le premier code d'autorisation inclus dans le fichier.

- Téléchargez les fichiers requis pour lancer le modèle de mise à l'échelle automatique VM-Series v2.1 à partir du référentiel GitHub.

©2023 Palo Alto Networks, Inc.

STEP 2 | Modifiez le fichier **init-cfg.txt** et chargez-le dans le dossier **/config**.

Comme vous utilisez Panorama pour amorcer les pare-feu VM-Series, votre fichier **init-cfg.txt** doit être modifié comme suit. Aucun fichier **bootstrap.xml** n'est nécessaire.

```
type=dhcp-client
```

```
ip-address=
```

```
default-gateway=
```

```
netmask=
```

```
ipv6-address=
```

```
ipv6-default-gateway=
```

```
hostname=
```

```
vm-auth-key=
```

```
panorama-server=
```

```
panorama-server-2=
```

```
tplname=AWS-tmplspoke1
```

```
dgname=AWS-dgspoke1
```

```
dns-primary=169.254.169.253
```

```
dns-secondary=8.8.8.8
```

```
op-command-modes=mgmt-interface-swap
```

```
dhcp-send-hostname=yes
```

 ©2023 Palo Alto Networks, Inc.

```
dhcp-send-client-id=yes
```

```
dhcp-accept-server-hostname=yesdhcp-accept-server-domain=yes
```

```
vm-series-auto-registration-id=
```

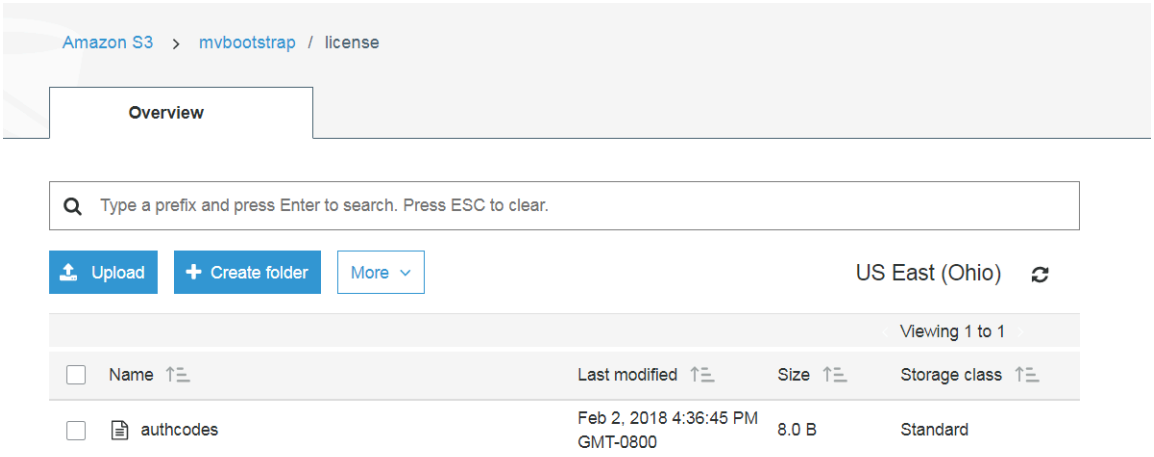
```
vm-series-auto-registration-pin-value=
```

Vérifiez que **`op-command-modes=mgmt-interface-swap`** existe. Il s'agit de la commande permettant de permuter l'interface de gestion (mgmt) et l'interface du dataplane (ethernet 1/1) sur le pare-feu VM-Series sur AWS. Utilisez l'adresse IP du serveur DNS AWS 169.254.169.253 pour une résolution plus rapide des noms DNS de l'équilibreur de charge.

Vous devez ajouter le PIN d'enregistrement automatique du certificat de périphérique au fichier init-cfg.txt pour installer automatiquement un certificat de périphérique lorsque votre instance de pare-feu VM-Series est déployée.

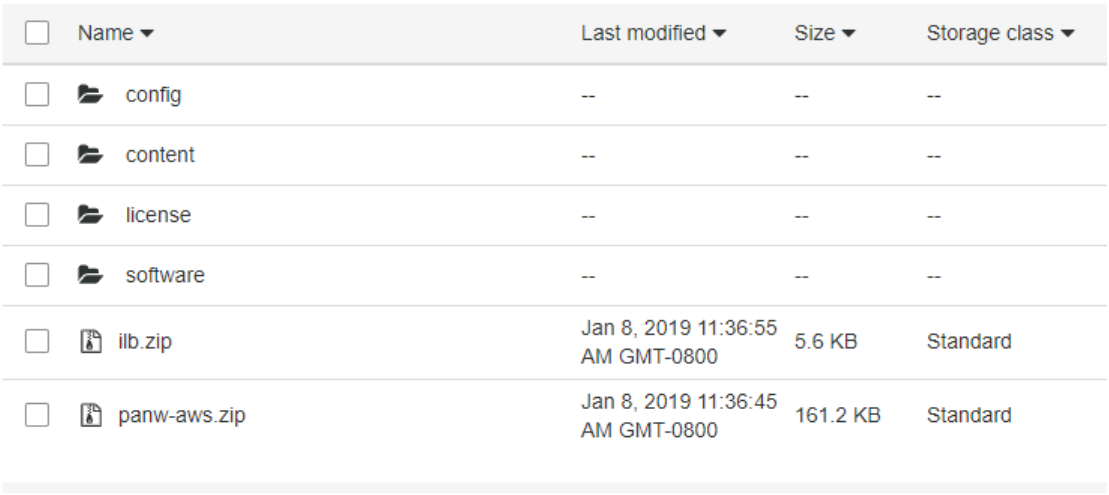
STEP 3 | (Pour BYOL uniquement) Ajoutez le code d'autorisation de licence au dossier **`/license`** de l'ensemble d'amorçage.

1. Utilisez un éditeur de texte pour créer un nouveau fichier texte nommé **`authcodes`** (sans extension).
2. Ajoutez le code d'autorisation de vos licences BYOL à ce fichier, puis enregistrez-le. Le code d'autorisation doit représenter un forfait et prendre en charge le nombre de pare-feu pouvant être requis pour votre déploiement. Si vous utilisez des codes d'autorisation individuels au lieu d'un forfait, le pare-feu ne récupère que la clé de licence pour le premier code d'autorisation inclus dans le fichier.



 ©2023 Palo Alto Networks, Inc.

STEP 4 | Chargez le code Lambda pour le modèle de pare-feu (`panw-aws-zip`) et le modèle d'application (`ilb.zip`) dans un compartiment S3. Vous pouvez utiliser le même compartiment S3 que celui que vous avez utilisé pour l'amorçage.



Name	Last modified	Size	Storage class
config	--	--	--
content	--	--	--
license	--	--	--
software	--	--	--
ilb.zip	Jan 8, 2019 11:36:55 AM GMT-0800	5.6 KB	Standard
panw-aws.zip	Jan 8, 2019 11:36:45 AM GMT-0800	161.2 KB	Standard

Si la pile d'applications est gérée par un compte différent du pare-feu, utilisez le compte d'application pour créer un autre compartiment s3 dans la même région AWS que le modèle de pare-feu et copiez le fichier `ilb.zip` dans ce compartiment s3.

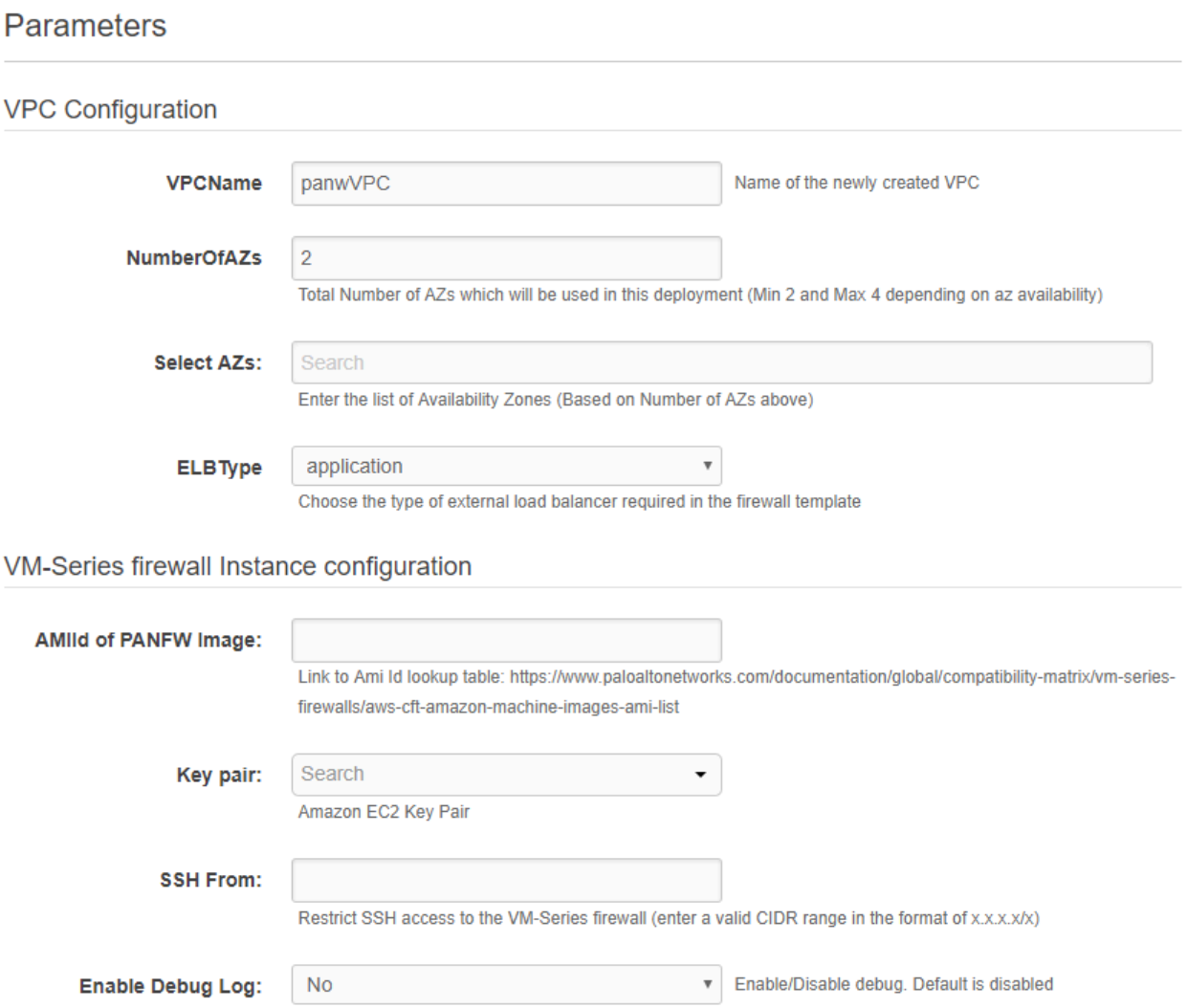
STEP 5 | Sélectionnez l'interface de pare-feu.

1. Dans la console de gestion AWS, sélectionnez **CloudFormation** > **Create Stack (Créer une pile)**.
2. Sélectionnez Upload a template to Amazon S3 (Charger un modèle sur Amazon S3) pour choisir le modèle d'application permettant de déployer les ressources que le modèle lance dans le même VPC que les pare-feu ou dans un VPC différent. Cliquez sur Open (Ouvrir) et Next (Suivant).
3. Spécifiez le Stack name (Nom de la pile). Le nom de la pile vous permet d'identifier de manière unique toutes les ressources déployées à l'aide de ce modèle.

©2023 Palo Alto Networks, Inc.

STEP 6 | Configurez les paramètres pour le VPC.

1. Assurez-vous de sélectionner au moins deux zones de disponibilité



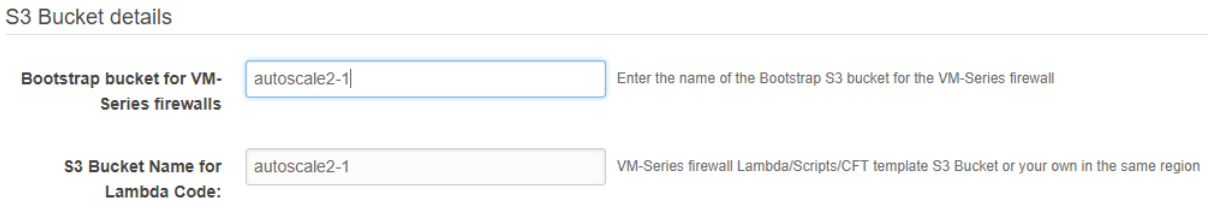
2. Recherchez l'ID AMI pour le pare-feu VM-Series et saisissez-le. Assurez-vous que l'ID AMI correspond à la région AWS, à la version de PAN-OS et à l'option de licence BYOL ou PAYG que vous avez choisi d'utiliser.
3. Sélectionnez la **Key pair** (Paire de clés) EC2 (à partir de la liste déroulante) pour lancer le pare-feu. Pour vous connecter aux pare-feu, vous devez fournir le nom de cette paire de clés et la clé privée qui lui est associée.
4. Pour le champ **SSH from** (SSH à partir de), les pare-feu seront gérés par Panorama et n'auront aucune EIP pour l'interface de gestion. Mais juste au cas où vous décidiez d'affecter une EIP, configurez la plage d'adresses IP à partir de laquelle vous vous connecteriez.
5. Sélectionnez **Yes** (Oui) si vous souhaitez **Enable Debug Log** (Activer le journal de débogage). L'activation du journal de débogage génère des journaux plus détaillés qui

 ©2023 Palo Alto Networks, Inc.

aident à résoudre les problèmes liés au déploiement. Ces journaux sont générés à l'aide du nom de la pile et sont enregistrés dans AWS CloudWatch.

Par défaut, le modèle utilise l'utilisation du processeur comme paramètre de mise à l'échelle pour les pare-feu VM-Series. Les statistiques PAN-OS personnalisées sont automatiquement publiées dans l'espace de noms CloudWatch qui correspond au nom de la pile que vous avez spécifié précédemment.

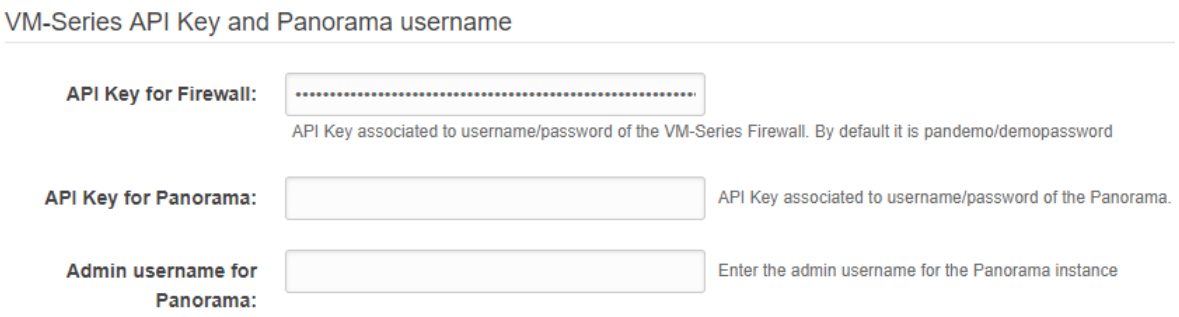
STEP 7 | Indiquez le nom du ou des compartiments Amazon S3.



1. Entrez le nom du compartiment S3 qui contient l'ensemble d'amorçage.

   Si le compartiment d'amorçage n'est pas configuré correctement ou si vous entrez un nom de compartiment incorrect, le processus d'amorçage échoue et vous ne pouvez pas vous connecter au pare-feu. Les vérifications de l'état pour les équilibreurs de charge échouent également.
2. Saisissez le nom du S3 bucket (Compartiment S3) qui contient le fichier panw-aws.zip. Comme mentionné précédemment, vous pouvez utiliser un compartiment S3 pour le code Lambda ou Bootstrap (Amorçage).

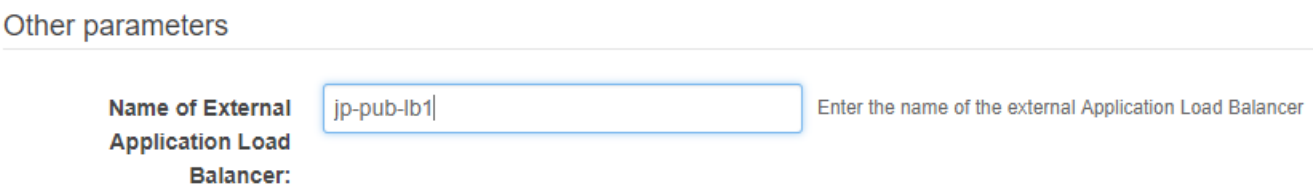
STEP 8 | Spécifiez les clés permettant d'activer l'accès API au pare-feu et à Panorama.



1. Entrez la clé que le pare-feu doit utiliser pour authentifier les appels d'API. La clé par défaut est basée sur l'exemple de fichier et ne doit être utilisée que pour les tests et l'évaluation. Pour un déploiement de production, vous devez créer une connexion PAN-OS distincte uniquement pour l'appel d'API et générer une clé associée.
2. Saisissez l'API Key (Clé API) pour permettre à AWS Lambda de passer des appels API à Panorama. Pour un déploiement de production, vous devez créer une connexion distincte uniquement pour l'appel d'API et générer une clé associée.

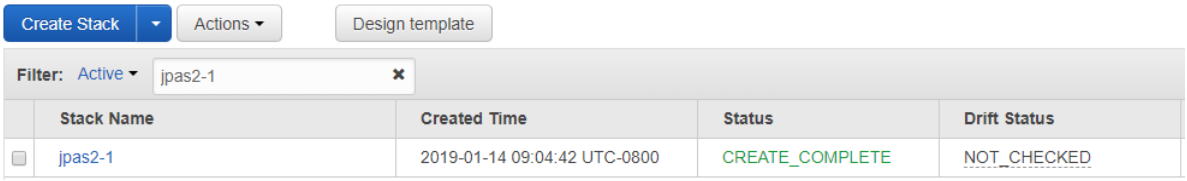
©2023 Palo Alto Networks, Inc.

STEP 9 | Entrez le nom de l'équilibreur de charge de l'application.



STEP 10 | Passez en revue les paramètres du modèle et lancez le modèle.

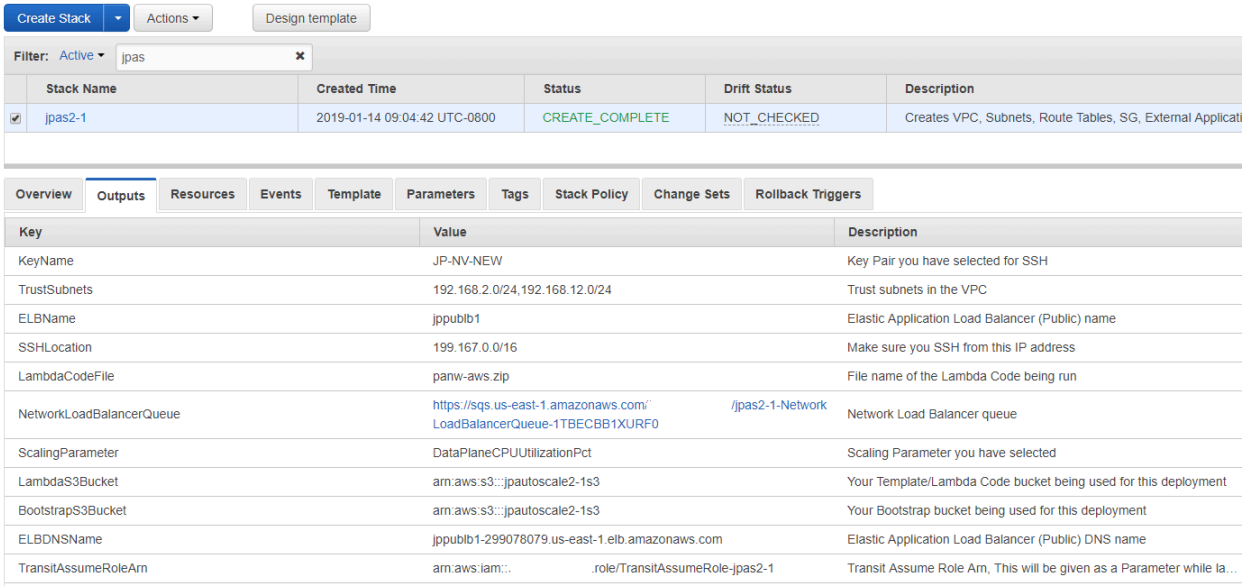
1. Sélectionnez **I acknowledge that this template might cause AWS CloudFormation to create IAM resources (Je reconnais que ce modèle peut entraîner la création de ressources IAM par AWS CloudFormation)**.
2. Cliquez sur **Create (Créer)** pour lancer le modèle. L'événement CREATE_IN_PROGRESS s'affiche.
3. En cas de déploiement réussi, le statut est mis à jour et passe à CREATE_COMPLETE.



 ©2023 Palo Alto Networks, Inc.

STEP 11 | Vérifiez que le modèle a lancé toutes les ressources requises.

1. Sur l'EC2 Dashboard (Tableau de bord EC2), sélectionnez Auto Scaling Groups (Groupes de mise à l'échelle automatique). Vérifiez que dans chaque AZ, vous avez un ASG pour les pare-feu VM-Series. Le préfixe du nom de l'ASG inclut le nom de la pile.
2. Dans la console de gestion AWS, cliquez sur le Stack Name (Nom de la pile) pour afficher l'Outputs (Résultats) pour la liste des ressources.
3. Vos Outputs (Résultats) doivent ressembler aux résultats de l'image suivante.
   - Prenez note du nom de la Network Load Balancer Queue (File d'attente de l'équilibreur de charge de réseau).
   - Prenez note du ELBDNSName (Nom du DNS public de l'équilibreur de charge Elastic).



Cela peut prendre jusqu'à 20 minutes pour que les pare-feu démarrent et soient disponibles pour gérer le trafic.

Lorsque vous avez terminé les tests ou un déploiement de production, la seule façon de garantir l'arrêt des charges consiste à supprimer complètement la pile. L'arrêt d'instances ou la modification du maximum d'ASG à 0 n'est pas suffisant.

STEP 12 | Enregistrez les informations suivantes sur le modèle de pare-feu. Vous devez fournir ces valeurs en tant qu'entrées lors du déploiement du modèle d'application.

- **Adresses IP de la passerelle NAT dans chaque AZ** : vous avez besoin de cette adresse IP pour restreindre l'accès HTTPS à votre Panorama afin que Lambda puisse utiliser les EIP de la passerelle NAT pour communiquer avec Panorama en cas de besoin.
- **URL SQS de l'équilibreur de charge réseau** : une fonction Lambda dans la pile de pare-feu surveille cette file d'attente pour apprendre les équilibreurs de charge de réseau que vous déployez et créer des règles de politique NAT (une par application) dans Panorama permettant aux pare-feu d'envoyer du trafic à l'adresse IP de l'équilibreur de charge de réseau.

©2023 Palo Alto Networks, Inc.

Lancement du modèle d'application (v2.1)

Les modèles d'application vous permettent de compléter la topologie sandwich et sont fournis afin que vous puissiez évaluer la solution de mise à l'échelle automatique. Ce modèle d'application déploie un équilibreur de charge de réseau et d'application et une paire de serveurs Web derrière le groupe de mise à l'échelle automatique des pare-feu VM-Series que vous avez déployé à l'aide du modèle de pare-feu.

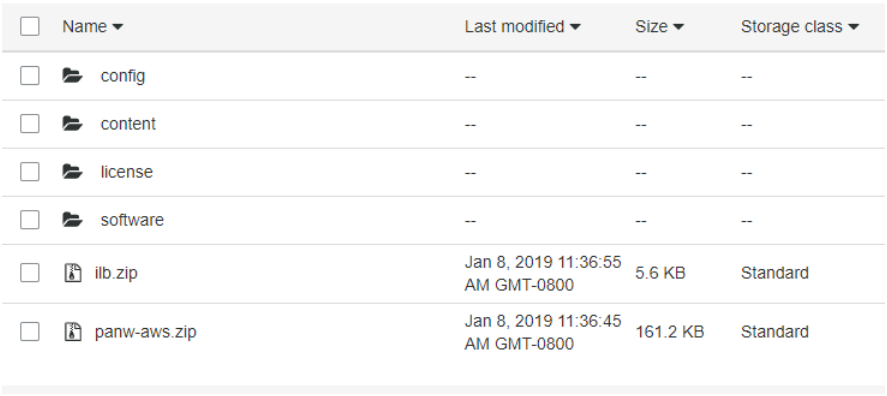
Utilisez ce modèle pour évaluer la solution, mais personnalisez votre propre modèle à déployer en production. Pour un modèle personnalisé, assurez-vous d'activer la messagerie SQS entre le modèle d'application et le modèle de pare-feu.

Lors du lancement du modèle d'application, vous devez sélectionner le modèle selon que vous souhaitez déployer le modèle d'application dans le même VPC dans lequel vous avez déployé le modèle de pare-feu ou dans un VPC distinct. Reportez-vous à la section Activation du trafic vers le service ELB (v2.0 et v2.1).

STEP 1 | Créez un compartiment S3 à partir duquel vous lancerez le modèle d'application.

- S'il s'agit d'un déploiement entre comptes, créez un nouveau compartiment.
- S'il existe un compte, vous pouvez créer un nouveau compartiment ou utiliser le compartiment S3 que vous avez créé précédemment (vous pouvez utiliser un compartiment pour tout).

STEP 2 | Chargez le fichier ilb.zip dans le compartiment S3.



STEP 3 | Sélectionnez le modèle de lancement d'application que vous souhaitez lancer.

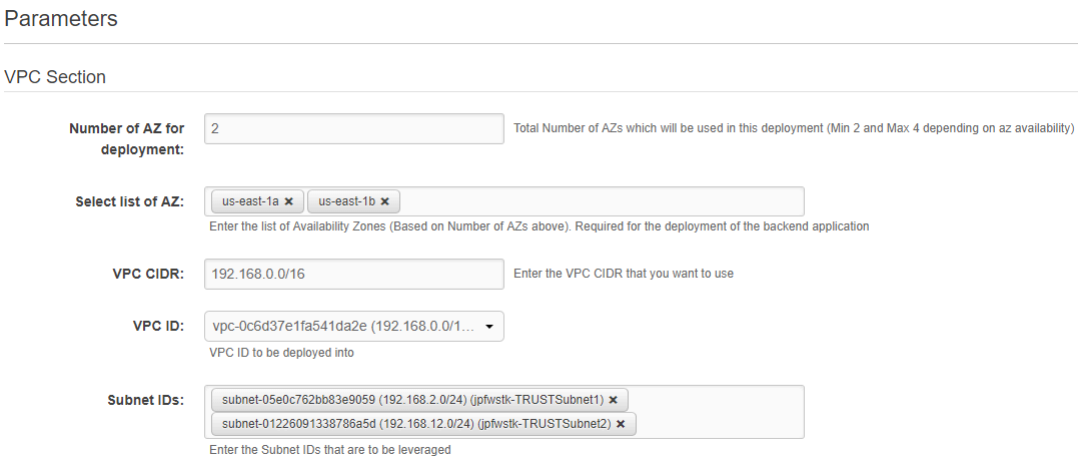
1. Dans la console de gestion AWS, sélectionnez **CloudFormation** > **CreateStack**
2. Sélectionnez Upload a template to Amazon S3 (Charger un modèle sur Amazon S3) pour choisir le modèle d'application permettant de déployer les ressources que le modèle lance dans le même VPC que les pare-feu ou dans un VPC différent. Cliquez sur **Open (Ouvrir)** et **Next (Suivant)**.
3. Spécifiez le Stack name (Nom de la pile). Le nom de la pile vous permet d'identifier de manière unique toutes les ressources déployées à l'aide de ce modèle.

STEP 4 | Configurez les paramètres pour le VPC et l'équilibreur de charge réseau.

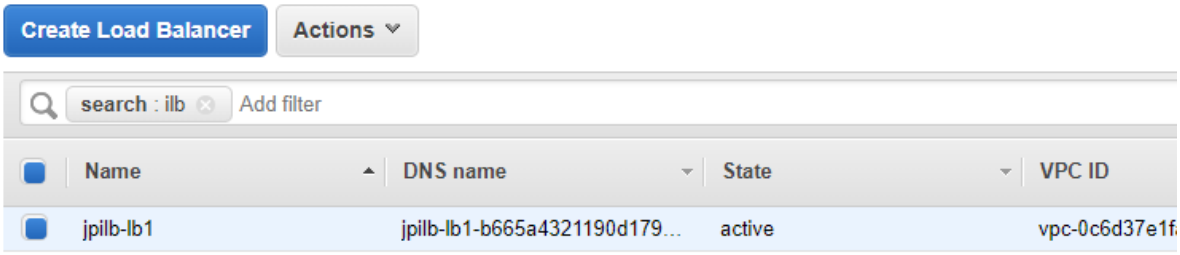
1. Sélectionnez les deux Availability Zones (Zones de disponibilité) que votre configuration va couvrir dans Select list of AZ (Sélectionner une liste d'AZ). Si vous effectuez un déploiement dans le même VPC, veillez à sélectionner les mêmes Availability Zones (Zones de disponibilité) que celles que vous avez sélectionnées pour le modèle de pare-feu.

©2023 Palo Alto Networks, Inc.

2. En cas de déploiement sur un nouveau VPC, saisissez un CIDR Block (Bloc CIDR) pour le VPC. Le CIDR par défaut est 192.168.0.0/16.
3. Si vous effectuez un déploiement sur le même VPC, vous sélectionnerez le précédent VPC et utiliserez les sous-réseaux approuvés.

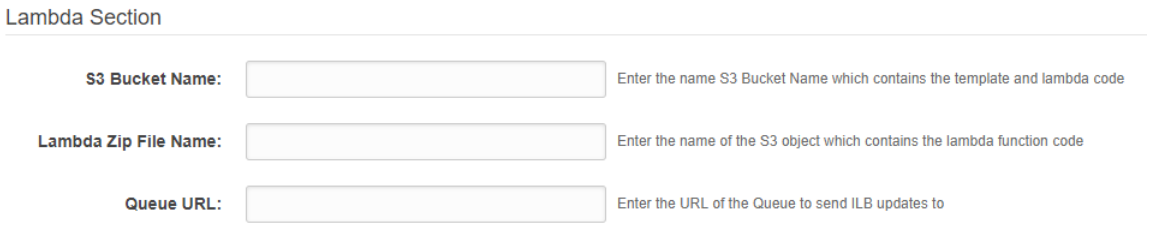


STEP 5 | Sélectionnez le type d'équilibreur de charge.



STEP 6 | Configurez les paramètres pour Lambda.

1. Saisissez le S3 Bucket Name (Nom du compartiment S3) où est stocké ilb.zip.
2. Saisissez le nom du Zip File Name (Nom du fichier zip).
3. Collez l'URL SQS que vous avez copiée précédemment.



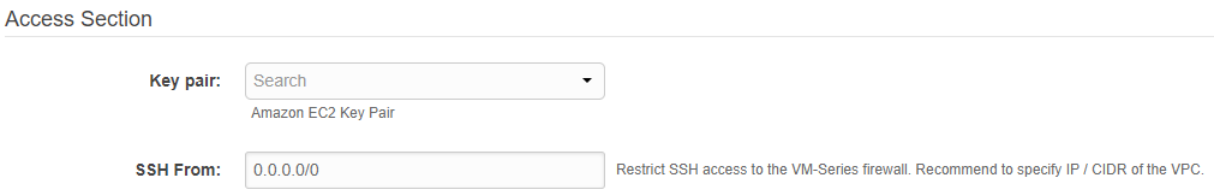
STEP 7 | Modifiez le Instance Type of Web Servers (Type d'instance EC2 du serveur Web) pour répondre à vos besoins de déploiement.



 ©2023 Palo Alto Networks, Inc.

STEP 8 | Sélectionnez la EC2 Key pair (Paire de clés EC2) (dans la liste déroulante) pour lancer les serveurs Web. Pour vous connecter aux serveurs Web, vous devez fournir le nom de la paire de clés et la clé privée associée.

STEP 9 | Sélectionnez l'adresse IP du réseau à partir duquel vous accéderez aux serveurs pour l'accès de gestion uniquement. Le trafic Web provient du nom ELBDNS que vous avez copié lorsque vous avez lancé le modèle de pare-feu.

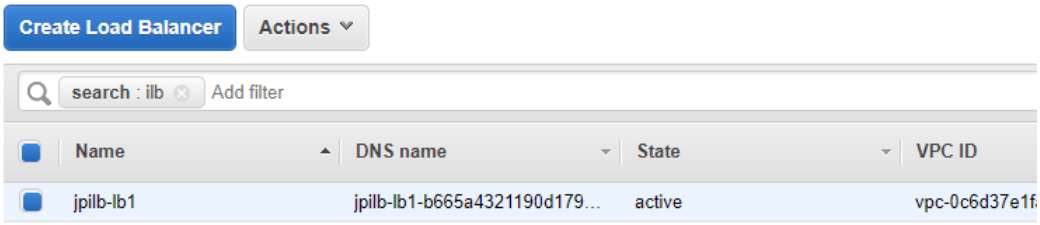


STEP 10 | Passez en revue les paramètres du modèle et lancez le modèle.

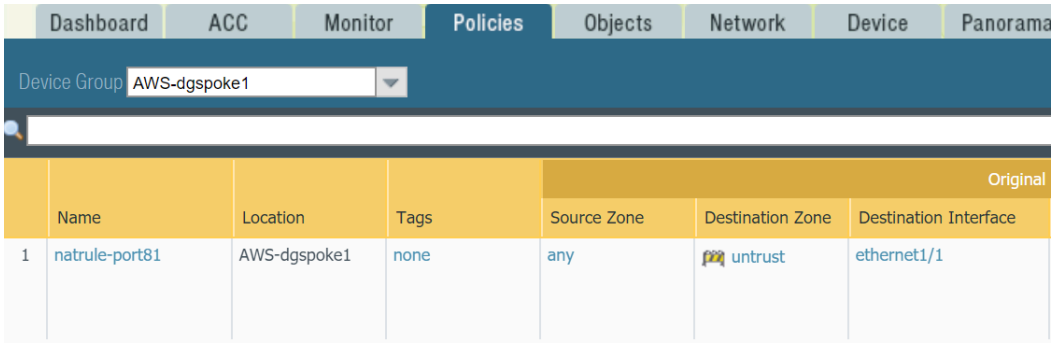
 ©2023 Palo Alto Networks, Inc.

STEP 11 | Une fois le modèle d'application terminé, l'activation des pages Web peut prendre jusqu'à 20 minutes.

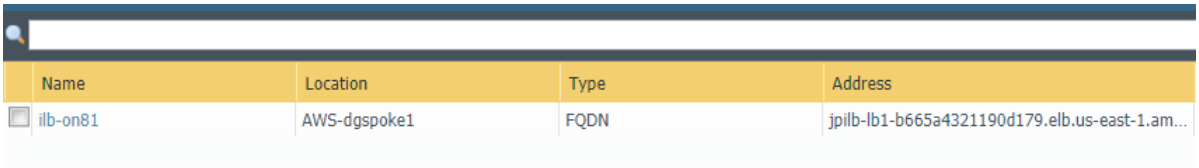
1. Vérifiez que l'équilibreur de charge du modèle d'application est marqué comme Active (Actif).



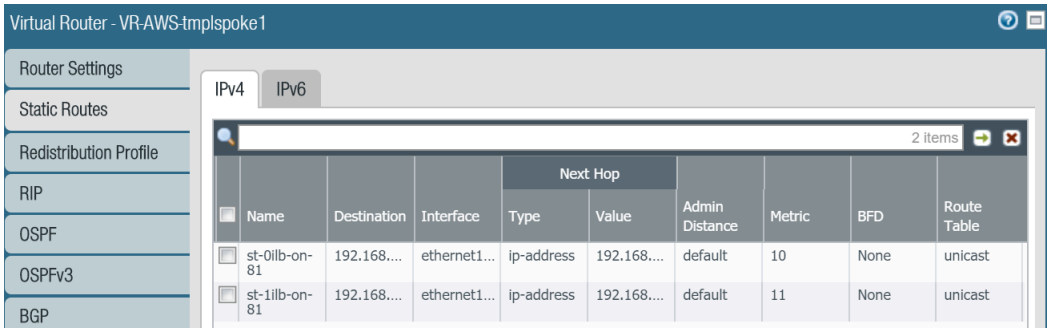
2. Vérifiez que Panorama dispose d'un objet NAT dans le Device Group (Groupe d'appareils).



3. Vérifiez que Panorama dispose d'un objet Address (Adresse) dans le Device Group (Groupe d'appareils).



4. Vérifiez que Panorama dispose de Static Routes (Itinéraires statiques) dans la pile de modèles.



STEP 12 | Obtenez le DNS name (Nom de DNS) que vous avez précédemment enregistré pour l'équilibreur de charge d'application et saisissez-le dans un navigateur Web.

©2023 Palo Alto Networks, Inc.

STEP 13 | Une fois le lancement réussi, votre navigateur doit afficher le résultat suivant.



Congratulations, you have successfully launched VM-Series ASG CloudFormation. This file is coming from Webserver Region: us-east-1

StackID: arn:aws:cloudformation:us-east-1: :stack/jpappstk1/1c197cb0-18f4-11e9-b92e-0ab87eb901cc

StackName: jpappstk1

Création d'une AMI (Image de machine Amazon) personnalisée (v2.1)

Une AMI personnalisée VM-Series vous offre la cohérence et la flexibilité nécessaires pour déployer un pare-feu VM-Series avec la version de PAN-OS que vous souhaitez utiliser sur votre réseau au lieu de se limiter à l'utilisation d'une AMI publiée sur l'AWS public Marketplace ou sur l'AWS GovCloud Marketplace. L'utilisation d'une AMI personnalisée accélère le processus de déploiement d'un pare-feu avec la version de PAN-OS de votre choix, car elle réduit le temps nécessaire à la configuration du pare-feu avec une AMI publiée sur l'AWS public ou l'AWS GovCloud Marketplace, puis effectue des mises à niveau logicielles vers la version PAN-OS que vous souhaitez utiliser sur votre réseau. De plus, vous pouvez utiliser l'AMI personnalisée dans les modèles CloudFormation de pare-feu VM-Series de mise à l'échelle automatique ou dans tout autre modèle que vous avez créé.

Vous pouvez créer une AMI personnalisée avec les licences BYOL, Bundle 1 (Forfait 1) ou Bundle 2 (Forfait 2). Le processus de création d'une AMI personnalisée nécessite que vous supprimiez toute la configuration du pare-feu et que vous effectuiez une restauration des données privées. Par conséquent, dans ce flux de travail, vous lancerez une nouvelle instance du pare-feu à partir de l'AWS Marketplace au lieu d'utiliser un pare-feu existant entièrement configuré.

Lorsque vous créez une AMI personnalisée avec une version BYOL du pare-feu, vous devez d'abord activer la licence sur le pare-feu afin de pouvoir accéder au contenu et aux mises à jour logicielles PAN-OS et les télécharger pour mettre à niveau votre pare-feu, puis désactiver la licence sur le pare-feu avant d'effectuer une restauration des données privées et créer l'AMI personnalisée. Si vous ne désactivez pas la licence, vous perdez la licence que vous avez appliquée sur cette instance de pare-feu.

STEP 1 | Lancez le pare-feu VM-Series depuis le Marketplace.

Reportez-vous à la section Lancement du pare-feu VM-Series.

STEP 2 | (Uniquement pour BYOL) Activez la licence.

STEP 3 | Installez le dernier contenu sur le pare-feu.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | (Uniquement pour BYOL) Désactivez la licence.

STEP 5 | Effectuez une réinitialisation des données privées.

Une réinitialisation des données privées supprime tous les journaux et restaure la configuration par défaut.

Les disques système ne sont pas effacés, de sorte que les mises à jour du contenu de l'étape 4 sont intactes.

1. Accédez à la CLI du pare-feu.
2. Procédez à l'Exportation d'une copie de la configuration.
3. Supprimez tous les journaux et restaurez la configuration par défaut.

```
request system private-data-reset
```

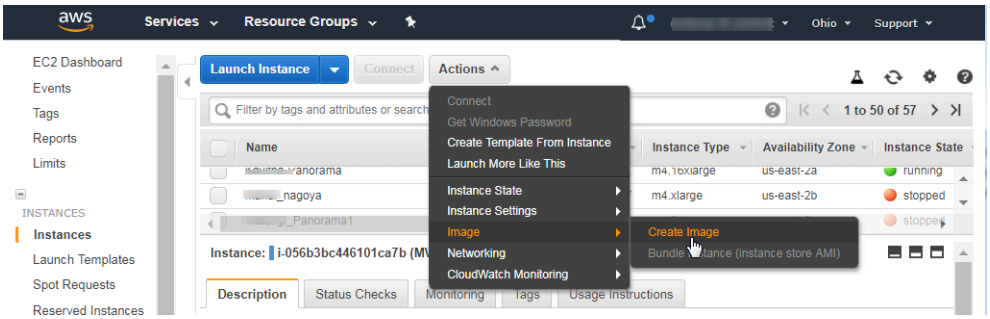
Appuyez sur **y** pour confirmer.

Le pare-feu redémarre pour initialiser la configuration par défaut.

©2023 Palo Alto Networks, Inc.

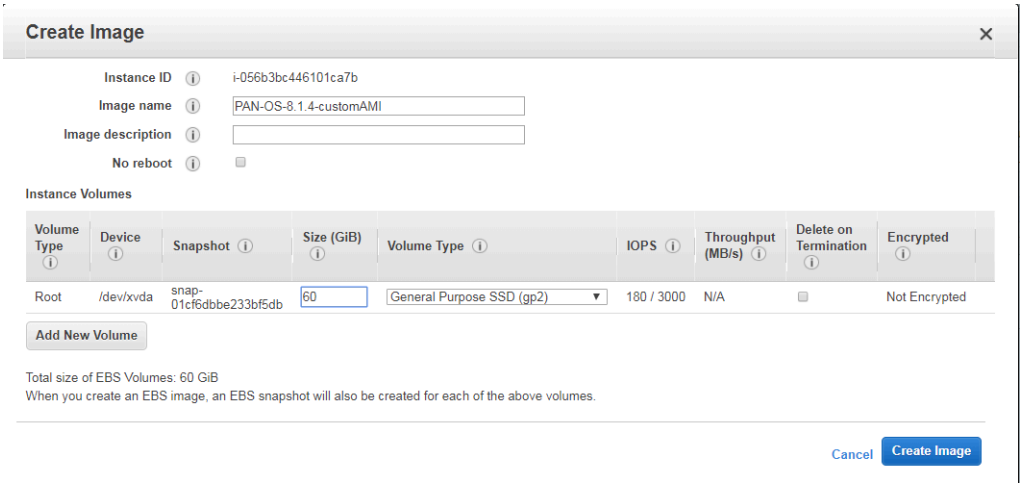
STEP 6 | Créez l'AMI personnalisée.

1. Connectez-vous à la console AWS et sélectionnez l'EC2 Dashboard (Tableau de bord EC2).
2. Cliquez sur **Stop** (Arrêter) pour arrêter le pare-feu VM-Series.
3. Sélectionnez l'instance de pare-feu VM-Series, puis cliquez sur **Image** > **Create Image (Créer une image)**.



4. Saisissez un nom d'image personnalisée, puis cliquez sur **Create Image** (Créer une image).

   L'espace disque requis de 60 Go est la configuration minimale requise.



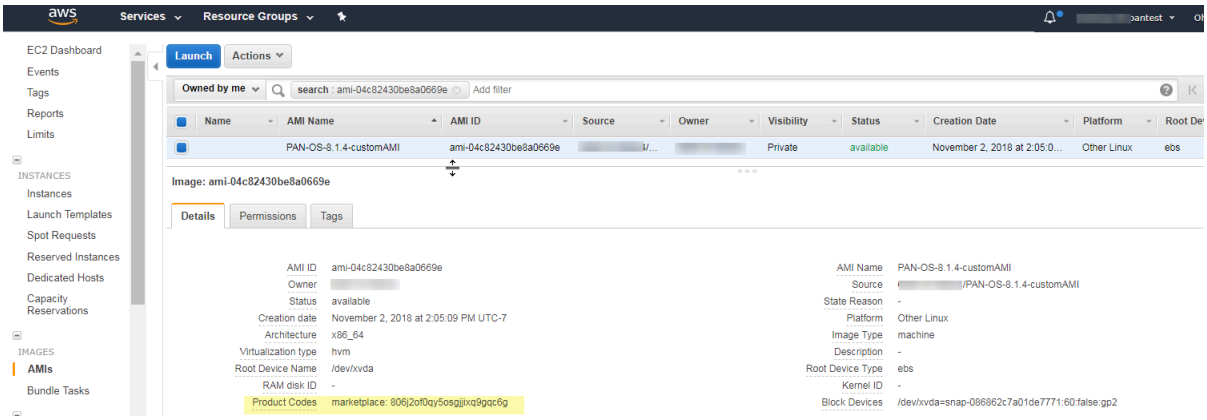
5. Vérifiez que l'AMI personnalisée est créée et que le code produit est correct.

   1. Sur l'EC2 Dashboard (Tableau de bord EC2), sélectionnez **AMI**.

   2. Sélectionnez l'AMI que vous venez de créer. Selon que vous avez sélectionné une AMI avec les options de licence BYOL, Bundle 1 (Forfait 1) ou Bundle 2 (Forfait 2), vous devez voir l'un des **Product Codes** (Codes produit) suivants dans les Details (Détails) :

   - BYOL : 6njl1pau431dv1qxipg63mvah
   - Forfait 1 : 6kxdw3bbmdeda3o6i1ggqt4km
   - Bundle 2—806j2of0qy5osgjjixq9gqc6g

©2023 Palo Alto Networks, Inc.



STEP 7 | Chiffrement du volume EBS pour le pare-feu VM-Series sur AWS.

Si vous envisagez d'utiliser l'AMI personnalisée avec le chiffrement EBS pour un déploiement de Mise à l'échelle automatique de pare-feu VM-Series avec le service Amazon ELB, vous devez utiliser la clé principale par défaut de votre compte AWS.

Suppression des modèles de mise à l'échelle automatique VM-Series (v2.1)

Si vous avez déployé les modèles à titre de test, supprimez-les pour économiser des ressources et réduire les coûts.

STEP 1 | Dans la console de gestion AWS, sélectionnez **Cloud Formation** > **Create Stack (Créer une pile)**.

STEP 2 | Recherchez le modèle de pare-feu et le modèle d'application que vous avez précédemment lancés et supprimez les deux modèles.

Pour plus d'informations sur la suppression des piles de modèles, reportez-vous à la section «Qu'est-ce que AWS CloudFormation ? »

Si vous ne supprimez pas votre pile de modèles, AWS vous facture des frais.

Messagerie SQS entre le modèle d'application et le modèle de pare-feu (v2.1)

Les pare-feu VM-Series déployés à l'aide de l'un des modèles de pare-feu peuvent détecter et envoyer le trafic aux équilibreurs de charge auxquels vous souhaitez distribuer automatiquement le trafic entrant. Pour ce faire, le modèle de pare-feu comprend une fonction lambda qui surveille les messages dans un SQS (Service de file d'attente simple). Le message permet à la fonction lambda de se familiariser avec un nouvel équilibreur de charge, puis de créer automatiquement une règle de politique NAT sur le pare-feu pour envoyer le trafic à l'adresse IP de l'équilibreur de charge. Pour acheminer le trafic correctement dans l'infrastructure AWS, le message doit également inclure des informations de base sur le DNS, l'ID de VPC et l'AZ à laquelle appartient l'équilibreur de charge.

Si vous créez votre propre modèle d'application, vous devez configurer votre modèle d'application pour publier les messages ADD et DEL dans l'URL SQS que le modèle de pare-feu utilise pour se familiariser avec les équilibreurs de charge auxquels il doit répartir le trafic dans votre environnement :

 ©2023 Palo Alto Networks, Inc.

- Message ADD-NLB qui informe les pare-feu lorsqu'un nouvel équilibreur de charge réseau est disponible.
- Message DEL-NLB qui informe les pare-feu lorsqu'un équilibreur de charge réseau a été arrêté et n'est plus disponible.
- Message ADD-ALB qui informe les pare-feu lorsqu'un nouvel équilibreur de charge d'application est disponible.
- Message DEL-ALB qui informe les pare-feu lorsqu'un équilibreur de charge d'application a été arrêté et n'est plus disponible.

Les exemples suivants de chaque type de message incluent des exemples de valeurs. Vous devez modifier ces messages avec les valeurs correspondant à votre déploiement.

Message ADD-NLB

```
msg_add_nlb= {
        "MSG-TYPE": "ADD-NLB",
        "AVAIL-ZONES": [
        {
            "NLB-IP":"192.168.2.101",
            "ZONE-NAME":"us-east-2a",
            "SUBNET-ID": "subnet-2a566243"
        },
        {
            "NLB-IP":"192.168.12.101",
            "ZONE-NAME":"us-east-2b",
            "SUBNET-ID": "subnet-2a566243 "
        }
```

 ©2023 Palo Alto Networks, Inc.

```
        ],

             "DNS-NAME": "publicelb1-2119989486.us-
east-2.elb.amazonaws.com",

            "VPC-ID": "vpc-42ba9f2b",

            "NLB-NAME": "publicelb1"

}
```

DEL-NLB Message

```
msg_del_nlb= {

 "MSG-TYPE": "DEL-NLB",

 "DNS-NAME": "publicelb1-2119989486.us-east-2.elb.amazonaws.com",

}
```

MESSAGE ADD-ALB

```
{ "AVAIL-ZONES": [

        {

            "SUBNET-CIDR": "172.32.0.0/24",

            "SUBNET-ID": "subnet-0953a3a8e2a8208a9",

            "ZONE-NAME": "us-east-2a"

        },

        {
```

 ©2023 Palo Alto Networks, Inc.

```
            "SUBNET-CIDR": "172.32.2.0/24",

            "SUBNET-ID": "subnet-0a9602e4fb0d88baa",

            "ZONE-NAME": "us-east-2c"

        },

        {

            "SUBNET-CIDR": "172.32.1.0/24",

            "SUBNET-ID": "subnet-0b31ed16f308b3c4d",

            "ZONE-NAME": "us-east-2b"

        }

    ],

    "VPC-PEERCONN-ID": "pcx-0538bb05dbe2e1b8e",

    "VPC-CIDR": "172.32.0.0/16",

    "ALB-NAME": "appILB-908-0",

    "ALB-ARN":"arn:aws:elasticloadbalancing:us-
east-2:018147215560:loadbalancer/app/appILB-908-0/1997ed20eeb5bcef",

    "VPC-ID": "vpc-0d9234597da6d9147",

    "MSG-TYPE": "ADD-ALB",

    "DNS-NAME": "internal-appILB-908-0-484644265.us-
east-2.elb.amazonaws.com"
```


 ©2023 Palo Alto Networks, Inc.

```
}
```

DEL-ALB Message

```
{
```

```
   "MSG-TYPE": "DEL-ALB",
```

```
   "DNS-NAME": "internal-appILB-908-0-484644265.us-
east-2.elb.amazonaws.com"
```

```
}
```

Reportez-vous à la documentation AWS pour savoir comment envoyer un message à une file d'attente Amazon SQS.

Mise à jour de la pile avec le modèle de mise à l'échelle automatique VM-Series pour AWS (v2.1)

Une mise à jour de la pile vous permet de modifier les ressources déployées par le modèle de pare-feu du modèle de mise à l'échelle automatique VM-Series. Au lieu de supprimer votre déploiement existant et de redéployer la solution, utilisez la mise à jour de la pile pour modifier les paramètres de configuration du lancement suivants .

Vous pouvez modifier le type d'instance AWS, la paire de clés de vos groupes de mise à l'échelle automatique et la clé APi associée au compte d'utilisateur administrateur sur le pare-feu.

Il n'est pas nécessaire de mettre à jour la pile pour modifier les notifications par défaut ou créer des alarmes de mise à l'échelle automatique. Reportez-vous à la section Modification des paramètres de mise à l'échelle et des statistiques CloudWatch (v2.1).

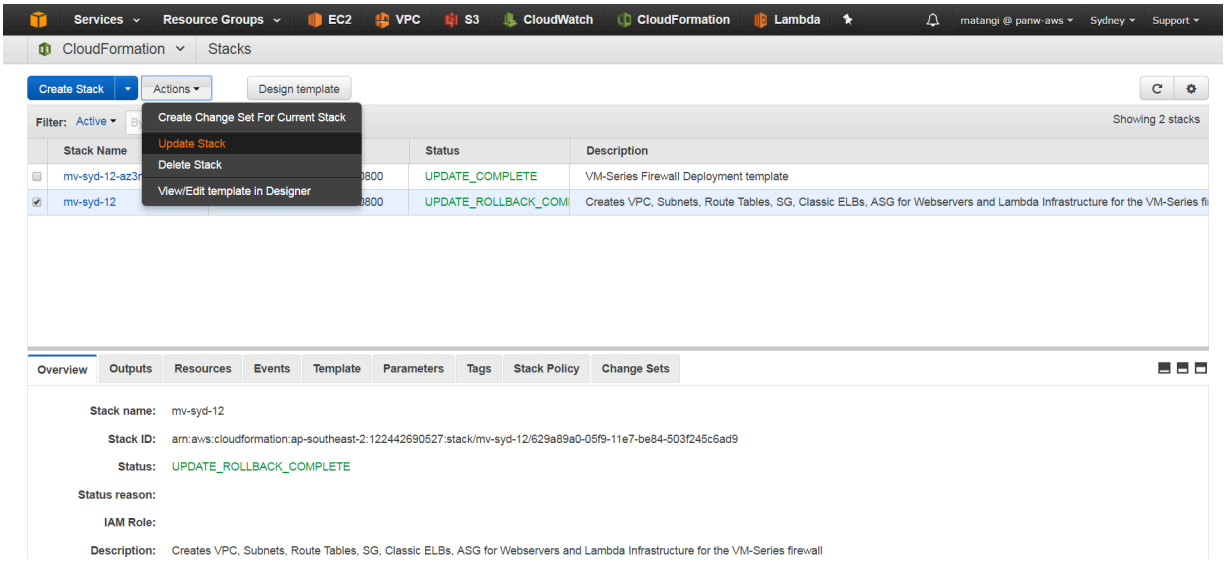
Lorsque vous déployez le modèle de mise à l'échelle automatique VM-Series, les groupes de mise à l'échelle automatique et la configuration de lancement sont automatiquement créés pour vous. La configuration de lancement est un modèle qu'un groupe de mise à l'échelle automatique utilise pour lancer une instance EC2. Il spécifie des paramètres tels que le type d'instance, la paire de clés de votre groupe de mise à l'échelle automatique ou la clé API associée au compte d'utilisateur administratif sur le pare-feu.

Pour les applications critiques, effectuez une mise à jour de la pile pendant une fenêtre de maintenance.

Vous pouvez mettre à jour votre pile directement ou créer des ensembles de modifications. Le flux de travail dans ce document vous guide à travers la mise à jour manuelle de la pile.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Dans la console AWS CloudFormation, sélectionnez la pile parente que vous souhaitez mettre à jour et choisissez **Actions** > **Update Stack (Mettre à jour la pile)**.

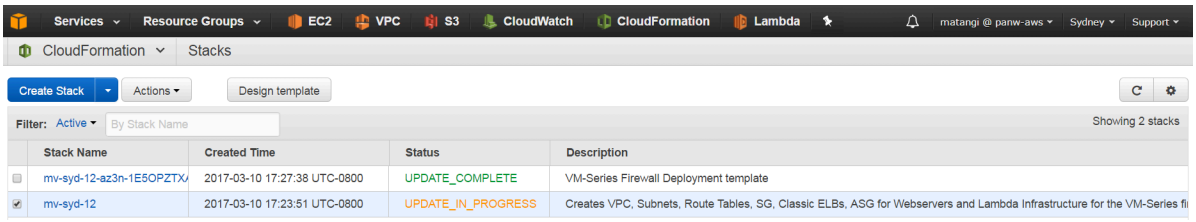


STEP 2 | Modifiez les ressources que vous souhaitez mettre à jour.

Vous pouvez modifier le type d'instance, le groupe de sécurité, la paire de clés pour les ressources de la pile ou la clé API associée au compte d'utilisateur administrateur sur le pare-feu.

Si vous créez un nouveau compte d'utilisateur administrateur ou modifiez les informations d'identification de l'administrateur existant sur le pare-feu, vous devez suivre le flux de travail de la section Modification du compte administrateur (v2.1) afin de mettre à jour cette pile et de déployer de nouveaux pare-feu avec la clé API mise à jour.

STEP 3 | Acceptez les notifications et passez en revue les modifications, puis cliquez sur **Update (Mettre à jour)** pour lancer la mise à jour de la pile.



Modification du compte administrateur (v2.1)

Si vous avez déjà déployé le modèle et souhaitez maintenant modifier le mot de passe du compte administrateur ou créer un nouveau compte utilisateur administrateur sur le pare-feu VM-Series, vous devez générer une nouvelle clé API et mettre à jour la pile de modèles avec la nouvelle clé API pour le compte utilisateur administrateur.

STEP 1 | Connectez-vous à l'interface Web du pare-feu et modifiez les informations d'identification d'un utilisateur administrateur existant, ou créez un nouveau compte.

STEP 2 | Générez la clé API.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Mettez à jour la clé API dans la pile pour vous assurer que les pare-feu nouvellement lancés ont le compte d'administrateur mis à jour.

Reportez-vous à la section Mise à jour de la pile avec le modèle de mise à l'échelle automatique VM-Series pour AWS (v2.0).

Modification des paramètres de mise à l'échelle et des statistiques CloudWatch (v2.1)

Cette tâche explique comment utiliser les statistiques PAN-OS personnalisées en tant que paramètres de mise à l'échelle pour déclencher des actions de mise à l'échelle automatique.

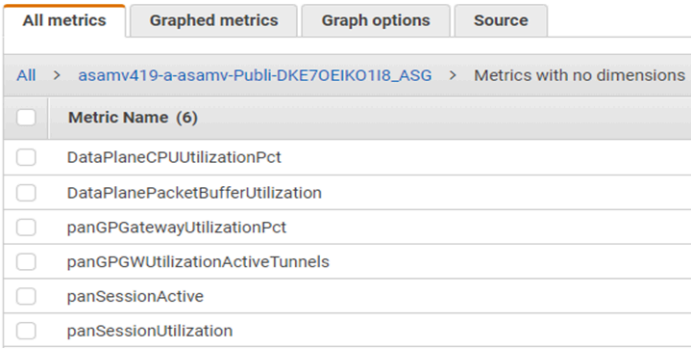
Lorsque vous procédez au lancement du modèle de pare-feu, le modèle crée un espace de noms avec des politiques de mise à l'échelle (augmentation et diminution) que vous pouvez utiliser pour définir des actions de mise à l'échelle automatique. Les noms de politique incluent l'espace de noms, comme indiqué ci-dessous :

- <Custom Namespace>-scalein – Supprimer 1 instance
- <Custom Namespace>-scaleout – Ajouter 1 instance

Chaque statistique PAN-OS comporte une notification par défaut que vous pouvez supprimer et remplacer par des actions de mise à l'échelle automatique. Pour chaque statistique, créez deux actions : une qui détermine quand ajouter un pare-feu VM-Series et une autre qui détermine quand supprimer un pare-feu VM-Series.

STEP 1 | Dans AWS, sélectionnez **Services** > **CloudWatch** > **Metrics (Statistiques)**.

STEP 2 | Choisissez un lien **Custom Namespace (Espace de noms personnalisé)** et sélectionnez le lien des statistiques pour afficher les statistiques PAN-OS personnalisées.



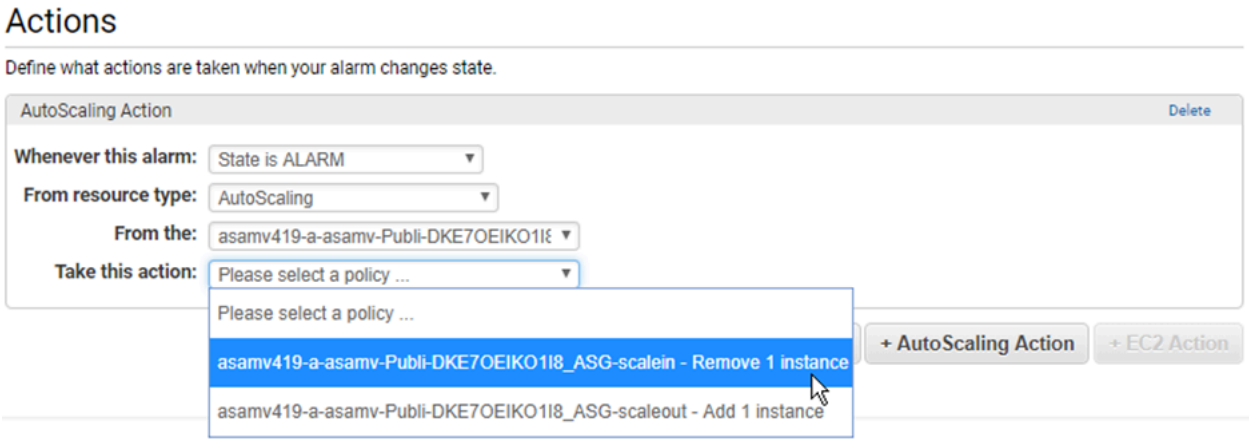
STEP 3 | Cochez une case pour sélectionner une statistique, puis sélectionnez l'onglet **Graphed metrics** (Statistiques graphiques).

1. Dans la colonne **Statistics** (Statistiques), choisissez un critère statistique (tel que moyen, minimum et maximum) et une période.
2. Dans la colonne **Actions**, cliquez sur la cloche « Create alarm » (Créer une alarme).

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Définissez une alarme qui supprime un pare-feu lorsque l'utilisation du processeur est inférieure ou égale aux critères que vous avez définis, sur la période que vous avez définie.

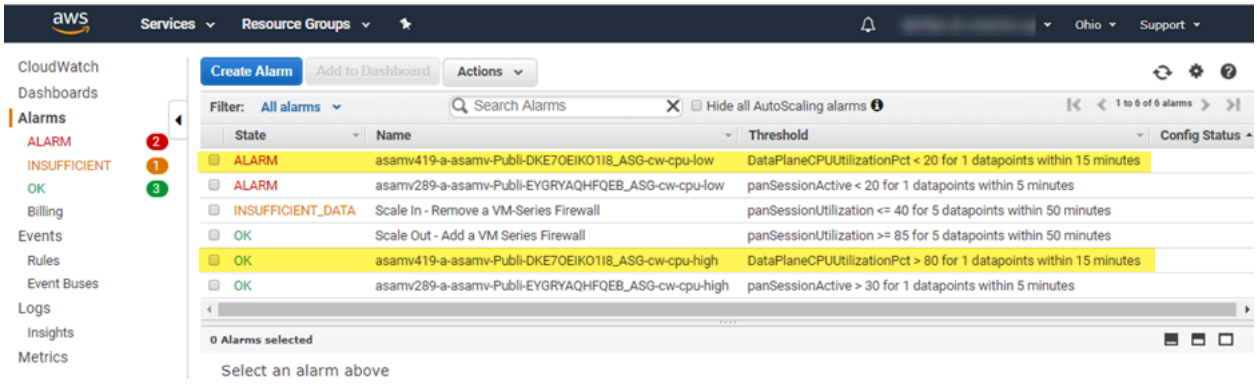
1. Sélectionnez **Edit** (Modifier) pour modifier le titre du graphique.
2. Sous **Alarm details** (Détails de l'alarme), remplissez les champs **Name** (Nom) et **Description**, choisissez un opérateur et définissez la valeur minimale pour conserver les instances actuelles. Si la valeur minimale n'est pas conservée, une instance est supprimée.
3. Sous **Actions**, cliquez sur **delete** (supprimer) la notification par défaut.
4. Sélectionnez **+AutoScaling Action** (Action de mise à l'échelle automatique (augmentation)).
   - Utilisez la liste **From the** (Depuis le) pour sélectionner votre espace de noms.
   - À partir de **Take this action** (Effectuer cette action), sélectionnez la politique pour supprimer une instance.



5. Sélectionnez **Create Alarm** (Créer une alarme).

STEP 5 | Créez une seconde alarme qui ajoute un pare-feu lorsque l'utilisation du processeur est supérieure ou égale aux critères que vous avez définis.

STEP 6 | Pour afficher vos alarmes, sélectionnez **Services** > **CloudWatch** > **Alarms (Alarmes)**.



Pour modifier une alarme depuis cette fenêtre, cochez la case à côté de l'alarme et sélectionnez **Action** > **Edit (Modifier)**.

©2023 Palo Alto Networks, Inc.

Liste des attributs surveillés dans AWS VPC

Lors de la configuration ou de la modification des machines virtuelles sur vos VPC AWS, deux façons s'offrent à vous de surveiller ces instances et de récupérer les étiquettes à utiliser comme critères de comparaison dans des groupes d'adresses dynamiques.

- **Source d'informations de machine virtuelle** : Sur un pare-feu de prochaine génération, vous pouvez surveiller un maximum de 32 étiquettes, soit 14 étiquettes prédéfinies et 18 paires clé-valeur (étiquettes).
- **Plug-in AWS sur Panorama** : le plug-in Panorama pour AWS vous permet de connecter Panorama à vos VPC AWS sur le cloud public et de récupérer le mappage d'adresse IP vers étiquette pour vos machines virtuelles. Panorama enregistre ensuite les informations de la machine virtuelle sur les pare-feu Palo Alto Networks® que vous avez configurés pour la notification. Grâce au plugin, Panorama peut récupérer un total de 32 étiquettes pour chaque machine virtuelle, soit 11 étiquettes prédéfinies et un maximum de 21 étiquettes définies par l'utilisateur.



La longueur maximale de la valeur de l'étiquette (nom et valeur inclus) doit être inférieure ou égale à 116 caractères. Si une étiquette a plus de 116 caractères, Panorama ne récupère pas l'étiquette et ne l'enregistre pas sur les pare-feu.

Attributs surveillés sur AWS-VPC		Source d'informations de machine virtuelle sur le pare-feu	Plugin AWS sur Panorama
ID AMI	ImageId.<ImageId string>	Oui	Oui
Architecture	Architecture.<Architecture string>	Oui	Non
Zone de disponibilité	AvailabilityZone.<string>	Oui	Oui
Système d'exploitation invité	GuestOS.<guest OS name>	Oui	Non
Profil de l'instance IAM	Iam-instance-profile.<instanceProfileArn>	Non	Oui
ID d'instance	InstanceId.<InstanceId string>	Oui	Non
État de l'instance	InstanceState.<instance state>	Oui	Non
Type d'instance	InstanceType.<instance type>	Oui	Non

©2023 Palo Alto Networks, Inc.

Attributs surveillés sur AWS-VPC		Source d'informations de machine virtuelle sur le pare-feu	Plugin AWS sur Panorama
Nom de la clé	KeyName.<KeyName string>	Oui	Oui
ID propriétaire La valeur de cet attribut est tirée de l'ENI.	Account-number.<OwnerId>	Non	Oui
Emplacement Location, nom du groupe	Placement.Tenancy.<string> Placement.GroupName.<string>	Oui	Oui
Nom DNS privé	PrivateDnsName.<Private DNS Name>	Oui	Non
Nom DNS public	PublicDnsName.<Public DNS Name>	Oui	Oui
ID de sous-réseau	SubnetID.<subnetID string>	Oui	Oui
ID du groupe de sécurité	Sg-id.<sg-xxxx>	Non	Oui
Security Group Name (Nom du groupe de sécurité)	Sg-name.<SecurityGroupName>	Non	Oui
ID VPC	VpcId.<VpcId string>	Oui	Oui
Étiquette (clé, valeur)	aws-tag.<key>.<value>	Oui ; Un maximum de 18 étiquettes définies par l'utilisateur sont prises en charge. Les étiquettes définies par l'utilisateur sont triées	Oui ; Un maximum de 21 étiquettes définies par l'utilisateur sont prises en charge. Les étiquettes définies par l'utilisateur sont triées par ordre alphabétique et les 21 premières étiquettes

©2023 Palo Alto Networks, Inc.

Attributs surveillés sur AWS-VPC		Source d'informations de machine virtuelle sur le pare-feu	Plugin AWS sur Panorama
		par ordre alphabétique et les 18 premières étiquettes peuvent être utilisées sur les pare-feu.	peuvent être utilisées sur les pare-feu.

Permissions de gestion d'identité et d'accès pour la surveillance dans AWS VPC

Afin d'activer la surveillance VM, les informations d'identification de connexion AWS de l'utilisateur liées à la clé d'accès et à la clé d'accès secrète AWS doivent disposer des permissions nécessaires pour les attributs mentionnés ci-dessus. Ces privilèges permettent au pare-feu d'initier les appels d'API afin de surveiller les machines virtuelles dans AWS VPC.

La politique IAM associée à l'utilisateur doit soit offrir un accès « en lecture » global, comme AmazonEC2ReadOnlyAccess, ou inclure des permissions individuelles pour tous les attributs surveillés. L'exemple de politique IAM suivant énumère les permissions nécessaires pour initier les actions de l'API afin de surveiller les ressources dans AWS VPC :

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Action": [ "ec2:DescribeAvailabilityZones", "ec2:DescribeImages",
 "ec2:DescribeInstances", "ec2:DescribeInstanceStatus",
 "ec2:DescribeKeyPairs", "ec2:DescribePlacementGroups",
 "ec2:DescribeRegions", "ec2:DescribeSubnets", "ec2:DescribeTags",
 "ec2:DescribeVpcs" ], "Resource": [ "*" ] } ] }
```


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur KVM

La machine virtuelle basée sur le noyau (KVM) est un module de virtualisation Open Source pour serveurs exécutant des distributions Linux. Le pare-feu VM-Series peut être déployé sur un serveur Linux exécutant l'hyperviseur KVM.

Ce guide suppose que vous disposiez d'une infrastructure informatique utilisant Linux et des connaissances élémentaires d'utilisation de Linux/des outils Linux. Les instructions s'appliquent exclusivement au déploiement du pare-feu VM-Series sur KVM.

- VM-Series sur KVM : configuration système requise et conditions préalables
- Déploiements pris en charge sur KVM
- Installation du pare-feu VM-Series sur KVM
- Réglage des performances de VM-Series pour KVM
- Délestage intelligent du trafic

VM-Series sur KVM : configuration système requise et conditions préalables

- Options d'association du VM-Series sur le réseau
- Conditions préalables du VM-Series sur KVM

Table 2: VM-Series sur système KVM : configuration système requise

Exigences	Description
Ressources matérielles	Reportez-vous à la section Configuration système requise pour VM-Series pour la configuration matérielle minimale requise pour votre modèle VM-Series.
Versions logicielles	Reportez-vous à la matrice de compatibilité pour plus d'informations sur les versions logicielles de KVM prises en charge.
Pilotes SR-IOV	Reportez-vous aux pilotes de la section Versions de pilotes PacketMMAP dans la matrice de compatibilité.
Pilotes DPDK	Reportez-vous à la section Versions de pilotes DPDK dans la matrice de compatibilité. Si vous utilisez l'un des pilotes de carte réseau pris en charge sur VM-Series sur KVM, DPDK est activé par défaut.
Interfaces réseau : cartes réseau et ponts logiciels	Le VM-Series sur KVM prend en charge un total de 25 interfaces : 1 interface de gestion et un maximum de 24 interfaces réseau pour le trafic de données. Le pare-feu VM-Series déployé sur KVM prend en charge les commutateurs virtuels basés sur le logiciel tels que le pont Linux ou le pont Open vSwitch, et dirigent la connectivité vers le PCI Pass-Thru ou une carte compatible avec SR-IOV. Si vous envisagez d'établir une connectivité à l'aide de PCI-passthrough ou de SR-IOV, vous ne pouvez pas configurer de commutateur vSwitch sur le port physique utilisé pour SR-IOV ou PCI-passthrough. Pour communiquer avec l'hôte et d'autres machines virtuelles sur le réseau, le pare-feu VM-Series doit avoir un accès exclusif au port physique et aux fonctions virtuelles associées sur cette interface. • Sur le pont Linux et OVS, les pilotes e1000 et Virtio sont pris en charge ; le pilote par défaut rtl8139 n'est pas pris en charge.

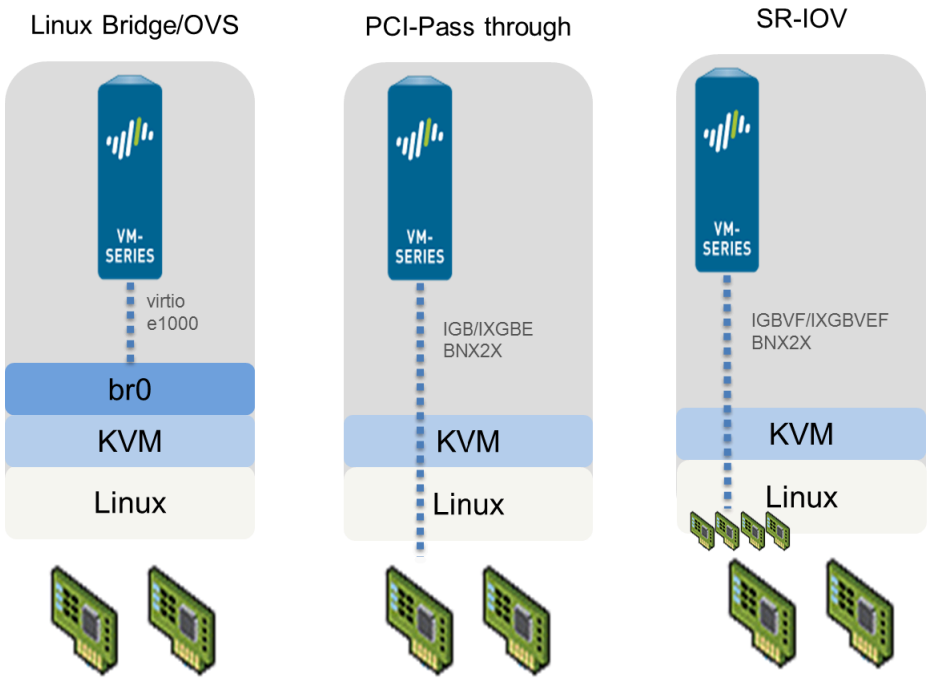
©2023 Palo Alto Networks, Inc.

Exigences	Description

	• Pour la prise en charge du PCI Pass-Thru/SR-IOV, le pare-feu VM-Series a été testé pour les cartes réseau suivantes :
	  • Carte réseau 1G basée sur Intel 82576 : Prise en charge de SR-IOV sur toutes les distributions Linux prises en charge ; prise en charge de PCI Pass-Thru.
	  • Carte réseau 10G basée sur Intel 82599 : Prise en charge de SR-IOV sur toutes les distributions Linux prises en charge ; prise en charge de PCI Pass-Thru.
	  • Carte réseau Intel X710 10G : Prise en charge de SR-IOV sur toutes les distributions Linux prises en charge ; prise en charge de PCI Pass-Thru.
	  • Carte réseau Intel X722 10G : Prise en charge de SR-IOV sur toutes les distributions Linux prises en charge ; prise en charge de PCI Pass-Thru.
	  • Carte réseau 10G basée sur Broadcom 57112 et 578xx : Prise en charge de SR-IOV sur toutes les distributions Linux prises en charge ; pas de prise en charge de PCI Pass-Thru.
	  • Carte réseau Mellanox ConnectX5 10G/25G/50G/100G : Prise en charge de SR-IOV sur toutes les distributions Linux prises en charge.
	  • Reportez-vous à la section Versions de pilotes PacketMMAP dans la matrix de compatibilité.
	
	  Interfaces compatibles avec SR-IOV affectées au pare-feu VM-Series ; elles doivent être configurées en tant qu'interfaces de couche 3 ou interfaces HA.

©2023 Palo Alto Networks, Inc.

Options d'association du VM-Series sur le réseau



- Avec un pont Linux ou OVS, le trafic de données utilise le pont logiciel pour connecter des invités au même hôte. Pour la connectivité externe, le trafic de données utilise l'interface physique à laquelle le pont est associé.
- Avec le PCI Pass-Thru, le trafic de données est transmis directement entre l'invité et l'interface physique à laquelle il est associé. Lorsque l'interface est associée à un invité, elle n'est pas disponible pour l'hôte ou les autres invités sur l'hôte.
- Avec SR-IOV, le trafic de données est transmis directement entre l'invité et la fonction virtuelle à laquelle il est associé.

Conditions préalables du VM-Series sur KVM

Avant d'installer le pare-feu VM-Series sur le serveur Linux, consultez les sections suivantes :

- Préparation du serveur Linux
- Préparation au déploiement du pare-feu VM-Series

Préparation du serveur Linux

Avant d'installer le pare-feu VM-Series sur KVM, vérifiez que vous disposez d'un environnement Linux fonctionnel et que votre infrastructure réseau prend en charge la connectivité requise par le déploiement que vous avez choisi.

- Vérifier la prise en charge de Linux
- Vérifiez l'infrastructure du réseau
- Installer les outils logiciels Mellanox
- Activez les fonctions virtuelles pour les NIC Mellanox CX5 sur le pare-feu VM-Series sur KVM
- Vérifier la configuration de l'hôte

©2023 Palo Alto Networks, Inc.

Vérifier la prise en charge de Linux

Vérifiez que vous disposez de l'environnement approprié pour prendre en charge votre installation.

- Vérifiez la version de la distribution Linux. Pour une liste des versions prises en charge, reportez-vous à VM-Series pour KVM dans la matrice de compatibilité.
- Vérifiez que vous avez installé et configuré les outils KVM et modules nécessaires à la création et à la gestion des machines virtuelles, Libvirt par exemple.
- Si vous souhaitez utiliser un contrôleur de disque SCSI pour accéder au disque sur lequel le pare-feu VM-Series stocke des données, utilisez la commande virsh pour associer le contrôleur virtio-scsi au pare-feu VM-Series. Vous pouvez alors modifier le modèle XML du pare-feu VM-Series pour autoriser l'utilisation du contrôleur virtio-scsi. Pour obtenir des instructions, reportez-vous à la section Autorisation de l'utilisation d'un contrôleur SCSI.

  KVM sur Ubuntu 12.04 ne prend pas en charge le contrôleur virtio-scsi.

Vérifiez l'infrastructure du réseau

Vérifiez que vous avez configuré l'infrastructure de mise en réseau pour rediriger le trafic entre les invités et le pare-feu VM-Series, et pour vous assurez que vous disposez de la connectivité avec un serveur externe ou Internet. Le pare-feu VM-Series peut se connecter via un pont Linux, Open vSwitch, PCI Pass-Thru ou une carte réseau compatible avec SR-IOV.

- Vérifiez que la liaison de toutes les interfaces que vous envisagez d'utiliser est active. Vous devrez parfois activer manuellement l'interface.
- Si vous utilisez un pont Linux ou OVS, vérifiez que vous avez configuré les ponts nécessaires à l'envoi/la réception de trafic vers/depuis le pare-feu. Si ce n'est pas le cas, créez le ou les pont(s) et vérifiez que vous êtes prêt à installer le pare-feu.
- Si vous utilisez SR-IOV ou PCI Pass-Thru, vérifiez le PCI-ID de toutes les interfaces. Pour afficher la liste, utilisez la commande suivante :

  ```
  Virsh nodedev-list –tree
  ```

  Reportez-vous à la section Vérification du PCI-ID de commande d'interfaces réseau sur le pare-feu VM-Series.
- Si vous utilisez SR-IOV ou PCI-passthrough, vérifiez que les extensions de virtualisation (VT-d/IOMMU) sont activées dans le BIOS. Par exemple, pour activer IOMMU, `intel_iommu=on` doit être défini dans `/etc/grub.conf`. Pour obtenir des instructions, reportez-vous à la documentation fournie par le fournisseur de votre système.

©2023 Palo Alto Networks, Inc.

- Si vous utilisez PCI Pass-Thru, vérifiez que le pare-feu VM-Series dispose d'un accès exclusif à la ou aux interfaces que vous envisagez d'associer.

  Pour autoriser l'accès exclusif, vous devez détacher manuellement la ou les interface(s) du serveur Linux.

  `Virsh nodedev-detach <pci id of interface>`

  Par exemple :

  `Virsh nodedev-detach pci_0000_07_10_0`

  Dans certains cas, vous devrez peut-être modifier **`/etc/libvirt/qemu.conf`** et supprimer le commentaire **`relaxed_acs_check = 1`**.

- Si vous utilisez SR-IOV, vérifiez que la fonction virtuelle est activée pour chaque port que vous envisagez d'utiliser sur la carte réseau. Avec SR-IOV, un seul port Ethernet (fonction physique) peut être fractionné en plusieurs fonctions virtuelles. Un invité peut être mappé à une ou plusieurs fonctions virtuelles.

  Activez les fonctions virtuelles en procédant comme suit :

  1. Créer un nouveau fichier à l'emplacement suivant : **`/etc/modprobe.d/`**
  2. Utilisez vi pour modifier le fichier pour rendre les fonctions persistantes :

     `vim /etc/modprobe.d/igb.conf`
  3. Activer le nombre de fonctions virtuelles requises :

     `options igb max_vfs=4`

     Dans l'exemple ci-dessus, après avoir enregistré les modifications et redémarré le serveur Linux, chaque interface (ou fonction physique) aura 4 fonctions virtuelles.

  Reportez-vous à la documentation fournie par le fournisseur de votre réseau pour plus de détails sur le nombre réel de fonctions virtuelles prises en charge et les instructions pour activer les fonctions virtuelles.

Installer les outils logiciels Mellanox

Si vous utilisez une carte Mellanox CX5, installez les outils logiciels Mellanox sur l'hôte. Avant l'installation, vérifiez la prise en charge Linux et votre infrastructure réseau.

STEP 1 | À partir de l'hôte, téléchargez le package pour Mellanox OpenFabric Enterprise Distribution pour Linux (MLNX_OFED) pour la version de votre système d'exploitation sur le lien suivant :

https://www.mellanox.com/products/infiniband-drivers/linux/mlnx_ofed

STEP 2 | Exécutez la commande d'installation :

`mlnxofedinstall`

Si tous les packages prérequis sont installés, la commande ci-dessus installe tous les packages MLNX_OFED. Passez à l'étape 3.

Si votre environnement ne dispose pas des packages requis, l'installateur liste tous les packages que vous devez installer. Après avoir installé les packages, réexécutez la commande d'installation et passez à l'étape 3.

STEP 3 | Redémarrez l'hôte.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Vérifiez l'état des outils logiciels Mellanox.

```
# mst status MST modules:
 ------------------------------------------------------------------
   MST PCI module is not loaded   MST PCI
 configuration module loaded MST devices:
 ------------------------------------------------------------------ /
dev/mst/mt4121_pciconf0     - PCI configuration cycles access.
         domain:bus:dev.fn=0000:3b:00.0 addr.reg=88 data.reg=92
         Chip revision is: 00
```

STEP 5 | Assurez-vous que Mellanox est mis à jour sur la liste PCI :

```
# lspci | grep Mellanox 3b:00.0 Ethernet controller: Mellanox
 Technologies MT28800 Family [ConnectX-5 Ex] 3b:00.1 Ethernet
 controller: Mellanox Technologies MT28800 Family [ConnectX-5 Ex]
```

Activez les fonctions virtuelles pour les NIC Mellanox CX5 sur le pare-feu VM-Series sur KVM

Installez les outils logiciels Mellanox avant d'activer les fonctions virtuelles sur les NIC Mellanox Cx5.

STEP 1 | Assurez-vous que les outils logiciels Mellanox ont démarré.

STEP 2 | Activez le nombre de fonctions virtuelles requises. Par exemple :

```
mlxconfig -d /dev/mst/mt4121_pciconf0 set SRIOV_EN=1 NUM_OF_VFS=4
```

Après avoir enregistré les modifications et redémarré le serveur Linux, chaque interface (ou fonction physique) de l'exemple ci-dessus aura 4 fonctions virtuelles. Reportez-vous à la

©2023 Palo Alto Networks, Inc.

documentation fournie par le fournisseur de votre réseau pour plus de détails sur le nombre réel de fonctions virtuelles prises en charge et pour obtenir des instructions sur leur activation.

Il est possible que vous voyiez le message d'erreur suivant la première fois que vous activez les fonctions virtuelles sur les NIC Mellanox Cx5 :

```
[ 1429.841162] mlx5_core 0000:3b:00.1:
 mlx5_port_module_event:1025:(pid 0): Port module
 event[error]: module 1, Cable error, One or more network
 ports have been powered down due to insufficient/
unadvertised power on the PCIe slot. Veuillez vous
 reporter au manuel d'utilisation de la carte pour les
 spécifications d'alimentation ou contacter l'assistance
 Mellanox
```

Pour résoudre le problème, saisissez la séquence de commandes suivante sur le serveur Linux :

```
# mlxconfig -d <dev> set ADVANCED_POWER_SETTINGS=1 #
 mlxconfig -d <dev> set DISABLE_SLOT_POWER_LIMITER=1 #
 reboot
```

STEP 3 | Vérifiez l'état des fonctions virtuelles.

```
# cat /sys/class/net/enp59s0f1/device/sriov_numvfs
```

(Facultatif) Si les fonctions virtuelles ne sont pas configurées correctement (l'état est 0 ou vide), exécutez la commande suivante :

```
# echo 4 > /sys/class/net/enp59s0f1/device/sriov_numvfs
```

STEP 4 | Répertoriez les périphériques PCI de manière à ce qu'ils correspondent précisément au nombre de fonctions virtuelles chargées sur la fonction physique respective pour Mellanox :

```
# lspci | grep Mellanox 3b:00.0 Ethernet controller: Mellanox
 Technologies MT28800 Family [ConnectX-5 Ex] 3b:00.1 Ethernet
 controller: Mellanox Technologies MT28800 Family [ConnectX-5 Ex]
 3b:00.2 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex Virtual Function] 3b:00.3 Ethernet controller:
 Mellanox Technologies MT28800 Family [ConnectX-5 Ex Virtual
 Function] 3b:00.4 Ethernet controller: Mellanox Technologies
 MT28800 Family [ConnectX-5 Ex Virtual Function] 3b:00.5 Ethernet
 controller: Mellanox Technologies MT28800 Family [ConnectX-5
 Ex Virtual Function] 3b:00.6 Ethernet controller: Mellanox
 Technologies MT28800 Family [ConnectX-5 Ex Virtual Function]
 3b:00.7 Ethernet controller: Mellanox Technologies MT28800 Family
```


©2023 Palo Alto Networks, Inc.

```
[ConnectX-5 Ex Virtual Function] 3b:01.0 Ethernet controller:
Mellanox Technologies MT28800 Family [ConnectX-5 Ex Virtual
Function] 3b:01.1 Ethernet controller: Mellanox Technologies
MT28800 Family [ConnectX-5 Ex Virtual Function]
```

Vérifier la configuration de l'hôte

Configurez l'hôte pour optimiser les performances de VM-Series. Reportez-vous à la section Réglage des performances de VM-Series pour KVM pour plus d'informations sur la configuration de chaque option ci-dessous.

- **Activez DPDK**. DPDK permet à l'hôte de traiter les paquets plus rapidement en contournant le noyau Linux. Au lieu de cela, les interactions avec la carte réseau sont effectuées à l'aide des pilotes et des bibliothèques DPDK. Open vSwitch est requis pour utiliser DPDK avec le pare-feu VM-Series.
- **Activez SR-IOV**. La virtualisation d'E/S racine unique (SR-IOV) permet à un périphérique physique PCIe unique sous un port racine unique d'apparaître comme plusieurs périphériques physiques distincts de l'hyperviseur ou de l'invité.
- **Activez la prise en charge de files d'attente multiples pour les cartes d'interface réseau**. Virtio-net à files d'attente multiples permet aux performances du réseau d'évoluer avec le nombre de processeurs virtuels et permet le traitement parallèle des paquets en créant plusieurs files d'attente TX et RX.
- **Isolation des ressources du processeur dans un nœud NUMA**. Vous pouvez améliorer les performances de VM-Series sur KVM en isolant les ressources du processeur de la machine virtuelle invitée sur un seul nœud NUMA (Non-Uniform Memory Access).

Préparation au déploiement du pare-feu VM-Series

- Achetez le modèle VM-Series et enregistrez le code d'autorisation sur le site Internet d'assistance client de Palo Alto Networks. Reportez-vous aux sections Création d'un compte de support et Enregistrer le pare-feu VM-Series.
- Obtenez l'image qcow2 et enregistrez-la sur le serveur Linux. Selon la procédure recommandée, copiez l'image dans le dossier suivant : /var/lib/libvirt/qemu/images.

  Si vous envisagez de déployer plusieurs instances du pare-feu VM-Series, effectuez le nombre de copies nécessaire de l'image. Chaque instance du pare-feu VM-Series conservant une liaison avec l'image .qcow2 utilisée pour déployer le pare-feu, pour éviter tout problème de corruption de données, assurez-vous que chaque image est indépendante et utilisée par une seule instance du pare-feu.

©2023 Palo Alto Networks, Inc.

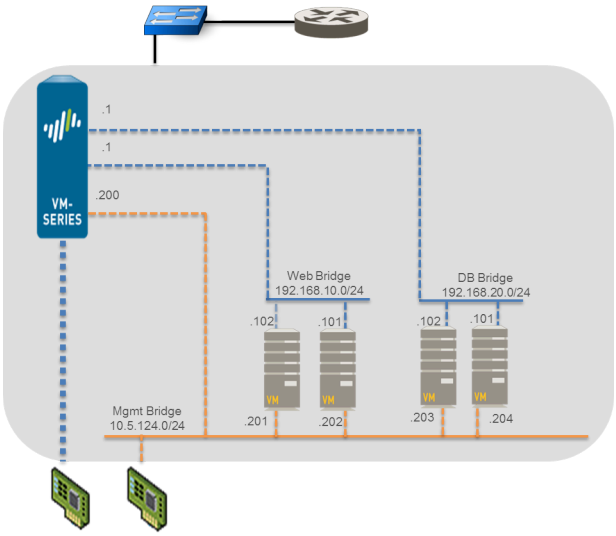
Déploiements pris en charge sur KVM

Vous pouvez déployer une instance du pare-feu VM-Series par hôte Linux (un locataire) ou plusieurs instances de pare-feu VM-Series sur un hôte Linux. Le pare-feu VM-Series peut être déployé avec des interfaces Virtual Wire, de Couche 2, ou de Couche 3. Si vous envisagez d'utiliser des interfaces compatibles avec SR-IOV sur le pare-feu VM-Series, vous ne pouvez configurer les interfaces qu'en tant qu'interfaces de couche 3.

- Sécurisation du trafic sur un hôte
- Sécurisation du trafic entre des hôtes Linux

Sécurisation du trafic sur un hôte

Pour sécuriser le trafic est-ouest entre les invités sur un serveur Linux, le pare-feu VM-Series peut être déployé avec des interfaces Virtual Wire, de Couche 2, ou de Couche 3. L'illustration ci-dessous montre le pare-feu avec des interfaces de couche 3, dans laquelle le pare-feu et les autres invités sont connectés via des ponts Linux. Dans ce déploiement, l'ensemble du trafic entre les serveurs Web et les serveurs de base de données est acheminé via le pare-feu ; le trafic entre les serveurs de base de données uniquement ou entre les serveurs Web uniquement est traité par le pont et n'est pas acheminé via le pare-feu.

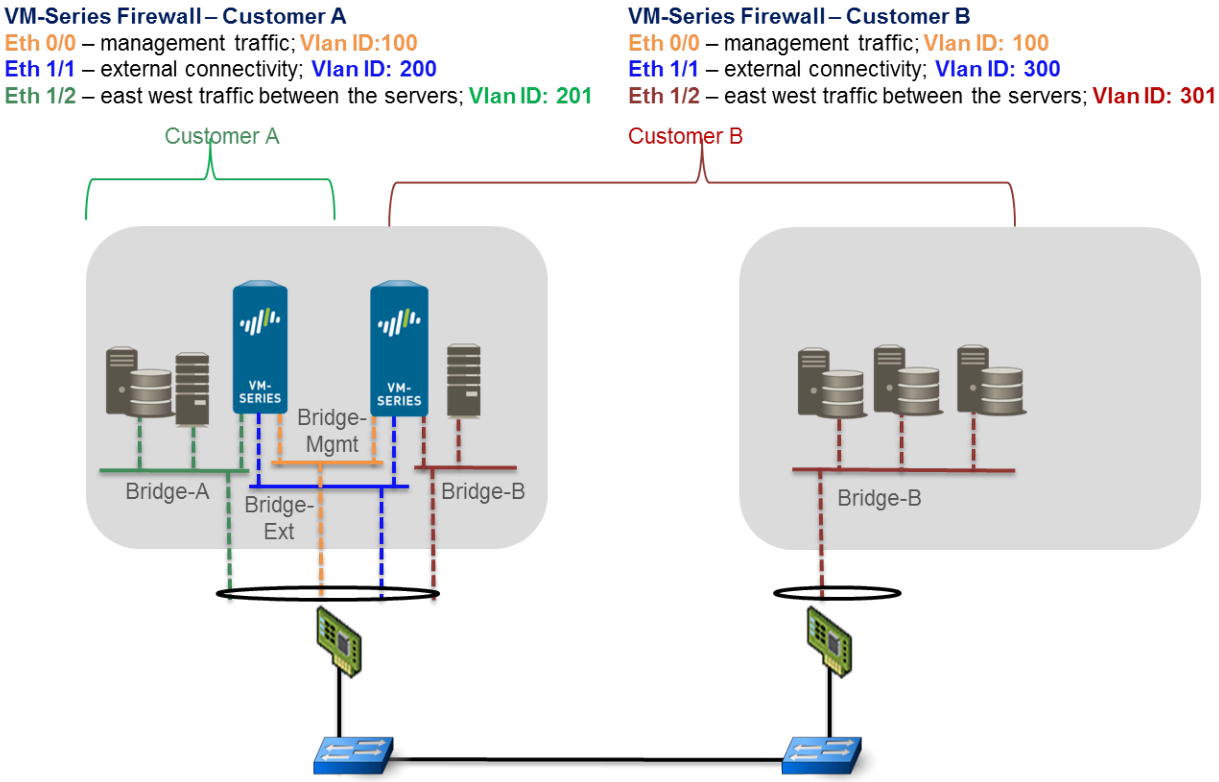


Sécurisation du trafic entre des hôtes Linux

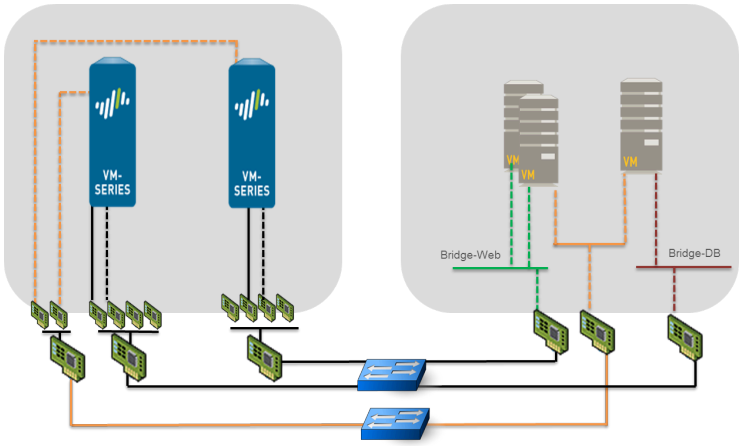
Pour sécuriser vos charges de travail, plusieurs instances de pare-feu VM-Series peuvent être déployées sur un hôte Linux. Par exemple, si vous souhaitez isoler le trafic de services ou clients distincts, vous pouvez utiliser des balises VLAN

pour isoler logiquement du trafic réseau et l'acheminer vers le pare-feu VM-Series approprié. Dans l'exemple suivant, un hôte Linux héberge les pare-feu VM-Series pour deux clients, Client A et Client B, et la charge de travail du Client B est répartie entre deux serveurs. Pour isoler le trafic et le diriger vers le pare-feu VM-Series configuré pour chaque client, des VLAN sont utilisés.

©2023 Palo Alto Networks, Inc.



Dans une autre variation de ce déploiement, une paire de pare-feu VM-Series est déployée dans une configuration haute disponibilité. Les pare-feu VM-Series dans l'illustration suivante sont déployés sur un serveur Linux avec des cartes compatibles avec SR-IOV. Avec SR-IOV, un seul port Ethernet (fonction physique) peut être fractionné en plusieurs fonctions virtuelles. Chaque fonction virtuelle associée au pare-feu VM-Series est configurée en tant qu'interface de couche 3. L'homologue actif de la paire HA sécurise le trafic acheminé depuis les invités déployés sur un autre serveur Linux.



©2023 Palo Alto Networks, Inc.

Installation du pare-feu VM-Series sur KVM

L'API libvirt utilisée pour gérer KVM inclut un ensemble d'outils vous permettant de créer et de gérer des machines virtuelles. Pour installer le pare-feu VM-Series sur KVM, vous pouvez utiliser l'une des méthodes suivantes.

- virt-manager : déployez VM-Series à l'aide du gestionnaire de machine virtuelle virt-manager. Virt-manager fournit un assistant pratique pour vous aider tout au long du processus d'installation.
- virsh : déployez VM-Series à l'aide de la ligne de commande KVM. Créez un fichier XML définissant l'instance de la machine virtuelle et un fichier XML d'amorçage définissant les paramètres de configuration initiaux du pare-feu. Installez ensuite le pare-feu en montant une image ISO en tant que CD-ROM.
- virt-install : une autre option pour déployer le pare-feu VM-Series à l'aide de la ligne de commande KVM. Utilisez cette option pour créer la définition du pare-feu VM-Series et l'installer.

Ce document décrit les étapes à suivre pour installer le pare-feu VM-Series sur KVM à l'aide de virt-manager et de virsh.

- Installation du pare-feu VM-Series à l'aide de Virt-Manager
- Installation du pare-feu VM-Series à l'aide d'une ISO
- Utilisation de la CLI du VM-Series pour permuter l'interface de gestion sur KVM
- Autorisation de l'utilisation d'un contrôleur SCSI
- Vérification du PCI-ID de commande d'interfaces réseau sur le pare-feu VM-Series

Installation du pare-feu VM-Series à l'aide de Virt-Manager

Appliquez la procédure suivante qui utilise virt-manager pour installer le pare-feu VM-Series sur un serveur exécutant KVM sur RHEL.

- Configuration du pare-feu VM-Series sur un hôte KVM
- Configuration initiale du pare-feu VM-Series sur KVM

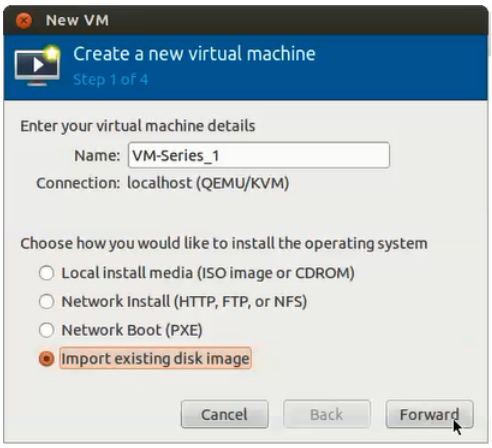
Configuration du pare-feu VM-Series sur un hôte KVM

Utilisez les instructions suivantes pour provisionner l'hôte KVM pour le pare-feu VM-Series.

©2023 Palo Alto Networks, Inc.

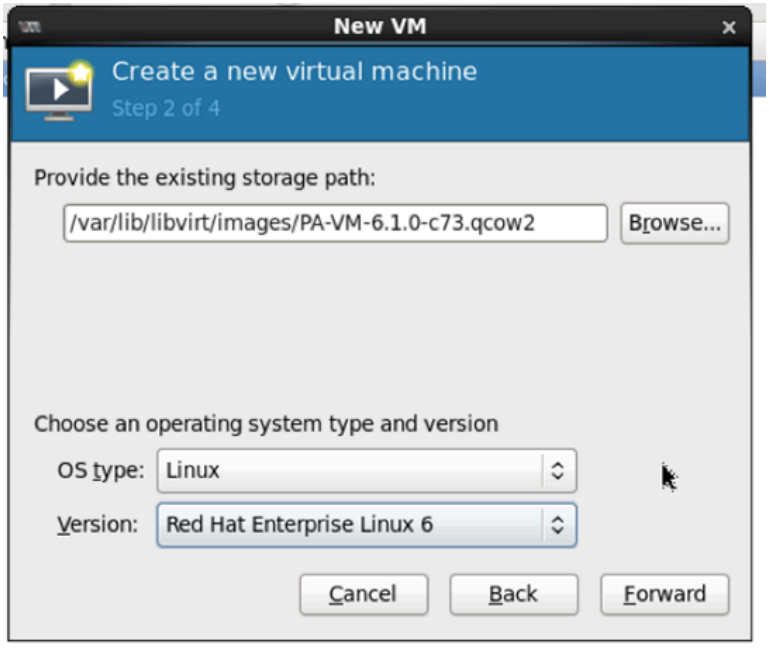
STEP 1 | Créez une nouvelle machine virtuelle et ajoutez le pare-feu VM-Series pour l'image KVM à virt-mgr.

1. Sur Virt-manager, sélectionnez **Create a new virtual machine (Créer une nouvelle machine virtuelle)**.
2. Donnez un **Name (Nom)** descriptif au pare-feu VM-Series.



3. Sélectionnez **Import existing disk image (Importer une image de disque existante)**, recherchez l'image, puis définissez l'**OS Type (Type de système d'exploitation)** : Linux et la **Version** : Red Hat Enterprise Linux 6.

Si vous préférez, vous pouvez conserver le type et la version du système d'exploitation Generic (Générique).

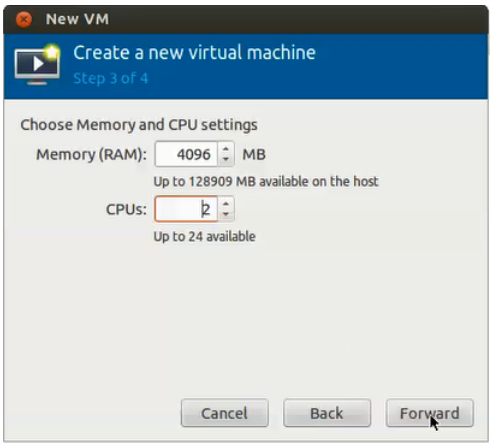


4. Pour ajouter des cartes réseau pour les interfaces de données :

 ©2023 Palo Alto Networks, Inc.

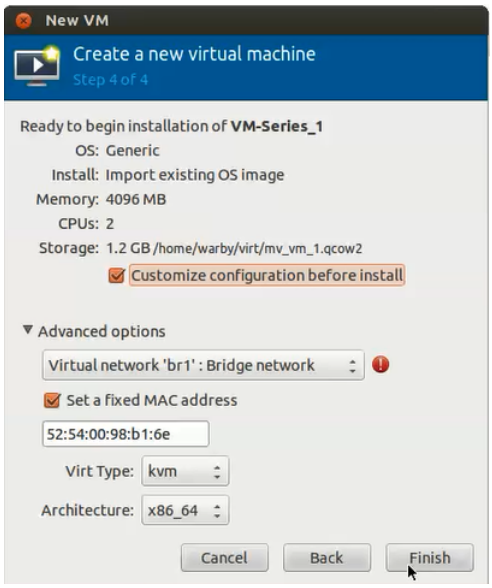
STEP 2 | Configurez les paramètres du processeur et de la mémoire.

1. Définissez la **Memory (Mémoire)** sur la mémoire minimale en fonction de la Configuration système requise pour VM-Series de votre modèle VM-Series.
2. Définissez le **CPU (Processeur)** sur les processeurs minimaux en fonction de la Configuration système requise pour VM-Series de votre modèle VM-Series.



STEP 3 | Activez la personnalisation de la configuration et sélectionnez le pont de l'interface de gestion.

1. Sélectionnez **Customize configuration before install (Personnaliser la configuration avant d'installer)**.
2. Sous Advanced options (Options avancées), sélectionnez le pont pour l'interface de gestion, et acceptez les valeurs par défaut.



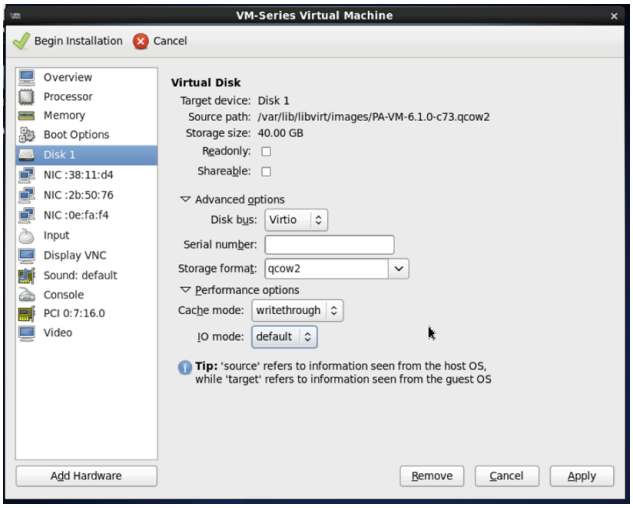
 ©2023 Palo Alto Networks, Inc.

STEP 4 | Configurez les paramètres du disque virtuel.

1. Sélectionnez **Disk (Disque)**, développez Advanced options (Options avancées) et sélectionnez le **Storage format (Format de stockage)** qcow2 et le **Disk Bus (Bus de disque)** Virtio ou IDE en fonction de votre configuration.

   Si vous voulez utiliser un bus de disque SCSI, reportez-vous à la section Autorisation de l'utilisation d'un contrôleur SCSI.

2. Développez Performance options (Options de performances) et définissez le **Cache mode (Mode cache)** pour sur **writethrough (double écriture)**. Ce paramètre réduit la durée d'installation et optimise la vitesse d'exécution sur le pare-feu VM-Series.



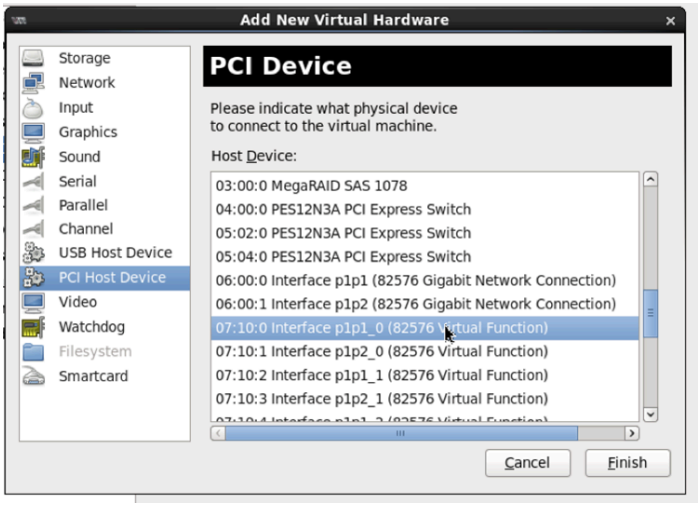
 ©2023 Palo Alto Networks, Inc.

STEP 5 | Configurez les cartes réseau.

1. Sélectionnez **Add Hardware (Ajouter un matériel)** > **Network (Réseau)** si vous utilisez un pont logiciel comme le pont Linux ou l'Open vSwitch.
2. Pour le **Host Device (Périphérique hôte)**, saisissez le nom du pont ou sélectionnez-le dans la liste déroulante.
3. Pour spécifier le pilote, définissez le **Device Model (Modèle de périphérique)** sur e-1000 ou virtio. Ce sont les seuls types d'interface virtuelle pris en charge.



4. Sélectionnez **Add Hardware (Ajouter un matériel)** > **PCI Host Device (Périphérique hôte PCI)** pour PCI Pass-Thru ou un périphérique compatible avec SR-IOV.

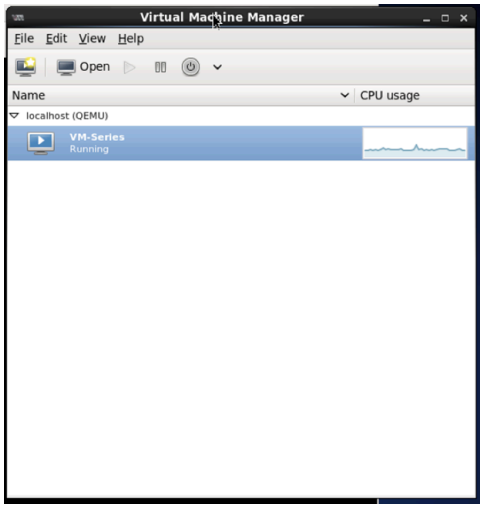


5. Dans la liste **Host Device (Périphérique hôte)**, sélectionnez l'interface sur la carte ou la fonction virtuelle.
6. Cliquez sur **Apply (Appliquer)** ou **Finish (Terminer)**.

©2023 Palo Alto Networks, Inc.

STEP 6 | Cliquez sur **Begin Installation (Démarrer l'installation)** Begin Installation. Patientez 5 à 7 minutes que l'installation se termine.

Par défaut, le modèle XML du pare-feu VM-Series est créé et stocké dans etc/libvirt/qemu.



STEP 7 | (Facultatif) Amorcez le pare-feu VM-Series.

Si vous utilisez l'amorçage pour effectuer la configuration de votre pare-feu VM-Series sur KVM, reportez-vous à la section Amorçage du pare-feu VM-Series sur KVM. Pour plus d'informations sur l'amorçage, reportez-vous à la section Amorçage du pare-feu VM-Series.

STEP 8 | Configurez les paramètres d'accès réseau pour l'interface de gestion.

1. Ouvrez une connexion à la console.
2. Connectez-vous au pare-feu avec le nom d'utilisateur/mot de passe par défaut : admin/admin.
3. Passez en mode Configuration en utilisant la commande suivante :

```
configure
```

4. Utilisez les commandes suivantes pour configurer l'interface de gestion :

1.
```
set deviceconfig system type static
```

2.
```
set deviceconfig system ip-address <Firewall-IP>
 netmask <netmask> default-gateway <gateway-IP> dns-setting
 servers primary <DNS-IP>
```

où *<Firewall-IP>* est l'adresse IP que vous voulez affecter à l'interface de gestion, *<netmask>* est le masque de sous-réseau, *<gateway-IP>* est l'adresse IP de la passerelle réseau et *<DNS-IP>* est l'adresse IP du serveur DNS.

3.
```
commit
```

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Vérifiez les ports sur l'hôte qui sont mappés aux interfaces sur le pare-feu VM-Series. Afin de vérifier l'ordre des interfaces sur l'hôte Linux, reportez-vous à la section Vérification du PCI-ID de commande d'interfaces réseau sur le pare-feu VM-Series.

Pour vous assurer que le trafic est géré par l'interface appropriée, utilisez la commande suivante pour identifier les ports sur l'hôte qui sont mappés aux ports sur le pare-feu VM-Series.

```
admin@PAN-VM> debug show vm-series interfaces all Phoenix_interface
 Base-OS_port Base-OS_MAC PCI-ID mgt                              eth0
 52:54:00:d7:91:52 0000:00:03.0 Ethernet1/1 eth1 52:54:00:fe:8c:80
 0000:00:06.0 Ethernet1/2 eth2 0e:c6:6b:b4:72:06 0000:00:07.0
 Ethernet1/3 eth3 06:1b:a5:7e:a5:78 0000:00:08.0 Ethernet1/4 eth4
 26:a9:26:54:27:a1 0000:00:09.0 Ethernet1/5 eth5 52:54:00:f4:62:13
 0000:00:10.2
```

STEP 10 | Accédez à l'interface Web du pare-feu VM-Series, puis configurez les interfaces et définissez des règles de sécurité et des règles NAT afin d'activer en toute sécurité les applications que vous souhaitez sécuriser.

Reportez-vous au Guide de l'administrateur PAN-OS.

Configuration initiale du pare-feu VM-Series sur KVM

Utilisez la console d'appareil virtuel sur le serveur KVM pour configurer l'accès réseau au pare-feu VM-Series. Par défaut, le pare-feu VM-Series utilise DHCP pour obtenir une adresse IP pour l'interface de gestion. Cependant, vous pouvez attribuer une adresse IP statique. Une fois la configuration initiale terminée, accédez à l'interface Web pour effectuer d'autres tâches de configuration. Si vous utilisez Panorama pour la gestion centralisée, reportez-vous auGuide de l'administrateur Panorama pour plus d'informations sur la gestion du périphérique à l'aide de Panorama.

Si vous utilisez l'amorçage pour effectuer la configuration de votre pare-feu VM-Series sur KVM, reportez-vous à la section Amorçage du pare-feu VM-Series sur KVM.

Pour des informations générales sur l'amorçage, reportez-vous à la section Amorçage du pare-feu VM-Series.

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

- Adresse IP du port MGT
- netmask
- Passerelle par défaut
- Adresse IP du serveur DNS

STEP 2 | Accédez à la console du pare-feu VM-Series.

1. Cliquez sur l'onglet **Console** sur le serveur KVM pour le pare-feu VM-Series, ou faites un clic droit dur le pare-feu VM-Series et sélectionnez **Open Console (Ouvrir la console)**.
2. Appuyez sur Entrée pour accéder à l'écran de connexion.
3. Saisissez le nom d'utilisateur/mot de passe (admin/admin) par défaut pour vous connecter.
4. Entrer **`configurer`** pour passer en mode de configuration.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configurez les paramètres d'accès réseau pour l'interface de gestion.

Entrez les commandes suivantes :

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> netmask <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

STEP 4 | Validez vos modifications et quittez le mode Configuration.

Saisissez **commit**.

Saisissez **exit**.

Installation du pare-feu VM-Series à l'aide d'une ISO

Créez manuellement la définition XML du pare-feu VM-Series, puis utilisez virsh pour importer la définition en tant qu'ISO. Virsh est l'outil le plus puissant vous permettant de gérer intégralement la machine virtuelle.

- Utilisation d'un fichier ISO pour déployer le pare-feu VM-Series
- Exemple de fichier XML pour le pare-feu VM-Series

Utilisation d'un fichier ISO pour déployer le pare-feu VM-Series

Si vous souhaitez transmettre un script au pare-feu VM-Series au démarrage, vous pouvez monter un CD-ROM avec un fichier ISO. Le fichier ISO vous permet de définir un fichier XML d'amorçage incluant les paramètres de configuration initiale du port de gestion du pare-feu. Au premier démarrage, le pare-feu VM-Series consulte le fichier **bootstrap-networkconfig.xml** et utilise ses valeurs.

Si une seule erreur se produit lors de l'analyse du fichier d'amorçage, le pare-feu VM-Series rejette l'ensemble de la configuration définie dans ce fichier et démarre avec les valeurs par défaut.

STEP 1 | Créez le fichier XML et définissez-le en tant qu'instance de machine virtuelle.

Pour un exemple de fichier, consultez Exemple de fichier XML pour le pare-feu VM-Series.

Dans cet exemple, le pare-feu VM-Series est nommé PAN_Firewall_DC1.

Par exemple :

```
user-PowerEdge-R510:~/kvm_script$ sudo vi /etc/libvirt/qemu/
PAN_Firewall_DC1.xml user-PowerEdge-R510:~/kvm_script$ sudo
 virsh define/etc/libvirt/qemu/PAN_Firewall_DC1.xml Domain
 PAN_Firewall_DC1_bootstp defined from /etc/libvirt/qemu/
PAN_Firewall_DC1.xml user-PowerEdge-R510:~/kvm_script$
 sudo virsh -q attach-interface PAN_Firewall_DC1_bootstp
 bridge br1 --model=virtio --persistent user-PowerEdge-
R510:~/kvm_script$ virsh list --all Id Name State
```


©2023 Palo Alto Networks, Inc.

```
 ------------------------------------------- -
 PAN_Firewall_DC1_bootstp shut off
```

STEP 2 | Créez le fichier XML d'amorçage.

Vous pouvez définir les paramètres de configuration initiale dans ce fichier et le nommer bootstrap-networkconfig.

Si vous ne souhaitez pas inclure un paramètre, panorama-server-secondary par exemple. Supprimez toute la ligne du fichier. Si vous laissez le champ d'adresse IP vide, le fichier ne sera pas correctement analysé.

Utilisez l'exemple suivant comme modèle pour le fichier bootstrap-networkconfig. Le fichier bootstrap-networkconfig ne peut inclure que les paramètres suivants :

```
<vm-initcfg> <hostname>VM_ABC_Company</hostname> <ip-
address>10.5.132.162</ip-address> <netmask>255.255.254.0</
netmask> <default-gateway>10.5.132.1</default-gateway> <dns-
primary>10.44.2.10</dns-primary> <dns-secondary>8.8.8.8</dns-
secondary> <panorama-server-primary>10.5.133.4</panorama-server-
primary> <panorama-server-secondary>10.5.133.5</panorama-server-
secondary> </vm-initcfg>
```

STEP 3 | Créez le fichier ISO. Dans cet exemple, nous utilisons mkisofs.

Enregistrez le fichier ISO dans le répertoire d'images (/var/lib/libvirt/image) ou le répertoire qemu (/etc/libvirt/qemu) pour vous assurer que le pare-feu a accès en lecture au fichier ISO.

Par exemple :

```
# mkisofs -J -R -v -V "Bootstrap" -A "Bootstrap" -ldots -l -
allow-lowercase -allow-multidot -o <iso-filename> bootstrap-
networkconfig.xml
```

STEP 4 | Associez le fichier ISO au lecteur de CD-ROM.

Par exemple :

```
# virsh -q attach-disk <vm-name> <iso-filename> sdc --type cdrom --
mode readonly –persistent\
```

Exemple de fichier XML pour le pare-feu VM-Series

```
<?xml version="1.0"?> <domain type="kvm"> <name>PAN_Firewall_DC1</
name> <memory>4194304</memory> <currentMemory>4194304</currentMemory>
 <vcpu placement="static">2</vcpu> <os> <type arch="x86_64">hvm</
type> <boot dev="hd"/> </os> <features> <acpi/> <apic/> <pae/> </
features> <clock offset="utc"/> <on_poweroff>destroy</on_poweroff>
 <on_reboot>restart</on_reboot> <on_crash>restart</on_crash>
 <devices> <emulator>/usr/libexec/qemu-kvm</emulator> <disk
```

 ©2023 Palo Alto Networks, Inc.

```
 type="file" device="disk"> <driver type="qcow2" name="qemu"/>
 <source file="/var/lib/libvirt/images/panos-kvm.qcow2"/> <target
 dev="vda" bus="virtio"/> </disk> <controller type="usb" index="0"/
> <controller type="ide" index="0"/> <controller type="scsi"
 index="0"/> <serial type="pty"> <source path="/dev/pts/1"/> <target
 port="0"/> <alias name="serial0"/> </serial> <console type="pty"
 tty="/dev/pts/1"> <source path="/dev/pts/1"/> <target type="serial"
 port="0"/> <alias name="serial0"/> </console> <input type="mouse"
 bus="ps2"/> <graphics type="vnc" port="5900" autoport="yes"/> </
devices> </domain>
```

*Pour modifier le nombre de processeurs virtuels (vCPU) affectés sur le pare-feu VM-Series, changez la valeur **2** en **4** ou **8** vCPUs dans cette ligne de l'exemple de fichier XML :*

```
<vcpu placement="static">2</vcpu>
```

Utilisation de la CLI du VM-Series pour permuter l'interface de gestion sur KVM

Par défaut, le pare-feu VM-Series affecte la première interface (eth0) comme interface de gestion. Toutefois, dans certains déploiements, la première interface doit être pré-mappée à une adresse IP publique. Par conséquent, l'interface de gestion doit être affectée à une interface différente. L'attribution d'une adresse IP publique à l'interface de gestion constitue un risque de sécurité.

Vous pouvez également activer l'échange d'interface de gestion dans le cadre de Composants du fichier init-cfg.txt *pendant l'amorçage.*

STEP 1 | Connectez-vous à la CLI du pare-feu VM-Series et saisissez la commande suivante :

```
set system setting mgmt-interface-swap enable yes
```

STEP 2 | Confirmez que vous voulez permuter l'interface et utiliser l'interface du dataplane eth1 comme interface de gestion.

STEP 3 | Redémarrez le pare-feu pour que la permutation prenne effet. Utilisez la commande suivante :

```
request restart system
```

STEP 4 | Vérifiez que les interfaces ont été permutées. Utilisez la commande suivante :

```
debug show vm-series interfaces all Phoenix_interface   Base-
OS_port   Base-OS_MAC        PCI-ID         Driver mgt(interface-
swap) eth0   0e:53:96:91:ef:29   0000:00:04.0   ixgbevf Ethernet1/1
          eth1    0e:4d:84:5f:7f:4d       0000:00:03.0   ixgbevf
```

Autorisation de l'utilisation d'un contrôleur SCSI

Si vous souhaitez que le pare-feu VM-Series utilise le type de bus de disque SCSI pour accéder au disque virtuel, suivez les instructions ci-dessous pour associer le contrôleur virtio-scsi au pare-feu, puis autorisez l'utilisation du contrôleur virtio-scsi.

 ©2023 Palo Alto Networks, Inc.

KVM sur Ubuntu 12.04 ne prend pas en charge le contrôleur virtio-scsi ; le contrôleur virtio-scsi ne peut être activé que sur le pare-feu VM-Series exécuté sur RHEL ou CentOS.

Ce processus requiert virsh car le gestionnaire Virt ne prend pas en charge le contrôleur virtio-scsi.

STEP 1 | Créez un fichier XML pour le contrôleur SCSI. Dans cet exemple, il est nommé virt-scsi.xml.

```
[root@localhost~]# cat /root/virt-scsi.xml <controller type='scsi'
 index='0' model='virtio-scsi'> <address type='pci' domain='0x0000'
 bus='0x00' slot='0x0b'function='0x0'/> </controller>
```

Assurez-vous que le logement utilisé pour le contrôleur virtio-scsi n'est pas en conflit avec un autre périphérique.

STEP 2 | Associez ce contrôleur au modèle XML du pare-feu VM-Series.

```
[root@localhost~]# virsh attach-device --config <VM-Series_name> /
root/virt-scsi.xml Device attached successfully
```

STEP 3 | Autorisez le pare-feu à utiliser le contrôleur SCSI.

```
[root@localhost~]# virsh attach-disk <VM-Series_name>/var/
lib/libvirt/images/PA-VM-6.1.0-c73.qcow2 sda --cache none --
persistent Disk attached successfully
```

STEP 4 | Modifiez le modèle XML du pare-feu VM-Series. Dans le modèle XML, modifiez le disque cible et le bus de disque utilisés par le pare-feu.

Par défaut, le modèle XML est stocké dans etc/libvirt/qemu.

```
<disk type='file' device='disk'> <driver name='qemu' type='qcow2'
 cache='writeback'/> <source file='/var/lib/libvirt/images/PA-
VM-7.0.0-c73.qcow2'/> <target dev='sda' bus='scsi'/> <address
 type='drive' controller='0' bus='0' target='0' unit='0'/> </disk>
```

Vérification du PCI-ID de commande d'interfaces réseau sur le pare-feu VM-Series

Que vous utilisiez une interface virtuelle (pont Linux/OVS) ou un périphérique PCI (PCI Pass-Thru ou une carte compatible avec SR-IOV) pour la connectivité au pare-feu VM-Series, ce dernier traite l'interface comme un périphérique PCI. L'affectation d'une interface sur le pare-feu VM-Series est basée sur le PCI-ID, une valeur combinant le bus, périphérique ou logement, et la fonction de l'interface. Les interfaces sont classées en commençant par le plus petit PCI-ID, ce qui signifie que l'interface de gestion (eth0) du pare-feu est affectée à l'interface avec le plus petit PCI-ID.

Supposons que vous affectez quatre interfaces au pare-feu VM-Series : trois interfaces virtuelles de type virtio et e1000, la quatrième étant un périphérique PCI. Pour afficher le PCI-ID de chaque

 ©2023 Palo Alto Networks, Inc.

interface, saisissez la commande **virsh dumpxml $ domain *<name of the VM-Series firewall>*** sur l'hôte Linux pour afficher la liste des interfaces associées au pare-feu VM-Series. Dans le résultat, vérifiez la configuration de mise en réseau suivante :

```
<interface type='bridge'> <mac address='52:54:00:d7:91:52'/> <source
 bridge='mgmt-br'/> <model type='virtio'/> <address type='pci'
 domain='0x0000' bus='0x00' slot='0x03' function='0x0'/> </interface>
 <interface type='bridge'> <mac address='52:54:00:f4:62:13'/>
 <source bridge='br8'/> <model type='e1000'/> <address type='pci'
 domain='0x0000' bus='0x00' slot='0x10' function='0x0'/> </interface>
 <interface type='bridge'> <mac address='52:54:00:fe:8c:80'/>
 <source bridge='br8'/> <model type='e1000'/> <address type='pci'
 domain='0x0000' bus='0x00' slot='0x06' function='0x0'/> </interface>
 <hostdev mode='subsystem' type='pci' managed='yes'> <source>
 <address domain='0x0000' bus='0x08' slot='0x10' function='0x1'/> </
source> <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
 function='0x0'/> </hostdev>
```

Dans cet exemple, le PCI-ID pour chaque interface est le suivant :

- PCI-ID de la première interface virtuelle : 00:03:00
- PCI-ID de la deuxième interface virtuelle : 00:10:00
- PCI-ID de la troisième interface virtuelle : 00:06:00
- PCI-ID de la quatrième interface virtuelle : 00:07:00

Ainsi, sur le pare-feu VM-Series, l'interface avec le PCI-ID 00:03:00 est affectée à eth0 (interface de gestion), l'interface avec le PCI-ID 00:06:00 à eth1 (ethernet1/1), l'interface avec le PCI-ID 00:07:00 à eth2 (ethernet1/2) et l'interface avec le PCI-ID 00:10:00 à eth3 (ethernet1/3).

 ©2023 Palo Alto Networks, Inc.

Réglage des performances de VM-Series pour KVM

Le pare-feu VM-Series pour KVM est un appareil haute performance, mais il peut nécessiter un réglage de l'hyperviseur pour obtenir les meilleurs résultats. Cette section décrit quelques bonnes pratiques et recommandations pour faciliter les meilleures performances du pare-feu VM-Series.

KVM utilise par défaut un pont Linux pour la mise en réseau des machines virtuelles. Cependant, les meilleures performances dans un environnement virtuel sont réalisées avec des interfaces d'E/S dédiées (PCI Pass-Thru ou SR-IOV). Si un commutateur virtuel est requis, utilisez un commutateur virtuel optimisé pour les performances (tel qu'Open vSwitch avec DPDK).

- Installation de KVM et Open vSwitch sur Ubuntu 16.04.1 LTS
- Activation d'Open vSwitch sur KVM
- Intégration d'Open vSwitch avec DPDK
- Activation de SR-IOV sur KVM
- Activation du mode d'accès VLAN (réseau local virtuel) avec SR-IOV
- Activation de la prise en charge de files d'attente multiples pour les cartes réseau sur KVM
- Isolation des ressources du processeur dans un nœud NUMA sur KVM

Installation de KVM et Open vSwitch sur Ubuntu 16.04.1 LTS

Pour faciliter l'installation, Ubuntu 16.04.1 LTS est recommandé comme plate-forme d'hyperviseur KVM.

STEP 1 | Installez KVM et OVS.

1. Connectez-vous à la CLI Ubuntu.
2. Exécutez les commandes suivantes :

```
$ sudo apt-get install qemu-kvm libvirt-bin ubuntu-vm-builder
 bridge-utils $ sudo apt-get install openvswitch-switch
```

STEP 2 | Vérifiez et comparez les versions des paquets pertinents.

Exécutez les commandes suivantes :

```
$ virsh --version 1.3.1 $ libvirtd --version libvirtd (libvirt)
 1.3.1 $ /usr/bin/qemu-system-x86_64 --version QEMU emulator
 version 2.5.0 (Debian 1:2.5+dfsg-5ubuntu10.6), Copyright (c)
 2003-2008 Fabrice Bellard $ ovs-vsctl --version ovs-vsctl (Open
 vSwitch) 2.5.0 Compiled Mar 10 2016 14:16:49 DB Schema 7.12.1
```

Activation d'Open vSwitch sur KVM

Activez OVS en modifiant les paramètres du réseau de définition XML de l'invité.

Modifiez la définition XML de l'invité comme suit.

 ©2023 Palo Alto Networks, Inc.

```
[...] <interface type='bridge'> <mac address='52:54:00:fb:00:01'/>
 <source bridge='ovsbr0'/> <virtualport type='openvswitch'/> <model
 type='virtio'/> <address type='pci' domain='0x0000' bus='0x00'
 slot='0x03' function='0x0'/> </interface> [...]
```

Intégration d'Open vSwitch avec DPDK

Pour intégrer Open vSwitch (OVS) avec DPDK, vous devez installer les composants requis, puis configurer OVS. DPDK est activé par défaut sur le pare-feu VM-Series pour KVM.

- Installation de QEMU, DPDK et OVS sur Ubuntu
- Configuration d'OVS et de DPDK sur l'hôte
- Modification du fichier de configuration du pare-feu VM-Series

Installation de QEMU, DPDK et OVS sur Ubuntu

Avant de pouvoir activer DPDK sur OVS, vous devez installer QEMU 2.5.0, DPDK 2.2.0 et OVS 2.5.1. Effectuez les procédures suivantes pour installer les composants.

STEP 1 | Connectez-vous à la CLI de l'hôte KVM.

STEP 2 | Installez QEMU 2.5.0 en exécutant les commandes suivantes :

```
apt-get install build-essential gcc pkg-config glib-2.0 libglib2.0-
dev libsdl1.2-dev libaio-dev libcap-dev libattr1-dev libpixman-1-
dev apt-get build-dep qemu apt-get install qemu-kvm libvirt-bin
 wget http://wiki.qemu.org/download/qemu-2.5.0.tar.bz2 tar xjvf
 qemu-2.5.0.tar.bz2 cd qemu-2.5.0 ./configure make make install
```

STEP 3 | Installez dpdk-2.2.0.

1. Exécutez les commandes suivantes :

   ```
   wget http://dpdk.org/browse/dpdk/snapshot/dpdk-2.2.0.tar.gz
    tar xzvf dpdk-2.2.0.tar.gz cd dpdk-2.2.0 vi config/
   common_linuxapp
   ```

2. Modifiez `CONFIG_RTE_APP_TEST=y` en **`CONFIG_RTE_APP_TEST=n`**
3. Modifiez `CONFIG_RTE_BUILD_COMBINE_LIBS=n` en **`CONFIG_RTE_BUILD_COMBINE_LIBS=y`**
4. Exécutez la commande suivante :

   ```
   vi GNUmakefile
   ```

5. Modifiez `ROOTDIRS-y := lib drivers app` en **`ROOTDIRS-y := lib drivers`**
6. Exécutez la commande suivante :

   ```
   make install T=x86_64-native-linuxapp-gcc
   ```

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Installez OVS 2.5.1 en exécutant les commandes suivantes :

```
wget http://openvswitch.org/releases/openvswitch-2.5.1.tar.gz tar
 xzvf openvswitch-2.5.1.tar.gz cd openvswitch-2.5.1 ./configure –
with-dpdk=”/root/dpdk-2.2.0/x86_64-native-linuxapp-gcc/” make make
 install
```

Configuration d'OVS et de DPDK sur l'hôte

Après avoir installé les composants nécessaires pour prendre en charge OVS et DPDK, vous devez configurer l'hôte pour utiliser OVS et DPDK.

STEP 1 | Connectez-vous à la CLI de l'hôte KVM.

STEP 2 | Si vous remplacez ou reconfigurez une configuration OVS-DPDK existante, exécutez les commandes suivantes pour réinitialiser toute configuration précédente. Répétez la commande pour chaque interface.

```
rm /usr/local/var/run/openvswitch/<interface-name>
```

STEP 3 | Configurez les HugePages initiales pour OVS.

```
echo 16384 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```

STEP 4 | Montez les HugePages pour QEMU :

```
mkdir /dev/hugepages mkdir /dev/hugepages/libvirt mkdir /dev/
hugepages/libvirt/qemu mount -t hugetlbfs hugetlbfs /dev/hugepages/
libvirt/qemu
```

STEP 5 | Utilisez la commande suivante pour supprimer un démon OVS existant.

```
killall ovsdb-server ovs-vswitchd
```

STEP 6 | Créez des répertoires pour le démon OVS.

```
mkdir -p /usr/local/etc/openvswitch
mkdir -p /usr/local/var/run/openvswitch
```

STEP 7 | Effacez les anciens répertoires.

```
rm -f /var/run/openvswitch/vhost-user*
rm -f /usr/local/etc/openvswitch/conf.db
```

STEP 8 | Initialisez la base de données de configuration.

```
ovsdb-tool create /usr/local/etc/openvswitch/conf.db\
```

 ©2023 Palo Alto Networks, Inc.

```
/usr/local/share/openvswitch/vswitch.ovsschema
```

STEP 9 | Créez un serveur de base de données OVS.

```
ovsdb-server --remote=punix:/usr/local/var/run/openvswitch/
db.sock \ --remote=db:Open_vSwitch,Open_vSwitch,manager_options
 \ --private-key=db:Open_vSwitch,SSL,private_key \ --
certificate=db:Open_vSwitch,SSL,certificate \ --bootstrap-ca-
cert=db:Open_vSwitch,SSL,ca_cert \ --pidfile --detach
```

STEP 10 | Initialisez OVS.

```
ovs-vsctl --no-wait init
```

STEP 11 | Démarrez le serveur de base de données.

```
export DB_SOCK=/usr/local/var/run/openvswitch/db.sock
```

STEP 12 | Installez le module igb_uio (pilote d'appareil réseau) pour DPDK.

```
cd ~/dpdk-2.2.0/x86_64-native-linuxapp-gcc/kmod modprobe uio insmod
 igb_uio.ko cd ~/dpdk-2.2.0/tools/
```

STEP 13 | Activez DPDK sur les interfaces en utilisant PCI-ID ou le nom de l'interface.

```
./dpdk_nic_bind.py --bind=igb_uio <your first data interface>
./dpdk_nic_bind.py --bind=igb_uio <your second data interface>
```

STEP 14 | Démarrez le démon OVS en mode DPDK. Vous pouvez modifier le nombre de cœurs pour ovs-vswitchd. En changeant -c 0x1 en -c 0x3, vous pouvez avoir deux cœurs pour exécuter ce démon.

```
ovs-vswitchd --dpdk -c 0x3 -n 4 -- unix:$DB_SOCK --pidfile --
detach
echo 50000 > /sys/kernel/mm/hugepages/hugepages-2048kB/
nr_hugepages
```

STEP 15 | Créez le pont OVS et connectez les ports au pont OVS.

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
 datapath_type=netdev
ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
ovs-vsctl add-br ovs-br1 -- set bridge ovs-br1
 datapath_type=netdev
ovs-vsctl add-port ovs-br1 dpdk1 -- set Interface dpdk1 type=dpdk
```

 ©2023 Palo Alto Networks, Inc.

STEP 16 | Créez des ports utilisateur vhost DPDK pour OVS.

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
 type=dpdkvhostuser
ovs-vsctl add-port ovs-br1 vhost-user2 -- set Interface vhost-user2
 type=dpdkvhostuser
```

STEP 17 | Définissez le nombre de files d'attente matérielles de la carte réseau utilisée par l'hôte.

```
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-rxqs=8
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-txqs=8
```

STEP 18 | Définissez le masque de processeur utilisé pour OVS.

```
ovs-vsctl set Open_vSwitch . other_config:pmd-cpu-mask=0xffff
```

STEP 19 | Définissez les autorisations nécessaires pour les ports utilisateur vhost DPDK. Dans l'exemple ci-dessous, 777 est utilisé pour donner des autorisations de lecture, d'écriture et d'exécution.

```
chmod 777 /usr/local/var/run/openvswitch/vhost-user1
chmod 777 /usr/local/var/run/openvswitch/vhost-user2
chmod 777 /dev/hugepages/libvirt/qemu
```

Modification du fichier de configuration du pare-feu VM-Series

Modifiez le fichier de configuration XML du pare-feu VM-Series afin de prendre en charge OVS et DPDK. Vous pouvez accéder au fichier de configuration XML ou procéder après le déploiement du pare-feu VM-Series. Si vous faites cela après avoir déployé le pare-feu, veillez à arrêter le pare-feu avant d'apporter des modifications. Les valeurs ci-dessous sont des exemples ; vos valeurs pour chaque paramètre varient en fonction de votre modèle VM-Series.

STEP 1 | Connectez-vous à la CLI de l'hôte KVM.

STEP 2 | Modifiez le fichier de configuration XML de votre pare-feu VM-Series.

1. Ouvrez le fichier de configuration XML à l'aide de **virsh edit $<*your-vm-series-name*>**.
2. Définissez le support de la mémoire pour la HugePage. Assurez-vous de fournir suffisamment de mémoire pour prendre en charge le modèle de pare-feu VM-Series que

 ©2023 Palo Alto Networks, Inc.

vous déployez sur l'hôte. Reportez-vous à la section Configuration système requise pour VM-Series pour plus d'informations.

```
<memory unit='KiB'>12582912</memory> <currentMemory
 unit='KiB'>6291456</currentMemory> <memoryBacking>
 <hugepages/>
```

3. Définissez les indicateurs de processeur nécessaires pour la machine virtuelle.

```
<cpu mode='host-model'>
```

4. Activez le partage de mémoire entre la machine virtuelle et l'hôte.

```
<numa> <cell id='0' cpus='0,2,4,6' memory='6291456'
 unit='KiB' memAccess='shared'/> <cell id='1' cpus='1,3,5,7'
 memory='6291456' unit='KiB' memAccess='shared'/> </numa>
```

5. Définissez les ports utilisateur vhost DPDK en tant qu'interfaces réseau du pare-feu VM-Series. En outre, définissez le nombre de files d'attente virtuelles virtio fournies au pare-feu VM-Series par l'hôte.

```
<interface type='vhostuser'> <mac address='52:54:00:36:83:70'/
> <source type='unix' path='/usr/local/var/run/openvswitch/
vhost-user1' mode='client'/> <model type='virtio'/>
 <driver name='vhost' queues='8'/> <address type='pci'
 domain='0x0000' bus='0x00' slot='0x04' function='0x0'/
> </interface> <interface type='vhostuser'> <mac
 address='52:54:00:30:d7:94'/> <source type='unix' path='/
usr/local/var/run/openvswitch/vhost-user2' mode='client'/
> <model type='virtio'/> <driver name='vhost' qeueus='8'>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
 function='0x0'/> </interface>
```

Activation de SR-IOV sur KVM

La virtualisation d'E/S racine unique (SR-IOV) permet à un périphérique physique PCIe unique sous un port racine unique d'apparaître comme plusieurs périphériques physiques distincts de l'hyperviseur ou de l'invité. Pour activer SR-IOV sur un invité KVM, définissez un pool de périphériques à fonction virtuelle (VF) associés à une carte réseau physique et attribuez automatiquement des périphériques VF depuis le pool vers les PCI ID.

Pour SR-IOV avec des interfaces réseau Intel 10 Go (pilote ixgbe), la version du pilote doit être 4.2.5 ou ultérieure pour prendre en charge les files d'attente multiples pour chaque interface NIC. Consultez la matrice de compatibilité pour la prise en charge des pilotes PacketMMAP et DPDK par la version de PAN-OS.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Définissez un réseau pour un pool de VF.

1. Générez un fichier XML avec du texte similaire à l'exemple suivant. Changez la valeur de **pf dev** en l'**ethdev** correspondant à la fonction physique de votre périphérique SR-IOV.

```
<network> <name>passthrough</name> <forward mode='hostdev'
 managed='yes'> <pf dev='eth3'/> </forward> </network>
```

2. Enregistrez le fichier XML.
3. Exécutez les commandes suivantes :

```
$ virsh net-define <path to network XML file>  $ virsh net-
autostart passthrough $ virsh net-start passthrough
```

STEP 2 | Pour garantir que le pare-feu VM-Series démarre en mode DPDK, modifiez la configuration XML de la VM invitée sur l'hyperviseur KVM pour ajouter ce qui suit :

```
<cpu mode='host-passthrough' check='none'/>
```

Cela permet de s'assurer que les indicateurs du processeur sont exposés.

Pour vérifier que les indicateurs du processeur sont exposés sur la VM :

```
cat /proc/cpuinfo
```

Dans la sortie **flags** (indicateurs) pour PAN-OS 10.2 ou ultérieur avec DPDK 18.11, vous avez besoin des indicateurs **AVX**, ou **AES** et **SSE**.

STEP 3 | Après la définition et le démarrage du réseau, modifiez la définition XML de l'invité pour spécifier le réseau.

```
<interface type='network'> <source network='passthrough'> </
interface>
```

Lorsque l'invité démarre, une VF est automatiquement attribuée à l'invité.

STEP 4 | Ajoutez l'adresse MAC multicast à l'hôte.

Lorsque SR-IOV est activé, le PF filtre le trafic de multidiffusion. Ce filtrage entraîne l'échec des applications qui dépendent de la multidiffusion, comme l'OSPF. Pour empêcher ce filtrage, vous devez ajouter manuellement l'adresse MAC multicast à l'hôte en utilisant la commande suivante :

```
#ip maddress add <multicast-mac> dev <interface-name>
```

Activation du mode d'accès VLAN (réseau local virtuel) avec SR-IOV

Les pare-feu VM-Series sur KVM peuvent fonctionner en mode d'accès VLAN pour prendre en charge les cas d'utilisation où il est déployé comme une fonction de réseau virtuel (VNF) qui offre la sécurité en tant que service dans un environnement de centre de données/cloud à plusieurs locataires. En mode d'accès VLAN, chaque VNF dispose d'interfaces de réseau virtuel (VNI) dédiées pour chaque réseau et envoie et reçoit des paquets vers/depuis les fonctions virtuelles (VF) SR-IOV sans étiquettes VLAN. Vous devez activer cette capacité sur les fonctions physiques et virtuelles de

 ©2023 Palo Alto Networks, Inc.

l'hyperviseur hôte. Lorsque vous activez ensuite le mode d'accès VLAN sur le pare-feu VM-Series, ce dernier peut envoyer et recevoir du trafic sans étiquettes VLAN à travers toutes ses interfaces de plan de données. De plus, si vous configurez des politiques QoS, le pare-feu peut appliquer la QoS sur l'interface d'accès et fournir un traitement différencié du trafic dans un déploiement multi-tenant.

Par défaut, le pare-feu VM-Series sur KVM fonctionne en mode VLAN tronc (trunk).

STEP 1 | Sur le système hôte, configurez la fonction physique et virtuelle pour fonctionner en mode d'accès VLAN.

`ip link set [inf_name] vf [vf_num] vlan [vlan_id]`.

Pour obtenir les meilleures performances du pare-feu VM-Series, veillez à :

- *Activer l'épinglage du processeur (CPU Pinning). Reportez-vous à la section* Isolation des ressources du processeur dans un nœud NUMA sur KVM.
- *Désactiver la protection contre les relectures, si vous avez configuré des tunnels IPSec.*

  Sur l'interface web du pare-feu, sélectionnez ***Network (Réseau)*** *>* ***IPSec Tunnels (Tunnels IPSec)*** *et choisissez un tunnel IPSec, puis cliquez sur* ***General (Général)****, sélectionnez* ***Show Advanced Options (Afficher les options avancées)*** *et décochez* ***Enable Replay Protection (Activer la protection contre les relectures).***

STEP 2 | Accédez à la CLI sur le pare-feu VM-Series.

STEP 3 | Activez le mode d'accès VLAN.

`request plugins vm-series vlan-mode access-mode on`

`on` active le mode d'accès VLAN. Pour utiliser le mode VLAN tronc, saisissez **`request plugins vm-series vlan-mode access-mode off`**.

STEP 4 | Redémarrez le pare-feu.

Saisissez **`request restart system`**.

STEP 5 | Vérifiez la configuration du mode VLAN.

`show plugins vm-series vlan-mode`

Activation de la prise en charge de files d'attente multiples pour les cartes réseau sur KVM

Modifiez la définition XML de l'invité pour activer le virtio-net à files d'attente multiples. Virtio-net à files d'attente multiples permet aux performances du réseau d'évoluer avec le nombre de processeurs virtuels et permet le traitement parallèle des paquets en créant plusieurs files d'attente TX et RX.

 ©2023 Palo Alto Networks, Inc.

Modifiez la définition XML de l'invité. Insérez une valeur de 1 à 256 pour N afin de spécifier le nombre de files d'attente. Pour de meilleurs résultats, faites correspondre le nombre de files d'attente avec le nombre de cœurs du dataplane configurés sur la machine virtuelle.

```
<interface type='network'> <source network='default'/> <model
 type='virtio'/> <driver name='vhost' queues='N'/> </interface>
```

Isolation des ressources du processeur dans un nœud NUMA sur KVM

Vous pouvez améliorer les performances de VM-Series sur KVM en isolant les ressources du processeur de la machine virtuelle invitée sur un seul nœud NUMA (Non-Uniform Memory Access). Sur KVM, vous pouvez voir la topologie NUMA **virsh**. L'exemple suivant provient d'un système NUMA à deux nœuds :

STEP 1 | Affichez la topologie NUMA. Dans l'exemple ci-dessous, il y a deux nœuds NUMA (sockets), chacun avec un processeur à quatre cœurs avec hyperthreading activé. Tous les ID de processeur pairs appartiennent à un nœud et tous les ID de processeur impairs appartiennent à l'autre nœud.

```
% virsh capabilities <…> <topology> <cells num='2'> <cell
 id='0'> <memory unit='KiB'>33027228</memory> <pages unit='KiB'
 size='4'>8256807</pages> <pages unit='KiB' size='2048'>0</
pages> <distances> <sibling id='0' value='10'/> <sibling
 id='1' value='20'/> </distances> <cpus num='8'> <cpu id='0'
 socket_id='1' core_id='0' siblings='0,8'/> <cpu id='2'
 socket_id='1' core_id='1' siblings='2,10'/> <cpu id='4'
 socket_id='1' core_id='2' siblings='4,12'/> <cpu id='6'
 socket_id='1' core_id='3' siblings='6,14'/> <cpu id='8'
 socket_id='1' core_id='0' siblings='0,8'/> <cpu id='10'
 socket_id='1' core_id='1' siblings='2,10'/> <cpu id='12'
 socket_id='1' core_id='2' siblings='4,12'/> <cpu id='14'
 socket_id='1' core_id='3' siblings='6,14'/> </cpus> </cell> <cell
 id='1'> <memory unit='KiB'>32933812</memory> <pages unit='KiB'
 size='4'>8233453</pages> <pages unit='KiB' size='2048'>0</
pages> <distances> <sibling id='0' value='20'/> <sibling id='1'
 value='10'/> </distances> <cpus num='8'> <cpu id='1' socket_id='0'
 core_id='0' siblings='1,9'/> <cpu id='3' socket_id='0' core_id='1'
 siblings='3,11'/> <cpu id='5' socket_id='0' core_id='2'
 siblings='5,13'/> <cpu id='7' socket_id='0' core_id='3'
 siblings='7,15'/> <cpu id='9' socket_id='0' core_id='0'
 siblings='1,9'/> <cpu id='11' socket_id='0' core_id='1'
 siblings='3,11'/> <cpu id='13' socket_id='0' core_id='2'
 siblings='5,13'/> <cpu id='15' socket_id='0' core_id='3'
 siblings='7,15'/> </cpus> </cell> </cells>
```

STEP 2 | Épinglez les processeurs virtuels (vCPU) d'un invité KVM à des processeurs physiques spécifiques ; utilisez l'attribut **cpuset** dans la définition XML de l'invité. Dans cet exemple, les 8 vCPU sont épinglés aux processeurs physiques dans le premier nœud NUMA. Si vous ne souhaitez pas épingler explicitement les vCPU, vous pouvez omettre le bloc **cputune**. Dans ce

 ©2023 Palo Alto Networks, Inc.

cas, tous les vCPU seront épinglés à la plage des processeurs spécifiés dans cpuset, mais ils ne seront pas explicitement mappés.

```
<vcpu cpuset='0,2,4,6,8,10,12,14'>8</vcpu> <cputune> <vcpupin
 vcpu='0' cpuset='0'/> <vcpupin vcpu='1' cpuset='2'/> <vcpupin
 vcpu='2' cpuset='4'/> <vcpupin vcpu='3' cpuset='6'/> <vcpupin
 vcpu='4' cpuset='8'/> <vcpupin vcpu='5' cpuset='10'/> <vcpupin
 vcpu='6' cpuset='12'/> <vcpupin vcpu='7' cpuset='14'/> </cputune>
```


©2023 Palo Alto Networks, Inc.

Délestage intelligent du trafic

Le délestage intelligent du trafic est un abonnement à la sécurité du pare-feu VM-Series qui, lorsqu'il est configuré avec le DPU NVIDIA BlueField-2, augmente le débit de capacité du pare-feu VM-Series. Le pare-feu VM-Series et le DPU BlueField-2 doivent être installés sur un hôte physique x86 exécutant Ubuntu 18.04, avec la version du noyau 4.15.0-20. Le pare-feu VM-Series doit être déployé en mode câble virtuel.

Le service de délestage intelligent du trafic (ITO) achemine les premiers paquets d'un flux vers le pare-feu pour inspection afin de déterminer si le reste des paquets du flux doit être inspecté ou déchargé. Cette décision est basée sur la politique ou sur la possibilité d'inspecter le flux (par exemple, le trafic crypté ne peut pas être inspecté) En inspectant uniquement les flux pouvant bénéficier de l'inspection de sécurité, la charge globale sur le pare-feu est considérablement réduite et les performances du pare-feu VM-Series augmentent sans sacrifier la sécurité.

Les limitations actuelles de l'évolutivité de NVIDIA BlueField-2 DPU sont les suivantes :

- Capacité de la table de session : 500 000 sessions
- Taux de mise à jour de la table de session : 7000 sessions/seconde
- Connexions par seconde : 20,000
- Taux de délestage en épingle à cheveux : ~ 90 Gbit/s pour des paquets de 1500 octets

Si le trafic de déchargement vers le DPU BlueField-2 dépasse 7000 sessions par seconde, ou si la table des sessions de délestage est pleine, le trafic passe toujours par le pare-feu VM-Series et est inspecté. Lorsque le nombre de sessions par seconde tombe en dessous de 7000, le délestage intelligent du trafic vers le Bluefield-2 DPU reprend.

La haute disponibilité active/passive est prise en charge pour les pare-feu VM-Series exécutés sur des hôtes physiques avec des configurations identiques.

Le délestage intelligent du trafic ne prend pas en charge le paramètre de session de vieillissement accéléré.

- Exigences de délestage intelligent du trafic
- Interfaces intelligentes de délestage du trafic
- Haute disponibilité
- Installer le BlueField-2 DPU
- Installation du pare-feu VM-Series
- Vérifiez le système BlueField-2 DPU
- Activer les fonctions virtuelles
- Installation ou mise à niveau du logiciel BlueField Bootstream
- Installation ou mise à niveau du package Debian
- Exécution d'un délestage intelligent du trafic
- Dépannage BlueField-2 DPU
- Dépannage PAN-OS

©2023 Palo Alto Networks, Inc.

- Références

Exigences de délestage intelligent du trafic

ITO nécessite un pare-feu VM-Series et un DPU BlueField-2 installés sur le même hôte physique x86. La haute disponibilité active/passive pour les pare-feu VM-Series est prise en charge.

Vous ne pouvez déployer qu'un seul pare-feu VM-Series et un DPU BlueField-2 par hôte.

- Commutateur réseau avec 2 ports 100 Go/s disponibles (4 pour HA).

  Si vous souhaitez utiliser des VLAN, assurez-vous que votre commutateur en est capable.
- Exigences matérielles de l'hôte physique X86.
  - Au moins 120 Go de RAM disponible (64 Go pour le serveur / 56 Go pour le pare-feu VM-Series)
  - Au moins 18 cœurs physiques
  - Bluefield-2 SmartNIC MBF2M516A-CEEOT avec deux ports 100 Go/s installés dans l'emplacement PCI-e 3 ou 4.
  - Un SFP 100GigE certifié pour chaque port du DPU BlueField2, tel que recommandé par le Guide de l'utilisateur du DPU NVIDIA BlueField Ethernet.
- Configuration requise pour le logiciel hôte X86.
  - Ubuntu 18.04, avec la version du noyau 4.15.0-20.
  - Version du flux de démarrage binaire Bluefield : 5.3-1.0.0.1

    Acceptez le contrat de licence utilisateur final pour démarrer le téléchargement.
- Machine virtuelle pour le pare-feu VM-Series.
  - PAN-OS 10.2 ou version ultérieure.
  - Plugin VM-Series 2.1.0 ou version ultérieure.
  - Pour obtenir une licence de délestage intelligent du trafic, créez un profil de déploiement logiciel NGFW pour 10.0.4 et versions ultérieures, avec un minimum de 18 vCPU et le service de délestage intelligent du trafic. Le profil peut inclure d'autres services de sécurité.

    Avec PAN-OS 10.1.1 ou version ultérieure et VM-Series Plugin 2.1.1 ou version ultérieure, pour obtenir une licence de délestage intelligent du trafic, créez un profil de déploiement logiciel NGFW pour 10.0.4 et versions ultérieures, avec un minimum de six (6) vCPU et le Service de délestage intelligent du trafic. Le profil peut inclure d'autres services de sécurité.

Interfaces intelligentes de délestage du trafic

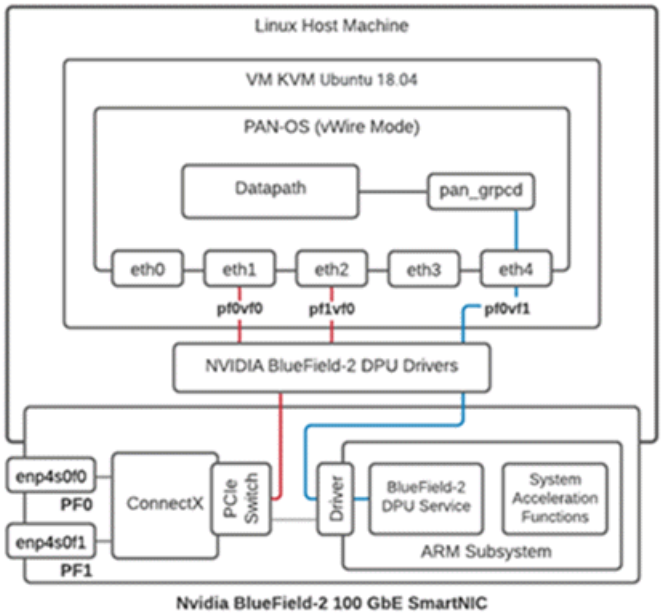
Un déploiement du délestage intelligent du trafic connecte trois types d'interfaces :

©2023 Palo Alto Networks, Inc.

- Interfaces virtuelles PAN-OS :
  - eth0 : interface de gestion
  - eth1, eth2 : plan de données
  - eth3 : Interface HA
  - eth4 : interface gRPC
- Interfaces physiques BlueField-2 DPU (créées à partir du système d'exploitation hôte).
- Interfaces physiques hôtes pour les ports BlueField-2 DPU 100 Go (créées à partir du système d'exploitation hôte).

Vous connectez les interfaces PAN-OS au DPU BlueField-2 via les fonctions virtuelles SR-IOV (VF) que vous créez sur l'hôte physique (voir Activer les fonctions virtuelles).

Dans la figure suivante, les deux ports BlueField-2 DPU sont représentés en tant que fonctions physiques PF0 et PF1. Ces PF peuvent être observés du côté hôte comme enp4s0f0 et enp4s0f1, et sont divisés en plusieurs VF pour la fonctionnalité SR-IOV.



- Le premier VF pour chaque PF doit être le port de données (eth1:pf0vf0).
- Un VF supplémentaire est requis pour le canal de contrôle de l'interface client/serveur gRPC (eth4:pf0v1).
- Les VF du côté hôte sont les suivantes :
  - enp4s0f0 est représenté par pf0vf0 et pf1vf0 sur le BlueField-2 DPU, et sont utilisés pour les données.
  - enp4s0f1 est représenté par pf0vf1 et est utilisé pour le trafic de contrôle gRPC.

Haute disponibilité

La haute disponibilité active/passive est prise en charge pour une paire de pare-feu VM-Series déployés en mode Vwire sur des hôtes physiques.

©2023 Palo Alto Networks, Inc.

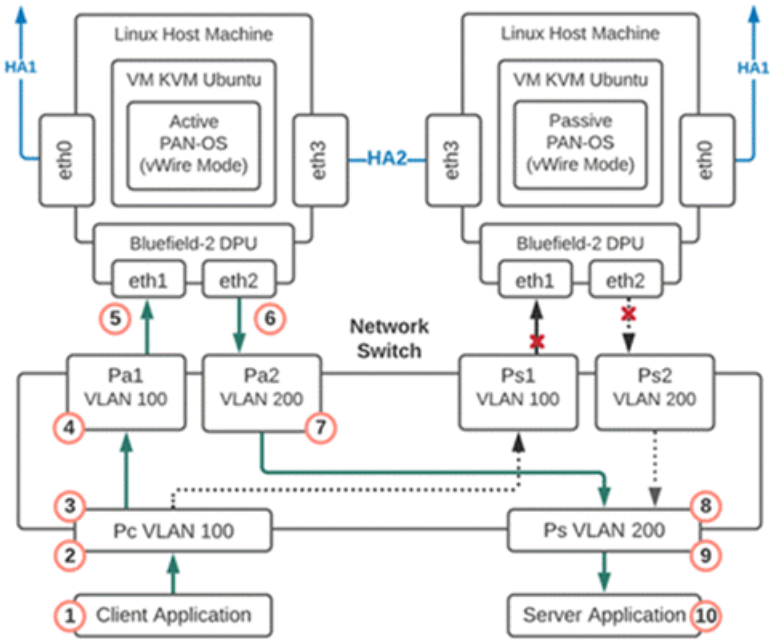
- Les pare-feu doivent être installés sur des hôtes physiques avec le BlueField-2 DPU configuré comme spécifié dans Exigences de délestage intelligent du trafic.
- Pour l'interface HA2 (voir les figures dans Flux de paquets actifs et Flux de paquets passif), utilisez la même interface Mellanox (cx-3, cx-4 ou cx-5) sur les deux hôtes.
- (facultatif) Pour prendre en charge la commutation du trafic, les hôtes doivent se trouver sur des VLAN distincts afin que vous puissiez utiliser des étiquettes VLAN pour sélectionner le principal, comme décrit dans Sécurisation du trafic entre des hôtes Linux.

ITO H/A se concentre sur la disponibilité du pare-feu VM-Series. Chaque pare-feu gère une table de session et chaque DPU BlueField-2 gère une table de flux. La configuration HA synchronise la table de session active, garantissant qu'elle est mise en miroir sur le pare-feu passif au moment de l'exécution. La table de session stocke à la fois les sessions nécessitant une inspection et les sessions marquées pour le déchargement.

HA utilise l'interface PAN-OS eth3, qui se trouve sur une carte réseau sur le pare-feu VM-Series. Eth3 est utilisé pour sélectionner le pare-feu actif et synchroniser les tables de session de pare-feu VM-Series sur la paire active/passive.

Flux de paquets actifs

Le schéma suivant décrit le flux de paquets actif pour une configuration HA qui utilise une configuration VLAN facultative.



1. Le paquet est envoyé de l'application cliente au commutateur réseau.
2. Le paquet arrive au port du commutateur qui est programmé pour ajouter une étiquette VLAN 100 aux paquets.
3. Les paquets étiquetés ne peuvent aller que vers le port Pa1 car l'interface du port Ps1 est en panne car ce pare-feu est en mode passif.
4. Le paquet arrive au port Pa1 et le VLAN 100 est supprimé du paquet et le paquet est délivré au pare-feu eth1.

©2023 Palo Alto Networks, Inc.

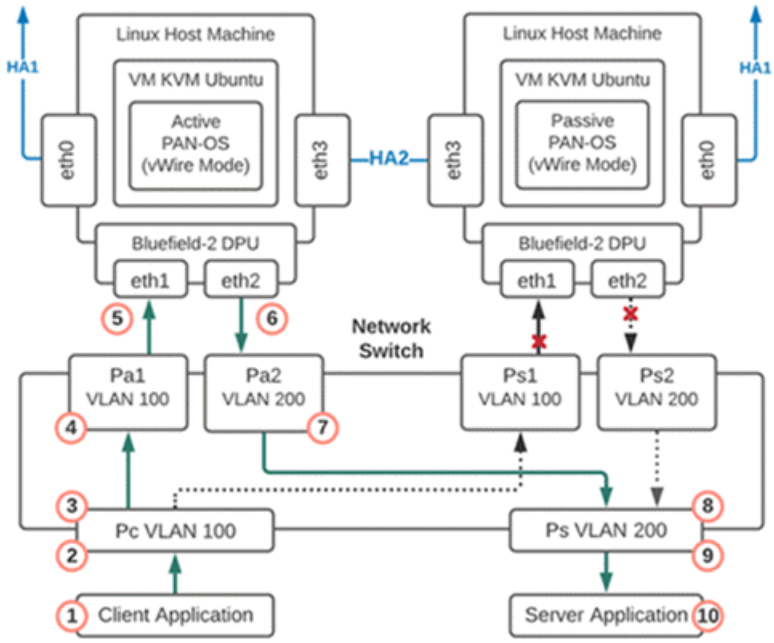
5. Le pare-feu fonctionne en mode vWire, le paquet est donc traité par le pare-feu puis envoyé à eth2.
6. Le paquet arrive au port Pa2 et le VLAN 200 est ajouté.
7. Le paquet est envoyé sur le port Pa2 et ne peut être délivré qu'au port Ps car l'autre port Ps2 du VLAN 200 est en panne.
8. Le paquet arrive au port Ps et l'étiquette VLAN 200 est supprimée.
9. Le paquet est envoyé sur le port Ps sans étiquette VLAN
10. Le paquet est livré au serveur.

Événement de basculement

Un événement de basculement se produit lorsqu'il y a une notification du pare-feu VM-Series actif ou que le pare-feu passif détecte que l'actif ne répond pas. Lorsque cela se produit, les connexions réseau aux ports Pa1 et Pa2 sont interrompues et les connexions réseau aux ports Ps1 et Ps2 deviennent actives.

Flux de paquets passif

Lorsque le pare-feu VM-Series est à l'état passif, le BlueField-2 DPU sur le membre passif est actif mais ne transmet pas le trafic jusqu'à ce qu'il y ait un basculement et que le pare-feu VM-Series co-localisé devienne actif. Le schéma suivant décrit le flux de paquets passif pour une configuration HA qui utilise une configuration VLAN facultative.



1. Le paquet est envoyé de l'application cliente au commutateur réseau.
2. Le paquet arrive au port du commutateur qui est programmé pour ajouter une étiquette VLAN 100 aux paquets.
3. Les paquets marqués ne peuvent aller que vers le port Ps1 car l'interface du port Pa1 est en panne et ce pare-feu est maintenant passé de passif à actif.
4. Le paquet arrive au port Ps1 et le VLAN 100 est supprimé du paquet et le paquet est délivré au pare-feu eth1.

©2023 Palo Alto Networks, Inc.

5. Le pare-feu fonctionne en mode vWire, le paquet est donc traité par le pare-feu puis envoyé à eth2.
6. Le paquet arrive au port Ps2 et le VLAN 200 est ajouté.
7. Le paquet est envoyé au port Ps2 et ne peut être délivré qu'au port Ps car l'autre port Pa2 du VLAN 200 est en panne.
8. Le paquet arrive au port Ps et l'étiquette VLAN 200 est supprimée.
9. Le paquet est envoyé sur le port Ps sans étiquette VLAN.
10. Le paquet est livré au serveur.

Installer le BlueField-2 DPU

Installez le BlueField-2 DPU sur l'hôte physique avant d'installer le pare-feu VM-Series. Pour plus d'informations sur le BlueField-2 DPU, consultez la documentation du logiciel : DOCUMENTATION DU LOGICIEL DE LA FAMILLE NVIDIA BLUEFIELD DPU V3.5.0.11563.

1. Installez le BlueField-2 DPU sur la machine hôte comme indiqué dans le Guide de l'utilisateur NVIDIA BlueField Ethernet DPU.
2. Installez les pilotes BlueField comme indiqué dans le Guide de démarrage rapide du logiciel NVIDIA BlueField-2 DPU.

Installation du pare-feu VM-Series

L'installation standard de KVM sur le pare-feu VM-Series installe PAN-OS. Suivez les étapes d'installation dans les sections suivantes.

- VM-Series sur KVM : configuration système requise et conditions préalables
- Installation du pare-feu VM-Series à l'aide de Virt-Manager ou Installation du pare-feu VM-Series à l'aide d'une ISO

Activer les fonctions virtuelles

Comme mentionné dans Interfaces intelligentes de délestage du trafic, les fonctions virtuelles (VF) connectent les interfaces PAN-OS au BlueField-2 DPU.

Le nombre maximal de fonctions virtuelles VF par port est de 2. Vous avez besoin d'un total de trois : deux pour le chemin de données et un pour l'interface de gestion.

©2023 Palo Alto Networks, Inc.

STEP 1 | Activez les fonctions virtuelles sur la machine hôte.

- Par défaut, le BlueField-2 DPU utilise la première VF pour le chemin de données, c'est-à-dire enp4s0f0v0 et enp4s0f1v0 dans l'exemple suivant.
- L'autre VF, enp4s0f0v1, est utilisée pour l'interface de gestion du service exécuté sur la carte BlueField-2 (à ne pas confondre avec l'interface de gestion du pare-feu VM-Series).

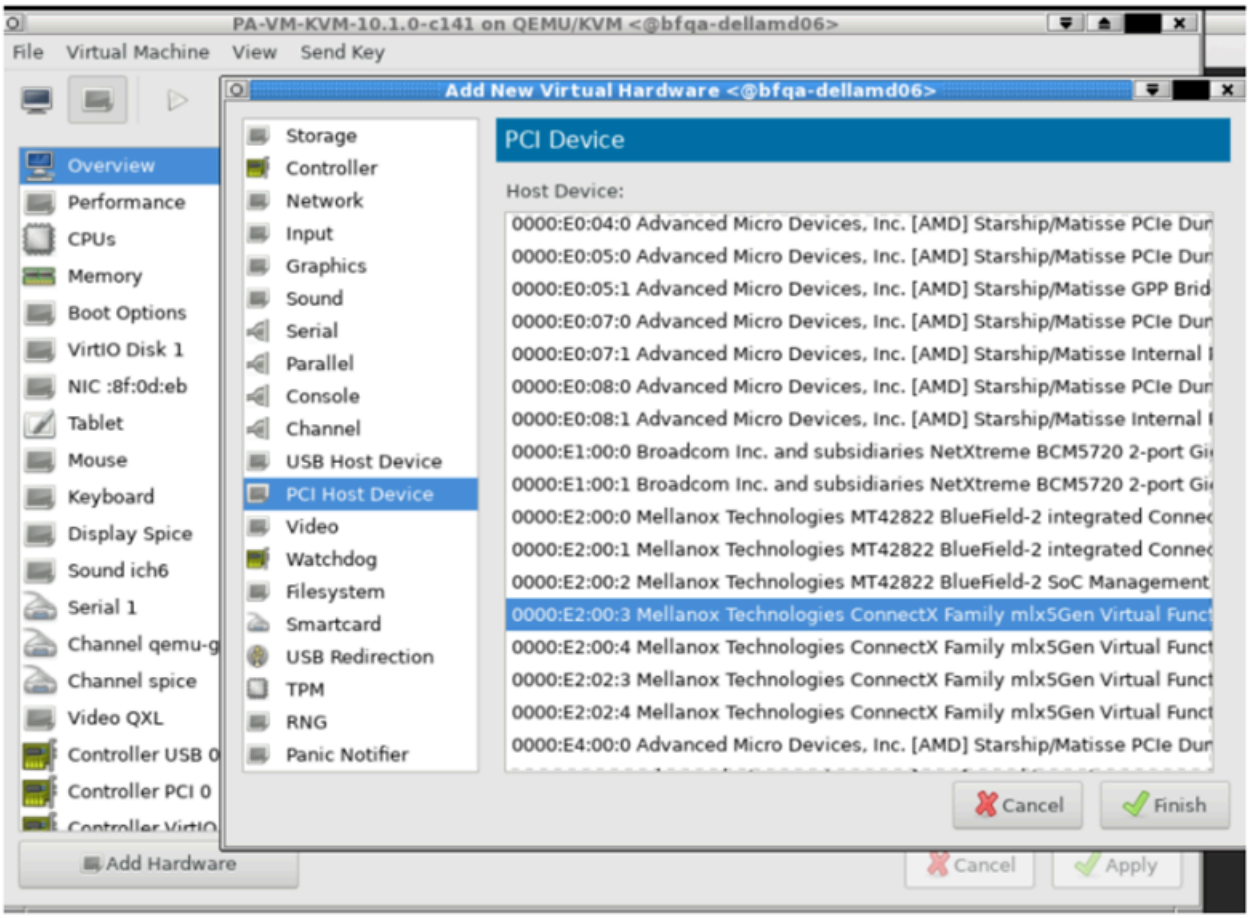
```
$ cat /sys/class/net/enp4s0f0/device/sriov_totalvfs
    8
$ echo 2 > /sys/class/net/enp4s0f0/device/sriov_numvfs
$ cat /sys/class/net/enp4s0f1/device/sriov_totalvfs
    8
$ echo 2 > /sys/class/net/enp4s0f1/device/sriov_numvfs
```


©2023 Palo Alto Networks, Inc.

STEP 2 | Allouez des VF au pare-feu VM-Series à partir de l'hyperviseur KVM.

Le PAN-OS invité ne démarrera pas à moins que les VF ne soient allouées à la VM.

1. Arrêtez la VM.
2. Sur KVM, utilisez virt-manager pour ajouter des VF à la VM.
   - Sélectionnez Add Hardware (Ajouter du matériel), sélectionnez VF0 de PF1 et cliquez sur Finish (Terminer).
   - Sélectionnez Add Hardware (Ajouter du matériel), sélectionnez VF0 de PF0 et cliquez sur Finish (Terminer).
   - Sélectionnez Add Hardware (Ajouter du matériel), sélectionnez VF1 de PF0 et cliquez sur Finish (Terminer).



Vérifiez le système BlueField-2 DPU

Le BlueField-2 DPU communique d'abord avec l'hôte lorsque le pilote du pilote Rshim est installé sur l'hôte. Le Rshim fournit une interface tty (accessible via minicom) et une interface de mise en réseau appelée tmfifo_net0. Avec l'interface tmfifo_net0, vous pouvez vous connecter au BlueField-2 DPU à partir de l'hôte. Le pilote Rshim s'exécute sur le système d'exploitation de l'hyperviseur x86 et, en fait, l'installation d'OFED installe un pilote Rshim par défaut.

©2023 Palo Alto Networks, Inc.

STEP 1 | Connectez-vous à la machine hôte.

```
$ ssh user@<host-ip-address>
```

```
$ password:
```

STEP 2 | Si l'interface réseau hôte du pilote Rshim n'a pas d'adresse IP, vous devez en créer une.

```
$ ip addr add dev tmfifo_net0 192.168.100.1/24
```

STEP 3 | Depuis la machine hôte, connectez-vous au sous-système BlueField-2 DPU.

```
$ ssh ubuntu@192.168.100.2
```

```
$ password: ubuntu
```

S'il s'agit de votre première connexion, le système vous invite à remplacer le mot de passe par défaut par un nouveau mot de passe.

STEP 4 | Modifiez le mot de passe par défaut sur le BlueField-2 DPU.

Connectez-vous au BlueField-2 DPU avec le nom d'utilisateur initial **ubuntu** et le mot de passe **ubuntu**.

Une fois connecté, le système vous invite à configurer un nouveau mot de passe.

```
WARNING: Your password has expired. You must change your password
 now and login again! Changing password for ubuntu. Current
 password: ***** New password: ***** Retype new password: *****
 passwd: password updated successfully
```

Déconnectez-vous et connectez-vous avec votre nouveau mot de passe.

STEP 5 | Vérifiez la version du logiciel.

```
$ ofed_info -s
```

Cela devrait renvoyer la version suivante ou une version ultérieure :

```
$ MLNX_OFED_LINUX-5.3-0.3.3
```

STEP 6 | Vérifiez que le Bluefield 2 DPU est dans le mode correct.

Le mode correct est le mode de propriété de la fonction CPU intégrée. Consultez la documentation Mode de propriété de la fonction CPU intégrée pour obtenir des instructions sur la vérification et la configuration du mode.

Installation ou mise à niveau du logiciel BlueField Bootstream

Suivez ces étapes pour vous assurer que vous disposez du dernier logiciel Bluefield bootstream (BFB) pour le BlueField-2 DPU. Le BFB comprend le système d'exploitation BlueField et d'autres logiciels tels que les pilotes et les interfaces réseau.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Téléchargez le package BFB sur l'hôte physique pour le BlueField-2 DPU.

Obtenez la dernière version du pilote pour le système d'exploitation exécuté sur les cœurs DPI ARM sur le site Web de NVIDIA. Vous devez accepter le contrat de licence de l'utilisateur final pour le télécharger.

STEP 2 | Installez le BFB à partir de l'emplacement de démarrage Rshim sur l'hôte physique.

Notez que le nom de fichier ci-dessous (la chaîne commençant par **DOCA** et se terminant par **.bfb**) ne contient pas d'espaces. Saisissez la commande sur une seule ligne.

```
$ cat DOCA_v1.0_BlueField_OS_Ubuntu_20.04-5.3-1.0.0.0-3.6.0.11699-1-aarch64.bfb > /dev/rshim0/boot
```

STEP 3 | Connectez-vous au BlueField-2 DPU.

Utilisez le nouveau mot de passe que vous avez créé dans Vérifiez le système BlueField-2 DPU.

```
$ ssh ubuntu@192.168.100.2
```

```
$ password:
```

STEP 4 | Appliquez la mise à niveau du micrologiciel sur le BlueField-2 DPU.

Entrez la commande suivante sur une seule ligne.

```
$ sudo /opt/mellanox/mlnx-fw-updater/firmware/mlxfwmanager_sriov_dis_aarch64_41686
```

STEP 5 | Redémarrez le système.

Déconnectez-vous du BlueField-2 DPU et revenez à l'hôte Linux.

```
$ ipmitool chassis power cycle
```

STEP 6 | Connectez-vous au BlueField-2 DPU.

```
$ ssh ubuntu@192.168.100.2
```

```
$ password:
```

STEP 7 | Démarrez le service opof (open offload) sur le BlueField-2 DPU. opof est un service autonome pour le moment.

Les VF doivent exister avant que vous ne démarriez opof. Reportez-vous à la section Activer les fonctions virtuelles.

```
$ opof_setup
$ service opof restart
```

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Vérifiez que le service opof fonctionne sans problème.

```
$ service opof status
```

Installation ou mise à niveau du package Debian

Si la version du package Debian est antérieure à 1.0.4, vous devez le mettre à niveau.

STEP 1 | Sur le BlueField-2 DPU, vérifiez la version du package opof.

```
$ opof -v
```

S'il est antérieur à la version 1.0.4, il doit être mis à niveau.

STEP 2 | Ajoutez le référentiel NVilDIA pour les packages.

```
$ cd /etc/apt/sources.list.d
```

Entrez chaque commande `wget` sur une seule ligne. Il n'y a pas d'espaces dans les URL :

```
wget https://linux.mellanox.com/public/repo/doca/1.0/ubuntu20.04/
doca.list
```

```
wget -qO - https://linux.mellanox.com/public/repo/doca/1.0/
ubuntu20.04/aarch64/GPG-KEY-Mellanox.pub | sudo apt-key add -
```

```
$ apt update
```

STEP 3 | Sur le BlueField-2 DPU, vérifiez le package Debian dans le référentiel.

```
$ apt search opof
```

```
Sorting... Done Full Text Search... Done opof/now 1.0.4 arm64
 [installed,local] Nvidia Firewall Open Offload Daemon
```

STEP 4 | Sur ARM, désinstallez le paquet Debian obsolète.

```
$ apt remove opof
```

STEP 5 | Installez le nouveau package Debian.

```
$ apt install opof
```

STEP 6 | Configurez et redémarrez le service opof.

```
$ opof_setup
```

```
$ service opof restart
```

STEP 7 | Vérifiez que le service opof fonctionne sans problème.

```
$ service opof status
```

Exécution d'un délestage intelligent du trafic

Cette solution nécessite un abonnement au logiciel de délestage intelligent du trafic et un minimum de 18 cœurs physiques pour les meilleures performances/débit. Par défaut, PAN-OS alloue 2 cœurs

 ©2023 Palo Alto Networks, Inc.

pour le délestage intelligent du trafic, 4 cœurs pour les processus de gestion et les 12 cœurs restants pour le traitement du plan de données.

- Configuration du délestage intelligent du trafic sur le pare-feu VM-Series
- Configuration du service de délestage intelligent du trafic sur le BlueField-2 DPU
- Démarrage ou redémarrage du service de délestage intelligent du trafic
- Obtention de l'état et de la santé du service

Configuration du délestage intelligent du trafic sur le pare-feu VM-Series

Suivez ces étapes pour activer le délestage intelligent du trafic sur PAN-OS.

STEP 1 | Affichez la VM PAN-OS. Cela suppose que vous avez déjà créé une instance de VM et que vous la redémarrez.

$ **virsh start <vm-name>**

STEP 2 | Utilisez SSH pour vous connecter à l'interface de gestion du pare-feu VM-Series.

$ **ssh admin@<panos-management-IP-address>**

```
$ admin@PA-VM>
```

STEP 3 | Vérifiez que le délestage intelligent du trafic est installé et sous licence.

admin@PA-VM> **show intelligent-traffic-offload**

```
Intelligent Traffic Offload:   Configuration             : Enabled
   Operation Enabled         : True   Min number packet         : 8
   Min Rate                  : 95   TCP ageing                : 12-
   UDP ageing                : 20
```

`Configuration:Enabled (Configuration : Activé)` signifie que le délestage intelligent du trafic est sous licence.

`Operation Enabled:True (Utilisation activée : Vrai)` signifie que vous avez redémarré un périphérique configuré.

STEP 4 | Activez le délestage intelligent du trafic.

Utilisez la commande suivante pour activer ITO sans redémarrer le système.

admin@PA-VM> **set session offload yes**

Vous pouvez également utiliser **set session offload no** pour désactiver l'ITO sans redémarrer le système.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Validez le délestage intelligent du trafic.

admin@PA-VM> **show session info | match offload**

```
Hardware session offloading: True Hardware UDP session offloading:
 True
```

Pour afficher les compteurs globaux, utilisez la commande suivante :

admin@PA-VM> **show counter global | match flow_offload**

Voir Compteurs de session pour plus d'informations sur l'organisation de la sortie et une description de chaque compteur.

Configuration du service de délestage intelligent du trafic sur le BlueField-2 DPU

Le service doit être construit comme décrit dans Configuration du délestage intelligent du trafic sur le pare-feu VM-Series.

STEP 1 | Depuis la machine hôte, connectez-vous au complexe BlueField-2 DPU.

$ **ssh ubuntu@192.168.100.2**

```
$ password: ubuntu $ ubuntu> sudo -i
```

STEP 2 | Configurez la configuration préliminaire dans le système d'exploitation BlueField-2 DPU.

root@bf2SmartNIC:~# **opof_setup**

```
[ INFO ] No num of hugepages specified, use 2048 [ INFO ] No gRPC
 port specified, use pf0vf1 Configure ovs fallback Configure grpc
 for pf0vf1 Reserved 2048*2MB hugepages
```

Démarrage ou redémarrage du service de délestage intelligent du trafic

Si le service ITO s'exécute sur un DPU, le service a probablement démarré automatiquement. Pour vérifier l'état, exécutez la commande suivante :

$ service opof status

Si le service opof n'est pas en cours d'exécution, saisissez la commande suivante pour démarrer le contrôleur :

$ service opof start

Pour redémarrer le service, exécutez la commande suivante :

$ service opof restart

Obtention de l'état et de la santé du service

Utilisez opof pour obtenir l'état et la santé du service. Chaque commande a sa propre aide en ligne de commande, par exemple : **$ opof -h**

 ©2023 Palo Alto Networks, Inc.

- Interroger une session :

  $ opof query -i <session_id>
- Statistiques de délestage du service de requête :

  $ opof stats

Dépannage BlueField-2 DPU

Utilisez la procédure suivante pour redémarrer le système.

1. Pour redémarrer le système, déconnectez-vous du BlueField-2 DPU et revenez au système d'exploitation hôte Linux.

   $ ipmitool chassis power cycle
2. Si les interfaces ne s'allument pas après le cycle d'alimentation, connectez-vous au BlueField-2 DPU et saisissez :

   $ /sbin/mlnx_bf_configure
3. Revenez au système d'exploitation hôte et saisissez :

   $ sudo /etc/init.d/openibd restart

Dépannage PAN-OS

Valider les flux de trafic

Le trafic de données peut être généré à partir du client et consommé via la configuration du délestage intelligent du trafic par un serveur. IPERF3 peut être utilisé pour générer du trafic, comme indiqué dans Exécuter les tests IPERF3. Une fois le trafic initié, les premiers paquets du flux sont envoyés à la PA-VM qui décide si le flux doit être délesté ou non.

Une politique de contrôle prioritaire sur l'application doit être définie pour identifier les flux à délester. Un flux TCP définit le fanion FIN/RST sur un paquet de contrôle et l'envoie à la PA-VM. Lorsque la PA-VM décide de délester le flux, utilisez show session all pour afficher les flux délestés. Utilisez **show session id <flowID>** pour fournir des informations sur l'état du flux. Un flux délesté a l'état **Offload: yes (Déchargement : oui)**.

Les compteurs de flux ne sont pas mis à jour tant que les paquets suivants du flux sont à l'état de délestage et transitent par le BlueField-2 DPU. Une fois le flux terminé, le service de délestage déclenche un temporisateur d'expiration (vieillissement TCP configuré à partir de la CLI). Lorsque le minuteur expire, le service collecte les statistiques de flux mises à jour et les envoie au pare-feu VM-Series. Le pare-feu met ensuite à jour ses compteurs de session de flux et **show session id <flowID>** renvoie les valeurs mises à jour.

Compteurs de session

Utilisez la commande suivante pour afficher les compteurs de session.

admin@PA-VM > **show counter global | match flow_offload**

Les colonnes de sortie pour chaque compteur sont :

Nom du compteur | Valeur | Taux | Gravité | Catégorie | Aspect | Description.

 ©2023 Palo Alto Networks, Inc.

- Valeur : nombre d'occurrences depuis le démarrage du système.
- Taux : fréquence de changement de compteur.
- Gravité : Info, Avertissement, Abandon. Utilisé pour le support technique.
- Catégorie : flux (un composant d'une session).
- Aspect : délestage pour un flux entier.

Nom du compteur	Description
flow_offload_rcv_cpu	Nombre de paquets reçus par CPU avec session délestée
flow_offload_session_update	Nombre de fois que la session doit être mise à jour
flow_offload_session_insert	Nombre de sessions insérées dans l'appareil de déchargement
flow_offload_session_delete	Nombre de sessions supprimées de l'appareil de déchargement
flow_offload_delete_msg_failed	Nombre de messages del vers GRPC qui ont échoué
flow_offload_add_msg_failed	Nombre de messages de session vers GRPC qui ont échoué
flow_offload_session_verify	Nombre de messages de vérification vers le périphérique de délestage
flow_offload_verify_msg_failed	Nombre de messages de vérification vers GRPC qui ont échoué
flow_offload_update_session_stat	HW indique l'expiration du flux
flow_offload_missing_session_stat	Impossible de trouver la session pour les statistiques
flow_offload_invalid_session	Décharger l'ID de session non valide
flow_offload_del_session_fail	Délestage Supprimer session invalide
flow_offload_add_session_fail	Échec de l'ajout de session de déchargement
flow_offload_get_session_fail	Échec du délestage de l'obtention de session
flow_offload_grpc_fail	Échec du délestage de l'appel grpc
flow_offload_active_session	Nombre de sessions déchargées actives
flow_offload_aged_session	Nombre de sessions délestées expirées
flow_offload_session	Nombre de sessions déchargées

©2023 Palo Alto Networks, Inc.

Exécuter les tests IPERF3

Iperf3 est une application simple en option pour générer du trafic efficace pour exécuter des tests de trafic de données. Pour exécuter le serveur en tant que service, utilisez **`iperf3 -s -D`**. Par défaut, l'application attend des paquets sur le port de destination TCP/UDP 5201, mais le port peut être modifié.

- Flux unique : pour les flux iperf3 uniques, saisissez :

```
iperf3 -c <server-ip-address> -t 60
```

- Flux multiples : pour lancer 20 flux simultanés pendant 60 secondes, saisissez :

```
iperf3 -c <ip of server> -P 20 -t 60
```

Validation du délestage intelligent du trafic

Vous pouvez utiliser les journaux de pare-feu VM-Series pour valider la connectivité entre le client ITO exécuté sur le pare-feu et le service de délestage sur le BlueField-2 DPU. La sortie de journal attendue pour un délestage réussi est la suivante.

admin@auto-pavm> **`less mp-log pan_grpcd.log`**

```
[PD] dec free list 0xe0ff022000 RS LIB INIT in DP! pan_fec_app_init:
 fec_data 0xe0feef1088, maxentries 120 [FEC] enc free list
 0xe0feef1100, dec free list 0xe0feef10b8 Creating dp grpc ring buf
 Initializing dp grpc ring buf Mapping flow data memory Found offload
 parameters Heart beat found 1 Established connection to offload
 device
```

Dépannage OPOF

Vous pouvez également afficher les journaux du service de délestage pour valider la connectivité :

root@linux:~# **`service opof status`**

```
● opof.service - Nvidia Firewall Intelligent Traffic Offload
 Daemon Loaded: loaded (/etc/systemd/system/opof.service; disabled;
 vendor preset: enabled) Active: active (running) since Fri
 2021-05-21 18:40:38 UTC; 3h 48min ago Docs: file:/opt/mellanox/
opof/README.md Process: 163906 ExecStartPre=/usr/sbin/opof_pre_check
 (code=exited, status=0/SUCCESS) Main PID: 163922 (nv_opof) Tasks:
 30 (limit: 19085) Memory: 50.7M CGroup: /system.slice/opof.service
 └─163922 /usr/sbin/nv_opof -n 1 -a 0000:03:00.0,representor=[0] -a
 0000:03:00.1,representor=[0] May 21 18:40:38 localhost.localdomain
 nv_opof[163922]: EAL: Probe PCI driver: mlx5_pci (15b3:a2d6) device:
 0000:03:00.0 (socket 0) May 21 18:40:38 localhost.localdomain
 nv_opof[163922]: EAL: Invalid NUMA socket, default to 0 May 21
 18:40:38 localhost.localdomain nv_opof[163922]: EAL: Probe PCI
 driver: mlx5_pci (15b3:a2d6) device: 0000:03:00.0 (socket 0) May
 21 18:40:38 localhost.localdomain nv_opof[163922]: EAL: Invalid
 NUMA socket, default to 0 May 21 18:40:38 localhost.localdomain
 nv_opof[163922]: EAL: Probe PCI driver: mlx5_pci (15b3:a2d6) device:
```

 ©2023 Palo Alto Networks, Inc.

```
0000:03:00.1 (socket 0) May 21 18:40:38 localhost.localdomain
nv_opof[163922]: EAL: Invalid NUMA socket, default to 0 May
21 18:40:38 localhost.localdomain nv_opof[163922]: EAL: Probe
PCI driver: mlx5_pci (15b3:a2d6) device: 0000:03:00.1 (socket
0) May 21 18:40:39 localhost.localdomain nv_opof[163922]: EAL:
No legacy callbacks, legacy socket not created May 21 18:40:39
localhost.localdomain nv_opof[163922]: EAL: No legacy callbacks,
legacy socket not created May 21 18:40:42 localhost.localdomain
nv_opof[163922]: Server listening on: 169.254.33.51:3443
```

Les journaux montrent que le délestage intelligent du trafic communique avec le pare-feu PA-VM VM-Series sur le `serveur à l'écoute` de l'adresse IP, et vous voyez les VF ainsi que d'autres détails des paramètres DPDK. Un journal de l'ajout d'un flux TCP qui est délesté est également joint.

Références

- Guide de l'utilisateur du BlueField Ethernet DPU de NVIDIA
- LOGICIEL DE LA FAMILLE BLUEFIELD DPU DE NVIDIA V3.5.0.11563 D
- Démon de délestage intelligent du trafic DPU de Nvidia
- OpenOffload gRPC GITHUB
- Guide de l'administrateur PAN-OS

©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur Hyper-V

Le pare-feu VM-Series peut être déployé sur un serveur exécutant Microsoft Hyper-V. Hyper-V est fourni comme hyperviseur autonome ou comme complément/rôle pour Windows Server.

- Déploiements pris en charge sur Hyper-V
- Configuration système requise sur Hyper-V
- Services d'intégration Linux
- Installation du pare-feu VM-Series sur Hyper-V

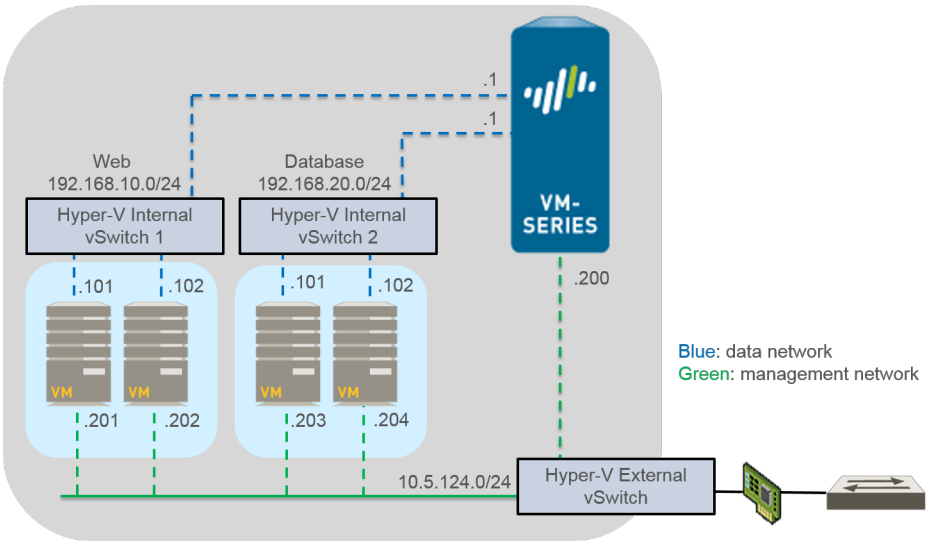
Déploiements pris en charge sur Hyper-V

Vous pouvez déployer une ou plusieurs instances de VM-Series sur les hôtes exécutant Hyper-V. Le placement du pare-feu VM-Series dépend de la topologie de votre réseau. VM-Series prend en charge les déploiements d'interface tap, câble virtuel, couche 2 et couche 3.

- Sécurisation du trafic sur un hôte Hyper-V
- Sécurisation du trafic entre plusieurs hôtes Hyper-V

Sécurisation du trafic sur un hôte Hyper-V

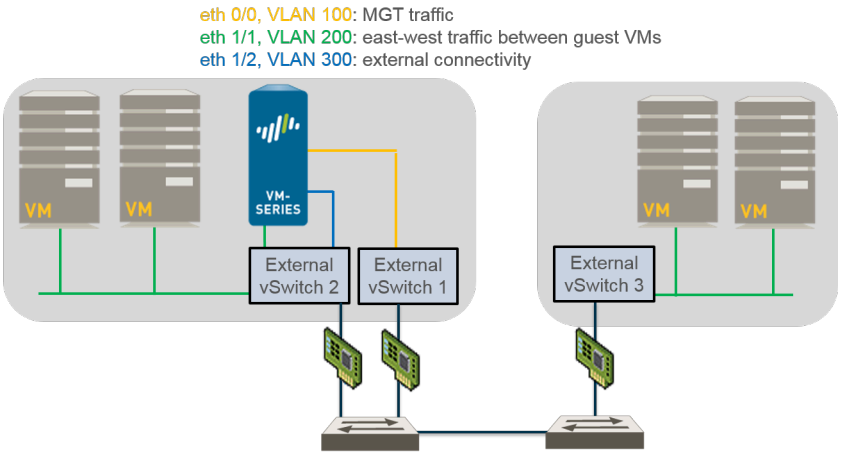
Le pare-feu VM-Series est déployé sur un hôte Hyper-V individuel avec d'autres VM invitées. Dans l'exemple ci-dessous, le pare-feu VM-Series possède des interfaces de couche 3 et le VM-Series et les autres VM invitées sont connectés par des vSwitch Hyper-V. Tout le trafic entre les serveurs Web et les serveurs de base de données est acheminé à travers le pare-feu. Le trafic entre les serveurs de base de données uniquement ou entre les serveurs Web uniquement est traité par le vSwitch externe et n'est pas acheminé à travers le pare-feu.



Sécurisation du trafic entre plusieurs hôtes Hyper-V

Vous pouvez déployer votre pare-feu VM-Series pour sécuriser le trafic de plusieurs hôtes Hyper-V. Dans l'exemple ci-dessous, le VM-Series est déployé en mode couche 2 pour protéger le trafic en provenance et à destination des VM invitées. Un seul pare-feu VM-Series protège le trafic entre quatre VM invitées réparties sur deux hôtes Hyper-V. L'étiquetage VLAN est utilisé pour isoler logiquement le trafic et le diriger vers le pare-feu. En outre, le trafic de gestion est découplé de tout autre trafic en le plaçant sur son propre vSwitch externe.

©2023 Palo Alto Networks, Inc.



 ©2023 Palo Alto Networks, Inc.

Configuration système requise sur Hyper-V

Le VM-Series exige une allocation minimum de ressource sur l'hôte Hyper-V, aussi veillez à respecter les exigences indiquées ci-dessous pour assurer des performances optimales.

- Le processeur de l'hôte doit être un processeur 64-bit x86 Intel ou AMD avec extension de virtualisation.
- Reportez-vous à la section Configuration système requise pour VM-Series pour la configuration matérielle minimale requise pour votre modèle VM-Series.
- Au minimum deux cartes réseau. Le pare-feu VM-Series prend en charge les cartes réseau synthétiques, qui fournissent de meilleures performances que les cartes réseau émulées. Hyper-V prend en charge jusqu'à huit cartes réseau synthétiques.
- Reportez-vous à la Matrice de compatibilité pour connaître les versions de Windows Server prises en charge.

  Le serveur hyper-V n'a pas d'interface graphique ; toute la configuration est effectuée avec PowerShell. Cependant, vous pouvez utiliser Hyper-V Manager tournant sur une machine à distance pour gérer le pare-feu. Si vous utilisez le module Hyper-V role add-on, vous pouvez gérer le pare-feu en utilisant Hyper-V Manager ou PowerShell.
- Le pare-feu VM-Series prend en charge SR-IOV/PCI-Passthrough.

  DPDK n'est pris en charge qu'avec les périphériques SRIOV Nvidia/Mellanox(Mlx5). Le mode Trunk (Tronc) avec SR-IOV n'est pas pris en charge.

©2023 Palo Alto Networks, Inc.

Services d'intégration Linux

Les services d'intégration Linux (Linux Integration Services ; LIS) sont un ensemble de pilotes et services qui améliorent les performances des machines virtuelles basées sur Linux sur Hyper-V. Le pare-feu VM-Series prend en charge les services suivants pour améliorer l'intégration entre l'hôte et la machine virtuelle :

- **Arrêt progressif**—Vous permet d'effectuer un arrêt progressif du pare-feu VM-Series depuis l'interface de gestion Hyper-V sans devoir vous connecter à l'invité.
- **Pulsation vers Hyper-V Manager**—Fournit la surveillance des pulsations de l'état de fonctionnement des VM invitées à partir de l'interface de gestion Hyper-V.
- **Visibilité de l'adresse IP de gestion du pare-feu**—Vous permet d'utiliser Hyper-V Manager pour afficher l'adresse IP attribuée à l'interface de gestion sur le pare-feu.

©2023 Palo Alto Networks, Inc.

Installation du pare-feu VM-Series sur Hyper-V

Utilisez les instructions présentées dans cette section pour déployer votre pare-feu VM-Series sur un hôte Hyper-V. Un compte de support Palo Alto Networks et une licence VM-Series valide sont requis pour télécharger le fichier image VHDX et installer le VM-Series sur l'hôte Hyper-V. Si vous n'avez pas encore enregistré dans votre compte le code d'autorisation de capacité contenu dans l'e-mail de confirmation de commande que vous avez reçu, avec votre compte de support, reportez-vous à la section Enregistrement du pare-feu VM-Series. Une fois l'enregistrement terminé, continuez les tâches suivantes :

- Avant de commencer
- Réglage des performances du pare-feu VM-Series sur Hyper-V
- Configuration du pare-feu VM-Series sur un hôte Hyper-V avec Hyper-V Manager
- Configuration du pare-feu VM-Series sur un hôte Hyper-V avec PowerShell
- Configuration initiale sur le pare-feu VM-Series

Avant de commencer

Avant d'installer et de configurer votre pare-feu VM-Series, vous devez connaître et prendre en compte les éléments suivants lorsque vous configurez votre pare-feu VM-Series :

- Types de commutateur virtuel
- Usurpation d'adresse MAC

Types de commutateur virtuel

Avant d'installer le VM-Series, vous devez créer les vSwitch nécessaires en vue de fournir la connectivité externe pour l'accès de gestion et pour l'acheminement du trafic en provenance et à destination des machines virtuelles que le pare-feu sécurisera. Hyper-V vous permet de créer trois types de vSwitch :

- **vSwitch externe** : se lie à une carte réseau physique et fournit l'accès vSwitch à un réseau physique.
- **vSwitch interne** : transmet le trafic entre les machines virtuelles et l'hôte Hyper-V. Ce type de vSwitch ne fournit aucune connectivité à une connexion réseau physique.
- **vSwitch privé** : transmet le trafic entre les machines virtuelles vers l'hôte Hyper-V uniquement.

Un vSwitch externe est requis la gestion du pare-feu VM-Series. Les autres vSwitch connectés au pare-feu VM-Series peuvent être de n'importe quel type et dépendront de la topologie de votre réseau.

Usurpation d'adresse MAC

Si vous déployez le pare-feu VM-Series avec des interfaces activées en mode couche 3, assurez-vous d'utiliser les adresses MAC attribuées par l'hyperviseur afin que l'hyperviseur et le pare-feu puissent gérer correctement les paquets. En alternative, utilisez Hyper-V manager pour autoriser l'usurpation d'adresse MAC sur la carte réseau virtuelle pour chaque interface du dataplane sur le pare-feu. Pour plus d'informations, consultez Adresses MAC attribuées par l'hyperviseur.

©2023 Palo Alto Networks, Inc.

Si vous déployez le pare-feu VM-Series avec des interfaces activées en mode couche 2 ou en mode câble virtuel, vous devez activer l'usurpation d'adresse MAC sur la carte réseau virtuelle dans Hyper-V pour chaque interface du dataplane sur le pare-feu. Ce réglage est requis pour assurer que les paquets envoyés par le VM-Series ne soient pas abandonnés par la carte réseau virtuelle si l'adresse MAC source ne correspond pas à l'adresse MAC de l'interface sortante.

Réglage des performances du pare-feu VM-Series sur Hyper-V

Le pare-feu VM-Series pour Hyper-V est un appareil haute performance, mais il peut nécessiter un réglage de l'hyperviseur pour obtenir les meilleurs résultats. Cette section décrit quelques bonnes pratiques et recommandations pour faciliter les meilleures performances du pare-feu VM-Series.

- Désactivation des files d'attente de machine virtuelle
- Isolation des ressources du processeur dans un nœud NUMA

Désactivation des files d'attente de machine virtuelle

Palo Alto Networks recommande de désactiver les files d'attente de machine virtuelle (VMQ) pour toutes les NIC (cartes réseau) sur l'hôte Hyper-V. Cette option est sujette à une mauvaise configuration et peut entraîner des performances réseau réduites lorsqu'elle est activée.

STEP 1 | Connectez-vous à Hyper-V Manager et sélectionnez votre machine virtuelle.

STEP 2 | Sélectionnez **Settings (Paramètres)** > **Hardware (Matériel)** > **Network Adapter (Carte réseau)** > **Hardware Acceleration (Accélération matérielle)**.

STEP 3 | Sous la file d'attente de la machine virtuelle, décochez la case **Enable virtual machine queue (Activer la file d'attente de machine virtuelle)**.

STEP 4 | Cliquez sur **Apply (Appliquer)** pour enregistrer vos modifications et **OK** pour quitter les paramètres de la machine virtuelle.

Isolation des ressources du processeur dans un nœud NUMA

Vous pouvez améliorer les performances de VM-Series pour Hyper-V en isolant les ressources du processeur de la machine virtuelle client sur un seul nœud NUMA (Non-Uniform Memory Access). Vous pouvez afficher les paramètres NUMA de votre machine virtuelle dans Hyper-V Manager en sélectionnant **Settings (Paramètres)** > **Hardware (Matériel)** > **Processor (Processeur)** > **NUMA**.

Configuration du pare-feu VM-Series sur un hôte Hyper-V avec Hyper-V Manager

Utilisez ces instructions pour déployer le pare-feu VM-Series sur Hyper-V en utilisant Hyper-V Manager.

STEP 1 | Téléchargez le fichier VHAX.

Enregistrez votre pare-feu VM-Series et obtenez le fichier VHAX.

1. Accédez à https://www.paloaltonetworks.com/services/support.
2. Filtrez par **PAN-OS for VM-Series Base Images (Images de base PAN-OS pour VM-Series)** et téléchargez le fichier VHAX. Par exemple, PA-VM-HPV-7.1.0.vhdx.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Configurez tous les vSwitch nécessaires.

Pour créer un vSwitch :

1. Dans Hyper-V Manager, sélectionnez l'hôte et sélectionnez **Action** > **Virtual Switch Manager (Gestionnaire de commutateur virtuel)** pour ouvrir la fenêtre Gestionnaire de commutateur virtuel.
2. Dans **Create virtual switch (Créer un commutateur virtuel)**, sélectionnez le type de vSwitch (externe, interne ou privé) à créer et cliquez sur **Create Virtual Switch (Créer un commutateur virtuel)**.

STEP 3 | Installez le pare-feu.

1. Sur Hyper-V Manager, sélectionnez l'hôte et sélectionnez **Action** > **New (Nouveau)** > **Virtual Machine (Machine virtuelle)**. Configurez les paramètres suivants dans l'assistant de nouvelle machine virtuelle :
   1. Choisissez un **Name (Nom)** et un **Location (Emplacement)** pour le pare-feu VM-Series. Le pare-feu VM-Series stocke le fichier VHAX à l'emplacement spécifié.
   2. Choisissez **Generation 1 (Génération 1)**. Il s'agit de l'option par défaut et de la seule version prise en charge.
   3. Pour **Startup Memory (Mémoire de démarrage)**, affectez la mémoire en fonction de la configuration système requise pour VM-Series de votre modèle VM-Series.

      N'activez pas la mémoire dynamique ; le pare-feu VM-Series exige une allocation de mémoire statique.

   4. Configurez le **Networking (Réseau)**. Sélectionnez un vSwitch externe pour connecter l'interface de gestion sur le pare-feu.
   5. Pour connecter le **Virtual Hard Disk (Disque dur virtuel)**, sélectionnez **Use an existing virtual hard disk (Utiliser un disque dur virtuel existant)** et recherchez le fichier VHAX que vous avez téléchargé au préalable.
   6. Examinez le récapitulatif et cliquez sur **Finish (Terminer)**.
2. Attribuez les processeurs virtuels au pare-feu.
   1. Sélectionnez la VM que vous avez créée et accédez à **Action** > **Settings (Paramètres)**.
   2. Sélectionnez **Processor (Processeur)** et entrez le nombre minimum de processeurs en fonction de la configuration système requise pour VM-Series de votre modèle VM-Series.
   3. Cliquez sur **OK**.

STEP 4 | Connectez au moins une carte réseau pour l'interface du dataplane sur le pare-feu.

1. Sélectionnez **Settings (Paramètres)** > **Hardware (Matériel)** > **Add Hardware (Ajouter du matériel)** et sélectionnez le **Hardware type (Type de matériel)** pour votre carte réseau.

   Carte réseau héritée et SR-IOV ne sont pas pris en charge. Si ces options sont sélectionnées, le pare-feu redémarrera en mode maintenance.

2. Cliquez sur **OK**.

©2023 Palo Alto Networks, Inc.

STEP 5 | (Facultatif) Activez l'usurpation d'adresse sur Hyper-V si vous n'utilisez pas la couche 3 avec une adresse MAC attribuée par l'hyperviseur.

1. Effectuez un double clic sur la carte réseau virtuelle du dataplane et cliquez sur **Advanced Settings (Paramètres avancés)**.
2. Cliquez sur la case **Enable MAC address spoofing (Activer l'usurpation des adresses MAC)** et cliquez sur **Apply (Appliquer)**.

STEP 6 | Mettez le pare-feu sous tension.

Sélectionnez le pare-feu dans la liste des **Virtual Machines (Virtual Machines)** et accédez à **Action** > **Start (Démarrer)** pour démarrer le pare-feu.

Configuration du pare-feu VM-Series sur un hôte Hyper-V avec PowerShell

Utilisez ces instructions pour déployer le pare-feu VM-Series sur Hyper-V en utilisant PowerShell.

STEP 1 | Téléchargez le fichier VHAX.

Enregistrez votre pare-feu VM-Series et obtenez le fichier VHAX.

1. Accédez à https://www.paloaltonetworks.com/services/support.
2. Filtrez par **PAN-OS for VM-Series Base Images (Images de base PAN-OS pour VM-Series)** et téléchargez le fichier VHAX. Par exemple, PA-VM-HPV-7.1.0.vhdx**.**

STEP 2 | Configurez tous les vSwitch nécessaires.

Créez un vSwitch à l'aide des commandes suivantes. Donnez au vSwitch un nom et choisissez le type de commutateur.

```
> New-VMSwitch -Name <"switch-name"> -SwitchType <switch-type>
```

STEP 3 | Installez le pare-feu VM-Series.

1. Créez la nouvelle machine virtuelle et définissez la mémoire en fonction de la configuration système requise pour VM-Series de votre modèle VM-Series.

```
> NEW-VM -Name <vm-name> -MemoryStartupBytes 4GB -
VHDPath <file-path-to-vhdx>
```

2. Définissez le nombre de processeurs en fonction de la configuration système requise pour VM-Series de votre modèle VM-Series.

```
> SET-VMProcessor –VMName <vm-name> –Count 2
```

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Connectez au moins une carte réseau pour l'interface de gestion sur le pare-feu.

Connectez la carte réseau par défaut créée durant la création de la VM pour le vSwitch de gestion.

```
> connect-VMNetworkAdapter -vmname <vm-name> -Name <"network-adapter-name"> -SwitchName <"management-vswitch">
```

STEP 5 | (Facultatif) Activez l'usurpation d'adresse sur Hyper-V si vous n'utilisez pas la couche 3 avec une adresse MAC attribuée par l'hyperviseur.

```
> Set-VMNetworkAdapter -vmname <vm-name> -Name <"network-adapter-name"> -MacAddressSpoofing On
```

STEP 6 | Mettez le pare-feu sous tension.

Par exemple :

```
> Start-VM -vmname <vm-name>
```

Configuration initiale sur le pare-feu VM-Series

Utilisez ces instructions pour effectuer la configuration initiale de votre pare-feu VM-Series. Par défaut, le pare-feu VM-Series utilise DHCP pour obtenir une adresse IP pour l'interface de gestion. Cependant, vous pouvez attribuer une adresse IP statique. Une fois la configuration initiale terminée, accédez à l'interface Web pour effectuer d'autres tâches de configuration. Si vous utilisez Panorama pour la gestion centralisée, reportez-vous au Guide de l'administrateur Panorama pour plus d'informations sur la gestion du périphérique à l'aide de Panorama.

Si vous utilisez l'amorçage pour effectuer la configuration de votre pare-feu VM-Series sur Hyper-V, reportez-vous à la section Amorçage du pare-feu VM-Series sur Hyper-V. Pour plus d'informations sur l'amorçage, reportez-vous à la section Amorçage du pare-feu VM-Series.

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

- Adresse IP du port de gestion
- netmask
- Passerelle par défaut
- Adresse IP du serveur DNS

STEP 2 | Accédez à la console du pare-feu VM-Series.

1. Dans Hyper-V Manager, sélectionnez le pare-feu VM-Series et cliquez sur **Connecter** dans la liste Action.
2. Connectez-vous au pare-feu avec le nom d'utilisateur et mot de passe par défaut : **admin/admin**
3. Passez en mode Configuration en utilisant la commande suivante : **configure**

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configurez les paramètres d'accès réseau pour l'interface de gestion.

Entrez les commandes suivantes :

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> netmask <netmask>
default-gateway <gateway-IP> dns-settingservers primary <DNS-IP>
```

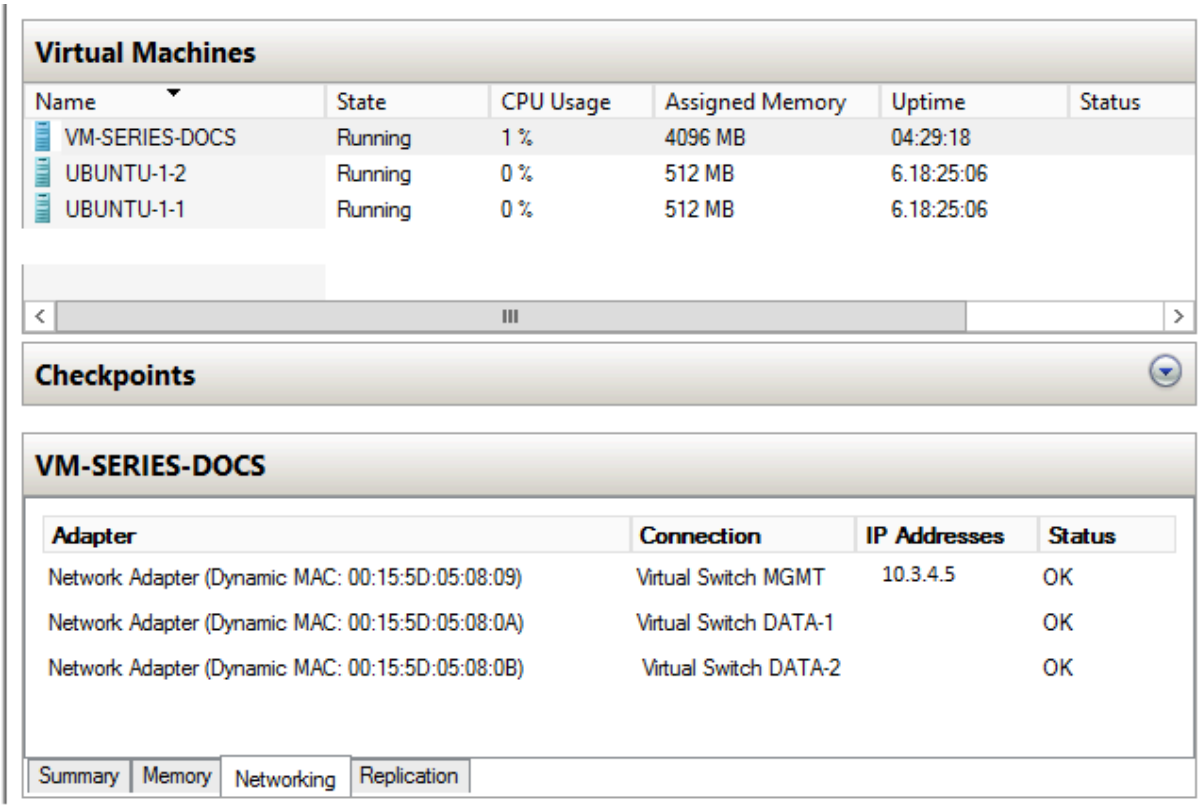
où *<Firewall-IP>* est l'adresse IP que vous voulez affecter à l'interface de gestion, *<netmask>* est le masque de sous-réseau, *<gateway-IP>* est l'adresse IP de la passerelle réseau et *<DNS-IP>* est l'adresse IP du serveur DNS.

STEP 4 | Validez vos modifications et quittez le mode Configuration.

1. Saisissez **commit**.
2. Saisissez **exit**.

STEP 5 | Vérifiez que vous voir l'adresse IP de l'interface de gestion depuis Hyper-V Manager.

1. Sélectionnez le pare-feu VM-Series dans la liste **Virtual Machines (Machines virtuelles)**.
2. Sélectionnez **Networking (Mise en réseau)**. La première carte réseau qui s'affiche dans la liste est utilisée pour l'accès de gestion au pare-feu ; les cartes suivantes dans la liste sont utilisées comme interfaces du dataplane sur le pare-feu.



 ©2023 Palo Alto Networks, Inc.

STEP 6 | Vérifiez l'accès réseau aux services externes nécessaire à la gestion de pare-feu, notamment au serveur de mise à jour Palo Alto Networks.

1. Utilisez l'utilitaire Ping pour vérifier la connectivité réseau au serveur Palo Alto Networks Update, comme illustré dans l'exemple suivant. Vérifiez que la résolution DNS se produit et que la réponse inclut l'adresse IP du serveur de mise à jour ; le serveur de mise à jour ne répond pas à une demande Ping.

```
admin@PA-220 > ping host updates.paloaltonetworks.com
```

```
PING updates.paloaltonetworks.com (10.101.16.13) 56(84)
 bytes of data. From 192.168.1.1 icmp_seq=1 Destination Host
 Unreachable From 192.168.1.1 icmp_seq=2 Destination Host
 Unreachable From 192.168.1.1 icmp_seq=3 Destination Host
 Unreachable From 192.168.1.1 icmp_seq=4 Destination Host
 Unreachable
```

Après avoir vérifié la résolution DNS, appuyez sur Ctrl + C pour arrêter la requête ping.

2. Utilisez la commande CLI suivante pour extraire des informations sur le droit de support pour le pare-feu à partir du serveur de mise à jour Palo Alto Network :

```
request support check
```

Si vous disposez de la connectivité, le serveur de mise à jour répond avec l'état de support pour votre pare-feu.

STEP 7 | (Facultatif) Vérifiez que votre configuration de trame jumbo VM-Series ne dépasse pas le MTU maximum pris en charge sur Hyper-V.

Le VM-Series possède une taille de MTU par défaut de 9 216 octets lorsque les trames jumbo sont activées. Toutefois, la taille de MTU maximum prise en charge par la carte réseau physique sur l'hôte Hyper-V est de 9 000 ou 9 014 octets selon les capacités de la carte réseau. Pour vérifier le MTU configuré sur Hyper-V :

1. Dans Windows Server 2012 R2, ouvrez le **Control Panel (Panneau de configuration)** et accédez à **Network and Internet (Réseau et Internet)** > **Network and Sharing Center (Centre Réseau et partage)** > **View network status and tasks (Afficher l'état et la gestion du réseau)**.
2. Cliquez sur une carte réseau ou un commutateur virtuel dans la liste.
3. Cliquez sur **Properties (Propriétés)**.
4. Cliquez sur **Configure (Configurer)**.
5. Sur l'onglet Advanced (Avancé), sélectionnez **Jumbo Packet (Paquet Jumbo)** dans la liste.
6. Sélectionnez 9 000 ou 9 014 octets dans le menu déroulant Value (Valeur).
7. Cliquez sur **OK**.

Si vous avez activé les trames jumbo sur Hyper-V, activez les trames Jumbo sur le pare-feu VM-Series et configurez la taille de MTU pour la faire correspondre à la taille configurée sur l'hôte Hyper-V.

©2023 Palo Alto Networks, Inc.

STEP 8 | Accédez à l'interface Web du pare-feu VM-Series, puis configurez les interfaces et définissez des règles de sécurité et des règles NAT afin d'activer en toute sécurité les applications que vous souhaitez sécuriser.

Reportez-vous au Guide de l'administrateur PAN-OS.

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur Azure

Le pare-feu VM-Series sur Azure apporte les fonctionnalités de sécurité du pare-feu de dernière génération Palo Alto Networks en tant que machine virtuelle dans l'Azure Marketplace. Le pare-feu de la série VM fournit un ensemble complet de fonctionnalités de sécurité pour assurer que vos charges de travail et vos données de machine virtuelle sont protégées, et les capacités que le pare-feu permet sont différentes des caractéristiques de sécurité indigènes comme les groupes de sécurité, les pare-feux d'applications Web et les pare-feux de ports originaux.

Sur Azure, le pare-feu VM-Series est disponible en modèle Bring Your Own License (BYOL) ou en modèle Pay-As-You-Go (paiement à l'usage ; PAYG) horaire. Microsoft Azure vous permet de déployer le pare-feu pour sécuriser vos charges de travail au sein du réseau virtuel dans le cloud, de sorte que vous puissiez déployer une solution de cloud public ou étendre les infrastructures informatiques internes pour créer une solution hybride.

- À propos du pare-feu VM-Series sur Azure
- Déploiements pris en charge sur Azure
- Déploiement du pare-feu VM-Series depuis l'Azure Marketplace (modèle de solution)
- Déploiement du pare-feu VM-Series depuis l'Azure China Marketplace (modèle de solution)
- Déploiements orchestrés par Panorama dans Azure
- Création d'une image personnalisée VM-Series pour Azure
- Utilisez les recommandations du Centre de sécurité Azure pour sécuriser vos charges de travail
- Déploiement du pare-feu VM-Series dans Azure Stack
- Activer Azure Application Insights sur le pare-feu VM-Series
- Surveillance VM sur Azure
- Configuration de la HA active/passive sur Azure
- Utilisation du modèle ARM pour déployer le pare-feu VM-Series
- Déploiement du modèle VM-Series et Azure Application Gateway
- Sécurisation des services Kubernetes dans Azure

À propos du pare-feu VM-Series sur Azure

Le pare-feu VM-Series sur Azure doit être déployé dans un réseau virtuel (VNet) en utilisant le mode de déploiement gestionnaire de ressources. Vous pouvez déployer le pare-feu VM-Series sur le cloud public Azure standard, Azure China et Azure Government, y compris le DoD sur Azure Government, qui répond aux exigences de sécurité relatives aux données DoD Impact de niveau 5 et aux normes FedRAMP élevées.

Le pare-feu VM-Series sur le Marketplace pour le cloud public Azure, Azure Government et les régions Azure DoD prend en charge le modèle BYOL (Bring Your Own License) et l'option PAYG (Pay-As-You-Go) horaire (mise sous licence basée sur l'utilisation). Pour plus de détails sur la mise sous licence, reportez-vous à la section Types de licence : pare-feu VM-Series et à la liste des régions Azure prises en charge dans lesquelles vous pouvez déployer le pare-feu VM-Series.

Pour Azure China, le pare-feu de série VM est disponible dans l'option BYOL seulement. Voir Deploy the VM-Series Firewall from the Azure China Marketplace (Solution Template) (Déployer le Pare-feu de la série VM à partir du marché chinois d'Azure (modèle de solution)) pour le flux de travail.

Vous pouvez également déployer le pare-feu de la série VM sur Azure Stack, la solution Cloud privée de Microsoft qui vous permet d'utiliser les services Azure dans le centre de données de votre organisation. Avec Azure Stack, vous pouvez construire une solution Cloud hybride qui unifie votre déploiement public d'Azure avec votre installation sur place d'Azure Stack. Vous pouvez télécharger l'offre de pare-feu de la série VM à partir du marché Azure et la mettre à la disposition de vos locataires sur la cheminée Azure. Pour plus d'informations, reportez-vous à la section Déployer le pare-feu VM-Series sur Azure Stack.

- Mise en réseau Azure et pare-feu VM-Series
- Intégration du Centre de sécurité Azure
- Modèles de pare-feu VM-Series sur Azure
- Configuration système minimale requise pour le VM-Series sur Azure
- Prise en charge de la haute disponibilité sur VM-Series sur Azure

Mise en réseau Azure et pare-feu VM-Series

L'infrastructure VNet Azure n'exige pas que les machines virtuelles disposent d'une interface réseau dans chaque sous-réseau. L'architecture inclut une table de routage interne (appelée itinéraires système) qui connecte directement toutes les machines virtuelles au sein d'un VNET de sorte que le trafic soit automatiquement transféré à une machine virtuelle dans n'importe quel sous-réseau. Pour une adresse IP de destination qui ne se trouve pas au sein du VNet, le trafic est envoyé à la passerelle Internet par défaut ou à une passerelle VPN, si elle est configurée. Pour diriger le trafic à travers le pare-feu VM-Series, vous devez créer des itinéraires définis par l'utilisateur (UDR) qui spécifient le saut suivant pour le trafic quittant un sous-réseau. Cet itinéraire force le trafic destiné à un autre sous-réseau à aller vers le pare-feu VM-Series au lieu d'utiliser les itinéraires du système pour accéder directement à la machine virtuelle dans l'autre sous-réseau. Par exemple, dans une application à deux niveaux avec un niveau Web et un niveau base de données, vous pouvez configurer des UDR pour diriger le trafic entre le sous-réseau Web et le sous-réseau base de données à travers le pare-feu VM-Series.

©2023 Palo Alto Networks, Inc.

Sur Azure, les UDR servent uniquement pour le trafic quittant un sous-réseau. Vous ne pouvez pas créer des itinéraires définis par l'utilisateur pour spécifier comme le trafic en provenance d'Internet entre dans un sous-réseau ou pour diriger le trafic vers des machines virtuelles au sein d'un sous-réseau. Les UDR vous permettent de diriger le trafic sortant vers une interface sur le pare-feu VM-Series afin que vous puissiez toujours vous assurer que le pare-feu sécurise également le trafic vers Internet.

Pour la documentation sur Microsoft Azure, reportez-vous à https://azure.microsoft.com/fr-fr/documentation.

Les modèles de solution pour le déploiement du pare-feu VM-Series qui sont disponibles dans l'Azure Marketplace possèdent trois interfaces réseau. Pour procéder à la Configuration de la HA active/passive sur Azure, vous devrez ajouter une interface supplémentaire pour le lien HA2. Si vous voulez personnaliser le modèle, utilisez les modèles ARM qui sont disponibles dans le référentiel GitHub.

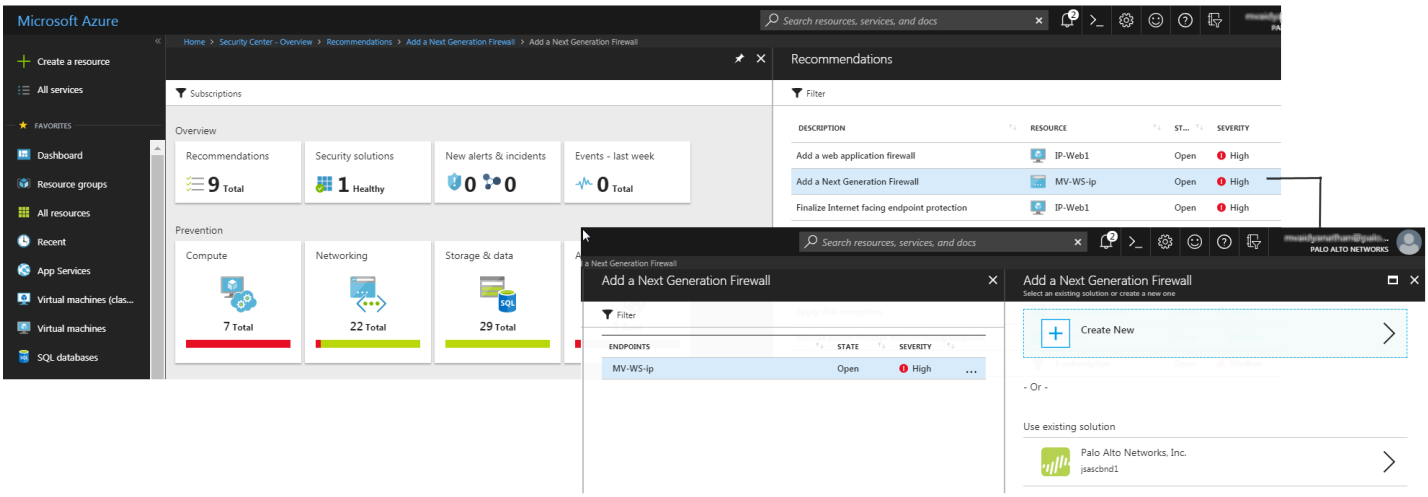
Intégration du Centre de sécurité Azure

Microsoft a arrêté la prise en charge du Centre de sécurité Azure pour les solutions de sécurité partenaires et l'a remplacée par Azure Sentinel.

Le pare-feu VM-Series est intégré au Centre de sécurité Azure pour fournir une vue unifiée de surveillance et d'alerte sur la position de sécurité de vos charges de travail Azure. Dans le Centre de sécurité Azure, le pare-feu VM-Series est disponible en tant que solution de sécurité partenaire, qui protège vos charges de travail Azure contre les menaces et atténue les éventuelles lacunes dans la sécurisation de votre entreprise et de votre propriété intellectuelle dans le cloud public. Pour activer cette intégration et afficher les journaux en tant qu'événements de sécurité, directement sur le tableau de bord du Centre de sécurité Azure, le pare-feu VM-Series sur Azure inclut un profil de transfert de journal par défaut.

Pour commencer, vous devez activer le Centre de sécurité Azure sur votre abonnement Azure. Vous disposez alors de deux façons d'activer cette intégration :

- **Déployer un pare-feu VM-Series en fonction d'une recommandation du tableau de bord d'Azure Security Center**.



Lorsque le tableau de bord d'Azure Security Center recommande de déployer un pare-feu VM-Series pour protéger une charge de travail exposée à Internet, vous ne pouvez déployer le pare-feu que dans un nouveau groupe de ressources ou un groupe de ressources existant qui est vide.

 ©2023 Palo Alto Networks, Inc.

C'est parce que Azure vous empêche actuellement de déployer un appareil multi-NIC dans un groupe de ressources existant. Par conséquent, après avoir déployé le pare-feu VM-Series, vous devez le configurer manuellement pour qu'il se trouve dans le chemin du trafic de la charge de travail que vous devez sécuriser.

Lorsque vous déployez le pare-feu à partir d'Azure Security Center, le pare-feu est lancé avec trois interfaces réseau : gestion, externe (non-sécurisé) et interne (sécurisé) – et une route définie par l'utilisateur (UDR) qui envoie tout le trafic sortant du sous-réseau sécurisé à l'interface sécurisée sur le pare-feu afin que le trafic Internet soit toujours inspecté par le pare-feu. La configuration par défaut inclut deux exemples de règles de stratégie de sécurité : la règle par ***outbound-default (défaut sortante)*** autorise tout le trafic de la zone d'approbation vers la zone non fiable sur le port par défaut de l'application, et la règle par ***inbound-default (défaut entrante)*** qui autorise tout le trafic de navigation Web depuis la zone non-sécurisé vers la zone sécurisé, après avoir inspecté le trafic avec les profils de sécurité antivirus, antispyware et de protection contre les vulnérabilités par défaut. Le pare-feu transfère également tous les fichiers interceptés au moyen de la règle entrante ou sortante vers le cloud public WildFire pour en faire l'analyse. Ces deux règles incluent un profil de filtrage d'URL qui bloque tout le trafic vers les catégories d'URL violation des droits d'auteur, dynamique-DNS, extrémisme, logiciels malveillants, hameçonnage et inconnues. Outre ces profils de sécurité, les deux règles de politique de sécurité sont activées pour journaliser à la fin de la session et pour transférer les journaux des menaces et des envois WildFire en tant qu'alertes de sécurité vers le tableau de bord du Centre de sécurité Azure.

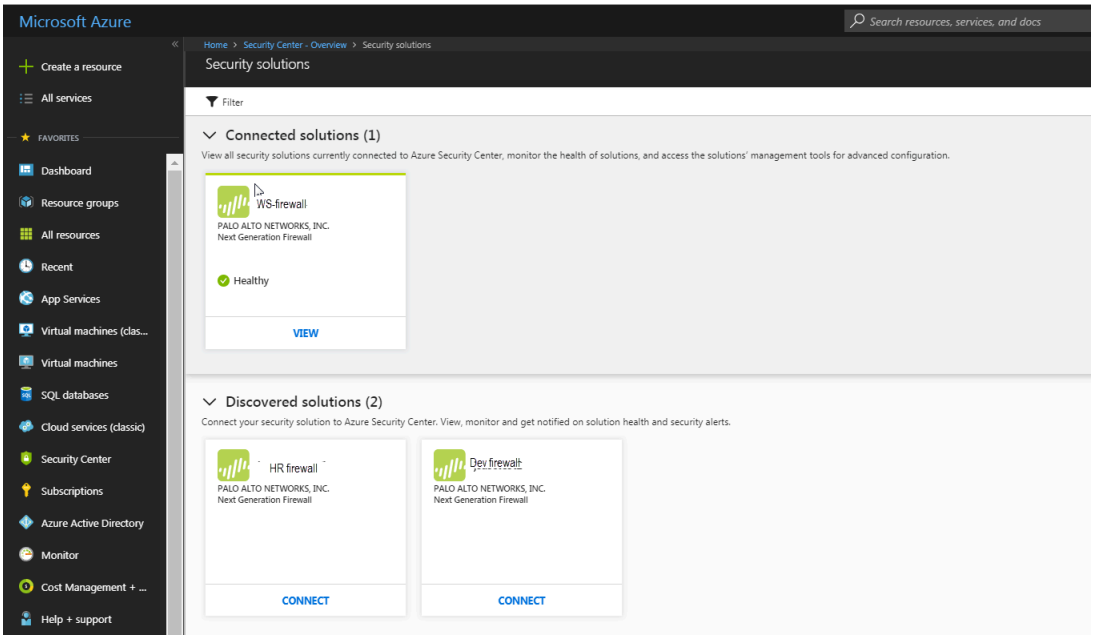
Pour faire usage de cette intégration et Déployer un pare-feu de série VM en fonction d'une recommandation du Centre de sécurité Azure au sein du même groupe de ressources que les charges de travail que vous souhaitez sécuriser, vous pouvez mettre en place une charge de travail avec une adresse IP publique exposée à Internet. Lorsque le Centre de sécurité Azure détecte le risque pour la sécurité, il déclenche une recommandation de déploiement d'un pare-feu de prochaine génération, et vous pouvez alors déployer le pare-feu de la série VM dans un nouveau groupe de ressources dans lequel vous pouvez ajouter vos charges de travail plus tard. Vous devez alors supprimer la charge de travail que vous avez échelonnée pour déclencher la recommandation.

- **Sélectionnez un pare-feu VM-Series que vous avez déjà déployé pour sécuriser vos charges de travail.** Si vous avez un abonnement standard au centre de sécurité Azure, le centre de sécurité Azure découvre et affiche tous les pare-feu de la série VM que vous avez déployés à partir du Azure Marketplace ou en utilisant un déploiement personnalisé avec le CLI Azure, PowerShell ou

 ©2023 Palo Alto Networks, Inc.

le modèle ARM. Les pare-feu de votre abonnement Azure sont regroupés sous Security Solutions (Solutions de sécurité) dans le tableau de bord d'Azure Security Center.

Microsoft Azure ne prend pas en charge la détection des pare-feu existants avec l'abonnement au niveau gratuit.



Pour Connecter un pare-feu de série VM existant à partir du centre de sécurité Azure, vous devez configurer une machine virtuelle Linux et configurer le transfert Syslog pour transférer les journaux de pare-feu au Common Event Format (format d'événements courants) en tant qu'alertes à Azure Security Center. La configuration supplémentaire permet une vue unique pour la surveillance de tous vos actifs Azure.

Le transfert d'un volume important de journaux vers le Centre de sécurité Azure peut entraîner des frais d'abonnement supplémentaires.

Modèles de pare-feu VM-Series sur Azure

Vous pouvez déployer le pare-feu VM-Series sur Azure en utilisant des modèles. Palo Alto Networks propose deux types de modèles : les modèles de solution et les modèles ARM.

- **Modèles de solution dans l'Azure Marketplace** — Les modèles de solution qui sont disponibles dans l'Azure Marketplace vous permettent de déployer le pare-feu VM-Series en utilisant le portail Azure. Vous pouvez utiliser un groupe de ressources et un compte de stockage existants (ou en créer de nouveaux) pour déployer le pare-feu VM-Series avec les paramètres par défaut suivants pour toutes les régions, à l'exception d'Azure China :
  - CIDR VNet 10.8.0.0/16 ; vous pouvez personnaliser le CIDR sur une plage d'adresses IP privées différente.
  - Trois sous-réseaux : 10.8.0.0/24 (gestion), 10.8.1.0/24 (non approuvé), 10.8.2.0/24 (approuvé)

©2023 Palo Alto Networks, Inc.

- Trois interfaces réseau, une dans chaque sous-réseau. Si vous personnalisez le CIDR VNet, les plages de sous-réseau se mappent selon vos modifications.

Pour utiliser le modèle de solution, reportez-vous à la section Déploiement du pare-feu VM-Series depuis l'Azure Marketplace (modèle de solution). Pour Azure China, reportez-vous à la section Déploiement du pare-feu VM-Series depuis l'Azure China Marketplace (modèle de solution).

- **Modèles ARM dans le référentiel GitHub** — En plus des déploiements basés sur le Marketplace, Palo Alto Networks fournit des modèles de gestionnaire de ressources Azure dans le référentiel GitHub pour simplifier le processus de déploiement du pare-feu VM-Series sur Azure.
  - Utilisation du modèle ARM pour déployer le pare-feu VM-Series — Le modèle ARM inclut deux fichiers JSON (un fichier de modèle et un fichier de paramètres) pour vous aider à déployer et configurer toutes les ressources au sein du VNet en une seule opération coordonnée. Ces modèles sont fournis dans le cadre d'une politique de support en tant que telle.

    Si vous voulez utiliser la CLI Azure pour localiser toutes les images disponibles de Palo Alto Networks, vous aurez besoin des détails suivants pour compléter la commande (show vm-image list) :

    - ***Publisher (Éditeur) : paloaltonetworks***
    - ***Offer (Offre) : vmseries-flex***
    - ***SKU : byol, bundle1, bundle2***
    - ***Version : 10.0.0 ou ultérieure***
  - Déploiement du modèle VM-Series et Azure Application Gateway pour prendre en charge une architecture de sécurité évolutive qui protège vos applications Web connectées à Internet à l'aide de deux pare-feu VM-Series entre une paire d'équilibreurs de charge Azure (externes et internes) VM-Series et Azure Application Gateway. Ce modèle n'est actuellement pas disponible pour Azure China.
  - Utilisez le modèle ARM pour déployer le pare-feu VM-Series dans un groupe de ressources existant, par exemple lorsque vous souhaitez Configuration de la HA active/passive sur Azure.

En plus des modèles ARM ci-dessus qui sont couverts par la politique de support officielle de Palo Alto Networks, Palo Alto Networks fournit des modèles pris en charge par la communauté dans le référentiel GitHub de Palo Alto Networks qui vous permettent d'explorer les solutions disponibles pour l'automatisation du cloud et la mise à l'échelle sur Azure.

Configuration système minimale requise pour le VM-Series sur Azure

Vous devez déployer le pare-feu VM-Series en mode gestionnaire de ressources Azure (ARM) uniquement ; le mode classique (déploiements basés sur la gestion de service) n'est pas pris en charge. Le pare-feu VM-Series sur Azure doit satisfaire les exigences suivantes :

 ©2023 Palo Alto Networks, Inc.

- VM Linux Azure des types suivants : modèles pris en charge.

  Ces types incluent la prise en charge de la mise en réseau accélérée (SR-IOV).
- Pour la mémoire, le disque et les cœurs de processeur requis pour déployer le pare-feu VM-Series, reportez-vous à la section Configuration système requise pour VM-Series.

  Vous pouvez ajouter de l'espace disque supplémentaire de 40 Go à 8 To à des fins de journalisation. Le pare-feu VM-Series utilise les disques gérés Azure si disponibles ; il n'utilise pas le disque temporaire fourni par Azure avec certains types d'instances.
- Jusqu'à huit interfaces réseau (NIC). Une interface principale est requise pour l'accès de gestion, et jusqu'à sept interfaces pour le trafic de données.

  Sur Azure, puisqu'une machine virtuelle n'a besoin d'aucune interface réseau dans chaque sous-réseau, vous pouvez configurer le pare-feu VM-Series avec trois interfaces réseau (une pour le trafic de gestion et deux pour le trafic du dataplane). Pour créer des règles de politique basées sur les zones, en plus de l'interface de gestion, vous avez besoin d'au moins deux interfaces du dataplane afin de pouvoir attribuer une interface du dataplane à la zone ***approuvée*** et l'autre interface du dataplane à la zone ***non approuvée***. Pour un déploiement HA, vous aurez besoin d'une autre interface pour la liaison HA2 entre les homologues HA.

  Puisque le VNet Azure est un réseau de couche 3, le pare-feu VM-Series sur Azure prend en charge uniquement les interfaces de couche 3.

Prise en charge de la haute disponibilité sur VM-Series sur Azure

Pour garantir la disponibilité, vous pouvez procéder à la Configuration de la HA active/passive sur Azure dans une configuration traditionnelle avec une synchronisation des sessions ou utiliser une architecture de mise à l'échelle à l'aide d'équilibreurs de charge natifs du cloud tels qu'Azure Application Gateway ou Azure Load Balancer pour distribuer le trafic sur un ensemble d'instances saines du pare-feu. Pour plus de détails, reportez-vous à la section Déploiement du modèle VM-Series et Azure Application Gateway.

Autorisations principales de VM-Series sur le service Azure

Pour que Panorama puisse interagir avec les API Azure et recueillir des informations sur vos charges de travail, vous devez créer une application Azure Active Directory et un principal de service qui dispose des autorisations requises pour s'authentifier auprès d'Azure AD et accéder aux ressources de votre abonnement.

Pour créer l'application Active Directory et le principal de service, suivez les instructions de la section Comment utiliser le portail pour créer une application Azure AD et un principal de service qui peut accéder aux ressources. Au cours du processus de génération de l'application, il y a une étape pour attribuer l'application à un rôle et attribuer un rôle IAM de lecteur à l'application.

Si vous ne disposez pas des autorisations nécessaires pour créer et enregistrer l'application AD, demandez à votre administrateur Azure AD ou à celui de votre abonnement de créer un principal de service.

Après l'enregistrement de l'application, notez ces valeurs afin de pouvoir les saisir ultérieurement dans le plugin Panorama pour Azure :

- ID de l'application

 ©2023 Palo Alto Networks, Inc.

- Clé secrète (notez-la lorsque vous créez la clé secrète ; elle n'est pas visible une fois que vous avez quitté la page).
- ID de locataire

Autorisations

Le tableau suivant indique les rôles intégrés minimum requis, ainsi que les autorisations granulaires si vous souhaitez personnaliser le rôle.

Prise en charge	Permissions
Haute disponibilité Azure	Reportez-vous à la section Configuration de la HA active/passive sur Azure.
Azure Application Insights Activer Azure Application Insights sur le pare-feu VM-Series	**"Microsoft.Authorization/*/read",** **"Microsoft.Network/networkInterfaces/*",** **"Microsoft.Network/networkSecurityGroups/*",** **"Microsoft.Network/virtualNetworks/*",** **"Microsoft.Compute/virtualMachines/read"**
Surveillance Azure Configuration du plugin Azure pour la surveillance sur Panorama	Nécessite un rôle minimum de **Reader (Lecteur)** pour le principal de service. Vous pouvez également ajouter les autorisations personnalisées suivantes : **"Microsoft.Compute/virtualMachines/read",** **"Microsoft.Network/networkInterfaces/read",** **"Microsoft.Network/virtualNetworks/read",** **"Microsoft.Network/locations/serviceTags/read"** **"Microsoft.Network/loadBalancers/read",** **"Microsoft.Network/publicIPAddresses/read"** **"Microsoft.Resources/subscriptions/resourcegroups/read",**
Déploiements orchestrés par Panorama Créez un rôle personnalisé et associez-le à un Active Directory (AD)	**"Microsoft.Resources/subscriptions/resourcegroups/*",** **"Microsoft.Resources/deployments/write",** **"Microsoft.Resources/deployments/operationStatuses/read",** **"Microsoft.Resources/deployments/read",** **"Microsoft.Resources/deployments/delete"**
	"Microsoft.Network/publicIPPrefixes/write",

©2023 Palo Alto Networks, Inc.

Prise en charge	Permissions
	"Microsoft.Network/publicIPPrefixes/read", "Microsoft.Network/publicIPPrefixes/delete", "Microsoft.Network/publicIPAddresses/write", "Microsoft.Network/publicIPAddresses/read", "Microsoft.Network/publicIPAddresses/delete", "Microsoft.Network/publicIPAddresses/join/action",
	"Microsoft.Network/natGateways/write", "Microsoft.Network/natGateways/read", "Microsoft.Network/natGateways/delete", "Microsoft.Network/natGateways/join/action",
	"Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/write", "Microsoft.Network/virtualNetworks/delete", "Microsoft.Network/virtualNetworks/subnets/write", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/delete", "Microsoft.Network/virtualNetworks/subnets/join/action",
	"Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read",
	"Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/delete", "Microsoft.Network/networkSecurityGroups/join/action",
	"Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/read",

©2023 Palo Alto Networks, Inc.

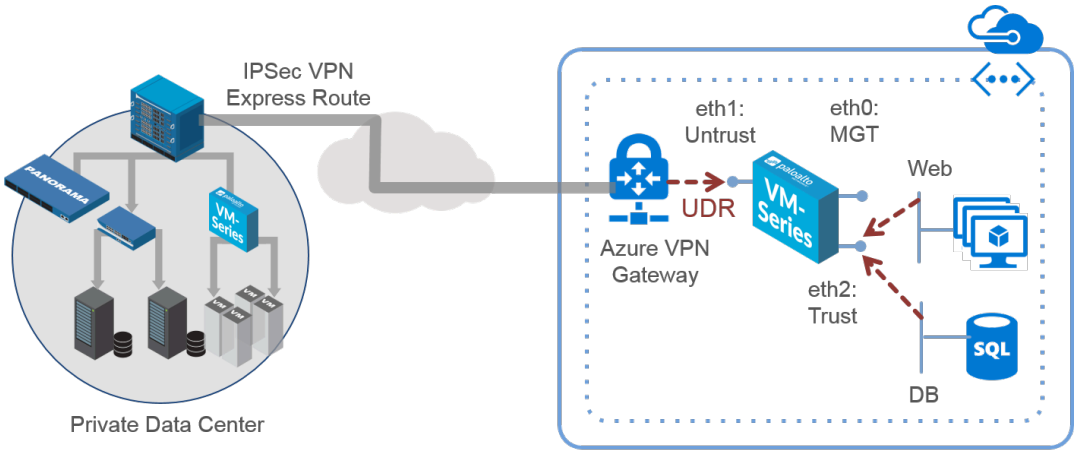
Prise en charge	Permissions
	"Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/probes/join/action", "Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
	"Microsoft.Network/locations/serviceTags/read",
	"Microsoft.Network/applicationGateways/read", "Microsoft.Network/networkInterfaces/read",
	"Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Compute/virtualMachineScaleSets/read", "Microsoft.Compute/virtualMachineScaleSets/delete", "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
	"Microsoft.Compute/virtualMachines/read",
	"Microsoft.Compute/images/read",
	"Microsoft.insights/components/write", "Microsoft.insights/components/read", "Microsoft.insights/components/delete",
	"Microsoft.insights/autoscalesettings/write"

©2023 Palo Alto Networks, Inc.

Déploiements pris en charge sur Azure

Utilisez le pare-feu VM-Series sur Azure pour sécuriser vos utilisateurs réseau dans les scénarios suivants :

- **Hybride et VNet vers VNet** : le pare-feu VM-Series sur Azure vous permet d'étendre en sécurité votre centre de données physique/cloud privé dans Azure en utilisant IPSec et ExpressRoute. Pour améliorer la sécurité de votre centre de données, si vous avez segmenté votre réseau et déployé vos charges de travail dans des VNet séparés, vous pouvez sécuriser le trafic circulant entre les VNet avec un tunnel IPSec et des politiques qui autorisent le trafic d'applications.



- **Inter-sous-réseau** : le pare-feu VM-Series peut servir de façade à vos serveurs dans un VNet et les protéger contre les menaces latérales pour le trafic inter-sous-réseau entre les applications dans une architecture à plusieurs niveaux.
- **Passerelle** : le pare-feu VM-Series sert de passerelle VNet pour protéger les déploiements vers Internet dans le réseau virtuel Azure (VNet). Le pare-feu VM-Series sécurise le trafic destiné aux serveurs dans le VNet et il protège également contre les menaces latérales pour le trafic inter-sous-réseau entre les applications dans une architecture à plusieurs niveaux.
- **GlobalProtect** : utilisez l'infrastructure Azure pour déployer rapidement et facilement le pare-feu VM-Series comme protection globale GlobalProtect™ et étendre votre politique de sécurité de passerelle aux utilisateurs et périphériques distants, quel que soit l'emplacement.

Vous pouvez continuer avec Déploiement du pare-feu VM-Series depuis l'Azure Marketplace (modèle de solution), Déploiement du pare-feu VM-Series dans Azure Stack, ou Orchestration d'un déploiement de pare-feu VM-Series dans Azure.

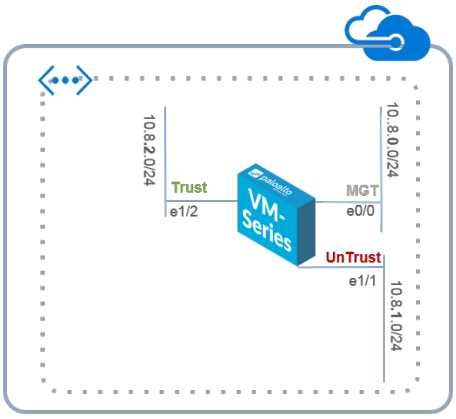
Vous pouvez également en apprendre davantage sur les modèles de pare-feu VM-Series sur Azure que vous pouvez utiliser pour déployer le pare-feu.

Pour en savoir plus sur l'amorçage, reportez-vous à la section Amorçage du pare-feu VM-Series.

©2023 Palo Alto Networks, Inc.

Déploiement du pare-feu VM-Series depuis l'Azure Marketplace (modèle de solution)

Les instructions suivantes décrivent la façon de déployer le modèle de solution pour le pare-feu de la série VM qui est disponible dans l'Azure® Government Marketplace. Pour utiliser les modèles Azure Resource Manager (ARM) personnalisables disponibles dans le référentiel GitHub, reportez-vous à la section Utilisation du modèle ARM pour déployer le pare-feu VM-Series.



STEP 1 | Configurez un compte Azure.

1. Si vous n'en avez pas déjà, créez-vous un compte Microsoft®.
2. Ouvrez une session sur le portail Azure (**`https://portal.azure.com`** ou **`https://portal.azure.us`**) en utilisant vos justificatifs d'identité de compte Microsoft.

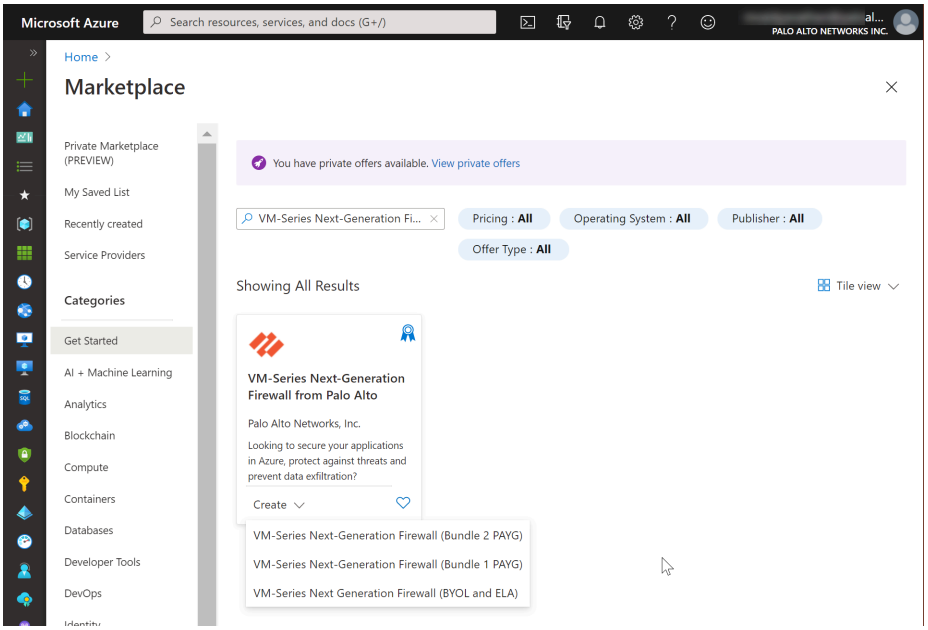
   *Si vous utilisez un abonnement d'essai, vous pourriez avoir besoin d'ouvrir une requête de prise en charge (**Help + Support (Aide + Assistance)** > **New Support Request (Nouvelle demande de prise en charge)**) pour augmenter le quota de cœurs de machines virtuelles attribués.*

STEP 2 | Trouvez le modèle de solution VM-Series dans l'Azure Marketplace.

1. Sélectionnez **Marketplace** > **Virtual Machines (Machines virtuelles)**.
2. Recherchez Palo Alto Networks® et une liste de pare-feu VM-Series s'affichera. Pour connaître les différences entre les modèles BYOL - Bring your own licence (apportez votre

©2023 Palo Alto Networks, Inc.

propre licence) et PAYG - Pay as you go (paiement à l'usage), reportez-vous à la section Licences de pare-feu VM-Series pour les clouds publics.



3. Sélectionnez une offre pour **Create (Créer)** un nouveau pare-feu VM-Series.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Déployez le pare-feu.

1. Configurez les paramètres de base pour le pare-feu.

   1. Sélectionnez votre **Subscription (Abonnement)** Azure.
   2. Créez un nouveau groupe de ressources ou sélectionnez un groupe de ressources existant qui soit vide. Le groupe de ressources aura toutes les ressources associées au pare-feu VM-Series pour ce déploiement.

      Azure a supprimé l'option permettant de sélectionner un groupe de ressources existant pour les solutions Marketplace qui activent plusieurs cartes réseau. (network interface controllers) NICs. Pour déployer le pare-feu dans un groupe de ressources existant, utilisez le modèle ARM dans le référentiel GitHub ou votre propre modèle ARM personnalisé.
   3. Sélectionnez la **Region (Région)** Azure dans laquelle vous déployez le pare-feu.
   4. Saisissez un **Username (Nom d'utilisateur)** pour l'administrateur du pare-feu.
   5. Sélectionnez l'**Authentication Type (Type d'authentification)** : mot de passe ou clé publique SSH.

      Vous devez activer l'authentification par clé SSH si vous prévoyez d'utiliser le pare-feu en mode opérationnel FIPS-CC. Bien que vous puissiez déployer le pare-feu VM-Series en utilisant un nom d'utilisateur et un mot de passe, vous ne pourrez pas vous authentifier en utilisant le nom d'utilisateur et le mot de passe après avoir modifié le mode opérationnel en FIPS-CC. Après être repassé en mode FIPS-CC, vous devez utiliser la clé SSH pour vous connecter et pouvoir ensuite configurer un nom d'utilisateur et un mot de passe que vous pourrez utiliser pour une connexion ultérieure à l'interface Web du pare-feu. Pour plus de détails sur la création de la clé SSH, reportez-vous à la documentation Azure.
   6. Saisissez un **Password (Mot de passe)** (31 caractères maximum) ou effectuez un copier-coller d'une **SSH public key (Clé publique SSH)** pour la sécurisation de l'accès administratif au pare-feu.
2. Configurez la mise en réseau.

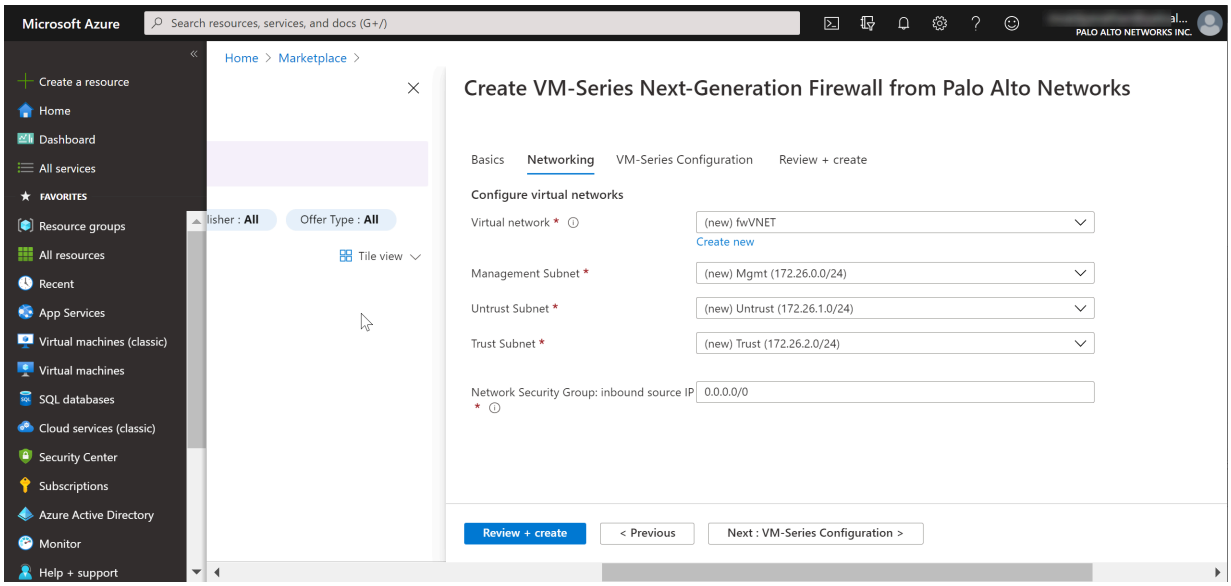
   1. Sélectionnez un réseau Azure Virtual Network (VNet) existant ou créez-en un nouveau, et entrez l'adresse IP pour le réseau virtuel (VNet). Par défaut, l'adresse IP CIDR (Classless Inter-Domain Routing) est 10.8.0.0/16.
   2. Configurez les sous-réseaux pour les interfaces réseau.

      Si vous utilisez les sous-réseaux par défaut, vous devez vérifier la configuration. Si vous utilisez un réseau virtuel existant (VNet), vous devez avoir défini trois sous-réseaux : un pour chacune des interfaces de gestion, approuvée et non approuvée. Si vous créez un nouveau VNet, vérifiez ou modifiez les préfixes de chaque sous-réseau. Les sous-réseaux par défaut sont 10.8.0.0/24 pour le sous-réseau de gestion, 10.8.1.0/24 pour le sous-réseau non approuvé et 10.8.2.0/24 pour le sous-réseau approuvé.
   3. Saisissez l'adresse IP source ou la plage IP (inclure le bloc CIDR) pouvant accéder au réseau virtuel. **Network Security Group: inbound source IP (Groupe de sécurité**

©2023 Palo Alto Networks, Inc.

réseau : IP source entrante) vous permet de limiter l'accès entrant au réseau virtuel Azure.

Restreindre l'accès au pare-feu. Assurez-vous de fournir un bloc CIDR qui correspond à votre réseau ou vos adresses IP de gestion dédiées. Ne rendez pas la plage de réseau source autorisée plus grande que nécessaire et ne configurez jamais la source autorisée comme 0.0.0.0/0. Vérifiez votre adresse IP avant de la configurer sur le modèle afin de vous assurer de ne pas rester bloqué.



3. Définissez l'accès de gestion au pare-feu.

   1. Utilisez la variable par défaut ((new) fwMgmtPublicIP) pour attribuer une **Public IP address** (Adresse IP publique) à l'interface de gestion (`eth0`) du pare-feu.

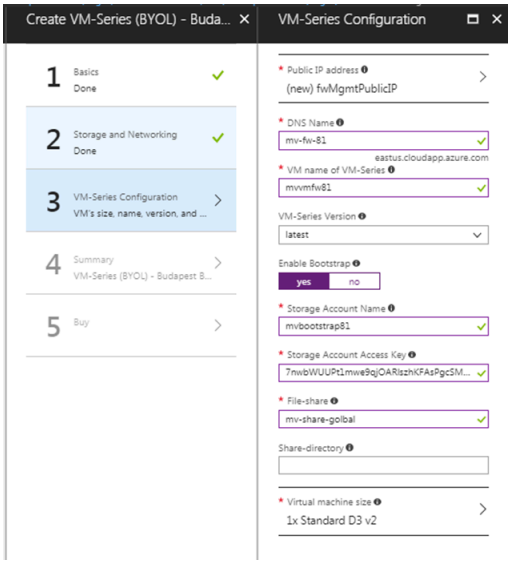
      La mise en réseau accélérée Azure n'est pas prise en charge sur l'interface de gestion.

   2. Saisissez un préfixe pour accéder au pare-feu en utilisant un nom de DNS. Vous devez combiner le préfixe que vous avez saisi avec le suffixe affiché à l'écran

©2023 Palo Alto Networks, Inc.

pour accéder à l'interface Web du pare-feu. Par exemple : ***<yourname><your-region>*.cloudapp.azure.com**

3. Sélectionnez le **VM-Series Version** le plus récent.
4. Saisissez un nom d'affichage permettant d'identifier le pare-feu VM-Series au sein du groupe de ressources.

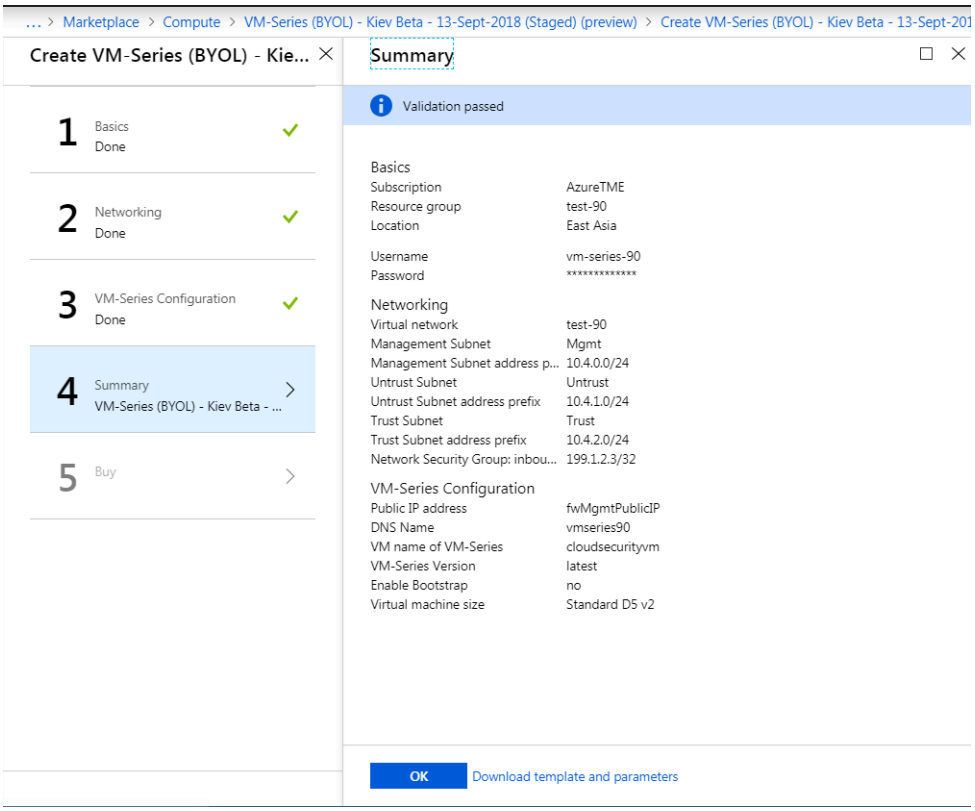


4. Ajoutez les informations pour configurer le pare-feu au lancement. Reportez-vous à la section Amorçage du pare-feu VM-Series dans Azure.
   1. Sélectionnez **yes (oui)** pour **Enable Bootstrap (Activer Bootstrap)**.
   2. Saisissez le **Storage Account Name (Nom du compte de stockage)** qui contient le Ensemble d'amorçage.
   3. Saisissez le **Storage Account Access (Compte de stockage)**. Ce pare-feu a besoin de cette clé d'accès pour s'authentifier auprès du compte de stockage et accéder aux fichiers stockés à l'intérieur.
   4. Ajoutez le **File share name (Nom du partage de fichiers)** auquel vous avez téléchargé les fichiers requis pour le démarrage du pare-feu. Le compte de stockage doit se trouver dans la même région que celle dans laquelle vous déployez le pare-feu et il doit disposer de la structure de dossier appropriée pour l'amorçage.
   5. Sélectionnez le niveau et la taille de la machine virtuelle Azure selon vos besoins. Utilisez le lien **Change size** (Changer la taille) pour afficher les types d'instances pris en

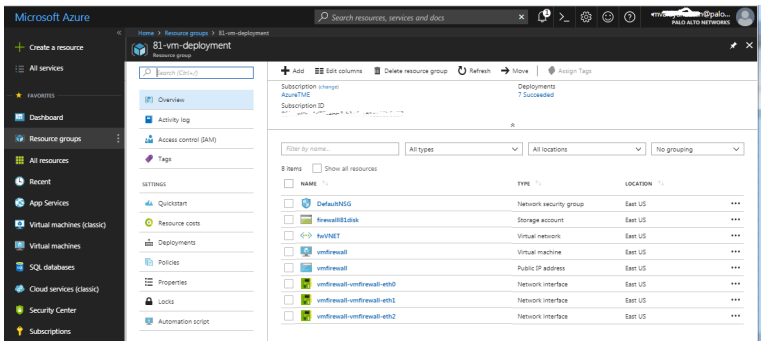
 ©2023 Palo Alto Networks, Inc.

charge et pour examiner la Configuration système minimale requise pour le VM-Series sur Azure.

5. Examinez le résumé et **OK**. Acceptez ensuite les conditions d'utilisation et la politique de confidentialité, puis cliquez sur **Create (Créer)** pour déployer le pare-feu.



6. Vérifiez que vous avez correctement déployé le pare-feu VM-Series.
   1. Sélectionnez **Dashboard (Tableau de bord)** > **Resource Groups (Groupes de ressources)** et sélectionnez le groupe de ressources.
   2. Sélectionnez votre groupe de ressources et consultez le **Overview (Apperçu)** pour connaître l'état détaillé sur lequel les ressources ont été déployées avec succès.

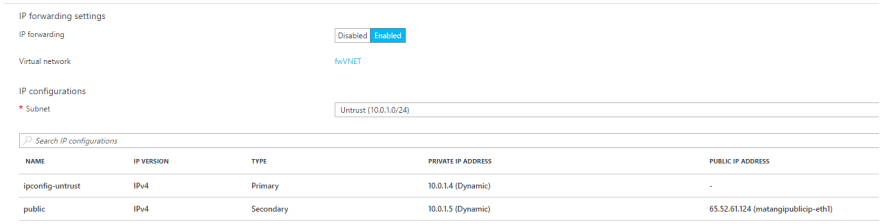


STEP 4 | Associez une adresse IP publique pour l'interface non approuvée du pare-feu VM-Series. Lorsque vous créez une nouvelle adresse IP publique, vous en obtenez une du bloc d'adresses IP que possède Microsoft, donc vous ne pouvez donc pas en choisir une spécifique.

©2023 Palo Alto Networks, Inc.

Le nombre maximal d'adresses IP publiques que vous pouvez attribuer à une interface est basé sur votre abonnement Azure.

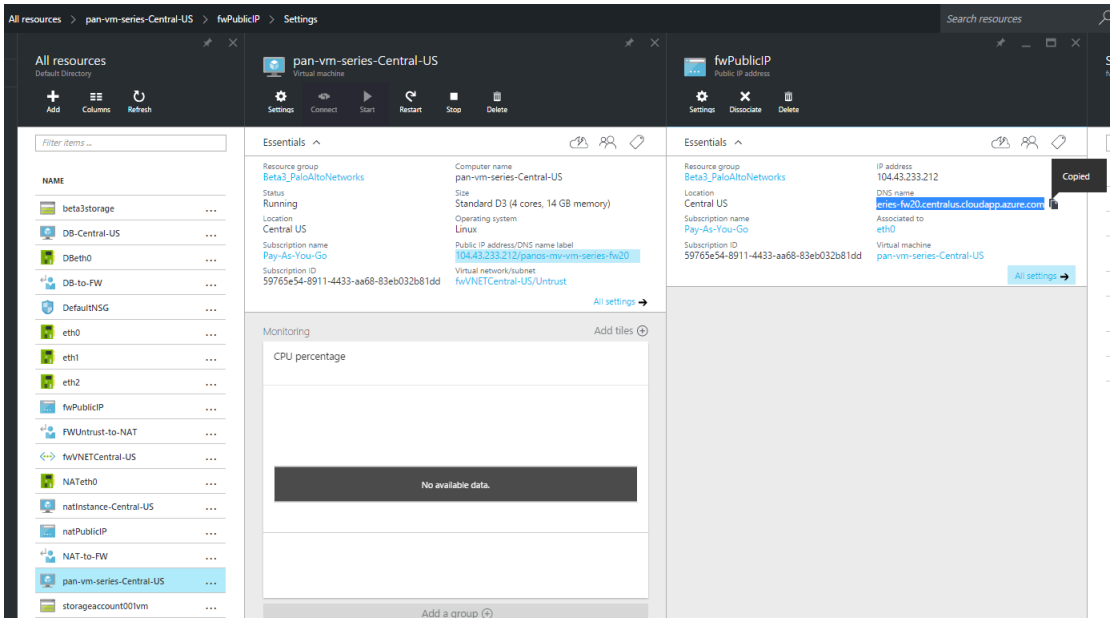
1. Sur le portail Azure, sélectionnez l'interface réseau pour laquelle vous souhaitez ajouter une adresse IP publique. (Par exemple, l'interface **eth1**).
2. Sélectionnez **IP Configurations (Configurations IP)** > **Add (Ajouter)** et, pour l'adresse IP publique, sélectionnez **Enabled (Activé)**. Créez une nouvelle adresse IP publique ou sélectionnez-en une disponible.
3. Vérifiez que vous pouvez afficher l'adresse IP secondaire associée à l'interface.



Lorsque vous associez une adresse IP secondaire à une interface réseau, le pare-feu VM-Series n'acquiert pas automatiquement l'adresse IP privée affectée à l'interface. Vous devrez configurer manuellement l'adresse IP privée à l'aide de l'interface Web du pare-feu VM-Series. Reportez-vous à l'étape Configurez les interfaces réseau du dataplane en tant qu'interfaces de couche 3 sur le pare-feu**.**

STEP 5 | Connectez-vous à l'interface Web du pare-feu.

1. Sur le portail Azure, dans **All Resources (Toutes les ressources)**, sélectionnez le pare-feu VM-Series et consultez le nom de DNS complet pour le pare-feu.



1. À l'aide d'une connexion sécurisée (https) depuis votre navigateur Web, connectez-vous au nom DNS du pare-feu.
2. Saisissez le nom d'utilisateurmot de passe que vous avez défini dans le fichier de paramètres. Vous verrez un avertissement de certificat mais il n'y a pas de problème - continuez vers la page Web.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Activez les licences sur le pare-feu VM-Series.

Pour la version BYOL

1. Créez un compte de support.
2. Enregistrez le pare-feu VM-Series (avec code d'autorisation).
3. Sur l'interface Web du pare-feu, sélectionnez **Device (Périphérique)** > **Licenses (Licenses)** et sélectionnez **Activate feature using authentication code (Activer la fonctionnalité à l'aide du code d'autorisation)**.
4. Saisissez le code d'autorisation de capacité (***auth-code***) enregistré sur le portail de support. Le pare-feu se connecte alors au serveur de mise à jour (`updates.paloaltonetworks.com`), télécharge la licence et redémarre automatiquement.
5. Connectez-vous à nouveau à l'interface Web et confirmez les éléments suivants sur le **Dashboard (Tableau de bord)** :
   - Un numéro de série valide s'affiche dans **Serial# (N° de série)**.

     Si le terme `Unknown(Inconnu)` s'affiche, cela signifie que le périphérique n'est pas sous licence. Pour afficher les journaux de trafic sur le pare-feu, vous devez installer une licence de capacité valide.
   - Le **VM Mode (Mode VM)** affiche Microsoft Azure.

Pour la version PAYG

1. Créez un compte de support.
2. Enregistrement modèle basé sur l'utilisation du pare-feu VM-Series pour les clouds publics (sans code d'autorisation).

STEP 7 | Configurez les interfaces réseau du plan de données en tant qu'interfaces de couche 3 sur le pare-feu.

Si vous hébergez plusieurs sites Web ou services avec des adresses IP et des certificats SSL différents sur un seul serveur, vous devrez peut-être configurer plusieurs adresses IP sur les interfaces de pare-feu VM-Series.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
2. Cliquez sur **ethernet 1/1** et configurez comme suit :
   - Définissez **Interface Type (Type d'interface)** sur **Layer3 (Couche 3)** (par défaut).
   - Dans l'onglet **Config (Configuration)**, affectez l'interface au routeur par défaut.
   - Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Définissez une nouvelle zone appelée **`Non approuvée`**, puis cliquez sur **OK**.
   - Dans l'onglet **IPv4**, sélectionnez **DHCP Client** (Client DHCP) si vous envisagez d'attribuer une seule adresse IP sur l'interface. Le pare-feu acquiert automatiquement l'adresse IP privée attribuée dans le modèle ARM. Si vous envisagez d'attribuer plus

 ©2023 Palo Alto Networks, Inc.

d'une adresse IP, sélectionnez **Static (Statique)** et entrez manuellement les adresses IP principale et secondaire attribuées à l'interface sur le portail Azure.

- Désactivez (effacez) **Créer automatiquement la route par défaut vers la passerelle par défaut fournie par le serveur** pour garantir que le trafic géré par cette interface ne soit pas transmis directement à la passerelle par défaut du réseau virtuel.

3. Cliquez sur **ethernet 1/2** et configurez comme suit :
   - Définissez **Interface Type (Type d'interface)** sur **Layer3 (Couche 3)** (par défaut).
   - Définissez la **Zone de destination** à **Trust (Confiance)**.
   - Définissiez **IP address (l'adresse IP) DHCP Client (Client DHCP)** ou **Static (Statique)**.
   - Désactivez (effacez) **Créer automatiquement la route par défaut vers la passerelle par défaut fournie par le serveur**pour garantir que le trafic géré par cette interface ne soit pas transmis directement à la passerelle par défaut du réseau virtuel.
4. **Commit (Valider)** vos modifications et vérifiez que l'état du lien de l'interface est actif.
5. Ajouter une route statique sur le routeur virtuel du pare-feu VM-Series pour tous les réseaux que le pare-feu doit acheminer.

   Par exemple, pour ajouter un itinéraire par défaut aux sous-réseaux de destination pour les serveurs que le pare-feu fixe :
   - Sélectionnez **Network (Réseau)** > **Virtual Router (routeur virtuel - VR)** > **default (par défaut)** >
   - Sélectionnez **Static Routes (Itinéraires statiques)** > **IPv4** et ajoutez l'adresse IP du saut suivant pour les serveurs de destination. Vous pouvez régler x.x.x.1 comme adresse IP suivante pour tout le trafic (destiné à 0.0.0.0/0 à partir de l'interface ethernet1/1).

STEP 8 | Configurez le pare-feu pour votre déploiement spécifique.

- **Gateway (Passerelle)** : déployez un équilibreur de charge tiers en façade de la zone Non approuvée.
- **Hybrid and Inter-VNet** : déployez une passerelle VPN Azure ou une machine virtuelle NAT en façade de la zone Non approuvée.
- **Inter-Subnet** : sur le pare-feu VM-Series, ajoutez une règle de politique de sécurité intrazone pour autoriser le trafic sur la base des sous-réseaux associé à l'interface Approuvée.
- **GlobalProtect™** : déployez une machine virtuelle NAT en façade de la zone Non approuvée.

STEP 9 | Dirigez le trafic vers le pare-feu VM-Series.

1. Pour vous assurer que le pare-feu VM-Series sécurise tout le trafic au sein du groupe de ressources Azure, configurez des itinéraires statiques sur le pare-feu.
2. Configurez les itinéraires définis par l'utilisateur pour diriger tout le trafic à travers les interfaces sur le pare-feu VM-Series. Consultez la documentation Azure sur les UDR pour plus de détails.

   Les itinéraires définis par l'utilisateur sur les sous-réseaux internes doivent envoyer tout le trafic via l'interface Approuvée. Les itinéraires définis par l'utilisateur sur le côté Non approuvé dirigent tout le trafic provenant d'Internet à travers l'interface Non approuvée sur le pare-feu VM-Series. Le trafic provenant d'Internet peut provenir d'une Azure Application

 ©2023 Palo Alto Networks, Inc.

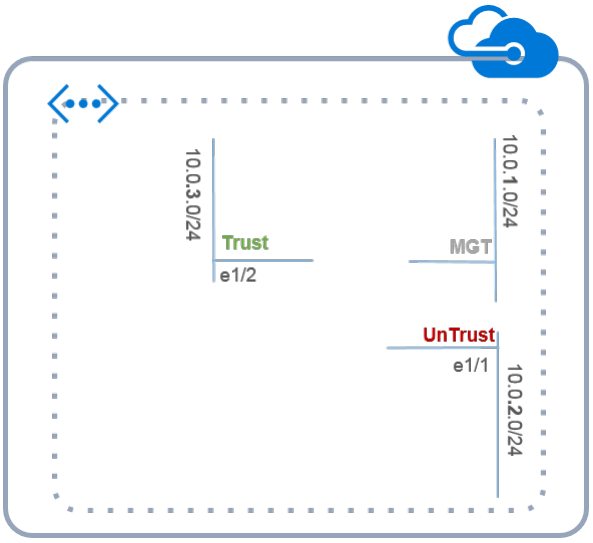
Gateway ou d'un équilibreur de charge Azure, ou de la passerelle VPN Azure en cas de déploiement hybride qui connecte votre réseau interne avec le cloud Azure.

STEP 10 | Pour publier des statistiques PAN-OS® sur Azure Application Insights, voir Enable Azure Application Insights on the VM-Series Firewall (Activer Azure Application Insights sur le pare-feu VM-Series).

©2023 Palo Alto Networks, Inc.

Déploiement du pare-feu VM-Series depuis l'Azure China Marketplace (modèle de solution)

Les instructions suivantes vous montrent comment déployer le modèle de solution pour le pare-feu VM-Series qui est disponible dans l'Azure China Marketplace. L'Azure China Marketplace ne prend en charge que le modèle BYOL du pare-feu VM-Series. Vous pouvez déployer le pare-feu dans un groupe de ressources existant vide ou dans un nouveau groupe de ressources. Le réseau virtuel par défaut dans le modèle est 10.0.0.0/16 et il déploie un pare-feu VM-Series avec 3 interfaces réseau, une interface de gestion et deux interfaces du dataplane, comme illustré ci-dessous. Pour utiliser les modèles ARM personnalisables disponibles dans le référentiel GitHub, reportez-vous à la section Utilisation du modèle ARM pour déployer le pare-feu VM-Series.



STEP 1 | Configurez un compte Azure.

1. Créez un compte Microsoft.
2. Connectez-vous au portail Azure (**`https://portal.azure.com`**) en utilisant vos justificatifs d'identité de compte Microsoft.

> *Si vous utilisez un abonnement d'essai, vous pourriez avoir besoin d'ouvrir une requête de prise en charge (**Help + Support (Aide + Assistance)** > **New Support Request (Nouvelle demande de prise en charge)**) pour augmenter le quota de cœurs de machines virtuelles attribués.*

©2023 Palo Alto Networks, Inc.

STEP 2 | Trouvez le modèle de solution VM-Series dans l'Azure Marketplace.

1. Recherchez Palo Alto Networks sur l'Azure Marketplace Chinois (https://market.azure.cn). L'offre pour les différentes versions de PAN-OS des pare-feu VM-Series s'affiche.



2. Sélectionnez une offre et cliquez sur **Immediate deployment of (Déploiement immédiat de)**.

STEP 3 | Déployez le pare-feu.

1. Sélectionnez votre **Subscription (Abonnement)** Azure.
2. Sélectionnez un groupe de ressources pour contenir toutes les ressources associées au pare-feu VM-Series dans ce déploiement.

   Vous pouvez déployer le pare-feu VM-Series dans un nouveau groupe de ressources ou un groupe de ressources existant vide. Pour déployer le pare-feu dans un groupe de ressources existant disposant d'autres ressources, utilisez le modèle ARM dans le référentiel GitHub ou votre propre modèle ARM personnalisé. Assurez-vous que les ressources existantes correspondent aux valeurs de paramètre fournies dans le modèle ARM.

   1. Si vous créez un nouveau groupe de ressources, saisissez un nom pour le groupe de ressources et sélectionnez la région Azure China dans laquelle vous souhaitez déployer le pare-feu.
   2. Si vous sélectionnez un groupe de ressources existant, sélectionnez la région Azure China pour ce groupe de ressources et sélectionnez le déploiement complet.
3. Configurez les paramètres de base pour le pare-feu.
   1. Saisissez le nom du compte de stockage pour un compte existant ou créez-en un nouveau.
   2. Entrez le nom du conteneur de stockage blob sur lequel l'image vhd du pare-feu mage sera copiée et enregistrée.
   3. Entrez un nom de DNS pour accéder à l'adresse IP publique sur l'interface de gestion (eth0) du pare-feu. Pour accéder à l'interface web du pare-feu,

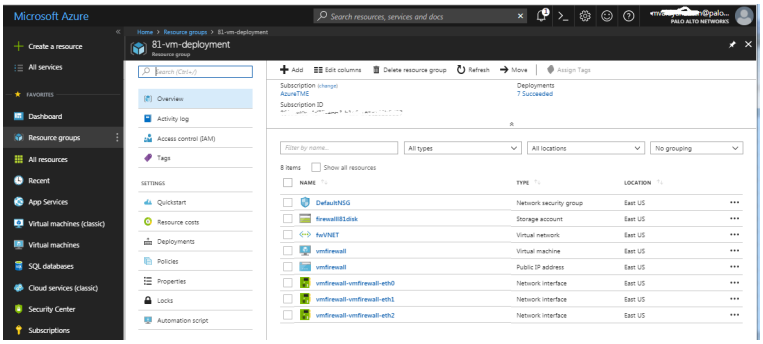
©2023 Palo Alto Networks, Inc.

vous devez combiner le préfixe que vous saisissez avec le suffixe, par exemple <yourDNSname><china_region>.cloudapp.azure.com.

4. Saisissez un **Username (Nom d'utilisateur)** pour l'administrateur du pare-feu.
5. Entrez un **Password (Mot de passe)** pour sécuriser l'accès administratif au pare-feu.
6. Sélectionnez le niveau et la taille de la machine virtuelle Azure selon vos besoins. Reportez-vous à la section Configuration système minimale requise pour le VM-Series sur Azure.
7. Saisissez un **VmName (Nom VM)** permettant d'identifier le pare-feu VM-Series au sein du groupe de ressources.
8. Utiliser un **PublicIPAddressName (Nom d'adresse IP publique)** pour étiqueter l'interface de gestion du pare-feu dans le groupe de ressources. Microsoft Azure lie le nom de DNS que vous avez défini avec ce nom afin que vous puissiez accéder à l'interface de gestion sur le pare-feu à partir de l'Internet public.
9. Saisissez un **VirtualNetworkNam (Nom du réseau virtuel)** pour identifier votre réseau virtuel (VNet). L'**Address Prefix (Préfixe d'adresse)** de l'adresse IP par défaut pour le réseau virtuel est 10.0.0.0/16. Vous pouvez le changer pour répondre à vos besoins d'adressage IP.
10. Configurez les sous-réseaux pour les interfaces réseau. Si vous utilisez un réseau virtuel existant, vous devez avoir défini trois sous-réseaux, un pour chacune des interfaces de gestion, approuvée et non approuvée. Si vous créez un nouveau VNet, vérifiez ou modifiez les préfixes de chaque sous-réseau. Les sous-réseaux par défaut sont 10.0.1.0/24, 10.0.2.0/24 et 10.0.3.0/24. Vous pouvez allouer ces sous-réseaux aux interfaces de gestion, approuvée et non approuvée comme vous le souhaitez.

4. Examinez le récapitulatif, acceptez les conditions d'utilisation et la politique de confidentialité, puis cliquez sur **Immediate deployment (Déploiement immédiat)** pour déployer le pare-feu. Le déploiement peut prendre 20 minutes, et vous pouvez utiliser le lien sur la page pour vérifier la progression.
5. Vérifiez que vous avez correctement déployé le pare-feu VM-Series.

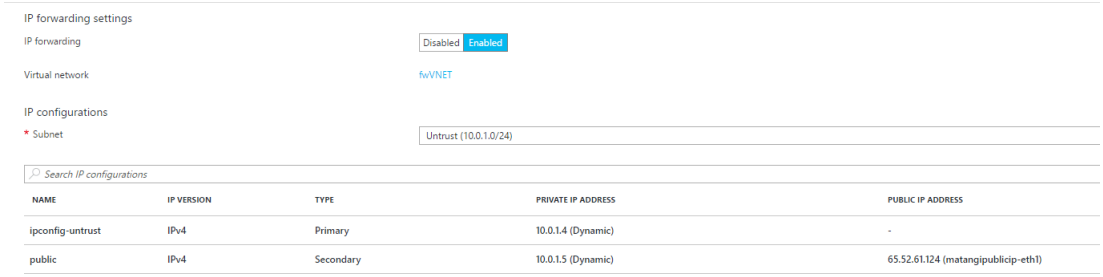
1. Connectez-vous au portail Azure China (https://portal.azure.cn) en utilisant vos identifiants Microsoft.
2. Sélectionnez **Dashboard (Tableau de bord)** > **Resource Groups (Groupes de ressources)**, et sélectionnez le groupe de ressources.
3. Sélectionnez **All Settings (Tous les paramètres)** > **Deployments (Déploiements)** > **Deployment History (Historique du déploiement)** pour consulter l'état détaillé



 ©2023 Palo Alto Networks, Inc.

STEP 4 | Associez une adresse IP publique pour l'interface non approuvée du pare-feu VM-Series. Cela vous permet d'accéder à l'interface depuis l'Internet public et est utile pour toute application ou service Internet.

1. Sur le portail Azure, sélectionnez l'interface réseau pour laquelle vous souhaitez ajouter une adresse IP publique. Par exemple, l'interface eth1.
2. Sélectionnez **IP Configurations (Configurations IP)** > **Add (Ajouter)** et, pour l'adresse IP publique, sélectionnez **Enabled (Activé)**. Créez une nouvelle adresse IP publique ou sélectionnez-en une disponible.
3. Vérifiez que vous pouvez afficher l'adresse IP secondaire associée à l'interface.



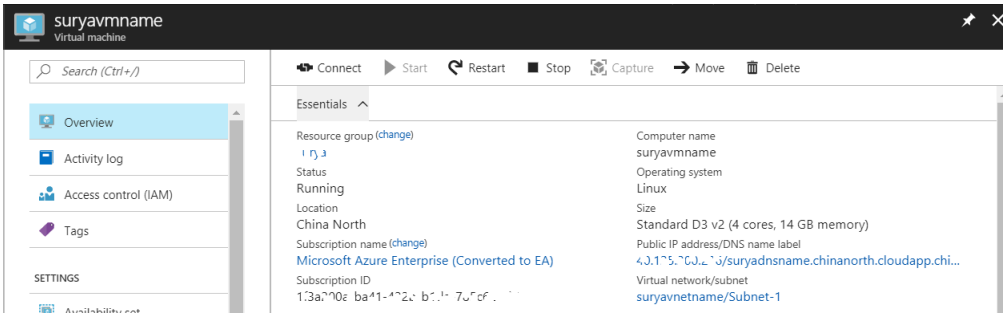
Lorsque vous associez une adresse IP secondaire à une interface réseau, le pare-feu VM-Series n'acquiert pas automatiquement l'adresse IP privée affectée à l'interface. Vous devrez configurer manuellement l'adresse IP privée à l'aide de l'interface Web du pare-feu VM-Series. Reportez-vous à l'étape Configurez les interfaces réseau du dataplane en tant qu'interfaces de couche 3 sur le pare-feu.

Chaque interface du pare-feu VM-Series sur Azure peut avoir une adresse IP privée dynamique (par défaut) ou statique et plusieurs adresses IP publiques (statiques ou dynamiques) associées. Le nombre maximal d'adresses IP publiques que vous pouvez attribuer à une interface est basé sur votre abonnement Azure. Lorsque vous créez une nouvelle adresse IP publique, vous en obtenez une du bloc d'adresses IP que possède Microsoft, vous ne pouvez donc pas en choisir une spécifique.

©2023 Palo Alto Networks, Inc.

STEP 5 | Connectez-vous à l'interface Web du pare-feu.

1. Sur le portail Azure, dans **All Resources (Toutes les ressources)**, sélectionnez le pare-feu VM-Series et consultez le nom de DNS complet pour le pare-feu.



2. En utilisant une connexion sécurisée (https) à partir de votre navigateur Web, connectez-vous au nom de DNS pour le pare-feu.
3. Saisissez le nom d'utilisateur/mot de passe que vous avez défini précédemment. Un avertissement de certificat s'affiche ; ne vous en préoccupez pas. Continuez vers la page Web.

STEP 6 | Activez les licences sur le pare-feu VM-Series.

1. Créez un compte de support.
2. Enregistrez le pare-feu VM-Series (avec code d'autorisation).
3. Sur l'interface Web du pare-feu, sélectionnez **Device (Périphérique)** > **Licenses (Licenses)** et sélectionnez **Activate feature using authentication code (Activer la fonctionnalité à l'aide du code d'autorisation)**.
4. Saisissez le code d'autorisation de capacité enregistré sur le portail de support. Le pare-feu se connecte alors au serveur de mise à jour (updates.paloaltonetworks.com), télécharge la licence et redémarre automatiquement.
5. Connectez-vous à nouveau à l'interface Web et confirmez les éléments suivants sur le **Dashboard (Tableau de bord)** :
   - Un numéro de série valide s'affiche dans **Serial# (N° de série)**.

     Si le terme Unknown (Inconnu) s'affiche, cela signifie que le périphérique n'est pas sous licence. Pour afficher les journaux de trafic sur le pare-feu, vous devez installer une licence de capacité valide.
   - Le **VM Mode (Mode VM)** affiche Microsoft Azure.

©2023 Palo Alto Networks, Inc.

STEP 7 | Configurez les interfaces réseau du plan de données en tant qu'interfaces de couche 3 sur le pare-feu.

Si vous hébergez plusieurs sites Web ou services avec des adresses IP et des certificats SSL différents sur un seul serveur, vous devrez peut-être configurer plusieurs adresses IP sur les interfaces de pare-feu VM-Series.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
2. Cliquez sur la liaison **ethernet 1/1** et configurez comme suit :
   - **Interface Type (Type d'interface)** : Layer3 (Couche 3) (par défaut).
   - Dans l'onglet Config (Configuration), affectez l'interface au routeur par défaut.
   - Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez New Zone (Nouvelle zone). Définissez une nouvelle zone appelée Non approuvée, puis cliquez sur OK.
   - Dans l'onglet **IPv4**, sélectionnez **DHCP Client (Client DHCP)** si vous envisagez d'attribuer une seule adresse IP sur l'interface. L'adresse IP privée attribuée au modèle ARM sera acquise automatiquement. Si vous envisagez d'attribuer plus d'une adresse IP, sélectionnez **Static (Statique)** et entrez manuellement les adresses IP principales et secondaires attribuées à l'interface sur le portail Azure.
   - Décochez la case **Automatically create default route to default gateway provided by server** (Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur). La désactivation de cette option garantit que le trafic géré par cette interface n'est pas directement dirigé vers la passerelle par défaut du réseau virtuel.
3. Cliquez sur le lien pour **ethernet 1/2** et configurez-le comme suit :
   - Définissez **Interface Type (Type d'interface)** sur Layer3 (Couche 3) (par défaut).
   - **Security Zone (Zone de sécurité)** : Approuvée
   - **Adresse IP** : Sélectionnez **DHCP Client (Client DHCP)** ou **Static (Statique)**.
   - Décochez la case **Automatically create default route to default gateway provided by server** (Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur). La désactivation de cette option garantit que le trafic géré par cette interface n'est pas directement dirigé vers la passerelle par défaut du réseau virtuel.
4. Cliquez sur **Commit (Valider)**. Vérifiez que la liaison des interfaces est active.

STEP 8 | Configurez le pare-feu pour votre déploiement spécifique.

- Passerelle : déployez un équilibreur de charge tiers en façade de la zone Non approuvée.
- Hybrid and inter-VNet : déployez une passerelle VPN Azure ou une machine virtuelle NAT en façade de la zone Non approuvée.
- Inter-sous-réseau : sur le pare-feu VM-Series, ajoutez une règle de politique de sécurité intrazone pour autoriser le trafic sur la base des sous-réseaux associé à l'interface Approuvée.
- GlobalProtect : déployez une machine virtuelle NAT en façade de la zone Non approuvée.

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Dirigez le trafic vers le pare-feu VM-Series.

1. Pour vous assurer que le pare-feu VM-Series sécurise tout le trafic au sein du groupe de ressources Azure, configurez des itinéraires statiques sur le pare-feu.
2. Configurez les UDR pour diriger l'ensemble du trafic à travers les interfaces du pare-feu VM-Series. Consultez la documentation Azure sur les UDR pour plus de détails.

   Les UDR sur les sous-réseaux internes doivent envoyer tout le trafic à travers l'interface Approuvée. Les UDR sur le côté Non approuvé dirigent tout le trafic provenant d'Internet à travers l'interface Non approuvée sur le pare-feu VM-Series. Le trafic provenant d'Internet peut provenir d'une Azure Application Gateway ou d'un équilibreur de charge Azure, ou de la passerelle VPN Azure en cas de déploiement hybride qui connecte votre réseau interne avec le cloud Azure.

 ©2023 Palo Alto Networks, Inc.

Déploiements orchestrés par Panorama dans Azure

Le plugin Panorama pour Azure déploie, configure et surveille de manière centralisée votre système de sécurité dans le cloud Azure. Il orchestre les déploiements VM-Series dans votre réseau Azure de manière à ce que vous puissiez activer les politiques de sécurité pour les pare-feu gérés. Le plugin se lie à vos pages de déploiement Azure ARM et Azure Monitor, vous offrant une visibilité sur l'état du déploiement, l'utilisation et les performances de vos pare-feux VM-Series.

Dans Azure, le plug-in orchestre le déploiement des ressources Azure telles que les équilibreurs de charge, les sous-réseaux et les passerelles NAT ainsi que les ensembles de mise à l'échelle automatique du pare-feu VM-Series. Dans Panorama, le plugin configure automatiquement les groupes de périphériques Panorama, les piles de modèles et les politiques NAT. Il lit les étiquettes à partir de vos ressources Azure, puis active de manière centralisée les politiques basées sur les étiquettes sur un groupe de pare-feux.

Le plug-in Panorama peut orchestrer des déploiements dans une ou plusieurs régions de votre environnement Azure. Un déploiement peut se composer d'une pile Hub, d'une pile entrante ou les deux, en fonction du trafic qui doit être sécurisé pour votre déploiement :

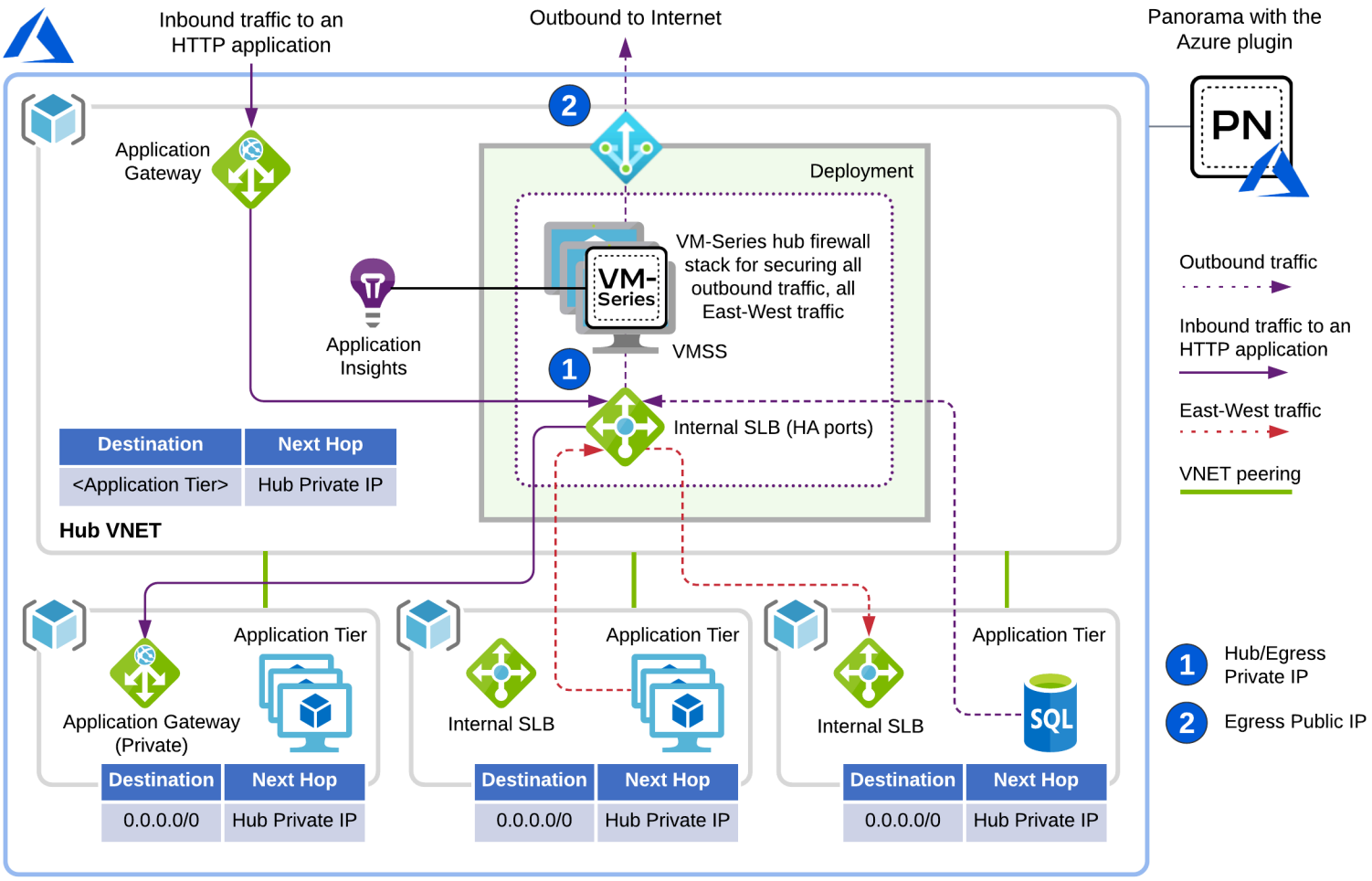
- Une pile de ***pare-feu Hub*** protège le trafic sortant et le trafic est-ouest entre vos charges de travail d'application.
- Une pile de ***pare-feu entrant*** permet de sécuriser le trafic vers et depuis vos applications publiques.

Vous pouvez configurer le nombre de pare-feu dans chaque pile. Vous avez la possibilité de configurer un nombre statique de pare-feux dans votre déploiement ou une plage que le VMSS doit utiliser pour la mise à l'échelle. Les deux piles dans le déploiement créent un VMSS ou des pare-feux VM-Series et elles peuvent chacune mettre à l'échelle jusqu'à 25 pare-feux.

Pile Hub

Un déploiement utilise une pile Hub et tire parti de l'équilibreur de charge Azure Internal Standard (avec ports HA) afin de mesurer et d'équilibrer la charge à travers un ensemble de pare-feu. Vous pouvez ensuite utiliser l'adresse IP privée de l'équilibreur de charge standard (**2**, « Adresse IP privée entrante/Hub » dans la figure suivante) pour acheminer le trafic vers les pare-feu pour l'inspection et la prévention des menaces. La pile Hub sécurise le trafic sortant et est-ouest de vos applications.

 ©2023 Palo Alto Networks, Inc.



Afin de protéger votre trafic sortant et le trafic est-ouest, ajoutez des règles d'acheminement dans vos VNET d'application afin de rediriger le trafic vers la pile Hub pour inspection.

Pile entrante

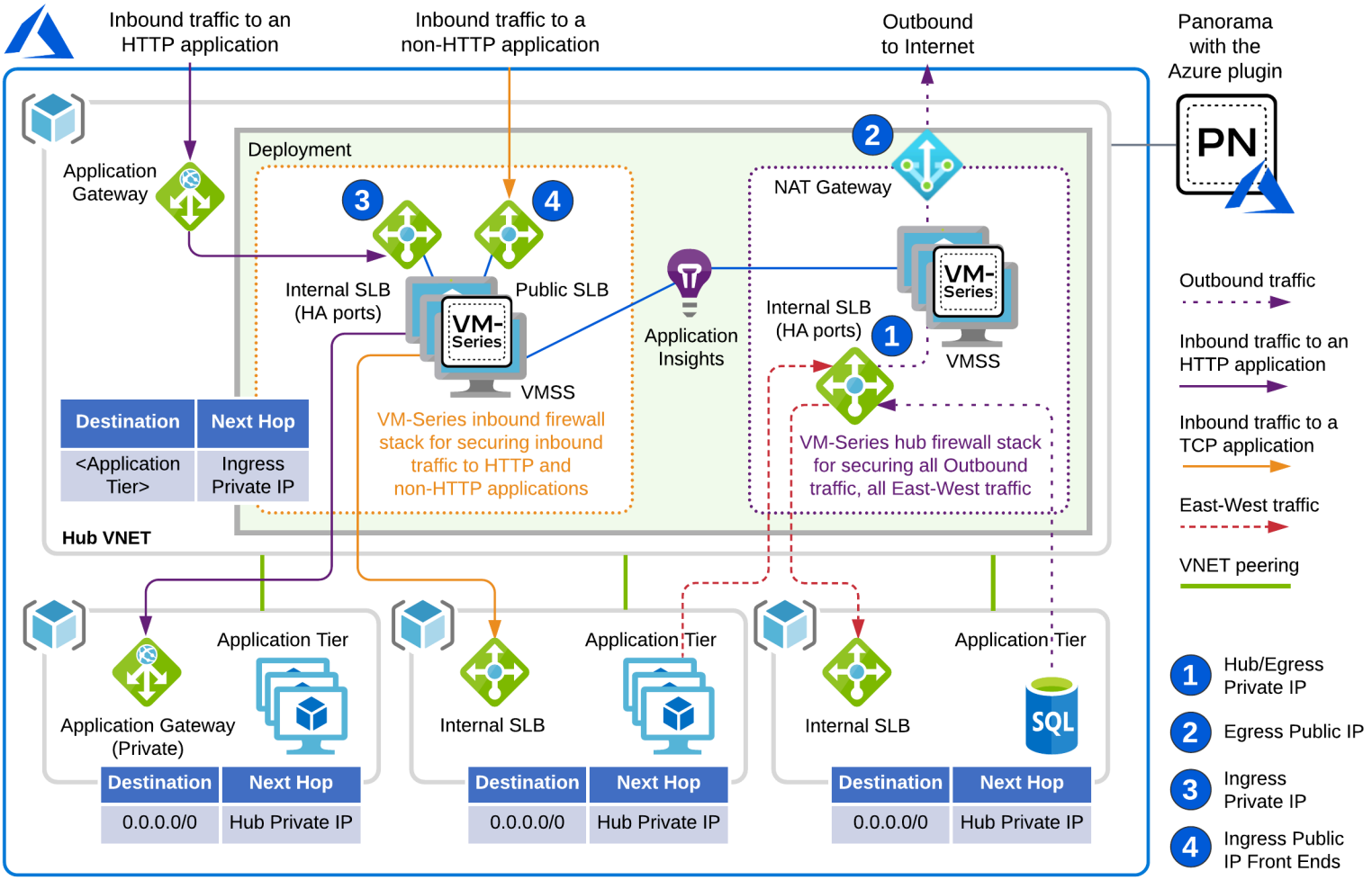
Une pile de pare-feu entrante est mise à l'échelle de manière indépendante et améliore la visibilité et la sécurité du trafic entrant de vos applications.

Chaque pile entrante peut sécuriser jusqu'à 10 applications.

Pour protéger votre trafic HTTP entrant, ajoutez des UDR dans les tables d'acheminement des sous-réseaux de la passerelle applicative pour acheminer tout le trafic vers la pile entrante (**3**, Adresse IP privée entrante dans la figure suivante). Pour protéger le trafic entrant non-HTTP, utilisez le plug-in Panorama pour créer des entrées frontales pour vos terminaux d'application (**4**, Entrées frontales de l'adresse IP publique entrante dans la figure suivante). Pour permettre l'inspection, le plugin Panorama crée automatiquement des règles d'équilibrage de charge sur l'équilibreur de charge Azure Public Standard, et des règles NAT sur les pare-feux.

Si vous avez uniquement du trafic entrant HTTP/HTTPS, vous pouvez ignorer la pile entrante et protéger ce trafic à l'aide de la seule pile Hub.

©2023 Palo Alto Networks, Inc.



Reportez-vous aux sections Préparation d'un déploiement orchestré et Orchestration d'un déploiement de pare-feu VM-Series dans Azure.

Préparation d'un déploiement orchestré

Effectuez les tâches suivantes avant d'orchestrer un pare-feu VM-Series sur Azure.

- Prérequis de configuration
- Autorisations d'orchestration
- Créez un rôle personnalisé et associez-le à un Active Directory (AD)
- Trouvez votre nom de domaine Azure Directory

Prérequis de configuration

Effectuez les tâches de base suivantes sur Panorama et Azure.

©2023 Palo Alto Networks, Inc.

- Azure
  - Créer un principal de service pour activer le plug-in pour effectuer des appels d'API.
  - Planifiez un bloc CIDR spécifiquement dédié au pare-feu VM-Series Transit VNet. Le plug-in gère ce bloc CIDR et l'utilise pour déployer le VNet du pare-feu initial et servir de futures mises à niveau pour les nouvelles piles de modèles.

    La plage de CIDR minimum est /22.
- Panorama
  - Assurez-vous de disposer d'une clé API de licence valide configurée sur Panorama. Cela permet au plug-in de gérer la suppression des licences sur les événements de mise à l'échelle automatique (augmentation). Voir Installez une clé API de désactivation de licence.
  - Installez la version la plus récente du plug-in VM-Series sur Panorama pour permettre l'ajout de la configuration Application Insight à la pile de modèles.
- Régions Azure qualifiées

  Les déploiements orchestrés par Panorama sont pris en charge dans toutes les régions prenant en charge le pare-feu VM-Series. Les régions suivantes ont été jugées qualifiées ; si vous procédez à un déploiement dans une région non répertoriée et que vous rencontrez un problème, contactez l'assistance.
  - Ouest États-Unis
  - Ouest États-Unis 2
  - Centre-Nord États-Unis
  - Est États-Unis
  - Est États-Unis 2
  - Ouest Europe
  - Centre-Ouest Allemagne
  - EAU Nord
  - Ouest Inde
  - Australie Sud-Est

Lorsque vous planifiez votre déploiement, notez que si vous exécutez actuellement un plug-in Panorama pour Azure version 2.x, la mise à niveau vers la version actuelle n'est pas autorisée. De même, une fois la version actuelle installée, le passage à un plugin version 2.x antérieur n'est pas autorisé. Voir plug-in Panorama pour Azure dans la Matrice de compatibilité.

Autorisations d'orchestration

Il y a un exemple de fichier JSON avec des autorisations pour le rôle de déployeur de modèles. Dans la section **`AssignableScopes`**, incluez tous les abonnements pertinents qui doivent être interrogés, y compris l'abonnement dans lequel le déploiement est déployé et TOUS les abonnements qui contiennent un VNET d'application apparié au VNet du pare-feu VM-Series où les ressources protégées existent.

```
{ "Name": "Template Deployment", "IsCustom": true,
 "Description": "Manage template deployments.",    "Actions":
```

 ©2023 Palo Alto Networks, Inc.

```
 [ "Microsoft.Resources/subscriptions/resourcegroups/*",
 "Microsoft.Resources/deployments/write", "Microsoft.Resources/
deployments/operationStatuses/read", "Microsoft.Resources/
deployments/read", "Microsoft.Resources/deployments/delete",
 "Microsoft.Network/publicIPPrefixes/write", "Microsoft.Network/
publicIPPrefixes/read", "Microsoft.Network/publicIPPrefixes/delete",
 "Microsoft.Network/publicIPAddresses/write", "Microsoft.Network/
publicIPAddresses/read", "Microsoft.Network/publicIPAddresses/
delete", "Microsoft.Network/publicIPAddresses/join/action",
 "Microsoft.Network/natGateways/write", "Microsoft.Network/
natGateways/read", "Microsoft.Network/natGateways/delete",
 "Microsoft.Network/natGateways/join/action", "Microsoft.Network/
virtualNetworks/read", "Microsoft.Network/virtualNetworks/write",
 "Microsoft.Network/virtualNetworks/delete", "Microsoft.Network/
virtualNetworks/subnets/write", "Microsoft.Network/virtualNetworks/
subnets/read", "Microsoft.Network/virtualNetworks/subnets/
delete", "Microsoft.Network/virtualNetworks/subnets/join/action",
 "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/
read", "Microsoft.Network/networkSecurityGroups/write",
 "Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/
networkSecurityGroups/delete", "Microsoft.Network/
networkSecurityGroups/join/action", "Microsoft.Network/loadBalancers/
write", "Microsoft.Network/loadBalancers/read", "Microsoft.Network/
loadBalancers/delete", "Microsoft.Network/loadBalancers/probes/join/
action", "Microsoft.Network/loadBalancers/backendAddressPools/join/
action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/
read", "Microsoft.Network/locations/serviceTags/read",
 "Microsoft.Network/applicationGateways/read", "Microsoft.Network/
networkInterfaces/read", "Microsoft.Compute/virtualMachineScaleSets/
write", "Microsoft.Compute/virtualMachineScaleSets/read",
 "Microsoft.Compute/virtualMachineScaleSets/delete",
 "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
 "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/images/
read", "Microsoft.insights/components/write", "Microsoft.insights/
components/read", "Microsoft.insights/components/delete",
 "Microsoft.insights/autoscalesettings/write" ] "NotActions": [ ],
 "AssignableScopes": [ "/subscriptions/{deployment-subscription}",
 "/subscriptions/{app1-subscription}", "/subscriptions/{app2-
subscription}", . . . ] }
```

Créez un rôle personnalisé et associez-le à un Active Directory (AD)

STEP 1 | Pour créer un Active Directory (AD) dans Azure, accédez à Azure Active Directory (AD) et cliquez sur **App Registrations** (Enregistrements d'applications) à gauche. Créez un rôle personnalisé à l'aide des autorisations requises par le plug-in.

Un exemple de JSON est inclus ci-dessous.

1. Cliquez sur **add** (ajouter) et indiquez un nom. Sélectionnez le rôle créé à partir du fichier JSON ci-dessus, laissez l'utilisateur d'Active Directory dans « Assign access to » (Attribuer l'accès à) puis sélectionnez l'Active Directory créé à la première étape et cliquez sur Save (Enregistrer).
2. Sélectionnez le type.

   Ne modifiez rien dans Redirect URI.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Créez un rôle personnalisé avec les autorisations requises par le plug-in.

Reportez-vous à la section Autorisations d'orchestration.

1. Connectez-vous à la CLI Azure.

```
az login
```

2. Créez un rôle personnalisé à partir du fichier dans Autorisations d'orchestration.

```
az role definition create --role-definition <role-json-file>
```

STEP 3 | Associez le rôle à l'Active Directory que vous avez créé à l'étape 1. Vous pouvez utiliser la console ou le CLI.

Vous devez répéter cette étape dans chaque abonnement défini dans la section ***`assignableScope`*** *du rôle personnalisé dans Autorisations d'orchestration.*

Console

1. Sur le portail Azure, accédez à **Subscriptions** (Abonnements) et sélectionnez votre abonnement.
2. À gauche, sélectionnez **Access Control (IAM)** (Contrôle d'accès [IAM]) puis **Role Assignments** (Attributions de rôles) sur la barre supérieure.
3. Sélectionnez **Add** (Ajouter) et **add role assignment** (ajouter une attribution de rôle).
   - Sélectionnez le rôle que vous avez créé à l'étape 3 et laissez l'utilisateur Active Directory (AD) dans « Assign access to » (Attribuer l'accès à).
   - Sélectionnez l'Active Directory (AD) créé à l'étape 1 et cliquez sur **Save (Enregistrer)**.

CLI :

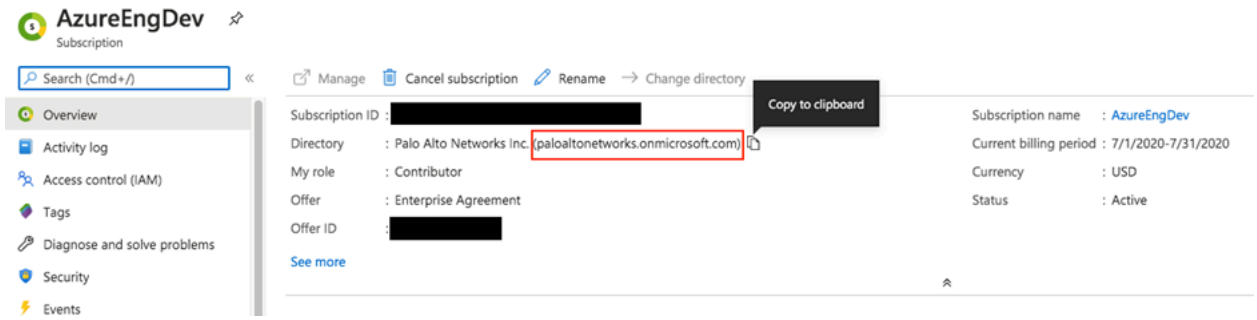
Dans la commande suivante, **`<role-name>`** se réfère au nom dans l'exemple de fichier JSON, dans l'exemple précédent, **`Template Deployment (Déploiement de modèle)`**.

```
az ad sp create-for-rbac --name <name-of-service-principal> --role
 <role-name> --output json
```

Trouvez votre nom de domaine Azure Directory

Pour que le plug-in fournisse des liens à votre déploiement Azure et à votre instance Application Insights dans le portail Azure, vous devez identifier le domaine du répertoire pour votre abonnement, comme indiqué ci-dessous :

 ©2023 Palo Alto Networks, Inc.



Orchestration d'un déploiement de pare-feu VM-Series dans Azure

Vous pouvez créer un maximum de dix déploiements orchestrés. En outre, chaque déploiement orchestré prend en charge jusqu'à 100 applications frontales.

Azure China et Azure Government ne sont pas pris en charge.

©2023 Palo Alto Networks, Inc.

STEP 1 | Créez un principal de service.

Les informations d'identification du principal de service que vous avez créé permettent au plug-in Panorama d'effectuer les appels d'API nécessaires à l'orchestration de votre déploiement

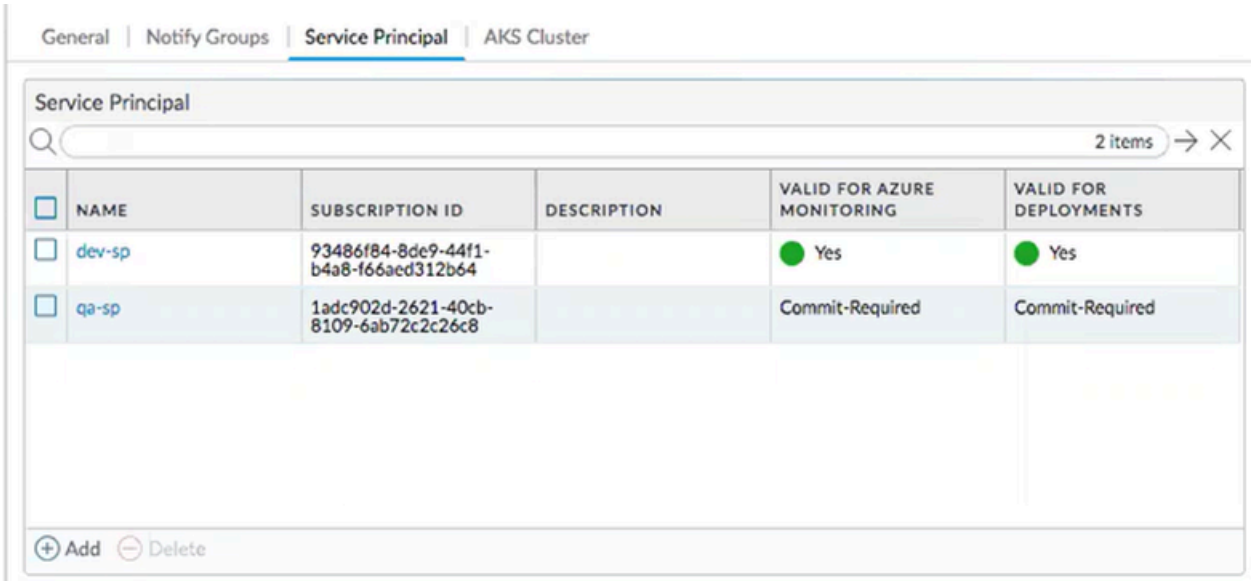
1. Sélectionnez **Setup (Configuration)** > **Service Principal (Principal de service)** > **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** et, s'il y a lieu, une **Description** pour identifier le compte de service.
3. Saisissez le **Subcription ID (l'ID d'abonnement)** pour l'abonnement Azure que vous voulez surveiller.

   Vous devez vous connecter à votre portail Azure pour obtenir cet ID d'abonnement.
4. Saisissez le**Client ID (ID de client)**. L'ID de client est l'ID d'application associé à votre application Azure Active Directory.
5. Saisissez le **Client Secret (Secret du client)** et entrez-le de nouveau pour confirmer.
6. Saisissez le **Tenant ID (ID de locataire)**.

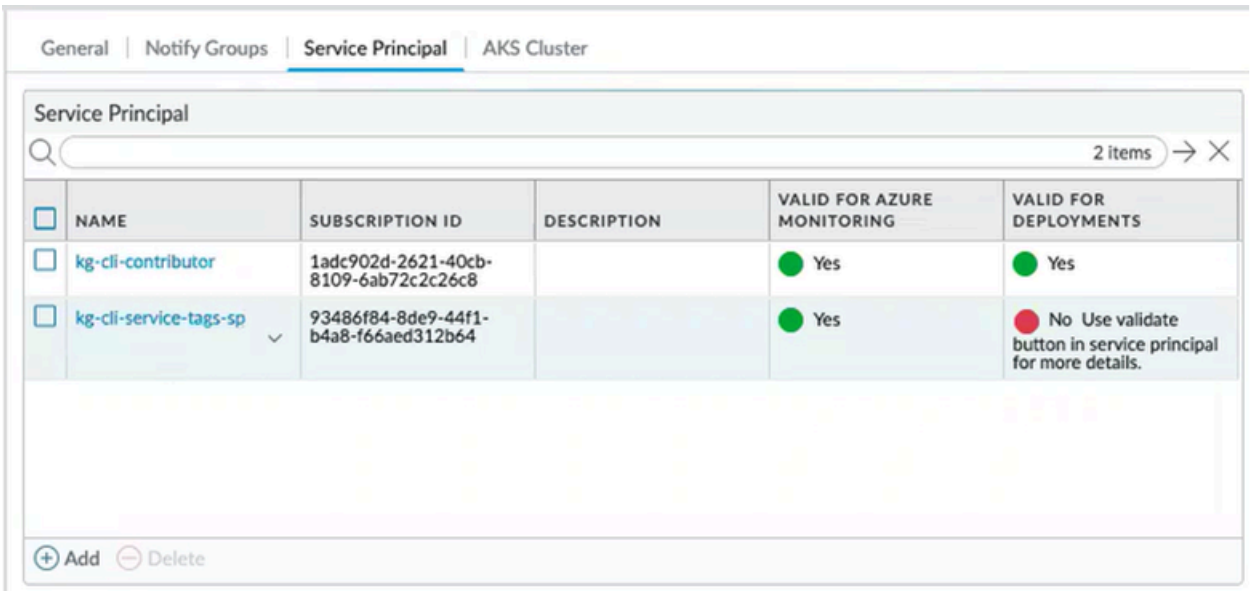
   Le numéro d'identification du locataire est celui que vous avez sauvegardé lorsque vous avez configuré l'application Active Directory (AD).
7. Cliquez sur **Validate (Valider)** pour vérifier que les clés et les ID que vous avez saisis sont valides et que Panorama peut communiquer avec l'abonnement Azure au moyen de l'API.

   La validation peut prendre jusqu'à une minute. Vous pouvez mettre à jour la page pour vérifier votre progression.
8. Une fois le principal de service est valide, validez vos modifications.

   La validation garantit que le principal de service est disponible lorsque vous configurez le déploiement.



 ©2023 Palo Alto Networks, Inc.



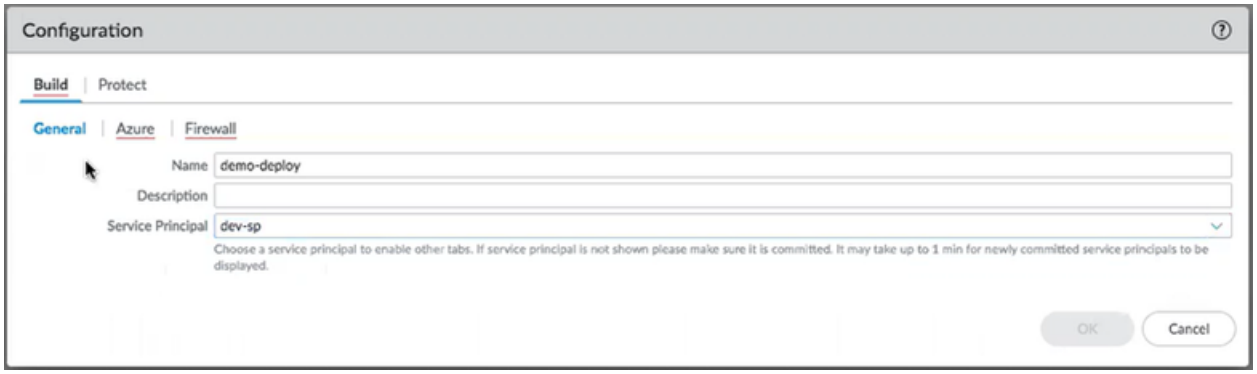
©2023 Palo Alto Networks, Inc.

STEP 2 | Configurez votre déploiement Azure.

1. Sélectionnez **Deployments (Déploiements)** et **Add (Ajouter)** une configuration.
2. Sélectionnez **Build (Créer)** > **General (Général)**.
   - Fournissez un **Name (Nom)** et une **Description** facultative.
   - Choisissez un principal de service dans la liste déroulante.

     Vous devez sélectionner un principal de service valide pour activer l'onglet **Azure**.

     Si vous ne voyez pas votre principal de service, revenez à l'étape 1 et assurez-vous que le principal de service est valide et qu'il a été validé.



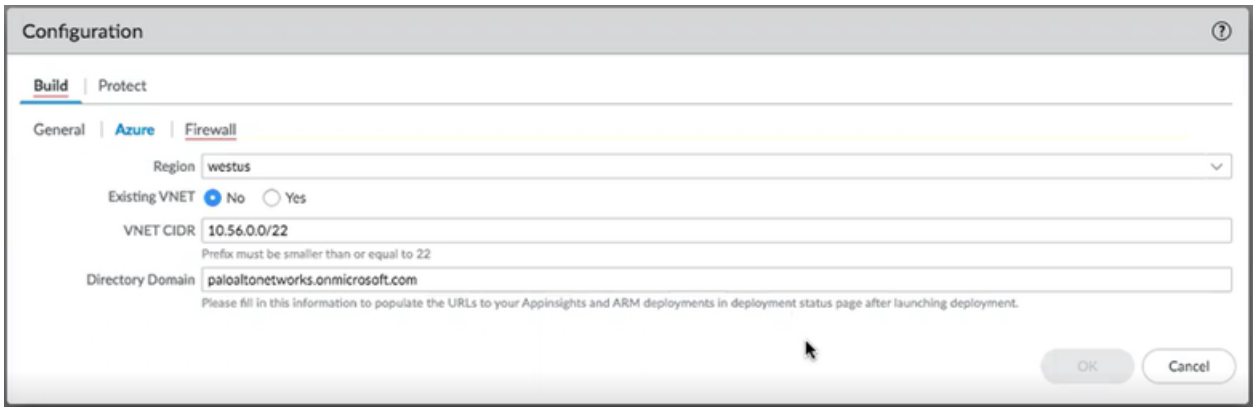
3. Dans l'onglet **Build (Créer)** > **Azure**, sélectionnez une région.

   La liste déroulante est dynamique : elle répertorie toutes les régions qui ont une image de pare-feu nouvelle génération Palo Alto Networks VM-Series.

   - **Existing VNET (VNET existant)**.
     - Sélectionnez **No (Non)** pour créer un nouveau VNET.

       Le plugin utilise le CIDR et le domaine de répertoire de VNET pour créer un VNET pour vous.
     - Sélectionnez **Yes (Oui)** pour indiquer un VNET existant.
   - **VNET CIDR (CIDR VNET)** : saisissez votre plage CIDR. Le préfixe doit être inférieur ou égal à /22. Par exemple, 192.168.0.0/22.
   - **Directory Domain (Domaine de répertoire)** : reportez-vous à la section Trouvez votre nom de domaine Azure Directory. Cette chaîne fait partie de l'URL de toutes les ressources de l'abonnement, et elle aide le plugin à se lier à vos déploiements.

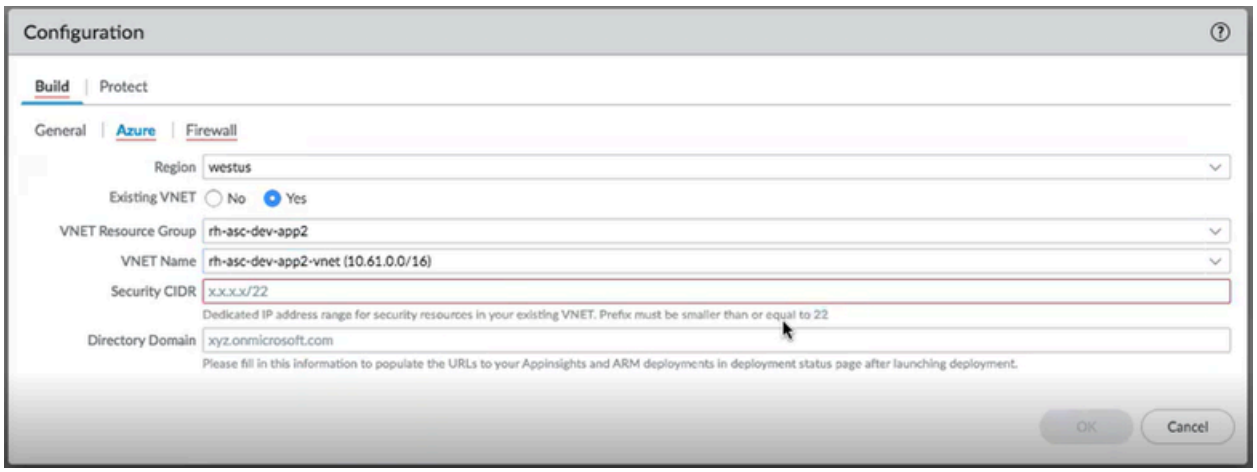
©2023 Palo Alto Networks, Inc.



Si vous sélectionnez **Yes (Oui)**, le plugin demande le groupe de ressources VNET, le nom de VNET, le CIDR de sécurité et le domaine de répertoire.

- **VNET Resource Group (Groupe de ressources VNET)** : choisissez parmi une liste de tous les groupes de ressources dans la région que vous avez sélectionnée.
- **VNET Name (Nom de VNET)** : choisissez parmi une liste de VNET dans le groupe de ressources que vous avez choisi.
- **Security CIDR (CIDR de sécurité)** : saisissez votre plage CIDR. Le préfixe doit être inférieur ou égal à /22. Par exemple, 192.168.0.0/22.
- **Directory Domain (Domaine de répertoire)** : reportez-vous à la section Trouvez votre nom de domaine Azure Directory. Cette chaîne fait partie de l'URL de toutes les ressources de l'abonnement, et elle aide le plugin à se lier à vos déploiements.

Le groupe de ressources VNET et le nom de VNET aident le plugin à localiser votre VNET existant. Tout ce que le plugin déploie va dans un groupe de ressources que le plugin gère.



 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configurez les piles de pare-feu VM-Series pour votre déploiement.

Vous pouvez déployer la pile Hub (Concentrateur) pour protéger le trafic sortant ou est-ouest. Vous pouvez déployer la pile Inbound (Entrant) pour protéger le trafic entrant. Vous pouvez également déployer les deux piles si tous les flux de trafic doivent être protégés.

Les paramètres de configuration sont les mêmes pour les deux piles.

- **License Type (Type de licence)** : sélectionnez BYOL, Bundle 1 (Forfait 1) ou Bundle 2 (Forfait 2).
- **License Authcode (Code d'autorisation de licence)** : (BYOL uniquement). Saisissez le code d'autorisation envoyé dans votre lettre de bienvenue.
- **VM Size (Taille de la VM)**
  - La liste déroulante affiche les tailles de VM qui correspondent au code d'autorisation que vous avez saisi.
  - Bundle1 (Forfait1) ou Bundle2 (Forfait2) : choisissez n'importe quelle taille de VM.

Existing Device Group (Groupe d'appareils existant) :le groupe d'appareils doit être unique, tant pour les piles que pour les déploiements. Autrement dit, vous devez disposer d'un groupe d'appareils dédié et distinct pour chaque pile dans chaque déploiement.

Si vous sélectionnez **No (Non)**, le plug-in crée un groupe d'appareils.

Si vous sélectionnez **Yes (Oui)**, sélectionnez un groupe d'appareils existant dans la liste déroulante.

- **Min Firewalls(Pare-feu min.)** : une valeur comprise entre 1 et 25 pour un VMSS.
- **Max Firewalls (Pare-feu max.)** : une valeur comprise entre 1 et 25 pour un VMSS.

STEP 4 | Sélectionnez **Build (Créer)** > **Firewall (Pare-feu)** > **Basic (De base)** pour configurer les informations communes aux deux piles.

Pour **Image Type (Type d'image)**, sélectionnez **Marketplace Image (Image Marketplace)** ou **Custom Image (Image personnalisée)**.

- **Image Resource Group (Groupe de ressources d'images)** : (image personnalisée uniquement) choisissez le groupe de ressources contenant votre image personnalisée. Pour une image personnalisée, la liste affiche tous les groupes de ressources qui contiennent une image de la région que vous avez sélectionnée à l'étape 2..b.
- **Image** : (image personnalisée uniquement) la liste déroulante affiche toutes les images du groupe de ressources que vous avez choisi.
- **Software Version** : (image Marketplace) seules les versions de logiciel valides sont affichées. Consultez la matrice de compatibilité pour connaître la version minimale de PAN-OS.
- **Username (Nom d'utilisateur)** : le nom d'utilisateur de l'administrateur pour le pare-feu que vous créez. Le nom doit être légal pour le pare-feu VM-Series et Azure. Reportez-vous à la section Quelles sont les exigences en matière de nom d'utilisateur lors de la création d'une VM ?.
- **Password (Mot de passe)** : le mot de passe de l'administrateur du pare-feu que vous créez. Le mot de passe doit respecter les exigences en matière de caractères et de longueur

 ©2023 Palo Alto Networks, Inc.

(31 caractères) pour le pare-feu VM-Series et Azure. Reportez-vous à la section Quelles sont les exigences en matière de mot de passe lors de la création d'une VM ?.

- **Confirm Password (Confirmer le mot de passe)** : saisissez à nouveau votre mot de passe.
- **Primary Panorama IP (IP Panorama principale)** : indiquez l'adresse IP Panorama que le pare-feu peut utiliser pour se connecter à Panorama au moment de son démarrage. Choisissez entre l'adresse IP publique ou privée affichée dans la liste déroulante, ou saisissez l'adresse IP Panorama.
- **Secondary Panorama IP (IP Panorama secondaire)** : (uniquement si Panorama est en configuration HA). Indiquez l'adresse IP Panorama secondaire que le pare-feu peut utiliser pour se connecter à Panorama au moment de son démarrage. Choisissez dans la liste déroulante ou saisissez la bonne adresse IP.
- **Configure Device Certificate PIN (Configurer le PIN du certificat de périphérique)**. Comme ces valeurs sont cryptées, vous devez saisir et confirmer chaque valeur.
  - **Device Certificate PIN ID (ID du PIN du certificat de périphérique)** : l'ID du certificat de périphérique.
  - **Confirm Device Certificate PIN ID (Confirmer le PIN du certificat de périphérique).**
  - **Device Certificate PIN Value (Valeur du PIN du certificat de périphérique)** : la valeur du PIN du certificat.
  - **Confirm Device Certificate PIN Value (Confirmer la valeur du PIN du certificat de périphérique).**

STEP 5 | Sélectionnez les valeurs par défaut facultatives **Build (Créer)** > **Firewall (Pare-feu)** > **Advanced (Avancé)**.

Cochez **Advanced (Avancé)** pour modifier les valeurs par défaut.

- **Autoscaling Metric (Métrique de mise à l'échelle automatique)** : la valeur par défaut est Data Plane CPU Util Percent (Pourcentage d'utilisation du processeur du plan de données).
- **Scale In Threshold (Seuil de mise à l'échelle [augmentation])** : acceptez la valeur par défaut ou définissez un seuil de mise à l'échelle (augmentation).
- **Scale Out Threshold (Seuil de mise à l'échelle [diminution])** : acceptez la valeur par défaut ou définissez un seuil de mise à l'échelle (diminution).
- **Jumbo Frame (Trame Jumbo)** désactivé par défaut.

Cliquez sur **OK** et validez vos modifications. Rafraîchissez la page jusqu'à ce que vous puissiez voir le bouton **Deploy (Déployer)**, et cliquez sur **Deploy (Déployer)** pour lancer le déploiement. Une fois le déploiement lancé, les informations sont écrites sur la page **Deployments (Déploiements)**.



Le déploiement prend entre 15 et 20 minutes.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Sélectionnez **Azure** > **Deployments (Déploiements)** pour voir l'état du déploiement.

- La colonne Resource Group (Groupe de ressources) affiche les groupes de ressources que le plugin a créés.
- L'interface de gestion du pare-feu utilise l'IP d'accès au pare-feu pour se connecter à Panorama. Vous devez mettre cette adresse en liste blanche pour que Panorama puisse se connecter avec Panorama afin d'obtenir la configuration nécessaire.

  Si Panorama est déployé dans un cloud public, assurez-vous d'ajouter l'adresse IP d'accès du pare-feu au groupe de sécurité de Panorama.

  Reportez-vous à la section Ports utilisés pour Panorama afin de déterminer quels ports vous devez ouvrir pour autoriser le trafic.
- Ouvrez le lien dans la colonne **Deployment Status (État du déploiement)** afin d'obtenir des détails supplémentaires sur chaque pile.
  - **Hub-Stack (Pile Hub)** : l'IP publique de la pile Hub correspond à l'IP d'accès au pare-feu dans le résumé du déploiement, car la passerelle NAT est la même pour le trafic de sortie du déploiement et le trafic de gestion des pare-feu.

    Tout le trafic sortant et est-ouest doit être acheminé vers **l'adresse IP privée de sortie** pour inspection. Vous pouvez diriger le trafic vers cette adresse si vous avez configuré des UDR.
  - **Inbound-Stack (Pile entrante)** : l'IP privée est l'adresse de l'équilibreur de charge interne Azure qui fait face aux pare-feu. Vous pouvez diriger le trafic vers cette adresse si vous configurez des UDR.
- Suivez les liens pour consulter les informations sur le déploiement et Application Insights sur Azure.
- Les détails du déploiement peuvent afficher des messages de réussite, d'avertissement et d'échec.

STEP 7 | Configurez la protection entrante pour les applications TCP/UDP principales.

L'équilibreur de charge public qui fait face à la pile du pare-feu entrant est le point d'entrée de toute application UDP ou TCP principale. Ajoutez la configuration suivante pour permettre

 ©2023 Palo Alto Networks, Inc.

au plugin de gérer la configuration nécessaire de l'équilibreur de charge et du pare-feu pour l'acheminement vers votre application principale.

1. Sélectionnez **Azure** > **Deployments (Déploiements)** et choisissez votre déploiement.
2. Sélectionnez l'onglet **Protect (Protéger)** et cliquez sur **Add (Ajouter)**.
3. Fournissez le **Name (Nom)** de l'application et choisissez un **Protocol (Protocole)**.

   Saisissez les détails de la protection :

   - **Frontend IP Type (Type d'IP frontale)** : sélectionnez une des options suivantes : New Public IP (Nouvelle IP publique), Existing Frontend (Frontal existant) ou Existing Public IP (IP publique existante).

     Si vous sélectionnez Existing Frontend (Frontal existant), le **Frontend Name (Nom du frontal)** répertorie tous les frontaux connus sur l'équilibreur de charge.
   - **Resource Group (Groupe de ressources)** : (IP publique existante uniquement) dans la liste déroulante, sélectionnez le groupe de ressources dans lequel se trouve l'adresse IP du frontal que vous souhaitez.
   - IP Name (Nom de l'IP) : (IP publique existante uniquement) à utiliser pour mapper l'IP à un frontal sur l'équilibreur de charge, configurer l'équilibreur de charge et créer une règle NAT.
   - **Frontend Port (Port du frontal)** : ajoutez le port du frontal qui doit être configuré pour recevoir le trafic sur l'équilibreur de charge public.
   - **Backend IP (IP principale)** : ajoutez l'adresse IP de votre application principale.
   - **Backend Port (Port principal)** : ajoutez le port sur lequel votre application principale s'attend à recevoir du trafic.

   Cliquez sur **OK**.
4. Cliquez sur **Commit (Valider)** pour ajouter la configuration sur l'équilibreur de charge et l'appliquer aux pare-feu.

©2023 Palo Alto Networks, Inc.

Création d'une image personnalisée VM-Series pour Azure

Vous pouvez créer une image de pare-feu VM-Series personnalisée pour une utilisation ultérieure dans votre déploiement Azure. Une image personnalisée vous donne la flexibilité et la cohérence nécessaires pour déployer le pare-feu VM-Series avec la version de PAN-OS que vous souhaitez utiliser au lieu d'être limité à l'utilisation d'une image disponible sur le marché Azure. Par ailleurs, votre image personnalisée peut inclure les dernières mises à jour de contenu et d'antivirus.

Pour créer une image personnalisée, vous devez supprimer toutes les données privées (configuration utilisateur, utilisateurs, configuration des plugins, etc.) avant de créer le VHD. En outre, suivez la procédure suivante pour préparer et créer une image personnalisée.

Si le pare-feu VM-Series utilisé pour créer votre image personnalisée a été déployé en utilisant un type de disque premium, tout pare-feu VM-Series déployé en utilisant l'image personnalisée doit être déployé en utilisant le même type de disque premium. Cependant, si vous créez une image en utilisant un pare-feu déployé avec un type de disque standard, vous pouvez déployer le pare-feu en utilisant un type de disque standard ou premium.

STEP 1 | Connectez-vous à Azure.

STEP 2 | Déployez le pare-feu VM-Series depuis l'Azure Marketplace.

STEP 3 | (Licence BYOL uniquement) Activez votre licence.

STEP 4 | Mise à niveau du pare-feu VM-Series vers PAN-OS 10.0.3. La mise à niveau vers PAN-OS 10.0.3 met également à niveau le plugin VM-Series vers la version 2.0.3.

STEP 5 | Accédez à l'interface de ligne de commande (CLI) du pare-feu VM-Series via SSH en utilisant le nom d'utilisateur et le mot de passe fournis dans le modèle Azure Marketplace.

STEP 6 | Vérifiez que votre pare-feu VM-Series dispose des bonnes versions de PAN-OS, de plugin VM-Series, de contenu et d'antivirus.

```
show system info
```

Si vous utilisez PAN-OS 10.1, assurez-vous de mettre à niveau le plug-in VM-Series vers la version 2.1.7 ou supérieure et si vous utilisez PAN-OS 10.2.0, assurez-vous que vous utilisez le plug-in VM-Series version 3.0.3 ou ultérieure.

STEP 7 | (Licence BYOL uniquement) Désactivez votre licence.

STEP 8 | Effectuez une réinitialisation des données privées sur le pare-feu VM-Series. Cette commande nécessite le redémarrage du pare-feu. Vous devez attendre que le pare-feu VM-Series ait terminé son redémarrage avant de continuer. Le redémarrage peut prendre entre cinq et sept minutes.

```
request system private-data-reset
```


©2023 Palo Alto Networks, Inc.

STEP 9 | Créer une nouvelle image VHD à partir de l'instance VM-Series.

1. Connectez-vous à la CLI Azure.
2. Vérifiez que vous utilisez le bon abonnement.

   ```
   az account set --subscription <subscription-id>
   ```

3. Exécutez les commandes suivantes pour généraliser la VM, lui permettant ainsi d'être imagée pour de multiples déploiements, et créez le nouveau VHD.

   ```
   az vm deallocate --resource-group <myResourceGroup> --name
   <myVM>
   ```

   ```
   az vm generalize --resource-group <myResourceGroup> --name
   <myVM>
   ```

STEP 10 | Créez un nouveau pare-feu VM-Series à partir de votre image personnalisée.

```
az image create --resource-group <myResourceGroup> --name <myImage>
--source <resource-id-of-VM>
```

STEP 11 | Après avoir déployé un pare-feu VM-Series avec votre image personnalisée, vérifiez votre déploiement.

1. Vous devez vous connecter au pare-feu à l'aide des informations d'identification fournies lors de l'affichage de la machine virtuelle (VM) à partir de l'image personnalisée.
2. Après vous être connecté avec succès, vérifiez que votre pare-feu fonctionne avec la bonne version de PAN-OS et possède les bonnes versions de contenu et d'antivirus.

   ```
   show system info
   ```

STEP 12 | (Facultatif) Copiez l'image personnalisée dans une autre région.

```
az image copy –source-resource-group <source-rg> –source-object-name
<pa-vm-image-name> –target-location <target-region> –target-resource-
group <destination-rg>
```


©2023 Palo Alto Networks, Inc.

Utilisez les recommandations du Centre de sécurité Azure pour sécuriser vos charges de travail

***Microsoft a** arrêté la prise en charge du Centre de sécurité Azure **pour les solutions de sécurité partenaires et l'a remplacée par** Azure Sentinel.*

Lorsque vous déployez de nouvelles charges de travail dans votre abonnement Azure qui est activé pour Azure Security Center, Azure Security Center vous permet de sécuriser ces charges de travail de deux façons. Dans un flux de travail, le Azure Security Center vous recommande de déployer une nouvelle instance du pare-feu de la série VM pour sécuriser une charge de travail d'application orientée Internet. Dans l'autre flux de travail, le Azure Security Center découvre les pare-feu de la série VM (solutions de sécurité partenaires) que vous avez déployés dans l'abonnement Azure et vous devez ensuite effectuer une configuration supplémentaire pour connecter le pare-feu de la série VM au Azure Security Center afin de pouvoir afficher les alertes sur le tableau de bord. Reportez-vous à la section Intégration du centre de sécurité Azure pour obtenir des détails sur l'intégration ainsi que les avantages et inconvénients de chaque flux de travail :

- Déployer un pare-feu de série VM en fonction d'une recommandation du Centre de sécurité Azure
- Connecter un pare-feu de série VM existant à partir du centre de sécurité Azure

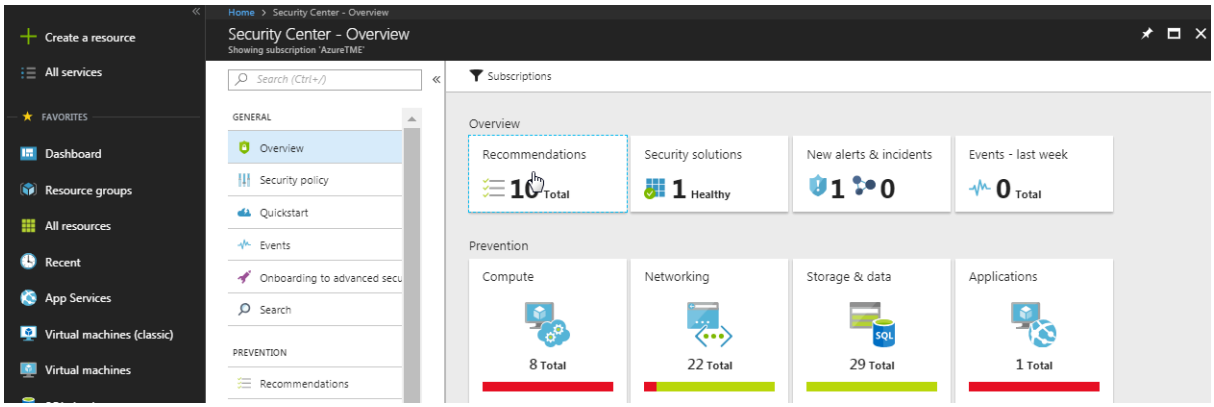
Déployer un pare-feu de série VM en fonction d'une recommandation du Centre de sécurité Azure

Le Centre de sécurité Azure analyse vos ressources Azure et formule des recommandations pour sécuriser les charges de travail qui ont besoin d'un pare-feu de prochaine génération. La recommandation s'affiche sur le tableau de bord et vous pouvez alors déployer une nouvelle instance du pare-feu de la série VM à partir du marché Azure ou vous pouvez utiliser le CLI d'Azure, Powershell ou un modèle ARM. L'avantage d'utiliser un déploiement personnalisé à l'aide de la CLI d'Azure, de Powershell ou d'un modèle ARM est que vous pouvez déployer le pare-feu de la série VM dans le même groupe de ressources que la charge de travail que vous devez protéger. Lorsque vous déployez le pare-feu de la série VM en utilisant le marché Azure, vous devez déployer le pare-feu dans un nouveau groupe de ressources ou un groupe de ressources vide seulement. Par conséquent, le déploiement sur le marché exige que vous vous assuriez que le trafic provenant de la charge de travail que vous voulez protéger est dirigé vers le pare-feu qui se trouve dans un groupe de résonance différent.

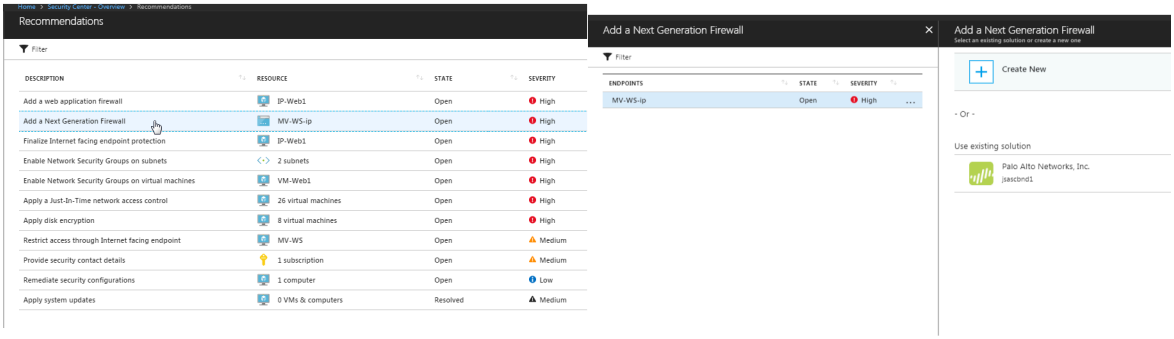
STEP 1 | Connectez-vous à votre portail Azure et accédez au tableau de bord du Centre de sécurité.

©2023 Palo Alto Networks, Inc.

STEP 2 | Sélectionnez **Recommendations**.



STEP 3 | Sélectionnez **Add a Next Generation Firewall (Ajoutez un Pare-feu de prochaine génération)**, sélectionnez la charge de travail que vous voulez protéger.



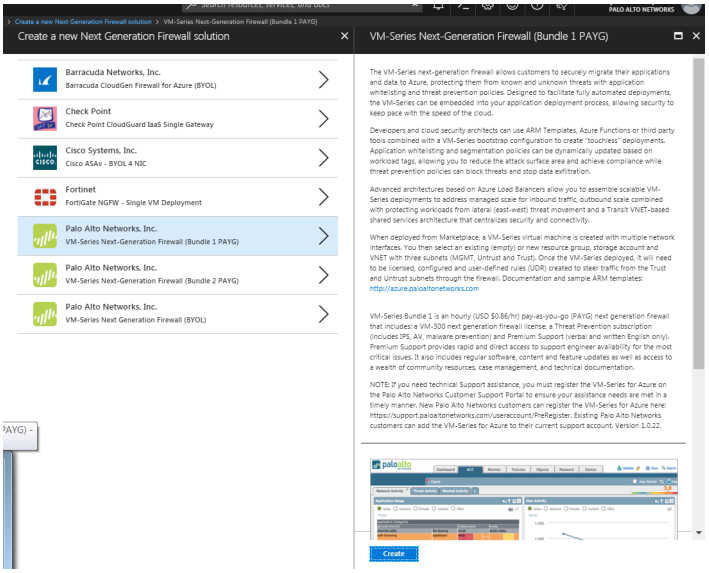
STEP 4 | Choisissez si vous voulez déployer une nouvelle instance du pare-feu de la série VM ou utiliser une instance existante du pare-feu de la série VM.

Pour utiliser ce flux de travail, mettre en place une charge de travail avec une adresse IP publique qui est exposée à Internet et déployer une instance du pare-feu de la série VM dans un nouveau groupe de ressources. Ensuite, supprimez la charge de travail que vous avez mise en scène et déployez vos charges de production au sein du groupe de ressources dans lequel vous avez déployé le pare-feu de la série VM.

- Pour **Create New** (En créer un nouveau), reportez-vous à la section Déploiement du pare-feu VM-Series depuis l'Azure Marketplace (modèle de solution).

©2023 Palo Alto Networks, Inc.

- Pour **utiliser la solution existance**, sélectionnez le pare-feu de la série VM que vous avez déjà déployé.

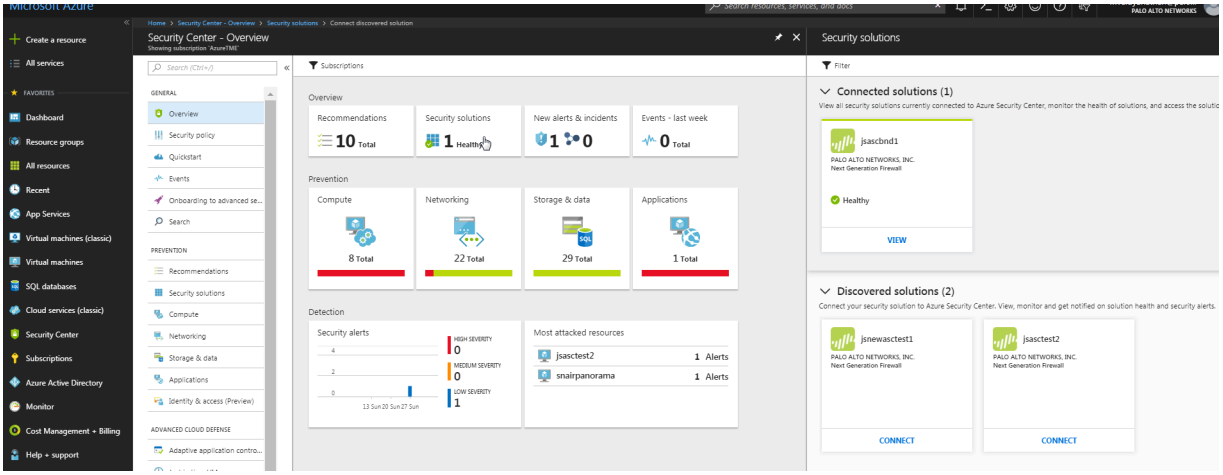


Connecter un pare-feu de série VM existant à partir du centre de sécurité Azure

Lorsque le Azure Security Center détecte que vous avez déployé le pare-feu de la série VM dans l'abonnement à Azure, il affiche le pare-feu comme solution de sécurité. Vous pouvez ensuite connecter le pare-feu de la série VM au Centre de sécurité en utilisant le format d'événement commun (FEC) sur le système et visualiser les journaux de pare-feu comme alertes sur le tableau de bord du Centre de sécurité.

STEP 1 | Connectez-vous à votre portail Azure et accédez au tableau de bord du Centre de sécurité.

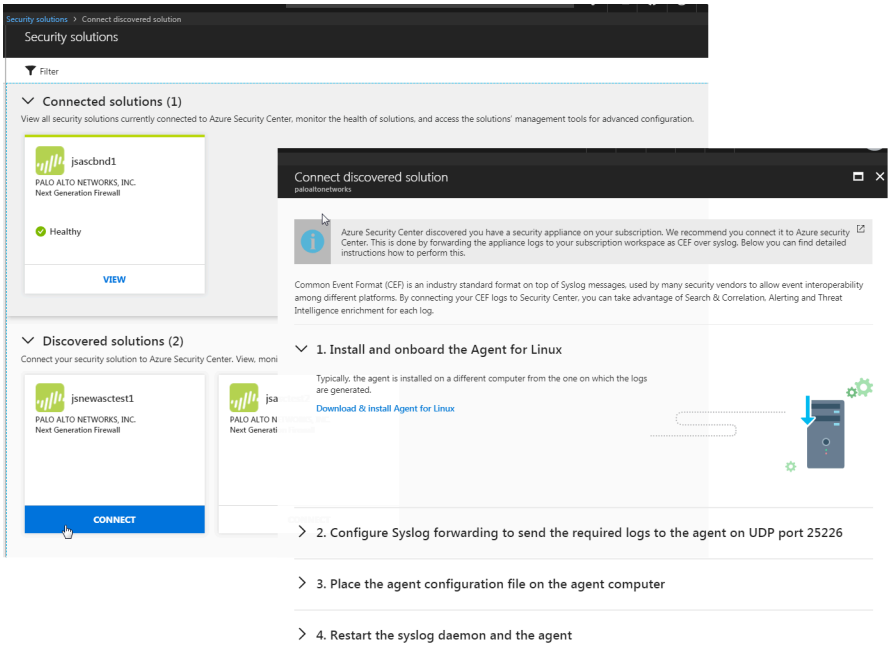
STEP 2 | Sélectionnez Security Solutions pour afficher tous les pare-feu de la série VM disponibles dans cet abonnement à Azure.



 ©2023 Palo Alto Networks, Inc.

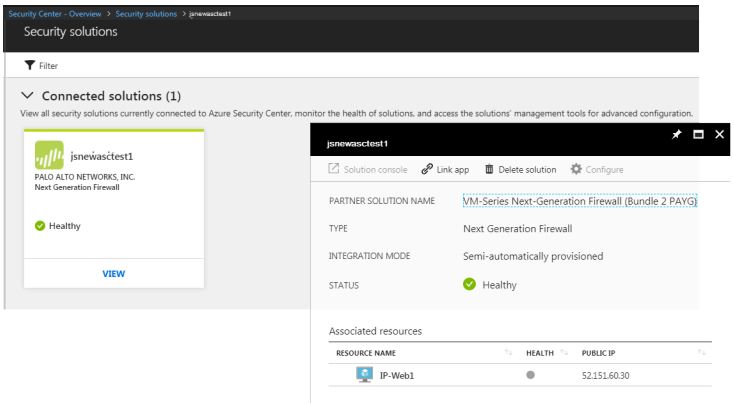
STEP 3 | Développez les solutions découvertes, sélectionnez l'instance de pare-feu de la série VM qui se trouve dans le même groupe de ressources que la charge de travail que vous souhaitez protéger et cliquez sur **Connect**.

Pour afficher les journaux des pare-feu comme des alertes dans le tableau de bord du Security Center (Centre de sécurité), vous devez suivre le processus en quatre étapes qui s'affiche à l'écran.



STEP 4 | Lors de la connexion réussie du pare-feu de la série VM au centre de sécurité, le pare-feu de la série VM s'affiche dans la liste des solutions connectées.

Cliquez sur View (Afficher) pour vérifier que le pare-feu protège la charge de travail que vous devez protéger.



Utiliser Panorama pour acheminer les journaux au centre de sécurité Azure

Si vous utilisez Panorama pour gérer vos pare-feu, vous pouvez utiliser des modèles et des groupes de périphériques pour transférer les journaux du pare-feu vers le Centre de sécurité Azure. Avec le profil par défaut du transfert du registre du centre de sécurité Azure, les registres des menaces et

©2023 Palo Alto Networks, Inc.

des incendies de forêt de gravité faible, moyenne, élevée ou critique générés sur le pare-feu sont affichés comme des alertes de sécurité sur le tableau de bord du centre de sécurité Azure. Pour que vous puissiez mieux cibler et trier les alertes, vous pouvez configurer des filtres de journaux granulairesuniquement pour transférer les journaux qui vous intéressent ou transférer uniquement les journaux de gravité critiques et élevés. Vous pouvez également associer de manière sélective le profil de transfert de journaux à quelques règles de stratégie de sécurité basées sur vos applications et vos besoins de sécurité.

Pour activer l'intégration du Centre de sécurité Azure à partir de Panorama, utilisez le flux de travail suivant.

STEP 1 | Ajoutez le pare-feu en tant que périphérique géré sur Panorama.

STEP 2 | À partir de Panorama, créez un modèle et un groupe de périphériques pour transférer les paramètres de transfert de journaux vers les pare-feu qui transmettront les journaux au Centre de sécurité Azure.

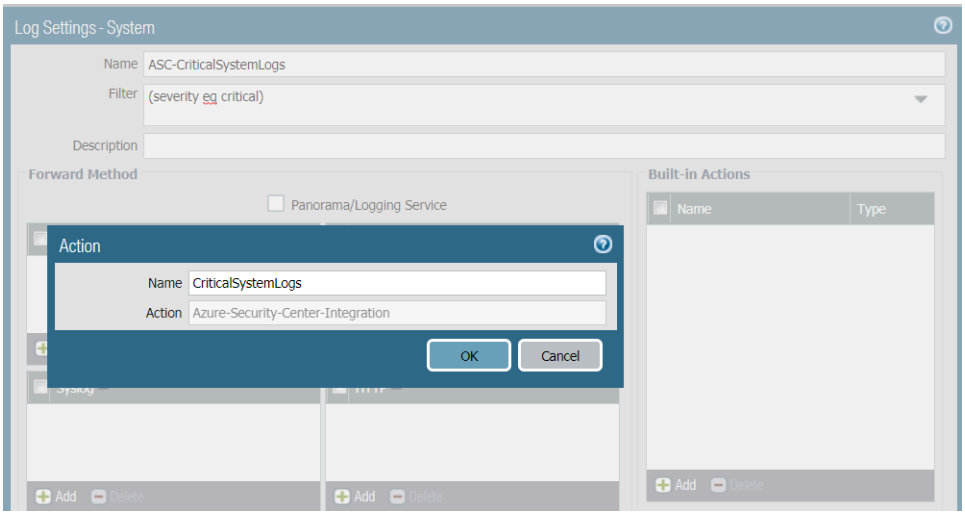
STEP 3 | Spécifiez les types de journaux à transmettre au service d'enregistrement.

La méthode d'activation du transfert dépend du type de journal. Pour les journaux générés en fonction d'une correspondance de stratégie, vous utilisez un profil de transfert de journaux dans

 ©2023 Palo Alto Networks, Inc.

un groupe de périphériques. Pour les autres types de journaux, vous utilisez la configuration des paramètres de journal dans un modèle.

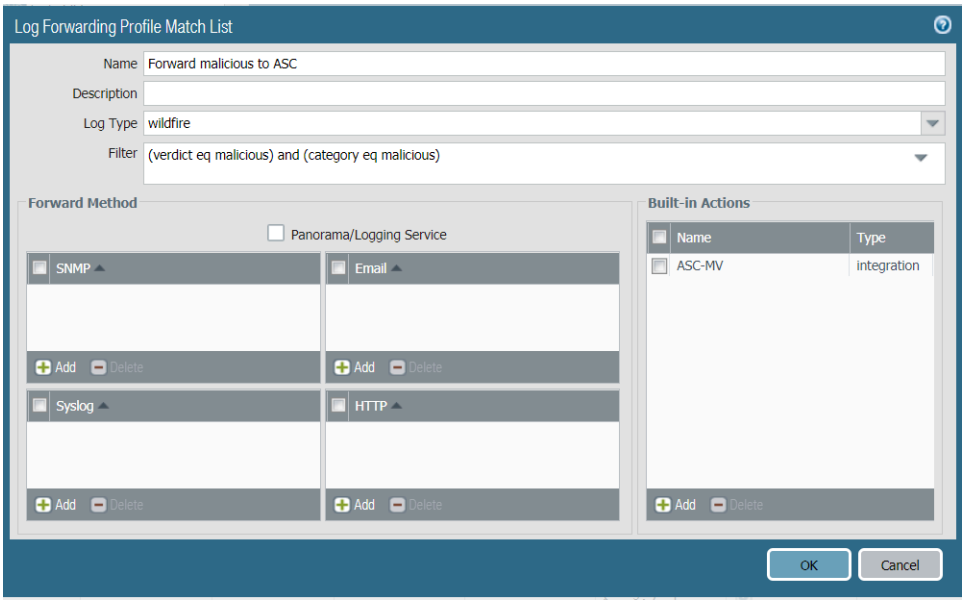
1. Configurez le transfert des journaux système, de configuration, User-ID et de correspondance HIP.
   1. Sélectionnez **Device (Appareil)** > **Log Settings (Paramètres des journaux)**.
   2. Sélectionnez le **Template (Modèle)** contenant les pare-feu que vous souhaitez transférer vers le service de journalisation.
   3. Pour chaque type de journal que vous transférez au service de journalisation, **Add (Ajoutez)** un filtre de liste de correspondance. Donnez-lui un **Name (Nom)**, vous pouvez également définir un **Filter (filtre)**.
   4. **Add (Ajoutez)** des actions intégrées et entrez **Name (Nom)**. L'action Azure-Security-Center-Integration sera sélectionnée automatiquement. Cliquez sur **OK**.



   5. Cliquez sur **OK**.
2. Configurez le transfert de tous les autres types de journaux qui sont générés lorsqu'une correspondance de stratégie se produit, telle que Trafic, Menace, Soumission WildFire, Filtrage d'URL, Filtrage des données et Journaux d'authentification. Pour transférer ces journaux, vous devez créer et attacher un profil de transfert de journal à chaque règle de stratégie pour laquelle vous souhaitez transférer les journaux.
   1. Sélectionnez le **Device Group (Groupe de périphériques)**, et ensuite, sélectionnez **Objects (Objets)** > **Log Forwarding (Transfert des journaux)** pour **Add (Ajouter)** un profil. Dans la liste de correspondance du profil de transfert de journaux, ajoutez chaque type de journal que vous souhaitez transférer.

 ©2023 Palo Alto Networks, Inc.

2. Sélectionnez **Add (Ajouter)** dans les actions intégrées pour permettre aux pare-feu du groupe d'appareils de transférer les journaux vers Azure Security Center.



3. Créez des politiques de sécurité de base dans le groupe de périphériques que vous venez de créer et sélectionnez **Actions** pour attacher le profil de transfert de journal que vous avez créé pour le transfert des journaux vers le Centre de sécurité Azure. Tant que le pare-feu possède des interfaces et des zones et une politique de sécurité de base, il ne laissera passer aucun trafic et seul le trafic qui correspond à la règle de politique de sécurité sera journalisé (par défaut).
4. Pour chaque règle que vous créez, sélectionnez **Actions** et sélectionnez le profil de transfert de journaux qui permet au pare-feu de transmettre les journaux vers le Centre de sécurité Azure.

STEP 4 | Validez vos modifications dans Panorama et envoyez-les au modèle et au groupe de périphériques que vous avez créés.

STEP 5 | Vérifiez que les journaux du pare-feu sont transmis vers le Centre de sécurité Azure.

1. Connectez-vous au portail Azure, sélectionnez **Azure Security Center (Centre de sécurité Azure)**.
2. Vérifiez que vous pouvez voir les journaux du pare-feu en tant qu'alertes de sécurité sur le tableau de bord du Centre de sécurité Azure.

©2023 Palo Alto Networks, Inc.

Déploiement du pare-feu VM-Series dans Azure Stack

Vous pouvez déployer le pare-feu de la série VM sur la Stack d'Azure pour sécuriser le trafic inter-sous-réseau entre les applications dans une architecture à plusieurs niveaux et le trafic sortant des serveurs dans votre déploiement de Stack d'Azure. Si vous voulez utiliser le pare-feu de la série VM comme passerelle pour sécuriser le trafic entrant destiné aux serveurs dans votre déploiement de la cheminée Azure, vous devez déployer un appareil NAT devant le pare-feu qui reçoit le trafic entrant et l'achemine au pare-feu. L'appliance NAT est nécessaire parce que sur la cheminée Azure, vous ne pouvez pas attribuer une adresse IP publique à une interface non primaire d'une machine virtuelle, comme le pare-feu de la série VM.

Le pare-feu de série VM sur la cheminée Azure n'a pas de prise en charge pour le bootstrap, les aperçus d'application Azure ou l'intégration du centre de sécurité Azure.

Contrairement à l'Azure public, vous n'avez pas de modèle de solution pour déployer le pare-feu de la série VM sur la cheminée Azure. Par conséquent, vous devez utiliser un modèle ARM pour déployer le pare-feu de la série VM. Pour commencer, vous pouvez utiliser l'exemple de modèle ARM appuyé par la collectivité dans GitHub, puis élaborer votre propre modèle ARM pour les déploiements de production.

STEP 1 | Téléchargez les articles du marché de Azure à AzureStack.

Pour déployer le pare-feu VM-Series sur Azure Stack, vous devez avoir accès à l'offre BYOL de l'image PAN-OS (8.1 ou version ultérieure) du pare-feu de la série VM. Vous pouvez télécharger l'image directement du marché Azure à Azure Stack dans un déploiement connecté.

STEP 2 | Accédez au portail Azure Stack.

Votre opérateur Azure Stack (un fournisseur de services ou un administrateur de votre organisation) doit fournir l'adresse URL exacte pour accéder au portail.

STEP 3 | Déployez le pare-feu VM-Series.

Un modèle de solution pour le pare-feu de série VM n'est pas disponible sur Azure Stack. Par conséquent, vous devez renvoyer à l'image que vous avez téléchargée à l'étape précédente, dans un modèle ARM, pour déployer le pare-feu de la série VM. Pour commencer, vous pouvez déployer l'exemple de modèle de GAD qui est disponible sur GitHub dans le cadre de la politique appuyée par la collectivité :

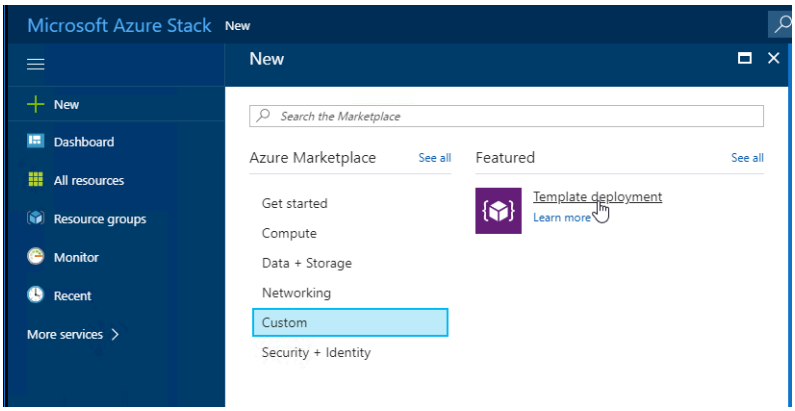
1. Obtenez l'exemple de modèle de Azure Stack GitHub.
   - Sélectionnez azurestackdeploy.json pour voir le contenu.
   - Cliquez sur Raw et copiez le contenu du fichier JSON.
2. Déployer l'exemple de modèle GitHub.Déployer l'exemple de modèle GitHub.

   Vous pouvez déployer le pare-feu dans un groupe de ressources existant vide ou dans un nouveau groupe de ressources. Le VNet par défaut dans le modèle est 192.168.0.0/16 et il déploie un pare-feu VM-Series avec trois interfaces réseau : une interface de gestion sur le sous-réseau 192.168.0.0/24 et deux interfaces de plan de données sur les sous-

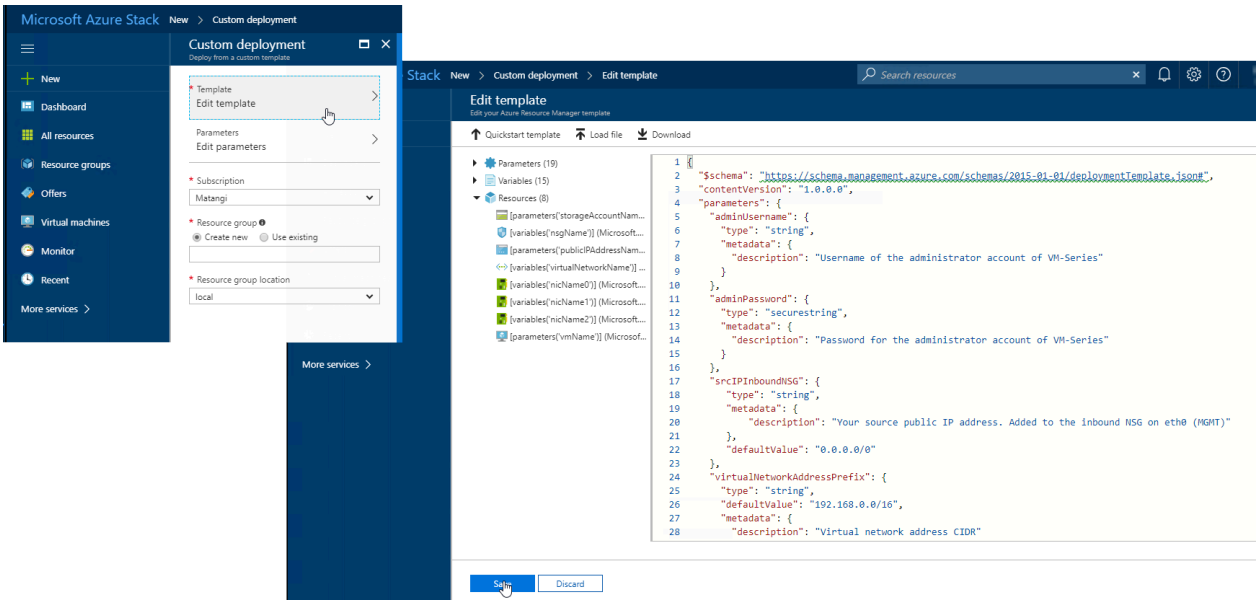
 ©2023 Palo Alto Networks, Inc.

réseaux 192.168.1.0/24 et 192.168.2.0/24. Vous pouvez personnaliser ces sous-réseaux en fonction de vos besoins.

- Ouvrez une session sur le portail Azure Stack.
- Sélectionnez **New (Nouveau)** > **Custom (Personnalisé)** > **Template deployment (Déploiement de modèle)**.

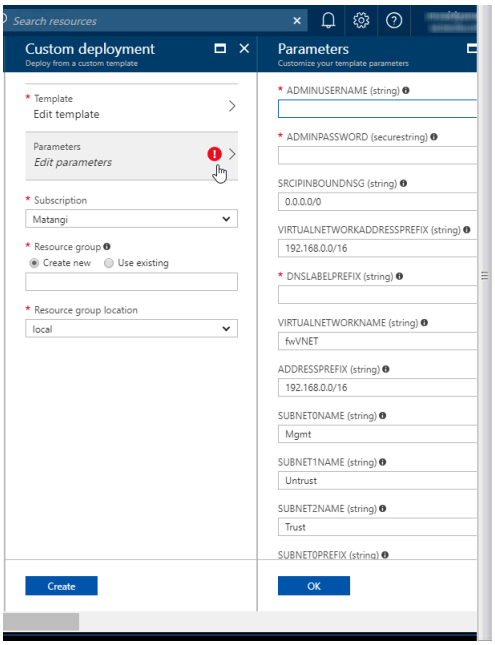


- **Edit template (Modifiez le modèle)**, supprimez tout le contenu existant dans le modèle et collez le contenu du modèle JSON que vous avez copié plus tôt et **Save (Sauvegardez)**.

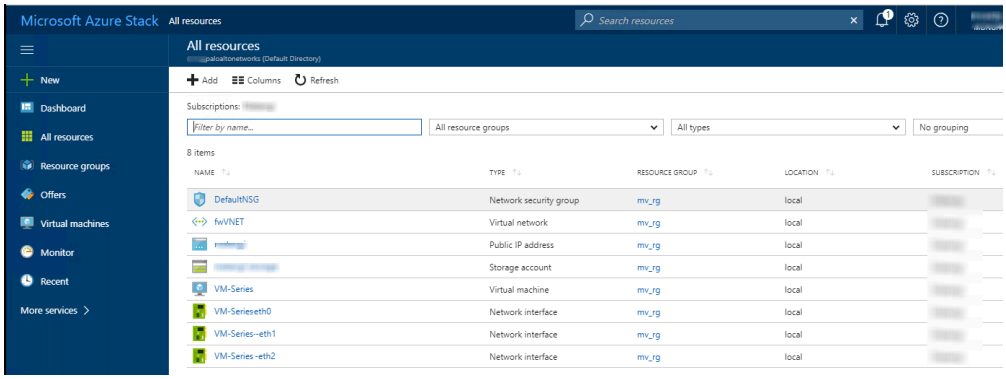


 ©2023 Palo Alto Networks, Inc.

- **Edit parameters (Modifiez les paramètres)**, saisissez les valeurs des paramètres requis et modifiez les valeurs par défaut au besoin, puis cliquez sur **OK**.



- Sélectionnez **Subscription (l'abonnement)**que vous souhaitez désactiver, puis cliquez sur **OK**.
- Choisissez un **Resource Group (Groupe de ressources)** groupe de ressources existant qui est vide ou créez un nouveau groupe, puis cliquez sur **OK**.
- Cliquez sur **Create (Créer)**. Une nouvelle vignette sur le tableau de bord affiche la progression du déploiement du modèle.



STEP 4 | Étapes suivantes :

1. Connectez-vous à l'interface Web du pare-feu.

   En utilisant une connexion sécurisée (https) à partir de votre navigateur Web, connectez-vous au nom de DNS pour le pare-feu. Saisissez le nom d'utilisateur/mot de passe que

 ©2023 Palo Alto Networks, Inc.

vous avez défini précédemment. Un avertissement de certificat s'affiche ; ne vous en préoccupez pas. Continuez vers la page Web.

2. Activez les licences sur le pare-feu VM-Series.

   1. Création d'un compte de soutien et Enregistrer le pare-feu de la série VM (avec le code d'auteur).
   2. Sur l'interface Web du pare-feu, sélectionnez **Device (Appareils)** > **Licenses (Licences)** et sélectionnez **Activate feature using authentication code (Activer la fonctionnalité à l'aide du code d'autorisation)**.
   3. Saisissez le code d'autorisation de capacité enregistré sur le portail de support. Le pare-feu se connecte alors au serveur de mise à jour (updates.paloaltonetworks.com), télécharge la licence et redémarre automatiquement.
   4. Reconnectez-vous à l'interface Web sur le **Dashboard (Tableau de bord)** et vérifiez qu'un numéro de **série** valide s'affiche.

      Le **VM Mode (Mode VM)** affiche Microsoft Azure.

      Si le terme Unknown (Inconnu) s'affiche, cela signifie que le périphérique n'est pas sous licence. Pour afficher les journaux de trafic sur le pare-feu, vous devez installer une licence de capacité valide.

STEP 5 | 7

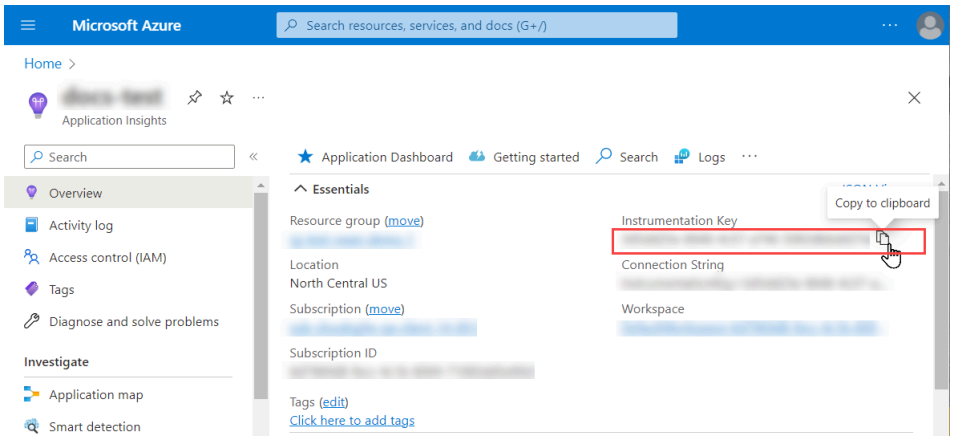
 ©2023 Palo Alto Networks, Inc.

Activer Azure Application Insights sur le pare-feu VM-Series

Le pare-feu VM-Series sur Azure peut publier des statistiques PAN-OS personnalisées nativement dans Azure Application Insights que vous pouvez utiliser pour surveiller les pare-feu directement à partir du portail Azure. Ces statistiques vous permettent d'évaluer les performances et les modèles d'utilisation que vous pouvez utiliser pour définir des alarmes et prendre des mesures pour automatiser des événements tels que le lancement ou l'arrêt des instances de pare-feu VM-Series. Reportez-vous à la section Statistiques PAN-OS personnalisées publiées pour la surveillance pour obtenir une description des statistiques disponibles.

STEP 1 | Sur le portail Azure, créez votre instance Application Insights pour surveiller le pare-feu et copiez la **Instrumentation Key (Clé d'instrumentation)** à partir de **Configure (Configuration)** > **Properties (Propriétés)**.

Le pare-feu a besoin de cette clé pour s'authentifier auprès de l'instance Application Insights et y publier ses métriques. Reportez-vous à la section Autorisations principales de VM-Series sur le service Azure pour connaître les autorisations requises.

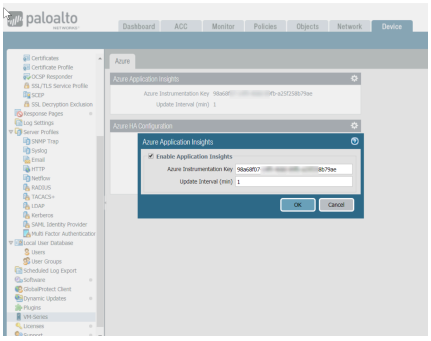


 ©2023 Palo Alto Networks, Inc.

STEP 2 | Activez le pare-feu pour publier les métriques dans votre instance Application Insights.

1. Connectez-vous au pare-feu VM-Series sur Azure.
2. Sélectionnez **Device (Appareil)** > **VM-Series** > **Azure**.
3. Modifiez **Azure Application Insights** et entrez la clé d'instrumentation copiée précédemment.

   L'intervalle par défaut pour la publication des statistiques est de cinq minutes. Vous pouvez changer l'intervalle et indiquer une valeur qui varie entre 1 et 60 minutes.



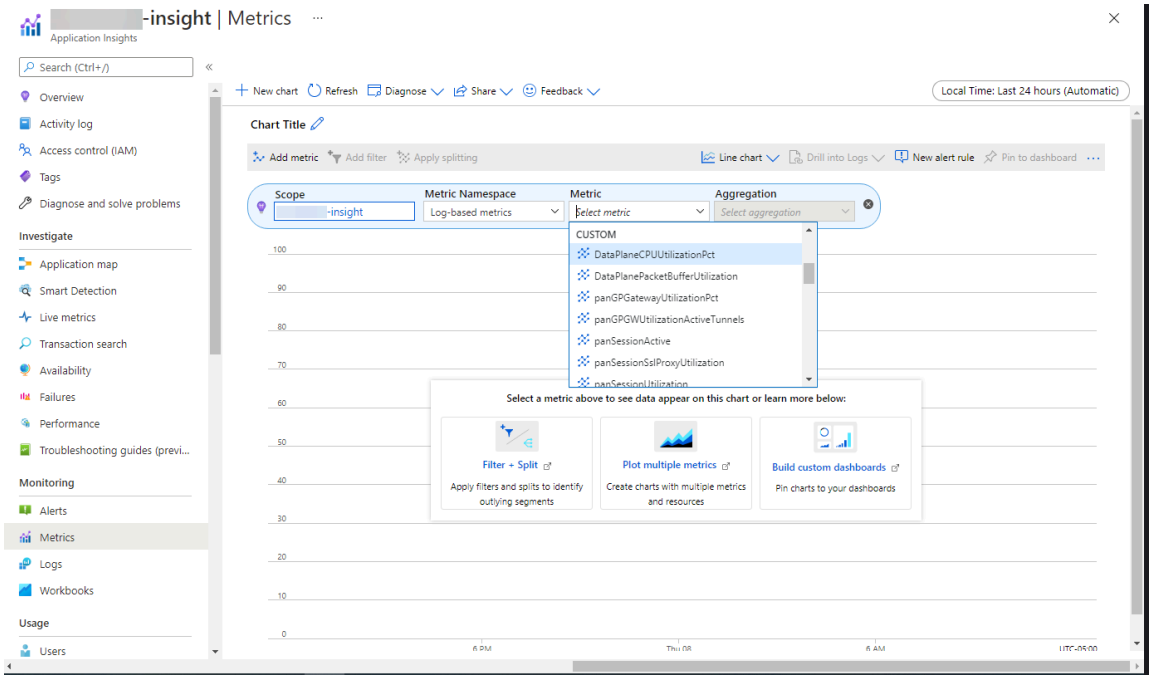
4. **Commit (Validez)** vos modifications.

   Le pare-feu génère un journal système dans lequel il consigne la réussite ou l'échec de l'authentification auprès d'Azure Application Insights.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Vérifiez si les statistiques s'affichent sur le tableau de bord Azure Application Insights.

1. Sur le portail Azure, sélectionnez l'instance Application Insights et **Monitoring (Surveillance)** > **Metrics (Métriques)** pour afficher les métriques personnalisées PAN-OS.



2. Sélectionnez le(s) métrique(s) que vous souhaitez surveiller pour voir les tendances et les alertes. Reportez-vous à la documentation de Microsoft Azure pour plus de détails sur l'exploration des métriques dans Application Insights.

 ©2023 Palo Alto Networks, Inc.

Surveillance sur Azure

La surveillance des ressources de Microsoft® Azure® vous permet de mettre à jour dynamiquement les règles de stratégie de sécurité pour appliquer de manière cohérente la stratégie de sécurité sur tous les actifs déployés de votre abonnement Azure. Pour activer cette capacité, vous devez installer le plug-in Panorama pour Azure et activer la communication API entre Panorama et vos abonnements à Azure. Panorama peut collecter le mappage adresse IP-balise de toutes vos ressources Azure et utilise l'API pour transmettre les informations sur les ressources Azure à votre pare-feu Palo Alto Networks®.

- À propos de la surveillance sur Azure
- Configuration du plugin Azure pour la surveillance sur Panorama
- Attributs surveillés à l'aide du plugin Panorama sur Azure

À propos de la surveillance sur Azure

Lorsque vous déployez ou arrêtez des machines virtuelles dans le cloud public Azure, vous pouvez utiliser le plug-in Panorama pour Azure pour appliquer de façon uniforme les règles de politique de sécurité sur ces charges de travail.

Le plugin Panorama pour Azure est conçu pour une échelle et vous permet de surveiller jusqu'à 100 abonnements Azure sur le Cloud public Azure. Avec ce plugin, vous utilisez Panorama comme point d'ancrage pour sonder vos abonnements pour les étiquettes, puis distribuez les métadonnées (carte IP d'adresse à étiquette) à de nombreux pare-feu dans un groupe d'appareils. Étant donné que Panorama communique avec vos abonnements Azure pour récupérer des informations sur les ressources Azure, vous pouvez rationaliser le nombre d'appels API effectués dans l'environnement cloud. Bien que vous puissiez définir la politique de sécurité localement sur le pare-feu, l'utilisation de Panorama et du plug-in centralise la gestion de la politique de sécurité, assurant ainsi l'uniformité des politiques pour les architectures hybrides et d'origine cloud.

Reportez-vous à la Matrice de compatibilité pour plus d'informations sur la version du plug-in Panorama.

Configuration du plugin Azure pour la surveillance sur Panorama

Pour trouver toutes les charges de travail que votre organisation a déployées dans le cloud Azure, vous devez installer le plug-in Azure sur Panorama et configurer les ***définitions de surveillance*** qui permettent à Panorama de s'authentifier sur vos abonnements Azure et d'extraire l'information sur les charges de travail Azure. Panorama récupère l'adresse IP privée principale des ressources Azure et les étiquettes connexes. Pour une liste des éléments de métadonnées pris en charge par Panorama, consultez Liste des attributs surveillés dans Azure.

Après que Panorama a détecté les attributs, pour déplacer l'information de la ressource de Panorama vers les pare-feu, vous devez ajouter les coupe-feu (matériel ou série VM) comme dispositifs gérés sur Panorama, et regrouper les pare-feu en un ou plusieurs groupes d'appareils. Vous pouvez ensuite préciser les groupes d'appareils qui font partie du ***groupe de notification***, qui est un élément de configuration dans une définition de surveillance, que Panorama utilise pour enregistrer le mappage de l'adresse IP à l'étiquette qu'il extrait d'Azure.

©2023 Palo Alto Networks, Inc.

Enfin, pour assurer l'application uniforme des politiques de sécurité dans l'ensemble de vos charges de travail Azure, vous devez établir des groupes d'adresses dynamiques et les renvoyer dans des règles de politique qui autorisent ou refusent le trafic vers les adresses IP des ressources Azure. Pour simplifier votre configuration et gérer vos politiques et objets de façon centralisée à partir de Panorama, vous pouvez définir les groupes d'adresses dynamiques et les règles de politique de sécurité sur Panorama et les déplacer vers les pare-feu plutôt que de gérer les groupes d'adresses dynamiques et les règles de politique de sécurité localement sur chaque pare-feu.

La fiche Azure sert à surveiller les ressources Azure sur le cloud public Azure. Azure Government ou Azure China ne sont pas pris en charge.

- Liste de planification pour la surveillance de la MV avec le plugin Azure
- Installer le Plugin Azure
- Configurer le plugin Azure pour la surveillance

Liste de planification pour la surveillance avec le plugin Azure

- Configurer l'application Active Directory et un directeur de service pour permettre l'accès à l'API – Pour que Panorama puisse interagir avec les API Azure et recueillir de l'information sur vos charges de travail, vous devez créer un directeur de service Active Directory Azure. Ce principal de service comporte les autorisations nécessaires pour s'authentifier auprès d'Azure AD et accéder aux ressources de votre abonnement.

  Pour terminer cette configuration, vous devez disposer des permissions nécessaires pour enregistrer une application auprès de votre locataire Azure AD et affecter l'application à un rôle de votre abonnement. Si vous ne disposez pas des autorisations nécessaires, demandez à votre administrateur Azure AD ou d'abonnement de créer un principal de service avec un rôle IAM de lecteur ou les autorisations personnalisées spécifiées à la section Autorisations principales de VM-Series sur le service Azure.
- Assurez-vous que l'ID d'abonnement est unique parmi les directeurs de service. Panorama vous permet d'utiliser un seul service principal pour surveiller un abonnement Azure. Vous pouvez surveiller jusqu'à 100 abonnements Azure avec 100 ressources principales de service. À partir du plug-in Panorama pour Azure version 3.2.0, vous pouvez surveiller jusqu'à 500 abonnements Azure. Prenez note des temps de traitement décrits dans le tableau ci-dessous.

	Nombre d'abonnements				
	100	200	300	400	500
Utilisation des ressources système	• Processeur : 22 % • Mémoire : 0,025 Mo	• Processeur : 23,8 % • Mémoire : 0,025 Mo	• Processeur : 31,8 % • Mémoire : 0,025 Mo	• Processeur : 28,6 % • Mémoire : 0,025 Mo	• Processeur : 39,2 % • Mémoire : 0,025 Mo
Temps moyen de traitement de toutes les définitions de surveillance	1 heure, 15 minutes	2 heures, 30 minutes	3 heures, 30 minutes	4 heures	5 heures

©2023 Palo Alto Networks, Inc.

	Nombre d'abonnements				
	100	200	300	400	500
Temps moyen de traitement des mises à jour des étiquettes	5 minutes	10 minutes	15 minutes	20 minutes	25 minutes

Les informations du tableau ci-dessus ont été capturées sur une instance avec 8 vCPU et 32 Go de mémoire.

- Panorama peut pousser jusqu'à 8 000 adresses IP pour cartographier les pare-feu ou le système virtuel assigné à un groupe de dispositifs. Passer en revue les exigences pour Panorama et les pare-feu gérés :
  - Configuration minimale requise (consultez les informations concernant le plug-in Panorama dans la Matrice de compatibilité) :

    Appareil virtuel Panorama ou appareil matériel Panorama exécutant Panorama 8.1.3 ou version ultérieure, avec un contrat support actif et une licence de gestion de périphériques pour la gestion des pare-feu.

    Pare-feu nouvelle génération sous licence exécutant PAN-OS 8.0 ou 8.1.
  - Vous devez ajouter les pare-feu comme dispositifs gérés sur Panorama et créer des groupes d'appareils de façon à pouvoir configurer Panorama pour aviser ces groupes à l'aide de l'information qu'il récupère. Les groupes d'appareils peuvent inclure des pare-feu de série VM ou des systèmes virtuels sur les pare-feu matériels.
  - Le nombre d'étiquettes que le plugin Panorama peut récupérer et enregistrer est le suivant :

    Sur Panorama exécutant la version 8.1.3 ou ultérieure et gérant des pare-feu exécutant PAN-OS version 8.1.3 ou précédente, les pare-feu ou systèmes virtuels inclus dans un groupe de périphériques peuvent disposer de 7 000 adresses IP comprenant 10 étiquettes chacune, ou de 6 500 adresses IP avec 15 étiquettes chacune.

    Sur Panorama version 8.1.3 ou ultérieure gérant des pare-feu exécutant PAN-OS 8.0.x, les pare-feu ou systèmes virtuels inclus dans un groupe de périphériques peuvent disposer de 2 500 adresses IP avec 10 étiquettes chacune.
    - Si vos appareils Panorama sont en configuration de disponibilité élevée, vous devez installer manuellement la même version du plugin Azure sur les deux appareils Panorama pairs.

      Vous configurez le plugin Azure sur le pair actif de Panorama seulement. Sur l'engagement, la configuration est synchronisée avec le pair passif Panorama. Seuls les pairs actifs de Panorama sondent les abonnements Azure que vous avez configurés pour la surveillance.

Installer le Plugin Azure

Pour commencer la surveillance sur Azure, vous devez télécharger et installer le plugin Azure sur Panorama. Si vous avez une configuration d'HA de Panorama, répétez ce processus d'installation sur chaque pair de Panorama.

©2023 Palo Alto Networks, Inc.

Si vous avez déjà installé un plugin Panorama, le processus d'installation (ou de désinstallation) d'un autre plugin nécessite un redémarrage Panorama pour vous permettre d'engager des changements. Alors, installez des plugins supplémentaires pendant une fenêtre de maintenance planifiée pour permettre un redémarrage.

Si vous avez un appareil Panorama autonome ou deux appareils Panorama installés dans une paire HA avec plusieurs plug-ins installés, les plug-ins peuvent ne pas recevoir les informations des indicateurs d'adresse IP mises à jour si un ou plusieurs des plug-ins ne sont pas configurés. Cela se produit, car Panorama ne transfère pas les informations des indicateurs d'adresse IP aux plug-ins non configurés. De plus, ce problème peut se présenter si un ou plusieurs plug-ins Panorama ne se trouvent pas dans l'état Registered (Enregistré) ou Success (Réussite) (l'état positif diffère sur chaque plug-in). Assurez-vous que vos plug-ins se trouvent dans l'état positif avant de continuer ou d'exécuter les commandes décrites ci-dessous.

Si vous rencontrez ce problème, il existe deux solutions alternatives :

- Désinstallez le ou les plug-ins non configurés. Il est déconseillé d'installer un plug-in que vous n'envisagez pas de configurer dans l'immédiat
- Vous pouvez utiliser les commandes suivantes pour contourner ce problème. Exécutez la commande suivante pour chaque plug-in non configuré sur chaque instance de Panorama afin que Panorama n'attende pas pour envoyer des mises à jour. Dans le cas contraire, vos pare-feu risquent de perdre certaines informations des indicateurs d'adresse IP.

  ```
  request plugins dau plugin-name <plugin-name> unblock-device-push yes
  ```

  Vous pouvez annuler cette commande en exécutant :

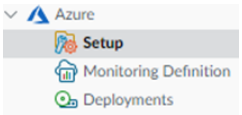
  ```
  request plugins dau plugin-name <plugin-name> unblock-device-push no
  ```

Les commandes décrites ne sont pas persistantes lors des redémarrages et doivent être réutilisées pour tout redémarrage ultérieur. Pour Panorama en paire HA, les commandes doivent être exécutées sur chaque Panorama.

STEP 1 | Connectez-vous à l'interface Web Panorama et sélectionnez **Panorama** > **Plugins** et cliquez sur **Check Now** pour obtenir le plugin AWS.

STEP 2 | Sélectionnez **Download (Téléchargez)** et **Install (Installez)** le plugin.

Après l'installation réussie, Panorama se rafraîchit et le plugin Azure s'affiche sur l'onglet **Panorama**.



STEP 3 | Redémarrez Panorama

Sélectionnez **Panorama** > **Setup (Configuration)** > **Operations** > **Reboot Panorama (Réamorcer Panorama)**.

Configurer le plugin Azure pour la surveillance

Pour commencer à surveiller les ressources dans votre déploiement de cloud public AWS, après avoir Install the Azure Plugin (installé la fiche Azure) vous devez créer une définition de surveillance. Cette définition précise le principal de service qui est autorisé à accéder aux ressources dans l'abonnement

 ©2023 Palo Alto Networks, Inc.

Azure que vous voulez surveiller et le groupe de notification qui comprend les pare-feu sur lesquels Panorama devrait appliquer tous les mappages d'adresse IP à étiquette qu'il récupère. Pour appliquer la politique, vous devez ensuite créer des groupes d'adresses dynamiques et les consulter dans la politique sur la sécurité. Les groupes d'adresses dynamiques vous permettent de filtrer les étiquettes auxquelles vous voulez associer, de sorte que le pare-feu puisse enregistrer l'adresse IP privée principale pour les étiquettes, puis permettre ou refuser l'accès au trafic à partir des charges de travail en fonction des règles de politique que vous définissez.

STEP 1 | Connectez-vous à l'interface Web Panorama.

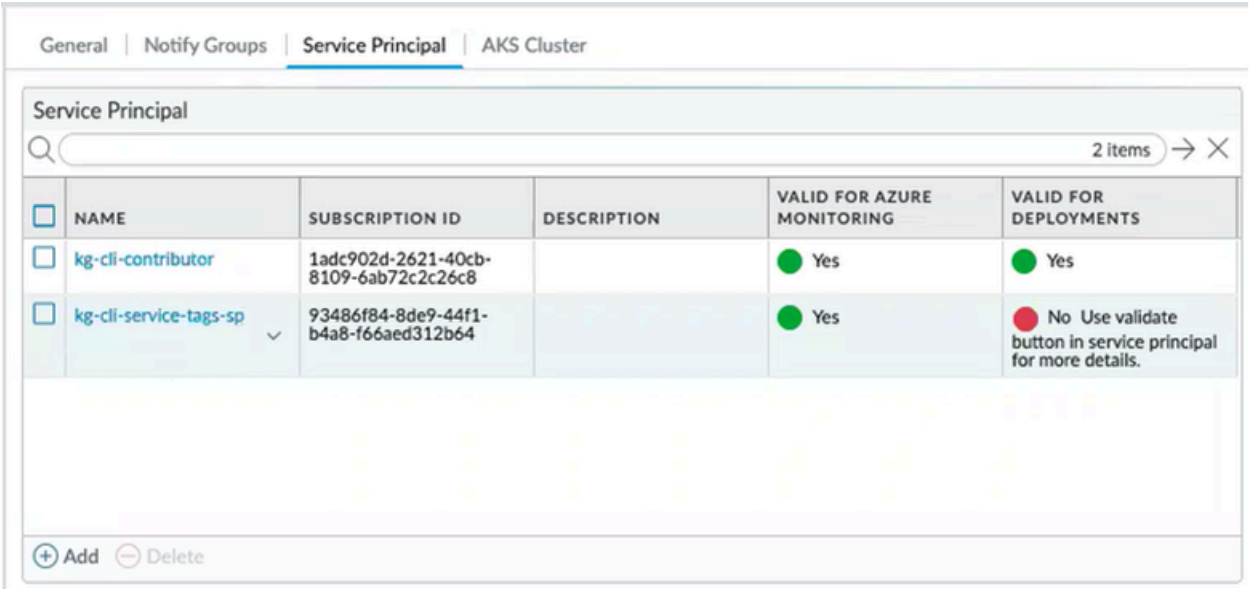
 ©2023 Palo Alto Networks, Inc.

STEP 2 | Préparer les objets suivants pour permettre la surveillance sur Azure.

- Ajoutez un principal de service.

  Le Service Principal est le compte de service que vous avez créé sur le portail Azure. Ce compte est associé à l'Azure AD et a des autorisations limitées d'accès et de surveillance des ressources dans votre abonnement Azure.

  1. Sélectionnez **Panorama** > **Plugins** > **Azure** > **Setup (Configuration)** > **Service Principal (Directeur de service)** > **Add (Ajouter)**.

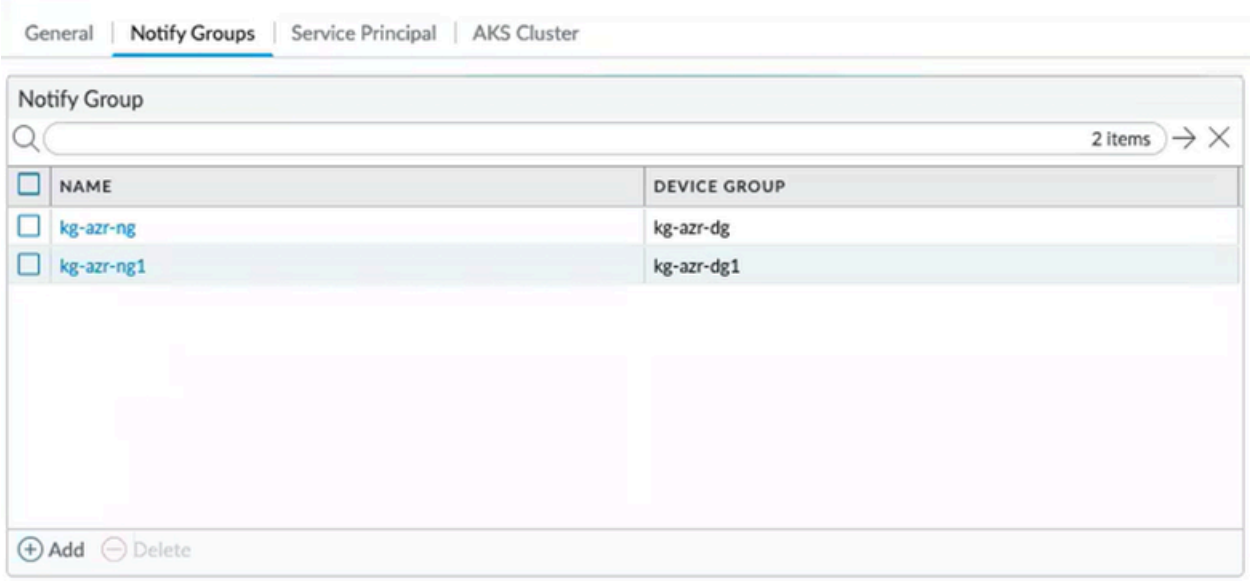


  2. Donnez un **nom** et s'il y a lieu, une **description** pour identifier le compte de service.
  3. Entrez le **Subcription ID (l'ID d'abonnement pour l'abonnement Azure)** que vous voulez surveiller. Vous devez vous connecter à votre portail Azure pour obtenir cet ID d'abonnement.
  4. Entrez **Client Secret :** et entrez-la de nouveau pour confirmer.
  5. Saisissez le **Tenant ID (ID de locateur)**. Le numéro d'identification du locataire est celui que vous avez sauvegardé lorsque vous avez créé l'application Active Directory.
  6. Cliquez sur **Valider** pour vérifier que les clés et les ID que vous avez entrés sont valides et que Panorama peut communiquer avec l'abonnement Azure au moyen de l'API.

- Ajoutez un groupe de notification.

  1. Sélectionnez **Panorama** > **Plugins** > **Azure** > **Setup (Configuration)** > **Notify Groups (Groupes de notification)** > **Add (Ajouter)**.

©2023 Palo Alto Networks, Inc.



2. Entrez un **Name (Nom)** et, s'il y a lieu, une **Description** pour identifier le groupe de pare-feu vers lequel Panorama pousse l'information qu'il extrait.
3. Sélectionnez les **Device Groups (groupes d'appareils)**, qui sont un groupe de pare-feu ou de systèmes virtuels, vers lesquels Panorama poussera l'information (carte IP d'adresse à étiquette) qu'il extrait de vos VPC AWS. Les pare-feu utilisent cette mise à jour pour déterminer la liste la plus récente des membres qui constituent les groupes d'adresses dynamiques référencés dans la politique.

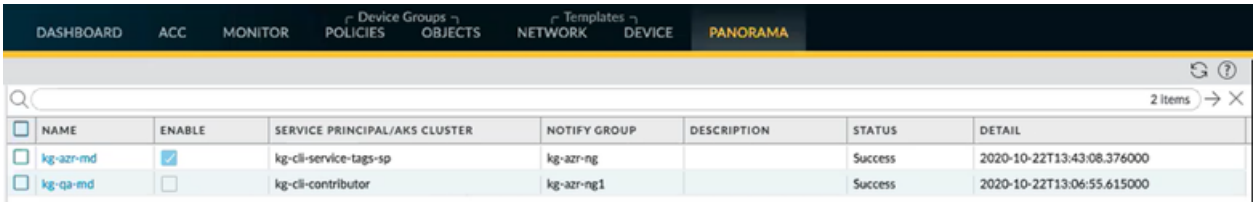
   Réfléchissez soigneusement à vos groupes d'appareils.

   - Étant donné qu'une définition de surveillance ne peut inclure qu'un seul groupe d'avis, assurez-vous de sélectionner tous les groupes d'appareils pertinents au sein de votre groupe d'avis. Si vous voulez désenregistrer les étiquettes que Panorama a enfoncées dans un pare-feu inclus dans un groupe de notification, vous devez supprimer la définition de surveillance.
   - Pour enregistrer des étiquettes à tous les systèmes virtuels sur un pare-feu activé pour plusieurs systèmes virtuels, vous devez ajouter chaque système virtuel à un groupe de dispositifs distinct sur Panorama et attribuer les groupes de dispositifs au groupe de notification. Panorama enregistrera les étiquettes dans un seul système virtuel, si vous attribuez tous les systèmes virtuels à un seul groupe d'appareils.
4. Vérifier que la surveillance est activée sur le plugin. Ce réglage doit être activé pour que Panorama communique avec le cloud public Azure pour la surveillance.

   La case à cocher **Enable Monitoring (Activer la surveillance)** se trouve dans **Panorama** > **Plugins (Plug-ins)** > **Azure** > **Setup (Configuration)** > **General (Général)**.

©2023 Palo Alto Networks, Inc.

STEP 3 | Créez une **Monitoring Definition (Définition de surveillance)**.



Lorsque vous ajoutez une nouvelle définition de surveillance, celle-ci est activée par défaut.

- Sélectionnez **Panorama** > **Plugins (Plug-ins)** > **Azure** > **Monitoring Definition (Définition de surveillance)**, pour **Add (Ajouter)** une nouvelle définition.
- Saisissez un **Name (Nom)** et éventuellement une **Description** pour identifier l'abonnement Azure pour lequel vous utilisez cette définition.
- Sélectionnez le **Service Principal (Principal de service)** et le **Notify Group (Groupe de notification)**.

  Panorama a besoin des clés et des ID que vous précisez dans la configuration Service Principal (Principal de service) pour générer un jeton Azure Bearer qui est utilisé dans l'en-tête de l'appel API pour recueillir des renseignements sur vos charges de travail.

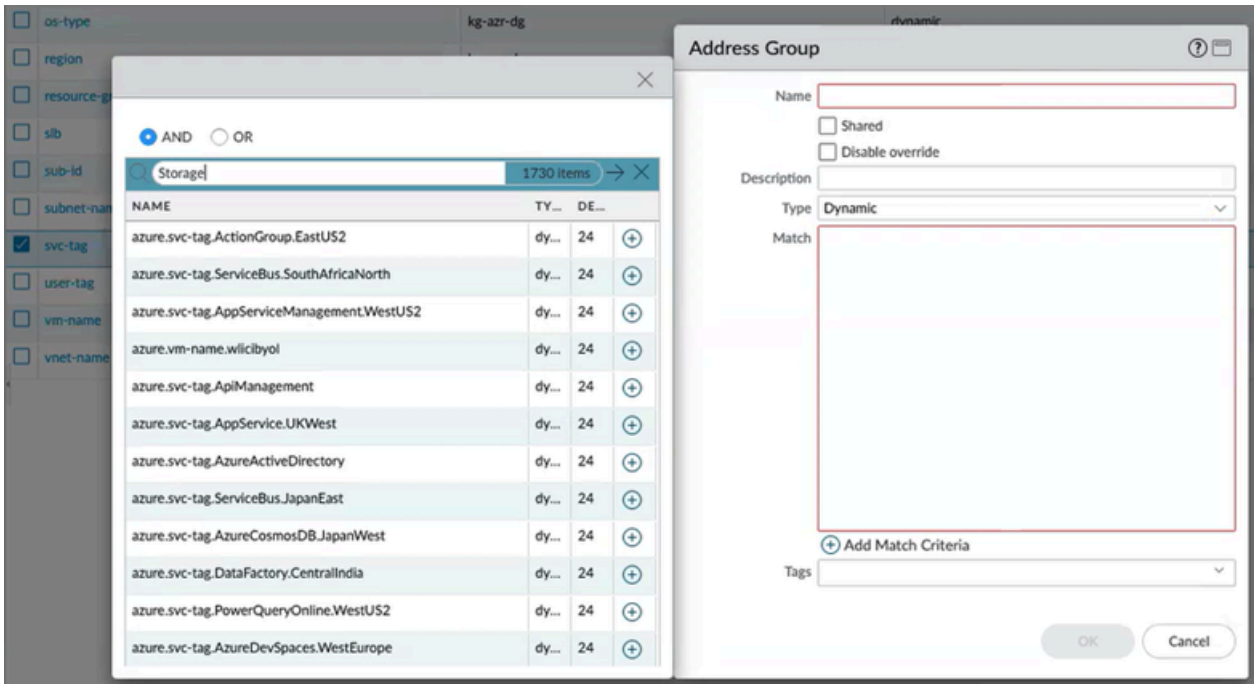
STEP 4 | **Engagez** les changements sur Panorama.

Assurez-vous que l'état de la définition de surveillance s'affiche comme « Succès ». S'il échoue, vérifiez que vous avez entré le code d'abonnement Azure avec exactitude et que vous avez fourni les bonnes clés et les bons numéros d'identification pour le service principal.

©2023 Palo Alto Networks, Inc.

STEP 5 | Vérifiez que vous pouvez visualiser l'information sur Panorama et définir les critères d'appariement pour les groupes d'adresses dynamiques.

Certaines extensions de navigateur peuvent bloquer les appels API entre Panorama et Azure, ce qui empêche Panorama de recevoir les critères de correspondance. Si Panorama n'affiche aucun critère de correspondance et que vous utilisez des extensions de navigateur, désactivez ces extensions et cliquez sur Synchronize Dynamic Objects (Synchroniser des objets dynamiques) pour renseigner les étiquettes disponibles dans Panorama.



 ©2023 Palo Alto Networks, Inc.

Sur le basculeur HA, le Panorama nouvellement actif tente de se reconnecter au nuage Azure et de récupérer les étiquettes pour toutes les définitions de la surveillance. S'il y a une erreur lors de la reconnexion d'une seule définition de surveillance, Panorama génère un message de journal système

```
Unable to process subscriptions after HA switch-over;
 user-intervention required.
```

Lorsque vous voyez cette erreur, vous devez vous connecter à Panorama et résoudre le problème, par exemple, en supprimant un abonnement non valide ou en fournissant des informations d'identification valides, et valider vos modifications pour permettre à Panorama de se reconnecter et de récupérer les étiquettes pour toutes les définitions de surveillance. Même lorsque Panorama est déconnecté du cloud Azure, les pare-feu ont la liste de toutes les étiquettes qui ont été récupérées avant le basculement et peuvent continuer d'appliquer la politique sur cette liste d'adresses IP. Panorama retire toutes les étiquettes associées à l'abonnement seulement lorsque vous supprimez une définition de surveillance. Comme pratique exemplaire, pour surveiller ce problème, vous pouvez configurer log forwarding to an HTTPS destination (un journal orienté action vers une destination HTTPS) *à partir de Panorama afin de pouvoir prendre des mesures immédiatement.*

Attributs surveillés à l'aide du plugin Panorama sur Azure

Lorsque vous utilisez le plugin Panorama pour Azure, Panorama réunit l'ensemble suivant d'éléments ou d'attributs de métadonnées sur les machines virtuelles dans votre déploiement Microsoft® Azure®. Panorama peut récupérer un total de 32 étiquettes pour chaque VM, 11 étiquettes prédéfinies et jusqu'à 21 étiquettes définies par l'utilisateur.

La longueur maximale d'une étiquette peut être de 127 caractères. Si une étiquette a plus de 127 caractères, Panorama ne récupère pas l'étiquette et ne l'enregistre pas sur les pare-feu. En outre, les étiquettes ne doivent pas contenir de caractères spéciaux non-ASCII tels que { ou ".

Les attributs suivants sont surveillés dans tous les plugins Panorama pour les versions Azure.

Machine virtuelle

Surveillance de machine virtuelle	Exemple
Nom de la machine virtuelle	azure-tag.vm-name.web_server1
Network Security Group Name (Nom du groupe de sécurité réseau)	azure-tag.nsg-name.myNSG

 ©2023 Palo Alto Networks, Inc.

Surveillance de machine virtuelle	Exemple
OS Type (Type de système d'exploitation)	azure-tag.os-type.Linux
Éditeur du système d'exploitation	azure-tag.os-publisher.Canonical
Offre de système d'exploitation	azure-tag.os-offer.UbuntuServer
SKU DU SYSTÈME D'EXPLOITATION	azure-tag.os-sku.14.04.5-LTS
Sous-réseau	azure-tag.subnet.webtier
VNet (Réseau virtuel)	azure-tag.vnet.untrustnet
Région Azure	Azure-tag.region.east-us
Nom du groupe de ressources	azure-tag.resource-group.myResourceGroup
ID d'abonnement	azure.sub-id.93486f84-8de9-44f1-b4a8-f66aed312b64
Étiquettes définies par l'utilisateur Jusqu'à 21 étiquettes définies par l'utilisateur sont prises en charge. Les étiquettes définies par l'utilisateur sont triées par ordre alphabétique, et les 21 premières étiquettes peuvent être utilisées sur les pare-feu.	azure-tag.mytag.value

Équilibreur de charge

Le plugin Panorama sur la version 3.0 ou ultérieure d'Azure prend en charge les étiquettes pour chaque passerelle d'application et l'équilibreur de charge standard (adresses IP publiques et privées). Chaque équilibreur de charge possède des étiquettes prédéfinies pour le groupe de ressources, le nom de l'équilibreur de charge et la région, et prend en charge jusqu'à 21 étiquettes définies par l'utilisateur et spécifiques à l'équilibrage de charge.

Étiquettes de l'équilibreur de charge	Exemple
Équilibreur de charge	azure.<type>.myLoadBalancer
Région Azure	Azure-tag.region.east-us
Nom du groupe de ressources	azure-tag.resource-group.myResourceGroup
Étiquettes définies par l'utilisateur	azure-tag.mytag.value

 ©2023 Palo Alto Networks, Inc.

Étiquettes de l'équilibreur de charge	Exemple
Jusqu'à 21 étiquettes définies par l'utilisateur sont prises en charge. Les étiquettes définies par l'utilisateur sont triées par ordre alphabétique, et les 21 premières étiquettes peuvent être utilisées sur les pare-feu.	

Sous-réseau/VNET

Le plugin Panorama sur la version 3.0 ou ultérieure d'Azure prend en charge les étiquettes pour chaque sous-réseau et VNET dans votre abonnement. Chaque sous-réseau et chaque étiquette VNET est associé à la plage CIDR IP complète, de sorte que vous pouvez créer des politiques basées sur une plage CIDR plutôt que sur des adresses IP individuelles. Le plugin interroge chaque sous-réseau et VNET de votre abonnement et crée des étiquettes pour chacun d'eux.

Étiquettes de sous-réseau et de VNET	Exemple
Nom de sous-réseau	azure.subnet-name.web
Nom de VNET	azure.vnet-name.myvnet

Surveillance des étiquettes de service

Le plugin Panorama sur la version 3.0 d'Azure prend en charge les étiquettes de service.

Les étiquettes de service Azure simplifient la sécurité des machines virtuelles et des réseaux virtuels Azure, car vous pouvez limiter l'accès au réseau aux seuls services Azure que vous souhaitez utiliser. Une étiquette de service représente un groupe de préfixes d'adresse IP pour un service Azure particulier. Par exemple, une étiquette peut représenter toutes les adresses IP de stockage.

Le plugin effectue un appel API quotidien (à 5h00 UTC) pour récupérer toutes les étiquettes de service du portail Azure, analyse la charge utile pour former des mappages de service IP et stocke les mappages dans la base de données du plugin. Les mappages sont transmis à configd, puis à Panorama. Si l'appel API ne renvoie pas d'informations sur le service, le plugin forme les mappages de service IP à partir du contenu de **`service_tags_public.json`**. Les journaux des plugins indiquent l'origine des mappages de service IP, la récupération quotidienne ou le fichier JSON.

Le plugin met également à jour les étiquettes de service pour une nouvelle installation du plugin, les événements de validation et le suivi de l'ajout ou de la suppression de définitions.

Un exemple de mappage de service IP est présenté ci-dessous :

```
Service Name: AppServiceManagementazure.svc-tag.<service-name>
 Example:     azure.svc-tag.AppServiceManagement.WestUS2 Public IP
 CIDRs:     13.166.40.0/26     54.179.89.0/18
```


©2023 Palo Alto Networks, Inc.

Configuration de la HA active/passive sur Azure

Vous pouvez configurer une paire de pare-feu VM-Series sur Azure dans une configuration haute disponibilité (HA) active/passive. Pour la HA sur Azure, vous devez déployer les deux homologues HA du pare-feu dans le même groupe de ressources Azure et vous devez installer la même version du Plug-in VM-Series sur les deux homologues HA.

- Configurer une HA active/passive sur Azure (trafic Nord-Sud et Est-Ouest) : si vous disposez d'une application Web déployée sur votre infrastructure Azure, et si vous devez sécuriser le trafic nord-sud, vous avez besoin d'une adresse IP flottante pour sécuriser le trafic lors du basculement. Cette adresse IP flottante, qui permet une connectivité externe, est toujours associée à l'homologue actif. Lors du basculement, le processus consistant à dissocier l'adresse IP et à la réassocier a l'homologue désormais actif peut prendre quelques minutes.
- Configurer une HA active/passive sur Azure (trafic Est-Ouest uniquement) : si vos exigences en matière d'accès et de sécurité de l'application sont contenues dans l'infrastructure Azure et si vous avez besoin de sécuriser le trafic est-ouest uniquement, vous n'avez pas besoin d'adresse IP flottante. Au lieu de cela, l'implémentation de la HA reconfigure automatiquement les UDR dans les tables de routage Azure pour fournir un temps de basculement plus rapide.

Pour activer la HA sur le pare-feu VM-Series sur Azure, vous devez créer une application Azure Active Directory et un principal de service qui incluent les autorisations répertoriées dans le tableau ci-dessous.

Type de HA Azure	Permissions	Portée du rôle

Déplacer l'adresse IP secondaire HA	`"Microsift.Authorization/*/read""Microsift.Compute/virtualMachines/read""Microsift.Network/networkInterfaces/*""Microsift.Network/networkSecurityGroups/*""Microsift.Network/virtualNetworks/join/action""Microsift.Network/virtualNetworks/subnets/join/action"`
	Les autorisations suivantes ne sont requises que si vous avez attribué une adresse IP publique à l'une de vos interfaces de données. L'interface SKU standard est recommandée.
	`"Microsift.Network/publicIPAddresses/join/action""Microsift.Network/publicIPAddresses/read""Microsift.Network/publicIPAddresses/write"`
		• Réseau virtuel dans lequel les VM sont déployées
		• Deux pare-feu VM-Series
		• NIC des deux pare-feu VM-Series
		• Network Security Group (Groupe de sécurité réseau)
		• Adresses IP publiques des pare-feu VM-Series

©2023 Palo Alto Networks, Inc.

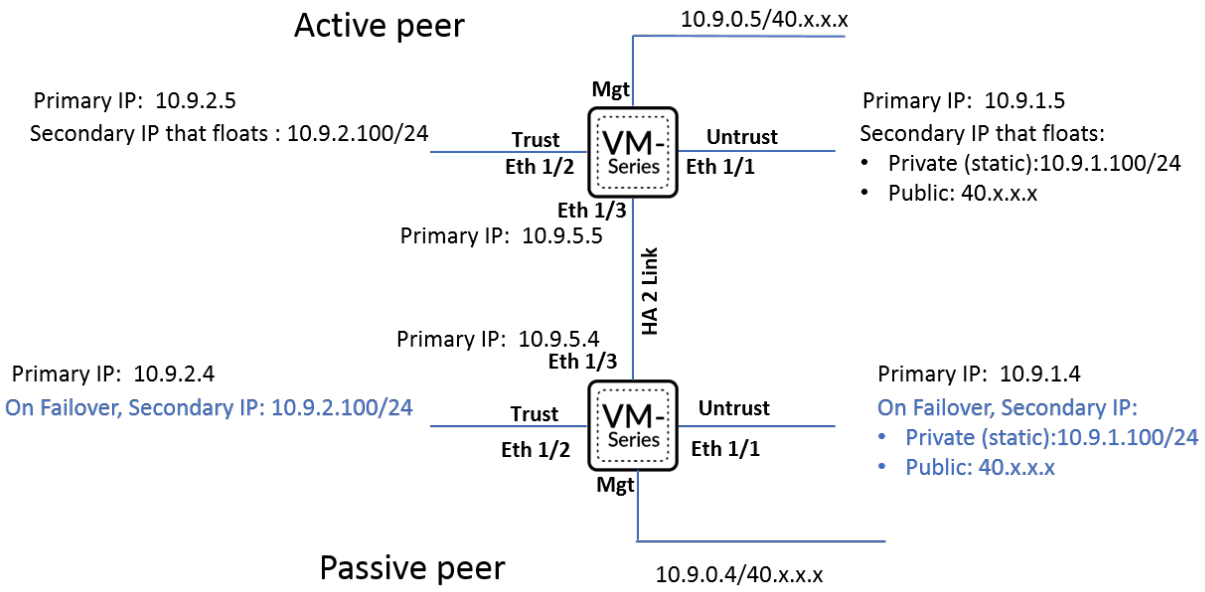
Type de HA Azure	Permissions	Portée du rôle
UDR HA	`"Microsift.Authorization/*/read""Microsift.Compute/virtualMachines/read""Microsift.Network/routeTables/*""Microsift.Network/networkInterfaces/*"`	• Deux pare-feu VM-Series • NIC des deux pare-feu VM-Series • Tables de routage associées à UDR

Déplacement IP secondaire et UDR	`"Microsift.Authorization/*/read""Microsift.Compute/virtualMachines/read""Microsift.Network/networkInterfaces/*""Microsift.Network/networkSecurityGroups/*""Microsift.Network/routeTables/*""Microsift.Network/virtualNetworks/join/action""Microsift.Network/virtualNetworks/subnets/join/action"`
	Les autorisations suivantes ne sont requises que si vous avez attribué une adresse IP publique à l'une de vos interfaces de données. L'interface SKU standard est recommandée.
	`"Microsift.Network/publicIPAddresses/join/action""Microsift.Network/publicIPAddresses/read""Microsift.Network/publicIPAddresses/write"`
		• Réseau virtuel dans lequel les VM sont déployées
		• Deux pare-feu VM-Series
		• NIC des deux pare-feu VM-Series
		• Network Security Group (Groupe de sécurité réseau)
		• Adresses IP publiques des pare-feu VM-Series
		• Tables de routage associées à UDR

Configurer une HA active/passive sur Azure (trafic Nord-Sud et Est-Ouest)

Si vous souhaitez sécuriser le trafic Nord-Sud vers vos applications dans votre infrastructure Azure, utilisez ce flux de travail avec des adresses IP flottantes capables de passer rapidement d'un homologue à l'autre. Dans la mesure où vous ne pouvez pas déplacer l'adresse IP associée à l'interface principale du pare-feu sur Azure, vous devez attribuer une adresse IP secondaire pouvant fonctionner en tant qu'adresse IP flottante. Lorsque le pare-feu actif tombe en panne, l'adresse IP flottante passe du pare-feu actif au pare-feu passif pour permettre au pare-feu passif de sécuriser de manière transparente le trafic dès qu'il devient l'homologue actif. En plus de l'adresse IP flottante, les homologues HA ont également besoin de liaisons HA, à savoir une liaison de contrôle (HA1) et une liaison de données (HA2), pour synchroniser les données et gérer les informations sur l'état.

©2023 Palo Alto Networks, Inc.



- Configurez le pare-feu pour activer la HA
- Configurez la HA active/passive sur le pare-feu VM-Series sur Azure

Configurez le pare-feu pour activer la HA

Rassemblez les détails suivants pour configurer la HA sur les pare-feu VM-Series sur Azure.

- Configurez l'application Active Directory et un directeur de service pour activer l'accès API programmatique.
  - Pour que le pare-feu puisse interagir avec les API Azure, vous devez créer un directeur de service Azure Active Directory. Ce directeur de service dispose des autorisations requises pour s'authentifier auprès d'Azure AD et accéder aux ressources de votre abonnement. Pour terminer cette configuration, vous devez disposer des autorisations nécessaires pour enregistrer une application auprès de votre locataire Azure AD et lui attribuer un rôle dans votre abonnement. Si vous ne disposez pas des permissions nécessaires, demandez à votre administrateur Azure AD ou celui de votre abonnement de créer un « Service Principal ». Consultez le tableau ci-dessus pour les autorisations requises. Copiez les détails suivants pour une utilisation ultérieure dans ce flux de travail :
    - **Client ID** (ID du client) : l'ID de l'application associée à Active Directory (sur le portail Azure, cliquez sur **Home (Accueil)** > **Azure Active Directory** > **App registrations (Enregistrements d'applications)**, sélectionnez votre application et copiez l'ID).
    - **Tenant ID** (ID de locataire) : l'ID de répertoire associé à l'Active Directory (sur le portail Azure, cliquez sur **Home [Accueil]** > **Azure Active Directory** > **Properties [Propriétés]** > **Directory ID [ID du répertoire]**, sélectionnez l'application et copiez l'ID).

 ©2023 Palo Alto Networks, Inc.

- **Azure Subscription ID** (ID d'abonnement Azure) : l'abonnement Azure dans lequel vous avez déployé les pare-feu. Vous devez vous connecter à votre portail Azure pour obtenir cet ID d'abonnement.
- **Resource Group Name** (Nom du groupe de ressources) : le nom du groupe de ressources dans lequel vous avez déployé les pare-feu que vous souhaitez configurer en tant qu'homologues HA. Les deux pare-feu doivent appartenir au même groupe de ressources.
- **Clé secrète** : la clé d'authentification associée à l'application Active Directory (sur le portail Azure, cliquez sur **Home (Accueil)** > **Azure Active Directory** > **Certificates & secrets (Certificats et secrets)**, copiez la **Value (Valeur)** dans **Client secrets (Secrets client)**. Si vous n'avez pas de clé secrète, créez-en d'abord une, puis copiez la valeur). Pour vous connecter en tant qu'application, vous devez fournir la valeur de clé et l'ID d'application.

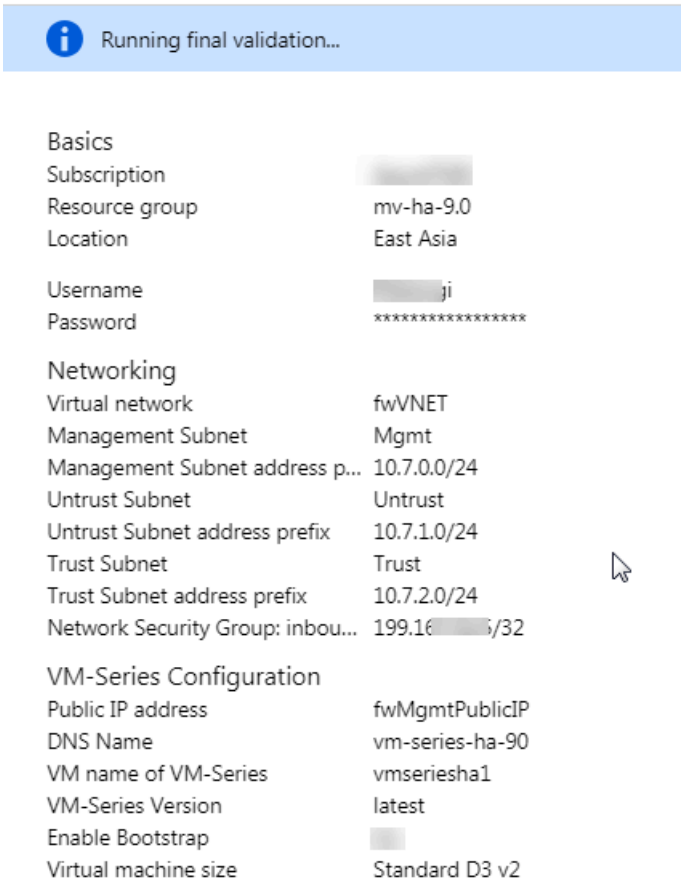
- Sachez où trouver les modèles dont vous avez besoin pour déployer les pare-feu VM-Series au sein du même groupe de ressources Azure.

  Pour une configuration HA, les deux homologues HA doivent appartenir au même groupe de ressources Azure. Si vous déployez la première instance du pare-feu à partir d'Azure Marketplace, vous devez utiliser votre modèle ARM personnalisé ou l'exemple de modèle GitHub de Palo Alto Networks pour le déploiement de la seconde instance du pare-feu dans le groupe de ressources existant. Si vous avez besoin d'un modèle personnalisé ou de l'exemple de modèle de Palo Alto

 ©2023 Palo Alto Networks, Inc.

Networks, Azure ne prend pas en charge la possibilité de déployer le pare-feu dans un groupe de ressources non vide.

Copiez les informations sur le déploiement pour la première instance de pare-feu. Par exemple :



- Faites correspondre le **VM Name of VM-Series** (Nom de VM du pare-feu VM-Series) comme indiqué dans la capture d'écran ci-dessus avec le **Hostname** (Nom d'hôte) sur l'interface Web du pare-feu. Vous devez ajouter le même nom sur **Device (Appareil)** > **Setup (Configuration)** > **Management (Gestion)**, car le nom d'hôte du pare-feu est utilisé pour déclencher un basculement.

- Planifiez la configuration de l'interface réseau sur les pare-feu VM-Series sur Azure.

  Pour configurer la HA, vous devez déployer les deux homologues HA dans le même groupe de ressources Azure et les deux pare-feu doivent avoir le même nombre d'interfaces réseau. Un minimum de quatre interfaces réseau est requis sur chaque homologue HA :

  - **Interface de gestion (eth0)** : adresse IP privée et publique associée à l'interface principale. L'adresse IP publique permet d'accéder à l'interface Web du pare-feu et à l'accès SSH.

    Vous pouvez utiliser l'interface d'adresse IP privée sur l'interface de gestion comme l'adresse IP de l'homologue HA1 pour la communication par liaison de contrôle entre homologues HA actif/passif. Si vous souhaitez une interface HA1 dédiée, vous devez associer une interface

 ©2023 Palo Alto Networks, Inc.

réseau supplémentaire à chaque pare-feu, ce qui signifie que vous avez besoin de cinq interfaces sur chaque pare-feu.

- **Interface non approuvée (eth1/1)** : adresse IP privée principale avec /32 masques réseau et une configuration de l'adresse IP secondaire avec une adresse IP privée (tout masque réseau) et une adresse IP publique.

  En cas de basculement, lorsque l'homologue passif passe à l'état actif, l'adresse IP publique associée à la configuration de l'adresse IP secondaire est détachée de l'homologue précédemment actif et rattachée à l'homologue HA désormais actif.
- **Interface approuvée (eth1/2)** : adresses IP privées principale et secondaire. En cas de basculement, lorsque l'homologue passif passe à l'état actif, l'adresse IP privée secondaire est détachée de l'homologue précédemment actif et rattachée à l'homologue HA désormais actif.
- **HA2 (eth 1/3)** : adresse IP privée principale. L'interface HA2 est la liaison de données utilisée par les homologues HA pour la synchronisation de sessions, les tables de transfert, les associations de sécurité IPSec et les tables ARP.

Interface	Homologue de pare-feu actif	Homologue de pare-feu passif	Description
Approuvée	Adresse IP secondaire	—	L'interface approuvée de l'homologue actif nécessite une configuration de l'adresse IP secondaire pouvant flotter vers l'autre homologue en cas de basculement. Cette configuration de l'adresse IP secondaire sur l'interface approuvée doit être une adresse IP privée avec le masque réseau des serveurs qu'il sécurise. En cas de basculement, le plug-in VM-Series appelle l'API Azure pour détacher cette adresse IP privée secondaire de l'homologue actif et la rattacher à l'homologue passif. Le rattachement de cette adresse IP à l'homologue désormais actif garantit que le pare-feu peut recevoir le trafic sur l'adresse IP flottante de l'interface non approuvée et l'envoyer à l'adresse IP flottante de l'interface approuvée et aux charges de travail.
Non approuvée	Adresse IP secondaire	—	L'interface non approuvée du pare-feu nécessite une configuration de l'adresse IP secondaire comprenant une adresse IP privée statique avec un masque réseau pour le sous-réseau non approuvé et une adresse IP publique pour accéder aux serveurs principaux ou aux charges de travail via Internet. En cas de basculement, le plug-in VM-Series appelle l'API Azure pour détacher la configuration de l'adresse IP secondaire de l'homologue actif et la rattacher à l'homologue passif avant qu'il passe à l'état actif. Ce processus de flottement de la configuration de l'adresse IP

 ©2023 Palo Alto Networks, Inc.

Interface	Homologue de pare-feu actif	Homologue de pare-feu passif	Description
			secondaire permet au pare-feu désormais actif de continuer à traiter le trafic entrant destiné aux charges de travail.
HA2	Ajoutez une NIC au pare-feu à partir de la console de gestion Azure.	Ajoutez une NIC au pare-feu à partir de la console de gestion Azure.	Sur les homologues actif et passif, ajoutez une liaison HA2 dédiée pour activer la synchronisation de session. L'interface par défaut pour HA1 est l'interface de gestion et vous pouvez choisir d'utiliser l'interface de gestion au lieu d'ajouter une interface supplémentaire au pare-feu. Pour activer le flux de données sur la liaison HA2, vous devez ajouter une interface réseau supplémentaire sur le portail Azure et configurer l'interface pour HA2 sur le pare-feu.

Configurez la HA active/passive sur le pare-feu VM-Series sur Azure

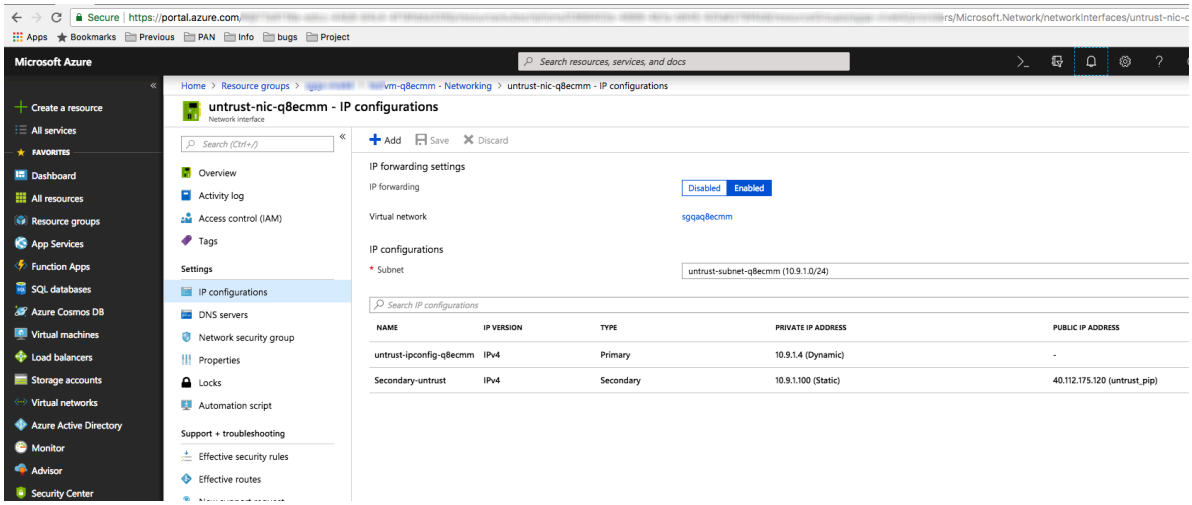
Dans ce flux de travail, vous déployez la première instance du pare-feu VM-Series à l'aide du modèle de solution de pare-feu VM-Series de l'Azure Marketplace et la seconde instance du pare-feu à l'aide de l'exemple de modèle GitHub.

La clé d'authentification (secret du client) associée à l'application Active Directory requise pour la configuration du pare-feu VM-Series dans une configuration HA est chiffrée avec le plug-in VM-Series version 1.0.4 sur le pare-feu et sur Panorama. La clé étant chiffrée dans le plug-in VM-Series version 1.0.4, vous devez installer la même version du plug-in sur Panorama et les pare-feu VM-Series gérés afin de gérer de manière centralisée les pare-feu à partir de Panorama.

©2023 Palo Alto Networks, Inc.

STEP 1 | Déployez le pare-feu VM-Series à l'aide d'un modèle de solution et configurez les interfaces réseau pour la HA.

1. Ajoutez une configuration d'adresse IP secondaire à l'interface non approuvée du pare-feu.



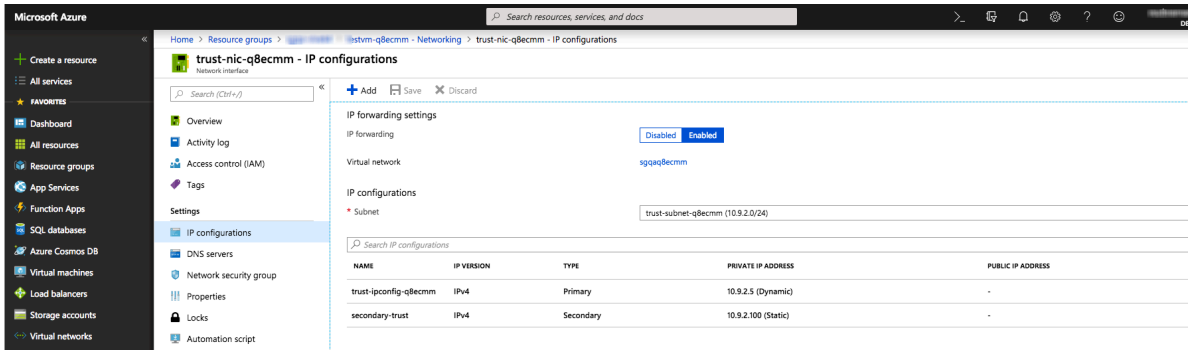
Vous devez associer la configuration d'adresse IP secondaire, avec une adresse IP privée (tout masque réseau) et une adresse IP publique, au pare-feu qui sera désigné comme homologue actif. La configuration d'adresse IP secondaire reste toujours avec l'homologue HA actif et passe d'un homologue à l'autre lorsqu'un basculement a lieu.

Dans ce flux de travail, ce pare-feu sera désigné comme l'homologue actif. L'homologue HA actif a une valeur numérique inférieure pour la priorité de l'appareil que vous avez configurée

 ©2023 Palo Alto Networks, Inc.

dans le cadre de la configuration HA sur le pare-feu et cette valeur indique une préférence pour laquelle le pare-feu assume le rôle d'homologue actif.

2. Ajoutez une configuration d'adresse IP secondaire à l'interface approuvée du pare-feu.



La configuration d'adresse IP secondaire de l'interface approuvée requiert uniquement une adresse IP privée statique. Cette adresse IP se déplace du pare-feu actif au pare-feu passif en

 ©2023 Palo Alto Networks, Inc.

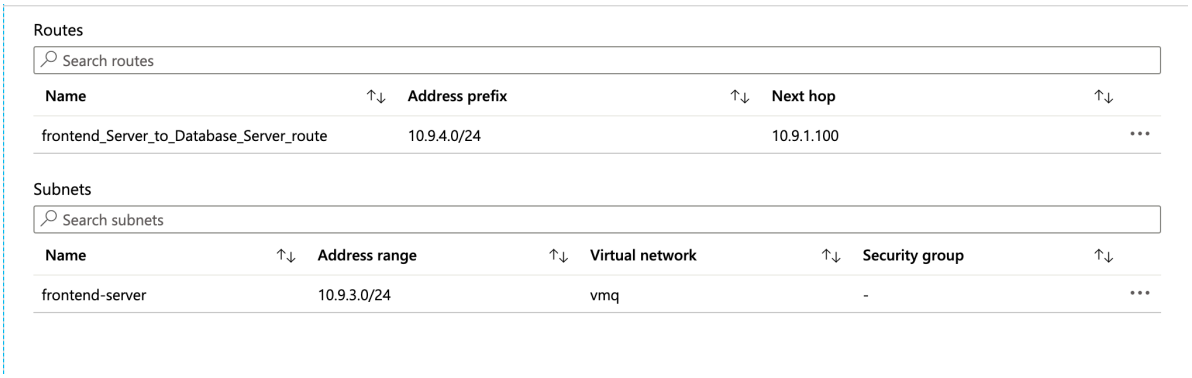
cas de basculement, de sorte que le trafic passe des interfaces non approuvée et approuvée aux sous-réseaux de destination sécurisés par le pare-feu.

3. Associez une interface réseau pour la communication HA2 entre les homologues HA du pare-feu.
   1. Ajoutez un sous-réseau au sein du réseau virtuel.
   2. Procédez à la Création et à l'Association d'une interface réseau au pare-feu.
4. Configurez votre table d'itinéraires sur Azure.

   Votre saut suivant devrait pointer vers l'adresse IP flottante comme indiqué ici :



 ©2023 Palo Alto Networks, Inc.



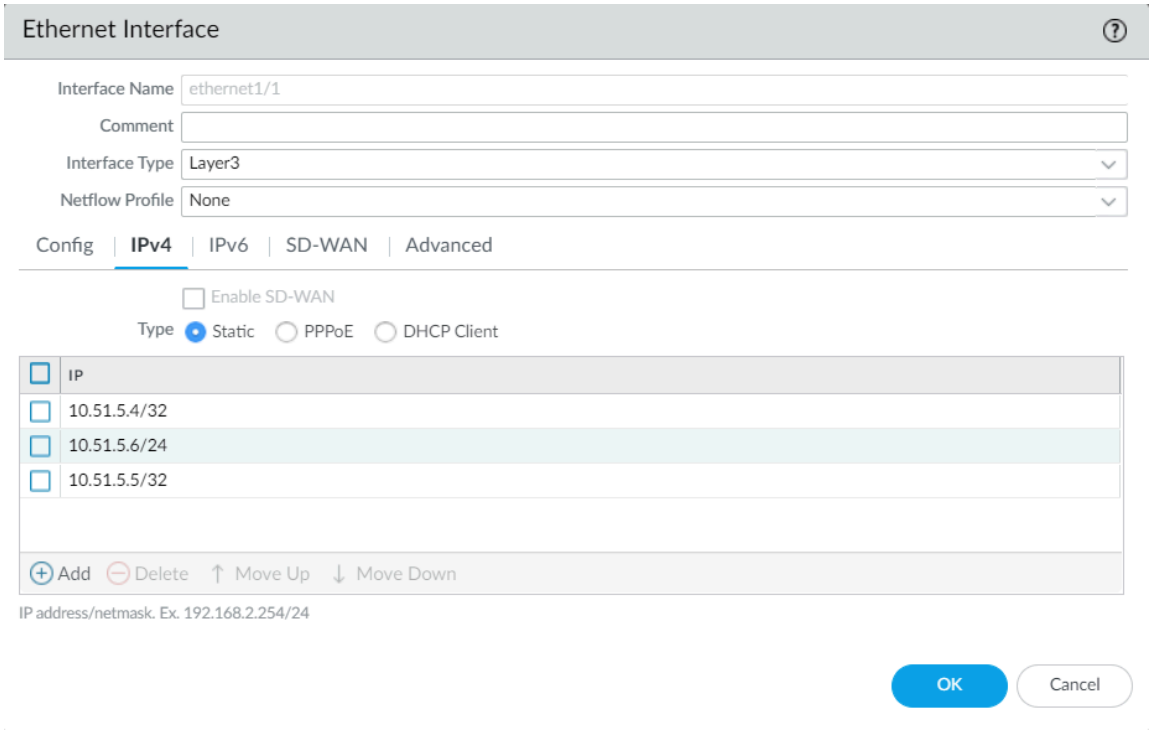
 ©2023 Palo Alto Networks, Inc.

STEP 2 | Configurez les interfaces sur le pare-feu.

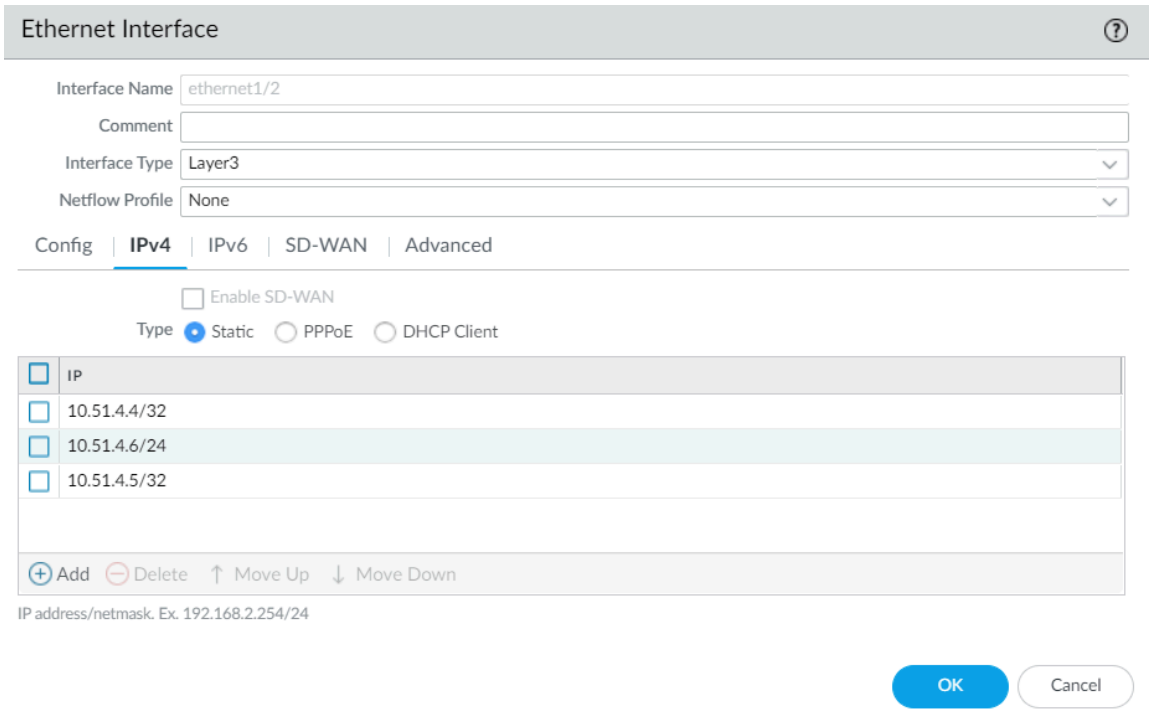
Effectuez ces étapes sur l'homologue HA actif avant de déployer et de configurer l'homologue HA passif.

1. Connectez-vous à l'interface Web du pare-feu.
2. Configurez ethernet 1/1 en tant qu'interface non approuvée (Untrust) et ethernet 1/2 en tant qu'interface approuvée (Trust).

   Sélectionnez **Network (Réseau)** > **Interfaces** et configurez comme suit :



 ©2023 Palo Alto Networks, Inc.



3. Configurez ethernet 1/3 en tant qu'interface HA.

   Pour configurer la liaison HA2, sélectionnez l'interface et définissez l'**Interface Type** (Type d'interface) sur **HA**. Définissez la Link Speed (Vitesse de liaison) et le Link Duplex (Duplex de liaison) sur Auto.



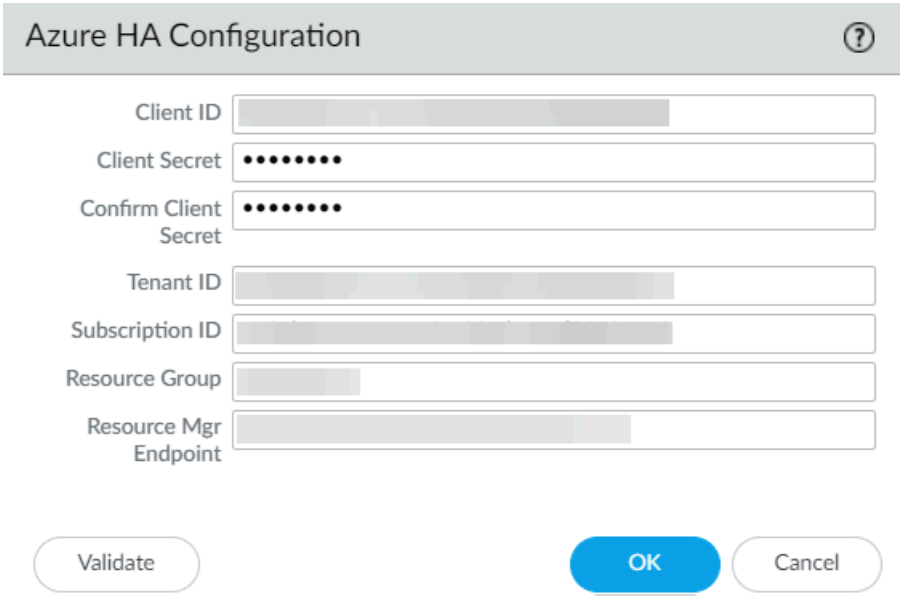
 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configurez le plug-in VM-Series pour vous authentifier auprès du groupe de ressources Azure dans lequel vous avez déployé le pare-feu.

Configurez la configuration HA Azure sur le plug-in VM-Series.

Pour chiffrer le secret du client, utilisez le plug-in VM-Series version 1.0.4 ou ultérieure. Si vous utilisez Panorama pour gérer vos pare-feu, vous devez installer le plug-in VM-Series version 1.0.4 ou ultérieure.

1. Sélectionnez **Device (Périphérique)** > **VM-Series** pour permettre un accès programmatique entre le plug-in de pare-feu et les ressources Azure.



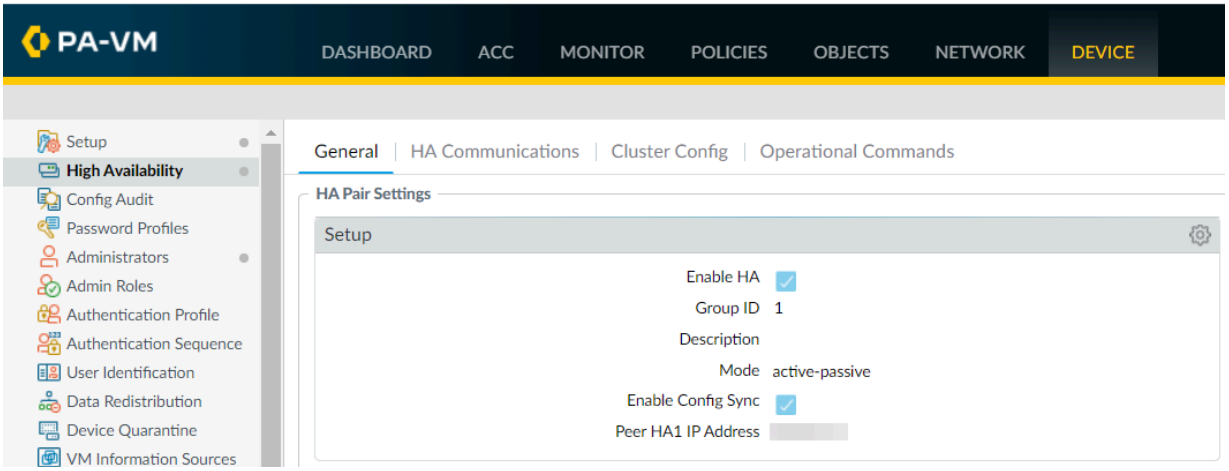
2. Saisissez le **Client ID** (ID de client). L'ID client est l'ID d'application associé à votre application Azure Active Directory.
3. Entrez **Client Secret :** et entrez-la de nouveau pour confirmer.
4. Saisissez le **Tenant ID (ID de locateur)**. Le numéro d'identification du locataire est celui que vous avez sauvegardé lorsque vous avez créé l'application Active Directory.
5. Entrez le **Subcription ID (l'ID d'abonnement pour l'abonnement Azure)** que vous voulez surveiller.
6. Entrez le nom du **groupe de ressources**.
7. (Pour les déploiements Azure Stack uniquement) Entrez l'URL **Resource Mgr Endpoint (Terminal du gestionnaire de ressources)**.

   Ce champ est disponible dans le plugin VM-Series 2.1.2 et versions ultérieures.

8. Cliquez sur **Validate** (Valider) pour vérifier que les clés et les ID que vous avez saisis sont valides et que le plug-in VM-Series peut communiquer avec succès avec les ressources Azure au moyen de l'API.

©2023 Palo Alto Networks, Inc.

STEP 4 | Activez HA.



1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **HA**.
2. Saisissez la **Peer HA1 IP address** (Adresse IP de l'homologue HA1) comme l'adresse IP privée de l'homologue passif.
3. (Facultatif) Modifiez la liaison de contrôle (HA1). Si vous ne prévoyez pas d'utiliser l'interface de gestion pour la liaison de contrôle et que vous avez ajouté une interface supplémentaire (par exemple, ethernet 1/4), modifiez cette section pour sélectionner l'interface à utiliser pour la communication HA1.
4. Modifiez la Data Link (Liaison de données) (HA2) pour utiliser le **Port** ethernet 1/3 et ajoutez l'adresse IP de cet homologue et l'adresse IP de la **Gateway** (Passerelle) du sous-réseau.

STEP 5 | **Commit (Validez)** les modifications.

STEP 6 | Configurez l'homologue HA passif au sein du même groupe de ressources Azure.

1. Déployez la seconde instance du pare-feu.
   - Téléchargez le modèle personnalisé et le fichier de paramètres à partir de GitHub.
   - Connectez-vous au portail Azure.
   - Recherchez un **custom template** (modèle personnalisé) et sélectionnez **Deploy from a custom template** (Déployer à partir d'un modèle personnalisé).
   - Sélectionnez **Build your own template in the editor (Créer votre propre modèle dans l'éditeur)** > **Load file (Charger un fichier)**.
   - Sélectionnez le fichier **azuredeploy.json** que vous avez téléchargé précédemment et cliquez sur **Save** (Enregistrer).
   - Renseignez les champs, acceptez les conditions et cliquez sur **Purchase** (Acheter).

     Assurez-vous que les entrées suivantes correspondent à celles de l'instance de pare-feu que vous avez déjà déployée : abonnement Azure, nom du Resource Group (Groupe de ressources), emplacement du Resource Group (Groupe de ressources), nom du VNet

 ©2023 Palo Alto Networks, Inc.

existant dans lequel vous souhaitez déployer le pare-feu, VNet CIDR (CIDR de VNet), noms de Subnet (Sous-réseau), Subnet CIDR (CIDR de sous-réseau) et IP Address (Adresse IP) de démarrage pour les sous-réseaux de gestion, approuvé et non approuvé.

2. Répétez l'Étape 1 et l'Étape 2 pour configurer les interfaces et le pare-feu en tant qu'homologue HA passif.
3. Ignorez l'Étape 3 et procédez à l'Activation HA (Étape 5). Dans l'Étape 4, modifiez les adresses IP en fonction de cet homologue HA passif.

STEP 7 | Une fois les deux pare-feu configurés, vérifiez qu'ils sont appariés en mode HA active/passive.

1. Accédez au **Dashboard (Tableau de bord)** sur les deux pare-feu et affichez le widget High Availability (Haute disponibilité).
2. Sur le pare-feu actif, cliquez sur le lien **Sync to peer** (Synchroniser avec l'homologue).
3. Vérifiez que les pare-feu sont appariés et synchronisés comme indiqué ci-dessous :
   - Sur le pare-feu passif : l'état du pare-feu local doit afficher **passive** (passif) et la **Running Config** (Configuration en cours) doit être **synchronized** (synchronisée).
   - Sur le pare-feu actif : l'état du pare-feu local doit afficher **active** (actif) et la **Running Config** (Configuration en cours) doit être **synchronized** (synchronisée).
4. Sur l'homologue passif, vérifiez que la configuration du plug-in VM-Series est maintenant synchronisée.

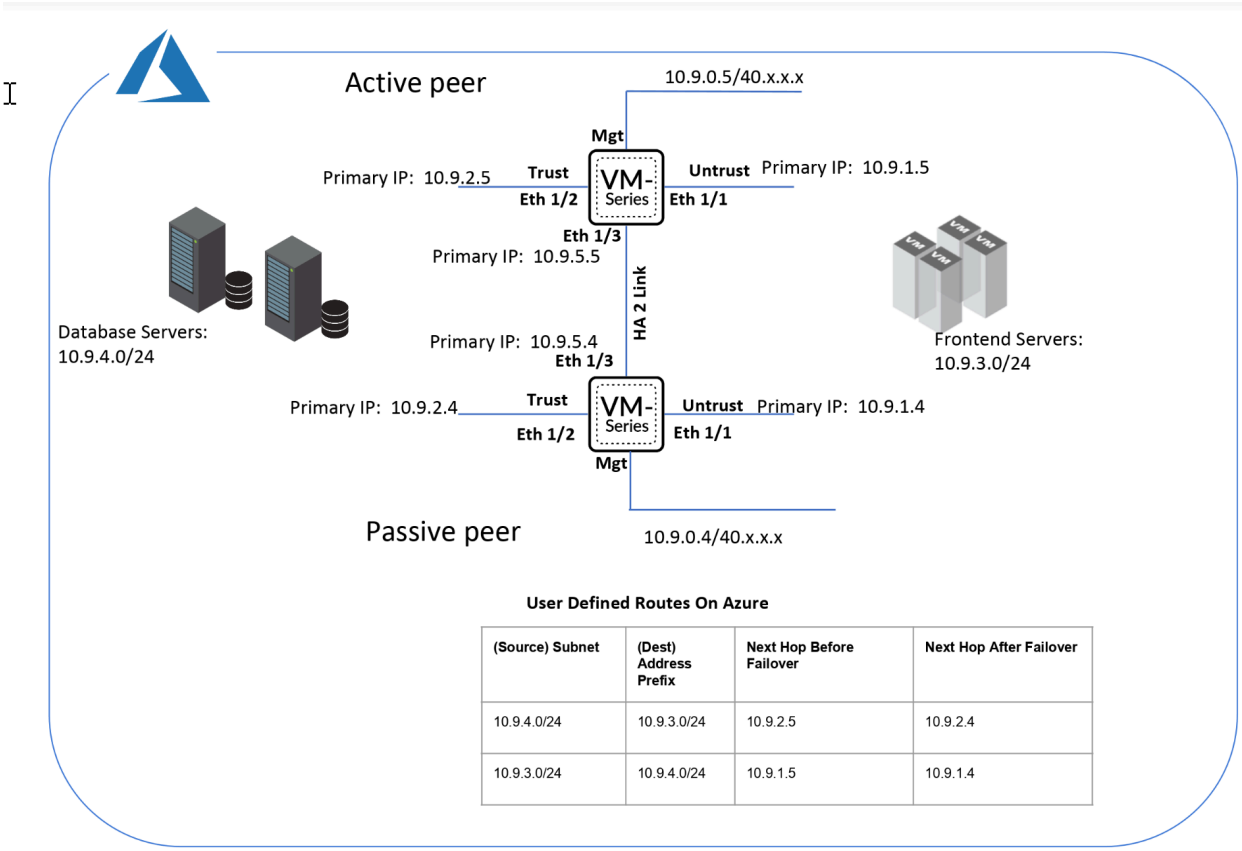
   Sélectionnez **Device (Appareil)** > **VM-Series** et vérifiez que vous pouvez afficher la configuration HA Azure que vous avez omis de configurer sur l'homologue passif.

Configurer une HA active/passive sur Azure (trafic Est-Ouest uniquement)

Si vos ressources sont toutes déployées dans l'infrastructure Azure et si vous n'avez pas besoin d'appliquer la sécurité pour le trafic nord-sud vers le VNet Azure, vous pouvez déployer une paire de pare-feu VM-Series en configuration haute disponibilité (HA) active/passive sans adresses IP flottantes. Les homologues HA auront toujours besoin de liaisons HA, à savoir une liaison de contrôle (HA1) et une liaison de données (HA2), pour synchroniser les données et gérer les informations sur l'état.

Vous devez disposer du Plug-in VM-Series version 1.0.9 ou ultérieure et vous devez déployer les deux homologues HA de pare-feu au sein du même groupe de ressources Azure.

 ©2023 Palo Alto Networks, Inc.



User Defined Routes On Azure

(Source) Subnet	(Dest) Address Prefix	Next Hop Before Failover	Next Hop After Failover
10.9.4.0/24	10.9.3.0/24	10.9.2.5	10.9.2.4
10.9.3.0/24	10.9.4.0/24	10.9.1.5	10.9.1.4

- Configurez le pare-feu pour activer la HA
- Configurez la HA active/passive sur le pare-feu VM-Series sur Azure

Configurez le pare-feu pour activer la HA

Rassemblez les détails suivants pour configurer la HA sur les pare-feu VM-Series sur Azure.

1. Configurez l'application Active Directory et un directeur de service pour activer l'accès API programmatique.
   - Pour que le pare-feu puisse interagir avec les API Azure, vous devez créer un directeur de service Azure Active Directory. Ce directeur de service dispose des autorisations requises pour s'authentifier auprès d'Azure AD et accéder aux ressources de votre abonnement. Pour terminer cette configuration, vous devez disposer des autorisations nécessaires pour enregistrer une application auprès de votre locataire Azure AD et lui attribuer un rôle dans votre abonnement. Si vous ne disposez pas des permissions nécessaires, demandez à votre administrateur Azure AD ou celui de votre abonnement de créer un « Service Principal ».

 ©2023 Palo Alto Networks, Inc.

Consultez le tableau ci-dessus pour les autorisations requises. Copiez les détails suivants pour une utilisation ultérieure dans ce flux de travail :

- **Client ID** (ID du client) : l'ID de l'application associée à Active Directory (sur le portail Azure, cliquez sur **Home (Accueil)** > **Azure Active Directory** > **App registrations (Enregistrements d'applications)**, sélectionnez votre application et copiez l'ID).
- **Tenant ID** (ID de locataire) : l'ID de répertoire associé à l'Active Directory (sur le portail Azure, cliquez sur **Home [Accueil]** > **Azure Active Directory** > **Properties [Propriétés]** > **Directory ID [ID du répertoire]**, sélectionnez l'application et copiez l'ID).
- **Azure Subscription ID** (ID d'abonnement Azure) : l'abonnement Azure dans lequel vous avez déployé les pare-feu. Vous devez vous connecter à votre portail Azure pour obtenir cet ID d'abonnement.
- **Resource Group Name** (Nom du groupe de ressources) : le nom du groupe de ressources dans lequel vous avez déployé les pare-feu que vous souhaitez configurer en tant qu'homologues HA. Les deux pare-feu doivent appartenir au même groupe de ressources.
- **Clé secrète** : la clé d'authentification associée à l'application Active Directory (sur le portail Azure, cliquez sur **Home (Accueil)** > **Azure Active Directory** > **Certificates & secrets (Certificats et secrets)**, copiez la **Value (Valeur)** dans **Client secrets (Secrets client)**. Si vous n'avez pas de clé secrète, créez-en d'abord une, puis copiez la valeur). Pour vous connecter en tant qu'application, vous devez fournir la valeur de clé et l'ID d'application.

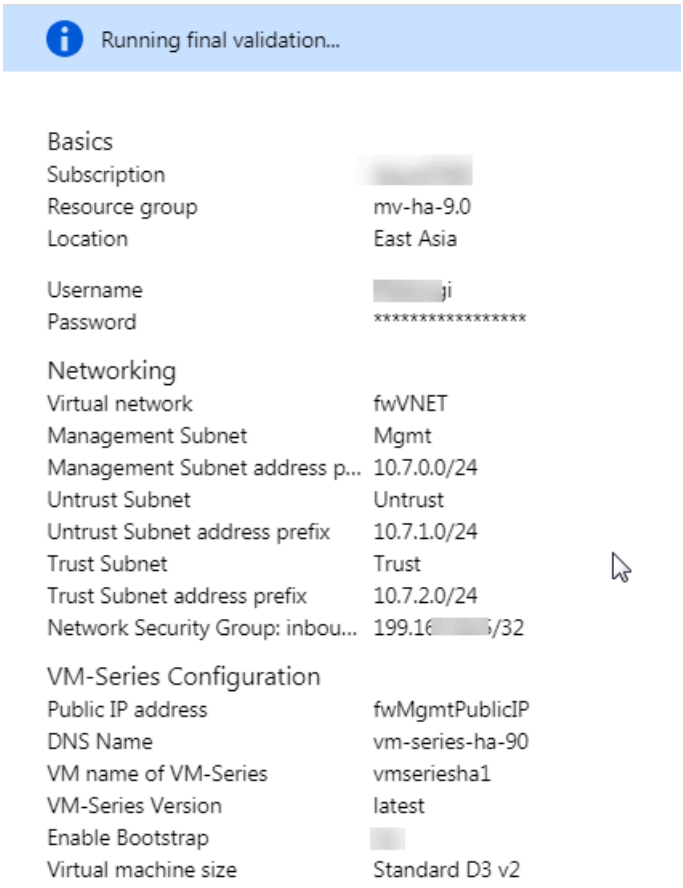
- Sachez où trouver les modèles dont vous avez besoin pour déployer les pare-feu VM-Series au sein du même groupe de ressources Azure.

  Pour une configuration HA, les deux homologues HA doivent appartenir au même groupe de ressources Azure. Si vous déployez la première instance du pare-feu à partir d'Azure Marketplace, vous devez utiliser votre modèle ARM personnalisé ou l'exemple de modèle GitHub de Palo Alto Networks pour le déploiement de la seconde instance du pare-feu dans le groupe de ressources existant. Si vous avez besoin d'un modèle personnalisé ou de l'exemple de modèle de Palo Alto

 ©2023 Palo Alto Networks, Inc.

Networks, Azure ne prend pas en charge la possibilité de déployer le pare-feu dans un groupe de ressources non vide.

Copiez les informations sur le déploiement pour la première instance de pare-feu. Par exemple :



- Faites correspondre le **VM Name of VM-Series** (Nom de VM du pare-feu VM-Series) comme indiqué dans la capture d'écran ci-dessus avec le **Hostname** (Nom d'hôte) sur l'interface Web du pare-feu. Vous devez ajouter le même nom sur **Device (Appareil)** > **Setup (Configuration)** > **Management (Gestion)**, car le nom d'hôte du pare-feu est utilisé pour déclencher un basculement.

- Planifiez la configuration de l'interface réseau sur les pare-feu VM-Series sur Azure.

  Pour configurer la HA, vous devez déployer les deux homologues HA dans le même groupe de ressources Azure et les deux pare-feu doivent avoir le même nombre d'interfaces réseau. Un minimum de quatre interfaces réseau est requis sur chaque homologue HA :

  - **Interface de gestion (eth0)** : adresse IP privée et publique associée à l'interface principale. L'adresse IP publique permet d'accéder à l'interface Web du pare-feu et à l'accès SSH.

    Vous pouvez utiliser l'interface d'adresse IP privée sur l'interface de gestion comme l'adresse IP de l'homologue HA1 pour la communication par liaison de contrôle entre homologues HA actif/passif. Si vous souhaitez une interface HA1 dédiée, vous devez associer une interface

 ©2023 Palo Alto Networks, Inc.

réseau supplémentaire à chaque pare-feu, ce qui signifie que vous avez besoin de cinq interfaces sur chaque pare-feu.

- **Interface non approuvée (Untrust - eth1/1)** : adresse IP privée principale avec masque réseau /32.

  Lors du basculement, lorsque l'homologue passive passe à l'état actif, le plug-in VM-Series envoie automatiquement le trafic vers l'adresse IP privée principale sur l'homologue passif. Les UDR Azure permettent le flux de trafic.
- **Interface approuvée (Trust - eth1/2)** : adresse IP privée principale. Lors du basculement, lorsque l'homologue passive passe à l'état actif, le plug-in VM-Series envoie automatiquement le trafic vers l'adresse IP privée principale sur l'homologue passif.
- **HA2 (eth 1/3)** : adresse IP privée principale. L'interface HA2 est la liaison de données utilisée par les homologues HA pour la synchronisation de sessions, les tables de transfert, les associations de sécurité IPSec et les tables ARP.

Interface	Homologue de pare-feu actif	Homologue de pare-feu passif	Description
HA2	Ajoutez une NIC au pare-feu à partir de la console de gestion Azure.	Ajoutez une NIC au pare-feu à partir de la console de gestion Azure.	Sur les homologues actif et passif, ajoutez une liaison HA2 dédiée pour activer la synchronisation de session. L'interface par défaut pour HA1 est l'interface de gestion et vous pouvez choisir d'utiliser l'interface de gestion au lieu d'ajouter une interface supplémentaire au pare-feu. Pour activer le flux de données sur la liaison HA2, vous devez ajouter une interface réseau supplémentaire sur le portail Azure et configurer l'interface pour HA2 sur le pare-feu.

Configurez la HA active/passive sur le pare-feu VM-Series sur Azure

Dans ce flux de travail, vous déployez la première instance du pare-feu VM-Series à l'aide du modèle de solution de pare-feu VM-Series de l'Azure Marketplace et la seconde instance du pare-feu à l'aide de l'exemple de modèle GitHub.

©2023 Palo Alto Networks, Inc.

La clé d'authentification (secret du client) associée à l'application Active Directory requise pour la configuration du pare-feu VM-Series dans une configuration HA est chiffrée avec le plug-in VM-Series version 1.0.9 sur le pare-feu et sur Panorama. La clé étant chiffrée dans le plug-in VM-Series version 1.0.9, vous devez installer la même version du plug-in sur Panorama et les pare-feu VM-Series gérés afin de gérer de manière centralisée les pare-feu à partir de Panorama.

STEP 1 | Déployez le pare-feu VM-Series à l'aide d'un modèle de solution et configurez les interfaces réseau pour la HA.

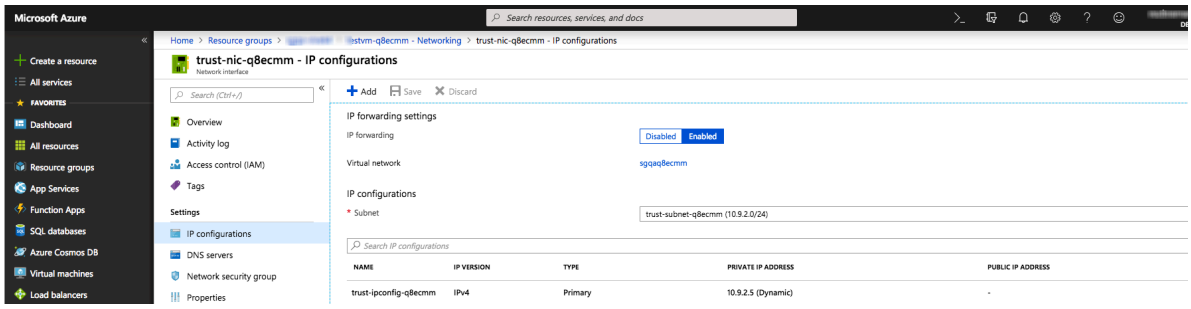
Pour sécuriser le trafic est-ouest dans un VNet Azure, vous n'avez besoin que d'une adresse IP principale pour les interfaces de pare-feu approuvées (Trust) et non approuvées (Untrust). Lorsqu'un basculement se produit, l'UDR change et la route pointe vers l'adresse IP principale de l'homologue qui passe à l'état actif.

1. Ajoutez une configuration IP principale à l'interface approuvée (Trust) de l'homologue de pare-feu actif.

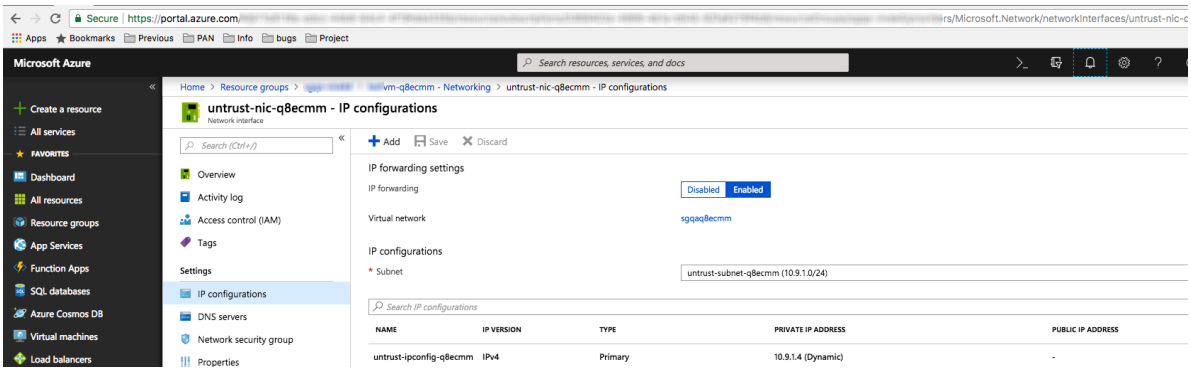
   Dans ce flux de travail, ce pare-feu sera désigné comme l'homologue actif. L'homologue HA actif a une valeur numérique inférieure pour la priorité du périphérique que vous avez

 ©2023 Palo Alto Networks, Inc.

configurée dans le cadre de la configuration HA sur le pare-feu et cette valeur indique une préférence pour laquelle le pare-feu assume le rôle d'homologue actif.



2. Ajoutez une configuration d'adresse IP principale à l'interface non approuvée (Untrust) de l'homologue du pare-feu actif.

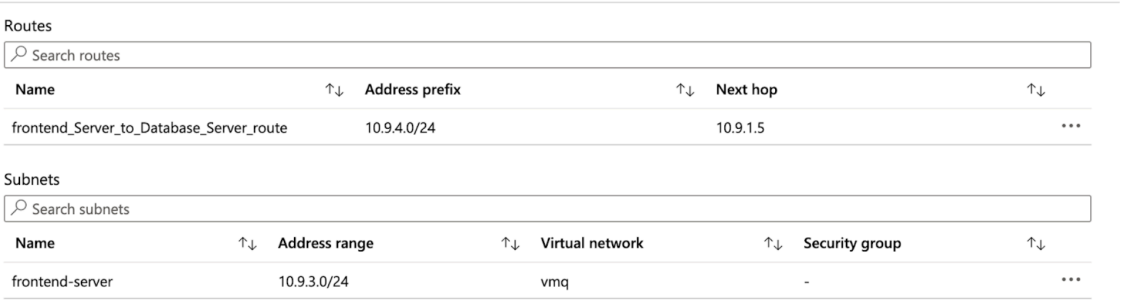


 ©2023 Palo Alto Networks, Inc.

3. Associez une interface réseau pour la communication HA2 entre les homologues HA du pare-feu.
   1. Ajoutez un sous-réseau au sein du réseau virtuel.
   2. Créez et associez une interface réseau au pare-feu.
4. Configurez votre table de routage sur Azure.

   Créez une route vers le prochain saut de l'adresse IP principale des interfaces approuvées (Trust) et non approuvées (Untrust) de l'homologue du pare-feu actif.

Example with Frontend Server to Database Server Route :



Example with Database Server to Frontend Server route:



Après le basculement, le prochain saut pour la route du serveur de base de données vers le serveur frontal passera de 10.9.2.5 à 10.9.2.4. De même, le prochain saut pour la route du serveur de frontal vers le serveur de base de données passera de 10.9.1.5 à 10.9.1.4.

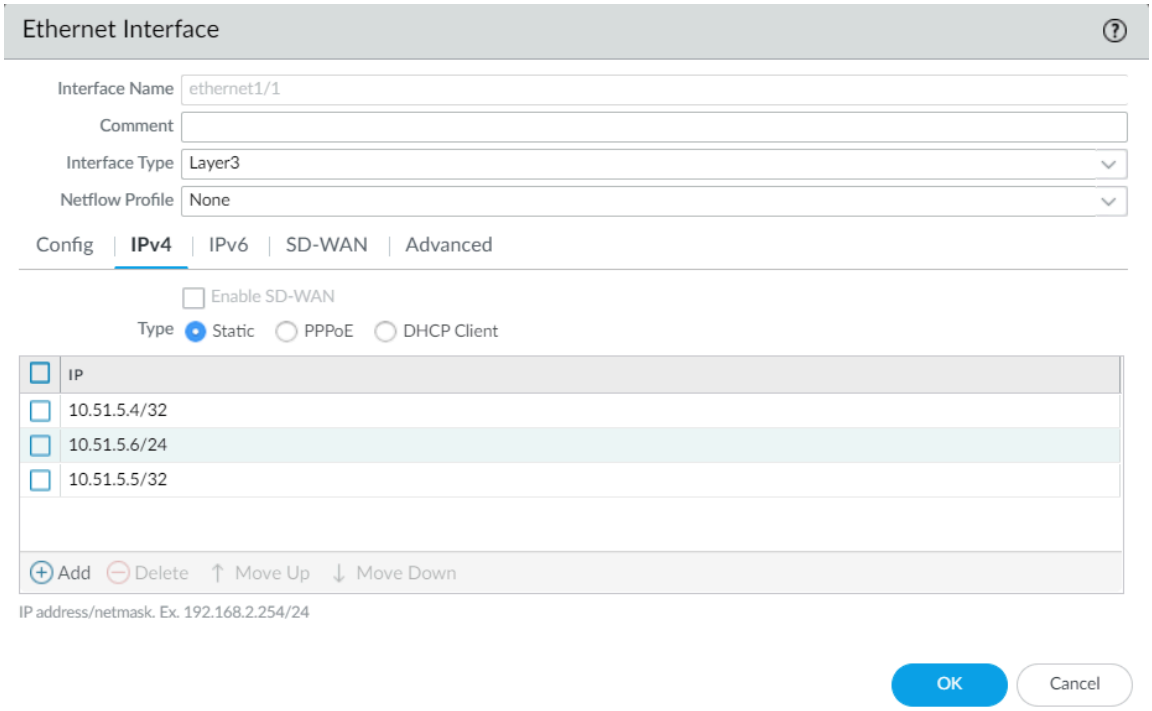
©2023 Palo Alto Networks, Inc.

STEP 2 | Configurez les interfaces sur le pare-feu.

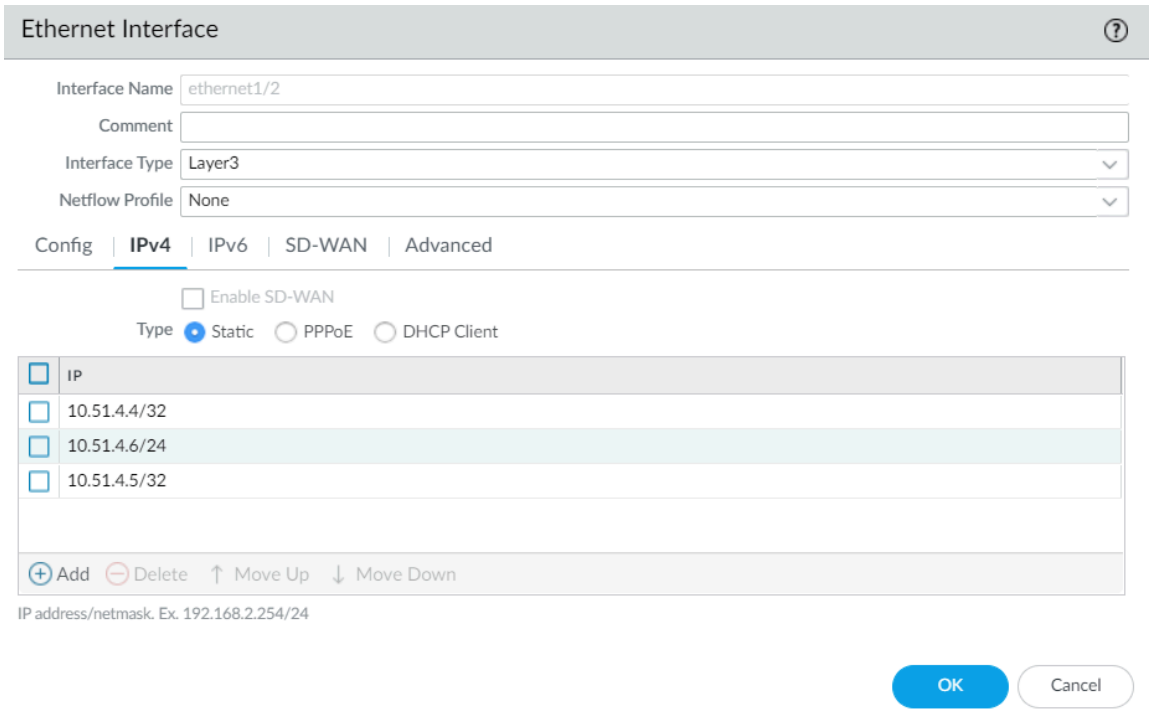
Effectuez ces étapes sur l'homologue HA actif avant de déployer et de configurer l'homologue HA passif.

1. Connectez-vous à l'interface Web du pare-feu.
2. Configurez ethernet 1/1 en tant qu'interface non approuvée et ethernet 1/2 en tant qu'interface non approuvée.

   Sélectionnez **Network (Réseau)** > **Interfaces** et configurez comme suit :



 ©2023 Palo Alto Networks, Inc.



3. Configurez ethernet 1/3 en tant qu'interface HA.

   Pour configurer la liaison HA2, sélectionnez l'interface et définissez l'**Interface Type** (Type d'interface) sur **HA**. Définissez la Link Speed (Vitesse de liaison) et le Link Duplex (Duplex de liaison) sur Auto.



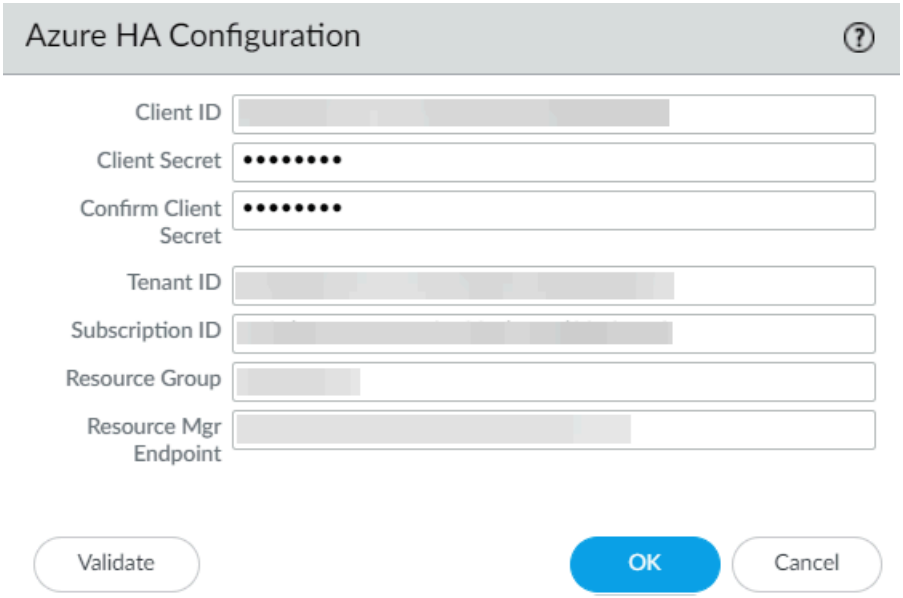
 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configurez le plug-in VM-Series pour vous authentifier auprès du groupe de ressources Azure dans lequel vous avez déployé le pare-feu.

Configurez la configuration HA Azure sur le plug-in VM-Series.

Pour chiffrer le secret du client, utilisez le plug-in VM-Series version 1.0.4 ou ultérieure. Si vous utilisez Panorama pour gérer vos pare-feu, vous devez installer le plug-in VM-Series version 1.0.4 ou ultérieure.

1. Sélectionnez **Device (Périphérique)** > **VM-Series** pour permettre un accès programmatique entre le plug-in de pare-feu et les ressources Azure.



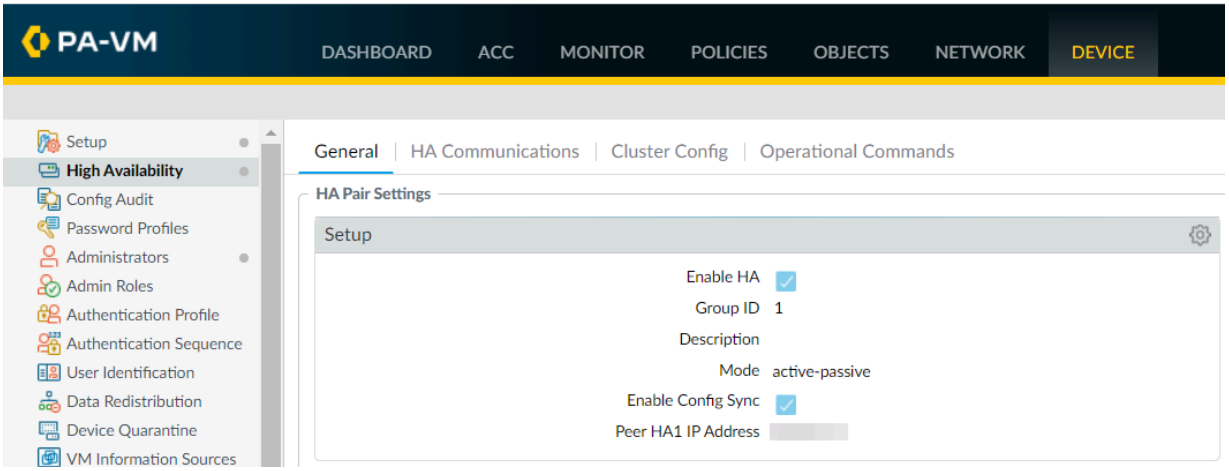
2. Saisissez le **Client ID** (ID de client). L'ID client est l'ID d'application associé à votre application Azure Active Directory.
3. Entrez **Client Secret :** et entrez-la de nouveau pour confirmer.
4. Saisissez le **Tenant ID (ID de locateur)**. Le numéro d'identification du locataire est celui que vous avez sauvegardé lorsque vous avez créé l'application Active Directory.
5. Entrez le **Subcription ID (l'ID d'abonnement pour l'abonnement Azure)** que vous voulez surveiller.
6. Entrez le nom du **groupe de ressources**.
7. (Pour les déploiements Azure Stack uniquement) Entrez l'URL **Resource Mgr Endpoint (Terminal du gestionnaire de ressources)**.

   Ce champ est disponible dans le plugin VM-Series 2.1.2 et versions ultérieures.

8. Cliquez sur **Validate** (Valider) pour vérifier que les clés et les ID que vous avez saisis sont valides et que le plug-in VM-Series peut communiquer avec succès avec les ressources Azure au moyen de l'API.

©2023 Palo Alto Networks, Inc.

STEP 4 | Activez HA.



1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **HA**.
2. Saisissez la **Peer HA1 IP address** (Adresse IP de l'homologue HA1) comme l'adresse IP privée de l'homologue passif.
3. (Facultatif) Modifiez la liaison de contrôle (HA1). Si vous ne prévoyez pas d'utiliser l'interface de gestion pour la liaison de contrôle et que vous avez ajouté une interface supplémentaire (par exemple, ethernet 1/4), modifiez cette section pour sélectionner l'interface à utiliser pour la communication HA1.
4. Modifiez la Data Link (Liaison de données) (HA2) pour utiliser le **Port** ethernet 1/3 et ajoutez l'adresse IP de cet homologue et l'adresse IP de la **Gateway** (Passerelle) du sous-réseau.

STEP 5 | **Commit (Validez)** les modifications.

STEP 6 | Configurez l'homologue HA passif au sein du même groupe de ressources Azure.

1. Déployez la seconde instance du pare-feu.
   - Téléchargez le modèle personnalisé et le fichier de paramètres à partir de GitHub.
   - Connectez-vous au portail Azure.
   - Recherchez un **custom template** (modèle personnalisé) et sélectionnez **Deploy from a custom template** (Déployer à partir d'un modèle personnalisé).
   - Sélectionnez **Build your own template in the editor (Créer votre propre modèle dans l'éditeur)** > **Load file (Charger un fichier)**.
   - Sélectionnez le fichier **azuredeploy.json** que vous avez téléchargé précédemment et cliquez sur **Save** (Enregistrer).
   - Renseignez les champs, acceptez les conditions et cliquez sur **Purchase** (Acheter).

     Assurez-vous que les entrées suivantes correspondent à celles de l'instance de pare-feu que vous avez déjà déployée : abonnement Azure, nom du Resource Group (Groupe de ressources), emplacement du Resource Group (Groupe de ressources), nom du VNet

 ©2023 Palo Alto Networks, Inc.

existant dans lequel vous souhaitez déployer le pare-feu, VNet CIDR (CIDR de VNet), noms de Subnet (Sous-réseau), Subnet CIDR (CIDR de sous-réseau) et IP Address (Adresse IP) de démarrage pour les sous-réseaux de gestion, approuvé et non approuvé.

2. Répétez l'Étape 1 et l'Étape 2 pour configurer les interfaces et le pare-feu en tant qu'homologue HA passif.
3. Ignorez l'Étape 3 et procédez à l'Activation HA (Étape 5). Dans l'Étape 4, modifiez les adresses IP en fonction de cet homologue HA passif.

STEP 7 | Une fois les deux pare-feu configurés, vérifiez qu'ils sont appariés en mode HA active/passive.

1. Accédez au **Dashboard (Tableau de bord)** sur les deux pare-feu et affichez le widget High Availability (Haute disponibilité).
2. Sur le pare-feu actif, cliquez sur le lien **Sync to peer** (Synchroniser avec l'homologue).
3. Vérifiez que les pare-feu sont appariés et synchronisés comme indiqué ci-dessous :
   - Sur le pare-feu passif : l'état du pare-feu local doit afficher **passive** (passif) et la **Running Config** (Configuration en cours) doit être **synchronized** (synchronisée).
   - Sur le pare-feu actif : l'état du pare-feu local doit afficher **active** (actif) et la **Running Config** (Configuration en cours) doit être **synchronized** (synchronisée).
4. Sur l'homologue passif, vérifiez que la configuration du plug-in VM-Series est maintenant synchronisée.

   Sélectionnez **Device (Appareil)** > **VM-Series** et vérifiez que vous pouvez afficher la configuration HA Azure que vous avez omis de configurer sur l'homologue passif.

 ©2023 Palo Alto Networks, Inc.

Utilisation du modèle ARM pour déployer le pare-feu VM-Series

En plus des déploiements basés sur le Marketplace, Palo Alto Networks fournit un référentiel GitHub qui héberge des exemples de modèles ARM que vous pouvez télécharger et personnaliser selon vos besoins. Les modèles ARM sont des fichiers JSON qui décrivent les ressources requises pour les ressources individuelles comme les interfaces réseau, une machine virtuelle complète, voire une pile d'application entière avec plusieurs machines virtuelles.

Les modèles ARM sont destinés aux utilisateurs avancés, et Palo Alto Networks fournit le modèle ARM dans le cadre de la politique appuyée par la communauté. Pour en savoir plus sur les modèles ARM, consultez la documentation Microsoft sur les modèles ARM.

Pour simplifier le déploiement de toutes les ressources requises, le modèle à deux niveaux (https://github.com/PaloAltoNetworks/azure/tree/master/two-tier-sample) comprend deux fichiers json :

- **Fichier de modèle**—Le fichier azureDeploy.json est le fichier de ressources principales qui déploie tous les composants au sein du groupe de ressource.
- **Fichier de paramètres**—Le fichier azureDeploy.parameters.json inclut les paramètres requis pour déployer correctement le pare-feu VM-Series dans le VNet. Il inclut les détails comme le niveau et la taille de la machine virtuelle, le nom d'utilisateur et le mot de passe pour le pare-feu et le nom du conteneur de stockage pour le pare-feu. Vous pouvez personnaliser ce fichier pour votre déploiement VNet Azure.

Pour vous aider à déployer le pare-feu en tant que passerelle pour les applications Internet, le modèle fournit le pare-feu VM-Series, un serveur de base de données et un serveur Web. Le VNet utilise l'espace d'adressage IP non routable 192.168.0.0/16. Vous pouvez modifier le modèle pour utiliser 172.16.0.0/12 ou 10.0.0.0/8.

Le modèle ARM fournit aussi les règles définies par l'utilisateur et les indicateurs de transfert IP nécessaires pour permettre au pare-feu VM-Series de sécuriser le groupe de ressources Azure. Pour les cinq sous-réseaux (Approuvé, Non approuvé, Web, Base de données et NAT) inclus dans le modèle, vous disposez de cinq tables de routage, une pour chaque sous-réseau, avec des règles définies par l'utilisateur pour le routage du trafic vers le pare-feu VM-Series et la machine virtuelle NAT.

Pour les quatre sous-réseaux (Approuvé, Non approuvé, Web et Base de données) inclus dans le modèle, vous disposez de quatre tables de routage, un pour chaque sous-réseau, avec des règles définies par l'utilisateur pour le routage du trafic vers le pare-feu VM-Series.

 ©2023 Palo Alto Networks, Inc.

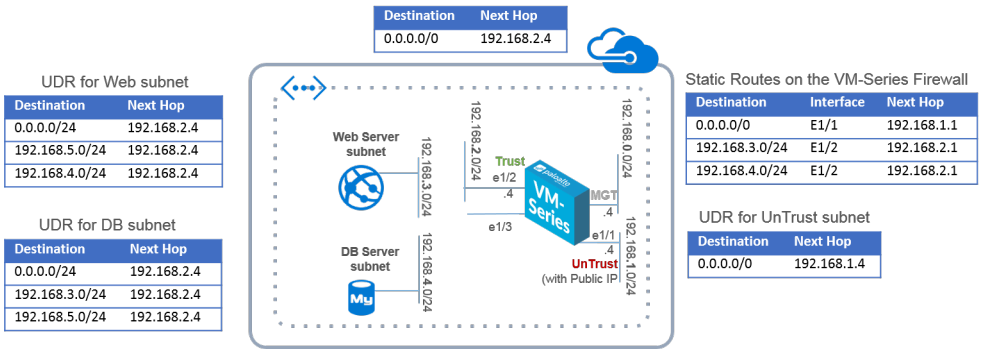


Figure 4: Déploiement du pare-feu VM-Series à l'aide du modèle ARM

STEP 1 | Téléchargez le modèle ARM à deux niveaux du dépôt GitHub.

Téléchargez et enregistrez les fichiers sur un client local :https://github.com/PaloAltoNetworks/azure/tree/master/two-tier-sample

STEP 2 | Créez un groupe de ressources sur Azure.

1. Connectez-vous à la CLI Azure en utilisant la commande : **`azurelogin`**

   Si vous avez besoin d'aide, reportez-vous à la documentation Azure sur l'installation de le CLI ou pour plus d'informations sur l'accès à la CLI sur Azure Government ou Azure China.
2. Basculez en mode gestionnaire de ressources en utilisant la commande : **`azureconfig mode arm`**.
3. Créez un groupe de ressources.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Déployez le modèle ARM.

1. Ouvrez le fichier de paramètres avec un éditeur de texte et modifiez les valeurs pour votre déploiement :

   Dans Azure China, vous devez modifier le chemin du compte de stockage qui héberge l'image VHD requise pour déployer le pare-feu VM-Series. Dans la section des variables du fichier modèle, recherchez le paramètre appelé ***userImageNameURI*** *et remplacez la valeur par l'emplacement où vous avez enregistré l'image VHD.*

2. Déployez le modèle dans le groupe de ressources que vous avez créé.

   ```
   azure group create -v -n "<YourResourceGroupName>" -l
    "<YourAzureLocation>" -d "<GiveASmallDeploymentLabel>" -f
    azureDeploy.json -e azureDeploy.parameters.json
   ```

3. Vérifiez la progression/l'état du déploiement à partir de la CLI Azure :

   ```
   azure group deployment show "<YourResourceGroupName>"
    "<YourDeploymentLabel>"
   ```

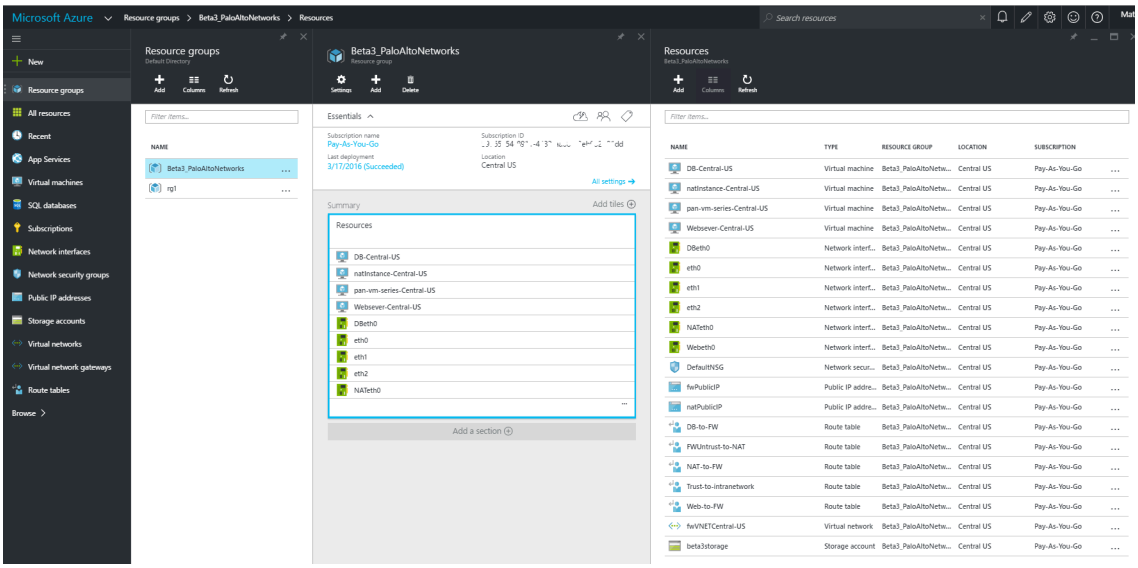
   Lorsque le modèle est correctement déployé, le message `ProvisioningStateis Running` apparaît.

   Si le message `ProvisioningStateis Failed (Échec de l'état de configuration)` apparaît, vous devez vérifier les erreurs sur le portail Azure dans ***Resource Group (Groupe de ressources) > Events (Événements)****. Filtrez uniquement les événements de la dernière heure, sélectionnez les événements les plus récents et examinez-les pour trouver les erreurs.*

4. Vérifiez que vous avez correctement déployé le pare-feu VM-Series.

   1. Sélectionnez **Dashboard (Tableau de bord)** > **Resource Groups (Groupes de ressources)**, puis le groupe de ressources.
   2. Sélectionnez **All Settings (Tous les paramètres)** > **Deployments (Déploiements)** > **Deployment History (Historique du déploiement)** pour consulter l'état détaillé.

 ©2023 Palo Alto Networks, Inc.



L'espace d'adressage au sein du VNet utilise le préfixe 192.168 qui est défini dans le modèle ARM.

5. Associez une adresse IP publique à l'interface non approuvée sur le pare-feu.

STEP 4 | Configurez le pare-feu en tant que passerelle VNet pour protéger votre déploiement vers Internet.

1. Connectez-vous à l'adresse IP de l'interface de gestion sur le pare-feu.
2. Configurez les interfaces réseau du dataplane en tant qu'interfaces de couche 3 sur le pare-feu (**Network (Réseau)** > **Interfaces** > **Ethernet**).
3. Ajoutez des règles statiques au routeur virtuel sur le pare-feu. Pour diriger le trafic à travers le pare-feu dans cet exemple, vous avez besoin de trois itinéraires statiques sur le pare-feu (**Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, sélectionnez le routeur et cliquez sur **Static Routes (Itinéraires statiques)**) :
   1. Dirigez tout le trafic sortant à travers la zone Non approuvée, ethernet1/1 sur le routeur Azure à 192.168.1.1.
   2. Dirigez tout le trafic entrant destiné au sous-réseau du serveur Web à travers la zone Approuvée, ethernet1/2 sur le routeur Azure à 192.168.2.1.
   3. Dirigez tout le trafic entrant destiné au sous-réseau du serveur de base de données à travers la zone Approuvée, ethernet1/2 sur le routeur Azure à 192.168.2.1.
4. Créez des règles de politique de sécurité (**Policies (Politiques)** > **Security (Sécurité)**) pour autoriser le trafic entrant et sortant sur le pare-feu. Vous avez aussi besoin de règles de politique de sécurité pour autoriser le trafic approprié dans les deux sens entre le sous-réseau du serveur Web et le serveur de base de données.
5. Cliquez sur **Commit (Valider)** pour valider les modifications apportées au pare-feu.
6. Vérifiez que le pare-feu VM-Series sécurise le trafic (**Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**).

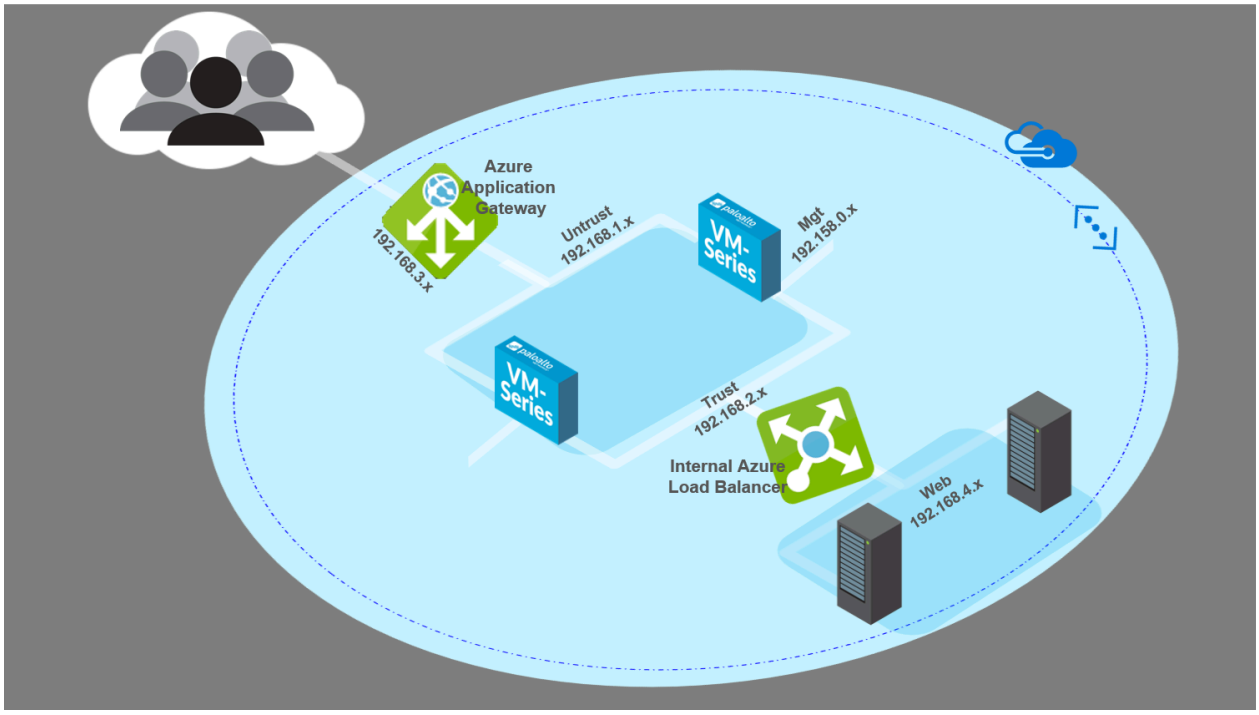
©2023 Palo Alto Networks, Inc.

Déploiement du modèle VM-Series et Azure Application Gateway

Le modèle VM-Series et Azure Application Gateway est un kit de démarrage que vous pouvez utiliser pour déployer des pare-feu VM-Series afin de sécuriser les charges de travail Web pour les déploiements Internet sur Microsoft Azure (actuellement non disponible pour Azure China).

Ce modèle déploie deux pare-feu VM-Series entre une paire d'équilibreurs de charge Azure (externes et internes). L'équilibreur de charge externe est un Azure Application Gateway, qui est un équilibreur de charge HTTP (couche 7) qui sert également de passerelle Internet, et qui reçoit le trafic et le distribue via le pare-feu VM-Series à l'équilibreur de charge interne. L'équilibreur de charge interne est un équilibreur de charge Azure (couche 4) qui sert de façade à une paire de serveurs Web. Le modèle prend en charge les versions Azure Marketplace et BYOL du pare-feu VM-Series.

À mesure que la demande sur vos charges de travail Web augmente et que vous augmentez la capacité du niveau de serveur Web, vous pouvez déployer manuellement des pare-feu VM-Series supplémentaires pour sécuriser votre niveau de serveur Web.

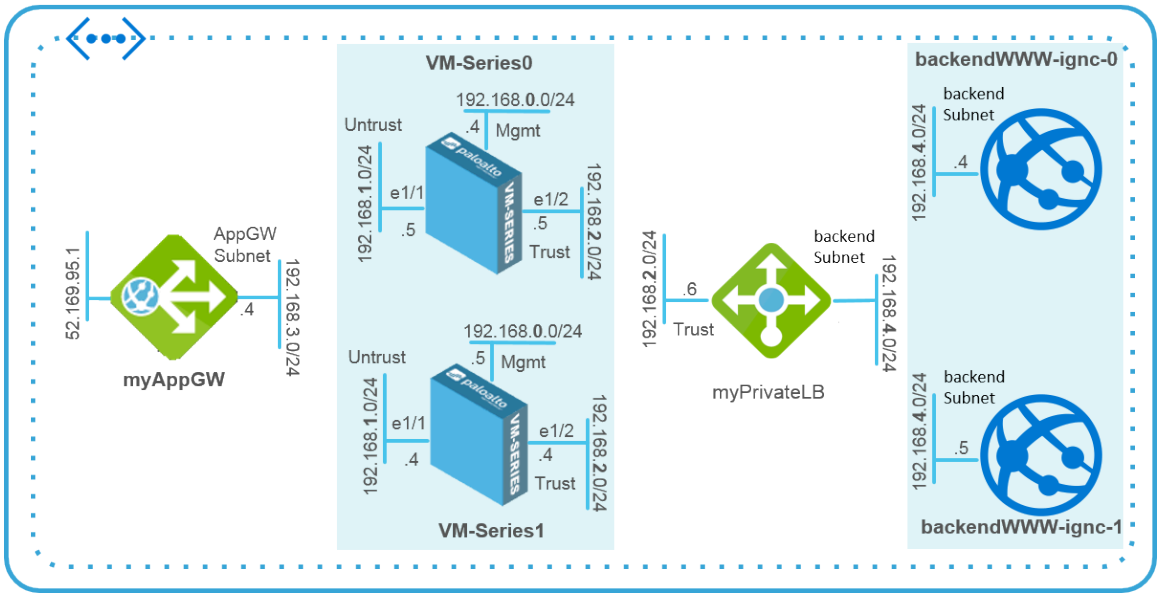


- Modèle VM-Series et Azure Application Gateway
- Commencer à utiliser le modèle VM-Series et Azure Appliction Gateway

©2023 Palo Alto Networks, Inc.

Modèle VM-Series et Azure Application Gateway

Les modèle VM-Series et Azure Application Gateway lance Azure Application Gateway (équilibreur de charge de couche 7) et un équilibreur de charge Azure (couche 4). Une paire de pare-feu VM-Series dans un ensemble de disponibilité et une paire d'exemples de serveurs Web exécutant Apache2 sur Ubuntu dans un autre ensemble de disponibilité sont imbriquées entre la passerelle d'application et l'équilibreur de charge. Les ensembles de disponibilité offrent une protection contre les coupures de courant planifiées ou non. Le diagramme de topologie suivant montre les ressources déployées par le modèle :



Vous pouvez utiliser un compte de stockage et un groupe de ressources nouveaux ou existants pour déployer toutes les ressources de cette solution dans un emplacement Azure. Il ne fournit pas de valeurs par défaut pour le nom du groupe de ressources et le nom du compte de stockage. Vous devez donc leur attribuer un nom. Alors que vous pouvez en créer un nouveau ou utiliser un réseau virtuel existant, le modèle crée un réseau virtuel par défaut nommé ***vnet-FW*** avec le bloc CIDR 192.168.0.0/16 et alloue cinq sous-réseaux (192.168.1.0/24 à 192.168.5.0/24) pour déployer Azure Application Gateway, les pare-feu VM-Series, l'équilibreur de charge Azure et les serveurs Web. Chaque pare-feu VM-Series est déployé avec trois interfaces réseau : ethernet0/1 dans le sous-réseau Mgmt (192.168.0.0/24), ethernet1/1 dans le sous-réseau non approuvé (192.168.1.0/24) et ethernet1/2 dans le sous-réseau approuvé (192.168.2.0/24).

Le modèle crée un groupe de sécurité réseau (NSG) qui autorise le trafic entrant à partir de n'importe quelle adresse IP source sur les ports 80, 443 et 22. Il déploie également la paire de pare-feu VM-Series et la paire de serveurs Web dans leurs ensembles de disponibilité respectifs afin de garantir qu'au moins une instance de chaque est disponible au cours d'une fenêtre de maintenance planifiée ou non planifiée. Chaque ensemble de disponibilité est configuré pour utiliser trois domaines d'erreur et cinq domaines de mise à jour.

Azure Application Gateway agit comme un service de proxy inverse, qui met fin à une connexion client et requêtes les demandes aux serveurs Web principaux. Azure Application Gateway est configuré avec un écouteur HTTP et utilise une sonde d'intégrité par défaut pour vérifier que l'adresse IP du pare-feu VM-Series (pour ethernet1/1) est saine et peut recevoir du trafic.

©2023 Palo Alto Networks, Inc.

Le modèle ne fournit pas de solution de mise à l'échelle automatique. Vous devez planifier vos besoins de capacité, puis déployer des ressources supplémentaires pour Adaptation du modèle *pour votre déploiement.*

Les pare-feu VM-Series ne sont pas configurés pour recevoir et sécuriser le trafic Web destiné aux serveurs Web. Par conséquent, vous devez au minimum configurer le pare-feu avec un itinéraire statique pour envoyer le trafic des pare-feu VM-Series au routeur par défaut, configurer la politique NAT de destination pour renvoyer le trafic vers l'adresse IP de l'équilibreur de charge et configurer la politique de sécurité règles. La règle de politique NAT est également requise pour que le pare-feu renvoie les réponses aux sondes d'intégrité à partir de l'écouteur HTTP sur Azure Application Gateway. Pour vous aider avec une configuration de pare-feu de base, le référentiel GitHub comprend un exemple de fichier de configuration appelé ***appgw-sample.xml*** que vous pouvez utiliser pour commencer.

Commencer à utiliser le modèle VM-Series et Azure Appliction Gateway

Le modèle VM-Series & Azure Application Gateway lance toutes les ressources dont vous avez besoin pour déployer et sécuriser vos charges de travail Web pour les déploiements Internet sur Microsoft Azure, à l'exception d'Azure China. Cette section fournit des détails sur la manière de déployer le modèle, de configurer les pare-feu pour acheminer et sécuriser le trafic destiné aux serveurs Web et d'étendre les capacités et les ressources fournies par ce modèle pour répondre à vos besoins de déploiement.

- Déploiement du modèle sur Azure
- Paramètres du modèle VM-Series et Azure Application Gateway
- Fichier de configuration modèle
- Adaptation du modèle

Déploiement du modèle sur Azure

Utilisez les instructions suivantes pour déployer le modèle sur Azure.

STEP 1 | Déployez le modèle.

Actuellement non disponible pour un déploiement dans Azure China.

1. Accédez au modèle depuis https://github.com/PaloAltoNetworks/azure-applicationgateway
2. Cliquez sur **Deploy to Azure (Déployer sur Azure)**.
3. Remplissez les détails pour déployer le modèle. Reportez-vous à la section Paramètres du modèle VM-Series et Azure Application Gateway pour une description et les valeurs par défaut, le cas échéant, pour chaque paramètre.

   Au minimum, vous devez choisir l'**Azure Subscription (Abonnement Azure)**, le **Resource Group (Groupe de ressources)**, le **Location (Emplacement)**, le **Storage Account Name (Nom du compte de stockage)** et un **Username/password (Nom d'utilisateur/mot de**

 ©2023 Palo Alto Networks, Inc.

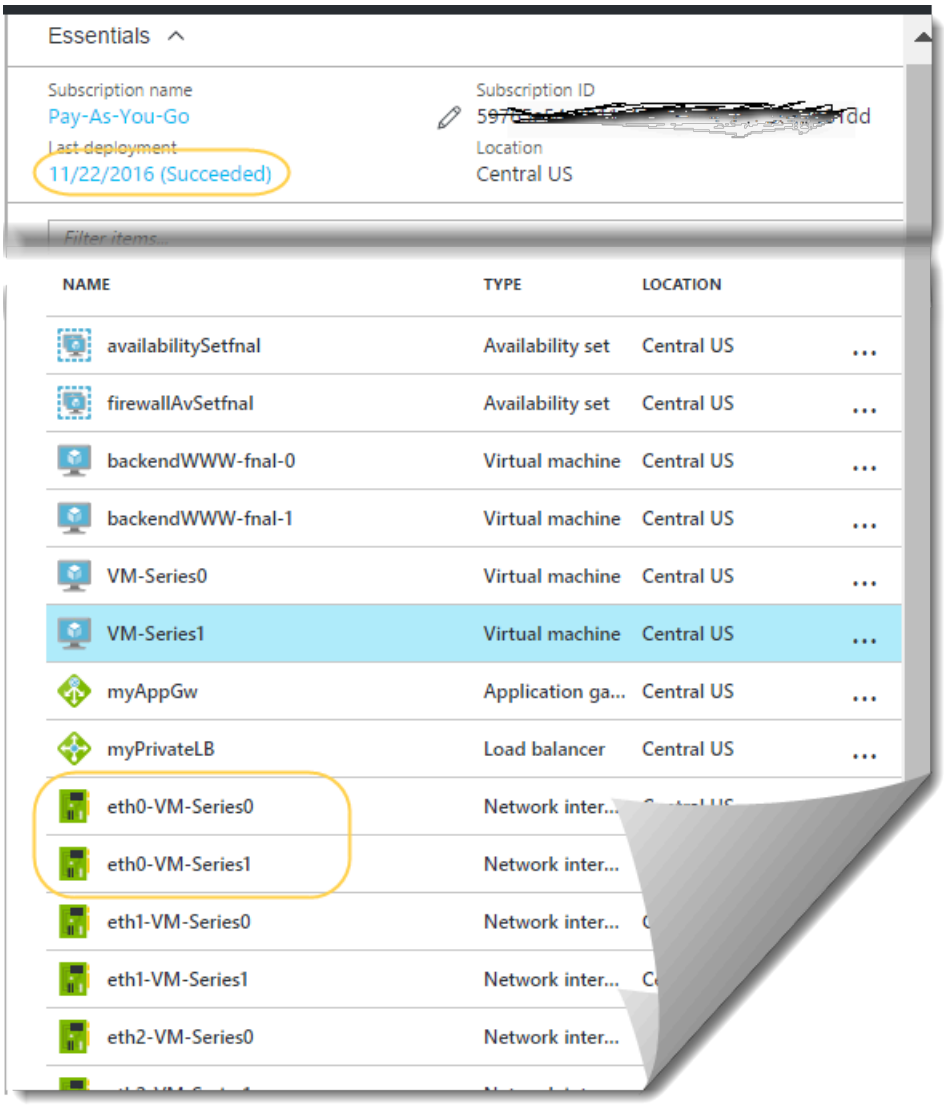
passe) ou une **SSH Key (Clé SSH)** pour le compte administrateur sur les pare-feu VM-Series.

4. Cliquez sur **Purchase (Acheter)** pour accepter les conditions générales et déployer les ressources.

   Si vous avez des erreurs de validation, cliquez pour afficher les détails et corriger vos erreurs.

5. Sur le portail Azure, vérifiez que vous avez déployé avec succès les ressources de modèle, y compris les pare-feu VM-Series.

   1. Sélectionnez **Dashboard (Tableau de bord)** > **Resource Groups (Groupes de ressources)**, puis le groupe de ressources.
   2. Sélectionnez **Overview (Aperçu)** pour examiner toutes les ressources qui ont été déployées. L'état du déploiement doit afficher **Succeeded (Réussi)**.



   3. Notez l'adresse IP publique ou le nom DNS attribué à **eth0-VM-Series0** et **eth0-VM-Series1** pour accéder à l'interface de gestion des pare-feu VM-Series.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Connectez-vous aux pare-feu.

1. En utilisant une connexion sécurisée (https) à partir de votre navigateur Web, connectez-vous à l'adresse IP pour eth0-VM-Series0 ou au nom de DNS pour le pare-feu.
2. Saisissez le nom d'utilisateur/mot de passe que vous avez défini dans le fichier de paramètres. Un avertissement de certificat s'affiche ; ne vous en préoccupez pas. Continuez vers la page Web.

STEP 3 | Configurez le pare-feu VM-Series.

Vous pouvez configurer le pare-feu manuellement ou importer le Fichier de configuration modèle fourni dans le GitHub référentiel et le personnaliser pour vos besoins de sécurité.

- **Configuration manuelle du pare-feu** — Vous devez au minimum :

1. Configurez les interfaces réseau du dataplane en tant qu'interfaces de couche 3 sur le pare-feu (**Network (Réseau)** > **Interfaces** > **Ethernet**).
2. Ajoutez une règle statique au routeur virtuel sur le pare-feu. Cette règle statique spécifie l'adresse IP de l'interface non approuvée du pare-feu comme adresse de destination pour tout trafic destiné à ethernet1/1. (**Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, sélectionnez le routeur et cliquez sur **Static Routes (Itinéraires statiques)**).
3. Créez des règles de politique de sécurité (**Policies (Politiques)** > **Security (Sécurité)**) pour autoriser le trafic entrant et sortant sur le pare-feu.
4. Ajoutez des politiques NAT (**Policies (Politiques)** > **NAT**). Vous devez créer les règles NAT de destination et de source sur le pare-feu pour envoyer le trafic vers les serveurs Web et le renvoyer au client qui a initié la requête.

   La règle NAT de destination s'applique à tout le trafic qui arrive sur l'interface non approuvée du pare-feu. Cette règle est requise pour traduire l'adresse IP de destination sur le paquet en celle de l'équilibreur de charge interne afin que tout le trafic soit dirigé vers l'équilibreur de charge interne et vers les serveurs Web principaux.

   La règle NAT source s'applique à tout le trafic provenant du serveur Web principal et est destinée à l'interface non approuvée du pare-feu. Cette règle traduit l'adresse source en l'adresse IP de l'interface approuvée sur le pare-feu.
5. **Commit (Validez)** vos modifications.

   - **Importation du fichier de configuration modèle :**
6. Téléchargez et enregistrez le fichier de configuration modèle sur votre client local.
7. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Operations (Opérations)**, cliquez sur **Import named configuration snapshot (Importer l'instantané de configuration**

 ©2023 Palo Alto Networks, Inc.

nommé), **Browse (Parcourir)** vers le fichier de configuration modèle que vous avez enregistré localement, puis cliquez sur **OK**.

8. Cliquez sur **Load named configuration snapshot (Charger l'instantané de la configuration)**, sélectionnez le **Name (Nom)** du fichier de configuration modèle que vous venez d'importer et cliquez sur **OK**.
9. Changez l'adresse IP des objets d'adresse et l'itinéraire statique pour faire correspondre l'adresse IP du bloc CIDR que vous avez utilisé. Mettez à jour les objets d'adresse pour utiliser les adresses IP privées pour eth1-VM-Series0 et eth1-VM-Series1.
10. IMPORTANT ! Créez un nouveau compte utilisateur administratif. Sélectionnez **Device (Périphérique)** > **Administrators (Administrateurs)** et **Add (Ajoutez)** un nouveau compte.
11. Modifiez le **Hostname (Nom d'hôte)** dans le widget General Settings (Paramètres généraux) dans **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**.
12. **Commit (Validez)** vos changements, et déconnectez-vous. La validation remplace la configuration en cours avec le fichier de configuration modèle et les mises à jour que vous venez de faire. Lors de la validation, le nom d'hôte et le compte administrateur que vous avez spécifiés lors du déploiement du modèle sont remplacés. Vous devez maintenant vous connecter en utilisant le nouveau compte utilisateur administratif et le nouveau mot de passe.
    - **Connexion au pare-feu** — Utilisez les informations d'identification que vous avez créées et supprimez le compte administrateur pandemo importé dans le fichier de configuration modèle.

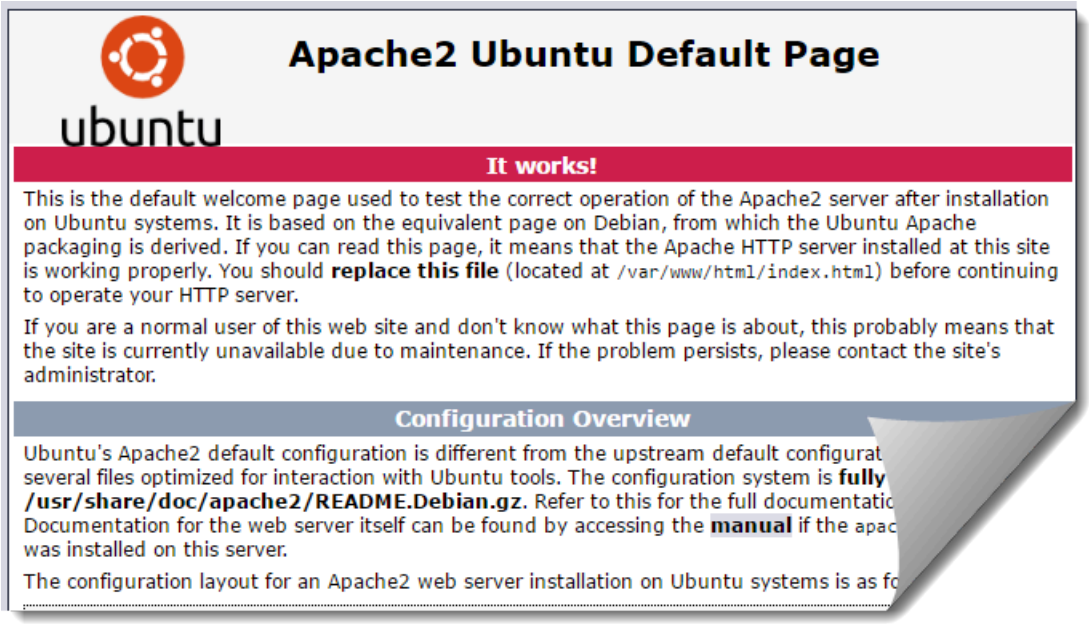
STEP 4 | Connectez-vous et configurez l'autre instance du pare-feu VM-Series.

Reportez-vous à l'étape Configurez le pare-feu VM-Series.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Vérifiez que vous avez correctement configuré les pare-feu.

Depuis votre navigateur Web, utilisez http pour accéder à l'adresse IP ou au nom DNS de la passerelle d'application. Vous devriez pouvoir afficher la page Web par défaut d'Apache 2 Ubuntu.



Si vous avez utilisé l'exemple de pare-feu de configuration, connectez-vous au pare-feu et affichez les journaux du trafic générés au démarrage de la session dans **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**.

Paramètres du modèle VM-Series et Azure Application Gateway

Le tableau suivant répertorie les paramètres obligatoires et facultatifs, ainsi que les valeurs par défaut, le cas échéant.

Paramètre	Description
Resource group (Groupe de ressources)	Créez-en un nouveau ou utilisez-en un existant (aucun par défaut).
Subscription (Abonnement)	Le type d'abonnement Azure que vous utiliserez pour couvrir le coût des ressources déployées avec le modèle.
Location (Emplacement)	Sélectionnez l'emplacement Azure dans lequel vous souhaitez déployer le modèle (aucun par défaut).
Network Security Group (Groupe de sécurité réseau)	
Network Security Group Name (Nom du groupe de sécurité réseau)	Le groupe de sécurité réseau limite les adresses IP source à partir desquelles les pare-feu et les serveurs Web de la VM-Series peuvent être accédés.

©2023 Palo Alto Networks, Inc.

Paramètre	Description
	Par défaut : nsg-mgmt
Network Security Group Inbound Src IP (IP source entrante du groupe de sécurité réseau)	Les adresses IP source qui peuvent se connecter au port de gestion des machines virtuelles déployées par le modèle. La valeur par défaut 0.0.0.0/0 signifie que vous pouvez vous connecter au port de gestion du pare-feu à partir de n'importe quelle adresse IP.
Storage Account (Compte de stockage)	
Storage Account Name (Nom du compte de stockage)	Créez-en un nouveau ou entrez le nom d'un compte de stockage existant (aucun par défaut). Le nom doit être mondialement unique.
Storage Account Type (Type de compte de stockage)	Choisissez entre le stockage standard et premium et vos besoins de réplication de données pour la redondance locale (LRS), la redondance géographique (GRS) et la redondance géographique d'accès en lecture (RAGRS). L'option par défaut est Locally Redondant Storage (LRS) (Stockage à redondance locale). Les autres options sont Standard GRS, Premium LRS et Standard RAGRS.
VNet (Réseau virtuel)	
Réseau virtuel	Créez un nouveau ou entrez le nom d'un réseau virtuel existant. Le nom par défaut pour le VNet est vnet-FW
Virtual Network Address Prefix (Préfixe d'adresse de réseau virtuel)	192.168.0.0/16
Azure Application Gateway (Passerelle d'application Azure)	
App Gateway Name (Nom de la passerelle d'application)	myAppGw
App Gateway DNS Name (Nom DNS de la passerelle d'application)	Saisissez un nom DNS mondialement unique pour Azure Application Gateway.
App Gateway Subnet Name and Prefix (Nom et préfixe de sous-réseau de la passerelle d'application)	Le nom par défaut est AppGWSubnet et le préfixe de sous-réseau est 192.168.3.0/24.

©2023 Palo Alto Networks, Inc.

Paramètre	Description
Azure Load Balancer and Web Servers (Équilibreur de charge Azure et serveurs Web)	
Internal Load Balancer Name (Nom de l'équilibreur de charge interne)	myPrivateLB
Internal Load Balancer Subnet Name and Prefix (Nom et préfixe de sous-réseau de l'équilibreur de charge interne)	Le nom par défaut est backendSubnet et le préfixe de sous-réseau est 192.168.4.0/24.
Backend Vm Size (Taille VM principale)	La taille par défaut est le niveau standard VM Azure D1. Utilisez la liste déroulante du modèle pour afficher les autres options VM Azure disponibles pour les serveurs Web principaux.
Firewalls (Pare-feu)	
Firewall Model (Modèle de pare-feu)	Choisissez parmi BYOL ou PAYG (forfait 1 ou 2, chaque forfait inclut le VM-300 et un ensemble d'abonnements).
Firewall Vm Name and Size (Nom et taille du pare-feu VM)	Le nom par défaut du pare-feu est VM-Series et la taille par défaut est niveau standard VM Azure D3. Utilisez la liste déroulante du modèle pour afficher les autres options VM Azure disponibles pour les pare-feu VM-Series
Mgmt Subnet Name and Prefix (Nom et préfixe de sous-réseau de gestion)	Le sous-réseau de gestion pour les pare-feu VM-Series et les serveurs Web déployés dans cette solution. Le nom par défaut est Mgmt et le préfixe du sous-réseau est 192.168.0.0/24.
Mgmt Public IP Address Name (Nom de l'adresse IP publique de gestion)	Entrez un nom d'hôte pour accéder à l'interface de gestion de chaque pare-feu. Les noms doivent être globalement uniques.
Trusted Subnet Name and Prefix (Nom et préfixe de sous-réseau approuvé)	Le sous-réseau auquel eth1/1 sur le pare-feu VM-Series est connecté. Ce sous-réseau connecte le pare-feu VM-Series à la passerelle d'application Azure. Le pare-feu reçoit le trafic Web destiné aux serveurs Web sur eth1/1. Le nom par défaut est Trust (Approuve) et le préfixe de sous-réseau est 192.168.2.0/24.

©2023 Palo Alto Networks, Inc.

Paramètre	Description
Untrusted Subnet Name (Nom de sous-réseau non approuvé)	Le sous-réseau auquel eth1/2 sur le pare-feu VM-Series est connecté. Le pare-feu reçoit le trafic Web sortant et de retour sur cette interface. Le nom par défaut est Untrust (Non approuvé) et le préfixe du sous-réseau est 192.168.1.0/24. Le nom doit être mondialement unique.
Username (Nom d'utilisateur)	Entrez le nom d'utilisateur du compte administrateur sur les pare-feu VM-Series et les serveurs Web.
Authentication Type (Type d'authentification)	Vous devez entrer un mot de passe pour l'authentification ou utiliser une clé publique SSH (aucun par défaut).

Fichier de configuration modèle

Pour vous aider à démarrer, le référentiel GitHub contient un exemple de fichier de configuration nommé ***appgw-sample.xml*** qui inclut les règles/objets suivants :

- **Objets d'adresse** : deux objets d'adresse, `firewall-untrust-IP` et `internal-load-balancer-IP`, que vous devrez modifier pour les faire correspondre aux adresses IP de votre configuration. Vous devez modifier ces objets d'adresse pour utiliser les adresses IP privées affectées à eth1-VM-Series0 et eth1-VM-Series1 sur le portail Azure.
- **Itinéraire statique** : le routeur virtuel par défaut sur le pare-feu dispose d'un itinéraire statique vers 192.168.1.1, et cette adresse IP est correcte si vous utilisez les valeurs de modèle par défaut. Si vous avez modifié le CIDR du sous-réseau non approuvé, vous devez mettre à jour l'adresse IP pour qu'elle corresponde à votre configuration. Tout le trafic provenant des serveurs Web principaux, destiné à la passerelle d'application, utilise cette adresse IP en tant que saut suivant pour fournir des paquets à l'interface non approuvée sur le pare-feu.
- **Règle de politique NAT** : la règle de politique NAT active le NAT de destination et le NAT source.
  - La règle NAT de destination s'applique à tout le trafic qui arrive sur l'interface non approuvée du pare-feu (ethernet1/2), qui est l'objet d'adresse firewall-untrust-IP. Cette règle traduit l'adresse IP de destination sur le paquet en celle de l'équilibreur de charge interne de sorte que tout le trafic est dirigé vers l'équilibreur de charge interne et donc vers les serveurs Web principaux.
  - La règle NAT source concerne tout le trafic provenant du serveur Web principal et est destinée à l'interface réseau non approuvée du pare-feu. Cette règle traduit l'adresse source en l'adresse IP de l'interface approuvée sur le pare-feu (ethernet1/2).
- **Règle de sécurité** : deux règles de politique de sécurité sont définies dans l'exemple de fichier de configuration. La première règle autorise tout trafic de navigation Web entrant et génère un journal au début d'une session sur le pare-feu. La deuxième règle bloque tout autre trafic et génère un journal au début et à la fin d'une session sur le pare-feu. Vous pouvez utiliser ces journaux pour surveiller l'ensemble du trafic vers les serveurs Web de ce déploiement.
- **Informations d'identification de l'utilisateur administratif** : l'exemple de fichier de configuration inclut un nom d'utilisateur et un mot de passe pour se connecter au pare-feu, défini sur

©2023 Palo Alto Networks, Inc.

pandemo/demopassword. Après avoir importé l'exemple de configuration, vous devez soit modifier le mot de passe et le définir sur un mot de passe personnalisé fort, soit créer un nouveau compte administrateur et supprimer le compte pandemo.

Adaptation du modèle

Au fur et à mesure que vos besoins évoluent, vous pouvez définir vos besoins en capacité et étendre le modèle de votre scénario de déploiement. Voici quelques façons de vous appuyer sur le modèle de démarrage pour répondre à vos besoins de capacité planifiés :

- Déployez des pare-feu VM-Series supplémentaires derrière Azure Application Gateway. Vous pouvez installer manuellement plus de pare-feu VM-Series dans le même ensemble de disponibilité ou lancer un nouvel ensemble de disponibilité et déployer manuellement d'autres pare-feu VM-Series.
- Configurez les pare-feu VM-Series au-delà de la configuration de base fournie dans l'exemple de fichier de configuration dans le référentiel GitHub.
- Activez l'équilibrage de charge HTTPS (déchargement SSL) sur Azure Application Gateway. Consultez la documentation Azure pour plus de détails.
- Ajoutez ou remplacez les exemples de serveurs Web inclus dans le modèle.

©2023 Palo Alto Networks, Inc.

Sécurisation des services Kubernetes dans Azure

Pour sécuriser les services Azure Kubernetes, vous devez d'abord installer le plug-in Azure sur Panorama et configurer un déploiement de Sécurisation des services Kubernetes dans Azure Azure. Le plug-in Azure pour Panorama prend en charge la surveillance VM et la Sécurisation des services Kubernetes dans Azurepar étiquette et permet de sécuriser le trafic entrant pour les clusters des services Azure Kubernetes (AKS) et de surveiller le trafic sortant des clusters AKS. Le déploiement orchestré Panorama vous permet de tirer parti des métriques de mise à l'échelle automatique et des seuils de mise à l'échelle (augmentation et diminution) pour gérer les augmentations de la demande de ressources de charge de travail d'application en mettant à l'échelle indépendamment les pare-feu VM-Series.

Pour sécuriser le trafic entrant pour votre cluster AKS, vous devez d'abord Sécurisation des services Kubernetes dans Azure. Le déploiement orchestré par Panorama fonctionne avec Sécurisation des services Kubernetes dans Azure pour collecter des informations sur votre réseau et vos ressources, puis pour créer une couche de mise à l'échelle automatique de pare-feu VM-Series pour les déploiements Sécurisation des services Kubernetes dans Azure. Reportez-vous à la Matrice de compatibilité Palo Alto Networks pour vérifier la configuration minimale (système d'exploitation, plug-in et versions de modèles) requise pour la sécurisation des clusters AKS.

Palo Alto Networks fournit un modèle AKS permettant de déployer un cluster de services Azure Kubernetes (AKS) dans un nouveau VNet Azure. Le plug-in Azure sur Panorama vous aide à configurer une connexion capable de surveiller les charges de travail de clusters Azure Kubernetes, de collecter des services que vous avez annotés comme « internal load balancer » (équilibreur de charge interne) et de créer des étiquettes que vous pouvez ensuite utiliser dans des groupes d'adresses dynamiques. Vous pouvez exploiter les groupes d'adresses dynamiques pour appliquer une politique de sécurité sur le trafic entrant acheminé aux services exécutés sur votre cluster AKS.

- Comment le plug-in Panorama pour Azure sécurise-t-il les services Kubernetes ?
- Sécurisation d'un cluster AKS

Comment le plug-in Panorama pour Azure sécurise-t-il les services Kubernetes ?

Vous pouvez utiliser les pare-feu VM-Series pour sécuriser le trafic entrant des clusters de services Azure Kubernetes (AKS). Le pare-feu VM-Series ne peut sécuriser que les services exposés par un équilibreur de charge (tel qu'un équilibreur de charge Azure). Le trafic sortant peut uniquement être surveillé.

Ce chapitre passe en revue les différents composants qui permettent au plug-in Azure pour Panorama de se connecter à un cluster AKS.

- Exigences
- Exemple de topologie en étoile pour sécuriser les clusters AKS
- Routage défini par l'utilisateur
- Communication du cluster AKS
- Groupes d'adresses dynamiques avec étiquettes Kubernetes

©2023 Palo Alto Networks, Inc.

Exigences

Cette solution nécessite les éléments suivants. Consultez les informations concernant le plug-in Panorama dans la matrice de compatibilité pour connaître la version minimale requise.

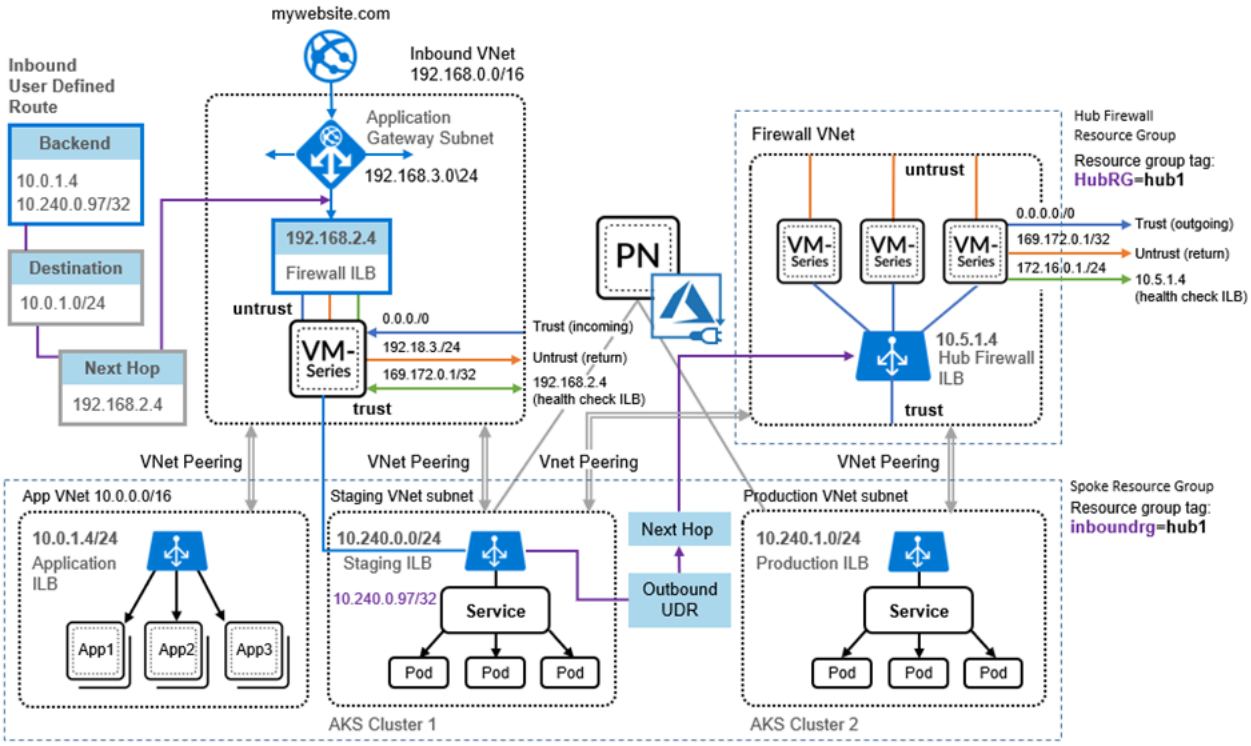
- Pare-feu VM-Series.
- Panorama : votre version de Panorama doit être identique ou supérieure à votre version de PAN-OS VM-Series.
- Plug-in Panorama pour Azure.
- Un déploiement orchestré par Panorama.
- Modèle AKS Azure version 1.0. Ce modèle crée un cluster AKS.

  Vous devez activer AKS advanced networking (mise en réseau avancée AKS) (CNI) pour le cluster.

  Un déploiement AKS nécessite une mise en réseau avancée pour configurer l'appairage VNet pour les réseaux virtuels en étoile (voir Exemple de topologie en étoile pour sécuriser les clusters AKS).

Exemple de topologie en étoile pour sécuriser les clusters AKS

Le diagramme suivant illustre un exemple de déploiement de mise à l'échelle automatique qui sécurise le trafic entrant pour les clusters Azure AKS. Examinons certains des composants.



- **Infrastructure de mise à l'échelle automatique** : les modèles de mise à l'échelle automatique Azure créent l'infrastructure de messagerie et l'architecture en étoile de base.
- **Clusters AKS** : le modèle AKS Palo Alto Networks crée un cluster AKS dans un nouveau VNet. Étant donné le nom du groupe de ressources Spoke, le modèle marque le cluster VNet et AKS avec le nom du groupe de ressources Spoke, de sorte que le groupe de ressources puisse être découvert par le plug-in de mise à l'échelle automatique Azure pour Panorama. Le plug-in Azure

©2023 Palo Alto Networks, Inc.

pour Panorama interroge les adresses IP des services sur l'ILB de transit afin d'en savoir plus sur les services du cluster AKS.

Un seul ensemble de mise à l'échelle de pare-feu Spoke peut être associé à un cluster AKS. Si vous exposez plusieurs services dans un même cluster AKS, ils doivent être protégés par le même Spoke.

Pour chaque groupe de ressources, créez un groupe d'adresses basé sur un sous-réseau. Dans le diagramme ci-dessus, par exemple, créez un groupe d'adresses pour 10.240.0.0/24 (cluster AKS Cluster 1).

- **Appairage VNet** : vous devez configurer manuellement l'appairage VNet pour communiquer avec d'autres VNets dans la même région.

  L'appairage inter-régions n'est pas pris en charge.

  Vous pouvez utiliser d'autres outils d'automatisation pour déployer les clusters AKS. En cas de déploiement dans un VNet existant (le VNet de pare-feu Hub, par exemple), vous devez configurer manuellement l'appairage VNet vers les groupes de ressources entrants et sortants en étoile, et étiqueter manuellement le cluster VNet et AKS avec le nom du groupe de ressources.

- **Routes et règles définies par l'utilisateur** : vous devez configurer manuellement les routes et les règles définies par l'utilisateur (voir Routage défini par l'utilisateur). Dans le diagramme ci-dessus, le trafic entrant peut être redirigé, selon les règles des UDR, vers le l'ILB du pare-feu pour inspection. Le trafic sortant d'un cluster AKS est redirigé vers l'ILB du pare-feu Hub avec des règles de routage définies par l'utilisateur (UDR) Azure. La solution suppose que Allow All (Tout autoriser) est la politique par défaut pour que l'orchestration de Kubernetes fonctionne telle quelle ; mais pour appliquer la politique, vous pouvez utiliser une liste d'autorisation ou de déni pour autoriser ou refuser le trafic sortant.

Routage défini par l'utilisateur

Vous devez créer manuellement un routage et des règles de routage définis par l'utilisateur pour régir le trafic entrant ou sortant.

Inbound (Entrant)

Dans le diagramme ci-dessus, le trafic entrant de la passerelle d'application est dirigé vers le pool principal et, sur la base des règles des UDR, redirigé vers l'ILB du pare-feu. Par exemple, créez un UDR pointant vers le sous-réseau VNet afin que le trafic des services Kubernetes soit dirigé vers l'ILB du pare-feu.

Sortant

Sur l'ensemble de pare-feu Hub, pour chaque cluster AKS protégé, vous devez créer des routes statiques pour le CIDR du sous-réseau du cluster, le saut suivant étant l'adresse de passerelle du sous-réseau de confiance VNet Hub.

Tout le trafic sortant d'un cluster AKS est dirigé vers l'ensemble de pare-feu Hub avec une seule règle UDR.

©2023 Palo Alto Networks, Inc.

Communication du cluster AKS

Le plug-in Panorama pour Azure ne peut communiquer qu'avec le nœud de contrôle AKS pour un cluster AKS donné. Pour le trafic AKS sortant, le saut suivant est l'ILB du pare-feu Hub. Comme le trafic sortant est surveillé, vous devez autoriser tout le trafic. Les rubriques suivantes mettent l'accent sur les pratiques courantes qui vous aident à établir la connectivité. Gardez-les à l'esprit lorsque vous planifiez vos réseaux et sous-réseaux.

- Création d'une authentification de cluster AKS
- Utilisation d'un groupe d'adresses pour identifier le trafic
- Ajout du groupe d'adresses de sous-réseau à la politique de premier niveau
- Prévention des interruptions d'applications lorsque les VNets de charges de travail et du cluster AKS sont appairés

Création d'une authentification de cluster AKS

Lorsque vous connectez le cluster AKS dans le plug-in Azure pour Panorama, vous devez entrer un jeton d'autorisation secret. Utilisez les commandes Kubernetes pour réaliser les étapes suivantes.

STEP 1 | Créez un ClusterRole (Rôle de cluster).

STEP 2 | Créez une ClusterRoleBinding (Liaison de rôle de cluster).

1. Créez un fichier `.yaml` pour ClusterRoleBinding. Par exemple, créez un fichier texte nommé `crb.yaml`.

```
 apiVersion: rbac.authorization.k8s.io   kind:
ClusterRoleBinding   metadata:      name: default-view
  roleRef:     apiGroup: rbac.authorization.k8s.io
    kind: ClusterRole     name: view   subjects:   - kind:
ServiceAccount   name: default   namespace: default
```

2. Utilisez Azure Cloud Shell pour appliquer la liaison de rôle `crb.yaml`.

   kubectl apply -f crb.yaml

3. Affichez le compte de service que vous venez de créer.

   kubectl get serviceaccounts

STEP 3 | Enregistrez les informations d'identification du compte de service dans un fichier `.json`.

1. Sur votre ordinateur local, accédez au répertoire dans lequel vous souhaitez enregistrer les informations d'identification.
2. Utilisez les commandes kubectl pour créer le jeton.

   MY_SA_TOKEN='kubectl get serviceaccounts default -o jsonpath='{.secrets[0].name}''

3. Affichez le nom du jeton.

   $ echo $MY_SA_TOKEN

4. Affichez les informations d'identification.

   kubectl get secret $MY_SA_TOKEN -o json

Vous avez besoin du jeton lorsque vous connectez le cluster AKS dans le plug-in Azure pour Panorama, à l'étape 3.d.

 ©2023 Palo Alto Networks, Inc.

Utilisation d'un groupe d'adresses pour identifier le trafic

Pour créer une certaine granularité pour le trafic sortant surveillé, créez un groupe d'adresses spécifique pour le sous-réseau VNet du cluster AKS (par exemple, 10.240.0.97/32 dans le diagramme ci-dessus). Vous pouvez ensuite écrire des règles qui autorisent le trafic entrant ou le trafic de retour plutôt que d'utiliser la fonction Allow All (Tout autoriser).

Si vous créez un groupe d'adresses, veillez à maintenir la communication entre le nœud de contrôle AKS et tout nœud esclave. Reportez-vous à la section Ajout du groupe d'adresses de sous-réseau à la politique de premier niveau.

Si la communication est interrompue, le trafic de l'application risque d'être perdu, ou le déploiement de votre application peut avoir des problèmes.

Ajout du groupe d'adresses de sous-réseau à la politique de premier niveau

Pour maintenir la connectivité, le groupe d'adresses doit faire partie de la politique de haut niveau dans Panorama. Vous pouvez configurer le groupe d'adresses du cluster, ou amorcer le cluster pour configurer le groupe d'adresses du cluster.

*Ajoutez le groupe d'adresses à la politique de premier niveau **avant** de configurer l'appairage VNet ou* Routage défini par l'utilisateur.

Prévention des interruptions d'applications lorsque les VNets de charges de travail et du cluster AKS sont appairés

Si un cluster AKS coexiste avec des charges de travail de VM qui s'exécutent dans des VNets séparés et que le VNet est appairé avec le Spoke (entrant) et le Hub (sortant) des charges de travail, vous devez créer des groupes d'adresses pour différencier les charges de travail et le trafic AKS, et ajouter le groupe d'adresses à la politique de premier niveau comme décrit ci-dessus.

Groupes d'adresses dynamiques avec étiquettes Kubernetes

Lors de la surveillance d'une ressource du cluster AKS, le plug-in Azure génère automatiquement les étiquettes IP suivantes pour les services AKS.

```
aks.<aks cluster name>.<aks service name>
```

Les étiquettes ne sont pas générées pour les nœuds, les pods ou les autres ressources.

Si le service AKS possède des étiquettes, l'étiquette est la suivante (une par étiquette) :

```
aks.<aks cluster name>.svc.<label>.<value>
```

Si une étiquette labelSelector est définie pour un cluster, le plug-in génère l'étiquette IP suivante :

```
aks_<labelSelector>.<aks cluster name>.<aks service name>
```

 ©2023 Palo Alto Networks, Inc.

Sécurisation d'un cluster AKS

Pour permettre à Panorama de se connecter aux équilibreurs de charge d'un cluster AKS (Azure Kubernetes Services), vous devez activer le plug-in Azure sur Panorama pour établir une connexion avec votre cluster AKS. Ensuite, vous devez configurer les groupes de périphériques et les modèles auxquels appartiennent les pare-feu pour que Panorama puisse envoyer les objets de configuration et les règles de politique à vos pare-feu gérés.

- Avant de commencer
- Utiliser le modèle pour déployer un cluster AKS
- Connecter le cluster AKS dans le plug-in Azure pour Panorama
- Configurer un appairage de VNet
- Rediriger le trafic vers un ILB de pare-feu
- Appliquer la politique au service AKS pertinent
- Déployer et sécuriser les services AKS

Avant de commencer

Pour sécuriser AKS, vous devez d'abord déployer la solution de mise à l'échelle automatique Azure disponible sur GitHub.

Pour sécuriser une application Web fonctionnant en tant que service au sein d'un cluster Kubernetes, vous devez planifier les VNets, les sous-réseaux et les UDR. Les pare-feu VM-Series et Panorama vous offrent la sécurité et la visibilité de vos services Kubernetes.

- Examinez « Comment le plug-in Panorama pour Azure sécurise-t-il les services Kubernetes ? ».
- Vous devez disposer d'une mise en réseau avancée AKS pour utiliser le modèle AKS de Palo Alto Networks.
- Concevez vos sous-réseaux AKS **avant** de déployer les clusters AKS. Examinez Exemple de topologie en étoile pour sécuriser les clusters AKS et Communication du cluster AKS.
  - Le modèle crée un seul cluster AKS (Service) à titre d'exemple. Vous devez spécifier les plages CIDR pour le VNet, le sous-réseau VNet et le service. Les plages CIDR ne doivent pas se chevaucher
  - Dimensionnez vos sous-réseaux en fonction de vos besoins. Évitez les plages inutilement larges, car elles peuvent affecter les performances.
  - Reportez-vous à la section Routage défini par l'utilisateur. Spécifiez des routes UDR spécifiques plutôt que des routes globales spécifiques à un sous-réseau.
- Planifiez la manière dont vous souhaitez appairer vos VNets. Si vous appairez des clusters AKS, assurez-vous d'avoir lu la section Communication du cluster AKS.
- Réfléchissez aux moyens par lesquels vous souhaitez identifier le trafic.
  - Si vous prévoyez d'utiliser un groupe d'adresses sur le trafic AKS sortant, reportez-vous à la section Ajout du groupe d'adresses de sous-réseau à la politique de premier niveau.
  - Si vous avez des noms de service ou des étiquettes qui ne sont pas uniques dans les espaces de noms, utilisez le sélecteur d'étiquettes pour filtrer à la fois une étiquette et un espace de noms afin d'obtenir un résultat unique.

 ©2023 Palo Alto Networks, Inc.

Utiliser le modèle pour déployer un cluster AKS

Le modèle Azure AKS est un échantillon qui fournit un cluster dans un nouveau VNet.

STEP 1 | Sur GitHub, rendez-vous sur PaloAltoNetworks/azure-aks et localisez le package de génération dans le référentiel.

STEP 2 | Décompressez le package de génération. Modifiez les fichiers **azuredeploy.json** et **parameters.json** pour votre propre déploiement, et enregistrez.

STEP 3 | Exécutez les commandes de CLI Azure suivantes pour déployer le modèle.

```
az group deployment validate --resource-group RG_NAME --template-
file azuredeploy.json --parameters @parameters.json
```

```
az group deployment create --name DEPLOYMENT_NAME --resource-
group RG_NAME --template-file azuredeploy.json --parameters
 @parameters.json
```

STEP 4 | Déployez vos applications ou services sur le cluster AKS.

1. Annotez votre fichier YAML de service pour que le type soit load balancer (équilibreur de charge), et annotez-le de la manière suivante : service.beta.kubernetes.io/azure-load-balancer-internal: "true". Par exemple :

   ```
     apiVersion: v1     kind: Service   metadata:    name: azure-
   vote-front    labels:    service: "azure-vote-front"    tier:
    "stagingapp"    annotations:    service.beta.kubernetes.io/
   azure-load-balancer-internal: "true"   spec:    type:
    LoadBalancer ports: - port: 80 selector: app: azure-vote-
   front
   ```

2. Si vous ne l'avez pas encore fait, créez une authentification de cluster AKS avant de continuer.
3. Déployez votre service sur votre cluster AKS.

   Par exemple, vous pouvez déployer votre application via kubectl :

   kubectl apply -f myapplication.yaml

   Pour un exemple, consultez : https://github.com/Azure-Samples/azure-voting-app-redis/blob/master/azure-vote-all-in-one-redis.yaml

©2023 Palo Alto Networks, Inc.

4. Utilisez kubectl pour obtenir l'adresse IP du service déployé.

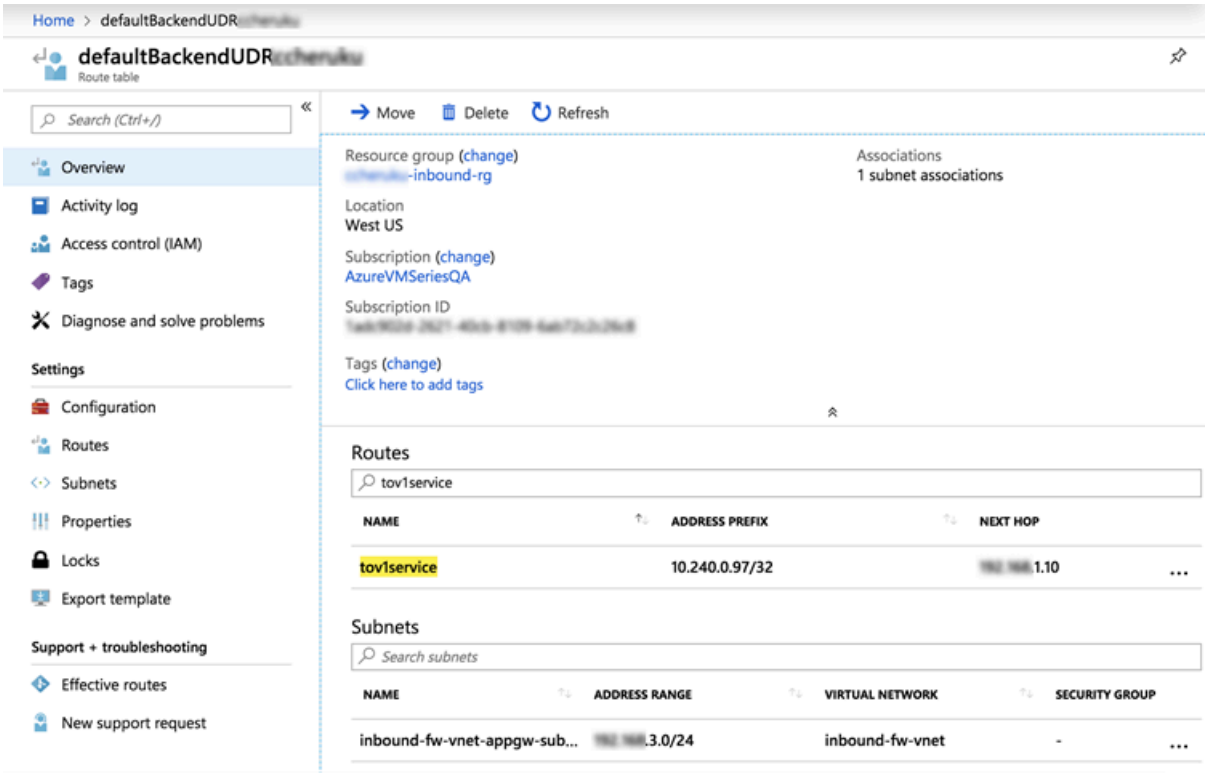
```
kubectl get services -o wide
```

```
NAME               TYPE           CLUSTER-IP     EXTERNAL-IP   PORT(S)          AGE    SELECTOR
azure-vote-back    ClusterIP      10.0.77.21     <none>        6379/TCP         2d23h  app=azure-vote-back
azure-vote-front   LoadBalancer   10.0.18.189    10.240.0.97   80:31937/TCP     2d23h  app=azure-vote-front
kubernetes         ClusterIP      10.0.0.1       <none>        443/TCP          2d23h  <none>
```

Dans la colonne EXTERNAL-IP (IP externe), 10.240.0.97 correspond à l'ILB, selon l'annotation que vous avez faite à l'étape a. Utilisez l'IP du service pour créer une route défini par l'utilisateur sur Azure.

STEP 5 | Créez une règle UDR pour diriger votre service vers l'ILB du pare-feu derrière la passerelle d'application.

Dans Azure, accédez à votre groupe de ressources Spoke entrant, consultez la table de routage et ajoutez une nouvelle route basée sur l'IP du service de destination. Dans l'écran suivant, la valeur dans la colonne **ADDRESS PREFIX (Préfixe d'adresse)** tov1service est l'adresse IP du service.



Connecter le cluster AKS dans le plug-in Azure pour Panorama

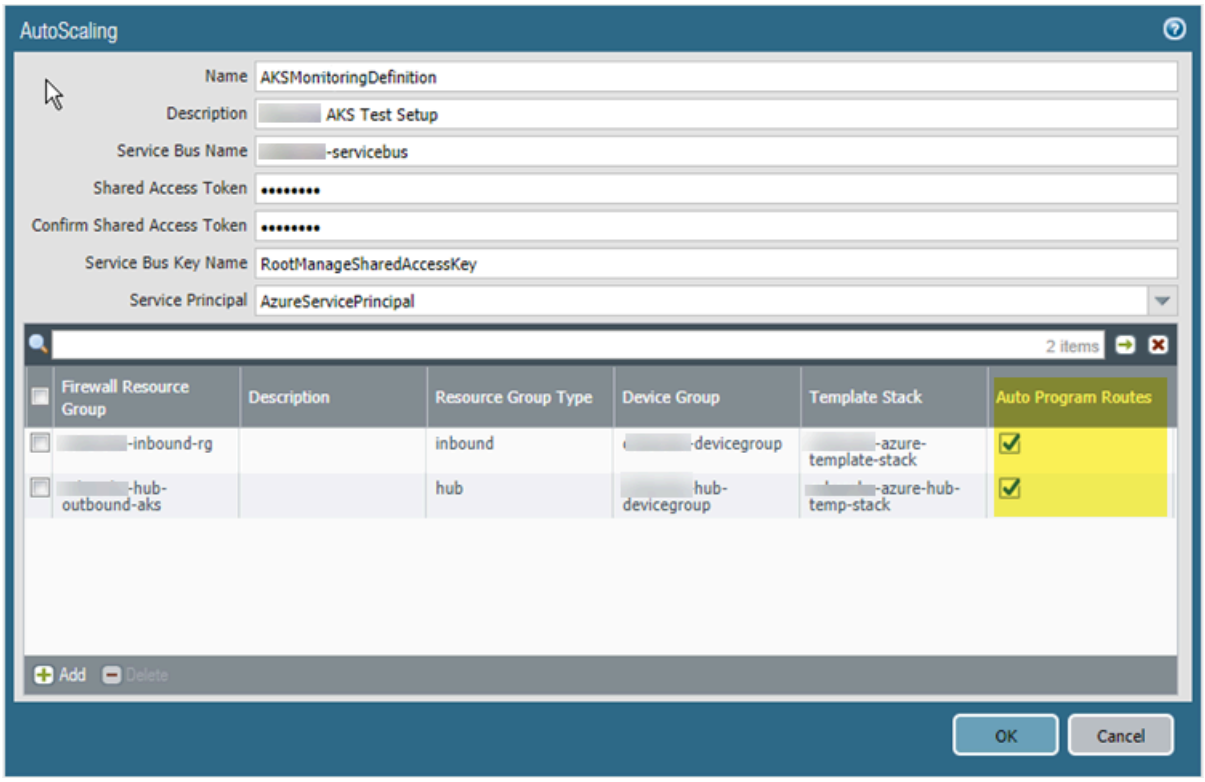
Cette tâche suppose que vous ayez déployé un déploiement orchestré de Panorama et que vous ayez créé des modèles, des piles de modèles et des groupes d'appareils.

Consultez l'aide en ligne de Panorama pour en savoir plus sur la manière de remplir chaque formulaire.

STEP 1 | Sélectionnez **Panorama** > **Azure** > **Deployments (Déploiements)** pour afficher la définition de surveillance que vous avez créée lorsque vous avez configuré le déploiement. Comme indiqué

 ©2023 Palo Alto Networks, Inc.

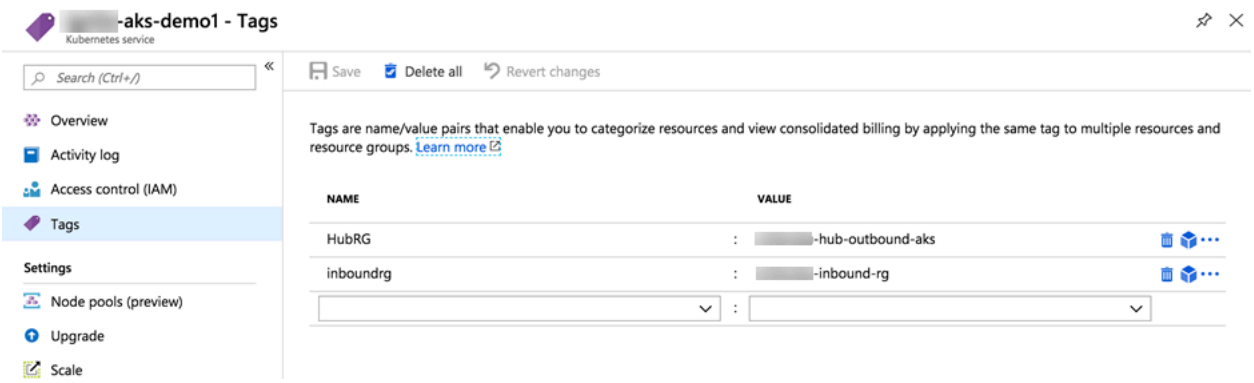
ci-dessous, si **Auto Program Routes (Programmation de routes automatique)** est activé, les routes du pare-feu sont programmés pour vous.



©2023 Palo Alto Networks, Inc.

STEP 2 | Dans AKS, étiquetez vos groupes de ressources. Les étiquettes sont des paires nom/valeur.

1. Sélectionnez **Home (Accueil)** > **Resource groups (Groupes de ressources)** et choisissez un groupe de ressources.
2. Sélectionnez **Tags (Étiquettes)** et définissez les paires nom/valeur. Comme le montre la figure suivante, les noms des étiquettes doivent être inboundgrouprg et HubRG :
   - inboundgrouprg : votre nom de groupe de ressources Spoke
   - HubRG :votre nom de groupe de ressources Hub



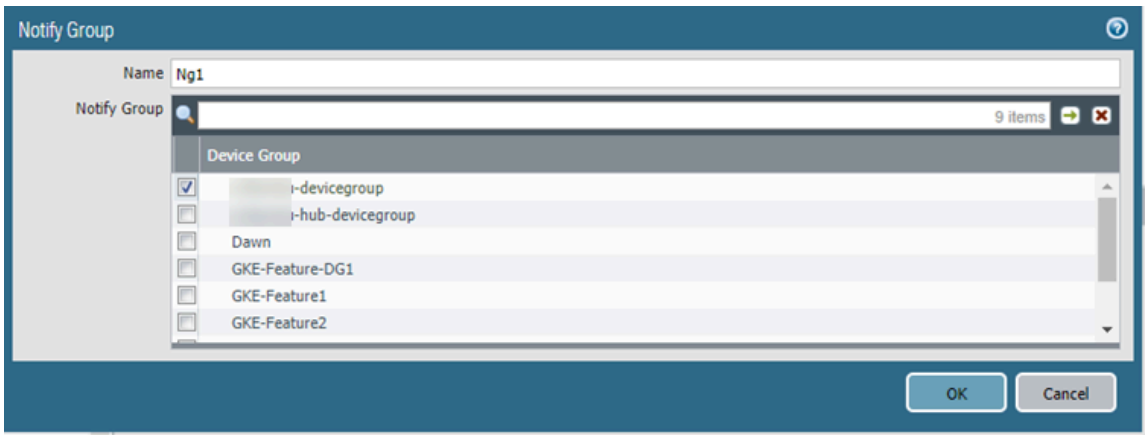
Le modèle prend le nom du groupe de ressources Spoke comme paramètre et marque le cluster VNet et AKS avec le nom du groupe de ressources Spoke, de sorte qu'il puisse être découvert par le plug-in Panorama pour Azure.

Les modèles déploient les ressources dans des VNets séparés. Si vous déployez manuellement le cluster AKS et le service dans le même VNet que le pare-feu Spoke, vous devez créer manuellement des étiquettes pour le nom du groupe de ressources Spoke.

 ©2023 Palo Alto Networks, Inc.

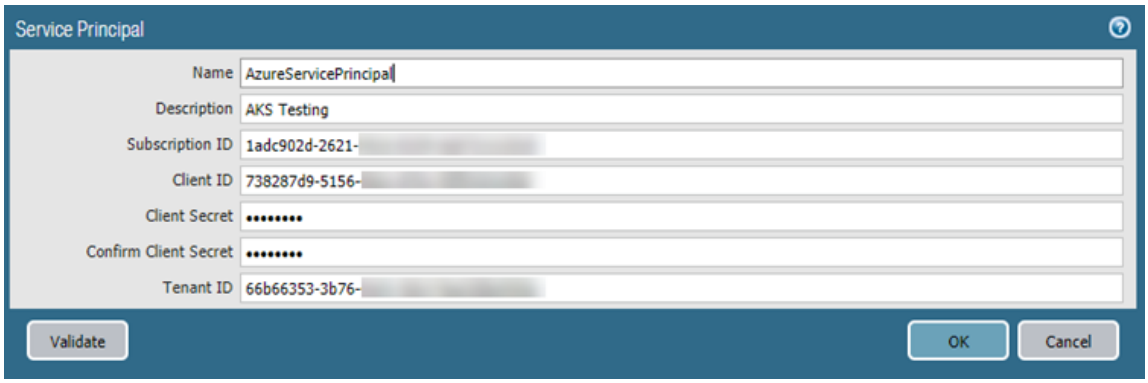
STEP 3 | Dans Panorama, sélectionnez **Panorama** > **Azure** > **Setup (Configuration)**.

1. Dans l'onglet **General (Général)**, activez la surveillance.
2. Dans l'onglet **Notify Groups (Groupes de notification)**, cliquez sur **Add (Ajouter)** pour ajouter un groupe de notification et sélectionnez les groupes de périphériques à notifier.



3. Dans l'onglet **Service Principal (Principal de service)**, cliquez sur **Add (Ajouter)** et **Validate (Valider)** pour ajouter et valider un principal de service.

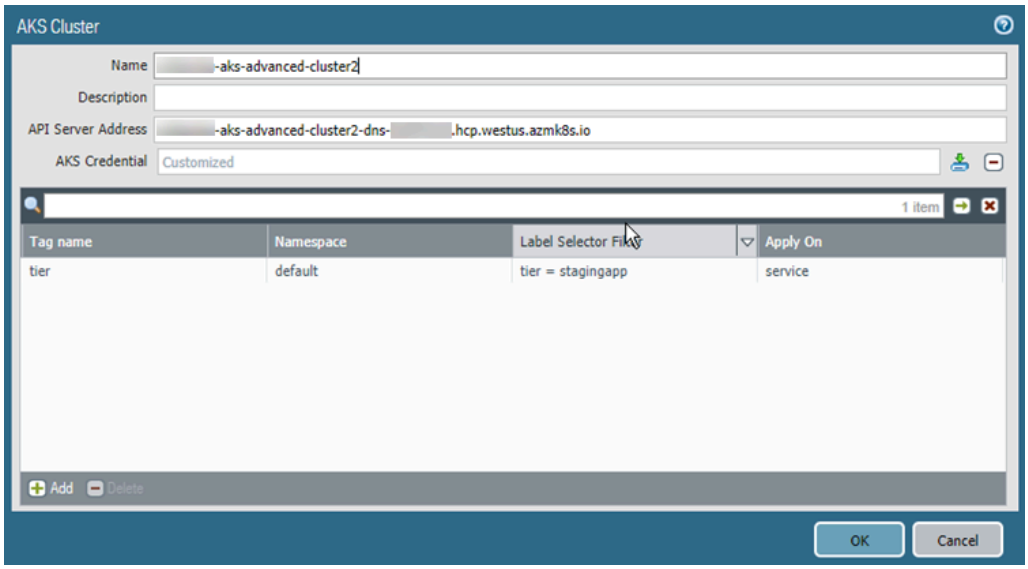
   Utilisez le principal de service que vous avez créé pour le déploiement orchestré.



4. Dans l'onglet **AKS Cluster (Cluster AKS)**, cliquez sur **Add (Ajouter)** pour ajouter un cluster AKS.
   - Saisissez le nom exact du cluster AKS.
   - Saisissez l'adresse du serveur API. Pour trouver l'adresse dans Azure, affichez votre service AKS et sélectionnez Overview (Aperçu).
   - Chargez le fichier JSON d'identification AKS (voir Création d'une authentification de cluster AKS).
5. Remplissez les champs restants et cliquez sur **Add (Ajouter)** pour ajouter une ou plusieurs étiquettes.

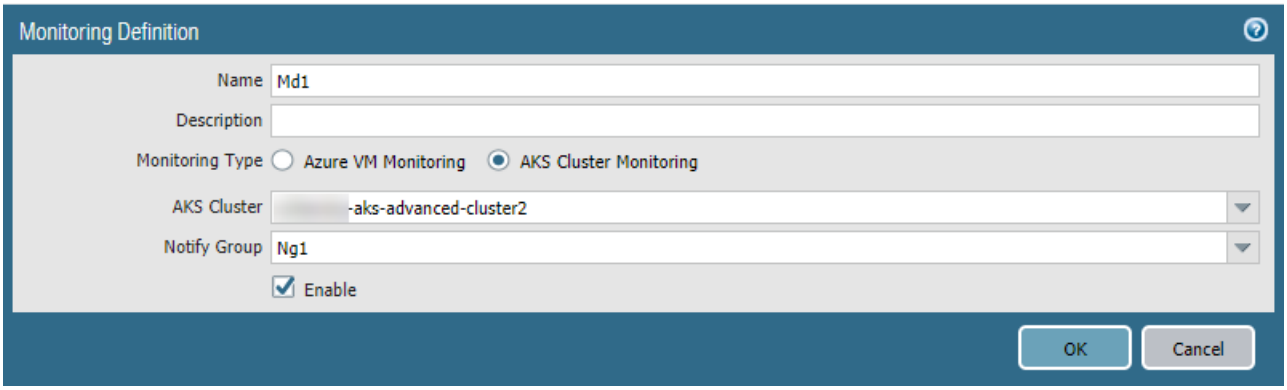
   Si vous avez des noms de service ou des étiquettes qui ne sont pas uniques dans les espaces de noms, utilisez le sélecteur d'étiquettes pour filtrer à la fois une étiquette et un espace de noms afin d'obtenir un résultat unique.

 ©2023 Palo Alto Networks, Inc.



STEP 4 | Sélectionnez **Panorama** > **Azure** > **Monitoring Definition (Définition de surveillance)**.

1. Ajoutez une définition de surveillance.
2. Saisissez un nom et une description, puis sélectionnez **AKS Cluster Monitoring (Surveillance de cluster AKS)**.
3. Sélectionnez un **AKS Cluster (Cluster AKS)** et un **Notify Group (Groupe de notification)**, cochez **Enable (Activer)** et cliquez sur **OK**.



Configurer un appairage de VNet

Si vous prévoyez d'utiliser un groupe d'adresses pour identifier le trafic, veillez à ajouter le groupe d'adresses du sous-réseau à votre politique Panorama de premier niveau avant de configurer l'appairage.

Après avoir déployé un cluster AKS, configurez l'appairage de VNet depuis le VNet entrant vers votre cluster, et depuis votre cluster vers le VNet du pare-feu.

Rediriger le trafic vers un ILB de pare-feu

Vous devez créer manuellement des routes définies par l'utilisateur (UDR) et des règles de routage pour rediriger le trafic vers un ILB particulier. À titre d'exemple, examinez comment le diagramme

 ©2023 Palo Alto Networks, Inc.

de la section « Comment le plug-in Panorama pour Azure sécurise-t-il les services Kubernetes ? » représente un UDR entrant.

STEP 1 | Créez des règles de routage d'URL qui redirigent le trafic Web vers le pool principal approprié.

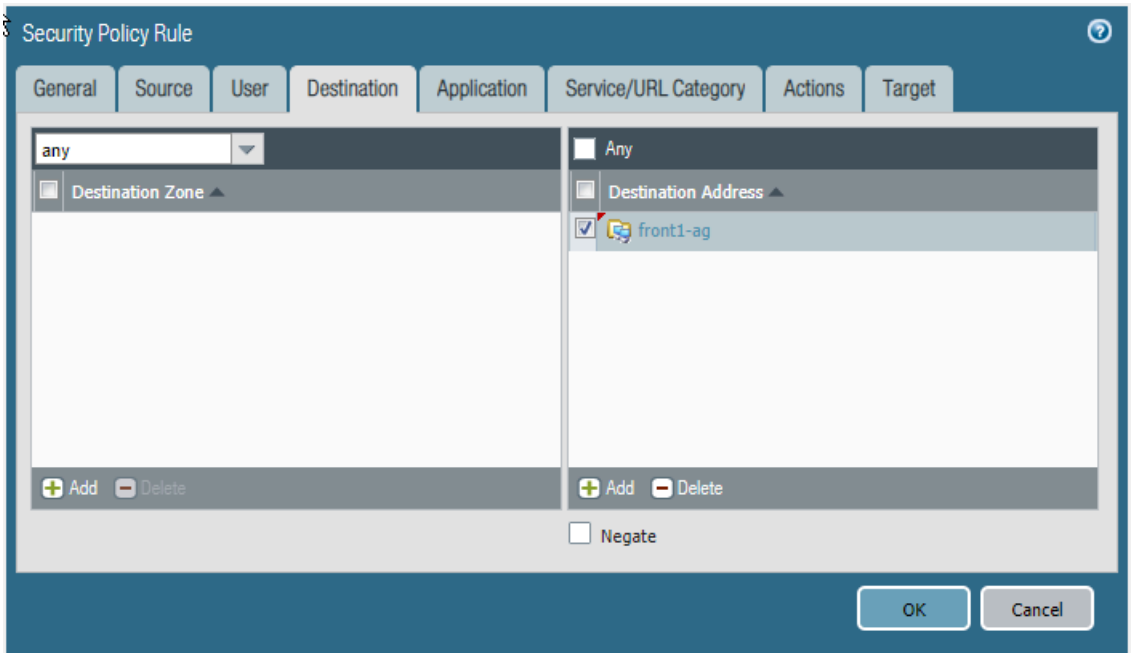
STEP 2 | Mettez à jour les règles UDR pour le sous-réseau de la passerelle d'application afin d'ajouter une route pour le CIDR de service, le saut suivant étant l'équilibreur de charge du pare-feu entrant du groupe de ressources du pare-feu Spoke.

Appliquer la politique au service AKS pertinent

STEP 1 | Dans Panorama, sélectionnez Policies (Politiques).

STEP 2 | Dans la liste **Device Group (Groupes de périphériques)**, choisissez le groupe de périphériques pour votre service AKS.

STEP 3 | Cliquez sur **Add (Ajouter)** pour ajouter une règle de politique de sécurité. Remplissez le formulaire et, dans l'onglet **Destination**, cliquez sur **Add (Ajouter)** pour ajouter l'adresse de destination ou le groupe d'adresses.



Déployer et sécuriser les services AKS

Ces étapes décrivent comment vous pouvez sécuriser le trafic entrant et sortant traversant les services Kubernetes en utilisant le pare-feu VM-Series et le plug-in Azure pour Panorama.

STEP 1 | Dans l'environnement de déploiement d'application, créez un fichier YAML pour l'application ou utilisez un fichier déjà existant. Voici un exemple de fichier YAML d'application :

```
apiVersion: apps/v1 kind: Deployment metadata:   name: azure-
vote-back spec:   replicas: 1   selector:     matchLabels:
       app: azure-vote-back   template:     metadata:       labels:
         app: azure-vote-back     spec:       containers:       -
 name: azure-vote-back         image: redis         resources:
```

 ©2023 Palo Alto Networks, Inc.

```
            requests:              cpu: 100m              memory:
 128Mi           limits:               cpu: 250m              memory:
 256Mi         ports:          - containerPort: 6379           name:
 redis --- apiVersion: v1 kind: Service metadata:   name: azure-
vote-back   labels:     service: backend spec:   ports:   - port:
 6379   selector:     app: azure-vote-back --- apiVersion: apps/
v1 kind: Deployment metadata:   name: azure-vote-front spec:
   replicas: 5   selector:     matchLabels:       app: azure-
vote-front   template:     metadata:       labels:          app:
 azure-vote-front     spec:       containers:       - name:
 azure-vote-front          image: microsoft/azure-vote-front:v1
         resources:            requests:              cpu: 100m
             memory: 128Mi           limits:              cpu: 250m
             memory: 256Mi         ports:          - containerPort:
 80         env:          - name: REDIS            value: "azure-
vote-back" --- apiVersion: v1 kind: Service metadata:   name:
 azure-vote-front   labels:     service: "azure-vote-front"
     type: "production"     providesecurity: "yes"     a:
 "value"     b: "value"     c: "value"     tier: "stagingapp"
   annotations:     service.beta.kubernetes.io/azure-load-balancer-
internal: "true" spec:   type: LoadBalancer   ports:   - port: 80
   selector:     app: azure-vote-front
```

STEP 2 | Modifiez votre fichier YAML pour étiqueter les services Kubernetes.

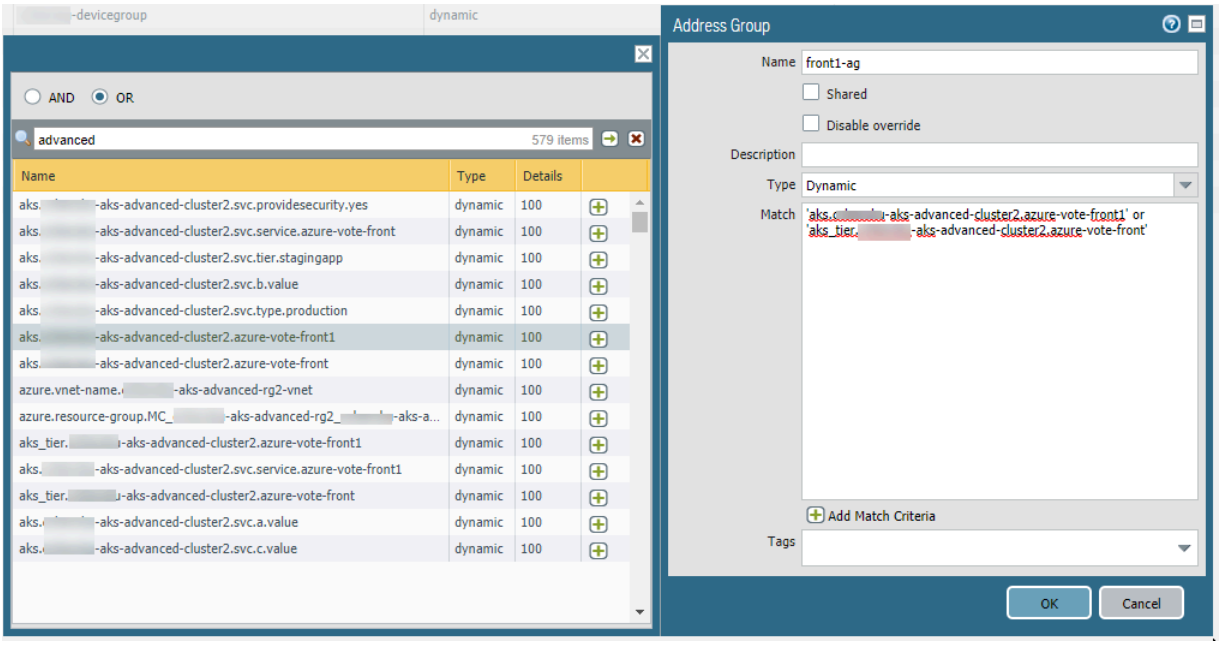
Les étiquettes permettent de créer le mappage étiquette-adresse IP correspondant lorsque vous utilisez le plug-in Panorama pour AKS pour vous connecter au cluster. Par exemple, dans l'exemple de fichier ci-dessus, recherchez les étiquettes d'application dans les métadonnées de service. Les voici : **`azure-vote-back`** and **`azure-vote-front`**.

STEP 3 | Dans votre cluster AKS, appliquez le fichier YAML.

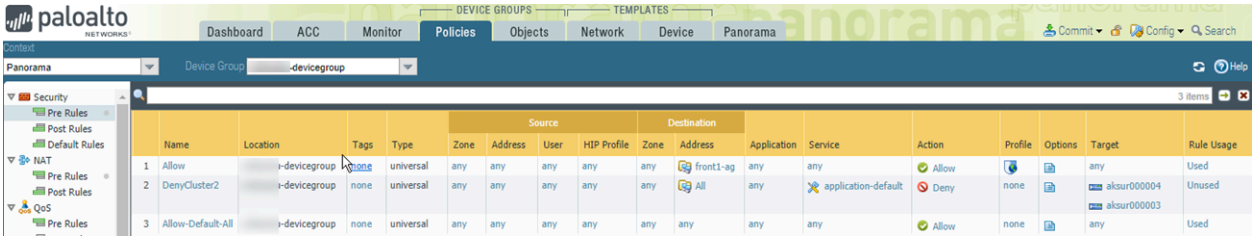
 ©2023 Palo Alto Networks, Inc.

STEP 4 | Dans Panorama, créez un groupe d'adresses en utilisant une étiquette de groupe de ressources.

1. Dans l'onglet **Objects (Objets)**, sélectionnez un groupe de périphériques dans la liste **Device Group (Groupe de périphériques)**.
2. Sélectionnez **Address Groups (Groupes d'adresses)** et cliquez sur **Add (Ajouter)** pour ajouter un groupe d'adresses.
   1. Spécifiez un nom et sélectionnez le type **Dynamic (Dynamique)**.
   2. Cliquez sur **Add (Ajouter)** pour ajouter des adresses. L'ajout engendre une fenêtre qui répertorie les adresses détectées. Le remplissage de la liste peut prendre plusieurs minutes.
   3. Vous pouvez choisir une ou plusieurs adresses pour les critères de correspondance. Sélectionnez AND (Et) ou OR (Ou) pour la relation des critères.
   4. Si vous avez plusieurs adresses, saisissez une chaîne dans la barre de recherche pour filtrer les résultats, comme le montre la figure suivante.
   5. Dans la liste d'adresses, cliquez sur le + pour inclure l'adresse dans les critères de correspondance de groupe d'adresses.
   6. Lorsque les critères de correspondance sont complets, cliquez sur **OK**.



STEP 5 | Affichez la politique utilisant le groupe d'adresses.



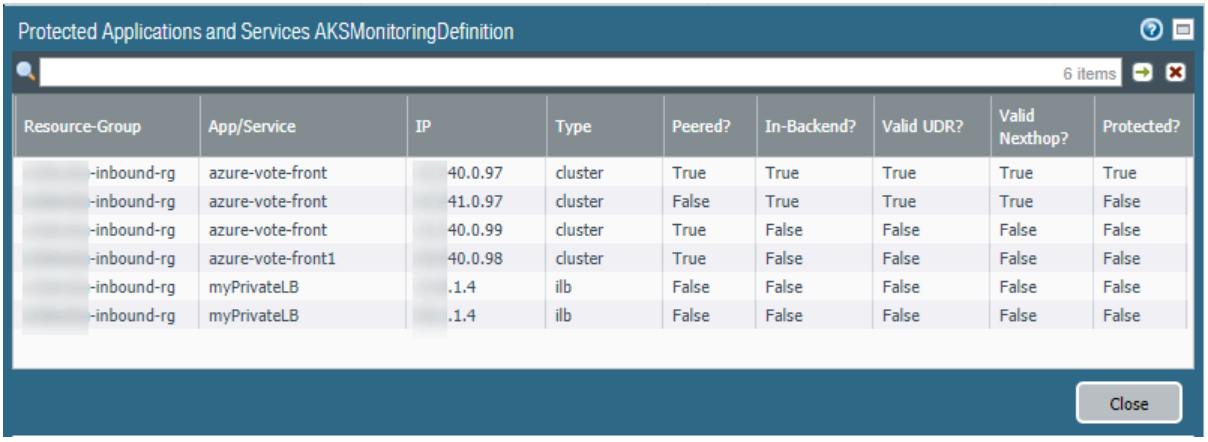
 ©2023 Palo Alto Networks, Inc.

STEP 6 | Affichez les services AKS sécurisés.

Dans **Panorama** > **Azure** > **Deployments (Déploiements)**, affichez votre définition de surveillance et, dans la colonne Action, sélectionnez le lien **Protected Applications and Services (Applications et services protégés)**.

La colonne **Protected? (Protégé ?)** résume l'état de sécurité de vos groupes de ressources. Le remplissage de la fenêtre peut prendre plusieurs minutes. Si vous avez de nombreux groupes de ressources, saisissez une chaîne dans la barre de recherche pour filtrer les résultats.

Ces résultats reposent sur la configuration du groupe de ressources Azure. Ils n'interrogent pas l'appartenance au groupe de périphériques ou à la pile de modèles.



 ©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur OpenStack

Le pare-feu VM-Series pour OpenStack vous permet de fournir une application sécurisée ainsi que la sécurité, les performances et la visibilité du réseau.

- Pare-feu VM-Series pour OpenStack
- Composants de VM-Series pour la solution OpenStack
- Modèle Heat pour un déploiement de passerelle de base
- Modèles Heat pour le chaînage de service et la mise à l'échelle de service
- Installation du pare-feu VM-Series dans un déploiement de passerelle de base
- Installation du pare-feu VM-Series avec mise à l'échelle ou chaînage de service

Déploiement VM-Series dans OpenStack

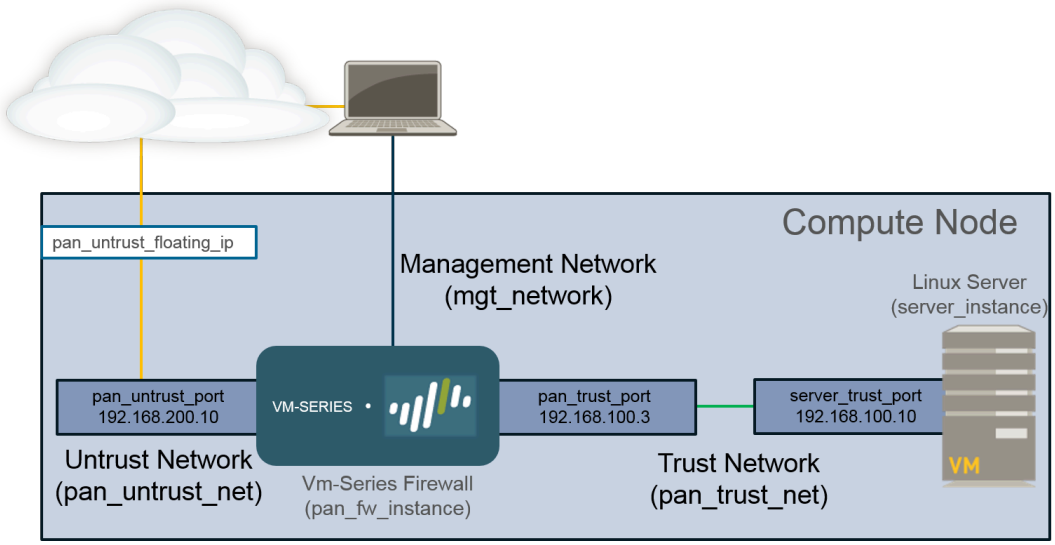
Les modèles Heat Orchestration fournis par Palo Alto Networks vous permettent de déployer le pare-feu VM-Series individuellement, via le chaînage de service, ou dynamiquement, avec la mise à l'échelle de service.

- Passerelle de base
- Chaînage de service et mise à l'échelle de service

Passerelle de base

Le pare-feu VM-Series pour OpenStack vous permet de déployer le pare-feu VM-Series sur l'hyperviseur KVM exécuté sur un nœud de calcul dans votre environnement OpenStack. Cette solution utilise les modèles Heat Orchestration et l'amorçage pour déployer le pare-feu VM-Series et un serveur Linux. Le pare-feu VM-Series protège le serveur Linux déployé en inspectant le trafic entrant et sortant du serveur. Les exemples de fichiers d'amorçage permettent au pare-feu VM-Series de démarrer avec une configuration de base pour gérer le trafic.

Ces fichiers de modèle Heat et les fichiers d'amorçage se combinent pour créer deux machines virtuelles, le pare-feu VM-Series et le serveur Linux, dans une configuration réseau similaire à celle illustrée ci-dessous.



Chaînage de service et mise à l'échelle de service

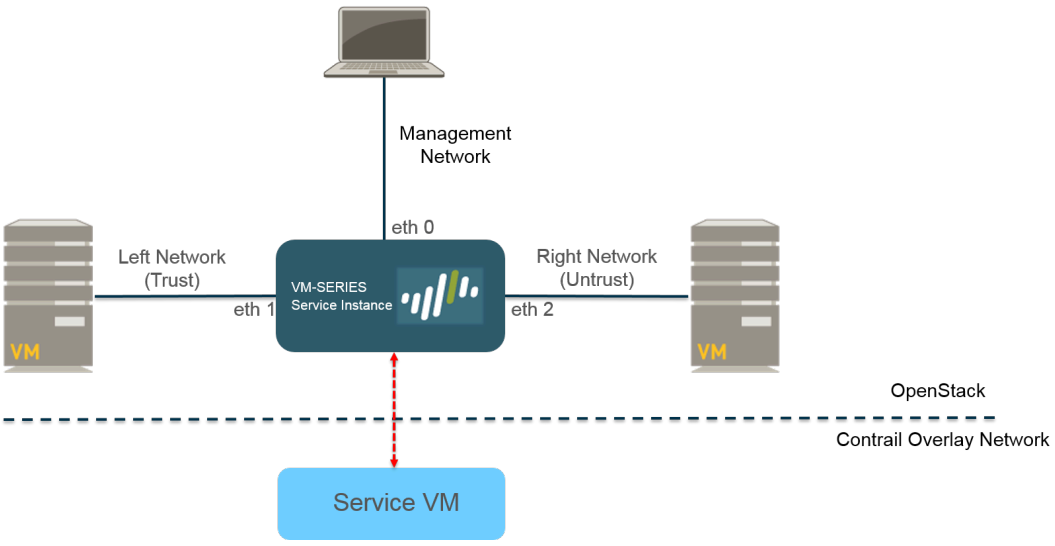
Le déploiement du pare-feu VM-Series par le biais du chaînage de service ou de la mise à l'échelle de service n'est pas pris en charge par OpenStack Queens.

Le chaînage de service est une fonctionnalité Contrail qui déploie un pare-feu VM-Series en tant qu'instance de service dans votre environnement OpenStack. Une chaîne de service est un ensemble de machines virtuelles de service, telles que des pare-feu ou des équilibreurs de charge, et chaque machine virtuelle de la chaîne de service est une instance de service. La mise à l'échelle de service vous permet de déployer dynamiquement des instances supplémentaires du pare-feu VM-Series.

©2023 Palo Alto Networks, Inc.

À l'aide des métriques d'utilisation du processeur ou d'octets entrants par seconde collectées par Ceilometer, OpenStack déploie ou arrête des instances supplémentaires du pare-feu VM-Series pour répondre aux besoins actuels de votre réseau.

Le pare-feu VM-Series de la solution OpenStack s'appuie sur des modèles Heat Orchestration pour configurer et déployer les composants requis pour le chaînage de service et la mise à l'échelle de service. Les modèles Heat fournis par Palo Alto Networks créent un modèle de service, une instance de service et une politique de service (pour diriger le trafic vers le pare-feu VM-Series) afin de déployer deux serveurs Linux et l'instance de pare-feu VM-Series.



 ©2023 Palo Alto Networks, Inc.

Composants de VM-Series pour la solution OpenStack

Le pare-feu VM-Series dans un environnement OpenStack a été testé avec les composants suivants.

Composant	Description
Logiciels	Reportez-vous à la matrice de compatibilité pour plus d'informations sur les versions logicielles prises en charge.
Ressources du matériel VM-Series	Reportez-vous à la section Configuration système requise pour VM-Series pour la configuration matérielle minimale requise pour votre modèle VM-Series. Dans OpenStack, les versions définissent le processeur, la mémoire et la capacité de stockage d'une instance de calcul. Lors de la configuration de votre modèle Heat, choisissez la version de calcul qui respecte ou dépasse la configuration matérielle requise pour le modèle VM-Series.
Fuel Master	Fuel est un outil de déploiement et de gestion basé sur l'interface utilisateur pour OpenStack.
OpenStack Controller	Ce nœud exécute la plupart des services OpenStack partagés, tels que l'API et la planification. En outre, l'interface utilisateur Horizon s'exécute sur ce nœud.
OpenStack Compute	Le nœud de calcul contient les machines virtuelles, y compris le pare-feu VM-Series, dans le déploiement OpenStack. Le nœud de calcul qui héberge VM-Series doit répondre aux critères suivants : • Type d'instance OS::Nova::Server • Autoriser la configuration d'au moins trois interfaces • Accepter l'image qcow2 de VM-Series • Accepter le paramètre de version de calcul ***Installez le nœud de calcul OpenStack sur un serveur nu, car le pare-feu VM-Series ne prend pas en charge la virtualisation imbriquée.***
Contrail Controller	Le nœud de contrôleur Contrail est un contrôleur de réseau défini par logiciel utilisé pour la gestion, le contrôle et l'analyse pour le réseau virtualisé. Il fournit des informations de routage aux nœuds de passerelle et de calcul. De plus, le contrôleur Contrail fournit la prise en charge nécessaire pour le chaînage de service et la mise à l'échelle de service.

©2023 Palo Alto Networks, Inc.

Composant	Description
Contrail Gateway	Le nœud de passerelle Contrail fournit une connectivité IP aux réseaux externes à partir de réseaux virtuels. Les MPLS sur les tunnels GRE de machines virtuelles se terminent au nœud de passerelle, où les paquets sont décapsulés et envoyés à leurs destinations sur les réseaux IP.
Ceilometer (télémétrie OpenStack)	Dans le cas du pare-feu VM-Series pour OpenStack, Ceilometer surveille l'utilisation du processeur pour la mise à l'échelle de service. Lorsque l'utilisation du processeur respecte les seuils définis, une nouvelle instance de service du pare-feu VM-Series est déployée ou arrêtée.
Fichiers de modèles Heat Orchestration	Palo Alto Networks fournit un exemple de modèle Heat pour le déploiement du pare-feu VM-Series. Ce modèle est constitué d'un modèle principal et d'un modèle d'environnement. Ces fichiers instancient une instance VM-Series avec une interface de gestion et deux interfaces de données. Dans un déploiement de passerelle de base, le modèle instancie un serveur Linux avec une interface. L'interface du serveur se connecte au réseau privé créé par le modèle. Dans un déploiement de chaînage ou de mise à l'échelle de service, les modèles instancient deux serveurs Linux avec un serveur attaché à chaque interface de données du pare-feu.
Fichiers d'amorçage du pare-feu VM-Series	Les fichiers d'amorçage du pare-feu VM-Series se composent d'un fichier init-cfg.txt, d'un fichier bootstrap.xml et de codes d'autorisation VM-Series. Avec les fichiers de modèle Heat, Palo Alto Networks fournit un exemple de fichiers init-cfg.txt et bootstrap.xml. Vous devez fournir vos propres codes d'autorisation pour la licence de votre pare-feu VM-Series et l'activation des abonnements. Reportez-vous à la section Amorçage du pare-feu VM-Series pour plus d'informations sur les fichiers d'amorçage VM-Series.

©2023 Palo Alto Networks, Inc.

Modèle Heat pour un déploiement de passerelle de base

Le fichier de modèle Heat inclut les quatre fichiers suivants pour vous aider à lancer le pare-feu VM-Series sur KVM dans OpenStack. Les quatre fichiers sont requis pour déployer le pare-feu VM-Series et le serveur Linux.

- **pan_basic_gw.yaml** — Définit les ressources créées pour prendre en charge le pare-feu VM-Series et le serveur Linux sur le nœud de calcul, telles que les interfaces et les adresses IP.
- **pan_basic_gw_env.yaml** : ce fichier d'environnement définit l'environnement dans lequel se trouvent le pare-feu VM-Series et les serveurs Linux. De nombreux paramètres du fichier pan_basic_gw.yaml référencent les paramètres définis dans ce fichier, tels que la version de VM-Series et le serveur Linux.
- **init-cfg.txt** — Inclut la commande opérationnelle pour activer DHCP sur l'interface de gestion du pare-feu.
- **bootstrap.xml** — Fournit la configuration de base pour le pare-feu VM-Series. Le fichier bootstrap.xml configure les interfaces de données et les adresses IP. Ces valeurs doivent correspondre aux valeurs correspondantes dans le fichier pan_basic_gw.yaml.

  En outre, le fichier bootstrap.xml inclut une règle NAT appelée untrust2trust. Cette règle convertit le port approuvé sur le serveur en port non approuvé du pare-feu VM-Series.

Vous avez deux options pour transmettre les fichiers d'amorçage à OpenStack : l'injection de fichiers (fichiers de personnalité) ou les données utilisateur.



L'injection de fichiers n'est plus prise en charge à partir d'OpenStack Queens. Vous devez utiliser les données utilisateur à la place.

Le tableau ci-dessous décrit les ressources créées par le fichier de modèle pan_basic_gw.yaml et fournit la valeur par défaut, le cas échéant.

Ressource	Description
pan_fw_instance	Un pare-feu VM-Series avec une interface de gestion et deux interfaces de données.
server_instance	Un serveur Linux avec une seule interface.
pan_trust_net	Une connexion au réseau interne auquel l'interface approuvée du pare-feu et l'interface approuvée du serveur sont associées.
pan_trust_subnet	Sous-réseau associé à l'interface approuvée sur le pare-feu (pan_trust_net) et a une valeur CIDR de 192.168.100.0/24.
pan_untrust_net	Réseau non approuvé auquel le port non approuvé du pare-feu est associé.
pan_untrust_subnet	Sous-réseau associé à l'interface non approuvée du pare-feu (pan_untrust_net) et a une valeur CIDR de 192.168.200.0/24.

©2023 Palo Alto Networks, Inc.

Ressource	Description
allow_ssh_https_icmp_secgroup	Groupe de sécurité qui autorise TCP sur les ports 22 et 443 et le trafic ICMP.
pan_untrust_port	Le port non approuvé du pare-feu VM-Series déployé en mode couche 3. Le modèle Heat fournit une adresse IP par défaut de 192.168.200.10 à ce port. Si vous modifiez cette adresse IP dans le modèle Heat, vous devez modifier l'adresse IP dans le fichier bootstrap.xml.
pan_untrust_floating_ip	Une adresse IP flottante affectée à partir du réseau public_network.
pan_untrust_floating_ip_assoc	Cela associe la pan_untrust_floating_ip au pan_untrust_port.
pan_trust_port	Le port approuvé du mode couche 3 du pare-feu VM-Series.
server_trust_port	Le port approuvé du mode couche 3 du serveur Linux. Le modèle Heat fournit une adresse IP par défaut de 192.168.100.10 à ce port. Si vous modifiez cette adresse IP dans le modèle Heat, vous devez modifier l'adresse IP dans le fichier bootstrap.xml.

Le fichier pan_basic_gw.yaml référence le fichier pan_basic_gw_env.yaml pour la plupart des valeurs nécessaires à la création des ressources nécessaires au déploiement du pare-feu VM-Series et du serveur Linux. Le fichier d'environnement de modèle Heat contient les paramètres suivants.

Paramètre	Description
mgmt_network	L'interface de gestion du pare-feu VM-Series se connecte au réseau spécifié dans ce paramètre. Le modèle ne crée pas le réseau de gestion. Vous devez le créer avant de déployer les modèles Heat. La valeur par défaut est mgmt_ext_net.
public_network	Adresses que le cluster OpenStack et les machines virtuelles du cluster utilisent pour communiquer avec le réseau externe ou public. Le réseau public fournit des adresses IP virtuelles pour les points de terminaison publics, qui sont utilisées pour se connecter aux API de services OpenStack. Le modèle ne crée pas le réseau public. Vous devez le créer avant de déployer les modèles Heat. La valeur par défaut est public_net.
pan_image	Ce paramètre spécifie l'image de base VM-Series utilisée par le modèle Heat lors du déploiement du pare-feu VM-Series. La valeur par défaut est pa-vm-7.1.4.
pan_flavor	Ce paramètre définit les ressources matérielles allouées au pare-feu VM-Series. La valeur par défaut est m1.medium. Cette valeur correspond à

©2023 Palo Alto Networks, Inc.

Paramètre	Description
	la configuration système requise pour VM-Series décrite dans le chapitre Configuration du pare-feu VM-Series sur KVM.
server_image	Ce paramètre indique au modèle Heat quelle image utiliser pour le serveur Linux. La valeur par défaut est Ubuntu-14.04.
server_flavor	Ce paramètre définit les ressources matérielles allouées au serveur Linux. La valeur par défaut est m1.small.
server_key	La clé du serveur est utilisée pour accéder au serveur Linux via SSH. La valeur par défaut est server_key. Vous pouvez modifier cette valeur en entrant une nouvelle clé de serveur dans le fichier d'environnement.

©2023 Palo Alto Networks, Inc.

Modèles Heat pour le chaînage de service et la mise à l'échelle de service

Le déploiement du pare-feu VM-Series par le biais du chaînage de service ou de la mise à l'échelle de service n'est pas pris en charge par OpenStack Queens.

Le fichier d'environnement de modèle Heat définit les paramètres spécifiques à l'instance de pare-feu VM-Series déployée via le chaînage de service ou la mise à l'échelle de service. Les paramètres définis dans le fichier d'environnement sont divisés en sections décrites ci-dessous. Il existe deux versions des modèles Heat pour le chaînage de service (vwire et L3), et une pour la mise à l'échelle de service.

Le chaînage de service nécessite les fichiers de modèle Heat et deux fichiers d'amorçage pour lancer l'instance de service de pare-feu VM-Series et deux serveurs Linux dans les réseaux gauche et droit.

- **Fichiers de modèle** : ce modèle définit les ressources créées pour prendre en charge le pare-feu VM-Series et deux serveurs Linux, tels que les interfaces et les adresses IP.
  - service_chaining_template_vm.yaml pour les déploiements vwire.
  - service_chaining_template_L3.yaml pour les déploiements L3.
  - service_scaling_template.yaml pour les déploiements de mise à l'échelle des services.
- **Fichier d'environnement** : ce fichier d'environnement définit l'environnement dans lequel se trouvent le pare-feu VM-Series et les serveurs Linux. De nombreux paramètres du modèle font référence aux paramètres définis dans ce fichier, tels que la version de VM-Series et les noms des serveurs Linux.
  - service_chaining_env_vm.yaml pour les déploiements vwire.
  - service_chaining_env_L3.yaml pour les déploiements L3.
  - service_scaling_env.yaml pour les déploiements de mise à l'échelle des services.
- **service_instance.yaml** (mise à l'échelle de service uniquement) : il s'agit d'un modèle Heat imbriqué référencé par Service_Scaling_template.yaml pour déployer l'instance de service. Il fournit les informations nécessaires pour déployer des instances de service pour la mise à l'échelle des événements.
- **init-cfg.txt** : fournit les informations minimales requises pour amorcer un pare-feu VM-Series. Le fichier init-cfg.txt fourni inclut uniquement la commande opérationnelle pour activer DHCP sur l'interface de gestion du pare-feu.
- **<file_name>_bootstrap.xml** : fournit la configuration de base pour le pare-feu VM-Series. Le fichier bootstrap.xml configure les interfaces de données. Ces valeurs doivent correspondre aux valeurs correspondantes dans les fichiers de modèles Heat.

Pour plus d'informations sur les fichiers init-cfg.txt et bootstrap.xml, reportez-vous à la section Fichiers de configuration d'amorçage.

Les tableaux suivants décrivent les paramètres du fichier d'environnement.

- Réseau virtuel
- Machine virtuelle

 ©2023 Palo Alto Networks, Inc.

- Modèle de service
- Instance de service
- IPAM
- Politique de service
- Alarme

Réseau virtuel

Les paramètres de configuration de réseau virtuel dans le fichier d'environnement de modèle Heat définissent le réseau virtuel qui connecte le pare-feu VM-Series et les deux serveurs Linux déployés par le modèle Heat.

Réseau virtuel (VN Config)	
management_network	L'interface de gestion du pare-feu VM-Series se connecte au réseau spécifié dans ce paramètre.
left_vn ou left_network	Nom du réseau virtuel gauche.
right_vn ou right_network	Nom du réseau virtuel droit.
left_vn_fqdn	Nom de domaine complet du réseau virtuel gauche.
right_vn_fqdn	Nom de domaine complet du réseau virtuel droit.
route_target	Modifiez cette valeur afin que la configuration de la cible d'itinéraire corresponde à celle de votre passerelle externe.

Machine virtuelle

Les paramètres de la machine virtuelle définissent les serveurs Linux gauche et droit. Le nom du tuple de port est défini ici et référencé par le modèle Heat. Dans Contrail, un tuple de port est un ensemble ordonné d'interfaces réseau virtuelles connectées à la même machine virtuelle. Avec un tuple de port, vous pouvez créer des ports et transmettre ces informations lors de la création d'une instance de service. Le modèle Heat crée les ports gauche, droit et de gestion, et les ajoute au tuple de port. Le tuple de port est ensuite lié à l'instance de service. Lorsque vous lancez l'instance de service à l'aide des modèles Heat, le tuple de port mappe la machine virtuelle de service sur la machine virtuelle déployée dans OpenStack.

Machine virtuelle (VM Config)	
flavor	La version des machines virtuelles gauche et droite. La valeur par défaut est m1.small.

©2023 Palo Alto Networks, Inc.

Machine virtuelle (VM Config)	
left_vm_image ou right_vm_image ou image	Le nom de l'image logicielle pour les machines virtuelles gauche et droite. Modifiez cette valeur pour qu'elle corresponde au nom de fichier de l'image téléchargée. La valeur par défaut est TestVM, qui est une image par défaut fournie par OpenStack.
svm_name	Le nom appliqué au pare-feu VM-Series.
left_vm_name et right_vm_name	Le nom des machines virtuelles gauche et droite.
port_tuple_name	Le nom du tuple de port utilisé par les deux serveurs Linux et le pare-feu VM-Series.
server_key	La clé du serveur est utilisée pour accéder aux machines virtuelles via SSH. La valeur par défaut est server_key. Vous pouvez modifier cette valeur en entrant une nouvelle clé de serveur dans le fichier d'environnement.

Modèle de service

Le modèle de service définit les paramètres de l'instance de service, tels que l'image logicielle, l'architecture de la machine virtuelle, le type de service et les interfaces. Les modèles de service sont configurés dans les limites d'un domaine et peuvent être utilisés sur tous les projets du domaine spécifié.

Modèle de service (ST Config)	
S_Tmp_name	Le nom du modèle de service.
S_Tmp_version	La version du modèle de service. La valeur par défaut est 2. Ne modifiez pas ce paramètre, car le modèle de service version 2 est requis pour prendre en charge les tuples de port.
S_Tmp_service_mode	Le mode de service est le mode réseau utilisé par l'instance de service de pare-feu VM-Series. Pour le modèle de réseau L3, la valeur par défaut est in-network. Pour le modèle de câble virtuel, la valeur par défaut est transparent.
S_Tmp_service_type	Le type de service déployé par le modèle. La valeur par défaut est firewall et ne doit pas être modifiée lors du déploiement du pare-feu VM-Series.
S_Tmp_image_name	Ce paramètre spécifie l'image de base VM-Series utilisée par le modèle Heat lors du déploiement du pare-feu VM-Series. Modifiez ce paramètre

©2023 Palo Alto Networks, Inc.

Modèle de service (ST Config)	
	pour qu'il corresponde au nom de l'image de pare-feu VM-Series téléchargée dans votre environnement OpenStack.
S_Tmp_flavor	Ce paramètre définit les ressources matérielles allouées au pare-feu VM-Series. La valeur par défaut est m1.large.
S_Tmp_interface_type_mgmt S_Tmp_interface_type_left S_Tmp_interface_type_right	Ces paramètres définissent le type d'interface pour les interfaces de gestion, gauche et droite.
domain	Le domaine dans lequel ce modèle de service est lié. La valeur par défaut est default-domain.

Instance de service

La partie d'instance de service du fichier d'environnement de modèle Heat fournit le nom de l'instance individuelle déployée par le modèle Heat et le modèle de service.

Instance de service (SI Config)	
S_Ins_name	Le nom de l'instance de service. Il s'agit du nom de l'instance de pare-feu VM-Series dans Contrail.
S_Ins_fq_name	Le nom complet de l'instance de service.

IPAM

La gestion d'adresse IP (IPAM) fournit les informations d'adresse IP pour les interfaces de l'instance de service. Modifiez ces paramètres pour mieux les adapter à votre environnement.

IPAM (IPAM Config)	
NetIPam_ip_prefix_mgmt	Le préfixe IP de l'interface de gestion sur le pare-feu VM-Series. La valeur par défaut est 172.2.0.0.
NetIPam_ip_prefix_len_mgmt	La longueur du préfixe IP de l'interface de gestion sur le pare-feu VM-Series. La valeur par défaut est /24.
NetIPam_ip_prefix_left	Le préfixe IP de l'interface gauche sur le pare-feu VM-Series. La valeur par défaut est 10.10.1.0.
NetIPam_ip_prefix_len_left	La longueur du préfixe IP de l'interface gauche sur le pare-feu VM-Series. La valeur par défaut est /24.

©2023 Palo Alto Networks, Inc.

IPAM (IPAM Config)	
NetIPam_ip_prefix_right	Le préfixe IP de l'interface droite sur le pare-feu VM-Series. La valeur par défaut est 10.10.2.0.
NetIPam_ip_prefix_len_right	La longueur du préfixe IP de l'interface droite sur le pare-feu VM-Series. La valeur par défaut est /24.
NetIPam_addr_from_start_right	Ce paramètre détermine comment les adresses IP sont affectées aux machines virtuelles sur les sous-réseaux décrits ci-dessus. Si la valeur est true (vrai), toute nouvelle machine virtuelle prend l'adresse IP disponible suivante. Si la valeur est false (faux), toute nouvelle machine virtuelle reçoit une adresse IP au hasard. La valeur par défaut est true (vrai).

Politique de service

La politique de service définit les règles de redirection de trafic et la politique qui renvoient le trafic passant entre les machines virtuelles gauche et droite vers l'instance de service du pare-feu VM-Series.

Politique de service (Policy Config)	
policy_name	Le nom de la politique de service dans Contrail qui redirige le trafic via le pare-feu VM-Series. Pour le modèle L3, la valeur par défaut est PAN_SVM_policy-L3. Pour le modèle de câble virtuel, la valeur par défaut est PAN_SVM_policy-vw.
policy_fq_name	Le nom complet qualifié de la politique de service.
simple_action	L'action par défaut de Contrail s'applique au trafic allant vers l'instance de service du pare-feu VM-Series. La valeur par défaut est pass, car le pare-feu VM-Series applique sa propre politique de sécurité au trafic.
protocol	Les protocoles autorisés par Contrail à passer au pare-feu VM-Series. La valeur par défaut est any (tout).
src_port_end et src_port_start	Utilisez ce paramètre pour spécifier le ou les ports sources à associer à la règle de politique. Vous pouvez saisir un seul port, une liste de ports séparés par des virgules ou une plage de ports sous la forme <port>-<port>. La valeur par défaut est -1 dans les modèles Heat fournis, ce qui signifie tout port source.
direction	Ce paramètre définit la direction du trafic autorisé par Contrail à passer au pare-feu VM-Series. La valeur par défaut est <> ou trafic bidirectionnel.

©2023 Palo Alto Networks, Inc.

Politique de service (Policy Config)	
dst_port_end et dst_port_start	Utilisez ce paramètre pour spécifier le ou les ports de destination devant être associés à la règle de politique. Vous pouvez saisir un seul port, une liste de ports séparés par des virgules ou une plage de ports sous la forme <port>-<port>. La valeur par défaut est -1 dans les modèles Heat fournis, ce qui signifie tout port de destination.

Alarme

Les paramètres d'alarme sont utilisés dans la mise à l'échelle de service et ne sont pas inclus dans les fichiers d'environnement de chaînage de service. Ces paramètres définissent les seuils utilisés par Contrail pour déterminer quand la mise à l'échelle doit avoir lieu. Cet ensemble de paramètres est uniquement utilisé pour le modèle Heat de mise à l'échelle de service.

La durée d'attente par défaut configurée sous les paramètres cooldown est destinée à permettre au pare-feu de démarrer. Si vous modifiez les valeurs d'attente, laissez suffisamment de temps à chaque nouvelle instance de pare-feu pour démarrer.

Alarme	
meter_name	La métrique surveillée par Ceilometer et utilisée par Contrail pour déterminer quand un pare-feu VM-Series supplémentaire doit être déployé ou réduit. Le modèle Heat utilise l'utilisation du processeur ou les octets par seconde comme métriques pour la mise à l'échelle du service.
cooldown_initial	Le délai d'attente de Contrail avant le lancement d'une instance de service supplémentaire après le lancement de l'instance de service initiale. La valeur par défaut est 1 200 secondes.
cooldown_scaleup	La durée pendant laquelle Contrail attend entre le lancement de l'instance de service supplémentaire après le lancement de l'instance du premier service d'extension. La valeur par défaut est 1 200 secondes.
cooldown_scaledown	La durée pendant laquelle Contrail attend entre la fermeture des instances de service supplémentaires après l'arrêt de la première instance de service d'extension. La valeur par défaut est 1 200 secondes.
period_high	L'intervalle pendant lequel la charge moyenne du processeur est calculée comme étant élevée avant de déclencher une alarme. La valeur par défaut est 300 secondes.
period_low	L'intervalle pendant lequel la charge moyenne du processeur est calculée comme étant faible avant de déclencher une alarme. La valeur par défaut est 300 secondes.

©2023 Palo Alto Networks, Inc.

Alarme	
threshold_high	La valeur de l'utilisation du processeur en pourcentage ou en octets par seconde référencée par Contrail avant le lancement d'un événement d'extension. La valeur par défaut est 40 % d'utilisation du processeur ou 2 800 octets par seconde.
threshold_low	La valeur de l'utilisation du processeur en pourcentage ou en octets par seconde référencée par Contrail avant de lancer un événement de réduction. La valeur par défaut est 20 % d'utilisation du processeur ou 12 000 octets par seconde.

©2023 Palo Alto Networks, Inc.

Installation du pare-feu VM-Series dans un déploiement de passerelle de base

Effectuez les étapes suivantes pour préparer les modèles Heat, les fichiers d'amorçage et les images logicielles nécessaires au déploiement du pare-feu VM-Series dans OpenStack. Après avoir préparé les fichiers, déployez le pare-feu VM-Series et le serveur Linux.

STEP 1 | Téléchargez les fichiers du modèle Heat et d'amorçage.

Téléchargez le package du fichier du modèle Heat à partir du référentiel GitHub.

STEP 2 | Téléchargez l'image VM-Series de base.

1. Connectez-vous au portail de support client de Palo Alto Networks.
2. Sélectionnez **Software Updates (Mises à jour logicielles)** et choisissez **PAN-OS for VM-Series KVM Base Images (PAN-OS pour les images de base KVM VM-Series)** du menu déroulant **Filter By (Filtrer par)**.
3. Téléchargez le fichier **qcow2** de VM-Series pour KVM.

STEP 3 | Téléchargez Ubuntu 14.04 et chargez l'image sur le contrôleur OpenStack.

Le modèle Heat nécessite une image Ubuntu pour lancer le serveur Linux.

1. Téléchargez Ubuntu 14.04.
2. Connectez-vous à l'interface utilisateur Horizon.
3. Sélectionnez **Project (Projet)** > **Compute (Calcul)** > **Images** > **Create Image (Créer une image)**.
4. Donnez un **Name (Nom)** à l'image Ubuntu 14.04 afin qu'il corresponde au paramètre dans le fichier pan_basic_gw_env.yaml.
5. Définissez la source d'image sur **Image File (Fichier image)**.
6. Cliquez sur **Choose File (Choisir le fichier)** et naviguez vers votre fichier image Ubuntu.
7. Définissez le format afin qu'il corresponde au format de fichier de votre image Ubuntu.
8. Cliquez sur **Create Image (Créer une image)**.

STEP 4 | Chargez VM-Series pour l'image de base KVM sur le contrôleur OpenStack.

1. Connectez-vous à l'interface utilisateur Horizon.
2. Sélectionnez **Project (Projet)** > **Compute (Calcul)** > **Images** > **Create Image (Créer une image)**.
3. **Name (Nommez)** l'image pour qu'elle corresponde au nom de l'image dans votre modèle Heat.
4. Définissez la source d'image sur **Image File (Fichier image)**.
5. Cliquez sur **Choose File (Choisir le fichier)** et accédez à votre fichier image VM-Series.
6. Définissez le format sur **QCOW2-QEMU Emulator**.
7. Cliquez sur **Create Image (Créer une image)**.

©2023 Palo Alto Networks, Inc.

STEP 5 | Chargez les fichiers d'amorçage. Vous avez deux options pour transmettre les fichiers d'amorçage à OpenStack : l'injection de fichiers (fichiers de personnalité) ou les données utilisateur. Pour transmettre les fichiers d'amorçage en utilisant les données utilisateur, vous devez placer les fichiers dans une archive tar (fichier .tgz) et l'encoder avec base64.

L'injection de fichiers n'est plus prise en charge à partir d'OpenStack Queens. Vous devez utiliser les données utilisateur à la place.

- Pour l'injection de fichiers, chargez les fichiers init-cfg.txt et bootstrap.xml ainsi que vos codes d'autorisation VM-Series sur votre contrôleur OpenStack ou sur un serveur Web auquel le contrôleur OpenStack peut accéder.
- Si vous utilisez la méthode **--user-data** pour transmettre l'ensemble d'amorçage au lecteur de configuration (config-drive), vous pouvez utiliser la commande suivante pour créer l'archive tar et l'encoder (fichier .tgz) avec base64 :

```
tar -cvzf <file-name>.tgz config/ license software content base64
 -i <in-file> -o <outfile>
```

STEP 6 | Modifiez le modèle pan_basic_gw.yaml pour qu'il renvoie vers les fichiers d'amorçage et les codes d'autorisation.

- Si vous utilisez les fichiers de personnalité, spécifiez le chemin du fichier ou l'adresse du serveur Web à l'emplacement de vos fichiers sous Personality (Personnalité). Supprimez les commentaires des lignes que vous n'utilisez pas.

```
  pan_fw_instance: type: OS::Nova::Server properties: image:
 { get_param: pan_image } flavor: { get_param: pan_flavor }
 networks: - network: { get_param: mgmt_network } - port:
 { get_resource: pan_untrust_port } - port: { get_resource:
 pan_trust_port } user_data_format: RAW config_drive: true
 personality: /config/init-cfg.txt: {get_file: "/opt/pan_bs/
init-cfg.txt"} # /config/init-cfg.txt: { get_file: "http://
web_server_name_ip/pan_bs/init-cfg.txt" } /config/bootstrap.xml:
 {get_file: "/opt/pan_bs/bootstrap.xml"} # /config/bootstrap.xml:
 { get_file: "http://web_server_name_ip/pan_bs/bootstrap.xml" } /
license/authcodes: {get_file: "/opt/pan_bs/authcodes"} # /
license/authcodes: {get_file: "http://web_server_name_ip/pan_bs/
authcodes"}
```

- Si vous utilisez les données utilisateur, spécifiez le chemin du fichier ou l'adresse du serveur Web à l'emplacement de vos fichiers sous User_data (Sonnées utilisateur). Si vous avez plus d'un

```
pan_fw_instance: type: OS::Nova::Server properties: image:
 { get_param: pan_image } flavor: { get_param: pan_flavor }
 networks: - port: { get_resource: mgmt_port } - port:
 { get_resource: pan_untrust_port } - port: { get_resource:
 pan_trust_port } user_data_format: RAW config_drive: true
 user_data: # get_file: http://10.0.2.100/pub/repository/panos/
images/openstack/userdata/boot.tgz get_file: /home/stack/newhot/
bootfiles.tgz
```

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Modifiez le fichier d'environnement du modèle pan_basic_gw_env.yaml en fonction de votre environnement. Assurez-vous que les valeurs de réseau public et de gestion correspondent à celles que vous avez créées dans votre environnement OpenStack. Définissez le paramètre pan_image pour qu'il corresponde au nom que vous avez attribué au fichier image de base VM-Series. Vous pouvez également changer votre clé de serveur ici.

```
root@node-2:~# cat basic_gateway/pan_basic_gw_env.yaml parameters:
 mgmt_network: mgmt_ext_net public_network: public_net pan_image:
 pa-vm-image pan_flavor: m1.medium server_image: Ubuntu-14.04
 server_flavor: m1.small server_key: server_key
```

STEP 8 | Déployez le modèle Heat.

1. Exécuter la commande **source openrc**
2. Exécutez la commande **heat stack-create <*stack-name*> -f <*template*> -e ./<*env-template*>**

```
root@node-2:~# heat stack-create stack1 -f pan_basic_gw.yaml -e pan_basic_gw_env.yaml
+--------------------------------------+------------+--------------------+---------------------+--------------+
| id                                   | stack_name | stack_status       | creation_time       | updated_time |
+--------------------------------------+------------+--------------------+---------------------+--------------+
| ebe40f9d-2781-4bb2-b246-f15c761f9045 |   stack1   | CREATE_IN_PROGRESS | 2017-01-25T13:36:59 | None         |
+--------------------------------------+------------+--------------------+---------------------+--------------+
```

STEP 9 | Vérifiez que votre pare-feu VM-Series a été déployé avec succès.

Vous pouvez utiliser les commandes suivantes pour vérifier l'état de création de la pile.

- Vérifier l'état de la pile avec **heat stack-list**
- Voir une liste détaillée des événements qui se sont produits pendant la création de la pile **heat event-list**
- Vérifier l'état de la pile avec **heat stack-show**

STEP 10 | Vérifiez que le pare-feu VM-Series inspecte de manière bidirectionnelle le trafic accédant au serveur Linux.

1. Connectez-vous au pare-feu.
2. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)** pour afficher la session SSH.

 ©2023 Palo Alto Networks, Inc.

Installation du pare-feu VM-Series avec mise à l'échelle ou chaînage de service

Effectuez les étapes suivantes pour préparer les modèles Heat, les fichiers d'amorçage et les images logicielles nécessaires au déploiement du pare-feu VM-Series. Après avoir préparé les fichiers, déployez le service de pare-feu VM-Series et deux serveurs Linux.

Le déploiement du pare-feu VM-Series par le biais du chaînage de service ou de la mise à l'échelle de service n'est pas pris en charge par OpenStack Queens.

STEP 1 | Téléchargez les fichiers du modèle Heat et d'amorçage.

Téléchargez le package du fichier du modèle Heat à partir du référentiel GitHub.

STEP 2 | Téléchargez l'image VM-Series de base.

1. Connectez-vous au portail de support client de Palo Alto Networks.
2. Sélectionnez **Software Updates (Mises à jour logicielles)** et choisissez **PAN-OS for VM-Series KVM Base Images (PAN-OS pour les images de base KVM VM-Series)** du menu déroulant **Filter By (Filtrer par)**.
3. Téléchargez le fichier **qcow2** de VM-Series pour KVM.

STEP 3 | Téléchargez Ubuntu 14.04 et chargez l'image sur le contrôleur OpenStack.

Pour le chaînage de service, vous pouvez utiliser l'image par défaut fournie par OpenStack, nommée TestVM. Ignorez cette étape lorsque vous utilisez TestVM. Une image Ubuntu est requise pour la mise à l'échelle de service.

1. Téléchargez Ubuntu 14.04.
2. Connectez-vous à l'interface utilisateur Horizon.
3. Sélectionnez **Project (Projet)** > **Compute (Calcul)** > **Images** > **Create Image (Créer une image)**.
4. Donnez un **Name (Nom)** à l'image Ubuntu 14.04 afin qu'il corresponde au paramètre dans le fichier pan_basic_gw_env.yaml.
5. Définissez la source d'image sur **Image File (Fichier image)**.
6. Cliquez sur **Choose File (Choisir le fichier)** et naviguez vers votre fichier image Ubuntu.
7. Définissez le format afin qu'il corresponde au format de fichier de votre image Ubuntu.
8. Cliquez sur **Create Image (Créer une image)**.

Une clé de serveur est requise lors de l'utilisation d'une image Ubuntu. Assurez-vous que la clé de serveur est ajoutée au fichier d'environnement.

©2023 Palo Alto Networks, Inc.

STEP 4 | Chargez VM-Series pour l'image de base KVM sur le contrôleur OpenStack.

1. Connectez-vous à l'interface utilisateur Horizon.
2. Sélectionnez **Project (Projet)** > **Compute (Calcul)** > **Images** > **Create Image (Créer une image)**.
3. **Name (Nommez)** l'image pour qu'elle corresponde au nom de l'image dans votre modèle Heat.
4. Définissez la source d'image sur **Image File (Fichier image)**.
5. Cliquez sur **Choose File (Choisir le fichier)** et accédez à votre fichier image VM-Series.
6. Définissez le format sur **QCOW2-QEMU Emulator**.
7. Cliquez sur **Create Image (Créer une image)**.

STEP 5 | Chargez les fichiers d'amorçage. Les fichiers doivent être chargés dans la structure de dossier décrite ici. Le modèle Heat utilise cette structure de dossier pour localiser les fichiers d'amorçage.

1. Connectez-vous à votre contrôleur OpenStack.
2. Créez la structure de dossier suivante :

   /root/bootstrap/config/

   /root/bootstrap/license/
3. À l'aide de SCP ou de FTP, ajoutez les fichiers init-cfg.txt et bootstrap.xml au dossier « config » et ajoutez vos codes d'autorisation VM-Series au dossier « license ».

STEP 6 | Modifiez le fichier d'environnement du modèle en fonction de votre environnement. Vérifiez que les noms d'image dans le fichier d'environnement correspondent aux noms que vous avez donnés aux fichiers lorsque vous les avez chargés.

```
parameters: # VN config management_network: 'mgmt_net'
 left_vn: 'left_net' right_vn: 'right_net' left_vn_fqdn:
 'default-domain:admin:left_net' right_vn_fqdn: 'default-
domain:admin:right_net' route_target: "target:64512:20000" # VM
 config flavor: 'm1.small' left_vm_image: 'TestVM' right_vm_image:
 'TestVM' svm_name: 'PAN_SVM_L3' left_vm_name: 'Left_VM_L3'
 right_vm_name: 'Right_VM_L3' port_tuple_name: 'port_tuple_L3'
 #ST Config S_Tmp_name: PAN_SVM_template_L3 S_Tmp_version: 2
 S_Tmp_service_mode: 'in-network' S_Tmp_service_type: 'firewall'
 S_Tmp_image_name: 'PA-VM-8.0.0' S_Tmp_flavor: 'm1.large'
 S_Tmp_interface_type_mgmt: 'management' S_Tmp_interface_type_left:
 'left' S_Tmp_interface_type_right: 'right' domain: 'default-
domain' # SI Config S_Ins_name: PAN_SVM_Instance_L3 S_Ins_fq_name:
 'default-domain:admin:PAN_SVM_Instance_L3' #IPAM Config
 NetIPam_ip_prefix_mgmt: '172.2.0.0' NetIPam_ip_prefix_len_mgmt: 24
 NetIPam_ip_prefix_left: '10.10.1.0' NetIPam_ip_prefix_len_left: 24
 NetIPam_ip_prefix_right: '10.10.2.0' NetIPam_ip_prefix_len_right:
 24 NetIPam_addr_from_start_true: true #Policy Config
 policy_name: 'PAN_SVM_policy-L3' policy_fq_name: 'default-
domain:admin:PAN_SVM_policy-L3' simple_action: 'pass' protocol:
 'any' src_port_end: -1 src_port_start: -1 direction: '< >'
 dst_port_end: -1 dst_port_start: -1
```

 ©2023 Palo Alto Networks, Inc.

STEP 7 | Modifiez les fichiers de modèle pour qu'ils renvoient vers les fichiers d'amorçage et les codes d'autorisation. Sous Personality (Personnalité), spécifiez le chemin du fichier à l'emplacement de vos fichiers. Supprimez les commentaires des lignes que vous n'utilisez pas.

```
Pan_Svm_instance: type: OS::Nova::Server depends_on:
 [ mgmt_InstanceIp, left_InstanceIp, right_InstanceIp ]
 properties: name: {get_param: svm_name } image: { get_param:
 S_Tmp_image_name } flavor: { get_param: S_Tmp_flavor } networks:
 - port: { get_resource: mgmt_VirtualMachineInterface } -
 port: { get_resource: left_VirtualMachineInterface } - port:
 { get_resource: right_VirtualMachineInterface } user_data_format:
 RAW config_drive: true personality: /config/init-cfg.txt:
 {get_file: "/root/bootstrap/config/init-cfg.txt"} # /config/
init-cfg.txt: { get_file: "http://10.4.1.21/op_test/config/
init-cfg.txt" } /config/bootstrap.xml: {get_file: "/root/
bootstrap/config/Service_Chaining_bootstrap_L3.xml"} # /config/
bootstrap.xml: { get_file: "http://10.4.1.21/op_test/config/
Service_Chaining_bootstrap_L3.xml" } # /license/authcodes:
 {get_file: "/root/bootstrap/license/authcodes"} # /license/
authcodes: {get_file: "http://10.4.1.21/op_test/license/authcodes"}
```

STEP 8 | Téléchargez les fichiers du modèle Heat.

1. Connectez-vous à votre contrôleur OpenStack.
2. Utilisez SCP ou FTP pour ajouter le fichier du modèle Heat et le fichier d'environnement.

STEP 9 | Déployez le modèle Heat.

1. Exécuter la commande **source openrc**
2. Exécutez la commande **heat stack-create <*stack-name*> -f <*template*> -e ./<*env-template*>**

STEP 10 | Vérifiez que votre pare-feu VM-Series a été déployé avec succès.

Vous pouvez utiliser les commandes suivantes pour vérifier l'état de création de la pile.

- Vérifier l'état de la pile avec **heat stack-list**
- Voir une liste détaillée des événements qui se sont produits pendant la création de la pile **heat event-list**
- Vérifier l'état de la pile avec **heat stack-show**

STEP 11 | Vérifiez que le pare-feu VM-Series inspecte de manière bidirectionnelle le trafic entre les serveurs Linux.

1. Connectez-vous au pare-feu.
2. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)** pour afficher la session SSH.

 ©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur la plateforme Google Cloud

Vous pouvez déployer un pare-feu de série VM sur un moteur Google Compute sur la plateforme Google Cloud.

- Déploiements pris en charge sur la plateforme Google Cloud
- Configuration du page-feu de la VM-Series (série VM) sur le cloud public de Google
- Déploiement du pare-feu VM-Series sur Google Cloud Platform
- Surveillance VM avec le plugin Panorama pour GCP
- Mise à l'échelle automatique du pare-feu VM-Series sur Google Cloud Platform

À propos du pare-feu VM-Series sur la plateforme Google Cloud

Les pare-feu VM-Series apportent des fonctionnalités de pare-feu de nouvelle génération à Google Cloud Platform (GCP).

Pour maximiser le rendement, les pare-feu de la série VM sur le GCP soutiennent les bibliothèques de Data Plane Development Kit (DPDK), qui offrent un traitement rapide des paquets et améliorent la performance du réseau en fonction de combinaisons précises de licences de pare-feu de la série VM et de la taille des machines virtuelles (MV) de la plateforme Google Cloud.

- Google Cloud Platform et le pare-feu VM-Series
- Exigences minimales du système pour le pare-feu de série VM

Google Cloud Platform et le pare-feu VM-Series

L'intégration du pare-feu de la série VM avec Google Cloud Platform (GCP) vous permet de déployer le pare-feu de la série VM comme une machine virtuelle (VM) tournant sur Google Compute Engine. Ce processus est simplifié lorsque vous Déployer le pare-feu de la série VM à partir du marché de la plateforme Google Cloud Launcher.

Après avoir déployé le pare-feu VM-Series, vous pouvez configurer les services facultatifs suivants :

- Activation de Google Stackdriver Monitoring sur le pare-feu VM-Series : à partir du pare-feu, transmettez les statistiques PAN-OS au service Google Stackdriver.
- Activer VM Monitoring pour suivre les modifications apportées aux machines virtuelles sur Google Cloud Platform : configurez une source d'informations VM qui surveille la zone de Google Cloud Platform spécifique où se trouvent vos instances. Les métadonnées de VM surveillées peuvent comprendre des propriétés prédéfinies du GCP (comme l'ID du projet) et des propriétés définies par l'utilisateur (comme les étiquettes et les étiquettes de réseau).

Exigences minimales du système pour le pare-feu de série VM

Vous devez choisir VM-Series Firewall License for Public Clouds (une licence de pare-feu de série VM pour les nuages publics) et une méthode de licence : apportez votre propre licence (BYOL) ou payez au fur et à mesure (PAYG). Pour déployer un pare-feu VM-Series sur une instance de Google Compute Engine, vous devez choisir un type de machine qui prend en charge les exigences du système VM-series pour la licence.

Une seule instance de moteur de calcul Google prend en charge jusqu'à 8 interfaces réseau. Si vous voulez configurer 8 interfaces, choisissez n1-standard-8 ou un type de machine à plus grande capacité.

Capacité	BYOL	Bundles 1 and 2	
		PAYG	Marketplace
Pare-feu VM-100	✓		

©2023 Palo Alto Networks, Inc.

Capacité	BYOL	Bundles 1 and 2	
		PAYG	Marketplace
Pare-feu VM-200	✓		
Pare-feu VM-300	✓	✓	✓
Pare-feu VM-1000-HV	✓		
Pare-feu VM-500	✓		
Pare-feu VM-700	✓		

Le pare-feu VM-Series prend en charge les types de machines standards prédéfinis répertoriés ci-dessous. Vous pouvez choisir un type de machine plus performant ou créer votre propre type de machine personnalisée, à condition que les besoins en ressources soient compatibles avec votre licence de pare-feu VM-Series.

- n1-standard-4
- n1-standard-8
- n1-standard-16
- n2-standard-4
- n2-standard-8
- n2-standard-16
- n2-standard-32

Types de machines personnalisées :

- e2-standard-4
- e2-standard-8
- e2-standard-16
- e2-standard-32

©2023 Palo Alto Networks, Inc.

Déploiements pris en charge sur la plateforme Google Cloud

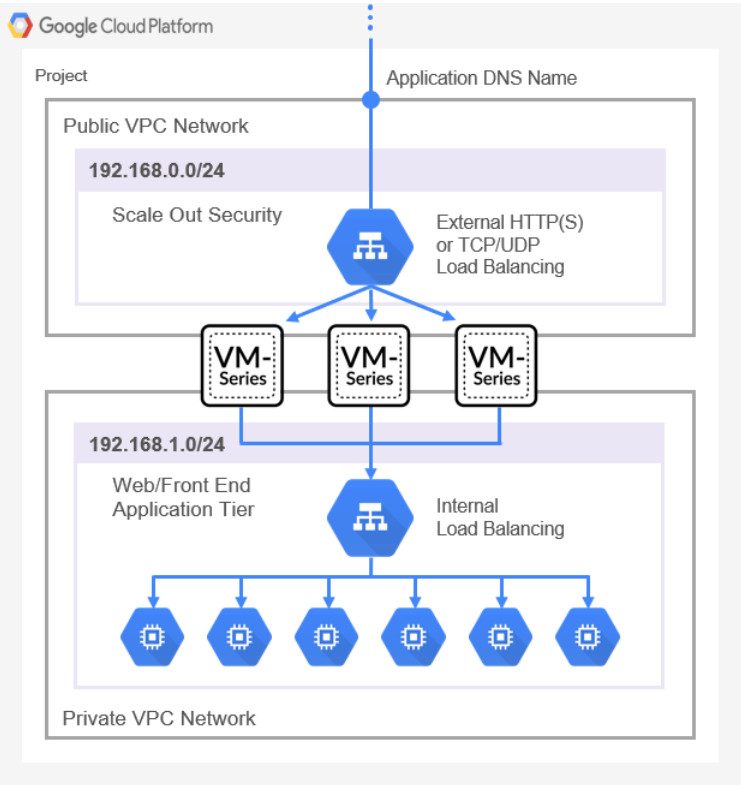
Vous pouvez déployer le pare-feu de la série VM sur un moteur Google® Compute dans un réseau dans votre VPCnetwork. Les types de rôles sont les suivants :

- Passerelle Internet
- Passerelle de segmentation
- Hybrid IPSec VPN

Passerelle Internet

Le pare-feu VM-Series sécurise le trafic Nord / Sud, vers et depuis l'Internet, afin de protéger les applications contre les menaces connues et inconnues. Un projet Google peut avoir jusqu'à cinq réseaux VPC. Pour un exemple typique d'une passerelle Internet, consultez les configuration examples de Google.

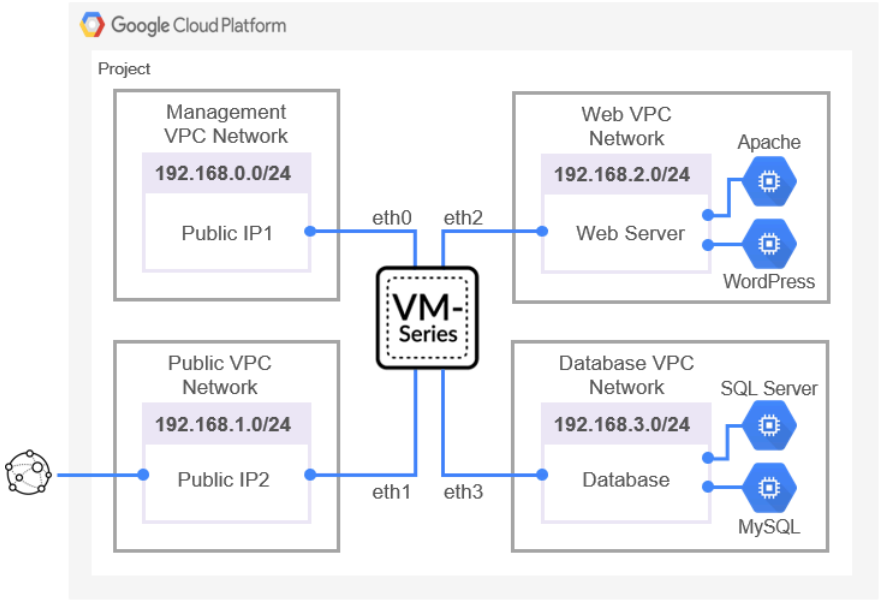
Dans les environnements de cloud public, il est courant d'utiliser une architecture de type « scaleout » (illustrée ci-dessous) plutôt que des VM possédant une plus grande portée et offrant une plus grande performance. Cette architecture (parfois appelée déploiement ***en sandwich***) évite la présence d'un seul point de défaillance et vous permet d'ajouter ou de supprimer des pare-feu si nécessaire.



 ©2023 Palo Alto Networks, Inc.

Passerelle de segmentation

Une passerelle de segmentation sécurise le trafic Est / Ouest entre les connexions VPC pour assurer la conformité de la protection des données et l'accès aux applications. La figure suivante montre un coupe-feu qui retient la circulation nord-sud et est-ouest.

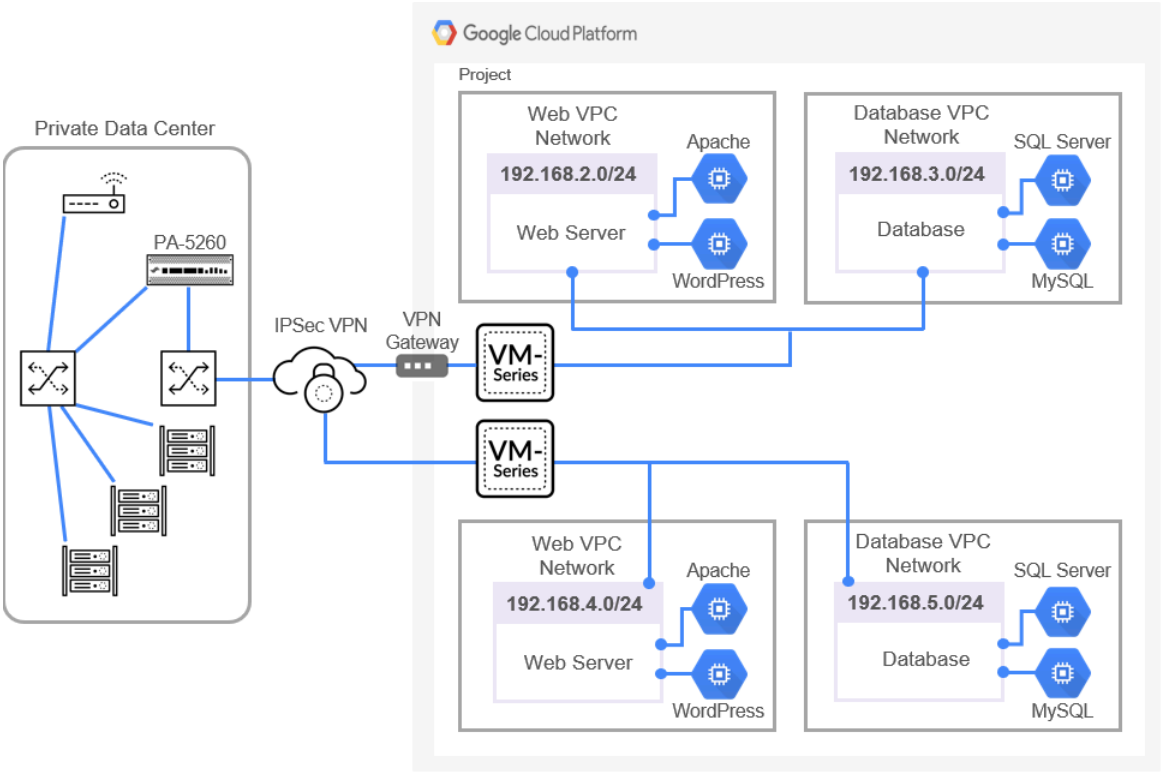


Hybrid IPSec VPN

Le pare-feu VM-Series sert de point de terminaison VPN IPSec, ce qui offre la possibilité de communications sécurisées depuis et vers des applications hébergées sur Google Cloud Platform.

Le déploiement suivant montre un VPN d'un site à un autre, depuis un réseau local vers un pare-feu VM-Series déployé sur Google Cloud Platform et une connexion IPSec depuis un réseau local vers une passerelle Google Cloud VPN.

©2023 Palo Alto Networks, Inc.



 ©2023 Palo Alto Networks, Inc.

Configuration du page-feu de la VM-Series (série VM) sur le cloud public de Google

Le processus pour Déployer le pare-feu de la série VM à partir du marché de la plateforme Google Cloud Launcher nécessite des tâches préparatoires.

Si vous déployez à l'aide de Google Marketplace, vous devez créer vos réseaux et sous-réseaux de projet, et planifier l'attribution des réseaux et des adresses IP pour les interfaces de pare-feu de la série VM à l'avance. Pendant le déploiement, vous devez choisir parmi les réseaux et sous-réseaux existants.

Reportez-vous aux rubriques suivantes lors de la planification de votre déploiement :

- Exigences générales
- Installation du plug-in VM-Series sur Panorama
- Installation du plug-in Panorama pour GCP
- Se préparer au déploiement à partir du GCP Marketplace

Exigences générales

Les composants de cette liste de contrôle sont courants pour le déploiement d'un pare-feu VM-Series que vous gérez directement ou avec Panorama. Des exigences supplémentaires s'appliquent pour le plug-in Panorama pour des services tels que la surveillance Stackdriver, la surveillance VM, la mise à l'échelle automatique ou la sécurisation des déploiements Kubernetes.

Consultez toujours la matrice de compatibilité pour des informations sur le plug-in Panorama pour les clouds publics. Cette version nécessite le logiciel suivant :

- **Compte GCP** – Vous devez avoir un compte d'utilisateur du GCP avec une adresse de courriel couplée et vous devez connaître le nom d'utilisateur et le mot de passe de cette adresse de courriel.
- **Google Cloud SDK** – si vous ne l'avez pas encore fait, installez Google Cloud SDK, qui inclut les API Google Cloud, gcloud et d'autres outils de ligne de commande. Vous pouvez utiliser l'interface de ligne de commande pour déployer le modèle de pare-feu et d'autres modèles.
- **PAN-OS sur les pare-feu VM-Series sur GCP** – pare-feu VM-Series exécutant une version de PAN-OS disponible à partir de Google Marketplace.
  - **Pare-feu VM-Series** – les pare-feu VM-Series que vous souhaitez gérer depuis Panorama doivent être déployés dans Google Cloud Platform à l'aide d'une image Palo Alto Networks depuis Google Marketplace. Les pare-feu doivent répondre aux Exigences minimales du système pour le pare-feu de série VM.
  - **Licences VM-Series** – vous devez activer une licence de pare-feu VM-Series pour obtenir un numéro de série. Un numéro de série est requis pour ajouter un pare-feu VM-Series à un appareil géré Panorama. Si vous utilisez le plug-in Panorama pour permettre à GCP de déployer des pare-feu VM-Series, vous devez fournir un code d'authentification BYOL. Google Marketplace gère la facturation de votre service, mais les pare-feu que vous déployez se connecteront directement au serveur d'octroi de licences de Palo Alto Networks.

 ©2023 Palo Alto Networks, Inc.

- **Plug-in VM-Series sur le pare-feu** – les pare-feu VM-Series exécutant PAN-OS version 9.0 ou ultérieure incluent le plug-in VM-Series, qui gère l'intégration avec les clouds publics et privés. Comme indiqué dans la matrice de compatibilité, le plug-in VM-Series a une version minimum qui correspond à chaque version de PAN-OS.

  Lors d'une mise à niveau majeure de PAN-OS, la version du plug-in VM-Series est automatiquement mise à niveau. Pour les versions mineures, il vous appartient de déterminer si une mise à niveau du plug-in VM-Series est nécessaire et, si tel est le cas, d'effectuer une mise à niveau manuelle. Reportez-vous à la section Installation du plug-in VM-Series sur Panorama.

- **Panorama exécuté en mode de gestion** – un appareil Panorama physique ou virtuel exécutant une version de PAN-OS identique ou ultérieure aux pare-feu gérés. Les instances virtuelles n'ont pas besoin d'être déployées dans GCP.
  - Vous devez disposer d'une version sous licence de Panorama.
  - Panorama doit disposer d'un accès réseau aux VPC dans lesquels les VM que vous souhaitez gérer sont déployées.
  - Si vous avez l'intention de gérer les VM déployées dans GCP, ou de configurer des fonctionnalité telles que la mise à l'échelle automatique, vos versions de PAN-OS et du plug-in VM-Series doivent répondre aux exigences du cloud public pour prendre en charge le plug-in Panorama pour GCP.
  - Plug-in VM-Series sur Panorama. Reportez-vous à la section Installation du plug-in VM-Series sur Panorama
- **Plug-in Panorama pour la version 2.0.0 de GCP** – le plug-in GCP gère les interactions requises pour octroyer une licence, effectuer un amorçage et configurer des pare-feu déployés avec la surveillance VM ou les modèles de mise à l'échelle automatique. Le plug-in GCP, associé aux modèles de surveillance VM ou de mise à l'échelle automatique, utilise les piles de modèles Panorama et les groupes d'appareils pour programmer des règles NAT qui orientent le trafic vers les pare-feu VM-Series gérés.

  Reportez-vous à la section Installation du plug-in Panorama pour GCP.

Installation du plug-in VM-Series sur Panorama

Sur Panorama, installez ou mettez à niveau la version du plug-in VM-Series qui prend en charge les fonctionnalités GCP que vous souhaitez configurer, comme détaillé dans le tableau de la matrice de compatibilité pour les clouds publics.

Installation initiale – étant donné que le plug-in VM-Series est facultatif sur Panorama, la première fois que vous installez, vous devez télécharger le plug-in VM-Series depuis le portail d'assistance puis accéder à **Panorama** > **Device deployment (Déploiement d'appareil)** > **Plugins (Plug-ins)** pour charger et installer.

Mise à niveau – accédez à **Panorama** > **Device Deployment (Déploiement d'appareil)** > **Plugins (Plug-ins)** et cliquez sur **Check Now (Vérifier maintenant)**. Installez une version qui réponde aux exigences du tableau de la matrice de compatibilité pour les clouds publics.

 ©2023 Palo Alto Networks, Inc.

Installation du plug-in Panorama pour GCP

Le plug-in Panorama pour GCP est requis si vous souhaitez utiliser Panorama pour gérer la surveillance VM ou les déploiements de mise à l'échelle automatique créés avec des modèles Palo Alto Networks. Installez la version du plug-in VM-Series qui prend en charge les fonctionnalités GCP que vous souhaitez configurer, comme détaillé dans le tableau de la matrice de compatibilité pour les clouds publics.

Vous ne pouvez pas mettre à niveau le plug-in Panorama pour GCP de la version 1.0.0 à la version 2.0.x. Si vous avez installé la version 1.0.0, supprimez-la avant d'installer la 2.0.x.

Si vous avez un appareil Panorama autonome ou deux appareils Panorama installés dans une paire HA avec plusieurs plug-ins installés, les plug-ins peuvent ne pas recevoir les informations des indicateurs d'adresse IP mises à jour si un ou plusieurs des plug-ins ne sont pas configurés. Cela se produit, car Panorama ne transfère pas les informations des indicateurs d'adresse IP aux plug-ins non configurés. De plus, ce problème peut se présenter si un ou plusieurs plug-ins Panorama ne se trouvent pas dans l'état Registered (Enregistré) ou Success (Réussite) (l'état positif diffère sur chaque plug-in). Assurez-vous que vos plug-ins se trouvent dans l'état positif avant de continuer ou d'exécuter les commandes décrites ci-dessous.

Si vous rencontrez ce problème, il existe deux solutions alternatives :

- Désinstallez le ou les plug-ins non configurés. Il est déconseillé d'installer un plug-in que vous n'envisagez pas de configurer dans l'immédiat
- Vous pouvez utiliser les commandes suivantes pour contourner ce problème. Exécutez la commande suivante pour chaque plug-in non configuré sur chaque instance de Panorama afin que Panorama n'attende pas pour envoyer des mises à jour. Dans le cas contraire, vos pare-feu risquent de perdre certaines informations des indicateurs d'adresse IP.

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  Vous pouvez annuler cette commande en exécutant :

  request plugins dau plugin-name <plugin-name> unblock-device-push no

Les commandes décrites ne sont pas persistantes lors des redémarrages et doivent être réutilisées pour tout redémarrage ultérieur. Pour Panorama en paire HA, les commandes doivent être exécutées sur chaque Panorama.

STEP 1 | Vérifiez votre installation Panorama.

Sur Panorama, assurez-vous que la version de votre PAN-OS répond aux exigences pour prendre en charge la mise à l'échelle de GCP.

STEP 2 | Supprimez le plug-in Panorama pour GCP v1.0.

Si le plug-in Panorama v1.0 est installé, vous devez le supprimer.

©2023 Palo Alto Networks, Inc.

STEP 3 | Installation du plug-in Panorama pour GCP.

Sélectionnez **Panorama** > **Plugins (Plug-ins)** et saisissez **gcp** dans la barre de recherche. **Installez** la version du plug-in VM-Series qui prend en charge les fonctionnalités que vous souhaitez configurer (voir le tableau de la matrice de compatibilité pour les clouds publics).

Après l'installation, vous pouvez voir le plug-in dans la liste **General Information** (Informations générales) sur le tableau de bord de Panorama. Affichez **Panorama** > **Google Cloud Platform (Plateforme Google Cloud)**, et vous voyez les interfaces **Setup (Configuration)**, **Monitoring Definition (Définition de la surveillance)** et **AutoScaling (Mise à l'échelle automatique)**.

STEP 4 | (Facultatif) Si vos appareils Panorama sont en configuration de disponibilité élevée, vous devez installer manuellement la même version du plugin Google sur les deux appareils Panorama pairs.

Configurez le plugin Google sur le pair actif de Panorama seulement. Sur l'engagement, la configuration est synchronisée avec le pair passif Panorama. Seuls les pairs actifs Panorama sondent les VM Google que vous avez configurées pour la surveillance VM.

Se préparer au déploiement à partir du GCP Marketplace

Vérifiez ces exigences pour vous assurer que vous disposez des comptes et des autorisations appropriés avant d'utiliser Google Marketplace pour déployer le pare-feu sur une instance de Google Compute Engine (GCE).

- Comptes et autorisations généraux
- Ressources Google disponibles
- Méthodes d'authentification Google
- Paire de clés SSH

Comptes et autorisations généraux

- Vous, et tous les utilisateurs que vous autorisez, devez avoir les rôles minimaux suivants ou autorisations Identity and Access Management (IAM) équivalentes pour vous connecter au pare-feu VM-Series :
  - **Compute Viewer** : Compute Viewer vous permet d'obtenir et de lister les ressources du moteur de calcul sans pouvoir lire les données qui y sont stockées.
  - **Storage Object Viewer (Visionneuse d'objets de stockage :**vous permet d'amorcer à l'aide d'un compartiment de stockage Google dans le même projet.

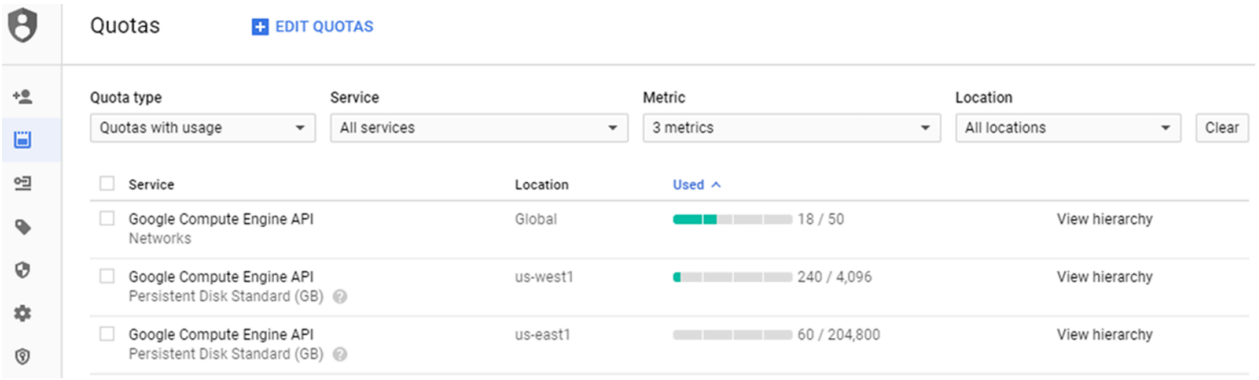
  Les utilisateurs de votre organisation peuvent disposer d'autorisations IAM *ou de* rôles *prédéfinis plus permissifs que nécessaire. Assurez-vous de bien restreindre l'accès au pare-feu VM-Series.*

  Vous pouvez également restreindre l'accès avec des comptes de service, comme décrit dans Méthodes d'authentification Google.
- **La surveillance Metric Writer** : requise pour Stackdriver.

 ©2023 Palo Alto Networks, Inc.

Ressources Google disponibles

Votre projet doit disposer de ressources suffisantes pour déployer le pare-feu VM-Series en tant qu'instance Google Compute Engine. Si vous déployez une solution GCP Marketplace, déterminez si la solution déploie d'autres machines virtuelles en plus du pare-feu. Dans la console Google Cloud, sélectionnez **IAM & admin (Gestion d'identité et d'accès et administration)** > **Quotas** afin d'examiner les quotas de ressources pour votre projet, ainsi que les réseaux et l'espace disque utilisés. Si vous manquez de ressources, vous pouvez demander à Google d'en affecter davantage à votre organisation.



Méthodes d'authentification Google

Le GCP soutient de multiples façons de se connecter à une instance. Vous pouvez vous authentifier avec un compte de service ou une paire de clés SSH.

1. **Comptes de service**—Les comptes de service s'appliquent aux applications ou aux VM — pas aux utilisateurs finaux. Ils sont couramment utilisés pour contrôler l'accès lorsque vous utilisez des programmes ou des scripts, ou lorsque vous accédez au pare-feu à partir de la ligne de commande gcloud. Si vous utilisez des comptes de service Google pour authentifier des instances ou des applications, vous devez connaître le e-mail du ou des comptes. Voir Création et gestion des clés de compte de service.

   L'utilisation d'un compte de service est nécessaire si vous voulez vous connecter au pare-feu de la série VM depuis l'extérieur du projet – que ce soit depuis un projet différent ou depuis la ligne de commande. Par exemple, si vous voulez activer un pare-feu de prochaine génération pour surveiller votre pare-feu de série VM, vous devez sauvegarder l'information du service du pare-feu de série VM dans un fichier JSON. Dans le pare-feu physique, vous téléchargez le fichier lorsque vous configurez la connexion.

   1. Sélectionnez **IAM & Admin (IAM et administrateur)** > **Service accounts (Comptes de service)** et choisissez **+Create Service Account (Créer un compte de service)**.

      Saisissez le nom et la description du compte de service, puis cliquez sur **Create (Créer)**.
   2. Sélectionnez un type de rôle dans le menu déroulant et, à droite, sélectionnez un niveau d'accès approprié.

      Par exemple, sélectionnez Project (Projet) > Editor (Éditeur). Vous pouvez sélectionner plusieurs rôles pour un compte de service. Lorsque vous avez terminé, cliquez sur **Continue (Continuer)**.

©2023 Palo Alto Networks, Inc.

3. Accordez à des utilisateurs spécifiques l'autorisation d'accéder à ce compte de service. Sélectionnez les membres dans la colonne **Permissions (Autorisations)** à droite pour leur donner l'autorisation d'accéder aux rôles de l'étape précédente.

2. **Clés SSH** – Si vous déployez le pare-feu de la série VM à partir du Marketplace, vous devez fournir une clé Open SSH en format RSA pour les métadonnées de l'instance du moteur Google Compute.

   Le pare-feu de série VM n'accepte qu'une seule clé au déploiement.

   Au moment du déploiement, vous collez la clé publique dans le déploiement du Marketplace, comme décrit dans Paire de clés SSH. Après le déploiement, vous utilisez la clé privée de SSH dans le pare-feu pour configurer le compte d'administrateur. Pour ajouter des utilisateurs, voir Manage Firewall Administrators (Gérer les administrateurs du Pare-feu).

Vous pouvez vous authentifier de plusieurs façons :

- **Créez des comptes de service pour les instances** – vous pouvez créer un compte de service pour une instance spécifique ou un groupe d'instances, et garantir des autorisations spécifiques, lesquelles peuvent ensuite être accordées aux utilisateurs.
- **Utilisez le compte de service par défaut pour votre projet** – Si vous utilisez la console de Google Cloud Platform (GCP™), vous avez ouvert une session avec votre adresse de courriel et pouvez accéder à une instance GCE en fonction des permissions ou des rôles que l'administrateur de projet a attribués à votre compte.

  Chaque instance de Google Compute Engine créée avec la console Google Cloud ou l'outil de ligne de commande gcloud possède un compte de service par défaut dont le nom figure au format d'adresse e-mail :

  ```
  <project-number>-compute@developer.gserviceaccount.com
  ```

  Pour afficher le nom du compte de service de l'instance de pare-feu, affichez les détails de l'instance et faites défiler vers le bas (reportez-vous à la section Compte de service par défaut de Compute Engine).

  Le compte de service par défaut peut gérer l'authentification auprès des VM dans le même projet qu'un pare-feu VM-Series. Les champs d'accès permettent au pare-feu de lancer des appels API vers les VM dans le projet de Google Cloud.
- **Utilisez les autorisations IAM et les API Google** - Si vous utilisez les API Google SDK et gcloud, vous devez appeler les API pour vous authentifier.
  - Vous utilisez habituellement le SDK de Google lorsque vous voulez gérer le pare-feu à partir d'une ligne de commande ou lorsque vous voulez exécuter un script pour configurer le pare-feu.
  - Vous devez accéder aux API Google si l'une des machines virtuelles que vous connectez possède une image personnalisée avec des applications nécessitant des API de Google.

Paire de clés SSH

Lorsque vous déployez le pare-feu VM-Series depuis Google Marketplace, vous avez besoin d'une paire de clés SSH pour vous authentifier auprès du pare-feu VM-Series.

 ©2023 Palo Alto Networks, Inc.

Créez la paire de clés selon la documentation de votre générateur de clés. Ne pas modifier le fichier de clés publiques. Modifier risque d'introduire des caractères illégaux.

Le pare-feu de série VM gère l'authentification différemment des instances GCE. Après le déploiement, vous vous connectez d'abord avec l'utilisateur **admin**. Le nom d'utilisateur par défaut du pare-feu VM-Series est accepté une seule fois. Après une connexion réussie, vous devez définir un nom d'utilisateur et un mot de passe d'administrateur pour l'interface Web VM-Series (reportez-vous à la section Déployer le pare-feu de la série VM à partir du marché de la plateforme Google Cloud Launcher).

Le champ **SSH key (Clé SSH)** dans l'interface de déploiement Google Marketplace affiche le signet suivant :

admin:ssh-rsa your-SSH-key

admin est le nom d'utilisateur de l'administrateur du pare-feu VM-Series requis pour se connecter au pare-feu pour la première fois. Vous ajoutez le préfixe **admin:** dans le champ Marketplace lorsque vous Déployer le pare-feu de la série VM à partir du marché de la plateforme Google Cloud Launcher.

Vous ne pouvez pas ouvrir une session dans le pare-feu de la série VM si vous ne fournissez pas toute la clé publique, ou si votre clé contient des caractères illégaux lorsque vous collez la clé dans le champ **SSH key (Clé SSH)** de Marketplace. Lorsque vous entrez SSH dans le pare-feu de la série VM pour la première fois, la clé publique est transférée au pare-feu.

Si la clé publique est corrompue, vous devez supprimer le déploiement et recommencer. Des réseaux et des sous-réseaux demeurent, mais les règles du pare-feu doivent être recréées.

STEP 1 | Créez une paire de clés SSH et enregistrez la paire de clés SSH à l'emplacement par défaut pour votre système d'exploitation mentionné dans la section Trouver une clé SSH.

- **Linux ou MacOS** – Utilisez `ssh-keygen` pour créer la paire de clés dans votre répertoire .ssh.
- **Windows** – Utilisez PuTTYgen pour créer la paire de clés.

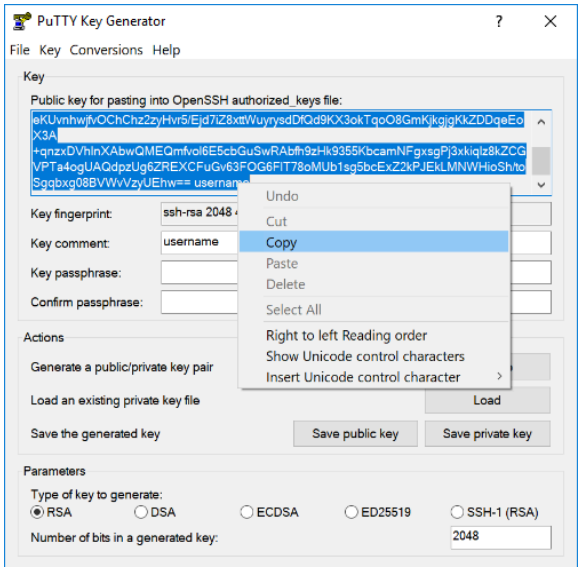
  Le contenu du champ **Key comment (commentaire clé)** n'a pas d'importance pour le pare-feu de la série VM; vous pouvez accepter la date par défaut (la date de création de la clé) ou entrer un commentaire qui vous aide à vous souvenir du nom de la paire de clés. Utilisez le bouton **Save private key (Sauvegarder la clé privée)** pour stocker la clé privée dans votre répertoire .ssh.

©2023 Palo Alto Networks, Inc.

STEP 2 | Sélectionnez la clé publique complète.

- **Linux ou MacOS** – Ouvrez votre clé publique dans un éditeur de texte et copiez-la.
- **Windows** – Vous devez utiliser le générateur de clés pour afficher la clé publique. Lancez PuTTYgen, cliquez sur **Load** et naviguez jusqu'à la clé privée que vous avez enregistrée dans votre répertoire .ssh.

  Dans PuTTYgen, faites défiler vers le bas pour vous assurer de sélectionner la touche au complet, cliquez avec le bouton droit de la souris et sélectionnez Copy (Copier).



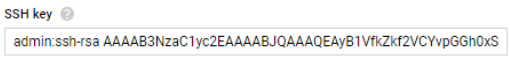
STEP 3 | Saisissez la clé publique dans le champ de clé SSH comme détaillé ci-dessous.

1. Dans le champ de la touche Marketplace SSH, **SSH key (Clé SSH)** supprimez le texte de l'espace réservé et entrez :

   `admin:`

   Assurez-vous qu'il n'y a pas d'espace supplémentaire après le cône.

2. Insérez le curseur après **`admin:`** et choisissez **Paste as plain text (Coller comme texte en clair)**. La clé doit être sur une seule ligne, comme indiqué ci-dessous :

3. Déplacez le curseur à la fin de la clé, ajoutez une espace et saisissez : **`admin`**

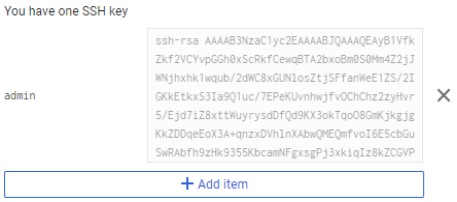
   Le contenu final du champ **SSH key (Clé SSH)** doit être :

   `admin:ssh-rsa` [CLÉ] **`admin`**

©2023 Palo Alto Networks, Inc.

STEP 4 | Vérifiez la clé.

Après le déploiement, et avant de tenter de vous connecter au pare-feu, consultez l'exemple de gestion et vérifiez la présence de sauts de ligne ou d'espaces supplémentaires dans la clé :



Si la clé est entièrement comprise sur une ligne et au format **admin:ssh-rsa** [CLÉ] **admin**, vous avez terminé.

STEP 5 | (facultatif) En cas de problème, vous devez remplacer la clé.

1. Cliquez sur **X** pour supprimer la clé et ensuite sur **+ Add item (+ ajouter l'élément)**.
2. Saisissez la clé comme décrit à l'étape 3. À présent, le champ **SSH key (Clé SSH)** doit afficher :

   admin:ssh-rsa [CLÉ] **admin**
3. Cliquez sur **Save (Sauvegarder)** pour déployer le déploiement mis à jour.
4. Vérifiez à nouveau la clé.

Planification du réseau en nuage privé virtuel (VPC)

Avant de déployer à partir de Google Marketplace, établissez un plan pour les réseaux VPC (appelés networks « *réseaux* »), les subnets (également appelés « *sous-réseaux* ») et les règles de pare-feu Google. Vous devez créer des réseaux et sous-réseaux avant de commencer à Déployer le pare-feu de la série VM à partir du marché de la plateforme Google Cloud Launcher.

La page de déploiement de Marketplace affiche seulement les réseaux et sous-réseaux qui existent au début du déploiement. S'il manque un réseau, vous devez quitter le déploiement, créer le réseau et recommencer.

- **Réseaux VPC**—Vous devez créer des réseaux personnalisés spécifiquement pour les interfaces réseau de pare-feu VM-Series.
  - Reportez-vous à la section Licences de pare-feu VM-Series pour les clouds publics pour déterminer le nombre d'interfaces réseau nécessaires, en fonction de votre licence de pare-feu VM-Series. Au minimum, configurez les trois réseaux et sous-réseaux VPC pour le lancement du pare-feu VM-Series.
  - Un projet Google Cloud Platform dispose d'un réseau par défaut avec des configurations et des règles de pare-feu prédéfinies ; vous pouvez supprimer le réseau par défaut, s'il n'est pas utilisé.
  - Par défaut, il y a jusqu'à cinq réseaux dans un projet. Votre administrateur Google Cloud Platform peut demander des réseaux supplémentaires pour votre projet.
  - Pour vous connecter à l'interface de gestion, vous devez créer des règles de coupe-feu du GCP qui vous permettent d'y accéder. Vous pouvez le faire pendant le déploiement si vous choisissez **Enable GCP Firewall rule for connections to Management interface (Activer la règle du Pare-feu du GCP pour les connexions à l'interface de gestion)**, puis fournissez un

 ©2023 Palo Alto Networks, Inc.

bloc CIDR pour **Source IP in GCP Firewall rule for connections to Management Interface (l'IP source dans la règle du pare-feu du GCP pour les connexions à l'interface de gestion)**.

Assurez-vous que vos réseaux comprennent toutes les instances que vous voulez protéger.

- **Sous-réseaux** – Une instance de moteur de calcul peut prendre en charge jusqu'à huit interfaces de couche 3 sur une seule instance. Les interfaces Management, Trust et Untrust utilisent trois interfaces et vous pouvez créer jusqu'à cinq interfaces supplémentaires d'avion de données. En général, les interfaces des plans de données représentent les réseaux d'applications.
- **Adresse IP**— Vous fournissez des plages d'adresses IP lorsque vous créez des sous-réseaux d'interface et vous avez la possibilité d'activer une adresse externe lorsque vous déployez un sous-réseau.
  - Lorsque vous créez des sous-réseaux, vous devez spécifier une plage d'adresses IP. Cette plage est utilisée pour votre réseau interne, afin qu'elle ne puisse donc pas chevaucher d'autres sous-réseaux.
  - Pendant le déploiement, vous pouvez choisir d'activer une adresse IP externe lorsque vous créez une interface réseau. Par défaut, on vous donne une adresse IP éphémère. Vous ne pouvez pas fournir une adresse IP statique réservée pendant le déploiement, mais vous pouvez promouvoir l'adresse éphémère à une adresse IP statique après avoir terminé le processus de déploiement (voir la section Promouvoir une adresse IP externe éphémère).

Planification d'interface réseau

Lorsque vous déployez Google Cloud Launcher par défaut, le déploiement de pare-feu VM-Series dispose de trois interfaces : l'interface de plan de gestion et les interfaces du dataplane Untrust et Trust. Vous pouvez définir des instances du plan de données supplémentaires, en fonction des ressources de calcul disponibles sur votre VM ; voir Licences de pare-feu VM-Series pour les clouds publics.

Pendant le déploiement, vous avez l'occasion de nommer ces interfaces.

Commande d'interface

Lorsque vous déployez avec le Marketplace, l'ordre des interfaces réseau est prédéfini. L'interface de gestion correspond à eth0, Untrust à eth1 et Trust to eth2. L'ordre est important car la mise en correspondance de l'interface de gestion avec eth0 et de l'interface non fiable avec eth1 garantit que vous réussissez si vous devez permuter l'interface de gestion pour équilibrer la charge.

Interfaces de gestion

La première interface réseau que vous ajoutez est mappée à eth0 sur le pare-feu et elle a la possibilité d'activer le transfert IP. Vous utilisez cette interface réseau pour gérer le pare-feu de la série VM. Habituellement, cette interface a une adresse IP externe.

Une adresse IP externe est uniquement requise si une interface du dataplane est connectée au sous-réseau public. Au moment de sa création, vous recevez une adresse IP éphémère mais vous pouvez la promouvoir sur une adresse IP statique après avoir terminé le déploiement (reportez-vous à la section Promotion d'une adresse IP externe éphémère*).*

 ©2023 Palo Alto Networks, Inc.

Interfaces du dataplane (Untrust, Trust)

Lorsque vous utilisez Google Cloud Launcher, l'ordre dans lequel vous ajoutez des interfaces est prédéterminé.

- Ajoutez l'interface Untrust après l'interface de gestion. This order means that the untrusted interface is mapped to eth1. Les interfaces Untrust sont généralement attachées au sous-réseau public et possèdent une adresse IP externe.

  Une adresse IP externe est uniquement requise si une interface du dataplane est connectée au sous-réseau public. Au moment de sa création, vous recevez une adresse IP éphémère mais vous pouvez la promouvoir sur une adresse IP statique, comme mentionné à la section Promotion d'une adresse IP externe éphémère.

- L'interface Trust doit suivre l'interface Untrust, afin qu'elle soit mappée à eth2. Le réseau Trust n'a souvent pas d'adresse IP externe. Vous pouvez ajouter d'autres interfaces d'avion de données après l'interface Trust.

Interfaces du dataplane supplémentaires

Planifiez des interfaces pour les applications que vous devez protéger, comme les serveurs Web, les bases de données et d'autres applications de votre réseau. Vous pouvez créer jusqu'à cinq interfaces supplémentaires pour les plans de données en plus des trois interfaces requises pour lancer votre coupe-feu. Assurez-vous que les applications que vous voulez protéger sont dans des réseaux qui se connectent au pare-feu de la série VM.

 ©2023 Palo Alto Networks, Inc.

Déploiement du pare-feu VM-Series sur Google Cloud Platform

Pour déployer le pare-feu VM-Series en utilisant le modèle de Marketplace GCP, vous devez d'abord créer un réseau VPC pour chaque interface du pare-feu. Après avoir déployé le pare-feu depuis Google Marketplace, vous pouvez vous connecter au pare-feu pour ajuster la configuration afin qu'elle fonctionne dans le cadre de votre configuration VPC GCP. Vous pouvez également activer la surveillance afin de collecter des métriques qui vous permettent d'améliorer la gestion des ressources ou de créer des règles de politique de sécurité qui s'adaptent automatiquement aux changements dans votre environnement d'application.

- Déployer le pare-feu de la série VM à partir du marché de la plateforme Google Cloud Launcher
- Échange de l'interface de gestion pour l'équilibrage de la charge de Google Cloud Platform
- Utilisation de la CLI du pare-feu VM-Series pour permuter l'interface de gestion
- Activation de la surveillance CloudWatch sur le VM-Series Firewall (pare-feu de la série VM)
- Permettre la surveillance de la MV pour suivre les changements de VM sur la plateforme de Google Cloud (GCP)
- Utilisation de groupes d'adresses dynamiques pour sécuriser des instances dans VPC
- Utiliser des modèles personnalisés ou le CLI de l'infonuagique pour déployer le Pare-feu de la série VM

Déployer le pare-feu de la série VM à partir du marché de la plateforme Google Cloud Launcher

Vous pouvez utiliser Google® Cloud Platform Marketplace pour déployer le pare-feu VM-Series sur une licence de capacité de vCPU fixe (Modèles VM-Series). Les images sous licence disponibles à partir de clouds publics sont les suivantes :

- VM-Series Next-Generation Firewall Bundle 1
- VM-Series Next-Generation Firewall Bundle 2
- Pare-feu de prochaine génération de la série VM (BYOL)

Reportez-vous à Déployer le pare-feu de la série VM à partir du marché de la plateforme Google Cloud Launcher pour en savoir plus sur ces options de licence.

Le Marketplace déploie une instance du pare-feu VM-Series qui possède au moins une interface de gestion et deux interfaces du dataplane. Vous pouvez ajouter des interfaces d'avion de données pour jusqu'à cinq instances de moteur Google Compute dans votre cloud privé virtuel (VPC).

Avant de déployer le pare-feu de la série VM, vous devez créer ou choisir un projet dans votre organisation et créer des réseaux et des sous-réseaux qui se brancheront au pare-feu, comme le décrit VPC Network Planning et Network Interface Planning.

Vous ne pouvez connecter plusieurs interfaces réseau au même réseau VPC. Chaque interface que vous créez doit disposer d'un réseau dédié avec au moins un sous-réseau. Assurez-vous que vos réseaux comprennent d'autres instances d'avion de données que vous créez.

STEP 1 | Choix d'une méthode d'amorçage.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Trouvez la liste des pare-feu de la série VM dans Marketplace.

1. Connectez-vous à Google Cloud Console.
2. Dans le menu Produits et services, sélectionnez **Marketplace**.
3. Chercher **`VM-Series`**.
4. Sélectionnez l'une des options de licence de pare-feu de la série VM.

STEP 3 | Cliquez sur **Launch on Compute Engine (Lancer sur Compute Engine)**.

STEP 4 | Name the instance and choose resources.

1. Entrez le **Deployment Name (Nom de déploiement)** (ce nom est affiché dans le gestionnaire de déploiement). Le nom doit être unique et ne peut entrer en conflit avec aucun autre déploiement du projet.
2. Sélectionnez une **Zone**. Voir Regions et zones pour une liste des zones prises en charge.
3. Sélectionnez **Machine Type (Type de machine)** en fonction de la Configuration système requise pour VM-Series pour votre licence et de la configuration minimale requise pour le pare-feu VM-Series sur Google Cloud Platform.

STEP 5 | **Spécifiez les métadonnées de l'instance**.

Les options **Bootstrap Bucket** et **Interface Swap** affectent la configuration initiale la première fois que les bottes de pare-feu de la série VM sont utilisées.

1. **Bootstrap Bucket** (facultatif) – Si vous prévoyez d'utiliser un fichier d'amorçage, saisissez le nom d'un compartiment de stockage ou le chemin d'accès à un dossier dans le compartiment de stockage qui contient l'ensemble d'amorçage. Vous devez avoir l'autorisation d'accéder au compartiment de stockage. Par exemple :

   `vmseries-bootstrap-gce-storagebucket=<bucketname>`

   ou

   `vmseries-bootstrap-gce-storagebucket=<bucketname/directoryname>`

   Si vous choisissez d'amorcer avec des métadonnées personnalisées, passez à l'étape 6.
2. **Interface Swap** (facultatif) – Échange de l'interface de gestion (eth0) et de la première interface d'avion de données (eth1) au moment du déploiement. L'échange d'interface n'est nécessaire que lorsque vous déployez le pare-feu de la série VM derrière Google Cloud Platform HTTP(S) Load Balancing. Pour plus de détails, reportez-vous à la section Échange de l'interface de gestion pour l'équilibrage de la charge de Google Cloud Platform.
3. **SSH key**—Paste in the public key from an SSH key pair. Suivez les instructions de votre OS dans Paire de clés SSH pour créer, copier et coller la clé. Les utilisateurs de Windows

 ©2023 Palo Alto Networks, Inc.

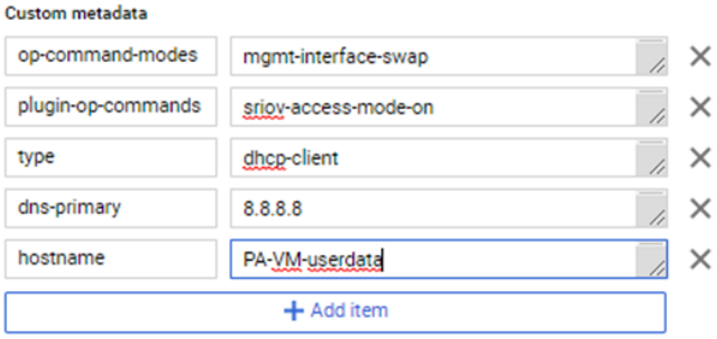
doivent visualiser la clé dans la pompe, copier à partir de l'interface utilisateur et coller dans le déploiement de Marketplace.

Si la clé n'est pas correctement formatée, le pare-feu de la série VM ne vous permet pas d'ouvrir une session. Vous devez supprimer le déploiement et recommencer.

4. Cliquez sur **More** pour afficher d'autres options de métadonnées. Les options **blockProjectKeys**, et **enableSerialConsole** sont les propriétés de l'instance; vous pouvez modifier ces métadonnées après un déploiement réussi.
   - **blockProjectKeys** (facultatif) – Si vous Block Project Keys (bloquez des clés de projet), vous ne pouvez utiliser que la clé publique SSH que vous fournissez pour accéder à l'instance.
   - **enableSerialConsole** (Facultatif)—Interacting with the Serial Console (Interaction avec la console de série) vous permet de surveiller la création d'une instance et d'effectuer des tâches interactives de débogage.

STEP 6 | **Spécifiez les métadonnées personnalisées**.

Si vous choisissez d'amorcer avec des métadonnées personnalisées, ajoutez les paires clé-valeur que vous n'avez pas ajoutées à l'étape 5. Reportez-vous à la section Composants du fichier init-cfg.txt pour consulter la liste des paires clé-valeur. Par exemple :



STEP 7 | **Configurez le disque de démarrage**.

1. **Boot disk type**— Sélectionner dans SSD Persistent Disk ou Standard Persistent Disk. Référez-vous aux Options de stockage.
2. Entrez la **Boot disk size (taille du disque Boot)** – la taille minimale est de 60 Go. Vous pouvez modifier la taille du disque plus tard, mais vous devez arrêter la MV pour ce faire.

STEP 8 | Configurez l'interface de gestion.

1. **Management VPC Network name**—Choisir un réseau existant
2. **Management Subnet name**—Choisissez un sous-réseau existant.
3. **Enable External IP for Management interface** (Facultatif)— Si vous activez cette option, vous pouvez utiliser l'adresse IP attribuée à l'interface de gestion du pare-feu de la série VM pour accéder à l'interface Web du pare-feu de la série VM.
4. **Enable GCP Firewall rule for connections to Management interface** (Activer la règle de pare-feu GCP pour les connexions à l'interface de gestion) (Facultatif) : cette option crée

 ©2023 Palo Alto Networks, Inc.

automatiquement une règle d'autorisation du pare-feu GCP pour une adresse IP source externe que vous fournissez.

5. **Source IP in GCP Firewall rule for connections to Management Interface** (Adresse IP source dans la règle de pare-feu GCP pour les connexions à l'interface de gestion) : si vous **Enable GCP Firewall rule for connections to Management interface** (Activer la règle de pare-feu GCP pour les connexions à l'interface de gestion), saisissez une adresse IP source ou un bloc CIDR.

   - N'utilisez pas 0.0.0.0/0. Fournissez une adresse IP ou un bloc CIDR qui correspond à votre réseau ou vos adresses IP de gestion dédiées. Ne définissez pas la portée du réseau source plus large que nécessaire.
   - Vérifiez l'adresse pour vous assurer de ne pas vous bloquer.

STEP 9 | Configurez l'interface du dataplane non approuvée.

1. **Untrust VPC Network name** (Nom du réseau VPC de l'interface non approuvée) : choisissez un réseau existant.
2. **Untrust Subnet name** (Nom de sous-réseau de l'interface non approuvée) : choisissez un sous-réseau existant.
3. **Enable External IP for Untrust** (Activer l'adresse IP externe pour l'interface non approuvée) : activez GCP pour fournir une adresse IP éphémère servant d'adresse IP externe.

STEP 10 | Configurez l'interface du dataplane approuvée.

1. **Trust VPC Network name** (Nom du réseau VPC approuvé) : choisissez un réseau existant.
2. **Trust Subnet name** (Nom du sous-réseau approuvé) : choisissez un réseau existant.
3. **Enable External IP for Trust** (Activer l'adresse IP externe approuvée) : activez GCP pour fournir une adresse IP éphémère servant d'adresse IP externe.

STEP 11 | Configurez des interfaces supplémentaires. Vous devez saisir le nombre d'interfaces du dataplane que vous souhaitez ajouter. La valeur par défaut est 0 (aucune). La page de déploiement affiche toujours des champs pour cinq plans de données supplémentaires numérotés de 4 à 8.

1. **Additional Dataplane interfaces** (Interfaces du dataplane supplémentaires) : saisissez le nombre d'instances du dataplane supplémentaires.

   Si ce nombre est 0 (valeur par défaut), les numéros du dataplane 4 à 8 sont ignorés même si vous remplissez les champs de l'interface. Si, par exemple, vous spécifiez 2 puis complétez les informations pour trois interfaces, seules les deux premières interfaces sont créées.

2. **Additional Dataplane # VPC name** (Nom VPC du numéro du dataplane supplémentaire) : choisissez un réseau existant.
3. **Dataplane # Subnet name** (Nom du sous-réseau du numéro du dataplane) : choisissez un sous-réseau existant.
4. **Enable External IP for dataplane # interface** (Activer l'adresse IP externe pour l'interface du numéro du dataplane) : activez GCP pour fournir une adresse IP éphémère servant d'adresse IP externe.

 ©2023 Palo Alto Networks, Inc.

STEP 12 | **Déployez** l'instance.

STEP 13 | Utilisez la section Gestionnaire de déploiement Google Cloud pour visualiser et gérer votre déploiement.

STEP 14 | Utilisez la CLI pour modifier le mot de passe de l'administrateur sur le pare-feu.

1. Connectez-vous au pare-feu VM-Series à partir de la ligne de commande. Dans votre outil SSH, connectez-vous à l'adresse IP externe de l'interface de gestion et spécifiez le chemin d'accès à votre clé privée.

   Utilisateurs Windows : utilisez PuTTY pour vous connecter au pare-feu VM-Series et émettre des instructions de ligne de commande. Pour spécifier le chemin d'accès à la clé privée, sélectionnez **Connection (Connexion)** > **SSH** > **Auth**. Dans **Private key file for authentication** (Fichier de clé privée pour l'authentification) : cliquez sur **Browse** (Parcourir) pour sélectionner votre clé privée.
2. Passez en mode configuration :

   ```
   VMfirewall> configure
   ```
3. Saisissez la commande suivante :

   ```
   VMfirewall# set mgt-config users admin password
   ```
4. Saisissez et confirmez un nouveau mot de passe pour l'administrateur.
5. Validez votre nouveau mot de passe :

   ```
   VMfirewall# commit
   ```
6. Revenez au mode de commande :

   ```
   VMfirewall# exit
   ```
7. (Facultatif) Si vous avez utilisé un fichier d'amorçage pour la permutation d'interface, utilisez la commande suivante pour afficher le mappage d'interface :

   ```
   VMfirewall> debug show vm-series interfaces all
   ```

STEP 15 | Accédez à l'interface Web du pare-feu VM-Series.

1. Dans un navigateur, créez une connexion sécurisée (https) à l'adresse IP de l'interface de gestion.

   Si vous obtenez une erreur réseau, vérifiez que vous avez une règle de pare-feu GCP autorisant la connexion.
2. Lorsque vous y êtes invité, saisissez le Username (Nom d'utilisateur) (admin) et le Password (Mot de passe) administrateur que vous avez spécifié à partir de la CLI.
3. (Facultatif) Si vous avez amorcé, alors procédez à la Vérification de l'achèvement de l'amorçage.

   Si vous rencontrez des problèmes, recherchez les informations de journal sur le pare-feu VM-Series. Choisissez **Monitor (Surveillance)** > **System (Système)** et, dans le champ de recherche manuelle, saisissez **`description contains 'bootstrap'`** et recherchez dans les résultats un message indiquant que l'amorçage a réussi.

Une fois connecté au pare-feu, vous pouvez ajouter des administrateurs et créer des interfaces, des zones, des règles NAT et des règles de politique, comme vous le feriez avec un pare-feu physique.

 ©2023 Palo Alto Networks, Inc.

Échange de l'interface de gestion pour l'équilibrage de la charge de Google Cloud Platform

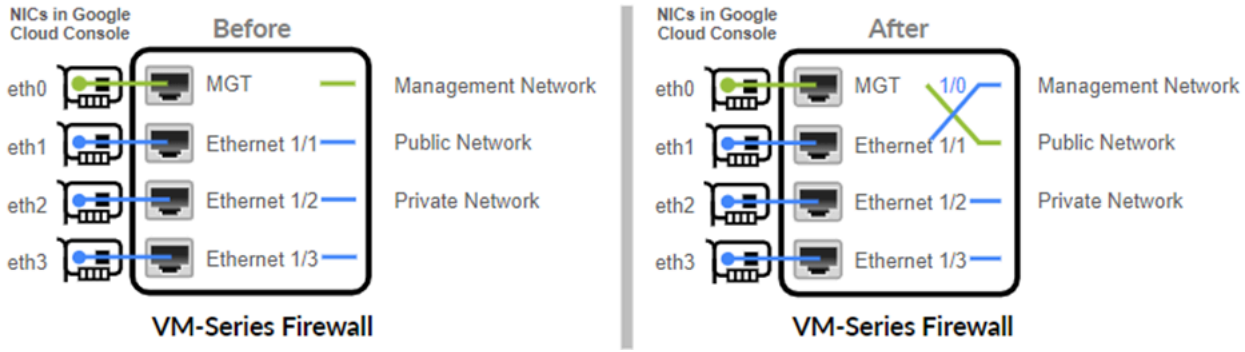
Étant donné que l'équilibrage de charge interne peut envoyer du trafic uniquement vers l'interface principale de l'instance Google Compute Engine à charge équilibrée suivante, le pare-feu VM-Series doit pouvoir utiliser eth0 pour le trafic du dataplane.

Le pare-feu peut recevoir le trafic du dataplane sur eth0 si le pare-feu VM-Series est derrière l'interface d'équilibrage de charge interne de Google Cloud Platform.

- Les pare-feu VM-Series sécurisent le trafic sortant directement vers Internet sans nécessiter de liaison VPN ou de liaison directe vers le réseau d'entreprise.
- Le pare-feu VM-Series sécurise une application Web lorsqu'il y a exactement un serveur dorsal, comme un serveur Web, pour chaque pare-feu. Les pare-feu et les serveurs Web de la série VM peuvent évoluer linéairement, par paires, derrière l'adresse d'équilibrage de charge interne de Google.

Pour permettre au pare-feu d'envoyer et de recevoir le trafic du dataplane sur eth0 au lieu de eth1, vous devez permuter le mappage de l'interface réseau d'équilibrage de charge interne dans le pare-feu afin que eth0 soit mappé à Ethernet 1/1 et eth1 à l'interface MGT.

Si possible, permutez l'association de l'interface de gestion avant de configurer le pare-feu et de définir des règles de politique.



La permutation avec laquelle les interfaces sont mises en correspondance permet à Google Cloud Platform pour distribuer et acheminer le trafic vers les instances en bonne santé du pare-feu VM-Series situés dans les zones identiques ou différents.

Permuter l'interface de gestion

Vous pouvez permuter les interfaces ou vous pouvez configurer le pare-feu après sa création.

Au moment de la création — Lorsque vous déployez le pare-feu de la série VM, vous pouvez activer l'échange d'interface de deux façons.

- Google Cloud Console — Dans le formulaire Create Instance, entrez une paire de valeurs clés dans le champ **Metadata** où **`mgmt-interface-swap`** est la clé et **`enable`** est la valeur.
- Fichier Bootstrap — Créer un fichier bootstrap qui comprend la commande opérationnelle **`mgmt-interface-swap`** dans la configuration bootstrap, comme décrit dans Bootstrap the VM-Series

©2023 Palo Alto Networks, Inc.

Firewall sur Google Cloud Platform. Dans le formulaire Créer une instance, entrez une paire clé-valeur dans le champ **Metadata (Métadonnées)** pour activer l'option d'amorçage.

À partir du pare-feu VM-Series : connectez-vous au pare-feu et utilisez l'interface CLI du pare-feu VM-Series pour permuter l'interface de gestion. Passez en mode Operational (Opérationnel) pour exécuter les commandes suivantes :

```
set system setting mgmt-interface-swap enable yes
```

- *Choisissez une méthode pour spécifier le paramètre d'échange d'interface: le fichier de configuration bootstrap, l'interface CLI du pare-feu ou le champ **Metadata (Métadonnées)** de l'instance Google Compute Engine (accessible depuis Google Cloud Console). L'utilisation d'une méthode garantit un comportement prévisible sur le pare-feu.*

  Dans Google Cloud Console, vous ne pouvez pas confirmer si vous avez échangé eth0 et eth1. Après la permutation, vous devez vous rappeler que l'équilibrage de charge est sur eth0 et que l'interface de gestion du pare-feu est eth1. Vous pouvez ainsi configurer l'équilibrage de charge de Google Cloud Platform et créer des règles de sécurité pour sécuriser l'équilibrage de charge sur un ou plusieurs pare-feu VM-Series.
- *Si vous avez configuré le pare-feu VM-Series avant la permutation, vérifiez si des adresses IP ont été modifiées pour eth0 et eth1.*

Utilisation de la CLI du pare-feu VM-Series pour permuter l'interface de gestion

Cette tâche est uniquement requise si votre architecture place le pare-feu VM-Series derrière l'équilibreur de charge interne de Google Cloud Platform.

Si vous n'avez pas permuté l'interface de gestion (MGT) avec l'interface du dataplane lors du déploiement du pare-feu, vous pouvez utiliser la CLI pour permettre au pare-feu de recevoir le trafic du dataplane sur l'interface principale.

STEP 1 | Déployer le pare-feu de la série VM à partir du marché de la plateforme Google Cloud Launcher.

Avant de continuer, vérifiez que le pare-feu possède au moins deux interfaces réseau (eth0 et eth1). Si vous lancez le pare-feu avec une seule interface, la commande de permutation d'interface provoquera l'amorçage du pare-feu en mode maintenance.

STEP 2 | Sur Google Cloud Console, affichez les détails de l'instance de machine virtuelle pour vérifier les adresses IP de l'interface réseau de l'interface eth1 et vérifiez que les règles de sécurité autorisent les connexions (HTTPS et SSH) à la nouvelle interface de gestion (eth1).

STEP 3 | Connectez-vous à la CLI du pare-feu VM-Series et saisissez la commande suivante :

```
set system setting mgmt-interface-swap enable yes
```

Vous pouvez afficher le mappage par défaut à partir de l'interface de ligne de commande. Le résultat ressemble à ceci :

 ©2023 Palo Alto Networks, Inc.

```
> debug show vm-series interfaces all Interface_name Base-
OS_port   mgt              eth0   Ethernet1/1      eth1
   Ethernet1/2      eth2
```

STEP 4 | Confirmez que vous voulez permuter l'interface (utiliser l'interface du dataplane eth1 comme interface de gestion).

STEP 5 | Redémarrez le pare-feu pour que la permutation prenne effet :

```
request restart system
```

STEP 6 | Vérifiez que les interfaces ont été permutées :

```
debug show vm-series interfaces all
```

Activation de la surveillance CloudWatch sur le VM-Series Firewall (pare-feu de la série VM)

Un pare-feu VM-Series sur une instance de Google® Compute Engine peut publier des métriques PAN-OS personnalisées sur Google Stackdriver. Ces métriques vous permettent d'évaluer les performances et les modèles d'utilisation, ce qui vous permet de gérer les ressources de votre pare-feu en conséquence.

- Les permissions de Google Stackdriver
- Activer Google Stackdriver

Les permissions de Google Stackdriver

Les exigences d'authentification varient selon que vous pouvez utiliser le compte de service par défaut pour authentifier ou que vous devez utiliser les API de Google pour authentifier.

Vous pouvez vous authentifier de deux façons :

- **Utilisez le compte de service par défaut pour l'instance VM-Series Firewall** – Si vous utilisez la console de Google Cloud Platform (GCP™), vous avez ouvert une session avec votre adresse de courriel et pouvez accéder à l'instance en fonction des permissions ou des rôles que l'administrateur de projet a attribués à votre compte.
- **Utilisez les autorisations IAM et les API Google** - Si vous utilisez les API Google SDK et gcloud, vous devez appeler les API pour vous authentifier. Vous utilisez habituellement le SDK de Google lorsque vous voulez gérer le pare-feu à partir d'une ligne de commande ou lorsque vous voulez exécuter un script pour configurer le pare-feu.

Chaque instance Google Compute Engine créée avec la console Google Cloud ou l'outil de ligne de commande gcloud possède un compte de service par défaut dont le nom figure au format d'adresse e-mail :

```
<project-number>-compute@developer.gserviceaccount.com
```

Pour voir le nom du compte de service pour l'instance du pare-feu, voir les détails de l'instance et faire défiler l'écran jusqu'au bas (voir le compte de service par défaut du moteur de calcul).

 ©2023 Palo Alto Networks, Inc.

Le compte de service par défaut peut gérer l'authentification pour surveiller les machines virtuelles dans le même projet qu'un pare-feu VM-Series.

- Les champs d'accès permettent au pare-feu de lancer des appels API pour surveiller les MV dans un projet de Google Cloud.
- Vous n'avez pas besoin d'accéder aux API Google, sauf si l'une des machines virtuelles contrôlées possède une image personnalisée avec des applications nécessitant des API de Google.

Si vous souhaitez configurer la surveillance à partir d'un pare-feu physique ou d'un pare-feu VM-Series dans un projet différent, vous devez utiliser les API de Google pour vous authentifier. Il y a deux conditions préalables :

- Les API Google doivent être installées.
- Votre compte doit avoir le rôle de rédacteur de mesures et de visualisateur de compte de Stackdriver.

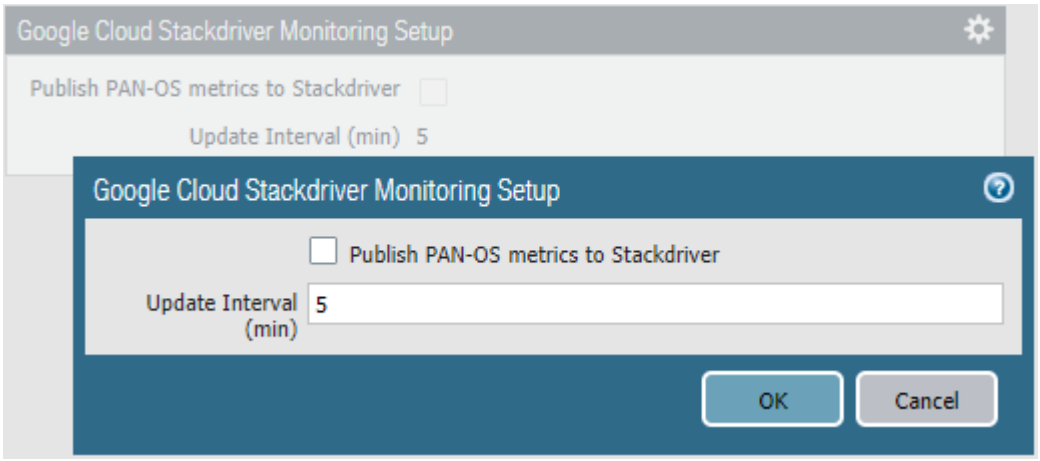
Activer Google Stackdriver

Pour obtenir une description des métriques PAN-OS que vous pouvez publier sur Google Stackdriver, consultez la rubrique métriques PAN-OS personnalisées publiées pour la surveillance.

STEP 1 | Transmettez les métriques PAN-OS à partir d'un pare-feu VM-série sur une instance Google Compute Engine Stackdriver.

1. Connectez-vous à l'interface Web sur le pare-feu VM-Series.
2. Sélectionnez **Device (Appareil)** > **VM-Series**. Sous Google Cloud Stackdriver Monitoring Setup, cliquez sur **Modifier** ( ).

   1. Cochez la case **Publish PAN-OS metrics to Stackdriver (Publier les métriques PAN-OS sur Stackdriver)**.



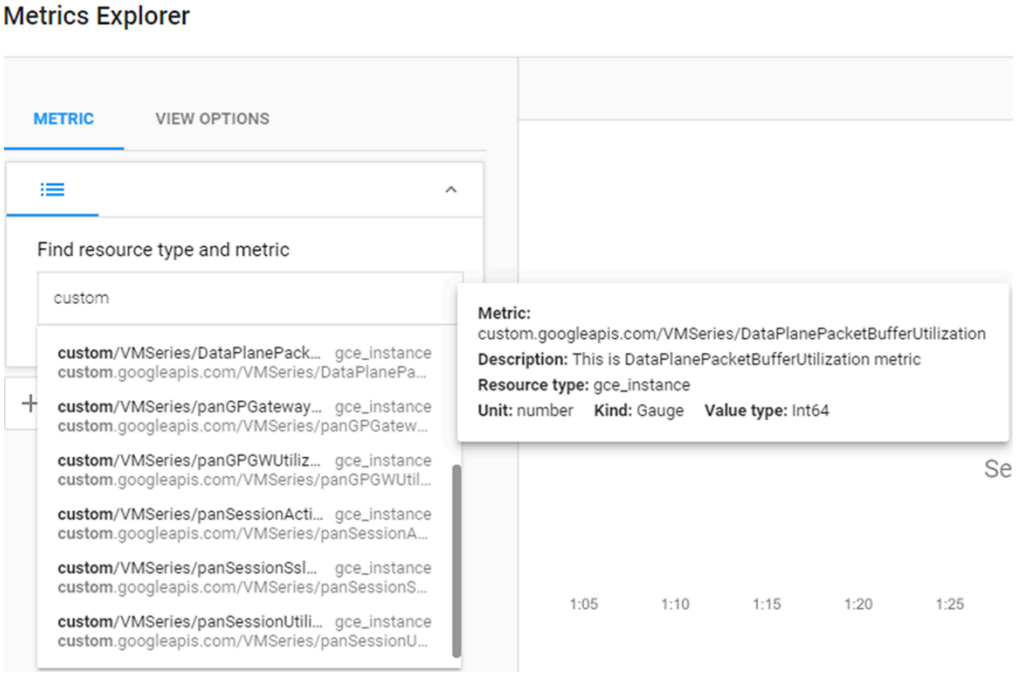
   2. Etablir **l'intervale de mise à jour** (de 1 à 60 minutes; par défaut, 5). Il s'agit de la fréquence à laquelle le pare-feu publie les métriques dans Stackdriver.
   3. Cliquez sur **OK**.
3. **Commit (Validez)** vos modifications.

   Attendez que le pare-feu commence à publier des métriques sur Stackdriver avant de configurer les alarmes pour les métriques PAN-OS.

©2023 Palo Alto Networks, Inc.

STEP 2 | Vérifiez que vous pouvez voir les métriques sur Stackdriver.

1. Dans Google Cloud Console, sélectionnez **Products and Services (Produits et services)** > **Monitoring (Surveillance)**.
2. Dans Stackdriver, choisissez **Resources (Ressources)** > **Metrics Explorer (Explorateur de statistiques)**.
3. Dans la section Trouver le type de ressource et la métrique, saisissez le paramètre **`personnalisé`** dans le champ de recherche pour filtrer les paramètres PAN-OS.



STEP 3 | Configurez les alertes et les actions pour les métriques PAN-OS sur Stackdriver. Voir Démarrage rapide de la surveillance pour Google Compute Engine, et Présentation des alertes Stackdriver.

Permettre la surveillance de la MV pour suivre les changements de VM sur la plateforme de Google Cloud (GCP)

Vous pouvez activer n'importe quel pare-feu exécutant PAN-OS 9.0 (virtuel ou physique) pour la surveillance des charges de travail d'applications déployées sur des instances de Google Compute Engine. VM Monitoring vous permet de surveiller un ensemble prédéfini d'éléments ou d'attributs de métadonnées sur le pare-feu VM-Series. Dans le Guide de l'administrateur PAN-OS 9.1, reportez-vous à la section Attributs surveillés sur les machines virtuelles dans les plateformes en cloud.

En connaissant les ajouts, les déplacements ou les suppressions de machines virtuelles dans un VPC Google, vous pouvez créer des règles de stratégie de sécurité qui s'adaptent automatiquement aux modifications de votre environnement d'application. Lorsque vous déployez ou déplacez des machines virtuelles, le pare-feu recueille des attributs (ou des éléments de métadonnées). Vous pouvez utiliser ces métadonnées pour la correspondance de stratégie ou pour définir des groupes d'adresses dynamiques (Reportez-vous à la section Utiliser des groupes d'adresses dynamiques pour sécuriser des instances dans le VPC).

 ©2023 Palo Alto Networks, Inc.

Vous pouvez configurer jusqu'à dix sources d'informations de machine virtuelle sur chaque pare-feu ou sur chaque système virtuel sur un pare-feu capable de gérer plusieurs systèmes virtuels. Les sources d'informations peuvent également être poussées à l'aide de modèles Panorama.

Pour effectuer la surveillance de la VM, vous devez avoir le rôle de rédacteur de mesures de surveillance de la IAM.

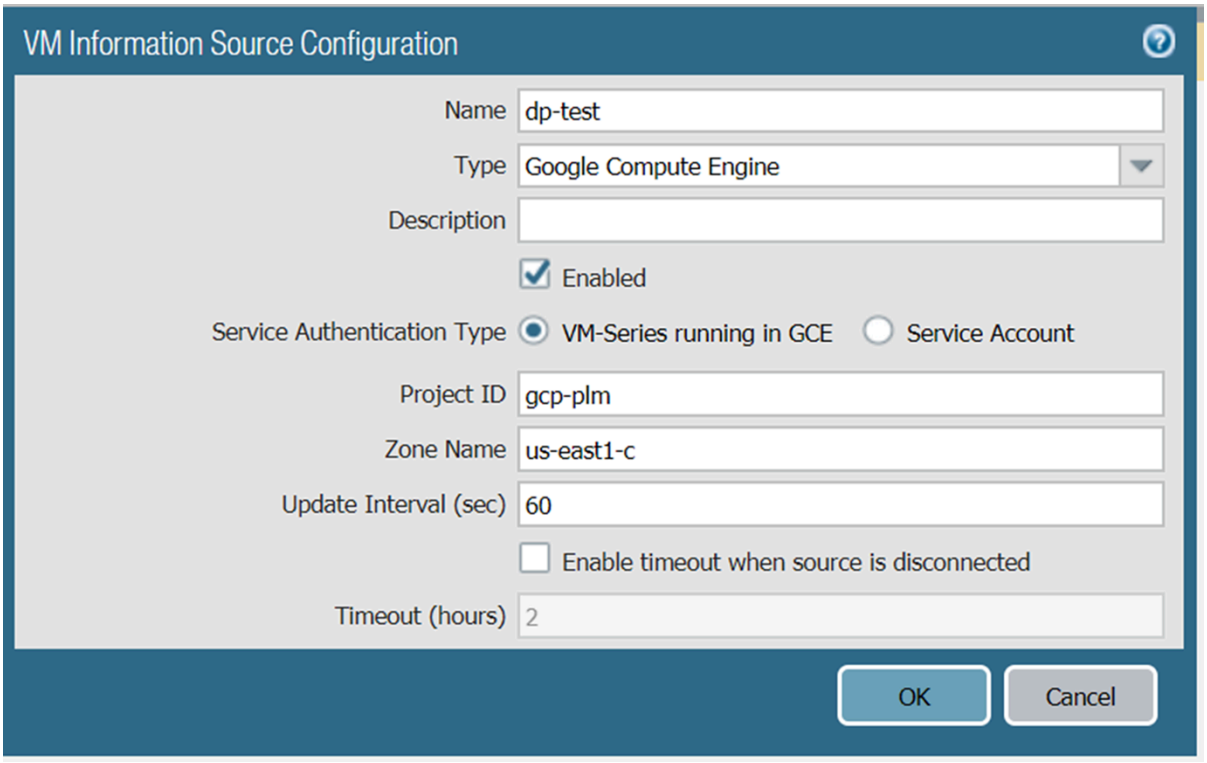
STEP 1 | Connectez-vous à votre pare-feu déployé.

STEP 2 | Activez la surveillance des machines virtuelles.

1. Sélectionnez **Device (Appareil)** > **VM Information Sources (Sources d'informations de machine virtuelle)**.
2. **Ajoutez** une source d'information VM et entrez les renseignements suivants :
   - Spécifiez un **Name (Nom)** pour identifier l'instance que vous souhaitez surveiller.
   - Sélectionnez le **Type** de Google Compute Engine.
   - Sélectionnez **Enabled (Activé)**.
   - Choisissez le **Service Authentication Type (Type d'authentification du service)**.
     - Si vous choisissez **VM-Series running in GCE (VM-Series s'exécutant dans GCE)**, vous devez vous authentifier au moyen du compte de service par défaut généré lors de la création d'une instance. Cela fait partie des métadonnées de l'instance.
     - Si vous voulez effectuer une surveillance à partir d'un pare-feu à l'extérieur du projet actuel, choisissez **Service Account**. Vous devez télécharger les justificatifs d'identité du service account (compte de service) en format JSON. Voir Création et gestion des clés de compte de service.
   - (Facultatif) Modifiez l'**Update interval (Intervalle de mise à jour)** sur une valeur entre 5 et 600 secondes. Par défaut, le pare-feu effectue des recherches toutes les 5 secondes. Les appels API sont mis en file d'attente et récupérés toutes les

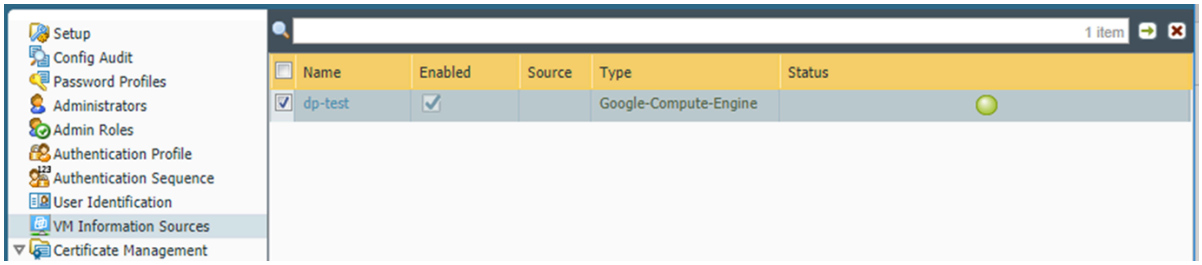
 ©2023 Palo Alto Networks, Inc.

60 secondes. Par conséquent, les mises à jour peuvent prendre 60 secondes plus l'intervalle d'interrogation donné.



- (Facultatif) Pour modifier le nombre d'heures avant le temps d'arrêt, vérifiez **Activer le temps d'arrêt lorsque la source est débranchée** et entrez le temps d'arrêt (heures) avant que la connexion à la source surveillée ne soit fermée (la plage est de 2 à 10 ; la valeur par défaut est 2).

  Si le coupe-feu ne peut pas accéder à l'hôte et que la limite spécifiée est atteinte, le coupe-feu ferme la connexion à la source.
- Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.



STEP 3 | Vérifiez l'état de la connexion.

Si l'état de connexion est Pending (En attente) ou Disconnected (Déconnecté), vérifiez que la source est opérationnelle et que le pare-feu peut accéder à la source. Si vous utilisez un autre port que le port de gestion MGT pour la communication avec la source surveillée, vous devez modifier l'itinéraire de service (sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Services**, cliquez sur **Service Route Configuration (Configuration de l'itinéraire de service)** et modifiez la **Source Interface (Interface source)** du service **VM Monitor (Surveillance des machines virtuelles)**).

©2023 Palo Alto Networks, Inc.

Utilisation de groupes d'adresses dynamiques pour sécuriser des instances dans VPC

Dans un environnement dynamique tel que Google Cloud Platform, où vous lancez de nouvelles instances à la demande, la charge administrative liée à la gestion des stratégies de sécurité peut être lourde. Procédez à l'utilisation de groupes d'adresses dynamiques dans la politique permet d'assurer la souplesse et de prévenir les interruptions de services ou les failles dans la protection.

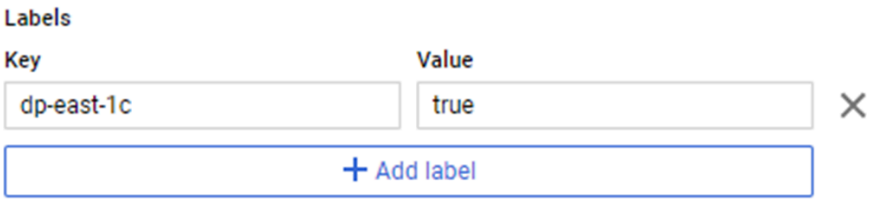
Ce flux de travail suppose que vous avez déployé le pare-feu de la série VM, configuré certaines applications sur des instances et activé la surveillance de Google Stackdriver.

STEP 1 | Configurez le pare-feu pour qu'il surveille le VPC.

STEP 2 | Étiquetez les instances dans le VPC.

Une étiquette est une paire nom-valeur. Vous pouvez étiqueter des ressources à partir de Google Cloud Console, à partir d'appels d'API Google ou à partir de Google Cloud Shell. Dans cette tâche, nous étiquetons des instances ; mais les étiquettes peuvent être appliquées à de nombreuses ressources, comme indiqué à la section Ressources d'étiquetage.

Vous pouvez également ajouter des étiquettes à partir du navigateur d'instance.

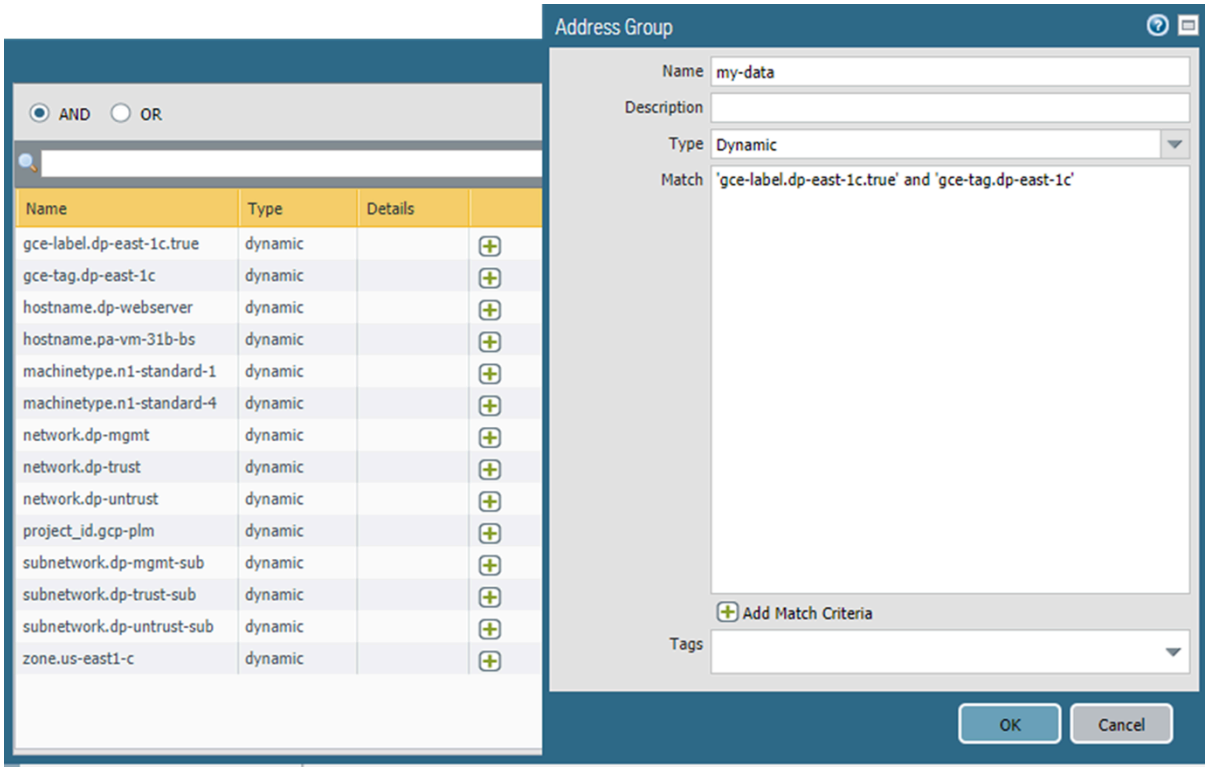


Les étiquettes que vous créez prennent en charge votre politique de différenciation de vos ressources d'une manière utile à votre stratégie de sécurité.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Créez un groupe d'adresses dynamiques sur le pare-feu.

1. Sélectionnez **Objects (Objets)** > **Address Groups (Groupes d'adresses)**.
2. Cliquez sur **Add** (Ajouter) pour ajouter un groupe d'adresses dynamiques et précisez un **Name** (Nom) et une **Description**.
3. Définissez **Type** sur **Dynamic (Dynamique)**.
4. Définissez les critères de correspondance.
   1. Cliquez sur **Add Match Criteria (Ajouter un critère de correspondance)**, puis sélectionnez l'opérateur **And (Et)** opérateur.
   2. Sélectionnez les attributs de filtrage ou de correspondance.



5. Cliquez sur **OK**.
6. Cliquez sur **Commit (Valider)**.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Utilisez le groupe d'adresses dynamiques dans une règle de politique de sécurité.

Créez une règle pour autoriser l'accès à Internet à tout serveur Web appartenant au groupe d'adresses dynamiques appelé my-data.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Cliquez sur **Add** (Ajouter) pour ajouter une règle et un **Name** (Nom) pour la règle et vérifiez que le **Rule Type** (Type de règle) est `universal` (universel).
3. Dans l'onglet **Source**, ajoutez Approuvée en tant que **Source Zone (Zone source)**.
4. Dans la section Source Address (Adresse source), cliquez sur **Add** (Ajouter) pour ajouter votre nouveau groupe my-data.
5. Dans l'onglet **Destination**, ajoutez Non approuvée en tant que **Destination Zone (Zone de destination)**.
6. Dans l'onglet **Service/URL Category (Catégorie de service/d'URL)**, vérifiez que le service est défini sur **application-default (Par défaut de l'application)**.
7. Dans l'onglet **Actions**, définissez la valeur **Action** sur Autoriser.
8. Dans les Profile Settings (Paramètres de profil), définissez les **Profile Type** (Type de profils) sur **Profiles** (Profils), puis joignez les profils par défaut pour Antivirus, Anti-Spyware et Vulnerability Protection (Protection contre les vulnérabilités).
9. Cliquez sur **OK**.
10. Cliquez sur **Commit (Valider)**.

STEP 5 | Vérifiez que les membres du groupe d'adresses dynamiques sont renseignés sur le pare-feu.

La politique est appliquée à toutes les adresses IP qui appartiennent à ce groupe d'adresses et s'affichent ici.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis choisissez la règle.
2. Sélectionnez **Inspect** (Inspecter) dans la liste déroulante. Vous pouvez également vérifier que les critères de correspondance sont corrects.
3. Cliquez sur **more** (plus) pour vérifier que la liste des adresses IP enregistrées s'affiche.

Utiliser des modèles personnalisés ou le CLI de l'infonuagique pour déployer le Pare-feu de la série VM

Les images officielles de la série VM publiées sur Google Cloud Platform Marketplace sont disponibles dans le projet **`paloaltonetworksgcp-public`**. Vous devez connaître le chemin d'accès sécurisé à ces images si vous voulez les appeler à partir de la ligne de commande **`gcloud`** ou vous y référer dans un modèle que vous avez écrit ou adapté.

- BYOL : vmseries-byol-*<version>*
- Forfait PAYG 1 : vmseries-bundle1-*<version>*
- Forfait PAYG 2 : vmseries-bundle2-*<version>*

Utilisez le CLI de l'infonuagique pour trouver les noms d'image actuels et le projet :

```
gcloud compute images list --project paloaltonetworksgcp-public
 --no-standard-images   NAME PROJECT FAMILY DEPRECATED STATUS
```

 ©2023 Palo Alto Networks, Inc.

```
   vmseries-bundle1-810 paloaltonetworksgcp-public READY   vmseries-
bundle2-810 paloaltonetworksgcp-public READY   vmseries-byol-810
 paloaltonetworksgcp-public READY
```

Ajouter l'indicateur **--uri** pour voir les chemins d'accès aux images :

```
  gcloud compute images list --project paloaltonetworksgcp-public
   --no-standard-images --uri
```

```
  https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-
public   /global/images/vmseries-bundle1-810   https://
www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-public
   /global/images/vmseries-bundle2-810   https://www.googleapis.com/
compute/v1/projects/paloaltonetworksgcp-public   /global/images/
vmseries-byol-810
```

Pour voir un exemple, téléchargez le modèle gcp-two-tier sur le site https://github.com/PaloAltoNetworks.

Ce modèle sépare le nom de l'image (qui comprend la version PAN-OS) du chemin d'accès à l'URL. Dans `two-tier-template.py` la variable ***image*** s'attend au nom de l'image ; par exemple : *vmseries-byol-810*. `vm-series-template.py` utilise les valeurs de ***COMPUTE_URL_BASE*** et ***sourceImage*** pour créer le chemin d'accès.

©2023 Palo Alto Networks, Inc.

Surveillance VM avec le plugin Panorama pour GCP

Le plug-in Panorama pour Google Cloud Platform (GCP) version 2.0.0 vous permet de créer une configuration de surveillance VM qui s'authentifie avec un projet GCP et surveille les pare-feu VM-Series et les autres VM déployées en son sein. Lorsque vous établissez une connexion à votre projet, le plug-in peut récupérer la communication IP-address-to-tag entre Panorama et les ressources GCP. Les étiquettes peuvent être des attributs prédéfinis, des étiquettes définies par l'utilisateur pour les VM et des étiquettes de réseau définies par l'utilisateur (voir Examiner et créer des étiquettes).

Le plug-in Panorama pour GCP récupère les adresses IP internes et externes à partir des VM en cours d'exécution, et récupère périodiquement les mappages IP-to-tag à partir des VM dans les VPC GCP connectés.

Vous pouvez utiliser des étiquettes pour organiser les VM en groupes d'adresses dynamiques, puis référencer vos étiquettes dans les règles de politique de sécurité qui autorisent ou interdisent le trafic vers des adresses IP de VM spécifiques. Pour appliquer la politique de sécurité de manière constante, vous pouvez ensuite appliquer des règles à vos pare-feu VM-Series.

- Configuration de la surveillance VM avec le plugin Panorama pour GCP

Configuration de la surveillance VM avec le plugin Panorama pour GCP

Cette rubrique décrit les étapes de préparation de vos ressources GCP pour la surveillance VM, passe en revue les éléments Panorama requis et décrit comment configurer la surveillance VM dans le plugin Panorama pour Google Cloud Platform (GCP).

- Configurer les ressources GCP pour la surveillance VM
- Examiner et créer des étiquettes
- Configuration de la surveillance VM avec le plugin Panorama pour GCP
  - Préparer Panorama pour configurer la surveillance VM
  - Configurer la surveillance VM

Configurer les ressources GCP pour la surveillance VM

Vous pouvez surveiller les pare-feu VM-Series que vous avez déployés depuis GCP Marketplace, les pare-feu que vous avez déployés avec des modèles de pare-feu de mise à l'échelle automatique, les instances GCE que vous avez créées depuis la console GCP ou de la ligne de commande gcloud, ou d'autres machines virtuelles déployées dans GCP. Si vous déployez des VM PAN-OS depuis Marketplace, suivez les instructions de la section Configuration du pare-feu VM-Series sur la plateforme Google Cloud.

Examiner les rôles IAM

Assurez-vous de disposer des autorisations minimales suivantes pour les tâches de surveillance VM :

©2023 Palo Alto Networks, Inc.

- Dans la console GCP, créez un compte de service pour votre projet et accordez la permission de propriétaire ou éditeur du projet.

  La création d'un compte de service ne peut pas être automatisée. Si vous n'avez pas l'autorisation de créer un compte de service, vous pouvez demander à un administrateur de le créer et de vous attribuer un rôle approprié.
- Consultez votre compte de service : lecture seule.
- Consultez les VM PAN-OS déployées depuis Google Marketplace : Compute Viewer.
- Attribuez une étiquette définie par l'utilisateur à une instance : propriétaire ou éditeur du projet, ou administrateur de l'instance.

Créer un compte de service

Avant d'utiliser le plugin GCP sur Panorama pour configurer la surveillance VM, vous devez utiliser la console GCP pour créer un compte de service qui accorde des autorisations d'accès à votre projet GCP, aux pare-feu VM-Series déployés dans celui-ci, à toutes les autres VM que vous souhaitez que Panorama gère, ainsi qu'aux réseaux et sous-réseaux connexes. Le plugin GCP pour Panorama récupère des attributs prédéfinis pour les ressources Google, des étiquettes de VM définies par l'utilisateur et des étiquettes de réseau définies par l'utilisateur.

Chaque projet dispose d'un compte de service par défaut qui a été automatiquement créé lors de la création du projet. Si vous créez un compte de service distinct spécifiquement pour la surveillance VM, vous avez un meilleur contrôle des utilisateurs et de leurs rôles. Vous pouvez configurer jusqu'à 100 comptes de service par projet.

STEP 1 | Dans la console Google Cloud Platform, sélectionnez le projet que vous souhaitez surveiller.

STEP 2 | Sélectionnez **IAM & Admin (IAM et administrateur)** > **Service accounts (Comptes de service)** et choisissez **+Create Service Account (Créer un compte de service)**.

Saisissez le nom et la description du compte de service, puis cliquez sur **Create (Créer)**.

STEP 3 | Sélectionnez un type de rôle dans le menu déroulant et, à droite, sélectionnez un niveau d'accès approprié.

Par exemple, sélectionnez Project (Projet) > Editor (Éditeur). Vous pouvez sélectionner plusieurs rôles pour un compte de service.

Lorsque vous avez terminé, cliquez sur **Continue (Continuer)**.

STEP 4 | Accordez à des utilisateurs spécifiques l'autorisation d'accéder à ce compte de service. Sélectionnez les membres dans la colonne **Permissions (Autorisations)** à droite pour leur donner l'autorisation d'accéder aux rôles de l'étape précédente.

STEP 5 | (Facultatif) Cliquez sur **+CREATE KEY (Créer une clé)** pour créer des informations d'identification qui vous permettent de vous authentifier auprès de la CLI Google Cloud pour accéder aux pare-feu VM-Series, aux réseaux et aux autres VM associés à ce compte de service.

La clé est téléchargée automatiquement. Veillez à la conserver dans un endroit sûr. Le format JSON de la clé privée générée est le suivant :

```
{ "type": "service_account", "project_id": "gcp-xxx",
 "private_key_id": "252e1e7a2e9c84b5d4dbb6195b1de074594b6499",
```

 ©2023 Palo Alto Networks, Inc.

```
 "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDAd0i
+RMKCtrsO\n4KHnzTAPrgoBjRgpjyNcvQmdUqHr\n-----END PRIVATE
 KEY-----\n", "client_email": "dlp-vm-monit-svc-acct@gcp-
xxx.iam.gserviceaccount.com", "client_id": "108932514695821539229",
 "auth_uri": "https://accounts.google.com/o/oauth2/auth",
 "token_uri": "https://oauth2.googleapis.com/token",
 "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/
v1/certs", "client_x509_cert_url": "https://www.googleapis.com/
robot/v1/metadata/x509/dlp-vm-monit-svc-acct%40gcp-
xxx.iam.gserviceaccount.com" }
```

Examiner et créer des étiquettes

« Étiquette » est un terme général qui désigne des attributs prédéfinis, des étiquettes définies par l'utilisateur et des étiquettes de réseau définies par l'utilisateur.

- Les étiquettes prédéfinies (attributs) sont automatiquement créées pour les VM Google. Lorsque vous configurez la surveillance VM, vous pouvez choisir de surveiller les 8 attributs prédéfinis, ou vous pouvez créer une liste personnalisée d'attributs à surveiller.
- Vous pouvez définir vos propres étiquettes pour les étiquettes de VM et les étiquettes de réseau.

Étiquetez les VM et les réseaux pour que vous puissiez les identifier et les regrouper afin de pouvoir structurer les règles pour appliquer la politique de sécurité. Vous pouvez étiqueter toute VM déployée dans votre projet Google, par exemple un pare-feu VM-Series, un serveur Web, un serveur d'application ou un équilibreur de charge.

- Les étiquettes doivent être associées à une VM. Cela s'applique également aux réseaux et aux sous-réseaux.
- Si plusieurs adresses IP sont associées à une instance (par exemple si vous avez étiqueté les interfaces approuvées et non approuvées du pare-feu VM-Series), Panorama génère plusieurs ensembles d'informations d'étiquettes.

Le nombre total d'étiquettes que le plugin Panorama peut récupérer et enregistrer dépend de la version de PAN-OS que Panorama exécute et de la version des pare-feu VM-Series gérés.

La zone Google, la région Google, le nom du VPC et le nom du sous-réseau sont utilisés pour étiqueter les interfaces réseau sur les VM à interfaces multiples spécifiques à l'interface réseau.

Attributs prédéfinis

Le plugin Google Cloud Platform pour Panorama récupère les étiquettes prédéfinies suivantes à partir de n'importe quelle VM gérée :

- **Project ID (ID du projet)** : par exemple, google.project-id.myProjectId.

  Pour trouver les informations sur votre projet dans la console Google, sélectionnez votre projet, puis **IAM & Admin (IAM et administrateur)** > **Settings (Paramètres)**.
- **Service account (Compte de service)** : votre compte de service sous la forme d'une adresse e-mail. Par exemple, google.svc-accnt.sa-name@project-id.iam.gserviceaccount.com.

  Pour trouver votre compte de service, consultez les détails de l'instance VM.
- **VPC name (Nom du VPC)** : le nom du réseau VPC pour une VM gérée. Par exemple, google.vpc-name.myvnet.

 ©2023 Palo Alto Networks, Inc.

- **Subnet name (Nom du sous-réseau)** : le nom d'un sous-réseau que vous avez créé pour une interface de VM gérée. Par exemple, pour l'interface non approuvée du pare-feu VM-Series, le nom du sous-réseau que vous avez créé pour l'interface non approuvée : google.subnet-name-untrust.web.
- **OS SKU (SKU du système d'exploitation)** : le système d'exploitation que vous avez choisi lorsque vous avez déployé la VM gérée. Par exemple, google.os-sku.centos-7.

  Cet attribut n'est pas pris en charge si la VM utilise une image personnalisée.

- **Google zone (Zone Google)** : la zone que vous avez sélectionnée lorsque vous avez déployé la VM. Par exemple, google.zone.us-east1-c.
- **Google region (Région Google)** : la région contenant la zone que vous avez sélectionnée. Par exemple, google.region.us-east1.
- **Instance group name (Nom du groupe d'instances)** : par exemple, google.instance-group.myInstanceGroup. Pour afficher ou créer un groupe d'instances dans la console Google, sélectionnez **Compute Engine** > **Instance Group (Groupe d'instances)**.

Étiquettes définies par l'utilisateur

Panorama utilise jusqu'à 16 étiquettes définies par l'utilisateur. Si vous avez plus de 16 étiquettes, Panorama classe vos étiquettes par ordre alphabétique et utilise les 16 premières étiquettes.

Consultez les exigences de Google concernant les paires clé-valeur des étiquettes : les clés ont une longueur minimale de 1 caractère et une longueur maximale de 63 caractères, et ne peuvent pas être vides. Les valeurs peuvent être vides et ont une longueur maximale de 63 caractères.

Pour créer ou afficher des étiquettes dans la console GCP, accédez à **Compute Engine** > **VM Instances (Instances VM)** et sélectionnez **Show Info Panel (Afficher le panneau d'informations)**. Sélectionnez une ou plusieurs VM et, dans le panneau **Info (Informations)**, sélectionnez **Labels (Étiquettes)**. Cliquez sur **+Add a label (Ajouter une étiquette)**, ajoutez une clé et une valeur, puis cliquez sur **Save (Enregistrer)**.

Étiquettes de réseau définies par l'utilisateur

Panorama utilise jusqu'à 8 étiquettes réseau définies par l'utilisateur. Si vous en avez plus de 8, Panorama classe vos étiquettes par ordre alphabétique et utilise les 8 premières étiquettes.

Notez que Google limite les étiquettes de réseau comme suit :

- 63 caractères maximum par étiquette.
- Vous pouvez utiliser des lettres minuscules, des chiffres et des tirets. Une étiquette doit commencer par une lettre minuscule et se terminer par un chiffre ou une lettre minuscule.

Pour créer ou afficher des étiquettes de réseau dans la console GCP, accédez à **Compute Engine** > **VM Instances (Instances VM)** et sélectionnez une instance. Cliquez sur **Edit (Modifier)** pour modifier l'instance puis faites défiler jusqu'à **Network Tags (Étiquettes de réseau)**, saisissez les étiquettes (séparées par des virgules), et cliquez sur **Save (Enregistrer)**. Reportez-vous à la section Configuration des étiquettes de réseau.

Configuration de la surveillance VM avec le plugin Panorama pour GCP

Après avoir étiqueté vos ressources GCP et créé un compte de service, mettez vos ressources à la disposition de Panorama afin de pouvoir mettre en place la surveillance VM.

 ©2023 Palo Alto Networks, Inc.

Préparer Panorama pour configurer la surveillance VM

Suivez ces étapes pour permettre à Panorama de gérer et de surveiller vos ressources GCP. Toute VM déployée dans GCP peut être un appareil géré dans Panorama.

STEP 1 | Dans Panorama, ajoutez les pare-feu VM-Series et les autres VM associées à votre projet GCP en tant qu'appareils gérés.

STEP 2 | Ajoutez un groupe d'appareils et attribuez-lui des appareils gérés. Un groupe d'appareils est un groupe de pare-feu ou de systèmes virtuels que vous souhaitez gérer en tant que groupe.

Une VM ne peut être membre que d'un seul groupe d'appareils. Planifiez soigneusement vos groupes d'appareils.

STEP 3 | Ajoutez un modèle. Nommez le modèle et acceptez le VPC par défaut.

STEP 4 | Ajoutez une pile de modèles. Cliquez sur **Add (Ajouter)** pour ajouter la pile, sur **Add (Ajouter)** pour ajouter le modèle que vous venez de créer, puis sélectionnez vos appareils.

STEP 5 | Cliquez sur Commit (Valider) pour valider les modifications.

Configurer la surveillance VM

STEP 1 | Si vous ne l'avez pas déjà fait, Installation du plug-in Panorama pour GCP.

STEP 2 | Connectez-vous à l'interface Web de Panorama et sélectionnez **Panorama** > **Google Cloud Platform**.

STEP 3 | Configurez la surveillance VM.

1. Configurez les paramètres généraux.

   1. Sélectionnez **Panorama** > **Google Cloud Platform** > **Setup (Configuration)** > **General (Général)**. Pour modifier les paramètres, cliquez sur l'engrenage.

      - Cochez **Enable Monitoring (Activer la surveillance)** pour autoriser la surveillance VM sur tous les projets pour lesquels vous configurez un compte de service.
      - Saisissez le **Monitoring Interval (Intervalle de surveillance)** en secondes. Il s'agit de la durée entre les événements de récupération des étiquettes.

2. **Ajoutez** un groupe de notification. Un groupe de notification est une liste de groupes d'appareils vers lesquels Panorama envoie les mappages adresse IP-à-étiquette et les mises à jour.

   Un projet ne peut avoir qu'un seul groupe de notification.

   1. **Panorama** > **Google Cloud Platform** > **Setup (Configuration)** > **Notify Groups (Groupes de notification)** et cliquez sur **Add (Ajouter)**.
   2. Saisissez un **Name (Nom)** pour identifier le groupe de pare-feu vers lequel Panorama envoie les informations sur les machines virtuelles (mappages adresse IP-à-étiquette) qu'il récupère.
   3. Sélectionnez les **Device Groups (Groupes d'appareils)** vers lesquels Panorama enverra les informations sur les machines virtuelles (mappages adresse IP-a-étiquette) extraites

 ©2023 Palo Alto Networks, Inc.

de votre projet. Les pare-feu VM-Series utilisent cette mise à jour pour déterminer la liste actuelle des membres des groupes d'adresses dynamiques référencés dans la politique de sécurité.

Planifiez soigneusement vos groupes d'appareils.

4. Sélectionnez des étiquettes prédéfinies ou personnalisées.
   - **Select All 8 Predefined Tags (Sélectionner les 8 étiquettes prédéfinies)** : choisissez cette option pour sélectionner tous les attributs (étiquettes) prédéfinis.
   - **Custom Tags (Étiquettes personnalisées)** : choisissez cette option afin de créer des listes d'étiquettes pour les attributs prédéfinis, les étiquettes définies par l'utilisateur et les étiquettes de réseau définies par l'utilisateur.
5. - Veillez à inclure tous les groupes d'appareils pertinents dans un seul groupe de notification.
   - Si vous voulez désenregistrer les étiquettes que Panorama a transmises à un pare-feu inclus dans un groupe de notification, vous devez supprimer la définition de surveillance.
   - Pour enregistrer des étiquettes dans tous les systèmes virtuels sur un pare-feu activé pour plusieurs systèmes virtuels, vous devez ajouter chaque système virtuel à un groupe d'appareils distinct sur Panorama et attribuer les groupes d'appareils au groupe de notification. Panorama enregistrera les étiquettes dans un seul système virtuel si vous attribuez tous les systèmes virtuels à un seul groupe d'appareils.

3. Cliquez sur **Add (Ajouter)** pour ajouter des informations d'identification pour le compte de service GCP.
   - Donnez un nom aux informations d'identification pour le compte de service.
   - (Facultatif) Saisissez une description du compte de service.
   - Cliquez sur **Browse (Parcourir)** pour charger le fichier JSON généré lorsque vous avez créé le compte de service.

Vous devez utiliser l'interface Web de Panorama. Vous ne pouvez pas utiliser la CLI pour ajouter un compte de service.

Vous ne pouvez utiliser un compte de service que pour un seul ensemble d'informations d'identification. Ne créez pas plusieurs ensembles d'informations d'identification à partir d'un seul fichier JSON.

Après avoir ajouté des informations d'identification pour le compte de service, vous pouvez les valider à partir de votre ligne de commande Panorama :

```
request plugins gcp validate-service-account <svc-acct-credential-name>
```

STEP 4 | Créez une **Monitoring Definition (Définition de surveillance)**.

Une définition de surveillance se compose des informations d'identification pour le compte de service pour votre projet et d'un groupe de notification. Toutes les ressources de mise en réseau de votre projet sont surveillées et les étiquettes récupérées sont envoyées aux groupes

 ©2023 Palo Alto Networks, Inc.

d'appareils que vous indiquez dans votre définition de surveillance. Lorsque vous ajoutez une nouvelle définition de surveillance, elle est activée par défaut.

Un projet ne peut avoir qu'une seule définition de surveillance, et une définition de surveillance ne peut inclure qu'un seul groupe de notification.

1. **Panorama** > **Google Cloud Platform** > **Monitoring Definition (Définition de surveillance)** et cliquez sur Add (Ajouter).
2. Donnez un **Name (Nom)** à la définition de surveillance.
3. Saisissez une **Description (Description)** facultative pour le projet et les ressources que vous surveillez.
4. Sélectionnez les informations d'identification pour le **Service Account (Compte de service)** que vous avez créées à l'étape précédente.
5. Sélectionnez un **Notify Group (Groupe de notification)**.
6. Sélectionnez **Enable (Activer)** pour activer la surveillance des éléments associés à ce compte de service.

STEP 5 | **Engagez** les changements sur Panorama.

Assurez-vous que l'état de la définition de surveillance s'affiche comme « Succès ». Si cela échoue, vérifiez que vous avez saisi l'ID du projet avec exactitude et que vous avez fourni les bonnes clés et les bons ID pour le service.

STEP 6 | Vérifiez que vous pouvez visualiser l'information VM sur Panorama et définir les critères d'appariement pour les groupes d'adresses dynamiques.

Sur le basculement HA, le Panorama nouvellement actif tente de se reconnecter à Google Cloud Platform et de récupérer les étiquettes pour toutes les définitions de surveillance. En cas d'erreur lors de la reconnexion d'une seule définition de surveillance, Panorama génère un message de journal système :

```
Unable to process subscriptions after HA switch-over; user-
intervention required. (Impossible de traiter les abonnements après
 le basculement HA ; intervention de l'utilisateur requise.)
```

Si vous voyez cette erreur, corrigez le problème dans Panorama. Par exemple, supprimez un abonnement non valide ou fournissez des informations d'identification valides, et validez vos modifications pour permettre à Panorama de se reconnecter et de récupérer les étiquettes pour toutes les définitions de surveillance.

Même lorsque Panorama est déconnecté de Google Cloud Platform, les pare-feu ont la liste de toutes les étiquettes qui ont été récupérées avant le basculement et peuvent continuer d'appliquer la politique sur cette liste d'adresses IP. Lorsque vous supprimez une définition de surveillance, Panorama supprime toutes les étiquettes associées aux VM enregistrées. Comme pratique exemplaire, vous pouvez configurer le transfert de journaux vers une destination HTTPS *à partir de Panorama afin de pouvoir prendre des mesures immédiatement.*

 ©2023 Palo Alto Networks, Inc.

Mise à l'échelle automatique du pare-feu VM-Series sur Google Cloud Platform

Le plugin Panorama pour Google Cloud Platform (GCP) version 2.0.0 vous aide à déployer le pare-feu VM-Series dans GCP et permet à Panorama de gérer les pare-feu VM-Series sécurisant la surveillance des VM ou les déploiements à échelle automatique dans GCP. L'utilisation de Panorama pour la gestion centralisée des politiques et des périphériques accroît l'efficacité opérationnelle de la gestion et de l'entretien d'un réseau distribué de pare-feu.

Grâce à Panorama, qui gère vos groupes d'instances GCP, vous pouvez créer des politiques d'activation d'applications qui protègent et contrôlent le réseau.

Le déploiement à échelle automatique permet d'utiliser une configuration de réseau VPC partagé ou un appairage de réseau VPC pour créer un réseau VPC commun dans lequel un projet hôte contient des réseaux VPC partagés et les pare-feu VM-Series, et un projet de service contient un déploiement d'application basé sur VM ou sur un conteneur (un cluster Kubernetes). Palo Alto Networks fournit des modèles pour vous aider à déployer les pare-feu VM-Series dans le projet hôte et à déployer une application modèle facultative dans le projet de service.

Les licences BYOL et PAYG peuvent être utilisées pour les pare-feu VM-Series. Lors de l'octroi des licences, les instances de pare-feu VM-Series parlent directement au serveur de licences de Palo Alto Networks.

Si vous choisissez BYOL, votre déploiement peut désactiver des instances de licence en réponse à un événement de réduction d'échelle. Si les informations de déploiement d'un pare-feu VM-Series sont configurées dans le plugin Panorama pour GCP et que le pare-feu est automatiquement supprimé, Panorama détecte l'état du pare-feu et le désenregistre automatiquement.

- Composants de mise à l'échelle automatique pour Google Cloud Platform
- Déploiement des modèles de mise à l'échelle automatique GCP 2

Composants de mise à l'échelle automatique pour Google Cloud Platform

Les déploiements typiques de GCP à échelle automatique utilisent un projet hôte et un projet de service et forment un réseau VPC commun entre les deux. Le plugin Panorama pour GCP peut assurer un déploiement à échelle automatique dans un seul projet avec des VPC hôtes et de service, ou des projets hôtes et de service dans une configuration de réseau VPC partagé ou VPC pairé, où le projet hôte contient les pare-feu VM-Series et les réseaux VPC partagés, et le projet de service contient le déploiement de votre application. Si votre application est déployée dans un cluster Kubernetes, un VPC pairé est nécessaire.

- Exigences relatives à la mise à l'échelle automatique
- Préparer le déploiement des modèles de mise à l'échelle automatique

Exigences relatives à la mise à l'échelle automatique

- **Exigences générales**—Assurez-vous que votre environnement répond aux exigences de base.

©2023 Palo Alto Networks, Inc.

- **Plug-in Panorama pour GCP**—Si vous ne l'avez pas fait, Installation du plug-in Panorama pour GCP.

  Si vous avez déjà installé le plugin Panorama pour GCP version 1.0.0, supprimez-le avant d'installer la version 2.0.X. Vous ne pouvez pas effectuer de mise à niveau.

- **Modèles de mise à l'échelle automatique de Palo Alto Networks version 1.0**—Palo Alto Networks fournit les modèles permettant de déployer des instances de pare-feu VM-Series dans le projet hôte et de configurer et déployer une application modèle dans un projet de service. Consultez À propos des modèles de mise à l'échelle automatique GCP pour plus d'informations sur les modèles.

  Téléchargez les modèles sur GitHub. Le fichier ZIP contient des fichiers ZIP distincts pour les modèles de pare-feu et d'application.

Préparer le déploiement des modèles de mise à l'échelle automatique

Effectuez les tâches suivantes avant de déployer les modèles de mise à l'échelle automatique.

- Préparer un projet hôte et les comptes de services requis
- Obtenez une clé API de mise sous licence
- Configurer le plugin Panorama pour GCP afin d'assurer un déploiement à l'échelle automatique
- Préparer un paquet d'amorçage de pare-feu VM-Series pour une mise à l'échelle automatique

Préparer un projet hôte et les comptes de services requis

Vous avez besoin d'un projet hôte et d'un projet de service pour former la topologie VPC partagée qui prend en charge le pare-feu et les modèles d'application. Vous pouvez créer un nouveau projet d'accueil ou préparer un projet existant pour qu'il vous serve d'hôte.

Pour configurer le VPC partagé, un administrateur de l'organisation doit accorder à l'administrateur du projet hôte le rôle admin du VPC partagé. L'admin du VPC partagé peut permettre à un projet d'agir en tant qu'hôte, et accorder le rôle admin de projet de service à l'administrateur de projet de service. Examinez la documentation GCP sur les rôles des administrateurs et de l'IAM.

STEP 1 | Dans la console GCP, créez un projet GCP pour agir en tant qu'hôte. Si vous souhaitez utiliser un projet existant, passez à l'étape suivante.

Pour créer un nouveau projet, sélectionnez votre organisation ou **No organization (Pas d'organisation)**, cliquez sur **New Project (Nouveau projet)** et remplissez les informations relatives à votre projet. Notez que c'est votre seule chance de **MODIFIER** l'ID du projet.

Le Google Cloud SDK doit être installé et configuré de manière à ce que vous puissiez vous authentifier auprès de votre projet hôte à partir du CLI. Vous utiliserez l'interface en ligne de commande pour déployer le modèle de pare-feu et le modèle d'application, et pour joindre le projet de service au projet hôte.

©2023 Palo Alto Networks, Inc.

STEP 2 | Activez les API et les services requis pour la mise à l'échelle automatique. Les API requises sont les suivantes :

- API du cloud Pub/Sub
- API du gestionnaire de déploiement de cloud
- API de stockage cloud
- API de Compute Engine
- API de gestion des groupes d'instance de Google Compute Engine
- API de mise à jour des groupes d'instance de Google Compute Engine
- API des groupes d'instance de Google Compute Engine
- API Kubernetes Engine
- API Stackdriver
- API Stackdriver Logging
- API Stackdriver Monitoring

Vous pouvez activer les API à partir de la console GCP ou de la CLI GCP, comme indiqué ci-dessous.

Activer les API depuis la console GCP

1. Sélectionnez le projet hôte et, dans le menu de navigation, sélectionnez **APIs & Services (API et services)**.
2. Recherchez et consultez chaque API requise.
3. Cliquez sur **ENABLE (Activer)** pour activer les API qui n'affichent pas l'état « API enabled » (API activé).

Activer les API depuis la CLI

1. Dans la CLI, consultez votre configuration pour vous assurer que vous êtes dans le bon projet.

```
gcloud config list
```

Si ce n'est pas le cas, définissez le projet comme suit :

```
gcloud config set project <project-name>
```

2. Exécutez les commandes suivantes pour activer les API requises.

```
gcloud services enable pubsub.googleapis.com gcloud
 services enable deploymentmanager.googleapis.com
 gcloud services enable storage-component.googleapis.com
 gcloud services enable compute.googleapis.com gcloud
 services enable replicapool.googleapis.com gcloud
 services enable replicapoolupdater.googleapis.com gcloud
 services enable resourceviews.googleapis.com gcloud
 services enable container.googleapis.com gcloud services
 enable stackdriver.googleapis.com gcloud services
```


©2023 Palo Alto Networks, Inc.

```
enable logging.googleapis.com gcloud services enable
monitoring.googleapis.com
```

3. Confirmez que les API requises sont activées.

```
gcloud services list --enabled
```

STEP 3 | Créez un compte de service pour le déploiement du pare-feu VM-Series et attribuez les rôles IAM nécessaires à la mise à l'échelle automatique d'un service ou d'un cluster Kubernetes.

Lorsque vous configurez les modèles de pare-feu, vous ajoutez l'adresse e-mail de ce compte de service au fichier `.yaml` du pare-feu VM-Series. Au sein du projet hôte, le modèle utilise les informations d'identification de ce compte de service pour créer un VPC hôte avec des sous-

 ©2023 Palo Alto Networks, Inc.

réseaux, déployer des pare-feu VM-Series dans le VPC, configurer les mesures personnalisées de Stackdriver, créer un sujet Pub/Sub, et plus encore.

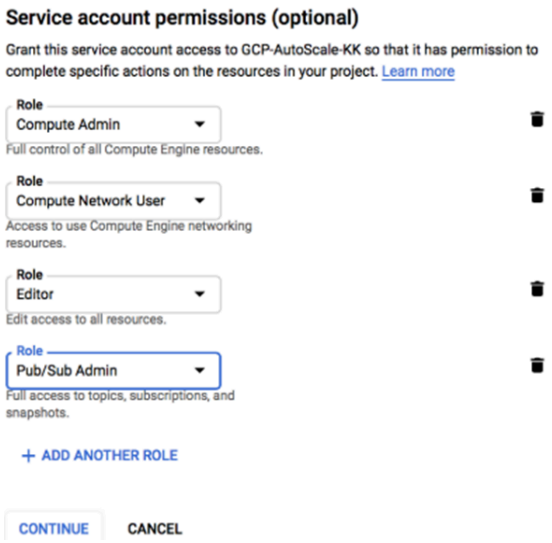
1. Dans la console GCP, sélectionnez **les comptes de service** > **IAM & Admin** et sélectionnez **+CREATE SERVICE ACCOUNT (+CRÉER UN COMPTE DE SERVICE)**.

   Remplissez les détails du compte de service et cliquez sur **CREATE (CRÉER)**.

2. Donnez au compte du service l'autorisation de mettre automatiquement à l'échelle les ressources dans ce projet.

   Sélectionnez un type de rôle dans le menu déroulant et, à droite, sélectionnez un niveau d'accès approprié. Par exemple, sélectionnez Project (Projet) > Editor (Éditeur). Vous pouvez sélectionner plusieurs rôles pour un compte de service.

   - Compute Engine > Compute Admin
   - Compute Engine > Compute Network User (Utilisateur de Compute Network)
   - Pub/Sub > Admin
   - Monitoring (Surveillance) > Monitoring Metric Writer
   - Stackdriver > Stackdriver Accounts Editor (Éditeur de comptes Stackdriver)
   - Storage (Stockage) > Storage Admin (Admin de stockage)
   - (GKE uniquement) Kubernetes > Kubernetes Engine Cluster Admin (Admin de cluster Kubernetes Engine)
   - (GKE uniquement) Kubernetes > Kubernetes Engine Viewer (Observateur Kubernetes Engine)



   Continuez lorsque vous avez fini d'ajouter des rôles.

3. Cliquez sur **+CREATE KEY (+CRÉER CLÉ)** pour créer une clé pour le compte du service hôte.

   - (En option) Ajoutez des adresses e-mail pour permettre à d'autres utilisateurs ou administrateurs d'accéder à ce compte de service.
   - Cliquez sur JSON pour télécharger la clé privée sous forme de JSON.
   - Conservez la clé dans un endroit sûr. Vous aurez besoin de cette clé lorsque vous Déploiement des modèles de mise à l'échelle automatique GCP.

©2023 Palo Alto Networks, Inc.

4. Cliquez sur **DONE (TERMINÉ)**.

STEP 4 | Créez un compte de service qu'un administrateur de Panorama peut utiliser pour interagir avec ce projet hôte.

1. Dans la console GCP, sélectionnez **les comptes de service** > **IAM & Admin** et sélectionnez **+CREATE SERVICE ACCOUNT (+CRÉER UN COMPTE DE SERVICE)**.
2. Remplissez les détails du compte de service et cliquez sur **CREATE (CRÉER)**.
3. Autorisez l'accès au compte de service.

   Sélectionnez un type de rôle dans le menu déroulant et, à droite, sélectionnez un niveau d'accès approprié. Par exemple, sélectionnez Project (Projet) > Editor (Éditeur). Vous pouvez sélectionner plusieurs rôles pour un compte de service.

   - Compute Engine > Compute Viewer
   - Deployment Manager (Responsable déploiement) > Viewer (Observateur)
   - Pub/Sub > Admin

   Cliquez sur **CONTINUE (CONTINUER)**.
4. Cliquez sur **+CREATE KEY (+CRÉER CLÉ)** pour créer une clé pour le compte du service hôte.
   - (En option) Ajoutez des adresses e-mail pour permettre à d'autres utilisateurs ou administrateurs d'accéder à ce compte de service.
   - Sélectionnez JSON pour télécharger la clé privée sous forme de JSON.
   - Conservez la clé dans un endroit sûr. Vous aurez besoin de cette clé lorsque vous Configurer le plugin Panorama pour GCP afin d'assurer un déploiement à l'échelle automatique.

STEP 5 | (en option) Dans la CLI, assurez-vous que vous pouvez communiquer avec votre nouveau projet hôte.

1. Définissez votre projet en fonction du projet hôte que vous venez de créer.

   ```
   gcloud set project <your-autoscale-host-project-name>
   ```
2. Créez une configuration pour la mise à l'échelle automatique. Votre nouvelle configuration est automatiquement activée, à moins que vous ne désactiviez l'activation.

   ```
   gcloud config configurations create <CONFIGURATION_NAME> gcloud config list
   ```

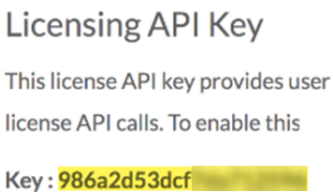
Obtenez une clé API de mise sous licence

Vous avez besoin d'une clé API de licence pour que Panorama puisse octroyer et retirer les licences des actifs gérés dans GCP.

©2023 Palo Alto Networks, Inc.

STEP 1 | Connectez-vous au Portail de support et sélectionnez**Assets** > **Licensing API (Licence de biens API)** et cliquer sur **Enable (Activer)**. La clé s'affiche.

Seul un Super utilisateur peut afficher le lien Activer pour générer cette clé. See How to Enable, Regenerate, Extend the Licensing API Key (Comment activer, régénérer, étendre la clé API de mise sous licence).



STEP 2 | Sélectionnez la clé et copiez-la.

STEP 3 | À partir de la CLI, entrez en SSH dans Panorama et lancez la commande suivante, en remplaçant <key> par la clé API que vous avez copiée depuis le portail de support :

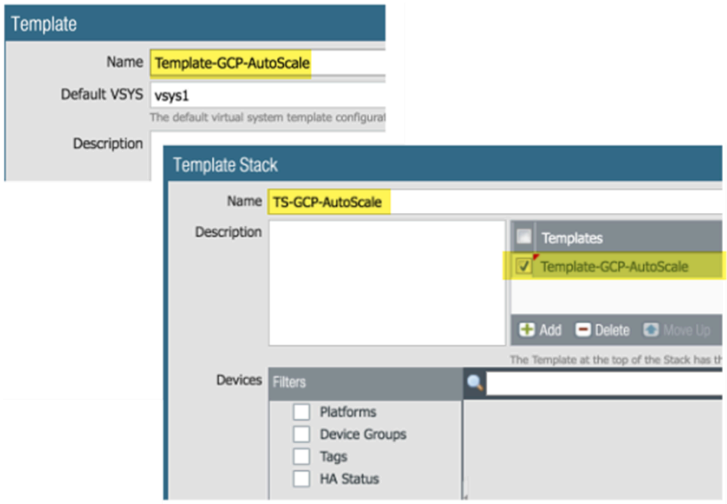
```
request license api-key set key <key>
```

```
API Key is successfully set (La clé API a bien été définie)
```

Configurer le plugin Panorama pour GCP afin d'assurer un déploiement à l'échelle automatique

Dans Panorama, créez des ressources pour soutenir le déploiement de pare-feu à échelle automatique.

STEP 1 | Créez un modèle, et une pile de modèles qui comprend le modèle, et **confirmez** les changements.



 ©2023 Palo Alto Networks, Inc.

STEP 2 | Dans le contexte du **Réseau**, sélectionnez soit le modèle, soit la pile de modèles. Sélectionnez **Virtual Routers (Routeurs virtuels)** et **Add (Ajouter)** un routeur virtuel.

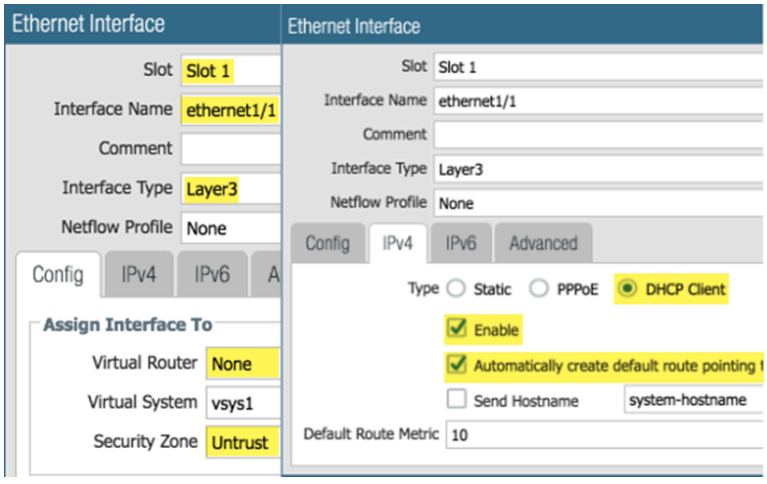
Lorsque le modèle de pare-feu crée des routes statiques, celles-ci sont ajoutées à ce routeur virtuel.

Définissez un seul routeur pour le déploiement de l'échelle automatique.



STEP 3 | Dans le contexte du **Réseau**, sélectionnez le modèle que vous avez créé, sélectionnez **Interfaces** et **Add Interface (Ajouter une interface)**.

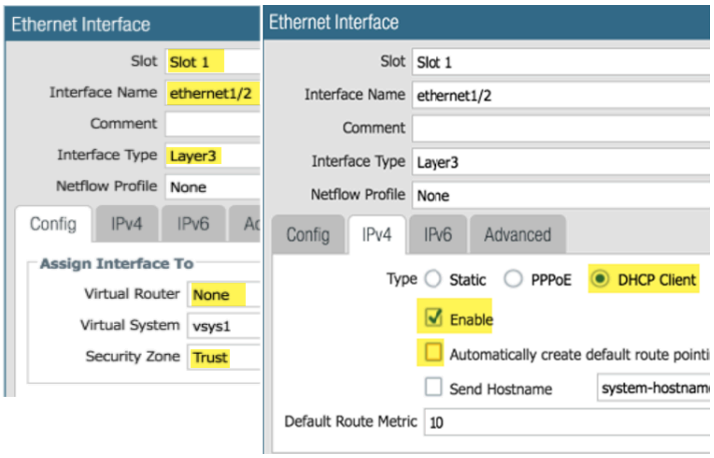
- Dans l'onglet Config, sélectionnez un emplacement, choisissez **Interface name (Nom de l'interface)** et sélectionnez **Interface Type (Type d'interface)** Layer3. Depuis le menu **Security Zone (Zone de sécurité)**, sélectionnez **New Zone (Nouvelle zone)**, nommez la zone « Untrust » (non approuvée), puis cliquez sur **OK**.
- Dans l'onglet **IPv4** activez **DHCP Client (Client DHCP)** et **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) et cliquez sur **OK**.



 ©2023 Palo Alto Networks, Inc.

STEP 4 | Ajouter l'interface Couche 3 ethernet1/2 (Approuvée).

- Dans l'onglet Config, choisissez le même emplacement que l'étape précédente, sélectionnez **Interface name (Nom de l'interface)** (ethernet1/2), et sélectionnez **Interface Type (Type d'interface)** Layer3. Depuis le menu **Security Zone (Zone de sécurité)**, sélectionnez **New Zone (Nouvelle zone)**, nommez la zone « Trust » (Approuvée), puis cliquez sur **OK**.
- Dans l'onglet **IPv4** désactivez **DHCP Client (Client DHCP)** et **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)** et cliquez sur **OK**.



STEP 5 | Retournez à votre pile de modèles et au routeur virtuel que vous avez créé précédemment. Placez les interfaces non approuvées et approuvées (ethernet1/1 et ethernet1/2) dans le routeur virtuel, et cliquez sur **OK**.

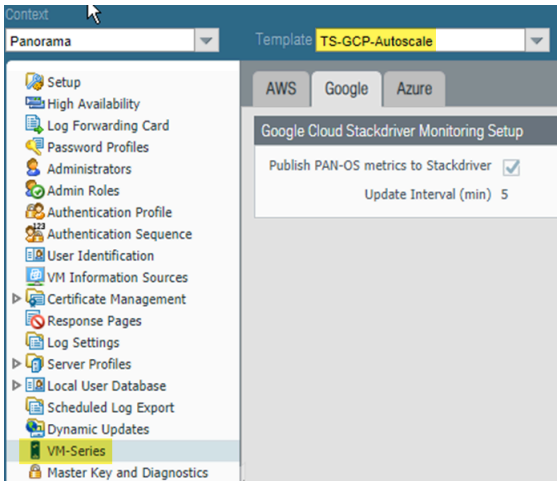


 ©2023 Palo Alto Networks, Inc.

STEP 6 | Configurez Stackdriver pour votre déploiement à échelle automatique.

Vous devez avoir le plugin VM-Series sur Panorama pour configurer Stackdriver.

1. Dans le contexte **Device (Périphérique)**, sélectionnez la pile de modèles que vous avez créée précédemment dans le menu déroulant Modèle.
2. Sélectionnez **Device (Périphérique)** > **VM-Series** > **Google** cliquez sur Edit (Modifier) cog ( ). Activez **Publish PAN-OS metrics to Stackdriver (Publier les métriques PAN-OS sur Stackdriver)**.



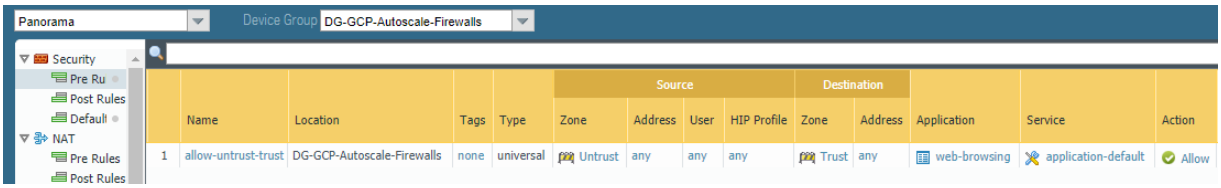
3. Validez vos modifications.

STEP 7 | Créez un groupe d'appareils qui fait référence au modèle ou à la pile de modèles que vous avez créés à l'étape 1.

Ce groupe d'appareils contient les pare-feu VM-Series que vous créez avec le modèle de pare-feu.

1. Ajoutez une politique de sécurité qui autorise le trafic de navigation sur le web de Non approuvé à Approuvé.

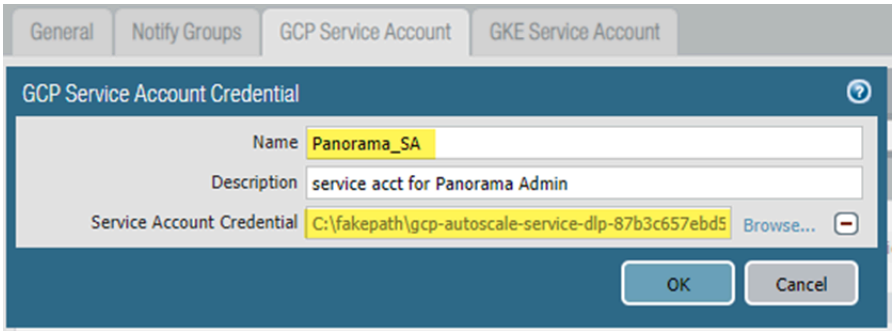
   Dans le contexte des politiques, sélectionnez le groupe d'appareils que vous venez de créer. Sélectionnez **Security (Sécurité)** > **Pre Rules (Pré-règles)** et **Add (Ajouter)** la politique de sécurité suivante.



 ©2023 Palo Alto Networks, Inc.

STEP 8 | Configurez le compte du service GCP pour le projet hôte.

1. Dans le contexte de Panorama, développez Google Cloud Platform, sélectionnez **Setup (Configurer)**, puis cliquez sur **Add (Ajouter)**.
2. Fournissez un nom et une description pour le compte de service hôte que vous avez créé à l'étape 4.
3. Téléchargez le fichier d'identification JSON que vous avez créé à l'étape 4.4.

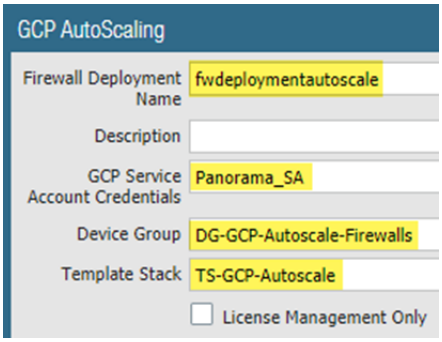


Après avoir ajouté des informations d'identification pour le compte de service, vous pouvez les valider à partir de votre ligne de commande Panorama (vous ne pouvez pas les valider depuis l'interface Web) :

```
request plugins gcp validate-service-account
 gcp_service_account <svc-acct-credential-name>
```

STEP 9 | Configurez la mise à l'échelle automatique sur le plugin Panorama pour GCP.

1. Dans le contexte de Panorama, développez Google Cloud Platform, sélectionnez AutoScaling (Mise à l'échelle automatique), puis cliquez sur **Add (Ajouter)**.
2. Fournissez le Nom du déploiement de pare-feu ainsi qu'une description facultative du déploiement.
3. Pour l'identification du compte de service GCP, indiquez le nom du compte de service GCP de l'étape 8.



4. Choisissez le groupe d'appareils que vous avez créé à l'étape 7, et la pile de modèles que vous avez créée à l'étape 1.
5. Désactivez **License Management Only (Gestion des licences uniquement)** pour garantir la sécurité du trafic.

STEP 10 | Validez vos modifications.

©2023 Palo Alto Networks, Inc.

Préparer un paquet d'amorçage de pare-feu VM-Series pour une mise à l'échelle automatique

Lors de l'amorçage, la demande initiale du pare-feu fournit l'adresse IP de l'hôte et le numéro de série, ainsi que la clé d'authentification de la VM afin que Panorama puisse valider la clé d'authentification de la VM et ajouter le pare-feu en tant qu'appareil géré. Panorama peut alors attribuer le pare-feu au groupe d'appareils et modèle appropriés afin que vous puissiez configurer et administrer de manière centralisée le pare-feu avec Panorama.

Dans ce cas, vous devez générer une clé d'authentification de VM sur Panorama et inclure la clé dans le fichier init-cfg.txt que vous utilisez pour l'amorçage. La clé d'autorisation VM permet à Panorama d'authentifier le pare-feu VM-Series qui vient d'être amorcé. L'ensemble d'amorçage doit inclure :

- Dans le répertoire /config, un fichier init-cfg.txt qui inclut l'adresse IP de Panorama
- Dans le répertoire /license, la clé d'authentification VM dans un fichier nommé authcodes.

  La durée de vie de la clé peut varier de 1 à 8 760 heures (1 an). Au bout du temps spécifié, la clé expire et Panorama n'enregistrera pas les pare-feu VM-Series sans une clé d'autorisation VM valide dans la requête de connexion.

STEP 1 | Configurez un compartiment de stockage Google avec les dossiers nécessaires pour amorcer le pare-feu VM-Series sur Google Cloud Platform. Vous pouvez utiliser un ensemble d'amorçage existant ou créer un nouvel ensemble d'amorçage, pour ces dossiers.

STEP 2 | Modifiez les valeurs dans l'exemple de fichier **`init-cfg.txt`** pour personnaliser le fichier en fonction de votre environnement.

Les modèles de pare-feu comprennent un exemple de fichier **`init-cfg.txt`**.

Paramètre	Valeur	Commentaire
type	dhcp-client	
Nom d'hôte	<pa-vm>	Nom facultatif que vous avez attribué lors de la préparation du projet hôte. Nécessaire uniquement si un hôte spécifique est nécessaire, et que dhcp-send-hostname est non.
vm-auth-key	<vmauthkey>	Une clé que Panorama doit valider avant d'ajouter un pare-feu en tant qu'appareil géré. Reportez-vous à la section Générer la clé d'authentification de VM sur Panorama.
panorama-server	<panorama-ip>	L'adresse IP du périphérique de gestion Panorama que

©2023 Palo Alto Networks, Inc.

Paramètre	Valeur	Commentaire
		vous avez configuré dans Configurer le plugin Panorama pour GCP afin d'assurer un déploiement à l'échelle automatique
tplname	<template-stack-name>	La pile de modèles que vous avez créée dans Configurer le plugin Panorama pour GCP afin d'assurer un déploiement à l'échelle automatique.
DgName	<dg-name>	Le nom du groupe d'appareils que vous avez créé dans le plugin Panorama pour GCP.
dns-primary		Votre serveur DNS principal.
dns-secondary		Votre serveur DNS secondaire.
dhcp-send-hostname	yes	Laisser tel quel.
dhcp-send-client-id	yes	Laisser tel quel.
dhcp-accept-server-hostname	yes	Laisser tel quel.
dhcp-accept-server-domain	yes	Laisser tel quel.

STEP 3 | Téléchargez votre fichier **`init-cfg.txt`**modifié dans le dossier **`/config`** dans votre ensemble d'amorçage.

STEP 4 | Si vous utilisez BYOL, créez un fichier texte nommé **`authcodes`** (sans extension), ajoutez votre code d'autorisation et téléchargez le fichier dans le dossier **`/license`**.

Déploiement des modèles de mise à l'échelle automatique GCP

- À propos des modèles de mise à l'échelle automatique GCP
- Déployer le modèle de pare-feu
- Préparer un projet de service
- Configurer le VPC partagé
- Déployer le modèle d'application
- Intégrer une nouvelle application
- Exemples de modèles de service GKE

©2023 Palo Alto Networks, Inc.

À propos des modèles de mise à l'échelle automatique GCP

Téléchargez les modèles de mise à l'échelle automatique Palo Alto Networks depuis https://github.com/PaloAltoNetworks/GCP-AutoScaling. Le fichier ZIP contient des fichiers ZIP distincts pour les modèles de pare-feu et d'application. Chaque fichier ZIP est un répertoire de modèles contenant plusieurs fichiers, mais les fichiers YAML sont les seuls que vous devez modifier.

- Modèles de pare-feu
- Modèle d'application

Modèles de pare-feu

Les fichiers du répertoire de pare-feu créent des pare-feu VM-Series et d'autres ressources de déploiement. Ils créent de nouveaux réseaux et les sous-réseaux familiers pour le pare-feu VM-Series : gestion, non approuvé et approuvé. Ils déploient également un service de messagerie Cloud Pub/Sub pour relayer les informations de GCP vers le plugin Panorama pour GCP. Une fois cette infrastructure en place, le plugin peut exploiter des groupes d'adresses dynamiques pour appliquer une politique de sécurité sur le trafic entrant acheminé vers les services exécutés sur GCP, et utiliser des métriques de mise à l'échelle automatique pour déployer les pare-feu VM-Series afin de répondre à la demande accrue de ressources de charge de travail d'application ou pour éliminer les pare-feu qui ne sont plus nécessaires.

Pour configurer votre équilibreur de charge, modifiez le fichier `.yaml` pour un équilibreur de charge d'application (ALB) ou un équilibreur de charge de réseau (NLB) externe.

- **ALB** (Équilibreur de charge externe HTTP)

  Pour personnaliser un ALB, modifiez `vm-series-fw-alb.yaml`.

  L'équilibreur de charge externe HTTP est un équilibreur de charge basé sur un proxy qui exécute le SNAT et le DNAT sur le trafic entrant d'Internet. L'équilibreur de charge HTTP est conçu pour prendre en charge uniquement les ports TCP 80 et 8080.

  Pour prendre en charge de multiples applications utilisant l'équilibreur de charge HTTP dans une architecture sandwich, nous pouvons utiliser ***urlMap*** et ***namedPort*** de l'équilibreur de charge HTTP GCP pour mapper différentes URL à différents ports de l'équilibreur de charge. À son tour, le pare-feu VM-Series peut traduire les ports vers différentes applications, chacune étant représentée par un équilibreur de charge interne par application.

- **NLB** (équilibreur de charge TCP)

  Pour personnaliser un NLB, modifiez `vm-series-fw-nlb.yaml`.

  L'équilibreur de charge TCP est un équilibreur de charge non basé sur un proxy, ce qui signifie qu'il n'exécute pas de NAT sur le trafic entrant d'Internet.

  L'équilibreur de charge TCP dans GCP permet d'ajouter plusieurs adresses IP frontales avec un port arbitraire, ce qui permet de prendre en charge plusieurs applications.

  Un autre avantage de l'équilibreur de charge TCP est que l'adresse IP originale du client est préservée, ce qui est préférable pour certaines applications.

Modèle d'application

Le répertoire d'application fournit un exemple d'application. Vous configurez et déployez un équilibreur de charge interne (ILB) pour permettre à vos serveurs d'applications de s'abonner au service Pub/Sub et de communiquer avec vos pare-feu VM-Series et le plugin GCP sur Panorama.

 ©2023 Palo Alto Networks, Inc.

Pour personnaliser le modèle d'application, modifiez **apps.yaml** comme décrit dans Déployer le modèle de pare-feu et Modèle d'application.

Déployer le modèle de pare-feu

Modifiez les Modèles de pare-feu du projet hôte.

STEP 1 | Modifiez les variables d'environnement **vm-series-fw-nlb.yaml** ou **vm-series-fw-alb.yaml** pour refléter votre environnement de cloud.

L'exemple de ce flux de travail est destiné au NLB. Reportez-vous à vm-series-fw-nlb.yaml et vm-series-fw-alb.yaml pour plus d'explications sur les paramètres du modèle.

```
properties:     region: us-east1     zones:     -us-east1-b     #
 Ne modifiez pas le champ lb-type.     lb-type: nlb     cloud-nat:
 yes     forwarding-rule-port: 80
```

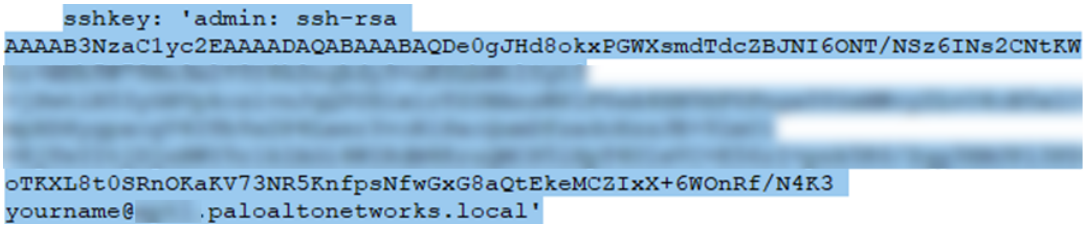
```
# Une seule application est autorisée     urlPath-namedPort-maps:
     - appName: app1
```

```
# clé ssh PUBLIQUE : - facultatif
```

Le modèle de pare-feu de mise à l'échelle automatique exige que vous saisissiez la valeur entre guillemets simples et que vous ajoutiez, avant la clé, **admin:** suivi d'un espace. Il s'agit de la

©2023 Palo Alto Networks, Inc.

même convention que celle utilisée pour le modèle Google Marketplace, telle que détaillée dans Paire de clés SSH. Par exemple :




```
    bootstrap-bucket: bootstrap-autoscale
```

```
    image: vmseries-byol-814     machine-type: n1-standard-4
```

Pour le compte de service, fournissez l'adresse e-mail du compte de service du projet hôte que vous avez créé précédemment (étape 3).

```
     service-account: sa-pan@gcp-autoscale-
kk.iam.gserviceaccount.com
```

La valeur de fw-instance-tag sera le nom du groupe d'instances géré dans le déploiement.

```
     fw-instance-tag: vm-series-fw
```

Choisissez une métrique pour la mise à l'échelle automatique. Les valeurs possibles sont les suivantes : panSessionActive, panSessionUtilization, DataPlaneCPUUtilizationPct, DataPlanePacketBufferUtilization ou panSessionUtilization.

```
metric: custom.googleapis.com/VMSeries/panSessionActive
```

```
max-size: 2 min-size: 1 target-type: GAUGE util-target: 100
```

```
# Déploiement Greenfield mgmt-network-cidr: 172.22.2.0/24 untrust-
network-cidr: 172.22.1.0/24 trust-network-cidr: 172.22.3.0/24 mgmt-
network-access-source-range: - 199.167.54.229/32 - 199.167.52.5/32
 mgmt-network-access-ports: - 22 - 443
```

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Déployez le modèle de pare-feu.

```
gcloud deployment-manager deployments create <your-template> --
config apps.yaml --automatic-rollback-on-error
```

Prenez note des résultats que le CLI imprime après le déploiement : les noms des sous-réseaux, le nom du déploiement et le nom du sujet Pub/Sub de Panorama. Vous avez besoin de ces valeurs pour configurer le VPC partagé et pour le déploiement du modèle d'application.

Le nom du déploiement de pare-feu doit être configuré dans la définition de mise à l'échelle automatique du plugin Panorama pour GCP.

Préparer un projet de service

Créez un projet de service distinct, ou choisissez un projet existant, pour votre application.

Pour en savoir plus sur les projets hôte et de service dans un VPC partagé, consultez la présentation du VPC partagé et passez en revue les rôles Administrateurs et IAM. Un administrateur de projet hôte doit avoir le rôle approprié pour mettre en place le VPC partagé et faire du projet d'application un projet de service pour le projet hôte. Consultez les instructions dans Mise en service d'un VPC partagé.

©2023 Palo Alto Networks, Inc.

STEP 1 | Activez les API du projet de service depuis la console GCP ou la CLI.

Les API requises sont les suivantes :

- ❑ API du gestionnaire de déploiement de cloud
- ❑ API du cloud Pub/Sub
- ❑ API de Compute Engine

Activer les API depuis la console GCP

1. Sélectionnez le projet de service et, dans le menu de navigation, sélectionnez **APIs & Services (API et services)**.
2. Recherchez et consultez chaque API requise.
3. Cliquez sur **ENABLE (Activer)** pour activer les API qui n'affichent pas l'état « API enabled » (API activé).

Activer les API depuis la CLI

1. Dans la CLI, consultez votre configuration pour vous assurer que vous êtes dans le bon projet.

```
gcloud config list
```

Si ce n'est pas le cas, définissez le projet comme suit :

```
gcloud config set project <project-name>
```

2. Exécutez les commandes suivantes pour activer les API requises.

```
gcloud services enable deploymentmanager.googleapis.com gcloud
 services enable pubsub.googleapis.com gcloud services enable
 compute.googleapis.com
```

3. Confirmez que les API requises sont activées.

```
gcloud services list --enabled
```

STEP 2 | Faites du projet d'application un projet de service pour le projet hôte.

Ajoutez le compte de service de l'administrateur du projet d'application / de service comme membre du projet d'hôte avec les rôles suivants :

- Utilisateur de Compute Network
- Administrateur de Pub/Sub

STEP 3 | Choisissez une configuration de VPC.

- Si le projet de service partage les réseaux du projet hôte, passez à Configurer le VPC partagé.
- Si le projet de service dispose de son propre réseau VPC pour le déploiement d'application, passez à Configurer un VPC appairé.

©2023 Palo Alto Networks, Inc.

Configurer le VPC partagé

Une fois que le modèle de pare-feu est déployé dans le projet hôte, configurez le projet de service qui prend en charge vos applications. Un administrateur possédant les informations d'identification du VPC partagé effectue ces tâches à partir du projet hôte. Pour en savoir plus sur le projet d'hôte et les projets de service dans le contexte d'un VPC partagé, consultez la présentation du VPC partagé.

STEP 1 | Créez un VPC partagé à l'aide du VPC approuvé créé lorsque vous avez déployé le modèle de pare-feu.

Configurez un VPC partagé pour le projet hôte (pare-feu) :

```
gcloud compute shared-vpc enable HOST_PROJECT_ID
```

STEP 2 | Associez le projet de service / application au projet hôte.

```
gcloud compute shared-vpc associated-projects add
[SERVICE_PROJECT_ID]--host-project [HOST_PROJECT_ID]
```

Des options supplémentaires sont disponibles pour partager uniquement des sous-réseaux spécifiques, plutôt que tous les sous-réseaux du projet hôte.

STEP 3 | Si vous souhaitez utiliser le modèle d'application d'exemple pour déployer une application, passez à Déployer le modèle d'application.

Si vous avez déjà déployé une application et que vous souhaitez la sécuriser dans votre déploiement de mise à l'échelle automatique, passez à Intégrer manuellement une application à un déploiement de mise à l'échelle automatique existant.

Si vous avez déployé un service dans un cluster GKE, passez à Intégrer un cluster GKE dans un VPC partagé.

Configurer un VPC appairé

Une connexion d'appairage de réseau VPC doit être établie entre deux VPC. Si les VPC font partie de deux projets différents, une connexion doit être créée dans **les deux** projets.

STEP 1 | Dans le projet hôte, appairez le réseau VPC approuvé du déploiement de pare-feu avec le VPC d'application.

```
gcloud beta compute networks peerings create [PEERING-NAME] \
     --network=[MY-LOCAL-NETWORK] \     --peer-project [SERVICE-
PROJECT-ID] \     --peer-network [PEER-NETWORK-NAME] \    [--
import-custom-routes] \    [--export-custom-routes]
```

STEP 2 | Dans le projet de service, appairez le réseau VPC approuvé du déploiement d'application avec le réseau VPC approuvé du déploiement de pare-feu.

```
gcloud beta compute networks peerings create [PEERING-NAME] \
     --network=[MY-LOCAL-NETWORK] \     --peer-project [HOST-
PROJECT-ID] \     --peer-network [PEER-NETWORK-NAME] \    [--
import-custom-routes] \     [--export-custom-routes]
```


©2023 Palo Alto Networks, Inc.

STEP 3 | Si vous souhaitez utiliser le modèle d'application d'exemple pour déployer une application, passez à Déployer le modèle d'application.

Si vous avez déjà déployé une application et que vous souhaitez la sécuriser dans votre déploiement de mise à l'échelle automatique, passez à Intégrer manuellement une application à un déploiement de mise à l'échelle automatique existant.

Si vous avez déployé un service dans un cluster GKE, passez à Intégrer un cluster GKE dans un VPC appairé.

Déployer le modèle d'application

L'administrateur du projet de service déploie le Modèle d'application du projet de service.

STEP 1 | Créez un projet d'application distinct (projet de service) pour déployer l'application (voir Préparer un projet de service).

STEP 2 | Préparez le fichier `apps.yaml` comme indiqué dans apps.yaml.

STEP 3 | Déployez une nouvelle application avec le modèle d'application et définissez une étiquette pour le port nommé.

```
gcloud deployment-manager deployments create <your-template> --
config apps.yaml --automatic-rollback-on-error
```

Passez à la section Afficher l'application intégrée dans le plugin Panorama pour GCP.

Intégrer une nouvelle application

Lorsque vous utilisez le Modèle d'application pour déployer une application, il s'occupe de la connexion au projet hôte. Vous pouvez sécuriser des applications que vous n'avez pas déployées avec le modèle d'application, à condition qu'elles soient déployées dans un projet de service avec les capacités décrites dans Préparer un projet de service.

- Intégrer manuellement une application à un déploiement de mise à l'échelle automatique existant
- Intégrer un cluster GKE

Intégrer manuellement une application à un déploiement de mise à l'échelle automatique existant

Pour sécuriser une application que vous avez déployée à l'aide d'un équilibreur de charge externe et d'un déploiement de pare-feu VM-Series à mise à l'échelle automatique, suivez ces étapes. Pour chaque application que vous intégrez, vous devez fournir le nom de l'application, les ports nommés et le chemin.

STEP 1 | Préparez-vous à ajouter un nouveau port nommé et un chemin URL à l'équilibreur de charge externe HTTP créé lorsque vous avez déployé le modèle de pare-feu.

STEP 2 | Mettez à jour tous les named-ports (ports nommés) des groupes d'instances avec un nom de service et des valeurs de port supplémentaires. L'exemple suivant intègre les applications `app2` et `app3`.

```
gcloud compute instance-groups set-named-ports fw-template2-fw-igm-
us-east1-b --zone us-east1-b --named-ports=app1:80,app2:81,app3:82
```


©2023 Palo Alto Networks, Inc.

```
 gcloud compute instance-groups set-named-ports fw-
template2-fw-igm-us-east1-c --zone us-east1-c --named-
ports=app1:80,app2:81,app3:82
```

STEP 3 | Créer un nouveau http-health-check (contrôle de santé http).

```
gcloud compute backend-services create fw-template2-backend-app3 --
protocol="HTTP" --port-name=app3 --http-health-checks=fw-template2-
healthcheck-app3 --load-balancing-scheme="EXTERNAL" --global
```

STEP 4 | Créez un nouveau service principal avec le port-name (nom de port) créé précédemment sur l'équilibreur de charge externe HTTP.

```
gcloud compute backend-services create fw-template2-backend-app3 --
protocol="HTTP" --port-name=app3 --http-health-checks=fw-template2-
healthcheck-app3 --load-balancing-scheme="EXTERNAL" --global
```

Vérifiez si le nouveau service principal est visible.

```
gcloud compute backend-services list
```

STEP 5 | Modifiez les url-maps (cartes URL) et ajoutez une nouvelle règle de chemin. Par exemple :

```
- paths:     - /app3     - /app3/*service:     https://
www.googleapis.com/compute/v1/projects/<project-name>/global/
backendServices/fw-template2-backend-app3
```

```
gcloud compute url-maps edit fw-template2-ext-loadbalancer
```

STEP 6 | Pour sécuriser cette application avec le pare-feu VM-Series, déclenchez manuellement le message Pub/Sub via la CLI gcloud. Cela envoie un message au sujet créé dans le modèle de pare-feu.

```
gcloud pubsub topics publish   projects/topics/hj-asg-891ca3-gcp-
pavmqa-panorama-apps-deployment   --attribute ilb-ip=172.22.9.34,
     app-deployment-name=hj-asg-891ca3-app1,     ilb-port=80,
     named-port=81,     network-cidr=172.22.9.0/24,     fw-
deployment-name=hj-asg-891ca3,     host-project=gcp-pavmqa,
     type=ADD-APP   --message "ADD-APP"
```

STEP 7 | Afficher l'application intégrée dans le plugin Panorama pour GCP.

STEP 8 | (Facultatif) Pour mettre à jour les attributs de l'application, tels que ilb-ip, ilb-port ou named-port, exécutez la commande pubsub :

```
gcloud pubsub topics publish projects/gcp-pavmqa/topics/hj-
asg-891ca3-gcp-pavmqa-panorama-apps-deployment   --attribute
```

 ©2023 Palo Alto Networks, Inc.

```
 ilb-ip=172.22.9.34,     app-deployment-name=hj-asg-891ca3-
app1,     ilb-port=80,     named-port=81,     network-
cidr=172.22.9.0/24,     fw-deployment-name=hj-asg-891ca3,     host-
project=gcp-pavmqa,     type=UPDATE-APP   --message "UPDATE-APP"
```

STEP 9 | (Facultatif) Pour arrêter la sécurisation de l'application, exécutez la commande suivante :

```
gcloud pubsub topics publish projects/gcp-pavmqa/topics/hj-
asg-891ca3-gcp-pavmqa-panorama-apps-deployment   --attribute ilb-
ip=172.22.3.20,app-deployment-name=fw-templ-3-app-1,     ilb-
port=80,     named-port=80,     fw-deployment-name=hj-asg-891ca3,
     type=DEL-APP   --message "DEL-APP"
```

Intégrer un cluster GKE

Pour intégrer un cluster GKE privé, le plugin GCP pour Panorama nécessite les informations suivantes.

- Dans GCP, exposez le frontal ELB du cluster au service GKE afin que le pare-feu VM-Series puisse obtenir les informations de port nommé pour le service.
- L'adresse du serveur API du cluster.
- Les informations d'identification du compte de service pour le service dans lequel le cluster est déployé, au format JSON.

Le nom du cluster GKE ne doit pas dépasser 24 caractères. Cela garantit que si vous déployez une mise à l'échelle automatique dans une configuration de VPC appairé, le nom de l'itinéraire statique ne dépasse pas 31 caractères.

- Intégrer un cluster GKE dans un VPC partagé
- Intégrer un cluster GKE dans un VPC appairé
- Afficher l'application intégrée dans le plugin Panorama pour GCP
- Afficher l'état du déploiement depuis la CLI

Intégrer un cluster GKE dans un VPC partagé

Pour intégrer un cluster GKE, vous devez partager le VPC de réseau approuvé du projet hôte avec le projet de service. Reportez-vous à la section Configurer le VPC partagé.

Pour des raisons de sécurité, seuls les clusters privés doivent être utilisés dans un déploiement de mise à l'échelle automatique. Reportez-vous à la section Créer un cluster privé.

STEP 1 | Définissez l'ID du projet hôte.

```
gcloud config set project [HOST_PROJECT_ID]
```

 ©2023 Palo Alto Networks, Inc.

STEP 2 | (Facultatif) Définissez la zone ou la région de calcul pour les clusters.

Si le cluster est zonal, saisissez ce qui suit :

```
gcloud config set compute/zone [COMPUTE_ZONE]
```

Si le cluster est régional, saisissez ce qui suit :

```
gcloud config set compute/region [COMPUTE_REGION]
```

STEP 3 | Dans le projet hôte, mettez à jour les plages secondaires dans le sous-réseau VPC approuvé.

```
gcloud compute networks subnets update [TRUST_SUBNETWORK_NAME]   --
add-secondary-ranges   [PODS_IP_RANGE_NAME] = [POD_RANGE_CIDR],
   [SERVICE_IP_RANGE_NAME]=[SERVICE_RANGE_CIDR]
```

Les plages d'IP des pods et des services doivent être les suivantes : 10.0.0.0/8, 172.16.0.0/12 ou 192.168.0.0/16, et ne peuvent pas chevaucher des plages d'IP existantes dans le sous-réseau.

STEP 4 | Dans le projet de service, créez un cluster privé dans le VPC partagé.

1. Définissez l'ID du projet de service.

   ```
   gcloud config set project [SERVicE_PROJECT_ID]
   ```

2. Créez un cluster privé dans le VPC partagé.

   ```
   gcloud container clusters create  [CLUSTER_NAME]   --project
    [SERVICE_PROJECT_ID]   --zone=[ZONE_NAME]   --enable-
   ip-alias   --enable-private-nodes   --network projects/
   [HOST_PROJECT_ID]/global/networks/[NETWORK_NAME]   --
   subnetwork projects/[HOST_PROJECT_ID]/regions/[REGION_NAME] /
   subnetworks/[TRUST_SUBNETWORK_NAME]   --cluster-secondary-
   range-name=[PODS_IP_RANGE_NAME]   --services-secondary-
   range-name=[SERVICE_IP_RANGE_NAME]   --master-ipv4-
   cidr=[MASTER_IPV4_CIDR]   --enable-master-authorized-networks
      --master-authorized-networks=[PANORAMA_MANAGEMENT_IP/32],
      [MY_MANAGEMENT_IP/32]
   ```

STEP 5 | Vérifiez le contexte de votre cluster actuel :

```
kubectl config current-context
```

STEP 6 | Vérifiez tous les contextes du cluster.

```
kubectl config get-context
```


©2023 Palo Alto Networks, Inc.

STEP 7 | Passez à un autre cluster.

```
kubectl config use-context [CONTEXT_NAME]
```

Si vous avez créé votre cluster dans la console GCP, générez une entrée kubeconfig :

```
gcloud container clusters get-credentials [CLUSTER_NAME]
```

STEP 8 | Créez un rôle de cluster dans un fichier `.yaml`. Par exemple, `gke_cluster_role.yaml`.

```
apiVersion: rbac.authorization.k8s.io/v1beta1 kind: ClusterRole
 metadata:   name: gke-plugin-role rules:   - apiGroups:       - ""
     resources:       - services     verbs:       - list
```

STEP 9 | Appliquez le rôle de cluster.

```
kubectl apply -f gke_cluster_role.yaml
```

STEP 10 | Créer une liaison de rôle de cluster dans un fichier `.yaml`. Par exemple, `gke_cluster_role_binding.yaml`.

```
kind: ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/
v1beta1 metadata:   name: gke-plugin-role-binding subjects:
   - kind: ServiceAccount     name: [SERVICEACCOUNT_NAME]
     namespace: default roleRef:   kind: ClusterRole   name: gke-
plugin-role   apiGroup: rbac.authorization.k8s.io
```

STEP 11 | Appliquez la liaison de rôle de cluster.

```
kubectl apply -f gke_cluster_role_binding.yaml
```

STEP 12 | Créez un compte de service.

```
kubectl create serviceaccount [SERVICEACCOUNT_NAME]
```

STEP 13 | Exportez le jeton secret du compte de service au format JSON.

```
MY_TOKEN=`kubectl get serviceaccounts [SERVICEACCOUNT_NAME] -o
 jsonpath='{.secrets[0].name}'` kubectl get secret $MY_TOKEN -o
 json > [FILE_NAME].json
```

STEP 14 | Obtenez l'adresse du serveur API.

```
kubectl config view --minify | grep server | cut -f 2- -d ":" | tr
 -d " "
```


©2023 Palo Alto Networks, Inc.

STEP 15 | Dans le plugin Panorama pour GCP, ajoutez les informations du compte de service.

Sélectionnez **Panorama** > **Google Cloud Platform** > **Setup (Configuration)**.

Donnez un nom aux informations d'identification, saisissez une description et l'**API server address (Adresse du serveur API)** de l'étape 14 et, pour les **GKE Service Account Credential (Informations d'identification du compte de service GKE)**, chargez le fichier JSON que vous avez exporté à l'étape 13.

Après avoir ajouté des informations d'identification pour le compte de service, vous pouvez les valider à partir de votre ligne de commande Panorama (vous ne pouvez pas les valider depuis l'interface Web) :

```
request plugins gcp validate-service-account gke_service_account
 <svc-acct-credential-name>
```

STEP 16 | Configurez la mise à l'échelle automatique sur le plugin Panorama pour GCP.

1. Dans le contexte de Panorama, développez Google Cloud Platform, sélectionnez AutoScaling (Mise à l'échelle automatique), puis cliquez sur **Add (Ajouter)**.
2. Fournissez le **Firewall Deployment Name (Nom du déploiement de pare-feu)** ainsi qu'une description facultative du déploiement.
3. Pour le **GCP Service Account Credential (Identification du compte de service GCP)**, indiquez le nom du compte de service GCP créé dans Préparer un projet hôte et les comptes de services requis, étape 4.
4. Choisissez le groupe d'appareils et la pile de modèles que vous avez créés lors de la configuration du plugin Panorama.
5. Désactivez **License Management Only (Gestion des licences uniquement)** pour garantir la sécurité du trafic.
6. Saisissez le **GKE Cluster Name (Nom du cluster GKE)** exact.
7. (Facultatif) Saisissez une **Description** du cluster GKE.
8. Saisissez le **Network CIDR (CIDR du réseau)** pour le cluster GKE.
9. Sélectionnez le **GKE Service Account (Compte de service GKE)** correspondant au cluster GKE.

STEP 17 | Validez vos modifications.

STEP 18 | (Facultatif) Créez et déployez un modèle de service selon Utilisation des exemples de modèles de service GKE, ou déployez un service GKE dans la console GCP.

Intégrer un cluster GKE dans un VPC appairé

Pour intégrer le cluster GKE, vous devez créer et appairer le VPC de service avec le réseau approuvé du pare-feu dans le projet hôte, comme décrit dans Configurer un VPC appairé.

Pour des raisons de sécurité, seuls les clusters privés doivent être utilisés dans un déploiement de mise à l'échelle automatique. Reportez-vous à la section Créer un cluster privé.

©2023 Palo Alto Networks, Inc.

STEP 1 | Définissez l'ID du projet.

```
gcloud config set project [PROJECT_ID]
```

STEP 2 | Définissez la zone ou la région de calcul pour les clusters.

Si le cluster est zonal, saisissez ce qui suit :

```
gcloud config set compute/zone [COMPUTE_ZONE]
```

Si le cluster est régional, saisissez ce qui suit :

```
gcloud config set compute/region [COMPUTE_REGION]
```

STEP 3 | Mettez à jour le réseau VPC du projet de service avec les plages d'IP secondaires pour les pods et les services.

```
gcloud compute networks subnets update [GKE_PEERED_VPC_SUBNETWORK]
 --region=[REGION] --add-secondary-ranges PODS_IP_RANGE_NAME=[ip
 cidr], SERVICE_IP_RANGE_NAME=[ip cidr]
```

STEP 4 | Activez la NAT cloud.

Le NAT cloud est nécessaire pour déployer un cluster privé.

```
gcloud compute routers create [ROUTER_NAME]   --network
 [NETWORK_NAME]   --region [REGION_NAME]
```

```
gcloud compute routers nats create [NAT_CONFIG_NAME]   --router-
region [REGION_NAME]   --router [ROUTER_NAME]   --nat-all-subnet-
ip-ranges   --auto-allocate-nat-external-ip
```

STEP 5 | Créez un nouveau cluster privé dans le VPC de service.

```
gcloud container clusters create [CLUSTER_NAME]   --
project [SERVICE_PROJECT_ID]   --zone=[ZONE_NAME]   --
enable-ip-alias   --network [NETWORK_NAME]   --subnetwork
 [SUBNETWORK_NAME]   --enable-private-nodes   --cluster-
secondary-range-name=[PODS_IP_RANGE_NAME]   --services-
secondary-range-name=[SERVICE_IP_RANGE_NAME]   --master-ipv4-
cidr=[MASTER_IPV4_CIDR]   --enable-master-authorized-networks
   --master-authorized-networks=[PANORAMA_MANAGEMENT_IP/32],
   [MY_MANAGEMENT_IP/32]
```


©2023 Palo Alto Networks, Inc.

STEP 6 | Vérifiez le contexte de votre cluster actuel :

```
kubectl config current-context
```

STEP 7 | Vérifiez tous les contextes du cluster.

```
kubectl config get-context
```

STEP 8 | Passez à un autre cluster.

```
kubectl config use-context [CONTEXT_NAME]
```

Si vous avez créé votre cluster dans la console GCP, générez une entrée kubeconfig :

```
gcloud container clusters get-credentials [CLUSTER_NAME]
```

STEP 9 | Créez un rôle de cluster dans un fichier `.yaml`. Par exemple, `gke_cluster_role.yaml`.

```
apiVersion: rbac.authorization.k8s.io/v1beta1 kind: ClusterRole
 metadata:   name: gke-plugin-role rules:   - apiGroups:       - ""
     resources:       - services     verbs:       - list
```

STEP 10 | Appliquez le rôle de cluster.

```
kubectl apply -f gke_cluster_role.yaml
```

STEP 11 | Créer une liaison de rôle de cluster dans un fichier `.yaml`. Par exemple, `gke_cluster_role_binding.yaml`.

```
kind: ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/
v1beta1 metadata:   name: gke-plugin-role-binding subjects:
   - kind: ServiceAccount     name: [SERVICEACCOUNT_NAME]
     namespace: default roleRef:   kind: ClusterRole   name: gke-
plugin-role   apiGroup: rbac.authorization.k8s.io
```

STEP 12 | Appliquez la liaison de rôle de cluster.

```
kubectl apply -f gke_cluster_role_binding.yaml
```

STEP 13 | Créez un compte de service.

```
kubectl create serviceaccount [SERVICEACCOUNT_NAME]
```

 ©2023 Palo Alto Networks, Inc.

STEP 14 | Exportez le jeton secret du compte de service au format JSON.

```
MY_TOKEN=`kubectl get serviceaccounts [SERVICEACCOUNT_NAME] -o
 jsonpath='{.secrets[0].name}'` kubectl get secret $MY_TOKEN -o
 json >[FILE_NAME].json
```

STEP 15 | Obtenez l'adresse du serveur API.

```
kubectl config view --minify | grep server | cut -f 2- -d ":" | tr
 -d " "
```

STEP 16 | Dans le plugin Panorama pour GCP, ajoutez les informations du compte de service.

Sélectionnez **Panorama** > **Google Cloud Platform** > **Setup (Configuration)**.

Donnez un nom aux informations d'identification et saisissez l'**API server address (Adresse du serveur API)** de l'étape 15, et téléchargez le fichier JSON que vous avez exporté à l'étape 14.

Après avoir ajouté des informations d'identification pour le compte de service, vous pouvez les valider à partir de votre ligne de commande Panorama :

```
request plugins gcp validate-service-account <svc-acct-credential-
name>
```

STEP 17 | Configurez la mise à l'échelle automatique sur le plugin Panorama pour GCP.

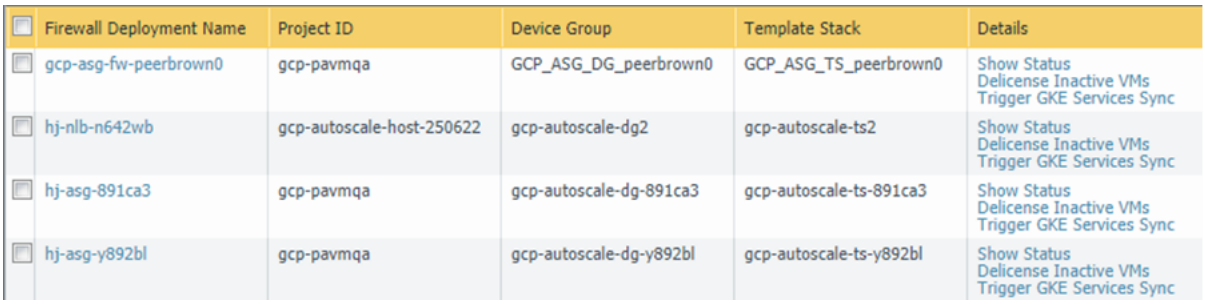
1. Dans le contexte de Panorama, développez Google Cloud Platform, sélectionnez AutoScaling (Mise à l'échelle automatique), puis cliquez sur **Add (Ajouter)**.
2. Fournissez le **Firewall Deployment Name (Nom du déploiement de pare-feu)** ainsi qu'une description facultative du déploiement.
3. Pour les **GCP Service Account Credential (Informations d'identification pour le compte de service GCP)**, indiquez le nom du compte de service GCP de l'étape 16.
4. Choisissez le groupe d'appareils et la pile de modèles que vous avez créés lors de la configuration du plugin Panorama.
5. Désactivez **License Management Only (Gestion des licences uniquement)** pour garantir la sécurité du trafic.
6. Saisissez le **GKE Cluster Name (Nom du cluster GKE)** exact.
7. (Facultatif) Saisissez une **Description** du cluster GKE.
8. Saisissez le **Network CIDR (CIDR du réseau)** pour le cluster GKE.
9. Sélectionnez le **GKE Service Account (Compte de service GKE)** correspondant au cluster GKE.

STEP 18 | (Facultatif) Dans votre projet de service, créez et déployez un modèle GKE selon Utilisation des exemples de modèles de service GKE, ou déployez un service GKE en utilisant la console GCP. Intégrer un cluster GKE

 ©2023 Palo Alto Networks, Inc.

Afficher l'application intégrée dans le plugin Panorama pour GCP

Sélectionnez **Panorama** > **Google Cloud Platform** > **Autoscaling (Mise à l'échelle automatique)** pour afficher votre application intégrée. La colonne **Details (Détails)** n'est visible que si vous avez une application intégrée.

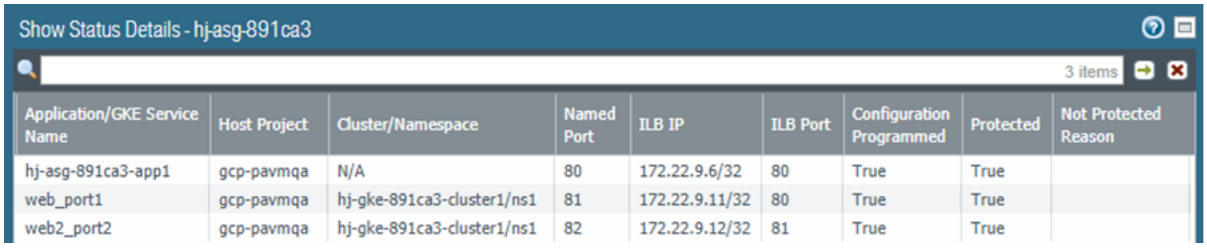


Firewall Deployment Name	Project ID	Device Group	Template Stack	Details
gcp-asg-fw-peerbrown0	gcp-pavmqa	GCP_ASG_DG_peerbrown0	GCP_ASG_TS_peerbrown0	Show Status Delicense Inactive VMs Trigger GKE Services Sync
hj-nlb-n642wb	gcp-autoscale-host-250622	gcp-autoscale-dg2	gcp-autoscale-ts2	Show Status Delicense Inactive VMs Trigger GKE Services Sync
hj-asg-891ca3	gcp-pavmqa	gcp-autoscale-dg-891ca3	gcp-autoscale-ts-891ca3	Show Status Delicense Inactive VMs Trigger GKE Services Sync
hj-asg-y892bl	gcp-pavmqa	gcp-autoscale-dg-y892bl	gcp-autoscale-ts-y892bl	Show Status Delicense Inactive VMs Trigger GKE Services Sync

Chaque lien dans la colonne Details (Détails) déclenche une action.

©2023 Palo Alto Networks, Inc.

- **Show Status (Afficher l'état)** : affiche les détails des applications intégrées dans un déploiement de pare-feu VM-Series GCP.



Application/GKE Service Name	Host Project	Cluster/Namespace	Named Port	ILB IP	ILB Port	Configuration Programmed	Protected	Not Protected Reason
hj-asg-891ca3-app1	gcp-pavmqa	N/A	80	172.22.9.6/32	80	True	True	
web_port1	gcp-pavmqa	hj-gke-891ca3-cluster1/ns1	81	172.22.9.11/32	80	True	True	
web2_port2	gcp-pavmqa	hj-gke-891ca3-cluster1/ns1	82	172.22.9.12/32	81	True	True	

Les champs suivants affichent les informations obtenues à partir du déploiement sélectionné. Vous avez spécifié ces valeurs dans le message Pub/Sub ou par l'intermédiaire de l'interrogation des services du cluster GKE.

- **Application/GKE Service Name (Nom du service d'application/GKE)** : un nom de déploiement d'application, ou le nom d'un service GKE.
- **Host Project (Projet hôte)** : le nom du projet hôte.
- **Cluster/Namespace (Cluster/espace de noms)** : un nom de cluster GKE suivi de l'espace de noms. Par exemple, **`mycluster/namespace9`**.
- **Named Port (Port nommé)** : le port attribué au port nommé pour le service.
- **ILB IP (IP ILB)** : l'adresse IP de l'ILB.
- **ILB Port (Port ILB)** : le numéro de port de l'ILB.

  Pour la mise à l'échelle automatique d'une application, cette propriété est **`ilb-port`** dans `apps.yaml`.

  Pour sécuriser un cluster GKE, cette valeur est le numéro de port du cluster GKE, tel que spécifié dans le fichier `.yaml` que vous avez utilisé pour déployer le service dans votre cluster.
- **Configuration Programmed (Configuration programmée)** : True (Vrai) si une règle de NAT existe ; False (Faux) si ce n'est pas le cas.
- **Protected (Protégé)** : True (Vrai) lorsqu'une application est intégrée avec succès ; False (Faux) si l'intégration a échoué. Si False (Faux), consultez la colonne **Not Protected Reason (Motif de non-protection)** pour obtenir une explication.
- **Not Protected Reason (Motif de non-protection)** : si **Protected (Protégé)** est False (Faux), cela affiche le motif pour lequel l'application n'est pas protégée. Voici quelques raisons courantes :
  - **Configuration Programmed (Configuration programmée)** : True (Vrai) si une règle de NAT existe ; False (Faux) si ce n'est pas le cas.
  - **Protected (Protégé)** : True (Vrai) lorsqu'une application est intégrée avec succès ; False (Faux) si l'intégration a échoué. Si False (Faux), consultez la colonne **Not Protected Reason (Motif de non-protection)** pour obtenir une explication.
  - **Not Protected Reason (Motif de non-protection)** : si **Protected (Protégé)** est False (Faux), cela affiche le motif pour lequel l'application n'est pas protégée. Voici quelques raisons courantes :
    - Vous avez déployé un service UDP dans le cluster GKE.

©2023 Palo Alto Networks, Inc.

    - Vous avez spécifié un port nommé qui est déjà utilisé. Une seule application peut écouter sur un port nommé spécifique.
    - Vous avez choisi l'option **License management only (Gestion des licences uniquement)** ; nous ne programmons donc pas la configuration.
    - Aucune étiquette correspondante n'a été trouvée pour les services GKE.
- **Delicense Inactive VMs (Supprimer les licences des VM inactives)** : répondez **Yes (Oui)** pour déclencher la fonction de suppression des licences des VM inactives.
- **Trigger GKE Services Sync (Déclencher la synchronisation des services GKE)** : répondez **Yes (Oui)** pour interroger les services exécutés dans les clusters et programmez la NAT, l'adresse et les objets de service, ainsi que les itinéraires statiques si nécessaire. Par défaut, Panorama interroge automatiquement 10 minutes après la fin de l'interrogation précédente.

Afficher l'état du déploiement depuis la CLI

Vous pouvez utiliser la CLI Panorama pour gérer les applications déployées. Les actions de ligne de commande sont parallèles à celles décrites dans Afficher l'application intégrée dans le plugin Panorama pour GCP. Dans les commandes suivantes, **autoscaling_name** correspond au nom du déploiement de pare-feu que vous avez saisi dans la configuration de mise à l'échelle automatique.

- Énumérez les applications intégrées (protégées).

```
show plugins gcp show-protected-apps autoscaling_name <fw-deployment-name>
```

- Déclenchez la fonction de suppression des licences pour les pare-feu dans le déploiement spécifié.

```
request plugins gcp force-delicensing autoscaling_name <fw-deployment-name>
```

- Pour un déploiement GKE, forcez le plugin à lire les messages Pub-Sub, et synchronisez les règles NAT qui sont programmées en fonction des messages Pub-Sub.

```
request plugins gcp gke-service-discovery autoscaling_name <fw-deployment-name>
```

Paramètres des modèles de mise à l'échelle automatique pour GCP

Vous pouvez télécharger le fichier `.zip` des modèles depuis https://github.com/PaloAltoNetworks/GCP-AutoScaling. Le fichier `.zip` contient des répertoires permettant de prendre en charge les modèles de pare-feu pour les configurations de l'équilibreur de charge de réseau et de l'équilibreur de charge d'application, ainsi que le modèle d'application.

Les fichiers YAML des modèles ont le format général suivant :

```
#Informations de droits d'auteur et de licence     :     :
 imports:                      <do not change>     :     : resources:
     -name: vm-series-fw       <do not change>     -type:vm-series-
fw.py    <do not change
    -properties:
```

 ©2023 Palo Alto Networks, Inc.

```
    :
    :
outputs:                        <do not change>     :     :
```

Dans tous les fichiers **.yaml**, vous personnalisez les propriétés des **ressources** pour votre déploiement. Ne modifiez rien dans les sections **imports** ou **outputs**.

- Modèles de pare-feu
- Modèle d'application

Modèles de pare-feu

Les sections suivantes détaillent les paramètres des fichiers **.yaml** de NLB et ALB.

- vm-series-fw-nlb.yaml
- vm-series-fw-alb.yaml

vm-series-fw-nlb.yaml

Dans le modèle **vm-series-fw-nlb.yaml**, modifiez **-properties**.

Paramètre	Valeur d'exemple	Commentaire
region	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <list of zones>	zones- us-central1-a	Le cas échéant, indiquez plusieurs zones comme suit : zones- us-central1-a- us-central1-b- us-central1-c- us-central1-f
lb-type	nlb	Ne le modifiez pas.
cloud-nat	yes	Ne le modifiez pas.
forwarding-rule-port	80	80 ou 8080
urlPath-namedPort-maps-appname	`urlPath-namedPort-maps -MyApplication`	Saisissez le nom de votre application.
sshkey	'admin:ssh-rsa <PASTE KEY>'	Examinez Paire de clés SSH. Entre guillemets simples, saisissez **admin:** suivi d'un espace, et collez votre clé. Il s'agit de la même convention que celle utilisée pour le modèle Google Marketplace.

©2023 Palo Alto Networks, Inc.

Paramètre	Valeur d'exemple	Commentaire
bootstrap-bucket	bootstrap-autoscale	Le nom du compartiment GCP contenant votre fichier d'amorçage.
image	vm-series-byol-814	L'image BYOL actuellement disponible sur Google Marketplace. Si vous utilisez PAYG ou un autre modèle de licence, l'image peut être différente.
machine-type	n1-standard-4	n1-standard-4 est la valeur par défaut pour BYOL. Si votre licence le permet, vous pouvez utiliser n'importe quel type de machine dans Exigences minimales du système pour le pare-feu de série VM.
service-account		Le nom du compte de service unique pour le projet hôte.
fw-instance-tag	vm-series-fw	L'étiquette d'instance que vous avez fournie dans GCP.
metric	custom.googleapis.com/VMSeries/panSessionActive	Le chemin de l'API personnalisée pour VM-Series et la métrique de mise à l'échelle automatique de votre choix. Ne fournissez qu'une seule des métriques suivantes. `panSessionActive panSessionUtilization DataPlaneCPUUtilizationPct DataPlanePacketBufferUtilization panSessionUtilization`
max-size	2	
min-size	1	

©2023 Palo Alto Networks, Inc.

Paramètre	Valeur d'exemple	Commentaire
target-type	GAUGE	Actuellement, GAUGE est le seul type valable.
util-target	100	
Pour déployer le pare-feu VM-Series, vous devez disposer d'un réseau et d'un sous-réseau dédiés pour les interfaces de gestion, non approuvées et approuvées du pare-feu. Remplissez les informations pour un déploiement greenfield (configurez le modèle pour créer de nouveaux réseaux) ou un déploiement brownfield (utilisez les réseaux existants). Veillez à supprimer ou à exclure par commentaire les paramètres de déploiement de réseau que vous n'utilisez pas.		
Déploiement greenfield : saisissez des valeurs pour créer des réseaux et sous-réseaux de gestion, approuvés et non approuvés pour le pare-feu.		
mgmt-network-cidr	172.22.2.0/24	
untrust-network-cidr	172.22.1.0/24	
trust-network-cidr	172.22.3.0/24	
mgmt-network-access-source-range- <permitted-ip-range>	`mgmt-network-access-source-range - <permitted-ip-range-1> - <permitted-ip-range-2>`	
mgmt-network-access-ports-<port-number>	`mgmt-network-access-ports - 22 - 443`	
Déploiement brownfield : saisissez le nom de chaque réseau ou sous-réseau existant.		
mgmt-network	my-mgmt-network	
mgmt-subnet	my-mgmt-subnet	
trust-network	my-trust-network	
trust-subnet	my-trust-subnet	
untrust-network	my-untrust-network	
untrust-subnet	my-untrust-subnet	

vm-series-fw-alb.yaml

Dans le modèle `vm-series-fw-alb.yaml`, modifiez `-properties`.

©2023 Palo Alto Networks, Inc.

Paramètre	Valeur d'exemple	Commentaire
region	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <list of zones>	zones- us-central1-a	Le cas échéant, indiquez plusieurs zones comme suit : zones- us-central1-a- us-central1-b- us-central1-c- us-central1-f
lb-type	alb	Ne le modifiez pas.
cloud-nat	yes	Ne le modifiez pas.
forwarding-rule-port	80	80
connection-draining-timeout	300	La valeur du délai d'expiration en secondes.
`urlPath-namedPort-maps: - appname: namedPort: urlMapPaths: - '/app1' - '/app1/*'`	`urlPath-namedPort-maps: - appName: app1 namedPort: 80 urlMapPaths: - '/app1' - '/app1/*' - appName: app2 namedPort: 81 urlMapPaths: - '/app2' - '/app2/*'`	Énumérez vos applications et le port nommé correspondant.
sshkey	'admin:ssh-rsa <PASTE KEY>'	Examinez Paire de clés SSH. Entre guillemets simples, saisissez **`admin:`** suivi d'un espace, et collez votre clé. Il s'agit de la même convention que celle utilisée pour le modèle Google Marketplace.
bootstrap-bucket	bootstrap-bucket-name	Le nom du compartiment GCP contenant votre fichier d'amorçage.
image	vm-series-byol-814	L'image BYOL actuellement disponible sur Google Marketplace. Si vous utilisez PAYG ou un autre modèle de licence, l'image peut être différente.

©2023 Palo Alto Networks, Inc.

Paramètre	Valeur d'exemple	Commentaire
machine-type	n1-standard-4	n1-standard-4 est la valeur par défaut pour BYOL. Si votre licence le permet, vous pouvez utiliser n'importe quel type de machine dans Exigences minimales du système pour le pare-feu de série VM.
service-account	Le nom du compte de service unique pour le projet de service.	
fw-instance-tag	vm-series-fw	L'étiquette d'instance que vous avez fournie dans GCP.
metric	custom.googleapis.com/VMSeries/panSessionActive	Le chemin de l'API personnalisée pour VM-Series et la métrique de mise à l'échelle automatique de votre choix. Ne fournissez qu'une seule des métriques suivantes. `panSessionActive panSessionUtilization DataPlaneCPUUtilizationPct DataPlanePacketBufferUtilization panSessionUtilization`
max-size	2	
min-size	1	
target-type	GAUGE	Actuellement, GAUGE est le seul type valable.
util-target	100	Saisissez la valeur cible d'utilisation d'objectif pour la mise à l'échelle automatique.
Déploiement greenfield : saisissez des valeurs pour créer des réseaux et sous-réseaux de gestion, approuvés et non approuvés pour le pare-feu.		
mgmt-network-cidr	192.168.12.0/24	
untrust-network-cidr	192.168.11.0/24	
trust-network-cidr	192.168.11.0/24	

©2023 Palo Alto Networks, Inc.

Paramètre	Valeur d'exemple	Commentaire
mgmt-network-access-source-range- <permitted-ip-range>	`mgmt-network-access-source-range- <permitted-ip-range-1>- <permitted-ip-range-2>`	
mgmt-network-access-ports-<port-number>	`mgmt-network-access-ports- 22- 443`	
Déploiement brownfield : saisissez le nom de chaque réseau ou sous-réseau existant.		
mgmt-network	existing-vpc-mgmt	
mgmt-subnet	existing-subnet-mgmt	
trust-network	existing-vpc-trust	
trust-subnet	existing-subnet-trust	
untrust-network	existing-vpc-untrust	
untrust-subnet	existing-subnet-untrust	

Modèle d'application
apps.yaml

Le modèle d'application crée la connexion entre le projet hôte (qui contient les pare-feu VM-Series) et le projet de service, qui contient l'application ou les services que le déploiement du pare-feu sécurise.

Paramètre	Valeur d'exemple	Commentaire
host-project	your-host-project-name	Le nom du projet contenant le déploiement de pare-feu VM-Series.
fw-deployment-name	my-vm-series-firewall-name	
region	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <list of zones>	zones- us-central1-a	Le cas échéant, indiquez plusieurs zones comme suit : `zones- us-central1-a - us-central1-b- us-central1-c- us-central1-f`

©2023 Palo Alto Networks, Inc.

Paramètre	Valeur d'exemple	Commentaire
app-machine-type	n1-standard-2	Le type de machine pour la VM qui exécute votre application ou service. Si votre licence le permet, vous pouvez utiliser n'importe quel type de machine dans Exigences minimales du système pour le pare-feu de série VM.
app-instance-tag	web-app-vm	Vous avez appliqué cette étiquette dans GCP.
sshkey	'admin:ssh-rsa <PASTE KEY>'	Examinez Paire de clés SSH. Entre guillemets simples, saisissez **`admin:`** suivi d'un espace, et collez votre clé. Il s'agit de la même convention que celle utilisée pour le modèle Google Marketplace.
trust-network	<project-name>/<vpc-network-name>	Pour un VPC partagé, <project-name> correspond au nom du projet hôte. Pour les VPC appairés, <project-name> correspond au nom du projet de service.
trust-subnet	<project-name>/<subnet-name>	Pour un VPC partagé, <project-name> correspond au nom du projet hôte. Pour les VPC appairés, <project-name> correspond au nom du projet de service.
trust-subnet-cidr	10.2.0.0/24	Pour un déploiement greenfield, le CIDR du sous-réseau approuvé du projet hôte (le paramètre trust-network-cidr dans le modèle de pare-feu). Pour un déploiement brownfield, le CIDR du réseau approuvé.
vm-series-fw-template-topic	<pubsub-topic>	Saisissez le nom du sujet créé par le déploiement de pare-feu.

©2023 Palo Alto Networks, Inc.

Paramètre	Valeur d'exemple	Commentaire
		Le modèle d'application publie un message dans le sujet pour programmer la configuration du pare-feu afin de transférer le trafic.
ilb-port	80	Saisissez le numéro de port pour la sortie internal-load-balancer-port de votre application.
urlPath-namedPort	83	Saisissez le numéro de port pour la sortie urlPath-namedPort.

Exemples de modèles de service GKE

Ces exemples de modèles montrent comment configurer un service GKE pour qu'il soit sécurisé par le pare-feu VM-Series. Pour connaître les bases de la création de vos propres services de cluster, Reportez-vous à la section Créer un cluster privé.

- Utilisation des exemples de modèles de service GKE
- gke_cluster_role.yaml
- gke_cluster_role_binding.yaml
- web-deployment.yaml
- web-service.yaml
- web-deployment-v2.yaml
- web-service-v2.yaml
- Plusieurs ports dans un même service

Utilisation des exemples de modèles de service GKE

Vous pouvez créer un modèle de service basé sur l'exemple de contenu des fichiers `.yaml` qui suivent. En général, vous créez un seul fichier `.yaml`.

Pour être sécurisés par le pare-feu VM-Series, les services du cluster doivent être étiquetés "panw-named-port=<named_port>", comme indiqué dans web-service.yaml et web-service-v2.yaml.

1. Déployez un fichier `.yaml` comme suit :

```
kubectl apply -f [FILE_NAME].yaml
```

2. Configurez le déploiement du VPC.
   - Dans un déploiement de VPC partagé, lancez le cluster GKE dans le VPC partagé comme décrit dans Configurer le VPC partagé.
   - Dans un déploiement de VPC appairé, appairez le VPC du cluster GKE au réseau approuvé du projet hôte. Reportez-vous à la section Configurer un VPC appairé.

©2023 Palo Alto Networks, Inc.

Après un déploiement, vous pouvez supprimer tous les services déployés dans le fichier `.yaml` du modèle de service comme suit :

```
kubectl delete -f [FILE_NAME].yaml
```

gke_cluster_role.yaml

```
apiVersion: rbac.authorization.k8s.io/v1beta1 kind: ClusterRole
 metadata:   name: gke-plugin-role rules:   - apiGroups:       - ""
     resources:       - services     verbs:       - list
```

gke_cluster_role_binding.yaml

```
kind: ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/
v1beta1 metadata:   name: gke-plugin-role-binding subjects:   - kind:
 ServiceAccount     name: hj-gke-891ca3-cluster1-sa     namespace:
 default roleRef:   kind: ClusterRole   name: gke-plugin-role
   apiGroup: rbac.authorization.k8s.io
```

web-deployment.yaml

```
apiVersion: extensions/v1beta1 kind: Deployment metadata:   name:
 web   namespace: default spec:   selector:    matchLabels:     run:
 web   template:    metadata:     labels:       run: web    spec:
     containers:     - image: gcr.io/google-samples/hello-app:1.0
       imagePullPolicy: IfNotPresent       name: web       ports:
       - containerPort: 8080        protocol:  TCP
```

web-service.yaml

```
apiVersion: v1 kind: Service metadata:   name: web   namespace:
 default   annotations:     cloud.google.com/load-balancer-type:
 "Internal"   labels:     panw-named-port-port1: "80" spec:   ports:
   # le port sur lequel ce service doit être desservi   - name: port1
     port: 80     protocol: TCP     targetPort: 8080   selector:
     run: web   type: LoadBalancer (Équilibreur de charge)
```

web-deployment-v2.yaml

```
apiVersion: extensions/v1beta1 kind: Deployment metadata:   name:
 web2   namespace: default spec:   selector:     matchLabels:
       run: web2   template:     metadata:       labels:         run:
 web2     spec:       containers:       - image: gcr.io/google-
samples/hello-app:2.0         imagePullPolicy: IfNotPresent
         name: web2         ports:         - containerPort: 8080
           protocol: TCP
```


©2023 Palo Alto Networks, Inc.

web-service-v2.yaml

```
apiVersion: v1   kind: Service   metadata:     name: web2
     namespace: default     annotations:       cloud.google.com/
load-balancer-type: "Internal"     labels:       panw-named-port-
port2: "81"   spec:     ports:     # le port sur lequel ce service
 doit être desservi     - name: port2       port: 81       protocol:
 TCP       targetPort: 8080     selector:       run: web2     type:
 LoadBalancer (Équilibreur de charge)
```

Plusieurs ports dans un même service

Pour plusieurs ports dans un même service, modifiez les étiquettes et mappez le nom et le numéro du port cible au format panw-named-port-*<service-spec-port-name>*, comme indiqué dans l'exemple ci-dessous.

```
apiVersion: v1 kind: Service metadata:   name: carts   annotations:
     cloud.google.com/load-balancer-type: "Internal"   labels:
     panw-named-port-carts-http: "6082"     panw-named-port-carts-
https: "6083"   namespace: default spec:   type: LoadBalancer
   ports:   # le port sur lequel ce service doit être desservi   -
 name: carts-http     : TCP     port: 80     targetPort: 80   - name:
 carts-https     protocol: TCP     port: 443     targetPort: 443
   selector:     name: carts
```


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Configuration d'un pare-feu VM-Series sur un réseau Cisco ENCS

Si vous avez virtualisé l'infrastructure de réseau traditionnelle basée sur un appareil dans votre succursale ou votre bureau distant avec l'appareil Enterprise Network Compute System (ENCS) Cisco série 5400, vous pouvez utiliser Enterprise NFV Infrastructure Software (NFVIS) pour déployer le pare-feu VM-Series au sein de votre réseau Cisco. Le pare-feu VM-Series sert de fonction réseau virtuel (VNF) dotée de fonctionnalités de pare-feu nouvelle génération permettant d'activer toutes les applications en toute sécurité et de protéger les utilisateurs de votre succursale ou de votre bureau distant ainsi que le réseau contre les menaces.

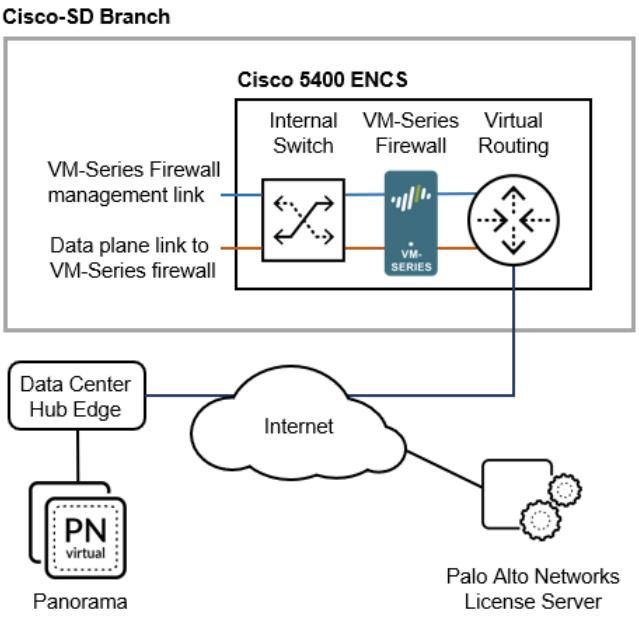
Les appareils Enterprise Network Compute System (ENCS) Cisco s'associent aux routeurs virtuels de services intégrés (ISRV) Cisco et au logiciel NFVIS pour prendre en charge des architectures réseau de succursale définie par logiciel (Succursale définie par logiciel).

- Planification de votre déploiement Cisco ENCS
- Préparation de l'image du pare-feu VM-Series pour Cisco ENCS
- Déploiement du pare-feu VM-Series sur Cisco ENCS

Planification de votre déploiement Cisco ENCS

Dans votre Cisco SD-Branch (Succursale définie par logiciel), déployez le pare-feu VM-Series sur l'appareil Cisco ENCS en tant que VNF offrant des fonctionnalités de pare-feu nouvelle génération pour sécuriser vos applications et vos utilisateurs au niveau de la succursale. Vous pouvez déployer le pare-feu dans un déploiement de câble virtuel, couche 2 ou couche 3, ainsi que dans une configuration à haute disponibilité.

Pour gérer le pare-feu VM-Series, l'appareil Panorama peut être déployé sur site ou dans le cloud. La topologie suivante montre le pare-feu VM-Series au niveau de la limite de la succursale.



Configuration requise pour Cisco ENCS

Pour les versions et les plateformes matérielles NFVIS prises en charge, reportez-vous à la matrice de compatibilité Palo Alto Networks.

- Dans NFVIS, configurez des réseaux et des ponts.
  - Créez des NIC virtuelles et connectez-les à un pont virtuel afin que l'appareil ENCS puisse diriger le trafic à travers le pare-feu VM-Series.

    Sur l'appareil Cisco ENCS, le pare-feu VM-Series prend en charge jusqu'à 8 interfaces du dataplane.

    Les interfaces du dataplane du pare-feu VM-Series sur Cisco ENCS prennent en charge le mode Virtio uniquement ; les modes de liaison ENCS SR-IOV et PCI ne sont pas pris en charge.
  - Configurez les connexions réseau pour l'accès de gestion au pare-feu VM-Series. Si vous utilisez Panorama, assurez-vous que Panorama dispose d'un accès réseau pour gérer le pare-feu que vous déployez.
- Python 2.7. Obligatoire sur votre ordinateur local si vous utilisez la ligne de commande pour la conversion.

©2023 Palo Alto Networks, Inc.

Pare-feu VM-Series et Panorama : configuration requise

- Pare-feu VM-Series : les modèles VM-50 et VM-100 sont recommandés. Les modèles VM-300, VM-500 et VM-700 sont également pris en charge, à condition que le matériel ENCS dispose des ressources suffisantes pouvant être attribuées au pare-feu VM-Series. Consultez la section Configuration système requise pour VM-Series pour vous assurer que l'appareil Cisco ENCS dispose des ressources suffisantes pour prendre en charge le modèle VM-Series de votre choix.
  - Fichier qcow2 (PAN-OS pour l'image de base KVM VM-Series) pour PAN-OS 9.1 ou version ultérieure. Reportez-vous aux sections Convertissez un fichier qcow2 à partir de l'interface utilisateur graphique, Étape 2 ou Convertissez un fichier qcow2 à partir de l'interface de ligne de commande, Étape 2.
  - Les codes d'autorisation d'abonnement et de licence de capacité de pare-feu VM-Series qui répondent à vos besoins. Reportez-vous à la section Types de licences de modèle VM-Series. Vous saisissez des codes d'autorisation dans l'interface utilisateur NFVIS ou les incluez dans le fichier texte **`authcodes`** du dossier de conversion comme décrit à la section Convertissez un fichier qcow2 à partir de l'interface de ligne de commande, Étape 4.
  - Avec PAN-OS 9.1, le pare-feu VM-Series sur Cisco ENCS prend en charge Virtio avec le mode DPDK activé par défaut.
- Appareil virtuel ou matériel Panorama. Bien que vous puissiez déployer un pare-feu VM-Series unique dans un réseau de Succursale définie par logiciel Cisco, il est plus courant de déployer des pare-feu dans de nombreuses succursales et de les gérer de manière centralisée avec Panorama.
  - Panorama version 9.1 ou ultérieure. La version doit être identique ou supérieure à la version de votre pare-feu VM-Series.
  - Une clé d'authentification VM est générée sur Panorama. Cette clé permet au pare-feu VM-Series de s'authentifier auprès de Panorama.

©2023 Palo Alto Networks, Inc.

Préparation de l'image du pare-feu VM-Series pour Cisco ENCS

Vous pouvez convertir un fichier qcow2 PAN-OS à partir de l'interface utilisateur graphique NFVIS ou de l'interface de ligne de commande.

- Convertissez un fichier qcow2 à partir de l'interface utilisateur graphique
- Convertissez un fichier qcow2 à partir de l'interface de ligne de commande

Convertissez un fichier qcow2 à partir de l'interface utilisateur graphique

Utilisez l'interface utilisateur graphique NFVIS pour saisir des informations sur le paquet d'image et l'amorçage.

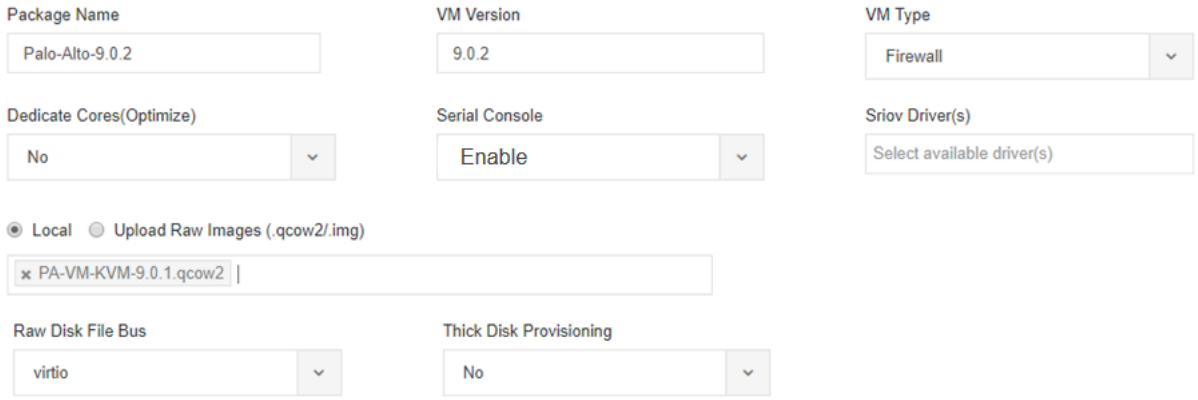
STEP 1 | Dans NFVIS, accédez à **VM Life Cycle (Cycle de vie de la machine virtuelle)** > **Image Repository (Référentiel d'image)** > **Image Packaging (Paquet d'image)**.

 ©2023 Palo Alto Networks, Inc.

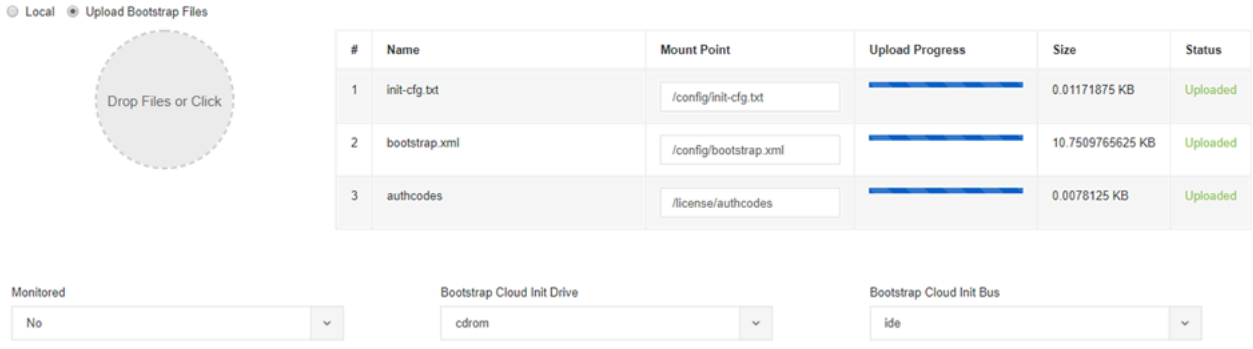
STEP 2 | Complétez les informations du paquet comme indiqué ci-dessous, en fournissant vos propres valeurs.

1. Saisissez un **Package Name** (Nom du paquet) et la **VM Version** (Version de machine virtuelle) et pour le **VM Type** (Type de machine virtuelle), choisissez **Firewall** (Pare-feu).
2. Cliquez sur **Enable (Activer)** pour activer la **Serial Console (Console série)**.
3. Laissez le champ **Sriov Driver(s)** (Pilote(s) Sriov) vide, car SR-IOV n'est pas pris en charge.
4. Sélectionnez **Local** pour choisir un fichier qcow2 que vous avez précédemment chargé ou cliquez sur **Upload Raw Images** (Charger des images brutes) pour charger un fichier qcow2.
   - Connectez-vous au Customer Support Portal (Portail assistance clientèle) de Palo Alto Networks.

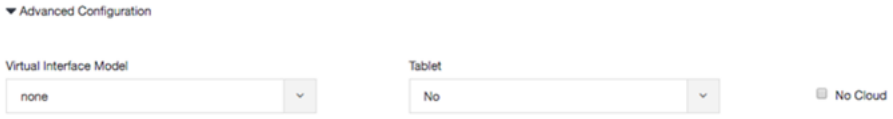
     Si vous ne l'avez pas déjà fait, créez un compte de support et procédez à l'enregistrement du pare-feu VM-Series.
   - Sélectionnez **Support (Prise en charge)** > **Software Updates (Mises à jour logicielles)** et dans la liste déroulante **Filter By (Filtrer par)**, sélectionnez **Pan OS for VM-Series KVM Base Image (Pan OS pour l'image de base KVM VM-Series)** par exemple, version 9.1.
   - Téléchargez l'image qcow2.



STEP 3 | Chargez les fichiers d'amorçage.

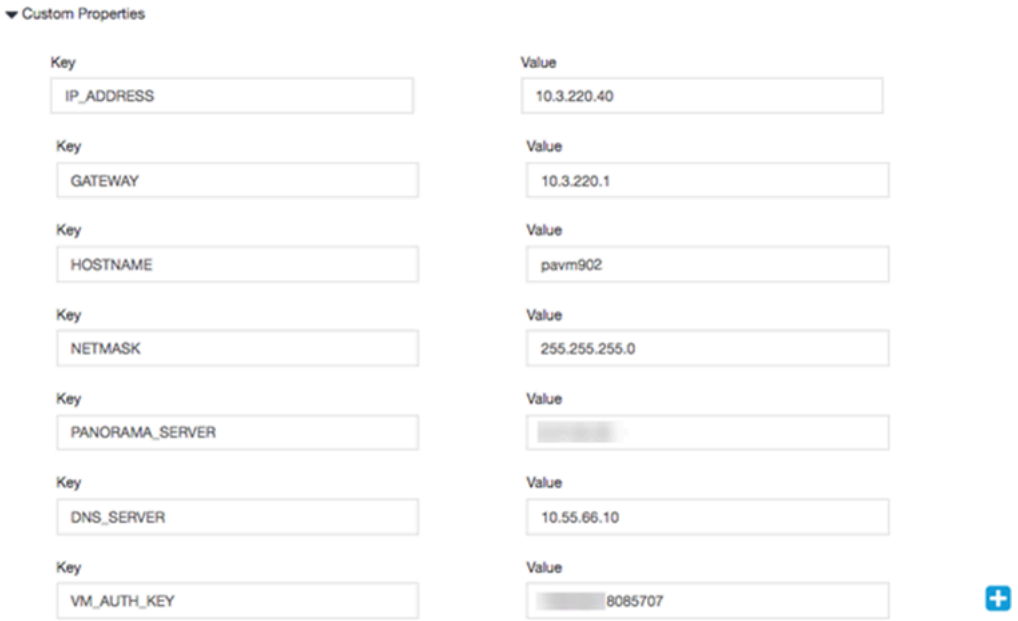


STEP 4 | Définissez la **Advanced Configuration** (Configuration avancée).



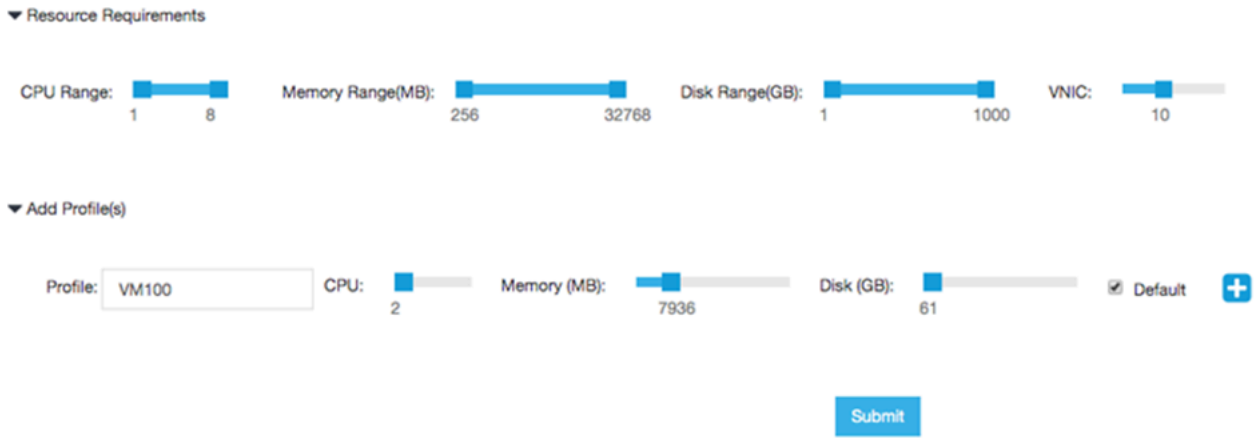
 ©2023 Palo Alto Networks, Inc.

STEP 5 | Saisissez des valeurs pour **Custom Properties** (Propriétés personnalisées).

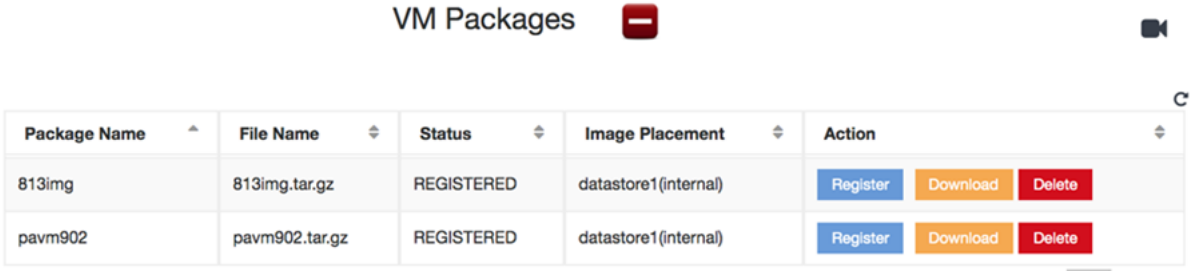


STEP 6 | Définissez des valeurs pour vos Resource Requirements (Besoins en ressources) et choisissez le profil Default (Par défaut) ou Add Profile(s) (Ajouter un ou plusieurs profils) pour la configuration actuelle.

Cliquez sur **Submit** (Envoyer) pour enregistrer votre paquet.



STEP 7 | Cliquez sur **Register** (Enregistrer) pour enregistrer l'image sélectionnée.



 ©2023 Palo Alto Networks, Inc.

Convertissez un fichier qcow2 à partir de l'interface de ligne de commande

Pour créer un fichier d'amorçage à partir de l'interface de ligne de commande, vous devez créer le fichier `image_properties_template.xml` puis utiliser l'utilitaire de paquet d'image VM pour créer un fichier `.tar` que vous convertirez en utilisant le script `nfvpt.py`. Le fichier généré est un fichier `tar.gz` pouvant être téléchargé à partir de l'interface utilisateur NFVIS.

STEP 1 | Créez ou choisissez un dossier sur votre ordinateur local (le dossier de conversion) dans lequel vous souhaitez télécharger et enregistrer les fichiers nécessaires à la conversion de l'image qcow2 du pare-feu VM-Series au format Cisco ENCS.

STEP 2 | Obtenez l'image qcow2 du pare-feu VM-Series.

1. Connectez-vous au Customer Support Portal (Portail assistance clientèle) de Palo Alto Networks.

   Si vous ne l'avez pas déjà fait, créez un compte de support et procédez à l'enregistrement du pare-feu VM-Series.
2. Sélectionnez **Support (Prise en charge)** > **Software Updates (Mises à jour logicielles)** et dans la liste déroulante **Filter By (Filtrer par)**, sélectionnez **Pan OS for VM-Series KVM Base Image (Pan OS pour l'image de base KVM VM-Series)** par exemple, version 9.1.
3. Téléchargez l'image qcow2 dans le dossier de conversion.

STEP 3 | Créez le fichier init-cfg.txt suivant dans le dossier de conversion.

```
type=static ip-address=${IP_ADDRESS} default-gateway=${GATEWAY}
 netmask=${NETMASK} ipv6-address=  ipv6-default-gateway=
 hostname=${HOSTNAME} vm-auth-key=${VM_AUTH_KEY} panorama-server=
${PANORAMA_SERVER} panorama-server-2=  tplname=  dgname=  dns-
primary=${DNS_SERVER} dns-secondary=  op-command-modes=jumbo-
frame, mgmt-interface-swap** dhcp-send-hostname=yes dhcp-send-
client-id=yes dhcp-accept-server-hostname=yes dhcp-accept-server-
domain=yes
```

STEP 4 | Créez un fichier texte nommé `authcodes` (sans extension) et saisissez les codes d'authentification pour la capacité et les abonnements du pare-feu VM-Series. Enregistrez le fichier dans le dossier de conversion.

STEP 5 | Créez le fichier suivant `image_properties_template.xml` dans le dossier de conversion et fournissez des valeurs pour votre déploiement :

```
<image_properties> <vnf_type>FIREWALL</vnf_type>
 <name>pafw</name> <version>9.1.0</version> <bootup_time>-1</
bootup_time> <root_file_disk_bus>virtio</root_file_disk_bus>
 <root_image_disk_format>qcow2</root_image_disk_format>
 <vcpu_min>2</vcpu_min> <vcpu_max>8</vcpu_max>
 <memory_mb_min>4096</memory_mb_min> <memory_mb_max>16384</
memory_mb_max> <vnic_max>8</vnic_max> <root_disk_gb_min>32</
root_disk_gb_min> <root_disk_gb_max>60</root_disk_gb_max>
 <console_type_serial>true</console_type_serial>
```

 ©2023 Palo Alto Networks, Inc.

```
 <sriov_supported>true</sriov_supported> <pcie_supported>false</
pcie_supported> <monitoring_supported>false</monitoring_supported>
 <monitoring_methods>ICMPPing</monitoring_methods>
 <low_latency>true</low_latency> <privileged_vm>true</
privileged_vm> <custom_property> <HOSTNAME> </HOSTNAME> </
custom_property> <custom_property> <IP_ADDRESS> </IP_ADDRESS>
 </custom_property> <custom_property> <NETMASK> </NETMASK>
 </custom_property> <custom_property> <GATEWAY> </GATEWAY>
 </custom_property> <custom_property> <PANORAMA_SERVER> </
PANORAMA_SERVER> </custom_property> <custom_property> <DNS_SERVER>
 </DNS_SERVER> </custom_property> <custom_property> <VM_AUTH_KEY>
 </VM_AUTH_KEY> </custom_property> <default_profile>VM-50</
default_profile> <profiles> <profile> <name>VM-50</name>
 <description>VM-50 profile</description> <vcpus>2</
vcpus> <memory_mb>5120</memory_mb> <root_disk_mb>60000</
root_disk_mb> </profile> <profile> <name>VM-100-n-200</name>
 <description>VM-100 and VM-200 profile</description> <vcpus>2</
vcpus> <memory_mb>7168</memory_mb> <root_disk_mb>60000</
root_disk_mb> </profile> <profile> <name>VM-300</name>
 <description>VM-300 profile</description> <vcpus>2</vcpus>
 <memory_mb>9216</memory_mb> <root_disk_mb>60000</root_disk_mb> </
profile> <profile> <name>VM-1000-HV</name> <description>VM-1000-
HV profile</description> <vcpus>4</vcpus> <memory_mb>9216</
memory_mb> <root_disk_mb>60000</root_disk_mb> </profile>
 <profile> <name>VM-500</name> <description>VM-500 profile</
description> <vcpus>4</vcpus> <memory_mb>16384</memory_mb>
 <root_disk_mb>60000</root_disk_mb> </profile> </profiles>
 <cdrom>true</cdrom> <bootstrap_file_1>/config/init-cfg.txt</
bootstrap_file_1> <bootstrap_file_2>/config/bootstrap.xml</
bootstrap_file_2> <bootstrap_file_3>/license/authcodes</
bootstrap_file_3> </image_properties>
```

STEP 6 | Téléchargez l'utilitaire de paquet d'image.

1. Connectez-vous à l'interface utilisateur Enterprise NFVIS et sélectionnez **VM Life Cycle (Cycle de vie de la machine virtuelle)** > **Image Repository (Référentiel d'image)**.
2. Cliquez sur l'onglet **Browse Datastore (Parcourir le magasin de données)** et accédez à **data (données)** > **intdatastore (magasin de données int.)** > **uploads (chargements)** > **vmpackagingutility (utilitaire de paquet VM)**.
3. Téléchargez `nfvisvmpackagingtool.tar` dans le dossier de conversion.
4. Décompressez le fichier :

```
tar -xvf nfvisvmpackagingtool.tar
```

STEP 7 | Dans le dossier de conversion contenant le qcow2, le fichier `init-config.txt` et le fichier `authcodes`, exécutez le script `nfvpt.py`. Reportez-vous à la documentation sur l'utilitaire de paquet d'image `nfvpt.py`.

L'exemple suivant crée le fichier image Palo-Alto-9.1.0 et un profil VM-100. Les options sont séparées par des espaces (l'exemple montre les options sur des lignes distinctes pour des raisons

 ©2023 Palo Alto Networks, Inc.

de clarté uniquement) et les options personnalisées sont des paires de valeurs de clés avec deux points comme séparateur.

```
./nfvpt.py -o Palo-Alto-9.1.0 -i PA-VM-KVM-9.1.0.qcow2 -n
 PAN902 -t FIREWALL -r 9.1.0 --monitored false --privileged
 true --bootstrap /config/init-cfg.txt:init-cfg.txt,/license/
authcodes:authcodes --min_vcpu 2 --max_vcpu 8 --min_mem 4096
 --max_mem 16384 --min_disk 10 --max_disk 70 --vnic_max 8 --
optimize true --console_type_serial true --profile VM-100,"VM-100
 profile",2,7168,61440 --default_profile VM-100 --custom
 HOSTNAME:hello --custom IP_ADDRESS:10.2.218.24 --custom
 NETMASK:255.255.255.0 --custom GATEWAY:10.2.218.1 --custom
 DNS_SERVER:10.55.66.10 --custom PANORAMA_SERVER:0.10.10.0 --custom
 VM_AUTH_KEY:123451234512345
```

STEP 8 | Téléchargez l'image convertie.

1. Dans l'interface utilisateur NFVIS, sélectionnez **VM Life Cycle (Cycle de vie de la machine virtuelle)** > **Image Repository (Référentiel d'image)** et cliquez sur l'icône bleue Images pour afficher le cercle **Drop Files or Click (Déposer les fichiers ou cliquer)**.
2. Faites glisser le fichier converti dans le cercle ou cliquez pour parcourir et sélectionner votre fichier.
3. Dans la colonne Status (État), cliquez sur **Start** (Démarrer).

   Une fois le téléchargement terminé, l'image est enregistrée et le fichier que vous avez chargé s'affiche dans l'onglet **Image Registration** (Enregistrement d'image) de la liste **Images**.

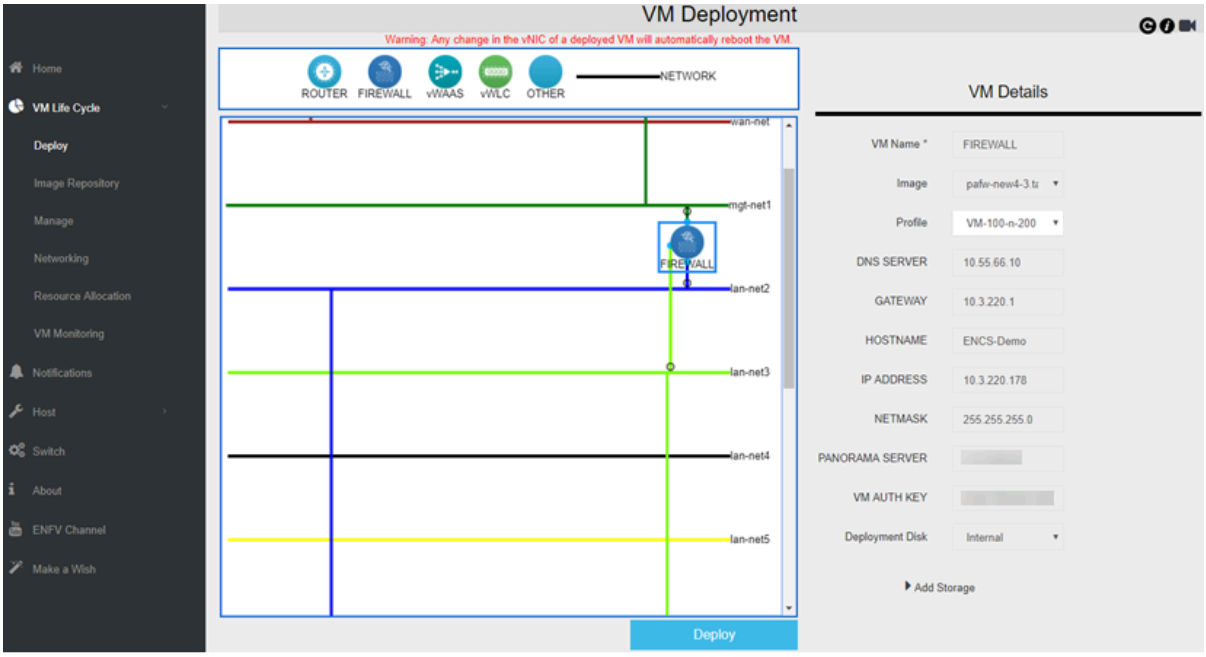
©2023 Palo Alto Networks, Inc.

Déploiement du pare-feu VM-Series sur Cisco ENCS

Avant de commencer à déployer le pare-feu, assurez-vous que vous avez créé des connexions réseau pour un accès de gestion au pare-feu VM-Series. Si vous utilisez Panorama, assurez-vous que Panorama dispose d'une connectivité de gestion avec le pare-feu.

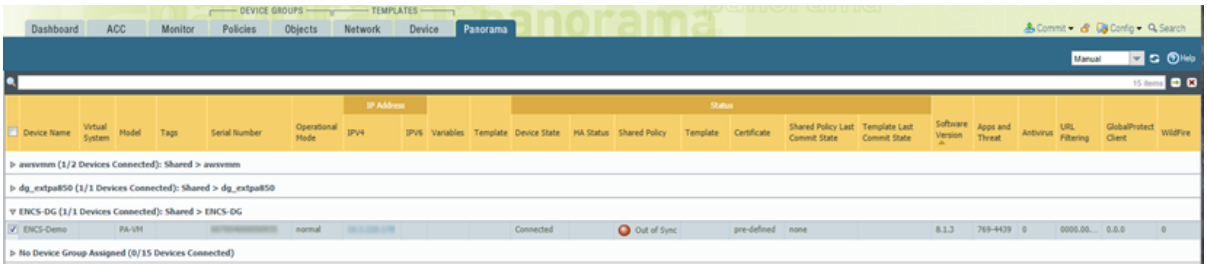
STEP 1 | Déployez le pare-feu VM-Series.

1. Dans Enterprise NFVIS, cliquez sur **VM Life Cycle (Cycle de vie de la machine virtuelle)** > **Deploy (Déployer)**.
2. Faites glisser l'icône du pare-feu vers le réseau approprié. Dans cet exemple, le pare-feu se connecte à un réseau de gestion et à un réseau LAN.



3. **Déployez** le pare-feu VM-Series.

   Si vous utilisez Panorama pour gérer le pare-feu, celui-ci s'affiche comme **Connected (Connecté)** sur **Panorama** > **Managed Devices (Appareils gérés)** > **Summary (Récapitulatif)**. Si le pare-feu n'est pas connecté à Panorama, vérifiez que vous avez fourni l'adresse IP Panorama correcte et que les appareils peuvent communiquer sur le réseau.

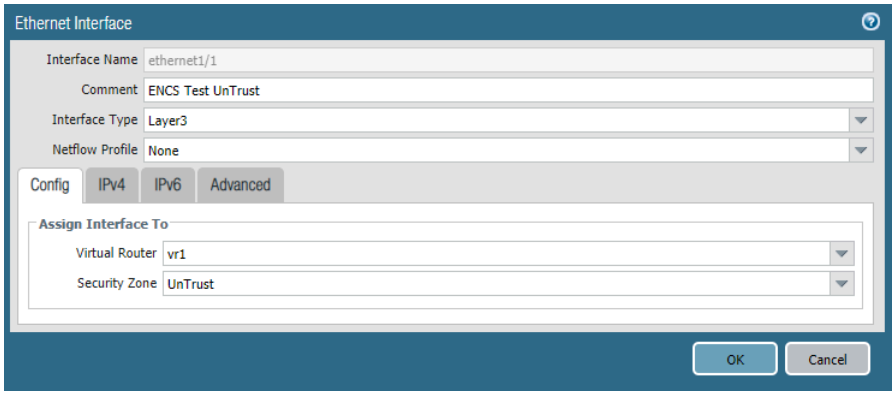


 ©2023 Palo Alto Networks, Inc.

STEP 2 | Configurez les interfaces du dataplane du pare-feu VM-Series.

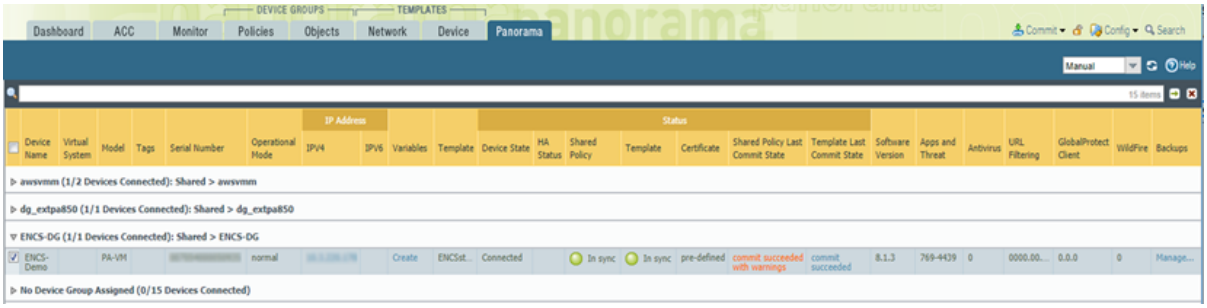
Reportez-vous à la section configuration d'une interface de couche 3, configuration d'une interface de couche 2 ou configuration des câbles virtuels. Si vous utilisez Panorama, les étapes suivantes vous expliquent comment configurer le pare-feu pour un déploiement de couche 3.

1. Procédez à l'Ajout d'un modèle et assignez le pare-feu au modèle.
2. Sélectionnez le **Network** (Réseau) et, dans le menu déroulant Template (Modèle), sélectionnez le modèle que vous avez créé.
3. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
4. Cliquez sur **ethernet 1/1** et configurez comme suit :
   - Définissez **Interface Type** (Type d'interface) sur **Layer3** (Couche 3).
   - Dans l'onglet **Config (Configuration)**, affectez l'interface au routeur par défaut.
   - Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Définissez une nouvelle zone appelée **Non approuvée** par exemple, puis cliquez sur **OK**.
   - Dans l'onglet **IPv4**, sélectionnez **DHCP Client** (Client DHCP) ou **Static** (Statique). Si vous choisissez Static (Statique), saisissez l'adresse IP.



5. Répétez les étapes b à e pour chaque interface réseau.
6. Cliquez sur **Commit (Valider)** > **Commit and Push (Valider et appliquer)** pour valider toutes vos modifications de configuration dans Panorama et les pare-feu gérés.

   Vérifiez que l'état de la liaison pour les interfaces de pare-feu est actif.

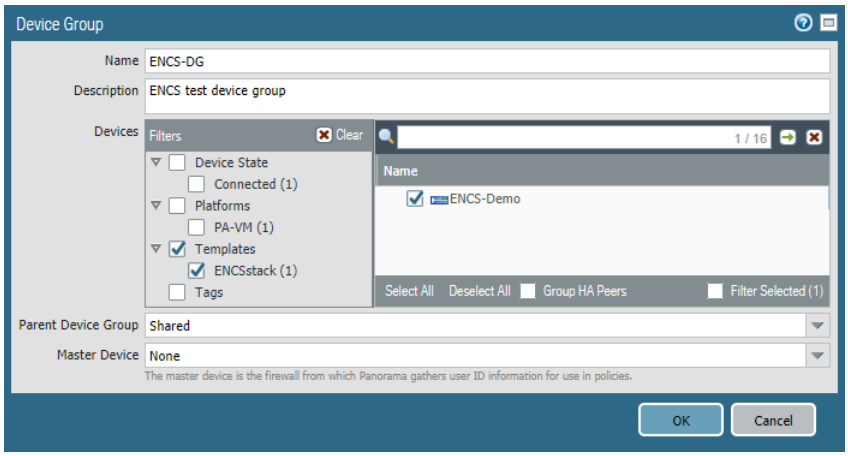


 ©2023 Palo Alto Networks, Inc.

STEP 3 | Configurez les politiques de sécurité pour activer en toute sécurité les applications et les utilisateurs de votre réseau.

Si vous utilisez Panorama, les étapes suivantes vous expliquent comment utiliser des groupes d'appareils pour gérer de manière centralisée les règles de politique de vos pare-feu gérés.

1. Procédez à l'Ajout d'un groupe d'appareils et affectez les pare-feu gérés à votre groupe d'appareils.



2. Configurez les politiques de sécurité pour le groupe d'appareils.

STEP 4 | Vérifiez que le pare-feu VM-Series sécurise le trafic sur votre réseau.

 ©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur Oracle Cloud Infrastructure

Déployez le pare-feu VM-Series sur Oracle Cloud Infrastructure (OCI). Avec le VM-Series sur OCI, vous pouvez protéger et segmenter vos charges de travail, empêcher les menaces avancées et améliorer la visibilité sur vos applications lorsque vous passez au cloud.

OCI est un service informatique en cloud public qui vous permet d'exécuter vos applications dans un environnement hébergé hautement disponible proposé par Oracle. Vous pouvez déployer le pare-feu VM-Series pour sécuriser vos applications et services exécutant votre environnement OCI.

- Types de formes OCI
- Déploiements pris en charge sur OCi
- Préparation à la configuration du pare-feu VM-Series sur OCI
- Déploiement du pare-feu VM-Series à partir du Marketplace Oracle Cloud
- Configuration de la HA active/passive dans OCI

Types de formes OCI

Les pare-feu VM-Series prennent en charge les formes de machine virtuelle OCI suivantes. Reportez-vous à la documentation sur l'Oracle Cloud Infrastructure pour plus d'informations sur les formes de machines virtuelles.

Modèle VM-Series	Forme OCI minimale
• VM-100 • VM-Series basé sur des crédits NFGW logiciels	VM.Standard2.4
• VM-300 • VM-Series basé sur des crédits NFGW logiciels	VM.Standard2.4
• VM-500 • VM-Series basé sur des crédits NFGW logiciels	VM.Standard2.8
• VM-700 • VM-Series basé sur des crédits NFGW logiciels	VM.Standard2.16
• VM-100, VM-300, VM-500 et VM-700 • VM-Series basé sur des crédits NFGW logiciels	VM.Optimized3.Flex

Vous pouvez déployer le pare-feu VM-Series sur une d'instance OCI avec plus de ressources que la Configuration système requise pour VM-Series minimale. Si vous choisissez une taille de forme plus grande pour le modèle de pare-feu VM-Series : bien que le pare-feu utilise uniquement la quantité maximale de cœurs et de mémoire vCPU répertoriés sur la page de configuration système requise, il tire parti des performances réseau plus rapides fournies par la forme la plus grande.

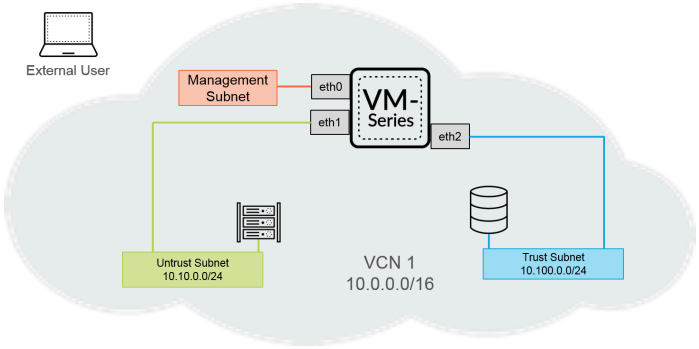
©2023 Palo Alto Networks, Inc.

Déploiements pris en charge sur OCi

Utilisez le pare-feu VM-Series sur OCI pour sécuriser vos environnements cloud dans les scénarios suivants :

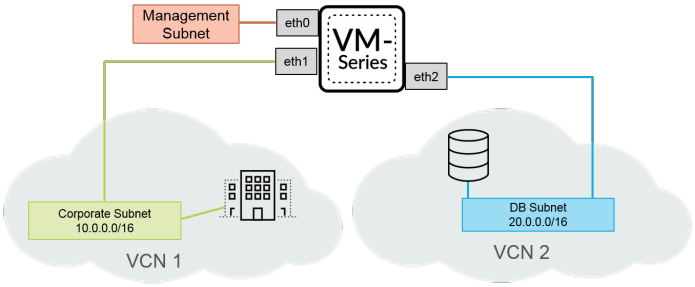
- Trafic nord-sud : vous pouvez utiliser le pare-feu VM-Series pour sécuriser le trafic entrant sur votre réseau cloud à partir d'une source non approuvée ou quittant votre réseau cloud pour atteindre une source non approuvée. Pour les deux types de trafic, vous devez configurer des règles de table de routage dans vos règles de politique Virtual Cloud Network (VCN) et NAT sur le pare-feu.

  Dans cet exemple, le trafic sortant quitte le sous-réseau approuvé de votre VCN. Vous devez configurer la politique de traduction des adresses source sur une adresse IP publique et une règle de table de routage qui redirige ce trafic vers le pare-feu. La règle de routage dirige le trafic sortant vers l'interface du pare-feu dans le sous-réseau approuvé du VCN. Lorsque le pare-feu reçoit ce trafic, il effectue la traduction de l'adresse source sur le trafic et applique toute autre politique de sécurité que vous avez configurée.



- Trafic inter-VCN (est-ouest) : le pare-feu VM-Series vous permet de sécuriser le trafic circulant au sein de votre environnement cloud entre VCNs. Chaque sous-réseau doit appartenir à un VCN différent car, par défaut, aucune règle de routage n'est utilisée pour activer le trafic au sein d'un VCN. Dans ce scénario, vous configurez une interface sur le pare-feu connecté à un sous-réseau dans chaque VCN.

  Dans l'exemple ci-dessous, un utilisateur du Trust Subnet (Sous-réseau approuvé) souhaite accéder aux données du DB Subnet (Sous-réseau de base de données). Configurez un itinéraire sur OCI qui atteint le saut suivant du CIDR du DB Subnet (Sous-réseau de base de données), qui dirige le trafic vers le réseau d'interface Trust Subnet (Sous-réseau approuvé) sur le pare-feu VM-Series.



 ©2023 Palo Alto Networks, Inc.

Pour plus d'informations, consultez Charges de travail sécurisées avec le pare-feu VM-Series de Palo Alto Networks à l'aide d'un réseau flexible.

©2023 Palo Alto Networks, Inc.

Préparation à la configuration du pare-feu VM-Series sur OCI

Le processus de déploiement du pare-feu VM-Series sur Oracle Cloud Infrastructure nécessite l'accomplissement de tâches de préparation.

- Réseaux cloud virtuels
- Clé SSH
- Données utilisateur de la configuration initiale

Réseaux cloud virtuels

Un réseau cloud virtuel (VCN) est un réseau virtuel privé que vous configurez dans votre environnement OCI. Pour déployer le pare-feu VM-Series dans l'environnement OCI, votre VCN doit avoir au moins trois cartes d'interface réseau virtuel (VNIC) pour l'interface de gestion et deux interfaces de données.

OCI utilise une série de tables de routage pour envoyer le trafic à partir de votre VCN et une table de routage est ajoutée à chaque sous-réseau. Un sous-réseau est une division de votre VCN. Si vous ne spécifiez pas de table de routage, le sous-réseau utilise la table de routage par défaut du VCN. Chaque règle de la table de routage spécifie un bloc CIDR de destination et un saut suivant (cible) pour tout trafic qui correspond au CIDR. OCI utilise uniquement la table de routage d'un sous-réseau si l'adresse IP de destination est en dehors du bloc CIDR spécifié du VCN ; les règles de routage ne sont pas nécessaires pour activer le trafic au sein du VCN. Et, si le trafic a des règles qui se chevauchent, OCI utilise la règle la plus spécifique de la table de routage pour acheminer le trafic.

Si aucune règle de routage ne correspond au trafic qui tente de quitter le VCN, le trafic est supprimé.

Chaque sous-réseau nécessite une table de routage et une fois que vous avez ajouté une table de routage à un sous-réseau, vous ne pouvez pas le modifier. Toutefois, vous pouvez ajouter, supprimer ou modifier des règles dans une table de routage après sa création.

Clé SSH

Vous devez créer une paire de clés SSH pour vous connecter au pare-feu pour la première fois. Vous ne pouvez pas utiliser le nom d'utilisateur et le mot de passe par défaut pour accéder au pare-feu pour la première fois. Après le premier démarrage du pare-feu, vous devez accéder au pare-feu par le CLI et créer un nouveau nom d'utilisateur et un nouveau mot de passe.

1. Créez une paire de clés SSH et enregistrez la paire de clés SSH à l'emplacement par défaut pour votre système d'exploitation.
   - Sur Linux ou MacOS, utilisez `ssh-keygen` pour créer la paire de clés dans votre répertoire .ssh.
   - Sur Windows, utilisez PuTTYgen pour créer la paire de clés.

     Le contenu du champ **Key comment (commentaire clé)** n'a pas d'importance pour le pare-feu de la série VM; vous pouvez accepter la date par défaut (la date de création de la clé) ou entrer un commentaire qui vous aide à vous souvenir du nom de la paire de clés. Utilisez le

 ©2023 Palo Alto Networks, Inc.

bouton **Save private key (Sauvegarder la clé privée)** pour stocker la clé privée dans votre répertoire .ssh.

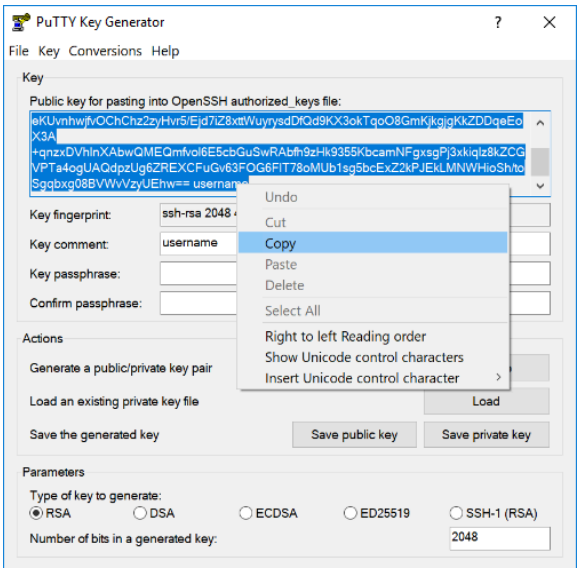
2. Sélectionnez la clé publique complète.

   - Linux ou MacOS :

     ouvrez votre clé publique dans un éditeur de texte et copiez-la.

   - Windows : Vous devez utiliser le générateur de clés pour afficher la clé publique. Lancez PuTTYgen, cliquez sur Load et naviguez jusqu'à la clé privée que vous avez enregistrée dans votre répertoire .ssh.

     Dans PuTTYgen, faites défiler vers le bas pour vous assurer de sélectionner la touche au complet, cliquez avec le bouton droit de la souris et sélectionnez Copy (Copier).



Données utilisateur de la configuration initiale

Vous devez fournir les paramètres d'amorçage suivants lors de la configuration de l'instance du pare-feu VM-Series. OCI utilise ces informations pour effectuer la configuration initiale du pare-feu, qui fournit au pare-feu un nom d'hôte et une licence et connecte le pare-feu à Panorama, le cas échéant.

Les champs relatifs à Panorama ne sont requis que si vous disposez d'un appareil Panorama et que vous souhaitez utiliser Panorama pour gérer votre pare-feu VM-Series.

Champ	Description
hostname=	Nom d'hôte pour le pare-feu.
vm-auth-key=	Clé d'authentification de la machine virtuelle pour l'enregistrement du pare-feu auprès de Panorama.
panorama-server=	Adresse IPv4 ou IPv6 du serveur Panorama principal. Ce champ n'est pas obligatoire, mais il

©2023 Palo Alto Networks, Inc.

Champ	Description
	est recommandé pour la gestion centralisée de vos pare-feu.
panorama-server-2=	Adresse IPv4 ou IPv6 du serveur Panorama secondaire. Ce champ n'est pas obligatoire, mais il est recommandé.
tplname=	Nom de la pile de modèle Panorama. Si vous ajoutez une adresse IP de serveur Panorama, appliquez le pare-feu à une pile de modèles sur Panorama et entrez le nom de la pile de modèles dans ce champ afin de pouvoir gérer de manière centralisée et envoyer les paramètres de configuration au pare-feu.
dgname=	Nom du groupe de périphériques Panorama. Si vous ajoutez une adresse IP de serveur Panorama, créez un groupe de périphériques sur Panorama et entrez le nom du groupe de périphériques dans ce champ afin de pouvoir regrouper logiquement les pare-feu et d'envoyer les règles de politique au pare-feu.
authcodes=	Utilisé pour enregistrer le pare-feu VM-Series auprès du serveur de licences de Palo Alto Networks.
op-command-modes=jumbo-frame	Utilisé pour activer le mode de trames jumbo sur le pare-feu VM-Series. Étant donné qu'OCI déploie les instances VM en mode jumbo par défaut, il est recommandé de lancer le pare-feu VM-Series en mode jumbo pour obtenir le meilleur débit.

Collez les paramètres d'amorçage dans la console OCI dans le format suivant.

hostname=<*fw-hostname*>

vm-auth-key=<*auth-key*>

panorama-server=<*panorama-ip*>

panorama-server-2=<*panorama2-ip*>

tplname=<*template-stack-name*>

dgname=<*device-group-name*>

authocodes=<*firewall-authcode*>

op-command-modes=jumbo-frame

©2023 Palo Alto Networks, Inc.

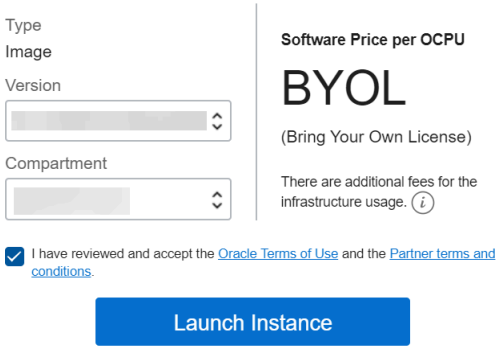
Déploiement du pare-feu VM-Series à partir du Marketplace Oracle Cloud

Effectuez la procédure suivante pour déployer le pare-feu VM-Series dans OCI à partir du Marketplace Oracle Cloud.

STEP 1 | Connectez-vous au Marketplace Oracle Cloud.

STEP 2 | Trouvez l'application du pare-feu VM-Series dans le Marketplace Oracle Cloud.

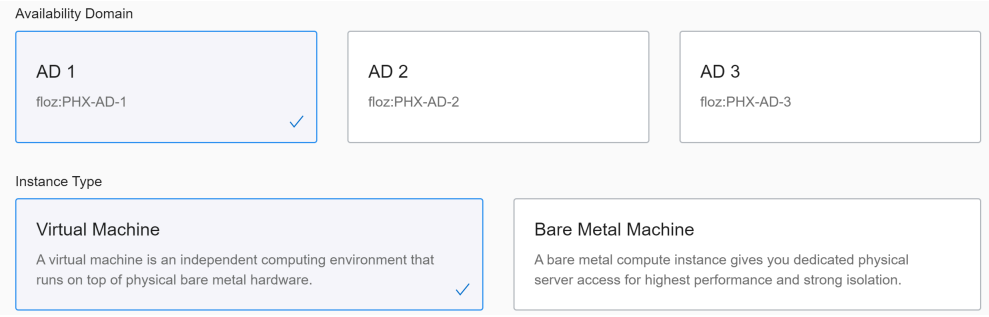
1. Recherchez Palo Alto Networks et une liste de pare-feu VM-Series s'affichera.
2. Sélectionnez une offre.
3. Cliquez sur **Get App (Obtenir l'application)**.
4. Sélectionnez votre **région** et cliquez sur **Sign In (Connexion)**.
5. Sélectionnez la **version** et le **compartiment**.
6. Acceptez les termes d'Oracle et du partenaire.
7. Cliquez sur **Launch Instance (Lancer l'instance)**.



STEP 3 | Saisissez un **Name** (Nom) descriptif pour votre instance de pare-feu VM-Series.

STEP 4 | Sélectionnez un **Availability Domain** (Domaine de disponibilité).

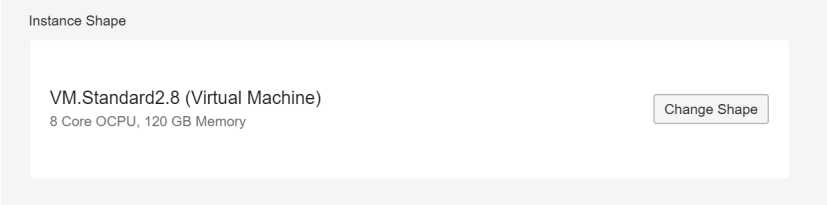
STEP 5 | Sélectionnez **Virtual Machine** (Machine virtuelle) dans **Shape Type** (Type de forme).



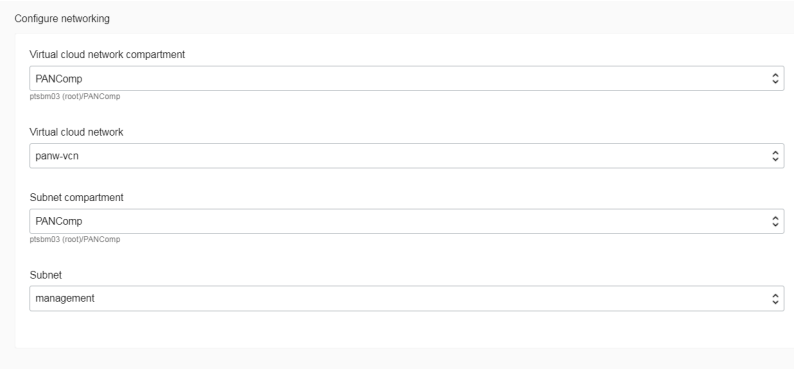
STEP 6 | Sélectionnez la forme avec le nombre de processeurs, la quantité de mémoire vive (RAM) et le nombre d'interfaces requises pour le modèle de pare-feu VM-Series. Reportez-vous à la page Calculer les formes pour obtenir la quantité de ressources fournies par les différentes formes

©2023 Palo Alto Networks, Inc.

de calcul. Reportez-vous à la section Configuration système requise pour VM-Series pour plus d'informations sur les ressources requises pour chaque modèle de pare-feu VM-Series.



STEP 7 | Dans Networking (Mise en réseau), sélectionnez votre **Virtual cloud network compartment** (Compartiment de réseau cloud virtuel), **Virtual cloud network** (Réseau cloud virtuel), **Subnet compartment** (Compartiment de sous-réseau) et **Subnet** (Sous-réseau) pour votre interface de gestion. Vous ne pouvez ajouter qu'une seule interface lorsque vous créez l'instance de pare-feu VM-Series. Vous ajouterez des interfaces supplémentaires par la suite.

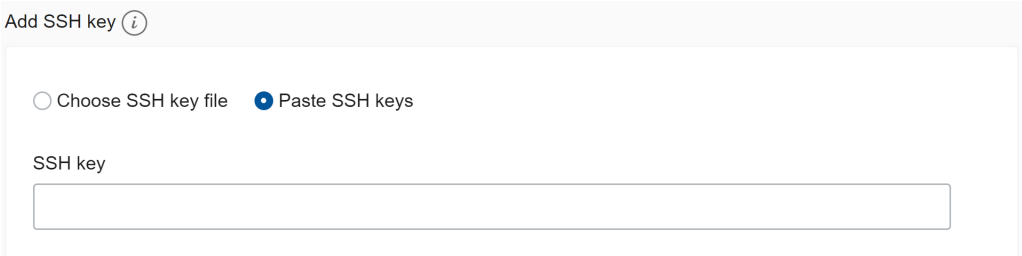


STEP 8 | (Facultatif) Définissez le volume de démarrage à une taille supérieure à la valeur par défaut. Par défaut, le volume de démarrage est défini sur 60 Go. Effectuez cette procédure si vous avez besoin d'un volume de démarrage plus important pour prendre en charge des fonctionnalités telles que l'association de journaux.

1. Sélectionnez **Custom boot volume size (in GB) (Taille de volume de démarrage personnalisée [en Go])**.
2. Saisissez une valeur supérieure ou égale à 60. 60 Go correspond à la taille de disque dur minimum requise par le pare-feu VM-Series.

STEP 9 | Ajoutez votre clé SSH.

1. Dans **Add SSH Key (Ajouter la clé SSH)**, sélectionnez **Paste SSH Key (Coller la clé SSH)**.
2. Collez votre clé SSH dans le champ fourni.



 ©2023 Palo Alto Networks, Inc.

STEP 10 | Ajoutez les paramètres d'amorçage.

1. Cliquez sur **Show Advanced Options (Afficher les options avancées)**.
2. Dans **User data (Données utilisateur)**, sélectionnez **Paste cloud-init script (Coller le script cloud-init)**.
3. Collez les paramètres d'amorçage dans le champ fourni.

   hostname=<*fw-hostname*>

   vm-auth-key=<*auth-key*>

   panorama-server=<*panorama-ip*>

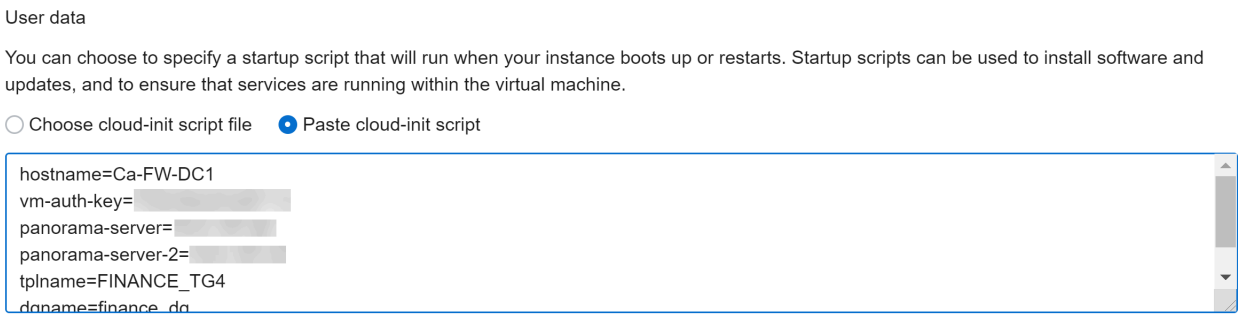
   panorama-server-2=<*panorama2-ip*>

   tplname=<*template-stack-name*>

   dgname=<*device-group-name*>

   authcodes=<*firewall-authcode*>

   op-command-modes=jumbo-frame



STEP 11 | Cliquez sur **Create (Créer)**.

Lorsque le pare-feu VM-Series est lancé, OCI crée et associe une VNIC principale à l'instance. Cette VNIC réside dans le sous-réseau que vous avez spécifié dans le paramètre de réseau de l'instance et se connecte à l'interface de gestion du pare-feu VM-Series.

STEP 12 | Configurez un nouveau mot de passe administratif pour le pare-feu.

1. Utilisez l'adresse IP de gestion vers SSH dans l'interface de ligne de commande (CLI) du pare-feu VM-Series.
2. Saisissez la commande suivante pour vous connecter au pare-feu :

   ssh-i <*private_key.pem*> admin@<*public-ip_address*>
3. Configurez un nouveau mot de passe à l'aide de la commande suivante, et suivez les invites affichées à l'écran :

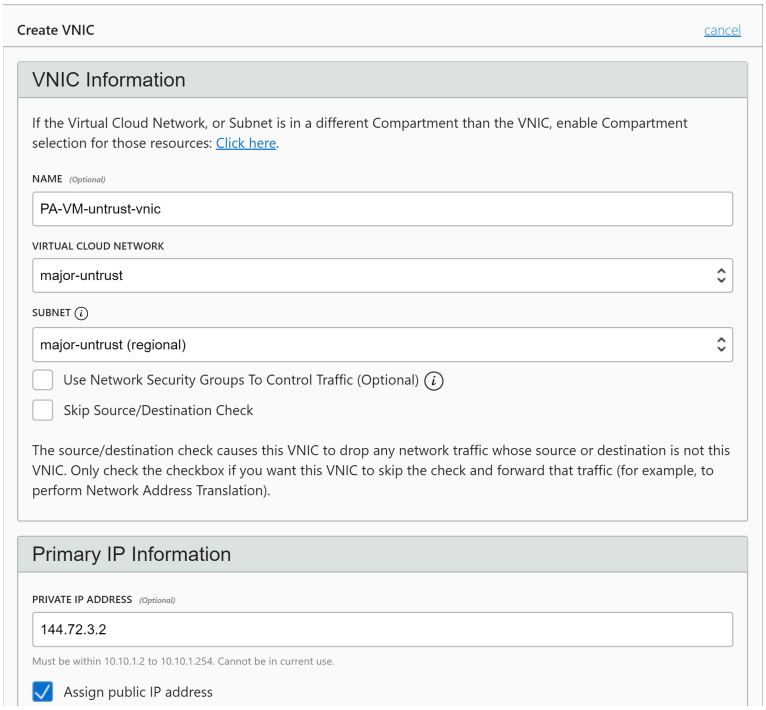
   configure

   set mgt-config users admin password

 ©2023 Palo Alto Networks, Inc.

STEP 13 | Associez une vNIC à votre instance de pare-feu VM-Series pour chaque interface de données. Vous devez associer au moins deux interfaces de données à votre instance de pare-feu : approuvée et non approuvée.

1. Sélectionnez votre instance de pare-feu VM-Series récemment lancée et sélectionnez **Attached VNICs (VNIC associées)** > **Create VNIC (Créer une VNIC)**.
2. Saisissez un **Name** (Nom) descriptif pour votre vNIC.
3. Sélectionnez votre VCN dans la liste déroulante **Virtual Cloud Network** (Réseau cloud virtuel).
4. Sélectionnez votre sous-réseau dans la liste déroulante **Subnet** (Sous-réseau).
5. Spécifiez une **Private IP Address** (Adresse IP privée). Cela n'est requis que si vous souhaitez choisir une adresse IP particulière pour la vNIC. Si vous ne spécifiez aucune adresse IP, OCI attribuera une adresse IP à partir du bloc CIDR que vous avez attribué au sous-réseau.
6. Sélectionnez **Assign Public IP Address** (Attribuer une adresse IP publique) pour les vNIC publiques, telles que votre sous-réseau non approuvé.
7. Cliquez sur **Create VNIC (Créer une VNIC)**.
8. Répétez cette procédure pour chaque vNIC requise par votre déploiement.



 ©2023 Palo Alto Networks, Inc.

STEP 14 | Configurez les interfaces réseau du plan de données en tant qu'interfaces de couche 3 sur le pare-feu.

1. Connectez-vous au pare-feu.
2. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
3. Cliquez sur la liaison **ethernet 1/1** et configurez comme suit :
   - **Interface Type (Type d'interface)** : **Layer3 (Couche 3)**
   - Dans l'onglet **Config (Configuration)**, affectez l'interface au routeur par défaut.
   - Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Définissez une nouvelle zone, zone non approuvée par exemple, puis cliquez sur **OK**.
   - Dans l'onglet **IPv4**, sélectionnez **Static** (Statique).
   - Cliquez sur **Add** (Ajouter) dans la section IP puis saisissez l'adresse IP et le masque réseau pour l'interface. Assurez-vous que l'adresse IP correspond à l'adresse IP que vous avez affectée au sous-réseau correspondant dans VCN. Par exemple, si vous ajoutez cette interface à votre zone non approuvée, veillez à attribuer l'adresse IP vNIC non approuvée configurée dans votre VCN.
4. Répétez cette procédure pour chaque vNIC configurée dans votre VCN, à l'exception de votre vNIC de gestion.



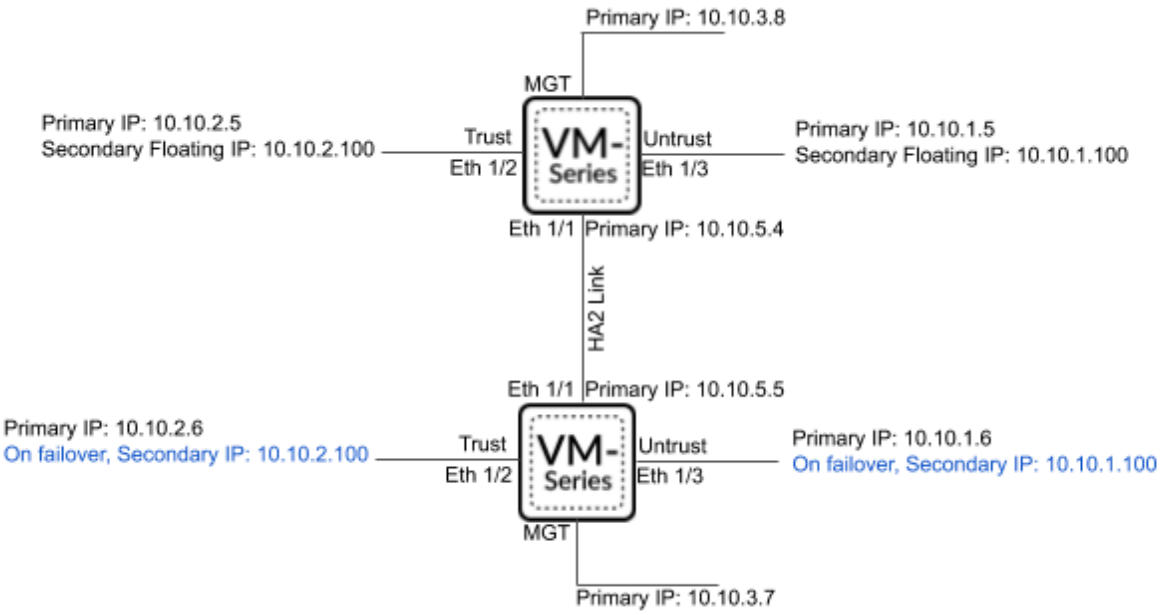
Supprimez toujours uniquement les interfaces situées en bas de la liste d'interfaces. La suppression des interfaces de pare-feu dans le mauvais ordre entraîne une non-correspondance d'interface entre le pare-feu et OCI. Par exemple, supposons que vous ayez cinq interfaces de données, que vous supprimiez ensuite l'interface deux du pare-feu et que vous ajoutiez une nouvelle interface en bas. Après le redémarrage du pare-feu, l'interface récemment ajoutée remplacera l'interface deux supprimée au lieu de se placer en bas de la liste.

©2023 Palo Alto Networks, Inc.

Configuration de la HA active/passive dans OCI

Vous pouvez configurer une paire de pare-feu VM-Series dans OCI dans une configuration haute disponibilité (HA) active/passive. Pour garantir la disponibilité dans une configuration HA dans OCI, vous devez créer une adresses IP flottante secondaire pouvant être rapidement transférée d'un homologue à un autre. Lorsque le pare-feu actif tombe en panne, l'adresse IP flottante passe du pare-feu actif au pare-feu passif pour permettre au pare-feu passif de sécuriser de manière transparente le trafic dès qu'il devient l'homologue actif. En plus de l'adresse IP flottante, les homologues HA ont également besoin de liaisons HA, à savoir une liaison de contrôle (HA1) et une liaison de données (HA2), pour synchroniser les données et gérer les informations sur l'état.

Le pare-feu VM-Series pour OCI en mode FIPS ne prend pas en charge la haute disponibilité.



Pour permettre aux pare-feu de déplacer l'adresse IP flottante lors du basculement, vous devez placer les instances de pare-feu dans un groupe dynamique dans OCI. Les groupes dynamiques vous permettent de regrouper les instances de pare-feu en tant qu'acteurs principaux et de créer une politique pour autoriser les instances dans le groupe dynamique à effectuer des appels d'API par rapport aux services OCI. Vous utiliserez des règles de correspondance pour ajouter des instances d'homologues HA au groupe dynamique, puis vous créerez la politique de l'IP flottante d'une VNIC à l'autre.

Les deux pare-feu VM-Series dans la paire HA doivent comporter le même nombre d'interfaces réseau. Chaque pare-feu requiert au minimum quatre interfaces : gestion (Management), non approuvée (Untrust), approuvée (Trust) et HA. Vous pouvez configurer des interfaces de données supplémentaires selon les besoins de votre déploiement.

- **Interface de gestion** : les adresses IP privées et publiques associées à l'interface principale. Vous pouvez utiliser l'adresse IP privée sur l'interface de gestion comme adresse IP pour l'interface HA1

©2023 Palo Alto Networks, Inc.

entre les homologues. Si vous souhaitez une interface HA dédiée, vous devez associer une interface supplémentaire à chaque pare-feu, pour un total de cinq interfaces chacun.

- Interfaces **non approuvées (Untrust)** et **approuvées (Trust)** : chacune de ces interfaces de données sur l'homologue HA actif nécessite une adresse IP principale et secondaire. Lors du basculement, lorsque l'homologue HA passif passe à l'état actif, l'adresse IP privée secondaire est dissociée de l'homologue précédemment actif et associée à l'homologue HA désormais actif.
- **Interface HA2** : cette interface comporte une adresse IP privée unique sur chaque homologue HA. L'interface HA2 est la liaison de données utilisée par les homologues pour la synchronisation de sessions, les tables de transfert, les associations de sécurité IPsec et les tables ARP.

©2023 Palo Alto Networks, Inc.

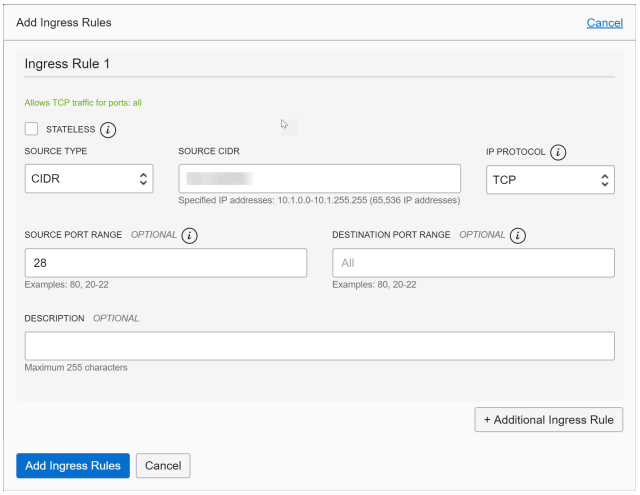
STEP 1 | Déploiement du pare-feu VM-Series à partir du Marketplace Oracle Cloud et configurez les interfaces réseau pour la HA.

1. (Facultatif) Configurez une interface HA1 dédiée sur chaque homologue HA.
   1. À partir de la console OCI, sélectionnez **Compute (Calcul)** > **Instances** et cliquez sur le nom de votre instance d'homologue active.
   2. Sélectionnez **Attached VNICs (VNIC attachées)** et cliquez sur **Create VNIC (Créer une VNIC)**.
   3. Saisissez un nom descriptif pour votre interface HA1.
   4. Sélectionnez le VCN et le sous-réseau.
   5. Spécifiez une adresse IP privée.
   6. Cliquez sur **Create VNIC (Créer une VNIC)**.
   7. Répétez ce processus sur l'instance de votre homologue passif.
2. Configurez une interface HA2 sur chaque homologue HA.
   1. À partir de la console OCI, sélectionnez **Compute (Calcul)** > **Instances** et cliquez sur le nom de votre instance d'homologue active.
   2. Sélectionnez **Attached VNICs (VNIC attachées)** et cliquez sur **Create VNIC (Créer une VNIC)**.
   3. Saisissez un nom descriptif pour votre interface HA2.
   4. Sélectionnez le VCN et le sous-réseau. L'interface HA2 doit se trouver sur un sous-réseau distinct de vos interfaces de données.
   5. Spécifiez une adresse IP privée.
   6. Cliquez sur **Create VNIC (Créer une VNIC)**.
   7. Répétez ce processus sur l'instance de votre homologue passif.
3. Ajoutez une adresse IP secondaire à vos interfaces de plan de données sur l'homologue actif.
   1. À partir de la console OCI, sélectionnez **Compute (Calcul)** > **Instances** et cliquez sur le nom de votre instance d'homologue active.
   2. Sélectionnez **Attached VNICs (VNIC attachées)** et cliquez sur votre VNIC non approuvée (Untrust).
   3. Sélectionnez **IP Addresses (Adresses IP)** et cliquez sur **Assign Private IP Address (Attribuer une adresse IP privée)**.
   4. Entrez l'adresse IP et cliquez sur **Assign (Attribuer)**.
   5. Répétez cette procédure pour chaque interface de plan de données sur votre homologue actif.

©2023 Palo Alto Networks, Inc.

STEP 2 | Créez des règles de sécurité pour autoriser les homologues HA à synchroniser les données et à maintenir les informations sur l'état. Par défaut, OCI autorise uniquement le trafic ICMP. Vous devez ouvrir les ports HA nécessaires.

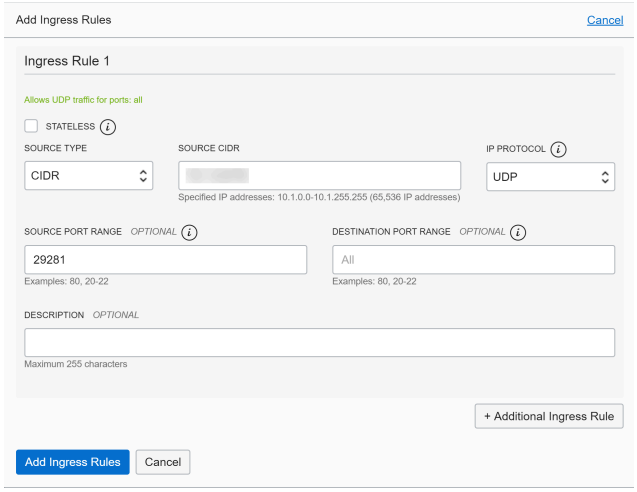
1. Ouvrez les ports pour votre interface HA1.
   1. Dans la console OCI, sélectionnez **Networking (Mise en réseau)** > **Virtual Cloud Networks** et sélectionnez votre VCN.
   2. Sélectionnez **Subnets (Sous-réseaux)** et sélectionnez le sous-réseau contenant votre interface HA1.
   3. Sélectionnez **Security Lists (Listes de sécurité)** et cliquez sur la liste de sécurité par défaut pour la modifier.
   4. Cliquez sur **Add Ingress Rule (Ajouter une règle Ingress)**.
   5. Saisissez le **CIDR source** qui inclut l'adresse IP du port HA1 de l'homologue HA.
   6. Sélectionnez **TCP** dans la liste déroulante **IP Protocol (Protocole IP)**.
   7. Cliquez sur **+Additional Ingress Rule (+ Règle Ingress supplémentaire)**. Vous devez créer deux règles supplémentaires pour les ports TCP 28260 et 28769.
   8. Si le chiffrement est activé sur votre pare-feu VM-Series pour la liaison HA1, créez une règle supplémentaire pour le port 28 ICMP et TCP.
   9. Cliquez sur **Add Ingress Rules (Ajouter des règles Ingress)**.



2. Ouvrez les ports pour votre interface HA2.
   1. Dans la console OCI, sélectionnez **Networking (Mise en réseau)** > **Virtual Cloud Networks** et sélectionnez votre VCN.
   2. Sélectionnez **Subnets (Sous-réseaux)** et sélectionnez le sous-réseau contenant votre interface HA2.
   3. Sélectionnez **Security Lists (Listes de sécurité)** et cliquez sur la liste de sécurité par défaut pour la modifier.
   4. Cliquez sur **Add Ingress Rule (Ajouter une règle Ingress)**.
   5. Saisissez le **CIDR source** qui inclut l'adresse IP du port HA2 de l'homologue HA.
   6. Sélectionnez **UDP** ou **IP** dans la liste déroulante **IP Protocol (Protocole IP)**.

©2023 Palo Alto Networks, Inc.

7. Si le mode de transport est UDP, saisissez **29281** dans **Source Port Name (Nom du port source)**. Si le mode de transport est IP, saisissez **99** dans **Source Port Name (Nom du port source)**.
8. Cliquez sur **Add Ingress Rules (Ajouter des règles Ingress)**.

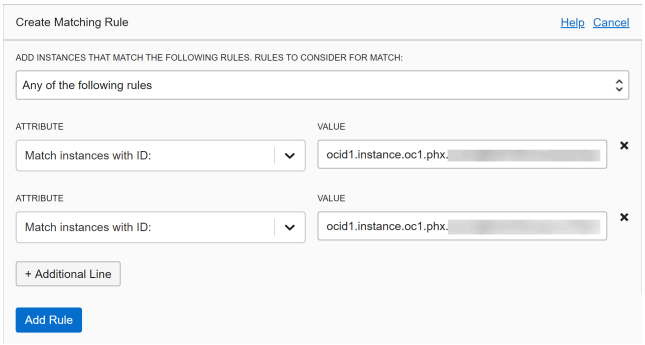


STEP 3 | Ajoutez les deux homologues HA à un groupe dynamique et créez une politique autorisant les homologues HA à déplacer les adresses IP flottantes. Vous devez disposer de l'OCID de chaque instance d'homologue HA pour créer les règles de correspondance du groupe dynamique,

 ©2023 Palo Alto Networks, Inc.

assurez-vous par conséquent de les avoir à portée de main pour les coller dans le générateur de règles.

1. Créez le groupe dynamique.
   1. Dans la console OCI Console, sélectionnez **Identity (Identité)** > **Dynamic Groups (Groupes dynamiques)** > **Create Dynamic Group (Créer un groupe dynamique)**.
   2. Saisissez un **nom** descriptif pour votre groupe dynamique.
   3. Cliquez sur **Rule Builder (Générateur de règles)**.
   4. Sélectionnez **l'une des règles suivantes** dans la liste déroulante.
   5. Sélectionnez **Match instances with ID: (Faire correspondre les instances à l'ID :)** dans la liste déroulante **Attributes (Attributs)** et collez l'un des OCID de l'homologue dans le champ **Value (Valeur)**.
   6. Cliquez sur **+Additional Line (+ Ligne supplémentaire)**.
   7. Sélectionnez **Match instances with ID: (Faire correspondre les instances à l'ID :)** dans la liste déroulante **Attributes (Attributs)** et collez l'autre OCID de l'homologue dans le champ **Value (Valeur)**.
   8. Cliquez sur **Add rule** (Ajouter une règle).

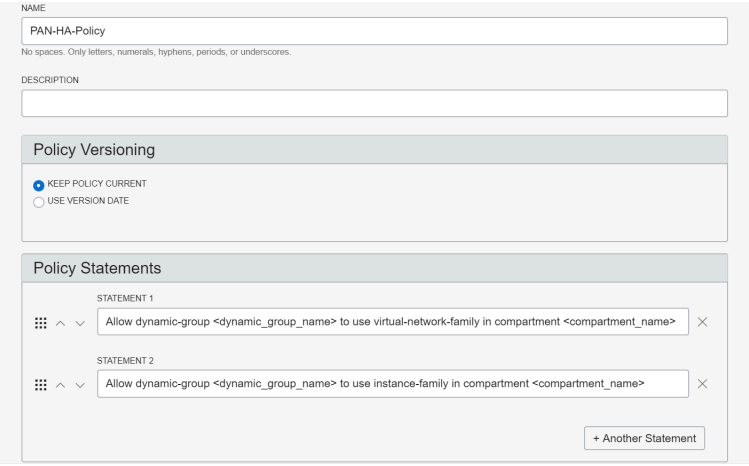


   9. Cliquez sur **Create Dynamic Group (Créer un groupe dynamique)**.
2. Créez la règle de politique.
   1. Dans la console OCI, sélectionnez **Identity (Identité)** > **Policies (Politiques)** > **Create Policy (Créer une politique)**.
   2. Saisissez un **nom** descriptif pour votre politique.
   3. Saisissez le premier énoncé de la politique.

      `Allow dynamic-group <dynamic_group_name> to use virtual-network-family in compartment <compartment_name>`
   4. Cliquez sur **+Another Statement (+ Autre énoncé)**.
   5. Saisissez le deuxième énoncé de la politique.

      `Allow dynamic-group <dynamic_group_name> to use instance-family in compartment <compartment_name>`
   6. Cliquez sur **Create (Créer)**.

©2023 Palo Alto Networks, Inc.



STEP 4 | Configurez les interfaces sur le pare-feu. Vous devez configurer la liaison de données HA2 et au moins deux interfaces Couche 3 pour vos interfaces non approuvée (Untrust) et approuvée (Trust). Terminez ce flux de travail sur le premier homologue HA puis répétez ces étapes sur le second homologue HA.

1. Connectez-vous à l'interface Web du pare-feu.

 ©2023 Palo Alto Networks, Inc.

2. (Facultatif) Si vous utilisez l'interface de gestion comme HA1, devez définir le type d'interface IP sur statique et configurer un serveur DNS.
   1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Interfaces** > **Management (Gestion)**.
   2. Définissez le **type d'IP** sur **Static (Statique)**.
   3. Saisissez l'**adresse IP** privée de la VNIC principale de votre instance de pare-feu VM-Series.
   4. Cliquez sur **OK**.
   5. Sélectionnez **Device (périphérique)** > **Setup (Configuration)** > **Services**.
   6. Cliquez sur **Edit (Modifier)**.
   7. Saisissez l'adresse IP du **serveur DNS principal**.
   8. Cliquez sur **OK**.
   9. **Commit (Validez)** vos modifications.
3. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**, puis cliquez sur votre interface non approuvée. Dans cet exemple, l'interface HA2 est 1/1, l'interface approuvée (Trust) est ethernet 1/2 et l'interface non approuvée (Untrust) est ethernet 1/3.
4. Cliquez sur la liaison **ethernet 1/1** et configurez comme suit :
   - **Interface Type (Type d'interface)** : **HA**
5. Cliquez sur le lien pour **ethernet 1/2** et configurez-le comme suit :
   - **Interface Type (Type d'interface)** : **Layer3 (Couche 3)**
   - Dans l'onglet **Config (Configuration)**, affectez l'interface au routeur par défaut.
   - Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Définissez une nouvelle zone, trust-zone par exemple, puis cliquez sur **OK**.
   - Dans l'onglet **IPv4**, sélectionnez **Static** (Statique).
   - Cliquez sur **Add (Ajouter)** dans la section IP puis saisissez l'adresse IP principale et le masque réseau pour l'interface. Assurez-vous que l'adresse IP correspond à l'adresse IP que vous avez affectée au sous-réseau correspondant dans VCN. Par exemple, si vous

 ©2023 Palo Alto Networks, Inc.

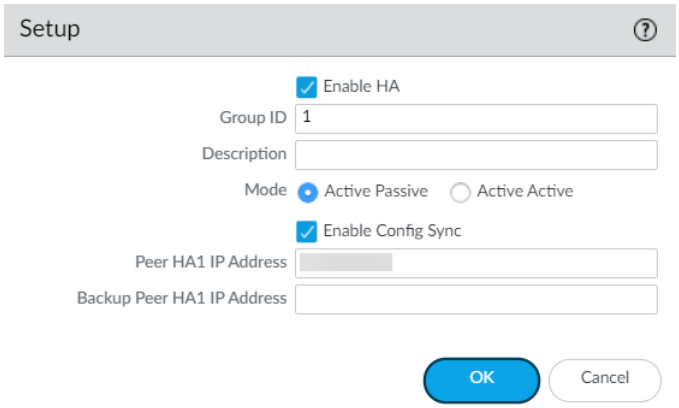
ajoutez cette interface à votre zone trust, veillez à attribuer l'adresse IP vNIC approuvée (Trust) configurée dans votre VCN.

- Cliquez sur **Add (Ajouter)** dans la section IP puis saisissez l'adresse IP flottante secondaire et le masque réseau.

6. Cliquez sur la liaison pour **ethernet 1/3** et configurez-le comme suit :
   - **Interface Type (Type d'interface)** : **Layer3 (Couche 3)**
   - Dans l'onglet **Config (Configuration)**, affectez l'interface au routeur par défaut.
   - Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Définissez une nouvelle zone, zone non approuvée par exemple, puis cliquez sur **OK**.
   - Dans l'onglet **IPv4**, sélectionnez **Static** (Statique).
   - Cliquez sur **Add (Ajouter)** dans la section IP puis saisissez l'adresse IP principale et le masque réseau pour l'interface. Assurez-vous que l'adresse IP correspond à l'adresse IP que vous avez affectée au sous-réseau correspondant dans VCN. Par exemple, si vous ajoutez cette interface à votre zone non approuvée, veillez à attribuer l'adresse IP vNIC non approuvée configurée dans votre VCN.
   - Cliquez sur **Add (Ajouter)** dans la section IP puis saisissez l'adresse IP flottante secondaire et le masque réseau.

STEP 5 | Activez HA.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**.
2. Modifiez les paramètres de configuration.
3. Saisissez l'adresse IP privée de l'homologue passif dans le champ **Peer HA1 IP address (Adresse IP de l'homologue HA1)**.
4. Cliquez sur **OK**.

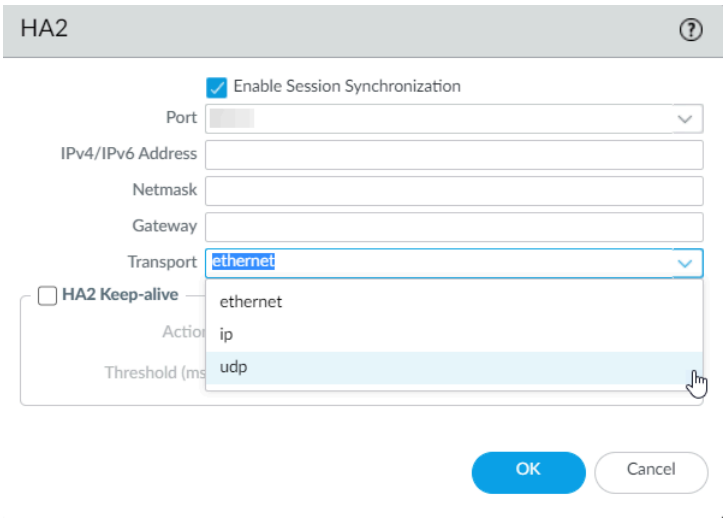


5. (Facultatif) Modifiez la liaison de contrôle (HA1). Si vous ne prévoyez pas d'utiliser l'interface de gestion pour la liaison de contrôle et que vous avez ajouté une interface

©2023 Palo Alto Networks, Inc.

supplémentaire (par exemple, ethernet 1/4), modifiez cette section pour sélectionner l'interface à utiliser pour la communication HA1.

6. Modifiez la Data Link (Liaison de données) (HA2) pour utiliser le **Port** ethernet 1/1 et ajoutez l'adresse IP de l'homologue actif et l'adresse IP de la **Gateway** (Passerelle) du sous-réseau.
7. Sélectionnez **IP** ou **UDP** dans la liste déroulante Transport. L'Ethernet n'est pas pris en charge.



8. Cliquez sur **OK**.

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

STEP 7 | Répétez l'étape 4 et l'étape 5 sur l'homologue HA passif.

STEP 8 | Une fois la HA configurée sur les deux pare-feu, vérifiez que les pare-feu sont appariés en mode HA active/passive.

1. Accédez au **Dashboard (Tableau de bord)** sur les deux pare-feu et affichez le widget High Availability (Haute disponibilité).
2. Sur l'homologue HA actif, cliquez sur **Sync to peer (Synchroniser à l'homologue)**.
3. Vérifiez que les pare-feu sont appariés et synchronisés.
   - Sur le pare-feu passif : l'état du pare-feu local doit afficher **Passive (Passif)** et la **Running Config (Configuration en cours)** doit être Synchronized (Synchronisée).
   - Sur le pare-feu actif : l'état du pare-feu local doit afficher **Active (Actif)** et la **Running Config (Configuration en cours)** doit être Synchronized (Synchronisée).

©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur Alibaba Cloud

Le déploiement du pare-feu VM-Series sur Alibaba Cloud protège les réseaux que vous créez dans Alibaba Cloud. Vous pouvez déployer des pare-feu VM-Series pour protéger les applications Internet et les déploiements de clouds hybrides.

- Pare-feu VM-Series sur Alibaba Cloud
- Configuration système minimale requise pour le pare-feu VM-Series sur Alibaba Cloud
- Préparation au déploiement du pare-feu VM-Series sur Alibaba Cloud
- Déploiement du pare-feu VM-Series sur Alibaba Cloud

Pare-feu VM-Series sur Alibaba Cloud

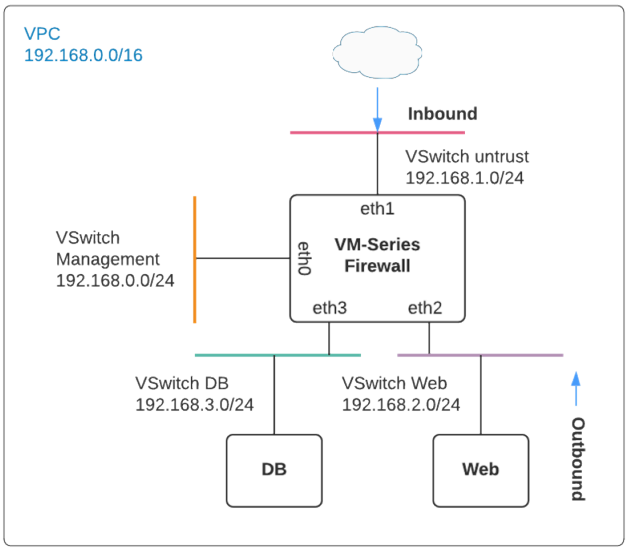
Vous pouvez déployer le pare-feu VM-Series pour sécuriser le trafic nord-sud entrant et sortant dans Alibaba Cloud.

La sécurisation du trafic est-ouest au sein du même VPC n'est pas prise en charge, car Alibaba Cloud ne prend pas en charge le routage de sous-réseau.

Le pare-feu VM-Series sur Alibaba Cloud s'exécute sur l'hyperviseur KVM et prend en charge jusqu'à 8 interfaces réseau lorsque vous sélectionnez une instance Alibaba Cloud avec des ressources suffisantes (voir Configuration système minimale requise pour le pare-feu VM-Series sur Alibaba Cloud).

Le pare-feu VM-Series sur Alibaba Cloud prend en charge les licences BYOL et l'ELA VM-Series dans les régions internationales et Chine continentale d'Alibaba Cloud. Les licences PAYG ne sont pas actuellement prises en charge.

Dans Alibaba Cloud, votre VPC isole logiquement votre réseau virtuel. Après avoir créé un VPC, vous pouvez créer des VSwitches pour segmenter davantage votre réseau privé virtuel, comme le montre le schéma suivant. DNAT et SNAT doivent être configurés sur le pare-feu pour sécuriser le trafic entrant.



Le trafic entrant provient d'un client extérieur à votre VPC et se dirige vers l'interface non approuvée du pare-feu VM-Series. Le pare-feu inspecte le trafic et l'envoie à une application via l'interface approuvée. Le trafic revenant de l'application doit passer par l'interface approuvée du pare-feu VM-Series, qui inspecte le flux de trafic de retour et l'envoie via l'interface non approuvée.

Le trafic sortant provient généralement d'une application externe. En règle générale, vous acheminez le trafic Internet dans un VPC vers une passerelle NAT (avec une EIP attachée). Pour ce faire, ajoutez un itinéraire de passerelle par défaut dans la table de routage VPC, avec l'adresse IP du pare-feu VM-Series du sous-réseau de l'application en tant que saut suivant. Configurez le SNAT à l'aide de l'adresse IP de l'interface non approuvée pour vous assurer que le trafic provenant d'Internet passe par le pare-feu VM-Series.

Reportez-vous à Sécurisation du trafic nord-sud sur Alibaba Cloud pour un exemple de configuration.

©2023 Palo Alto Networks, Inc.

Configuration système minimale requise pour le pare-feu VM-Series sur Alibaba Cloud

Sur Alibaba Cloud, vous pouvez déployer le pare-feu VM-Series sur l'hyperviseur KVM (voir Déploiements VM-Series).

- Pare-feu VM-Series : configuration logicielle requise
- Recommandations sur les types d'instances Alibaba Cloud pour le pare-feu VM-Series
- CLI Alibaba Cloud

Pare-feu VM-Series : configuration logicielle requise

Assurez-vous que vous disposez des logiciels et des licences nécessaires pour effectuer un déploiement VM-Series sur Alibaba Cloud.

- Pour déployer le pare-feu VM-Series sur Alibaba Cloud, vous devez utiliser une image VM-Series que vous obtenez sur Alibaba Marketplace. L'image intègre la version 10.0.3 de PAN-OS et la version 2.0.3 du plugin VM-Series.
- Avant le déploiement, choisissez la licence BYOL ou ELA VM-Series, une licence de capacité et un forfait d'abonnement. Reportez-vous à la section Types de licences de modèle VM-Series.
- Vous devez activer SSH dans le pare-feu VM-Series pour terminer le déploiement. Si votre système d'exploitation ne prend pas en charge SSH, installez un logiciel tiers, tel que Putty.

Recommandations sur les types d'instances Alibaba Cloud pour le pare-feu VM-Series

Avant de créer le pare-feu VM-Series, vous devez choisir un type d'instance Elastic Compute Service (ECS) qui prend en charge la configuration système minimale requise pour votre modèle VM-Series. Examinez la documentation sur le type d'instance pour vous assurer que le type d'instance ECS dispose des ressources nécessaires pour sécuriser la configuration de votre réseau.

Modèle VM-Series	Types d'instances Elastic Compute Service
VM-100	ecs.g5.xlarge, ecs.sn2ne.xlarge
VM-300	ecs.g5.xlarge, ecs.sn2ne.xlarge
VM-500	ecs.g5.2xlarge, ecs.sn2ne.2xlarge
VM-700	ecs.g5.4xlarge, ecs.sn2ne.4xlarge

CLI Alibaba Cloud

Aliyun version 3.0.4 ou supérieure. Reportez-vous à la section Préparez-vous à utiliser l'interface de ligne de commande Aliyun.

©2023 Palo Alto Networks, Inc.

Préparation au déploiement du pare-feu VM-Series sur Alibaba Cloud

Cette tâche utilise la CLI Aliyun pour créer un VPC et des vSwitch pour le pare-feu VM-Series. Toutefois, vous devez définir votre réseau avant de commencer. Évaluez les applications que vous souhaitez protéger et déterminez où vous allez déployer le pare-feu VM-Series pour inspecter et sécuriser le trafic nord-sud.

- Choisissez les licences et planifiez les réseaux
- Préparez-vous à utiliser l'interface de ligne de commande Aliyun

Choisissez les licences et planifiez les réseaux

Évaluez les applications dont vous avez besoin pour protéger et créer des réseaux permettant au pare-feu VM-Series d'inspecter le trafic d'applications entrant et sortant.

STEP 1 | Procédez à la Planification et conception de votre VPC.

1. Planifiez des réseaux, y compris des Blocs CIDR pour vos VPC et vSwitch.

   Reportez-vous à Création d'un VPC et configuration des réseaux pour un exemple de procédure.
2. Planifiez vos adresses IP. Si vous avez besoin d'adresses ou de plages d'adresses spécifiques, reportez-vous au Guide de l'utilisateur d'adresse IP élastique.
3. Planifiez des groupes de sécurité.

STEP 2 | Évaluez vos configurations réseau et applications et calculez la capacité de pare-feu dont vous avez besoin pour sécuriser vos applications et vos réseaux.

STEP 3 | Obtenez les licences de pare-feu VM-Series.

Bien que vous n'ayez pas besoin de licence pour installer le pare-feu VM-Series (vous pouvez activer une licence après l'installation), vous devez choisir un modèle VM-Series et un type d'instance ECS appropriés avant de déployer le pare-feu.

1. Choisissez un modèle VM-Series.

   Le pare-feu VM-Series prend en charge jusqu'à 8 interfaces, à condition que le modèle VM-Series et l'instance Alibaba Cloud disposent de ressources suffisantes. Vous pouvez utiliser le modèle

   Utilisez le modèle VM-Series que vous avez choisi pour sélectionner l'une des Recommandations sur les types d'instances Alibaba Cloud pour le pare-feu VM-Series.
2. Choisissez une licence de capacité VM-Series qui répond à vos besoins.
3. Achetez un forfait d'abonnement BYOL (si vous n'en avez pas déjà un). Vous recevez un code d'authentification pour votre abonnement VM-Series et vous devez le fournir lors du déploiement.

©2023 Palo Alto Networks, Inc.

STEP 4 | Planifiez la configuration des autorisations et des comptes Alibaba pour accéder au pare-feu VM-Series. Pour commencer, consultez la FAQ sur la sécurité et découvrez les rôles RAM d'instance.

Préparez-vous à utiliser l'interface de ligne de commande Aliyun

Ce chapitre porte sur la console ECS, cependant, tout ce que vous faites dans la console ECS peut être effectué à partir de l'interface de ligne de commande Aliyun. La CLI est nécessaire si vous souhaitez utiliser le pare-feu VM-Series pour sécuriser l'équilibrage de charge sur Alibaba Cloud.

Installez et configurez une version récente d'Aliyun, la Command Line Interface (interface de ligne de commande - CLI) d'Alibaba Cloud.

STEP 1 | Procédez à la Création d'une clé d'accès et sauvegardez l'Access Key ID (ID de clé d'accès) et la Secret Access Key (Clé d'accès secrète) dans un endroit sûr.

STEP 2 | Téléchargez une version prise en charge d'Aliyun sur le site https://github.com/aliyun/aliyun-cli.

STEP 3 | Procédez à l'Installation d'Aliyun.

STEP 4 | Procédez à la Configuration d'Aliyun.

La configuration vous invite à saisir vos informations d'Access Key (Clé d'accès) et d'autres informations.

Si votre déploiement utilise un compartiment de stockage, la région doit correspondre à la région de votre compartiment.

```
aliyun configure Configuring profile '' in '' authenticate
 mode... Access Key Id [*************8rq]: *************8rq
 Access Key Secret [**************************tM2]:
 **************************tM2 Default Region Id [us-west-1]:
 us-west-1 Default Output Format [json]: json (Only support
 json)) Default Language [zh|en] en: en Saving profile[] ...Done.
 available regions: ...
```


©2023 Palo Alto Networks, Inc.

Déploiement du pare-feu VM-Series sur Alibaba Cloud

Le pare-feu VM-Series utilise au minimum trois interfaces : gestion, non approuvée et approuvée. Lorsque vous créez un VPC Alibaba Cloud, celui-ci est logiquement isolé. Pour segmenter votre réseau privé virtuel en sous-réseaux, vous devez créer des VSwitches, chacun ayant son propre bloc CIDR. Le pare-feu VM-Series ayant plusieurs interfaces, il peut inspecter le trafic sur tous les sous-réseaux.

Généralement, le trafic entrant externe rencontre l'interface non approuvée du pare-feu VM-Series. Le pare-feu inspecte le trafic entrant et l'envoie à une application via l'interface approuvée. Le trafic de retour de l'application se dirige vers l'interface approuvée du pare-feu, où le pare-feu inspecte le trafic de retour et l'envoie via l'interface non approuvée.

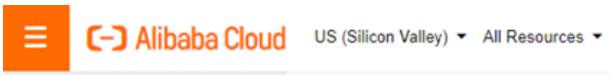
Les tâches suivantes montrent comment utiliser la console pour créer l'infrastructure de pare-feu VM-Series.

- Création d'un VPC et configuration des réseaux
- Création et configuration du pare-feu VM-Series
- Sécurisation du trafic nord-sud sur Alibaba Cloud
- Configuration de l'équilibrage de charge sur Alibaba Cloud

Création d'un VPC et configuration des réseaux

Utilisez la console Alibaba Cloud pour créer un VPC, des vSwitches, des groupes de sécurité et des règles de groupe de sécurité.

STEP 1 | Ouvrez la console VPC et sélectionnez votre région dans le menu. Notez que la région que vous sélectionnez doit fournir un des types d'instance que Palo Alto Networks prend en charge.



STEP 2 | Sur la page d'accueil de la console Alibaba Cloud, sélectionnez **Products and Services (Produits et services)** > **Networking (Mise en réseau)** > **Virtual Private Cloud (Cloud privé virtuel)**.

STEP 3 | **Créez un VPC**.

Dans cette étape, vous créez un VPC et les vSwitches de gestion, approuvé et non approuvé. La console ECS crée un VPC et un commutateur de la même manière.

1. Sélectionnez **Create VPC (Créer un VPC)**.

   Spécifiez le nom du VPC, un bloc CIDR IPv4 et une description. Reportez-vous à la section Créer un VPC.

Propriété	Valeur
Name (Nom)	Votre choix.
IPV4 CIDR Bock (Bloc CIDR IPV4)	Votre choix. Reportez-vous à la section Questions fréquentes sur les blocs CIDR.

©2023 Palo Alto Networks, Inc.

Propriété	Valeur
Resource Group (Groupe de ressources)	Votre choix.

2. Sélectionnez **Create VSwitch (Créer un VSwitch)**.
   - Nommez le vSwitch **`Gestion`**.
   - Choisissez la **Zone**, spécifiez un **IPv4 CIDR Block (Bloc CIDR IPv4)** qui est un sous-ensemble du bloc que vous avez spécifié pour le VPC, et indiquez une **Description**.
   - En bas, cliquez sur **Add (Ajouter)** pour ajouter un autre vSwitch (ne cliquez pas sur **OK** avant d'avoir ajouté tous les vSwitches).

   Reportez-vous à la section Créer un VSwitch.
3. Cliquez sur **Add (Ajouter)** pour ajouter le vSwitch non approuvé de la même manière.
4. Cliquez sur **Add (Ajouter)** pour ajouter le vSwitch approuvé.
5. Cliquez sur **OK**.

   Consultez les détails du VPC et apportez les modifications nécessaires avant de cliquer sur **Complete (Terminer)**.

STEP 4 | Créez des groupes de sécurité et des règles de groupe de sécurité.

- Sur la page d'accueil de la console Alibaba Cloud, sélectionnez **Elastic Compute Service** > **Networking & Security (Mise en réseau et sécurité)** > **Security Groups (Groupes de sécurité)**.
- En haut à droite, cliquez sur **Create Security Group (Créer un groupe de sécurité)**.

1. Créez le groupe de sécurité de gestion.

   Reportez-vous à la section Créer un groupe de sécurité pour remplir les champs suivants.

Propriété	Valeur
Modèle	Personnaliser
Security Group Name (Nom du groupe de sécurité)	Gestion
Security Group Type (Type du groupe de sécurité)	De base
Network Type (Type de réseau)	VPC
VPC	Sélectionnez le VPC que vous avez créé précédemment.

©2023 Palo Alto Networks, Inc.

Propriété	Valeur
Resource Group (Groupe de ressources)	Votre choix.

- Remplissez le formulaire et cliquez sur **OK**.

  La console ECS vous invite à créer des règles pour ce groupe de sécurité. Cette tâche décrit certaines règles de base du groupe de sécurité qui vous permettent de faire apparaître le pare-feu VM-Series. Vous pouvez créer plus de règles pour appliquer les exigences de sécurité de votre réseau.

2. Sélectionnez **Create Rules Now (Créer des règles maintenant)** et créez des règles pour HTTPS et SSH.

   Sélectionnez l'onglet Inbound (Entrant) et cliquez sur **Add Security Group Rule (Ajouter une règle de groupe de sécurité)**.

   - Créez une règle entrante pour autoriser HTTPS dans ce groupe de sécurité. Par exemple :

Propriété	Valeur
Rule Direction (Sens de la règle)	Inbound (Entrant)
Action (Action)	Allow (Autoriser)
Protocol Type (Type de protocole)	HTTPS (443)
Priority (Priorité)	100
Authorization Type (Type d'autorisation)	Reportez-vous à la section Ajouter des règles de groupe de sécurité.
Authorization Object (Objet d'autorisation)	

   - Cliquez sur **Add Security Group Rule (Ajouter une règle de groupe de sécurité)** pour créer une règle entrante afin d'autoriser SSH sur l'interface de gestion.

Propriété	Valeur
Rule Direction (Sens de la règle)	Inbound (Entrant)
Action (Action)	Allow (Autoriser)
Protocol Type (Type de protocole)	TCP personnalisé
Port Range (Plage de ports)	1/65535

©2023 Palo Alto Networks, Inc.

Propriété	Valeur
Authorization Type (Type d'autorisation)	Reportez-vous à la section Ajouter des règles de groupe de sécurité.
Authorization Object (Objet d'autorisation)	

Cliquez sur **OK** et sur **Back (Retour)** pour retourner à la page des groupes de sécurité.

3. Sélectionnez **Create Security Group (Créer un groupe de sécurité)** et créez le groupe de sécurité non approuvé.

   Lorsque vous y êtes invité, créez une règle pour le groupe de sécurité non approuvé.

Propriété	Valeur
Rule Direction (Sens de la règle)	Inbound (Entrant)
Action (Action)	Allow (Autoriser)
Protocol Type (Type de protocole)	TCP personnalisé
Port Range (Plage de ports)	1/65535
Priority (Priorité)	100
Authorization Type (Type d'autorisation)	Reportez-vous à la section Ajouter des règles de groupe de sécurité.
Authorization Object (Objet d'autorisation)	

Cliquez sur **OK** et sur **Back (Retour)** pour retourner à la page des groupes de sécurité.

4. Créez le groupe de sécurité approuvé.

   Lorsque vous y êtes invité, cliquez sur **Add Security Group Rule (Ajouter une règle de groupe de sécurité)** et dupliquez la règle non approuvée.

   Passez à la section Création et configuration du pare-feu VM-Series.

Création et configuration du pare-feu VM-Series

Cette tâche utilise la console ECS pour créer une instance de pare-feu VM-Series avec un minimum de trois interfaces : gestion, approuvée et non approuvée. Une instance ECS prend en charge une seule carte d'interface réseau par défaut et y connecte automatiquement une Elastic Network Interface (ENI). Pour prendre en charge le pare-feu VM-Series, vous devez créer séparément les ENI approuvée et non approuvée et les connecter à votre instance.

©2023 Palo Alto Networks, Inc.

STEP 1 | Sur la page d'accueil de la console Alibaba Cloud, sélectionnez **Elastic Compute Service** > **Instances & Images (Instances et images)** > **Instances**, et cliquez sur **Create Instance (Créer une instance)** en haut à droite.

STEP 2 | Sélectionnez **Custom Launch (Lancement personnalisé)**.

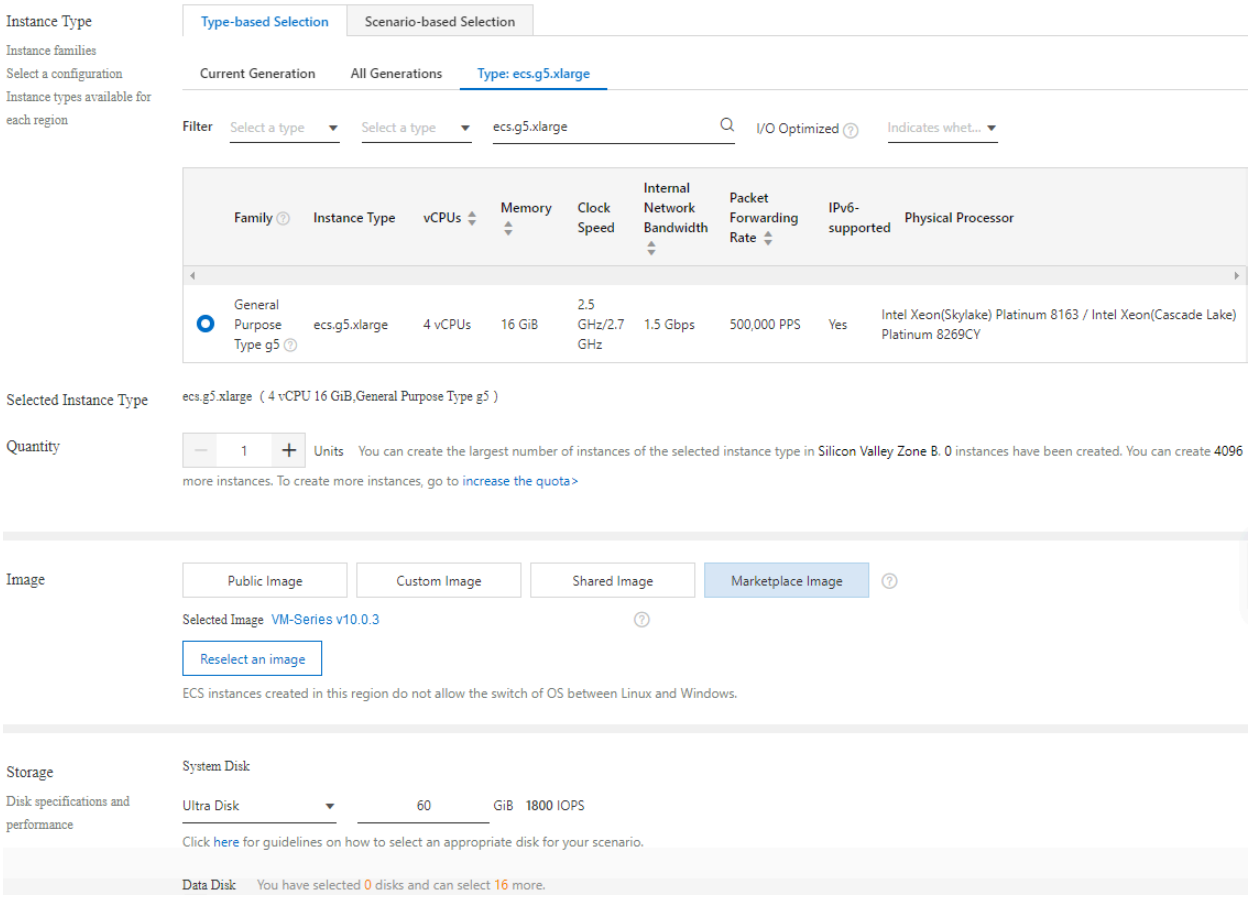
STEP 3 | Configurations de base.

1. Remplissez les valeurs suivantes. Par exemple :

Propriété	Valeur
Méthode de facturation	Subscription (Abonnement).
Région	Votre choix. Vous pouvez également sélectionner une Zone. La région que vous sélectionnez doit fournir un des types d'instance requis.
Type d'instance	Un des types dans Recommandations sur les types d'instances Alibaba Cloud pour le pare-feu VM-Series. Vous pouvez utiliser la sélection basée sur le type pour rechercher le type d'instance.
Image	Sélectionnez **Marketplace Image (Image Marketplace)** et recherchez « VM-Series » sur Alibaba Marketplace. L'image combine le système d'exploitation et le pare-feu VM-Series.
Stockage	Choisissez un type de disque et spécifiez 60 Go.
Instantané	Votre choix.

 ©2023 Palo Alto Networks, Inc.

Propriété	Valeur
Durée	Votre choix.



2. Sélectionnez **Next: Networking** (Suivant : mise en réseau).

STEP 4 | Sur la page Networking (Mise en réseau), fournissez les valeurs suivantes.

1. Network (Réseau) : sélectionnez VPC.
   - Choisissez le VPC que vous avez créé dans Création d'un VPC et configuration des réseaux.
   - Choisissez le vSwitch de gestion.
2. Public IP Address (Adresse IP publique).

   Si vous n'avez pas d'adresse IP publique, activez l'option **Assign Public IP address (Attribuer une adresse IP publique)** et le système vous en attribuera une. Si vous devez utiliser une adresse IP spécifique ou une adresse dans une plage spécifique, vous

©2023 Palo Alto Networks, Inc.

pouvez demander une adresse IP personnalisée. Reportez-vous au Guide de l'utilisateur d'adresse IP élastique.

3. Security Group (Groupe de sécurité).

   Sélectionnez le groupe de sécurité de gestion.

4. Elastic Network Interface.

   L'interface de gestion est déjà connectée à eth0.

5. Sélectionnez **Next: System Configurations** (Suivant : configurations du système).

STEP 5 | Sur la page System Configurations (Configurations du système), renseignez les valeurs suivantes.

1. Connectez-vous avec vos informations d'identification : Sélectionnez la **Key Pair (Paire de clés)**.

   L'authentification par mot de passe n'est pas prise en charge.

2. Nommez l'instance de pare-feu VM-Series et fournissez un nom d'hôte.

   Apportez les corrections nécessaires.

   Sélectionnez **Aperçu** pour afficher vos paramètres jusqu'à présent.

3. Après **Advanced (Avancé) (basé ou rôles de RAM d'instance ou cloud-init)**, cliquez sur **Show (Afficher)**.

   - Le rôle de RAM est facultatif.
   - Dans le champ User Data (Données utilisateur), saisissez les informations d'amorçage de base sous forme de paires clé-valeur séparées par des sauts de ligne. Reportez-vous à la section Saisir une configuration de base en tant que données utilisateur (clouds publics). Par exemple, saisissez les informations suivantes dans le champ **User Data (Données utilisateur)**.

```
type=dhcp-client hostname=Ca-FW-DC1 vm-auth-
key=7550362253**** panorama-server=10.*.*.20 panorama-
server-2=10.*.*.21 tplname=FINANCE_TG4 dgname=finance_dg op-
cmd-dpdk-pkt-io=on dhcp-send-hostname=yes dhcp-send-client-
id=yes dhcp-accept-server-hostname=yes dhcp-accept-server-
domain=yes authcodes=I7115398 vm-series-auto-registration-
pin-id=abcdefgh1234**** vm-series-auto-registration-pin-
value=zyxwvut-0987****
```

   op-command-modes *(mgmt-interface-swap et jumbo frame) n'est pas pris en charge pour Alibaba Cloud.*

   op-cmd-dpdk-pkt-io=on *prend en charge DPDK. Si vous voulez spécifier PacketMMAP, spécifiez op-cmd-dpdk-pkt-io=off*

   Le regroupement est facultatif. Sélectionnez **Preview (Prévisualisation)**pour voir la configuration avant de commander.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Consultez les modalités de service et sélectionnez **Create Order (Créer une commande)** pour créer l'instance de pare-feu VM-Series.

Visualisez le bon de commande et sélectionnez **Subscribe (S'abonner)**.

STEP 7 | Sur la page d'accueil de la console, choisissez > **Elastic Compute Service** > **Networks and Security (Réseaux et sécurité)** > **ENIs (ENI)** et sélectionnez **Create ENI (Créer une ENI)** dans le coin supérieur droit. Créez des interfaces réseau élastiques pour les interfaces non approuvées et approuvées.

1. Créez l'ENI non approuvée.

   Dans la colonne **Actions**, sélectionnez **Bind to Instance (Lier à l'instance)** et sélectionnez l'instance que vous venez de créer.
2. Créez l'ENI approuvée et liez-la à l'instance.

STEP 8 | Attribuez des adresses IP élastiques (EIP).

Attribuez des adresses EIP à l'interface de gestion du pare-feu VM-Series et à l'interface réseau non approuvée. Dans cet exemple, l'interface approuvée n'est pas exposée à Internet, vous n'avez donc pas besoin d'une troisième adresse IP.

Si vous avez déjà deux EIP, passez à l'étape suivante.

1. Associez une EIP à l'interface de gestion du pare-feu VM-Series.
2. Associez une EIP à l'interface réseau non approuvée du pare-feu VM-Series.

   La seconde interface que vous associez est affectée à l'interface réseau 1 sur le pare-feu VM-Series.

STEP 9 | Redémarrez votre instance pour associer les nouvelles interfaces réseau.

Dans la liste Instances, sélectionnez votre instance puis cliquez sur **Manage (Gérer)** et **Restart (Redémarrer)** en haut à droite.

STEP 10 | Accédez au pare-feu VM-Series via SSH avec la clé de sécurité et définissez le mot de passe administrateur :

```
developer1$ ssh -i dev1-vpc1.pem admin@18.***.145.153
 Welcome admin. admin> configure Entering configuration mode
 [edit] admin# set mgt-config users admin password Enter
 password:<password> Confirm password:<password> [edit]
 admin# commit
```

STEP 11 | Accédez à l'interface Web du pare-feu VM-Series.

Ouvrez un navigateur Web et saisissez l'EIP pour l'interface de gestion.

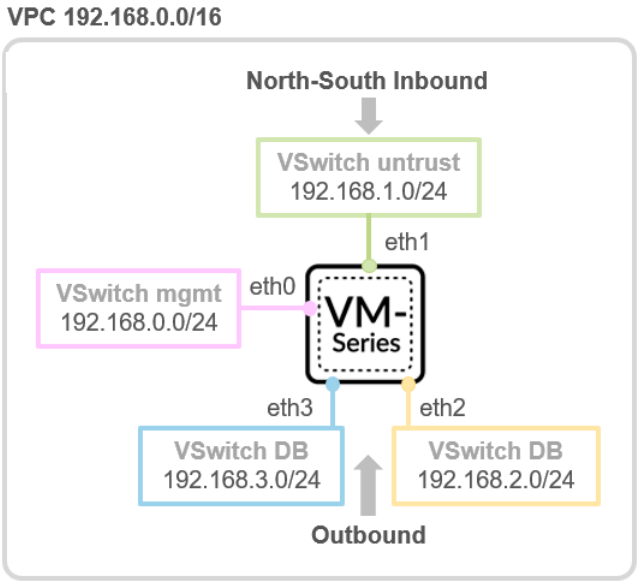
Sécurisation du trafic nord-sud sur Alibaba Cloud

Après avoir créé un VPC, vous pouvez créer des VSwitch pour segmenter votre réseau privé virtuel en sous-réseaux. Cet exemple montre un VPC avec CIDR 192.168.0.0/16 ; vous pouvez saisir vos propres valeurs. Quatre vSwitch créent quatre sous-réseaux.

©2023 Palo Alto Networks, Inc.

Nom du vSwitch	Interface	Exemple de CIDR
mgmt	eth0	192.168.0.0/24
non approuvé	eth1	192.168.1.0/24
Web	eth2	192.168.2.0/24
db	eth3	192.168.3.0/24.

Dans le schéma suivant, le pare-feu VM-Series se connecte à deux sous-réseaux de confiance, web et db. Le trafic entrant est initié lorsqu'un client externe accède à l'interface non approuvée du pare-feu VM-Series. Le pare-feu inspecte le trafic et l'envoie à une application. Par exemple, le pare-feu envoie le trafic vers un serveur Web via l'interface approuvée. Le trafic qui revient du serveur Web doit atteindre l'interface approuvée du pare-feu VM-Series. Le pare-feu inspecte le flux de trafic de retour et l'envoie via l'interface non approuvée.



DNAT et SNAT doivent être configurés sur le pare-feu pour sécuriser le trafic entrant.

STEP 1 | Créez des règles NAT pour le trafic entrant.

Voici un exemple des règles NAT pour la protection du trafic entrant.

```
          <nat> <rules> <entry name="inbound_web"> <source-
translation> <dynamic-ip-and-port> <interface-address>
 <interface>ethernet1/2</interface> </interface-address>
 </dynamic-ip-and-port> </source-translation> <destination-
translation> <translated-address>web_server</translated-address>
 </destination-translation> <to> <member>untrust</member> </to>
 <from> <member>any</member> </from> <source> <member>any</member>
 </source> <destination> <member>fw_untrust</member> </destination>
 <service>any</service> <to-interface>ethernet1/1</to-interface>
 </entry> </rules> </nat> <address> <entry name="fw_untrust"> <ip-
netmask>192.168.1.4</ip-netmask> </entry> <entry name="fw_trust">
 <ip-netmask>192.168.2.201</ip-netmask> </entry> <entry
```

 ©2023 Palo Alto Networks, Inc.

```
name="web_server"> <ip-netmask>192.168.2.203</ip-netmask> </entry>
</address>
```

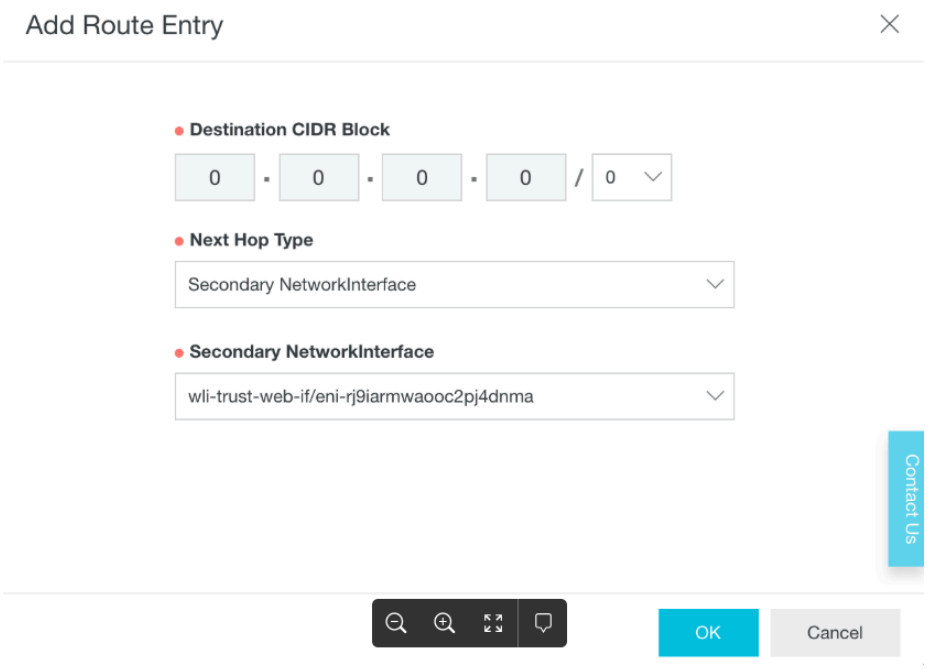
STEP 2 | Sécurisez le trafic sortant.

Comme indiqué dans le diagramme ci-dessus, une application initie le trafic sortant. Par exemple, un serveur Web doit exécuter **`yum install`** pour mettre à jour les paquets rpm. En règle générale, le trafic Internet dans un VPC est acheminé vers une passerelle NAT (avec une EIP

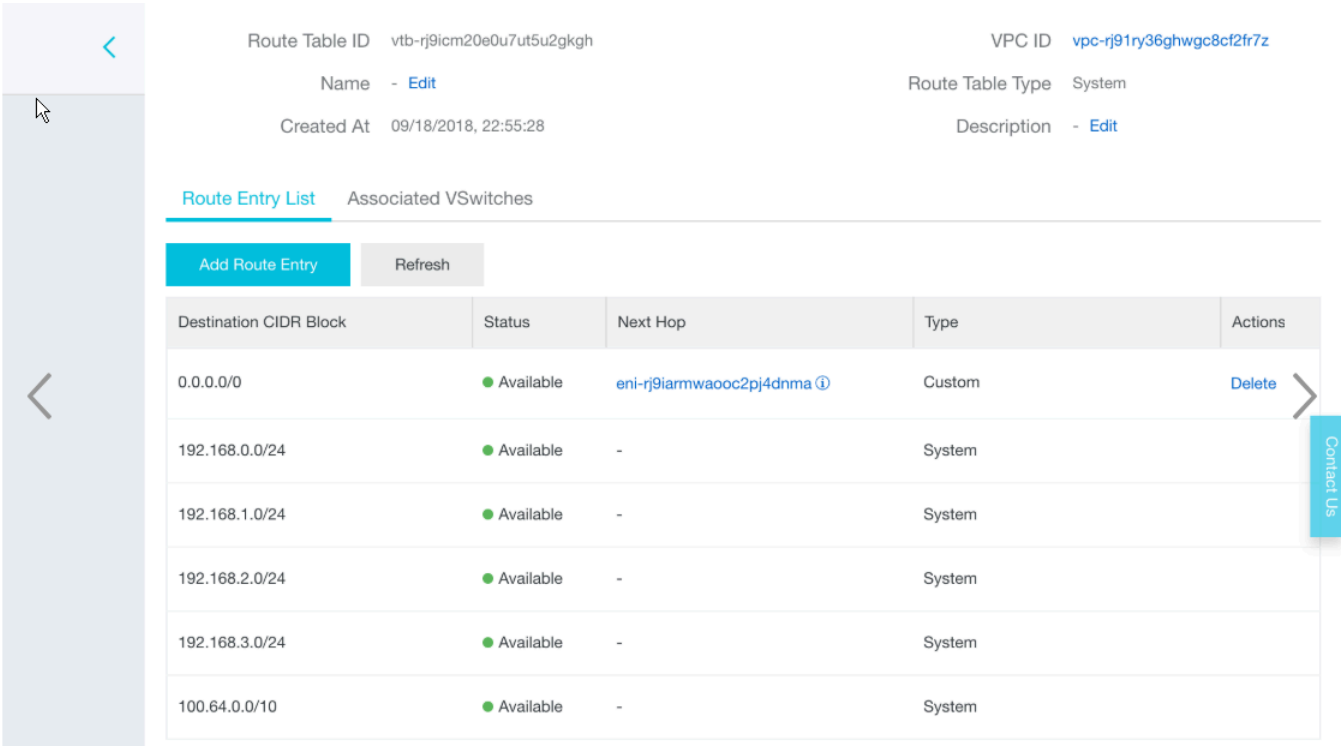
©2023 Palo Alto Networks, Inc.

attachée). Pour sécuriser le trafic sortant, vous devez obliger le trafic sortant à passer par le pare-feu VM-Series.

1. Ajoutez un itinéraire de passerelle par défaut dans la table de routage VPC avec une adresse IP de pare-feu dans le sous-réseau du serveur Web en tant que saut suivant.



2. Affichez votre entrée dans la table de routage.



3. Configurez les règles SNAT à l'aide de l'adresse IP de l'interface non approuvée pour vous assurer que le trafic renvoyé par Internet passe par le pare-feu VM-Series.

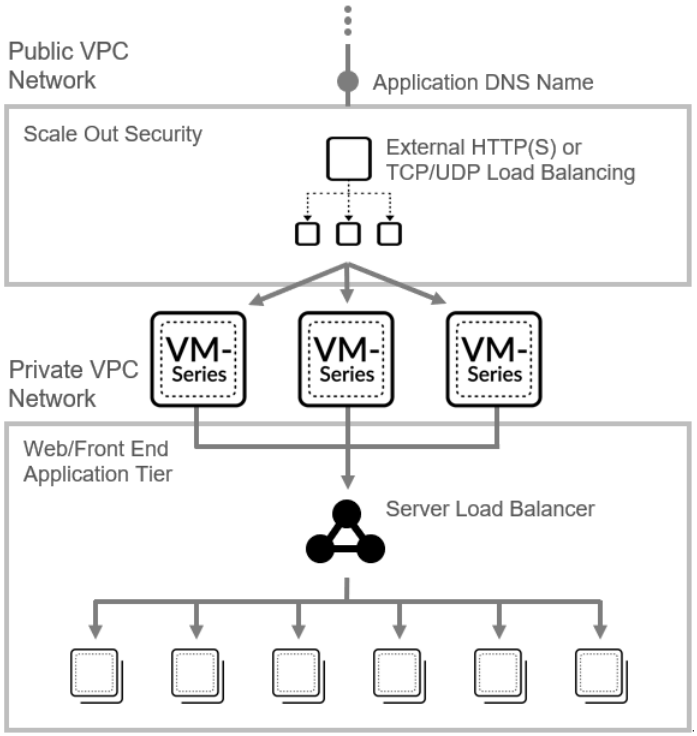
©2023 Palo Alto Networks, Inc.

Voici un exemple de configuration SNAT.

```
            <nat> <rules> <entry name="outbound_web">
 <source-translation> <dynamic-ip-and-port> <interface-
address> <interface>ethernet1/1</interface> </interface-
address> </dynamic-ip-and-port> </source-translation> <to>
 <member>untrust</member> </to> <from> <member>trust</member>
 </from> <source> <member>any</member> </source> <destination>
 <member>any</member> </destination> <service>any</service>
 <to-interface>any</to-interface> </entry> </rules> </nat>
```

Configuration de l'équilibrage de charge sur Alibaba Cloud

Sur Alibaba Cloud, vous pouvez déployer le pare-feu VM-Series dans une configuration en sandwich d'équilibreur de charge dans laquelle le pare-feu est déployé entre un réseau public et un réseau privé, comme indiqué ci-dessous.



Dans la section Création d'un VPC et configuration des réseaux, vous avez créé les ENI approuvée et non approuvée et les avez liées à l'instance de pare-feu VM-Series en tant qu'ENI secondaires.

Lorsque vous utilisez la console pour ajouter plusieurs serveurs principaux à Alibaba Server Load Balancer (SLB), le SLB envoie le trafic à l'ENI principale des serveurs principaux du saut suivant. Étant donné que l'ENI principale est l'interface de gestion, le trafic doit être inspecté via l'interface non approuvée (ENI secondaire).

Pour vous assurer que le trafic Internet est dirigé vers les interfaces du plan de données plutôt que vers l'interface de gestion, utilisez la CLI Alibaba pour connecter les ENI non approuvées du pare-feu VM-Series à votre instance SLB.

©2023 Palo Alto Networks, Inc.

Vous devez installer Command Line Interface (interface en ligne de commande - CLI) Aliyun *pour utiliser les commandes CLI suivantes.*

STEP 1 | Créez les VPC publics et privés pour une configuration sandwich d'équilibreur de charge et déployez les pare-feu VM-Series.

Les étapes restantes sont des exemples de commandes CLI que vous pouvez adapter à votre environnement.

STEP 2 | Procédez à la Création de l'équilibreur de charge.

```
slb CreateLoadBalancer --RegionId us-west-1 --LoadBalancerName
 wli-slb --VpcId vpc-rj91ry36ghwgc8cf2fr7z --LoadBalancerSpec
 slb.s1.small --AddressType internet --MasterZoneId us-
west-1a --SlaveZoneId us-west-1b { "NetworkType": "classic",
 "LoadBalancerName": "**********", "Address": "***********,
 "ResourceGroupId": "rg-************ofi", "RequestId": "0B8BA2AA-
E837-****-****-B82A8A1D5FBB", "AddressIPVersion": "ipv4",
 "LoadBalancerId": "lb-******************mvz", "VSwitchId": "",
 "VpcId": "vpc-****************r7z" }
```

STEP 3 | Procédez à l'Ajout des serveurs principaux.

Utilisez la CLI pour ajouter des interfaces une à la fois. L'ordre dans lequel vous ajoutez les interfaces détermine quelle carte d'interface réseau reçoit l'interface.

```
aliyun slb AddBackendServers --LoadBalancerId lb-
******************mvz --BackendServers '[ { "ServerId":"eni-
******************bzw", "Type":"eni","Weight":"100" } ]'
```

STEP 4 | Créez un écouteur HTTP qui effectue une vérification de l'état.

```
aliyun slb CreateLoadBalancerHTTPListener --LoadBalancerId lb-
******************mvz --ListenerPort 80 --StickySession on --
HealthCheck on --HealthCheckURI '/'
```


©2023 Palo Alto Networks, Inc.

Configuration d’un pare-feu dans Cisco ACI

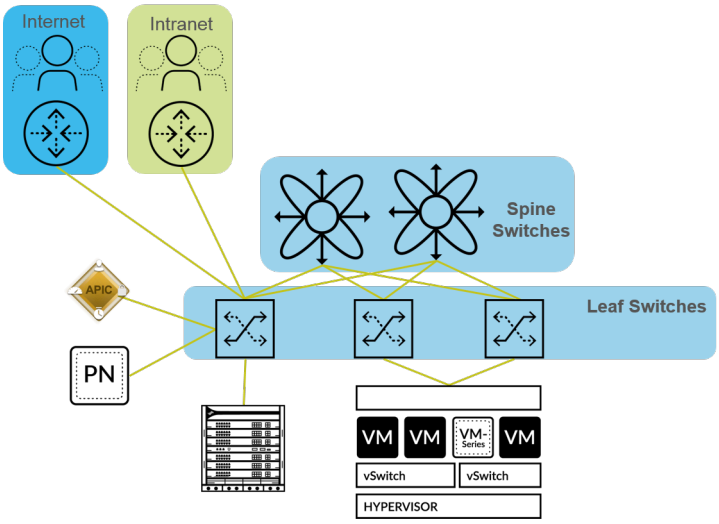
Palo Alto Networks s’intègre en tant que service à Cisco Application-Centric Infrastructure (ACI). ACI est une solution SDN (réseau défini par logiciel) permettant de déployer facilement de nouvelles charges de travail et de nouveaux services réseau. À l’aide d’un contrôleur SDN appelé APIC (Cisco Application Policy Infrastructure Controller), vous déployez le service de pare-feu entre les groupes de terminaux (EPG). Les EPG agissent comme un conteneur pour les applications ou les niveaux d’application. Lorsque vous placez un pare-feu entre des EPG, la politique de sécurité configurée sur le pare-feu sécurise le trafic entre les EPG. L’APIC fournit un seul volet de gestion de la topologie réseau, des politiques réseau et de la connectivité pour l’ensemble du centre de données et prend en charge l’insertion de périphériques L4-L7, tels qu’un pare-feu matériel ou VM-Series. Panorama est requis pour la gestion centralisée de la sécurité.

- Intégration du pare-feu Palo Alto Networks à Cisco ACI
- Préparation de votre environnement ACI pour l’intégration
- Intégration du pare-feu à Cisco ACI en mode politique réseau
- Surveillance des terminaux dans Cisco ACI

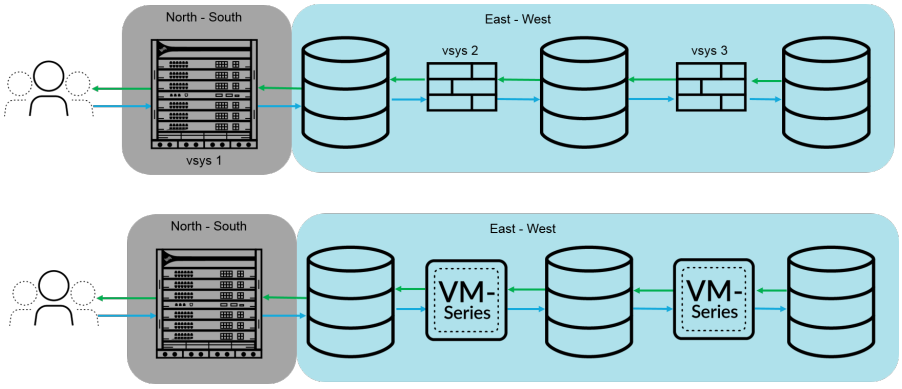
Intégration du pare-feu Palo Alto Networks à Cisco ACI

L'intégration de Palo Alto Networks à Cisco ACI vous permet d'insérer un pare-feu entre les EPG en tant que service de couche 4 à couche 7. Le pare-feu sécurise ensuite le trafic est-ouest entre les niveaux d'application dans ces EPG ou le trafic nord-sud entre les utilisateurs et les applications.

La figure ci-dessous montre un exemple de déploiement d'ACI physique qui inclut des pare-feu intégrés de Palo Alto Network. Toutes les entités de l'infrastructure ACI sont connectées à des commutateurs feuilles, et ces commutateurs feuilles sont connectés à des commutateurs Spine plus grands. Lorsque les utilisateurs accèdent à l'application, l'infrastructure ACI déplace le trafic vers la destination correcte. Pour sécuriser le trafic entre les niveaux d'application, l'administrateur réseau insère les pare-feu Palo Alto Networks en tant que services L4 à L7 entre chaque EPG et crée un graphique de service pour définir les services fournis par le périphérique L4 à L7.



Une fois les services de pare-feu déployés, le trafic circule désormais logiquement comme indiqué ci-dessous. Trafic vers et depuis les utilisateurs finaux et chaque niveau de l'application, quel que soit le lieu ou la manière dont chaque entité est physiquement connectée au réseau.



Lorsque le pare-feu est intégré à Cisco ACI, le trafic est envoyé au pare-feu avec une redirection basée sur une politique (PBR). De plus, la configuration du pare-feu et celle de l'APIC sont complètement distinctes. Le mode politique réseau ne dépend d'aucune autre intégration de configuration entre le pare-feu et l'APIC. Il offre donc une plus grande flexibilité de configuration et de déploiement du pare-feu.

©2023 Palo Alto Networks, Inc.

Pour le trafic est-ouest, définissez un domaine de pont et un sous-réseau dans l'infrastructure ACI du pare-feu. Configurez les contrats entre les EPG qui envoient le trafic au pare-feu à l'aide d'un PBR. Le PBR transfère le trafic au pare-feu en fonction d'une politique contenant l'adresse IP et MAC du pare-feu. Les interfaces de pare-feu sont toujours en mode Layer 3 (Couche 3) et le trafic est reçu et acheminé vers l'infrastructure ACI. Vous pouvez configurer des interfaces distinctes pour les connexions des consommateurs et fournisseurs ou une interface unique pour le trafic entrant et sortant. La procédure décrite dans ce document utilise une interface unique, car elle simplifie l'intégration. Vous n'avez pas besoin de configurer autant d'interfaces, d'adresses IP ou de VLAN. Toutefois, lorsque vous utilisez une interface unique, vous ne pouvez pas utiliser les informations sur la zone pour définir la politique de sécurité et vous devez modifier la politique intra-zone par défaut sur le pare-feu pour refuser le trafic.

Pour le trafic nord-sud, vous devez utiliser une politique dédiée appelée L3Out. Une L3Out contient les informations nécessaires au locataire pour se connecter à des appareils de routage externes et accéder à des réseaux externes. Les connexions L3Out contiennent un EPG de réseau externe qui représente les réseaux accessibles via la politique L3Out. Tout comme la L3Out peut regrouper tous les réseaux externes dans un seul EPG, vous pouvez utiliser une ACI d'objet vzAny pour représenter tous les EPG d'une VRF. L'utilisation d'un objet vzAny simplifie l'application du contrat de trafic sortant car, chaque fois qu'un nouvel EPG est ajouté au VRF, le contrat est automatiquement appliqué. Dans ce scénario, le réseau externe fournit le contrat et l'objet vzAny (tous les EPG internes) le consomme.

La section suivante fournit des détails supplémentaires sur les composants et les concepts qui constituent l'intégration entre le pare-feu nouvelle génération et Cisco ACI.

- Modèles de graphique de service
- Déploiements multicontextes

Modèles de graphique de service

Les pare-feu sont déployés dans Cisco ACI via des graphiques de service. Un graphique de service vous permet d'intégrer des appareils de couche 4 à 7, tels qu'un pare-feu, dans le flux de trafic sans qu'il soit nécessaire que l'appareil L4-L7 soit la passerelle par défaut pour les serveurs de l'infrastructure ACI.

Les pare-feu sont représentés dans l'infrastructure ACI en tant qu'appareil L4-L7 que vous configurez dans l'APIC en tant que cluster d'appareils. Un seul pare-feu ou deux pare-feu déployés en tant que paire HA sont configurés en tant que cluster d'appareils. Chaque cluster d'appareils comporte une ou plusieurs interfaces logiques qui décrivent les informations d'interface du cluster d'appareils et mappent le chemin d'accès du pare-feu membre avec un VLAN du domaine de serveur de surveillance de machine virtuelle (VMM) ou physique.

Les modèles de graphique de service définissent le cluster d'appareils de pare-feu que vous intégrez dans le flux de trafic entre les EPG. En outre, le modèle de graphique de service définit la manière dont le pare-feu est intégré et les interfaces logiques attribuées aux EPG des fournisseurs et consommateurs. Après avoir créé votre modèle de graphique de service, vous l'attribuez à des EPG et à des contrats. Étant donné que le modèle de graphique de service n'est pas lié à un EPG ou à un contrat spécifique, vous pouvez le réutiliser avec plusieurs EPG. L'APIC déploie ensuite le modèle de graphique de service en le connectant au domaine de pont entre les EPG.

 ©2023 Palo Alto Networks, Inc.

Déploiements multicontextes

L'intégration Cisco ACI prend en charge les pare-feu physiques divisés en contextes gérés par ACI en tant que pare-feu individuels. Sur le pare-feu, ces contextes sont les systèmes virtuels (vsys) sur les pare-feu, et chaque pare-feu est autorisé à prendre en charge un certain nombre d'instances de vsys. Lors du déploiement d'un pare-feu multi-systèmes virtuels dans ACI, vous devez configurer un gestionnaire de châssis dans le locataire et l'attribuer au service de pare-feu.

©2023 Palo Alto Networks, Inc.

Préparation de votre environnement ACI pour l'intégration

Avant de pouvoir intégrer le pare-feu à un package de périphérique, vous devez effectuer les étapes suivantes pour préparer votre environnement Cisco ACI.

STEP 1 | Déployez Panorama.

STEP 2 | Déployez le pare-feu.

- Pare-feu physique : connectez le port de gestion hors bande du pare-feu à un port de commutation feuille et connectez au moins une interface de données de pare-feu au commutateur. Les interfaces de pare-feu sur un pare-feu physique sont configurées avec des réseaux locaux virtuels (VLAN) pour assurer la connectivité aux réseaux corrects. Déployez le pare-feu en fonction du guide d'installation spécifique à la plate-forme.
- Pare-feu VM-Series : lors de la configuration du matériel virtuel pour le pare-feu VM-Series, définissez le groupe de ports pour l'interface de gestion. Chaque pare-feu VM-Series connecté au réseau nécessite sa propre carte réseau virtuelle (NIC). Déployez le pare-feu VM-Series en fonction de votre hyperviseur.

STEP 3 | Configurez l'adresse IP de gestion sur chaque pare-feu et Panorama.

Effectuez la configuration initiale sur :

- le pare-feu matériel ;
- le pare-feu série VM ;
- Panorama

STEP 4 | Ajoutez votre ou vos pare-feu en tant que périphérique(s) géré(s).

STEP 5 | Installez des licences de fonctionnalités sur votre ou vos pare-feu.

- Enregistrez et activez les licences sur votre pare-feu physique.
- Enregistrez et Activation des licences de modèle VM-Series sur votre pare-feu VM-Series.
- Gérez les licences de pare-feu en utilisant Panorama.

STEP 6 | Établissez l'infrastructure ACI Cisco et la connectivité de gestion.

Dans le cadre de cette configuration, créez un domaine physique et un espace de noms VLAN. Assurez-vous que les interfaces de données des pare-feu physiques font partie du domaine physique.

STEP 7 | Créez un profil de domaine VMM Cisco ACI.

Si vous utilisez des machines virtuelles ou le pare-feu VM-Series, créez un profil de domaine de serveur de surveillance de machine virtuelle (VMM) pour l'environnement VMware vSphere. Le domaine VMM spécifie la politique de connectivité entre vSphere et l'infrastructure ACI.

©2023 Palo Alto Networks, Inc.

Intégration du pare-feu à Cisco ACI en mode politique réseau

En mode politique réseau, vous intégrez une paire de pare-feu en haute disponibilité (HA) dans le trafic est-ouest ou nord-sud en utilisant une redirection basée sur une politique vers une seule interface logique HA. Le pare-feu et l'infrastructure ACI sont configurés séparément et les objets d'adresse situés sur le pare-feu sont mappés aux EPG de l'infrastructure ACI.

Vous pouvez utiliser le mode politique réseau pour déployer un pare-feu de Palo Alto Networks afin de sécuriser le trafic est-ouest ou nord-sud.

- Déploiement du pare-feu pour sécuriser le trafic est-ouest en mode politique réseau
- Déploiement du pare-feu pour sécuriser le trafic nord-sud en mode politique réseau

Déploiement du pare-feu pour sécuriser le trafic est-ouest en mode politique réseau

La procédure suivante explique comment déployer un pare-feu de Palo Alto Networks pour sécuriser le trafic est-ouest dans votre environnement Cisco ACI à l'aide du mode non géré avec une redirection basée sur une politique. Cette procédure suppose que vous avez effectué les tâches suivantes :

- Les pare-feu sont opérationnels et connectés à un commutateur feuille dans votre environnement Cisco ACI. De plus, l'interface de gestion de chaque pare-feu doit être accessible par l'APIC.
- Les pare-feu sont déployés en mode HA active/passive. Cette procédure ne couvre pas la configuration réseau HA et suppose que vous l'avez déjà effectuée.

Pour sécuriser le trafic est-ouest, définissez un domaine de pont et un sous-réseau dans l'infrastructure ACI du pare-feu. Configurez les contrats entre les EPG qui envoient le trafic au pare-feu à l'aide d'un PBR. Le PBR transfère le trafic au pare-feu en fonction d'une politique contenant l'adresse IP et MAC du pare-feu. Les interfaces de pare-feu sont toujours en mode Layer 3 (Couche 3) et le trafic est reçu et acheminé vers l'infrastructure ACI. Vous pouvez configurer des interfaces distinctes pour les connexions des consommateurs et fournisseurs ou une interface unique pour le trafic entrant et sortant. La procédure décrite dans ce document utilise une interface unique, car elle simplifie l'intégration. Vous n'avez pas besoin de configurer autant d'interfaces, d'adresses IP ou de VLAN. Toutefois, lorsque vous utilisez une interface unique, vous ne pouvez pas utiliser les informations sur la zone pour définir la politique de sécurité et vous devez modifier la politique intra-zone par défaut sur le pare-feu pour refuser le trafic.

Cette procédure déploie le pare-feu en mode one-arm. En mode one-arm, le trafic entre et sort du pare-feu via une interface unique. Cette interface de pare-feu commune est utilisée pour les interfaces des consommateurs et fournisseurs dans le modèle de graphique de service. L'utilisation d'une interface unique simplifie l'intégration avec le pare-feu en réduisant le nombre d'adresses IP, de VLAN et d'interfaces que vous devez configurer. Toutefois, le modèle de déploiement one-arm étant intra-zone, vous ne pouvez pas utiliser les informations sur la zone pour définir la politique de sécurité.

Sur le pare-feu :

- Création d'un routeur virtuel et d'une zone de sécurité

 ©2023 Palo Alto Networks, Inc.

- Configuration des interfaces réseau
- Configuration d'un itinéraire statique par défaut
- Création des objets d'adresse pour les EPG
- Création de règles de politique de sécurité

Sur le Cisco APIC :

- Création d'un domaine et d'un pool de VLAN
- Configuration d'une politique d'interface pour LLDP et LACP pour le trafic est-ouest
- Établissement de la connexion entre le pare-feu et l'infrastructure ACI
- Création d'un domaine de pont et d'une VRF
- Création d'un appareil L4-L7
- Création d'une redirection basée sur une politique
- Création et application d'un modèle de graphique de service

Création d'un routeur virtuel et d'une zone de sécurité

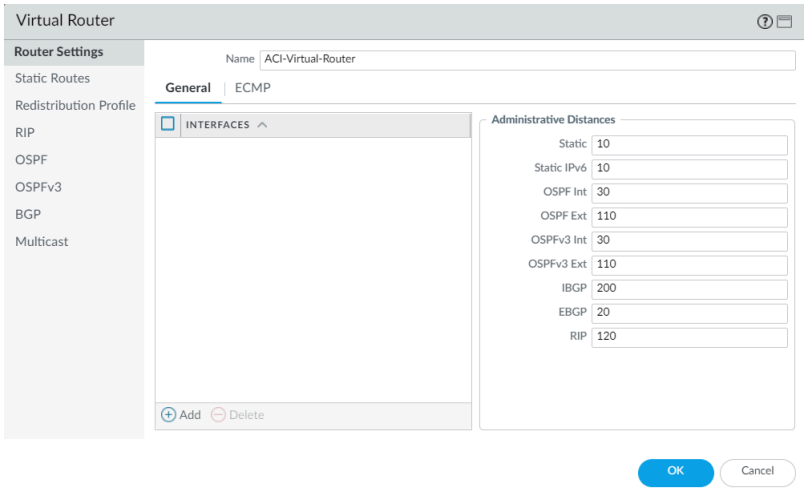
Configurez un routeur virtuel et une zone sur le pare-feu pour chaque VRF du locataire.

STEP 1 | Connectez-vous au pare-feu.

STEP 2 | Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, puis cliquez sur **Add (Ajouter)**.

STEP 3 | Donnez un **Name** (Nom) descriptif au routeur virtuel.

STEP 4 | Cliquez sur **OK**.



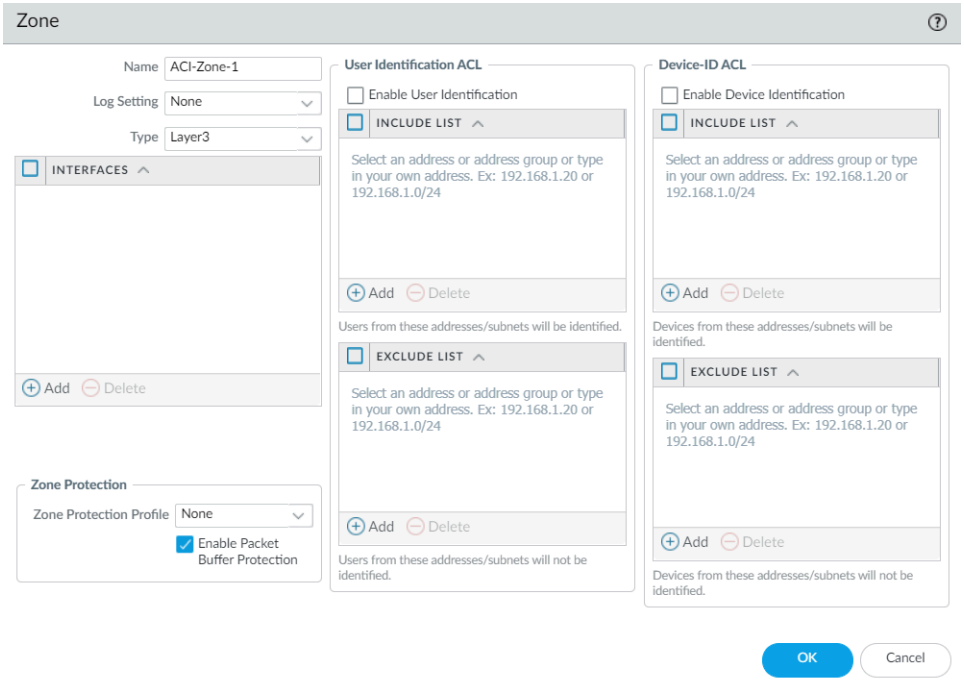
STEP 5 | Sélectionnez **Network (Réseau)** > **Zones**, puis cliquez sur **Add (Ajouter)**.

STEP 6 | Donnez un **Name** (Nom) descriptif à la zone.

STEP 7 | Choisissez Layer3 (Couche 3) dans la liste déroulante **Type**.

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Cliquez sur **OK**.



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

Configuration des interfaces réseau

Configurez les interfaces Ethernet qui connectent le pare-feu aux commutateurs feuilles ACI. Le numéro d'ID de VLAN utilisé dans cette configuration doit être un membre du pool de VLAN affecté aux pare-feu dans ACI.

Le pare-feu VM-Series ne prend pas en charge les groupes Ethernet agrégé.

STEP 1 | Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et cliquez sur **Add Aggregate Group (Ajouter un groupe agrégé)**.

STEP 2 | Saisissez un nombre pour le groupe agrégé dans le second champ **Interface Name** (Nom d'interface).

STEP 3 | Sélectionnez Layer 3 (Couche 3) dans la liste déroulante **Interface Type** (Type d'interface).

STEP 4 | Sélectionnez l'onglet **LACP** et cliquez sur **Enable LACP** (Activer LACP).

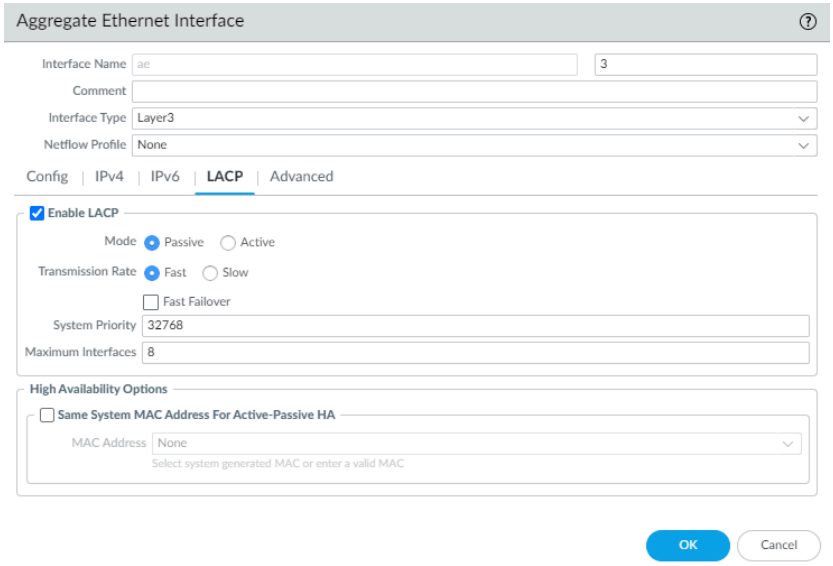
STEP 5 | Sélectionnez **Fast** (Rapide) comme **Transmission Rate** (Vitesse de transmission).

©2023 Palo Alto Networks, Inc.

STEP 6 | Dans High Availability Options (Options de haute disponibilité), cochez **Enable in HA Passive State** (Activer à l'état HA passive).

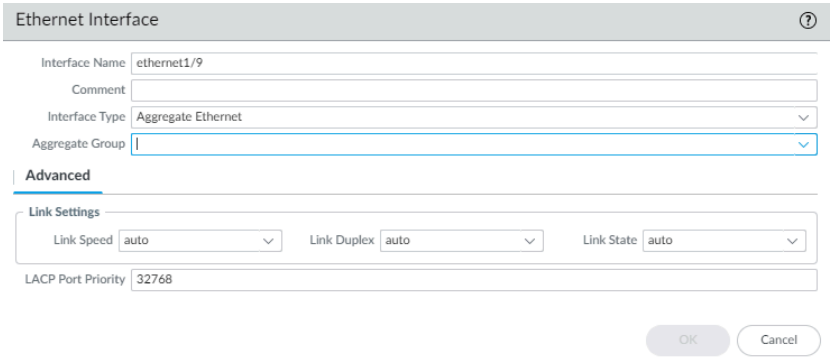
*Ne cochez pas **Same System MAC Address for Active-Passive HA** (Même adresse MAC système pour la HA active/passive). Cette option fait en sorte que la paire de pare-feu apparaisse comme un seul appareil pour le commutateur, de sorte que le trafic sera acheminé vers les deux pare-feu au lieu du seul pare-feu actif.*

STEP 7 | Cliquez sur **OK**.



STEP 8 | Cliquez sur le nom d'une interface Ethernet pour la configurer et l'ajouter au groupe agrégé.

1. Sélectionnez **Aggregate Ethernet** dans la liste déroulante Interface Type (Type d'interface).
2. Sélectionnez l'interface que vous avez définie dans la configuration du groupe Aggregate Ethernet.
3. Cliquez sur **OK**.
4. Répétez cette étape pour chaque autre interface membre du groupe Aggregate Ethernet.



 ©2023 Palo Alto Networks, Inc.

STEP 9 | Ajoutez une sous-interface sur l'interface Aggregate Ethernet pour le locataire et le VRF.

1. Sélectionnez la ligne de votre groupe Aggregate Ethernet et cliquez sur **Add Subinterface** (Ajouter une sous-interface).
2. Dans le second champ **Interface Name** (Nom d'interface), saisissez un suffixe numérique pour identifier la sous-interface.
3. Dans le champ **Tag** (Étiquette), saisissez l'étiquette VLAN de la sous-interface.
4. Sélectionnez le routeur virtuel que vous avez configuré précédemment dans la liste déroulante **Virtual Router** (Routeur virtuel).
5. Sélectionnez la zone que vous avez configurée précédemment dans la liste déroulante **Zone**.
6. Sélectionnez l'onglet **IPv4**.
7. Sélectionnez le type **Static** (Statique).
8. Cliquez sur **Add** (Ajouter) et saisissez l'adresse IP et le masque réseau de la sous-interface en notation CIDR.
9. Cliquez sur **OK**.

Configuration d'un itinéraire statique par défaut

Configurez un itinéraire statique par défaut pour diriger le trafic des sous-interfaces Ethernet vers le routeur de sous-réseau.

STEP 1 | Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel que vous avez précédemment créé dans cette procédure.

STEP 2 | Cliquez sur **Static Routes (Itinéraires statiques)** > **IPv4**, puis sur **Add (Ajouter)**.

STEP 3 | Saisissez un **Name (Nom)** descriptif.

STEP 4 | Saisissez 0.0.0.0/0 dans le champ **Destination**.

STEP 5 | Dans la liste déroulante **Interface**, sélectionnez le groupe Aggregate Ethernet que vous avez créé précédemment dans cette procédure.

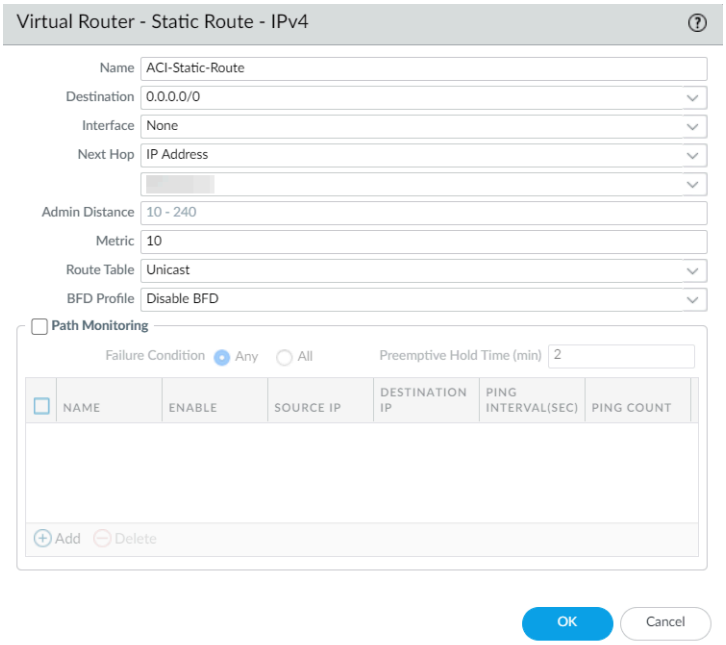
STEP 6 | Sélectionnez l'IP Address (Adresse IP) dans la liste déroulante **Next Hop (Saut suivant)** et saisissez l'adresse IP du routeur de saut suivant.

STEP 7 | Cliquez sur **OK**.

STEP 8 | Cliquez de nouveau sur **OK**.

©2023 Palo Alto Networks, Inc.

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



Création des objets d'adresse pour les EPG

Vous devez définir des objets d'adresse et les mapper sur des groupes de terminaux (EPG) à utiliser dans la politique de sécurité. Les groupes d'adresses constituent le meilleur moyen de mapper les groupes de sécurité sur un groupe de serveurs à l'aide d'une plage d'adresses IP de terminaux. Créez un objet d'adresse pour chacun de vos EPG.

STEP 1 | Sélectionnez **Objects (Objets)** > **Address (Adresse)**, puis cliquez sur **Add (Ajouter)**.

STEP 2 | Saisissez un nom descriptif pour votre objet d'adresse.

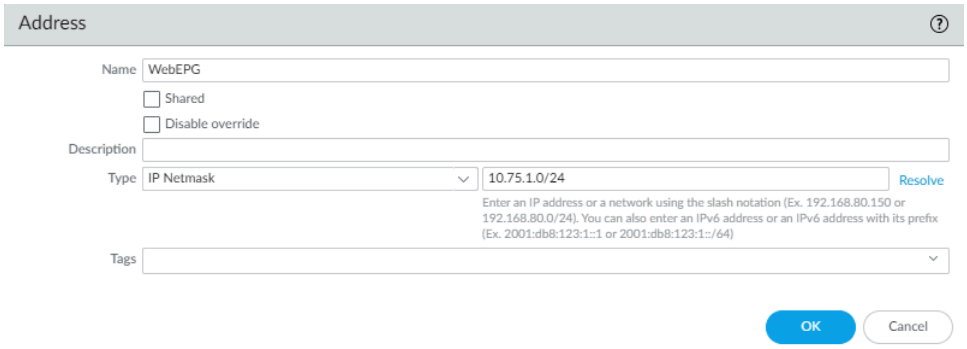
STEP 3 | Sélectionnez IP Netmask (Masque réseau IP) dans la liste déroulante **Type**.

STEP 4 | Saisissez le IP Netmask (Masque réseau IP).

STEP 5 | Cliquez sur **OK**.

STEP 6 | Répétez ce processus pour chaque EPG.

STEP 7 | **Commit (Validez)** vos modifications.



 ©2023 Palo Alto Networks, Inc.

Création de règles de politique de sécurité

Créez des règles de politique de sécurité pour contrôler le trafic entre vos EPG. Par défaut, le pare-feu autorise tout le trafic intra-zone. Par conséquent, étant donné que les EPG sont dans la même zone, tout est autorisé entre ces EPG. Avant de créer de nouvelles règles, vous devez faire passer la règle intra-zone par défaut de Allow (Autoriser) à Deny (Refuser).

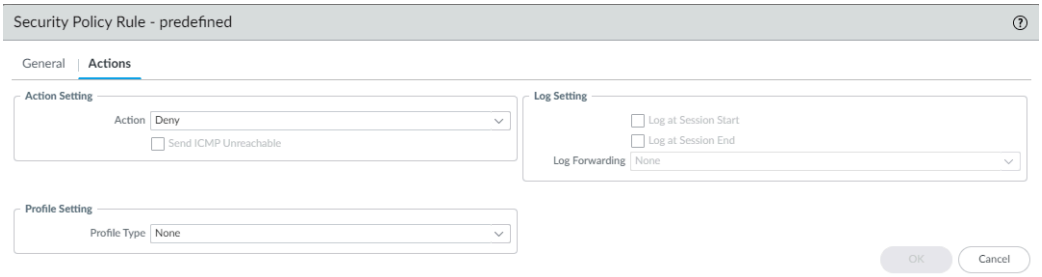
STEP 1 | Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.

STEP 2 | Cliquez sur intrazone-default pour mettre la ligne en surbrillance, puis cliquez sur **Override** (Remplacer).

STEP 3 | Sélectionnez l'onglet **Action**.

STEP 4 | Sélectionnez Deny (Refuser) dans la liste déroulante **Action**.

STEP 5 | Cliquez sur **OK**.



STEP 6 | Configurez des règles de politique de sécurité supplémentaires en fonction de vos besoins en utilisant les objets d'adresse et la zone que vous avez créés pour votre EPG.

Création d'un domaine et d'un pool de VLAN

Configurez le pool de VLAN qui sera utilisé pour allouer les VLAN au pare-feu lorsque vous associez des interfaces à l'infrastructure ACI pour les EPG. Le VLAN du pare-feu doit avoir une plage de VLAN statiques.

Configurez un domaine dédié pour le pare-feu. Un domaine pour le pare-feu est requis pour mapper les VLAN aux EPG. Créez un domaine physique pour un pare-feu physique et créez un domaine VMM pour un pare-feu VM-Series.

©2023 Palo Alto Networks, Inc.

STEP 1 | Créez un pool de VLAN.

1. Connectez-vous à votre APIC.
2. Sélectionnez **Fabric (Infrastructure)** > **Access Policies (Politiques d'accès)** > **Pools** > **VLAN**.
3. Faites un clic droit sur **VLAN** et sélectionnez **Create VLAN Pool** (Créer un pool de VLAN).
4. Saisissez un **Name** (Nom) descriptif pour votre pool de VLAN.
5. Sélectionnez **Dynamic Allocation** (Allocation dynamique) pour le mode d'allocation.
6. Cliquez sur le bouton plus (+) à droite de **Encap Blocks** (Blocs d'encap.).
7. Saisissez votre plage de VLAN dans le champ **VLAN Range** (Plage de VLAN).
8. Sélectionnez **Static Allocation** (Allocation statique) dans la liste déroulante Allocation Mode (Mode d'allocation).
9. Cliquez sur **OK**.
10. Cliquez sur **Submit (Envoyer)**.

STEP 2 | (Pare-feu physique uniquement) Créez un domaine physique.

1. Sélectionnez **Fabric (Infrastructure)** > **Access Policies (Politiques d'accès)** > **Physical and External Domains (Domaines physiques et externes)** > **Physical Domains (Domaines physique)**.
2. Faites un clic droit sur **Physical Domain** (Domaine physique) et sélectionnez **Create Physical Domain** (Créer un domaine physique).
3. Saisissez un **Name** (Nom) descriptif pour votre domaine physique.
4. Sélectionnez le pool de VLAN que vous avez créé lors de la procédure précédente dans la liste VLAN Pool (Pool de VLAN).
5. Cliquez sur **Submit (Envoyer)**.

©2023 Palo Alto Networks, Inc.

STEP 3 | (Pare-feu VM-Series uniquement) Créez un domaine VMM.

1. Sélectionnez **Virtual Networking (Mise en réseau virtuelle)** > **VMM Domains (Domaines VMM)** > **VMware**.
2. Faites un clic droit sur **VMware** et sélectionnez **Create vCenter Domain** (Créer un domaine vCenter).
3. Saisissez un **Name** (Nom) descriptif pour votre domaine VMM.
4. Sélectionnez **VMware vSphere Distributed Switch** (Commutateur distribué vSphere VMware) dans la liste déroulante **Virtual Switch** (Commutateur virtuel).
5. Sélectionnez **VLAN** dans la liste déroulante **Encapsulation**.
6. Sélectionnez votre pool de VLAN dans la liste déroulante **VLAN Pool** (Pool de VLAN).
7. Cliquez sur le bouton plus (+) à droite de **vCenter Credentials** (Informations d'identification vCenter).
8. Saisissez un **Profile Name** (Nom de profil) descriptif et vos informations de connexion vCenter.
9. Cliquez sur le bouton plus (+) à droite de **vCenter**.
10. Saisissez un **Name (Nom)** descriptif.
11. Sélectionnez vCenter dans la liste déroulante Type.
12. Saisissez votre adresse IP vCenter dans **IP/Hostname**.
13. Sélectionnez le profil vCenter Credentials (Informations d'identification vCenter) que vous venez de créer dans la liste déroulante **Associated Credential** (Informations d'identification associées).
14. Cliquez sur **Submit (Envoyer)**.

Configuration d'une politique d'interface pour LLDP et LACP pour le trafic est-ouest

Créez une politique qui active LLDP et LACP sur les interfaces ACI qui se connectent à votre pare-feu.

LLDP est nécessaire pour que le transfert fonctionne correctement dans l'environnement ACI. ACI ne déploie aucune interface de routeur de sous-réseau sur un commutateur feuille, à moins qu'il ne détecte un terminal final sur le commutateur qui en nécessite une. LLDP aide à déterminer si une interface de routeur de sous-réseau est requise.

LACP offre une résilience et une vitesse de récupération supérieures en cas d'échec d'une liaison.

STEP 1 | Créez une politique d'interface LLDP.

1. Sélectionnez **Fabric (Infrastructure)** > **Access Policies (Politiques d'accès)** > **Interface Policies (Politiques d'interface)** > **Policies (Politiques)** > **LLDP Interface (Interfaces LLDP)**.
2. Faites un clic droit sur **LLDP Interface** (Interface LLDP) et sélectionnez **Create LLDP Interface Policy** (Créer une politique d'interface LLDP).
3. Saisissez un **Name** (Nom) descriptif pour votre politique d'interface LLDP.
4. Sélectionnez **Enabled** (Activé) pour **Receive State** (État de réception).
5. Sélectionnez **Enabled** (Activé) pour **Transmit State** (État de transmission).
6. Cliquez sur **Submit (Envoyer)**.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Créez une politique de canal de port pour activer LACP.

1. Sélectionnez **Fabric (Infrastructure)** > **Access Policies (Politiques d'accès)** > **Interface Policies (Politiques d'interface)** > **Policies (Politiques)** > **Port Channel (Canal de port)**.
2. Faites un clic droit sur **Port Channel** (Canal de port) et sélectionnez **Create Port Channel Policy** (Créer une politique de canal de port).
3. Saisissez un **Name** (Nom) descriptif pour votre politique de canal de port.
4. Sélectionnez **LACP Active** (LACP actif) dans la liste déroulante **Mode**.
5. Cliquez sur **Submit (Envoyer)**.

Établissement de la connexion entre le pare-feu et l'infrastructure ACI

Connectez votre pare-feu au commutateur feuille via une connexion VPC à l'aide de l'interface Ethernet (ou du groupe Aggregate Ethernet) que vous avez configurée sur votre pare-feu précédemment au cours de cette procédure. Connectez l'interface ou les interfaces aux mêmes ports des commutateurs feuilles.

STEP 1 | Sélectionnez **Fabric (Infrastructure)** > **Access Policies (Politiques d'accès)** > **Quick Start (Démarrage rapide)**.

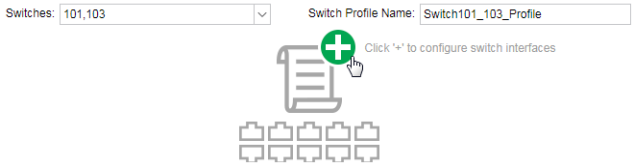
STEP 2 | Cliquez sur **Configure an interface, PC, and VPC (Configurer une interface, un PC et un VPC)**.

STEP 3 | Cliquez sur le plus (+) vert et blanc.



STEP 4 | Sélectionnez le ou les commutateurs feuilles auxquels le pare-feu est connecté à partir de la liste déroulante **Switches (Commutateurs)**.

STEP 5 | Cliquez sur le plus (+) vert et blanc.



STEP 6 | Sélectionnez VPC comme **Interface Type (Type d'interface)**.

STEP 7 | Dans le champ **Interfaces**, saisissez le numéro de l'interface que votre pare-feu utilise pour se connecter au commutateur feuille.

STEP 8 | Saisissez un nom descriptif dans le champ **Interface Selector Name (Nom du sélecteur d'interface)**.

STEP 9 | Sélectionnez **LLDP-Enabled (Activation par LLDP)** dans la liste déroulante **LLDP Policy (Politique LLDP)**.

STEP 10 | Sélectionnez **LACP Active (LACP actif)** dans la liste déroulante **Port Channel Policy (Politique de canal de port)**.

 ©2023 Palo Alto Networks, Inc.

STEP 11 | Sélectionnez **Bare Metal (Sans système d'exploitation)** pour un pare-feu physique ou **ESX Hosts (Hôtes ESX)** pour le VM-Series dans la liste déroulante **Attached Device Type (Type d'appareil connecté)**.

STEP 12 | Sélectionnez **Choose One (En choisir un)** pour **Domain (Domaine)**.

STEP 13 | Sélectionnez le domaine physique ou le domaine VMM que vous avez créé précédemment dans cette procédure dans la liste déroulante **Domain (Domaine)**.

STEP 14 | Cliquez sur **Save (Enregistrer)**.

STEP 15 | Cliquez sur **Save (Enregistrer)**, puis sur **Submit (Envoyer)**.

STEP 16 | Répétez cette procédure pour le deuxième pare-feu de votre paire HA.

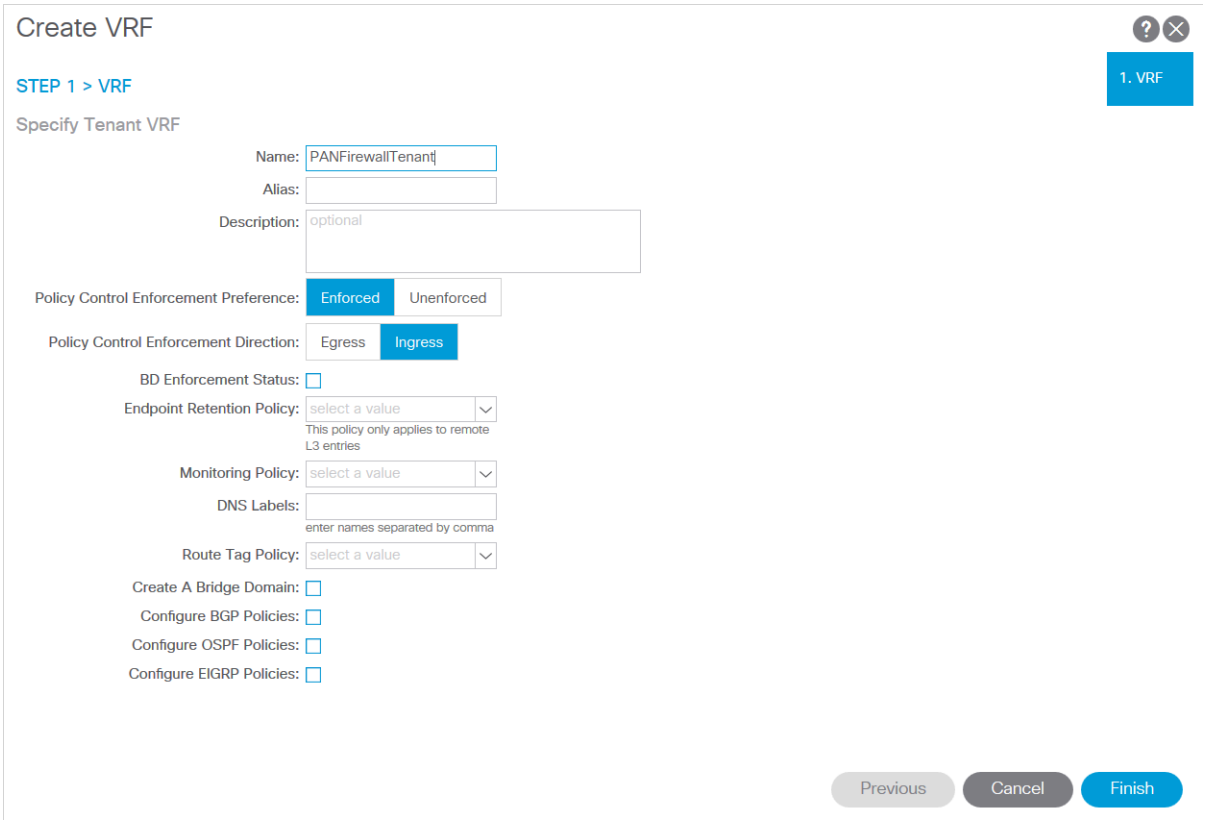
Création d'un domaine de pont et d'une VRF

Un locataire nécessite une VRF pour tous les sous-réseaux et domaines de pont. Dans cet exemple, vous allez créer une seule VRF commune pour le pare-feu et les terminaux. Configurez ensuite un domaine de pont dédié pour votre pare-feu et désactivez l'apprentissage du dataplane. La désactivation de l'apprentissage du dataplane est nécessaire pour utiliser la redirection basée sur une politique dans un domaine de pont.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Créez une VRF.

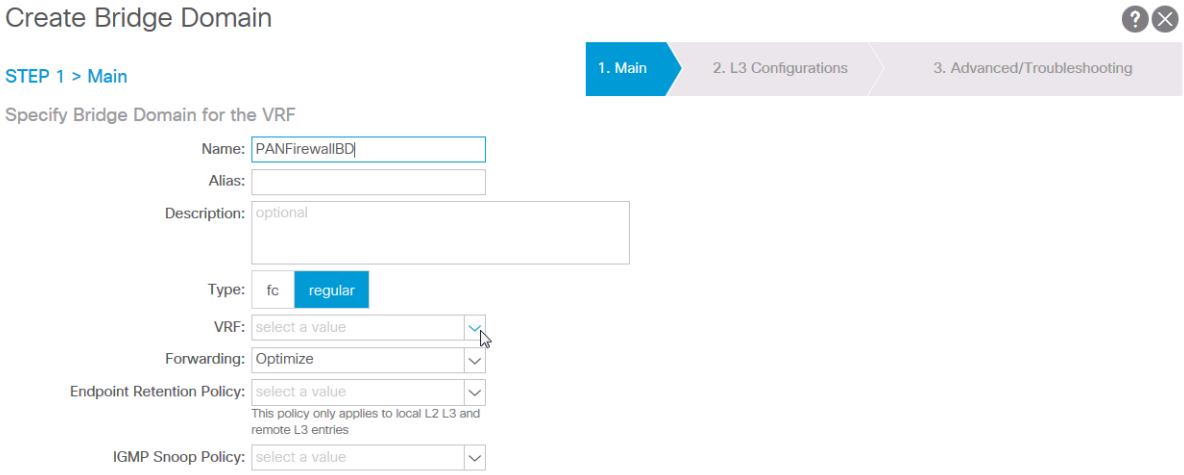
1. Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire.
2. Sélectionnez **Networking (Mise en réseau)** > **VRFs**.
3. Faites un clic droit sur **VRFs** et sélectionnez **Create VRF** (Créer une VRF).
4. Saisissez un **Name** (Nom) descriptif pour votre VRF.
5. Décochez la case **Create A Bridge Domain** (Créer un domaine de pont).
6. Cliquez sur **Finish (Terminer)**.



 ©2023 Palo Alto Networks, Inc.

STEP 2 | Créez un domaine de pont pour le pare-feu.

1. Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire.
2. Sélectionnez **Networking (Mise en réseau)** > **Bridge Domains (Domaines de pont)**.
3. Faites un clic droit sur **Bridge Domains** (Domaines de pont) et sélectionnez **Create Bridge Domain** (Créer un domaine de pont).
4. Saisissez un **Name** (Nom) descriptif pour votre domaine de pont.
5. Sélectionnez le VRF que vous avez créé lors de la procédure précédente dans la liste déroulante **VRF**.
6. Cliquez sur **Next (Suivant)**.



Création d'un appareil L4-L7

Vous devez définir le pare-feu en tant qu'appareil L4-L7 dans l'APIC afin qu'ACI puisse l'insérer dans le flux de trafic. Vous configurez les appareils L4-L7 dans l'APIC en tant que cluster d'appareils, qui est une construction qui représente un seul pare-feu ou une paire HA de pare-feu, agissant comme un seul appareil. Les clusters d'appareils ont une ou plusieurs interfaces logiques, qui définissent le chemin d'accès des pare-feu membres avec un VLAN du domaine physique.

STEP 1 | Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire.

STEP 2 | Sélectionnez **Services** > **L4-L7** > **Devices (Appareils)**.

STEP 3 | Faites un clic droit sur **Devices** (Appareils) et sélectionnez **Create L4-L7 Device (Créer un appareil L4-L7)**.

STEP 4 | Décochez la case **Managed** (Géré).

STEP 5 | Saisissez un **Name** (Nom) descriptif pour votre appareil L4-L7.

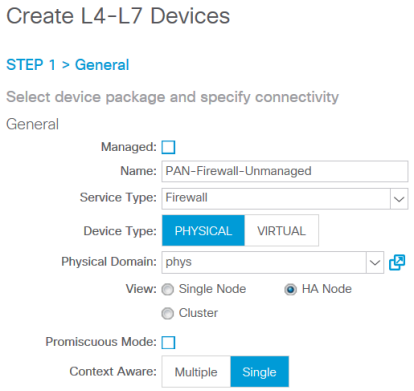
STEP 6 | Sélectionnez **Firewall** (Pare-feu) dans la liste déroulante **Service Type** (Type de service).

STEP 7 | Sélectionnez **Physical** (Physique) pour un pare-feu physique ou **Virtual** (Virtuel) pour un pare-feu VM-Series dans la liste déroulante **Device Type** (Type d'appareil).

STEP 8 | Sélectionnez le domaine physique ou VMM que vous avez créé précédemment dans la liste déroulante **Domain** (Domaine).

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Sélectionnez HA Node (Nœud HA) pour **View** (Affichage).



STEP 10 | Sous **Device 1** (Appareil 1), cliquez sur l'icône du plus (+) à droite de **Device Interfaces** (Interfaces d'appareil).

STEP 11 | Saisissez un **Name** (Nom) descriptif pour cette interface.

STEP 12 | Sous **Path** (Chemin d'accès), sélectionnez le chemin d'accès au pare-feu principal de votre paire HA.

STEP 13 | Cliquez sur **Update (Mettre à jour)**.

STEP 14 | Sous **Device 2** (Appareil 2), cliquez sur l'icône du plus (+) à droite de **Device Interfaces** (Interfaces d'appareil).

STEP 15 | Saisissez un **Name** (Nom) descriptif pour cette interface.

STEP 16 | Sous **Path** (Chemin d'accès), sélectionnez le chemin d'accès au pare-feu secondaire de votre paire HA.

STEP 17 | Cliquez sur **Update (Mettre à jour)**.

STEP 18 | Sous **Cluster**, cliquez sur l'icône du plus (+) à droite de **Cluster Interfaces** (Interfaces de cluster).

STEP 19 | Saisissez un **Name** (Nom) descriptif pour le cluster.

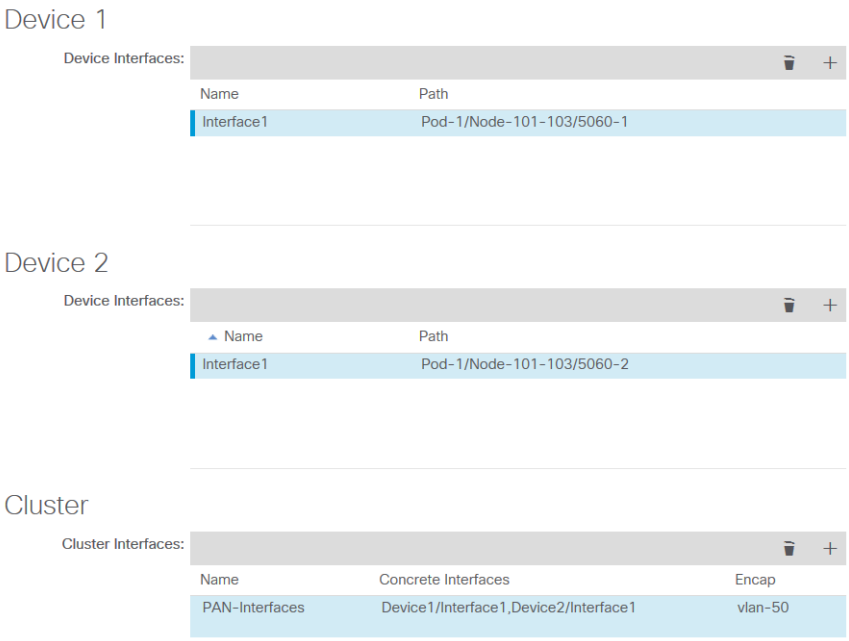
STEP 20 | Sélectionnez les deux interfaces que vous avez configurées ci-dessus dans la liste sous **Concrete Interfaces** (Interfaces concrètes). L'APIC nécessite la configuration de deux interfaces. Cependant, comme il n'y a qu'une seule connexion entre le pare-feu et l'infrastructure ACI, une seule des interfaces est utilisée.

STEP 21 | Sous **Encap**, saisissez un VLAN à partir du pool de VLAN statiques que vous avez créé précédemment. Le trafic sera redirigé vers le pare-feu sur le VLAN assigné ici.

STEP 22 | Cliquez sur **Update (Mettre à jour)**.

 ©2023 Palo Alto Networks, Inc.

STEP 23 | Cliquez sur **Finish (Terminer)**.



Création d'une redirection basée sur une politique

Configurez la redirection basée sur une politique qui envoie le trafic de vos EPG au pare-feu. La redirection basée sur une politique exploite l'adresse MAC de l'interface sur le pare-feu. Avant de configurer le paramètre PBR sur l'APIC, vous devez obtenir l'adresse MAC du pare-feu.

STEP 1 | Obtenez l'adresse MAC du pare-feu.

1. Connectez-vous à la CLI du pare-feu.
2. Utilisez **`command show interface all`** pour afficher les adresses MAC de vos interfaces configurées.
3. Copiez l'adresse MAC de l'interface qui recevra le trafic redirigé.

©2023 Palo Alto Networks, Inc.

STEP 2 | Créez la redirection basée sur une politique L4-L7.

1. Connectez-vous à l'APIC.
2. Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire.
3. Sélectionnez **Policies (Politiques)** > **Protocol (Protocole)** > **L4-L7 Policy Based Redirect (Redirection basée sur une politique L4-L7)**.
4. Faites un clic droit sur **L4-L7 Policy Based Redirect** (Redirection basée sur une politique) et sélectionnez **Create L4-L7 Policy Based Redirect** (Créer une redirection basée sur une politique L4-L7).
5. Saisissez un **Name** (Nom) descriptif pour votre redirection basée sur une politique.
6. Cliquez sur l'icône du plus (+) à droite de **Destinations**.
7. Dans le champ **IP**, saisissez l'adresse IP de l'interface qui recevra le trafic redirigé.
8. Dans le champ **MAC**, saisissez l'adresse MAC que vous avez copiée à partir de la CLI du pare-feu.
9. Cliquez sur **OK**.
10. Cliquez sur **Submit (Envoyer)**.

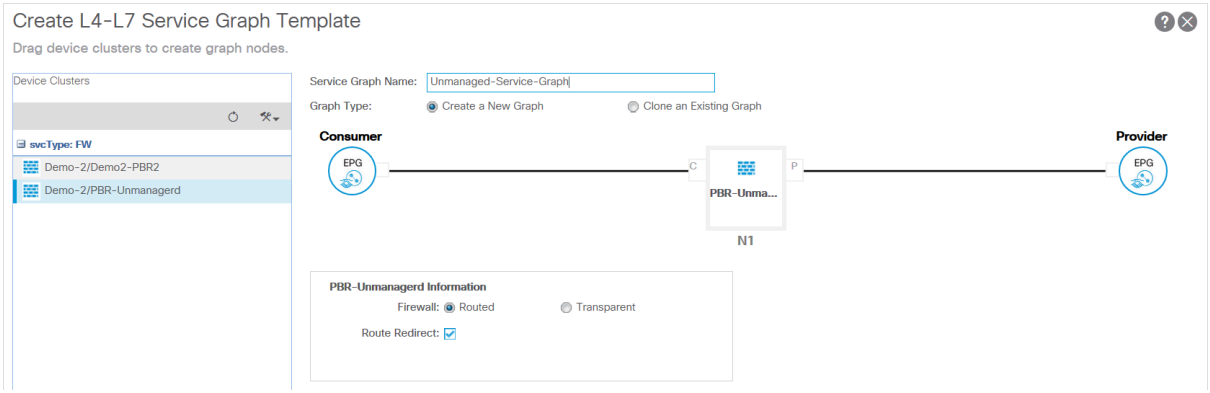
Création et application d'un modèle de graphique de service

Créez un modèle de graphique de service qui utilise le cluster d'appareils représentant le pare-feu dans une intégration de redirection basée sur une politique. Après avoir créé le graphique de service, vous devez l'appliquer aux EPG pour protéger le trafic. Un contrat et des règles de filtre de contrat définissent le trafic pouvant être transféré au pare-feu.

©2023 Palo Alto Networks, Inc.

STEP 1 | Créez un modèle de graphique de service.

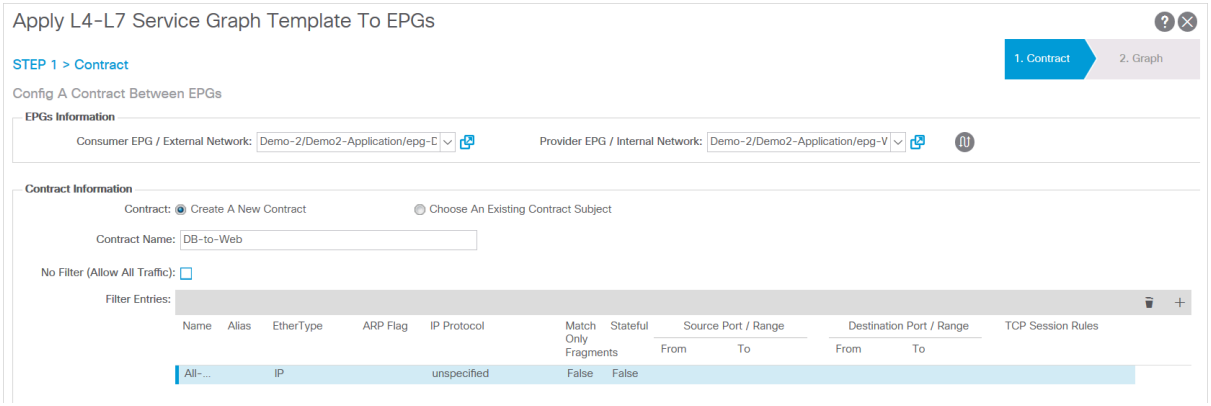
1. Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire.
2. Sélectionnez **Services** > **L4-L7** > **L4-L7 Service Graph Templates (Modèles de graphique de service L4-L7)**.
3. Faites un clic droit sur **L4-L7 Service Graph Template** (Modèle de graphique de service L4-L7) et sélectionnez **Create L4-L7 Service Graph Template** (Créer un modèle de graphique de service L4-L7).
4. Saisissez un **Graph Name** (Nom du graphique) descriptif pour votre modèle de graphique de service.
5. Sélectionnez **Create a New One** (Créer un nouveau) pour **Graph Type** (Type de graphique).
6. Cliquez et faites glisser l'appareil L4-L7 que vous avez créé lors de la procédure précédente entre les EPG des consommateurs et fournisseurs.
7. Sélectionnez **Routed** (Acheminé) pour **Firewall** (Pare-feu).
8. Sélectionnez **Routed Redirect** (Redirection acheminée).
9. Cliquez sur **Submit (Envoyer)**.



 ©2023 Palo Alto Networks, Inc.

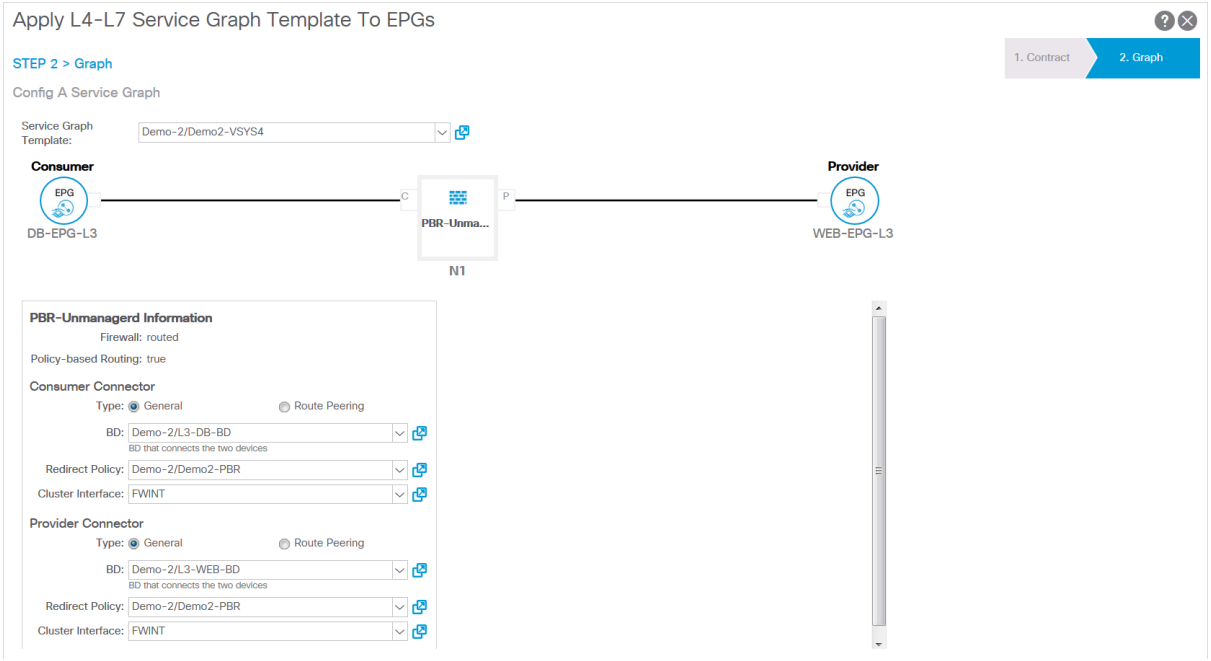
STEP 2 | Appliquez le modèle de graphique de service.

1. Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire.
2. Sélectionnez **Services** > **L4-L7**.
3. Dans le panneau **EPGs Information** (Informations sur les EPG), sélectionnez vos EPG de consommateurs et de fournisseurs dans les listes déroulantes **Consumer EPG** (EPG de consommateurs) et **Provider EPG** (EPG de fournisseurs).
4. Sélectionnez **Create a New Contract** (Créer un nouveau contrat).
5. Saisissez un **Contract Name** (Nom de contrat) descriptif.
6. Décochez la case No Filter **(Allow All Traffic)** (Aucun Filtre (Autoriser tout le trafic)). L'utilisation de cette option n'est pas recommandée. Pour permettre à tout le trafic entre les EPG d'être redirigé vers le pare-feu, il est recommandé de créer un filtre.
7. Cliquez sur l'icône du plus (+) à droite de **Filter Entries** (Filtrer les entrées).
8. Créez une règle (ou des règles) pour définir le trafic autorisé à passer entre les EPG et redirigé vers le pare-feu.
9. Cliquez sur **Next (Suivant)**.



10. Sélectionnez le modèle de graphique de service que vous avez créé lors de la procédure précédente dans la liste déroulante **Service Graph Template** (Modèle de graphique de service).
11. Dans le panneau Consumer (Consommateur) et Provider (Fournisseur), sélectionnez le domaine de pont contenant votre pare-feu dans la liste déroulante **BD**.
12. Sélectionnez la redirection basée sur la politique que vous avez créée précédemment dans les listes déroulantes **Redirect Policy** (Politique de redirection).
13. Sélectionnez l'interface de cluster que vous avez créée avec votre appareil L4-L7 dans les listes déroulantes **Cluster Interface** (Interface de cluster).

©2023 Palo Alto Networks, Inc.



Déploiement du pare-feu pour sécuriser le trafic nord-sud en mode politique réseau

Utilisez le mode politique réseau pour sécuriser le trafic nord-sud entrant et sortant de votre centre de données à l'aide du mode non géré avec une redirection basée sur une politique. Cette procédure suppose que vous avez effectué les tâches suivantes :

- Les pare-feu sont opérationnels et connectés à un commutateur feuille dans votre environnement Cisco ACI. De plus, l'interface de gestion de chaque pare-feu doit être accessible par l'APIC.
- Les pare-feu sont déployés en mode HA active/passive. Cette procédure ne couvre pas la configuration réseau HA et suppose que vous l'avez déjà effectuée.

Pour établir une connectivité externe vers des réseaux extérieurs à votre infrastructure ACI, vous devez configurer un L3Out. Et L3Out est une politique dédiée contenant les paramètres requis pour connecter des appareils de routage externes à un locataire. De plus, un L3Out contient un EPG externe (appelé réseau externe dans l'interface utilisateur de l'APIC) qui représente les réseaux accessibles via le L3Out. L'EPG externe n'est pas rempli dynamiquement et suit un modèle de confiance zéro, vous devez donc définir les réseaux dans l'EPG. Pour faciliter la configuration, vous pouvez configurer un réseau de 0.0.0.0/0 pour affecter tous les réseaux à l'EPG externe.

Pour sécuriser le trafic entrant, connectez votre pare-feu ou vos pare-feu d'une paire HA à vos commutateurs feuilles limite. Les commutateurs feuilles limite sont des commutateurs feuilles qui fournissent des connexions de couche 3 à des routeurs externes. Les pare-feu s'apparient avec les commutateurs feuilles limite à l'aide du protocole OSPF (ouverture du chemin le plus court en premier) configuré sur chaque commutateur feuille de la paire de VPC et communique avec les pare-feu à l'aide d'une interface de commutateur virtuel (SVI). Sur le pare-feu, vous configurez un routeur virtuel dédié aux interfaces qui se connectent à votre centre de données. De plus, cette procédure comprend

Pour le trafic sortant, le pare-feu annonce les réseaux externes aux commutateurs feuilles limite à l'aide du protocole OSPF. De plus, l'EPG de réseau externe est configuré pour autoriser tous les

©2023 Palo Alto Networks, Inc.

réseaux annoncés par le pare-feu dans cet EPG. Vous créez un contrat entre un objet géré vzAny et l'EPG de réseaux externes pour permettre au trafic provenant de tout EPG de la VRF d'atteindre les réseaux externes via le pare-feu. L'objet géré vzAny vous permet de consolider tous les EPG d'une VRF en un ou plusieurs contrats au lieu de créer un contrat distinct pour chaque EPG. Les EPG collectés dans l'objet géré vzAny consomment le contrat fourni par l'EPG externe.

Contrairement au mode gestionnaire de service, la gestion dans l'infrastructure ACI et les pare-feu est effectuée séparément.

Sur l'APIC :

- Création d'un domaine routé externe et d'un pool de VLAN
- Configuration d'une politique d'interface pour LLDP et LACP pour le trafic nord-sud
- Création d'un réseau acheminé externe
- Configuration des sous-réseaux pour publier sur le pare-feu externe
- Création d'un contrat sortant
- Création d'un contrat Web entrant
- Application des contrats sortants et entrants aux EPG

Sur le pare-feu :

- Création d'un routeur virtuel et d'une zone de sécurité pour le trafic nord-sud
- Configuration des interfaces réseau
- Configuration de la redistribution des itinéraires et OSPF
- Configuration de NAT pour les connexions externes

Création d'un domaine routé externe et d'un pool de VLAN

Créez un pool de VLAN pour allouer les VLAN au pare-feu lorsque vous associez des interfaces à l'infrastructure afin de prendre en charge les EPG de votre infrastructure ACI. Vous devez utiliser une plage de VLAN statiques pour le pare-feu.

De plus, vous devez créer un domaine physique pour mapper les VLAN aux EPG. La procédure suivante crée un domaine physique dédié au pare-feu.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Créez un pool de VLAN.

1. Connectez-vous à votre APIC.
2. Sélectionnez **Fabric (Infrastructure)** > **Access Policies (Politiques d'accès)** > **Pools** > **VLAN**.
3. Faites un clic droit sur **VLAN** et sélectionnez **Create VLAN Pool** (Créer un pool de VLAN).
4. Saisissez un **Name** (Nom) descriptif pour votre pool de VLAN.
5. Sélectionnez **Dynamic Allocation** (Allocation dynamique) pour le mode d'allocation.
6. Cliquez sur le bouton plus (+) à droite de **Encap Blocks** (Blocs d'encap.).
7. Saisissez votre plage de VLAN dans le champ **VLAN Range** (Plage de VLAN).
8. Sélectionnez **Static Allocation** (Allocation statique) dans la liste déroulante Allocation Mode (Mode d'allocation).
9. Cliquez sur **OK**.
10. Cliquez sur **Submit (Envoyer)**.

STEP 2 | Créez un domaine routé externe.

1. Sélectionnez **Fabric (Infrastructure)** > **Access Policies (Politiques d'accès)** > **Physical and External Domains (Domaines physiques et externes)** > **External Domains (Domaines externes)**.
2. Faites un clic droit sur **External Routed Domain** (Domaine routé externe) et sélectionnez **Create Layer 3 Domain** (Créer un domaine de couche 3).
3. Saisissez un **Name** (Nom) descriptif pour votre domaine physique.
4. Sélectionnez le pool de VLAN que vous avez créé lors de la procédure précédente dans la liste VLAN Pool (Pool de VLAN).
5. Cliquez sur **Submit (Envoyer)**.

Configuration d'une politique d'interface pour LLDP et LACP pour le trafic nord-sud

Créez une politique qui active LLDP et LACP sur les interfaces ACI qui se connectent à votre pare-feu.

LLDP est nécessaire pour que le transfert fonctionne correctement dans l'environnement ACI. ACI ne déploie aucune interface de routeur de sous-réseau sur un commutateur feuille, à moins qu'il ne détecte un terminal final sur le commutateur qui en nécessite une. LLDP aide à déterminer si une interface de routeur de sous-réseau est requise.

LACP offre une résilience et une vitesse de récupération supérieures en cas d'échec d'une liaison.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Créez une politique d'interface LLDP.

1. Sélectionnez **Fabric (Infrastructure)** > **Access Policies (Politiques d'accès)** > **Interface Policies (Politiques d'interface)** > **Policies (Politiques)** > **LLDP Interface (Interfaces LLDP)**.
2. Faites un clic droit sur **LLDP Interface** (Interface LLDP) et sélectionnez **Create LLDP Interface Policy** (Créer une politique d'interface LLDP).
3. Saisissez un **Name** (Nom) descriptif pour votre politique d'interface LLDP.
4. Sélectionnez **Enabled** (Activé) pour **Receive State** (État de réception).
5. Sélectionnez **Enabled** (Activé) pour **Transmit State** (État de transmission).
6. Cliquez sur **Submit (Envoyer)**.

STEP 2 | Créez une politique de canal de port pour activer LACP.

1. Sélectionnez **Fabric (Infrastructure)** > **Access Policies (Politiques d'accès)** > **Interface Policies (Politiques d'interface)** > **Policies (Politiques)** > **Port Channel (Canal de port)**.
2. Faites un clic droit sur **Port Channel** (Canal de port) et sélectionnez **Create Port Channel Policy** (Créer une politique de canal de port).
3. Saisissez un **Name** (Nom) descriptif pour votre politique de canal de port.
4. Sélectionnez **LACP Active** (LACP actif) dans la liste déroulante **Mode**.
5. Cliquez sur **Submit (Envoyer)**.

Création d'un réseau acheminé externe

Les pare-feu transmettent les informations de routage IP à l'ACI sur un réseau OSPF de couche 3. ACI utilise une interface de commutateur virtuel (SVI) sur les commutateurs feuilles avec une adresse IP sur chaque commutateur pour la résilience de la connexion. Créez un réseau acheminé de couche 3 à apparier avec le pare-feu à l'aide d'OSPF.

STEP 1 | Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire.

STEP 2 | Sélectionnez **Networking (Mise en réseau)** > **External Routed Networks (Réseaux acheminés externes)**.

STEP 3 | Faites un clic droit sur **External Routed Networks (Réseaux routés externes)** et sélectionnez **Create Routed Outside (Créer routé extérieur)**.

STEP 4 | Saisissez un **Name** (Nom) descriptif pour votre **Routed Network** (Réseau acheminé).

STEP 5 | Sélectionnez votre VRF avec une connectivité externe dans la liste déroulante **VRF**.

STEP 6 | Sélectionnez le domaine routé externe que vous avez créé précédemment dans la liste déroulante **External Routed Domain** (Domaine routé externe).

STEP 7 | Sélectionnez **OSPF**.

STEP 8 | Saisissez un **OSPF Area ID** (ID de zone OSPF). L'Area ID (Identifiant de zone) peut être exprimé en nombre décimal ou sous forme décimale séparée par un point. Par exemple, Area 1 (Zone 1) est identique à la Area 0.0.0.1 (Zone 0.0.0.1) ou Area 271 (Zone 271) est identique à la Area 0.0.1.15 (Zone 0.0.1.15). La plage d'Area ID (ID de zone) est comprise entre 0 (0.0.0.0) et 4294967295 (255.255.255.255).

 ©2023 Palo Alto Networks, Inc.

STEP 9 | Sélectionnez **Regular Area** (Zone régulière) pour le **OSPF Area Type** (Type de zone OSPF).

STEP 10 | Cliquez sur le bouton plus (+) à droite de **Nodes and Interface Profiles** (Profils d'interface et nœud) pour créer un profil de nœud avec un nœud destiné aux commutateurs feuilles limite qui se connectent au pare-feu.

STEP 11 | Saisissez un **Name** (Nom) descriptif pour votre **Node Profile** (Profil de nœud).

STEP 12 | Associez des nœuds à votre Node Profile (Profil de nœud).

1. Cliquez sur le bouton plus (+) à droite de **Nodes** (Nœuds). Cela ouvre la fenêtre **Select Node** (Sélectionner un nœud).
2. Sélectionnez le nœud auquel votre pare-feu est connecté dans la liste déroulante **Node ID** (ID de nœud).
3. Saisissez l'adresse IP du routeur connecté au commutateur feuille dans **Router ID** (ID de routeur).
4. Cliquez sur **OK**.
5. Cliquez sur le bouton plus (+) à droite de **Nodes and Interface Profiles** (Nœuds et profils d'interface).
6. Saisissez un **Name** (Nom) descriptif pour votre **Node Profile** (Profil de nœud).
7. Cliquez sur le bouton plus (+) à droite de **Nodes** (Nœuds). Cela ouvre la fenêtre **Select Node** (Sélectionner un nœud).
8. Sélectionnez le nœud auquel votre pare-feu HA secondaire est connecté dans la liste déroulante **Node ID** (ID de nœud).
9. Saisissez l'adresse IP du routeur connecté au second commutateur feuille dans **Router ID** (ID de routeur).
10. Cliquez sur **OK**.

 ©2023 Palo Alto Networks, Inc.

STEP 13 | Connectez un profil d'interface OSPF pour votre profil de nœud.

1. Saisissez un **Name** (Nom) descriptif pour votre profil d'interface OSPF.
2. Cliquez sur **Next (Suivant)**.
3. Sélectionnez **Create OSPF Interface Policy** (Créer une stratégie d'interface OSPF) dans la liste déroulante OSPF Policy (Politique OSPF).
4. Saisissez un **Name** (Nom) descriptif pour votre politique d'interface OSPF.
5. Sélectionnez **MTU Ignorer** (Ignorer MTU).
6. Cliquez sur **Submit (Envoyer)**.
7. Cliquez sur **Next (Suivant)**.
8. Cliquez sur **SVI**.
9. Cliquez sur le bouton plus (+) à droite de **SVI Interfaces** (Interfaces SVI). Cela ouvre la fenêtre **Select SVI** (Sélectionner SVI).
10. Cliquez sur **Virtual Port Channel** (Canal de port virtuel).
11. Sélectionnez le Path (Chemin d'accès) au port et à l'interface de canal de port où le pare-feu se connecte au commutateur feuille.
12. Dans **Encap**, saisissez l'encapsulation VLAN utilisée pour votre profil extérieur de couche 3.
13. Sélectionnez **Trunk** (Tronc) pour Mode.
14. Dans le champ **Side A IPv4 Primary Address** (Adresse principale IPv4 côté A), saisissez l'adresse IP principale du chemin d'accès associé au profil extérieur de couche 3.
15. Dans le champ **Side B IPv4 Primary Address** (Adresse principale IPv4 côté B), saisissez l'adresse IP secondaire du chemin d'accès associé au profil extérieur de couche 3.
16. Cliquez sur **OK**.

STEP 14 | Cliquez sur **OK** pour fermer la fenêtre Create Interface Profile (Créer un profil d'interface).

STEP 15 | Cliquez sur **OK** pour fermer la fenêtre Create Node Profile (Créer un profil de nœud).

STEP 16 | Cliquez sur **Next (Suivant)**.

STEP 17 | Cliquez sur le bouton plus (+) à droite de **External EPG Networks** (Réseaux EPG externes). Cela ouvre la fenêtre **Create Routed Outside** (Créer un réseau extérieur acheminé).

STEP 18 | Saisissez un **Name** (Nom) descriptif pour votre External Network (Réseau externe).

STEP 19 | Ajoutez un sous-réseau à votre réseau externe.

1. Cliquez sur le bouton plus (+) à droite de **Subnets** (Sous-réseaux).
2. Saisissez l'adresse IP et le masque de la passerelle par défaut du sous-réseau.
3. Sélectionnez **Export Route Route Subnet** (Exporter le sous-réseau de contrôle d'itinéraires).
4. Sélectionnez **External Subnets for External EPG** (Sous-réseaux externes pour EPG externe).
5. Cliquez sur **OK**.

STEP 20 | Cliquez sur **Finish (Terminer)**.

 ©2023 Palo Alto Networks, Inc.

Configuration des sous-réseaux pour publier sur le pare-feu externe

Par défaut, les sous-réseaux de l'infrastructure ACI ne sont pas annoncés aux réseaux externes. Vous devez configurer les sous-réseaux pour qu'ils soient publiés en externe.

STEP 1 | Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire.

STEP 2 | Sélectionnez **Networking (Mise en réseau)** > **Bridge Domains (Domaines de pont)** > **<your bridge domain>**.

STEP 3 | Cliquez sur **L3 Configurations**.

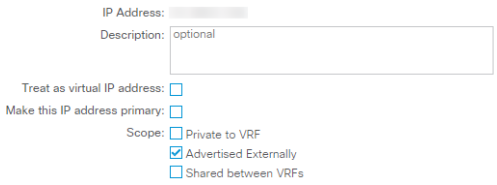
STEP 4 | Cliquez sur le bouton plus (+) à droite de **Associated L3 Outs** (Sorties couche 3 associées).

STEP 5 | Sélectionnez la connexion réseau acheminée externe de couche 3 créée lors de la procédure précédente dans le menu déroulant **L3 Out** (Sortie couche 3).

STEP 6 | Cliquez sur **Update (Mettre à jour)**.

STEP 7 | Sélectionnez **Networking (Mise en réseau)** > **Bridge Domains (Domaines de pont)** > **<your bridge domain>** > **Subnets (Sous-réseaux)** > **<externally advertised subnet>**.

STEP 8 | Définissez la Scope (Portée) sur **Advertised Externally** (Annonce externe).



STEP 9 | Cliquez sur **Submit (Envoyer)**.

Création d'un contrat sortant

Créez un contrat avec un filtre qui autorise le trafic DNS, NTP, HTTP et HTTPS. Vous utiliserez ce contrat pour autoriser tous les terminaux de la VRF à atteindre les réseaux externes, tout en limitant le trafic envoyé au pare-feu.

STEP 1 | Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire.

STEP 2 | Sélectionnez **Contrats (Contrats)** > **Filters (Filtres)**

STEP 3 | Faites un clic droit sur **Filters** (Filtres) et sélectionnez **Create Filter** (Créer un filtre).

STEP 4 | Saisissez un **Name** (Nom) descriptif pour le filtre.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Créez une entrée de filtre pour le trafic UDP.

1. Cliquez sur le bouton plus (+) à droite de **Entries** (Entrées).
2. Saisissez un **Name** (Nom) descriptif pour le filtre **UDP**.
3. Sélectionnez **IP** dans la liste déroulante **EtherType**.
4. Sélectionnez **udp** dans la liste déroulante **IP Protocol** (Protocole IP).
5. Sélectionnez **dns** dans la liste déroulante **Destination Port From** (Port de destination depuis).
6. Cliquez sur **Update (Mettre à jour)**.

STEP 6 | Créez une entrée de filtre pour le trafic TCP.

1. Cliquez sur le bouton plus (+) à droite de **Entries** (Entrées).
2. Saisissez un **Name** (Nom) descriptif pour le filtre **TCP**.
3. Sélectionnez **IP** dans la liste déroulante **EtherType**.
4. Sélectionnez **tcp** dans la liste déroulante **IP Protocol** (Protocole IP).
5. Sélectionnez **dns** dans la liste déroulante **Destination Port From** (Port de destination depuis).
6. Cliquez sur **Update (Mettre à jour)**.

STEP 7 | Créez une entrée de filtre pour le trafic NTP.

1. Cliquez sur le bouton plus (+) à droite de **Entries** (Entrées).
2. Saisissez un **Name** (Nom) descriptif pour le filtre **NTP**.
3. Sélectionnez **IP** dans la liste déroulante **EtherType**.
4. Sélectionnez **udp** dans la liste déroulante **IP Protocol** (Protocole IP).
5. Dans le champ **Destination Port From** (Port de destination depuis), saisissez 123.
6. Cliquez sur **Update (Mettre à jour)**.

STEP 8 | Créez une entrée de filtre pour le trafic HTTP.

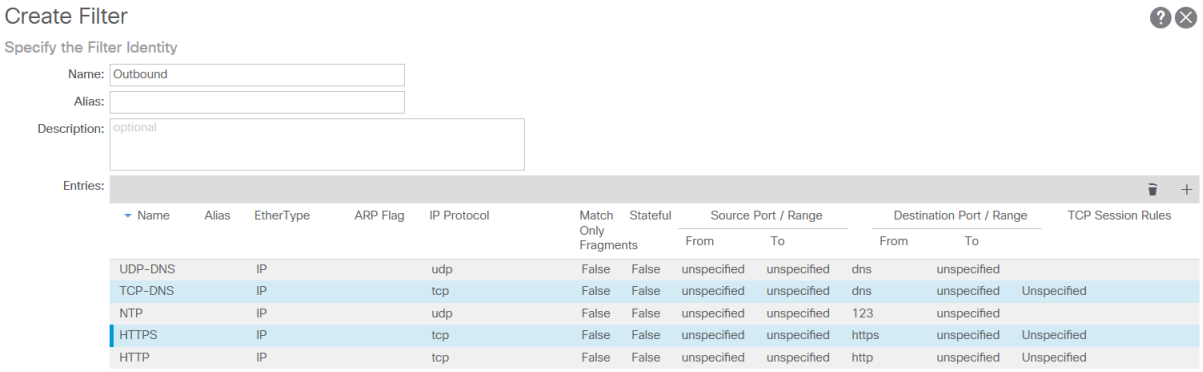
1. Cliquez sur le bouton plus (+) à droite de **Entries** (Entrées).
2. Saisissez un **Name** (Nom) descriptif pour le filtre **HTTP**.
3. Sélectionnez **IP** dans la liste déroulante **EtherType**.
4. Sélectionnez **tcp** dans la liste déroulante **IP Protocol** (Protocole IP).
5. Sélectionnez **http** dans la liste déroulante **Destination Port From** (Port de destination depuis).
6. Cliquez sur **Update (Mettre à jour)**.

©2023 Palo Alto Networks, Inc.

STEP 9 | Créez une entrée de filtre pour le trafic HTTPS.

1. Cliquez sur le bouton plus (+) à droite de **Entries** (Entrées).
2. Saisissez un **Name** (Nom) descriptif pour le filtre **HTTP**.
3. Sélectionnez **IP** dans la liste déroulante **EtherType**.
4. Sélectionnez **tcp** dans la liste déroulante **IP Protocol** (Protocole IP).
5. Sélectionnez **https** dans la liste déroulante **Destination Port From** (Port de destination depuis).
6. Cliquez sur **Update (Mettre à jour)**.

STEP 10 | Cliquez sur **Submit (Envoyer)**.



STEP 11 | Créez un contrat pour le trafic sortant.

1. Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire et sélectionnez **Contracts** (Contrats).
2. Faites un clic droit sur **Contracts** (Contrats) et sélectionnez **Create Contract** (Créer un contrat).
3. Saisissez un **Name** (Nom) descriptif pour votre **Contrat** (Contrat).
4. Cliquez sur le bouton plus (+) à droite de **Subjects** (Sujets).
5. Saisissez un **Name** (Nom) descriptif pour votre **Subject** (Sujet).
6. Dans Filter Chain (Chaîne de filtres), cliquez sur le bouton plus (+) à droite de **Filters** (Filtres).
7. Sélectionnez le filtre que vous avez précédemment créé dans la liste déroulante.
8. Cliquez sur **OK**.

STEP 12 | Cliquez sur **Submit (Envoyer)**.

Création d'un contrat Web entrant

Vous devez également créer un contrat et des filtres pour permettre au trafic entrant d'atteindre les serveurs situés derrière le pare-feu. La procédure suivante décrit le processus de création d'un contrat et de filtres permettant au trafic Web HTTP et HTTPS d'accéder aux ressources situées derrière le pare-feu.

STEP 1 | Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire.

STEP 2 | Sélectionnez **Contrats (Contrats)** > **Filters (Filtres)**

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Faites un clic droit sur **Filters** (Filtres) et sélectionnez **Create Filter** (Créer un filtre).

STEP 4 | Saisissez un **Name** (Nom) descriptif pour le filtre.

STEP 5 | Créez une entrée de filtre pour le trafic HTTP.

1. Cliquez sur le bouton plus (+) à droite de **Entries** (Entrées).
2. Saisissez un **Name** (Nom) descriptif pour le filtre **HTTP**.
3. Sélectionnez **IP** dans la liste déroulante **EtherType**.
4. Sélectionnez **tcp** dans la liste déroulante **IP Protocol** (Protocole IP).
5. Sélectionnez **http** dans la liste déroulante **Destination Port From** (Port de destination depuis).
6. Cliquez sur **Update (Mettre à jour)**.

STEP 6 | Créez une entrée de filtre pour le trafic HTTPS.

1. Cliquez sur le bouton plus (+) à droite de **Entries** (Entrées).
2. Saisissez un **Name** (Nom) descriptif pour le filtre **TCP**.
3. Sélectionnez **IP** dans la liste déroulante **EtherType**.
4. Sélectionnez **tcp** dans la liste déroulante **IP Protocol** (Protocole IP).
5. Sélectionnez **https** dans la liste déroulante **Destination Port From** (Port de destination depuis).
6. Cliquez sur **Update (Mettre à jour)**.

STEP 7 | Cliquez sur **Submit (Envoyer)**.

STEP 8 | Créez un contrat pour le trafic Web entrant.

1. Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire et sélectionnez **Contracts** (Contrats).
2. Faites un clic droit sur **Contracts** (Contrats) et sélectionnez **Create Contract** (Créer un contrat).
3. Saisissez un **Name** (Nom) descriptif pour votre **Contrat** (Contrat).
4. Cliquez sur le bouton plus (+) à droite de **Subjects** (Sujets).
5. Saisissez un **Name** (Nom) descriptif pour votre **Subject** (Sujet).
6. Dans Filter Chain (Chaîne de filtres), cliquez sur le bouton plus (+) à droite de **Filters** (Filtres).
7. Sélectionnez le filtre que vous avez précédemment créé dans la liste déroulante.
8. Cliquez sur **OK**.

STEP 9 | Cliquez sur **Submit (Envoyer)**.

Application des contrats sortants et entrants aux EPG

Vous devez maintenant appliquer les contrats entrants et sortants aux EPG appropriés.

Pour que tous les EPG (collecte d'EPG) au sein d'une VRF puissent envoyer le trafic vers une destination externe, chaque EPG interne doit passer un contrat avec l'EPG externe. En règle générale, vous devez créer un contrat distinct entre chaque EPG interne et l'EPG externe.

 ©2023 Palo Alto Networks, Inc.

Cependant, en utilisant un objet vzAny, vous pouvez appliquer le même contrat à tous les EPG de manière dynamique. La collecte d'EPG consomme le contrat et l'EPG externe fournit le contrat. Vous pouvez configurer des profils de trafic spécifiques dans le contrat ou envoyer tout le trafic au pare-feu et lui permettre de contrôler le trafic sortant du centre de données. De plus, le contrat est automatiquement appliqué à tout nouvel EPG qui rejoint le VRF.

Appliquez le contrat entrant de sorte que l'EPG interne soit le fournisseur et que l'EPG externe soit le consommateur. Le trafic qui circule vers l'EPG interne est d'abord contrôlé par rapport au contrat et tout trafic autorisé est ensuite sécurisé par le pare-feu si nécessaire.

STEP 1 | Appliquez le contrat sortant à tous les EPG de la VRF.

1. Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire.
2. Sélectionnez **Networking (Mise en réseau)** > **VRFs** > **<you VRF>** > **EPG Collection for VRF (Collecte d'EPG pour VRF)**.
3. Cliquez sur le bouton plus (+) à droite de **Consumed Contracts (Contrats consommés)**.
4. Sélectionnez votre contrat sortant racine dans la liste déroulante **Name (Nom)**.
5. Cliquez sur **Update (Mettre à jour)**.
6. Sélectionnez **Networking (Mise en réseau)** > **External Routed Networks (Réseaux acheminés externes)** > **<your external routed network>** > **Networks (Réseaux)** > **External (Externe)**.
7. Cliquez sur le bouton plus (+) à droite de **Provided Contracts** (Contrats fournis).
8. Sélectionnez votre contrat sortant racine dans la liste déroulante **Name (Nom)**.
9. Cliquez sur **Update (Mettre à jour)**.

STEP 2 | Appliquez le contrat entrant afin qu'un EPG interne le fournisse à l'EPG externe.

1. Dans l'onglet **Tenants** (Locataires), double-cliquez sur le nom de votre locataire.
2. Sélectionnez **Application Profiles (Profils d'application)** > **<your application profile>** > **Application EPGs (EPG d'application)** > **<your application EPG>** > **Contracts (Contrats)**.
3. Faites un clic droit sur **Contracts** (Contrats) et sélectionnez **Add Provided Contract** (Ajouter le contrat fourni).
4. Sélectionnez votre contrat entrant racine dans la liste déroulante **Contract** (Contrat).
5. Cliquez sur **Submit (Envoyer)**.
6. Sur le même locataire, sélectionnez **Networking (Mise en réseau)** > **External Routed Networks (Réseaux acheminés externes)** > **<your external routed network>** > **Networks (Réseaux)** > **External (Externe)**.
7. Dans l'onglet Contracts (Contrats), cliquez sur le bouton plus (+) à droite de **Consumed Contracts (Contrats consommés)**.
8. Sélectionnez votre contrat entrant racine dans la liste déroulante **Name (Nom)**.
9. Cliquez sur **Update (Mettre à jour)**.

Création d'un routeur virtuel et d'une zone de sécurité pour le trafic nord-sud

Créez un routeur virtuel et une zone de sécurité sur le pare-feu pour correspondre au locataire et au VRF sur ACI.

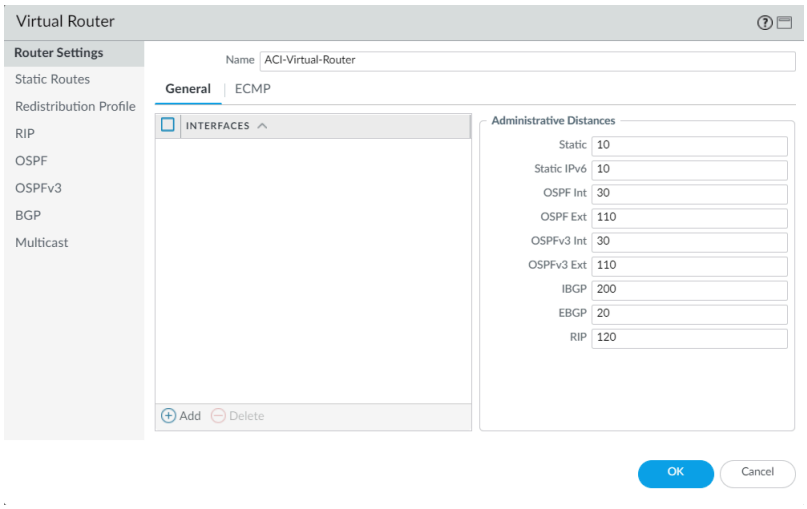
STEP 1 | Connectez-vous au pare-feu.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, puis cliquez sur **Add (Ajouter)**.

STEP 3 | Donnez un **Name** (Nom) descriptif au routeur virtuel.

STEP 4 | Cliquez sur **OK**.

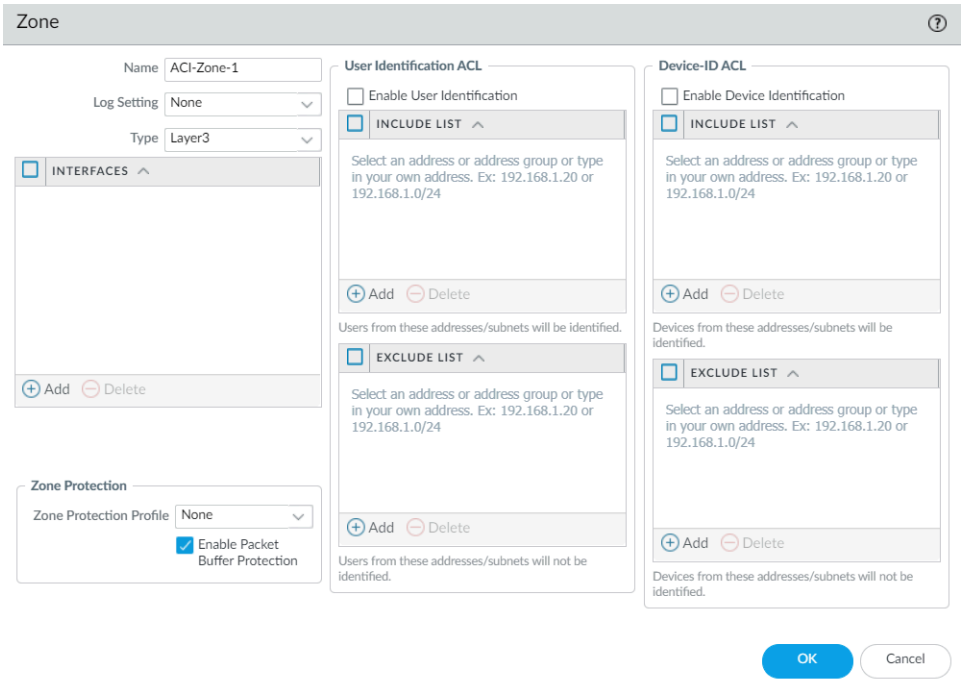


STEP 5 | Sélectionnez **Network (Réseau)** > **Zones**, puis cliquez sur **Add (Ajouter)**.

STEP 6 | Donnez un **Name** (Nom) descriptif à la zone.

STEP 7 | Choisissez Layer3 (Couche 3) dans la liste déroulante **Type**.

STEP 8 | Cliquez sur **OK**.



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

©2023 Palo Alto Networks, Inc.

Configuration des interfaces réseau

Configurez une interface Ethernet agrégée, des interfaces membres et une sous-interface utilisées par votre pare-feu pour se connecter aux commutateurs feuilles ACI. Si vous utilisez un pare-feu VM-Series, utilisez des interfaces discrètes au lieu d'interfaces agrégées.

Le pare-feu VM-Series ne prend pas en charge les groupes Ethernet agrégé.

STEP 1 | Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et cliquez sur **Add Aggregate Group (Ajouter un groupe agrégé)**.

STEP 2 | Saisissez un nombre pour le groupe agrégé dans le second champ **Interface Name** (Nom d'interface).

STEP 3 | Sélectionnez Layer 3 (Couche 3) dans la liste déroulante **Interface Type** (Type d'interface).

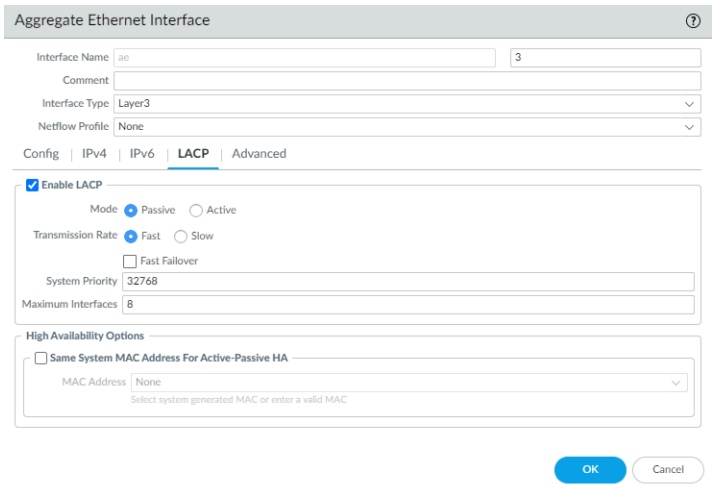
STEP 4 | Sélectionnez l'onglet **LACP** et cliquez sur **Enable LACP** (Activer LACP).

STEP 5 | Sélectionnez **Fast** (Rapide) comme **Transmission Rate** (Vitesse de transmission).

STEP 6 | Dans High Availability Options (Options de haute disponibilité), cochez **Enable in HA Passive State** (Activer à l'état HA passive).

*Ne cochez pas **Same System MAC Address for Active-Passive HA** (Même adresse MAC système pour la HA active/passive). Cette option fait en sorte que la paire de pare-feu apparaisse comme un seul appareil pour le commutateur, de sorte que le trafic sera acheminé vers les deux pare-feu au lieu du seul pare-feu actif.*

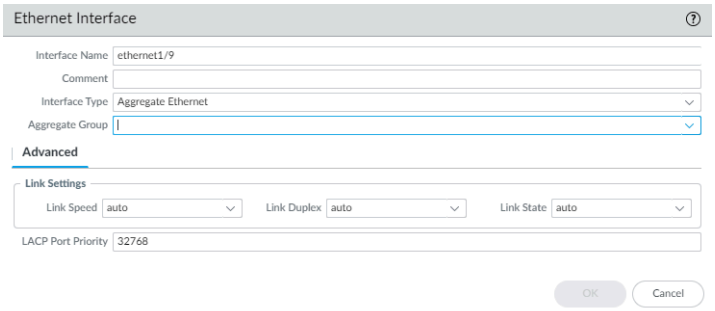
STEP 7 | Cliquez sur **OK**.



 ©2023 Palo Alto Networks, Inc.

STEP 8 | Cliquez sur le nom d'une interface Ethernet pour la configurer et l'ajouter au groupe agrégé.

1. Sélectionnez **Aggregate Ethernet** dans la liste déroulante Interface Type (Type d'interface).
2. Sélectionnez l'interface que vous avez définie dans la configuration du groupe Aggregate Ethernet.
3. Cliquez sur **OK**.
4. Répétez cette étape pour chaque autre interface membre du groupe Aggregate Ethernet.



STEP 9 | Ajoutez une sous-interface sur l'interface Aggregate Ethernet pour le locataire et le VRF.

1. Sélectionnez la ligne de votre groupe Aggregate Ethernet et cliquez sur **Add Subinterface** (Ajouter une sous-interface).
2. Dans le second champ **Interface Name** (Nom d'interface), saisissez un suffixe numérique pour identifier la sous-interface.
3. Dans le champ **Tag** (Étiquette), saisissez l'étiquette VLAN de la sous-interface.
4. Sélectionnez le routeur virtuel que vous avez configuré précédemment dans la liste déroulante **Virtual Router** (Routeur virtuel).
5. Sélectionnez la zone que vous avez configurée précédemment dans la liste déroulante **Zone**.
6. Sélectionnez l'onglet **IPv4**.
7. Sélectionnez le type **Static** (Statique).
8. Cliquez sur **Add** (Ajouter) et saisissez l'adresse IP et le masque réseau de la sous-interface en notation CIDR.
9. Cliquez sur **OK**.

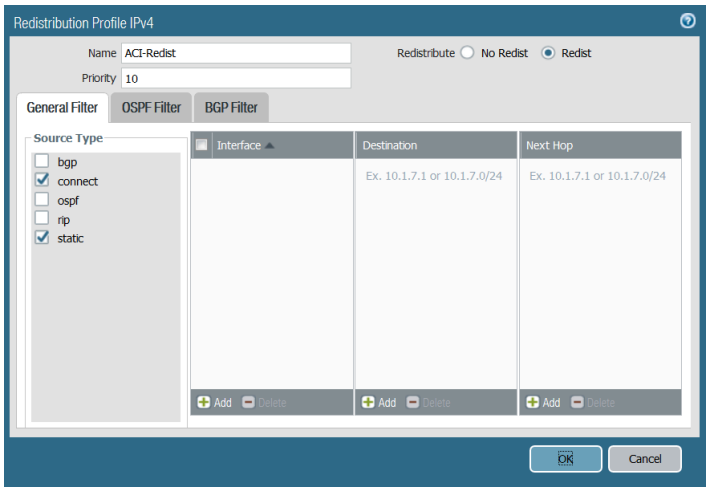
Configuration de la redistribution des itinéraires et OSPF

Configurez la redistribution des itinéraires pour rendre les informations d'acheminement à partir du pare-feu disponibles pour les routeurs externes connectés à vos commutateurs feuilles. Ensuite, configurez OSPF sur le pare-feu et attribuez un identifiant de routeur, un numéro de zone et une interface pour former des adjacences.

©2023 Palo Alto Networks, Inc.

STEP 1 | Configurez la redistribution des itinéraires.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel que vous avez précédemment créé.
2. Sélectionnez **Redistribution Profile (Profil de redistribution)** > **IPv4** > **Add (Ajouter)**.
3. Saisissez un **Name** (Nom) descriptif pour votre profil de redistribution.
4. Déterminez une priorité.
5. Pour **Redistribute** (Redistribuer), sélectionnez **Redist**.
6. Cochez **connect** (connexion) et **static** (statique) dans **General Filter** (Filtre général).
7. Cliquez sur **OK**.



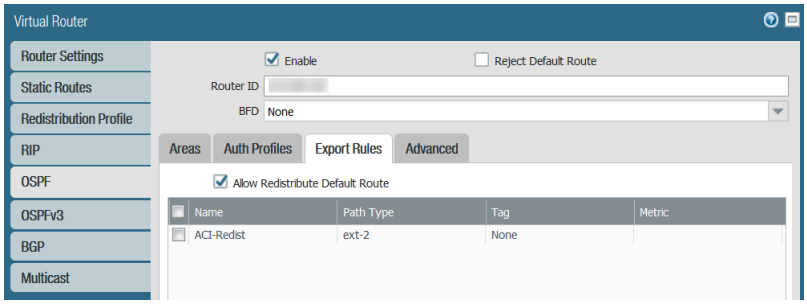
STEP 2 | Configurez OSPF.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel que vous avez précédemment créé.
2. Sélectionnez **Router Settings (Paramètres des routeurs)** > **ECMP** et **Enable (Activer)**.
3. Sélectionnez **OSPF** et choisissez **Enable** (Activer).
4. Saisissez le **Router ID** (ID de routeur) de l'OSPF.
5. Dans **Area** (Zone), cliquez sur **Add** (Ajouter).
6. Saisissez l'**Area ID** (ID de zone). Cette valeur doit correspondre à la valeur que vous avez attribuée lors de la création du réseau routé externe sur l'APIC. Sur le pare-feu, cette valeur

©2023 Palo Alto Networks, Inc.

doit être saisie sous forme décimale séparée par un point. Par exemple, si vous avez saisi un Area ID (ID de zone) de 10 dans l'APIC, l'équivalent sur le pare-feu est 0.0.0.10.

7. Sélectionnez **Interface** > **Add (Ajouter)**.
8. Saisissez l'interface qui se connecte à votre EPG de réseau externe et cliquez sur **OK**.
9. Sélectionnez **Export Rules (Règles d'exportation)** > **Add (Ajouter)**.
10. Sélectionnez le profil de redistribution que vous avez créé ci-dessus dans la liste déroulante **Name** (Nom) et cliquez sur **OK**.
11. Sélectionnez **Allow Redistribute Default Route** (Autoriser la redistribution des itinéraires par défaut).
12. Cliquez sur **OK**.



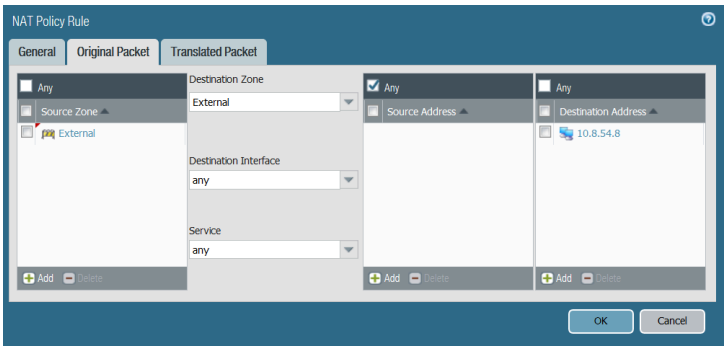
Configuration de NAT pour les connexions externes

Vous ne devez configurer la NAT que si le pare-feu possède une interface externe utilisée pour la connexion à des réseaux extérieurs à votre centre de données. Bien que la NAT ne soit pas requise, vous pouvez utiliser cette procédure pour convertir l'adressage IP privé de votre centre de données en un adressage IP public extérieur. Commencez à configurer la NAT en configurant la traduction d'adresse pour le trafic entrant sur le serveur à l'intérieur d'un EPG de votre centre de données. Configurez ensuite une politique NAT traduisant l'adresse source du trafic sortant de tout EPG vers l'adresse IP de l'interface externe.

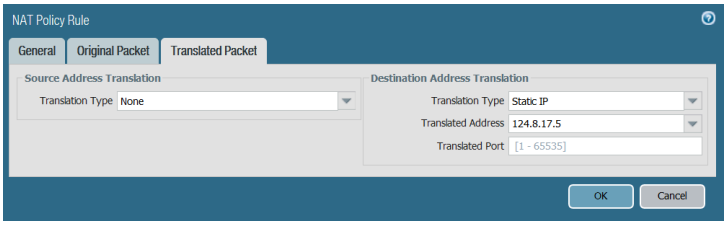
 ©2023 Palo Alto Networks, Inc.

STEP 1 | Configurez la traduction d'adresse pour le trafic entrant dans un EPG dans votre centre de données.

1. Sélectionnez **Policies (Politiques)** > **NAT**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name** (Nom) descriptif pour la règle de politique NAT.
3. Sélectionnez **Original Packet** (Paquet d'origine) et cliquez sur **Add** (Ajouter) sous **Source Zone** (Zone source).
4. Sélectionnez la zone source dans la liste déroulante.
5. Sélectionnez la zone de destination dans la liste déroulante **Destination Zone** (Zone de destination).
6. Sélectionnez **Any** (Tout) pour la **Source Address** (Adresse source).
7. Cliquez sur **Add** (Ajouter) sous **Destination Address** (Adresse de destination) et saisissez l'adresse IP externe.



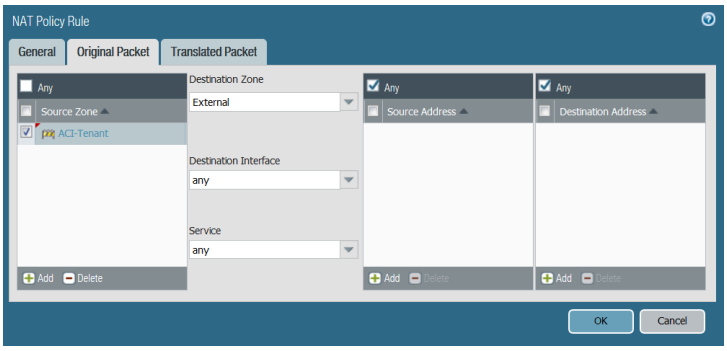
8. Dans l'onglet **Translated Packet** (Paquet traduit), sélectionnez le **Translation Type** (Type de traduction) dans **Destination Address Translation** (Traduction d'adresse de destination).
9. Sélectionnez une adresse dans la liste déroulante **Translated Address** (Adresse traduite).
10. Cliquez sur **OK**.



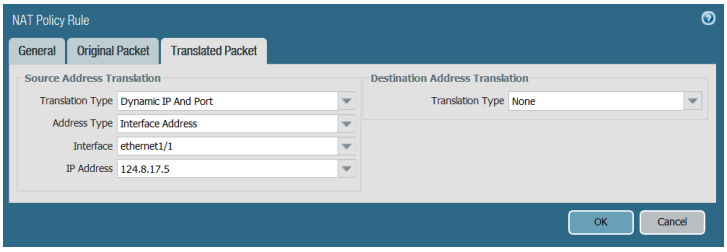
 ©2023 Palo Alto Networks, Inc.

STEP 2 | Configurez la traduction d'adresse pour le trafic sortant.

1. Sélectionnez **Policies (Politiques)** > **NAT**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name** (Nom) descriptif pour votre politique NAT sortante.
3. Sélectionnez **Original Packet** (Paquet d'origine) et cliquez sur **Add** (Ajouter) sous **Source Zone** (Zone source).
4. Sélectionnez la zone qui correspond à votre locataire ACI et au VRF.
5. Sélectionnez la zone externe dans la liste déroulante **Destination Zone** (Zone de destination).



6. Dans l'onglet **Translated Packet** (Paquet traduit), sélectionnez le **Translation Type** (Type de traduction) dans **Source Address Translation** (Traduction d'adresse source).
7. Saisissez les informations d'adresse requises supplémentaires.
8. Cliquez sur **OK**.



STEP 3 | **Commit (Validez)** vos modifications.

©2023 Palo Alto Networks, Inc.

Surveillance des terminaux dans Cisco ACI

Le plug-in Cisco ACI pour Panorama vous permet de créer une politique de sécurité pour votre infrastructure Cisco ACI à l'aide de groupes d'adresses dynamiques. Le plug-in surveille les modifications d'une infrastructure APIC (Application Policy Infrastructure Controller) dans votre environnement Cisco ACI et partage ces informations avec Panorama. Chaque Panorama sur lequel le plug-in Cisco ACI est installé peut prendre en charge jusqu'à 16 clusters APIC. Et chaque définition de surveillance possède un cluster et un groupe de notification.

Le nombre de terminaux que peut surveiller le plug-in Cisco ACI dépend de la quantité de mémoire allouée à Panorama. Si vous disposez d'un appareil virtuel Panorama, veillez à attribuer la quantité de mémoire nécessaire aux terminaux de votre environnement. Reportez-vous au Guide d'administration de Panorama pour plus d'informations sur la préparation de votre Panorama virtuel.

Mémoire Panorama	Terminaux
8 Go	10,000
16 Go	20,000

Le plug-in Cisco ACI traite les informations sur les terminaux et les convertit en un ensemble d'étiquettes pouvant être utilisées comme critères de correspondance pour le placement d'adresses IP dans les groupes d'adresses dynamiques. Les étiquettes sont créées dans le format suivant :

cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.{epg_<EPG> | uepg_<micro-EPG>}

- **cisco.cl_<cluster>** : cette étiquette regroupe les adresses IP dans un Dynamic Address Group (groupe d'adresses dynamiques) basé sur le cluster Cisco ACI et affiche le nom de votre cluster.
- **cisco.cl_<cluster>.tn_<tenant>** : cette étiquette regroupe les adresses IP dans un Dynamic Address Group (groupe d'adresses dynamiques) basé sur un locataire et affiche le nom de votre cluster et de votre locataire.
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>** : cette étiquette regroupe les adresses IP dans un Dynamic Address Group (groupe d'adresses dynamiques) basé sur le profil d'application et affiche le nom de votre cluster, locataire et profil d'application.
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.epg_<EPG>** : cette étiquette regroupe les adresses IP dans un Dynamic Address Group (groupe d'adresses dynamiques) basé sur EPG et affiche le nom de votre cluster, locataire, profil d'application et EPG.
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.uepg_<micro-EPG>** : cette étiquette regroupe les adresses IP dans un Dynamic Address Group (groupe d'adresses dynamiques) basé sur micro-EPG et affiche le nom de votre cluster, locataire, profil d'application et micro-EPG.
- **cisco.cl_<cluster>.tn_<tenant>.l2out_<L2-external-endpoint>** : cette étiquette regroupe les adresses IP en Dynamic Address Group (groupe d'adresses dynamiques) basés sur le terminal externe L2 et affiche le nom de votre cluster, locataire et terminal externe L2.
- **cisco.cl_<cluster>.tn_<tenant>.bd_<bridge-domain>.subnet_<subnet>** : cette étiquette regroupe les adresses IP dans un Dynamic Address Group (groupe d'adresses dynamiques) basé sur le sous-réseau et affiche le nom de votre cluster, locataire, domaine de pont et sous-réseau.

©2023 Palo Alto Networks, Inc.

Pour récupérer les informations de mappage d'adresse IP vers une étiquette des terminaux, vous devez configurer une définition de surveillance pour chaque infrastructure APIC de votre environnement Cisco ACI. La définition de surveillance spécifie le nom d'utilisateur et le mot de passe permettant à Panorama de se connecter aux APIC. Elle spécifie également les groupes d'appareils et les groupes de notification correspondants contenant les pare-feu auxquels Panorama envoie les étiquettes. Une fois que vous avez configuré la définition de surveillance et que le plug-in Cisco ACI a récupéré les étiquettes, vous pouvez créer des groupes d'adresses dynamiques et ajouter les étiquettes en tant que critères de correspondance.

Le plug-in Cisco ACI utilise deux intervalles pour récupérer des informations de l'APIC. Le premier est l'intervalle de surveillance.

- Intervalle de surveillance : l'intervalle de surveillance est la durée pendant laquelle le plug-in attend avant de rechercher des modifications dans l'infrastructure. Si aucune modification ne s'est produite, l'intervalle de surveillance est réinitialisé. Si des modifications sont détectées, le plug-in les traite avant de réinitialiser l'intervalle de surveillance. L'intervalle de surveillance par défaut est de 60 secondes. Vous pouvez définir l'intervalle de surveillance de 60 secondes à un jour (86 400 secondes).
- Intervalle de synchronisation complète : l'intervalle de synchronisation complète est la durée pendant laquelle le plug-in attend avant de mettre à jour les objets dynamiques de toutes les infrastructures, quelles que soient les modifications apportées. Cela garantit que le plug-in est synchronisé avec l'infrastructure, même si un événement de modification est manqué par l'intervalle de surveillance. L'intervalle de synchronisation complète par défaut est de 10 minutes. Vous pouvez définir un intervalle de synchronisation complète de 600 secondes (10 minutes) à 86 400 secondes (un jour).

  Vous devez configurer l'intervalle de synchronisation complète via la CLI Panorama.

Si vous configurez une valeur d'intervalle de surveillance supérieure à celle de l'intervalle de synchronisation complète, l'intervalle de synchronisation complète est ignoré et une synchronisation complète est effectuée à chaque intervalle de surveillance.

Si Panorama perd sa connexion avec l'APIC, il tentera de se reconnecter cinq fois. Après cinq tentatives infructueuses, Panorama arrête de surveiller les modifications dans vos clusters et affiche les tentatives de reconnexion dans le journal système. Pour récupérer et commencer à surveiller vos clusters, vous devez effectuer une validation sur Panorama.

- Installation du plug-in Panorama pour Cisco ACI
- Configuration du plug-in Cisco ACI
- Plug-in Panorama pour le tableau de bord ACI

Installation du plug-in Panorama pour Cisco ACI

Pour commencer à surveiller les terminaux sur Cisco ACI, téléchargez et installez le plug-in Cisco ACI sur Panorama.

Si vous avez une configuration d'HA de Panorama, répétez ce processus d'installation sur chaque pair de Panorama. Lors de l'installation de la fiche sur les Panoramas d'une paire HA, installez la fiche sur le pair passif avant le pair actif. Après avoir installé le plug-in sur l'homologue passif, il passera à un état non fonctionnel. L'installation du plug-in sur l'homologue actif renvoie l'homologue passif à un état fonctionnel.

 ©2023 Palo Alto Networks, Inc.

Si vous avez un appareil Panorama autonome ou deux appareils Panorama installés dans une paire HA avec plusieurs plug-ins installés, les plug-ins peuvent ne pas recevoir les informations des indicateurs d'adresse IP mises à jour si un ou plusieurs des plug-ins ne sont pas configurés. Cela se produit, car Panorama ne transfère pas les informations des indicateurs d'adresse IP aux plug-ins non configurés. De plus, ce problème peut se présenter si un ou plusieurs plug-ins Panorama ne se trouvent pas dans l'état Registered (Enregistré) ou Success (Réussite) (l'état positif diffère sur chaque plug-in). Assurez-vous que vos plug-ins se trouvent dans l'état positif avant de continuer ou d'exécuter les commandes décrites ci-dessous.

Si vous rencontrez ce problème, il existe deux solutions alternatives :

- Désinstallez le ou les plug-ins non configurés. Il est déconseillé d'installer un plug-in que vous n'envisagez pas de configurer dans l'immédiat
- Vous pouvez utiliser les commandes suivantes pour contourner ce problème. Exécutez la commande suivante pour chaque plug-in non configuré sur chaque instance de Panorama afin que Panorama n'attende pas pour envoyer des mises à jour. Dans le cas contraire, vos pare-feu risquent de perdre certaines informations des indicateurs d'adresse IP.

  `request plugins dau plugin-name <plugin-name> unblock-device-push yes`

  Vous pouvez annuler cette commande en exécutant :

  `request plugins dau plugin-name <plugin-name> unblock-device-push no`

Les commandes décrites ne sont pas persistantes lors des redémarrages et doivent être réutilisées pour tout redémarrage ultérieur. Pour Panorama en paire HA, les commandes doivent être exécutées sur chaque Panorama.

STEP 1 | Vérifiez que votre Panorama virtuel dispose de suffisamment de mémoire pour prendre en charge les terminaux dans votre environnement ACI.

STEP 2 | Sélectionnez **Panorama** > **Plugins**.

STEP 3 | Sélectionnez **Check Now (Vérifiez maintenant)**pour récupérer la liste des mises à jour disponibles.

STEP 4 | Sélectionnez **Download (Télécharger)** dans la colonne Action pour installer le plug-in (module d'extension).

STEP 5 | Sélectionnez la version du plug-in et cliquez sur **Install (Installer)** dans la colonne Action pour installer le plug-in. Panorama vous alertera lorsque l'installation est terminée.



Configuration du plug-in Cisco ACI

Après avoir installé le plug-in, vous devez définir l'intervalle de surveillance, configurer un groupe de notification et établir une connexion entre Panorama et l'infrastructure APIC.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | (Facultatif) Configurez l'intervalle de synchronisation complète.

1. Connectez-vous à la CLI Panorama.
2. Passez en mode de configuration.

   admin@Panorama> configure
3. Utilisez la commande suivante pour définir l'intervalle de synchronisation complète. L'intervalle par défaut est de 600 secondes (10 minutes). La plage est comprise entre 600 et 86 400 secondes (un jour).

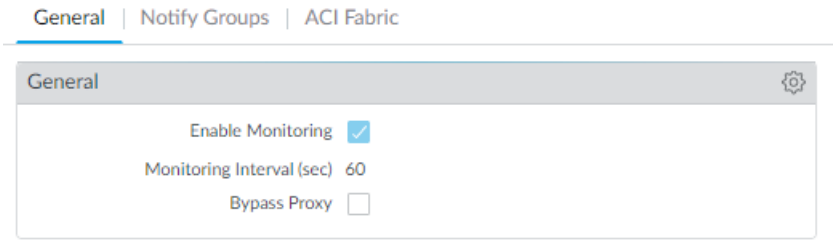
   admin@Panorama# **set plugins cisco full-sync-interval <interval-in-seconds>**

STEP 2 | Connectez-vous à l'interface Web Panorama.

STEP 3 | Vous devez ajouter les pare-feu comme dispositifs gérés sur Panorama et créer des groupes d'appareils de façon à pouvoir configurer Panorama pour aviser ces groupes à l'aide de l'information VM qu'il récupère. Les groupes d'appareils peuvent inclure des pare-feu de série VM ou des systèmes virtuels sur les pare-feu matériels.

STEP 4 | Activez la surveillance, définissez l'intervalle de surveillance et activez le contournement du proxy.

1. Sélectionnez **Panorama** > **Cisco ACI** > **Setup (Configuration)** > **General (Général)**.
2. Sélectionnez **Enable Monitoring** (Activer la surveillance). Cela active la surveillance de tous les clusters de votre déploiement.
3. Définissez le **Monitoring Interval** (Intervalle de surveillance) en secondes. L'intervalle de surveillance correspond à la fréquence à laquelle Panorama récupère les informations réseau mises à jour à partir de l'APIC. La valeur par défaut est de 60 secondes et la plage est comprise entre 60 secondes et 86 400 secondes (un jour).
4. (Facultatif) Sélectionnez Bypass proxy (Contourner le proxy) pour ignorer les paramètres du serveur proxy, configurés sur Panorama sous **Panorama** > **Setup (Configuration)** > **Services** > **Proxy Server (Serveur proxy)** pour la communication entre Panorama et l'APIC. Ceci permet à Panorama de communiquer directement avec l'APIC tout en maintenant la communication par proxy pour d'autres services.



STEP 5 | Créez un groupe de notification.

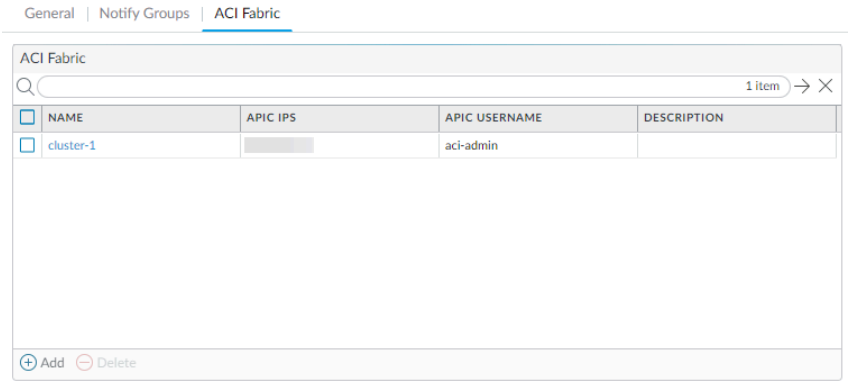
1. Sélectionnez **Panorama** > **Cisco ACI** > **Setup (Configuration)** > **Notify Groups (Groupes de notification)**.
2. Cliquez sur **Add (Ajouter)**.
3. Saisissez un **Name** (Nom) descriptif pour votre groupe de notification.
4. Sélectionnez les groupes d'appareils dans votre déploiement ACI.

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Ajoutez des informations sur l'infrastructure ACI.

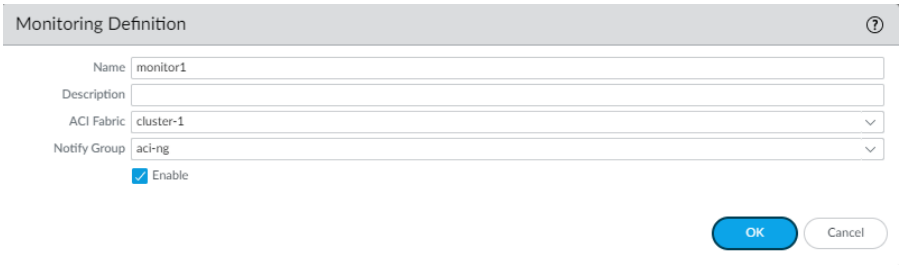
1. Sélectionnez **Panorama** > **Cisco ACI** > **Setup (Configuration)** > **ACI Fabric (Infrastructure ACI)**.
2. Saisissez un **Name** (Nom) descriptif pour votre cluster.
3. Saisissez l'adresse IP ou le FQDN de chaque APIC du cluster sous forme de liste séparée par des virgules.

   Lorsque vous utilisez un FQDN, n'incluez pas https:// dans l'URL.
4. Saisissez votre nom d'utilisateur pour l'APIC.
5. Saisissez et confirmez votre mot de passe APIC.
6. Cliquez sur **OK**.



STEP 7 | Configurez la définition de surveillance.

1. Sélectionnez **Panorama** > **Cisco ACI** > **Monitoring Definition (Définition de surveillance)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name** (Nom) descriptif et éventuellement une Description pour identifier le Cisco ACI pour lequel vous utilisez cette définition.
3. Sélectionnez les **Cluster Info** (Informations sur le cluster) et le **Notify Group** (Groupe de notification).
4. Cliquez sur **OK**.



STEP 8 | **Commit (Validez)** vos modifications.

©2023 Palo Alto Networks, Inc.

STEP 9 | Vérifiez que vous pouvez visualiser l'information EPG sur Panorama et définir les critères d'appariement pour les groupes d'adresses dynamiques.

Certaines extensions de navigateur peuvent bloquer les appels API entre Panorama et l'APIC, ce qui empêche Panorama de recevoir les critères de correspondance. Si Panorama n'affiche aucun critère de correspondance et que vous utilisez des extensions de navigateur, désactivez ces extensions et cliquez sur Synchronize Dynamic Objects (Synchroniser des objets dynamiques) pour renseigner les étiquettes disponibles dans Panorama.

Panorama ne traite pas immédiatement les nouvelles définitions de surveillance et ne remplit pas les critères de correspondance disponibles pour les adresses dynamiques. Vous devez attendre la durée de votre intervalle de surveillance configuré avant de vérifier ces informations EPG.

STEP 10 | Vérifiez que les adresses de vos EPG sont ajoutées aux groupes d'adresses dynamiques.

1. Sélectionnez **Panorama** > **Objects (Objets)** > **Address Groups (Groupes d'adresses)**.
2. Cliquez sur **More (Plus)** dans la colonne Addresses (Adresses) d'un groupe d'adresses dynamiques.

   Panorama affiche une liste des adresses IP ajoutées à ce groupe d'adresse dynamique en fonction des critères de correspondance que vous avez spécifiés.

STEP 11 | Utilisez des groupes d'adresses dynamiques dans une politique.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Cliquez sur **Add (Ajouter)** et saisissez un **Name (nom)** et une **Description (description)** pour identifier la politique.
3. Ajoutez la **Source Zone (Zone source)** pour indiquer la zone d'où provient le trafic.
4. Ajoutez la **Destination Zone (Zone de destination)** dans laquelle se termine le trafic.
5. Pour **Destination Address (Adresse de destination)**, sélectionnez le groupe d'adresses dynamiques que vous venez de créer.
6. Indiquez l'action (**Allow (Autoriser)** ou **Deny (Refuser)**) pour le trafic, puis associez éventuellement les profils de sécurité par défaut à la règle.
7. Répétez les étapes 1 à 6 pour créer une autre règle de politique.
8. Cliquez sur **Commit (Valider)**.

   Reportez-vous à la section Utilisation de groupes d'adresses dynamiques dans la politique pour obtenir plus d'informations.

STEP 12 | Vous pouvez mettre à jour les objets dynamiques à partir de l'APIC à tout moment en synchronisant les objets dynamiques. La synchronisation des objets dynamiques vous permet de conserver le contexte des modifications dans l'environnement virtuel et vous permet d'activer des applications grâce à la mise à jour automatique des groupes d'adresses dynamiques utilisés dans les règles de politique.

1. Sélectionnez **Panorama** > **Cisco ACI** > **Monitoring Definition (Définition de surveillance)**.

 ©2023 Palo Alto Networks, Inc.

2. Cliquez sur **Synchronize Dynamic Objects** (Synchroniser les objets dynamiques).

Sur le basculement HA, le Panorama nouvellement actif tente de se reconnecter à l'APIC et de récupérer les étiquettes pour toutes les définitions de surveillance. S'il y a une erreur de reconnecter ne serait-ce qu'une définition de surveillance, Panorama génère un message de journal de système.

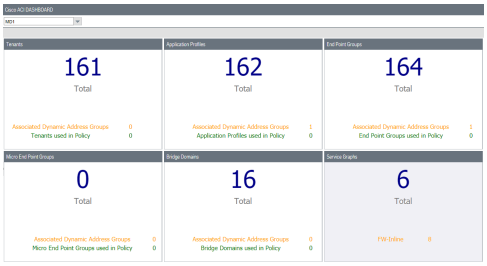
```
Unable to process subscriptions after HA switch-over;
 user-intervention required. (Impossible de traiter les
 abonnements après le basculement HA ; intervention de
 l'utilisateur requise.)
```

Lorsque vous voyez cette erreur, vous devez vous connecter à Panorama et régler le problème, par exemple, en supprimant une adresse IP APIC invalide ou en fournissant des informations d'identification valides, et valider vos modifications pour permettre à Panorama de se reconnecter et de récupérer les étiquettes pour toutes les définitions de surveillance. Même lorsque Panorama est déconnecté de l'APIC, les pare-feu ont la liste de toutes les étiquettes qui ont été récupérées avant le basculement et peuvent continuer d'appliquer la politique sur cette liste d'adresses IP. Si vous effectuez une validation avant de résoudre l'erreur de basculement, le Panorama nouvellement actif ne transmettra aucune information de mappage IP vers étiquette et ne supprimera pas les informations de mappage des pare-feu. Comme pratique exemplaire, pour surveiller ce problème, vous pouvez configurer log forwarding to an HTTPS destination (un journal orienté action vers une destination HTTPS) *à partir de Panorama afin de pouvoir prendre des mesures immédiatement.*

Plug-in Panorama pour le tableau de bord ACI

Le plug-in Panorama pour le tableau de bord Cisco ACI offre une vue d'ensemble de l'infrastructure ACI surveillée par le plug-in. Le tableau de bord se compose de deux pages : La première page donne un aperçu des différents objets surveillés par le plug-in sur un ensemble de vignettes cliquables. En cliquant sur une vignette, vous accédez à la deuxième page qui fournit des informations supplémentaires sur l'objet affiché sur la vignette.

Après avoir installé le plug-in, vous pouvez accéder au tableau de bord en sélectionnant **Panorama** > **Cisco ACI** > **Dashboard (Tableau de bord)**.



 ©2023 Palo Alto Networks, Inc.

Le tableau de bord n'interroge et ne compte que les politiques de sécurité de règle « avant » configurées sur Panorama. Il n'inclut pas les règles règle « après », les règles par défaut ou les règles NAT.

Vignettes du tableau de bord	Description
Tenant Tags (Étiquettes du tenant) *Si le score de d'état de vie d'un tenant est égal à zéro (0) sur l'APIC, Panorama ne récupère pas les informations concernant ce tenant. Par conséquent, le compte du tenant sur Panorama ne correspondra pas au total sur l'APIC.*	Affiche le nombre total de tenants que Panorama a récupérés dans l'APIC. En outre, cela affiche le nombre de groupes d'adresses dynamiques associés aux tenants et le nombre de tenants utilisés dans la politique. Cliquez sur la vignette pour explorer et visualiser les colonnes suivantes. • **Tenant Name (Nom du tenant)** : répertorie tous les tenants récupérés par Panorama. • **Tenant Tag (Étiquette du tenant)** : l'étiquette Panorama associée à chaque tenant. • **Dynamic Address Group (Groupe d'adresses dynamiques)** : affiche les groupes d'adresses dynamiques associés à l'étiquette répertoriée. • **In Policy (Dans la politique)** : indique si le groupe d'adresses dynamiques répertorié est utilisé dans la politique.
Application Profiles (Profils d'application)	Affiche le nombre total de profils d'application que Panorama a récupérés dans l'APIC. En outre, cela affiche le nombre de groupes d'adresses

©2023 Palo Alto Networks, Inc.

Vignettes du tableau de bord	Description
	dynamiques associés aux profils d'application et le nombre de profils d'application utilisés dans la politique. Cliquez sur la vignette pour explorer et visualiser les colonnes suivantes. • **Application Profile Name (Nom du profil d'application)** : répertorie tous les profils d'application récupérés par Panorama. • **Tenant Name (Nom du tenant)** : affiche le tenant associé au profil d'application répertorié. • **Application Profile Tag (Étiquette du profil d'application)** : l'étiquette Panorama associée à chaque profil d'application. • **Dynamic Address Group (Groupe d'adresses dynamiques)** : affiche les groupes d'adresses dynamiques associés à l'étiquette répertoriée. • **In Policy (Dans la politique)** : indique si le groupe d'adresses dynamiques répertorié est utilisé dans la politique.
End Point Groups (Groupes de terminaux)	Affiche le nombre total de groupes de terminaux que Panorama a récupérés dans l'APIC. En outre, cela affiche le nombre de groupes d'adresses dynamiques associés aux EPG et le nombre d'EPG utilisés dans la politique. Cliquez sur la vignette pour explorer et visualiser les colonnes suivantes. • **EPG Name (Nom de l'EPG)** : répertorie tous les EPG récupérés par Panorama. • **Application Profile Name (Nom du profil d'application)** : répertorie le profil d'application associé à l'EPG. • **Tenant Name (Nom du tenant)** : affiche le tenant associé au profil d'application répertorié. • **EPG Tag (Étiquette de l'EPG)** : l'étiquette Panorama associée à chaque EPG. • **Dynamic Address Group (Groupe d'adresses dynamiques)** : affiche les groupes d'adresses dynamiques associés à l'étiquette répertoriée. • **In Policy (Dans la politique)** : indique si le groupe d'adresses dynamiques répertorié est utilisé dans la politique.
Micro End Point Groups (Groupes de micro terminaux)	Affiche le nombre total de groupes de micro terminaux que Panorama a récupérés dans l'APIC. En outre, cela affiche le nombre de groupes d'adresses dynamiques associés aux micro EPG et le nombre de micro EPG utilisés dans la politique. Cliquez sur la vignette pour explorer et visualiser les colonnes suivantes. • **Micro EPG Name (Nom de l'EPG)** : répertorie tous les EPG récupérés par Panorama.

©2023 Palo Alto Networks, Inc.

Vignettes du tableau de bord	Description
	• **Application Profile Name (Nom du profil d'application)** : répertorie le profil d'application associé au micro EPG. • **Tenant Tag (Étiquette du tenant)** : affiche le tenant associé au profil d'application répertorié. • **Micro EPG Tag (Étiquette de l'EPG)** : l'étiquette Panorama associée à chaque micro EPG. • **Dynamic Address Group (Groupe d'adresses dynamiques)** : affiche les groupes d'adresses dynamiques associés à l'étiquette répertoriée. • **In Policy (Dans la politique)** : indique si le groupe d'adresses dynamiques répertorié est utilisé dans la politique.
Bridge Domains (Domaines de pont)	Affiche le nombre total de domaines de pont que Panorama a récupérés dans l'APIC. En outre, cela affiche le nombre de groupes d'adresses dynamiques associés aux domaines de pont et le nombre de domaines de pont utilisés dans la politique. Cliquez sur la vignette pour explorer et visualiser les colonnes suivantes. • **Bridge Domain Name (Nom du domaine de pont)** : répertorie tous les domaines de pont récupérés par Panorama. • **Tenant Name (Nom du tenant)** : affiche le tenant associé au domaine de pont répertorié. • **Bridge Domain Tag (Étiquette du domaine de pont)** : l'étiquette Panorama associée à chaque domaine de pont. • **Dynamic Address Group (Groupe d'adresses dynamiques)** : affiche les groupes d'adresses dynamiques associés à l'étiquette répertoriée. • **In Policy (Dans la politique)** : indique si le groupe d'adresses dynamiques répertorié est utilisé dans la politique.
Service Graphs (Graphiques de service)	Affiche le nombre total de graphiques de service surveillés par le plug-in, ainsi que le nombre de pare-feu en fonction des graphiques de service surveillés. Cliquez sur la vignette pour explorer et visualiser les colonnes suivantes. • **Service Graph Name (Nom du graphique de service)** : répertorie tous les graphiques de service récupérés par Panorama. • **Producer EPG (EPG du producteur)** : affiche l'EPG du producteur associé au graphique de service. • **FW InLine** : affiche le pare-feu associé au graphique de service.

©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur Cisco CSP

Vous pouvez déployer le pare-feu VM-Series en tant que service virtuel réseau sur la plate-forme Cisco Cloud Security (CSP). La plate-forme Cisco CSP étant une plate-forme KVM RHEL, le pare-feu VM-Series est déployé à l'aide du pare-feu VM-Series pour l'image de base KVM.

Avec le pare-feu VM-Series sur Cisco CSP, vous pouvez protéger vos charges de travail, empêcher les menaces avancées et améliorer la visibilité sur les applications de votre réseau virtuel.

- VM-Series sur Cisco CSP : configuration système requise
- Déploiement du pare-feu VM-Series sur Cisco CSP

VM-Series sur Cisco CSP : configuration système requise

Vous pouvez créer et déployer plusieurs instances, autonomes ou en tant que paire HA, du pare-feu VM-Series sur votre Cisco CSP.

Le pare-feu VM-Series possède les exigences suivantes :

- Consultez la matrice de compatibilité pour connaître les versions de CSP et PAN-OS prises en charge.
- Ensemble d'amorçage converti en fichier ISO
- Reportez-vous à la section Configuration système requise pour VM-Series pour obtenir la configuration matérielle minimale requise pour votre modèle VM-Series.
- Au moins deux interfaces de réseau (CNRV). Un vmNIC dédié pour l'interface de gestion et l'autre pour l'interface de données. Il est possible d'ajouter jusqu'à huit vmNIC supplémentaires pour le trafic de données.
- Le pare-feu VM-Series sur Cisco CSP prend en charge tous les modèles VM-Series à l'exception du VM-50.
- SR-IOV et mode Packet MMAP (Paquet MMAP) uniquement ; DPDK n'est pas pris en charge.

©2023 Palo Alto Networks, Inc.

Déploiement du pare-feu VM-Series sur Cisco CSP

Effectuez la procédure suivante pour déployer le pare-feu VM-Series sur Cisco CSP.

STEP 1 | Téléchargez le fichier image de base qcow2 VM-Series à partir du Portail assistance clientèle.

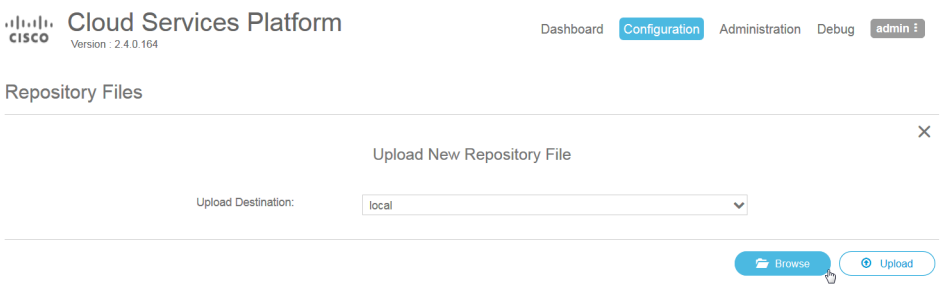
STEP 2 | Créez un fichier ISO d'amorçage pour le pare-feu VM-Series.

1. Créez un Ensemble d'amorçage pour votre pare-feu VM-Series.
2. Créez un fichier ISO contenant l'ensemble d'amorçage à l'aide de votre outil préféré.

STEP 3 | Connectez-vous à l'interface Web Cisco CSP.

STEP 4 | Téléchargez le fichier ISO et l'image qcow2 du pare-feu VM-Series.

1. Sélectionnez **Configuration** > **Repository (Référentiel)**.
2. Cliquez sur l'icône du plus (+).
3. Cliquez sur **Browse** (Parcourir) et accédez à votre fichier qcow2.
4. Cliquez sur **Upload (Télécharger)**.
5. Cliquez sur **Browse** (Parcourir) et accédez à votre fichier ISO.
6. Cliquez sur **Upload (Télécharger)**.



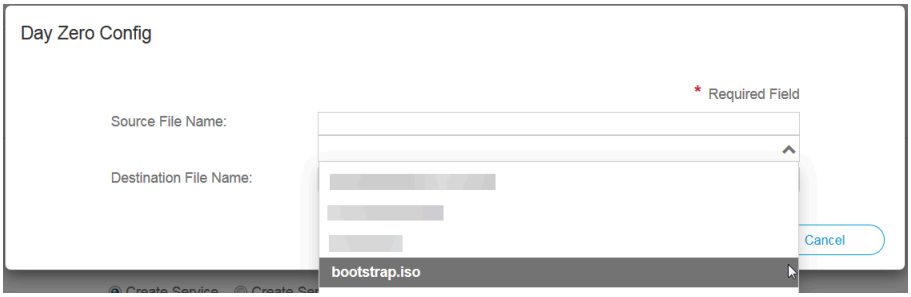
 ©2023 Palo Alto Networks, Inc.

STEP 5 | Créez le service de pare-feu VM-Series.

1. Saisissez un **Name** (Nom) descriptif au pare-feu VM-Series.
2. Sélectionnez le **Target Host Name** (Nom du serveur cible) dans la liste déroulante.
3. Sélectionnez le fichier qcow2 que vous avez chargé à partir de la liste déroulante **Image Name** (Nom de l'image).



4. Sélectionnez la Day Zero Config (Configuration du jour zéro).
   1. Cliquez sur l'icône du plus (+) de **Day Zero Config** (Configuration du jour zéro).
   2. Sélectionnez le fichier ISO d'amorçage dans la liste déroulante **Source File Name** (Nom du fichier source).
   3. Cliquez sur **Submit (Envoyer)**.



5. Allouez le nombre de cœurs et de mémoire requis pour votre Modèle de pare-feu VM-Series.
6. Ajoutez suffisamment de vNIC pour prendre en charge le nombre d'interfaces VM-Series configurées dans votre fichier ISO d'amorçage.

Reportez-vous à la section Documentation sur la plate-forme Cisco Cloud Service pour plus d'informations sur la création et le déploiement d'une instance de service.

STEP 6 | Une fois le processus d'amorçage terminé, connectez-vous à votre pare-feu VM-Series à l'aide de l'adresse IP de gestion que vous avez spécifiée dans le fichier ISO d'amorçage.

Le pare-feu doit être activé et configuré en fonction des paramètres que vous avez définis dans l'ensemble d'amorçage.

©2023 Palo Alto Networks, Inc.

Surveillance de terminal pour Cisco TrustSec

Installez et configurez le plug-in Panorama pour Cisco TrustSec afin de récupérer les adresses IP des terminaux dans votre environnement et d'élaborer une politique de sécurité pour ces terminaux en utilisant les groupes d'adresses dynamiques.

- Plug-in Panorama pour Cisco TrustSec
- Installation du plug-in Panorama pour Cisco TrustSec
- Configuration du plug-in Panorama pour Cisco TrustSec
- Dépannage du plug-in Panorama pour Cisco TrustSec

Plug-in Panorama pour Cisco TrustSec

Le plug-in Panorama pour Cisco TrustSec vous permet de créer une politique de sécurité pour votre environnement TrustSec en utilisant des groupes d'adresses dynamiques. Le plug-in surveille les changements dans les groupes de sécurité TrustSec, enregistre ces informations avec Panorama et transmet les informations d'IP au pare-feu, afin que Panorama puisse appliquer la bonne politique aux terminaux correspondants. Le plug-in Panorama pour Cisco TrustSec prend en charge jusqu'à 16 serveurs pxGrid (Cisco ISE).

Le plugin Panorama pour Cisco TrustSec prend actuellement en charge les objets dynamiques, mais pas les objets statiques.

Le plug-in Panorama traite les informations sur les terminaux et les convertit en un ensemble d'étiquettes que vous pouvez utiliser comme critères de correspondance pour le placement d'adresses IP dans les groupes d'adresses dynamiques. Panorama crée une étiquette pour chaque étiquette de groupe de sécurité (SGT) sur vos serveurs pxGrid. Les étiquettes sont créées dans le format suivant :

cts.svr_<pxgrid-server-name>.sgt_<SGT-name>

Pour récupérer les informations de mappage d'adresse IP à étiquette des terminaux, vous devez configurer une définition de surveillance pour chaque serveur pxGrid de votre environnement. La configuration du serveur pxGrid spécifie le nom d'utilisateur et le mot de passe et est référencée par la définition de surveillance qui permet à Panorama de se connecter au pxGrid. En outre, vous pouvez configurer le plug-in pour vérifier l'identité du serveur pxGrid avec un profil de certificat sur Panorama. Elle spécifie également les groupes d'appareils et les groupes de notification correspondants contenant les pare-feu auxquels Panorama envoie les étiquettes. Une fois que vous avez configuré la définition de surveillance et que le plug-in a récupéré les étiquettes, vous pouvez créer des groupes d'adresses dynamiques et ajouter les étiquettes en tant que critères de correspondance.

Le plug-in Panorama pour Cisco TrustSec versions 1.0.2 et ultérieures prend en charge les modes de surveillance Bulk Sync et PubSub. Le plug-in sélectionne un mode en fonction de la version de Panorama – mode Bulk Sync si la version de Panorama est antérieure à la 10.0.0 et mode PubSub sur Panorama version 10.0.0 ou ultérieure. L'interface utilisateur affiche les options de configuration pour le mode de surveillance par défaut.

- Bulk Sync
- PubSub

Bulk Sync

Le mode Bulk Sync utilise deux intervalles pour récupérer les informations de vos serveurs pxGrid : l'intervalle de surveillance et l'intervalle de synchronisation complète. Ce mode est le mode par défaut lorsque le plug-in Panorama pour Cisco TrustSec version 1.0.2 ou ultérieure est installé sur une version de Panorama antérieure à la 10.0.0. Les versions de Panorama antérieures à la 10.0.0 prennent en charge les mises à jour des onglets IP vers configd toutes les 10 secondes.

- **Intervalle de surveillance** : l'intervalle de surveillance est la durée pendant laquelle le plug-in attend avant de rechercher des modifications. Si aucune modification ne s'est produite, l'intervalle de surveillance est réinitialisé. S'il y a des modifications, le plug-in les traite avant de réinitialiser

©2023 Palo Alto Networks, Inc.

l'intervalle de surveillance. L'intervalle de surveillance par défaut est de 60 secondes. Vous pouvez définir l'intervalle de surveillance de 10 secondes à un jour (86 400 secondes).

L'intervalle de surveillance minimum est de 30 secondes lorsque le plug-in Panorama pour Cisco TrustSec 1.0.0 est installé.

- **Intervalle de synchronisation complète** : l'intervalle de synchronisation complète est la durée pendant laquelle le plug-in attend avant de mettre à jour les objets dynamiques de tous les serveurs pxGrid, quelles que soient les modifications apportées. Cela garantit que le plug-in est synchronisé avec le serveur pxGrid, même si un événement de modification est manqué par l'intervalle de surveillance. Vous pouvez définir un intervalle de synchronisation complète de 600 secondes (10 minutes) à 86 400 secondes (un jour). Vous devez configurer l'intervalle de synchronisation complète à partir de la CLI Panorama.

Si l'intervalle de surveillance est supérieure à l'intervalle de synchronisation complète, l'intervalle de synchronisation complète est ignoré et une synchronisation complète est effectuée à chaque intervalle de surveillance.

PubSub

Le mode PubSub surveille les notifications directement à partir du serveur Cisco ISE (le démon d'abonnement), analyse les étiquettes IP et transmet les informations pertinentes au démon de traitement des étiquettes. PubSub est le mode par défaut lorsque le plug-in Panorama pour Cisco TrustSec version 1.0.2 ou ultérieure est installé sur la version 10.0.0 ou ultérieure de Panorama. Les versions 10.0.0 et ultérieures de Panorama prennent en charge les mises à jour des onglets IP vers configd toutes les 100 millisecondes.

- **Intervalle de push** : l'intervalle de push est la durée entre les push. Si le push précédent dure trop longtemps, le push suivant se déclenche dès qu'il est terminé. L'intervalle de push minimum est de 100 millisecondes (0 secondes) et le maximum est de 60 secondes. L'intervalle de push par défaut est de 0 secondes.
- **Activer la synchronisation complète** : activez cette option pour déclencher une mise à jour complète. Si vous activez la synchronisation complète, vous pouvez définir l'intervalle de synchronisation complète. La valeur par défaut est non.
- **Intervalle de synchronisation complète** : l'intervalle de synchronisation complète est la durée pendant laquelle le plug-in attend avant de mettre à jour les objets dynamiques de tous les serveurs pxGrid, quelles que soient les modifications apportées. L'intervalle de synchronisation complète par défaut est de 10 minutes. Vous pouvez définir un intervalle de synchronisation complète de 600 secondes (10 minutes) à 86 400 secondes (un jour). Vous devez configurer l'intervalle de synchronisation complète à partir de la CLI Panorama.
- **Intervalle de reconnexion** – l'intervalle de reconnexion initial est de 1 seconde, et il est doublé si la reconnexion précédente a échoué. L'intervalle de reconnexion maximum est de 64 s. Il n'y a pas de limite au nombre de tentatives de reconnexion.

©2023 Palo Alto Networks, Inc.

Installation du plug-in Panorama pour Cisco TrustSec

Pour commencer à surveiller les terminaux avec Cisco TrustSec, téléchargez et installez le plug-in Cisco TrustSec sur Panorama. Pour corréler la version du plugin avec la version de Panorama, consultez les plugins Panorama dans la matrice de compatibilité.

La mise à niveau ou la rétrogradation d'un plugin Cisco TrustSec nécessite une validation.

Si vous avez une configuration d'HA de Panorama, répétez ce processus d'installation sur chaque pair de Panorama. Lors de l'installation du plug-in sur des appareils Panorama d'une paire HA, installez le plug-in sur l'homologue passif avant l'homologue actif. Après avoir installé le plug-in sur l'homologue passif, il passera à un état non fonctionnel. L'installation du plug-in sur l'homologue actif renvoie l'homologue passif à un état fonctionnel.

Si vous avez un appareil Panorama autonome ou deux appareils Panorama installés dans une paire HA avec plusieurs plug-ins installés, les plug-ins peuvent ne pas recevoir les informations des indicateurs d'adresse IP mises à jour si un ou plusieurs des plug-ins ne sont pas configurés. Cela se produit, car Panorama ne transfère pas les informations des indicateurs d'adresse IP aux plug-ins non configurés. De plus, ce problème peut se présenter si un ou plusieurs plug-ins Panorama ne se trouvent pas dans l'état Registered (Enregistré) ou Success (Réussite) (l'état positif diffère sur chaque plug-in). Assurez-vous que vos plug-ins se trouvent dans l'état positif avant de continuer ou d'exécuter les commandes décrites ci-dessous.

Si vous rencontrez ce problème, il existe deux solutions alternatives :

- Désinstallez le ou les plug-ins non configurés. Il est déconseillé d'installer un plug-in que vous n'envisagez pas de configurer dans l'immédiat
- Vous pouvez utiliser les commandes suivantes pour contourner ce problème. Exécutez la commande suivante pour chaque plug-in non configuré sur chaque instance de Panorama afin que Panorama n'attende pas pour envoyer des mises à jour. Dans le cas contraire, vos pare-feu risquent de perdre certaines informations des indicateurs d'adresse IP.

  `request plugins dau plugin-name <plugin-name> unblock-device-push yes`

  Vous pouvez annuler cette commande en exécutant :

  `request plugins dau plugin-name <plugin-name> unblock-device-push no`

Les commandes décrites ne sont pas persistantes lors des redémarrages et doivent être réutilisées pour tout redémarrage ultérieur. Pour Panorama en paire HA, les commandes doivent être exécutées sur chaque Panorama.

STEP 1 | Sélectionnez **Panorama** > **Plugins**.

STEP 2 | Cliquez sur **Check Now (Vérifier maintenant)** pour obtenir la dernière version du plug-in.

STEP 3 | Sélectionnez **Download (Télécharger)** dans la colonne Action pour installer le plug-in (module d'extension).

STEP 4 | Sélectionnez la version du plug-in et cliquez sur **Install (Installer)** dans la colonne Action pour installer le plug-in. Panorama vous alertera lorsque l'installation est terminée.

©2023 Palo Alto Networks, Inc.

Configuration du plug-in Panorama pour Cisco TrustSec

Après avoir installé le plug-in, vous devez également attribuer un groupe de notification à la configuration de votre plug-in Cisco TrustSec. Un groupe de notification est une liste de groupes de périphériques qui comprend les pare-feu vers lesquels Panorama doit pousser toutes les étiquette qu'il récupère sur le serveur pxGrid.

Chaque Panorama avec le plug-in Cisco TrustSec installé peut prendre en charge jusqu'à 16 serveurs pxGrid et 16 définitions de surveillance. Et chaque définition de surveillance possède un serveur pxGrid et un groupe de notification.

Le plugin Panorama pour Cisco TrustSec prend actuellement en charge les objets dynamiques, mais pas les objets statiques.

Les instructions de configuration suivantes couvrent à la fois les modes de surveillance Bulk Sync et PubSub ; certaines fonctionnalités de l'interface utilisateur sont activées, ou visibles en fonction du mode de surveillance.

STEP 1 | Configurez l'intervalle de synchronisation complète si vous souhaitez modifier la valeur par défaut de 600 secondes (10 minutes).

1. Connectez-vous à la CLI Panorama.
2. Passez en mode de configuration.

   ```
   admin@Panorama> configure
   ```
3. Utilisez la commande suivante pour définir l'intervalle de synchronisation complète. La plage est comprise entre 600 et 86 400 secondes (un jour).

   ```
   admin@Panorama# set plugins cisco_trustsec full-sync-interval
   <interval-in-seconds>
   ```

STEP 2 | Connectez-vous à l'interface Web Panorama.

STEP 3 | Vous devez ajouter les pare-feu comme dispositifs gérés sur Panorama et créer des groupes d'appareils de façon à pouvoir configurer Panorama pour aviser ces groupes à l'aide de l'information VM qu'il récupère. Les groupes d'appareils peuvent inclure des pare-feu de série VM ou des systèmes virtuels sur les pare-feu matériels.

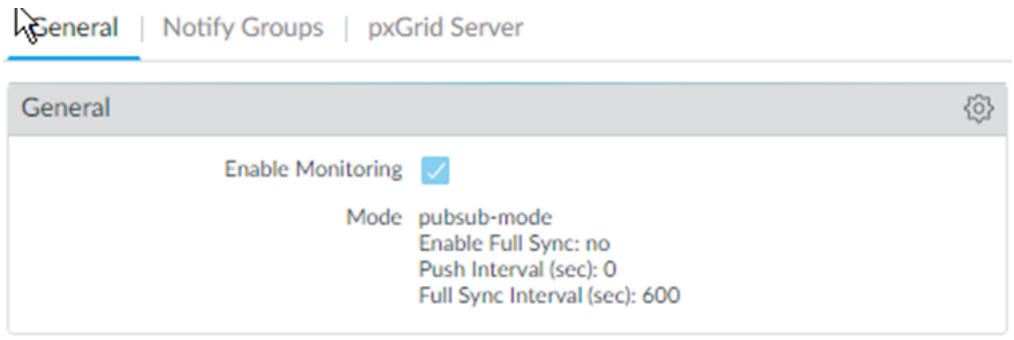
©2023 Palo Alto Networks, Inc.

STEP 4 | Configurez la surveillance Cisco TrustSec.

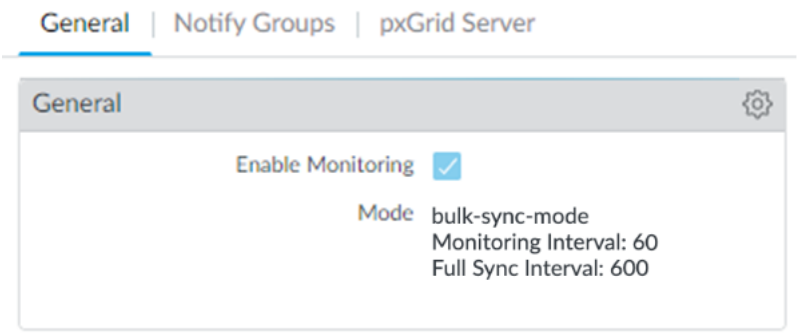
1. Sélectionnez **Panorama** > **Cisco TrustSec** > **Setup (Configuration)** > **General (Général)**.

   Enable Cisco TrustSec Monitoring (Activer la surveillance Cisco TrustSec) est activé par défaut. Cela active la surveillance de tous les clusters de votre déploiement.

   L'interface utilisateur sélectionne le mode de surveillance PubSub si le plugin Panorama pour Cisco TrustSec 1.0.2 ou supérieur est installé sur Panorama 10.0.0 ou supérieur :

   Le plugin sélectionne le mode Bulk Sync (Synchronisation en masse) lorsqu'il est installé sur une version de Panorama inférieure à 10.0.0 :

2. Cliquez sur l'icône « engrenage » pour modifier les paramètres de configuration.

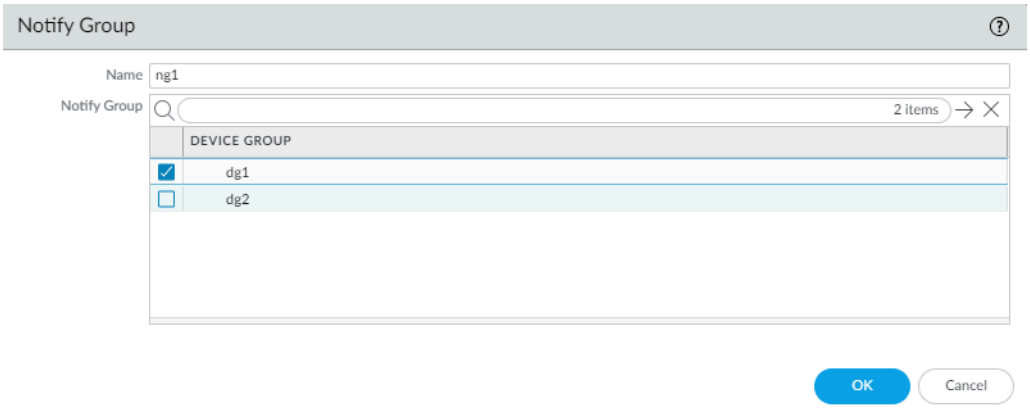
   - **Push Interval (Intervalle de push)** (PubSub uniquement)—Minimum 0, maximum 60 secondes, la valeur par défaut est 0 (100 millisecondes).
   - **Enable Full Sync (Activer synchronisation complète)** (PubSub uniquement, en option)—Sélectionnez cette option pour activer la synchronisation complète. La valeur par défaut est non.
   - **Full Sync Interval (Intervalle de synchronisation complète)**.
     - PubSub—Si Enable Full Sync (Activer synchronisation complète) est sélectionné, vous pouvez régler l'intervalle de synchronisation complète en secondes. La plage est de 600 secondes à 86 400 secondes (un jour), et la valeur par défaut est de 600
     - Bulk Sync (Synchronisation en masse)—Activé par défaut en mode de synchronisation en masse. La plage est de 600 secondes à 86 400 secondes (un jour), et la valeur par défaut est de 600.
   - **Monitoring Interval (Intervalle de surveillance)** (Bulk Sync uniquement)—10 à 86 400 secondes, la valeur par défaut est 60 - Définit l'intervalle d'interrogation durant lequel Panorama interroge le serveur pxGrid pour obtenir des informations sur les

 ©2023 Palo Alto Networks, Inc.

adresses des points terminaux. Il s'agit de la période entre la fin d'un événement de surveillance et le début de l'événement suivant.

STEP 5 | Créez un groupe de notification.

1. Sélectionnez **Panorama** > **Cisco TrustSec** > **Setup (Configuration)** > **Notify Groups (Groupes de notification)**.
2. Cliquez sur **Add (Ajouter)**.
3. Saisissez un **Name** (Nom) descriptif pour votre groupe de notification.
4. Sélectionnez les groupes de périphériques que vous avez créés précédemment.



STEP 6 | (Facultatif) Si vous activez la vérification de l'identité du serveur sur le serveur pxGrid, configurez un profil de certificat sur Panorama.

STEP 7 | Créez, activez et acceptez le nom du client pxGrid et le mot de passe du client.

1. Connectez-vous à la CLI Panorama.
2. Exécutez la commande suivante pour créer le nom du client.
   - Si vous avez un profil de certificat, créez le nom du client comme suit :

     admin@Panorama> request plugins cisco_trustsec create-account client-name <client-name> host <ise-server-ip>
   - Si vous avez ignoré l'étape 6 et que vous n'avez pas de certificat, saisissez :

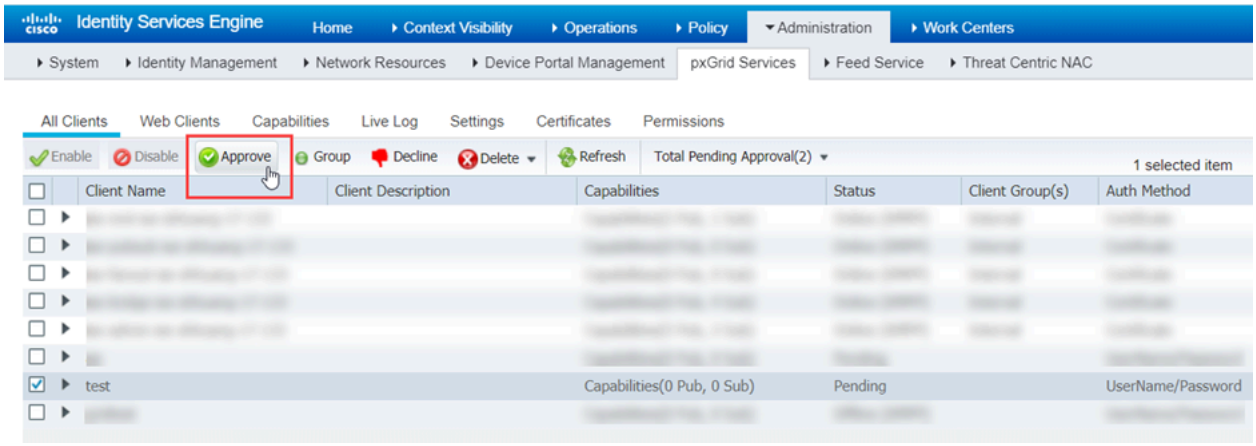
     request plugins cisco_trustsec create-account server-cert-verification-enabled no client-name <client-name>host <host-name>
3. Exécutez la commande suivante pour créer le nom du client.

```
admin@Panorama> request plugins cisco_trustsec create-
account client-name test host 10.10.10.15 AccountCreate in
 progress... AccountCreate successful.   client nodename:
 test client password: PmVKBmPgf63Hypq AccountActivate in
```

 ©2023 Palo Alto Networks, Inc.

```
progress... AccountActivate successful. Please approve the
account on the server.
```

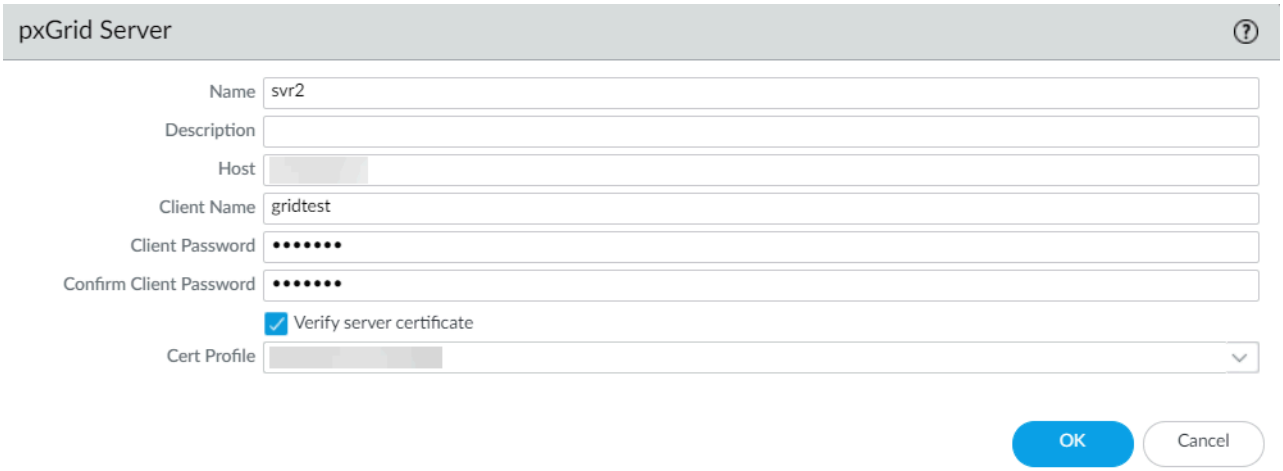
4. Connectez-vous au serveur Cisco ISE pour accepter le compte.
5. Sélectionnez **Administration** > **pxGrid Services (Services pxGrid)** > **All Clients (Tous les clients)**.
6. Sélectionnez le nom du client que vous créez sur Panorama.
7. Cliquez sur **Approve (Accepter)**.



 ©2023 Palo Alto Networks, Inc.

STEP 8 | Ajoutez les informations sur les serveurs pxGrid. Le plug-in Panorama pour Cisco TrustSec prend en charge jusqu'à 16 serveurs pxGrid (Cisco ISE).

1. Sélectionnez **Panorama** > **Cisco TrustSec** > **Setup (Configuration)** > **pxGrid Server (Serveur pxGrid)**.
2. Saisissez un **nom** descriptif pour votre serveur pxGrid.
3. Dans le champ **Host (Hôte)**, saisissez l'adresse IP ou le FQDN de votre serveur pxGrid.
4. Saisissez le nom du client que vous avez créé à l'étape précédente.
5. Saisissez et confirmez le mot de passe du client que vous avez généré à l'étape précédente.
6. Vérifiez l'identité du serveur pxGrid.
   1. Sélectionnez **Verify server certificate (Vérifier le certificat du serveur)**.
   2. Sélectionnez le profil de votre certificat depuis la liste déroulante **Cert Profile (Profil du certificat)**.
7. Cliquez sur **OK**.



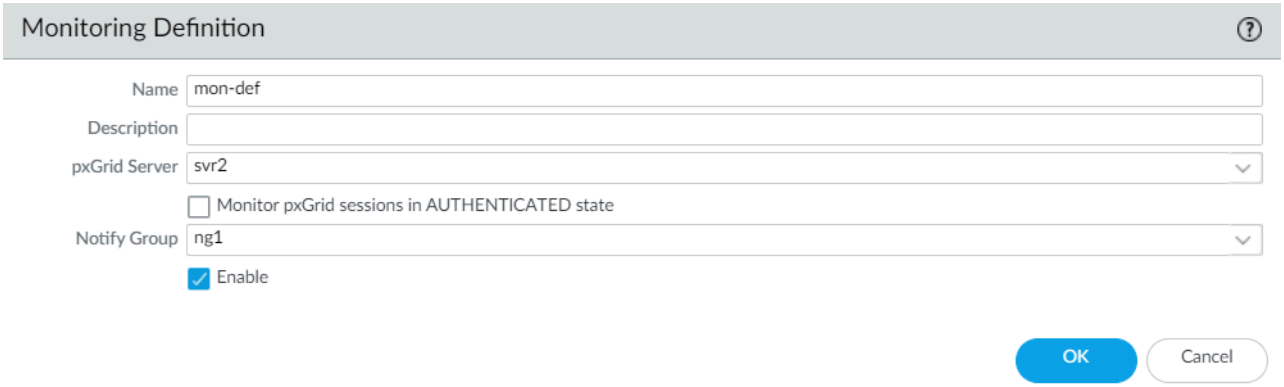
STEP 9 | Configurez la définition de surveillance.

1. Sélectionnez **Panorama** > **Cisco TrustSec** > **Monitoring Definition (Définition de surveillance)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un **nom** descriptif et éventuellement une **description** pour identifier la définition de surveillance.
3. Sélectionnez le **serveur pxGrid**.
4. (Facultatif) Configurez Panorama de manière à **surveiller les sessions pxGrid en état AUTHENTICATED (AUTHENTIFIÉE)**. Par défaut, Panorama récupère les mappages IP-Tag à partir des sessions en état « Started » (Démarrée). Les sessions ISE ont l'état « Started » (Démarrée) lorsqu'il y a un paquet de démarrage comptable correspondant.

©2023 Palo Alto Networks, Inc.

Si aucun paquet de démarrage comptable n'est présent pour la session, alors l'état de la session est « AUTHENTICATED » (AUTHENTIFIÉE).

5. Sélectionnez le **Notify Group (Groupe de notification)**.
6. Cliquez sur **OK**.



STEP 10 | **Commit (Validez)** vos modifications.

STEP 11 | Créez des sessions ISE actives afin que Panorama puisse apprendre les étiquettes SGT pour le groupe d'adresses dynamiques. Pour créer des sessions actives, utilisez ISE pour authentifier les périphériques.

Panorama ne collecte pas les étiquettes SGT par défaut sur ISE.

 ©2023 Palo Alto Networks, Inc.

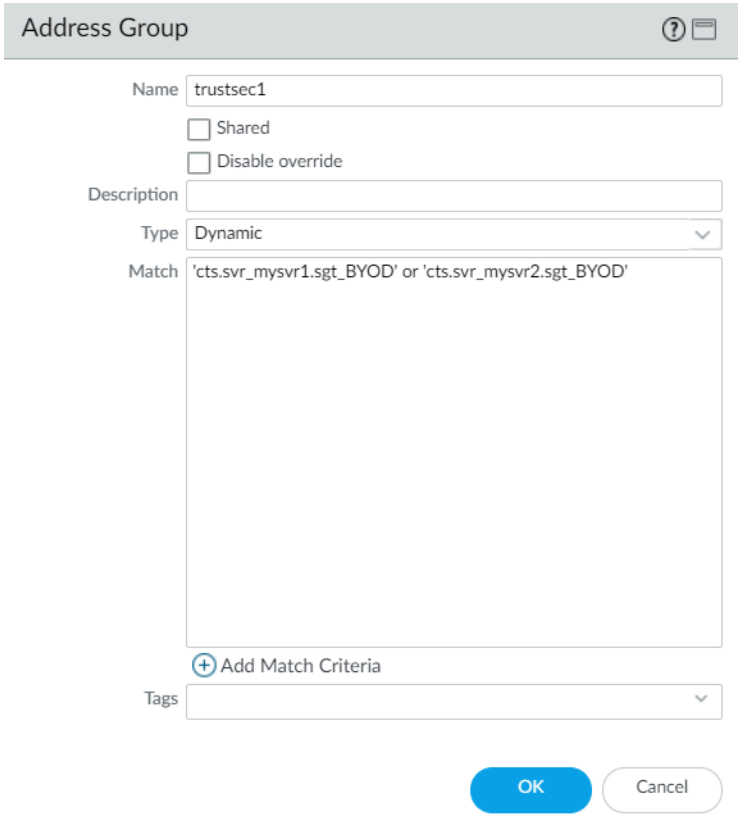
STEP 12 | Créez des groupes d'adresses dynamiques et vérifiez que les adresses sont ajoutées aux groupes d'adresses dynamiques.

1. Sélectionnez **Objects (Objets)** > **Address Groups (Groupes d'adresses)**.
2. Sélectionnez le groupe de périphériques que vous avez créé pour les terminaux de surveillance dans votre environnement Cisco TrustSec dans la liste déroulante **Device Group (Groupe de périphériques)**.
3. Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** et une **Description** pour le groupe d'adresses dynamiques.

   La convention de dénomination du Dynamic Address Group (groupe d'adresses dynamiques) est : **`cts.svr_<server-name>.sgt_<SGT-name>`**
4. Définissez le **Type (type)** sur **Dynamic (Dynamique)**.
5. Cliquez sur **Add Match Criteria (Ajouter des critères de correspondance)**.
6. Sélectionnez l'opérateur **And (Et)** ou **Or (Ou)** et cliquez sur l'icône plus (+) à côté du nom du groupe de sécurité pour l'ajouter au groupe d'adresses dynamiques.

   Panorama ne peut afficher que les étiquettes de groupe de sécurité qu'il a apprises lors des sessions actives. Les étiquettes de groupe de sécurité dans les sessions en direct apparaissent dans la liste des critères de correspondance.
7. Sélectionnez **Panorama** > **Objects (Objets)** > **Address Groups (Groupes d'adresses)**.
8. Cliquez sur **More (Plus)** dans la colonne Addresses (Adresses) d'un groupe d'adresses dynamiques.

   Panorama affiche une liste des adresses IP ajoutées à ce groupe d'adresse dynamique en fonction des critères de correspondance que vous avez spécifiés.



 ©2023 Palo Alto Networks, Inc.

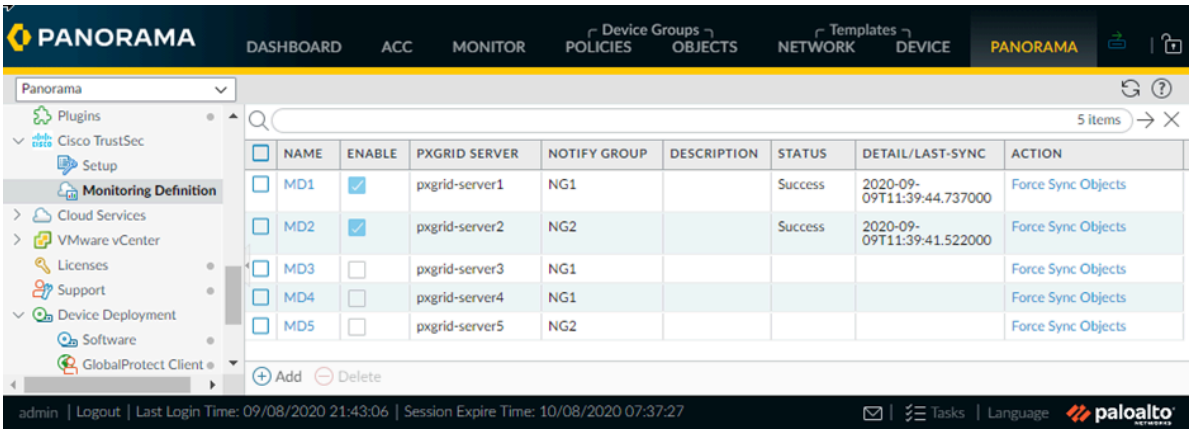
STEP 13 | Utilisez des groupes d'adresses dynamiques dans une politique.

Les groupes d'adresses dynamiques sont vides jusqu'à ce que vous les rattachiez à une politique. Vous ne verrez aucune adresse IP dans votre groupe d'adresses dynamiques, à moins qu'une politique ne l'utilise.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Cliquez sur **Add (Ajouter)** et saisissez un **Name (nom)** et une **Description (description)** pour identifier la politique.
3. Ajoutez la **Source Zone (Zone source)** pour indiquer la zone d'où provient le trafic.
4. Ajoutez la **Destination Zone (Zone de destination)** dans laquelle se termine le trafic.
5. Pour **Destination Address (Adresse de destination)**, sélectionnez le groupe d'adresses dynamiques que vous venez de créer.
6. Indiquez l'action (**Allow (Autoriser)** ou **Deny (Refuser)**) pour le trafic, puis associez éventuellement les profils de sécurité par défaut à la règle.
7. Répétez les étapes 1 à 6 pour créer une autre règle de politique.
8. Cliquez sur **Commit (Valider)**.

STEP 14 | (Facultatif) Mettez à jour les objets dynamiques à partir du serveur pxGrid à tout moment en synchronisant les objets dynamiques. La synchronisation des objets dynamiques vous permet de conserver le contexte des modifications dans l'environnement virtuel et vous permet d'activer des applications grâce à la mise à jour automatique des groupes d'adresses dynamiques utilisés dans les règles de politique.

1. Sélectionnez **Panorama** > **Cisco TrustSec** > **Monitoring Definition (Définition de surveillance)**.
2. Cliquez sur **Synchronize Dynamic Objects** (Synchroniser les objets dynamiques).



 ©2023 Palo Alto Networks, Inc.

Dépannage du plug-in Panorama pour Cisco TrustSec

- Commandes d'état du plug-in
- Commandes de débogage
- Journaux de débogage

Commandes d'état du plug-in

- Effacer les compteurs :

```
clear plugins cisco_trustsec counters
```

- Afficher l'état de surveillance :

```
show plugins cisco_trustsec status
```

- Afficher les compteurs :

```
show plugins cisco_trustsec counters
```

Commandes de débogage

- Vérifier les adresses IP dans les groupes d'adresses dynamiques.

```
show object registered-ip tag <tag>
```

```
show object registered-ip all
```

- Récupérer les étiquettes d'une adresse IP depuis un serveur. Les mappages d'étiquettes d'adresse IP récupérés sont consignés dans **plugin_cisco_trustsec.log**. Aucun mappage d'étiquette d'adresse IP n'est transmis au groupe de notification associé au serveur. Aucune nouvelle tentative en cas d'échec.

```
debug plugins cisco_trustsec query pxgrid-server $server-name ip
 $ip-address
```

- Forcer la synchronisation avec un serveur et transmettre les mappages au processus configd. Aucune nouvelle tentative en cas d'échec.

```
request plugins cisco_trustsec synchronize-dynamic-objects name
 $server-name
```


©2023 Palo Alto Networks, Inc.

- Forcer la synchronisation avec tous les serveurs et transmettre les mappages au processus configd. Aucune nouvelle tentative en cas d'échec.

```
request plugins cisco_trustsec synchronize-dynamic-objects all
```

- Forcer la synchronisation des mappages à partir du processus configd vers les pare-feu VM-Series. Aucune nouvelle tentative en cas d'échec.

```
request plugins cisco_trustsec sync
```

Journaux de débogage

Les journaux se trouvent dans les emplacements suivants sur le disque :

```
/opt/plugins/var/log/pan/plugin_cisco_trustsec.log /opt/plugins/
var/log/pan/plugin_cisco_trustsec_sub.log /opt/plugins/var/
log/pan/plugin_cisco_trustsec_ret.log /opt/plugins/var/log/pan/
plugin_cisco_trustsec_proc.log
```

La limite de taille d'un fichier journal (partagé par tous les plug-ins installés sur votre périphérique Panorama) est de 10 millions d'octets. Un fichier journal peut accepter 93 000 connexions de session. Si vous configurez la rotation des journaux, un journal de sauvegarde peut prendre en charge 186 000 connexions de session.

- Modifier le niveau de débogage du plug-in.

```
request plugins debug level $level plugin-name cisco_trustsec
```

  - **désactivé** : aucun journal de débogage.
  - **faible** : vider uniquement les journaux de débogage de base.
  - **moyen** : vider les journaux de débogage détaillés.
  - **élevé** : vider tout, y compris les messages de requête/réponse avec les serveurs.
- Fusionner les journaux en un fichier journal unique :

```
request plugins cisco_trustsec merge-logs
```

- Afficher le journal de débogage dans la CLI :
  - Plug-in Cisco TrustSec version 1.0.2 ou ultérieure installée sur une version de Panorama antérieure à la 10.0.0 :

```
tail mp-log plugin_cisco_trustsec_merged.log
```

  - Plug-in Cisco TrustSec version 1.0.2 ou ultérieure installée sur Panorama version 10.0.0 ou ultérieure :

```
tail follow yes plugins-log
```


©2023 Palo Alto Networks, Inc.

Configuration du pare-feu VM-Series sur Nutanix AHV

Le pare-feu VM-Series pour Nutanix AHV vous permet de déployer le pare-feu VM-Series sur les périphériques capables d'exécuter l'hyperviseur Nutanix Acropolis. Si vous utilisez Panorama afin de gérer vos pare-feu VM-Series sur Nutanix AHV, vous pouvez utiliser le plug-in Panorama pour Nutanix afin d'effectuer la surveillance VM. Cela vous permet d'informer de manière dynamique le pare-feu de tout changement dans votre environnement Nutanix. Ainsi, vous avez l'assurance que votre politique est appliquée aux machines virtuelles au fur et à mesure qu'elles rejoignent votre réseau.

- Déploiement du pare-feu VM-Series sur Nutanix AHV
- Surveillance VM sur Nutanix

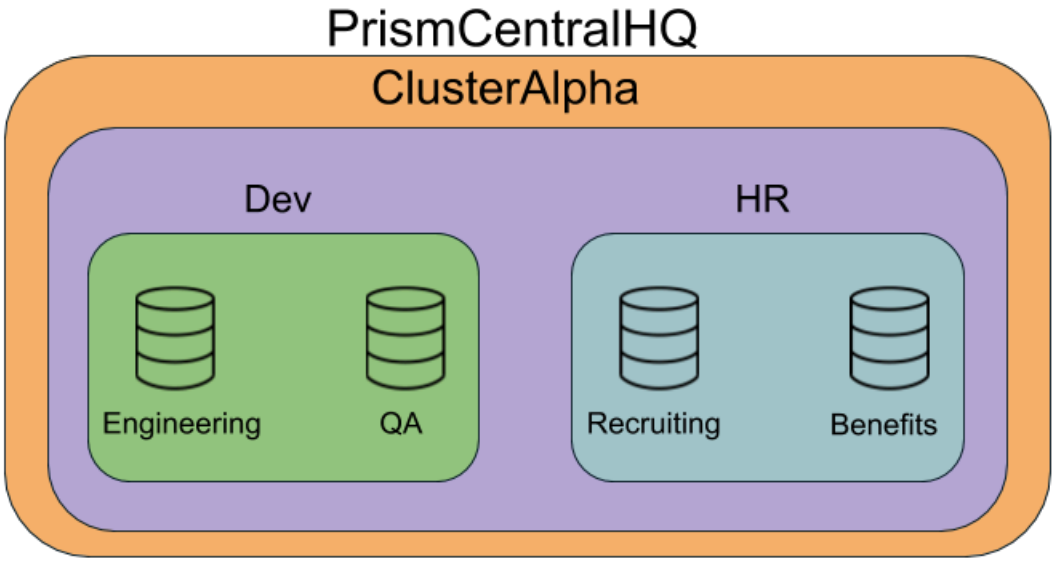
Surveillance VM sur Nutanix

Installez et configurez le plug-in Panorama pour Nutanix afin de surveiller les modifications dans votre environnement Nutanix et créer une politique à l'aide des groupes d'adresses dynamiques.

- À propos de la surveillance VM sur Nutanix
- Installation du plug-in Panorama pour Nutanix
- Configuration du plug-in Panorama pour Nutanix

À propos de la surveillance VM sur Nutanix

Le plug-in Panorama pour Nutanix facilite l'utilisation de groupes d'adresses dynamiques en surveillant les machines virtuelles dans votre environnement Nutanix. Prism Central regroupe les entités dans vos environnements Nutanix par catégories et les filtre ensuite par valeur. Panorama crée des étiquettes basées sur les catégories et valeurs que vous définissez dans Prism Central. Lorsqu'une machine virtuelle est placée dans une catégorie et se voit attribuer une valeur, Panorama applique l'étiquette correspondante à l'adresse IP de la machine virtuelle. Vous pouvez ensuite créer une politique de sécurité en utilisant des étiquettes comme critères de correspondance pour des groupes d'adresses dynamiques dans Panorama.



Dans l'exemple ci-dessus, nous disposons de deux catégories – Dev et HR – avec deux valeurs dans chacune d'elles. Et ces catégories font partie du cluster, qui fait partie de Prism Central. Après avoir commencé à surveiller votre environnement Nutanix, Panorama utilise la valeur, la catégorie, le cluster et Prism Central pour former des étiquettes. Lorsque vous affichez les critères de correspondance pour les groupes d'adresses dynamiques, les étiquettes sont répertoriées au format suivant.

ntnx.PC-<prism-central-name>.CL-<cluster-name>.<category>.<value>

Avec les informations dans l'exemple ci-dessus, Panorama crée les étiquettes suivantes.

`ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.Dev.Engineering`

©2023 Palo Alto Networks, Inc.

ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.Dev.QA

ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.HR.Recruiting

ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.HR.Benefits

Pour sécuriser ces charges de travail dans ces catégories, utilisez ce type d'étiquettes comme critères de correspondance dans des groupes d'adresses dynamiques. Vous pouvez ensuite utiliser les groupes d'adresses dynamiques comme groupes d'adresses source et de destination dans vos règles de politique de sécurité. Lorsqu'une machine virtuelle rejoint un groupe d'adresse dynamique, la politique que vous avez créée s'applique automatiquement.

Installation du plug-in Panorama pour Nutanix

Pour démarrer avec la surveillance des terminaux sur Nutanix, téléchargez et installez le plug-in Panorama for Nutanix.

Si vous avez une configuration d'HA de Panorama, répétez ce processus d'installation sur chaque pair de Panorama. Lors de l'installation de la fiche sur les Panoramas d'une paire HA, installez la fiche sur le pair passif avant le pair actif. Après avoir installé le plug-in sur l'homologue passif, il passera à un état non fonctionnel. L'installation du plug-in sur l'homologue actif renvoie l'homologue passif à un état fonctionnel.

Si vous avez un appareil Panorama autonome ou deux appareils Panorama installés dans une paire HA avec plusieurs plug-ins installés, les plug-ins peuvent ne pas recevoir les informations des indicateurs d'adresse IP mises à jour si un ou plusieurs des plug-ins ne sont pas configurés. Cela se produit, car Panorama ne transfère pas les informations des indicateurs d'adresse IP aux plug-ins non configurés. De plus, ce problème peut se présenter si un ou plusieurs plug-ins Panorama ne se trouvent pas dans l'état Registered (Enregistré) ou Success (Réussite) (l'état positif diffère sur chaque plug-in). Assurez-vous que vos plug-ins se trouvent dans l'état positif avant de continuer ou d'exécuter les commandes décrites ci-dessous.

Si vous rencontrez ce problème, il existe deux solutions alternatives :

- Désinstallez le ou les plug-ins non configurés. Il est déconseillé d'installer un plug-in que vous n'envisagez pas de configurer dans l'immédiat
- Vous pouvez utiliser les commandes suivantes pour contourner ce problème. Exécutez la commande suivante pour chaque plug-in non configuré sur chaque instance de Panorama afin que Panorama n'attende pas pour envoyer des mises à jour. Dans le cas contraire, vos pare-feu risquent de perdre certaines informations des indicateurs d'adresse IP.

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  Vous pouvez annuler cette commande en exécutant :

  request plugins dau plugin-name <plugin-name> unblock-device-push no

Les commandes décrites ne sont pas persistantes lors des redémarrages et doivent être réutilisées pour tout redémarrage ultérieur. Pour Panorama en paire HA, les commandes doivent être exécutées sur chaque Panorama.

STEP 1 | Connectez-vous à l'interface utilisateur de Panorama.

STEP 2 | Sélectionnez **Panorama** > **Plugins**.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Sélectionnez **Check Now (Vérifiez maintenant)**pour récupérer la liste des mises à jour disponibles.

STEP 4 | Sélectionnez **Download (Télécharger)** dans la colonne Action pour installer le plug-in (module d'extension).

STEP 5 | Sélectionnez la version du plug-in et cliquez sur **Install (Installer)** dans la colonne Action pour installer le plug-in. Panorama vous alertera lorsque l'installation est terminée.

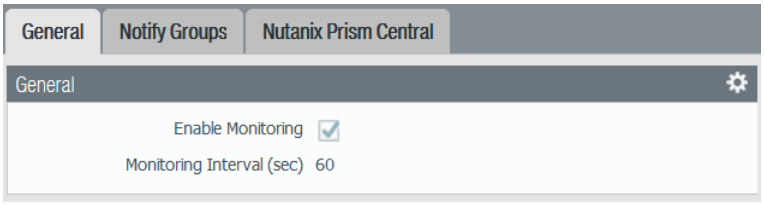
Configuration du plug-in Panorama pour Nutanix

Après avoir installé le plug-in, effectuez la procédure suivante pour établir une connexion entre Panorama et Prism Central.

STEP 1 | Connectez-vous à l'interface Web Panorama.

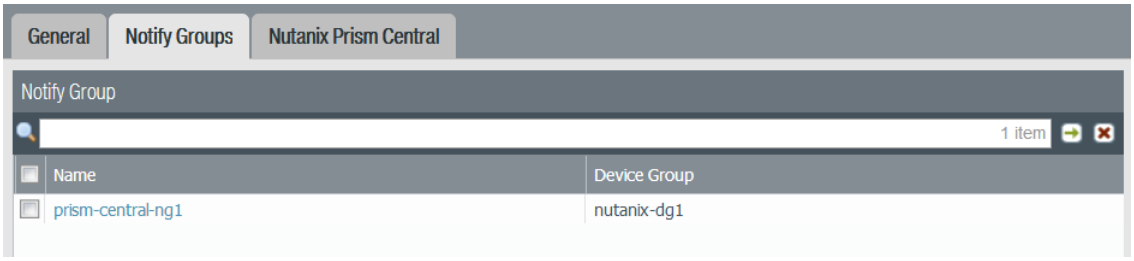
STEP 2 | Activez la surveillance et définissez l'intervalle de surveillance.

1. Sélectionnez **Panorama** > **Nutanix** > **Setup (Configuration)** > **General**.
2. Sélectionnez **Enable Monitoring** (Activer la surveillance).
3. Définissez le **Monitoring Interval** (Intervalle de surveillance) en secondes. L'intervalle de surveillance correspond à la fréquence à laquelle Panorama récupère les informations réseau mises à jour à partir de Prism Central.



STEP 3 | Créez un groupe de notification.

1. Sélectionnez **Panorama** > **Nutanix** > **Setup (Configuration)** > **Notifiy Groups (Groupes de notification)**.
2. Cliquez sur **Add (Ajouter)**.
3. Saisissez un **Name** (Nom) descriptif pour votre groupe de notification.
4. Sélectionnez les groupes de périphériques dans votre déploiement de Nutanix.



 ©2023 Palo Alto Networks, Inc.

STEP 4 | Ajoutez les informations Prism Central.

1. Sélectionnez **Panorama** > **Nutanix** > **Setup (Configuration)** > **Nutanix Prism Central**.
2. Cliquez sur **Add (Ajouter)**.
3. Saisissez un **Name (Nom)** descriptif pour votre Prism Central.
4. Saisissez l'adresse IP ou le FQDN pour Prism Central.
5. Saisissez votre nom d'utilisateur Prism Central.
6. Saisissez et confirmez votre mot de passe Prism Central.
7. Cliquez sur **Validate (Valider)** pour confirmer que vous avez bien saisi les informations d'identification Prism Central.

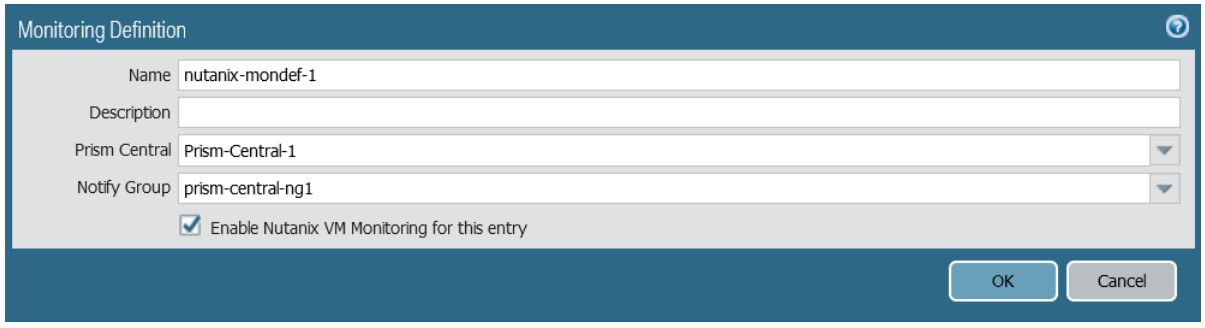
   Si vous retournez dans la fenêtre Nutanix Prism Central Info après avoir cliqué sur OK et que vous cliquez sur le bouton Validate (Valider), vous recevrez un message d'erreur de validation des informations d'identification. Ceci est le comportement attendu. Même si Panorama affiche des points dans le champ consacré au mot de passe, le champ est vide ; la validation ne fonctionnera donc pas, même si Panorama est bien connecté à Prism Central.

8. Cliquez sur **OK**.



STEP 5 | Configurez la définition de surveillance.

1. Sélectionnez **Panorama** > **Nutanix** > **Monitoring Definition (Définition de surveillance)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name** (Nom) descriptif et éventuellement une Description pour identifier le Prism Central pour lequel vous utilisez cette définition.
3. Sélectionnez le **Prism Central** et le **Notify Group (Groupe de notification)**.
4. Cliquez sur **OK**.

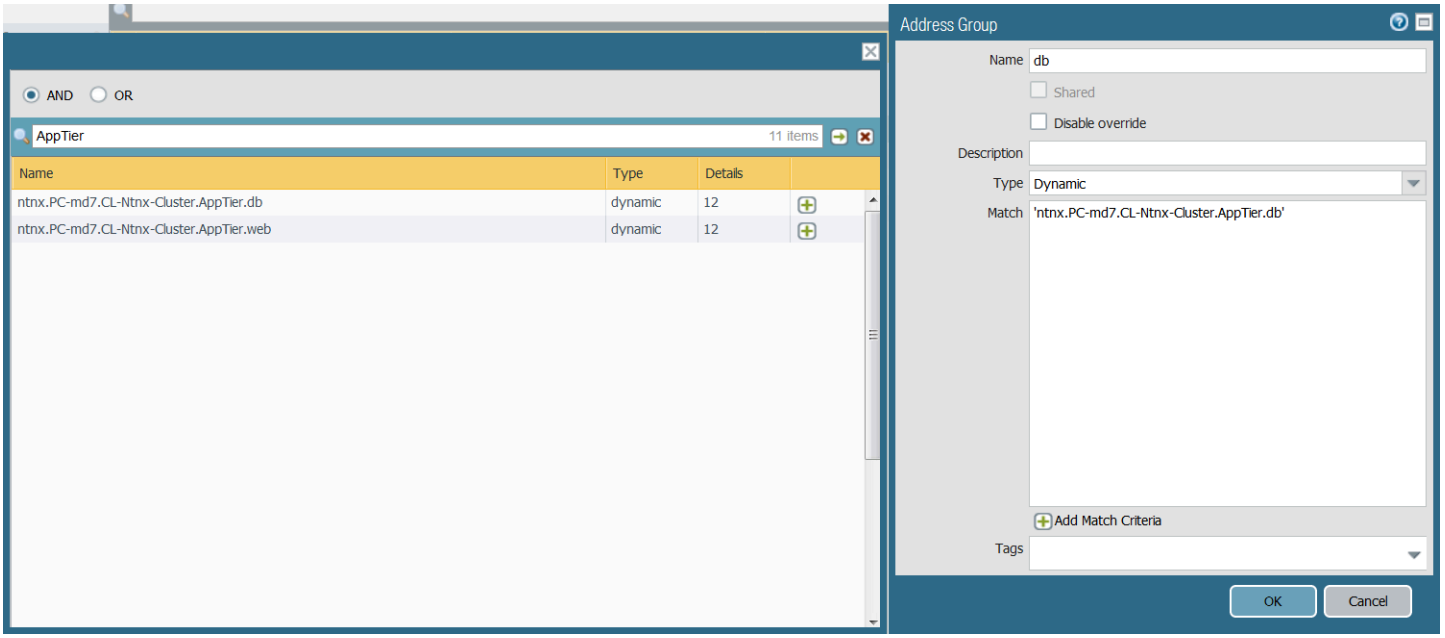


 ©2023 Palo Alto Networks, Inc.

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

STEP 7 | Vérifiez que vous pouvez visualiser l'information VM sur Panorama et définir les critères d'appariement pour les groupes d'adresses dynamiques.

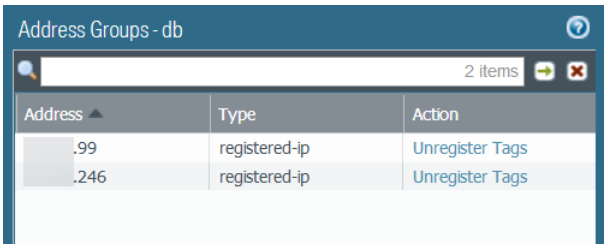
1. Sélectionnez **Panorama** > **Objects (Objets)** > **Address Groups (Groupes d'adresses)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** descriptif pour vos groupes d'adresses dynamiques.
3. Sélectionnez **Dynamic (Dynamique)** dans la liste déroulante Type.
4. Cliquez sur **Add Match Criteria (Ajouter des critères de correspondance)**. Vous pouvez sélectionner des étiquettes dynamiques comme critères de correspondance pour renseigner les membres du groupe. Sélectionnez l'opérateur **And (Et)** ou **Or (Ou)**, puis choisissez les attributs que vous souhaitez filtrer ou mettre en correspondance et cliquez sur **OK (OK)**.
5. **Commit (Validez)** vos modifications.



STEP 8 | Vérifiez que les adresses de vos machines virtuelles sont ajoutées aux groupes d'adresses dynamiques.

1. Sélectionnez **Panorama** > **Objects (Objets)** > **Address Groups (Groupes d'adresses)**.
2. Cliquez sur **More (Plus)** dans la colonne Addresses (Adresses) d'un groupe d'adresses dynamiques.

   Panorama affiche une liste des adresses IP ajoutées à ce groupe d'adresse dynamique en fonction des critères de correspondance que vous avez spécifiés.



 ©2023 Palo Alto Networks, Inc.

STEP 9 | Utilisez des groupes d'adresses dynamiques dans une politique.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Cliquez sur **Add (Ajouter)** et saisissez un **Name (nom)** et une **Description (description)** pour identifier la politique.
3. Ajoutez la **Source Zone (Zone source)** pour indiquer la zone d'où provient le trafic.
4. Ajoutez la **Destination Zone (Zone de destination)** dans laquelle se termine le trafic.
5. Pour **Destination Address (Adresse de destination)**, sélectionnez le groupe d'adresses dynamiques que vous venez de créer.
6. Indiquez l'action (**Allow (Autoriser)** ou **Deny (Refuser)**) pour le trafic, puis associez éventuellement les profils de sécurité par défaut à la règle.
7. Répétez les étapes 1 à 6 pour créer une autre règle de politique.
8. Cliquez sur **Commit (Valider)**.

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Amorçage du pare-feu VM-Series

L'amorçage vous permet de créer un processus renouvelable et rationalisé pour le déploiement de nouveaux pare-feu VM-Series sur votre réseau, car il vous permet de créer un ensemble avec la configuration modèle pour votre réseau, puis d'utiliser cet ensemble pour déployer les pare-feu VM-Series partout.

Vous pouvez soit amorcer le pare-feu avec une configuration **complète** de sorte que le pare-feu soit entièrement configuré au démarrage, ou bien commencer avec une configuration **de base** : une configuration initiale minimale qui vous permet de démarrer le pare-feu et de vous enregistrer ensuite auprès de Panorama pour compléter la configuration.

Si vous choisissez la configuration **de base** et que vous déployez sur AWS, Azure ou GCP, vous pouvez utiliser l'ensemble d'amorçage et un fichier `init-cfg.txt`. Il est également possible d'effectuer un amorçage avec les **données de l'utilisateur**. Au lieu de fournir des paramètres de configuration d'amorçage dans les fichiers, vous les entrez sous forme de paires clé-valeur directement dans l'interface utilisateur AWS ou GCP lorsque vous lancez un pare-feu VM-Series. Azure a un processus similaire avec lequel vous fournissez les paramètres d'amorçage dans un modèle ou un autre fichier texte accessible depuis la CLI Azure.

Si vous créez l'ensemble d'amorçage, vous le livrez à partir d'un dispositif externe (comme un disque virtuel, un CD-ROM virtuel ou un dispositif de stockage cloud (comme un compartiment).

- Choix d'une méthode d'amorçage
- Flux d'amorçage du pare-feu VM-Series
- Ensemble d'amorçage
- Fichiers de configuration d'amorçage
- Génération de la clé d'authentification VM sur Panorama
- Création du fichier init-cfg.txt
- Création du fichier bootstrap.xml
- Préparation des licences pour l'amorçage
- Préparation de l'ensemble d'amorçage
- Amorçage du pare-feu VM-Series sur AWS
- Amorçage du pare-feu VM-Series dans Azure
- Amorçage du pare-feu VM-Series sur ESXi
- Amorçage du pare-feu VM-Series sur la Google Cloud Platform
- Amorçage du pare-feu VM-Series sur Hyper-V
- Amorçage du pare-feu VM-Series sur KVM
- Vérification d'achèvement de l'amorçage
- Erreurs d'amorçage

Choix d'une méthode d'amorçage

Vous pouvez amorcer le pare-feu VM-Series avec une **configuration de base** ou une **configuration complète**.

Une configuration **complète** utilise l'ensemble d'amorçage et comprend tout ce dont vous avez besoin pour configurer entièrement le pare-feu au démarrage. Cela comprend les paramètres de configuration (dans init-cfg.txt), les mises à jour du contenu et les versions des logiciels. Une configuration complète peut inclure à la fois init-cfg.txt et des fichiers bootstrap.xml.

Méthode de configuration	Localisation de configuration	Commentaire
Spécifiez les informations de configuration complètes dans /config/bootstrap.xml dans l'ensemble d'amorçage.	**Stockage cloud public** Compartiment AWS S3, compte de stockage Azure ou compartiment de stockage Google.	• Ensemble d'amorçage complet dans le compartiment de stockage. • Nécessite un stockage cloud et un rôle IAM pour y accéder.

Une configuration **de base** est une configuration minimale qui vous permet de lancer, d'obtenir une licence et d'enregistrer le pare-feu VM-Series. La configuration de base ne prend pas en charge les plugins, le contenu, les images logicielles ou bootstrap.xml.

Après avoir démarré le pare-feu, vous pouvez vous connecter à Panorama pour compléter la configuration, ou vous connecter au pare-feu pour mettre à jour manuellement le contenu et les logiciels. Le tableau suivant compare brièvement trois façons de stocker et d'accéder à une configuration de base :

Méthode de configuration	Localisation de configuration	Commentaire
init-cfg.txt Enregistrez les paramètres de configuration de base sous forme de paires clé-valeur dans le fichier config/init-cfg.txt de l'ensemble d'amorçage.	**Stockage cloud public** • Compartiment AWS S3 • Compte de stockage Azure • Compartiment de stockage GCP	• Nécessite un stockage cloud et un rôle IAM pour y accéder. L'administrateur de Panorama doit également avoir accès au compartiment.
Données utilisateur Entrez les paramètres de configuration dans l'interface utilisateur du cloud public sous forme de paires clé-valeur.	**Instance VM** • Alibaba : Données utilisateur • AWS : Données utilisateur • Azure : Données personnalisées • GCP : Métadonnées GCP	• Les paramètres de configuration initiale sont stockés avec la VM. • Il n'est pas nécessaire d'avoir un stockage séparé et le rôle IAM associé.

©2023 Palo Alto Networks, Inc.

Méthode de configuration	Localisation de configuration	Commentaire
	• Infrastructure Cloud Oracle : Données utilisateur	
AWS Secret Manager Entrez les paramètres de configuration dans AWS Secret Manager sous forme de paires clé-valeur.	Crypté dans AWS Secret Manager.	• Vous avez besoin d'un rôle IAM pour créer un secret. D'autres peuvent être autorisés à obtenir le secret. • Pour obtenir le secret, passez le nom secret en utilisant les données utilisateur.

Consultez le flux de travail du pare-feu VM-Series pour comparer le flux de travail pour les configurations de base et complètes.

- Configurations de base
- Terminer la configuration

Configurations de base

Une configuration de base comprend la configuration initiale et les licences. Vous pouvez utiliser l'ensemble d'amorçage pour transmettre les paires clé-valeur pour la configuration initiale, ou vous pouvez entrer les paires clé-valeur des paramètres d'amorçage comme données utilisateur.

Si vous n'utilisez pas Panorama, vous pouvez utiliser la configuration initiale pour amorcer le pare-feu, puis vous connecter et compléter la configuration manuellement. Si vous utilisez Panorama, votre configuration initiale doit inclure des paramètres d'amorçage pour les adresses IP de vos serveurs Panorama et la clé d'authentification VM afin que le pare-feu amorcé puisse s'enregistrer auprès de Panorama et compléter la configuration complète.

- Ajouter une configuration de base à l'ensemble d'amorçage
- Saisir une configuration de base en tant que données utilisateur (clouds publics)
- Enregistrer une configuration de base dans AWS Secrets Manager

Ajouter une configuration de base à l'ensemble d'amorçage

La configuration initiale est une configuration minimale qui vous permet de lancer, d'obtenir une licence et d'enregistrer le pare-feu VM-Series, et de vous connecter avec Panorama, le cas échéant. Vous fournissez la configuration (init-cfg.txt) dans l'ensemble d'amorçage.

Saisir une configuration de base en tant que données utilisateur (clouds publics)

Lorsque vous déployez le pare-feu VM-Series à partir de l'interface utilisateur d'un cloud public, vous pouvez saisir les paramètres de configuration en tant que données utilisateur lors du processus de lancement ou de déploiement. Si vous disposez des autorisations suffisantes pour déployer un pare-feu à partir de votre compte cloud et accéder à Panorama (si vous l'utilisez), vous pouvez ignorer la création d'un ensemble d'amorçage, la création de fichiers de configuration et d'autres tâches d'amorçage liées au stockage cloud (un compartiment de stockage, des rôles IAM ou des comptes de service qui accordent un accès externe au stockage).

 ©2023 Palo Alto Networks, Inc.

Les paramètres de configuration comprennent les valeurs de Composants du fichier init-cfg.txt, et les valeurs supplémentaires suivantes disponibles uniquement en tant que données utilisateur :

- **authcodes**—Le code d'authentification utilisé pour enregistrer le pare-feu VM-Series. Par exemple, **authcodes=I7115398**.
- **mgmt-interface-swap**—Utilisé pour échanger l'interface de gestion lorsque le pare-feu VM-Series est derrière un équilibreur de charge dans un déploiement AWS ou GCP. Par exemple, **mgmt-interface-swap=enable**.

Vous pouvez saisir les paramètres de configuration sous forme de paires de valeurs clés directement dans l'interface utilisateur Alibaba, AWS, GCP ou OCI. Vous pouvez également définir la configuration à partir d'un fichier texte ou d'un modèle natif cloud, tel qu'un modèle AWS Cloud Formation, un modèle ARM Azure, un fichier YAML GCP ou un modèle Terraform.

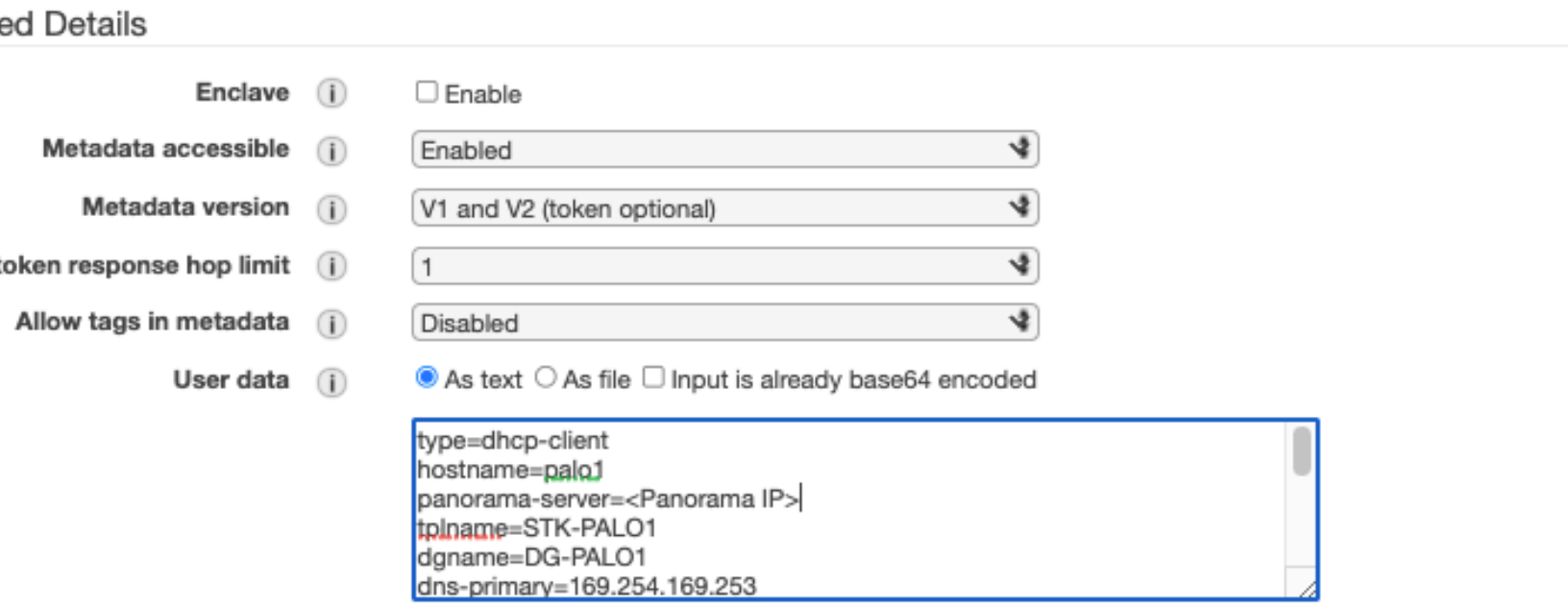
Chaque cloud a un terme différent pour les données utilisateur, et utilise des séparateurs différents entre les paramètres d'amorçage.

- **Données utilisateur Alibaba Cloud** —Utilisez une nouvelle ligne (\n) pour chaque paramètre, et si un paramètre a plusieurs options, utilisez des virgules pour les séparer.
- **Données utilisateur AWS** : utilisez un point-virgule ou un saut de ligne (\n). Si un paramètre a plus d'une option, séparez les options par une virgule. Par exemple :

```
  type=dhcp-client hostname=palo1 panorama-server=<PANORAMA-1 IP>
 panorama-server-2=<PANORAMA-2 IP> tplname=STK-NGFW-01 dgname=DG-
NGFW-01 dns-primary=169.254.169.253 dns-secondary=8.8.8.8 op-
command-modes=mgmt-interface-swap dhcp-send-hostname=yes dhcp-send-
client-id=yes dhcp-accept-server-hostname=yes dhcp-accept-server-
domain=yes vm-auth-key= <YOUR AUTH KEY HERE> authcodes= <<YOUR AUTH
 CODE HERE>
```

 ©2023 Palo Alto Networks, Inc.

Si vous choisissez de sauvegarder votre configuration de base dans AWS Secrets Manager, saisissez le nom secret comme une paire clé-valeur dans le champ des données utilisateur. Par exemple :



- **Azure Custom Data** : utilisez un point-virgule. Si un paramètre a plus d'une option, séparez les options par une virgule. Par exemple :

```
type=dhcp-client; op-command-modes=jumbo-frame; plugin-op-
commands=numa-perf-optimize:enable,set-dp-cores:30 vm-series-auto-
registration-pin-id=abcdefgh1234****; vm-series-auto-registration-
pin-value=zyxwvut-0987****
```

- **Métadonnées personnalisées GCP**—Dans un fichier, tel qu'un fichier YAML ou un modèle Terraform, utilisez une nouvelle ligne (\n) pour chaque paramètre, et si un paramètre a plusieurs options, utilisez des virgules pour les séparer. Par exemple :

```
type=dhcp-client op-command-modes=mgmt-interface-swap,jumbo-frame
 plugin-op-commands=numa-perf-optimize:enable,set-dp-cores:30 vm-
series-auto-registration-pin-id=abcdefgh1234**** vm-series-auto-
registration-pin-value=zyxwvut-0987****
```

- **Données utilisateur Cloud Infrastructure Oracle**—Utilisez une nouvelle ligne (\n) pour chaque paramètre, et si un paramètre a plusieurs options, utilisez des virgules pour les séparer.

©2023 Palo Alto Networks, Inc.

Enregistrer une configuration de base dans AWS Secrets Manager

Vous pouvez utiliser AWS Secrets Manager pour stocker la configuration de base comme un secret, puis utiliser les données utilisateur pour amorcer une VM avec les paramètres stockés dans le secret. Pour effectuer cette tâche, vous devez obtenir l'autorisation d'utiliser Secrets Manager.

- Le créateur du secret doit disposer des autorisations complètes de l'administrateur Secrets Manager. Un administrateur Secrets Manager peut autoriser d'autres personnes à utiliser le secret, comme décrit dans Authentication and access control for AWS Secrets Manager (Authentification et contrôle d'accès pour AWS Secrets Manager).

  Par exemple, la déclaration de politique générale suivante vous permet d'obtenir la valeur secrète :

  ```
  { "Version": "2012-10-17", { "Effect": "Allow",
   "Action": "secretsmanager:GetSecretValue", "Resource":
   "arn:aws:secretsmanager:us-east-1:688382******:secret:My_bts-
  ******" } }
  ```

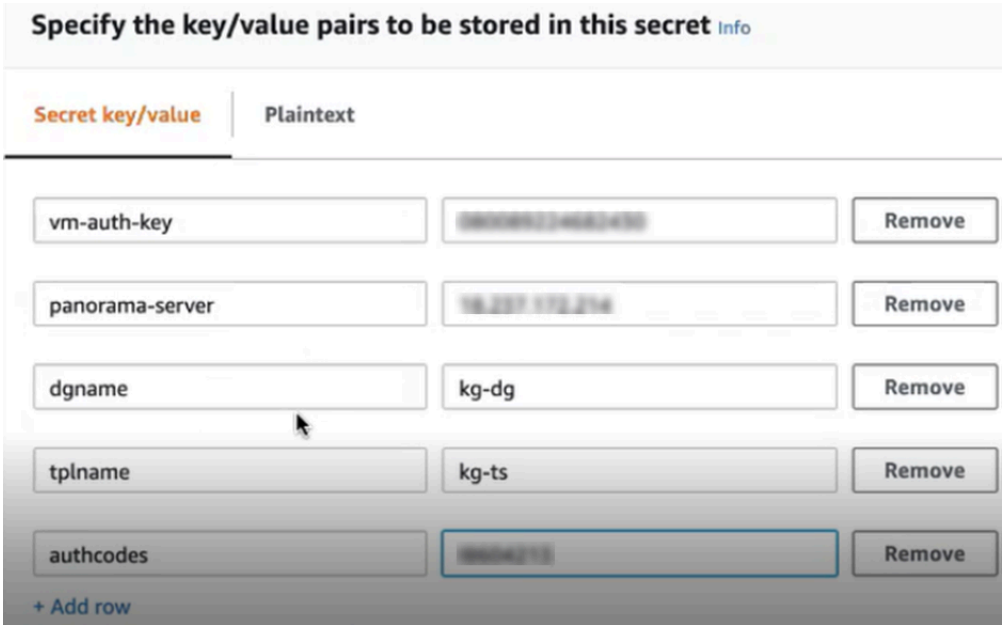
  Consultez Actions, Resources, and Context Keys You Can Use in an IAM Policy or Secret Policy for AWS Secrets Manager (Actions, ressources et clés de contexte que vous pouvez utiliser dans une politique IAM ou une politique secrète pour AWS Secrets Manager) pour voir les actions qui nécessitent une autorisation, telles que la liste, l'obtention et la rotation du secret.
- (En option) Pour crypter le secret, vous pouvez utiliser DefaultEncryptionKey de AWS Secrets Manager.

STEP 1 | Connectez-vous à la console AWS et sous Security, Identity and Compliance (Sécurité, Identité et Conformité), sélectionnez **Secrets Manager** et sélectionnez **Store a new secret (Stocker un nouveau secret)**.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Sélectionnez **un autre type de secrets**.

1. Saisissez les paires clé-valeur pour définir la configuration de base.



> ***mgmt-interface-swap*** *ne fonctionne pas comme une paire clé-valeur dans un secret AWS. Il doit être saisi comme suit :* ***op-command-modes=mgmt-interface-swap***

2. Sélectionnez DefaultEncryptionKey, et cliquez sur **Next (Suivant)**.

STEP 3 | Fournissez le nom et la description du secret.

1. Modifier les autorisations de ressources pour accéder de manière sécurisée aux secrets sur les comptes AWS. Par exemple :

```
{ "Version": "2012-10-17", "Statement": [ { "Sid":
 "VisualEditor0", "Effect": "Allow", "Action":
 "s3:ListBucket", "Resource": "arn:aws:s3:::sn-
bootstrap" }, { "Sid": "VisualEditor1", "Effect":
 "Allow", "Action": "s3:GetObject", "Resource":
 "arn:aws:s3:::sn-bootstrap/*" }, { "Effect": "Allow",
 "Action": "secretsmanager:GetSecretValue", "Resource":
 "arn:aws:secretsmanager:us-east-1:688382******:
 secret:My_bootstrap" } ] }
```

2. (En option) Vous pouvez examiner le secret depuis la ligne de commande (si vous avez l'autorisation). Par exemple :

```
# aws secretsmanager get-secret-value --secret-id My_bootstrap
 { "ARN": "arn:aws:secretsmanager:us-east-1:688382******:
 secret:My_bootstrap", "Name": "My_bootstrap", "VersionId":
 "01b6853d-e187-479f-**********", "SecretString": "{\"mgmt-
interface-swap\":\"enable\", \"vm-auth-key\":\"AAA\",
\"panorama-server\":\"10.*.*.1\", \"panorama-server-2\":
\"10.*.*.2\",\"dgname\":\"dg-s0000h\", \"tplname\":\"tpl-
```

 ©2023 Palo Alto Networks, Inc.

```
santosh\",\"license-authcode\":\"AAAA\"}", "VersionStages":
 [ "AWSCURRENT" ], "CreatedDate": 1581018411.847 }
```

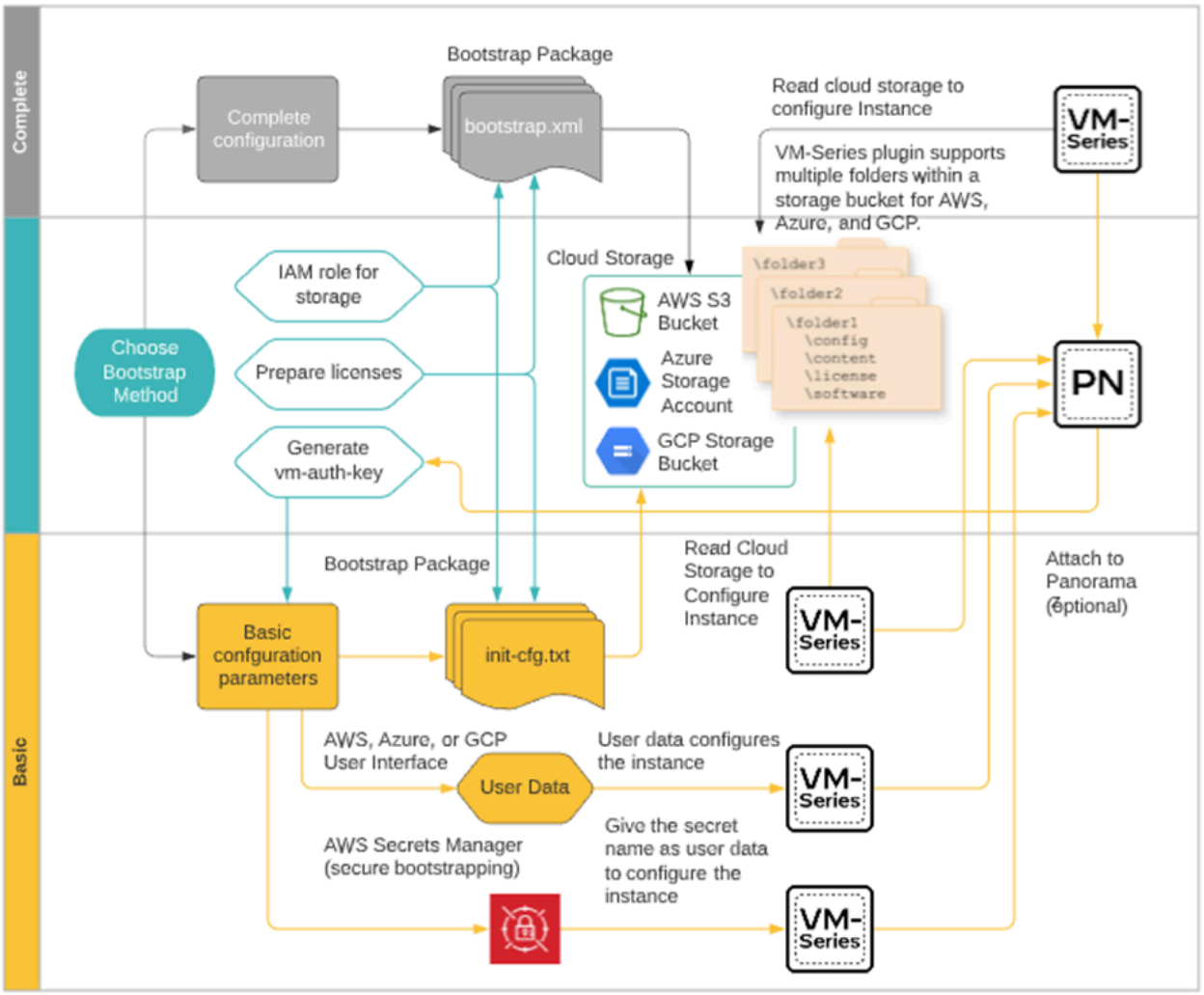
Terminer la configuration

Une configuration complète permet de s'assurer que le pare-feu est entièrement configuré au démarrage. Le fichier bootstrap.xml comprend la configuration initiale, les licences, les logiciels, le contenu et une version du plugin VM-Series. Vous pouvez créer **`bootstrap.xml`** manuellement ou vous pouvez exporter une configuration existante, comme décrit dans Create the bootstrap.xml File (Créer le fichier bootstrap.xml).

 ©2023 Palo Alto Networks, Inc.

Flux d'amorçage du pare-feu VM-Series

Utilisez le flux de travail suivant pour amorcer votre pare-feu VM-Series. Reportez-vous à la figure suivante pour une présentation des procédures d'amorçage complète et basique.



STEP 1 | (Facultatif) Pour des raisons de sécurité, vous ne pouvez amorcer un pare-feu que lorsqu'il se trouve dans la configuration d'usine par défaut. Si vous voulez utiliser l'ensemble d'amorçage pour amorcer un pare-feu VM-Series qui a déjà été configuré, effectuez le rétablissement des paramètres d'usine par défaut du pare-feu.

STEP 2 | Choisissez une méthode d'amorçage.

Après vous être familiarisé avec l'ensemble d'amorçage, évaluez si vous souhaitez utiliser une configuration complète, ou utiliser une configuration de base et éventuellement utiliser Panorama pour gérer le pare-feu amorcé.

Si vous choisissez une configuration de base, décidez si vous voulez utiliser l'ensemble d'amorçage ou si vous voulez saisir les paramètres de configuration comme paires clé-valeur dans les données utilisateur.

©2023 Palo Alto Networks, Inc.

STEP 3 | (Facultatif) Si vous souhaitez utiliser Panorama pour gérer les pare-feu VM-Series qui sont amorcés, générez la clé d'authentification VM sur Panorama. Vous devez inclure cette clé dans le fichier **`init-cfg.txt`** (**`vm-auth-key`**) ou saisir la paire clé-valeur en tant que données utilisateur.

STEP 4 | Préparez les licences pour l'amorçage.

STEP 5 | Si vous choisissez la configuration de base et que vous prévoyez d'amorcer avec des données utilisateur, passez à l'étape 7.

Si vous prévoyez d'utiliser la configuration de base et l'ensemble d'amorçage, créez le fichier init-cfg.txt et préparez l'ensemble d'amorçage.

Si vous choisissez la configuration complète, créez le fichier bootstrap.xml et préparez l'ensemble d'amorçage complet.

STEP 6 | Préparez l'ensemble d'amorçage et enregistrez-le dans le format de distribution approprié pour votre hyperviseur.

STEP 7 | Amorcez le pare-feu VM-Series.

- Amorçage du pare-feu VM-Series sur AWS
- Amorçage du pare-feu VM-Series dans Azure
- Amorçage du pare-feu VM-Series sur ESXi
- Amorçage du pare-feu VM-Series sur la Google Cloud Platform
- Amorçage du pare-feu VM-Series sur Hyper-V
- Amorçage du pare-feu VM-Series sur KVM

STEP 8 | Vérifiez l'achèvement de l'amorçage.

©2023 Palo Alto Networks, Inc.

Ensemble d'amorçage

Le processus d'amorçage est lancé uniquement lors du premier démarrage lorsque le pare-feu se trouve dans la configuration d'usine par défaut.

- Structure de l'ensemble d'amorçage
- Livraison de l'ensemble d'amorçage

Structure de l'ensemble d'amorçage

L'ensemble d'amorçage doit inclure les dossiers `/config`, `/license`, `/software` et `/content`, même s'ils sont vides. Le dossier `/plugins` est facultatif. Pour obtenir un exemple, consultez Préparation de l'ensemble d'amorçage.

- **Dossier /config**—Contient les fichiers de configuration. Le dossier peut contenir deux fichiers : `init-cfg.txt` et `bootstrap.xml`. Pour plus de renseignements, consultez Bootstrap Configuration Files (Fichiers de configuration d'amorçage).

  Si vous souhaitez pré-enregistrer des pare-feu VM-Series avec Panorama avec l'amorçage, vous devez générer une clé d'authentification VM sur Panorama et inclure la clé générée dans le fichier `init-cfg.txt`. Reportez-vous à la section Générez la clé d'authentification VM sur Panorama*.*

- **Dossier /license**—Contient les clés de licence ou les codes d'authentification pour les licences et les abonnements que vous voulez activer sur les pare-feu. Si le pare-feu ne dispose pas de connectivité à Internet, vous devez obtenir les clés de licence manuellement sur le portail d'assistance de Palo Alto Networks ou utiliser l'API de mise sous licence pour obtenir les clés et enregistrer ensuite chaque clé dans ce dossier. Pour plus de détails, reportez-vous à la section Préparation des licences pour l'amorçage.

  Vous devez inclure un ensemble de codes d'authentification au lieu de codes individuels de sorte que le pare-feu ou le service d'orchestration puisse extraire simultanément toutes les clés de licence associées au pare-feu. Si vous utilisez des codes d'authentification individuels au lieu d'un ensemble, le pare-feu ne récupèrera que la clé de licence pour le premier code d'authentification inclus dans le fichier.

- **Dossier /software**—Contient les images de logiciel nécessaires pour mettre à niveau un nouveau pare-feu VM-Series vers la version de PAN-OS désirée pour votre réseau. Vous devez inclure toutes les versions de logiciel intermédiaire entre la version actuelle et la version finale du logiciel PAN-OS vers laquelle vous voulez mettre à niveau le pare-feu VM-Series. Reportez-vous à VM-Series Firewall Hypervisor Support (Support de l'hyperviseur de pare-feu VM-Series) dans Compatibility Matrix (Matrice de compatibilité).
- **Dossier /content**—Contient l'application et les mises à jour relatives aux menaces, les mises à jour de WildFire, et la base de données de filtrage des URL BrightCloud pour les abonnements valides sur le pare-feu VM-Series. Vous devez inclure les versions de contenu minimales requises pour la version PAN-OS souhaitée. Si vous n'avez pas la version de contenu minimale requise associée à la version PAN-OS, le pare-feu VM-Series ne peut pas effectuer la mise à jour du logiciel.
- **Dossier /plugins**-Facultatif Contient une seule image de plug-in VM-Series.

 ©2023 Palo Alto Networks, Inc.

Livraison de l'ensemble d'amorçage

Le type de fichier utilisé pour fournir l'ensemble d'amorçage au pare-feu VM-Series varie selon votre hyperviseur. Utilisez le tableau ci-dessous pour déterminer le type de fichier pris en charge par votre hyperviseur o fournisseur de cloud.

Périphérique externe pour l'amorçage (format de l'ensemble d'amorçage)	AWS	Azure	ESXi	Google	Hyper-V	KVM
CD-ROM (image ISO)	—	—	Oui	—	Oui	Oui
Dispositif de stockage de bloc	—	—	Oui	—	Oui	Oui
Storage Account (Compte de stockage)	—	Oui	—	—	—	—
Storage Bucket	Oui	—	—	Oui	—	—

Lorsque vous associez le périphérique au pare-feu, le pare-feu recherche un ensemble d'amorçage et, s'il en existe un, le pare-feu utilise les paramètres définis dans l'ensemble d'amorçage.

Si vous avez inclus une adresse IP de serveur Panorama dans le fichier, le pare-feu se connecte à Panorama. Si le pare-feu possède une connectivité à Internet, il contacte le serveur de licence pour mettre à jour l'UUID et obtenir les clés de licence et les abonnements. Le pare-feu est alors ajouté comme ressource dans le portail de support de Palo Alto Networks. Si le pare-feu ne dispose pas de connectivité à Internet, il utilise les clés de licence que vous avez incluses dans l'ensemble d'amorçage ou il se connecte à Panorama pour récupérer les licences appropriées et les déployer sur les pare-feu gérés.

©2023 Palo Alto Networks, Inc.

Fichiers de configuration d'amorçage

L'ensemble d'amorçage doit inclure la configuration de base dans **config/init-cfg.txt**. La configuration complète (dans le fichier **/config/bootstrap.xml**) est facultative.

Lorsque vous incluez le fichier **init-cfg.txt** et le fichier **bootstrap.xml** dans l'ensemble d'amorçage, le pare-feu fusionne les configurations de ces fichiers, et si certains paramètres se superposent, le pare-feu utilise les valeurs définies dans le fichier **init-cfg.txt**.

- init-cfg.txt
- bootstrap.xml

init-cfg.txt

Cela inclut les informations de base pour la configuration de l'interface de gestion sur le pare-feu, comme le type d'adresse IP (fixe ou DHCP), l'adresse IP (IPv4 uniquement ou IPv4 et IPv6), le masque de réseau et la passerelle par défaut. L'adresse IP du serveur de DNS, l'adresse IP de Panorama et les paramètres de groupe de périphériques et piles de modèle sont en option.

Vous pouvez utiliser le nom générique **init-cfg.txt**, ou, pour être plus précis, vous pouvez faire précéder le nom du fichier de l'UUID ou du numéro de série de chaque pare-feu (par exemple : **0008C100105-init-cfg.txt**).

Lorsque le pare-feu démarre, il recherche un fichier texte qui correspond à son UUID ou à son numéro de série et, s'il ne les trouve pas, il recherche le fichier ayant le nom générique **init-cfg.txt**. Pour un exemple de fichier, reportez-vous à la section Créer le fichier init-cfg.txt.

Si vous utilisez Panorama pour gérer vos pare-feu VM-Series amorcés :

- *Vous devez générer une clé d'authentification de machine virtuelle sur Panorama et inclure la clé dans le fichier **init-cfg.txt**. Pour plus d'informations, reportez-vous à la section* Génération de la clé d'authentification VM sur Panorama*.*
- *L'appliance Panorama qui gère les pare-feu doit être en mode Panorama. Si vous utilisez une appliance Panorama en mode Gestion uniquement, les journaux du pare-feu sont supprimés car Panorama en mode Gestion uniquement ne dispose pas d'un groupe de collecteurs de journaux pouvant stocker les journaux du pare-feu.*

bootstrap.xml

Le fichier facultatif **bootstrap.xml** contient une configuration complète du pare-feu. Si vous n'utilisez pas Panorama pour gérer de manière centralisée vos pare-feu, le fichier **bootstrap.xml** permet d'automatiser le processus de déploiement des pare-feu configurés au démarrage.

Vous pouvez définir la configuration manuellement ou exporter la configuration d'exploitation (**running-config.xml**) à partir d'un pare-feu existant et enregistrer le fichier sous le nom **bootstrap.xml**. Si vous exportez le fichier **bootstrap.xml**, assurez-vous d'exporter le fichier XML à partir d'un pare-feu déployé sur la même plate-forme ou hyperviseur que votre déploiement. Reportez-vous à la section Création du fichier bootstrap.xml.

 ©2023 Palo Alto Networks, Inc.

Génération de la clé d'authentification VM sur Panorama

Si vous voulez utiliser Panorama pour gérer les pare-feu VM-Series que vous amorcez, vous devez générer une clé d'authentification VM sur Panorama et inclure la clé dans le fichier de configuration de base (init-cfg.txt). La clé d'autorisation VM permet à Panorama d'authentifier le pare-feu VM-Series qui vient d'être amorcé. Ainsi, pour gérer le pare-feu avec Panorama, vous devez inclure l'adresse IP pour Panorama et la clé d'autorisation VM dans le fichier de configuration de base, ainsi que les codes d'autorisation de licence dans le dossier /license de l'ensemble d'amorçage. Le pare-feu peut alors fournir l'adresse IP, le numéro de série et la clé d'autorisation VM dans sa requête de connexion initiale à Panorama de sorte que Panorama puisse vérifier la validité de la clé d'autorisation VM et ajouter le pare-feu comme périphérique géré. Si vous fournissez un groupe de périphériques et un modèle dans le fichier de configuration de base, Panorama attribuera le pare-feu au groupe de périphériques et modèle appropriés afin que vous puissiez configurer et administrer de manière centralisée le pare-feu avec Panorama.

La durée de vie de la clé peut varier de 1 à 8 760 heures (1 an). Au bout du temps spécifié, la clé expire et Panorama n'enregistrera pas les pare-feu VM-Series sans une clé d'autorisation VM valide dans la requête de connexion.

STEP 1 | Connectez-vous à la CLI de Panorama ou accédez à l'API :

- Dans l'interface de ligne de commande, utilisez la commande opérationnelle suivante :

  ```
  request bootstrap vm-auth-key generate lifetime <1-8760>
  ```

  Par exemple, pour générer une clé dont la validité est de 24 heures, saisissez :

  ```
  request bootstrap vm-auth-key generate lifetime 24
  Clé d'authentification VM 755036225328715 générée. Expire à :
   2015/12/29 12:03:52
  ```

- Dans l'API, utilisez l'URL suivant :

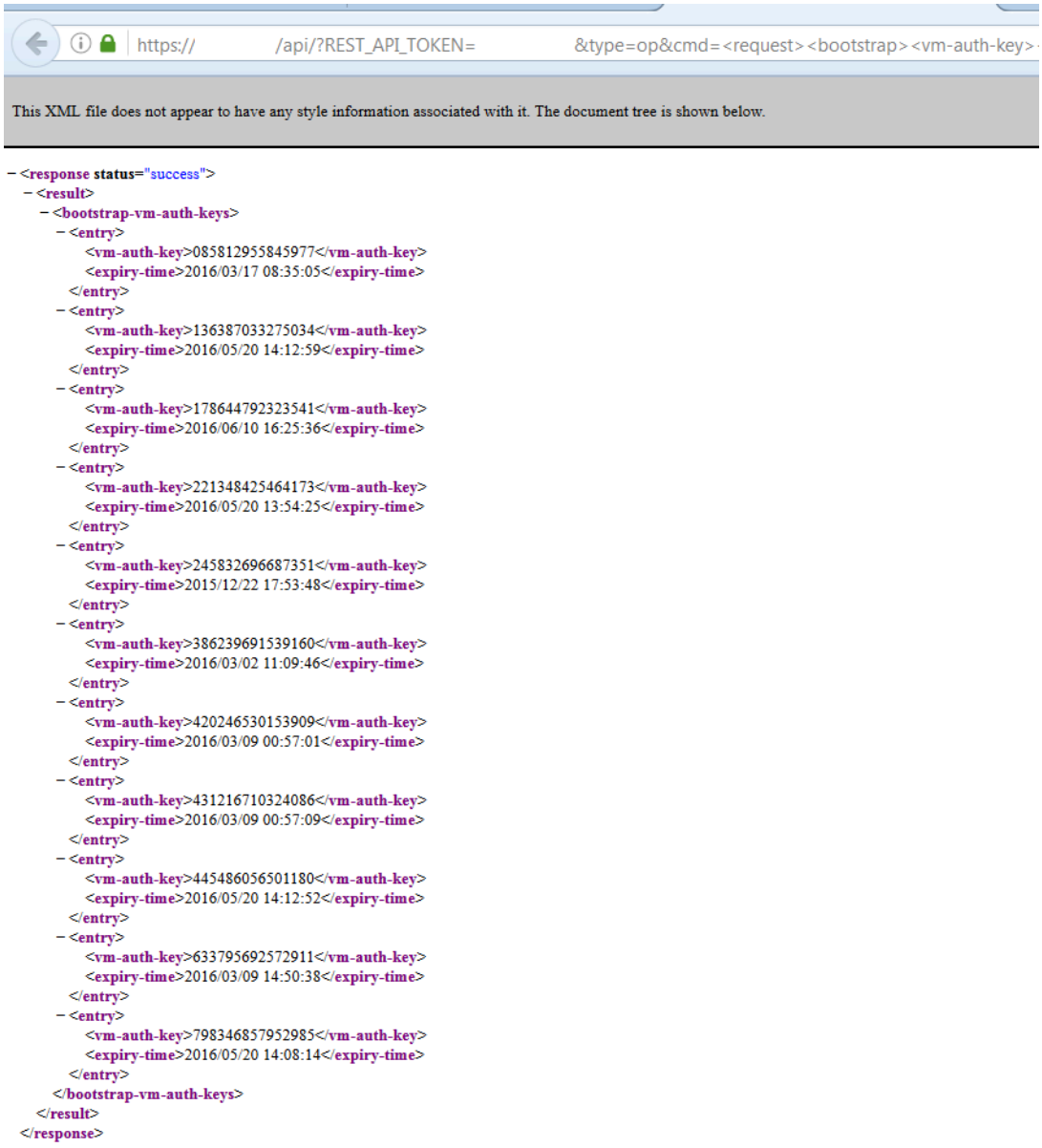
  https://<*Panorama_IP_address*>/api/?type=op&cmd=<request><bootstrap><vm-auth-key><generate><lifetime><number-of-hours></lifetime></generate></vm-auth-key></bootstrap></request>

  où la durée de vie est le nombre d'heures de validité de la clé d'autorisation VM.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | Vérifiez la durée de validité des clés d'autorisation VM que vous avez générées sur Panorama. Assurez-vous que la durée de validité laisse suffisamment de temps aux pare-feu pour s'enregistrer sur Panorama.

```
https://<Panorama_IP_address>/api/?
type=op&cmd=<request><bootstrap><vm-auth-key><show></show></vm-
auth-key></bootstrap></request>
```



STEP 3 | Ajoutez la clé d'autorisation VM générée au fichier de configuration de base (init-cfg.txt). Reportez-vous à la section Création du fichier init-cfg.txt.

 ©2023 Palo Alto Networks, Inc.

Création du fichier init-cfg.txt

Le fichier **init-cfg.txt** est requis pour amorcer le pare-feu VM-Series. Il fournit les informations de base dont le pare-feu a besoin pour se connecter à votre réseau.

- Composants du fichier init-cfg.txt
- Fichier init-cfg.txt modèle

Exécutez la procédure suivante pour créer le fichier **init-cfg.txt**.

STEP 1 | Créez un nouveau fichier texte.

Utilisez un éditeur de texte comme Bloc-notes, EditPad ou tout autre éditeur de texte pour créer un fichier texte.

STEP 2 | Ajoutez la configuration réseau de base pour l'interface de gestion sur le pare-feu.

Si l'un des paramètres requis est absent du fichier, le pare-feu quitte l'opération d'amorçage et démarre en utilisant l'adresse IP par défaut, 192.168.1.1. Vous pouvez consulter le journal système sur le pare-feu pour détecter la raison de l'échec de l'amorçage. Pour les erreurs, reportez-vous à la section API de mise sous licence**.**

Il n'y a pas d'espace entre la clé et la valeur dans chaque champ. N'ajoutez pas d'espaces, car ils pourraient causer des erreurs durant l'analyse syntaxique du côté mgmtsrvr.

- Pour configurer l'interface de gestion avec une adresse IP fixe, vous devez spécifier l'adresse IP, le type d'adresse, la passerelle par défaut et le masque de réseau. Une adresse IPv4 est requise. L'adresse IPv6 est facultative. Pour la syntaxe, reportez-vous à la section Fichier init-cfg.txt modèle.
- Pour configurer l'interface de gestion comme client DHCP, vous devez spécifier uniquement le type d'adresse. Si vous activez le client DHCP sur l'interface de gestion, le pare-feu ignore les valeurs d'adresse IP, passerelle par défaut, masque de réseau, adresse IPv6 et passerelle par défaut IPv6 définies dans le fichier. Pour la syntaxe, reportez-vous à la section Fichier init-cfg.txt modèle.

Lorsque vous activez le DHCP sur l'interface de gestion, le pare-feu prend l'adresse IP attribuée par le DHCP et il est accessible sur le réseau. Vous pouvez voir l'adresse IP attribuée par le DHCP sur le widget Informations générale dans le tableau de bord ou avec la commande CLI **show system info**. Toutefois, l'adresse IP fixe de gestion statique par défaut 192.168.1.1 est conservée dans la configuration d'exploitation (**show config running**) sur le pare-feu. Cette adresse IP fixe vous permet de rétablir en permanence la connectivité de votre pare-feu, en cas de perte d'accès au DHCP sur le pare-feu.

STEP 3 | Ajoutez la clé d'autorisation VM pour enregistrer un pare-feu VM-Series sur Panorama.

Pour ajouter un pare-feu VM-Series sur Panorama, vous devez ajouter la clé d'autorisation VM que vous avez générée sur Panorama dans le fichier de configuration de base (**init-cfg.txt**). Pour plus de détails sur la génération d'une clé, reportez-vous à la section Génération de la clé d'authentification VM sur Panorama.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | Ajoutez les détails pour l'accès à Panorama.

- Ajoutez les adresses IP pour les serveurs Panorama principal et secondaire.
- Spécifiez le modèle et le groupe de périphériques auxquels vous voulez attribuer le pare-feu.

STEP 5 | (Recommandé) Ajoutez le PIN d'enregistrement VM-Series et la valeur pour l'installation du certificat de périphérique.

Si vous souhaitez installer le certificat de périphérique sur le pare-feu VM-Series au lancement, vous devez générer l'ID et la valeur du PIN d'enregistrement VM-Series sur le CSP et l'inclure dans le fichier **`init-cfg.txt`**. Ce PIN et cette valeur s'appliquent également à toutes les licences de site qui utilisent la licence PAYG.

STEP 6 | (Facultatif) Incluez des paramètres supplémentaires pour le pare-feu.

- Ajoutez l'adresse IP pour les serveurs DNS principal et secondaire.
- Ajoutez le nom d'hôte pour le pare-feu.
- Activez les trames jumbo ou le systèmes virtuels multiples
- Activez la permutation de l'interface de gestion (mgmt) et de l'interface du plan de données (ethernet 1/1) pour le pare-feu VM-Series sur AWS ou GCP. Pour plus d'informations sur la modification de l'interface de gestion, reportez-vous à la section Mappage d'interface de gestion pour l'utilisation avec Amazon ELB ou Échange de l'interface de gestion pour l'équilibrage de la charge de Google Cloud Platform.
- Activez ou désactivez DPDK.

Composants du fichier init-cfg.txt

Le tableau suivant décrit les paramètres d'amorçage dans le fichier **`init-cfg.txt`**.

Champ	Description
type=	Type d'adresse IP de gestion : static ou dhcp-client. Ce champ est obligatoire.
ip-address=	Adresse IPv4. Ce champ est ignoré si le type est dhcp-client. Si le type est statique, une adresse IPv4 est requise. Le champ ipv6-address est facultatif et peut être inclus. Vous ne pouvez pas spécifier l'adresse IP de gestion et la configuration du masque réseau pour le pare-feu VM-Series dans AWS et Azure. Si ces valeurs sont définies, le pare-feu ignore les valeurs que vous avez spécifiées.
default-gateway=	Passerelle IPv4 par défaut pour l'interface de gestion. Ce champ est ignoré si le type est dhcp-client. Si le type est static et que ip-address est utilisé, ce champ est obligatoire.
netmask=	Masque réseau IPv4. Ce champ est ignoré si le type est dhcp-client. Si le type est static et que ip-address est utilisé, ce champ est obligatoire.

©2023 Palo Alto Networks, Inc.

Champ	Description
ipv6-address=	(Facultatif) Adresse IPv6 et longueur du préfixe de l'interface de gestion. Ce champ est ignoré si le type est dhcp-client. Si le type est static, ce champ peut être spécifié avec le champ ip-address, qui est obligatoire.
ipv6-default-gateway=	Passerelle IPv6 par défaut pour l'interface de gestion. Ce champ est ignoré si le type est dhcp-client. Si le type est static et que ipv6-address est utilisé, ce champ est obligatoire.
hostname=	Nom d'hôte pour le pare-feu.
panorama-server=	Adresse IPv4 ou IPv6 du serveur Panorama principal. Ce champ n'est pas obligatoire, mais il est recommandé pour la gestion centralisée de vos pare-feu.
panorama-server-2=	Adresse IPv4 ou IPv6 du serveur Panorama secondaire. Ce champ n'est pas obligatoire, mais il est recommandé.
tplname=	Nom de la pile de modèle Panorama. Si vous ajoutez une adresse IP de serveur Panorama, appliquez le pare-feu à une pile de modèles sur Panorama et entrez le nom de la pile de modèles dans ce champ afin de pouvoir gérer de manière centralisée et envoyer les paramètres de configuration au pare-feu.
dgname=	Nom du groupe de périphériques Panorama. Si vous ajoutez une adresse IP de serveur Panorama, créez un groupe de périphériques sur Panorama et entrez le nom du groupe de périphériques dans ce champ afin de pouvoir regrouper logiquement les pare-feu et d'envoyer les règles de politique au pare-feu.
cgname=	Nom du groupe de collecteurs Panorama. Si vous souhaitez amorcer le pare-feu pour envoyer des journaux à un groupe de collecteurs Panorama, vous devez d'abord configurer un groupe de collecteurs sur Panorama, puis configurer le pare-feu pour transférer les journaux vers Panorama. Sur les appareils de série M, un groupe de collecteurs par défaut est prédéfini et contient déjà le collecteur de journaux local en tant que membre. Sur l'appareil virtuel Panorama, vous devez ajouter le groupe de collecteurs et ajouter le collecteur de journaux local en tant que membre.
dns-primary=	Adresse IPv4 ou IPv6 du serveur de DNS principal.
dns-secondary=	Adresse IPv4 ou IPv6 du serveur de DNS secondaire.

 ©2023 Palo Alto Networks, Inc.

Champ	Description
vm-auth-key=	Clé d'authentification de machine virtuelle pour Panorama (voir Génération de la clé d'authentification VM sur Panorama). Ce champ est ignoré lors de l'amorçage de pare-feu matériels.

op-command-modes=	Les valeurs suivantes sont admises : multi-vsys, Jumbo-frame, mgmt-interface-swap. Si vous saisissez plusieurs valeurs, utilisez un espace ou une virgule pour séparer les entrées.
	• **multi-vsys** (pare-feu matériels uniquement) : autorise plusieurs systèmes virtuels.
	• **jumbo frame** : autorise le réglage à 9192 octets pour la taille de MTU par défaut de toutes les interfaces de couche 3.
	• **mgmt-interface-swap** (pare-feu VM-Series sur AWS, Google, ESXi et KVM uniquement) : vous permet de permuter l'interface de gestion (MGT) avec l'interface du plan de données (ethernet 1/1) lors du déploiement du pare-feu. Pour plus d'informations, reportez-vous à la section
	  • Mappage d'interface de gestion pour l'utilisation avec Amazon ELB
	  • Échange de l'interface de gestion pour l'équilibrage de la charge de Google Cloud Platform
	  • Utilisation de la CLI du VM-Series pour permuter l'interface de gestion sur ESXi
	  • Utilisation de la CLI du VM-Series pour permuter l'interface de gestion sur KVM

op-cmd-dpdk-pkt-io=	La valeur **on** ou **off** vous permet d'activer ou de désactiver le kit de développement du dataplane (DPDK) dans les environnements où le pare-feu prend en charge DPDK. DPDK permet à l'hôte de traiter les paquets plus rapidement en contournant le noyau Linux. Les interactions avec la carte réseau sont effectuées à l'aide des pilotes et des bibliothèques DPDK.
plugin-op-commands=	Spécifiez les commandes d'opération du plugin VM-Series. *Les commandes multiples doivent être saisies sur une seule liste, séparée par des virgules, sans espaces.* • **sriov-access-mode-on** : cette commande n'est valide que pour le pare-feu VM-Series sur les hyperviseurs ESXi et KVM. Pour KVM uniquement, si vous activez **sriov-access-mode-on**, n'activez pas **op-command-modes=jumbo-frame**. • **aws-gwlb-inspect:enable** : active Intégration VM-Series avec un équilibreur de charge de passerelle AWS.

©2023 Palo Alto Networks, Inc.

Champ	Description
	• **aws-gwlb-associate-vpce:<vpce-id>@ethernet<subinterface>** : permet de Association d'un terminal VPC à une interface VM-Series ou une sous-interface sur le pare-feu. L'interface spécifiée est affectée à une zone de sécurité. • **aws-gwlb-overlay-routing:enable** : utilisez cette commande pour Activation du routage de superposition pour le VM-Series sur AWS en cas d'intégration à un AWS GWLB. • **set-dp-cores:<#-cores>** : personnalisez le nombre de vCPU de plan de données pour un pare-feu VM-Series exécutant PAN-OS 10.2 ou version ultérieure déployé avec une licence logicielle NGFW. Cette option n'est pas prise en charge sur NSX-T. Pour plus d'informations, consultez Personnalisation des cœurs de plan de données. • **numa-perf-optimize:enable** : active l'optimisation des performances NUMA sur le pare-feu VM-Series avec le plug-in VM-Series 2.1.2 ou version ultérieure installé. Pour plus d'informations, consultez Activation de l'optimisation des performances NUMA sur le VM-Series.
dhcp-send-hostname=	La valeur yes ou no provient du serveur DHCP. Si la valeur est yes, le pare-feu envoie son nom d'hôte au serveur DHCP. Ce champ est uniquement pris en compte si le type est dhcp-client.
dhcp-send-client-id=	La valeur yes ou no provient du serveur DHCP. Si la valeur est yes, le pare-feu envoie son ID client au serveur DHCP. Ce champ est uniquement pris en compte si le type est dhcp-client.
dhcp-accept-server-hostname=	La valeur yes ou no provient du serveur DHCP. Si la valeur est yes, le pare-feu accepte son nom d'hôte de la part du serveur DHCP. Ce champ est uniquement pris en compte si le type est dhcp-client.
dhcp-accept-server-domain=	La valeur yes ou no provient du serveur DHCP. Si la valeur est yes, le pare-feu accepte son serveur de DNS de la part du serveur DHCP. Ce champ est uniquement pris en compte si le type est dhcp-client.
vm-series-auto-registration-pin-id ET vm-series-auto-registration-pin-value	L'ID et la valeur du PIN d'enregistrement VM-Series pour l'installation du certificat de périphérique sur le pare-feu VM-Series. L'ID et la valeur du PIN vous permettent également d'activer automatiquement les licences de site pour AutoFocus et Cortex Data Lake sur les instances PAYG du pare-feu. Vous devez générer ces informations dans l'ID et la valeur du PIN d'enregistrement sur le CSP Palo Alto Networks. Reportez-vous à la section Installation d'un certificat de périphérique sur le pare-feu VM-Series pour obtenir des informations sur la création d'un ID de PIN et de sa valeur.

©2023 Palo Alto Networks, Inc.

Fichier init-cfg.txt modèle

Les exemples suivants de fichiers de configuration de base montrent tous les paramètres qui sont pris en charge dans le fichier ; les paramètres obligatoires sont en **gras**.

Exemple de fichier init-cfg.txt (adresse IP fixe)	Exemple de fichier init-cfg.txt (client DHCP)
type=static	**type=dhcp-client**
ip-address=10.*.*.19	ip-address=
default-gateway=10.*.*.1	default-gateway=
netmask=255.255.255.0	netmask=
ipv6-address=2001:400:f00::1/64	ipv6-address=
ipv6-default-gateway=2001:400:f00::2*	ipv6-default-gateway=
hostname=Ca-FW-DC1	hostname=Ca-FW-DC1
vm-auth-key=7550362253****	vm-auth-key=7550362253****
panorama-server=10.*.*.20	panorama-server=10.*.*.20
panorama-server-2=10.*.*.21	panorama-server-2=10.*.*.21
tplname=FINANCE_TG4	tplname=FINANCE_TG4
dgname=finance_dg	dgname=finance_dg
dns-primary=10.5.6.6	dns-primary=10.5.6.6
dns-secondary=10.5.6.7	dns-secondary=10.5.6.7
op-command-modes=jumbo-frame,mgmt-interface-swap**	op-command-modes=jumbo-frame,mgmt-interface-swap**
op-cmd-dpdk-pkt-io=***	op-cmd-dpdk-pkt-io=***
plugin-op-commands=	plugin-op-commands=
dhcp-send-hostname=no	dhcp-send-hostname=yes
dhcp-send-client-id=no	dhcp-send-client-id=yes
dhcp-accept-server-hostname=no	dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=no	dhcp-accept-server-domain=yes
vm-series-auto-registration-pin-id=abcdefgh1234**	**vm-series-auto-registration-pin-id=abcdefgh1234****
vm-series-auto-registration-pin-value=zyxwvut-0987**	**vm-series-auto-registration-pin-value=zyxwvut-0987****

©2023 Palo Alto Networks, Inc.

Vous ne pouvez pas spécifier l'adresse IP de gestion et la configuration du masque réseau pour le pare-feu VM-Series dans AWS. Si cette valeur est définie, le pare-feu ignore les valeurs que vous avez spécifiées car AWS utilise un fichier de métadonnées dorsal pour attribuer l'adresse IP de gestion et le masque de réseau.

**La passerelle IPv6 par défaut est requise si vous incluez une adresse IPv6.*

***La commande opérationnelle `mgmt-interface-swap` concerne uniquement un pare-feu VM-Series dans AWS ou GCP.*

****`oop-cmd-dpdk-pkt-io=off` permet de désactiver DPDK sur le pare-feu VM-Series sur ESXi, KVM et GCP (DPDK est activé par défaut).*

***** `vm-series-auto-registration-pin-id` et `vm-series-auto-registration-pin-value` sont requis dans deux cas d'utilisation :*

- *Activation des licences de site – AutoFocus ou Cortex Data Lake – avec les options de licence Pay-As-You-Go (PAYG) du pare-feu VM-Series.*
- *Récupérez et installez le certificat de périphérique sur le pare-feu VM-Series.*

 ©2023 Palo Alto Networks, Inc.

Création du fichier bootstrap.xml

Utilisez ces instructions pour exporter la configuration à partir d'un pare-feu exécuté sur la même plateforme ou le même hyperviseur que votre déploiement cible.

STEP 1 | Exportez la configuration d'un pare-feu.

1. Sélectionnez **Device (Appareil)** > **Setup (Configuration)** > **Operations (Opérations)**.
2. Sélectionnez la configuration que vous souhaitez exporter.
   - Pour exporter la configuration d'exploitation, dans la section Configuration Management (Gestion de la configuration), exécutez **Export named configuration snapshot (Exporter un instantané de la configuration nommée)** et sélectionnez **running config.xml (configuration d'exploitation.xml)** dans le menu déroulant.
   - Pour exporter une version précédente de la configuration du pare-feu, dans la section Gestion de la configuration, exécutez **Export configuration version (Exporter une version de la configuration)** et sélectionnez la version de configuration appropriée dans le menu déroulant.

STEP 2 | Renommez le fichier de configuration et enregistrez.

1. Renommez le fichier `bootstrap.xml`.

   Pour que l'amorçage soit réussi, le nom de fichier doit correspondre exactement (sensible à la casse).
2. Enregistrez le fichier `bootstrap.xml` au même emplacement que le fichier `init-cfg.txt`.

 ©2023 Palo Alto Networks, Inc.

Préparation des licences pour l'amorçage

Pour mettre le pare-feu sous licence durant l'opération d'amorçage, vous devez acheter les codes d'autorisation et enregistrer les licences et abonnements sur le portail d'assistance de Palo Alto Networks avant de commencer l'amorçage.

Pour les pare-feu VM-Series fonctionnant en BYOL (ne s'applique pas à la mise sous licence basée sur l'utilisation – PAYG), vous devez disposer d'un ensemble de codes d'autorisation qui inclut le code d'autorisation de capacité, l'abonnement au support et tout autre abonnement dont vous avez besoin. L'opération de préparation des licences pour l'amorçage dépend du fait que le pare-feu dispose ou non d'un accès à Internet lors de l'amorçage :

- Accès direct à Internet : le pare-feu est connecté directement à Internet.
- Accès indirect à Internet : le pare-feu est géré par Panorama, qui possède un accès direct à Internet et la capacité d'extraire les clés de licence pour le compte du pare-feu.
- Aucun accès à Internet : le pare-feu utilise un service d'orchestration ou un script personnalisé pour extraire les clés de licence pour le compte du pare-feu.

- Pour les pare-feu VM-Series avec accès à Internet.

  Saisissez le code d'autorisation dans le dossier `/license` lors de la Préparation de l'ensemble d'amorçage.

- Pour les pare-feu VM-Series avec accès indirect à Internet.
  1. Enregistrez le code d'autorisation sur le portail d'assistance de Palo Alto Networks.
     1. Accédez au portail d'assistance, connectez-vous et sélectionnez **Assets (Ressources)** > **Register New Device (Enregistrer un nouveau périphérique)** > **Register device using Serial Number or Authorization Code (Enregistrer l'appareil à l'aide du numéro de série ou du code d'autorisation)**.
     2. Suivez les étapes pour Enregistrement du pare-feu VM-Series.
     3. Cliquez sur **Submit (Envoyer)**.
  2. Activez les codes d'autorisation sur le portail d'assistance de Palo Alto Networks pour générer les clés de licence.
     1. Accédez au portail d'assistance, connectez-vous et sélectionnez l'onglet **Assets** (Ressources).
     2. Pour chaque numéro de série, cliquez sur le lien **Action**.
     3. Sélectionnez le bouton **Activate Auth-Code (Activer le code d'autorisation)**.
     4. Saisissez le **Authorization code (Code d'autorisation)**, puis cliquez sur **Agree (Accepter)** et **Submit (Envoyer)**.
     5. Télécharger les clés de licence et enregistrez-les dans un dossier local.
     6. Continuez la Préparation de l'ensemble d'amorçage ; vous devez ajouter les clés de licence que vous avez téléchargées au dossier `\license` dans l'ensemble d'amorçage.

©2023 Palo Alto Networks, Inc.

- Pour un script personnalisé ou un service d'orchestration pouvant accéder à Internet pour le compte des pare-feu.

  Le script ou le service doit extraire l'ID du processeur et l'UUID depuis l'hyperviseur sur lequel le pare-feu est déployé et accéder au portail d'assistance de Palo Alto Networks avec l'ID de processeur, l'UUID, la clé de l'API et le code d'autorisation pour obtenir les clés requises. Reportez-vous à la section API de mise sous licence.

 ©2023 Palo Alto Networks, Inc.

Préparation de l'ensemble d'amorçage

Dans AWS, Azure ou GCP, vous pouvez créer l'ensemble d'amorçage dans votre stockage de cloud public.

- Le plugin VM-Series version 1.0.13 ou antérieure et les versions 2.0.0 et 2.0.1 prennent en charge un ensemble d'amorçage par compartiment de stockage.
- Le plug-in VM-Series version 2.0.2 ou ultérieure prend également en charge les sous-dossiers dans votre compartiment de stockage sur le cloud public. Au sein d'un compartiment, vous pouvez créer plusieurs dossiers et sous-dossiers, chacun contenant un ensemble d'amorçage. Généralement, un dossier représente la configuration pour un groupe de VM, comme un groupe d'appareils Panorama.

  Pour accéder à l'ensemble d'amorçage, indiquez le chemin complet vers le dossier d'amorçage. Par exemple : `my-storage/my-firewalls/bootstrap-2020-10-15`

Utilisez la procédure suivante pour préparer l'ensemble d'amorçage.

STEP 1 | Créez la structure de dossier de niveau supérieur pour l'ensemble d'amorçage.

Sur votre client ou ordinateur portable local, ou dans un compartiment de stockage du cloud public, créez les dossiers suivants :

```
/config
/content
/software
/license
/plugins
```

Vous pouvez laisser un dossier vide, mais vous devez disposer des quatre dossiers **`/config`**, **`/license`**, **`/software`** et **`/content`**. Le dossier **`/plugins`** est facultatif et n'est requis que si vous mettez à niveau le Plug-in VM-Series indépendant d'une version PAN-OS.

Ne placez aucun autre fichier ou dossier dans cette structure d'amorçage. L'ajout d'autres fichiers ou dossiers entraînera un échec de l'amorçage.

```
/my-storage                          /my-firewalls
       /internal     /external             /config        /config
         /content       /content           /license       /license
         /plugins       /plugins           /software      /software
```

STEP 2 | Ajoutez du contenu au sein de chaque dossier.

Pour une vue d'ensemble du processus, reportez-vous à la section Ensemble d'amorçage. Pour plus d'informations sur les fichiers dans le dossier **`/config`**, reportez-vous à la section Fichiers de configuration d'amorçage.

```
/config
  0008C100105-init-cfg.txt
  0008C100107-init-cfg.txt
  bootstrap.xml
```

```
/content
  panupv2-all-contents-488-2590
  panup-all-antivirus-1494-1969
  panup-all-wildfire-54746-61460
/software
  PanOS_vm-10.0.0
/license
  authcodes
  0001A100110-url3.key
  0001A100110-threats.key
  0001A100110-url3-wildfire.key
/plugins
  vm_series-2.0.2
```

- *Si vous enregistrez les clés dans le dossier `license`, vous pouvez utiliser une convention de dénomination de fichier qui fonctionne pour vous, mais vous devez conserver l'extension `.key` dans le nom de fichier. Pour les codes d'autorisation, créez un fichier texte nommé `authcodes` (sans extension de fichier), ajoutez vos codes d'autorisation dans ce fichier et enregistrez-le dans le dossier `license`.*
- *Utilisez un ensemble de codes d'authentification au lieu de codes individuels de sorte que le pare-feu ou le service d'orchestration puisse extraire simultanément toutes les clés de licence associées au pare-feu. Si vous utilisez des codes d'authentification individuels au lieu d'un ensemble, le pare-feu ne récupèrera que la clé de licence pour le premier code d'authentification inclus dans le fichier.*
- *Dans le dossier `/plugins`, ne fournissez qu'un seul fichier binaire du plug-in VM-Series. Ne fournissez pas plusieurs versions de plug-in.*

STEP 3 | Créez l'ensemble d'amorçage.

Pour les pare-feu VM-Series, créez l'image au format approprié pour votre hyperviseur. Reportez-vous à la section Livraison de l'ensemble d'amorçage.

 ©2023 Palo Alto Networks, Inc.

Amorçage du pare-feu VM-Series sur AWS

STEP 1 | Choisissez une méthode d'amorçage.

- Pour ajouter une configuration de base à l'ensemble d'amorçage, passez à l'étape 2.
- Pour entrer une configuration de base en tant que données utilisateur ou utiliser des données utilisateur pour obtenir la configuration de base à partir d'un secret AWS, passez à l'étape 3.

STEP 2 | Préparez un compartiment S3, et un rôle IAM pour permettre l'accès en lecture.

Pour amorcer l'utilisation d'un fichier, vous devez connaître les autorisations AWS S3 et IAM requises pour terminer cette opération. Pour les instructions détaillées sur la création d'une politique, reportez-vous à la documentation AWS sur la Création de politiques gérées par le client.

L'interface de gestion du pare-feu VM-Series doit pouvoir accéder au compartiment S3 pour effectuer l'amorçage. Vous pouvez attribuer une adresse IP publique ou une adresse IP élastique à l'interface de gestion afin que le compartiment S3 soit accessible sur Internet. Vous pouvez également créer un point de terminaison VPC AWS dans la même région que le compartiment S3 si vous préférez créer une connexion privée entre votre VPC et le compartiment S3 et ne souhaitez pas activer l'accès Internet sur l'interface de gestion du pare-feu. Pour plus d'informations, reportez-vous à la documentation AWS sur la configuration des Points de terminaison VPC.

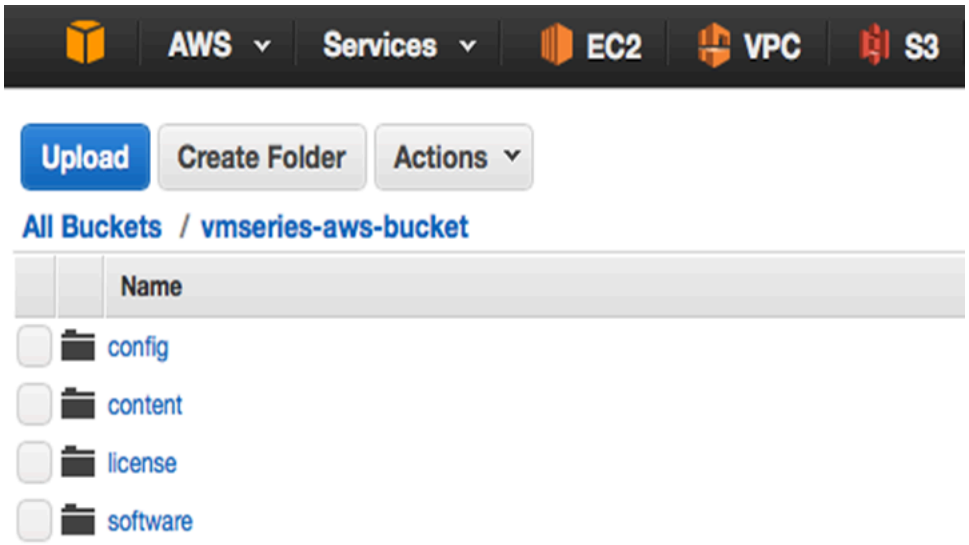
1. Créez un rôle IAM avec la politique en ligne pour autoriser un accès en lecture au compartiment S3 [ListBucket, GetObject]. Pour obtenir des instructions détaillées sur la création d'un rôle IAM, la détermination des comptes ou des services AWS qui peuvent assumer le rôle et la détermination des actions et des ressources API que l'application peut utiliser après avoir assumé le rôle, reportez-vous à la documentation AWS qui porte sur les rôles IAM dans Amazon EC2. Lors du lancement du pare-feu VM-Series, vous devez associer ce rôle pour autoriser l'accès au compartimentS3 et aux objets inclus dans le compartiment afin de réussir l'amorçage.
2. Sur la console AWS, créez un compartiment Amazon Simple Storage Service (S3), ou créez un sous-répertoire dans un compartiment S3 existant.

   Le compartiment S3 dans l'exemple suivant, vmseries-aws-bucket, se trouve au niveau du dossier racine All Buckets (Tous les compartiments).

```
{    "Version": "2012-10-17",    "Statement":
 [    {       "Effect": "Allow",       "Action":
 ["s3:ListBucket"],       "Resource":
 ["arn:aws:s3:::<bucketname>"]    },    {       "Effect":
 "Allow",       "Action": ["s3:GetObject"],       "Resource":
 ["arn:aws:s3:::<bucketname>/*"]       }    ] }
```


©2023 Palo Alto Networks, Inc.

3. Créez les dossiers dans le compartiment S3 comme décrit dans Préparation de l'ensemble d'amorçage.
   - Créez la structure directement dans votre compartiment S3.



   - (En option) Ajoutez du contenu au sein de chaque dossier. Vous pouvez laisser un dossier vide, mais vous devez disposer de tous les dossiers \config, \content, \license, et \software. Le dossier /plugins est facultatif.

> *Si vous avez autorisé la connexion dans Amazon S3, un dossier Logs (Journaux) est automatiquement créé dans le compartiment S3. Le dossier Logs facilite la résolution des problèmes d'accès au compartiment S3.*

STEP 3 | Lancez le pare-feu VM-Series sur AWS. Choisissez l'une des options suivantes.

- **`init-cfg.txt`**—Si vous utilisez un fichier pour configurer le pare-feu, joignez le rôle IAM que vous avez créé à l'étape 2.1, agrandissez la section **Advanced Details (Détails avancés)**, et dans le champ **User Data (Données utilisateur)**, indiquez le chemin d'accès à un compartiment, répertoire ou sous-répertoire S3. Par exemple,

```
vmseries-bootstrap-aws-s3bucket=<bucketname>
```

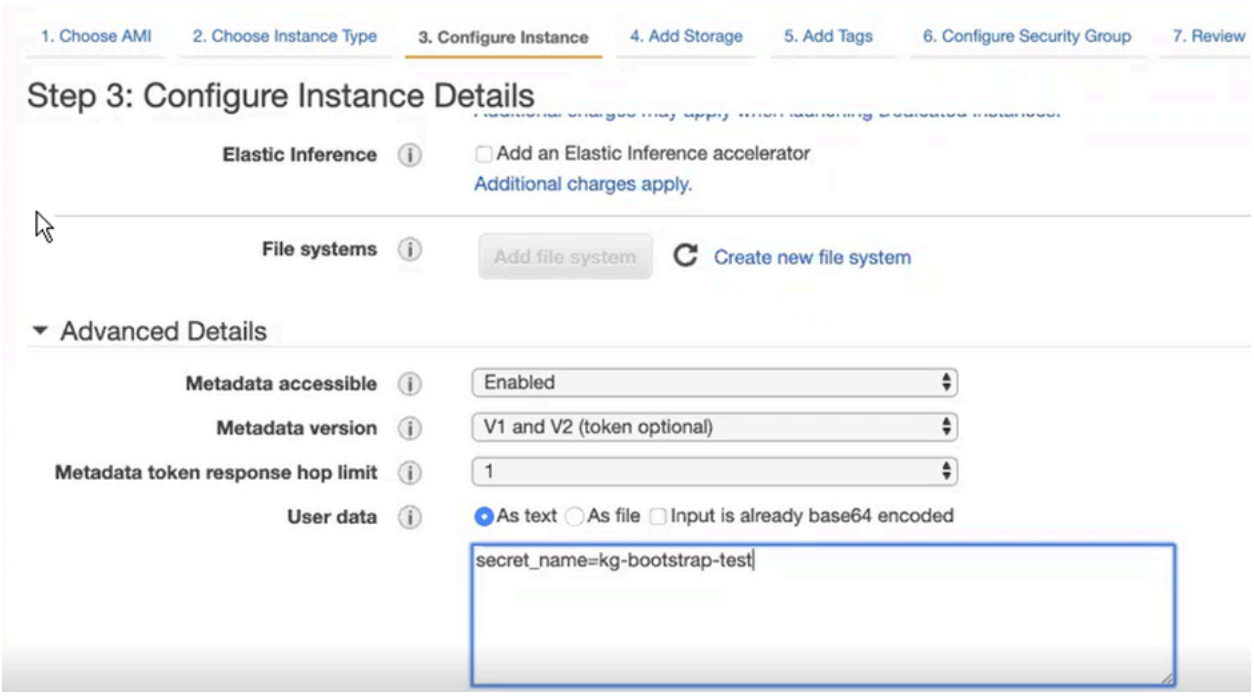
  ou

```
vmseries-bootstrap-aws-s3bucket=<bucketname/directoryname>
```

- **Données utilisateur**—Si vous utilisez des données utilisateur pour configurer le pare-feu, développez la section **Advanced Details (Détails avancés)** et, dans le champ **User Data (Données utilisateur)** saisissez les paramètres d'amorçage initiaux comme décrit dans Saisir une configuration de base en tant que données utilisateur (clouds publics).
- **AWS Secrets Manager**—Si vous avez enregistré votre configuration de base comme décrit dans Enregistrer une configuration de base dans AWS Secrets Manager, développez la section **Advanced Details (Détails avancés)** et, dans le champ **User Data (Données utilisateur)**,

©2023 Palo Alto Networks, Inc.

choisissez **As text (Sous forme de texte)** et saisissez le nom du secret comme une paire clé-valeur. Par exemple :

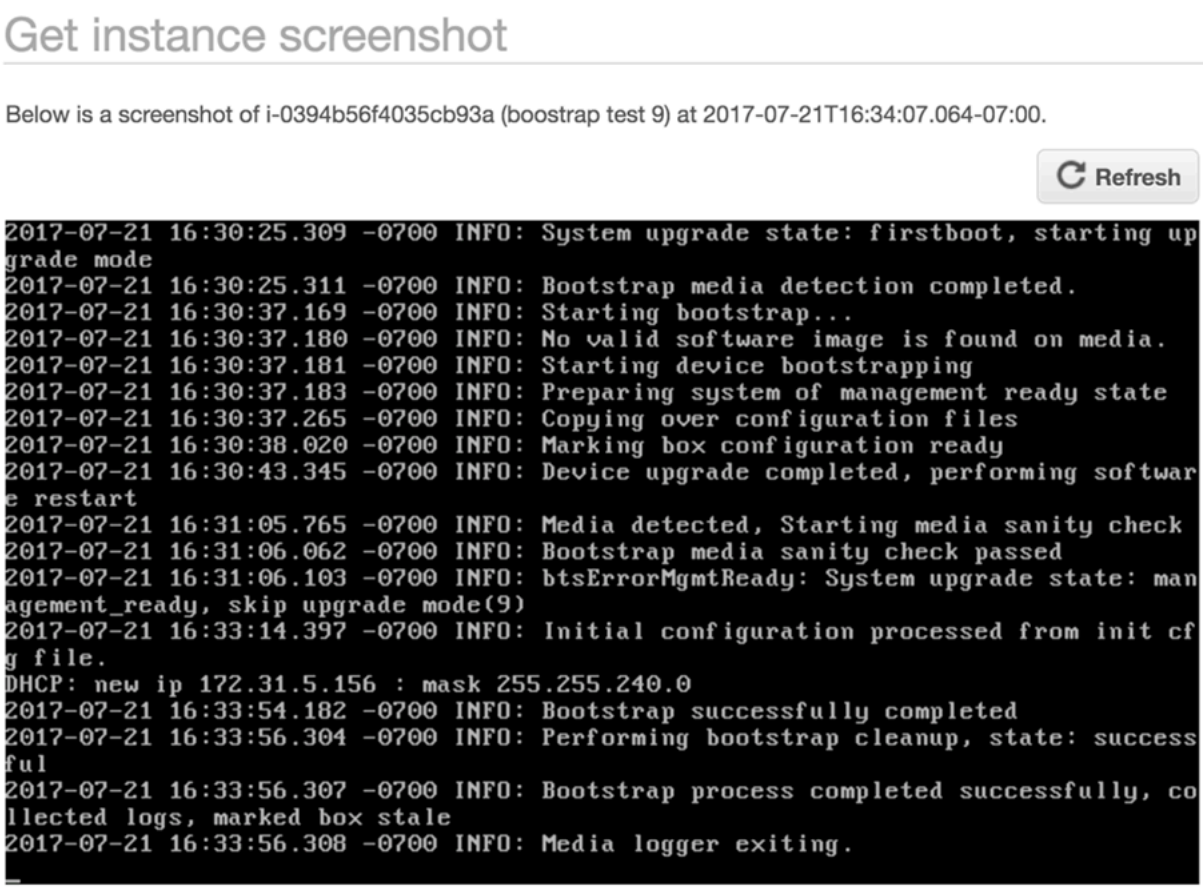


Sélectionnez **Review and Launch (Vérifier et lancer)**. Pour plus de détails, reportez-vous à la section Lancement du pare-feu VM-Series sur AWS.

©2023 Palo Alto Networks, Inc.

STEP 4 | Vérifiez l'achèvement de l'amorçage. Sélectionnez l'instance de pare-feu dans la console de gestion AWS et choisissez **Actions** > **Instance Settings (Paramètres d'instance)** > **Get Instance Screenshot (Obtenir une capture d'écran de l'instance)**.

- La capture d'écran montre l'amorçage en cours. Un exemple d'amorçage réussi est présenté ci-dessous :



- Si vous utilisez un compartiment S3 et que le compartiment S3 n'a pas les bonnes autorisations ou que vous n'avez pas les quatre dossiers dans le compartiment S3, vous voyez le message d'erreur suivant :



 ©2023 Palo Alto Networks, Inc.

Amorçage du pare-feu VM-Series dans Azure

Le pare-feu VM-Series sur Azure prend en charge le service ***Azure Files*** pour l'amorçage.

STEP 1 | Choisissez une méthode d'amorçage.

- Pour ajouter une configuration de base à l'ensemble d'amorçage, passez à l'étape 2.

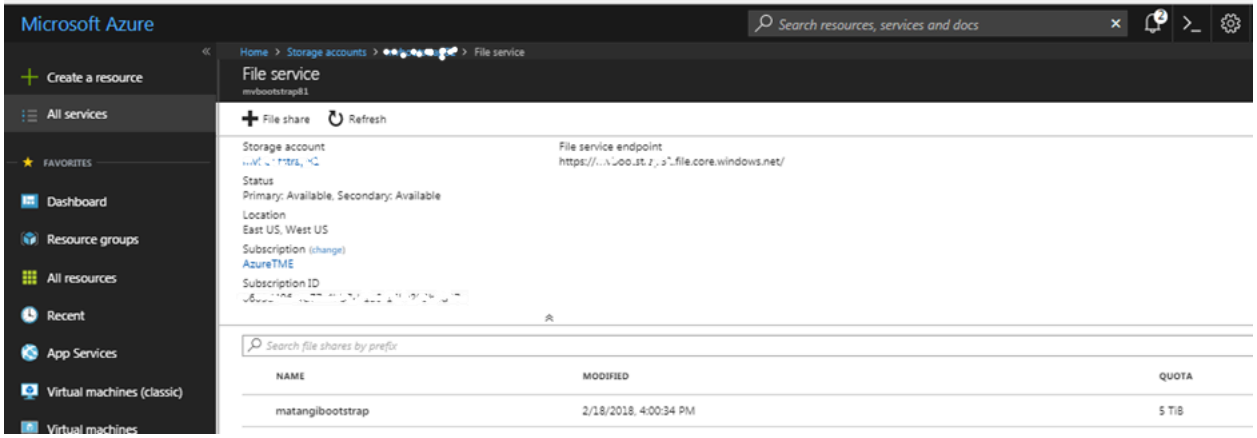
  Pour gérer les fichiers d'amorçage du pare-feu VM-Series sur Azure, vous devez connaître les comptes de stockage sur Azure et savoir comment créer un partage de fichiers et des objets d'annuaire contenant la structure de dossiers requise pour le module d'amorçage. Vous pouvez partager un partage de fichiers Azure sur de nombreuses machines virtuelles afin que tous les pare-feu déployés dans la même région que le compte de stockage hébergeant le partage de fichiers puissent accéder aux fichiers simultanément.

  L'interface de gestion du pare-feu VM-Series doit pouvoir accéder au partage de fichiers qui contient les fichiers d'amorçage afin qu'ils puissent effectuer l'amorçage.

- Pour Saisir une configuration de base en tant que données utilisateur (clouds publics), passez à l'étape 3.2.

STEP 2 | Configurez les fichiers d'amorçage dans un service Azure Files.

1. Sur le portail Azure, sélectionnez ou créez un compte de stockage.
2. Créez un partage de fichiers dans le service Azure Files.

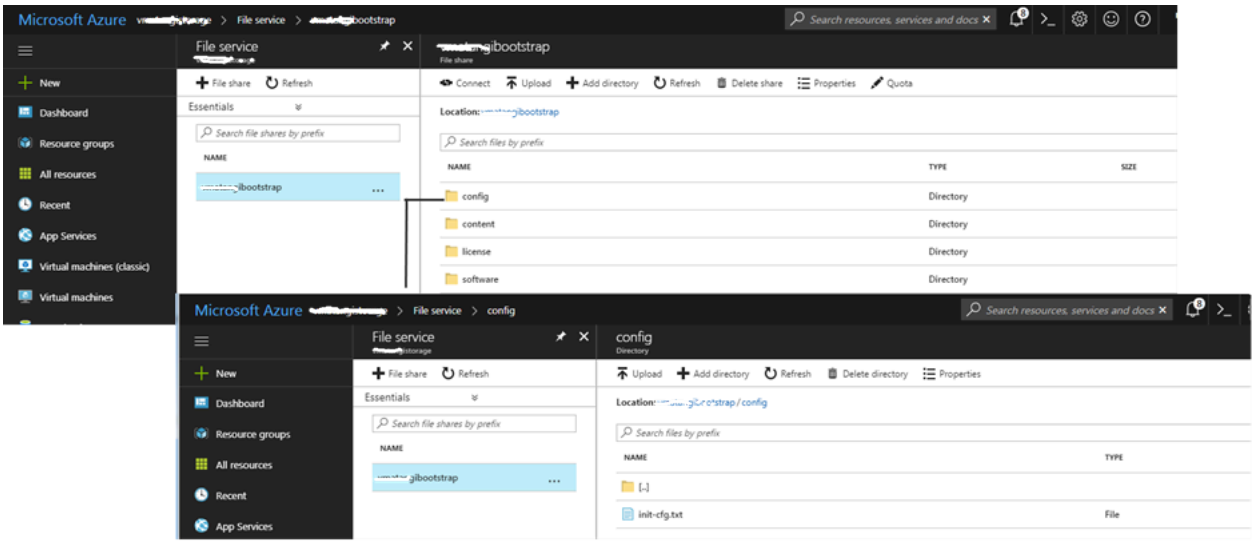


3. Créez les dossiers dans le compte de stockage.

   - Créez la structure de répertoire de premier niveau pour l'ensemble d'amorçage directement dans le dossier racine et créez un sous-dossier pour chaque configuration d'amorçage.
   - Ajoutez des dossiers de contenu au sein de chaque dossier. Vous pouvez laisser un dossier vide, mais vous devez disposer des quatre dossiers (config, license, software

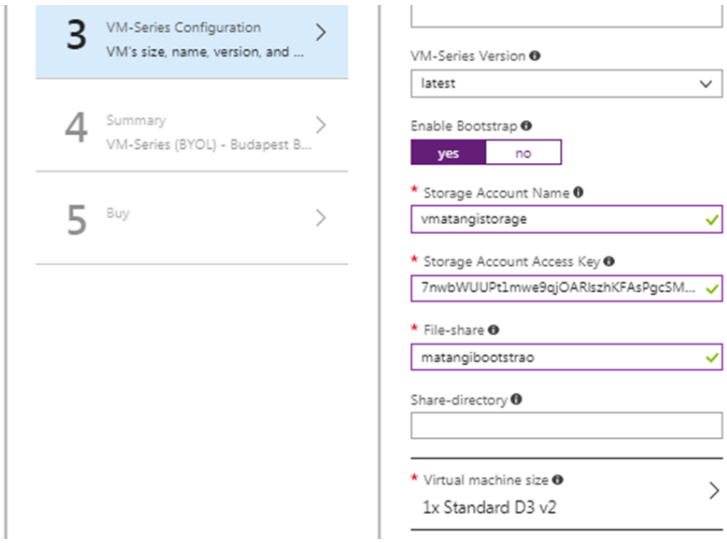
 ©2023 Palo Alto Networks, Inc.

et content) dans le dossier parent. Sur cette capture d'écran, vous pouvez voir que le répertoire **config** contient le fichier **init-cfg.txt**.



STEP 3 | Déploiement du pare-feu VM-Series depuis Azure Marketplace (modèle de solution).

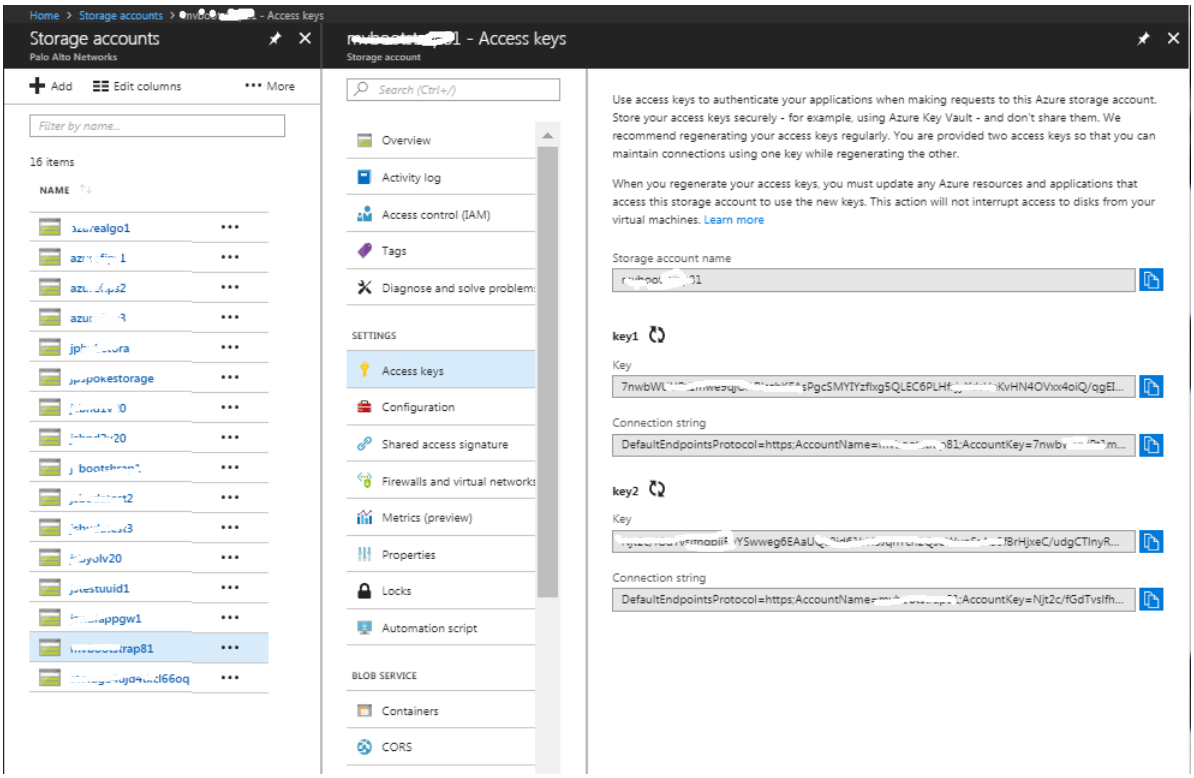
- Si vous utilisez un fichier pour configurer le pare-feu, passez à l'étape 3.1
- Si vous utilisez des données personnalisées pour configurer le pare-feu, passez à l'étape 3.2.



1. Si vous choisissez d'utiliser l'ensemble d'amorçage, sélectionnez **Enable Bootstrap: Yes (Activer l'amorçage : Oui)** et fournissez les informations requises pour accéder au partage de fichiers contenant les fichiers d'amorçage.
    1. **Nom du compte de stockage** : il s'agit du compte de stockage Azure dans lequel vous avez créé le partage de fichiers pour les dossiers d'amorçage.
    2. **Clé d'accès au compte de stockage** : ce pare-feu a besoin de cette clé d'accès pour s'authentifier auprès du compte de stockage et accéder aux fichiers stockés à l'intérieur.

©2023 Palo Alto Networks, Inc.

Pour copier cette clé d'accès, sélectionnez le nom du compte de stockage, puis sélectionnez **Settings (Paramètres)** > **Access Keys (Clés d'accès)**.



3. **File-share (partage de fichiers)**—Le nom du partage de fichiers qui contient l'ensemble d'amorçage.
4. (En option) **Share-directory (Répertoire de partage)**—Le chemin d'accès à un sous-répertoire dans le partage de fichiers. Si vous avez un partage de fichiers commun qui sert de référentiel pour les configurations de l'amorçage pour différentes configurations, vous pouvez utiliser un répertoire de partage pour créer une hiérarchie de dossiers et accéder à un ensemble spécifique de sous-dossiers dans le partage de fichiers commun.

2. Entrez les paramètres de configuration en tant que données personnalisées. Pour les paires clé-valeur, consultez Saisir une configuration de base en tant que données utilisateur (clouds publics). Séparez chaque paire clé-valeur par un point-virgule. Par exemple :

```
type=dhcp-client; op-command-modes=jumbo-frame; vm-series-
auto-registration-pin-id=abcdefgh1234****; vm-series-auto-
registration-pin-value=zyxwvut-0987****
```

Fournir des données personnalisées en utilisant l'une des méthodes décrites dans les sections Custom data and Cloud-Init on Azure Virtual Machines (Données personnalisées et Cloud-Init sur les machines virtuelles Azure).

STEP 4 | Vérifiez l'achèvement de l'amorçage.

©2023 Palo Alto Networks, Inc.

Amorçage du pare-feu VM-Series sur ESXi

Vous pouvez amorcer le pare-feu VM-Series à l'aide d'une image ISO ou d'un disque dur virtuel.

- Amorçage du pare-feu VM-Series sur ESXi avec un fichier ISO
- Amorçage du pare-feu VM-Series sur ESXi avec un périphérique de stockage de bloc

Amorçage du pare-feu VM-Series sur ESXi avec un fichier ISO

Utilisez ces instructions pour amorcer le pare-feu VM-Series sur un serveur ESXi à l'aide d'un fichier ISO.

STEP 1 | Créez une image ISO et chargez-la dans le magasin de données d'un système de fichier de machine virtuelle (VMFS) ou sur un volume du système de fichier réseau (NFS).

1. Préparation de l'ensemble d'amorçage.
2. Créez une image ISO. L'outil que vous utilisez pour créer l'image varie en fonction du système d'exploitation de votre client.
3. Chargez l'image ISO dans un magasin de données de VMFS ou sur un volume du NFS qui est accessible à l'hôte ESX/ESXi.

STEP 2 | Déployez le pare-feu.

1. Configuration du pare-feu VM-Series sur un serveur ESXi.

   Par défaut, le pare-feu est déployé avec deux interfaces réseau : une pour le trafic de gestion et une pour le trafic de données. Assurez-vous que la première interface Ethernet sur le pare-feu, qui est l'interface de gestion, est connectée au groupe de ports du commutateur virtuel attribué à la gestion de périphérique.
2. Ne mettez pas le pare-feu sous tension.

STEP 3 | Associez l'image d'amorçage au pare-feu.

1. Sélectionnez le pare-feu VM-Series dans la liste **Inventory (Inventaire)**.
2. Cliquez sur **Edit Settings (Modifier les paramètres)** et sélectionnez **Virtual Hardware (Matériel virtuel)**.
3. Sélectionnez **Datastore iso file (Fichier ISO de magasin de données)** dans le menu déroulant **CD DVD drive (Lecteur CD DVD)** et cliquez sur **Browse (Parcourir)** pour rechercher l'image ISO.
4. Mettez le pare-feu sous tension. Le pare-feu commencera l'opération d'amorçage, qui prendra plusieurs minutes. Les messages d'état indiquant la réussite ou l'échec de l'opération s'afficheront sur la console.
5. Vérification d'achèvement de l'amorçage.

Amorçage du pare-feu VM-Series sur ESXi avec un périphérique de stockage de bloc

Utilisez ces instructions pour amorcer le pare-feu VM-Series sur un serveur ESXi à l'aide d'un périphérique de stockage de bloc.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Créez l'ensemble d'amorçage et le disque dur virtuel.

1. Créez l'ensemble d'amorçage.
2. Déployez une machine virtuelle Linux.
3. Sur la machine Linux, Préparation de l'ensemble d'amorçage. Vous pouvez laisser le dossier vide, mais vous devez disposer des quatre dossiers.
4. Associez un nouveau disque de données de moins de 39 Go à la machine virtuelle Linux.
5. Partitionnez le disque et formatez le système de fichier en ext3.
6. Créez un dossier pour le nouveau système de fichier et montez le disque sur la machine virtuelle Linux.
7. Copiez le contenu de votre ensemble d'amorçage sur le disque.
8. Démontez le disque.
9. Dissociez le disque de la machine virtuelle Linux. Prenez note du fichier disque décrivant le disque d'amorçage que vous avez créé. Il affiche le nom du magasin de données et le chemin d'accès au disque. En outre, ne cochez pas la case Delete Files From Datastore (Supprimer les fichiers du magasin de données), car cela supprime le disque.

STEP 2 | Déployez le pare-feu.

1. Configuration du pare-feu VM-Series sur un serveur ESXi.
2. Ne mettez pas le pare-feu sous tension.

STEP 3 | Associez l'ensemble d'amorçage au pare-feu.

1. Sélectionnez le pare-feu VM-Series dans la liste Inventory (Inventaire).
2. Cliquez sur **Edit Settings (Modifier les paramètres)** et sélectionnez **Virtual Hardware (Matériel virtuel)**.
3. Dans la liste déroulante New Device (Nouveau périphérique), sélectionnez **Existing Hard Disk (Disque dur existant)**. Sélectionnez le disque d'amorçage en fonction du magasin de données et du chemin notés précédemment.
4. Mettez le pare-feu sous tension. Le pare-feu commencera l'opération d'amorçage, qui prendra plusieurs minutes. Les messages d'état indiquant la réussite ou l'échec de l'opération s'afficheront sur la console.
5. Vérification d'achèvement de l'amorçage.

©2023 Palo Alto Networks, Inc.

Amorçage du pare-feu VM-Series sur la Google Cloud Platform

STEP 1 | Choisissez une méthode d'amorçage.

STEP 2 | Connectez-vous à Google Cloud Console.

- Pour ajouter une configuration de base à l'ensemble d'amorçage,, créez des fichiers d'amorçage comme décrit dans la section Prepare the Bootstrap Package (Préparer l'ensemble d'amorçage), et passez à l'étape 3.
- Pour entrer une configuration de base sous forme de métadonnées personnalisées, passez à l'étape 4.

 ©2023 Palo Alto Networks, Inc.

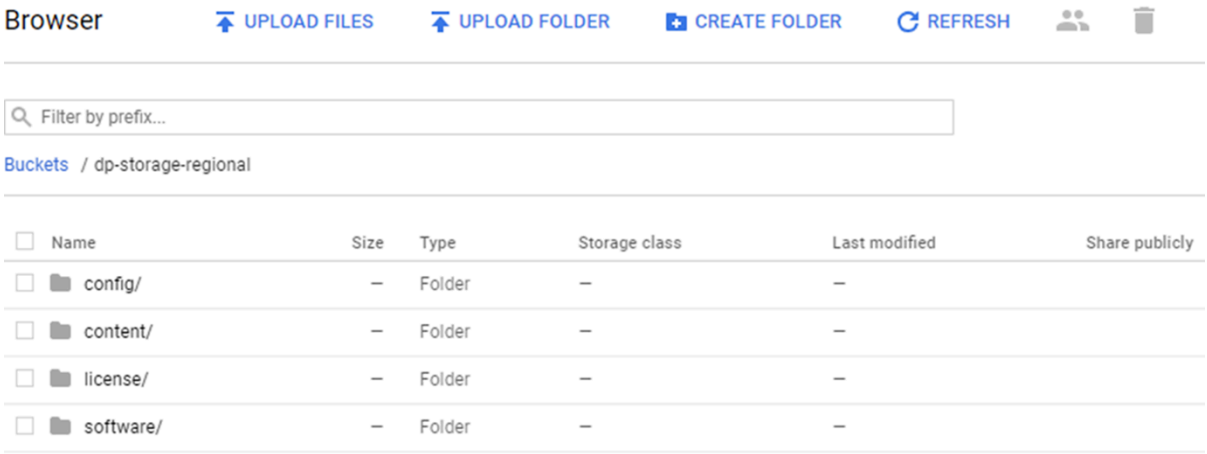
STEP 3 | Sélectionnez **Storage (Stockage)** > **Browser (Navigateur)**, puis cliquez sur **Create Bucket (Créer un compartiment).**.

Vous pouvez utiliser ce compartiment pour amorcer le pare-feu lorsque vous Déployer le pare-feu de la série VM à partir du marché de la plateforme Google Cloud Launcher.

Si vous avez l'intention d'amorcer le pare-feu à l'aide d'un compartiment de stockage Google dans un même projet, vous devez disposer des droits IAM devstorage.read_only.

Vous pouvez créer et remplir le compartiment au niveau supérieur, ou vous pouvez créer un compartiment avec des sous-dossiers à l'intérieur afin que plusieurs ensembles d'amorçage puissent partager le même compartiment.

1. Entrez le nom du compartiment, choisissez la classe de stockage par défaut et choisissez un emplacement. Notez que l'emplacement du compartiment de stockage doit être compatible avec la zone que vous spécifiez pour l'instance de moteur de calcul.
2. Cliquez sur **Create (Créer)**.
3. Dans le navigateur de stockage, cliquez sur le nom du compartiment pour l'ouvrir.
4. Cliquez sur **Create Folder (Créer dossier)** appelez-le `config`. Cliquez sur **Create (Créer)**.
5. Répétez l'étape et créez des dossiers pour `content (contenu)`, `license`, et `software (logiciel)`, comme illustré ci-dessous. Tous les dossiers doivent être présents, même s'ils sont vides.



6. (Facultatif) Si vous avez créé un fichier **`init-cfg.txt`**, ouvrez le dossier `config`. Cliquez sur**Upload Files (Télécharger fichier)**, sélectionnez fichier **`init-cfg.txt`**, et cliquez sur **Open (ouvrir)**.
7. Ouvrez le dossier `License` et téléchargez le fichier **`authcodes`**.
8. Continuez jusqu'à ce que tous les fichiers d'amorçage soient téléchargés.

STEP 4 | Ajoutez les paramètres de configuration initiale sous forme de métadonnées. **Ajoutez** chaque paire clé-valeur comme décrit dans Saisir une configuration de base en tant que données utilisateur (clouds publics).

STEP 5 | Reportez-vous à la section Déployer le pare-feu de la série VM à partir du marché de la plateforme Google Cloud Launcher pour obtenir des détails sur le déploiement.

 ©2023 Palo Alto Networks, Inc.

Amorçage du pare-feu VM-Series sur Hyper-V

Vous pouvez amorcer le pare-feu VM-Series à l'aide d'une image ISO ou d'un disque dur virtuel.

- Amorçage du pare-feu VM-Series sur Hyper-V avec un fichier ISO
- Amorçage du pare-feu VM-Series sur Hyper-V avec un périphérique de stockage de bloc

Amorçage du pare-feu VM-Series sur Hyper-V avec un fichier ISO

Utilisez ces instructions pour amorcer le pare-feu VM-Series sur un serveur Hyper-V avec un fichier ISO.

STEP 1 | Créez une image ISO.

1. Préparation de l'ensemble d'amorçage.
2. Créez une image ISO. L'outil que vous utilisez pour créer l'image varie en fonction du système d'exploitation de votre client.
3. Chargez l'image ISO à un emplacement accessible sur l'hôte Hyper-V.

STEP 2 | Déployez le pare-feu.

1. Configuration du pare-feu VM-Series sur un hôte Hyper-V avec Hyper-V Manager.

   Par défaut, le pare-feu est déployé avec deux interfaces réseau : une pour le trafic de gestion et une pour le trafic de données. Assurez-vous que la première interface Ethernet sur le pare-feu, qui est l'interface de gestion, est connectée au vSwitch attribué à la gestion de périphérique.
2. Ne mettez pas le pare-feu sous tension.

STEP 3 | Associez l'image d'amorçage au pare-feu.

1. Dans Hyper-V Manager, sélectionnez le pare-feu VM-Series dans la liste **Virtual Machines (Machines virtuelles)**.
2. Cliquez sur **Settings (Paramètres)** > **Hardware (Matériel)** > **IDE Controller (Contrôleur IDE)** > **DVD Drive (Lecteur DVD)**.

   Si vous disposez de plusieurs lecteurs de DVD, l'image ISO doit être appliquée au premier lecteur.
3. Sous Média, cliquez sur le bouton radio **Image file (Fichier image)**.
4. Cliquez sur **Browse (Parcourir)** et sélectionnez l'image ISO que vous avez chargée.
5. Cliquez sur **Apply (Appliquer)** et **OK** pour quitter les paramètres de la machine virtuelle.
6. Mettez le pare-feu sous tension. Le pare-feu commencera l'opération d'amorçage, qui prendra plusieurs minutes. Les messages d'état indiquant la réussite ou l'échec de l'opération s'afficheront sur la console.
7. Vérification d'achèvement de l'amorçage.

©2023 Palo Alto Networks, Inc.

Amorçage du pare-feu VM-Series sur Hyper-V avec un périphérique de stockage de bloc

Utilisez ces instructions pour amorcer le pare-feu VM-Series sur un serveur Hyper-V à l'aide d'un périphérique de stockage de bloc.

STEP 1 | Créez l'ensemble d'amorçage et le disque dur virtuel.

1. Déployez une machine virtuelle Linux.
2. Sur la machine Linux, Préparation de l'ensemble d'amorçage. Vous pouvez laisser le dossier vide, mais vous devez disposer des quatre dossiers.
3. Associez un nouveau disque de données de moins de 39 Go à la machine virtuelle Linux.
   1. Mettez la machine virtuelle Linux hors tension.
   2. Dans Hyper-V, sélectionnez la machine virtuelle Linux dans la liste Virtual Machines (Machines virtuelles).
   3. Sélectionnez **Settings (Paramètres)** > **Hardware (Matériel)** > **IDE Controller (Contrôleur IDE)**.
   4. Sélectionnez **Hard Drive (Disque dur)**, puis cliquez sur **Add (Ajouter)**.
   5. Sélectionnez **Virtual Hard Disk (Disque dur virtuel)** et cliquez sur **New (Nouveau)**.
   6. Suivez les instructions à l'écran pour créer un nouveau disque dur virtuel (VHD). Notez le nom et le chemin d'accès du nouveau disque dur virtuel.
   7. Cliquez sur **Apply (Appliquer)** puis **OK** pour quitter les paramètres de la machine virtuelle.
   8. Mettez la machine virtuelle Linux sous tension.
4. Connectez-vous à la CLI de la machine virtuelle Linux.
5. Partitionnez le disque et formatez le système de fichier en ext3.
6. Créez un dossier pour le nouveau système de fichier et montez le disque sur la machine virtuelle Linux.
7. Copiez le contenu de votre ensemble d'amorçage sur le disque.
8. Démontez le disque.
9. Dissociez le disque de la machine virtuelle Linux.
   1. Mettez la machine virtuelle Linux hors tension.
   2. Sélectionnez la machine virtuelle Linux dans la liste Virtual Machines (Machines virtuelles).
   3. Sélectionnez **Settings (Paramètres)** > **Hardware (Matériel)** > **IDE Controller (Contrôleur IDE)**.
   4. Sélectionnez le VHD que vous avez créé.
   5. Cliquez sur **Remove (Retirer)**. Cela dissocie le disque dur virtuel mais ne le supprime pas.

STEP 2 | Déployez le pare-feu.

1. Configuration du pare-feu VM-Series sur un hôte Hyper-V avec Hyper-V Manager.
2. Ne mettez pas le pare-feu sous tension.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Associez l'image du disque d'amorçage au pare-feu.

1. Sélectionnez le pare-feu dans la liste Virtual Machines (Machines virtuelles).
2. Sélectionnez **Settings (Paramètres)** > **Hardware (Matériel)** > **IDE Controller (Contrôleur IDE)**.
3. Sélectionnez **Hard Drive (Disque dur)**, puis cliquez sur **Add (Ajouter)**.
4. Sélectionnez **Virtual Hard Disk (Disque dur virtuel)** et cliquez sur **Browse (Parcourir)**.
5. Accédez au VHD d'amorçage que vous avez créé, sélectionnez-le et cliquez sur **Open (Ouvrir)**.
6. Cliquez sur **Apply (Appliquer)** et **OK** pour quitter les paramètres de la machine virtuelle.
7. Mettez le pare-feu sous tension. Le pare-feu commencera l'opération d'amorçage, qui prendra plusieurs minutes. Les messages d'état indiquant la réussite ou l'échec de l'opération s'afficheront sur la console.
8. Vérification d'achèvement de l'amorçage.

 ©2023 Palo Alto Networks, Inc.

Amorçage du pare-feu VM-Series sur KVM

Vous pouvez amorcer le pare-feu VM-Series sur KVM à l'aide d'une image ISO ou d'un disque dur virtuel.

- Amorçage du pare-feu VM-Series sur KVM avec un fichier ISO
- Amorçage du pare-feu VM-Series sur KVM avec un périphérique de stockage de bloc

Amorçage du pare-feu VM-Series sur KVM avec un fichier ISO

Utilisez ces instructions pour amorcer le pare-feu VM-Series sur un serveur KVM à l'aide d'un fichier ISO.

STEP 1 | Créez une image ISO.

1. Préparez l'ensemble d'amorçage.
2. Créez une image ISO. L'outil que vous utilisez pour créer l'image varie en fonction du système d'exploitation de votre client.
3. Chargez l'image ISO à un emplacement accessible sur l'hôte KVM.

STEP 2 | Déployez le pare-feu.

1. Installez le pare-feu VM-Series sur KVM.

   Par défaut, le pare-feu est déployé avec deux interfaces réseau : une pour le trafic de gestion et une pour le trafic de données. Assurez-vous que la première interface Ethernet sur le pare-feu, qui est l'interface de gestion, est connectée au groupe de ports du commutateur virtuel attribué à la gestion de périphérique.
2. Ne mettez pas le pare-feu sous tension.

STEP 3 | Associez l'image d'amorçage au pare-feu.

1. Dans virt-manager, effectuez un double clic sur le pare-feu VM-Series pour ouvrir la console.
2. Consultez les détails du matériel VM en accédant à **View (Affichage)** > **Details (Détails)**.
3. Ouvrez le menu Add New Virtual Hardware (Ajouter un nouveau matériel virtuel) en cliquant sur **Add Hardware (Ajouter du matériel)**.
4. Modifiez le type de périphérique en CDROM IDE.
5. Cliquez sur le bouton radio **Select managed or other existing storage (Sélectionner un stockage géré ou autre stockage existant)** et cliquez sur **Browse (Parcourir)**. Repérez l'image ISO que vous avez créée et cliquez sur **Choose Volume (Choisir un volume)**.
6. Cliquez sur **Finish (Terminer)** pour quitter le menu Ajouter un nouveau matériel virtuel.
7. Mettez le pare-feu sous tension en accédant à **Virtual Machine (Machine virtuelle)** > **Run (Exécuter)**. Le pare-feu commencera l'opération d'amorçage, qui prendra plusieurs minutes. Les messages d'état indiquant la réussite ou l'échec de l'opération s'afficheront sur la console.
8. Vérifiez l'achèvement de l'amorçage.

 ©2023 Palo Alto Networks, Inc.

Amorçage du pare-feu VM-Series sur KVM avec un périphérique de stockage de bloc

Utilisez ces instructions pour amorcer le pare-feu VM-Series sur un serveur KVM à l'aide d'un périphérique de stockage de bloc.

STEP 1 | Créez l'ensemble d'amorçage et le disque dur virtuel.

1. Créez l'ensemble d'amorçage.
2. Créez une nouvelle image disque de moins de 39 Go, partitionnez le disque et formatez le système de fichiers en tant que ext3. Les outils que vous utilisez pour compléter ce processus varient en fonction de votre système d'exploitation.
3. Montez le fichier image disque et copiez l'ensemble d'amorçage préparé dans les fichiers image disque.
4. Copiez le contenu de votre ensemble d'amorçage sur le disque.
5. Démontez l'image de disque.
6. Chargez le fichier image disque à un emplacement accessible sur l'hôte KVM.

STEP 2 | Déployez le pare-feu.

1. Installez le pare-feu VM-Series sur KVM.
2. Ne mettez pas le pare-feu sous tension.

STEP 3 | Associez l'image du disque d'amorçage au pare-feu.

1. Dans virt-manager, effectuez un double clic sur le pare-feu VM-Series pour ouvrir la console.
2. Consultez les détails du matériel VM en sélectionnant **View (Affichage)** > **Details (Détails)**.
3. Ouvrez le menu Add New Virtual Hardware (Ajouter un nouveau matériel virtuel) en cliquant sur **Add Hardware (Ajouter du matériel)**.
4. Sélectionnez **Storage (Stockage)** puis **Select or create custom storage (Sélectionner ou créer un stockage personnalisé)**.
5. Cliquez sur le bouton **Manage (Gestion)** pour ouvrir la boîte de dialogue **Choose Storage Volume (Choisir le volume de stockage)** et sélectionnez le fichier image disque que vous avez précédemment créé.
6. Cliquez sur Choose Volume (Choisir le volume).
7. Assurez-vous que le type de périphérique est Disk Device (Périphérique de disque) et ne modifiez pas le Bus Type (Type de bus).
8. Cliquez sur Finish (Terminer).
9. Mettez le pare-feu sous tension. Le pare-feu commencera l'opération d'amorçage, qui prendra plusieurs minutes. Les messages d'état indiquant la réussite ou l'échec de l'opération s'afficheront sur la console.
10. Vérifiez l'achèvement de l'amorçage.

 ©2023 Palo Alto Networks, Inc.

Vérification d'achèvement de l'amorçage

Vous pouvez voir les journaux d'état de base sur la console durant l'amorçage et vous pouvez vérifier que l'opération est terminée.

STEP 1 | Si vous avez inclus les champs **`panorama-server`**, **`tplname`** et **`dgname`** dans votre fichier **`init-cfg.txt`**, vérifiez les périphériques gérés par Panorama, le groupe d'appareils et le nom de modèle.

STEP 2 | Vérifiez les paramètres généraux du système et la configuration. Accédez à l'interface Web et sélectionnez **Dashboard (Tableau de bord)** > **Widgets** > **System (Système)** ou utilisez les commandes opérationnelles CLI **`show system info`** et **`showconfig running`**.

STEP 3 | Vérifiez l'installation de la licence. Sélectionnez **Device** > **Licenses** ou utilisez les commandes opérationnelles de la CLI **`request license info`**.

STEP 4 | Si Panorama est configuré, gérez les versions de contenu et les versions de logiciel depuis Panorama. Si Panorama n'est pas configuré, utilisez l'interface Web pour gérer les versions de contenu et les versions de logiciel.

©2023 Palo Alto Networks, Inc.

Erreurs d'amorçage

Si vous recevez un message d'erreur durant l'opération d'amorçage, consultez le tableau suivant pour obtenir les détails.

Message d'erreur (gravité)	Raisons
Erreur d'image d'amorçage (élevée)	• Aucun périphérique externe n'a été détecté avec l'ensemble d'amorçage. Ou • Une erreur critique s'est produite lors du démarrage à partir de l'image sur le périphérique externe. L'opération d'amorçage a été annulée.
Aucun fichier de configuration d'amorçage sur le périphérique externe (élevée)	Le périphérique externe ne contenait pas le fichier de configuration d'amorçage.
Paramètres erronés ou absents pour les informations réseau obligatoires dans le fichier de configuration d'amorçage (élevée)	Les paramètres réseau requis pour l'amorçage étaient incorrects ou absents. Le message d'erreur indique les valeurs (adresse IP, masque réseau, passerelle par défaut) qui ont causé l'échec de l'amorçage.
Échec de l'installation d'une clé de licence pour le fichier <license-key-filename> (élevée)	La clé de licence n'a pas pu être appliquée. Cette erreur indique que la clé de licence utilisée était invalide. Le résultat inclut le nom de la clé de licence qui n'a pas pu être appliquée.
Échec d'installation de clé de licence avec un code d'autorisation <authcode> (élevée)	Le code d'autorisation de licence n'a pas pu être appliqué. Cette erreur indique que le code d'autorisation de licence utilisé était invalide. Le résultat inclut le nom du code d'autorisation qui n'a pas pu être appliqué.
Échec de validation de mise à jour de contenu (élevée)	Les mises à jour de contenu n'ont pas été correctement appliquées.
Support USBO préparé correctement en utilisant l'ensemble fourni (information)	L'image d'amorçage a été correctement compilée sur la clé USB. <username> : Préparation USB réussie en utilisant l'ensemble <bundlename>

©2023 Palo Alto Networks, Inc.

Message d'erreur (gravité)	Raisons
Amorçage réussi (information)	Le pare-feu a été correctement configuré avec le fichier de configuration d'amorçage. Le résultat inclut les clés de licence installées et le nom de fichier de la configuration d'amorçage. Sur les pare-feu VM-Series uniquement, la version de PAN-OS et la version de mise à jour de contenu sont également affichées.

Consultez les informations sur l'Ensemble d'amorçage et comment effectuer la Préparation de l'ensemble d'amorçage.

©2023 Palo Alto Networks, Inc.