paloalto TECHDOCS

Guía de implementación de VM-Series

Version 11.1



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

November 14, 2022

Table of Contents

Acerca del cortafuegos VM-Series 15

Implementaciones de VM-Series 16
VM-Series en alta disponibilidad 17
Compatibilidad con IPv6 en la nube pública 19
Actualización del cortafuegos VM-Series 21
Plugin VM-Series 22
Configure el plugin VM-Series en el cortafuegos 22
Actualización del plugin de VM-Series 23
Habilitar tramas gigantes en el cortafuegos VM-Series 26
Direcciones MAC asignadas por el hipervisor 28
Métricas personalizadas de PAN-OS publicadas para la supervisión 30
Interfaz utilizada para acceder a servicios externos en el cortafuegos de VM-Series 32
Compatibilidad con controladores PacketMMAP y DPDK 33
Habilitar la optimización del rendimiento de NUMA en el VM-Series 35
Habilite ZRAM en el cortafuegos VM-Series 37

Compatibilidad de sistemas virtuales en cortafuegos VM-Series 39

Licencias y requisitos previos para la compatibilidad con sistemas virtuales en VM-Series 40
Requisitos del sistema para la compatibilidad con sistemas virtuales en VM-Series 41
Habilitar el soporte de múltiples sistemas virtuales en el cortafuegos VM-Series 42
Habilitar el soporte de múltiples sistemas virtuales en VM-Series en la consola de Panorama 45
Habilitación de la compatibilidad con varios sistemas virtuales mediante el método de arranque 47

Licencia del cortafuegos VM-Series 49

Licencias de cortafuegos VM-Series 50
Tipos de licencia 50
vCPU flexibles y licencias de modelos fijos 51
Implementación flexible de vCPU y modelos fijos 53
Creación de una cuenta de asistencia técnica 55
Número de serie y formato de ID de CPU para el cortafuegos VM-Series 56
Utilice la gestión de licencias de software de cortafuegos basado en Panorama 57
Créditos NGFW de software 62
Límites máximos basados en la memoria 65
Activación de créditos 84
Crear un perfil de implementación 85
Gestionar un perfil de implementación 88

 ©2024 Palo Alto Networks, Inc.

Registrar el cortafuegos VM-Series (Créditos NGFW de software)....90
Aprovisionar Panorama....93
Migrar Panorama a una licencia NGFW de software....94
Transferir créditos....98
Renueve su licencia de créditos Software NGFW....100
Desactivar licencia (créditos NGFW de software)....104
Retirada de licencias de cortafuegos terminados incorrectamente....105
Establecer el número de las vCPU licenciadas....106
Personalizar núcleos de plano de datos....107
Migración de un cortafuegos a una licencia VM-Series flexible....108
API de licencias Software NGFW....110
Modelos VM-Series....121
Requisitos del sistema para VM-Series....122
Sobresuscripción de la CPU....125
Modo Lite de VM-50....125
Tipos de licencia del modelo VM-Series....126
Activar licencias del modelo VM-Series....138
Registro del cortafuegos VM-Series....144
Instalación de un certificado de dispositivo en el cortafuegos VM-Series....146
Cambio entre las licencias BYOL y PAYG....154
Cambio entre licencias del modelo VM-Series....155
Desactivación de licencia(s)....159
Renovación de los paquetes de licencias de cortafuegos VM-Series....163
API de licencias basada en modelos....165
¿Qué ocurre cuando la licencia caduca?....172
Licencias para proveedores de servicios de seguridad en la nube (CSSP)....175
Obtención de los Códigos de autenticación para los paquetes de licencia CSSP....175
Registro del cortafuegos VM-Series con un código de autenticación CSSP....176
Adición de información del cliente final para un cortafuegos VM-Series registrado....177

Configuración un cortafuegos VM-Series en un servidor ESXi....183

Implementaciones compatibles en el hipervisor vSphere de VMware (ESXi)....184
VM-Series en requisitos y limitaciones del sistema ESXi....185
VM-Series en requisitos del sistema de ESXi....185
VM-Series en limitaciones del sistema de ESXi....186
Instalación de un cortafuegos VM-Series en el hipervisor vSphere de VMware (ESXi)....188
Planificación de las interfaces para la VM-Series para ESXi....188
Aprovisionamiento del cortafuegos VM-Series en un servidor ESXi....189
Configuración inicial en VM-Series en ESXi....192

 ©2024 Palo Alto Networks, Inc.

Añadir espacio en disco adicional al cortafuegos VM-Series....194
Uso de VMware Tools en el cortafuegos VM-Series en ESXi y vCloud Air....195
Utilice vMotion para mover el cortafuegos VM-Series entre hosts....197
Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión en ESXi....198
Configurar el protocolo de control de agregación de enlaces....199
Supervisión de VM en vCenter....202
Acerca de VM Monitoring en VMware vCenter....202
Instalación del plugin de Panorama para VMware vCenter....203
Configure el plugin de Panorama para VMware vCenter....204
Solución de problemas de implementaciones de ESXi....208
Solución de problemas básicos....208
Problemas de instalación....208
Problemas de licencia....210
Problemas de conectividad....211
Ajuste de rendimiento de VM-Series para ESXi....213
Instalación del controlador NIC en ESXi....213
Habilitación de VPN en ESXi....214
Habilitación de SR-IOV en ESXi....214
Habilitación del modo de acceso VLAN ESXi con SR-IOV....215
Habilitación del soporte de colas múltiples para NIC en ESXi....217
Ajuste de función de red virtual (VNF) para el rendimiento....217

Configuración del cortafuegos VM-Series en vCloud Air....231

Acerca del cortafuegos VM-Series en vCloud Air....232
Implementaciones compatibles con vCloud Air....233
Implementación del cortafuegos VM-Series en vCloud Air....234

Configuración del cortafuegos VM-Series en VMware NSX-T....241

Configuración del cortafuegos VM-Series en VMware NSX-T (norte-sur)....242
Implementaciones compatibles del cortafuegos VM-Series en VMware NSX-T (norte-sur)....242
Componentes del cortafuegos VM-Series en NSX-T (norte-sur)....243
Implementación del cortafuegos VM-Series en NSX-T (norte-sur)....244
Amplíe la política de seguridad de NSX-V a NSX-T....258
Configuración del cortafuegos VM-Series en NSX-T (este-oeste)....261
Componentes del cortafuegos VM-Series en NSX-T (este-oeste)....261
Integración del cortafuegos VM-Series en NSX-T (este-oeste)....263
Implementaciones compatibles del cortafuegos VM-Series en VMware NSX-T (este-oeste)....264
Implementación de VM-Series mediante el flujo de trabajo basado en las operaciones....266

 ©2024 Palo Alto Networks, Inc.

Implementación de VM-Series mediante el flujo de trabajo basado en la seguridad 284
Eliminar una definición de servicio de Panorama 317
Migración de VM-Series en operación NSX-T a implementación basada en seguridad 317
Amplíe la política de seguridad de NSX-V a NSX-T 324
Utilice la migración in situ para trasladar su VM-Series de NSX-V a NSX-T 326

Configuración del cortafuegos VM-Series en AWS 333

Acerca del cortafuegos VM-Series en AWS 334
Tipos de instancias EC2 de AWS 334
Cortafuegos VM-Series en AWS GovCloud 335
Cortafuegos VM-Series en AWS China 335
Cortafuegos VM-Series en AWS Outposts 335
Terminología de AWS 336
Asignación de interfaz de gestión para su uso con Amazon ELB 339
Ajuste del rendimiento para el cortafuegos VM-Series en AWS 340
Implementaciones compatibles con AWS 342
Implementación del cortafuegos VM-Series en AWS 345
Obtención de la AMI 345
Hoja de trabajo para la planificación de VM-Series en la VPC de AWS 349
Inicio del cortafuegos VM-Series en AWS 351
Inicio del cortafuegos VM-Series en AWS Outposts 360
Creación de una imagen Amazon Machine Image personalizada (AMI) 370
Cifrado del volumen EBS para el cortafuegos VM-Series en AWS 372
Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión 373
Habilitación de la supervisión de CloudWatch en el cortafuegos VM-Series 374
Inicio de cortafuegos VM-Series y logs de estado en AWS 378
Implementaciones orquestadas de Panorama en AWS 385
Preparación para una implementación de AWS organizada 387
Organice una implementación del cortafuegos VM-Series en AWS 392
Ver el estado de implementación 400
Flujo de tráfico y configuraciones 402
Integración de VM-Series con un balanceador de carga Gateway de AWS 409
Integración manual de VM-Series con un balanceador de carga Gateway 412
Grupo de escalado automático de VM-Series con el balanceador de carga Gateway de AWS 444
Habilitar la resiliencia de sesión en el VM-Series para AWS 458
Alta disponibilidad para el cortafuegos VM-Series en AWS 461
Descripción general de HA en AWS 461
Funciones de IAM para HA 463

 ©2024 Palo Alto Networks, Inc.

Enlaces de HA....466
Sondeos de heartbeat y mensajes de saludo....466
Prioridad y preferencia de dispositivos....466
Temporizadores de HA....467
Configuración de HA activa/pasiva en AWS mediante una IP secundaria....467
Configuración de HA activa/pasiva en AWS mediante Interface Move....473
Migración de HA activa/pasiva en AWS....477
Utilice AWS Secrets Manager para almacenar certificados VM-Series....483
Caso de uso: Protección de las instancias de EC2 en AWS Cloud....486
Caso de uso: Uso de grupos de direcciones dinámicas para proteger las nuevas instancias de EC2 en la VPC....501
Caso de uso: Cortafuegos VM-Series como puertas de enlace de GlobalProtect en AWS....505
Componentes de la infraestructura de GlobalProtect....506
Implementación de gateways de GlobalProtect en AWS....506
Supervisión de recursos en AWS....508
Supervisión de recursos en AWS con el complemento de AWS en Panorama....508
Configuración del plugin AWS para la supervisión de VM en Panorama....508
Lista de atributos supervisados en la VPC de AWS....526
Permisos de IAM requeridos para supervisar la VPC de AWS....528

Configuración del cortafuegos VM-Series en KVM....529

VM-Series en KVM: especificaciones y requisitos previos....530
Opciones para conectar el VM-Series en la red....532
Requisitos previos de la serie VM en KVM....532
Implementaciones compatibles en KVM....538
Protección del tráfico en un host único....538
Protección del tráfico en una serie de hosts Linux....538
Instalación del cortafuegos VM-Series en KVM....540
Instalación del cortafuegos VM-Series en Hyper-V....540
Instalación del cortafuegos VM-Series utilizando un archivo ISO....547
Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión en KVM....549
Habilitación del uso de un controlador SCSI....549
Comprobación de PCI-ID para la ordenación de interfaces de red en el cortafuegos VM-Series....550
Configurar el protocolo de control de agregación de enlaces....551
Ajuste de rendimiento de VM-Series para KVM....555
Instalación de KVM y Open vSwitch en Ubuntu 16.04.1 LTS....555
Habilitación de Open vSwitch en KVM....555
Integración de Open vSwitch con DPDK....556
Habilitación de SR-IOV en KVM....560

 ©2024 Palo Alto Networks, Inc.

Habilitación del modo de acceso VLAN con SR-IOV 561
Habilitación del soporte de múltiples colas para NIC en KVM 562
Aislamiento de recursos de CPU en un nodo NUMA en KVM 563
Descarga tráfico inteligente 564
Descarga de tráfico inteligente: Compatibilidad con la Capa 3 (enrutamiento estático y dinámico) 564
Descarga de tráfico inteligente: Compatibilidad con NAT para Virtual Wire y L3 566
Descarga de tráfico inteligente: Requisitos 568
Descarga de tráfico inteligente: Interfaces 568
Descarga de tráfico inteligente: Escalabilidad 569
Descarga de tráfico inteligente: High Availability 570
Instalación de la DPU BlueField-2 572
Instale el cortafuegos VM-Series 573
Habilitar funciones virtuales 573
Compruebe el sistema DPU BlueField-2 574
Instale o actualice el software BlueField Bootstream 576
Instalar o actualizar el paquete Debian 577
Ejecute la Descarga de tráfico inteligente 578
Solución de problemas de la DPU BlueField-2 580
Descarga de tráfico inteligente: Resolución de problemas de tráfico 580
Descarga basada en software de corte 584

Configuración del cortafuegos VM-Series en Hyper-V 585

Implementaciones compatibles con Hyper-V 586
Protección del tráfico en un host Hyper-V único 586
Protección del tráfico en hosts Hyper-V múltiples 586
Requisitos del sistema en Hyper-V 588
Servicios de integración de Linux 589
Instalación del cortafuegos serie VM en Hyper-V 590
Antes de comenzar 590
Ajuste de rendimiento del cortafuegos VM-Series en Hyper-V 591
Provisión de cortafuegos VM-Series en un host Hyper-V con gestor de Hyper-V 591
Provisión de cortafuegos VM-Series en un host Hyper-V con PowerShell 593
Configuración inicial del cortafuegos VM-Series 594

Configuración del cortafuegos VM-Series en Azure 597

Acerca del cortafuegos VM-Series en Azure 598
Azure Networking y el cortafuegos VM-Series 598
Integración del centro de seguridad de Azure 599
Plantillas de cortafuegos VM-Series en Azure 601

 ©2024 Palo Alto Networks, Inc.

Requisitos mínimos del sistema para VM-Series en Azure..... 602
Soporte para alta disponibilidad (HA) en VM-Series en Azure.....603
VM-Series en permisos de entidad de servicio de Azure..... 603
Implementaciones compatibles con Azure.....607
Implementación del cortafuegos VM-Series desde Azure Marketplace (plantilla de soluciones).....608
Implemente la plantilla de solución de Azure para un único cortafuegos VM-Series..... 614
Implemente la plantilla de solución Azure para cortafuegos de alta resiliencia VM-Series con balanceadores de carga..... 623
Implementación del cortafuegos VM-Series desde Azure China Marketplace (plantilla de soluciones).....633
Implementaciones organizadas de Panorama en Azure..... 639
Preparación para una implementación organizada..... 641
Organice una implementación del cortafuegos VM-Series en Azure..... 645
Implementar el VM-Series con el balanceador de carga de gateway de Azure..... 655
Creación de una imagen personalizada de VM-Series para Azure..... 664
Uso de las recomendaciones del centro de seguridad de Azure para proteger sus cargas de trabajo.....666
Implementación de un cortafuegos VM-Series basado en una recomendación del centro de seguridad de Azure.....666
Conexión de un cortafuegos VM-Series existente desde el centro de seguridad de Azure..... 668
Uso de Panorama para reenviar logs al centro de seguridad de Azure..... 670
Implementación del cortafuegos serie VM en Azure Stack.....673
Implementación del cortafuegos VM-Series en Azure Stack HCI..... 677
Habilitación de Application Insights de Azure en el cortafuegos VM-Series.....699
Implementación de Application Insights mediante espacio de trabajo.....701
Migración manual de Application Insights..... 704
Eliminación de Application Insights..... 709
Cambiar a una versión anterior..... 709
Supervisión en Azure..... 710
Acerca de la supervisión en Azure.....710
Configuración del plugin Azure para la supervisión en Panorama..... 710
Atributos supervisados con el plugin Panorama en Azure.....723
Configuración de la HA activo/pasivo en Azure..... 726
Configuración de HA activa/pasiva en Azure (tráfico norte-sur y este-oeste)..... 727
Configuración de HA activa/pasiva en Azure (solo tráfico este-oeste).....741
Utilice Azure Key Vault para almacenar certificados VM-Series..... 754
Uso de la plantilla ARM para implementar el cortafuegos VM-Series..... 757
Implementación de la plantilla VM-Series y Azure Application Gateway.....761
Plantilla VM-Series y Azure Application Gateway..... 762

 ©2024 Palo Alto Networks, Inc.

Comience a usar la plantilla VM-Series y Azure Application Gateway..... 763
Servicios seguros de Kubernetes en Azure..... 772
¿Cómo funciona el complemento de Panorama para Azure Secure Kubernetes Services?..... 772
Proteger un clúster AKS..... 777
Configuración del cortafuegos VM-Series en OpenStack..... 789
Implementaciones VM-Series en OpenStack..... 790
Gateway básico..... 790
Encadenamiento de servicios y Escalado de servicios..... 790
Componentes de VM-Series para la solución OpenStack..... 792
Plantilla Heat para una implementación básica de puerta de enlace..... 794
Plantillas Heat para encadenamiento de servicios y escalado de servicios..... 797
Red virtual..... 798
Máquina virtual..... 798
Plantilla de servicio..... 799
Instancia de servicio..... 800
IPAM..... 800
Política de servicio..... 801
Alarma..... 802
Instalación del cortafuegos VM-Series en una implementación de puerta de enlace básica..... 804
Instalación del cortafuegos VM-Series con encadenamiento y escalado de servicios..... 807
Configuración del cortafuegos VM-Series en Google Cloud Platform..... 811
Acerca del cortafuegos VM-Series en Google Cloud Platform..... 812
Google Cloud Platform y el cortafuegos VM-Series..... 812
Requisitos mínimos del sistema para el cortafuegos VM-Series..... 812
Implementaciones admitidas en Google Cloud Platform..... 814
Puerta de enlace de Internet..... 814
Puerta de enlace de segmentación..... 814
VPN IPSec híbrida..... 815
Cree una imagen personalizada del cortafuegos VM-Series para Google Cloud Platform..... 816
Preparación para configurar los cortafuegos VM-Series en la nube pública de Google..... 819
Requisitos generales..... 819
Instalación del complemento VM-Series en Panorama..... 820
Instalación del complemento de Panorama para GCP..... 820
Prepárese para implementar desde GCP Marketplace..... 822
Implementación del cortafuegos VM-Series en Google Cloud Platform..... 829

 ©2024 Palo Alto Networks, Inc.

Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace....829
Intercambio de interfaces de gestión para el equilibrio de carga de Google Cloud Platform....833
Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión....835
Habilitación de la supervisión de Google Stackdriver en el cortafuegos VM-Series....836
Habilitación de supervisión de VM para el registro de cambios de VM en Google Cloud Platform (GCP)....838
Uso de grupos de direcciones dinámicas para proteger instancias dentro de la VPC....841
Uso de plantillas personalizadas o la CLI de gcloud para implementar el cortafuegos VM-Series....843
Habilite la resiliencia de sesión en VM-Series para GCP....844
Supervisión de VM con el complemento de Panorama para GCP....848
Configuración de supervisión de VM con el complemento de Panorama para GCP....848
Escalado automático del cortafuegos VM-Series en Google Cloud Platform....855
Componentes de escalado automático para Google Cloud Platform....855
Implementar plantillas de escalado automático de GCP....867
Configurar HA activa/pasiva en Google Cloud Platform....895
Arquitectura de alta disponibilidad activa/pasiva en GCP....895
Implementar el HA activa/pasiva en GCP....897

Configuración de un cortafuegos VM-Series en una red Cisco ENCS....909

Planificación de su implementación ENCS de Cisco....910
Preparación de la imagen del cortafuegos VM-Series para Cisco ENCS....912
Convertir un archivo qcow2 desde la interfaz gráfica de usuario....912
Convertir un archivo qcow2 desde la interfaz de línea de comandos....914
Implemente el cortafuegos VM-Series en Cisco ENCS....917

Configuración del cortafuegos VM-Series en Oracle Cloud Infrastructure....921

Tipos de formas OCI....922
Implementaciones compatibles con OCI....923
Preparación para la configuración del cortafuegos VM-Series en OCI....924
Implementación del cortafuegos VM-Series desde Oracle Cloud Marketplace....927
Configuración de la HA activa/pasiva en OCI....932

Configuración del cortafuegos VM-Series en IMB Cloud....943

Acerca del cortafuegos VM-Series en IBM Cloud....944

©2024 Palo Alto Networks, Inc.

Información sobre licencias....944
Requisitos del sistema para el cortafuegos VM-series en IBM Cloud....944
Prepárese para configurar los cortafuegos VM-Series en IBM Cloud....945
Requisitos previos....945
Dependencias....945
Requisitos generales....946
Implemente el cortafuegos VM-Series utilizando IBM Cloud Schematics....948
Alta resiliencia para el cortafuegos VM-Series en IBM Cloud....950
Configuración del VM-Series de IBM VPC para alta disponibilidad....950
Implementación del cortafuegos VM-Series....950
Implemente el NLB....951
Configurar grupos de seguridad....951
Configurar rutas personalizadas....951
Consideraciones sobre las conmutaciones por error de NLB y las rutas personalizadas....951
Caso de uso: Implementar un NLB usando el cortafuegos VM-Series....952

Configuración del cortafuegos VM-Series en Alibaba Cloud....953

Cortafuegos VM-Series en Alibaba Cloud....954
Requisitos mínimos del sistema para el cortafuegos VM-Series en Alibaba Cloud....955
Requisitos de software del cortafuegos VM-Series....955
Recomendaciones de tipo de instancia de Alibaba Cloud para el cortafuegos VM-Series....955
CLI de Alibaba Cloud....956
Preparación para la implementación del cortafuegos VM-Series en Alibaba Cloud....957
Seleccione licencias y planifique las redes....957
Preparación para el uso de la interfaz de línea de comandos de Aliyun....958
Implemente el cortafuegos VM-Series en Alibaba Cloud....959
Cree una VPC y configure redes....959
Creación y configuración del cortafuegos VM-Series....962
Asegurar el tráfico norte-sur en Alibaba Cloud....966
Configuración del equilibrio de carga en Alibaba Cloud....969
Configuración de la HA activa/pasiva en Alibaba Cloud....971
Arquitectura....971
Implementar la HA activa/pasiva en Alibaba Cloud....973

Configuración de un cortafuegos en Cisco ACI....991

Integración del cortafuegos de Palo Alto Networks con Cisco ACI....992
Plantillas de gráficos de servicio....993
Implementaciones de contexto múltiple....994
Preparación de su entorno ACI para la integración....995
Integre el cortafuegos con Cisco ACI en modo de política de red....996

 ©2024 Palo Alto Networks, Inc.

Implementación del cortafuegos para asegurar el tráfico este-oeste en el modo de política de red ... 996
Implementación del cortafuegos para asegurar el tráfico norte-sur en el modo de política de red ... 1013
Supervisión de los endpoints en Cisco ACI ... 1030
Instalación del complemento de Panorama para Cisco ACI ... 1031
Configure el plugin Cisco ACI ... 1032
Complemento de Panorama para el panel de Cisco ACI ... 1036

Configuración del cortafuegos VM-Series en Cisco CSP ... 1041
Requisitos del sistema para VM-Series en Cisco CSP ... 1042
Implemente el cortafuegos VM-Series en Cisco CSP ... 1043

Configuración del cortafuegos VM-Series en Nutanix AHV ... 1045
Supervisión de máquinas virtuales en Nutanix ... 1046
Acerca de la supervisión de máquinas virtuales en Nutanix ... 1046
Instalación del complemento de Panorama para Nutanix ... 1047
Configuración del complemento de Panorama para Nutanix ... 1048

Arranque del cortafuegos VM-Series ... 1053
Seleccione un método de arranque ... 1054
Configuración básica ... 1055
Configuración completa ... 1058
Flujo de trabajo de arranque del cortafuegos VM-Series ... 1059
Paquete de arranque ... 1061
Estructura del paquete de arranque ... 1061
Entrega del paquete de arranque ... 1062
Archivos de configuración de arranque ... 1063
init-cfg.txt ... 1063
bootstrap.xml ... 1063
Generación de la clave de autenticación de VM en Panorama ... 1065
Creación del archivo init-cfg.txt ... 1067
Componentes de archivo de init-cfg.txt ... 1068
Archivo de muestra de init-cfg.txt ... 1072
Creación del archivo bootstrap.xml ... 1076
Preparación de las licencias para el arranque ... 1077
Preparación del paquete de arranque ... 1079
Arranque del cortafuegos VM-Series en AWS ... 1081
Arranque del cortafuegos VM-Series en Azure ... 1085
Arranque del cortafuegos VM-Series en Azure Stack HCI ... 1088
Arranque del cortafuegos VM-Series en ESXi ... 1099
Arranque del cortafuegos VM-Series en ESXi con una ISO ... 1099

 ©2024 Palo Alto Networks, Inc.

Arranque del cortafuegos VM-Series en ESXi con un dispositivo de almacenamiento en bloque....1099
Arranque del cortafuegos VM-Series en Google Cloud Platform....1101
Arranque del cortafuegos VM-Series en Hyper-V....1103
Arranque del cortafuegos VM-Series en Hyper-V con una ISO....1103
Arranque del cortafuegos VM-Series en Hyper-V con un dispositivo de almacenamiento en bloque....1103
Arranque del cortafuegos VM-Series en KVM....1106
Arranque del cortafuegos VM-Series en KVM con una ISO....1106
Arranque del cortafuegos VM-Series en KVM con un dispositivo de almacenamiento en bloque....1106
Verificación de la realización del bootstrap....1108
Errores de arranque....1109

 ©2024 Palo Alto Networks, Inc.

Acerca del cortafuegos VM-Series

El cortafuegos VM-Series de Palo Alto Networks es la versión virtualizada del cortafuegos de última generación de Palo Alto Networks. Es ideal para su uso en un entorno virtualizado o en la nube, donde puede proteger tanto el tráfico horizontal como vertical.

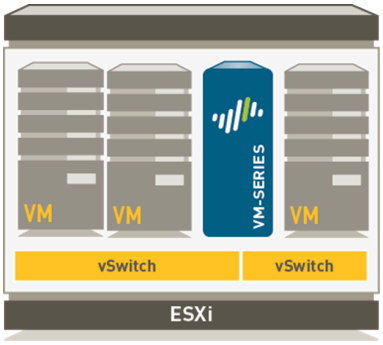
- Implementaciones de VM-Series
- VM-Series en alta disponibilidad
- Actualización del cortafuegos VM-Series
- Plugin VM-Series
- Habilitar tramas gigantes en el cortafuegos VM-Series
- Direcciones MAC asignadas por el hipervisor
- Métricas personalizadas de PAN-OS publicadas para la supervisión
- Interfaz utilizada para acceder a servicios externos en el cortafuegos de VM-Series
- Compatibilidad con controladores PacketMMAP y DPDK
- Habilitar la optimización del rendimiento de NUMA en el VM-Series
- Habilite ZRAM en el cortafuegos VM-Series

Implementaciones de VM-Series

El cortafuegos VM-Series puede implementarse en las siguientes plataformas:

- **VM-Series para el hipervisor vSphere de VMware (ESXi) y vCloud Air**

  Puede implementar cualquier modelo VM-Series como máquina virtual invitada en ESXi de VMware; ideal para la nube o las redes en las que es necesario el factor de forma virtual.

  Para más detalles, consulte Configuración un cortafuegos VM-Series en un servidor ESXi y Configuración del cortafuegos VM-Series en vCloud Air.

- **VM-Series en VMware NSX-T**

  Puede implementar los modelos VM-100, VM-300, VM-500 o VM-700 en su entorno NSX-T.

  Para obtener más detalles, consulte Configuración del cortafuegos VM-Series en VMware NSX-T (norte-sur).

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

  Puede implementar cualquier modelo VM-Series, excepto el VM-50, en instancias EC2 en la nube de AWS.

  Para más detalles, consulte Configuración del cortafuegos VM-Series en AWS.

- **VM-Series para Google Cloud Platform**

  Puede implementar cualquier modelo VM-Series, excepto el VM-50 y VM-50 Lite en las instancias de Google Compute Engine. Para obtener más detalles, consulte Configuración del cortafuegos VM-Series en Google Cloud Platform.

- **VM-Series para módulo de virtualización de Kernel (KVM)**

  Puede implementar cualquier cortafuegos VM-Series en un servidor Linux que ejecute el hipervisor KVM. Para más detalles, consulte Configuración del cortafuegos VM-Series en KVM.

- **VM-Series para Microsoft Hyper-V**

  Puede implementar cualquier cortafuegos VM-Series en un servidor de Windows Server 2012 R2 con el plugin de función de Hyper-V habilitado o un servidor Hyper-V 2012 R2 independiente. Para más detalles, consulte Configuración del cortafuegos VM-Series en Hyper-V.

- **VM-Series para Microsoft Azure**

  Puede implementar cualquier modelo VM-Series, excepto el VM-50, en Azure VNet.

  Para más detalles, consulte Configuración del cortafuegos VM-Series en Azure.

©2024 Palo Alto Networks, Inc.

VM-Series en alta disponibilidad

La alta disponibilidad (HA) es una configuración en la que dos cortafuegos se colocan en un grupo y su configuración se sincroniza para prevenir el fallo de un único punto en su red. La conexión de heartbeat entre los peers del cortafuegos garantiza una conmutación por error sin problemas en el caso de que falle un peer. La configuración de los cortafuegos en un clúster de dos dispositivos proporciona redundancia y le permite garantizar la continuidad de la actividad empresarial. En una configuración de HA en los cortafuegos VM-Series, ambos peers deben implementarse en el mismo tipo de hipervisor, tener recursos de hardware idénticos (como núcleos CPU/interfaces de red) asignados a ellos y tener configuradas las mismas licencias/suscripciones. Para obtener más información sobre HA en los cortafuegos de Palo Alto Networks, consulte Alta disponibilidad.

Los cortafuegos VM-Series admiten una alta disponibilidad activa/activa o activa/pasiva de estado con sincronización de sesión y configuración. El modo de implementación activo/activo es compatible con virtual wire e implementaciones de Capa 3 en algunos hipervisores de nube privada y se recomienda solo si cada cortafuegos necesita sus propias instancias de enrutamiento y usted necesita una redundancia completa en tiempo real de los dos cortafuegos en todo momento. Para configurar el cortafuegos VM-Series como un par de HA, consulte Configuración de la HA activa/pasiva y Configuración de la HA activa/activa.

Si está implementando el cortafuegos VM-Series en la nube pública, como en los Servicios web de Amazon (AWS) o Azure, puede usar la configuración tradicional de HA activa/pasiva; ver Alta disponibilidad para cortafuegos VM-Series en AWS y Configuración de la HA activo/pasivo en Azure.

Funciones/enlaces compatibles	ESX	KVM	AWS	NSX V	NSX T (N/S)	Hyper-V	Azure	GCP	OCI
HA activa/pasiva	Sí	Sí	yes (sí)	No	Sí	Sí	yes (sí)	No	Sí
HA activo/activo	Sí	yes (sí)	No	No	No	Sí	No	No	No
HA 1	Sí	Sí	yes (sí)	No	Sí	Sí	Sí	Sí	Sí
HA2—(sincronización de sesión y keepalive)	Sí	Sí	yes (sí)	No	Sí	Sí	Sí	Sí	Sí
HA3	Sí	yes (sí)	No	No	No	Sí	No	No	No

La compatibilidad con HA1 y HA2 para VM-Series en GCP requiere PAN-OS 10.0x o posterior y el complemento VM-Series 2.0.5 o posterior.

©2024 Palo Alto Networks, Inc.

La alta disponibilidad para el cortafuegos VM-Series en NSX-T (E/O) se logra a través de la función NSX-T llamada comprobación del estado del servicio. Esta función de NSX-T le permite simular alta disponibilidad en caso de que falle una instancia del servicio. Cuando se configura con el cortafuegos VM-Series, si falla una instancia de servicio VM-Series, cualquier tráfico dirigido a ese cortafuegos se redirige a otra instancia de cortafuegos en el clúster (para implementaciones de clúster de servicio) o una instancia de cortafuegos en otro host (para implementaciones basadas en host). Consulte Configuración de definición de servicio en Panorama para el cortafuegos VM-Series en NSX-T (E/O) para obtener más información.

 ©2024 Palo Alto Networks, Inc.

Compatibilidad con IPv6 en la nube pública

Use la siguiente tabla para revisar las características del VM-Series (enumeradas por categoría) compatibles con el tráfico IPv6 en la nube pública.

Actualmente, VM-Series es compatible con la nube de AWS.

Característica de VM-Series	AWS (versión 11.0.x o posterior)
Networking	
Rutas estáticas IPv6	#
Túnel estático IPv6 sobre IPv4	#
BGP a TGW	#
Tunelización GRE	#
ECMP	#
Compatibilidad con doble pila para interfaces de Capa 3	#
Enrutamiento mejorado de VPC	#
Detección de vecinos y de direcciones duplicadas	#
Inspección del contenido del túnel	#
NPTv6 (traducción de prefijos sin estado)	#
Detección de reenvío bidireccional (BFD)	#
Configuración de dirección dinámica de host (solo cliente DHCP)	#
QoS	
Política de QoS	#
Marcado de QoS	#
DSCP (basado en sesión)	#
VPN	

©2024 Palo Alto Networks, Inc.

Característica de VM-Series	AWS (versión 11.0.x o posterior)
GlobalProtect	#
IKE/IPSec *La compatibilidad se limita al tráfico IPv4 para el túnel IPSec/ VPN. Es compatible con el tráfico IPv6 con túnel IPv4.*	#
IKEv2	#
Túnel IPSec IPv6 sobre IPv4	#
Compatibilidad con GWLB para transmitir tráfico IPv6 encapsulado en el encabezado IPv4 GENEVE	#
Dispositivo	
HA: activo/pasivo	#
HA: transporte IPv6 para HA1 y HA2	#
Supervisión de rutas de alta disponibilidad (endpoint IPv6)	#
User-ID	
Asigna la dirección IPv6 a los usuarios	#
Portal de autenticación para IPv6	#
Conexión a agentes de User-ID a través de IPv6	#
API XML de User-ID para IPv6	#
IPv6 de agente de Terminal Server	#

©2024 Palo Alto Networks, Inc.

Actualización del cortafuegos VM-Series

La actualización de la versión PAN-OS o del modelo VM-Series le permite añadir las últimas funciones y correcciones que ayudan a mejorar las capacidades de seguridad y el rendimiento de sus cortafuegos.

La versión estándar de PAN-OS es solo eso; la versión normal de PAN-OS que se puede instalar en todos los cortafuegos de Palo Alto Networks. Las versiones PAN-OS XFR son solo para cortafuegos VM-Series y pueden incluir nuevas características y correcciones de errores para los cortafuegos VM-Series. Si instala una imagen de PAN-OS XFR en los cortafuegos VM-Series, las funciones y correcciones no estarán disponibles en las versiones de PAN-OS anteriores a la versión de software que ha instalado.

Dado que las imágenes XFR incluyen características y correcciones que son específicas de los cortafuegos VM-Series, si actualiza a una versión XFR, debe permanecer en las versiones XFR para mantener las características específicas de dicha versión hasta la próxima versión principal de PAN-OS. Todas las correcciones y capacidades disponibles en XFR se integrarán acumulativamente en la próxima versión principal de PAN-OS.

Palo Alto Networks no publica imágenes de base de VM-Series para cada versión de mantenimiento de PAN-OS. Si no hay ninguna imagen base disponible para la versión de destino de PAN-OS, actualice el cortafuegos VM-Series a la versión de destino o cambie a una versión anterior.

- #unique_25
- #unique_26
- #unique_27
- #unique_28
- #unique_29
- #unique_30
- #unique_31

Si desea obtener instrucciones sobre la instalación de su cortafuegos VM-Series, consulte Implementaciones de VM-Series.

Verifique la Requisitos del sistema para VM-Series *para su modelo de cortafuegos antes de actualizar. Si su cortafuegos tiene menos de 5,5 GB de memoria, la capacidad del sistema (número de sesiones, reglas, zonas de seguridad, objetos de direcciones, etc.) en el cortafuegos estará limitada a la del VM-50 Lite.*

 ©2024 Palo Alto Networks, Inc.

Plugin VM-Series

Los cortafuegos VM-Series incluyen el plugin VM-Series, una arquitectura de plugin integrada para la integración con proveedores de nube pública o hipervisores de nube privada. El plugin VM-Series se puede actualizar manualmente independientemente de PAN-OS, lo que permite a Palo Alto Networks® acelerar el lanzamiento de nuevas funciones, correcciones o integraciones con nuevos proveedores de nube o hipervisores.

El plugin VM-Series le permite gestionar las interacciones específicas de la nube entre los cortafuegos VM-Series y las plataformas de nube pública compatibles: AWS, GCP y Azure. El plugin permite la publicación de métricas personalizadas para los servicios de supervisión en la nube (como AWS CloudWatch), arranque, configuración de la información de aprovisionamiento de credenciales de usuario desde entornos de nube pública y actualizaciones integradas para bibliotecas en la nube o agentes en PAN-OS.

El plugin de VM-Series no gestiona las capacidades que son comunes a los cortafuegos de la VM-Series y a los cortafuegos basados en hardware. Por ejemplo, VM Monitoring no es parte del plugin VM-Series porque es una característica central de PAN-OS que le ayuda a aplicar la política de manera consistente en las cargas de trabajo de su máquina virtual, tanto desde cortafuegos VM-Series como desde los cortafuegos basados en hardware.

El complemento VM-Series no gestiona Complementos de Panorama*. Para conocer la diferencia entre el plugin de la VM-Series y los complementos de Panorama, consulte* Plugins de la VM-Series y plugin de Panorama.

El plugin VM-Series es un componente integrado que se puede actualizar o cambiar a una versión anterior, pero no eliminar. Cada versión de PAN-OS incluye una versión específica del plugin VM-Series que corresponde a la versión de software de PAN-OS. Cuando cambia a una versión anterior del software PAN-OS, la versión del plugin también cambia a una versión compatible con la versión PAN-OS. Puede actualizar o cambiar a una versión anterior del plugin VM-Series localmente en el cortafuegos virtual o gestionar la versión del plugin de forma central desde Panorama.

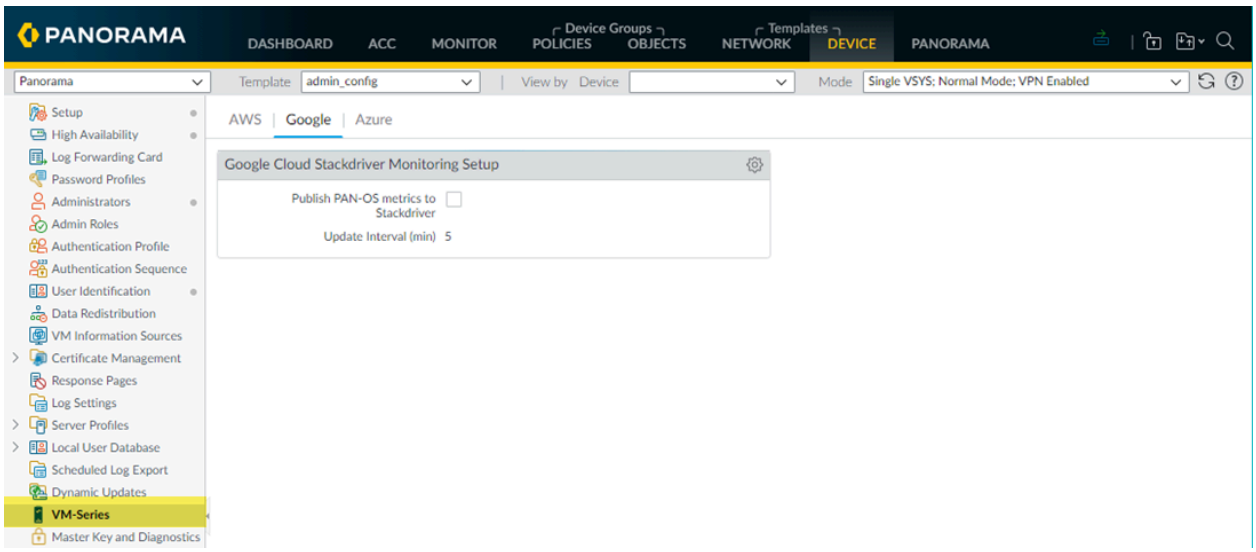
Para permitir que Panorama gestione la versión del plugin VM-Series o las métricas específicas de la nube que publican sus cortafuegos gestionados, debe instalar manualmente el plugin VM-Series en Panorama como se describe en Plugins de Panorama.

- Configure el plugin VM-Series en el cortafuegos
- Actualización del plugin de VM-Series

Configure el plugin VM-Series en el cortafuegos

Seleccione **Device (Dispositivo)** > **VM-Series** para configurar la integración del complemento para el proveedor de nube en el que se implementa esta instancia del cortafuegos VM-Series.

 ©2024 Palo Alto Networks, Inc.



Si el cortafuegos se implementa en un hipervisor o nube sin una interfaz pública (por ejemplo, VMware ESXi), la pestaña se denomina VM-Series y muestra un mensaje general.

Actualización del plugin de VM-Series

Cuando se lanza una actualización de plugin independiente de PAN-OS, puede actualizar de forma independiente la versión del plugin desde su cortafuegos VM-Series (como una actualización de software o de contenido) o desde un archivo de arranque.

Cada versión de plugin proporciona información de compatibilidad de PAN-OS e incluye nuevas funciones o correcciones de errores para uno o más entornos de nube.

STEP 1 | Antes de realizar la actualización, consulte las Notas de la versión más recientes para obtener información sobre si un nuevo plugin de VM-Series afecta su entorno.

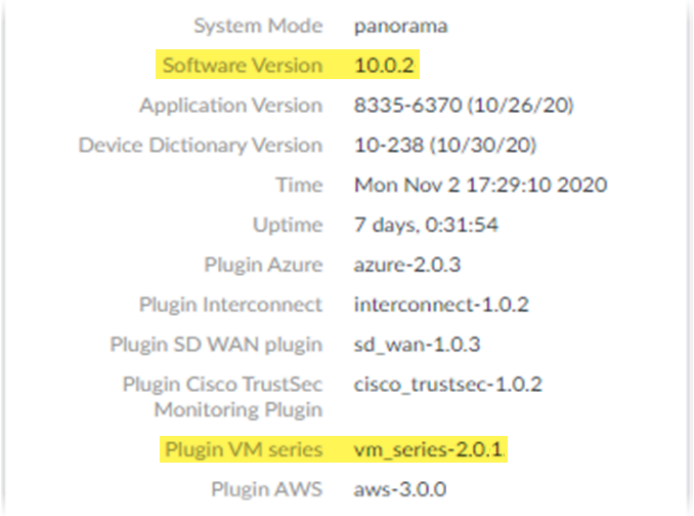
Por ejemplo, supongamos que una nueva versión del plugin VM-Series solo incluye las funciones de AWS. Para aprovechar las nuevas funciones, debe actualizar el plugin en sus instancias de cortafuegos VM-Series en AWS.

No instale una actualización que no corresponda a su entorno.

VM-Series 3.0.0 Plugin solo es compatible con PAN-OS 10.2.0.

 ©2024 Palo Alto Networks, Inc.

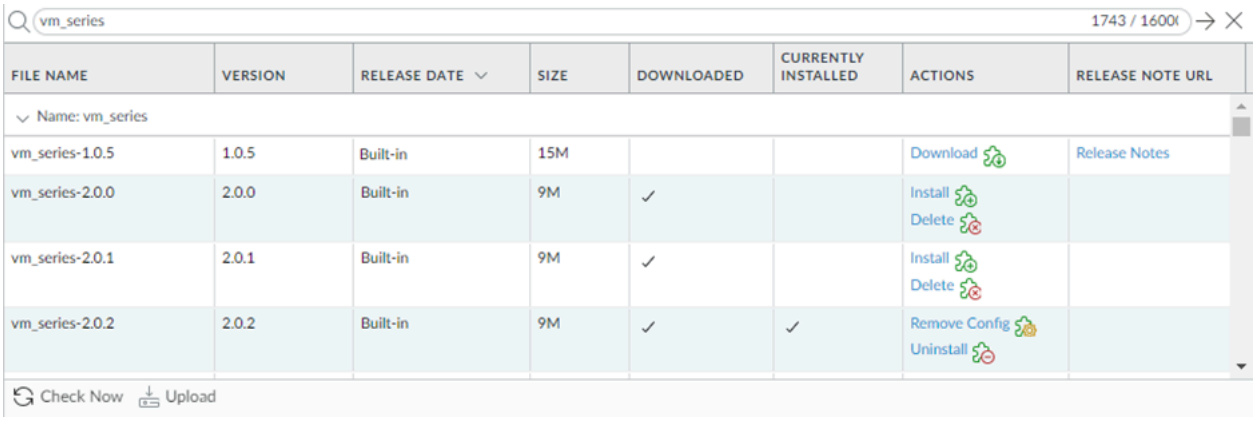
STEP 2 | Inicie sesión en el cortafuegos VM-Series y verifique el panel para ver la versión del plugin.



STEP 3 | Seleccione **Panorama** > **Plugins (Complementos)** y escriba **`vm_series`** en el campo de búsqueda.

Seleccione **Check Now (Comprobar ahora)** para ver las versiones disponibles.

STEP 4 | Seleccione una versión del complemento de VM-Series y haga clic en **Download (Descargar)**.

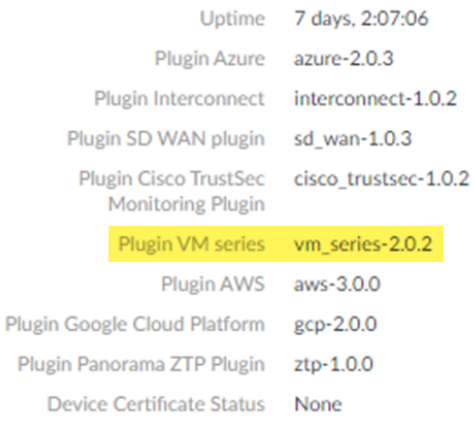


STEP 5 | Cuando finalice la descarga, haga clic en **Install (Instalar)** en la columna **Actions (Acciones)**.

El cortafuegos desinstala automáticamente la versión del complemento instalada anteriormente.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Consulte el **Dashboard (Panel)** para verificar que el complemento se ha actualizado correctamente.



 ©2024 Palo Alto Networks, Inc.

Habilitar tramas gigantes en el cortafuegos VM-Series

De manera predeterminada, el tamaño de la unidad máxima de transmisión (maximum transmission unit, MTU) para los paquetes enviados en una interfaz de Capa 3 es 1500 bytes. Este tamaño puede establecerse manualmente a cualquier tamaño de 512 a 1500 bytes por interfaz. Algunas configuraciones requieren tramas Ethernet con un valor de MTU mayor a 1500 bytes. Estas se llaman tramas gigantes.

Para usar tramas gigantes en un cortafuegos, debe habilitar específicamente las tramas gigantes a nivel global. Cuando están habilitadas, el tamaño predeterminado de MTU para todas las interfaces de Capa 3 se configura a un valor de 9192 bytes. Este valor predeterminado puede establecerse en cualquier valor en el rango de 512 a 9216 bytes.

Luego de establecer un tamaño de trama gigante global, este se convierte en el valor predeterminado para todas las interfaces de Capa 3 que no tenían explícitamente un valor de MTU establecido a nivel de configuración de la interfaz. Esto puede convertirse en un problema si solo desea cambiar las tramas gigantes de algunas interfaces. En estas situaciones, debe establecer el valor de MTU en cada interfaz de Capa 3 que no desee utilizar el valor predeterminado.

El siguiente procedimiento describe cómo habilitar las tramas gigantes en un cortafuegos, cómo establecer el valor predeterminado de MTU para todas las interfaces de Capa 3 y, luego, cómo configurar un valor diferente para una interfaz específica.

Las instancias del cortafuegos VM-Series implementadas con múltiples nodos NUMA, aparecen en modo MMAP de paquetes cuando la compatibilidad con tramas gigantes está habilitada. Debe deshabilitar la compatibilidad con tramas gigantes para usar DPDK en una instancia de cortafuegos VM-Series implementada con varios nodos NUMA.

STEP 1 | Habilite las tramas gigantes y establezca un valor global predeterminado de MTU.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y edite la sección Session Settings (Configuración de sesión).
2. Seleccione **Enable Jumbo Frame (Habilitar trama gigante)**.
3. Introduzca un valor en **Global MTU** (MTU global).

   El valor predeterminado es 9192. El rango de valores aceptables es el siguiente: 512 - 9216.
4. Haga clic en **OK (Aceptar)**.

   Se muestra un mensaje que le informa que habilitar o deshabilitar el modo de Tramas gigantes requiere un reinicio y que las interfaces de Capa 3 hereden el valor de **Global MTU (MTU global)**.
5. Haga clic en **Yes (Sí)**.

   Se muestra un mensaje para informarle que se habilitó Tramas gigantes y le recuerda que se requiere un reinicio del dispositivo para que este cambio se active.
6. Haga clic en **OK (Aceptar)**.
7. Haga clic en **Commit (Confirmar)**.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Establezca un valor de MTU para una interfaz de Capa 3 y reinicie el cortafuegos.

El valor configurado para la interfaz cancela el valor global de MTU.

1. Seleccione **Network (Red)** > **Interfaces**.
2. Seleccione una interfaz en **Interface type** (Tipo de interfaz) Capa 3.
3. Seleccione **Advanced (Avanzado)** > **Other Info (Otra información)**.
4. Introduzca un valor en **MTU**.

   El valor predeterminado es 9192. El rango de valores aceptables es el siguiente: 512 - 9216.
5. Haga clic en **OK (Aceptar)**.
6. Haga clic en **Commit (Confirmar)**.
7. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y seleccione **Reboot Device (Reiniciar dispositivo)**.

 ©2024 Palo Alto Networks, Inc.

Direcciones MAC asignadas por el hipervisor

Por defecto, el cortafuegos VM-Series utiliza la dirección MAC asignada a la interfaz física por el host/hipervisor para implementar el cortafuegos VM-Series con interfaces de capa 3. El cortafuegos puede usar la dirección MAC asignada por el hipervisor en sus respuestas ARP. Esta capacidad permite a los conmutadores sin aprendizaje, como vSwitch de VMware dirigir el tráfico a la interfaz del plano de datos en el cortafuegos sin requerir que el modo promiscuo esté habilitado en vSwitch. Si ni el modo promiscuo ni el uso de la dirección MAC asignada del hipervisor están habilitados, el host dejará caer la trama cuando detecte un fallo de coincidencia entre la dirección MAC de destino para una interfaz y la dirección MAC asignada del host.

No hay ninguna opción para habilitar o deshabilitar el uso de las direcciones MAC asignadas por el hipervisor en AWS y Azure. Está habilitado de manera predeterminada para ambas plataformas y no se puede deshabilitar.

Si está implementando el cortafuegos VM-Series en Capa 2, cable virtual o modos de interfaces tap, debe habilitar el modo promiscuo en el conmutador virtual al que se conecta el cortafuegos. El uso de la dirección MAC asignada por el hipervisor solo es relevante para las implementaciones de Capa 3, donde el cortafuegos suele ser la puerta de enlace predeterminada para las máquinas virtuales invitadas.

Cuando se habilita la funcionalidad de la dirección MAC asignada por el hipervisor en el cortafuegos VM-Series, tome nota de los siguientes requisitos:

- **Dirección IPv6 en una interfaz**: en una configuración de HA activa/pasiva (consulte VM-Series en alta disponibilidad), las interfaces de Capa 3 que usan direcciones IPv6 no deben usar direcciones generadas por EUI-64 como el identificador de interfaz (ID de interfaz). Debido a que EUI-64 usa direcciones MAC de 48 bit para derivar la dirección IPv6 para la interfaz, la dirección IP no es estática. Esto resulta en un cambio en la dirección IP para el peer de HA cuando el hardware que aloja el cortafuegos VM-Series cambia en una conmutación por error y produce una falla de HA.
- **Arrendamiento en una dirección IP**: cuando la dirección MAC cambia, el cliente DHCP, la retransmisión DHCP y las interfaces PPPoE podrían liberar las direcciones IP porque el arrendamiento de la dirección IP original podría terminar.
- **Direcciones MAC y ARP gratuitos**: los cortafuegos VM-Series con direcciones MAC asignadas al hipervisor en una configuración de alta disponibilidad funcionan de manera diferente que los dispositivos de hardware con respecto a las direcciones MAC. Los cortafuegos de hardware usan direcciones MAC variables autogeneradas entre dispositivos en un par de HA y la única dirección MAC utilizada en cada interfaz del plano de datos (por ejemplo, eth 1/1) se reemplaza con una dirección MAC virtual que es común a la interfaz del plano de datos en ambos peers de HA. Cuando habilita el uso de la dirección MAC asignada al hipervisor en el cortafuegos VM-Series en HA, la dirección MAC virtual no se utiliza. La interfaz del plano de datos en cada peer de HA es única y como la especifica el hipervisor.

  Debido a que cada interfaz del plano de datos tiene una dirección MAC única, cuando se produce una conmutación por error, el cortafuegos VM-Series debe enviar un ARP gratuito de modo que los dispositivos vecinos pueden conocer el emparejamiento de la dirección IP/MAC actualizado. Por lo tanto, para habilitar una conmutación por error de estado, los dispositivos de redes no deben bloquear ni ignorar los ARP gratuitos; asegúrese de deshabilitar la función de envenenamiento antiARP en los dispositivos interconexión de redes, si es necesario.

 ©2024 Palo Alto Networks, Inc.

Realice los siguientes pasos para configurar el cortafuegos VM-Series para utilizar las direcciones MAC de la interfaz proporcionadas por el host/hipervisor.

STEP 1 | Seleccione **Device (Dispositivo)** > **Management (Gestión)** > **Setup (Configuración)** > **General Settings (Configuración general)**.

STEP 2 | Haga clic en el icono **Edit (Editar)**.

STEP 3 | Active la opción para **Use Hypervisor Assigned MAC Address (Usar la dirección MAC asignada por el hipervisor)**.

Cuando se produce un cambio de la dirección MAC, el cortafuegos genera un log del sistema para registrar esta transición y la interfaz genera un ARP gratuito.

STEP 4 | Haga clic en **OK (Aceptar)**.

STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar el cambio en el cortafuegos. No necesita reiniciar el cortafuegos.

 ©2024 Palo Alto Networks, Inc.

Métricas personalizadas de PAN-OS publicadas para la supervisión

El cortafuegos publica de manera nativa las siguientes métricas en los sistemas de supervisión de la nube pública como AWS® CloudWatch, Azure® Application Insights y Google® Stackdriver. Estas métricas le permiten evaluar el rendimiento y los patrones de uso del cortafuegos de modo que pueda establecer alarmas y tomar medidas para automatizar eventos como el inicio o la finalización de instancias de los cortafuegos VM-Series. Debido a que estas métricas se publican mediante actualizaciones de contenido en el cortafuegos, asegúrese de tener la versión mínima de lanzamiento de contenido que se requiere para habilitar esta función en su cortafuegos VM-Series.

Métrica	Description (Descripción)
Utilización de CPU del plano de datos (%)	Supervisa el uso de la CPU del plano de datos y mide la carga de tráfico en el cortafuegos.
Uso del búfer de paquetes del plano de datos (%)	Supervisa el uso del búfer del plano de datos y mide su utilización. Si se produce una subida repentina en el tráfico, la supervisión del uso del búfer le permite asegurarse de que el cortafuegos no agote el búfer del plano de datos y cause el descarte de paquetes.
Túneles activos de la puerta de enlace de GlobalProtect™	Supervisa el número de sesiones activas de GlobalProtect en un cortafuegos desplegado como una puerta de enlace de GlobalProtect. Utilice esta métrica si usa este cortafuegos VM-Series como una puerta de enlace VPN para proteger a los usuarios remotos. Consulte la ficha técnica para conocer la cantidad máxima de túneles activos admitida en su modelo de cortafuegos.
Utilización del túnel de la puerta de enlace de GlobalProtect (%)	Supervisa los túneles activos de GlobalProtect en una puerta de enlace y mida el uso del túnel. Utilice esta métrica si usa este cortafuegos VM-Series como una puerta de enlace VPN para proteger a los usuarios remotos.
panSessionConnectionsPerSecond	Supervisa la velocidad por segundo de la nueva conexión establecida.
panSessionThroughputKbps	Supervisa el rendimiento en Kbps.
panSessionThroughputPps	Supervisa el número de paquetes por segundo.
Sesiones activas	Supervisa el número total de sesiones que están activas en el cortafuegos. Una sesión activa es una sesión que se encuentra en la tabla de búsqueda de flujo cuyos paquetes serán inspeccionados y reenviados, según lo requiera la política.

©2024 Palo Alto Networks, Inc.

Métrica	Description (Descripción)
Utilización de la sesión (%)	Supervisa las sesiones TCP, UDP, ICMP y SSL que están actualmente activas y la tasa de paquetes, la tasa de establecimiento de conexiones nuevas y el rendimiento del cortafuegos para determinar la utilización de la sesión.
Utilización del proxy SSL (%)	Supervisa el porcentaje de sesiones de proxy de reenvío de SSL con clientes para el descifrado SSL/TLS.

Para publicar estas métricas, consulte:

- Habilitar la supervisión de CloudWatch en el cortafuegos VM-Series
- Habilitar Azure Application Insights en el cortafuegos VM-Series
- Habilitar la supervisión de Google Stackdriver en el cortafuegos VM-Series

©2024 Palo Alto Networks, Inc.

Interfaz utilizada para acceder a servicios externos en el cortafuegos de VM-Series

Para acceder a los servidores de Palo Alto Networks y recuperar licencias y actualizaciones de contenido y software, y para publicar métricas PAN-OS personalizadas o recuperar direcciones IP y asignación de etiquetas para supervisar máquinas virtuales en su implementación, el cortafuegos VM-Series usa la interfaz de gestión excepto donde se indica a continuación. Para usar una interfaz del plano de datos en lugar de una interfaz de gestión compatible, debe configurar una ruta de servicio que especifique la interfaz del plano de datos que el cortafuegos puede usar para acceder al servidor o servicio.

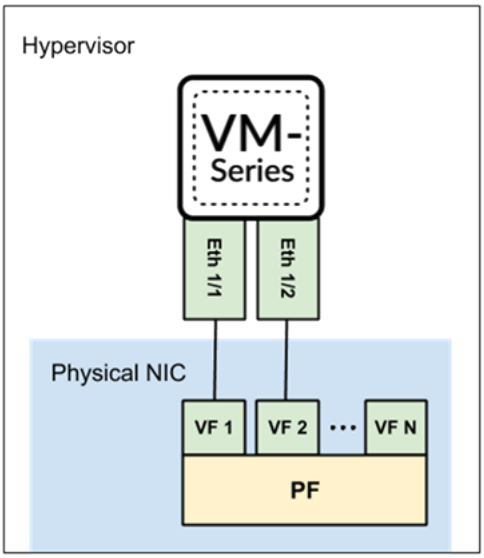
Acceso a la interfaz de servidor o servicio	Interfaz utilizada en el cortafuegos VM-Series
Licencias	Solo interfaz de gestión
Actualizaciones de software	Interfaz de gestión o Ruta de servicio
Bootstrapping desde una ubicación de almacenamiento en la nube, como el bucket de AWS S3, el servicio de archivos de almacenamiento de Azure o la interfaz de gestión del bucket	Solo interfaz de almacenamiento, incluso cuando se intercambian interfaces *Si el archivo de bootstrap.xml incluye códigos de autenticación de licencia, no puede usar una ruta de servicio. Para aplicar la licencia al cortafuegos, debe usarse la interfaz de gestión.*
Publicación de métricas de PAN-OS en un servicio de supervisión en la nube como AWS CloudWatch, Azure Application Insights o Google Stackdriver	Interfaz de gestión únicamente, incluso cuando las interfaces se intercambian
Supervisión de VM	Interfaz de gestión o Ruta de servicio

©2024 Palo Alto Networks, Inc.

Compatibilidad con controladores PacketMMAP y DPDK

La virtualización de entrada/salida de raíz única (SR-IOV) se basa en la comunicación entre los controladores de función virtual (VF) en el cortafuegos VM-Series, y los controladores de función física (PF) en el host (el hipervisor). El host utiliza controladores PF para comunicarse con sus NIC físicas y el cortafuegos VM-Series utiliza controladores de función virtual para comunicarse con los controladores de función física.

El siguiente diagrama es una visualización simple de ese concepto.



SR-IOV

¿Por qué utilizar SR-IOV? SR-IOV es una tecnología de aceleración de paquetes que permite que una máquina virtual acceda directamente a los paquetes desde la NIC. Por el contrario, cuando se usa un conmutador virtual, el host procesa los paquetes, envía los paquetes a través de un conmutador virtual y luego la máquina virtual recibe sus paquetes.

En la Matriz de compatibilidad, Versiones del controlador de PacketMMAP enumera tanto la versión del host como la versión del controlador nativo en el cortafuegos VM-Series. Por ejemplo, i40e en el host y en el cortafuegos, i40e (para PCI-passthrough) e i40evf (para SR-IOV).

Para SR-IOV, consideremos una NIC que usa el controlador i40e PF. El host se comunica con la NIC a través del controlador i40e. El cortafuegos VM-Series puede utilizar su controlador VF (i40evf) para comunicarse directamente con el controlador PF del host. Esto permite el acceso directo al cortafuegos VM-Series, lo que mejora la velocidad de procesamiento de paquetes. Para garantizar la compatibilidad, instale una versión del controlador PF del host que posteriormente será la versión del controlador PF nativo.

PCI-Passthrough

¿Por qué el cortafuegos VM-Series tiene controladores PF nativos? Como se menciona en Opciones para conectar VM-Series en la red, cuando se usa PCI-passthrough, la NIC está reservada para el cortafuegos VM-Series, por lo que el host (u otros invitados en el host) no pueden acceder a la NIC. En

 ©2024 Palo Alto Networks, Inc.

una configuración de PCI-passthrough, el cortafuegos VM-Series utiliza su controlador PF nativo para comunicarse directamente con la NIC del host.

Consulte la lista Versiones del controlador de PacketMMAP para determinar qué versión del controlador PF instalar en el host. Instale una versión de PF que sea superior al controlador PF nativo del cortafuegos VM-Series.

Consulte Habilitación de SR-IOV en ESXi y Habilitación de SR-IOV en KVM para PCI-Passthrough.

DPDK

PAN-OS tiene dos modos de procesamiento de paquetes, DPDK (predeterminado) y MMAP, y cada modo tiene un controlador nativo correspondiente en el cortafuegos VM-Series. Por ejemplo, si el cortafuegos está en modo DPDK, el cortafuegos usa la versión del controlador DPDK i40evf para comunicarse con el controlador i40e del host (cuando se usa SR-IOV). De forma alternativa, cuando el cortafuegos es Packet MMAP, utilizará una versión diferente del controlador i40evf para comunicarse con el controlador i40e del host.

Puede habilitar DPDK en el host (el hipervisor) o en el invitado (el cortafuegos VM-Series). La habilitación de ambos proporciona los mejores resultados.

- La compilación de OVS con DPDK es parte de la habilitación de DPDK en el host

  . Consulte Configuración de OVS y DPDK en el host.
- El DPDK de VM-Series habilita el controlador DPDK nativo en el cortafuegos VM-Series, por lo que no es necesario habilitar DPDK en el host, pero se recomienda para obtener el mejor rendimiento.

 ©2024 Palo Alto Networks, Inc.

Habilitar la optimización del rendimiento de NUMA en el VM-Series

Para mejorar el rendimiento de los cortafuegos VM-Series, puede habilitar la optimización del rendimiento del acceso a memoria no uniforme (NUMA). Cuando la optimización del rendimiento de NUMA está habilitada, el plano de datos del cortafuegos VM-Series utiliza vCPU conectadas al nodo NUMA 0. El plano de datos del cortafuegos VM-Series utiliza vCPU que pertenecen únicamente al nodo NUMA 0. El plano de gestión de VM-Series usa el núcleo 0, y el plano de datos de VM-Series puede usar las vCPU restantes en el nodo 0 de NUMA. Esta característica requiere PAN-OS 10.1.1 o posterior y el complemento VM-Series 2.1.1 o posterior.

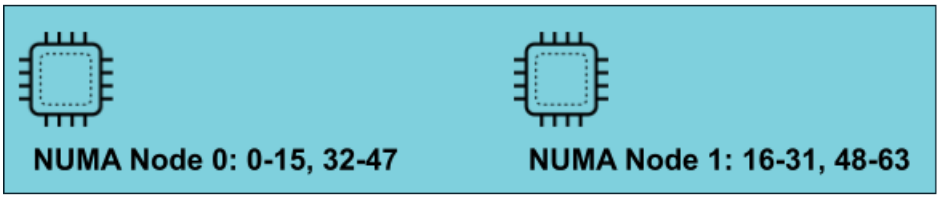
La optimización del rendimiento de NUMA está deshabilitada de forma predeterminada en PAN-OS 10.1.

Si tiene un dispositivo que contiene 64 núcleos en dos nodos NUMA, cuando la optimización del rendimiento de NUMA no está habilitada, las vCPU de plano de datos utilizadas por el cortafuegos VM-Series pueden estar en nodos diferentes, lo que afecta al rendimiento. Por ejemplo, si el sistema está organizado como se muestra en el ejemplo siguiente, e implementa un cortafuegos VM-Series con 32 núcleos totales con 24 núcleos de plano de datos.

Sin la optimización del rendimiento de NUMA, el cortafuegos VM-Series utiliza los núcleos 1 a 15 en el nodo 0 y del 16 al 24 en el nodo 1 porque asigna núcleos en orden numérico, independientemente de la ubicación del nodo. Con la optimización de NUMA habilitada, la serie VM-Series solo utiliza núcleos en el nodo 0, en este caso del 1 al 15 y del 33 al 39, independientemente del orden numérico. Los núcleos no utilizados por el plano de datos se asignan al plano de gestión.

Con la optimización del rendimiento de NUMA con la configuración personalizada del núcleo del plano de datos, la configuración de NUMA tiene prioridad. Por ejemplo, para una máquina virtual (VM) de 64 CPU con la optimización del rendimiento de NUMA habilitada y la configuración del núcleo del plano de datos 47, la configuración de NUMA tiene prioridad.

Si el número de núcleos asignados al cortafuegos VM-Series supera el número de vCPU en el nodo 0, el VM-Series utiliza todos los núcleos del nodo 0, pero no utiliza ningún núcleo de otros nodos. Por ejemplo, si asigna 30 núcleos al cortafuegos VM-Series pero el Nodo 0 solo tiene 24 núcleos, el cortafuegos VM-Series solo usará los 24 núcleos del Nodo 0 para el plano de datos.



STEP 1 | Inicie sesión en la CLI de VM-Series.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Ejecute el siguiente comando.

```
request plugins vm_series numa-perf-optimize enable on
Optimización del rendimiento de NUMA anterior: ninguno
Optimización del rendimiento de NUMA solicitada: Habilitado
Reinicie PA-VM.
```

STEP 3 | Una vez finalizado el reinicio, inicie sesión en la CLI del VM-Series y compruebe que la optimización de NUMA estaba habilitada.

```
show plugins vm_series numa-perf-optimize
Optimización del rendimiento de NUMA: Habilitado
```

STEP 4 | Compruebe el número de núcleos del plano de datos.

```
show plugins vm_series dp-cores
Núcleos DP actuales:31 núcleos DP personalizados configurados: 47
(Núcleos totales actuales: 64)
```

STEP 5 | Para deshabilitar la optimización del rendimiento de NUMA, utilice el siguiente comando. Este comando requiere que reinicie el cortafuegos VM-Series.

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

 ©2024 Palo Alto Networks, Inc.

Habilite ZRAM en el cortafuegos VM-Series

Si el cortafuegos VM-Series experimenta condiciones bajas o se queda sin memoria, puede habilitar ZRAM para mejorar el uso de la memoria. ZRAM, también llamado compcache (caché comprimida), es un módulo del kernel de Linux para crear un dispositivo de bloque comprimido en RAM. Cuando está habilitado, ZRAM se utiliza como disco de intercambio y permite una E/S de intercambio más rápida porque reside en la RAM.

Complete los pasos siguientes para habilitar ZRAM.

STEP 1 | Inicie sesión en la CLI de VM-Series.

STEP 2 | Busque la memoria total en la máquina virtual mediante el siguiente comando de la CLI.

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

```
KiB Mem: 9202656 total, 566504 libres, 3475840 usados, 5160312
 búf/caché KiB Mem: 9202656 total, 497112 libres, 3481944 usados,
 5223600 búf/caché KiB Mem: 9202656 total, 511744 libres, 3466768
 usados, 5224144 búf/caché KiB Mem: 9202656 total, 511668 libres,
 3466340 usados, 5224648 búf/caché KiB Mem: 9202656 total, 512124
 libres, 3465700 usados, 5224832 búf/caché KiB Mem: 9202656 total,
 511436 libres, 3465976 usados, 5225244 búf/caché KiB Mem: 9202656
 total, 510984 gratis, 3465944 usado, 5225728 búf/caché
```

STEP 3 | Convierta la memoria total anterior de KB a MB. Por ejemplo:

9202656 / 1024 = 8987 MB

Tome nota del valor total de memoria en MB. Necesitará este valor en el siguiente paso.

STEP 4 | Habilite ZRAM mediante los dos comandos de la CLI siguientes.

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

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

STEP 5 | Reinicie el cortafuegos VM-Series.

STEP 6 | Compruebe que ZRAM esté habilitada.

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

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Compatibilidad de sistemas virtuales en cortafuegos VM-Series

PAN-OS 11.1.3 y versiones posteriores Los sistemas virtuales son instancias de cortafuegos separados y lógicos en un único cortafuegos físico de Palo Alto Networks. En lugar de usar múltiples cortafuegos, las empresas y proveedores de servicios gestionados pueden usar un único par de cortafuegos (para una alta disponibilidad) y habilitar en ellos sistemas virtuales. Cada sistema virtual (vsys) es un cortafuegos independiente y gestionado de forma separada cuyo tráfico está separado del de otros sistemas virtuales. Los sistemas virtuales son más fáciles de gestionar coexistiendo dentro de un cortafuegos. Los beneficios adicionales de los sistemas virtuales incluyen escalabilidad mejorada, administración segmentada y reducción de los gastos de capital y operativos. Para obtener más información, consulte Beneficios de sistemas virtuales y Componentes y segmentación de los sistemas virtuales.

El soporte del sistema virtual en el cortafuegos VM-Series solo está disponible en la versión 11.1.3 y superior de PAN-OS.

Licencias y requisitos previos para la compatibilidad con sistemas virtuales en VM-Series

PAN-OS 11.1.3 y versiones posteriores Requisitos de licencia

El cortafuegos VM-Series es com sistemas virtuales solo con licencia flexible con **un** sistema virtual por defecto. Debe tener una licencia de sistema virtual para ser compatible con varios sistemas virtuales. Puede comprar licencias adicionales según sus requisitos hasta un número máximo admitido en un nivel específico. Para obtener más información, consulte Suscripción y servicios.

Utilice una licencia de cortafuegos flexible VM-Series e instancias de nivel 3 o 4 que admitan un mínimo de 16 vCPU o más.

- *La serie VM-series en una instancia de nivel 3 admite un máximo de 25 sistemas virtuales.*
- *VM-Series en una instancia de nivel 4 admite un máximo de 100 sistemas virtuales.*

Para obtener información sobre el número máximo para un objeto o recurso en particular que una sola implementación de cortafuegos VM-Series puede crear, almacenar, gestionar o interactuar en base a una memoria o un nivel asignado, consulte Límites máximos en base a un nivel y una memoria.

PAN-OS 11.1.3 y versiones posteriores Requisitos previos

Asegúrese de instalar la licencia del sistema virtual en el cortafuegos VM-Series para añadir varios sistemas virtuales en la interfaz web del cortafuegos o en la consola de Panorama.

©2024 Palo Alto Networks, Inc.

Requisitos del sistema para la compatibilidad con sistemas virtuales en VM-Series

PAN-OS 11.1.3 y versiones posteriores Requisitos del sistema

La compatibilidad del sistema virtual con el cortafuegos VM-Series solo está disponible en la plataforma **KVM**.

Los siguientes son los requisitos del sistema para asignar los recursos de hardware mínimos para aprovechar la compatibilidad del sistema virtual con el cortafuegos VM-Series:

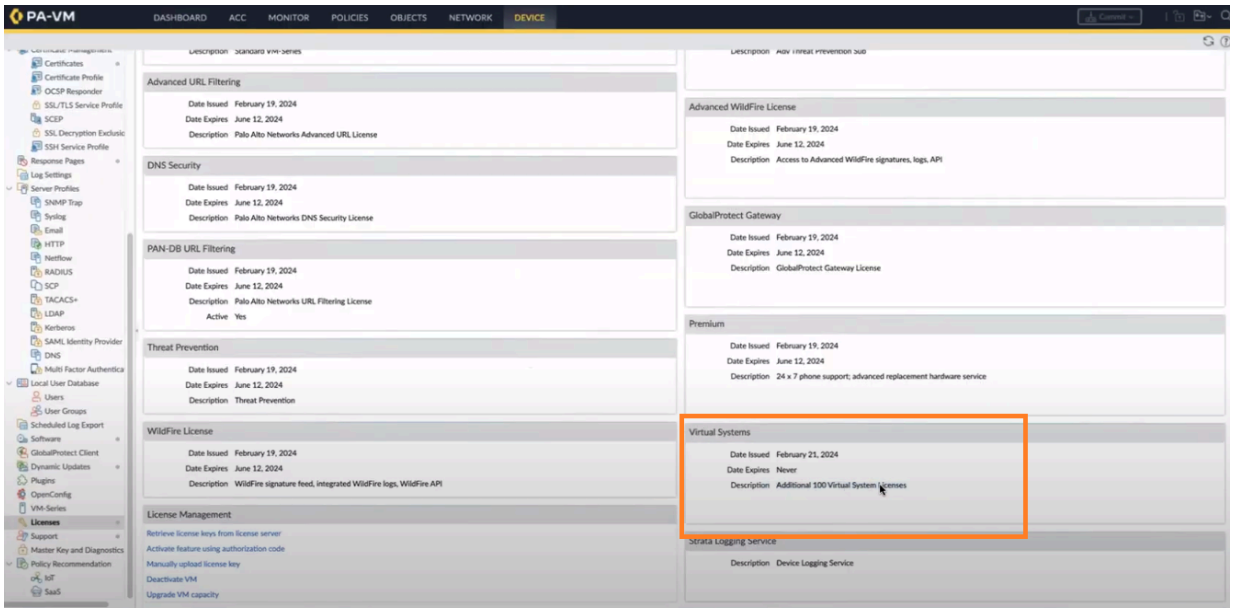
PAN-OS	Plataformas compatibles	VCPU compatibles	Memoria mínima y disco duro
11.1.3 y superior	KVM	Para obtener más información sobre las VCPU compatibles según el modelo del VM-Series, consulte Requisitos del sistema de VM-Series. *Utilice una licencia de cortafuegos flexible VM-Series e instancias de nivel 3 o 4 que admitan un mínimo de 16 vCPU o más.*	Para obtener más información sobre los requisitos mínimos de memoria y disco duro según el modelo VM-Series, consulte Requisitos del sistema de VM-Series.

©2024 Palo Alto Networks, Inc.

Habilitar el soporte de múltiples sistemas virtuales en el cortafuegos VM-Series

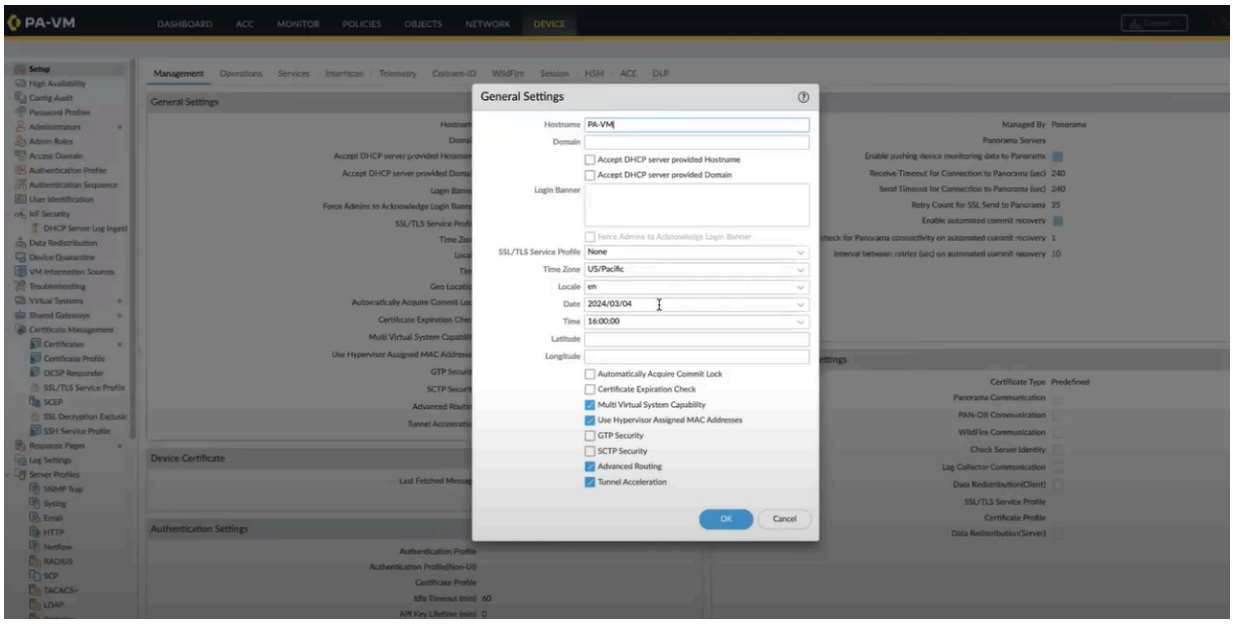
PAN-OS 11.1.3 y versiones posteriores Después de instalar la licencia de sistema virtual en su cortafuegos, realice los siguientes pasos para habilitar la compatibilidad con varios sistemas virtuales en VM-Series:

1. Inicie sesión en la interfaz web del cortafuegos y navegue hasta **Dispositivo** > **Licencias**.



 ©2024 Palo Alto Networks, Inc.

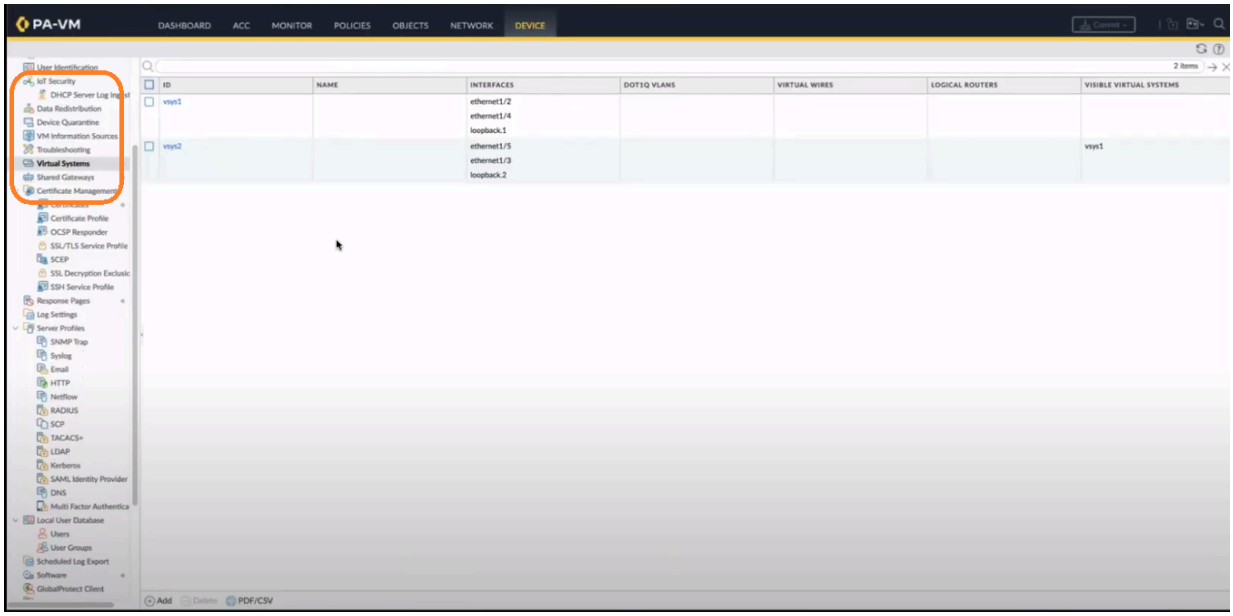
2. Vaya a **Configuración general** y, a continuación, active la casilla de verificación de **Capacidad multisistema virtual**.



3. Haga clic en **OK (Aceptar)**.

 ©2024 Palo Alto Networks, Inc.

4. Ahora puede ver la opción **Sistemas virtuales** en el panel izquierdo.



5. Haga clic en **Añadir** para crear varios sistemas virtuales según el número de vsys que tenga en su licencia de sistemas virtuales.

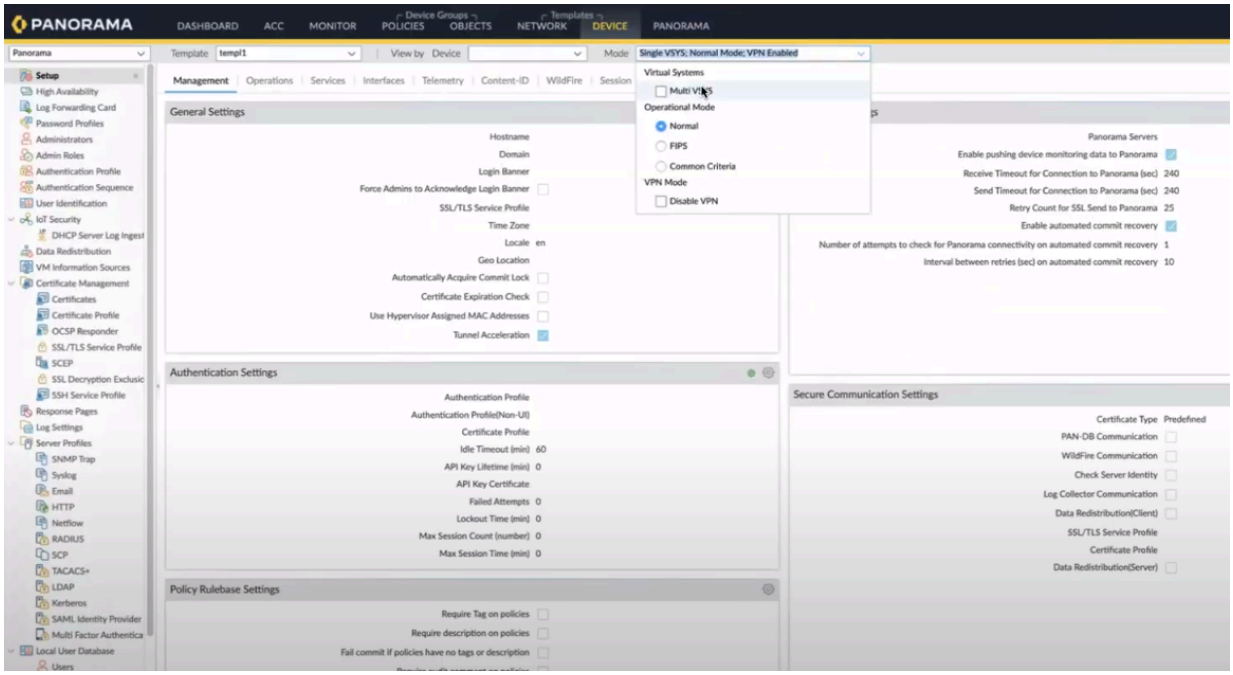
   Para actualizar el número de vsys en su licencia de sistemas virtuales, debe Editar el perfil de implementación y cambiar el número de licencias vsys y, a continuación, actualizar el perfil de implementación

 ©2024 Palo Alto Networks, Inc.

Habilitar el soporte de múltiples sistemas virtuales en VM-Series en la consola de Panorama

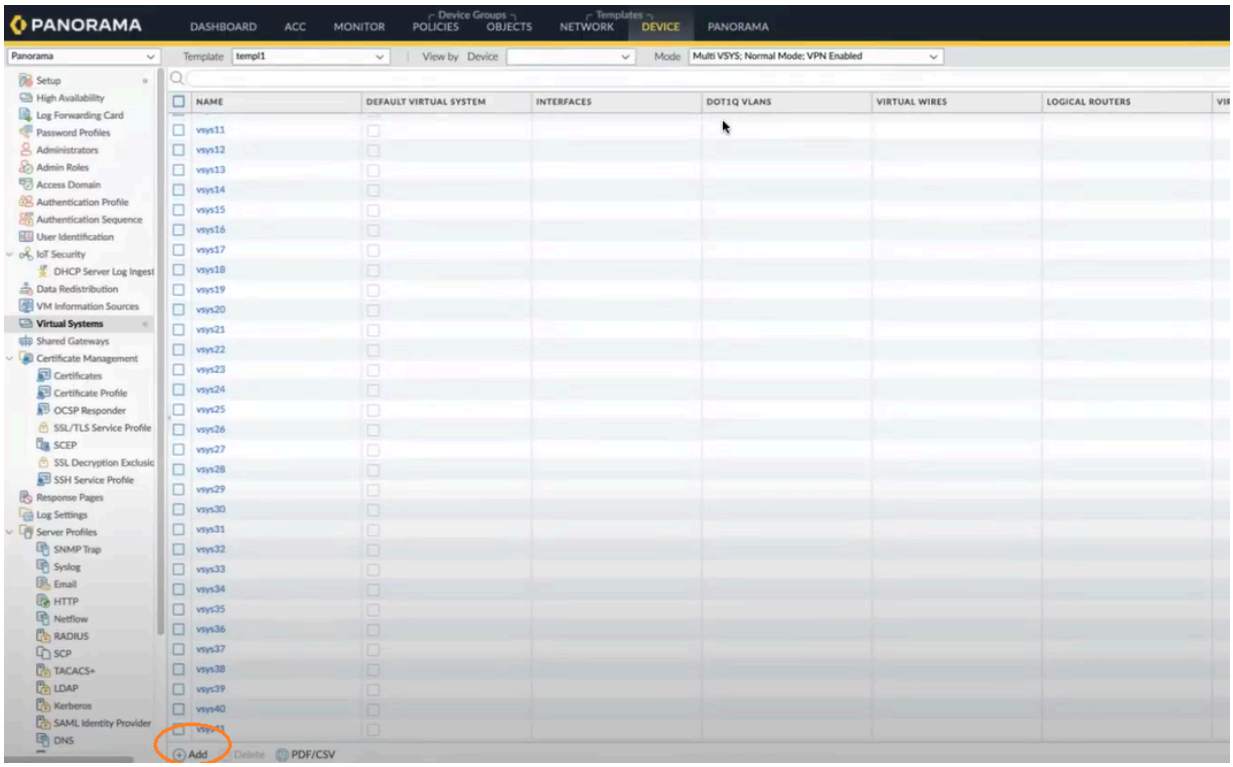
PAN-OS 11.1.3 y versiones posteriores Después de habilitar la compatibilidad con varios sistemas virtuales en el cortafuegos VM-Series, realice los siguientes pasos para configurar varios sistemas virtuales mediante la consola de Panorama.

1. Inicie sesión en Panorama.
2. Vaya a **Dispositivo** y seleccione la casilla **Multi Vsys**.



 ©2024 Palo Alto Networks, Inc.

3. Vaya a **Sistemas virtuales** y, a continuación, haga clic en **Añadir** para configurar sistemas virtuales en su cortafuegos.



4. Configure Sistemas virtuales en su cortafuegos VM-Series.
5. Seleccione **Commit (Enviar) > Push to Devices (Enviar a dispositivos)** y envíe toda la configuración gestionada de Panorama a cada vsys del cortafuegos multivsys.

 ©2024 Palo Alto Networks, Inc.

Habilitación de la compatibilidad con varios sistemas virtuales mediante el método de arranque

PAN-OS 11.1.3 y versiones posteriores Puede habilitar la compatibilidad con varios sistemas virtuales en el cortafuegos VM-Series mediante el método de arranque. Almacene los parámetros de configuración básicos como pares clave-valor en `config/init-cfg.txt` en el paquete de arranque.

Para obtener más información, consulte Arranque del cortafuegos VM-Series y Seleccione un método de arranque.

Para habilitar la compatibilidad con varios sistemas virtuales, debe configurar el siguiente parámetro como par clave-valor en el archivo `config/init-cfg.txt`.

```
op-command-modes=multi-vsys
```

Para obtener más información, consulte Crear el archivo init-cfg.txt y Componentes de archivo init-cfg.txt.

©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Licencia del cortafuegos VM-Series

El cortafuegos VM-Series soporta dos tipos de licencia (BYOL y PayGo) y dos modelos de licencia diferentes: créditos de cortafuegos de nueva generación de software (software NGFW) para configuraciones flexibles que especifique con un perfil de implementación, y configuraciones fijas del modelo VM-Series. Ambos modelos también ofrecen licencias de servicios de seguridad y otras características.

Si es un socio autorizado de CSSP, consulte Licencias para proveedores de servicios de seguridad en la nube (CSSP) para obtener información de su interés.

Consulte los siguientes temas para obtener detalles sobre cómo crear una cuenta de soporte y gestionar licencias:

- Licencias de cortafuegos VM-Series
- Creación de una cuenta de asistencia técnica
- Número de serie y formato de ID de CPU para el cortafuegos VM-Series
- Utilice la gestión de licencias de software de cortafuegos basado en Panorama
- Créditos NGFW de software
- Modelos VM-Series
- Licencias para proveedores de servicios de seguridad en la nube (CSSP)

Licencias de cortafuegos VM-Series

En este capítulo se compara la siguiente información de licencia:

- Tipos de licencia: BYOL frente a PayGo
- vCPU flexibles y licencias de modelos fijos: vCPU flexibles frente a modelos fijos)
- Implementación flexible de vCPU y modelos fijos: Resumen de los pasos de implementación para modelos flexibles y fijos.

Tipos de licencia

Las nuevas licencias de capacidad (créditos NGFW que no son de software) ya no están disponibles para la venta. Sin embargo, cuenta con renovaciones de un (1) año para licencias de capacidad (perpetuas y de tiempo limitado).

Palo Alto Networks actualmente admite dos tipos de licencia: Traiga su propia licencia (BYOL) y PAYG (Pay-As-You-Go, también llamado PayGo).

Tipo	Description (Descripción)
BYOL	Créditos NGFW de software:disponible en cortafuegos VM-Series que ejecutan todas las versiones de PAN-OS. Los cortafuegos VM-Series que ejecutan las versiones 10.0.4 y posteriores de PAN-OS ofrecen funciones avanzadas y mayor flexibilidad. El coste de licencia flexible se basa en el número de vCPU, los servicios de seguridad que ha habilitado y si elige aprovisionar Panorama para gestionar el cortafuegos o actuar como recopilador de logs. Consulte Créditos NGFW de software para obtener una explicación detallada.
BYOL	Licencias de modelo VM-Series: disponibles para su uso con todas las versiones de PAN-OS. El número de vCPU se fija de acuerdo con el modelo de VM-Series elegido. *Las vCPU flexibles, disponibles con PAN-OS 10.0.4 y versiones posteriores, admiten funciones avanzadas y más vCPU.* El coste de la licencia de capacidad se basa en el modelo VM-Series, la memoria del dispositivo, los costes de almacenamiento y el derecho a asistencia técnica. Los servicios de seguridad y una implementación de Panorama para administrar sus cortafuegos son costes adicionales. Los tipos de licencia de capacidad son: • **Acuerdo de licencia empresarial de VM-Series (ELA de múltiples modelos)**:un acuerdo de licencia integral de uno o tres años para cortafuegos VM-Series. Una licencia individual puede incluir un modelo, servicios de seguridad, un derecho de soporte y una licencia opcional de gestión de dispositivos para Panorama. La ELA multi modelo cuenta con un grupo de tokens desde el que se asignan tokens para dar autorización a cortafuegos VM-Series. (Es exclusivo de ELA y no es lo mismo que el grupo de créditos NGFW de software). • Licencia perpetua de capacidad del modelo VM-Series con derecho a asistencia técnica y/o paquete de servicios de seguridad 1 o paquete 2.

 ©2024 Palo Alto Networks, Inc.

Tipo	Description (Descripción)
	• Licencia de capacidad de cortafuegos a término con derecho de asistencia técnica y su elección de servicios de seguridad.
PayGo	Comprado en un mercado de nube pública (como AWS, Azure o GCP) o de un proveedor de servicios de seguridad en la nube (CSSP). Disponible en la versión de PAN-OS compatible con su proveedor. En las versiones de PAN-OS anteriores a la 9.1.1, PayGo solo admitía el modelo VM-300 de la serie VM-Series. Para PAN-OS 9.1.1 y posteriores, PayGo puede admitir modelos fijos. Los modelos de máquina virtual tradicionales, como VM-100, VM-300, VM-500 y VM-700 son compatibles.

vCPU flexibles y licencias de modelos fijos

¿Cuál es la diferencia entre las licencias NGFW de software flexibles de vCPU y las licencias de modelos VM-Series fijas de vCPUl? Cobran por cosas diferentes, y se financian de manera diferente. Las siguientes tablas proporcionan una comparativa rápida y vínculos a mayores detalles.

	vCPU flexibles	Modelo VM-Series (vCPU fijas)
Description (Descripción)	El coste se basa en el número de vCPU y los servicios de seguridad elegidos. No hay un coste para Panorama excepto por las vCPU que consume. Usted compra créditos NGFW de software reutilizables que expiran al final de un plazo predeterminado. Después de activar sus créditos, puede dividirlos en grupos de crédito. Para usar sus créditos, elija un perfil de crédito y cree uno o más perfiles de implementación. Elija su propia combinación de componentes de cortafuegos como plataforma: vCPU de VM-Series, servicios de seguridad, Panorama virtual para la gestión o Recopilación de logs dedicados y un derecho a asistencia técnica. Todos los cortafuegos implementados con un perfil tienen licencia con el mismo código de autenticación y se puede administrar desde el perfil de implementación.	El coste se basa en la licencia de capacidad del modelo VM-Series, la memoria del dispositivo y el almacenamiento. Panorama y los servicios de seguridad se compran por separado. • Acuerdo de licencia empresarial de VM-Series (ELA de múltiples modelos):un acuerdo de licencia integral de uno o tres años para cortafuegos VM-Series. La ELA multi modelo cuenta con un grupo de tokens desde el que se asignan tokens para dar autorización a cortafuegos VM-Series. • Licencia perpetua de capacidad del modelo VM-Series con derecho a asistencia técnica y/o paquete de servicios de seguridad 1 o paquete 2. • Licencia de capacidad de cortafuegos a término con derecho de asistencia técnica y su elección de servicios de seguridad.

 ©2024 Palo Alto Networks, Inc.

	vCPU flexibles	Modelo VM-Series (vCPU fijas)
Activación	Requiere un correo electrónico de activación. La activación y el registro se producen automáticamente.	Requiere un correo electrónico de activación y un paso de registro separado después de la activación.
Servicios de seguridad	Prevención de amenazas, seguridad DNS, GlobalProtect, WildFire, filtrado de URL, SD-WAN, DLP y otros servicios a medida que estén disponibles. Al crear el perfil de implementación, puede elegir cualquier combinación de servicios de seguridad. Puede añadir o quitar servicios de seguridad de su perfil en cualquier momento.	**Paquete 1**: Prevención de amenazas y derecho a asistencia técnica premium. **Paquete 2**: Prevención de amenazas, seguridad DNS, GlobalProtect, WildFire, filtrado de URL, SD-WAN, DLP y derecho de asistencia premium.
Versión de PAN-OS	Hasta 64 vCPU flexibles y opciones de servicio avanzadas para cortafuegos que ejecutan 10.0.4 y posteriores.	Puede implementar un modelo VM-Series (vCPU fijas) en cualquier versión de PAN-OS.
Financiación	Créditos reutilizables que le permiten consumir componentes de cortafuegos como plataforma. Después de comprar créditos, debe activarlos, asociándolos a una cuenta particular para su organización. Los créditos activados financian un grupo de créditos a partir del cual puede crear un perfil de implementación. Cuando se implementan cortafuegos, se consumen créditos. Cuando se desactivan los cortafuegos, los créditos se liberan y se devuelven a su grupo de créditos para su uso posterior.	• ELA de múltiples modelos: tokens. • Licencia perpetua de capacidad del modelo VM-Series con derecho a asistencia técnica y/o paquete de servicios de seguridad 1 o paquete 2. La configuración se determina en el momento de la compra. No puede cambiar la configuración a menos que compre una nueva licencia. • Licencia de capacidad de cortafuegos a término con derecho de asistencia técnica y su elección de servicios de seguridad.
Configuración de implementación	Flexible. Un perfil de implementación se puede cambiar en cualquier momento. Los cambios en el perfil se propagan a todos los cortafuegos que comparten el código de autenticación del perfil de implementación.	La capacidad del modelo VM-Series no cambia, pero si tiene un ELA, puede añadir servicios de seguridad. Las licencias perpetuas y temporales se configuran y pagan por adelantado y no cambian.
Implementación	Después de la activación del crédito, cree un perfil de implementación para un entorno o caso de uso específico (como "Proteger mi entorno de NSX") y configure las vCPU del cortafuegos, los servicios de seguridad y un Panorama	Aceptar la ELA de VM-Series. Implementación y configuración del cortafuegos VM-Series. Active la licencia de modelo y registre el cortafuegos.

 ©2024 Palo Alto Networks, Inc.

	vCPU flexibles	Modelo VM-Series (vCPU fijas)
	virtual opcional. Puede crear cualquier número de perfiles de implementación y personalizarlos en cualquier momento. Debe tener el rol de administrador de crédito del Portal de atención al cliente (solo se aplica a la administración de cuentas) para activar y gestionar los créditos NGFW de software.	
Panorama	Al crear un perfil de implementación, puede optar por añadir Panorama para la gestión o como recopilador de logs dedicado para cortafuegos que usan un perfil de implementación. Este Panorama puede gestionar cortafuegos implementados con el código de autenticación compartido del perfil de implementación.	Panorama es un gasto aparte. Se puede utilizar un Panorama físico o virtual para la gestión del cortafuegos o para la recopilación de logs.
Actualizar o cambiar a versión anterior	Si el cortafuegos VM-Series. o Panorama tiene una conexión a Internet, los cambios en el perfil de implementación se aplican automáticamente al cortafuegos. Si el cortafuegos no tiene conexión a Internet, deténgalo manualmente. En Assets (Activos) > Software NGFW Credits (Créditos NGFW de software) cambie el perfil de implementación, luego en el CSP, descargue las claves de licencia y transfiéralas a la VM, obtenga el perfil del CSP, transfiéralo a la VM, reinicie la VM y aplique la licencia. No tiene que reiniciar el cortafuegos en ninguno de los casos.	El cambio a un modelo diferente requiere un cambio de licencia y un reinicio.

Implementación flexible de vCPU y modelos fijos

Las siguientes listas de comprobación comparan los procesos de implementación de los créditos NGFW de software y los métodos de licencia de modelo VM-Series.

vCPU flexibles	vCPU fijas (modelo VM-Series)
1. Creación de una cuenta de asistencia técnica.	**1.** Creación de una cuenta de asistencia técnica.

©2024 Palo Alto Networks, Inc.

vCPU flexibles	vCPU fijas (modelo VM-Series)
2. Activación de créditos. Su organización puede tener muchas cuentas para representar diferentes centros de costes. Durante el registro, usted asocia su compra de créditos con una cuenta. 3. Crear un perfil de implementación. 4. Implemente el cortafuegos VM-Series en Alibaba, AWS, Azure, Cisco ACI, Cisco CSP, Cisco ENCS, ESXi, Google Cloud Platform, Hyper-V, KVM, OpenStack. Oracle Cloud Infrastructure, vCloud Air, NSX-T, o NSX-V. 5. Instalación de un certificado de dispositivo en el cortafuegos VM-Series (para licencias de sitio como Cortex Data Lake y Auto Focus).	2. Activar licencias del modelo VM-Series. 3. Registro del cortafuegos VM-Series. 4. Implemente el cortafuegos VM-Series en Alibaba, AWS, Azure, Cisco ACI, Cisco CSP, Cisco ENCS, ESXi, Google Cloud Platform, Hyper-V, KVM, OpenStack. Oracle Cloud Infrastructure, vCloud Air, NSX-T, o NSX-V. 5. Instalación de un certificado de dispositivo en el cortafuegos VM-Series (para licencias de sitio como Cortex Data Lake y Auto Focus).

©2024 Palo Alto Networks, Inc.

Creación de una cuenta de asistencia técnica

Necesita una cuenta de soporte para iniciar sesión en el Portal de atención al cliente (CSP). Debe iniciar sesión para activar y gestionar créditos NGFW de software, acceder a actualizaciones de software o abrir un caso con la asistencia técnica de Palo Alto Networks. Su cuenta de asistencia le permite ver y administrar todos los activos (dispositivos, licencias y suscripciones) que registró en Palo Alto Networks.

Para todas las opciones de licencias, excepto para las licencias basadas en uso que actualmente solo están disponibles en AWS, se requiere una cuenta de asistencia de modo que pueda descargar el paquete de software requerido para instalar el cortafuegos VM-Series.

Si tiene una cuenta de soporte existente, puede descargar e instalar el software de cortafuegos VM-Series y luego continuar con el Registro del cortafuegos VM-Series.

STEP 1 | Vaya a https://support.paloaltonetworks.com/UserAccount/PreRegister.

STEP 2 | Introduzca la dirección de correo electrónico corporativa para asociarla con la cuenta de asistencia.

STEP 3 | Seleccione una de las siguientes opciones y complete los detalles en el formulario de registro de usuarios:

Para una licencia basada en el uso en AWS

1. Haga clic en **Register your Amazon Web Services VM-Series Instance (Registrar su instancia VM-Series de Amazon Web Services)**.
2. En la Consola de administración de AWS, busque el ID de instancia de AWS, el código de producto de AWS y la Zona de AWS en la que usted implementó el cortafuegos.
3. Complete los demás detalles.

Para todas las demás licencias

1. Haga clic en **Register device using Serial Number or Authorization Code (Registrar el dispositivo mediante un número de serie o código de autorización)**.
2. Introduzca el código de autorización de la capacidad y el número del pedido de venta o el ID de cliente.
3. Complete los demás detalles.

STEP 4 | **Submit (Enviar)** el formulario. Recibirá un correo electrónico con un enlace para activar su cuenta de usuario.

Complete los pasos para activar la cuenta. Luego de verificar su cuenta y de completar el registro, puede iniciar sesión en el portal de asistencia.

 ©2024 Palo Alto Networks, Inc.

Número de serie y formato de ID de CPU para el cortafuegos VM-Series

Cuando inicia una instancia del cortafuegos VM-Series, cada instancia del cortafuegos se identifica de forma exclusiva con la ID de la CPU y el número de serie del cortafuegos. El formato de la ID de la CPU y el número de serie incluyen información sobre el hipervisor y el tipo de licencia para cada instancia del cortafuegos VM-Series.

- Con el modelo de licencias basado en el uso de los cortafuegos de vm-series, en el momento del lanzamiento, el cortafuegos genera un número de serie y un ID de CPU, y se utilizan estos detalles para Registro del modelo basado en el uso del cortafuegos VM-Series para nubes públicas (sin código de autenticación).
- Con el modelo BYOL, se registra un modelo fijo de cortafuegos VM-Series o un cortafuegos VM-Series con una licencia flexible en el portal de atención al cliente (CSP).
  - Para un cortafuegos con acceso directo a internet, puede aplicar el código de autenticación en el cortafuegos para generar un archivo de licencia que incluya el número de serie.
  - Para un cortafuegos que está fuera de línea, debe usar el CSP para introducir la ID de CPU, el UUID y el código de autenticación para generar un archivo de licencia que incluya el número de serie. A continuación, puede instalar la licencia en el cortafuegos.

Tipo de licencia	Número de serie	ID de CPU
BYOL	15 dígitos, todos numéricos Ejemplo: 0071 **51** 345678909	<Hypervisor>:<ActualCPUID> Ejemplo: **ESX**:12345678
PAYG	15 dígitos, alfanuméricos Ejemplo: **4** DE0YTAYOGMYYTN	<Hypervisor>:<Instance-ID>:<CloudProductCode>:<CloudRegion> Ejemplo: `AWSMP:1234567890abcdef0: 6kxdw3bbmdeda 3o6i1ggqt4km:us-west1`

©2024 Palo Alto Networks, Inc.

Utilice la gestión de licencias de software de cortafuegos basado en Panorama

El complemento de la licencia de cortafuegos de software de Panorama le permite licenciar automáticamente un cortafuegos VM-Series cuando se conecta a Panorama. Si los cortafuegos VM-Series se encuentran en el perímetro de su implementación y no tienen conectividad con el servidor de licencias de Palo Alto Networks, el complemento de la licencia de cortafuegos de software simplifica el proceso de activación de la licencia mediante Panorama para dar licencia el cortafuegos VM-Series.

Además, el complemento de la licencia de cortafuegos de software simplifica la activación y desactivación de licencias de cortafuegos VM-Series en entornos que utilizan el escalado automático y la automatización para implementar y eliminar cortafuegos según lo requieran los cambios en la nube.

Las licencias de pago por uso (PAYG, del inglés Pay-as-you-go) no son compatibles con este complemento.

No utilice el complemento de la licencia de cortafuegos de software para dar licenciar al cortafuegos VM-Series para VMware NSX. El complemento de Panorama para VMware NSX licencia automáticamente los cortafuegos VM-Series implementados en NSX y NSX-T

.

Además, no utilice este complemento para dar licencia a cortafuegos implementados en grupos de dispositivos que incluyan instancias del cortafuegos VM-Series implementado en NSX-T.

Para instalar el complemento de la licencia de cortafuegos de software de Panorama, debe utilizar Panorama 10.0.0 o posterior y el complemento VM-Series 2.0.4 o posterior. Los cortafuegos VM-Series deben ejecutar PAN-OS 9.1.0 o posterior.

El cortafuegos VM-Series para Azure requiere el complemento VM-Series 2.0.8 o posterior.

Si tiene un Panorama independiente o dos dispositivos Panorama instalados en un par de alta disponibilidad con varios complementos instalados, es posible que los complementos no reciban información actualizada sobre la etiqueta IP si uno o más de los complementos no están configurados. Esto ocurre porque Panorama no reenviará la información de la etiqueta IP a los complementos no configurados. Además, este problema puede ocurrir si uno o más de los complementos de Panorama no están en el estado Registrado o Correcto (el estado positivo varía según cada complemento). Asegúrese de que sus complementos estén en el estado positivo antes de continuar o ejecutar los comandos que se describen a continuación.

Si encuentra este problema, hay dos soluciones:

- Desinstale el complemento o complementos no configurados. Se recomienda que no instale un complemento que no planifique configurar de inmediato

 ©2024 Palo Alto Networks, Inc.

- Puede utilizar los siguientes comandos para solventar este problema. Ejecute el siguiente comando para cada complemento no configurado en cada instancia de Panorama, para evitar que Panorama espere para enviar actualizaciones. Si no lo hace, sus cortafuegos pueden perder cierta información de la etiqueta IP.

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

  Puede cancelar este comando ejecutando:

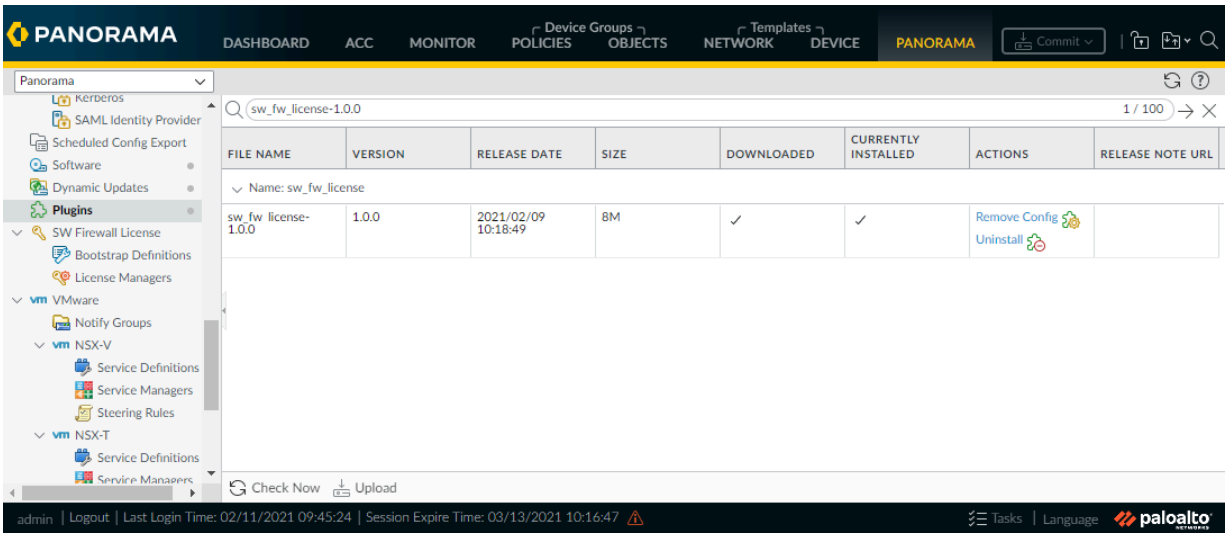
  `request plugins dau plugin-name <plugin-name> unblock-device-push no`

Los comandos descritos no son persistentes en los reinicios y deben usarse de nuevo para cualquier reinicio posterior. Para Panorama en el par de HA, los comandos deben ejecutarse en cada Panorama.

STEP 1 | Instale el complemento de la licencia de cortafuegos de software de Panorama.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Plugins (Complementos)**.
3. Haga clic en **Check Now (Comprobar ahora)** para obtener la lista de complementos disponibles.
4. Busque sw_fw_license para localizar el complemento.
5. Seleccione **Download (Descargar)** e **Install (Instalar)** para instalar el complemento de licencias de software.

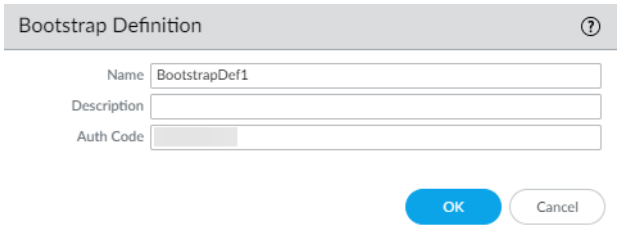
Después de realizar la instalación correctamente, Panorama se actualiza y el complemento de licencias de software se muestra en la pestaña **Panorama**.



 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configure una definición de arranque bootstrap.

1. Seleccione **Panorama** > **SW cortafuegos License (Licencia de cortafuegos de SW)** > **Bootstrap Definitions (Definiciones de arranque)**.
2. Haga clic en **Add (Añadir)**.
3. Introduzca un **Name (Nombre)** descriptivo para identificar la definición de bootstrap.
4. (Opcional) Introduzca una **Description (Descripción)** de la definición de Bootstrap.
5. Introduzca el **Auth Code (Código de autenticación)** que Panorama utilizará para dar una licencia al cortafuegos VM-Series cuando se conecte a Panorama.
6. Haga clic en **OK (Aceptar)**.



STEP 3 | Configurar un Gestor de licencias.

1. Seleccione **Panorama** > **SW cortafuegos License (Licencia de cortafuegos de SW)** > **License Managers (Administradores de licencias)**.
2. Haga clic en **Add (Añadir)**.
3. Introduzca un **Name (Nombre)** descriptivo para identificar el Gestor de licencias.
4. (Opcional) Introduzca una **Description (Descripción)** del Gestor de licencias.
5. Seleccione un **Device Group (Grupo de dispositivos)** del menú desplegable. Cuando un cortafuegos VM-Series arrancado mediante el administrador de licencias se conecta a Panorama, este se coloca en el grupo de dispositivos especificado.
6. Seleccione una **Template Stack (Pila de plantillas)** en el menú desplegable. Cuando un cortafuegos VM-Series arrancado mediante el administrador de licencias se conecta a Panorama, se coloca en la Pila de plantillas especificada.
7. En el campo **Auto Deactivate (Desactivación automática)**, especifique la cantidad de tiempo, en horas, que Panorama debe esperar antes de desactivar la licencia de un cortafuegos VM-Series desconectado. Si selecciona **Never (Nunca)**, Panorama no desactiva un cortafuegos VM-Series desconectado. La desactivación automática se establece en Nunca de forma predeterminada. Puede establecer el tiempo de desactivación, en horas, de una a 24.

   Antes de desactivar, configure la clave API mediante:

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

   Cuando se configura un intervalo de desactivación automática, el complemento también puede desactivar la licencia de los cortafuegos VM-Series detenidos, además de los cortafuegos desconectados.

STEP 4 | (Opcional) Cree un archivo `init-cfg.txt` para arrancar el cortafuegos VM-Series. Después de configurar un gestor de licencias, puede copiar y pegar los parámetros de arranque generados por Panorama al implementar los cortafuegos VM-Series. Dependiendo de la implementación, los parámetros mostrados pueden ser un subconjunto de los que se muestran en la imagen siguiente.

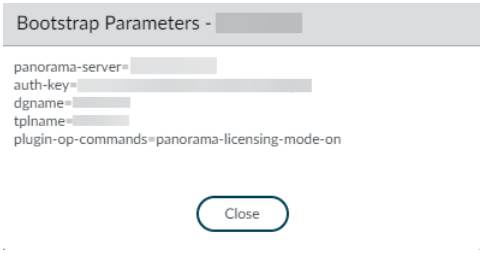
 ©2024 Palo Alto Networks, Inc.

Por ejemplo, si el dispositivo Panorama se implementa en una nube pública, los parámetros de arranque no incluirán la dirección IP pública de Panorama. En ese caso, debe ingresar manualmente la dirección IP pública en el archivo `init-cfg.txt`. Panorama siempre generará la clave de autenticación y **`plugin-op-commands=panorama-licensing-mode-on`** para su uso en su `init-cfg.txt`.

Panorama genera la clave de autenticación que se muestra aquí y la utiliza para autenticar la conexión del cortafuegos VM-Series a Panorama. Además, esta clave de autenticación se usa en lugar de la clave de autenticación de máquina virtual que usted puede generar en Panorama y añadir a su archivo init-cfg.txt.

Si usa la clave de autenticación que se muestra aquí en el archivo init-cfg.txt, no use una clave de autenticación de máquina virtual generada manualmente.

1. Seleccione **Panorama** > **SW cortafuegos License (Licencia de cortafuegos de SW)** > **License Managers (Administradores de licencias)**.
2. En la columna Acción de un gestor de licencias determinado, haga clic en **Show Bootstrap Parameters (Mostrar parámetros de bootstrap)**.
3. Copie la información mostrada y péguela en un editor de texto para crear un archivo `init-cfg.txt` para el arranque.
4. Haga clic en **Close (Cerrar)** cuando haya terminado.

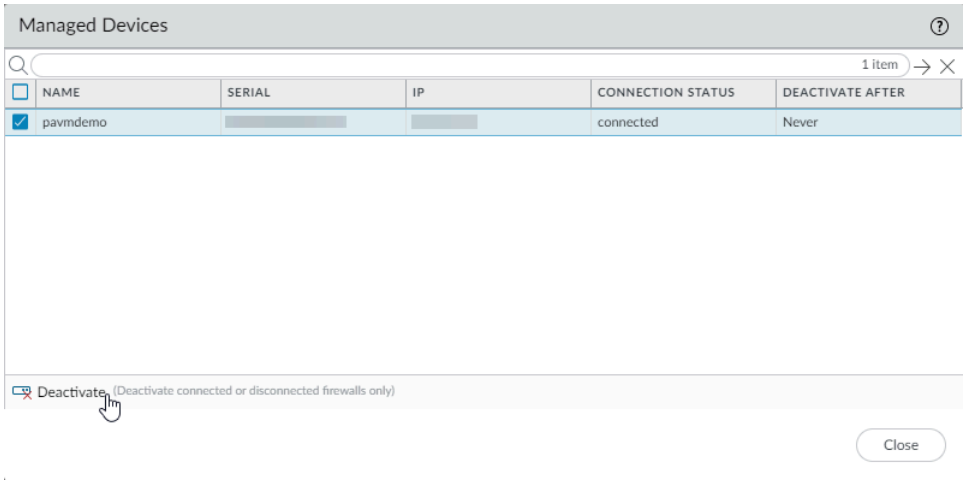


STEP 5 | (Opcional) Vea y desactive un cortafuegos VM-Series gestionado. En el diálogo **Show Devices (Mostrar dispositivos)**, puede ver los dispositivos asociados a un gestor de licencias determinado. Puede ver el nombre, el número de serie, la dirección IP de administración, el estado de la conexión y la cantidad de tiempo que Panorama debe esperar para desactivar un cortafuegos desconectado. Además, puede desactivar manualmente la licencia del cortafuegos gestionado VM-Series.

1. Seleccione **Panorama** > **SW cortafuegos License (Licencia de cortafuegos de SW)** > **License Managers (Administradores de licencias)**.
2. En la columna Acción de un gestor de licencias determinado, haga clic en **Show Devices (Mostrar dispositivos)**.

 ©2024 Palo Alto Networks, Inc.

3. Para desactivar manualmente un cortafuegos de VM-Series gestionado conectado o desconectado (pero aún no activado), seleccione uno o más cortafuegos VM-Series de la lista y haga clic en **Deactivate (Desactivar)**.



STEP 6 | (Opcional) Compruebe que Panorama haya completado las llamadas a la API necesarias para licenciar los cortafuegos conectados.

1. Inicie sesión en la interfaz de línea de comandos de Panorama.
2. Ejecute el siguiente comando.

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

 ©2024 Palo Alto Networks, Inc.

Créditos NGFW de software

Los créditos NGFW de software se pueden utilizar para financiar NGFW de software (VM-Series y CN-Series), servicios de seguridad entregados en la nube (CDSS) o dispositivos Panorama virtuales en redes con o sin acceso a Internet (redes con muros de aire, por ejemplo).

Cree un perfil de implementación para configurar uno o más cortafuegos en función de la versión de PAN-OS, el número de vCPU por cortafuegos, el número total de cortafuegos admitidos por el perfil de implementación, la administración de Panorama o la recopilación de logs y los servicios de seguridad. Todas las máquinas virtuales creadas con un perfil de implementación comparten el mismo código de autenticación.

- vCPU fijas: compatible con todas las versiones de PAN-OS. Basado en Modelos VM-Series y paquetes de servicios de seguridad. Cambiar el modelo o las opciones de servicio requiere una nueva licencia.
- vCPU flexibles: seleccione un número flexible de vCPU y una selección flexible de servicios de seguridad Puede modificar el perfil de implementación para añadir o disminuir el número de vCPU, añadir nuevos servicios a medida que estén disponibles o quitar servicios. El número máximo de vCPU para un perfil de implementación es 64.

Los créditos NGFW de software se basan en términos. Los términos se pueden definir por cualquier cantidad de tiempo entre 1 y 5 años. Tanto los créditos asignados como los no asignados expiran al final del plazo acordado. Puede comprar créditos adicionales para un grupo de créditos, pero la fecha de vencimiento debe ser la misma que la del grupo de destino. Utilice el Software NGFW Credit Estimator para calcular y obtener créditos para su perfil de implementación.

Si tiene una conexión al servidor de licencias y deja de usar un cortafuegos, un servicio de seguridad o una implementación de Panorama, los créditos asignados a ese recurso se devuelven al grupo de créditos y se pueden reasignar a un nuevo recurso.

Si no tiene conexión a Internet y no puede conectarse al servidor de actualización de Palo Alto Networks (por ejemplo, se encuentra en una red con muros de aire), puede gestionar el cortafuegos VM-Series localmente desde su interfaz de usuario o desde Panorama. A continuación, el administrador debe iniciar sesión en el Portal de atención al cliente para devolver el token de licencia y poder reutilizar los fondos.

Utilice la tabla **Hipervisor compatible** a continuación y las tablas **Total de vCPU en el plano de datos** que siguen para asegurarse de que asigna los recursos de hardware necesarios para el número elegido de vCPU.

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

©2024 Palo Alto Networks, Inc.

Perfil de memoria	Hipervisores compatibles	Disco duro mínimo
Nivel 1 (4,5 GB, 5 GB, 5,5 GB, 6 GB de memoria)	ESXi, Hyper-V, KVM	• Con 4,5 GB de memoria: 32 GB (60 GB en el arranque) • 60GB
Nivel 1	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, Cisco ENCS, NSX-T	60GB
Nivel 2	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, Cisco ENCS, NSX-T	60GB
Nivel 3	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, NSX-T	60GB
Nivel 4	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, NSX-T	60GB

Para todos los perfiles de memoria enumerados anteriormente, las vCPU mínimas son 2.

Nivel 1 requiere un mínimo de 32 GB de espacio en el disco duro. Sin embargo, dado que la imagen base de VM-Series es común para todas las combinaciones de vCPU, debe asignar 60 GB de espacio en el disco duro hasta que tenga la licencia de un cortafuegos VM-Series con 4,5 GB de memoria.

Para obtener el mejor rendimiento, todos los núcleos requeridos deben estar disponibles en un solo socket de CPU.

De forma predeterminada, las vCPU de plano de gestión y de plano de datos se asignan en una relación de uno a tres, a menos que asigne cuatro o menos vCPU. Además, las vCPU del plano de datos máximos están vinculadas a la memoria asignada, como se describe en las tablas a continuación. Por ejemplo, si asigna 16 vCPU a un cortafuegos VM-Series, se asignan cuatro vCPU al plano de gestión y 12 al plano de datos. Si tiene 20 vCPU y 20 GB de memoria en un cortafuegos VM-Series, se asignan 12 vCPU al plano de datos y el resto se asigna al plano de gestión.

Como alternativa, puede utilizar la CLI del cortafuegos VM-Series para Personalizar núcleos de plano de datos. Esto le permite especificar el número de vCPU asignadas al plano de datos en el cortafuegos VM-Series.

El número máximo de núcleos totales (plano de gestión y plano de datos) es 64, independientemente del perfil de memoria.

 ©2024 Palo Alto Networks, Inc.

Nivel 1	4,5 GB	5 GB	5,5 GB	6 GB	6,5 GB	7 GB	8 GB
vCPU de plano de datos predeterminado	1	1	1	1	2	2	2
vCPU del plano de gestión predeterminado	1	1	1	1	2	2	2

Nivel 2	9 GB	10 GB	12 GB	14 GB	16 GB	18 GB	20 GB
vCPU de plano de datos predeterminado	4	4	4	4	12	12	12
vCPU del plano de gestión predeterminado	2	2	2	2	4	4	4

Nivel 3	20 GB	24 GB	28 GB	32 GB	36 GB	40 GB	44 GB	48 GB	52 GB	56 GB	64 GB
vCPU de plano de datos predeterminado	12	12	12	12	12	12	12	12	12	24	47
vCPU del plano de gestión predeterminado	4	4	4	4	4	4	4	4	4	8	17

Nivel 4	121 - 128 GB
vCPU de plano de datos predeterminado	47
vCPU del plano de gestión predeterminado	17

Continúe con las tareas NGFW de software:

- #unique_75
- Activación de créditos
- Crear un perfil de implementación
- Gestionar un perfil de implementación
- Registrar el cortafuegos VM-Series (Créditos NGFW de software)
- Aprovisionar Panorama

©2024 Palo Alto Networks, Inc.

- Migrar Panorama a una licencia NGFW de software
- Transferir créditos
- Renueve su licencia de créditos Software NGFW
- Desactivar licencia (créditos NGFW de software)
- Retirada de licencias de cortafuegos terminados incorrectamente
- Establecer el número de las vCPU licenciadas
- Personalizar núcleos de plano de datos
- Migración de un cortafuegos a una licencia VM-Series flexible
- API de licencias Software NGFW

Límites máximos basados en la memoria

¿Dónde puedo usar esto?	¿Qué necesito?
• Cortafuegos VM-Series	☐ Cortafuegos VM-Series financiado por Créditos NGFW de software

Las siguientes tablas proporcionan el número máximo para un objeto o recurso en particular que una sola implementación de cortafuegos VM-Series puede crear, almacenar, gestionar o interactuar en base a una memoria o un nivel asignado. Estos límites se aplican a los cortafuegos VM-Series que usan licencias financiadas con créditos NGFW de software.

Para el escalado de la memoria, los incrementos de memoria se agrupan en cuatro niveles que representan la capacidad de configuración del cortafuegos VM-Series. Independientemente de la cantidad de memoria que asigne a una instancia del cortafuegos VM-Series, el nivel en el que se encuentra la cantidad de memoria determina el límite para los valores que no son de sesión, como reglas de seguridad, objetos de dirección, perfiles de seguridad, etc.

El perfil de memoria y la cantidad total de vCPU determinan cuántos núcleos se asignan automáticamente al plano de gestión y al plano de datos. Además, tiene la opción de personalizar la distribución de los núcleos del plano de datos.

Si está utilizando la licencia de software NGFW, puede seleccionar un perfil de memoria que sea compatible con sus requisitos para uno o más de los siguientes recursos:

- 11.2 y posteriores
- 11.1

11.2 y posteriores

Sesiones

Nivel 1	4,5 GB	5 GB	5,5 GB	6 GB	6,5 GB	7 GB	8 GB
Núm. máx. de sesiones (IPv4 o IPv6)	20.000	40.000	50.000	100 000	200.000	250.000	300.000

©2024 Palo Alto Networks, Inc.

Nivel 1	4,5 GB	5 GB	5,5 GB	6 GB	6,5 GB	7 GB	8 GB
Máximo de vCPU del plano de datos predeterminado	1	1	1	1	2	2	2

Nivel 2	9 GB	10 GB	12 GB	14 GB	16 GB	18 GB	20 GB
Núm. máx. de sesiones (IPv4 o IPv6)	400.000	500.000	800.000	1.100.000	1.100.000	1.200.000	1.800.000
Máximo de vCPU del plano de datos predeterminado	4	4	4	4	12	12	12

Nivel 3	24 GB	28 GB	32 GB	36 GB	40 GB	44 GB
Núm. máx. de sesiones (IPv4 o IPv6)	2.500.000	2.800.000	3.500.000	4.500.000	5.500.000	6.750.000
Máximo de vCPU del plano de datos predeterminado	12	12	12	12	12	12

Nivel 3 (continuación)	48 GB	52 GB	56 GB	64 GB
Núm. máx. de sesiones (IPv4 o IPv6)	7.000.000	8.150.000	8.500.000	8.250.000
Máximo de vCPU del plano de datos predeterminado	12	12	24	47

Nivel 4	121 - 128 GB
Núm. máx. de sesiones (IPv4 o IPv6)	10.000.000
Máximo de vCPU del plano de datos predeterminado	47

©2024 Palo Alto Networks, Inc.

Políticas

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Reglas de seguridad	1.500	10.000	20.000	65.000
Horarios de reglas de seguridad	256	256	256	256
Reglas NAT	3.000	8.000	15 000	16.000
Reglas de descifrado	1.000	1.000	2.000	5000
Reglas de anulación de aplicaciones	1.000	1.000	2.000	4.000
Reglas de inspección del contenido del túnel	100	500	2.000	8.500
Reglas SD-WAN	100	300	300	1.000
Reglas de reenvío basado en políticas	100	500	2.000	2.000
Reglas del portal cautivo	1.000	1.000	2.000	8.000
Reglas de protección contra ataques por denegación de servicio	1.000	1.000	1.000	2.000

Zonas de seguridad

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Núm. máx. de zonas de seguridad	40	200	200	17.000

Objetos (direcciones y servicios)

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Objetos de dirección	10.000	20.000	40.000	160.000
Grupos de direcciones	1.000	2.500	4.000	80.000
Miembros por grupo de direcciones	2.500	2.500	2.500	2.500
Objetos de servicio	2.000	2.000	5000	12.000
Grupos de servicios	500	250	500	6.000
Miembros por grupo de servicio	500	500	500	2.500

©2024 Palo Alto Networks, Inc.

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Objetos de dirección FQDN	2.000	2.000	2.000	6.144
N.º máx. de direcciones IP de DAG* (capacidad de todo el sistema)	2.500	300.000	300.500	500.000
Etiquetas por dirección IP	32	32	32	64

*Rendimiento del cortafuegos medido con las funciones App-ID y User-ID habilitadas utilizando transacciones AppMix.

Perfiles de seguridad

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Perfiles de seguridad	375	750	750	750

App-ID

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Firmas de App-ID personalizadas	6.000	6.000	6.000	6.000
App-ID personalizados compartidos	512	512	512	512
App-ID personalizados (específico del sistema virtual)	6.416	6.416	6.416	6.416

User-ID

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Asignaciones de IP-User (plano de administración)	524.288	524.288	524.288	524.288
Asignaciones de IP-User (plano de datos)	64.000	512.000	512.000	512.000
Grupos activos y únicos utilizados en la política (conjunto de grupos LDAP, grupos de API XML y grupo de usuarios dinámicos).*	1.000	10.000	10.000	10.000
Número de agentes de User-ID	100	100	100	100
Servidores supervisados para User-ID	100	100	100	100

©2024 Palo Alto Networks, Inc.

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Agentes de Terminal Server	400	2.000	2.500	2.500
Etiquetas por usuario* (PAN-OS 9.1 y posterior)	32	32	32	32

*Rendimiento del cortafuegos medido con las funciones App-ID y User-ID habilitadas utilizando transacciones AppMix.

Descifrado SSL

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Máximo de certificados de entrada SSL	1.000	1.000	1.000	4.000
Caché de certificado SSL (Proxy de reenvío)	128	4.000	8.000	32.000
Núm. más. de sesiones de descifrado simultáneas	6.400	50.000	100 000	2.000.000
Espejo de puerto SSL	Sí	Sí	Sí	Sí
Intermediario de descifrado SSL	No	No	Sí	Sí
Compatible con HSM	Sí	Sí	Sí	Sí

URL Filtering

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Núm. total de entradas para la lista de permitidos, la lista de bloqueo y las categorías personalizadas	25.000	25.000	100 000	100 000
Núm. máx. de categorías personalizadas	2.849	2.849	2.849	2.849
Núm. máx. de categorías personalizadas (específicas del sistema virtual)	500	500	500	500
Tamaño de la caché del plano de datos para el filtrado de URL	90.000	90.000	250.000	250.000
Tamaño de la caché dinámica del plano de gestión	100 000	100 000	600.000	900.000

©2024 Palo Alto Networks, Inc.

EDL

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número máximo de listas personalizadas	30	30	30	30
Número máximo de direcciones IP por sistema	50.000	50.000	50.000	150.000
Número máximo de dominios DNS por sistema	50.000	2.000.000	2.000,00	4 000 000
Número máximo de URL por sistema	50.000	100 000	100 000	250.000
Intervalo de comprobación más corto (minutos)	5	5	5	5

Interfaces

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Gestión: fuera de banda	N/A	N/A	N/A	N/A
Gestión: alta disponibilidad 10/100/1000	N/A	N/A	N/A	N/A
Gestión: alta disponibilidad de 40 Gbps	N/A	N/A	N/A	N/A
Gestión: alta disponibilidad de 10 Gbps	N/A	N/A	N/A	N/A
Tráfico - 10/100/1000	N/A	N/A	N/A	N/A
Tráfico - 100/1000/10000	N/A	N/A	N/A	N/A
Tráfico: SFP de 1 Gbps	N/A	N/A	N/A	N/A
Tráfico: 10 Gbps SFP+	N/A	N/A	N/A	N/A
Tráfico: 40 / 100Gbps QSFP+ / QSFP28	N/A	N/A	N/A	N/A
Etiquetas 802.1q por dispositivo	4.094	4.094	4.094	4.094
Etiquetas 802.1q por interfaz física	4.094	4.094	4.094	4.094
Núm. máximo de interfaces (lógicas y físicas)	2.048	4.096	4.096	4.096
Núm. máximo de interfaces agregadas	N/A	N/A	N/A	N/A

©2024 Palo Alto Networks, Inc.

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número máximo de interfaces virtuales SD-WAN	300	1.000	1.000	1.000

Enrutadores virtuales

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Enrutadores virtuales	3	20	125	225

Cables virtuales

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Cables virtuales	12	12	12	12

Virtual Systems

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Sistemas virtuales base	1	1	1	1
Número máximo de sistemas virtuales Se requieren licencias adicionales para las capacidades del sistema virtual por encima de la capacidad del sistema virtual base	N/A	N/A	N/A	N/A

Enrutamiento

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Tamaño de la tabla de reenvío de IPv4* (Entradas compartidas entre enrutadores virtuales)	5000	32.000	100 000	Para añadir
Tamaño de la tabla de reenvío de IPv6* (Entradas compartidas entre enrutadores virtuales)	5000	32.000	100 000	Para añadir
Tamaño de la tabla de reenvío total del sistema	5000	32.000	100 000	Para añadir

©2024 Palo Alto Networks, Inc.

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número máximo de mapas de ruta por enrutador virtual	50	50	50	Para añadir
Número máx. de pares de enrutamiento (dependiente del protocolo)	500	1.000	1.000	Para añadir
Entradas estáticas: Proxy DNS	1.024	1.024	1.024	Para añadir
Sesiones de detección de reenvío bidireccional (BFD)	128	1.024	1.024	Para añadir

*Rendimiento del cortafuegos medido con las funciones App-ID y User-ID habilitadas utilizando transacciones AppMix.

Reenvío de L2

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Tamaño de la tabla ARP por dispositivo	2.500	32.000	128.000	132.000
Tamaño de la tabla de vecinos de IPv6	2.500	32.000	128.000	132.000
Tamaño de la tabla de MAC por dispositivo	2.500	32.000	128.000	132.000
Número máx. de entradas ARP por dominio de difusión	2.500	32.000	128.000	132.000
Número máx. de entradas MAC por dominio de difusión	2.500	32.000	128.000	132.000

NAT

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Capacidad total de la regla NAT	3.000	8.000	8.000	Para añadir
Número máx. de reglas NAT (estáticas)* (La configuración de las reglas NAT estáticas a plena capacidad requiere que no se utilicen otros tipos de reglas NAT).	3.000	8.000	8.000	Para añadir
Número máx. de reglas NAT (DIP)* (La configuración de las reglas NAT DIP a plena capacidad requiere que no se utilicen otros tipos de reglas NAT).	2.000	8.000	8.000	Para añadir

©2024 Palo Alto Networks, Inc.

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número máx. de reglas NAT (DIPP)	400	2.000	2.000	Para añadir
Número máx. de IP traducidas (DIP)	128.000	160.000	160.000	Para añadir
Número máx. de IP traducidas (DIPP)* (La capacidad de IP traducida de DIPP es proporcional al valor de sobresuscripción del grupo de DIPP. La capacidad que se muestra aquí se basa en un valor de sobresuscripción de 1x).	400	2.000	2.000	Para añadir
Sobresuscripción predeterminada del grupo DIPP* (Reutilización de IP de origen y puerto de origen en sesiones simultáneas)	2	8	8	Para añadir

*Rendimiento del cortafuegos medido con las funciones App-ID y User-ID habilitadas utilizando transacciones AppMix.

Asignación de dirección

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Servidores DHCP	3	20	125	Para añadir
Agentes de retransmisión de DHCP* (La capacidad máxima representa el total de servidores DHCP y agentes de retransmisión DHCP combinados)	500	500	500	Para añadir
Número máximo de direcciones asignadas	64.000	64.000	64.000	Para añadir

*Rendimiento del cortafuegos medido con las funciones App-ID y User-ID habilitadas utilizando transacciones AppMix.

High Availability

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Dispositivos compatibles	2	2	2	2
Número máx. de direcciones virtuales	128	32	128	Para añadir

©2024 Palo Alto Networks, Inc.

QoS

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número de políticas de QoS	500	2.000	4.000	Para añadir
Interfaces físicas compatibles con QoS	6	12	12	12
Nodos de texto no cifrado por interfaz física	31	63	63	63
Marcado DSCP por política	Sí	Sí	Sí	Sí
Subinterfaces compatibles	N/A	N/A	N/A	N/A

IPSec VPN

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número máx. de pares de IKE	1.000	1.000	2.000	Para añadir
Sitio a sitio (con ID de proxy)	1.000	4.000	8.000	Para añadir
Túneles SD-WAN IPSec	1.000	1.000	2.000	Para añadir

VPN de cliente de GlobalProtect

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Núm. máx. de túneles (SSL, IPSec e IKE con XAUTH)	500	6.000	12.000	Para añadir

VPN sin cliente de GlobalProtect

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número máx. de túneles SSL	100	1.200	2.500	25.000

©2024 Palo Alto Networks, Inc.

Multidifusión

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Replicación (interfaces de salida)	100	100	100	Para añadir
Rutas	2.000	4.000	4.000	Para añadir

11.1

Sesiones

Nivel 1	4,5 GB	5 GB	5,5 GB	6 GB	6,5 GB	7 GB	8 GB
Núm. máx. de sesiones (IPv4 o IPv6)	20.000	40.000	50.000	100 000	200.000	300.000	500.000
Máximo de vCPU del plano de datos predeterminado	1	1	1	1	2	2	2

Nivel 2	9 GB	10 GB	12 GB	14 GB	16 GB	18 GB	20 GB
Núm. máx. de sesiones (IPv4 o IPv6)	600.000	800.000	1 000 000	1.200.000 1.100.000 (con complemento VM-Series 5.0.1 y posterior)	1.800.000 1.100.000 (con complemento VM-Series 5.0.1 y posterior)	2.000.000 1.200.000 (con complemento VM-Series 5.0.1 y posterior)	2.800.000 1.800.000 (con complemento VM-Series 5.0.1 y posterior)
Máximo de vCPU del plano de datos predeterminado	4	4	4	4	12	12	12

Nivel 3	24 GB	28 GB	32 GB	36 GB	40 GB	44 GB
Núm. máx. de sesiones (IPv4 o IPv6)	3.600.000	4.400.000	5.200.000	6.000.000	6.800.000	6.800.000

©2024 Palo Alto Networks, Inc.

Nivel 3	24 GB	28 GB	32 GB	36 GB	40 GB	44 GB
Máximo de vCPU del plano de datos predeterminado	12	12	12	12	12	12

Nivel 3 (continuación)	48 GB	52 GB	56 GB	64 GB
Núm. máx. de sesiones (IPv4 o IPv6)	7.600.000	8.400.000	9.200.000	10.000.000
Máximo de vCPU del plano de datos predeterminado	12	12	24	47

Nivel 4	121 - 128 GB
Núm. máx. de sesiones (IPv4 o IPv6)	14.000.000
Máximo de vCPU del plano de datos predeterminado	47

Políticas

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Reglas de seguridad	1.500	10.000	20.000	65.000
Horarios de reglas de seguridad	256	256	256	256
Reglas NAT	3.000	8.000	15 000	16.000
Reglas de descifrado	1.000	1.000	2.000	5000
Reglas de anulación de aplicaciones	1.000	1.000	2.000	4.000
Reglas de inspección del contenido del túnel	100	500	2.000	8.500
Reglas SD-WAN	100	300	300	1.000
Reglas de reenvío basado en políticas	100	500	2.000	2.000
Reglas del portal cautivo	1.000	1.000	2.000	8.000
Reglas de protección contra ataques por denegación de servicio	1.000	1.000	1.000	2.000

©2024 Palo Alto Networks, Inc.

Zonas de seguridad

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Núm. máx. de zonas de seguridad	40	200	200	17.000

Objetos (direcciones y servicios)

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Objetos de dirección	10.000	20.000	40.000	160.000
Grupos de direcciones	1.000	2.500	4.000	80.000
Miembros por grupo de direcciones	2.500	2.500	2.500	2.500
Objetos de servicio	2.000	2.000	5000	12.000
Grupos de servicios	500	250	500	6.000
Miembros por grupo de servicio	500	500	500	2.500
Objetos de dirección FQDN	2.000	2.000	2.000	6.144
N.º máx. de direcciones IP de DAG* (capacidad de todo el sistema)	2.500	300.000	300.500	500.000
Etiquetas por dirección IP	32	32	32	64

*Rendimiento del cortafuegos medido con las funciones App-ID y User-ID habilitadas utilizando transacciones AppMix.

Perfiles de seguridad

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Perfiles de seguridad	375	750	750	750

App-ID

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Firmas de App-ID personalizadas	6.000	6.000	6.000	6.000
App-ID personalizados compartidos	512	512	512	512

©2024 Palo Alto Networks, Inc.

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
App-ID personalizados (específico del sistema virtual)	6.416	6.416	6.416	6.416

User-ID

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Asignaciones de IP-User (plano de administración)	524.288	524.288	524.288	524.288
Asignaciones de IP-User (plano de datos)	64.000	512.000	512.000	512.000
Grupos activos y únicos utilizados en la política (conjunto de grupos LDAP, grupos de API XML y grupo de usuarios dinámicos).*	1.000	10.000	10.000	10.000
Número de agentes de User-ID	100	100	100	100
Servidores supervisados para User-ID	100	100	100	100
Agentes de Terminal Server	400	2.000	2.500	2.500
Etiquetas por usuario* (PAN-OS 9.1 y posterior)	32	32	32	32

*Rendimiento del cortafuegos medido con las funciones App-ID y User-ID habilitadas utilizando transacciones AppMix.

Descifrado SSL

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Máximo de certificados de entrada SSL	1.000	1.000	1.000	4.000
Caché de certificado SSL (Proxy de reenvío)	128	4.000	8.000	32.000
Núm. más. de sesiones de descifrado simultáneas	6.400	50.000	100 000	2.000.000
Espejo de puerto SSL	Sí	Sí	Sí	Sí
Intermediario de descifrado SSL	No	No	Sí	Sí

©2024 Palo Alto Networks, Inc.

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Compatible con HSM	Sí	Sí	Sí	Sí

URL Filtering

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Núm. total de entradas para la lista de permitidos, la lista de bloqueo y las categorías personalizadas	25.000	25.000	100 000	100 000
Núm. máx. de categorías personalizadas	2.849	2.849	2.849	2.849
Núm. máx. de categorías personalizadas (específicas del sistema virtual)	500	500	500	500
Tamaño de la caché del plano de datos para el filtrado de URL	90.000	90.000	250.000	250.000
Tamaño de la caché dinámica del plano de gestión	100 000	100 000	600.000	900.000

EDL

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número máximo de listas personalizadas	30	30	30	30
Número máximo de direcciones IP por sistema	50.000	50.000	50.000	150.000
Número máximo de dominios DNS por sistema	50.000	2.000.000	2.000,00	4 000 000
Número máximo de URL por sistema	50.000	100 000	100 000	250.000
Intervalo de comprobación más corto (minutos)	5	5	5	5

Interfaces

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Gestión: fuera de banda	N/A	N/A	N/A	N/A

©2024 Palo Alto Networks, Inc.

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Gestión: alta disponibilidad 10/100/1000	N/A	N/A	N/A	N/A
Gestión: alta disponibilidad de 40 Gbps	N/A	N/A	N/A	N/A
Gestión: alta disponibilidad de 10 Gbps	N/A	N/A	N/A	N/A
Tráfico - 10/100/1000	N/A	N/A	N/A	N/A
Tráfico - 100/1000/10000	N/A	N/A	N/A	N/A
Tráfico: SFP de 1 Gbps	N/A	N/A	N/A	N/A
Tráfico: 10 Gbps SFP+	N/A	N/A	N/A	N/A
Tráfico: 40 / 100Gbps QSFP+ / QSFP28	N/A	N/A	N/A	N/A
Etiquetas 802.1q por dispositivo	4.094	4.094	4.094	4.094
Etiquetas 802.1q por interfaz física	4.094	4.094	4.094	4.094
Núm. máximo de interfaces (lógicas y físicas)	2.048	4.096	4.096	4.096
Núm. máximo de interfaces agregadas	N/A	N/A	N/A	N/A
Número máximo de interfaces virtuales SD-WAN	300	1.000	1.000	1.000

Enrutadores virtuales

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Enrutadores virtuales	3	20	125	225

Cables virtuales

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Cables virtuales	12	12	12	12

Virtual Systems

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Sistemas virtuales base	1	1	1	1

©2024 Palo Alto Networks, Inc.

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número máximo de sistemas virtuales Se requieren licencias adicionales para las capacidades del sistema virtual por encima de la capacidad del sistema virtual base	N/A	N/A	N/A	N/A

Enrutamiento

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Tamaño de la tabla de reenvío de IPv4* (Entradas compartidas entre enrutadores virtuales)	5000	32.000	100 000	Para añadir
Tamaño de la tabla de reenvío de IPv6* (Entradas compartidas entre enrutadores virtuales)	5000	32.000	100 000	Para añadir
Tamaño de la tabla de reenvío total del sistema	5000	32.000	100 000	Para añadir
Número máximo de mapas de ruta por enrutador virtual	50	50	50	Para añadir
Número máx. de pares de enrutamiento (dependiente del protocolo)	500	1.000	1.000	Para añadir
Entradas estáticas: Proxy DNS	1.024	1.024	1.024	Para añadir
Sesiones de detección de reenvío bidireccional (BFD)	128	1.024	1.024	Para añadir

*Rendimiento del cortafuegos medido con las funciones App-ID y User-ID habilitadas utilizando transacciones AppMix.

Reenvío de L2

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Tamaño de la tabla ARP por dispositivo	2.500	32.000	128.000	132.000
Tamaño de la tabla de vecinos de IPv6	2.500	32.000	128.000	132.000
Tamaño de la tabla de MAC por dispositivo	2.500	32.000	128.000	132.000

©2024 Palo Alto Networks, Inc.

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número máx. de entradas ARP por dominio de difusión	2.500	32.000	128.000	132.000
Número máx. de entradas MAC por dominio de difusión	2.500	32.000	128.000	132.000

NAT

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Capacidad total de la regla NAT	3.000	8.000	8.000	Para añadir
Número máx. de reglas NAT (estáticas)* (La configuración de las reglas NAT estáticas a plena capacidad requiere que no se utilicen otros tipos de reglas NAT).	3.000	8.000	8.000	Para añadir
Número máx. de reglas NAT (DIP)* (La configuración de las reglas NAT DIP a plena capacidad requiere que no se utilicen otros tipos de reglas NAT).	2.000	8.000	8.000	Para añadir
Número máx. de reglas NAT (DIPP)	400	2.000	2.000	Para añadir
Número máx. de IP traducidas (DIP)	128.000	160.000	160.000	Para añadir
Número máx. de IP traducidas (DIPP)* (La capacidad de IP traducida de DIPP es proporcional al valor de sobresuscripción del grupo de DIPP. La capacidad que se muestra aquí se basa en un valor de sobresuscripción de 1x).	400	2.000	2.000	Para añadir
Sobresuscripción predeterminada del grupo DIPP* (Reutilización de IP de origen y puerto de origen en sesiones simultáneas)	2	8	8	Para añadir

*Rendimiento del cortafuegos medido con las funciones App-ID y User-ID habilitadas utilizando transacciones AppMix.

©2024 Palo Alto Networks, Inc.

Asignación de dirección

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Servidores DHCP	3	20	125	Para añadir
Agentes de retransmisión de DHCP* (La capacidad máxima representa el total de servidores DHCP y agentes de retransmisión DHCP combinados)	500	500	500	Para añadir
Número máximo de direcciones asignadas	64.000	64.000	64.000	Para añadir

*Rendimiento del cortafuegos medido con las funciones App-ID y User-ID habilitadas utilizando transacciones AppMix.

High Availability

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Dispositivos compatibles	2	2	2	2
Número máx. de direcciones virtuales	128	32	128	Para añadir

QoS

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número de políticas de QoS	500	2.000	4.000	Para añadir
Interfaces físicas compatibles con QoS	6	12	12	12
Nodos de texto no cifrado por interfaz física	31	63	63	63
Marcado DSCP por política	Sí	Sí	Sí	Sí
Subinterfaces compatibles	N/A	N/A	N/A	N/A

©2024 Palo Alto Networks, Inc.

IPSec VPN

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número máx. de pares de IKE	1.000	1.000	2.000	Para añadir
Sitio a sitio (con ID de proxy)	1.000	4.000	8.000	Para añadir
Túneles SD-WAN IPSec	1.000	1.000	2.000	Para añadir

VPN de cliente de GlobalProtect

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Núm. máx. de túneles (SSL, IPSec e IKE con XAUTH)	500	6.000	12.000	Para añadir

VPN sin cliente de GlobalProtect

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Número máx. de túneles SSL	100	1.200	2.500	25.000

Multidifusión

Función	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Replicación (interfaces de salida)	100	100	100	Para añadir
Rutas	2.000	4.000	4.000	Para añadir

Activación de créditos

Dentro de su organización puede crear muchas cuentas, cada una con un propósito distinto. Durante la activación, solo puede elegir una cuenta por grupo de crédito predeterminado. Una vez que su grupo de créditos está activo, los usuarios a los que se les concedió la función de administrador de créditos pueden asignar los créditos para las implementaciones e incluso transferir créditos a otros grupos.

Si tiene una cuenta CSP existente y es un superusuario o un administrador, el sistema añade automáticamente la función de administrador de crédito a su perfil. Si no tiene una cuenta existente, el CSP crea automáticamente una cuenta para usted y añade la función de administrador de crédito a su perfil.

 ©2024 Palo Alto Networks, Inc.

Usted (el comprador) recibe un correo electrónico detallando la suscripción, el ID del grupo de créditos, la fecha de inicio y finalización de la suscripción, la cantidad de créditos comprados y la descripción del grupo de créditos predeterminado (consulte "grupos de crédito predeterminados" en Licencias de cortafuegos VM-Series).

Guarde este correo electrónico en un sitio seguro para futuras referencias.

STEP 1 | En el correo electrónico, haga clic en **Start Activation (Iniciar activación)** para ver los grupos de crédito disponibles.

STEP 2 | Seleccione el grupo de créditos que desea activar. Puede usar el campo de búsqueda para filtrar su lista de cuentas por número o nombre.

Si ha comprado varios grupos de crédito (consulte Créditos NGFW de software), se seleccionan automáticamente. Las marcas de verificación representan los enlaces de activación para los créditos de incorporación.

Se le solicitará una autenticación o inicio de sesión.

*Si anula la selección de un grupo de créditos, verá un recordatorio que le pregunta si desea activar esos créditos, debe volver al correo electrónico y hacer clic en el vínculo **Start Activation (Iniciar activación)**.*

STEP 3 | Seleccione **Start Activation (Iniciar activación)**.

STEP 4 | Seleccione la cuenta de soporte (puede buscar por número de cuenta o nombre).

STEP 5 | Seleccione el grupo de créditos predeterminado.

STEP 6 | Seleccione **Deposit Credits (Depositar créditos)**.

Verá un mensaje que indica que el depósito se realizó correctamente.

STEP 7 | (opcional) Si esta es su primera activación de crédito, verá el cuadro de diálogo **Create Deployment Profile (Crear perfil de implementación)**.

Continúe a Crear un perfil de implementación.

Crear un perfil de implementación

Para crear un perfil de implementación, debe tener una Cuenta del Portal de atención al cliente (CSP) y el acceso a un grupo de créditos activado.

Antes de comenzar, calcule el número de cortafuegos que usarán la configuración en el perfil de implementación. No tiene que implementar todos los cortafuegos a la vez.

©2024 Palo Alto Networks, Inc.

STEP 1 | Si ya tiene un grupo de créditos, inicie sesión en la cuenta y, desde el panel, seleccione **Products (Productos)** > **Software NGFW Credits (Créditos NGFW de software)** > **Create Deployment Profile (Crear perfil de implementación)**.

Si acaba de activar un grupo de créditos, verá el formulario **Create Deployment Profile (Crear perfil de implementación)**.

1. Seleccione el tipo de cortafuegos VM-Series.
2. Seleccione la versión PAN-OS.
   - **Fixed Models (Modelos fijos)** (Modelos VM-Series)
   - **vCPU flexibles (PAN-OS 10.0.4 y superior)**
3. Haga clic en **Next (Siguiente)**.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Perfil de VM-Series.

1. **Profile Name (Nombre de perfil)**.

   Asigne un nombre al perfil.

2. **Number of Firewalls (Número de cortafuegos)**.

   Introduzca el número de cortafuegos que este perfil implementa, suponiendo que tiene suficientes créditos. No tiene que implementarlos todos a la vez.

3. PAN-OS 11.1.3 y versiones posteriores**Número de vSYS**

   Introduzca el número de soporte de sistemas virtuales que necesita en su cortafuegos VM-Series.

   Utilice una licencia de cortafuegos flexible VM-Series e instancias de nivel 3 o 4 que admitan un mínimo de 16 vCPU o más.

   - *La serie VM-series en una instancia de nivel 3 admite un máximo de 25 sistemas virtuales.*
   - *VM-Series en una instancia de nivel 4 admite un máximo de 100 sistemas virtuales.*

   Para obtener información sobre el número máximo para un objeto o recurso en particular que una sola implementación de cortafuegos VM-Series puede crear, almacenar, gestionar o interactuar en base a una memoria o un nivel asignado, consulte Límites máximos en base a un nivel y una memoria.

4. **Modelo de cortafuegos**:

   Seleccione un modelo VM-Series.

   Planned vCPU/Firewall (Cortafuegos/vCPU planificado) (PAN-OS 10.0.4 o superior).

   Introduzca el número de vCPU por cortafuegos.

   Caso de uso de seguridad: Seleccione un caso de uso.

5. **Customize Subscriptions (Personalizar suscripciones)**.

   Después de seleccionar un caso de uso, puede añadir o quitar servicios de seguridad.

6. (opcional) **Use Credits to Enable VM Panorama (Utilice créditos para habilitar VM Panorama)**.

   Seleccione los casos de uso de Panorama: gestión y/o recopilador de logs.

STEP 3 | (opcional) Coloque el ratón sobre el signo de interrogación después de **Protect more, save more (Proteger más, ahorrar más)** para ver cómo su asignación de crédito afecta los ahorros.

STEP 4 | Haga clic en **Calculate Estimated Cost (Calcular coste estimado)** para ver el total de crédito y el número de créditos disponibles antes de la implementación.

(opcional) Pase el ratón sobre el signo de interrogación después de la estimación para ver el desglose del crédito para cada componente.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | **Create the Deployment Profile (Crear el perfil de implementación)**.

Es posible que tenga que esperar varios segundos para que el perfil aparezca en la lista de pestañas **Current Deployment Profiles (Perfiles de implementación actuales)**. Antes de que se complete la asignación, la columna **Credits Consumed/Allocated (Créditos utilizados/asignados)** muestra 0 y **Update Pending (Pendiente de actualización)**. Desplácese hasta la parte inferior y vaya a la última página para encontrar su perfil.

Para ver su perfil de implementación más adelante, haga clic en el botón **Details (Detalles)** del grupo de créditos principal y seleccione **Current Deployment Profiles (Perfiles de implementación actuales)**.

- Tenga en cuenta el código de autenticación para su perfil en el extremo derecho; Los códigos de autenticación de crédito NGFW de software comienzan con D.
- La columna **Credits Consumed/Allocated (Créditos utilizados/asignados)** muestra 0 y **Update Pending (Pendiente de actualización)** antes de que se complete la asignación.
- La pestaña **Audit Trail (Auditar seguimiento)** muestra las **Credit Transactions (Transacciones de crédito)** y los **Deployment Profiles (Perfiles de implementación)** que gestiona. También puede buscar un perfil por tiempo en esta pestaña.

  Utilice la búsqueda para localizar su perfil y expanda la fila para ver la configuración que especificó al crear el perfil.

Gestionar un perfil de implementación

Después de crear su perfil de implementación, puede editarlo, copiarlo o eliminarlo. Además, puede transferir un perfil de implementación de un grupo de créditos a otro.

- Editar un perfil de implementación
- Clonación de un perfil de implementación
- Transferir un perfil de implementación
- Eliminar un perfil de implementación

Editar un perfil de implementación

STEP 1 | Seleccione **Products (Productos)** > **Software NGFW Credits (Créditos de NGFW de software)** y haga clic en el botón **Details (Detalles)** en el grupo de crédito que utilizó para crear su perfil.

STEP 2 | Seleccione la pestaña **Current Deployment Profiles (Perfiles de implementación actuales)**.

STEP 3 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Edit Profile (Editar perfil)**.

STEP 4 | Realice los cambios y seleccione **Update Deployment Profile (Actualizar perfil de implementación)**.

STEP 5 | Seleccione la pestaña **Audit Trail (Auditar seguimiento)** y utilice la búsqueda para localizar su perfil.

Utilice la búsqueda para localizar su perfil y expanda la fila para ver la configuración que especificó al crear el perfil.

 ©2024 Palo Alto Networks, Inc.

Clonación de un perfil de implementación

STEP 1 | Seleccione **Products (Productos)** > **Software NGFW Credits (Créditos de NGFW de software)** y haga clic en el botón **Details (Detalles)** en el grupo de crédito que utilizó para crear su perfil.

STEP 2 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Clone Profile (Clonar perfil)**.

STEP 3 | Cambie el nombre del perfil, realice cualquier otro cambio y seleccione **Create Deployment Profile (Crear perfil de implementación)**.

STEP 4 | Seleccione la pestaña **Audit Trail (Auditar seguimiento)** y utilice la búsqueda para localizar su perfil.

Expanda la fila para ver la configuración que clonó. Es una nueva configuración con un nombre de perfil y un código de autenticación diferentes.

Transferir un perfil de implementación

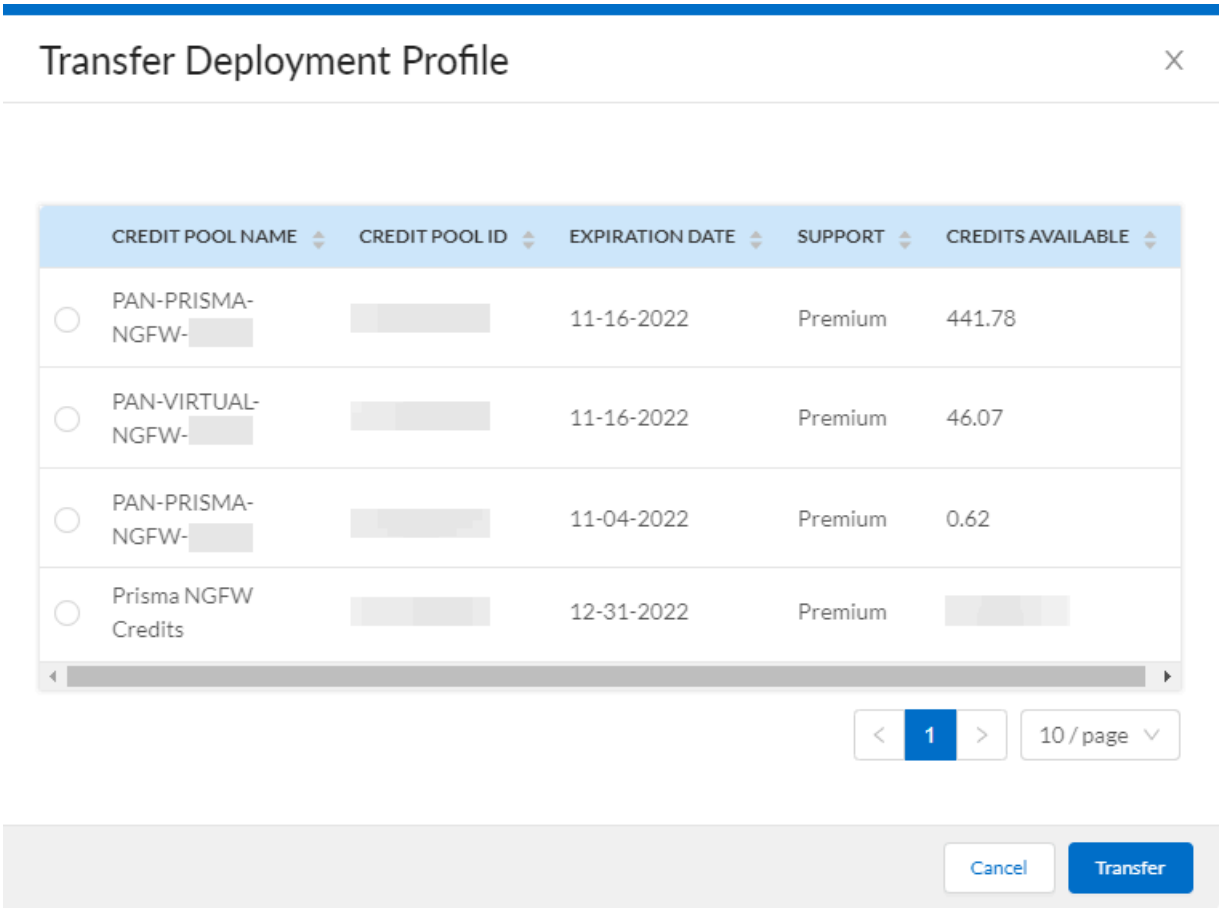
Utilice el siguiente procedimiento para transferir un perfil de implementación de un grupo de créditos a otro.

STEP 1 | Seleccione **Products (Productos)** > **Software NGFW Credits (Créditos de NGFW de software)** y haga clic en el botón **Details (Detalles)** en el grupo de crédito que utilizó para crear su perfil.

STEP 2 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Transfer Profile (Transferir perfil)**.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Seleccione el grupo de créditos de destino y haga clic en **Transfer (Transferir)**.



Eliminar un perfil de implementación

Antes de eliminar un perfil de implementación, debe Desactivar licencia (créditos NGFW de software) el cualquier perfil usando el perfil de implementación y luego desactivar la máquina virtual.

Si su perfil de implementación se utilizó para habilitar Panorama, debe desaprovisionar esa instancia de Panorama antes de eliminar el perfil de implementación.

STEP 1 | Seleccione **Products (Productos)** > **Software NGFW Credits (Créditos de NGFW de software)** y haga clic en el botón **Details (Detalles)** en el grupo de crédito que utilizó para crear su perfil.

STEP 2 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Delete (Eliminar)**.

Registrar el cortafuegos VM-Series (Créditos NGFW de software)

El registro requiere acceso al portal de atención al cliente de Palo Alto Networks (el CSP) y una cuenta de soporte. Cree uno si es necesario.

Durante la activación, un administrador activa un grupo de créditos y estos se depositan. Cuando alguien crea un perfil de implementación, se crea un código de autenticación. Complete uno de los siguientes procedimientos para iniciar el registro.

 ©2024 Palo Alto Networks, Inc.

- El dispositivo puede acceder al CSP
- El dispositivo no puede acceder al CSP

Siga estos pasos si el cortafuegos puede conectarse al CSP:

1. Inicie sesión en el CSP con las credenciales de su cuenta.
2. Seleccione **Products (Productos)** > **Assets (Activos)** > **Software NFGW Credits (Créditos NFGW de software)**.

   Localice su grupo de crédito y vea **Details (Detalles)**.
3. Vea **los perfiles de implementación actuales** y seleccione (o cree) un perfil.

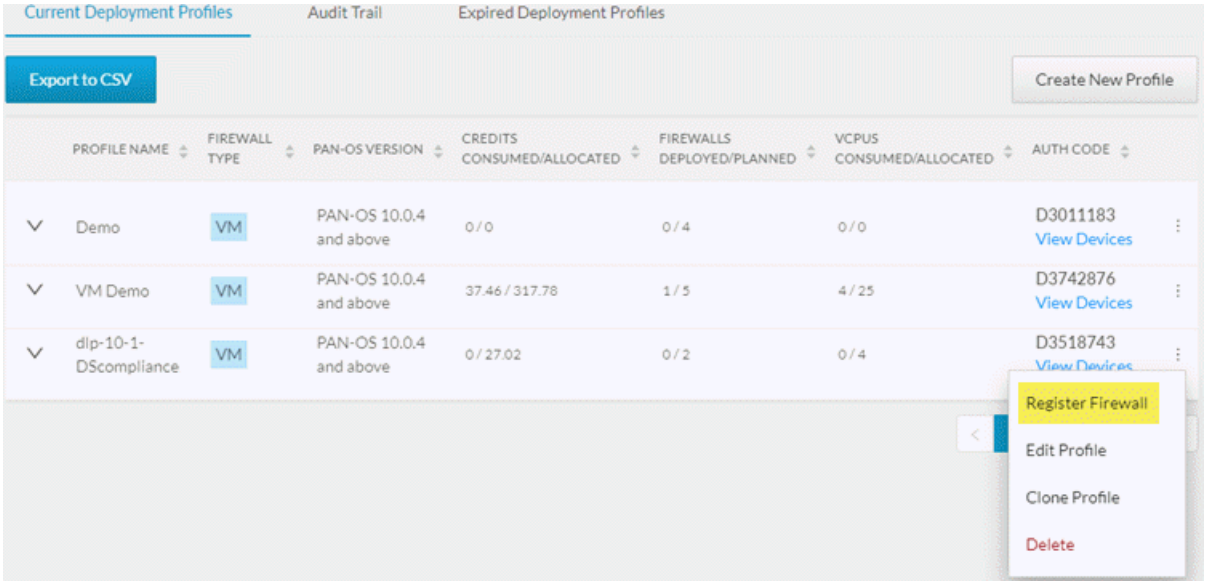
   Utilizará el código de autenticación de este perfil para otorgar licencias a cualquier cortafuegos que cree con él. Un código de autenticación para una licencia de cortafuegos flexible comienza con la letra D.
4. Inicie sesión en la interfaz web del cortafuegos VM-series.
5. Verifique la configuración del servidor de actualizaciones de Palo Alto Networks.
   1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**.
   2. Confirme que **Update Server (Servidor de actualizaciones)** está definido en `updates.paloaltonetworks.com`.
   3. Confirme que la opción **Verify Update Server Identity (Verificar identidad del servidor de actualización)** esta seleccionada.
6. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)**.
   1. Seleccione el enlace **Activate feature using authorization code (Activar característica mediante código de autorización)**.
   2. Escriba el código de autorización de VM-Series desde el perfil de implementación.
   3. Haga clic en **OK (Aceptar)** para confirmar la actualización de la licencia. El cortafuegos se pone en contacto con el servidor de actualizaciones de Palo Alto Networks y consume los tokens necesarios para su cortafuegos según el modelo de VM-Series.
7. Confirme que **Dashboard (Panel)** muestra un número de serie válido y que la licencia muestra **PA-VM** en la pestaña **Device (Dispositivo)** > **Licenses (Licencias)**.
8. Verifique que su cortafuegos esté registrado en el CSP:
   - Seleccione **Products (Productos)** > **Assets (Activos)** > **Software NFGW Credits (Créditos NFGW de software)**
   - Columna de código de autenticación, **View Devices (Ver dispositivos)** y localizar el número de serie de la implementación.
   - En el grupo de créditos, los créditos consumidos, los cortafuegos implementados y las vCPU consumidas deben incrementarse para reflejar la implementación.

 ©2024 Palo Alto Networks, Inc.

- **Siga los siguientes pasos si el cortafuegos *no* puede conectarse al CSP**:

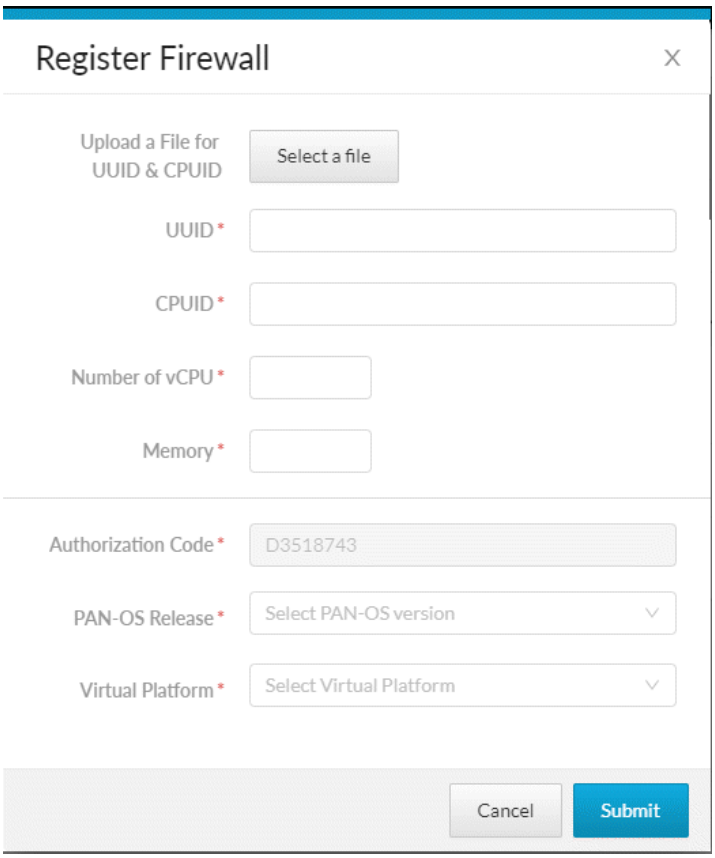
  Este flujo de trabajo añade su cortafuegos a la base de datos de soporte. Dado que el cortafuegos no puede conectarse al servidor de licencias, debe pasar manualmente las licencias del CSP al cortafuegos.

  1. Inicie sesión en el CSP con las credenciales de su cuenta.
  2. Seleccione el nuevo perfil y seleccione los puntos suspensivos verticales (Más opciones) y **Register Firewall (Registre el cortafuegos)**.



  Esto abre el formulario de registro del dispositivo. Introduzca la información de su cortafuegos y haga clic en **Submit (Enviar)**:

 ©2024 Palo Alto Networks, Inc.



Esta asocia el cortafuegos con el perfil y su código de autenticación y asigna un número de serie.

3. Haga clic en **View Devices (Ver dispositivos)** para ver los cortafuegos asociados en **Software NGFW Devices (Dispositivos NGFW de software)**.

   En la columna **License (Licencia)**, descargue cada clave de licencia en una ubicación desde la que pueda transferir los archivos de forma segura al cortafuegos.

4. Inicie sesión en el cortafuegos y seleccione Licencias **Device (Dispositivo)** > **Licenses (Licencias)**.

   Las claves de licencia se deben instalar a través de la interfaz web. El cortafuegos no es compatible con la instalación de la clave de licencia a través de SCP o FTP.

   - Haga clic en **Manually Upload License (Cargar licencia manualmente)**.
   - Confirme que el Panel muestra un número de serie válido y que la licencia **PA-VM** se muestra en la pestaña **Device (Dispositivo)** > **Licenses (Licencias)**.

Aprovisionar Panorama

Esta opción solo es visible si seleccionó Panorama cuando se creó el perfil de implementación. Puede editar el perfil, si es necesario.

STEP 1 | Seleccione **Products (Productos)** > **Assets (Activos)** > **Software NGFW Credits (Créditos de NGFW de software)** y haga clic en el botón **Details (Detalles)** en el grupo de créditos que utilizó para crear su perfil.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Provision Panorama (Aprovisionar panorama)** y **Provision (Aprovisionar)**. Verá la lista de cortafuegos aprovisionados para el perfil de implementación actual.

Esto crea un Panorama, asigna un número de serie y el tipo de modelo PAN-PRA-1000-CP, y registra el Panorama como activo. El Panorama que acaba de aprovisionar es el último Panorama de la lista. Tenga en cuenta que el código de autenticación comienza con F (por lo que no es lo mismo que el perfil de implementación), pero la fecha de vencimiento es la misma que la del grupo de crédito de su perfil.

Copie el número de serie.

STEP 3 | Desde el perfil de implementación, seleccione **View Devices (Ver dispositivos)** y seleccione **Panorama** en la página Dispositivos NGFW de software. Esto muestra todas los Panorama NGFW de SW.

Search By (Buscar por) número de serie utilizando el número de serie que copió.

También puede seleccionar **Assets (Activos)** > **Software NGFW Devices (Dispositivos NGFW de software)** y **Search by (Buscar por)** número de serie con el número de serie que copió.

STEP 4 | Después de configurar el dispositivo virtual Panorama, añada el número de serie a Panorama.

1. Inicie sesión en Panorama.
2. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** > **General Settings (Configuración general)** y haga clic en el icono **Edit (Editar)**.
3. Introduzca el número de serie que ha copiado del CSP en el campo **Serial Number (Número de serie)**.
4. Haga clic en **OK (Aceptar)** para guardar los cambios.
5. Confirme sus cambios de configuración.

   Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** sus cambios

Migrar Panorama a una licencia NGFW de software

Puede migrar licencias de VM-ELA o Panorama virtuales perpetuas a licencias de Software de cortafuegos de nueva generación (Software NGFW).

- Migrar un Panorama con acceso al CSP
- Migrar un par de alta disponibilidad Panorama que pueda acceder al CSP
- Migrar una Panorama independiente que no tiene acceso al CSP a una licencia flexible
- Migrar un par de alta disponibilidad (HA) que no puede acceder al CSP a una licencia flexible

Migrar un Panorama con acceso al CSP

Complete el siguiente procedimiento para migrar su licencia VM-ELA o Panorama virtual perpetua a una licencia de software NGFW. Esta migración le permite mover sus dispositivos Panorama existentes a la licencia NGFW de software sin interrupciones mientras conserva su número de serie existente. Dado que el número de serie no cambia, se conservan los registros y las políticas existentes.

STEP 1 | Seleccione **Products (Productos)** > **Assets (Activos)** > **Software NGFW Credits (Créditos de NGFW de software)** y haga clic en el enlace **Details (Detalles)** en el grupo de crédito que utilizó para crear su perfil.

 ©2024 Palo Alto Networks, Inc.

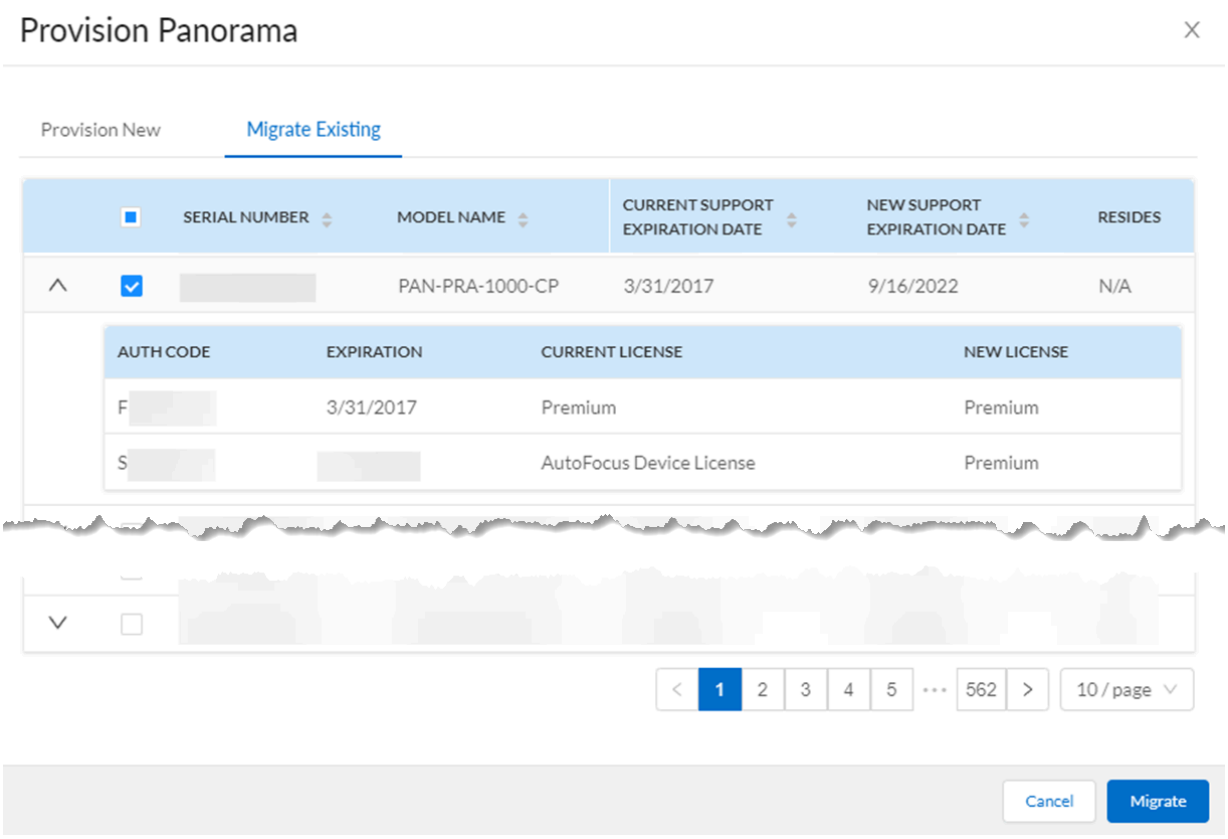
STEP 2 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Provision Panorama (Aprovisionar panorama)** y haga clic en **Migrate Existing (Migrar existente)**.

El CSP muestra todos los dispositivos Panorama virtuales asociados a su cuenta.

STEP 3 | Active la casilla de verificación de cada Panorama virtual que se vaya a migrar.

STEP 4 | Haga clic en **Migrate (Migrar)**.

Compruebe que se ha actualizado la **Fecha de caducidad de soporte actual**. Además, puede expandir cada fila para ver las licencias individuales aplicadas al Panorama seleccionado.



Migrar un par de alta disponibilidad Panorama que pueda acceder al CSP

Complete el siguiente procedimiento para migrar un par de alta disponibilidad (HA) con VM-ELA o licencias perpetuas a una licencia de NGFW de software. Esta migración le permite mover sus dispositivos Panorama existentes a la licencia NGFW de software sin interrupciones mientras conserva su número de serie existente. Debido a que los números de serie no cambian, se conservan los registros y las políticas existentes.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Seleccione **Products (Productos)** > **Assets (Activos)** > **Software NGFW Credits (Créditos de NGFW de software)** y haga clic en el enlace **Details (Detalles)** en el grupo de crédito que utilizó para crear su perfil.

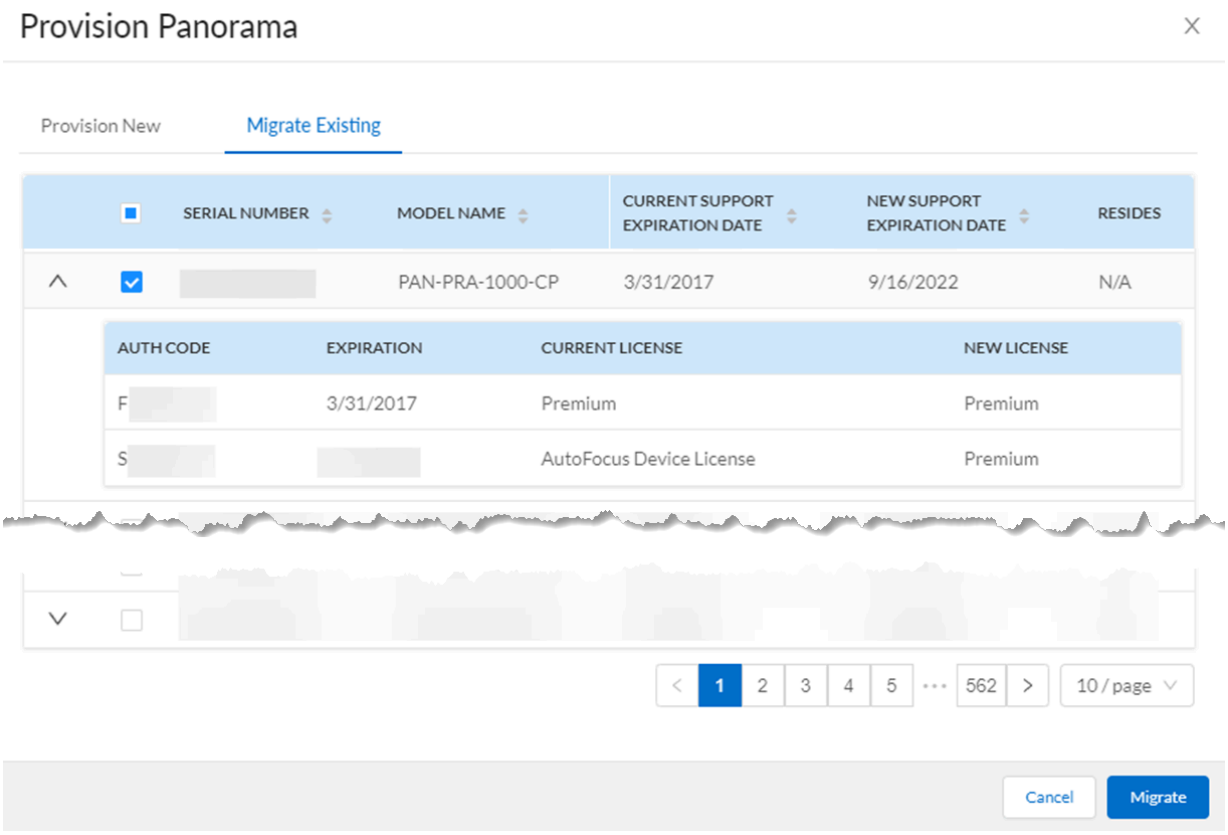
STEP 2 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Provision Panorama (Aprovisionar panorama)** y haga clic en **Migrate Existing (Migrar existente)**.

El CSP muestra todos los dispositivos Panorama virtuales asociados a su cuenta.

STEP 3 | Marque la casilla de cada Panorama virtual que se va a migrar.

STEP 4 | Seleccione **Migrate (Migrar)**.

Compruebe que se ha actualizado la **Fecha de caducidad de soporte actual**. Además, puede expandir cada fila para ver las licencias individuales aplicadas al Panorama seleccionado.



Migrar una Panorama independiente que no tiene acceso al CSP a una licencia flexible

Complete el siguiente procedimiento para migrar su licencia de VM-ELA o Panorama virtual perpetua a una licencia NGFW de software aunque su Panorama no pueda acceder al CSP. La migración sin el CSP

 ©2024 Palo Alto Networks, Inc.

requiere un cambio de número de serie, pero permite que los dispositivos Panorama migren a licencias de NGFW de software y conserven las políticas existentes.

La versión mínima para la compatibilidad con Panorama es la 8.1. Si debe actualizar PAN-OS, hágalo antes de iniciar el proceso de migración. Si desea gestionar cortafuegos que utilizan vCPU flexibles y servicios avanzados, la versión de PAN-OS debe ser 10.0.4 o posterior.

STEP 1 | En su Panorama, actualice si es necesario y anote el número de serie y la fecha de vencimiento del soporte actual.

STEP 2 | En el CSP, seleccione **Products (Productos)** > **Assets (Activos)** > **Software NGFW Credits (Créditos de NGFW de software)** y haga clic en el vínculo **Detalles** de un grupo de créditos. Seleccione un perfil de implementación o cree uno.

STEP 3 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Provision Panorama (Aprovisionar panorama)** y luego **Migrate Existing (Migrar existente)**.

El CSP muestra todos los dispositivos Panorama virtuales asociados a su cuenta.

STEP 4 | Compruebe cada Panorama virtual que se va a migrar y seleccione **Migrate (Migrar)**.

STEP 5 | En Panorama, sustituya el número de serie por el número de serie del Panorama que aprovisionó en el CSP. Espere un minuto y, a continuación, actualice la página.

STEP 6 | En el CSP, seleccione su Panorama aprovisionado y descargue todas las licencias (la licencia de soporte, la licencia de gestión y Panorama como administrador de logs si su perfil de implementación lo incluye.

Pase las licencias de forma segura a su Panorama.

STEP 7 | Cargue todas las licencias NGFW de software.

STEP 8 | Compruebe que se ha actualizado la **Fecha de caducidad de soporte actual**. Además, puede expandir cada fila para ver la licencia de soporte y/o la licencia de registro aplicada al Panorama seleccionado.

Migrar un par de alta disponibilidad (HA) que no puede acceder al CSP a una licencia flexible

Utilice este procedimiento cuando el par de alta disponibilidad (HA) no pueda comunicarse con el CSP. Este procedimiento inicia una conmutación por error.

STEP 1 | Seleccione **Products (Productos)** > **Assets (Activos)** > **Software NGFW Credits (Créditos de NGFW de software)** y haga clic en el botón **Details (Detalles)** en el grupo de créditos.

STEP 2 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Provision Panorama (Aprovisionar panorama)**.

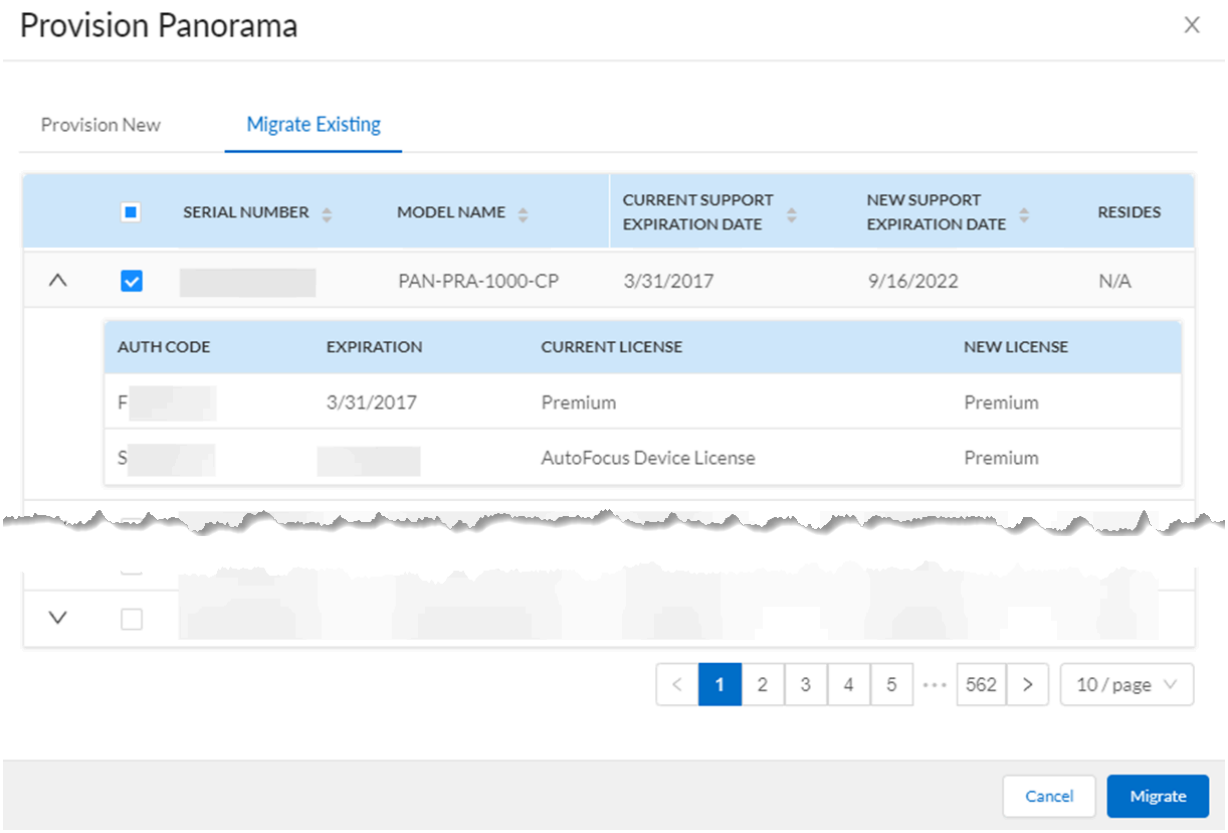
El CSP muestra todos los dispositivos Panorama virtuales asociados a la cuenta de soporte actual.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Seleccione **Provision New (Aprovisionar nuevo)**, marque la casilla correspondiente a cada panorama virtual que se vaya a migrar y seleccione **Migrate (Migrar)**.

Los Panoramas migrados se muestran como dispositivos Software NGFW.

STEP 4 | Compruebe que se ha actualizado la **Fecha de caducidad de soporte actual**. Además, puede expandir cada línea para ver las licencias individuales aplicadas al Panorama seleccionado.



Transferir créditos

Desde el Portal de atención al cliente (CSP), transfiera créditos a un grupo de créditos en la misma cuenta, entre grupos de créditos del mismo contrato o a un grupo de créditos en una cuenta diferente a la que tiene acceso.

Los créditos se deben transferir entre los grupos dentro del mismo contrato (padre / hijo).

- Cuenta de CSP diferente
- Grupo diferente en esta cuenta

 ©2024 Palo Alto Networks, Inc.

Cuenta de CSP diferente

STEP 1 | Inicie sesión en su cuenta de CSP.

STEP 2 | Seleccione **Products (Productos)** > **Software NGFW Credits (Créditos NGFW de software)**.

- Identifique el grupo de crédito de origen y anote el ID del grupo de crédito.
- Identifique el grupo de crédito de destino y anote el ID del grupo de crédito.

  Si el destino está en una cuenta diferente, selecciónelo en el menú desplegable **Current Account (Cuenta actual)** en la parte superior izquierda y seleccione **Products (Productos)** > **Software NGFW Credits (Créditos de NGFW de software)**. Busque el destino y anote el tipo de crédito y el ID del grupo de créditos.

STEP 3 | Vaya al grupo de crédito de origen y haga clic en **Transfer Credits (Transferir créditos)** en la parte inferior izquierda.

STEP 4 | Seleccione una cuenta CSP diferente.

1. **Transfer to (Transferir a)**: seleccione un nombre de cuenta.
2. **As Credit Type (Como tipo de crédito)**: seleccione un tipo de crédito. En estos momentos, el tipo de origen y destino debe ser el mismo.
3. **Credit Pool ID# (Nº de ID del grupo de crédito)**: elija un número de identificación del grupo de crédito.

   Si la cuenta de destino no tiene ningún grupo de crédito del tipo elegido, el CSP le solicitará que cree un grupo de crédito.
4. **Amount to transfer (Cantidad a transferir)**: introduzca la cantidad a transferir.

STEP 5 | Seleccione **Update Credits (Actualizar créditos)**.

Es posible que deba esperar un poco o actualizar la pantalla para ver el cambio.

STEP 6 | Para ver las transacciones de crédito de un grupo, seleccione **Details (Detalles)** y seleccione **Audit Trail (Auditar seguimiento)**.

Grupo diferente en esta cuenta

STEP 1 | Inicie sesión en su cuenta de CSP.

STEP 2 | Seleccione **Products (Productos)** > **Software NGFW Credits (Créditos NGFW de software)**.

- Identifique el grupo de crédito de destino y anote el ID del grupo de crédito.
- Si no hay un grupo de crédito de destino del tipo que especifica, se le solicitará que cree un nuevo grupo de crédito.

STEP 3 | Vaya al grupo de crédito de origen y seleccione **Transfer Credits (Transferir créditos)** en la parte inferior izquierda.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Seleccione **Different Pool in this Account (Grupo diferente en esta cuenta)**.

1. **New credit type (Nuevo tipo de crédito)**: elija un tipo de crédito. En estos momentos, el tipo de origen y destino debe ser el mismo.
2. **Credit Pool ID# (Nº de ID del grupo de crédito)**: elija un número de identificación del grupo de crédito.

   Si la cuenta de destino no tiene ningún grupo de crédito del tipo elegido, el CSP le solicitará que cree un grupo de crédito.
3. **Amount to transfer (Cantidad a transferir)**: introduzca la cantidad a transferir.

STEP 5 | Seleccione **Update Credits (Actualizar créditos)**.

Es posible que deba esperar un poco o actualizar la pantalla para ver el cambio.

STEP 6 | Para ver las transacciones de crédito de un grupo, seleccione **Details (Detalles)** y seleccione **Audit Trail (Auditar seguimiento)**.

Si desea transferir créditos entre grupos, las fechas de vencimiento deben ser las mismas en ambos grupos de créditos.

Renueve su licencia de créditos Software NGFW

Cuando un perfil de implementación caduca, se mueve de la pestaña Perfiles de implementación actuales a la pestaña Renovar perfiles. Sin embargo, si renueva el contrato y el número de créditos es igual o mayor que el número de créditos antes de la renovación, los perfiles de implementación vuelven automáticamente a la pestaña Perfiles de implementación actuales y no requieren ninguna otra acción.

Tiene la opción de renovar sus créditos NGFW de software con un número reducido. Para ello, primero debe reducir y configurar el consumo de créditos de los perfiles de implementación existentes hasta el número de uso previsto (reducido) antes de renovar su contrato. Si el total del nuevo grupo de créditos es mayor o igual que el número de créditos asignados a los perfiles de implementación, no es necesario realizar una renovación manual. Si renueva con menos créditos, pero no cambia su consumo de créditos, debe elegir manualmente qué perfiles de implementación renovar con el nuevo total del grupo de créditos.

Desde la pestaña Renovar perfiles, puede renovar cualquiera de sus perfiles de implementación sin interrumpir las operaciones de su cortafuegos VM-Series. Una vez que un perfil de implementación caduque y se mueva a la pestaña Renovar perfiles, tiene 30 días para renovar el perfil. Los perfiles de implementación que no se renueven en el plazo de 30 días pasan a la pestaña Perfil de implementación caducado. Consulte ¿Qué ocurre cuando la licencia caduca? para obtener más información.



Después de la renovación, es posible que observe algunos cambios entre sus perfiles de implementación. Los grupos de créditos Prisma NGFW Credits y Virtual NGFW Credits ahora se denominan grupos de créditos Software NGFW Credits. Además, el número de créditos en su grupo puede cambiar después de la renovación debido a cambios en el modelo de precios del producto.

STEP 1 | Inicie sesión en el Portal de atención al cliente de Palo Alto Networks.

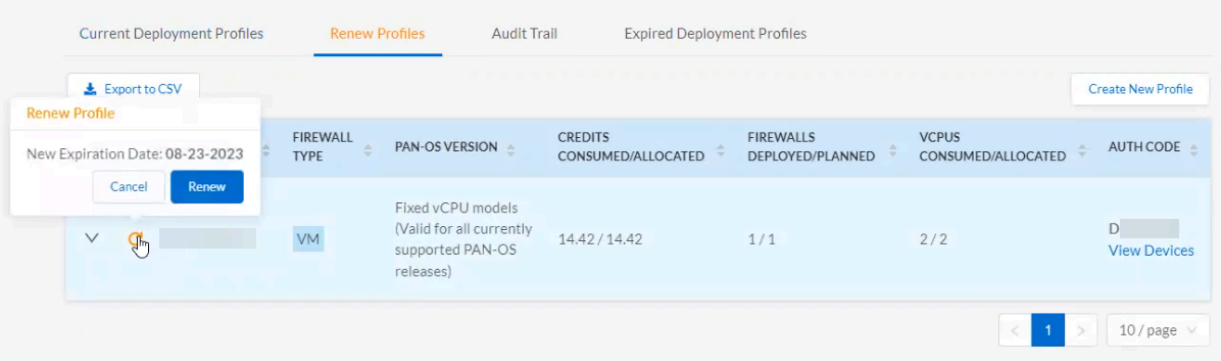
STEP 2 | Seleccione **Products (Productos)** > **Software NGFW Credits (Créditos NGFW de software)**.

STEP 3 | Localice el perfil de implementación que desea renovar y haga clic en **Details (Detalles)**.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Seleccione **Renew Profiles (Renovar perfiles)**.

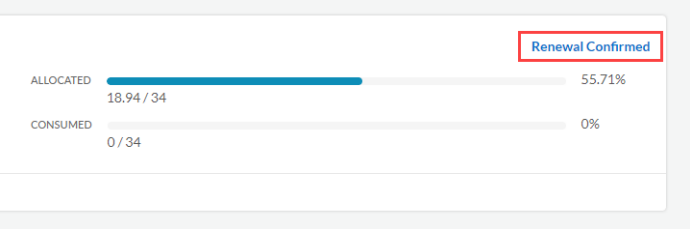
STEP 5 | Haga clic en el icono Renovar y, a continuación, haga clic en **Renew (Renovar)** para confirmar.



STEP 6 | Compruebe que ha renovado correctamente el perfil de implementación.

1. Haga clic en **Current Deployment Profiles (Perfiles de implementación actuales)**.
2. Confirme que la lista muestra el perfil de implementación renovado.

   Además, puede volver al panel de control de Software NGFW para ver su grupo de créditos. Después de una renovación correcta, el grupo de crédito muestra **Renewal Confirmed (Renovación confirmada)**. Este mensaje permanece hasta el final de la fecha de caducidad de los créditos de NGFW de software.



Renovación con suscripciones heredadas

Las suscripciones heredadas (WildFire, URL Filtering, Threat Prevention) ya no están disponibles y se han sustituido por las versiones avanzadas ((Advanced WildFire, Advanced URL Filtering, Advanced Threat Prevention). Si el perfil de implementación tiene suficientes créditos disponibles para cubrir las suscripciones avanzadas, el perfil de implementación consume el número necesario de créditos adicionales al completar el proceso de renovación descrito anteriormente; No se requiere ninguna acción adicional.

Si el grupo de créditos que se va a renovar incluye suscripciones heredadas, es posible que tenga que modificar ese perfil de implementación para que las suscripciones avanzadas se incluyan. Tiene un período de gracia de 30 días para modificar el perfil de implementación. Si no lo hace, el perfil de implementación caduca.

 ©2024 Palo Alto Networks, Inc.

Si el perfil de implementación no tiene suficientes créditos sin usar para cubrir las suscripciones avanzadas, debe modificar ese perfil de implementación. Tiene dos opciones para modificar el perfil de implementación: aumentar el número de créditos del grupo de créditos o reducir verticalmente las suscripciones actuales para liberar suficientes créditos para las suscripciones avanzadas. Además, puede liberar créditos NGFW de software eliminando los cortafuegos implementados actualmente.

Si elige Transferir un perfil de implementación con las suscripciones heredadas, después de renovarlas, no es posible transferirlas a un grupo de créditos que incluya perfiles de implementación con suscripciones avanzadas. Los perfiles de implementación con suscripciones heredadas (y sin suscripciones avanzadas) no son compatibles con grupos de créditos con suscripciones avanzadas.

STEP 1 | Inicie sesión en el Portal de atención al cliente de Palo Alto Networks.

STEP 2 | Seleccione **Products (Productos)** > **Software NGFW Credits (Créditos NGFW de software)**.

STEP 3 | Localice el perfil de implementación que desea renovar y haga clic en **Details (Detalles)**.

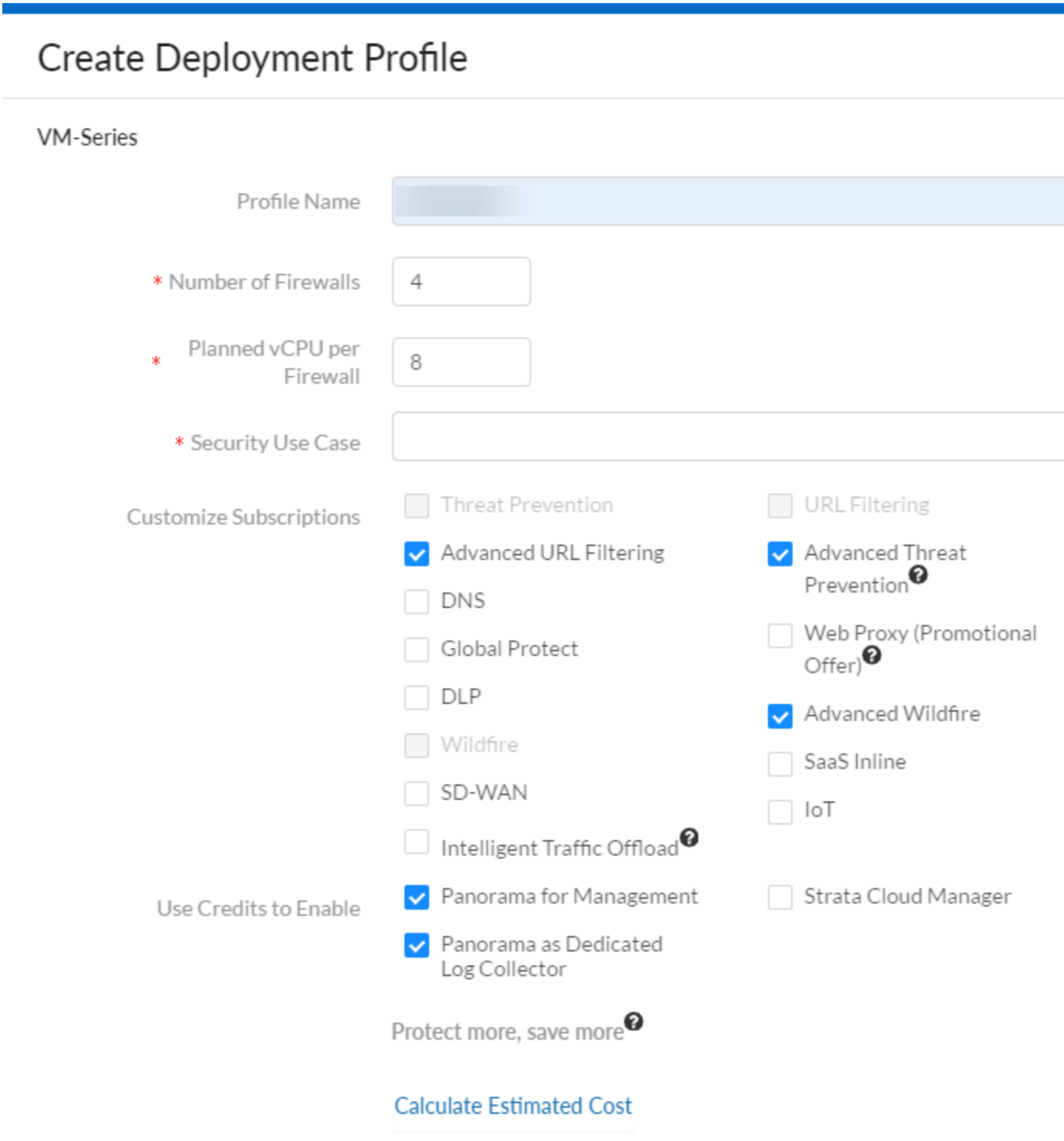
STEP 4 | Seleccione **Renew Profiles (Renovar perfiles)**.

STEP 5 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Edit Profile (Editar perfil)**.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Modifique su perfil de implementación.

1. Personalice sus suscripciones.
2. Haga clic en **Update Deployment Profile (Actualizar perfil de implementación)**.



STEP 7 | Haga clic en el icono Renovar y, a continuación, haga clic en **Renew (Renovar)** para confirmar.

 ©2024 Palo Alto Networks, Inc.

Desactivar licencia (créditos NGFW de software)

Debe desactivar cualquier licencia del CSP **antes** de eliminar un cortafuegos (o la máquina virtual que hospeda el cortafuegos) o los créditos de licencia no pueden volver a su grupo de créditos.

Cuando tiene acceso al servidor de licencias, la desactivación del cortafuegos en el CSP elimina automáticamente las licencias y los créditos restantes se devuelven al perfil de implementación. Después de desactivar la licencia, debe eliminar el cortafuegos o continuará consumiendo créditos.

Si no tiene acceso a Internet, debe exportar el token de licencia desde el cortafuegos. Luego, en el CSP, inicie la desactivación y cargue el token (o pegue el texto del token) para completar la desactivación.

- Acceso a Internet
- Sin acceso a Internet
- Sin acceso a internet: gestión de Panorama

- Acceso directo a internet.
  1. Seleccione **Products (Productos)** > **Assets (Activos)** > **Software NGFW Credits (Créditos NGFW de software)** y haga clic en el botón **Details (Detalles)** en el grupo de créditos que utilizó para crear su perfil de implementación.
  2. Localice su perfil de implementación y, en el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Deactivate Firewall (Desactivar cortafuegos)**.
  3. Compruebe el cortafuegos que desea desactivar y seleccione **Deactivate Firewall (Desactivar cortafuegos)**.

- Sin acceso a Internet.
  1. Inicie sesión en la interfaz web del cortafuegos y seleccione **Device (Dispositivo)** > **Licenses (Licencias)**.
  2. En la sección Gestión de licencias seleccione **Deactivate VM (Desactivar VM)**.

     Compruebe la lista de licencias/derechos que se desactivarán en el cortafuegos.
  3. Seleccione **Complete Manually (Completar manualmente)** para iniciar la desactivación.

     Haga clic en el enlace **Exportar token de licencia** para guardar el archivo de token en el cliente. Un nombre de archivo de token tiene este aspecto: `20150128_1307_dact_lic.01282015.130737.tok`

     En este punto, la licencia se ha desactivado en el cortafuegos, pero los créditos no se han devuelto al grupo de créditos.
  4. Utilice el archivo de token para registrar los cambios con el servidor de licencias:
     1. Inicie sesión en el sitio web de asistencia técnica de Palo Alto Networks.
     2. Seleccione **Products (Productos)** > **VM-Series Auth-Codes (Códigos de autenticación de VM-series)** > **Deactivate License(s) [Desactivar licencia(s)]**.

     En el formulario para Desactivar licencias, pegue el texto del token, o copie el token en un equipo con acceso a Internet, y cargue el archivo de token en el CSP para completar la retirada de la licencia.
  5. Eliminar la máquina virtual (VM)

 ©2024 Palo Alto Networks, Inc.

- Sin acceso a Internet: gestión de panorama
  1. Inicie sesión en la interfaz web de Panorama y seleccione **Panorama** > **Device Deployment (Implementación de dispositivo)** > **Licenses (Licencias)**.
  2. Seleccione **Deactivate VMs (Desactivar las VM)** y seleccione el cortafuegos VM-Series que desea desactivar.
  3. Seleccione **Complete Manually (Completar manualmente)** para exportar el archivo de token.
  4. Haga clic en el vínculo **Export license token (Exportar token de licencia)** para guardar el archivo de token. Un nombre de archivo de token tiene este aspecto: 20150128_1307_dact_lic.01282015.130737.tok

     Si la exportación se realiza correctamente, se muestra un mensaje de finalización y el cortafuegos se reinicia automáticamente.
  5. Utilice el archivo de token para registrar los cambios con el servidor de licencias.
     1. Inicie sesión en el sitio web de asistencia técnica de Palo Alto Networks.
     2. Seleccione **Products (Productos)** > **VM-Series Auth-Codes (Códigos de autenticación de VM-series)** > **Deactivate License(s) [Desactivar licencia(s)]**.

     En el formulario para Desactivar licencias, pegue el texto del token, o copie el token en un equipo con acceso a Internet, y cargue el archivo de token en el CSP para completar la retirada de la licencia.
  6. (opcional) Elimine el cortafuegos VM-Series desactivado como un dispositivo gestionado en Panorama.

     En lugar de eliminar los cortafuegos desactivados, puede crear un grupo de dispositivos separado y asignarlos a él.

     1. Select **Panorama** > **Managed Devices (Dispositivo gestionado)**.
     2. Seleccione el cortafuegos que ha desactivado y haga clic en **Delete (Eliminar)**.

Retirada de licencias de cortafuegos terminados incorrectamente

Puede retirar la licencia de un cortafuegos al que ya no tiene acceso o que se canceló involuntariamente a través del portal de atención al cliente. Por ejemplo, si su hipervisor falla o elimina accidentalmente un cortafuegos y ya no puede iniciar sesión en dicho cortafuegos, realice el siguiente procedimiento para eliminar la licencia de ese cortafuegos y liberar sus Créditos de Software NGFW para uso futuro.

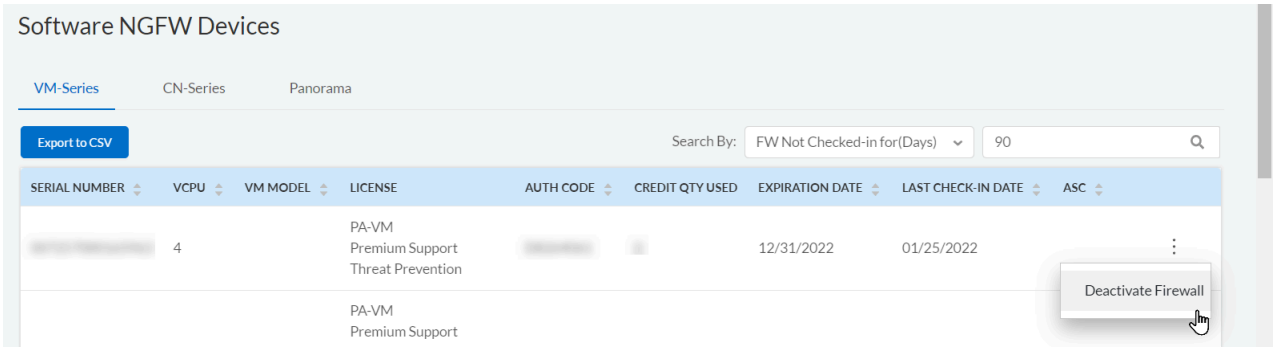
STEP 1 | Inicie sesión en el Portal de atención al cliente.

STEP 2 | Seleccione **Software NGFW Devices (Dispositivos de Software NGFW)**.

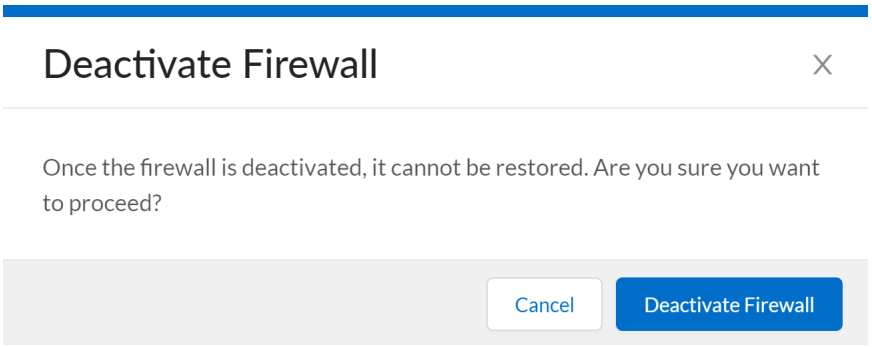
STEP 3 | Seleccione **FW Not Checked-in for (Days) [Cortafuegos no registrado durante (días)]** en el menú desplegable **Search By (Buscar por)** e introduzca el número de días en los que quiere buscar.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Para cancelar la licencia de un cortafuegos, haga clic en Más opciones (tres puntos verticales) a la derecha y luego haga clic en **Deactivate Firewall (Desactivar cortafuegos)**.



STEP 5 | Haga clic en **Deactivate Firewall (Desactivar cortafuegos)** para confirmar la desactivación del cortafuegos seleccionado. Después de desactivar el cortafuegos, los créditos se devuelven a su grupo de créditos.



Establecer el número de las vCPU licenciadas

Puede especificar el número de vCPU con licencia cuando se utilizan créditos NGFW de software en lugar de otorgar licencias todas a las vCPU disponibles en la instancia de proceso elegida. Esto le permite utilizar una instancia de cálculo más grande sin consumir más créditos NGFW de software de los necesarios.

Esta característica requiere el complemento VM-Series 2.1.4 o posterior.

Puede especificar el número de vCPU a las que se van a otorgar licencia utilizando el comando bootstrap plugin op o la CLI del cortafuegos VM-Series.

- Para establecer el número de núcleos al arrancar un cortafuegos VM-Series, añada el siguiente comando al archivo init-cfg.txt.

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

  Por ejemplo:

  `plugin-op-commands=set-cores:4`

 ©2024 Palo Alto Networks, Inc.

- Para establecer el número de núcleos en un cortafuegos VM-Series que ya se ha implementado, use el siguiente comando CLI.

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

  Por ejemplo:

  request plugins vm_series set-cores cores 16

  Debe reiniciar el cortafuegos VM-Series para que este cambio surta efecto.

Personalizar núcleos de plano de datos

Como se mencionó en Créditos NGFW de software, cuando se implementa un cortafuegos con créditos NGFW, de software el perfil de memoria y el número total de vCPU determinan cuántos núcleos se asignan automáticamente al plano de gestión y al plano de datos. Las configuraciones predeterminadas funcionan bien en la mayoría de los casos.

Personalizar núcleos de plano de datos es una función opcional que le permite personalizar el número de núcleos de plano de datos de dos formas:

- Durante la implementación inicial, use el parámetro de arranque del archivo `init-cfg.txt` file bootstrap parameter **plugin-op-commands=set-dp-cores:<#-cores>**. Consulte Componentes de archivo de init-cfg.txt.
- Desde un cortafuegos implementado, utilice el comando de la CLI de VM-Series para **request plugins vm_series dp-core <#-cores>**. Este procedimiento se describe a continuación.

Normalmente, aumenta el número de núcleos del plano de datos (lo que disminuye el número de núcleos del plano de gestión) para mejorar el rendimiento. La personalización del núcleo del plano de datos no requiere un cambio en el perfil de implementación, ni créditos adicionales, porque el número total de vCPU sigue siendo la misma.

- La personalización del núcleo del plano de datos es compatible con cortafuegos que ejecutan PAN-OS 10.1 o posterior con licencia con un grupo de crédito NGFW de software para 10.0.4 y superior.
- La personalización del núcleo del plano de datos no es compatible con:
  - NSX-T
  - Descarga tráfico inteligente

Siga estos pasos para personalizar los núcleos del plano de datos en el cortafuegos VM-Series.

STEP 1 | Inicie sesión en el cortafuegos VM-Series y vea la cantidad de núcleos.

```
admin@PA-VM(active)>show plugins vm_series dp-cores
Núcleos DP actuales del dispositivo: 13 (número total de núcleos:
 18)
```

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Cambie el número de núcleos del plano de datos.

Tenga en cuenta que debe tener al menos un núcleo del plano de gestión y que tener muy pocos núcleos afecta al rendimiento.

En este ejemplo, aumentamos los planos de datos a 14.

```
admin@PA-VM(active)>request plugins vm_series dp-cores 14
Núcleos DP actuales del dispositivo: 14 (número total de núcleos:
 18)
```

STEP 3 | Reinicie el cortafuegos VM-Series.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en**Reboot Device (Reiniciar dispositivo)**

STEP 4 | Utilice **`show plugins vm_series dp-cores`** para verificar que el número de núcleos DP haya cambiado.

Migración de un cortafuegos a una licencia VM-Series flexible

Puede migrar su licencia perpetua o ELA de cortafuegos VM-Series a una licencia de cortafuegos flexible de VM-Series (financiada con créditos NGFW de software).

Al migrar desde una licencia perpetua o ELA, es posible que tenga que reiniciar el cortafuegos para completar la migración. En un perfil de implementación de vCPU fijo, el cortafuegos consume créditos en función del modelo VM-Series. Después de migrar a un perfil de implementación con vCPU fijas, cada cortafuegos conserva su número de serie y no requiere un reinicio. En un perfil de implementación con vCPU flexibles, el cortafuegos consume créditos en función del número de vCPU configuradas en el cortafuegos de origen. Después de la migración, es posible que tenga que Establecer el número de las vCPU licenciadas en el cortafuegos para garantizar que se consuma el número esperado de créditos. Para establecer el número de vCPU con licencia, es necesario reiniciar el cortafuegos.

Compruebe y establezca el número de vCPU con licencia antes de la migración si recibe un mensaje de error que indica que no tiene suficientes créditos en el perfil de implementación para admitir la solicitud.

Si los cortafuegos VM-Series se implementan en un entorno de producción, se recomienda realizar la migración durante un período de mantenimiento.

Complete uno de los siguientes procedimientos para migrar sus licencias.

- Cortafuegos independiente con acceso al CSP
- Verificar la migración

Cortafuegos independiente con acceso al CSP

Este proceso no interrumpe el tráfico que se mueve a través del cortafuegos.

STEP 1 | Inicie sesión en la interfaz web del cortafuegos VM-series.

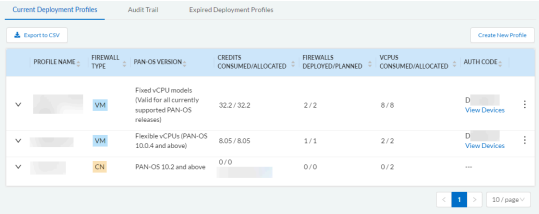
 ©2024 Palo Alto Networks, Inc.

STEP 2 | Verifique la configuración del servidor de actualizaciones de Palo Alto Networks.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)**.
2. Confirme que **Update Server (Servidor de actualizaciones)** está definido en `updates.paloaltonetworks.com`.
3. Confirme que la opción **Verify Update Server Identity (Verificar identidad del servidor de actualización)** esta seleccionada.

STEP 3 | Inicie sesión en el CSP y Crear un perfil de implementación.

Utilizará el código de autenticación de este perfil. Un código de autenticación para una licencia de cortafuegos flexible comienza con la letra D, como se muestra a continuación.



STEP 4 | Inicie sesión en el cortafuegos VM-Series.

STEP 5 | Instalación de una clave de API de licencia.

STEP 6 | Seleccione **Device (Dispositivo)** > **Licenses (Licencias)**.

STEP 7 | Escriba el código de autorización de VM-Series desde el nuevo perfil de implementación.

STEP 8 | Haga clic en **OK (Aceptar)** para confirmar la actualización de la licencia. El cortafuegos se pone en contacto con el servidor de actualización de Palo Alto Networks y consume los tokens necesarios para el cortafuegos basado en el modelo VM-Series.

STEP 9 | Si va a migrar a un perfil de implementación con vCPU flexibles, es posible que tenga que establecer el número de vCPU utilizadas por el cortafuegos. Para establecer el número de vCPU con licencia, es necesario reiniciar el cortafuegos VM-Series para que este cambio surta efecto.

1. Determine si el cortafuegos VM-Series requiere menos vCPU que el número de vCPU disponibles en la instancia de máquina virtual.
2. Establecer el número de las vCPU licenciadas.

STEP 10 | (Opcional) Verificar la migración.

STEP 11 | Repita este proceso para cada cortafuegos VM-Series en su implementación.

Verificar la migración

Compruebe que la migración de la licencia se ha realizado correctamente.

STEP 1 | En el dispositivo, compruebe que la fecha de caducidad de la licencia se ha actualizado correctamente.

STEP 2 | Compruebe que todas las suscripciones habilitadas en el perfil de implementación se aplican al dispositivo.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | En el CSP, verifique que el número previsto de créditos asignados y los créditos consumidos coinciden con su grupo de créditos.

STEP 4 | En el CSP, compruebe que los tokens asociados o el número de licencias se han devuelto al código de autenticación anterior.

API de licencias Software NGFW

Use la API de licencias de software NGFW para crear y gestionar códigos de autenticación de grupos de créditos, recuperar el grupo de créditos adjunto a un código de autenticación, todas las licencias basadas en modelos en un cortafuegos VM-Series. Además, la API de licencias le permite autorizar a cortafuegos que no tienen acceso directo a Internet y no pueden llegar al servidor de licencias de Palo Alto Networks. Puede gestionar licencias manualmente o automatizar las licencias con un script personalizado o un servicio de orquestación.

Para usar la API, a cada cuenta de soporte se le asigna un ID de cliente y un secreto de cliente únicos. Utilizará el ID de cliente y el secreto de cliente asociados con su cuenta de atención al cliente para generar un token de acceso. Cada llamada a la API debe incluir el token de acceso para autenticar la solicitud en el servidor de licencias. Cuando se autentica, el servidor de licencias envía la respuesta en formato json (content-type application/json). Póngase en contacto con su representante de ventas de Palo Alto Networks para obtener su ID de cliente y su secreto de cliente.

- Genere sus credenciales de cliente de OAuth
- Gestionar perfiles de implementación mediante la API de licencias
- Crear un perfil de implementación con la API de licencias
- Actualizar un perfil de implementación con la API de licencias
- Obtener números de serie asociados a un código de autenticación usando la API
- Desactivar un cortafuegos VM-Series mediante la API

Genere sus credenciales de cliente de OAuth

Palo Alto Networks utiliza OAuth 2.0 para limitar el acceso a la API de créditos del NGFW de software. Para usar la API de créditos de NGFW de software para gestionar sus perfiles de implementación, primero debe generar credenciales de OAuth (ID de cliente y clave secreta) en el CSP de Palo Alto Networks. El ID de cliente y la clave secreta son necesarios para realizar llamadas API al servidor de licencias de Palo Alto Networks.

Si la opción de generar las credenciales del cliente no aparece en el CSP, comuníquese con su representante de ventas.

STEP 1 | Inicie sesión en el CSP.

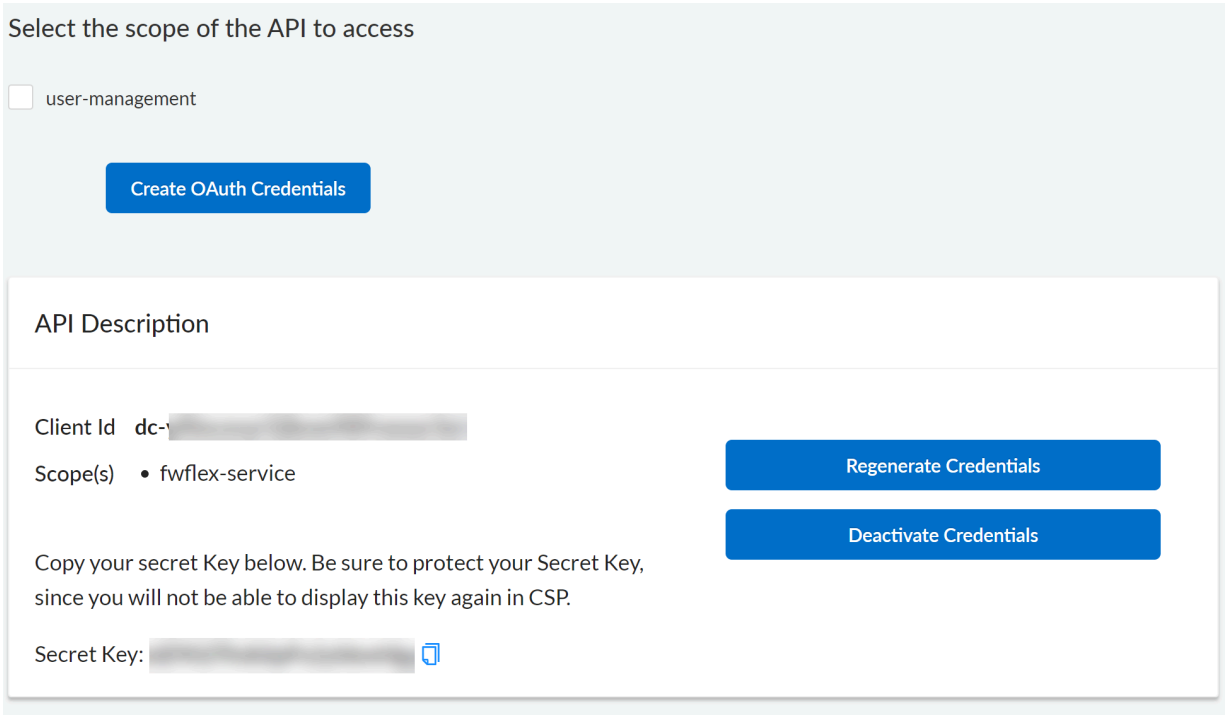
STEP 2 | Seleccione **Account Management (Gestión de cuentas)** > **OAuth API Management (Gestión de API con OAuth)**.

STEP 3 | Seleccione el alcance del **servicio fwflex**.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Haga clic en **Create OAuth Credentials (Crear credenciales OAuth)**.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

STEP 5 | Copie su **Client ID (ID de cliente)** y **Secret Key (Clave secreta)**. Guarde su clave secreta en un lugar seguro. No podrá recuperar la clave secreta de nuevo.

Gestionar perfiles de implementación mediante la API de licencias

Utilice las siguientes API para recuperar información sobre un perfil de implementación existente o para eliminar un perfil de implementación que ya no usa.

- Obtener todos los grupos de crédito
- Obtener un ID de grupo de crédito por grupo de crédito
- Obtenga todos los perfiles de implementación en un grupo de crédito
- Obtener un perfil de implementación
- Eliminar un perfil de implementación

Obtener todos los grupos de crédito

Utilice esta API para recuperar información sobre todos los grupos de créditos asociados con su cuenta de CSP.

Parámetros de encabezado: **`token`**

Método de solicitud: OBTENER

URL: **`https://api.paloaltonetworks.com/tms/v1/creditPool`**

Solicitud API de muestra:

```
curl --location --request GET 'https://api.paloaltonetworks.com/tms/
v1/creditPool' \ --header 'token: <your-token>'
```

Muestra de respuesta de API:

```
{ "data": [ { "creditPoolId": 31586#####, "poolName": "Software
 NGFW Credits", "supportType": "Platinum", "expirationDate":
 "02/07/2026", "totalCredits": 27.84, "creditsAllocated":
 0.0, "creditsConsumed": 0.0, "creditsAvailable": 27.84 },
 { "creditPoolId": 99394#####, "poolName": "Software NGFW Credits",
 "supportType": "Premium", "expirationDate": "10/27/2023",
 "totalCredits": 47.0, "creditsAllocated": 13.68, "creditsConsumed":
 0.0, "creditsAvailable": 33.32 }, { "creditPoolId": 90775#####,
 "poolName": "Software NGFW Credits", "supportType": "Premium
 Partner", "expirationDate": "04/13/2025", "totalCredits": 34.0,
 "creditsAllocated": 0.0, "creditsConsumed": 0.0, "creditsAvailable":
 34.0 } ] }
```

Obtener un ID de grupo de crédito por grupo de crédito

Parámetros de encabezado: **`token`**

Parámetros de ruta: **`creditPoolId`**

Método de solicitud: OBTENER

URL: **`https://api.paloaltonetworks.com/tms/v1/creditPool/{creditPoolId}`**

 ©2024 Palo Alto Networks, Inc.

Solicitud API de muestra:

```
curl --location --request GET 'https://api.paloaltonetworks.com/tms/
v1/creditPool/<creditPoolId>' \ --header 'token: <your-token>'
```

Muestra de respuesta de API:

```
{ "data": { "creditPoolId": 97101#####, "poolName": "Software
 NGFW Credits", "supportType": "Premium", "expirationDate":
 "02/20/2026", "totalCredits": 194.0, "creditsAllocated": 172.75,
 "creditsConsumed": 43.94, "creditsAvailable": 21.25 } }
```

Obtenga todos los perfiles de implementación en un grupo de crédito

Utilice esta API para obtener los detalles de un perfil de implementación específico.

Parámetros de encabezado: **`token`**

Parámetros de ruta: **`creditPoolId`**

Método de solicitud: OBTENER

URL: **`https://api.paloaltonetworks.com/tms/v1/creditPool/{creditPoolId}/deploymentProfile`**

Solicitud API de muestra:

```
curl --location --request GET 'https://api.paloaltonetworks.com/
tms/v1/creditPool/<creditPoolId>/deploymentProfile' \ --header
 'token:<your-token>'
```

Muestra de respuesta de API:

```
{ "data": [ { "profileName": "Credit Pool 1", "dAuthCode":
 "D#######", "type": "VM", "panOsVersion": "10.0.4_or-above",
 "creditsAllocated": 41.860000610351562, "creditsConsumed":
 20.930000305175781, "vCpuConsumed": 2, "vCpuAllocated": 4,
 "fWsDeployed": 1, "fWsPlanned": 2, "status": "Updated" },
 { "profileName": "Credit Pool 2", "dAuthCode": "D#######", "type":
 "VM", "panOsVersion": "10.0.3_or-below", "creditsAllocated":
 32.200000762939453, "creditsConsumed": 0.0, "vCpuConsumed": 0,
 "vCpuAllocated": 4, "fWsDeployed": 0, "fWsPlanned": 2, "status":
 "Created" } ] }
```

Obtener un perfil de implementación

Utilice esta API para obtener los detalles de un perfil de implementación específico.

Parámetros de encabezado: **`token`**

Parámetros de ruta: **`authCode`**

Método de solicitud: OBTENER

URL: **`https://api.paloaltonetworks.com/tms/v1/deploymentProfile/{authCode}`**

 ©2024 Palo Alto Networks, Inc.

Solicitud API de muestra:

```
curl --location --request GET 'https://api.paloaltonetworks.com/tms/
v1/deploymentProfile/<authCode>' \ --header 'token:<your-token>'
```

Muestra de respuesta de API:

```
{ "data": { "profileName": "deployment-profile-1", "dAuthCode":
 "D#######", "type": "VM", "panOsVersion": "10.0.3_or-below",
 "creditsAllocated": 43.7, "creditsConsumed": 0.0, "vCpuConsumed":
 0, "vCpuAllocated": 8, "fWsDeployed": 0, "fWsPlanned": 1, "status":
 "Updated" } } }
```

Eliminar un perfil de implementación

Utilice esta API para eliminar un perfil de implementación específico.

Parámetros de encabezado: **`token`**

Parámetros de ruta: **`authCode`**

Método de solicitud: ELIMINAR

URL: **`https://api.paloaltonetworks.com/v1/deployment-profile/auth-code/{auth-code}`**

Solicitud API de muestra:

```
curl --location --request DELETE 'https://api.paloaltonetworks.com//
tms/v1/deploymentProfile/<authCode>' \ --header 'token:<your-token>'
```

Muestra de respuesta de API:

```
{ "isDeleted": true, "dAuthcode": "D#######", "message": "Deleted" }
```

Crear un perfil de implementación con la API de licencias

Parámetros de encabezado: `token`

Solicitar parámetros del cuerpo: `creditPoolId`, `name`, `type`,`panOs`, `firewallQuantity`, `vCpuQuantity`,`panorama` y `subs`

Método de solicitud: POST

URL: **`https://api.paloaltonetworks.com/tms/v1/deploymentProfile`**

Utilice la siguiente API para crear un nuevo perfil de implementación para dar licencia a los cortafuegos VM-Series y CN-Series mediante créditos de Software NGFW. La respuesta de API devuelve el código de autenticación del Software NGFW que usará para otorgar licencia a sus cortafuegos.

Parámetros	Description (Descripción)
`creditPoolId` Este parámetro es necesario.	Este perfil de implementación se añade al grupo de créditos con el número de identificación que introduzca aquí.

 ©2024 Palo Alto Networks, Inc.

Parámetros	Description (Descripción)
`name`	El nombre del perfil de implementación.
`type` Este parámetro es necesario.	Para VM-Series, introduzca **`vm`**.
`panOs`	Para cortafuegos VM-Series con vCPU flexibles, introduzca **`10.0.4_o_posterior`**. Para cortafuegos VM-Series de modelo fijo, introduzca **`10.0.3_o_inferior`**
`firewallQuantity` Este parámetro es necesario.	El número de cortafuegos. Este valor debe ser superior a cero (0).
`vCpuQuantity`	Número de vCPU planificadas por cortafuegos. Esto es necesario si el **`tipo`** está establecido en VM-Flex. Además, el valor de vCPU debe ser superior a cero (0) y menor o igual a 64.
`vmModel`	Este parámetro es necesario al crear un perfil de implementación para cortafuegos VM-Series de modelo fijo. • Para VM-50, introduzca **`50`**. • Para VM-100, introduzca **`100`**. • Para VM-300, introduzca **`300`**. • Para VM-500, introduzca **`500`**. • Para VM-700, introduzca **`700`**.
`panorama`	Este parámetro le permite utilizar créditos de Software NGFW para habilitar Panorama. Utilice **`PAN`** para habilitar Panorama o **`DLC`** para habilitar Panorama como un recopilador de logs dedicado.
`suscripciones`	Especifique suscripciones para añadirlas a su perfil de implementación. Puede introducir varias suscripciones con algunas limitaciones. • Prevención de amenazas (TP) • Protección avanzada frente a amenazas (ATP) • Filtrado de URL (URL4) • Filtrado de URL avanzado (AURL) • DNS (DNS)

 ©2024 Palo Alto Networks, Inc.

Parámetros	Description (Descripción)
	• Global Protect (GP) • DLP (DLP) • Wildfire (WF) • Advanced Wildfire (AWF) • SD-WAN (SDWAN) • Descarga inteligente de tráfico (ITO) • Proxy web (WP) Si **`panOsVersion`** se deja en blanco, este campo es obligatorio.

Solicitud API de muestra:

```
curl --location --request POST 'https://api.paloaltonetworks.com/tms/
v1/deploymentProfile' \ --header 'token: <your-token>' \ --header
 'Content-Type: application/json' \ --data-raw '{ "creditPoolId":
 97101#####, "name":"3-16-1", "type": "VM", "panOS": "10.0.4_or-
above", "firewallQuantity": 1, "vCpuQuantity": 2, "panorama":
 [ "Management", "LogCollector" ], "subscriptions": [ "DNS", "GP",
 "DLP" ] }'
```

Muestra de respuesta de API:

```
{ "profileId": 29###, "authCode": "D#######", "success": true,
 "message": "Deployment profile saved successfully." }
```

La respuesta devuelve el código de autenticación completo.

Actualizar un perfil de implementación con la API de licencias

Parámetros de ruta: `authCode`

Parámetros de encabezado: `token`

Solicitar parámetros del cuerpo: `creditPoolId`, `name`, `type`,`panOs`, `firewallQuantity`, `vCpuQuantity`,`panorama` y `subs`

Método de solicitud: PATCH

URL: **`https://api.paloaltonetworks.com/tms/v1/deploymentProfile/{authCode}`**

Utilice la siguiente API para actualizar un perfil de implementación existente para dar licencia a sus cortafuegos VM-Series y CN-Series utilizando créditos de Software NGFW.

 ©2024 Palo Alto Networks, Inc.

Parámetros	Description (Descripción)
`creditPoolId` Este parámetro es necesario.	El ID del grupo de créditos del grupo de crédito propietario del perfil de implementación que está actualizando.
`name`	El nombre del perfil de implementación. Si proporciona un nombre, debe ser único dentro de su cuenta de CSP.
`type` Este parámetro es necesario.	Para VM-Series, introduzca **`vm`**.
`panOs`	Para cortafuegos VM-Series con vCPU flexibles, introduzca **`10.0.4_o_posterior`**. Para cortafuegos VM-Series de modelo fijo, introduzca **`10.0.3_o_inferior`**
`firewallQuantity` Este parámetro es necesario.	El número de cortafuegos. Este valor debe ser superior a cero (0).
`vCpuQuantity`	Número de vCPU planificadas por cortafuegos. Esto es necesario si el **`tipo`** está establecido en VM-Flex. Además, el valor de vCPU debe ser superior a cero (0) y menor o igual a 64.
`vmModel`	Este parámetro es necesario al crear un perfil de implementación para cortafuegos VM-Series de modelo fijo. • Para VM-50, introduzca **`50`**. • Para VM-100, introduzca **`100`**. • Para VM-300, introduzca **`300`**. • Para VM-500, introduzca **`500`**. • Para VM-700, introduzca **`700`**.
`panorama`	Este parámetro le permite utilizar créditos de Software NGFW para habilitar Panorama. Utilice **`PAN`** para habilitar Panorama o **`DLC`** para habilitar Panorama como un recopilador de logs dedicado.
`suscripciones`	Especifique suscripciones para añadirlas a su perfil de implementación. Puede introducir varias suscripciones con algunas limitaciones. • Prevención de amenazas (TP)

 ©2024 Palo Alto Networks, Inc.

Parámetros	Description (Descripción)
	• Protección avanzada frente a amenazas (ATP) • Filtrado de URL (URL4) • Filtrado de URL avanzado (AURL) • DNS (DNS) • Global Protect (GP) • DLP (DLP) • Wildfire (WF) • Advanced Wildfire (AWF) • SD-WAN (SDWAN) • Descarga inteligente de tráfico (ITO) • Proxy web (WP) Si **`panOsVersion`** se deja en blanco, este campo es obligatorio.

Solicitud de muestra para JSON de actualización del perfil de implementación:

```
curl --location --request PATCH 'https://
apitest.paloaltonetworks.com/tms/v1/deploymentProfile/D7984130' \ --
header 'token: <your-token>' \ --header 'Content-Type: application/
json' \ --data-raw '{ "creditPoolId": 97101#####, "name":"3-15-3",
 "type": "VM", "panOS": "10.0.4_or-above", "firewallQuantity": 1,
 "vCpuQuantity": 2, "panorama": [ "LogCollector" ], "subscriptions":
 [ "URL4", "AIOPS" ] }'
```

Muestra de respuesta de API:

```
{ "profileId": 29###, "authCode": "D#######", "success": true,
 "message": "Deployment profile saved successfully." }
```

La respuesta devuelve el código de autenticación completo.

Obtener números de serie asociados a un código de autenticación usando la API

Parámetros de encabezado: `token`

Parámetros de consulta: `auth_code`

Método de solicitud: OBTENER

URL: **`https://api.paloaltonetworks.com/tms/v1/firewallserialnumbers?auth_code=<authcode>`**

Utilice la siguiente API para recuperar una lista de números de serie asociados con un código de autenticación especificado.

 ©2024 Palo Alto Networks, Inc.

Solicitud API de muestra:

```
curl --location --request GET 'https://api.paloaltonetworks.com/tms/
v1/firewallserialnumbers?auth_code=<authcode>'\ --header 'token:
 <your-token>' \
```

Muestra de respuesta de API:

```
{ "vm_series": [ "00799##########" ], "cn_panorama": [], "panorama":
 [], "cn_firewall": [] }
```

Desactivar un cortafuegos VM-Series mediante la API

Parámetros de encabezado: `token`

Parámetros de consulta: `auth_code, serial_numbers`

Método de solicitud: ELIMINAR

URL: **`https://api.paloaltonetworks.com/tms/v1/firewall/deactivate`**

Utilice la siguiente API para eliminar uno o más recursos de cortafuegos asociados con un código de autenticación especificado. Para eliminar varios recursos del cortafuegos, inserte cada número de serie separado por comas.

Solicitud API de muestra:

```
curl --location --request DELETE 'https://
api.paloaltonetworks.com/tms/v1/firewall/deactivate?
auth_code=<authcode>&serial_numbers=<serialnumber>,<serialnumber>'\
 --header 'token: <your-token>' \
```

Muestra de respuesta de API:

```
{ "success": ["00799##########","00799##########" ], "failed": [],
 "auth_code": "D#######", "failure_reason": [] }
```

 ©2024 Palo Alto Networks, Inc.

Modelos VM-Series

El cortafuegos VM-Series está disponible en los siguientes modelos de vCPU fijos: VM-50, VM-100, VM-200, VM-300, VM-500, VM-700 y VM-1000-HV. Estos modelos están disponibles para todas las versiones compatibles de PAN-OS, a menos que se indique lo contrario a continuación. El paquete de software (archivo *.xva*, *.ova*, o *.vhdx*) que se usa para implementar el cortafuegos VM-Series es común en todos los modelos.

Puede migrar su ELA de modelo fijo o licencia perpetua a una

licencia flexible *y conservar el modelo fijo, o puede sustituir la licencia con una licencia de vCPU flexible. Consulte* Licencias de cortafuegos VM-Series *para comparar los métodos de licencia.*

- Todos los modelos se pueden implementar como máquinas virtuales invitadas en VMware ESXi y vCloud Air, KVM, Microsoft Hyper-V, Cisco ACI, Cisco ENCS y Cisco CSP.
- En entornos de nube pública (Amazon Web Services, Azure, Google Cloud Platform, Oracle Cloud Infrastructure, Alibaba Cloud), todos los modelos, excepto el VM-50 son compatibles.
- Para VMware NSX, solo se admiten los cortafuegos VM-100, VM-300, VM-500 y VM-700.

Cuando aplica la licencia de capacidad en el cortafuegos VM-Series, el número de modelo y las capacidades asociadas se implementan en el cortafuegos. La capacidad se define por el número de sesiones, reglas, zonas de seguridad, objetos de dirección, túneles VPN de IPSec y túneles VPN de SSL que el cortafuegos VM-Series está optimizado para gestionar. Para asegurarse de adquirir el modelo correcto para sus requisitos de red, utilice la siguiente tabla para comprender la capacidad máxima de cada modelo y las diferencias de capacidad por modelo:

Modelo	Sesiones	Reglas de seguridad	Direcciones IP dinámicas	Zonas de seguridad	Túneles VPN de IPSec	Túneles VPN de SSL
VM-50	50.000	• 250 • 200 en modo Lite	1.000	15	• 250 • 25 en modo Lite	• 250 • 25 en modo Lite
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

©2024 Palo Alto Networks, Inc.

Para obtener información sobre las plataformas en las que puede implementar el cortafuegos VM-Series, consulte Implementaciones de VM-Series. Para obtener más información acerca de los modelos de cortafuegos VM-Series, consulte la herramienta de comparación de cortafuegos de Palo Alto Networks. También puede revisar la información general en Acerca del cortafuegos de la VM-Series.

- Requisitos del sistema para VM-Series
- Sobresuscripción de la CPU
- Modo Lite de VM-50
- Tipos de licencia del modelo VM-Series
- Activar licencias del modelo VM-Series
- Registro del cortafuegos VM-Series
- Instalación de un certificado de dispositivo en el cortafuegos VM-Series
- Cambio entre las licencias BYOL y PAYG
- Cambio entre licencias del modelo VM-Series
- Desactivación de licencia(s)
- Renovación de los paquetes de licencias de cortafuegos VM-Series
- API de licencias basada en modelos

Requisitos del sistema para VM-Series

Cada instancia del cortafuegos VM-Series requiere una asignación de recursos mínima: número de CPU, memoria y espacio en disco en su servidor host. Use la tabla a continuación para verificar que asigna los recursos de hardware necesarios para su modelo VM-Series o perfil de memoria.

PAN-OS 11.1 añade funciones y capacidades adicionales, por lo que necesita un poco más de memoria. Para proporcionar la misma capacidad de sesión que una versión anterior a PAN-OS 10.2, debe aumentar la asignación mínima de memoria. Cuando no aumenta la memoria mínima de las configuraciones anteriores a PAN-OS 11.1, se reduce la capacidad de sesión máxima.

Modelo VM-Series	Hipervisores compatibles	VCPU compatibles	Memoria mínima	Memoria mínima con GTP habilitad	Disco duro mínimo	Recuent máximo de sesiones (heredad	Sesión con capacida ampliad en PAN-OS 10.2*	Memoria recomenda para el recuento de sesiones heredadas
VM-50	ESXi, Hyper-V, KVM	2	• 5,5GB • 4,5GB en modo Lite	• 6 GB • 5 GB en modo Lite	32 GB (60 GB en el arranque)	• 65.000 • 50.000 en modo Lite	• 50.000 • 25.000 en modo Lite	• 6 GB • 5,5GB

©2024 Palo Alto Networks, Inc.

Modelo VM-Series	Hipervisores compatibles	VCPU compatibles	Memoria mínima	Memoria mínima con GTP habilitad	Disco duro mínimo	Recuent máximo de sesiones (heredad	Sesión con capacida ampliad en PAN-OS 10.2*	Memoria recomenda para el recuento de sesiones heredadas
VM-100	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, NSX, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, Cisco ENCS, NSX-T (VM-100) *La VM-100 en Azure requiere 4 vCPU.*	2	6,5GB	7,5 GB	60GB	250.000	200.000	7 GB
VM-300	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, NSX, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, Cisco ENCS, NSX-T (VM-300)	2, 4	9 GB**	10GB	60GB	800.000	600.000	10GB
VM-500	AWS, Azure, Cisco ACI, Cisco CSP, ESXi, Google Cloud Platform,	2, 4, 8	16GB	20 GB	60GB	2.000.000	1.800.000	18 GB

©2024 Palo Alto Networks, Inc.

Modelo VM-Series	Hipervisores compatibles	VCPU compatibles	Memoria mínima	Memoria mínima con GTP habilitad	Disco duro mínimo	Recuent máximo de sesiones (heredad	Sesión con capacida ampliad en PAN-OS 10.2*	Memoria recomenda para el recuento de sesiones heredadas
	Hyper-V, KVM, OCI, NSX-T							
VM-700	AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, NSX-T	2, 4, 8 y 16	56GB	64 GB	60GB	10.000.000	00.000.000	56GB

*Modelo fijo de cortafuegos VM-Series con licencias financiadas con créditos de NGFW de software.

**En PAN-OS 11.0, es posible que 9 GB pueda no ser suficiente, dependiendo del conjunto de características o la combinación de conjuntos de características (como GTP o funciones de alto rendimiento) utilizadas en el cortafuegos. Si experimenta problemas relacionados con los recursos de memoria, aumente la memoria a 11 GB para adaptarse a los requisitos de memoria adicionales de algunas de las características o la combinación de características.

***En PAN-OS 11.0, se necesita un aumento adicional de memoria de 4 GB (20 GB) para adaptarse a los requisitos de memoria de la función Web Proxy.

Puede habilitar el modo Lite en VM-50. El modo Lite es un modo de funcionamiento alternativo para entornos donde los recursos son limitados. Consulte el modo VM-50 Lite para obtener más información.

Para obtener el mejor rendimiento, todos los núcleos necesarios deben estar disponibles en un solo socket de CPU.

Para el funcionamiento, el cortafuegos VM-50 requiere un mínimo de 32 GB de espacio en el disco duro. Sin embargo, debido a que la imagen base de la VM-Series es común para todos los modelos, debe asignar 60 GB de espacio en el disco duro hasta que obtenga la licencia del VM-50.

El número de vCPU asignadas al plano de gestión y las asignadas al plano de datos difieren según el número total de vCPU asignadas al cortafuegos VM-Series. Si asigna más CPU virtuales que las admitidos oficialmente por la licencia, cualquier CPU virtual adicional se asignará al plano de gestión.

 ©2024 Palo Alto Networks, Inc.

vCPU totales	vCPU del plano de administración	vCPU del plano de datos
2	1	1
4	2	2
8	2	6
16	4	12

Sobresuscripción de la CPU

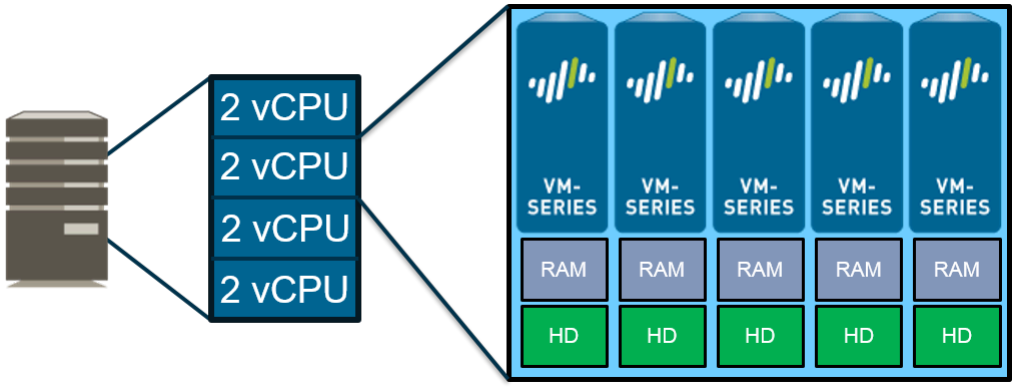
El cortafuegos VM-Series admite un exceso de suscripciones de CPU en todos los modelos. La sobresuscripción de la CPU le permite implementar una mayor densidad de cortafuegos VM-Series en hipervisores que se ejecutan en la arquitectura x86. Puede implementar entre dos (2: 1) y cinco (5: 1) cortafuegos VM-Series por asignación requerida de CPU. Cuando planifique su implementación, use la siguiente fórmula para calcular el número de cortafuegos VM-Series que su hardware puede admitir.

(número total de CPU x Relación de sobresuscripción) / CPU por cortafuegos = número total de cortafuegos VM-Series

Por ejemplo, en una relación de 5: 1, una máquina host con 16 CPU físicas y al menos 180 GB de memoria (40 × 4,5 GB) puede admitir hasta 40 instancias al VM-50. Cada VM-50 requiere dos vCPU y cinco VM-50 pueden estar asociados a cada par de vCPU.

(16 CPUs x 5)/2 = 40 cortafuegos VM-50

Más allá de cumplir con los Requisitos del sistema VM-Series mínimos, no se requiere configuración adicional para aprovechar la sobresuscripción. Implemente cortafuegos VM-Series de forma habitual y la sobresuscripción de recursos se produce automáticamente. Al planificar su implementación, considere otras funciones, como conmutadores virtuales y máquinas invitadas en el host que requieren sus propios recursos de hardware.



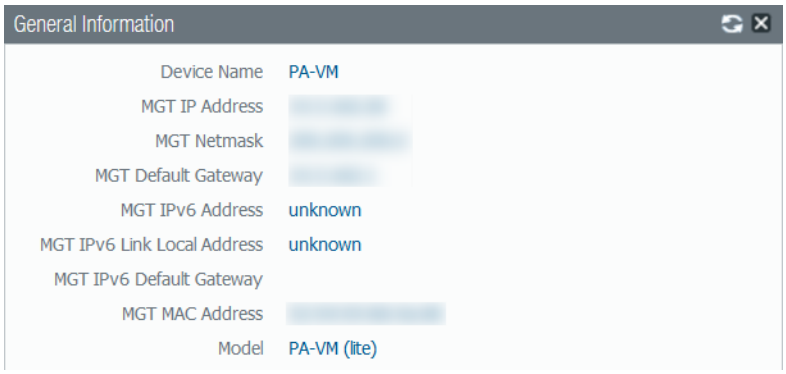
Modo Lite de VM-50

El VM-50 estándar, aunque el modelo más pequeño de VM-Series, requiere más recursos de los disponibles en algunos entornos. El modo Lite de VM-50 brinda una alternativa para los entornos en los

 ©2024 Palo Alto Networks, Inc.

cuales los recursos de hardware están restringidos. El VM-50 Lite requiere 4,5GB de memoria en lugar de 5,5GB que requiere la VM-50 estándar. El VM-50 Lite usa la misma licencia que VM-50 estándar pero viene en modo Lite cuando se le asigna 4,5GB de RAM.

- *En las implementaciones de alta disponibilidad, ambos cortafuegos VM-Series deben contar con licencia igual que VM-50 Lite para evitar problemas de falta de coincidencia de capacidad. En el caso de una falta de coincidencia de licencia de capacidad, el VM-50 (no Lite) se considera como el modelo que tiene mayor capacidad; el VM-50 deja de funcionar mientras que el VM-50 Lite sigue siendo funcional.*
- *El modo VM-50 Lite no admite tramas gigantes; los modos VM-50 y VM-50 Lite no son compatibles con el aprendizaje automático en línea de WildFire.*



Tipos de licencia del modelo VM-Series

Las nuevas licencias de capacidad (créditos NGFW que no son de software) ya no están disponibles para la venta. Sin embargo, cuenta con renovaciones de un (1) año para licencias de capacidad (perpetuas y de tiempo limitado).

Las siguientes licencias y suscripciones están disponibles para el cortafuegos VM-Series:

- **Licencia de capacidad**: El cortafuegos VM-Series requiere una licencia básica, también llamada *licencia de capacidad*, para habilitar el número de modelo (VM-50, VM-100, VM-200, VM300, VM-500, VM-700, o VM-1000-HV) y las capacidades asociadas en el cortafuegos. Las licencias de capacidad se incluyen en un paquete y pueden ser perpetuas o temporales:
  - **Licencia ilimitada**: una licencia sin fecha de vencimiento le permite usar el cortafuegos VM-Series en la capacidad con licencia por tiempo indefinido. Las licencias ilimitadas están disponibles únicamente para la licencia de capacidad de VM-Series.
  - **Licencia por período**: una licencia por período le permite usar el cortafuegos VM-Series por un período específico de tiempo. Tiene una fecha de vencimiento y se le solicitará renovar la licencia antes de que está se venza. Las licencias por período están disponibles para las licencias de capacidad, los derechos de asistencia y las suscripciones.
- **VM-Series ELA**: para entidades de alto crecimiento, el acuerdo de licencia empresarial (Enterprise Licensing Agreement, ELA) de VM-Series proporciona una opción de licencia con precio fijo que

 ©2024 Palo Alto Networks, Inc.

permite la implementación ilimitada de los cortafuegos VM-Series con BYOL. El ELA se ofrece por uno o tres años sin conciliación al final del período.

Hay dos opciones de VM-series ELA:

- Si adquirió el VM-Series ELA antes del 4 de diciembre de 2018, tiene el legacy VM-Series ELA que incluye su elección de un solo modelo VM-Series en cualquier hipervisor compatible o entorno de nube pública. Con este ELA, recibe un código de autorización para una licencia que le brinda suscripciones de capacidad, asistencia técnica, GlobalProtect, Filtrado de URL de PAN-DB, Prevención de amenazas y WildFire para cada instancia del cortafuegos VM-Series. También obtiene implementaciones ilimitadas del dispositivo virtual de Panorama incluido con una licencia de gestión de dispositivos para 1000 cortafuegos en cada uno.

  Palo Alto Networks comenzó a eliminar la antigua VM-Series ELA el 16 de abril de 2019. Los clientes de licencias empresariales existentes serán notificados por su representante de asistencia técnica cuando su cuenta se migre al ELA de múltiples modelos. Los tokens de licencia se distribuirán de acuerdo con el acuerdo de suscripción del cortafuegos VM-Series; no es necesario realizar ninguna acción adicional para el funcionamiento continuo de sus cortafuegos. Si le gustaría Administre los tokens de licencia ELA de VM-Series, debe designar un administrador de ELA. Solo un rol de superusuario en el Portal de atención al cliente (CSP) de Palo Alto Networks puede asignar un administrador de ELA.
- Los Acuerdo de licencia empresarial de VM-Series (ELA de múltiples modelos) que compre después del 4 de diciembre de 2018 (ya sea como una nueva compra o como una recompra de la antigua serie ELA de VM-Series) se denomina ELA de múltiples modelos de VM-Series e incluirá la mayoría de los modelos de la cartera de cortafuegos VM-Series, junto con GlobalProtect , Filtrado de URL de PAN-DB, Prevención de amenazas, suscripciones de WildFire y derechos de asistencia técnica. También obtiene implementaciones ilimitadas del dispositivo virtual de Panorama con una licencia de gestión de dispositivos para 1000 cortafuegos en cada uno.

Licencias de cortafuegos VM-Series para nubes públicas

La estrategia de licencia del cortafuegos VM-Series es la misma para AWS, Azure y Google Cloud Platform. Existen diferentes tipos de licencias (consulte Tipos de licencias: cortafuegos VM-Series) y los métodos de licencias Licencia existente y Pago por consumo:

- **Licencia existente (BYOL)**: una licencia que se adquiera a un socio, revendedor o directamente en Palo Alto Networks. La licencia BYOL admite licencias de capacidad individual, licencias de asistencia y paquetes de suscripción.
  - En las licencias BYOL, debe aplicar el código de autenticación luego de implementar el cortafuegos VM-Series.
  - Una paquete de licencia BYOL tiene un código de autenticación único que puede incluir en el paquete de arranque (consulte Arranque del cortafuegos VM-Series). Todas las suscripciones incluidas en el paquete tienen licencia cuando se inicia el cortafuegos.



Una licencia BYOL para el cortafuegos VM-Series en OCI GovCloud requiere PAN-OS 10.1.2 o posterior para los modos FIPS y no FIPS.

 ©2024 Palo Alto Networks, Inc.

- **Pago por consumo (Pay-as-you-go, PAYG)**: también llamada licencia *basada en el uso* o de *pago por uso*. Las licencias de PAYG se pueden comprar en su proveedor de nube:
  - AWS: Compre desde AWS Marketplace. Admite opciones de PAYG anual y por hora.
  - Azure: Compre desde Azure Marketplace. Admite la opción de PAYG por hora.
  - Google Cloud Platform: Compre desde Google Cloud Platform Marketplace. Google Cloud Platform es compatible con la opción de pago por minuto PAYG.
  - Oracle Cloud Infrastructure: (PAN-OS 10.0.3 o posterior) Adquiérala en Oracle Cloud Marketplace.

    La licencia VM-Series en OCI PAYG no es compatible con el modelo VM-100.

  Con los paquetes de licencias de PAYG, el cortafuegos posee una licencia previa y ya está listo para usar tan pronto como lo implemente; no recibirá un código de autenticación. Cuando detenga o finalice el cortafuegos desde la consola de Cloud, las licencias de PAYG se suspenden o finalizan.

  Una licencia PAYG aplica una licencia de capacidad Vm-Series basada en el hardware asignado a la instancia. La instancia PAYG verifica la cantidad de recursos de hardware disponibles para la instancia y aplica la mayor licencia de capacidad de cortafuegos VM-Series permitida para los recursos disponibles. Por ejemplo, si la instancia tiene 2 vCPU y 16 GB de memoria, se aplica una licencia de capacidad VM-100 en función del número de vCPU. Sin embargo, si la instancia tiene 16 vCPU y 16 GB de memoria, se aplica una licencia VM-500 en función de la cantidad de memoria. Para obtener más información sobre los requisitos de recursos del modelo VM-Series, consulte Requisitos del sistema para VM-Series.

  La instalación de una versión anterior de PAN-OS no es compatible con una instancia de cortafuegos PAYG que se implementó inicialmente con PAN-OS 9.1.2. Las instancias de cortafuegos implementadas antes de PAN-OS 9.1.2 pueden cambiar a versiones anteriores de PAN-OS.

  Las licencias de PAYG están empaquetadas de la siguiente manera:

Funciones de la licencia	Paquete 1	Paquete 2	Paquete 3
Licencia de capacidad de cortafuegos 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
Soporte premium	✓	✓	✓
Prevención contra amenazas (AV, IPS y prevención de malware)	✓	✓	
GlobalProtect		✓	✓
PAN-DB URL Filtering		✓	
WildFire		✓	✓
DNS Security		✓	✓

 ©2024 Palo Alto Networks, Inc.

Funciones de la licencia	Paquete 1	Paquete 2	Paquete 3
Filtrado de URL avanzado			✓
Prevención avanzada de amenazas			✓

Cuando se utiliza la CLI del cortafuegos VM-Series para ver su licencia PAYG en vigor, el comando ***show system info*** *(mostrar información del sistema) muestra un valor diferente del resultado que se muestra para el comando* ***request license info*** *(solicitar información de licencia). Para las versiones de PAN-OS 9.1.1 y anteriores, el comando* ***request license info*** *siempre muestra el modelo como VM-300, independientemente del modelo de VM-series que se haya aplicado.*

No puede cambiar entre las licencias PAYG y BYOL. Para pasar de PAYG a BYOL, comuníquese con su socio de ventas o representante de ventas de Palo Alto Networks para comprar una licencia de BYOL y obtener un código de autenticación de BYOL que puede usar para activar la licencia de su cortafuegos. Si ha implementado su cortafuegos y desea cambiar la licencia, consulte Cambio entre las licencias BYOL y PAYG.

Si tiene una copia de evaluación del cortafuegos VM-Series y desea convertirla en una copia con licencia completa (comprada) para el mismo tipo de licencia (BYOL a BYOL), puede desactivar la licencia de evaluación y activar la licencia adquirida. Consulte Actualización del cortafuegos VM-Series *para obtener instrucciones.*

Acuerdo de licencia empresarial de VM-Series (ELA de múltiples modelos)

El Acuerdo de licencia empresarial de VM-Series (ELA de VM-Series) es un acuerdo de licencia integral de uno o tres años que le permite comprar cortafuegos VM-Series, junto con las suscripciones a GlobalProtect, Filtrado de URL de PAN-DB, Prevención de amenazas, WildFire y Seguridad DNS. También incluye un derecho a asistencia técnica y una licencia de gestión de dispositivos para Panorama. El ELA de múltiples modelos de VM-Series proporciona una gestión de licencias simplificada con un único contrato que le permite implementar cualquier modelo del cortafuegos VM-Series que satisfaga las necesidades de seguridad de su empresa.

Cuando compra el ELA de múltiples modelos de VM-Series, hace una previsión del número de cortafuegos que necesitará durante el período de su suscripción. De acuerdo con su previsión y una asignación adicional que se adapta al crecimiento futuro, su cuenta en el Portal de atención al cliente (CSP) se acredita con un conjunto de tokens de licencia que le permite implementar cualquier modelo del cortafuegos VM-Series. Dependiendo del modelo de cortafuegos y el número de cortafuegos que implemente, se deducirá una cantidad específica de tokens de su grupo de tokens de licencia disponible. Los tokens utilizados de su cuenta se calculan en función del valor de cada modelo de cortafuegos:

- VM-50—10 tokens
- VM-100—25 tokens
- VM-300—50 tokens
- VM-500—140 tokens
- VM-700—300 tokens

 ©2024 Palo Alto Networks, Inc.

Con el ELA de VM-Series no hay un vencimiento real al final del término, lo que significa que no se le facturará de manera retroactiva incluso si implementa más cortafuegos que su previsión original. Por lo tanto, para equilibrar la flexibilidad con la responsabilidad, los términos de uso del ELA de VM-Series incluyen un período limitado y sin límites que explica cómo puede consumir tokens e implementar cortafuegos según sea necesario. Para obtener más detalles, consulte los Condiciones del ELA. Los cortafuegos VM-Series que implementa con el ELA de VM-Series no tienen una licencia perpetua y, una vez finalizado el periodo, debe renovar el acuerdo para ampliar el derecho a asistencia y obtener acceso continuo a las actualizaciones del software y versiones de contenido en los cortafuegos.

Con la función de administrador de ELA en el CSP, puede transferir o dividir los tokens de licencias con otros administradores que pertenecen a diferentes departamentos y cuentan con sus propias cuentas de CSP. Este uso compartido permite a otros administradores de su empresa implementar el cortafuegos VM-Series según demanda, siempre y cuando tengan tokens disponibles en sus respectivas cuentas CSP. Consulte Administre los tokens de licencia ELA de VM-Series para invitar a otros administradores a compartir tokens de ELA e implementar cualquier modelo del cortafuegos VM-Series que cumpla con las necesidades de seguridad de su empresa. También puede recuperar tokens para eliminar cuentas CSP del ELA de VM-Series si desea redistribuir tokens a medida que cambian las necesidades de su organización.

Vea los vídeos de ELA de múltiples modelo para VM-Series

- Administre los tokens de licencia ELA de VM-Series
- Aceptar la ELA de VM-Series

Administre los tokens de licencia ELA de VM-Series

El Acuerdo de licencia empresarial de VM-Series (ELA de múltiples modelos) (ELA de VM-Series) le brinda la flexibilidad de tener un solo contrato que puede compartir con otros administradores de su empresa. Debe contar con el rol de superusuario en el Portal de atención al cliente (CSP) de Palo Alto Networks para activar el ELA y, al activar el código de autorización de ELA, usted hereda el rol de administrador de ELA en el CSP.

Con el rol de administrador de ELA, puede administrar el conjunto de tokens de licencia disponible para implementar cortafuegos y suscripciones de VM-Series incluidas en el acuerdo. Puede invitar a otros administradores a compartir los tokens del ELA de VM-Series, ceder qué modelos y cuántas instancias de cortafuegos de la VM-Series están disponibles para cada administrador, así como eliminar las cuentas de CSP de su ELA de VM-Series. Dependiendo de lo que asigne para cada beneficiario, recibirán una cantidad específica de tokens que luego podrán usar para implementar los cortafuegos VM-Series.

Las compras y cesiones adicionales no se añaden directamente al número de cortafuegos VM-Series disponibles en una cuenta CSP; en su lugar, los tokens de licencia de ELA se añaden al conjunto de tokens ELA de VM-Series. Los tokens de licencia ELA se pueden asignar posteriormente, por el administrador de ELA, a una cuenta CSP determinada para aumentar la cantidad de cortafuegos VM-Series disponibles.

STEP 1 | (Solo para clientes del ELA de VM-Series heredada) Designe un administrador de ELA para gestionar los tokens.

Los clientes de licencias empresariales existentes que han migrado al ELA de múltiples modelos deben designar un administrador de ELA para gestionar los tokens de licencia de ELA de VM-Series. Después de la conversión, no es necesaria ninguna otra acción para continuar con el funcionamiento de sus cortafuegos, sin embargo, no podrá (re)asignar tokens para cortafuegos en proceso de

 ©2024 Palo Alto Networks, Inc.

implementación hasta que se haya asignado un administrador de ELA. Solo un administrador con un rol de superusuario en el CSP tiene la capacidad de designar un administrador de ELA, que a su vez, puede gestionar tokens o ceder tokens a otros administradores.

1. Inicie sesión en el Portal de atención al cliente (CSP) de Palo Alto Networks.
2. Seleccione **Members (Miembros)** > **Manage Users (Gestionar usuarios)**.
3. Haga clic en el icono de lápiz debajo de **Actions (Acciones)** para editar el usuario al que desea asignar el rol de administrador de ELA.
4. Seleccione **ELA Administrator (Administrador de ELA)** y luego haga clic en la marca de verificación para añadir el nuevo rol al usuario seleccionado.
5. Continúe al paso 3.

STEP 2 | Active el código de autorización de ELA.

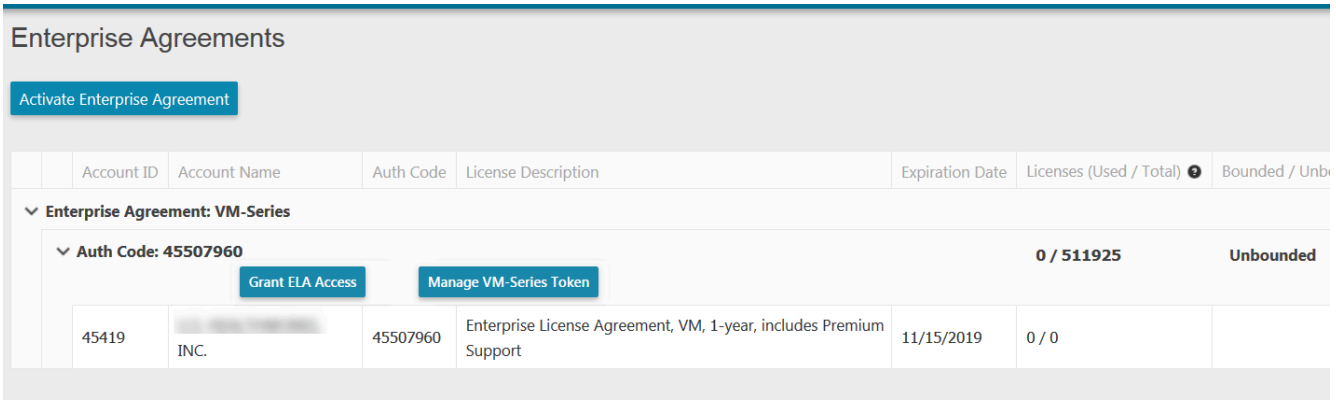
El usuario administrativo que activa el ELA hereda el rol de administrador y superusuario de ELA en el CSP y tiene la capacidad de gestionar los tokens o ceder los tokens a otros administradores.

1. Inicie sesión en el Portal de atención al cliente (CSP) de Palo Alto Networks.
2. Seleccione **Products (Productos)** > **Enterprise Agreements (Acuerdos empresariales)** > **Activate Enterprise Agreement (Activar acuerdo empresarial)**.
3. Introduzca el **Authorization code (Código de autorización)** y haga clic en **Agree and Submit (Aceptar y enviar)** el EULA.

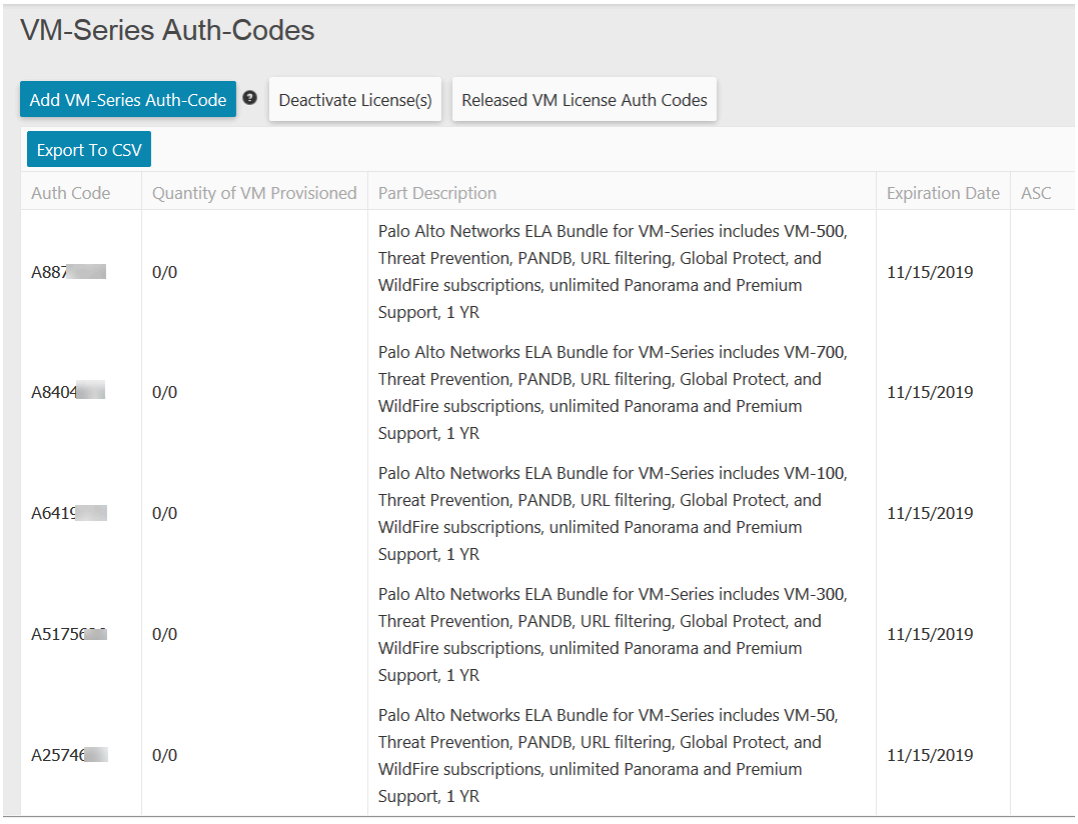
   Verifique que el código de autorización esté registrado en su cuenta bajo Acuerdos empresariales: VM-Series. La página muestra el Código de autenticación, el ID de la cuenta, el Nombre de la cuenta, la Descripción de la licencia, la Fecha de caducidad, el número de

 ©2024 Palo Alto Networks, Inc.

Licencias (utilizadas/totales) que tiene, y cuántas están disponibles para implementar dentro del período limitado y sin límites del acuerdo.



4. Seleccione **Products (Productos)** > **VM-Series Auth-Codes (Códigos de autorización de VM-Series)** para ver los códigos de autorización para la implementación de cada modelo del cortafuegos VM-Series y las suscripciones asociadas incluidas con el ELA.

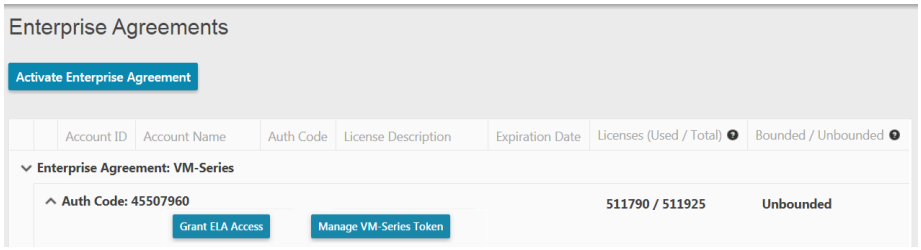


STEP 3 | Conceda acceso ELA a otros administradores en su empresa.

Esta capacidad le permite compartir el ELA de VM-Series con otros administradores dentro de su empresa o departamento para que puedan implementar los cortafuegos VM-Series según demanda.

 ©2024 Palo Alto Networks, Inc.

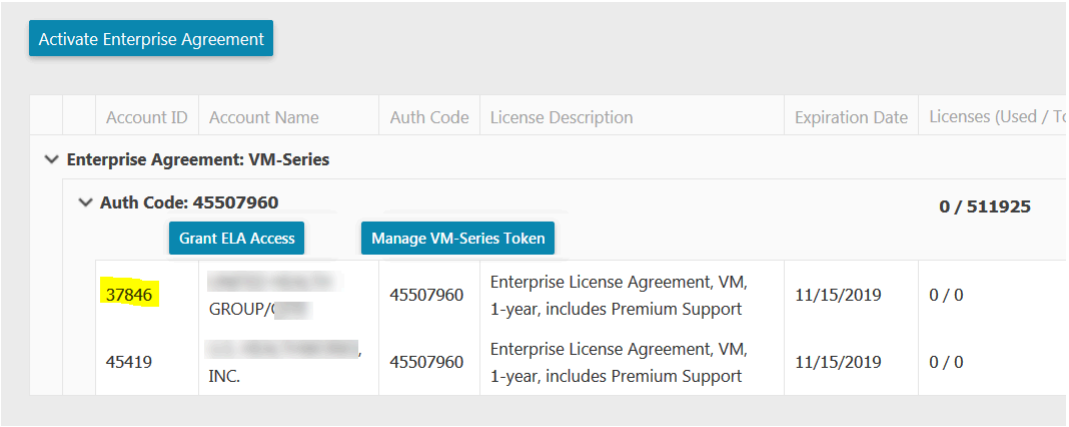
Como administrador de ELA, puede proporcionar acceso a otros usuarios que estén registrados con una dirección de correo electrónico en el CSP.



1. En **Products (Productos)** > **Enterprise Agreements (Acuerdos empresariales)**, seleccione **Grant ELA Access (Proporcionar acceso de ELA)**.
2. Introduzca la dirección del **Destination Email (Correo electrónico de destino)** del administrador al que desea invitar.

   La dirección de correo electrónico de destino que introduzca arriba debe ser de un usuario registrado en el CSP con un rol de superusuario para que pueda iniciar sesión y aceptar la cesión. Si la dirección de correo electrónico no está registrada en el CSP, primero debe crear una nueva cuenta para el usuario en **Members (Miembros)** > **Create New User (Crear nuevo usuario)**.
3. Seleccione **Notify User (Notificar al usuario)** para enviar un correo electrónico de notificación a la dirección de correo electrónico que introdujo.

   El destinatario debe iniciar sesión en el CSP para Aceptar la ELA de VM-Series. Después de que el receptor acepta la concesión, el ID de cuenta está disponible en **Products (Productos)** > **Enterprise Agreements (Acuerdos empresariales)** como se muestra en la siguiente captura de pantalla.



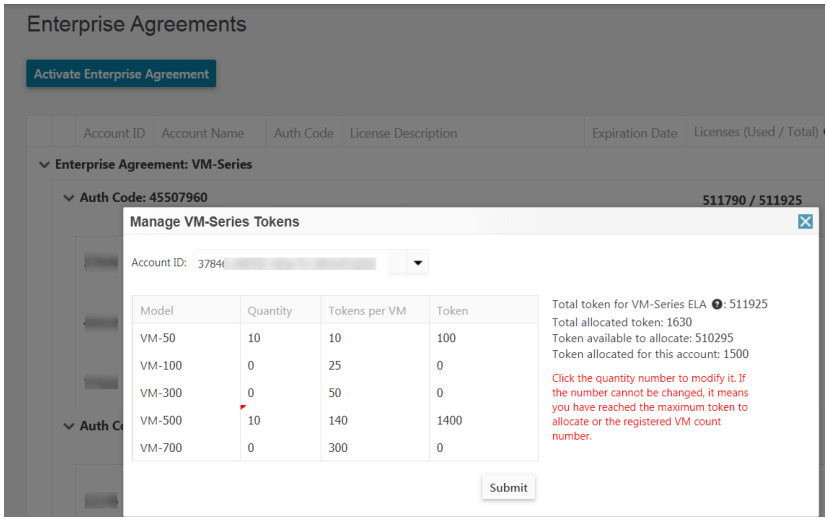
STEP 4 | Asignación de tokens para la implementación de cortafuegos.

1. Seleccione **Products (Productos)** > **Enterprise Agreements (Acuerdos empresariales)** > **Manage VM-Series Token (Gestionar tokens de VM-Series)**.

   Para cada ID de cuenta, puede especificar el número de cortafuegos por modelo que desea asignar. En función de la cantidad y el modelo de cortafuegos, el número de tokens se calcula

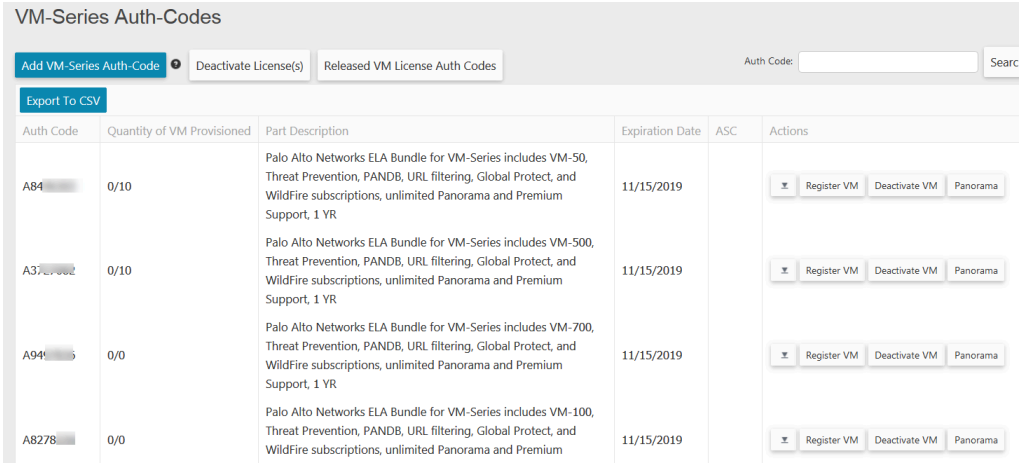
 ©2024 Palo Alto Networks, Inc.

automáticamente y queda disponible para su uso. En este ejemplo, está permitiendo 10 instancias de VM-50 y 10 de VM-500.



2. Verifique que el número exacto de instancias de cortafuegos estén depositados en la cuenta.

   Seleccione **Products (Productos)** > **VM-Series Auth-Code (Código de autenticación de VM-Series)** para confirmar los códigos de autenticación asignados. En este ejemplo, la cuenta tiene la capacidad de aprovisionar 10 instancias de VM-50 y 10 de VM-500. A medida que los destinatarios implementan cortafuegos, el número de tokens se deduce del conjunto total disponible, y puede ver el número de instancias de cortafuegos que han aprovisionado como una proporción del número total que asignó para ellos. A medida que sus necesidades de seguridad evolucionan, tiene la flexibilidad de asignar más cantidades y permitir el acceso a un modelo de cortafuegos VM-Series diferente, siempre que tenga tokens disponibles.



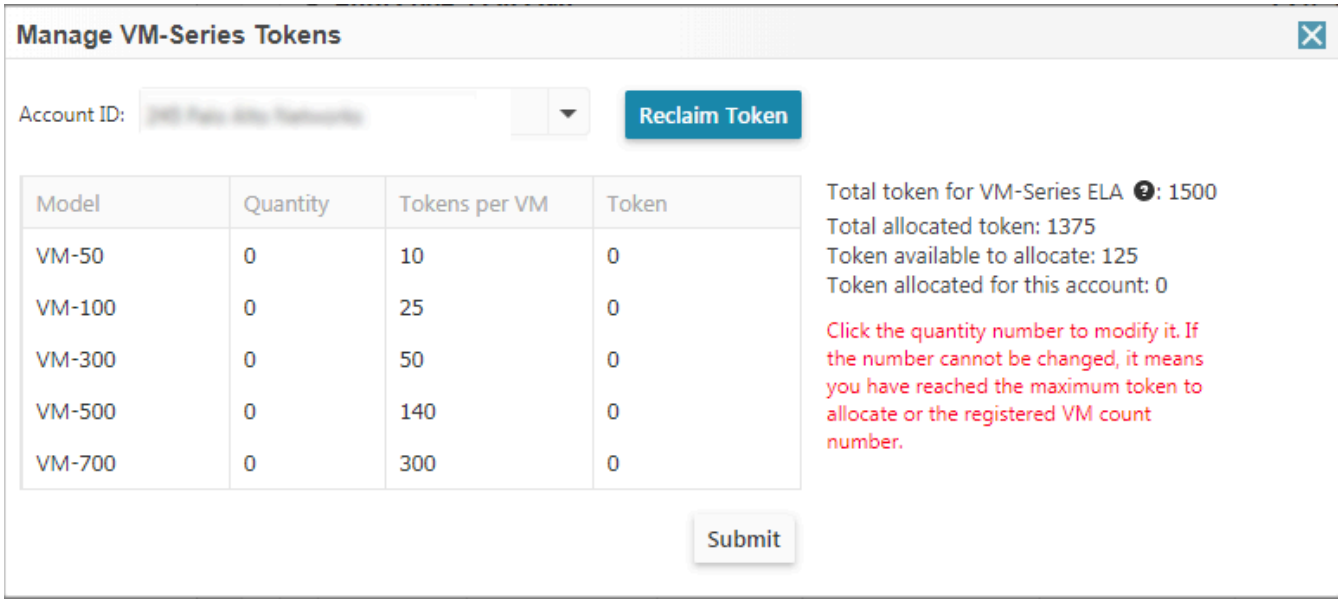
 ©2024 Palo Alto Networks, Inc.

STEP 5 | Elimine una cuenta CSP del ELA de VM-Series para recuperar tokens.

No puede recuperar una parte de los tokens asignados a una cuenta CSP. Cuando recupera tokens, elimina una cuenta CSP en su totalidad del ELA de VM-Series y reasigna todos los tokens asociados al conjunto de tokens.

1. Verifique que todos los tokens asociados con la cuenta CSP que desea eliminar no estén siendo utilizados por los cortafuegos VM-Series. Desactive los cortafuegos VM-Series según sea necesario para aprovisionar tokens para su eliminación.
2. Seleccione **Products (Productos)** > **Enterprise Agreements (Acuerdos empresariales)** > **Manage VM-Series Token (Gestionar tokens de VM-Series)**.

   Seleccione el ID de la cuenta de la que desea recuperar tokens y haga clic en **Reclaim Token (Recuperar token)**. Si hay tokens disponibles para recuperar, recibirá una confirmación de la correcta eliminación.



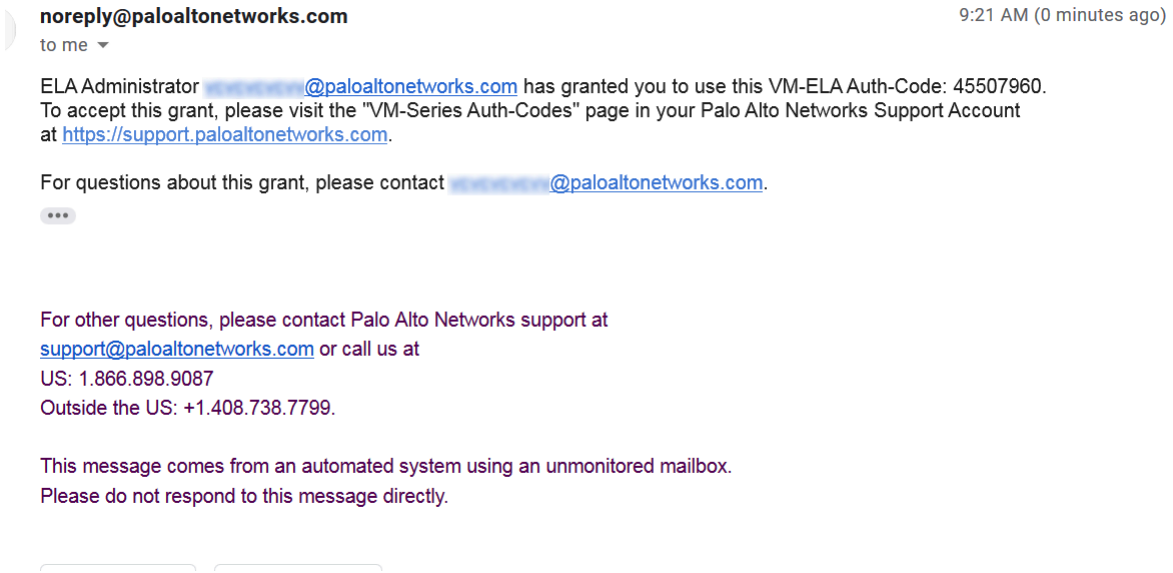
Aceptar la ELA de VM-Series

Si su empresa ha adquirido un ELA de VM-Series, su administrador de ELA puede invitarle a compartir el contrato y compartir el conjunto de tokens de licencia para que tenga acceso a los códigos de autenticación del cortafuegos VM-Series que le permiten implementar cortafuegos VM-Series a demanda. Cuando recibe una concesión para acceder a la ELA de VM-Series, recibe una notificación por correo electrónico que incluye un enlace para iniciar sesión en el Portal de atención al cliente (CSP) de Palo Alto Networks y debe aceptar los términos de uso. Después de aceptar los términos de uso de ELA, el administrador de ELA puede asignar qué modelos de cortafuegos VM-Series va a usar y a cuántos tiene derecho; el número correspondiente de tokens ELA de VM-Series se depositarán en su cuenta.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Revise su bandeja de entrada de correo electrónico para ver la notificación de cesión.

La notificación incluye la dirección de correo electrónico del administrador de ELA que le ha invitado a compartir el ELA de VM-Series.



STEP 2 | Aceptar la cesión.

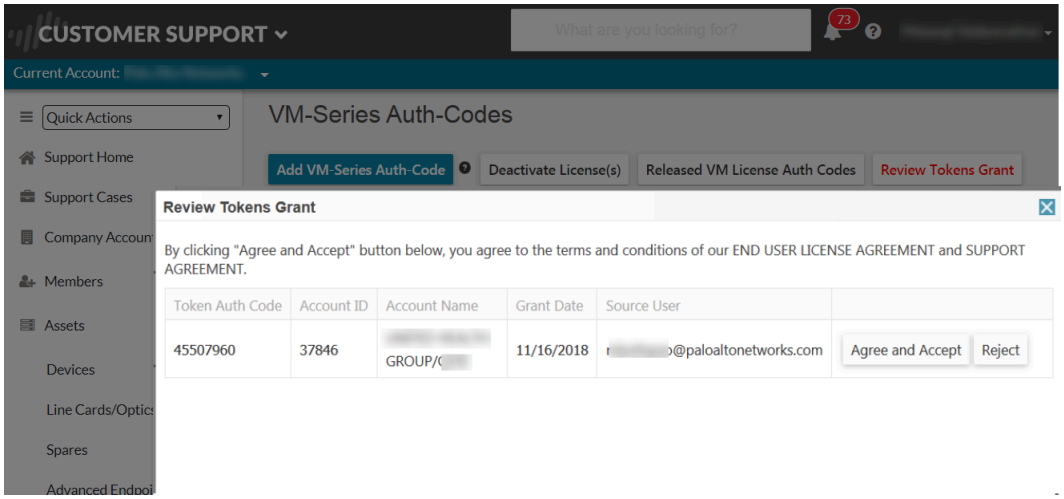
Debe revisar los términos, y aceptar el EULA y el acuerdo de asistencia técnica antes de que el administrador de ELA pueda asignar tokens que le permitan implementar cortafuegos VM-Series.

1. Inicie sesión en el Portal de atención al cliente (CSP) de Palo Alto Networks.
2. Seleccione **VM-Series Auth Codes (Códigos de autenticación de VM-Series)** para **Review Tokens Grant (Revisar cesión de tokens)**.

   Debe aceptar el EULA y el acuerdo de asistencia técnica para aceptar la cesión. Si lo rechaza, el administrador de ELA que le otorgó la subvención recibe una notificación por correo electrónico de que rechazó la cesión. Asegúrese de informar al administrador de ELA de que ha aceptado

 ©2024 Palo Alto Networks, Inc.

la cesión para que pueda asignar los modelos de cortafuegos VM-Series y el número que puede implementar.



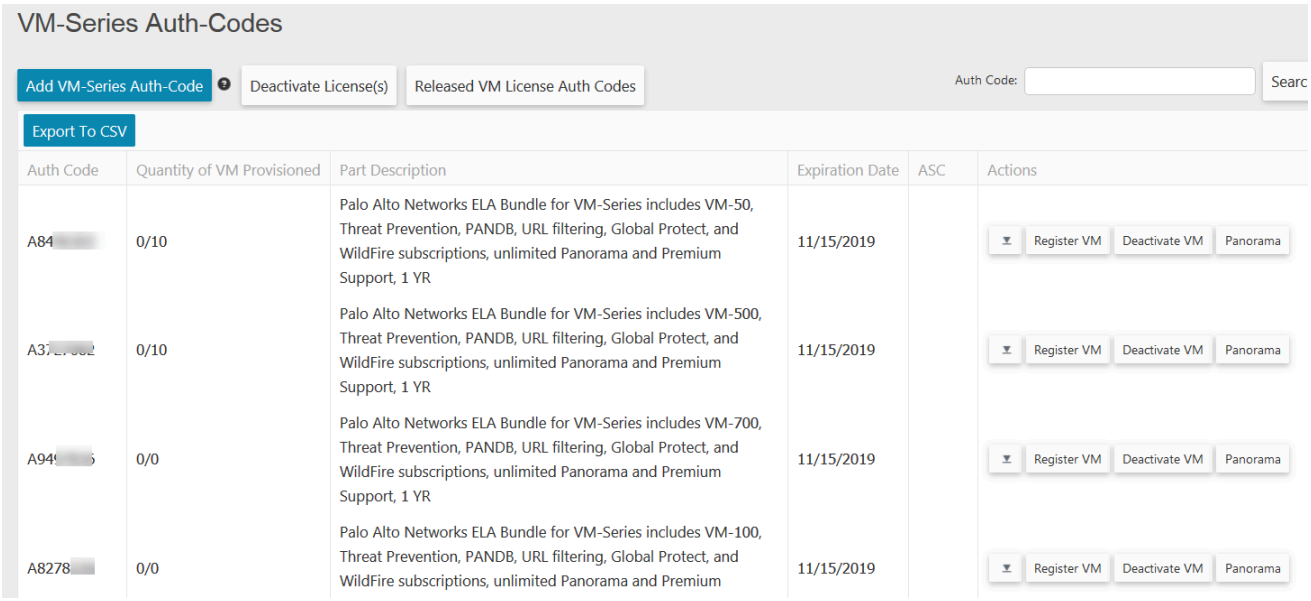
Si pertenece a varias cuentas en el CSP y acepta accidentalmente la cesión en la cuenta incorrecta, debe solicitar al administrador de ELA que le reenvíe la cesión. No comience a usar el código de autenticación para aprovisionar cortafuegos hasta que acepte la cesión en la cuenta correcta.

STEP 3 | Compruebe qué modelos de VM-Series y cuántos se asignan para usted.

Después de que el administrador de ELA asigne los modelos de cortafuegos VM-Series y el número de instancias que puede aprovisionar, puede seleccionar **Assets (Activos)** > **VM-Series Auth Codes (Códigos de autenticación de VM-Series)** para ver qué modelos y cuántos de cada uno de estos están asignados para usted. Por ejemplo, la cesión en la siguiente captura de pantalla muestra los códigos

 ©2024 Palo Alto Networks, Inc.

de autenticación que le permiten implementar 10 instancias de cada uno de los modelos VM-50 y VM-500.



A medida que implementa cortafuegos y los registra en el CSP, la cantidad de cortafuegos aprovisionados se incrementa. El **Quantity of VM Provisioned (Número de VM aprovisionados)** muestra la relación de aprovisionado a total disponible para cada modelo.

Activar licencias del modelo VM-Series

Para activar la licencia en su cortafuegos VM-Series, deberá haber implementado el cortafuegos VM-Series y haber completado la configuración inicial. Para implementar el cortafuegos, consulte Implementaciones de VM-Series.

Use las instrucciones de esta sección para todos los modelos BYOL que incluyen AWS, Azure y la nube pública de Google. Para las licencias basadas en el uso en nubes públicas, no es necesario que active la licencia. Debe registrar el modelo basado en el uso del cortafuegos VM-Series para nubes públicas (sin código de autenticación) para activar su derecho a la asistencia premium.

Para los modelos basados en el uso del cortafuegos VM-Series en AWS Marketplace, se admiten instancias con ID de instancia de AWS cortos y largos.

Hasta que haya activado la licencia en el cortafuegos VM-Series, el cortafuegos no tendrá un número de serie, la dirección MAC de las interfaces del plano de datos no serán únicas y sólo se admitirá un número mínimo de sesiones. Como las direcciones MAC no son únicas hasta que el cortafuegos recibe licencia, para evitar problemas por superposición de direcciones MAC asegúrese de no tener múltiples cortafuegos VM-Series sin licencia.

Cuando activa la licencia, el servidor de licencias usa la UUID y la Id. de la CPU de la máquina virtual para generar un número de serie único para el cortafuegos VM-Series. El código de autenticación de capacidad, junto con el número de serie, se usa para validar su autorización.

 ©2024 Palo Alto Networks, Inc.

*La pestaña de **Licencia** del cortafuegos VM-Series muestra un archivo de licencia VM-300 estándar para todos los modelos de licencia. Para encontrar la información específica de su modelo de licencia, consulte la información del sistema en la interfaz de usuario o use la CLI para ver la **`información del sistema`**.*

Después de conceder la licencia de un cortafuegos VM-Series, si necesita eliminar y volver a implementar el cortafuegos VM-Series, asegúrese de Desactivar las licencias en el cortafuegos. Desactivar la licencia le permite transferir las licencias activas a una nueva instancia del cortafuegos VM-Series sin la ayuda del soporte técnico.

- Activación de la licencia para el cortafuegos VM-Series (versión independiente)
- Activación de la licencia para el cortafuegos VM-Series para VMware NSX
- Solución de problemas de activación de licencia

Activación de la licencia para el cortafuegos VM-Series (versión independiente)

Si ha elegido no usar el flujo de trabajo de arranque utilizando un paquete de suscripción, debe implementar el cortafuegos VM-Series y completar la configuración inicial antes de poder activar la licencia en su cortafuegos VM-Series.

- Acceso directo a internet
- Sin acceso a Internet

- Acceso directo a internet

  Para activar la licencia, el cortafuegos debe estar configurado con una dirección IP, máscara de red, puerta de enlace predeterminada y dirección IP de servidor DNS.

  El cortafuegos debe tener una configuración DNS válida y tener conectividad de red para acceder al servidor de licencias de Palo Alto Networks.

  1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y seleccione el enlace **Retrieve license keys from license server (Recuperar claves de licencia del servidor de licencias)**.
  2. El cortafuegos se conectará con el servidor de actualización (updates.paloaltonetworks.com), descargará la licencia y se reiniciará automáticamente.
  3. Vuelva a iniciar sesión en la interfaz web y confirme que **Dashboard (Panel)** muestra un número de serie válido. Si aparece el término **Desconocido**, significa que el dispositivo no tiene licencia.
  4. En **Device (Dispositivo)** > **Licenses (Licencias)**, compruebe que se añade la licencia **PA-VM** al dispositivo.

     Si ve un mensaje de error, consulte la Solución de problemas de activación de licencia.

- Sin acceso a Internet

  1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y haga clic en el vínculo **Activate Feature using Auth Code (Activar función usando el código de autenticación)**.
  2. Haga clic en **Download Authorization File (Descargar archivo de autorización)** y descargue el archivo **authorizationfile.txt** en la máquina cliente.
  3. Copie el archivo **authorizationfile.txt** en un ordenador que tenga acceso a internet e inicie sesión en el portal de asistencia técnica. Haga clic en el vínculo **My VM-Series Auth-Codes**

 ©2024 Palo Alto Networks, Inc.

(Mis códigos de autenticación de VM-Series) y seleccione el código de autenticación aplicable en la lista y haga clic en el vínculo **Register VM (Registrar VM)**.

4. Cargue el archivo de autorización en la pestaña **Register Virtual Machine (Registrar máquina virtual)**. Seleccione la versión de PAN-OS y el hipervisor en el que ha implementado el cortafuegos para completar el proceso de registro. El número de serie de su cortafuegos VM-Series se añadirá a sus registros de cuenta.
5. Vaya a **Products (Productos)** > **Assets (Activos)** > **NGFW** y busque el dispositivo VM-Series que acaba de registrar, y haga clic en el enlace **PA-VM**. Esto descargará la clave de licencia de VM-Series en la máquina cliente.
6. Copie la clave de licencia en la máquina que puede acceder a la interfaz web del cortafuegos VM-Series y desplácese hasta **Device (Dispositivo)** > **Licenses (Licencias)**.

   Las claves de licencia se deben instalar a través de la interfaz web. El cortafuegos no es compatible con la instalación de la clave de licencia a través de SCP o FTP.
7. Haga clic en **Manually Upload License (Subir clave de licencia manualmente)** e introduzca la clave de licencia. Cuando la licencia de capacidad se haya activado en el cortafuegos se producirá el reinicio.
8. Inicie sesión en el dispositivo y confirme que **Dashboard (Panel)** muestra un número de serie válido y que la licencia muestra **PA-VM** en la pestaña **Device (Dispositivo)** > **Licenses (Licencias)**.

Activación de la licencia para el cortafuegos VM-Series para VMware NSX

Panorama sirve como punto central de administración de los cortafuegos VM-Series para NSX de VMware y el proceso de activación de licencia es automático cuando Panorama tiene acceso directo a Internet. Panorama se conecta con el servidor de actualizaciones de Palo Alto Networks para recuperar las licencias, y cuando se implementa un nuevo cortafuegos VM-Series para NSX, se comunica con Panorama para obtener la licencia. Si Panorama no está conectado a internet, deberá licenciar manualmente cada instancia del cortafuegos VM-Series para que el cortafuegos puede conectarse con Panorama.

Para esta solución integrada, el código de autenticación (por ejemplo, PAN-VM-1000-HV-SUB-BND-NSX2) incluye licencias para la prevención de amenazas, filtrado de URL, suscripciones a WildFire y asistencia premium para el período requerido.

Para activar la licencia, debe haber completado las siguientes tareas:

- Registrado el código de autenticación en la cuenta de asistencia. Si no registra el código de autenticación, el servidor de licencias no podrá crear una licencia.
- Introduzca el código de autenticación en la definición de servicios de Panorama. En Panorama, seleccione **VMware Service Manager (Administrador de servicios VMWare)** para añadir el **Authorization Code (Código de autorización)** a la **VMware Service Definition (Definición de servicio VMware)**.

  Si ha adquirido un código de autenticación de prueba, puede activar la licencia hasta en un máximo de 5 cortafuegos VM-Series con licencias de capacidad VM-1000-HV durante un período de 30 o 60 días. Dado que esta solución le permite implementar un cortafuegos VM-Series por host ESXi, el clúster de ESXi puede incluir un máximo de 5 hosts ESXi si se usa una licencia de prueba.

 ©2024 Palo Alto Networks, Inc.

El siguiente proceso de activación de licencias es manual. Si tiene un script personalizado o un servicio de orquestación, puede usar la API de licencias para automatizar el proceso de recuperación de las licencias para los cortafuegos VM-Series.

- Activación de licencias en cortafuegos VM-Series en NSX cuando Panorama tiene acceso a Internet
- Activación de licencias en cortafuegos VM-Series en NSX cuando Panorama no tiene acceso a Internet
- Solución de problemas de activación de licencia

Activación de licencias en cortafuegos VM-Series en NSX cuando Panorama tiene acceso a Internet

Complete el siguiente procedimiento para activar el cortafuegos VM-Series para NSX cuando Panorama tenga acceso a Internet.

STEP 1 | Verifique que el nuevo cortafuegos VM-Series está conectado a Panorama.

1. Inicie sesión en Panorama.
2. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** y compruebe que el cortafuegos se muestra como Conectado.

STEP 2 | Verifique que todos los cortafuegos tienen licencia.

Seleccione **Panorama** > **Device Deployment (Implementación de dispositivos)** > **Licenses (Licencias)** y verifique que Panorama tiene el código de autenticación coincidente y las licencias aplicadas para cada cortafuegos.

Si no ve las licencias, haga clic en **Refresh (Actualizar)**. Seleccione los cortafuegos VM-Series para los que quiere recuperar licencias de suscripción y haga clic en **OK (Aceptar)**.

Activación de licencias en cortafuegos VM-Series en NSX cuando Panorama no tiene acceso a Internet

Complete el siguiente procedimiento para activar el cortafuegos VM-Series para NSX cuando Panorama no tenga acceso a internet.

STEP 1 | Localice la ID de CPU y la UUID del cortafuegos VM-Series.

1. Desde el servidor vCenter obtenga la dirección IP del cortafuegos.
2. Inicie sesión en la interfaz web y seleccione **Dashboard (Panel)**.
3. Obtenga la **ID de CPU** y la **UUID** para el cortafuegos en el widget de información general.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Active el código de autenticación y genere la claves de licencia.

1. Inicie sesión en el sitio web de asistencia de Palo Alto Networks con sus credenciales de cuenta. Si necesita una cuenta nueva, consulte Creación de una cuenta de asistencia técnica.
2. Seleccione **Products (Productos)** > **VM-Series Auth Codes (Códigos de autenticación de VM-Series)**, haga clic en **Add VM-Series Auth Codes (Añadir códigos de autenticación de VM-Series)** para acceder al código de autenticación.
3. Seleccione **Register VM (Registrar VM)** en la fila correspondiente al código de autenticación que acaba de registrar, introduzca la ID de CPU y la UUID del cortafuegos y haga clic en **Submit (Enviar)**. El portal generará un número de serie para el cortafuegos.
4. Seleccione **Products (Productos)** > **Assets (Activos)** > **NGFW** y busque el número de serie.
5. Haga clic en el enlace de la columna Acciones para descargar cada clave localmente a su ordenador portátil. Además de la clave de licencia de suscripción, debe obtener la licencia de capacidad y las claves de licencias de asistencia.

STEP 3 | Cargue las claves en el cortafuegos.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y seleccione **Manually upload license key (Subir clave de licencia manualmente)**.
3. **Browse (Examinar)** para seleccionar una clave y haga clic en **OK (Aceptar)** para instalar la licencia en el cortafuegos.

   Instale el archivo de claves de licencia de capacidad (pa-vm.key) en primer lugar. Cuando aplique la clave de licencias de capacidad, se reiniciará el cortafuegos VM-Series. Al reiniciar, el cortafuegos tendrá un número de serie que puede usarse para registrar el cortafuegos como dispositivo gestionado en Panorama.
4. Repita el proceso para instalar cada clave en el cortafuegos.
5. Seleccione el **Dashboard (Panel)** y verifique que puede ver el **Serial # (Nº de serie)** en el widget de información general.

STEP 4 | Añada el número de serie del cortafuegos en Panorama.

Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** y haga clic en **Add (Añadir)** para introducir al número de serie para el cortafuegos VM-Series para NSX. El cortafuegos podrá conectarse con Panorama para que pueda obtener su configuración y reglas de política.

Solución de problemas de activación de licencia

En esta sección, se tratan algunos de los problemas más comunes relacionados con la activación de su licencia.

Error: Memoria insuficiente

La licencia de una PA-VM sin suficiente memoria provoca un error similar al siguiente:

```
Server error : failed key check : Resource check failed. Memory
 needed: 6.5GB, allocated memory: 4,8 GB
```

Para solucionar este problema, aprovisione la memoria adicional que requiere la licencia y obtenga la licencia con el comando.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Aprovisione la memoria adicional que requiere la licencia.

STEP 2 | Ejecute el siguiente comando:

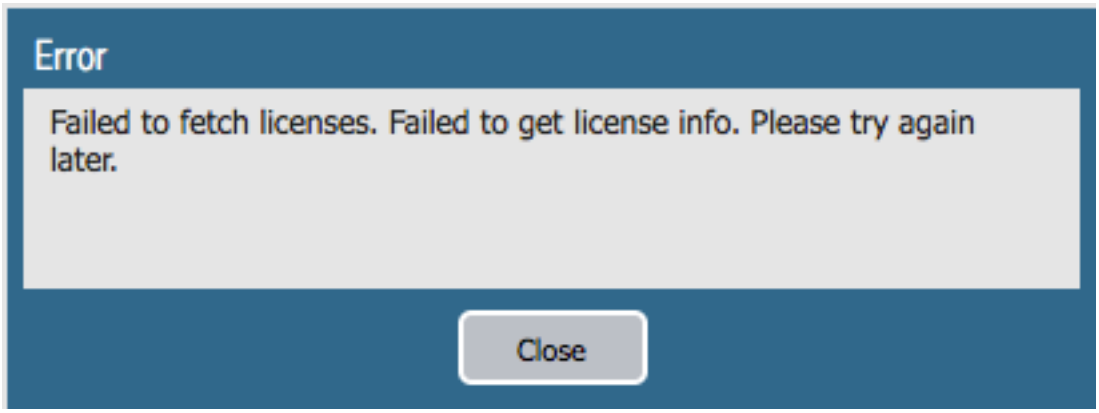
```
request license fetch
```

Si usa cualquier otro comando, fallará con el siguiente error:

```
Server error : failed to fetch license: No es posible
 aplicar una función de licencia de aprovisionamiento a un
 dispositivo ya aprovisionado.
```

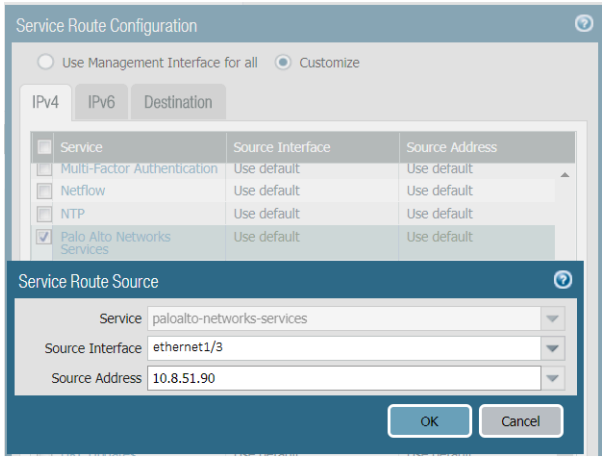
Error: No se pudieron recuperar licencias

Si ve un error que dice **Error al recuperar las licencias. No se pudo obtener la información de la licencia. Vuelva a intentarlo más tarde** o aparece un mensaje de error genérico.



Si ve este error, complete los siguientes pasos de verificación.

STEP 1 | ¿Puede el cortafuegos dirigir el tráfico al servidor de Palo Alto Networks utilizando una ruta de servicio? De manera predeterminada, el cortafuegos utiliza la interfaz de gestión para acceder al servidor. Si planifica usar una interfaz del plano de datos, asegúrese de haber configurado una ruta de servicio.



 ©2024 Palo Alto Networks, Inc.

STEP 2 | ¿Funciona el enrutamiento a través de internet? SSH al cortafuegos y haga ping a una dirección IP accesible al público, como 4.2.2.2. Asegúrese de utilizar la opción origen si está utilizando una interfaz del plano de datos. Por ejemplo: ping count 3 source 10.0.1.1 host 4.2.2.2.

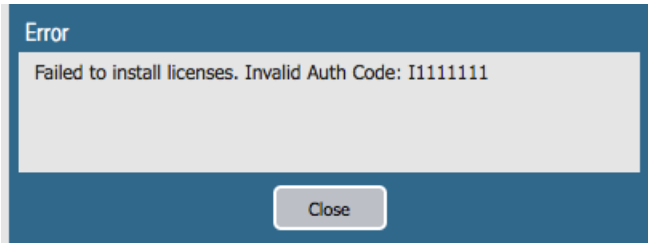
STEP 3 | ¿Está la DNS configurada correctamente? SSH al cortafuegos y haga ping a un nombre DNS como google.com. Por ejemplo:

```
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
```

Error: Invalid Authcode (Código de autenticación no válido)

Si ves un error que dice Código de autenticación no válido, complete los siguientes pasos de verificación.



STEP 1 | Has introducido el código de autenticación correctamente.

STEP 2 | Ha registrado el código de autenticación en su cuenta en el portal de asistencia técnica.

STEP 3 | Su código de autenticación no ha alcanzado la capacidad máxima de aprovisionamiento para los cortafuegos VM-Series.

1. Para licencias heredadas, inicie sesión en el CSP y seleccione **Assets (Activos)** > **VM-Series Auth-Codes (Códigos de autenticación de VM-Series)**
2. Para los Créditos NGFW de software, si conoce el perfil de implementación, inicie sesión en el CSP y seleccione **Assets (Activos)** > **Software NGFW Credits (Créditos NGFW de software)**, localice su perfil y haga clic en **Details (Detalles)**.

   También puede seleccionar **Assets (Activos)** > **Software NGFW Devices (Dispositivos NGFW de software)** y buscar por código de autenticación, Auth-Code.

Registro del cortafuegos VM-Series

Cuando adquiere un cortafuegos VM-Series, recibe un correo electrónico que incluye un código de autorización para una licencia de capacidad del modelo VM-Series, un código de autorización de derecho de asistencia y uno o varios códigos de autorización para las licencias de suscripción. Para usar los códigos de autorización, debe registrar el código en la cuenta de asistencia del sitio web de asistencia técnica de Palo Alto Networks. En el caso de la solución NSX integrada en VMware, el correo electrónico contiene un único código de autorización que agrupa la licencia de capacidad para una o más instancias del modelo VM-Series, el derecho de asistencia y una o más licencias de suscripción.

 ©2024 Palo Alto Networks, Inc.

No recibirá un código de autenticación para las licencias basadas en el uso en nubes públicas (AWS, Azure o Google Cloud Platform). Sin embargo, para activar su derecho a asistencia premium en Palo Alto Networks, debe crear una cuenta de asistencia y registrar el cortafuegos VM-Series en el sitio web de asistencia técnica de Palo Alto Networks.

Siga las instrucciones de esta sección para registrar el código de autorización de capacidad con su cuenta de asistencia técnica:

- Registrar el cortafuegos VM-Series (Créditos NGFW de software)
- Registro del cortafuegos VM-Series (con código de autenticación)
- Registro del modelo basado en el uso del cortafuegos VM-Series para nubes públicas (sin código de autenticación)

Registro del cortafuegos VM-Series (con código de autenticación)

Complete el siguiente procedimiento para registrar el cortafuegos VM-Series con un código de autenticación.

STEP 1 | Inicie sesión en el sitio web de asistencia de Palo Alto Networks con sus credenciales de cuenta. Si es necesario, cree una cuenta de asistencia técnica.

STEP 2 | Seleccione **Products (Productos)** > **VM-Series Auth-Codes (Códigos de autenticación del VM-Series)** > **Add VM-Series Auth-Code (Añadir código de autenticación del VM-Series**.

STEP 3 | En el campo **Add VM-Series Auth-Code (Añadir códigos de autorización de VM-Series)** introduzca el código de autenticación de capacidad que recibió por correo electrónico y haga clic en la marca de verificación a la derecha para guardarlo. La página mostrará la lista de códigos de autenticación registrados en su cuenta de asistencia técnica.

Puede hacer un seguimiento del número de cortafuegos VM-Series que se han implementado y el número de licencias que siguen disponibles con cada código de autenticación. Cuando se hayan usado todas las licencias disponibles, el código de autenticación dejará de aparecer en la página Códigos de autenticación de VM-Series. Para ver todos los activos que se han implementado, seleccione **Assets (Activos)** > **Devices (Dispositivos)**.

Registro del modelo basado en el uso del cortafuegos VM-Series para nubes públicas (sin código de autenticación)

Para registrar cortafuegos basados en el uso en el Portal de atención al cliente (CSP) de Palo Alto Networks, puede utilizar el registro automático o el registro manual. El registro automático de los cortafuegos basados en el uso le permite registrar sin problemas el cortafuegos tan pronto como lo inicie y acceda a los derechos de licencia del sitio asociados con su cuenta de CSP. Para obtener más detalles, consulte Instalación de un certificado de dispositivo en el cortafuegos VM-Series.

Utilice el siguiente flujo de trabajo para registrar manualmente sus cortafuegos VM-Series. Antes de comenzar el proceso de registro manual, inicie sesión en el cortafuegos VM-Series y anote el número de serie y la ID de la CPU (UUID es opcional) del panel.

STEP 1 | Inicie sesión en el Sitio web de atención al cliente de Palo Alto Networks y haga clic en **Products (Productos)** > **Devices (Dispositivos)** > **Register New Devices (Registrar nuevos dispositivos)**.

1. Seleccione **Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace (Registrar modelos de VM-Series basados en el uso [por hora/anual]**

 ©2024 Palo Alto Networks, Inc.

adquiridos en el Marketplace de la nube pública) o Proveedor de servicios de seguridad en la nube (Cloud Security Service Provider, CSSP).

2. Seleccione su proveedor de **Cloud Marketplace** y haga clic en **Next (Siguiente)**.

STEP 2 | Introduzca el **Serial # (N.º de serie)**, la **CPU ID (ID de CPU)** y la **UUID** del cortafuegos VM-Series.

Por ejemplo, desde el Panel del cortafuegos VM-Series en su VM, verá la siguiente información.

*Si tiene pensado usar el cortafuegos fuera de línea, seleccione la casilla de verificación **Offline (Desconectado)** e introduzca la versión de PAN-OS que planea usar.*

STEP 3 | Debe **Agree and Submit (Aceptar y enviar)** para aceptar el EULA y registrar el cortafuegos.

STEP 4 | Verifique que se muestren los detalles en las licencias que adquirió en la página **Assets (Activos)** de CSP.

Instalación de un certificado de dispositivo en el cortafuegos VM-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• VM-SERIES	❑ Licencia de la serie VM-Series ❑ Cuenta del Portal de atención al cliente (CSP) con una de las siguientes funciones de usuario: Superusuario, usuario estándar, usuario limitado, investigador de amenazas, función de prueba de AutoFocus, superusuario de grupo, usuario estándar de grupo, usuario limitado de grupo, investigador de amenazas de grupo, usuario del Centro de servicio autorizado (ASC) y usuario de Servicio completo de ASC. ❑ Acceso de superusuario al cortafuegos VM-Series

El cortafuegos requiere un certificado de dispositivo para recuperar los derechos de licencia del sitio y acceder de manera segura a servicios en la nube como WildFire, AutoFocus y Cortex Data Lake. Hay tres métodos para aplicar una licencia de sitio a su cortafuegos VM-Series: contraseña única, PIN de registro automático y Panorama para cortafuegos gestionados. Cada contraseña o PIN se genera en el Portal de atención al cliente y es exclusivo de su cuenta de asistencia técnica de Palo Alto Networks. El método que utilice depende del tipo de licencia utilizado para implementar su cortafuegos y si sus cortafuegos están gestionados por Panorama. Para instalar correctamente el certificado del dispositivo, el cortafuegos VM-Series requiere una conexión a Internet saliente, y los siguientes nombres de dominio y puertos completamente cualificados deben estar permitidos en su red.

- Contraseña de un solo uso (OTP): para los cortafuegos VM-Series que ya se han registrado con el servidor de licencias de Palo Alto Networks, debe generar una contraseña de un solo uso en el portal de atención al cliente y aplicarla a su cortafuegos VM-Series. Utilice este método para cortafuegos

 ©2024 Palo Alto Networks, Inc.

VM-Series con una licencia BYOL o ELA en implementaciones no gestionadas a pequeña escala, y cortafuegos VM-Series implementados manualmente y gestionados por Panorama.

- PIN de registro: este método le permite aplicar una licencia de sitio a su cortafuegos VM-Series en el inicio inicial. Utilice este método para los cortafuegos VM-Series con licencias basadas en uso (PAYG), que se inician durante el inicio o con cualquier tipo de implementación automatizada, independientemente del tipo de licencia. El PIN de registro automático le permite registrar automáticamente sus cortafuegos basados en el uso durante el inicio con el Portal de atención al cliente y recuperar las licencias de sitio.
- Si utiliza Panorama para gestionar el cortafuegos VM-Series, consulte Instalar el certificado del dispositivo en un cortafuegos gestionado.

Para el cortafuegos VM-Series en NSX-V y NSX-T, puede añadir el PIN de registro automático a la configuración de la definición de servicio para que el cortafuegos obtenga el certificado del dispositivo en el arranque inicial. Consulte la configuración de definición de servicio para NSX-T (norte-sur) y NSX-T (este-oeste) para obtener más información. Si actualiza los cortafuegos implementados anteriormente a la versión PAN-OS compatible con certificados de dispositivo, puede aplicar un certificado de dispositivo a esos cortafuegos individualmente usando una contraseña de un solo uso.

Utilice contraseñas de un solo uso y PIN de registro automático antes de que caduquen. Si no lo hace, debe volver al Portal de atención al cliente para generar uno nuevo.

FQDN	Ports (Puertos)
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • https://certificatetrusted.paloaltonetworks.com • https://certificate.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 y TCP 443

Recuperar licencias automáticamente durante el inicio

El cortafuegos requiere el certificado del dispositivo para obtener los derechos de licencia y acceder de forma segura a los servicios en la nube. Para recuperar las licencias del sitio cuando inicie el cortafuegos, debe incluir el ID de PIN de registro automático y el valor en los parámetros de arranque. El ID de PIN de registro automático y el valor se pueden utilizar con los métodos de arranque básico o completo. Consulte Seleccione un método de arranque para obtener más detalles sobre las opciones y la configuración de arranque.

 ©2024 Palo Alto Networks, Inc.

El PIN de registro automático es válido solo durante el período de tiempo especificado. Para entornos totalmente automatizados, como las implementaciones de escalado automático de la serie VM-Series, el PIN de registro automático debe regenerarse antes de la fecha de vencimiento y el nuevo ID y valor del PIN actualizarse en los parámetros de arranque.

STEP 1 | Inicie sesión en el portal de asistencia técnica de Palo Alto Networks con las credenciales de su cuenta.

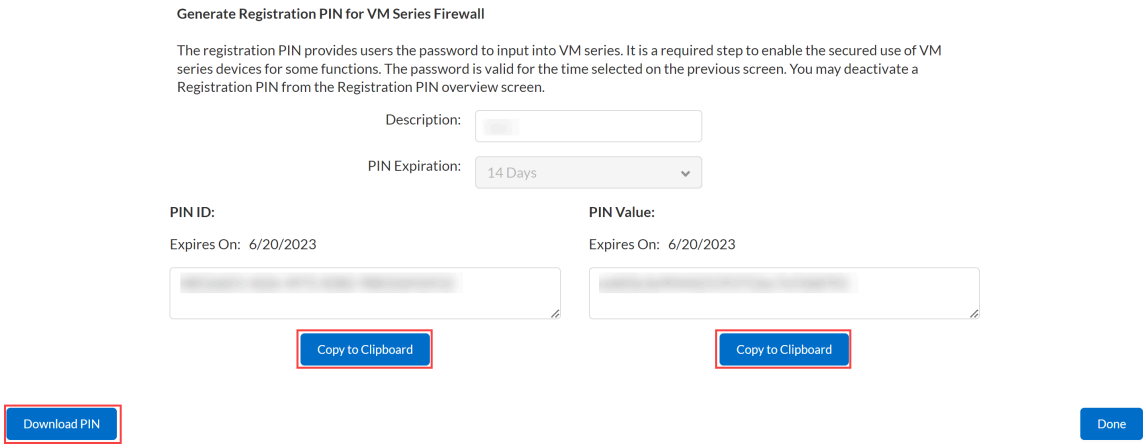
Si necesita una nueva cuenta, consulte Cómo crear una nueva cuenta de usuario del portal de atención al cliente.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Genere el PIN de registro de VM-Series.

1. Seleccione **Assets (Activos)** > **Device Certificates (Certificados de dispositivo)** y **Generate Registration PIN (Generar PIN de registro)**.
2. Introduzca un **Description (Descripción)** y un periodo de tiempo para la **PIN Expiration (Vencimiento de PIN)**.
3. Haga clic en **Generate Registration PIN (Generar PIN de registro)**.
4. Guarde el ID y el valor del PIN.
5. Asegúrese de iniciar el cortafuegos antes de que caduque el PIN.

 ©2024 Palo Alto Networks, Inc.



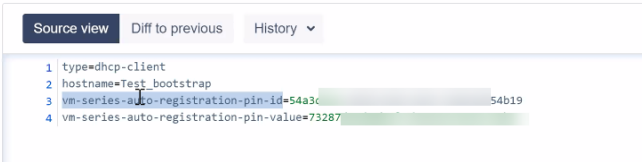
 ©2024 Palo Alto Networks, Inc.

STEP 3 | Añada el ID y el valor del PIN de registro en el archivo init-cfg.txt.

STEP 4 | Además de los parámetros obligatorios, debe incluir:

```
vm-series-auto-registration-pin-id=
```

```
vm-series-auto-registration-pin-value=
```



STEP 5 | Compruebe que se ha obtenido el certificado del dispositivo y que puede ver las licencias previstas en el cortafuegos.

Recuperar manualmente un certificado de dispositivo

 ©2024 Palo Alto Networks, Inc.

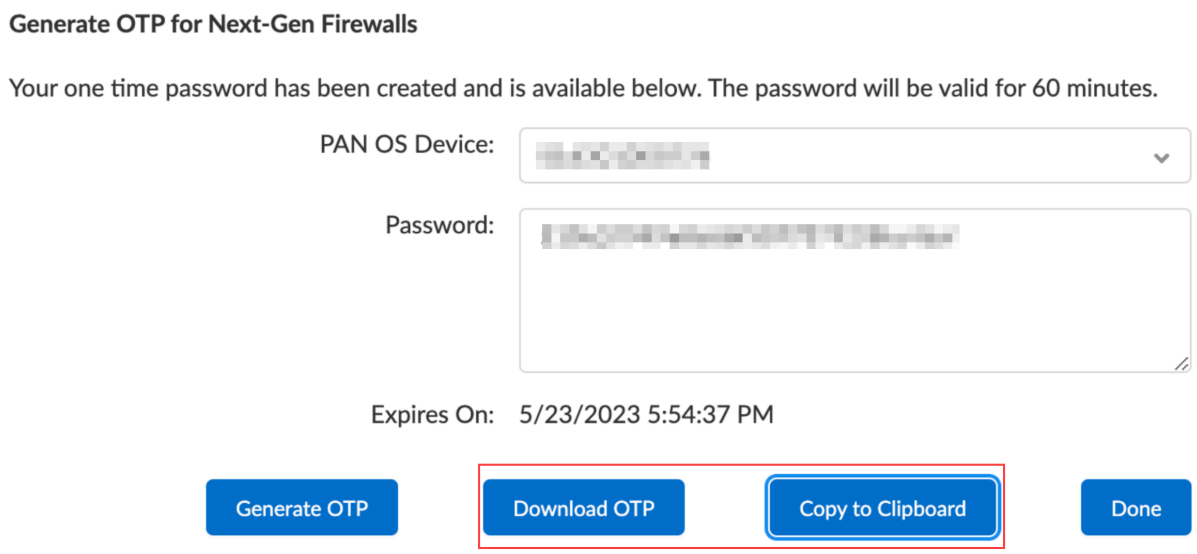
STEP 1 | Genere la contraseña de un solo uso (OTP).

La vida útil de una OTP es de 60 minutos y caduca si no se usa dentro de dichos 60 minutos.

Intentos del cortafuegos de recuperar la OTP del Portal de atención al cliente una vez. Si el cortafuegos no puede recuperar la OTP por cualquier motivo, la OTP caduca y deberá generar una nueva OTP.

1. Inicie sesión en el Portal de atención al cliente con una función de usuario que tiene permiso para generar una OTP.

   Registre su cortafuegos VM-Series, si aún no lo ha hecho.
2. Seleccione **Assets (Activos)** > **Device Certificates (Certificados del dispositivo)** y **Generate OTP (Generar OTP)**.
3. Para el **Device Type (Tipo de dispositivo)**, seleccione **Generate OTP for Next-Gen Firewall (Generar OTP para cortafuegos de nueva generación)** y haga clic en **Next (Siguiente)**.
4. Seleccione el número de serie de su **PAN OS Device (Dispositivo PAN OS)** y **Generate OTP (Generar OTP)**.
5. **Download OTP (Descargar OTP)** o **Copy to Clipboard (Copiar al Portapapeles)**.



 ©2024 Palo Alto Networks, Inc.

STEP 2 | Inicie sesión en la interfaz web del cortafuegos como superusuario.

Se requiere un administrador con privilegios de acceso de superusuario para aplicar la OTP utilizada para instalar el certificado de dispositivo.

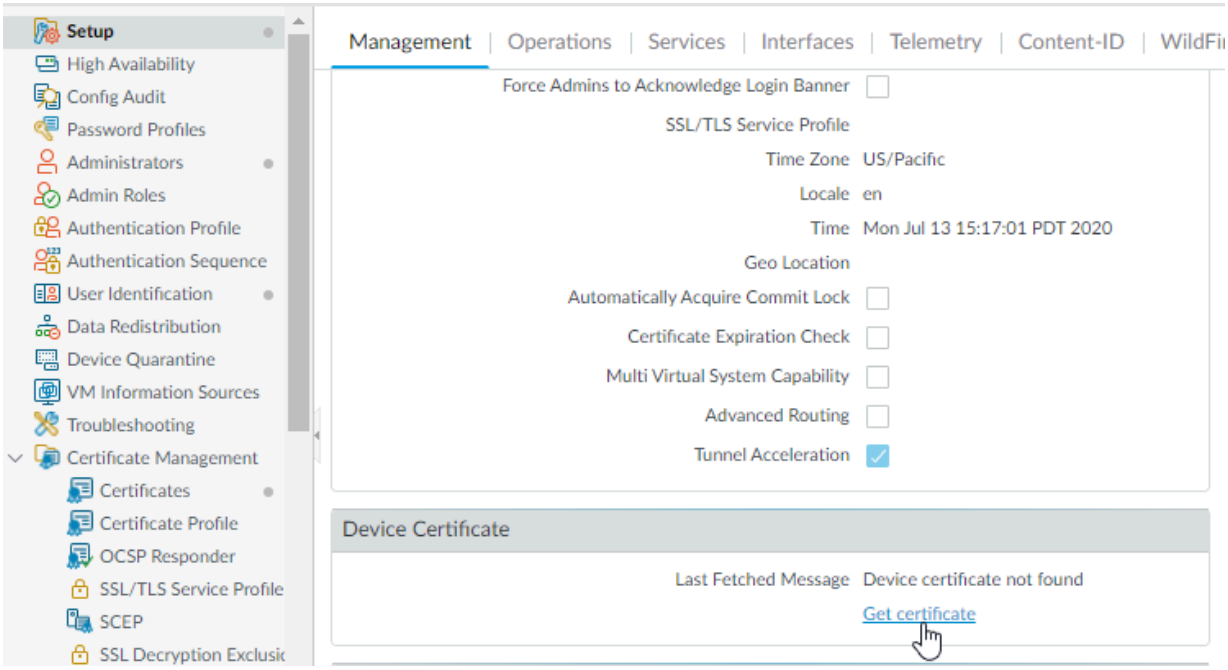
STEP 3 | Configure el servidor de protocolo de tiempo de redes (NTP) para sus cortafuegos.

Es necesario un servidor NTP para validar la fecha de vencimiento de la certificación del dispositivo y asegurarse de que el certificado del dispositivo no caduque antes de tiempo o no sea válido.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y seleccione la **Template (Plantilla)**.
2. Seleccione una de las siguientes opciones según su plataforma:
   - En plataformas de múltiples sistemas virtuales, seleccione **Global** y edite la sección Services.
   - En plataformas de un único sistema virtual, edite la sección Servicios.
3. Seleccione **NTP** e introduzca el nombre de host o la dirección IP del **Primary NTP Server (Servidor NTP primario)**.
4. (Opcional) Introduzca un nombre de host o la dirección IP del **Secondary NTP Server (Servidor NTP secundario)**.
5. (Opcional) Para autenticar actualizaciones de tiempo de los servidores NTP, en **Authentication Type (Tipo de autenticación)**, seleccione uno de los siguientes en cada servidor:
   - **None (Ninguna)** (opción por defecto): deshabilita la autenticación NTP.
   - **Symmetric Key (Clave simétrica)**: el cortafuegos usa intercambio de clave simétrica (secretos compartidos) para autenticar las actualizaciones de tiempo.
     - **Key ID (ID de clave)**: introduzca el ID de clave (1-65534).
     - **Algorithm (Algoritmo)**: seleccione el algoritmo que se debe utilizar en la autenticación del NTP (**MDS** o **SHA1**).
6. Haga clic en **OK (Aceptar)** para guardar los cambios.
7. Seleccione las opciones**Confirmar** y **Confirmar y enviar** a sus cortafuegos de gestión.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Seleccione **Setup (Configuración)** > **Management (Gestión)** > **Device Certificate (Certificado de dispositivo)** y **Get Certificate (Obtener certificado)**.



STEP 5 | Compruebe que se ha obtenido el certificado del dispositivo y que pueda ver la licencia del sitio en el cortafuegos.

Cambio entre las licencias BYOL y PAYG

El cortafuegos VM-Series no se puede convertir entre las opciones de licencia de BYOL y PAYG. Si ya implementó y configuró un cortafuegos VM-Series con la opción PAYG o BYOL en AWS, Azure o Google Cloud Platform, y ahora desea cambiar a la otra opción, use las siguientes instrucciones para guardar y exportar la configuración en su cortafuegos existente, implementar un nuevo cortafuegos y, luego, restaurar la configuración en el nuevo cortafuegos.

STEP 1 | Guarde una copia de seguridad del archivo de configuración actual y almacénela en un servidor externo.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y **Export named configuration snapshot (Exportar instantáneas de configuración con nombre)**.
2. Seleccione el archivo XML que contiene su configuración en uso (por ejemplo, running-config.xml) y haga clic en **OK (Aceptar)** para exportar el archivo de configuración.
3. Guarde el archivo exportado en una ubicación externa al cortafuegos.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Implemente un nuevo cortafuegos y regístrese o active la licencia, según corresponda.

Para una nueva instancia de PAYG, realice lo siguiente:

1. En AWS, Azure o Google Cloud Platform, seleccione la imagen de software para el paquete de licencias PAYG que desea implementar.
2. Implemente un nuevo cortafuegos VM-Series en la nube pública de AWS, Azure o Google. Consulte Configuración del cortafuegos VM-Series en AWS, Configuración del cortafuegos VM-Series en Azure o Configuración el cortafuegos VM-Series en Google Cloud Platform.
3. Registro del modelo basado en el uso del cortafuegos VM-Series para nubes públicas (sin código de autenticación).

Para una nueva instancia de BYOL:

1. Póngase en contacto con su representante de ventas o revendedor para comprar una licencia de BYOL y obtenga un código de autenticación de BYOL que puede usar para licenciar su cortafuegos.
2. Registre el cortafuegos VM-Series (con código de autenticación).
3. Implemente un nuevo cortafuegos VM-Series en la nube pública de AWS o Azure. Consulte Configuración del cortafuegos VM-Series en AWS, Configuración del cortafuegos VM-Series en Azure o Configuración el cortafuegos VM-Series en Google Cloud Platform.
4. Active la licencia para el cortafuegos VM-Series (versión independiente).

STEP 3 | En el cortafuegos recientemente implementado, restaure la configuración que exportó.

1. Acceda a la interfaz web del nuevo cortafuegos implementado.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**, haga clic en **Import named configuration snapshot (Importar instantánea de configuración con nombre)**, vaya al archivo de configuración en el host externo y haga clic en **OK (Aceptar)**.
3. Haga clic en **Load named configuration snapshot (Cargar instantánea de configuración con nombre)**, seleccione el **Name (Nombre)** del archivo de configuración que acaba de importar, y haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** para sobrescribir la configuración en ejecución con la instantánea que acaba de importar.
5. Verifique que la configuración en el nuevo cortafuegos coincida con el cortafuegos que está reemplazando, antes de eliminar el cortafuegos o desactivar las licencias en el cortafuegos sustituido.

Cambio entre licencias del modelo VM-Series

Puede cambiar la licencia de su cortafuegos VM-Series implementado actualmente con la opción BYOL. Por ejemplo, puede pasar de un paquete de suscripción a un contrato de licencia empresarial (ELA) y viceversa, sin interrumpir el tráfico que se mueve a través del cortafuegos. También puede cambiar la licencia en un cortafuegos individual o en varios cortafuegos simultáneamente desde Panorama.

No utilice este procedimiento para cambiar licencias perpetuas o ELA entre PAYG y BYOL. Consulte Cambio entre las licencias BYOL y PAYG *para obtener más información.*

Complete uno de los siguientes procedimientos para realizar uno de los siguientes cambios de licencia:

- Paquete de suscripción 1 a paquete de suscripción 2

 ©2024 Palo Alto Networks, Inc.

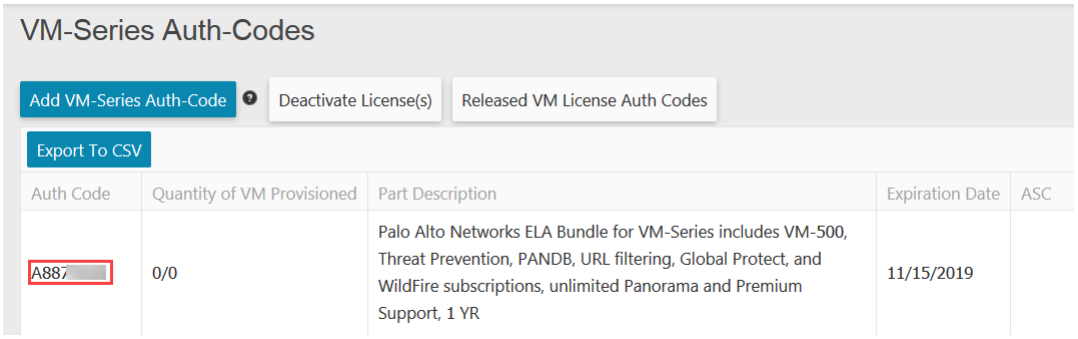
- Paquete de suscripción 1 o 2 a un ELA
- Licencia de capacidad a paquete de suscripción o ELA

Antes de cambiar a una licencia ELA, debe asignar suficientes tokens para apoyar al número de cortafuegos VM-Series implementados actualmente. Consulte Acuerdo de licencia empresarial de VM-Series (ELA de múltiples modelos) para obtener más información sobre los tokens requeridos para cada modelo VM-Series.

 ©2024 Palo Alto Networks, Inc.

- Cambie una licencia en un cortafuegos independiente.
  1. Registre su código de autorización.
     - Para un paquete de suscripción, registre su nuevo código de autorización.
     - Para una ELA, active el código de autorización de ELA.

     No utilice el código de autorización de ELA para activar cortafuegos VM-Series individuales. Después de registrar su ELA, use los códigos de autorización del modelo VM-Series para activar los cortafuegos individuales. Puede encontrar estos códigos de autorización en el Portal de atención al cliente en ***Products (Productos)*** *>* ***VM-Series Auth-Codes (Códigos de autenticación de VM-Series)****.*
  2. Inicie sesión en la interfaz web del cortafuegos VM-series.
  3. Verifique la configuración del servidor de actualizaciones de Palo Alto Networks.
     1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)**.
     2. Confirme que **Update Server (Servidor de actualizaciones)** está definido en updates.paloaltonetworks.com.
     3. Confirme que la opción **Update Server Identity (Actualizar la identidad del servidor)** esta seleccionada.
  4. Aplique un código de autorización VM-Series. Un código de autorización de cortafuegos para un ELA comienza con la letra A, como se muestra a continuación.

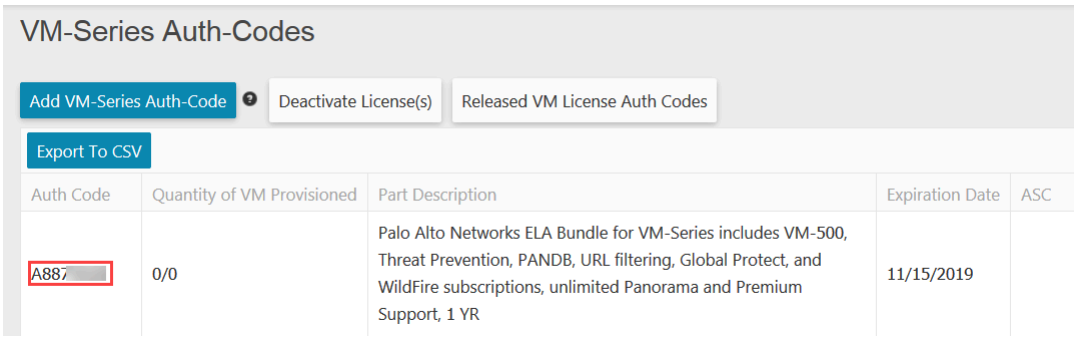
     

     1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y seleccione el vínculo **Activate feature using authentication code (Activar función usando el código de autenticación)**.
     2. Introduzca su código de autorización VM-Series.
     3. Haga clic en **OK (Aceptar)** para confirmar la actualización de la licencia. El cortafuegos se pone en contacto con el servidor de actualizaciones de Palo Alto Networks y consume los tokens necesarios para su cortafuegos según el modelo de VM-Series.
     4. Verifique que la licencia se ha actualizado correctamente mediante la verificación de la fecha de vencimiento de la licencia.
  5. Repita este proceso para cada cortafuegos VM-Series en su implementación.

 ©2024 Palo Alto Networks, Inc.

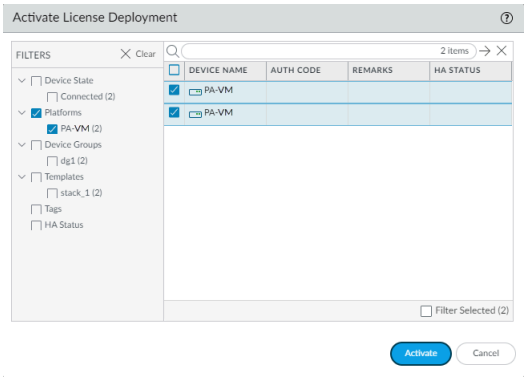
- Cambie las licencias en cortafuegos gestionados usando Panorama.
  1. Registre su código de autorización.
     - Para un paquete de suscripción, registre su nuevo código de autorización.
     - Para una ELA, active el código de autorización de ELA.

     No utilice el código de autorización de ELA para activar cortafuegos VM-Series individuales. Después de registrar su ELA, use los códigos de autorización del modelo VM-Series para activar los cortafuegos individuales. Puede encontrar estos códigos de autorización en el Portal de atención al cliente en ***Products (Productos)*** *>* ***VM-Series Auth-Codes (Códigos de autenticación de VM-Series)****.*
  2. Inicie sesión en la interfaz web de Panorama.
  3. Verifique la configuración del servidor de actualizaciones de Palo Alto Networks para los cortafuegos.
     1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)**.
     2. Confirme que **Update Server (Servidor de actualizaciones)** está definido en updates.paloaltonetworks.com.
     3. Confirme que la opción **Update Server Identity (Actualizar la identidad del servidor)** esta seleccionada.
  4. Aplique un código de autorización VM-Series. Un código de autorización de cortafuegos para un ELA comienza con la letra A, como se muestra a continuación.

     1. Seleccione **Panorama** > **Device Deployment (Implementación de dispositivo)** > **Licenses (Licencias)** y haga clic en **Activate (Activar)**.
     2. Introduzca su código de autorización VM-Series.
     3. Use los filtros para seleccionar los cortafuegos gestionados para obtener la licencia.
     4. Introduzca su código de autorización en la columna **Auth Code (Código de autenticación)** para cada cortafuegos.
     5. Haga clic en **Activate (Activar)** para confirmar la actualización de la licencia. Panorama se pone en contacto con el servidor de actualizaciones de Palo Alto Networks y consume los tokens necesarios para sus cortafuegos según el modelo de la VM-Series.

 ©2024 Palo Alto Networks, Inc.



6. Verifique que la licencia se ha actualizado correctamente mediante la verificación de la fecha de vencimiento de la licencia.

Desactivación de licencia(s)

El proceso de desactivación de la licencia le permite autogestionar las licencias. Si desea eliminar una o varias licencias o suscripciones activas atribuidas a un cortafuegos (cortafuegos VM-Series o basado en hardware) o desactivar el cortafuegos VM-Series y anular la designación de todas las suscripciones y licencias activas, comience el proceso de desactivación en el cortafuegos o Panorama (y no en el portal de asistencia de Palo Alto Networks).

Para desactivar satisfactoriamente una licencia, debe instalar una clave de API de desactivación de licencia y habilitar la verificación de la identidad del servidor de actualización (habilitada de manera predeterminada). PAN-OS usa esta clave de API de desactivación para autenticarse con todas las actualizaciones que permite una licencia. La API de desactivación no es necesaria para la desactivación manual de la licencia, donde no existe conexión entre el cortafuegos y el servidor de licencias.

Si el cortafuegos/Panorama posee acceso a internet y puede comunicarse con los servidores de licencias de Palo Alto Networks, el proceso de eliminación de licencia se completa automáticamente con solo hacer clic en un botón. Si el cortafuegos/Panorama no tiene acceso a internet, debe completar el proceso manualmente en dos pasos. En el primer paso, desde el cortafuegos o Panorama, genere y exporte un archivo de token de licencia que incluya información sobre las claves desactivadas. En el segundo paso, mientras permanece abierta la sesión en el portal de asistencia de Palo Alto Networks, cargue el archivo de token para disociar las claves de licencia del cortafuegos.

- Desactivación de la licencia de una función o suscripción con CLI
- Deshabilitar VM

Desactivación de la licencia de una función o suscripción con CLI

Si ha instalado una licencia/suscripción en un cortafuegos o necesita reasignarla a otro cortafuegos, puede desactivar la licencia individual y reutilizar el mismo código de autorización en otro cortafuegos sin la ayuda del Soporte técnico. Esta capacidad solo es compatible en la CLI y se admite tanto en dispositivos físicos como virtuales que ejecutan PAN-OS. Este procedimiento se suele utilizar con licencias de modelo fijo perpetuas o ELA.

- Acceso a Internet (modo automático)
- Sin acceso a Internet (modo manual)

 ©2024 Palo Alto Networks, Inc.

Acceso a Internet (modo automático)

STEP 1 | Inicie sesión en la CLI del cortafuegos.

STEP 2 | Vea el nombre de la clave de licencia para la función que desea desactivar.

```
request license deactivate key features
```

STEP 3 | Desactive la licencia o suscripción.

Utilice el modo automático para eliminar la clave de licencia.

```
request license deactivate key features <name> mode auto
```

El nombre es el nombre completo del archivo de clave de licencia. Por ejemplo:

```
admin@vmPAN2> request license deactivate key features <name>
```

```
WildFire_License_2015_01_28_I5820573.key mode auto007200002599
 WildFire License Success Successfully removed license keys
```

Sin acceso a Internet (modo manual)

Utilice el modo manual para eliminar la clave de licencia y generar un token de licencia para una licencia basada en el modelo. Este procedimiento asume que ha instalado la clave API de licencia en su cortafuegos.

STEP 1 | Inicie sesión en la CLI del cortafuegos.

STEP 2 | Vea el nombre de la clave de licencia para la función que desea desactivar.

```
request license deactivate key features
```

STEP 3 | Desactive la licencia manualmente desde la línea de comandos.

```
request license deactivate key features <name> mode manual
```

Por ejemplo:

```
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
```

El archivo de token utiliza el formato `dact_lic.timestamp.tok`, donde "timestamp" está en formato `dmmyyyy.hrminsec`.

STEP 4 | Verifique que se generó el archivo de token.

```
show -token-files
```

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Exporta el archivo de token.

Introduzca este comando en una sola línea:

```
scp export license-token-file to <username@serverIP>
from <token_filename>
```

Por ejemplo:

```
scp export license-token-file to admin@10.1.10.55:/tmp/ from
dact_lic.01282015.100502.tok
```

STEP 6 | Inicie sesión en el Portal de atención al cliente de Palo Alto Networks.

1. Haga clic en el enlace **Deactivate License(s) (Desactivar licencias)** en la pestaña **Assets (Activos)**.
2. Seleccione **Products (productos)** > **VM-Series Auth-Codes (Códigos de autenticación de VM-Series)** y seleccione **Deactivate License(s) [Desactivar licencia(s)]**.
3. Cargue el archivo del token para completar la desactivación.

Deshabilitar VM

Cuando ya no necesita una instancia BYOL del cortafuegos VM-Series, usted puede liberar todas las licencias activas (licencias de suscripción, licencias de capacidad basadas en el modelo y derechos de asistencia) de la interfaz web, la CLI o la API de XML en el cortafuegos o Panorama. Las licencias se devuelven a su cuenta y podrá utilizar los mismos códigos de autorización en una instancia diferente del cortafuegos VM-Series.

Desactivar un VM elimina todas las licencias/derechos y coloca al cortafuegos VM-Series en el estado de sin licencia; el cortafuegos no tendrá un número de serie y podrá admitir solo un número mínimo de sesiones. Debido a que la configuración del cortafuegos queda intacta, puede volver a aplicar un conjunto de licencias y restaurar la funcionalidad completa del cortafuegos, si es necesario.

*Asegúrese de desactivar las licencias **antes** de eliminar el cortafuegos VM-Series. Si elimina el cortafuegos antes de desactivar las licencias, tiene dos opciones:*

***Gestionado por Panorama**:desactive la licencia de Panorama.*

***No gestionado por Panorama**: póngase en contacto con el Servicio de atención al cliente de Palo Alto Networks para obtener asistencia para la desactivación.*

- Desactivar la máquina virtual del cortafuegos
- Desactivar la VM de Panorama

Desactivar la máquina virtual del cortafuegos

Complete el siguiente proceso para desactivar la licencia de máquina virtual del cortafuegos.

STEP 1 | Inicie sesión en la interfaz web y seleccione **Device (Dispositivo)** > **Licenses (Licencias)**.

STEP 2 | En la sección Gestión de licencias seleccione **Deactivate VM (Desactivar VM)**.

Solo puede ver esta opción en una máquina virtual. No está allí en un cortafuegos físico.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Compruebe la lista de licencias/derechos que se desactivarán en el cortafuegos.

STEP 4 | Seleccione una de las siguientes opciones para iniciar la desactivación de VM:

- (Acceso con Internet al servidor de licencias de Palo Alto Networks) Seleccione **Continue (Continuar)**.

  Se le solicitará que reinicie el cortafuegos; al reiniciar, las licencias se desactivan.

- (Sin internet):seleccione **Complete Manually (Completar manualmente)**.

  Haga clic en el enlace **Export license token (Exportar token de licencia)** para guardar el archivo de token en su ordenador local. Aquí hay un nombre de archivo de token de ejemplo: 20150128_1307_dact_lic.01282015.130737.tok

  Se le solicitará que reinicie el cortafuegos; al reiniciar, las licencias se desactivan.

STEP 5 | (Proceso manual: sin internet) Utilice el archivo de token para registrar los cambios en el servidor de licencias:

1. Inicie sesión en el sitio web de asistencia técnica de Palo Alto Networks.
2. Seleccione **Products (Productos)** > **VM-Series Auth-Codes (Códigos de autenticación de VM-series)** > **Deactivate License(s) [Desactivar licencia(s)]**.
3. Mientras permanece abierta la sesión en el sitio web de asistencia técnica de Palo Alto Networks, cargue el archivo de token para completar la desactivación.

Desactivar la VM de Panorama

Complete el siguiente proceso para desactivar una licencia de VM de Panorama.

STEP 1 | Inicie sesión en la interfaz web de Panorama y seleccione **Panorama** > **Device Deployment (Implementación de dispositivo)** > **Licenses (Licencias)**.

STEP 2 | Seleccione **Deactivate VMs (Desactivar las VM)** y seleccione el cortafuegos VM-Series que desea desactivar.

STEP 3 | Seleccione una de las siguientes opciones para desactivar VM:

- Haga clic en **Continue (Continuar)** si Panorama puede comunicarse directamente con los servidores de licencias de Palo Alto Networks y puede registrar los cambios. Para verificar que las licencias se desactivaron en el cortafuegos, seleccione **Refresh on Panorama (Actualizar en Panorama)** > **Device Deployment (Implementación de dispositivo)** > **Licenses (Licencias)**. El cortafuegos se reiniciará automáticamente.
- **Complete Manually (Completar manualmente)**: si Panorama no tiene acceso a Internet, Panorama genera un archivo de token.

  Haga clic en el enlace **Export license token (Exportar token de licencia)** para guardar el archivo de token en su ordenador local. Aquí hay un nombre de archivo de token de ejemplo: 20150128_1307_dact_lic.01282015.130737.tok

  El mensaje de proceso finalizado correctamente se muestra en pantalla y el cortafuegos se reiniciará automáticamente.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | (Solo proceso manual: sin internet) Utilice el archivo de token para registrar los cambios en el servidor de licencias.

1. Inicie sesión en el sitio web de asistencia técnica de Palo Alto Networks.
2. Seleccione **Products (Productos)** > **VM-Series Auth-Codes (Códigos de autenticación de VM-series)** > **Deactivate License(s) [Desactivar licencia(s)]**.
3. Cargue el archivo del token para completar la desactivación.

STEP 5 | Elimine el cortafuegos VM-Series desactivado como un dispositivo gestionado en Panorama.

1. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)**.
2. Seleccione el cortafuegos que desactivó de la lista de dispositivos gestionados y haga clic en **Delete (Eliminar)**.

En lugar de eliminar los cortafuegos, si lo prefiere, puede crear un grupo de dispositivos separado y asignar los cortafuegos VM-Series desactivados a este grupo de dispositivos.

Renovación de los paquetes de licencias de cortafuegos VM-Series

Cuando el paquete de licencias de su cortafuegos VM-Series deba renovarse, puede iniciar sesión en el portal de atención al cliente de Palo Alto Networks y ajustar la cantidad de licencias para satisfacer sus necesidades de implementación. Cuando inicie la renovación, podrá revisar sus tendencias de uso y en función de sus necesidades futuras, seleccione entre las siguientes opciones:

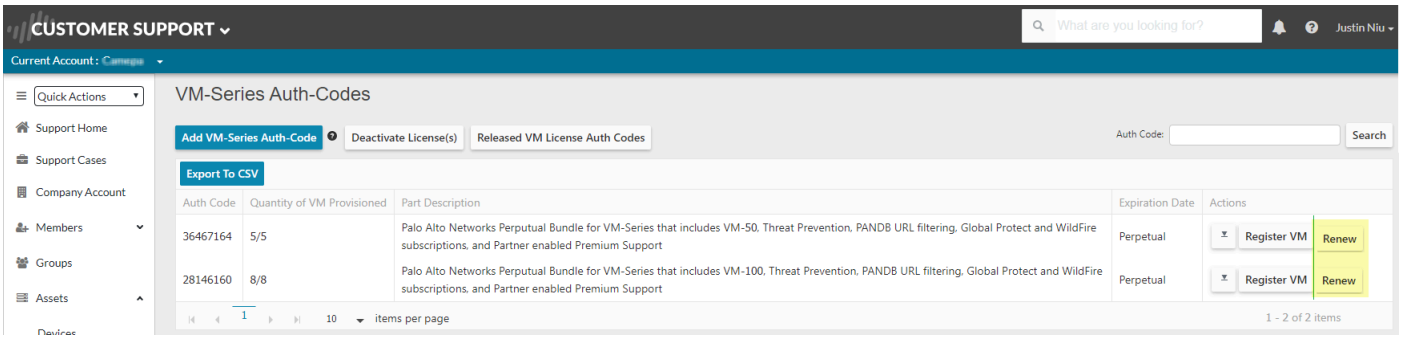
- **Renew (Renovación)**: puede optar por renovar todas las licencias o aumentar o disminuir la cantidad que requiere licencias. Si disminuye el número de licencias que necesita, debe optar por un paquete básico para los cortafuegos que no renueva; de lo contrario, perderá la porción que no renueve. Si aumenta la cantidad de licencias, la adición se añade a su código de autorización existente.
- **Change to Basic Bundle (Cambiar a paquete básico)**: si tiene una licencia de paquete 1 o paquete 2 para VM-Series que incluya suscripciones, puede cambiar a un paquete básico que incluye una licencia con capacidad ilimitada y derecho a asistencia técnica. Cuando cambia a un paquete básico, mantiene el modelo de cortafuegos VM-Series que compró previamente. Todos los cortafuegos implementados actualmente asociados al código de autorización existente continuarán funcionando y el derecho a asistencia técnica tendrá una nueva fecha de vencimiento. Para los cortafuegos sin licencia, recibirá un nuevo código de autorización que podrá usar para implementar nuevas instancias.
- **Forfeit (Pérdida)**: renuncie a las licencias que ya no necesita. Si implementó el cortafuegos que no desea renovar, debe seleccionar el número de serie de las instancias en las que desea interrumpir las renovaciones. Puede continuar usando las interfaces de estos cortafuegos con las versiones de software y contenido instaladas actualmente, pero sus suscripciones y sus derechos a asistencia técnica ya no serán válidos. Y para renunciar a la licencia de los cortafuegos VM-Series que no ha aprovisionado, simplemente seleccione la cantidad que desea renunciar.

STEP 1 | Inicie sesión en el portal de asistencia técnica de Palo Alto Networks con las credenciales de su cuenta.

 ©2024 Palo Alto Networks, Inc.

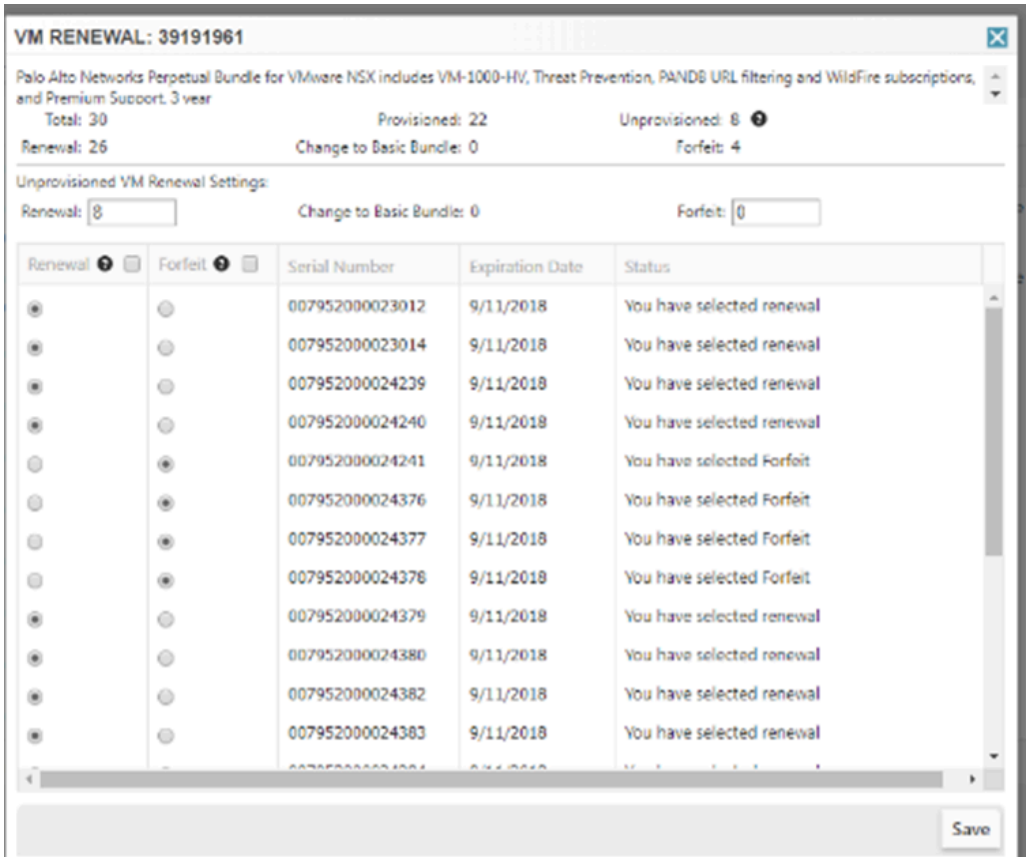
STEP 2 | Seleccione **Products (productos)** > **VM-Series Auth-Codes (Códigos de autenticación de VM-Series)** y busque el código de autenticación que desea renovar.

La opción **Renew (Renovar)** se muestra en los códigos de autorización que se pueden seleccionar para la renovación.



STEP 3 | Haga clic en el enlace **Renew (Renovar)** para seleccionar los números de serie que desea **Renew (Renovar)**, **Change to Basic Bundle (Cambiar a paquete básico)** o **Forfeit (Perder)**.

Si ha aprovisionado el cortafuegos, seleccione la opción apropiada en la fila que corresponde al Número de serie. Si tiene instancias no aprovisionadas del cortafuegos, seleccione la cantidad para cada opción de renovación que elija en **Unprovisioned VM Renewal Settings (Configuración de renovación de VM no provista)**.



 ©2024 Palo Alto Networks, Inc.

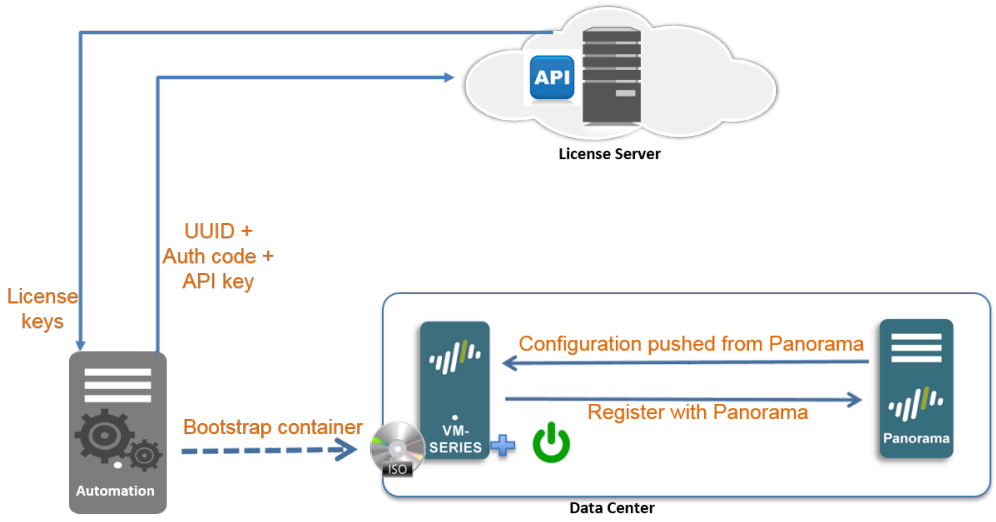
STEP 4 | Haga clic en **Save (Guardar)** para guardar sus cambios.

Recibirá una confirmación en la pantalla de que los cambios se enviaron y se procesarán. Después de enviar los cambios, si selecciona Renovar de nuevo, puede ver el estado de su solicitud con cada número de serie. Si el proceso de renovación se ha iniciado y necesita realizar revisiones adicionales, no podrá guardar los cambios. Para obtener ayuda, puede ponerse en contacto con el equipo de renovaciones en renewals@paloaltonetworks.com.

API de licencias basada en modelos

Utilice la API de licencias basada en modelos para registrar códigos de autenticación, recuperar licencias adjuntas a un código de autenticación, renovar licencias o desactivar todas las licencias basadas en modelos en un cortafuegos VM-Series. Además, la API de licencias le permite autorizar a cortafuegos que no tienen acceso directo a Internet y no pueden llegar al servidor de licencias de Palo Alto Networks. Puede gestionar licencias manualmente o automatizar las licencias con un script personalizado o un servicio de orquestación.

También puede utilizar el Complemento Panorama Software Firewall License para tareas de licencia, incluidas las licencias sin conexión. El complemento requiere Panorama 10.0.0 o posterior con el complemento VM-Series 2.0.4 o posterior, y los cortafuegos administrados VM-Series deben ejecutar PAN-OS 9.1.0 o posterior y VM-Series plugin 2.0.4 o posterior; el cortafuegos VM-Series para Azure requiere el complemento VM-Series 2.0.8.



Para las licencias basadas en modelos, la API le permite ver los detalles de un código de autenticación de modo que pueda hacer el seguimiento del número de licencias no usadas adjuntas a un código de autenticación o paquete de códigos de autenticación que le permite activar la licencia de más de una instancia del cortafuegos. Un paquete de códigos de autenticación incluye el modelo VM-Series, suscripciones y soporte en un formato simple y fácil de solicitar; puede usar este paquete múltiples veces para las licencias de cortafuegos VM-Series, según los implemente.

Para usar la API, se asigna a cada cuenta de soporte una clave única. Cada llamada de API es una solicitud POST, y la solicitud debe incluir la clave de API para autenticar la solicitud al servidor de licencias. Cuando se autentica, el servidor de licencias envía la respuesta en formato json (content-type application/json).

 ©2024 Palo Alto Networks, Inc.

- Instalación de una clave de API de licencia
- Gestión de la clave de API de licencias
- Uso de la API de licencias
- Códigos de error de API de licencias

Instalación de una clave de API de licencia

La clave de API de licencia se puede utilizar para activar, cambiar o desactivar una licencia. Este procedimiento se aplica a un cortafuegos VM-Series o a una implementación de Panorama.

Debe tener **privilegios de superusuario** para recuperar la clave de API de licencia del Portal de asistencia al cliente y usar la CLI para instalar la clave en el cortafuegos o Panorama.

En panorama, cuando instala una clave de API de licencia, Panorama envía la clave API a sus dispositivos gestionados. Si el dispositivo gestionado tiene una clave API instalada, Panorama sobrescribe la clave API anterior con la nueva.

STEP 1 | Recupere la clave de API de la licencia del Portal de atención al cliente.

1. Inicie sesión en el portal de atención al cliente.
2. Seleccione **Products (Productos)** > **API Key Management (Gestión de clave de API)**.
3. Seleccione **Licensing API (API de licencias)** en el menú desplegable Seleccionar una clave de API.
4. Copie la clave de API.

tion Programming Interface (API) key is a unique identifier that authenticates a user or app calling Palo Alto Networks REST APIs. Each
ific Palo Alto Networks service. For example, Licensing API key work only with Licensing APIs, and Threat Vault API keys work only with

PI key Licensing API

ing APIs to manage firewall licenses (e.g., renew licenses, register auth codes, retrieve licenses attached to auth codes, deactivate licens

Licensing API key, click the Enable link below. You can also revoke an API key or regenerate an API key (which revokes the previous API

ate 12/06/2024

Extend Regenerate

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Use la CLI para instalar la clave de API copiada en el paso anterior. Pegue la clave en la solicitud:

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

La máquina virtual se reiniciará después de establecer la clave de API dentro de una máquina virtual.

STEP 3 | (opcional) Para reemplazar una clave de API de desactivación de licencia, use el siguiente comando de CLI para eliminar una clave de API instalada.

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

Si elimina la clave de API, debe instalar otra clave de desactivación de licencias antes de poder desactivar las licencias.

Gestión de la clave de API de licencias

Para obtener la clave API requerida para usar la API de licencia, su cuenta debe tener privilegios de superusuario en el portal de atención al cliente. La misma clave se utiliza para activar y desactivar la licencia.

La fecha de vencimiento de la clave API es la misma que la de la última suscripción en su cuenta de asistencia técnica. Si renueva sus suscripciones actuales y necesita restablecer la fecha de vencimiento de la clave API, puede volver a generar una clave (y reemplazar la clave existente con esta nueva clave siempre que la haya usado) o ponerse en contacto con la asistencia al cliente de Palo Alto Networks para obtener ayuda para ampliar el término de su clave API existente.

STEP 1 | Obtenga su clave de API de licencias.

1. Inicie sesión en el Portal de asistencia técnica de Palo Alto Networks con una cuenta que tenga privilegios de superusuario.
2. Seleccione **Products (Productos)** > **Assets (Activos)** > **API Key Management (Gestión de clave de API)**.
3. Haga clic en **Enable (Habilitar)** para ver su clave y copiarla para su uso. Una vez que genera una clave, la tecla se activa hasta que la regenere o deshabilite.

STEP 2 | Regenere o revoque la clave de API.

1. Puede regenerar una nueva clave de API o revocar el uso de la clave.
   - Haga clic en **Regenerate (Regenerar)** para generar una nueva clave. Si sospecha que una clave de API puede estar comprometida, puede generar una nueva clave. La regeneración invalida automáticamente la clave anterior.
   - Seleccione **Disable (Deshabilitar)** si no tiene previsto usar la clave. La deshabilitación de la clave API la revoca.

Uso de la API de licencias

El URI base para acceder a la API de licencia es https://api.paloaltonetworks.com/api/license; en función de la tarea que desee realizar, por ejemplo, activar licencias, desactivar licencias o rastrear el uso de licencias: la URL cambiará.

Una solicitud de API debe usar el método HTTP POST y usted debe incluir la clave API en el encabezado de solicitud HTTP apikey y pasar los parámetros de solicitud como datos de formulario codificados en URL con `content-type application/x-www-form-urlencoded`.

 ©2024 Palo Alto Networks, Inc.

La versión de la API es opcional y puede incluir los siguientes valores: 0 o 1. Si se especifica, debe incluirse en el encabezado de solicitud HTTP de `versión`. La versión actual de la API es 1; si no especifica una versión o especifica la versión 0, la solicitud usa la versión actual de la API.

Todas las respuestas de API se presentan en json.

Antes de comenzar, obtenga su clave de API de licencias y cópiela en su unidad local. Esto es necesario antes de poder realizar cualquiera de las siguientes tareas:

- Activación de licencias
- Desactivación de licencias
- Seguimiento del uso de licencia

Activación de licencias

Encabezado: apikey

Parámetros: `uuid`, `cpuid`, `authCode`, `memoria`, `serialNumber` y `vCPU`

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

Los parámetros uuid, cpuid, authCode y serialNumber se aplican a todas las licencias VM-Series, independientemente de la versión de PAN-OS.

Los parámetros opcionales de `memoria` y `vCPU` solo se aplican a vCPU flexibles (PAN-OS 10.0.4 y posteriores).

- Para la activación inicial de la licencia, proporcione los parámetros en la solicitud de API. Por ejemplo:

```
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 no ha guardado las claves de licencia o ha tenido problemas de conexión de red durante la activación inicial de la licencia, puede recuperar las licencias de un cortafuegos que haya activado previamente.

  En la solicitud de API, proporcione `cpuid` y `uuid`, o proporcione el `serialNumber` del cortafuegos.

Muestra de solicitud para activación de licencia inicial usando 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
```

Muestra de respuesta de API:

```
[{"lfidField":"13365773","partidField":"PAN-SVC-PREM-
VM-300","featureFi--eld": "Premium","feature_descField":"Soporte
 telefónico 24 x 7; servicio de hardware de
 sustitución avanzado","keyField":"m4iZEL1t3n6Oa
+6ll1L7itDZTphYw48N1AMOZXutDgExC5f5pOA52+Qg1jmAxanB
```

 ©2024 Palo Alto Networks, Inc.

```
\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
\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>
```


El feature_Field de la respuesta indica el tipo de clave que sigue en el keyField. Copie cada clave en un archivo de texto y guárdelo con la extensión .key. Debido a que la clave está en formato json, no tiene nuevas líneas. Asegúrese de convertirlo a nuevas líneas si su analizador lo requiere. Asegúrese de dar un nombre adecuado a cada clave y guardarlo en la /carpeta de licencia del paquete de arranque. Por ejemplo, incluya el código de autenticación con el tipo de clave para nombrarlo como I3306691_1pa-vm.key (para la clave de licencia de capacidad), I3306691_1threat.key (para la clave de licencias de prevención de amenazas), I3306691_1wildfire.key (para la clave de licencias de suscripción WildFire).

Solicitud de API de muestra para recuperar licencias activadas previamente con Curl:

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

Muestra de respuesta de 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,
```


 ©2024 Palo Alto Networks, Inc.

```
 "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
\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>
```


Desactivación de licencias

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

Parámetros: encryptedToken

Para desactiva la licencia o licencias de un cortafuegos que no tiene acceso directo a internet, debe generar la archivo de token de licencia localmente en el cortafuegos y utilizar este archivo de token en la solicitud de API. Para obtener más información sobre cómo generar el archivo de token de licencia, consulte Desactivar VM o Desactivar licencia (créditos NGFW de software) y Desactivación de la licencia de una función o suscripción con CLI.

Encabezado: apikey

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

Muestra de solicitud de API para activación de licencia inicial usando Curl:

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

Muestra de respuesta de 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}]$
```


 ©2024 Palo Alto Networks, Inc.

Seguimiento del uso de licencia

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

Parámetros: authCode

Encabezado: apikey

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

Muestra de solicitud de API para seguimiento de licencia usando Curl:

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

Muestra de respuesta de 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"}]}.....
```

Códigos de error de API de licencias

Los códigos de error de HTTP que devuelve el servidor de licencias son:

- 200 Éxito
- 400 Error
- 401 Clave API no válida
- 500 Error de servidor

 ©2024 Palo Alto Networks, Inc.

¿Qué ocurre cuando la licencia caduca?

Las subscripciones y licencias del cortafuegos VM-Series de Palo Alto Networks proporcionan al cortafuegos una funcionalidad adicional o acceso a un servicio proporcionado en la nube de Palo Alto Networks. Cuando una licencia está a 30 días de su vencimiento, se muestra un mensaje de advertencia en el log del sistema todos los días hasta que renueve la suscripción o caduque. Cuando la licencia caduca, algunas suscripciones siguen funcionando con una capacidad limitada y otras dejan de funcionar por completo. Aquí puede conocer qué sucede cuando caduca cada suscripción.

El momento preciso de vencimiento de la licencia es a las 12:00 a.m., hora del meridiano de Greenwich (GMT) de la fecha de vencimiento. Por ejemplo, si la fecha de vencimiento de su licencia es el 20 de diciembre de 2024, la funcionalidad cesará a las 12:00 a. m. GMT del 20 de diciembre de 2024. Todas las funciones relacionadas con la licencia funcionan en GMT, independientemente de la zona horaria configurada en el cortafuegos.

(Licencia de Panorama) Si la licencia de asistencia técnica vence, Panorama aún puede gestionar cortafuegos y recopilar logs, pero las actualizaciones de software y contenido no estarán disponibles. Las versiones de contenido y software de Panorama deben ser las mismas o superiores a las versiones de los cortafuegos gestionados o, de lo contrario, se producirán errores. Para obtener más información, consulte Compatibilidad de versiones de Panorama, el recopilador de logs, el cortafuegos y WildFire.

Licencia	Comportamiento de caducidad
VM-SERIES	**Puede seguir realizando las siguientes acciones:** Puede seguir configurando y utilizando el cortafuegos que implementó antes de que caduque la licencia sin cambios en la capacidad de la sesión. El cortafuegos no se reiniciará automáticamente y no causará una interrupción en el tráfico. Sin embargo, si el cortafuegos se reinicia por cualquier motivo, este entra en un estado sin licencia. Aunque no tiene licencia, un cortafuegos admite un máximo de 1.200 sesiones. No se restringen otras características ni opciones de configuración del plano de gestión.
Threat Prevention	Aparecen alertas en el log del sistema que indican que la licencia ha caducado. **Puede seguir realizando las siguientes acciones:** • Utilice firmas instaladas en el momento en que caducó la licencia, a no ser que instale una nueva actualización de contenido solo para aplicaciones, ya sea manualmente o como parte de una programación automática. Si lo hace, la actualización eliminará sus firmas de amenazas existentes y ya no recibirá protección contra ellas. • Utilizar y modificar App-ID™ personalizado y firmas de amenazas.

 ©2024 Palo Alto Networks, Inc.

Licencia	Comportamiento de caducidad
	Ya no puede realizar las siguientes acciones: • Instalar nuevas firmas. • Revertir las firmas a versiones anteriores.
DNS Security	**Puede seguir realizando las siguientes acciones:** • Usar firmas DNS locales si tiene una licencia de Threat Prevention activa. **Ya no puede realizar las siguientes acciones:** • Obtener nuevas firmas DNS.
Filtrado avanzado de URL/ filtrado de URL	**Puede seguir realizando las siguientes acciones:** • Aplicar la política con categorías de URL personalizadas. • Aplique la política utilizando las categorías de PALO ALTO NETWORKS-DB que estaban en su caché local cuando caducó la licencia. **Ya no puede realizar las siguientes acciones:** • Obtener actualizaciones en las categorías de PAN-DB almacenadas en caché. • Conéctese a la base de datos de filtrado de URL de PAN-DB. • Obtener categorías de PAN-DB de URL no almacenadas en caché. • Analice las solicitudes de URL en tiempo real mediante el filtrado de URL avanzado.
WildFire	**Puede seguir realizando las siguientes acciones:** • Envíe Portable ejecutable (PE) para análisis. • Obtener actualizaciones de firmas cada 24-48 horas si dispone de una suscripción a Threat Prevention activa. **Ya no puede realizar las siguientes acciones:** • Proporcionar actualizaciones de cinco minutos a través de las nubes pública y privada de WildFire. • Reenviar tipos de archivos avanzados como APK, archivos Flash, PDF, archivos de Microsoft Office, applets Java, archivos Java (.jar y .class) y enlaces de correo electrónico HTTP/HTTPS contenidos en mensajes de correo electrónico SMTP y POP3. • Usar la API de WildFire. • Utilice un dispositivo WildFire para alojar una nube privada de WildFire o una nube híbrida de WildFire.

 ©2024 Palo Alto Networks, Inc.

Licencia	Comportamiento de caducidad
AutoFocus	**Puede seguir realizando las siguientes acciones:** • Usar la lista dinámica externa con datos de AutoFocus para un periodo de gracia de tres meses. **Ya no puede realizar las siguientes acciones:** • Acceder al portal de AutoFocus. • Ver el resumen de inteligencia de AutoFocus para el log de supervisión o los artefactos de ACC.
Cortex Data Lake	**Puede seguir realizando las siguientes acciones:** • Almacenar datos de logs durante un periodo de gracia de 30 días. Después de ese periodo, se eliminarán. • Reenviar logs a Cortex Data Lake hasta que acabe el periodo de gracia de 30 días.
GlobalProtect	**Puede seguir realizando las siguientes acciones:** • Utilice la aplicación los endpoints que ejecutan Windows o macOS • Configurar una o varias puertas de enlace internas y externas. **Ya no puede realizar las siguientes acciones:** • Acceder a la aplicación Linux OS ni a la aplicación móvil para iOS, Android, Chrome OS y Windows 10 UWP. • Usar las puertas de enlace externas de IPv6. • Ejecutar comprobaciones HIP. • Usar VPN sin cliente. • Aplicar túneles divididos sobre la base del dominio de destino, proceso de cliente y aplicación de transmisión de vídeo.
Soporte	**Ya no puede realizar las siguientes acciones:** • Recibir actualizaciones de software. • Descargar imágenes de VM. • Beneficiarse del soporte técnico.

 ©2024 Palo Alto Networks, Inc.

Licencias para proveedores de servicios de seguridad en la nube (CSSP)

El programa de socios de CSSP de Palo Alto Networks permite a los proveedores de servicios brindar seguridad como servicio o como aplicación alojada a sus clientes finales. Las ofertas de licencias que proporciona Palo Alto Networks para socios autorizados de proveedores de servicios de seguridad en la nube (CSSP) son diferentes de las ofertas para usuarios empresariales.

Para los socios de CSSP, Palo Alto Networks es compatible con un modelo basado en el uso para los cortafuegos VM-Series combinados con suscripciones y asistencia técnica. Los socios de CSSP pueden combinar una licencia de capacidad basada en términos para los Modelos VM-Series con una opción de licencias de suscripción para prevención de amenazas, filtrado de URL, AutoFocus, GlobalProtect y WildFire, y derechos a asistencia técnica que brindan acceso al soporte técnico y a actualizaciones de software. Si ha planificado la implementación de los cortafuegos en una configuración de HA, puede optar por la rentable opción de alta disponibilidad.

- Obtención de los Códigos de autenticación para los paquetes de licencia CSSP
- Registro del cortafuegos VM-Series con un código de autenticación CSSP
- Adición de información del cliente final para un cortafuegos VM-Series registrado

Obtención de los Códigos de autenticación para los paquetes de licencia CSSP

Para convertirse en un socio de CSSP, debe inscribirse en el programa de socios de CSSP de Palo Alto Networks. Para obtener información sobre cómo inscribirse en el programa CSSP, comuníquese con el responsable comercial de canal de Palo Alto Networks. Si está inscrito, el portal de soporte de red de Palo Alto proporciona herramientas que le permiten seleccionar un paquete de licencia, realizar un seguimiento del uso de la licencia y aplicar los derechos de licencia.

Un paquete de licencia es una combinación de las siguientes opciones:

- Términos de uso: las opciones de pago por uso son por hora, mensuales, 1 año y 3 años.
- Modelo de cortafuegos VM-Series: Los modelos VM-100, VM-200, VM-300 y VM-1000-HV que le dan el número de modelo y las capacidades asociadas con cada modelo.
- Paquete de suscripción: las tres opciones son básico, paquete 1 y paquete 2. La opción básica no incluye ninguna suscripción; el paquete 1 tiene la licencia de prevención de amenazas que incluye IPS, AV, prevención de malware; el paquete 2 tiene las licencias de Prevención de amenazas (incluye IPS, AV, prevención de malware), Seguridad DNS, GlobalProtect, WildFire y PAN-DB URL Filtering.
- Nivel de soporte: soporte premium o backline.
- cortafuegos redundantes: la opción es de alta disponibilidad (HA) o sin HA. Esta opción es una opción rentable si planifica implementar un par de cortafuegos redundantes.

La oferta PAN-VM-300-SP-PREM-BND1-YU, por ejemplo, es un paquete de un año que incluye el VM-300 con soporte premium y el paquete de suscripción 1. Cada paquete admite hasta un máximo de 10.000 instancias del cortafuegos VM-Series.

Después de seleccionar su paquete de licencia, recibirá un correo electrónico con su código de autenticación; el proceso de gestión puede tardar hasta 48 horas.

©2024 Palo Alto Networks, Inc.

STEP 1 | Inicie sesión en el sitio web de asistencia de Palo Alto Networks con sus credenciales de cuenta. Si necesita una cuenta nueva, consulte Creación de una cuenta de asistencia técnica.

STEP 2 | Seleccione **CSSP** > **Order History (Historial de pedido)** para ver la lista de códigos de autenticación registrados en su cuenta de asistencia técnica.

A medida que implementa cortafuegos, debe registrar cada instancia del cortafuegos contra un código de autenticación.

Registro del cortafuegos VM-Series con un código de autenticación CSSP

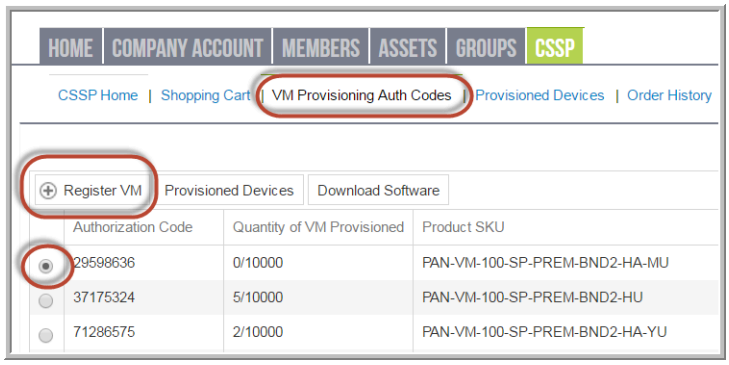
Para activar la licencia en su cortafuegos VM-Series, deberá haber implementado el cortafuegos VM-Series y haber completado la configuración inicial. Como socio de CSSP, puede elegir entre las siguientes opciones para registrar un cortafuegos:

- API: Use la API de licencias Si tiene un script personalizado o un servicio de orquestación. Con esta opción, el cortafuegos no necesita acceso directo a internet.
- Bootstrap: Utilice esta opción para configurar automáticamente el cortafuegos y activar la licencia en el primer arranque. Consulte Arranque del cortafuegos VM-Series.
- Interfaz web de cortafuegos: Puede Activar la licencia para el cortafuegos VM-Series (versión autónoma) usando la interfaz web del cortafuegos. Este flujo de trabajo es válido para cortafuegos con o sin acceso a internet.
- Portal de atención al cliente: Use esta opción para registrar manualmente el cortafuegos en el portal de atención al cliente de Palo Alto Networks, como se muestra a continuación.

STEP 1 | Inicie sesión en el sitio web de asistencia de Palo Alto Networks con sus credenciales de cuenta. Si necesita una cuenta nueva, consulte Creación de una cuenta de asistencia técnica.

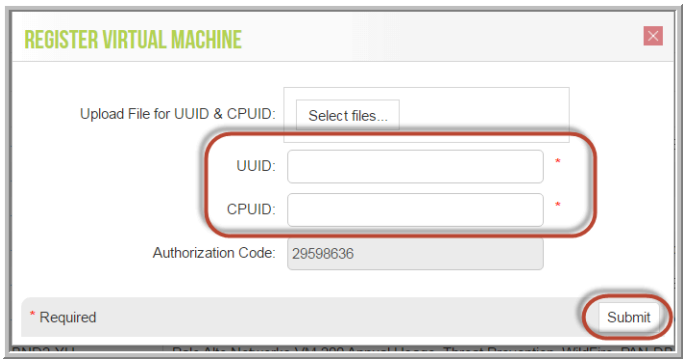
STEP 2 | Seleccione **CSSP** > **Order History (Historial de pedido)** para ver la lista de códigos de autenticación registrados en su cuenta de asistencia técnica.

STEP 3 | Seleccione **CSSP** > **VM Provisioning Auth Codes (Códigos de autenticación de provisión de VM)**, seleccione un **Authorization Code (Código de autorización)** y haga clic en **Register VM (Registrar VM)**.



 ©2024 Palo Alto Networks, Inc.

STEP 4 | Introduzca el **UUID** y **CPUID** de la instancia de VM y haga clic en **Submit (Enviar)**. El portal generará un número de serie para el cortafuegos.



Puede hacer un seguimiento del número de cortafuegos VM-Series que se han implementado y el número de licencias que siguen disponibles con cada código de autenticación. Para ver el número total de cortafuegos registrados con un código de autenticación específico, seleccione ***CSSP > VM Provisioning Auth Codes (Códigos de autenticación de provisión de VM)****, luego seleccione un* ***Authorization Code (Código de autorización)*** *y haga clic en* ***Provisioned Devices (Dispositivos provisionados)****.*

Adición de información del cliente final para un cortafuegos VM-Series registrado

Para titulares de licencias de CSSP, después de registrar el cortafuegos, puede usar el portal de asistencia técnica de Palo Alto Networks o la API de licencias para vincular el número de serie del cortafuegos VM-Series con el cliente al que se proporcionó el cortafuegos.

- Adición de información del cliente final para un cortafuegos VM-Series registrado (Portal de atención al cliente). El portal de atención al cliente se autentica con nombre de usuario y contraseña.
- Adición de información del cliente final para un cortafuegos VM-Series registrado (API). La API se autentica con la clave de la API de licencias.

Adición de información del cliente final para un cortafuegos VM-Series registrado (Portal de atención al cliente)

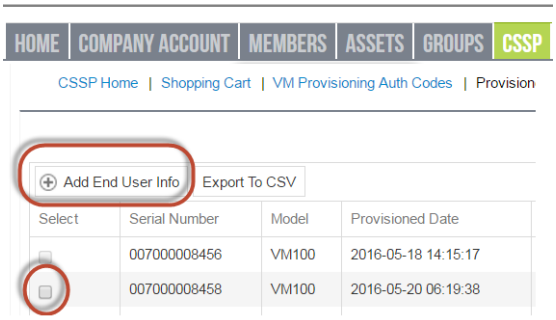
Complete el siguiente procedimiento para añadir información del cliente final para un cortafuegos registrado a través del Portal de atención al cliente.

STEP 1 | Inicie sesión en el sitio web de asistencia de Palo Alto Networks con sus credenciales de cuenta.

STEP 2 | Seleccione **CSSP** > **Provisioned Devices (Dispositivos provisionados)**.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Seleccione el **Serial Number (Número de serie)** y haga clic en **Add End User Info (Añadir información de usuario final)**.

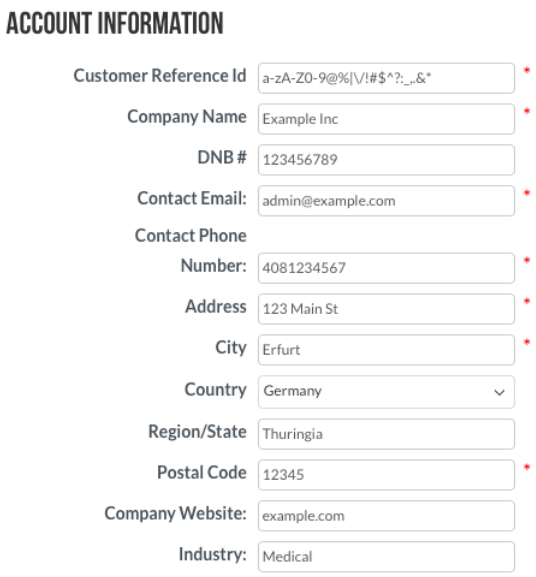


 ©2024 Palo Alto Networks, Inc.

STEP 4 | Introduzca la **Account Information (Información de la cuenta)** para el cliente de la siguiente manera.

- ID de referencia del cliente: Obligatorio
- Nombre de la empresa: Obligatorio
- N.º de DNB: Número del Sistema universal de numeración de datos (DUNS)
- Correo electrónico de contacto: Obligatorio, dirección de correo electrónico de usuario final
- Número de teléfono del contacto: Número de teléfono del usuario final
- Address: Obligatorio, dirección del usuario final
- País: Obligatorio, ISO Código de país de 2 letras
- Ciudad: Obligatorio, nombre de la ciudad del usuario final
- Región/Estado: Obligatorio; para los Estados Unidos y Canadá, debe introducir un código de subdivisión de 2 letras ISO; para todos los demás países, cualquier cadena de texto es válida
- Código postal: Obligatorio, código postal del usuario final
- Página Web de la empresa: URL del sitio web del usuario final
- Sector: Tipo de sector del usuario final, por ejemplo, redes o consultoría

Haga clic en **Submit (Confirmar)** para guardar el perfil.



*Después de añadir la información de la cuenta, puede encontrar todos los cortafuegos registrados para un cliente. En **Search Existing End User (Buscar usuario final existente)**, introduzca la ID del cliente o el nombre del cliente y haga clic en **Search (Buscar)** para encontrar todos los cortafuegos aprovisionados para el cliente.*

Adición de información del cliente final para un cortafuegos VM-Series registrado (API)

La URL para acceder a la API es https://api.paloaltonetworks.com/api/license/ReportEndUserInfo.

Una solicitud de API debe usar el método HTTP POST y debe incluir encabezados de solicitudes HTTP que incluyan la clave API y especifiquen el tipo de contenido como JSON. Las respuestas de API están en formato JSON.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Obtenga su clave de API de licencias.

STEP 2 | Use la API ReportEndUserInfo para agregar información de usuario final para un cortafuegos VM-Series que está registrado en un CSSP.

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

Encabezados:

- Tipo de contenido: application/json
- apiKey: *Clave API*

Parámetros:

- `SerialNumbers`: Obligatorio, proporcione al menos un número de serie de cortafuegos válido
- `CustomerReferenceId`: Obligatorio
- `CompanyName`: Obligatorio, nombre de la empresa del usuario final
- `DnBNumber`: Número del Sistema universal de numeración de datos (DUNS)
- `PhoneNumber`: Número de teléfono del usuario final
- `EndUserContactEmail`: Obligatorio, dirección de correo electrónico de usuario final
- `Address`: Obligatorio, dirección del usuario final
- `Country`: Obligatorio, ISO Código de país de 2 letras
- `City`: Obligatorio, nombre de la ciudad del usuario final
- `Región/Estado`: Obligatorio; para los Estados Unidos y Canadá, debe introducir un código de subdivisión de 2 letras ISO; para todos los demás países, cualquier cadena alfa es válida
- `PostalCode`: Obligatorio, código postal del usuario final
- `Industry`: Tipo de sector del usuario final, por ejemplo, redes o consultoría
- `WebSite`: URL del sitio web del usuario final
- `CreatedBy`: Sistema o persona que envía esta información

Solicitud de muestra para añadir información del usuario final para un cortafuegos VM-Series registrado usando 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":
```

 ©2024 Palo Alto Networks, Inc.

```
 "4081234567", "WebSite": "example.com", "EndUserContactEmail":
 "admin@example.com", "CreatedBy": "Jane Doe"}'
```

Muestra de respuesta de API:

```
"{"Message": "Información del usuario final actualizada
 correctamente"}"
```

Si recibe un error, consulte Códigos de error de API de licencias.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Configuración un cortafuegos VM-Series en un servidor ESXi

El cortafuegos VM-Series se distribuye en el formato abierto de alianza de virtualización (Open Virtualization Alliance, OVA), que es un método estándar de empaquetamiento e implementación de máquinas virtuales. Puede instalar esta solución en cualquier dispositivo x86 capaz de ejecutar VMware ESXi.

Para implementar un cortafuegos VM-Series debe estar familiarizado con VMware y vSphere, incluidas las redes vSphere, la instalación y configuración de host ESXi y la implementación de máquinas virtuales invitadas.

Si desea automatizar el proceso de implementación de un cortafuegos VM-Series, puede crear una plantilla estándar de referencia con la configuración y políticas óptimas y usar la API de vSphere y la API XML de PAN-OS para implementar rápidamente nuevos cortafuegos VM-Series en su red.

Consulte los siguientes temas para obtener información:

- Implementaciones compatibles en el hipervisor vSphere de VMware (ESXi)
- VM-Series en requisitos y limitaciones del sistema ESXi
- Instalación de un cortafuegos VM-Series en el hipervisor vSphere de VMware (ESXi)
- Supervisión de VM en vCenter
- Solución de problemas de implementaciones de ESXi
- Ajuste de rendimiento de VM-Series para ESXi

Implementaciones compatibles en el hipervisor vSphere de VMware (ESXi)

Puede implementar una o varias instancias del cortafuegos VM-Series en el servidor ESXi. La ubicación del cortafuegos VM-Series en la red dependerá de su topología. Seleccione de las siguientes opciones (para entornos que no usan VMware NSX):

- **Un cortafuegos VM-Series por host ESXi:** todos los servidores VM del host ESXi atraviesan el cortafuegos antes de salir del host por la red física. Los servidores VM se adjuntan al cortafuegos a través de los conmutadores estándar virtuales. Los servidores invitados no tienen ninguna otra conectividad de red, por lo que el cortafuegos visualiza y controla todo el tráfico del host ESXi. Una variación de este caso de uso es también exigir que todo el tráfico fluya por el cortafuegos, incluido el tráfico de servidor a servidor (tráfico horizontal) en el mismo host ESXi.
- **Un cortafuegos VM-Series por red virtual**: implemente un cortafuegos VM-Series para cada red virtual. Si diseñó su red de modo que uno o más hosts ESXi tengan un grupo de máquinas virtuales que pertenezcan a la red interna, un grupo que pertenezca a la red externa y otro a DMZ, puede implementar un cortafuegos VM-Series para salvaguardar los servidores de cada grupo. Si un grupo o red virtual no comparte un conmutador virtual o grupo de puertos con otra red virtual, estará totalmente aislado de las demás redes virtuales del host. Como no hay otra ruta física o virtual a ninguna otra red, los servidores de cada red virtual deben usar el cortafuegos para comunicarse con cualquier otra red. El cortafuegos tiene visibilidad y control sobre todo el tráfico que abandona el conmutador virtual (estándar o distribuido) conectado a cada red virtual.
- **Entorno híbrido**: se usan hosts físicos y virtuales. El cortafuegos VM-Series puede remplazar un dispositivo de cortafuegos físico en una ubicación de agregación tradicional. Un entorno híbrido obtiene los beneficios de una plataforma de servidor común para todos los dispositivos y desvincula las dependencias de actualización de software y hardware.

Continúe con VM-Series en requisitos y limitaciones del sistema ESXi e Instalación de un cortafuegos VM-Series en el hipervisor vSphere de VMware (ESXi).

 ©2024 Palo Alto Networks, Inc.

VM-Series en requisitos y limitaciones del sistema ESXi

Esta sección enumera los requisitos y las limitaciones del cortafuegos VM-Series en el hipervisor vSphere de VMware (ESXi). Para implementar el cortafuegos VM-Series, consulte Instalación de un cortafuegos VM-Series en el hipervisor vSphere de VMware (ESXi).

- VM-Series en requisitos del sistema de ESXi
- VM-Series en limitaciones del sistema de ESXi

VM-Series en requisitos del sistema de ESXi

Puede crear e implementar una o varias instancias del cortafuegos VM-Series en el servidor ESXi. Como todas las instancias del cortafuegos necesitan una asignación de recursos mínima (cantidad de CPU, memoria y espacio en disco) en el servidor ESXi, asegúrese de cumplir las especificaciones que aparecen a continuación para garantizar un rendimiento óptimo.

El cortafuegos VM-Series tiene los siguientes requisitos:

- La CPU del host debe ser una CPU Intel o AMD basada en x86 con extensión de virtualización.
- Consulte la Matriz de compatibilidadpara versiones compatibles de ESXi. La compatibilidad para la versión vmx se basa en el OVA que utiliza para implementar el cortafuegos VM-Series, y no es posible modificar esta versión. La actualización o cambio de versión del software VM-Series a una versión anterior no cambia la versión vmx que se habilitó al inicio.
- Consulte Requisitos del sistema VM-Series para ver los requisitos mínimos de hardware para su modelo VM-Series.
- Mínimo de dos interfaces de red (vNIC). Una es una vNIC dedicada para la interfaz de gestión y la otra para la interfaz de datos. A continuación, podrá añadir hasta ocho vNIC más para el tráfico de datos. Para añadir interfaces adicionales, use VLAN Guest Tagging (VGT) en el servidor ESXi o configure subinterfaces en el cortafuegos.

  La dirección MAC asignada por hipervisor está habilitada de forma predeterminada. vSphere asigna una dirección MAC vNIC única a cada interfaz del plano de datos del cortafuegos serie VM. Si deshabilita las direcciones MAC asignadas por hipervisor, el cortafuegos VM-Series asigna cada interfaz de una dirección MAC desde su propio grupo. Debido a que esto provoca que difieran las direcciones MAC de cada interfaz, debe habilitar el modo promiscuo en el grupo de puertos del conmutador virtual al que las interfaces del plano de datos del cortafuegos están adjuntas; esto permite que el cortafuegos reciba tramas (consulte Aprovisionamiento del cortafuegos VM-Series en un servidor ESXi. Si no está habilitado ni el modo promiscuo ni la dirección MAC asignada por el hipervisor, el cortafuegos no recibe tráfico. Esto se debe a que vSphere no reenvía tramas a una máquina virtual cuando la dirección MAC de destino de la trama y la dirección MAC vNIC no coinciden.
- El Kit de desarrollo del plano de datos (DPDK) está habilitado de forma predeterminada en los cortafuegos VM-Series en ESXi. Para obtener más información acerca de DPDK, consulte Habilitación de VPN en ESXi.

 ©2024 Palo Alto Networks, Inc.

- Para obtener el mejor rendimiento del cortafuegos VM-Series, puede realizar los siguientes ajustes en el host antes de implementar el cortafuegos VM-Series. Consulte Ajuste de rendimiento de VM-Series para ESXi para más información.
  - **Habilite DPDK**. DPDK permite que el host procese los paquetes más rápido eludiendo el kernel de Linux. En cambio, las interacciones con NIC se realizan utilizando controladores y bibliotecas DPDK.
  - **Habilite SR-IOV**. La virtualización de E/S de raíz única (SR-IOV) permite que un único dispositivo físico PCIe bajo un único puerto raíz parezca ser múltiples dispositivos físicos separados para el hipervisor o el invitado.

    No configure un vSwitch en el puerto físico en el que habilita SR-IOV. Para comunicarse con el host u otras máquinas virtuales de la red, el cortafuegos VM-Series debe tener acceso exclusivo al puerto físico y a las funciones virtuales asociadas (associated virtual functions, VF) en esa interfaz.
  - **Habilite el soporte de colas múltiples para NIC**. Las colas múltiples permiten que el rendimiento de la red escale con el número de vCPU y permite el procesamiento paralelo de paquetes a través de la creación de múltiples colas TX y RX.

VM-Series en limitaciones del sistema de ESXi

La funcionalidad del cortafuegos VM-Series es muy parecida a las de los cortafuegos de hardware de Palo Alto Networks, pero con las siguientes limitaciones:

- No utilice la funcionalidad de instantáneas de VMware en VM-Series en ESXi. Las instantáneas pueden afectar el rendimiento y provocar pérdida del paquete intermitente e inconsistente. Consulte la recomendación de VMware para el uso de instantáneas.

  Si necesita las copias de seguridad de la configuración, utilice Panorama o desde el cortafuegos, seleccione **Export named configuration snapshot (Exportar instantáneas de configuración con nombre)** (Device [Dispositivo] > Set up [Configuración] > Operations [Operaciones]). Si se usa **Export named configuration snapshot (Exportar instantáneas de configuración con nombre)**, se exporta la configuración activa (`running-config.xml`) en el cortafuegos y se permite que la guarde en cualquier ubicación de red.
- Se recomienda usar núcleos CPU dedicados.
- La Supervisión de enlaces de alta disponibilidad (HA) no se admite en los cortafuegos VM-Series en ESXi. Utilice la supervisión de ruta para comprobar la conectividad con una dirección IP de destino o con la dirección IP de siguiente salto.
- Es posible configurar hasta 10 puertos en total; esta es una limitación de VMware. Se utilizará un puerto para el tráfico de gestión y hasta 9 para el tráfico de datos.
- Únicamente se admite el controlador vmxnet3.
- Los sistemas virtuales no son compatibles.
- La tecnología vMotion del cortafuegos VM-Series es compatible en vSphere 6.5, 6.7 y 7.0 si los hosts ESXi tienen una configuración de CPU homogénea. Se requiere PAN-OS 9.1.6 y posterior para Utilice vMotion para mover el cortafuegos VM-Series entre hosts instalados en vSphere 6.5 o 6.7.
- La transmisión forjada y el modo promiscuo deben estar habilitados en los grupos de puertos ESXi vSwitch conectados a las interfaces de Capa 2 y vwire en el cortafuegos VM-Series.

 ©2024 Palo Alto Networks, Inc.

- Para usar dispositivos PCI con el cortafuegos VM-Series en ESXi, la E/S asignada en la memoria (MMIO) debe ser inferior a 4 GB. Puede deshabilitar la MMIO superior a 4 GB en el BIOS de su servidor. Esto es una limitación de ESXi.
- Cuando se utiliza ESXi 7.0, las interfaces no aparecen cuando se conectan las funciones virtuales a máquinas virtuales con acceso de dispositivo PCI.

 ©2024 Palo Alto Networks, Inc.

Instalación de un cortafuegos VM-Series en el hipervisor vSphere de VMware (ESXi)

Para instalar un cortafuegos VM-Series debe tener acceso a la plantilla Open Virtualization Alliance format (OVA). Use el código de autenticación que recibió con el correo electrónico de cumplimentación del pedido para registrar su cortafuegos VM-Series y descargar la plantilla de OVA. La plantilla de OVA es un archivo zip que se contiene tres tipos de archivos:

- .mf: El archivo de manifiesto de OVF que contiene los resúmenes de SHA-1 de los archivos individuales del paquete
- .ovf: El archivo descriptivo de OVF que contiene todos los metadatos del paquete y su contenido
- .vmdk: El archivo de imagen de disco que contiene la versión virtual del cortafuegos

Complete las siguientes tareas para instalar y configurar el cortafuegos VM-Series en ESXi.

- Planificación de las interfaces para la VM-Series para ESXi
- Aprovisionamiento del cortafuegos VM-Series en un servidor ESXi
- Configuración inicial en VM-Series en ESXi
- (Opcional) Añadir espacio en disco adicional al cortafuegos VM-Series
- Uso de VMware Tools en el cortafuegos VM-Series en ESXi y vCloud Air
- Utilice vMotion para mover el cortafuegos VM-Series entre hosts
- Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión en ESXi

Planificación de las interfaces para la VM-Series para ESXi

La planificación de la asignación de los controladores de interfaz de red virtuales (vNIC) e interfaces del cortafuegos VM-Series, puede evitar reinicios y problemas de configuración. La siguiente tabla describe la asignación predeterminada entre los vNIC de VMware y las interfaces de VM-Series cuando los 10 vNIC están habilitados en ESXi.

VMware vNIC	Interfaces de 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)

©2024 Palo Alto Networks, Inc.

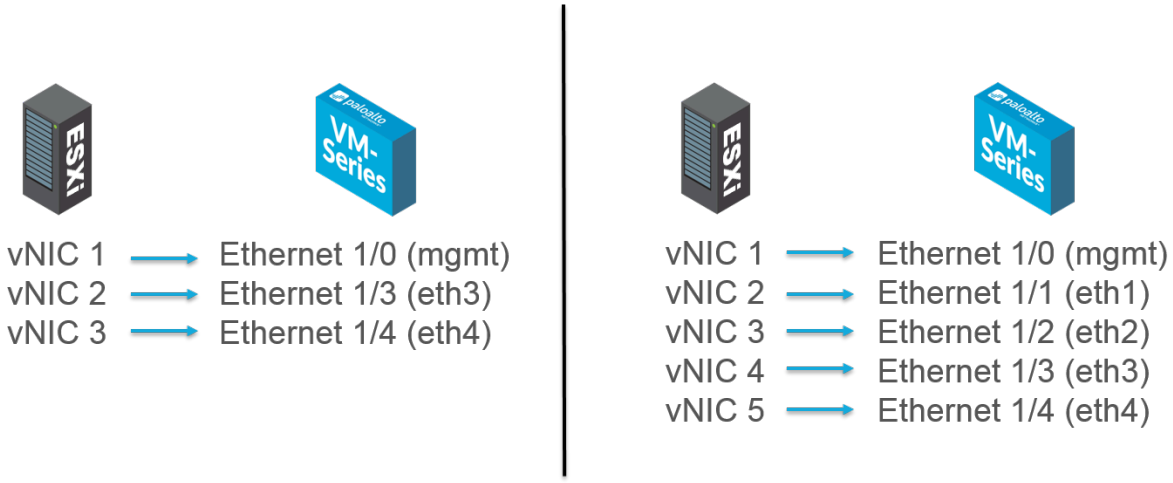
VMware vNIC	Interfaces de VM-Series
8	Ethernet 1/7 (eth7)
9	Ethernet 1/8 (eth8)
10	Ethernet 1/9 (eth9)

La asignación en el cortafuegos VM-Series sigue siendo la misma sin importar qué vNIC añada en ESXi. Las interfaces que active en el cortafuegos siempre toman el próximo vNIC disponible en ESXi.

En el siguiente diagrama, eth3 y eth4 en el cortafuegos VM-Series están emparejados con los vNIC 2 y 3 en ESXi, y se quita la asignación de eth1 y eth2, como se muestra a la izquierda.

Si desea añadir dos interfaces adicionales y al mismo tiempo mantener la asignación actual, active vNIC 4 y 5 y reinicie el cortafuegos. La asignación vNIC existente se preserva porque añadió las interfaces después de la última interfaz asignada.

Si activa eth1 y eth2 en el cortafuegos VM-Series, las interfaces se reordenan automáticamente como se muestra a la derecha, lo que provoca una falta de coincidencia de asignación que afecta el tráfico.



Para evitar los problemas descritos en el ejemplo anterior, puede hacer lo siguiente:

- Cuando aprovisione el host ESXi por primera vez, active los nueve vNIC después del primero. La adición de todos los nueve vNIC como marcadores de posición antes de encender el cortafuegos VM-Series le permite usar cualquier interfaz VM-Series sin importar el orden.
- Si todos los vNIC están activos, no es necesario reiniciar cuando añade interfaces adicionales. Dado que cada vNIC en ESXi requiere que elija una red, puede crear un grupo de puertos vacíos como marcador de posición de red.
- No elimine los vNIC del cortafuegos VM-Series para evitar errores de asignación.

Aprovisionamiento del cortafuegos VM-Series en un servidor ESXi

Siga estas instrucciones para implementar el cortafuegos VM-Series en un servidor ESXi (independiente). Para implementar el cortafuegos VM-Series edición NSX, consulte Configuración del cortafuegos VM-Series en VMware NSX-T.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Descargue el archivo OVA.

Registre su cortafuegos VM-Series y obtenga un archivo OVA del sitio web de asistencia al cliente de Palo Alto Networks.

Los archivos OVA contienen la instalación básica. Cuando la instalación básica haya finalizado, debe descargar e instalar la versión más reciente de PAN-OS desde el portal de asistencia. Con ello se asegura de contar con los ajustes más recientes implementados desde la creación de la imagen básica. Para obtener instrucciones, consulte #unique_25.

STEP 2 | Antes de implementar el archivo OVA, configure los conmutadores estándar virtuales o conmutadores distribuidos virtuales que necesitará para el cortafuegos VM-Series.

Si está implementando el cortafuegos VM-Series con interfaces de Capa 3, su cortafuegos usa Direcciones MAC asignadas por el hipervisor *por defecto. Si elige deshabilitar el hipervisor asignado a la dirección MAC o si implementa el cortafuegos con capa 2, cable virtual o interfaces tap, debe configurar (establecer en* ***Accept [Aceptar]****) cualquier conmutador virtual que se adjunte al cortafuegos VM-Series para permitir los siguientes modos: modo promiscuo, cambios en direcciones MAC y transmisiones falsificadas.*

Configure un conmutador estándar virtual o un conmutador distribuido virtual con el objetivo de recibir tramas para el cortafuegos VM-Series.

Conmutador estándar virtual

1. Vaya a **Home (Inicio)** > **Hosts and Clusters (Hosts y clústeres)** y seleccione un host.
2. Haga clic en la pestaña **Configure (Configurar)** y vea **Virtual Switches (Conmutadores virtuales)**. Para cada conmutador virtual conectado al cortafuegos VM-Series, haga clic en **Properties (Propiedades)**.
3. Resalte el grupo de puertos correspondiente a un conmutador virtual y haga clic en **Edit Settings (Editar ajustes)**. En las propiedades de vSwitch, haga clic en la pestaña **Security (Seguridad)** y establezca **Promiscuous Mode, MAC Address Changes (Modo promiscuo, Cambios de dirección MAC)** y **Forged Transmits (Transmisiones falsificadas)** en **Accept (Aceptar)**; a continuación, haga clic en **OK (Aceptar)**. Este cambio se propaga a todos los grupos de puertos del conmutador virtual.

Conmutador distribuido virtual

1. Seleccione **Home (Inicio)** > **Networking (Redes)**. Seleccione el conmutador distribuido virtual y resalte el **Distributed Port Group (Grupo de puertos distribuido)** que desea editar.
2. Haga clic en **Edit Settings (Editar configuración)** y seleccione **Policies (Políticas)** > **Security (Seguridad)**; a continuación, establezca **Promiscuous Mode, MAC Address Changes (Modo promiscuo, cambios en direcciones MAC)** y **Forged Transmits (Transmisiones falsificadas)** en **Accept (Aceptar)**; haga clic en **OK (Aceptar)**.

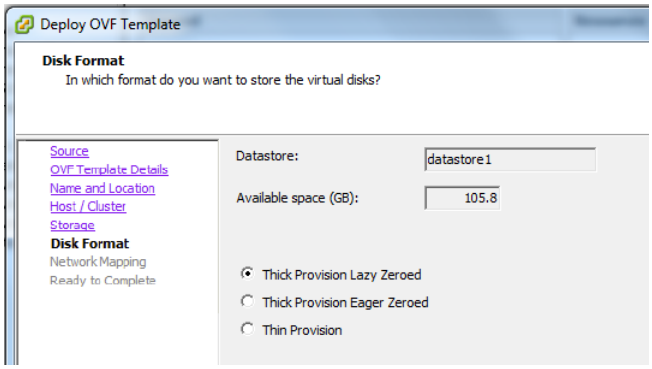
 ©2024 Palo Alto Networks, Inc.

STEP 3 | Implemente el OVA.

Si añade interfaces adicionales (vNIC) al cortafuegos VM-Series, debe reiniciarlo (porque las nuevas interfaces se detectan durante el ciclo de inicio). Para minimizar la necesidad de reiniciar el cortafuegos, active la interfaces en la implementación inicial o durante el período de mantenimiento.

Para ver el progreso de la instalación, supervise la lista ***Recent Tasks (Tareas recientes)****.*

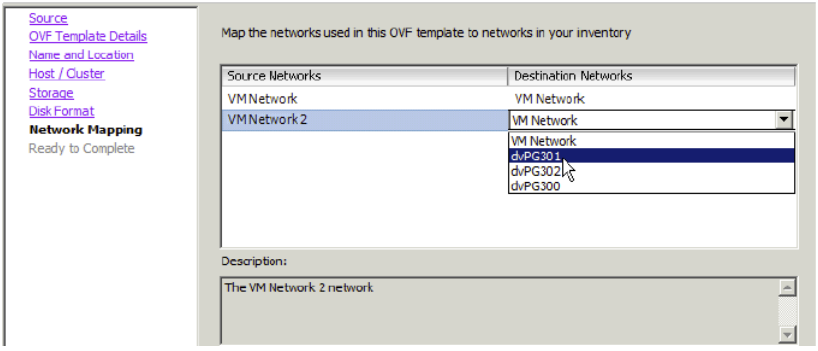
1. Inicie sesión en vCenter mediante el cliente vSphere. También puede ir directamente al host ESXi de destino si es necesario.
2. Desde el cliente web vSphere, vaya a **Hosts and Clusters (Hosts y clústeres)**, haga clic derecho en su host y seleccione **Deploy OVF Template (Implementar plantilla OVF)**.
3. Busque el archivo OVA que descargó anteriormente. Seleccione el archivo y haga clic en **Next (Siguiente)**. Revise los detalles de la plantilla y haga clic en **Next (Siguiente)**.
4. Asigne un nombre a la instancia del cortafuegos VM-Series y, en la ventana **Inventory Location (Ubicación de inventario)**, seleccione un Data Center (Centro de datos) y Folder (Carpeta) y haga clic en **Next (Siguiente)**.
5. Seleccione un host ESXi para el cortafuegos VM-Series y haga clic en **Next (Siguiente)**.
6. Seleccione el almacén de datos que se utilizará para el cortafuegos VM-Series y haga clic en **Next (Siguiente)**.
7. Deje la configuración predeterminada para el suministro del almacén de datos y haga clic en **Next (Siguiente)**. El valor predeterminado es **Thick Provision Lazy Zeroed (Suministro estándar diferido a cero)**.



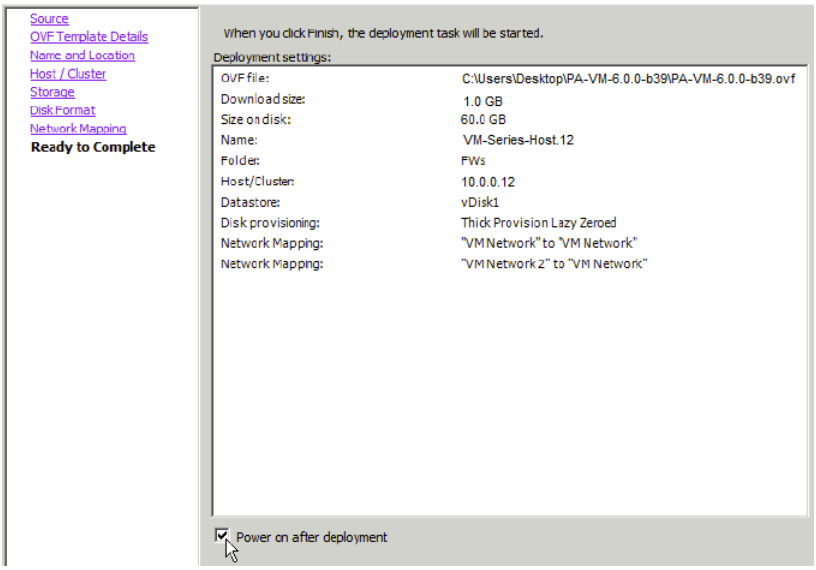
8. Seleccione las redes que se utilizarán para las dos vNIC iniciales. La primera vNIC se utiliza para la interfaz de gestión y la segunda vNIC, para el primer puerto de datos. Asegúrese de que

 ©2024 Palo Alto Networks, Inc.

las **Source Networks (Redes de origen)** se asignan a las **Destination Networks (Redes de destino)** correctas.



9. Revise los detalles, seleccione la casilla de verificación **Power on after deployment (Activación tras implementación)** y, a continuación, haga clic en **Next (Siguiente)**.



10. Cuando haya finalizado la implementación, haga clic en la pestaña **Summary (Resumen)** para revisar el estado actual.

Configuración inicial en VM-Series en ESXi

Utilice la consola del dispositivo virtual en el servidor ESXi para configurar el acceso de red al cortafuegos VM-Series. De forma predeterminada, el cortafuegos VM-Series usa DHCP para obtener una dirección IP para la interfaz de gestión, pero también puede asignar una dirección IP estática. Después de completar la configuración inicial, acceda a la interfaz web para completar otras tareas de configuración. Si usa Panorama para la gestión central, consulte la Guía del administrador de Panorama para saber más sobre la gestión del dispositivo mediante Panorama.

Si está utilizando bootstrapping para realizar la configuración del cortafuegos VM-Series en ESXi, consulte Arranque del cortafuegos VM-Series en ESXi.

Para obtener más información sobre el arranque, consulte Arranque del cortafuegos serie VM.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Obtenga la información necesaria de su administrador de red.

- Dirección IP para el puerto MGT
- Máscara de red
- Puerta de enlace predeterminada
- Dirección IP de servidor DNS

STEP 2 | Acceda a la consola del cortafuegos VM-Series.

1. Seleccione la ficha **Console (Consola)** en el servidor ESXi para el cortafuegos VM-Series o haga clic en el botón derecho del cortafuegos VM-Series y seleccione **Open Console (Abrir consola)**.
2. Pulse Intro para acceder a la pantalla de inicio de sesión.
3. Introduzca el nombre de usuario/contraseña predeterminados (admin/admin) para iniciar sesión.
4. Introduzca **`configure`** para pasar al modo de configuración.

STEP 3 | Defina la configuración de acceso a la red para la interfaz de gestión.

Introduzca los siguientes comandos:

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> Máscara de
 red <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

STEP 4 | Confirme los cambios y salga del modo de configuración.

Introduzca **`commit (confirmar)`**.

Introduzca **`exit (salir)`**.

STEP 5 | Verifique el acceso a la red para los servicios externos requeridos para la gestión del cortafuegos, como el servidor de actualizaciones de Palo Alto Networks.

1. Compruebe la utilidad del ping para verificar la conectividad de red al servidor de actualizaciones de Palo Alto Networks como se muestra en el siguiente ejemplo. Verifique que la resolución DNS se produzca y la respuesta incluya la dirección IP del servidor de actualización (el servidor de actualización no responde a solicitudes de ping). Cuando haya comprobado la resolución DNS, pulse Ctrl+C para detener la solicitud de 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
```

 ©2024 Palo Alto Networks, Inc.

2. Use el siguiente comando de la CLI para recuperar información sobre el derecho a la asistencia para el cortafuegos del servidor de actualización de Palo Alto Networks: request support check. Si tiene conectividad, el servidor de actualización responde con el estado de la asistencia para su cortafuegos.

STEP 6 | Aplique el código de autenticación de capacidad y recupere la licencia antes de comenzar con la prueba del cortafuegos VM-Series.

Un cortafuegos VM-Series sin licencia puede procesar hasta 1230 sesiones simultáneas aproximadamente. En función del entorno, el límite de sesiones se puede alcanzar muy rápidamente, lo que puede provocar resultados impredecibles.

Añadir espacio en disco adicional al cortafuegos VM-Series

Para PAN-OS 11.1.x y versiones posteriores, el cortafuegos VM-Series requiere un disco virtual de 60 GB, de los cuales 11 GB se utilizan para el registro de logs de forma predeterminada, y ampliable. Esto no se aplica si está actualizando el cortafuegos VM-Series desde PAN-OS 11.0.x o una versión anterior.

Para PAN-OS 11.1.x y versiones posteriores, el espacio en disco del cortafuegos VM-Series se divide de la siguiente manera:

Espacio en disco	Función
1 G	Partición de arranque
12 G	sysroot0
12 G	sysroot1
16 G	configuraciones de pan
8 G	repositorio de pan
11 G	logs de pan (ampliable)

- En implementaciones grandes, use Panorama para añadir datos desde todos los cortafuegos de última generación y ofrecer visibilidad en todo el tráfico de su red. Panorama brinda realización de informes y almacenamiento de logs centralizados.
- En implementaciones más pequeñas en las que no usa Panorama, puede añadir un disco virtual nuevo para aumentar la capacidad de almacenamiento de logs. El disco virtual nuevo puede admitir de 60 GB a 2 TB de capacidad de almacenamiento para los logs. Esta tarea se describe a continuación.

Cuando el dispositivo virtual se configura para usar un disco virtual, el cortafuegos VM-Series ya no almacena logs. Si el dispositivo pierde conectividad con el disco virtual, los logs se podrían perder durante el intervalo de fallo. Si es necesario, coloque el disco virtual recientemente creado en un almacén de datos que brinde redundancia RAID. RAID 10 ofrece el mejor rendimiento de escritura para aplicaciones con características de registro elevado.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Desactive el cortafuegos VM-Series.

STEP 2 | En el servidor ESXi, añada el disco virtual al cortafuegos.

1. Seleccione el cortafuegos VM-Series en el servidor ESXi.
2. Haga clic en **Edit Settings (Editar configuración)**.
3. Haga clic en **Add (Añadir)** para iniciar el asistente de adición de hardware y seleccione las siguientes opciones cuando se le solicite:
   1. Seleccione **Hard Disk (Disco duro)** para el tipo de hardware.
   2. Seleccione **Create a new virtual disk (Crear un nuevo disco virtual)**.
   3. Seleccione **SCSI** como el tipo de disco virtual.
   4. Seleccione el formato de disco **Thick Provisioning (Suministro estándar)**.
   5. En el campo de ubicación, seleccione **Store with the virtual machine option (Almacenar con la máquina virtual)**. No es necesario que el almacén de datos resida en el servidor ESXi.
   6. Verifique que la configuración es correcta y haga clic en **Finish (Finalizar)** para salir del asistente. El nuevo disco se añadirá a la lista de dispositivos del dispositivo virtual.

STEP 3 | Inicie el cortafuegos.

Si se inicia el cortafuegos, se inicia el disco virtual para el primer uso. El tiempo que tarda en completarse el proceso de inicialización varía según el tamaño del nuevo disco virtual.

Cuando el nuevo disco virtual se inicializa y se prepara, PAN-OS mueve todos los logs del disco existente al nuevo disco virtual. Las nuevas entradas de logs se escriben ahora en el disco virtual nuevo.

PAN-OS también genera una entrada de log de sistema que registra el disco nuevo.



Si reutiliza un disco virtual que se utilizó previamente para almacenar logs de PAN-OS, todos los logs del disco existente se sobrescriben.

STEP 4 | Compruebe el tamaño del disco virtual nuevo.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**.
2. En la sección Configuración de log e informes, compruebe que la capacidad de **Log Storage (Almacenamiento de log)** muestra con precisión la nueva capacidad del disco.

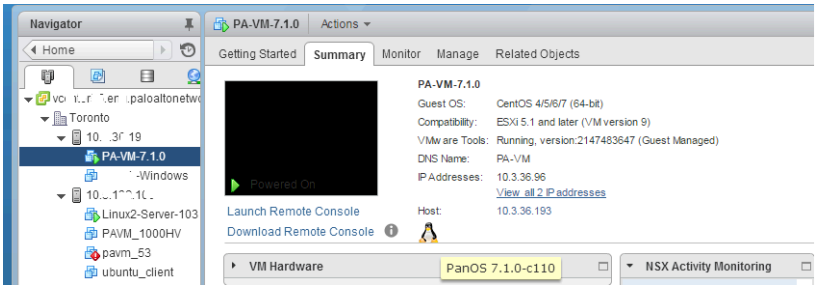
Uso de VMware Tools en el cortafuegos VM-Series en ESXi y vCloud Air

Las herramientas VMware mejoran la gestión del cortafuegos VM-Series desde el servidor vCenter y vCloud Director. Kas herramientas VMware se incluyen con la imagen de software para el cortafuegos VM-Series y todas las actualizaciones están disponibles con una nueva imagen OVF. No puede instalar o actualizar manualmente las herramientas VMware con el servidor vCenter o vCloud Director.

 ©2024 Palo Alto Networks, Inc.

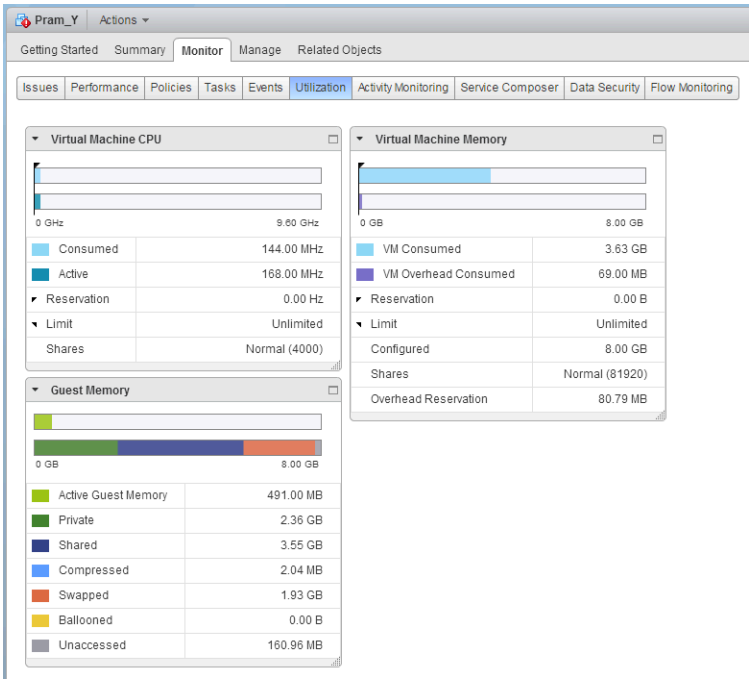
- Visualice la dirección o direcciones IP en la interfaz de gestión y la versión del software en el cortafuegos y Panorama.

  En la sección de hosts y clústeres del servidor vCenter, seleccione el cortafuegos o Panorama y visualice la pestaña **Resumen** para obtener información sobre la dirección o direcciones IP asignadas a la interfaz de gestión y la versión de software instalada.



- Visualice las métricas de uso de recursos en el disco duro, la memoria y el CPU. Utilice estos parámetros para habilitar alarmas en el servidor vCenter.

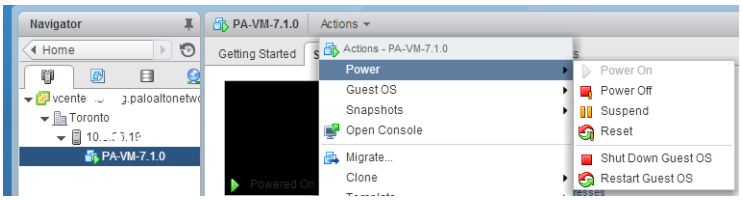
  En la sección de hosts y clústeres del servidor vCenter, seleccione el cortafuegos o Panorama y visualice la pestaña **Monitor (Supervisar)** > **Utilization (Utilización)** para obtener información sobre el disco duro, la memoria y la utilización de la CPU.



 ©2024 Palo Alto Networks, Inc.

- Apague o reinicie el cortafuegos o Panorama desde el servidor vCenter.

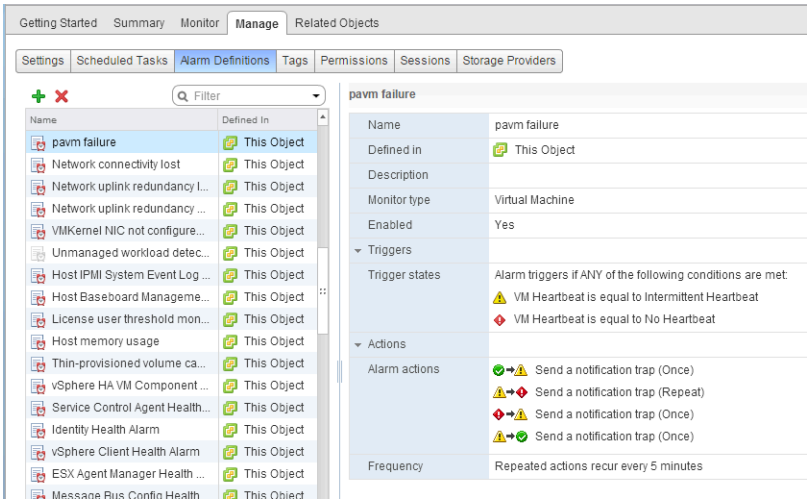
  En la sección de hosts y clústeres del servidor vCenter, seleccione el cortafuegos o Panorama y seleccione el menú desplegable **Actions (Acciones)** > **Power (Encendido)**.



- Cree definiciones de alarmas para eventos sobre los que desea recibir notificaciones, o para los que desea especificar una acción automatizada.

  Consulte en la Documentación de VMware detalles sobre la creación de definiciones de alarmas.

  En la sección de hosts y clústeres del servidor vCenter, seleccione el cortafuegos o Panorama y seleccione **Manage (Gestionar)** > **Alarm Definitions (Definiciones de alarmas)** para añadir una nueva activación y especificar una acción cuando se alcanza un umbral. Por ejemplo, faltan heartbeats para una duración específica, o cuando el uso de recursos de memoria supera un umbral. La siguiente instantánea de pantalla muestra cómo utilizar las notificaciones para el monitorizado de heartbeats en el cortafuegos o Panorama.



Utilice vMotion para mover el cortafuegos VM-Series entre hosts

Para mantener el flujo de tráfico mientras utiliza vMotion para mover su cortafuegos VM-Series en VMware ESXi entre hosts ESXi con configuraciones de CPU homogéneas, debe utilizar la CLI de PAN-OS para pausar la supervisión de heartbeats internos del cortafuegos VM-Series durante vMotion. Puede especificar el periodo de tiempo, en minutos, que se pausa la supervisión de heartbeats. La supervisión de heartbeats se puede pausar hasta por 60 minutos. Cuando el intervalo de pausa caduca o usted finaliza deliberadamente el intervalo de pausa, se reanuda la supervisión de heartbeats.

La tecnología vMotion del cortafuegos VM-Series es compatible en vSphere 6.5, 6.7 y 7.0 si los hosts ESXi tienen una configuración de CPU homogénea.

 ©2024 Palo Alto Networks, Inc.

Estos comandos no son necesarios cuando se usa vMotion si está ejecutando vSphere 7.0 o posterior.

STEP 1 | Inicie sesión en la CLI del cortafuegos VM-Series.

STEP 2 | Establezca el intervalo de pausa de supervisión de heartbeat mediante el siguiente comando. La pausa comienza tan pronto como se ejecuta el comando. Si vMotion tarda más de lo esperado, puede volver a ejecutar este comando para establecer un nuevo intervalo más largo que se inicie cuando el comando se vuelva a ejecutar.

```
request system heartbeat-pause set interval <pause-time-in-minutes>
```

Puede ver el tiempo restante en el intervalo de pausa usando el siguiente comando.

```
request system heartbeat-pause show interval
```

STEP 3 | (Opcional) Si completa vMotion antes de que haya transcurrido el intervalo de pausa, puede finalizar la pausa estableciendo el intervalo en cero (0).

```
request system heartbeat-pause set interval 0
```

Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión en ESXi

De forma predeterminada, el cortafuegos VM-Series asigna la primera interfaz (eth0) como interfaz de gestión. Sin embargo, en algunas implementaciones, la primera interfaz debe estar preasignada a una dirección IP pública. Por lo tanto, la interfaz de gestión debe asignarse a una interfaz diferente. La asignación de una dirección IP pública a la interfaz de gestión es un riesgo para la seguridad.

Este procedimiento requiere el complemento VM-Series 2.0.7 o posterior.

Alternativamente, puede habilitar el intercambio de la interfaz de gestión como parte del Componentes de archivo de init-cfg.txt *cuando se realiza el bootstrapping o arranque.*

STEP 1 | Inicie sesión en la CLI del cortafuegos VM-Series e introduzca el comando siguiente:

```
set system setting mgmt-interface-swap enable yes
```

STEP 2 | Confirme que desea intercambiar la interfaz y utilice la interfaz del plano de datos eth1 como interfaz de gestión.

STEP 3 | Reinicie el cortafuegos para que se produzca el intercambio. Utilice el comando siguiente:

```
request restart system
```

STEP 4 | Verifique que se hayan intercambiado las interfaces. Utilice el comando siguiente:

```
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
```

 ©2024 Palo Alto Networks, Inc.

Configurar el protocolo de control de agregación de enlaces

La agregación de enlaces implica configurar un *grupo de interfaces de agregación de enlaces* y configurar el *Protocolo de control de agregación de enlaces*. Un grupo de interfaz de agregación utiliza la agregación de enlaces IEEE 802.1AX para combinar varias interfaces de Ethernet en una sola interfaz virtual que conecta el cortafuegos a otro dispositivo de red o cortafuegos. Este grupo de agregación aumenta el ancho de banda entre pares al equilibrar la carga de tráfico en las interfaces combinadas. También proporciona redundancia; cuando una interfaz falla, las interfaces restantes continúan manteniendo el tráfico.

Por defecto, la detección de fallos de interfaz es automática solo en la capa física, entre peers conectados directamente. Sin embargo, si habilita el protocolo de control de agregación de enlaces, la detección de fallos es automática en la capa física y de enlace de datos, independientemente de si los pares están conectados directamente. LACP también permite la conmutación por error automática a interfaces en espera si configura reservas activas.

Para configurar un grupo de interfaces de agregación y LACP, consulte Configurar un grupo de interfaces de agregación.

Crear una interfaz de Ethernet de agregación con Panorama

No añada máquinas virtuales de Panorama asociadas con funciones virtuales desde la misma función física a la misma interfaz de Ethernet de agregación. Hacerlo crea un bucle. Crear una interfaz de Ethernet de agregación:

Configurar una interfaz de Ethernet de agregación:

1. Seleccione **Network (Red)>Interfaces>Ethernet** y **Add Aggregate Group (Añadir grupo de agregación)**.
2. En el campo adyacente a **Interface Name (Nombre de interfaz) de solo lectura,** introduzca un número para identificar el grupo de agregación. El intervalo es de 1 al número máximo de grupos de interfaz de agregación admitidos por el cortafuegos.
3. Para el **Interface Type (Tipo de interfaz)**, seleccione **HA**, **Virtual Wire**, **Layer 2 (Capa 2)** o **Layer 3 (Capa 3)**.
4. Configure los parámetros restantes para el **Interface Type** que seleccionó.
5. Confirme los cambios.

Después de crear la interfaz de agregación, agregue enlaces a ella.

Agregar enlaces a la interfaz de Ethernet de agregación

Para añadir enlaces a la interfaz de Ethernet de agregación:

STEP 1 | En Panorama, agregue una interfaz de Ethernet para actuar como oyente en modo pasivo para el par. Seleccione **Network (Red) > Interface (Interfaz)**.

STEP 2 | Seleccione una interfaz de Ethernet para actuar como un par.

STEP 3 | En la pantalla **Aggregate Ethernet Interface (Interfaz de Ethernet de agregación)**, seleccione **LACP**.

STEP 4 | Haga clic en **Enable LACP (Habilitar LACP)**.

STEP 5 | Asegúrese de que el modo es **Passive (Pasivo)**.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Haga clic en **OK (Aceptar)**.

STEP 7 | Confirme los cambios en Panorama.

STEP 8 | Confirme el cambio de configuración. Haga clic en **Yes (Sí)**.

Crear la interfaz de Ethernet de agregación usando la CLI

Utilice los siguientes comandos de la CLI para crear una interfaz de Ethernet de agregación:

```
admin@PA-VM# set network interface aggregate-ethernet ae1 ae1 <value>
 Aggregate interface name: ae1 - ae16
```

Por ejemplo,

```
admin@PA-VM# set network interface aggregate-ethernet ae1
```

Asociar una interfaz secundaria usando la CLI

Utilice los siguientes comandos de la CLI para asociar una interfaz secundaria:

```
admin@PA-VM# set network interface ethernet ethernet1/1 aggregate-
group ae1 aggregate-ethernet ae1 <value> Aggregate interface group
```

Por ejemplo,

```
set network interface ethernet ethernet1/1 aggregate-group ae1
```

Mostrar la configuración de la interfaz con la CLI

Utilice los siguientes comandos de la CLI para mostrar la configuración de la interfaz:

```
admin@PA-VM> show interface all total configured hardware
 interfaces: 4 name id speed/duplex/state mac address
 ------------------------------------------------------------------------------
 ethernet1/1 16 10000/full/up ba:db:ee:fb:ad:30 ethernet1/2
 17 10000/full/up 52:54:00:ce:8a:f5 ethernet1/3 18 10000/full/
up ba:db:ee:fb:ad:30 ae1 48 [n/a]/[n/a]/up ba:db:ee:fb:ad:30
 aggregation groups: 1 ae1 members: ethernet1/1 ethernet1/3 total
 configured logical interfaces: 2 name id vsys zone forwarding
 tag address ------------------- ----- ---- ----------------
 ------------------------ ------ ------------------ ethernet1/2 17 1
 trust vr:default 0 192.168.20.196/24 ae1 48 1 untrust vr:default 0
 192.168.10.110/24
```

Mostrar la configuración de la interfaz de Ethernet de agregación mediante la CLI

Utilice los siguientes comandos de la CLI para mostrar la configuración de la interfaz de Ethernet de agregación:

```
admin@PA-VM> show interface ae1
 ------------------------------------------------------------------------------
 Name: ae1, ID: 48 Link status: Runtime link speed/duplex/
state: [n/a]/[n/a]/up Configured link speed/duplex/state:
```

 ©2024 Palo Alto Networks, Inc.

```
auto/auto/auto MAC address: Port MAC address ba:db:ee:fb:ad:30
Aggregate group members: 2 ethernet1/1 ethernet1/3
Operation mode: layer3 Untagged sub-interface support: no
--------------------------------------------------------------------------------
Name: ae1, ID: 48 Operation mode: layer3 Virtual router default
Interface MTU 1500 Interface IP address: 192.168.10.110/24
Interface management profile: ae-mgmt-profile ping: yes telnet:
no ssh: yes http: yes https: yes snmp: no response-pages: no
userid-service: no Service configured: Zone: untrust, virtual
system: vsys1 Adjust TCP MSS: no Ignore IPv4 DF: no Policing: no
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Physical port counters read from MAC:
--------------------------------------------------------------------------------
rx-broadcast 0 rx-bytes 7874426 rx-multicast 0 rx-unicast 151353
tx-broadcast 0 tx-bytes 9320 tx-multicast 0 tx-unicast 130
--------------------------------------------------------------------------------
Hardware interface counters read from CPU:
--------------------------------------------------------------------------------
bytes received 3920 bytes transmitted 7406 packets received
40 packets transmitted 123 receive incoming errors 0
receive discarded 0 receive errors 0 packets dropped 0
--------------------------------------------------------------------------------
Logical interface counters read from CPU:
--------------------------------------------------------------------------------
bytes received 7854114 bytes transmitted 7700 packets received
150927 packets transmitted 130 receive errors 0 packets dropped
150614 packets dropped by flow state check 0 forwarding errors 0 no
route 0
```

Configurar la agregación de enlaces en el Switch utilizando la CLI

Active la agregación de enlaces en el switch:

```
int eth1/4 channel-group 1 mode on int eth1/8 channel-group 1 mode on
```

Verifique la configuración:

```
show running-config interface Ethernet 1/4 interface Ethernet 1/4 no
 lldp transmit no lldp receive no switchport Channel-group 1 mode on
 show running-config interface Ethernet 1/8 interface Ethernet 1/8 no
 lldp transmit no lldp receive no switchport Channel-group 1 mode on
```

 ©2024 Palo Alto Networks, Inc.

Supervisión de VM en vCenter

Instale y configure el plugin de Panorama para VMware vCenter, para recuperar las direcciones IP para invitados en su entorno de vCenter y utilizar esa información para crear políticas utilizando grupos de direcciones dinámicas.

El plugin de Panorama para VMware vCenter no admite servidores proxy.

- Acerca de VM Monitoring en VMware vCenter
- Instalación del plugin de Panorama para VMware vCenter
- Configure el plugin de Panorama para VMware vCenter

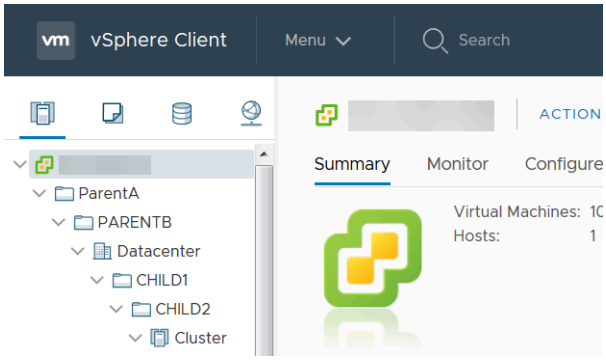
Acerca de VM Monitoring en VMware vCenter

El complemento de Panorama para VMware vCenter le proporciona el conjunto de herramientas para crear políticas para su entorno vCenter usando Grupos de direcciones dinámicas. Los grupos de direcciones dinámicas le permiten crear una política que se adapta automáticamente a los cambios en su entorno, como la adición o eliminación de nuevos elementos. El plugin vCenter de VMware supervisa los cambios en su entorno vCenter y comparte esa información con Panorama.

El plugin procesa la información que recibe de vCenter y la convierte en un conjunto de etiquetas en Panorama que puede usar como criterios de coincidencia para asignar direcciones IP a grupos de direcciones dinámicas. Cada etiqueta tiene un prefijo que describe la jerarquía sobre la máquina virtual.

En este ejemplo, cada etiqueta en Panorama comienza con el prefijo que se muestra a continuación. Cada etiqueta incluye el nombre del vCenter, el nombre del centro de datos y el nombre del clúster; si tiene carpetas en su jerarquía de vCenter, las etiquetas incluirán los nombres de las carpetas. El orden de los objetos en la etiqueta coincide con el orden en la jerarquía de vCenter.

vcenter.<vcenter-name>_ParentA_ParentB_Datacenter_CHILD1_CHILD2_Cluster_<tag>



El complemento de Panorama para vCenter de VMware no admite etiquetas asociadas a vApps o a grupos de recursos.

Las etiquetas se muestran en Panorama en los siguientes formatos:

- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_vmname.<vm-name>**: esta etiqueta asigna las direcciones IP de la máquina virtual en función del nombre de la máquina virtual.

©2024 Palo Alto Networks, Inc.

- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_guestos.<guest-os>**: esta etiqueta asigna las direcciones IP de la máquina virtual en función del sistema operativo invitado.
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_annotation.<annotation>**: esta etiqueta asigna las direcciones IP de la máquina virtual en función de la anotación.
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_vlanId.<vlan-ID>**: esta etiqueta asigna las direcciones IP de la máquina virtual en función del ID de VLAN.
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_host-ip.<host-ip>**: esta etiqueta asigna las direcciones IP de la máquina virtual en función de la dirección IP del host.
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_<tag-category>.<user-defined-tag>**: esta etiqueta asigna las direcciones IP de la máquina virtual en función de las etiquetas definidas por el usuario creadas en vCenter.

El plugin admite un máximo de 16 etiquetas definidas por el usuario por máquina virtual. No se procesan las etiquetas definidas por el usuario más allá de 16.

El plugin de Panorama para vCenter no puede procesar etiquetas que tengan más de 128 caracteres; esto incluye letras, números y caracteres especiales. Los espacios en blanco en los nombres de objetos de vCenter se sustituyen con barras diagonales. Además, Panorama no es compatible con caracteres especiales no ASCII o los siguientes caracteres especiales:**'<>&"** en los nombres de VM y anotaciones de vCenter. Panorama rechaza etiquetas que contienen caracteres no compatibles.

Para recuperar la información de asignación de la dirección IP a la etiqueta del endpoint, debe configurar una definición de monitorización para cada vCenter en su entorno virtual. La definición de monitorización especifica el nombre de usuario y la contraseña que permite a Panorama conectarse a vCenter. También especifica los grupos de dispositivos y los grupos de notificación correspondientes que contienen los cortafuegos a los que Panorama envía las etiquetas. Después de configurar la definición de monitorización y de que el plugin de Panorama para VMware vCenter recupera las etiquetas, puede crear DAG y añadir las etiquetas como criterios de coincidencia.

Instalación del plugin de Panorama para VMware vCenter

Para comenzar con la supervisión de endpoints en vCenter, descargue e instale el plugin de Panorama para VMware vCenter.

Si tiene una configuración de HA en Panorama, repita el proceso de instalación en cada peer Panorama. Al instalar el complemento en Panorama en un par de HA, instale el complemento en el par pasivo antes de hacerlo en el par activo. Después de instalar el complemento en el peer pasivo, pasará a un estado no funcional. La instalación del plugin en el peer activo devuelve el peer pasivo a un estado funcional.

Si tiene un Panorama independiente o dos dispositivos Panorama instalados en un par de alta disponibilidad con varios complementos instalados, es posible que los complementos no reciban información actualizada sobre la etiqueta IP si uno o más de los complementos no están configurados. Esto ocurre porque Panorama no reenviará la información de la etiqueta IP a los complementos no configurados. Además, este problema puede ocurrir si uno o más de los complementos de Panorama no están en el estado Registrado o Correcto (el estado positivo varía según cada complemento). Asegúrese de que sus complementos estén en el estado positivo antes de continuar o ejecutar los comandos que se describen a continuación.

Si encuentra este problema, hay dos soluciones:

 ©2024 Palo Alto Networks, Inc.

- Desinstale el complemento o complementos no configurados. Se recomienda que no instale un complemento que no planifique configurar de inmediato
- Puede utilizar los siguientes comandos para solventar este problema. Ejecute el siguiente comando para cada complemento no configurado en cada instancia de Panorama, para evitar que Panorama espere para enviar actualizaciones. Si no lo hace, sus cortafuegos pueden perder cierta información de la etiqueta IP.

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

  Puede cancelar este comando ejecutando:

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

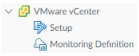
Los comandos descritos no son persistentes en los reinicios y deben usarse de nuevo para cualquier reinicio posterior. Para Panorama en el par de HA, los comandos deben ejecutarse en cada Panorama.

STEP 1 | Seleccione **Panorama** > **Plugins (Complementos)**.

STEP 2 | Seleccione **Upload (Cargar)** y haga clic en **Browse (Examinar)** para localizar el archivo del plugin.

STEP 3 | Haga clic en **OK (Aceptar)** para completar la descarga.

STEP 4 | Seleccione la versión del complemento y haga clic en **Install (Instalar)** en la columna Action (Acción) para instalar el complemento. Panorama le alertará cuando se complete la instalación.



Configure el plugin de Panorama para VMware vCenter

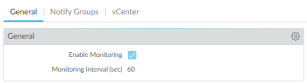
Después de instalar el plugin, complete el siguiente procedimiento para establecer una conexión entre Panorama y vCenter.

Para que el complemento supervise las máquinas virtuales en su entorno vCenter, debe tener instaladas las herramientas de VMware. En vCenter, las direcciones IP de las máquinas virtuales no son recuperables externamente; solo son visibles a través de las herramientas de VMware. Además, se requieren permisos de solo lectura nativos para que el complemento recupere la información de la dirección IP de vCenter.

STEP 1 | Inicie sesión en la interfaz web de Panorama.

STEP 2 | Habilite la supervisión y establezca el intervalo de supervisión.

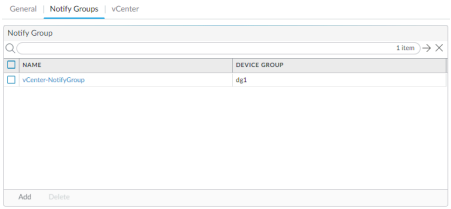
1. Seleccione **Panorama** > **VMware vCenter** > **Setup (Configuración)** > **General**.
2. Seleccione **Enable Monitoring (Habilitar supervisión)**. Esto permite la supervisión de todos los vCenters en su implementación.
3. Establezca el **Monitoring Interval (Intervalo de supervisión)** en segundos. El intervalo de supervisión es la frecuencia con la que Panorama recupera la información de red actualizada de vCenter. El valor predeterminado es 60 segundos y tiene un intervalo de 60 a 84600 segundos.



 ©2024 Palo Alto Networks, Inc.

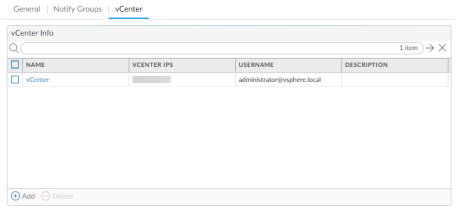
STEP 3 | Cree un grupo de notificación.

1. Seleccione **Panorama** > **VMware vCenter** > **Setup (Configuración)** > **Notify Groups (Grupos de notificación)**.
2. Haga clic en **Add (Añadir)**.
3. Introduzca un **Name (Nombre)** descriptivo para el grupo de notificación.
4. Seleccione los grupos de dispositivos en su implementación de vCenter.



STEP 4 | Añada información de vCenter. El plugin de Panorama para VMware vCenter admite hasta 16 instancias de vCenter.

1. Seleccione **Panorama** > **VMware vCenter** > **Setup (Configuración)** > **vCenter**.
2. Introduzca un **Name (Nombre)** descriptivo para su vCenter.
3. Introduzca la dirección IP o FQDN para vCenter y el puerto, si corresponde.
4. Introduzca su nombre de usuario de vCenter.
5. Introduzca y confirme su contraseña de vCenter.
6. Haga clic en **Validar** para verificar que Panorama pueda conectarse a vCenter usando las credenciales de inicio de sesión que introdujo.
7. Haga clic en **OK (Aceptar)**.



 ©2024 Palo Alto Networks, Inc.

STEP 5 | Configure hasta 16 definiciones de supervisión.

Una instancia de vCenter solo se puede asignar a una definición de supervisión.

1. Seleccione **Panorama** > **VMware vCenter** > **Monitoring Definition (Definición de monitorización)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** descriptivo y, opcionalmente, una descripción para identificar el vCenter para el que usa esta definición.
3. Seleccione la **vCenter** y el **Notify Group (Grupo de notificación)**.
4. Haga clic en **OK (Aceptar)**.



STEP 6 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 7 | Compruebe que puede ver la información de la VM en Panorama y defina los criterios de coincidencia para los grupos de direcciones dinámicas.

Debe usar el operador OR cuando use más de una etiqueta en los criterios de coincidencia; el uso del operador AND no funciona.

Algunas extensiones del navegador pueden bloquear las llamadas a la API entre Panorama y vCenter, lo que evita que Panorama reciba criterios de coincidencia. Si Panorama no muestra ningún criterio de coincidencia y usted está usando extensiones de navegador, deshabilite las extensiones y Sincronizar objetos dinámicos para completar las etiquetas disponibles para Panorama.

STEP 8 | Verifique que las direcciones en sus máquinas virtuales se añaden a las DAG.

1. Seleccione **Panorama** > **Objects (Objetos)** > **Address Groups (Grupos de direcciones)**.
2. Haga clic en **More (Más)** en la columna de direcciones de una DAG.

   Panorama muestra una lista de direcciones IP añadidas a ese DAG en función de los criterios de coincidencia que haya especificado.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Usar grupos de direcciones dinámicas en la política.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Haga clic en **Add (Añadir)** y escriba un **Name (Nombre)** y una **Description (Descripción)** para la política.
3. Añada la **Source Zone (Zona de origen)** para especificar la zona desde la que se origina el tráfico.
4. Añada la **Destination Zone (Zona de destino)** donde finaliza el tráfico.
5. Para la **Destination Address (Dirección de destino)**, seleccione el grupo de direcciones dinámicas que ha creado anteriormente.
6. Especifique la acción (**Permitir** o **Denegar**) para el tráfico y, de manera opcional, incluya los perfiles de políticas de seguridad en la regla.
7. Repita los pasos del 1 al 6 para crear otra regla de política.
8. Haga clic en **Commit (Confirmar)**.

STEP 10 | Puede actualizar los objetos dinámicos desde vCenter en cualquier momento mediante la sincronización de objetos dinámicos. La sincronización de objetos dinámicos le permite mantener el contexto en los cambios del entorno virtual y activar aplicaciones, ya que actualiza de forma automática los grupos de direcciones dinámicas en las reglas de la política.

1. Seleccione **Panorama** > **VMware NSX** > **Monitoring Definition (Definición de monitorización)**.
2. Haga clic en **Synchronize Dynamic Objects (Sincronizar objetos dinámicos)**.

STEP 11 | Si un cortafuegos en su implementación de vCenter se reinicia o se desconecta de Panorama, ese cortafuegos pierde la sincronización con el plugin de Panorama para vCenter y no recibe actualizaciones. Después de que el cortafuegos se vuelva a conectar con Panorama, debe sincronizar manualmente Panorama y el cortafuegos.

1. Inicie sesión en la CLI de Panorama.
2. Ejecute el siguiente comando.

```
admin@Panorama> request plugins vmware_vcenter sync
```

 ©2024 Palo Alto Networks, Inc.

Solución de problemas de implementaciones de ESXi

Muchos de los pasos de solución de problemas para el cortafuegos VM-Series son muy parecidos a los de las versiones de hardware de PAN-OS. Si se produce algún problema, debería comprobar los contadores de la interfaz y archivos de log de sistema y, si es necesario, utilizar la depuración para crear capturas.

La siguientes secciones describen cómo solucionar algunos problemas comunes:

- Solución de problemas básicos
- Problemas de instalación
- Problemas de licencia
- Problemas de conectividad

Solución de problemas básicos

Recomendación de herramientas de solución de problemas de red

Resulta útil tener una estación de solución de problemas aparte para capturar el tráfico o inyectar paquetes de prueba en el entorno virtualizado. Puede ser útil crear un SO nuevo desde cero con las herramientas de solución de los problemas más comunes instaladas, como tcpdump, nmap, hping, traceroute, iperf, tcpedit, netcat, etc. A continuación esta máquina puede apagarse y convertirse en una plantilla. Cada vez que se necesiten herramientas, el cliente de solución de problemas (máquina virtual) puede implementarse rápidamente en el conmutador virtual en cuestión y usarse para aislar problemas de redes. Cuando la prueba esté completa, la instancia podrá simplemente descartarse y la plantilla se volverá a usar la siguiente vez que sea necesaria.

Para problemas relacionados con el rendimiento en el cortafuegos, primero compruebe el **Dashboard (Panel)** en la interfaz web del cortafuegos. Para ver alertas o crear un archivo de asistencia técnica o de volcado de estadísticas, desplácese a **Device (Dispositivo)** > **Support Asistencia técnica)**.

Para obtener información del cliente vSphere, vaya a **Home (Inicio)** > **Inventory (Inventario)** > **VMs and Templates (VM y plantillas)**, seleccione la instancia del cortafuegos VM-Series y haga clic en la pestaña **Summary (Resumen)**. Bajo **Resources (Recursos)**, compruebe las estadísticas de la memoria consumida, la CPU y el almacenamiento. Para conocer el historial de recursos, haga clic en la ficha **Performance (Rendimiento)** y supervise el consumo de recursos a lo largo del tiempo.

Problemas de instalación

- Problemas con la implementación de OVA
- ¿Por qué el cortafuegos se inicia en modo de mantenimiento?
- ¿Cómo modificar el archivo de imagen base de la licencia de VM-1000-HV?

 ©2024 Palo Alto Networks, Inc.

Problemas con la implementación de OVA

- VM-Series se proporciona como un archivo zip en el formato abierto de la alianza de virtualización (Open Virtualization Alliance, (OVA) que se expande en tres archivos.

  Si tiene problemas para implementar la imagen de OVA, asegúrese de que los tres archivos estén desempaquetados y que se pueda acceder a ellos. Si es necesario, descargue y extraiga la imagen de OVA de nuevo.
- El disco virtual en la imagen de OVA es casi de 1 GB. Debe estar presente en el ordenador que ejecuta el cliente vSphere o se debe poder acceder como una URL para la imagen de OVA.
  - Asegúrese de que la conexión de red entre el cliente de vSphere y el host ESXi de destino tenga baja latencia y suficiente ancho de banda. Si la conexión es deficiente, la implementación de OVA puede tardar horas o agotar el tiempo de espera y fallar.

    Puede minimizar este problema si hospeda la imagen en un dispositivo en la misma red que el host ESXi.
  - Cualquier cortafuegos en la ruta debe permitir los puertos TCP 902 y 443 del cliente vSphere a los hosts ESXi.
- La compilación ESX 6.5.0 4887370 lo limita a 2 núcleos de CPU por socket. Si implementa un VM-300, VM-500 o VM-700 al cual desea asignar más de 2 CPU virtuales por socket, consulte VMware KB: https://kb.vmware.com/s/article/53354, para obtener una solución.

¿Por qué el cortafuegos se inicia en modo de mantenimiento?

Si adquirió la licencia del VM-1000-HV y está implementando el cortafuegos VM-Series en modo independiente en un servidor ESXi de VMware, debe asignar el mínimo de memoria requerida por su modelo VM-Series.

Para evitar el inicio en modo de mantenimiento, debe modificar el archivo de imagen base (consulte ¿Cómo modifico el archivo de imagen base de la licencia de VM-1000-HV?) o edite los ajustes del host ESXi o el servidor vCenter antes de encender el cortafuegos VM-Series.

Además, verifique que la interfaz sea VMXnet3. Si configura el tipo de interfaz en cualquier otro formato, el cortafuegos arrancará en el modo de mantenimiento.

¿Cómo modificar el archivo de imagen base de la licencia de VM-1000-HV?

Si adquirió la licencia del VM-1000-HV y está implementando el cortafuegos VM-Series en modo independiente en un servidor ESXi de VMware, siga estas instrucciones para modificar los siguientes atributos que se definen en el archivo de imagen base (.ova o .xva) del cortafuegos VM-Series.

Importante: La modificación de valores distintos de los enumerados aquí invalidará el archivo de imagen base.

STEP 1 | Abra el archivo de imagen base, por ejemplo 7.0.0, con una herramienta de edición de texto como el bloc de notas.

STEP 2 | Busque 4096 y cambie la asignación de memoria a 5012 (es decir, 5 GB) de la siguiente forma:

```
4096MB of memory<Item> <rasd:AllocationUnits>byte * 2^20</
rasd:AllocationUnits> <rasd:Description>Tamaño<rasd:ElementName></
rasd:Description> de memoria 4096MB de memoria</rasd:ElementName>
 <rasd:InstanceID>2<rasd:ResourceType></rasd:InstanceID>
```

 ©2024 Palo Alto Networks, Inc.

```
 44096</rasd:VirtualQuantity> <rasd:AllocationUnits><Item>
 byte * 2^20<rasd:Description></rasd:AllocationUnits>
 Tamaño</rasd:Description> <rasd:ElementName>de memoria
 5120MB de memoria</rasd:ElementName> <rasd:InstanceID>2</
rasd:InstanceID> <rasd:ResourceType>55120<rasd:VirtualQuantity></
rasd:ResourceType> </rasd:ResourceType> <rasd:VirtualQuantity></
rasd:VirtualQuantity>
```

STEP 3 | Cambie el número de núcleos de CPU virtuales que se asignan de 2 a 4 u 8 como desee para su implementación:

```
<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>
```

También puede implementar el cortafuegos y antes de activar el cortafuegos VM-Series, editar la asignación de la CPU virtual y la memoria directamente en el host ESXi o el servidor vCenter.

Problemas de licencia

- ¿Por qué no puedo aplicar la licencia de funciones o asistencia técnica?
- ¿Por qué mi cortafuegos VM-Series clonado no tiene una licencia válida?
- ¿Si se mueve el cortafuegos VM-Series se invalidará la licencia?

¿Por qué no puedo aplicar la licencia de funciones o asistencia técnica?

¿Ha aplicado el código de autenticación de capacidad en el cortafuegos VM-Series? Antes de que pueda activar la licencia de funciones o asistencia técnica, debe aplicar el código de autenticación de capacidad para que el dispositivo pueda obtener un número de serie. Este número de serie es necesario para activar las otras licencias en el cortafuegos VM-Series.

¿Por qué mi cortafuegos VM-Series clonado no tiene una licencia válida?

VMware asigna una UUID a cada máquina virtual que incluye el cortafuegos VM-Series. Así, cuando un cortafuegos VM-Series se clona, se le asigna una nueva UUID. Como el número de serie y la licencia de cada instancia del cortafuegos VM-Series está vinculada a la UUID, si clona el cortafuegos VM-Series con licencia, el cortafuegos nuevo no tendrá una licencia válida. Necesita un nuevo código de autenticación para activar la licencia en el cortafuegos que acaba de implementar. Debe aplicar el código de autenticación de capacidad y una nueva licencia de asistencia técnica para obtener actualizaciones de funcionalidad, asistencia técnica y software en el cortafuegos VM-Series.

 ©2024 Palo Alto Networks, Inc.

¿Si se mueve el cortafuegos VM-Series se invalidará la licencia?

Si mueve el cortafuegos VM-Series manualmente de un host a otro, asegúrese de seleccionar la opción **This guest was moved (Se ha movido este invitado)** para evitar que se invalide la licencia.

Problemas de conectividad

- ¿Por qué el cortafuegos VM-Series no recibe tráfico de la red?

¿Por qué el cortafuegos VM-Series no recibe tráfico de la red?

En el cortafuegos VM-Series, compruebe los registros de tráfico (**Monitor (Supervisar)** > **Logs**. Si los logs están vacíos, use el siguiente comando CLI para ver los paquetes de las interfaces del cortafuegos VM-Series:

```
show counter global filter delta yes Global counters:
 Elapsed time since last sampling: 594.544 seconds
 ------------------------------------------------------------------------------
 Total counters shown: 0
 ------------------------------------------------
 -------------------------------
```

En el entorno vSphere, compruebe lo siguiente:

- Compruebe los grupos de puertos y confirme que el cortafuegos y las máquinas virtuales están en el grupo de puertos correcto

  Asegúrese de que las interfaces se asignan correctamente.

  Adaptador de red 1 = gestión

  Adaptador de red 2= Ethernet1/1

  Adaptador de red 3= Ethernet1/2

  Para cada máquina virtual, compruebe los ajustes para verificar que la interfaz se asigna al grupo de puertos correcto.

 ©2024 Palo Alto Networks, Inc.

- Compruebe que se ha habilitado el modo promiscuo para cada grupo de puertos o para todo el conmutador, o que ha configurado el cortafuegos en Direcciones MAC asignadas por el hipervisor.

  Como las direcciones MAC de PAN-OS del plano de datos son distintas de las direcciones MAC de vNIC asignadas por vSphere, el grupo de puertos (o todo el vSwitch) debe estar en modo promiscuo si no está habilitado para usar la dirección MAC asignada al hipervisor:

  - Compruebe la configuración de VLAN en vSphere.

    El uso de la configuración VLAN en el grupo de puertos vSphere tiene dos objetivos: determina qué grupos de puertos comparten un dominio de 2 niveles, y determina si se etiquetan los puertos de vínculo superior (802.1Q).

  - Compruebe los ajustes de puerto de conmutador físico

    Si se especifica un ID de VLAN en un grupo de puertos con puertos de vínculo superior, vSphere usará 802.1Q para etiquetar las tramas salientes. La etiqueta debe coincidir con la configuración del conmutador físico, de lo contrario el tráfico no pasará.

    Compruebe las estadísticas del puerto si usa conmutadores distribuidos virtuales (vDS); los conmutadores estándar no proporcionan estadísticas de puerto

 ©2024 Palo Alto Networks, Inc.

Ajuste de rendimiento de VM-Series para ESXi

El cortafuegos VM-Series para ESXi es un dispositivo de alto rendimiento pero puede requerir el ajuste del hipervisor para lograr los mejores resultados. Esta sección describe algunas de las prácticas recomendadas y recomendaciones para facilitar el mejor rendimiento del cortafuegos dVM-Series. Para obtener el mejor rendimiento, se recomienda ESXi 6.0.0.0 o una versión posterior.

- Instalación del controlador NIC en ESXi
- Habilitación de VPN en ESXi
- Habilitación de SR-IOV en ESXi
- Habilitación del modo de acceso VLAN ESXi con SR-IOV
- Habilitación del soporte de colas múltiples para NIC en ESXi
- Ajuste de función de red virtual (VNF) para el rendimiento

Instalación del controlador NIC en ESXi

Para obtener el mejor rendimiento, utilice SR-IOV con las interfaces de red Intel de 10 GB que requieren que el controlador ixgbe 4.4.1 admita múltiples colas para cada interfaz.

STEP 1 | Obtenga una lista de interfaces de red en el host ESXi.

1. Inicie sesión en el la CLI del host ESXi.
2. Use el siguiente comando para devolver una lista de interfaces de red:

```
$ esxcli network nic list
```

STEP 2 | Determine la versión del controlador para una interfaz en particular.

Puede usar cualquiera, **ethtool** o **esxcli**, para determinar la versión del controlador actualmente instalado. El siguiente ejemplo usa vNIC4 y muestra la versión del controlador 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:
 Ninguno
```

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Instale el nuevo controlador.

1. Descargue el controlador ixgbe 4.4.1 del sitio web de VMware. Extraiga el contenido y envíelo a un directorio local, y busque los archivos .zip o .vib para su controlador.
2. Cree una carpeta nueva en el almacén de datos del host de ESXi.
3. Copie el archivo local .zip o .vib que extrajo a la carpeta nueva en el almacén de datos de su host ESXi.
4. Habilite el modo de mantenimiento en el host ESXi.
5. Use uno de los siguientes comandos para instalar el controlador nuevo, usando -d para los archivos .zip o usando -v para los archivos .vib.

   - ```
     $ esxcli software vib install -d <path to driver .zip file>
     ```
   - ```
     $ esxcli software vib install -v <path to driver .vib file>
     ```

   Debe especificar la ruta absoluta al archivo .zip o .vib. Por ejemplo:

   ```
   $ esxcli software vib install -d "/vmfs/volumes/
   Datastore/DirectoryName/DriverName.zip"
   ```
6. Verifique la instalación de VIB.

   ```
   $ esxcli software vib list
   ```
7. Reinicie el host ESXi.

Habilitación de VPN en ESXi

El Kit de desarrollo de plano de datos (DPDK) mejora el rendimiento de VM-Series al aumentar la velocidad de procesamiento de paquetes de la tarjeta de interfaz de red (NIC). En el cortafuegos VM-Series, DPDK está habilitado por defecto en ESXi.

Para aprovechar el DPDK, debe utilizar una NIC con uno de los controladores DPDK compatibles mencionados en Versiones del controlador de DPDK:

Si desactiva DPDK, la NIC usa PacketMMap en lugar de DPDK. Puede deshabilitar el LRO usando el comando **`set system setting dpdk-pkt-io off`**.

Consulte la Matriz de compatibilidad para ver la compatibilidad de hipervisor ESXi y Compatibilidad de los controladores PacketMMAP y DPDK con la versión PAN-OS.

Habilitación de SR-IOV en ESXi

La virtualización de E/S de raíz única (SR-IOV) permite que un único dispositivo físico PCIe bajo un único puerto raíz parezca ser múltiples dispositivos físicos separados para el hipervisor o el invitado. Para activar la SR-IOV, habilite los dispositivos de funciones virtuales en la NIC SR-IOV y modifique la configuración de invitados en vCenter.

SR-IOV en VM-Series para ESXi requiere uno de los controladores NIC de Intel mencionados en Versiones del controlador PacketMMAP. Consulte la Matriz de compatibilidad para la compatibilidad del controlador SR-IOV y DPDK con la versión PAN-OS.

 ©2024 Palo Alto Networks, Inc.

Hay dos formas de habilitar SR-IOV en ESXi.

- **SR-IOV passthrough (Envío SR-IOV)**: en este método, se habilita los dispositivos de función virtual en la NIC de SR-IOV y modifica la configuración de invitado en vCenter, añadiendo la interfaz VF SR-IOV como tipo de adaptador "SR-IOV passthrough". Consulte Asignar una función virtual como adaptador de envío SR-IOV a una máquina virtual.

  Este método, que es el preferido para PAN-OS 8.1.2 y posteriores, le permite añadir la función física de SR-IOV a un vSwitch o DvSwitch.
- **PCI Adaptor (Adaptador PCI)**: este método era necesario para PAN-OS 8.0 a 8.1.1. Puede ver el flujo de trabajo del Adaptador PCI en Habilitar SR-IOV en ESXi en la Guía de implementación 8.1.

  El método del Adaptador PCI tiene la limitación de que no puede configurar un vSwitch en el puerto físico en el que habilita SR-IOV. El cortafuegos VM-Series debe tener acceso exclusivo al puerto físico y a las funciones virtuales asociadas (associated virtual functions, VF) en esa interfaz para comunicarse con el host u otras máquinas virtuales de la red. Consulte Añadir un dispositivo PCI en vSphere Web Client.

Habilitación del modo de acceso VLAN ESXi con SR-IOV

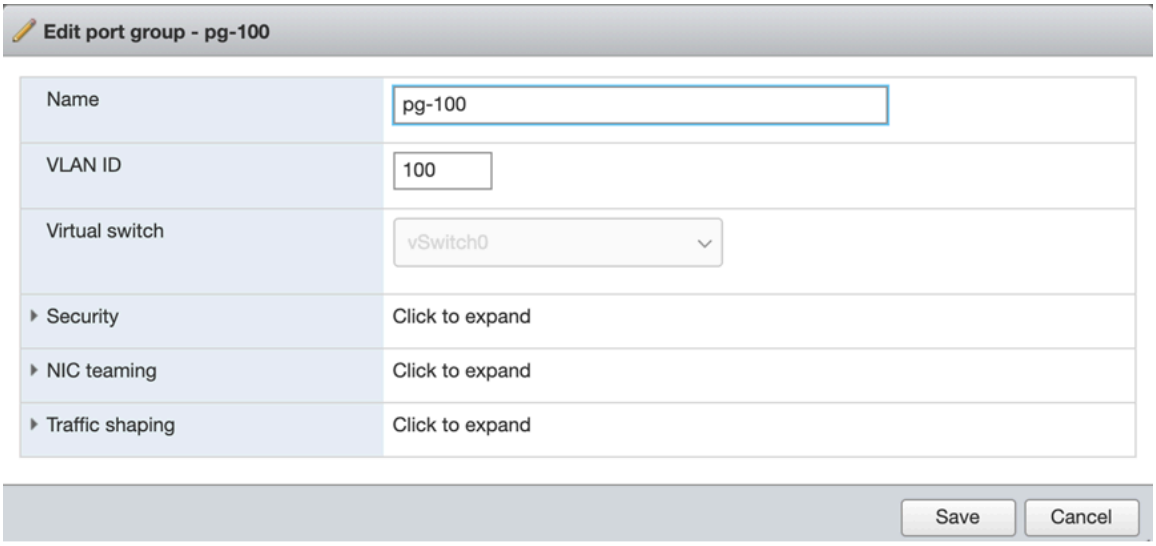
Los cortafuegos VM-Series en ESXi pueden funcionar en modo de acceso VLAN para admitir casos de uso en los que se implementa como una función de red virtual (VNF) que ofrece seguridad como servicio en un entorno de centro de datos/nube de múltiples inquilinos. En el modo de acceso VLAN, cada VNF tiene interfaces de red virtual (VNI) dedicadas para cada red y envía y recibe paquetes a y desde las funciones virtuales (VF) de SR-IOV sin etiquetas VLAN; debe habilitar esta capacidad en las funciones físicas y virtuales en el hipervisor host. Cuando activa el modo de acceso VLAN en el cortafuegos VM-Series, el cortafuegos puede enviar y recibir tráfico sin etiquetas VLAN en todas sus interfaces de plano de datos. Además, si configura las políticas de QoS, el cortafuegos puede aplicar QoS en la interfaz de acceso y proporcionar un tratamiento diferenciado del tráfico en una implementación de múltiples inquilinos.

De forma predeterminada, el cortafuegos VM-Series en ESXi funciona en modo troncal VLAN.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | En el sistema host, configure la función física y virtual para operar en modo de acceso VLAN.

1. Haga clic en **Networking (Redes)** en el inventario de VMware Host Client y haga clic en **Port groups (Grupos de puertos)**.
2. En la lista que desea editar, haga clic con el botón secundario en el grupo de puertos y seleccione **Edit settings (Editar configuración)**. Escriba un nuevo **Name (Nombre)** de grupo de puertos. Introduzca un nuevo valor para el **VLAN ID (ID de VLAN)**.



Para obtener el mejor rendimiento en el cortafuegos VM-Series, asegúrese de:

- *Habilitar la fijación de CPU.*
- *Deshabilite la Protección de reproducción, si ha configurado Túneles IPSec.*

  En la interfaz web del cortafuegos, seleccione ***Network (Red)*** *>* ***IPSec Tunnels (Túneles IPSec)****, seleccione un túnel IPSec, haga clic en* ***General*** *seleccione* ***Show Advanced Options (Mostrar opciones avanzadas)*** *y deshabilite* ***Enable Replay Protection (Habilitar protección de reproducción)****.*

STEP 2 | Acceda a la CLI en el cortafuegos VM-Series.

STEP 3 | Habilite el modo de acceso VLAN.

```
request plugins vm-series vlan-mode access-mode on
```

on habilita el modo de acceso VLAN; para usar el modo troncal VLAN, introduzca **`request plugins vm-series vlan-mode access-mode off`**.

STEP 4 | Reinicie el cortafuegos.

```
request restart system
```

STEP 5 | Verifique la configuración del modo VLAN.

```
show plugins vm-series vlan-mode
```

 ©2024 Palo Alto Networks, Inc.

Habilitación del soporte de colas múltiples para NIC en ESXi

Las colas múltiples permiten que el rendimiento de la red escale con el número de vCPU y permite el procesamiento paralelo de paquetes a través de la creación de múltiples colas TX y RX. Modifique el archivo .vmx o acceda a la Configuración avanzada para habilitar múltiples colas.

El ajuste de pNIC también se aplica a NSX-T, ya que ESXi es el hipervisor para las implementaciones de NSX-T.

STEP 1 | Habilite múltiples colas.

1. Abra el archivo .vmx.
2. Añada el siguiente parámetro:

```
ethernetX.pnicFeatures = “4”
```

STEP 2 | Habilite receive-side scaling (RSS).

1. Inicie sesión en la CLI en el host ESXi.
2. Ejecute el siguiente comando:

```
$ vmkload_mod -u ixgbe $ vmkload_mod ixgbe RSS=”4,4,4,4,4,4”
```

STEP 3 | Para obtener el mejor rendimiento, asigne hilos de CPU adicionales por dispositivo ethernet/vSwitch. Esto está limitado por la cantidad de recursos de CPU de reserva disponibles en el host ESXi.

1. Abra el archivo .vmx.
2. Añada el siguiente parámetro:

```
ethernetX.ctxPerDev = “1”
```

Ajuste de función de red virtual (VNF) para el rendimiento

Este tema proporciona una guía para afinar la Virtualización de funciones de red (VNF) para implementaciones VM-Series. Es una referencia para ayudarle a elegir algunas de las configuraciones de parámetros para una implementación VM-Series. Antes de intentar afinar debe estar familiarizado con los pasos necesarios para la instalación del cortafuegos VM-Series en el hipervisor VMware vSphere (ESXi), incluido cómo configurar los parámetros y atributos del ajuste.

Es posible que esta guía no se pueda aplicar a las implementaciones VM-Series en entornos de caja blanca o caja gris dirigidos a casos de uso de SD-WAN, MSSP o CSSP.

VM-Series es un dispositivo de alto rendimiento y está disponible en varios formatos, dependiendo del tamaño, la huella del hipervisor y su ubicación de implementación en la nube pública o privada.

Los cambios de configuración global y a nivel de host afectan a otras máquinas virtuales que se ejecutan en el mismo host. Debe tener en cuenta cualquier sacrificio o compensación, y elegir con prudencia los parámetros que mejor se adapten a su implementación.

- Parámetros de puesta apunto de ESXi

 ©2024 Palo Alto Networks, Inc.

- Casos de uso
- Referencias

Parámetros de puesta apunto de ESXi

Para obtener los mejores resultados en el rendimiento de VM-Series, puede afinar los parámetros de E/S de red, hipervisor y hardware.

Los parámetros mencionados aquí no se aplican a todos los modelos de implementación.

- Configuración de BIOS
- Configuración física
- Configuración de NIC virtual
- Consideraciones sobre recursos y NUMA

Configuración de BIOS

Esta sección recomienda configuraciones de BIOS Power Management, Hyperthreading e Intel VT-D que pueden mejorar el rendimiento del cortafuegos VM-Series y concluye con una configuración de BIOS de muestra.

- Gestión de energía
- Hyperthreading
- Tecnología de virtualización de Intel para E/S dirigida
- Ejemplo de configuración de BIOS

Gestión de energía

Para las aplicaciones sensibles a la latencia, cualquier forma de gestión de la energía añade latencia a la ruta donde un sistema inactivo (en uno de varios modos de ahorro de energía) responde a un evento externo. VMware recomienda configurar el ajustes de gestión de energía del BIOS en "alto rendimiento estático" (sin gestión de energía controlada por el sistema operativo), desactivando efectivamente cualquier forma de gestión de energía activa. Los servidores con unidades centrales de procesamiento Intel Nehalem class y posterior (Intel Xeon 55xx y posterior) ofrecen otras dos opciones de gestión de la energía: Estados C e Intel Turbo Boost.

La opción de dejar los estados C habilitados puede dar como resultado el aumento de la latencia de la memoria y, por lo tanto, no se recomienda para cargas de trabajo de baja latencia. Incluso el estado C mejorado, conocido como C1E, introduce latencias más largas para llevar a las CPU del estado de reposo (inactivo) a la máxima potencia. VMware recomienda deshabilitar C1E en el BIOS para reducir aún más las latencias.

- Para HP, fije el modo de regulación de energía (Power Regulator Mode) en modo estático alto y desactive el procesador QPI, la compatibilidad con estado C y la compatibilidad con C1E.
- Para Dell, fije el modo de gestión de energía, la energía de la CPU y la gestión del rendimiento en Máximo rendimiento.

Otro parámetro a tener en cuenta es el de Estados P. Por razones de rendimiento, desactive la configuración del estado P en el BIOS.

 ©2024 Palo Alto Networks, Inc.

Intel Turbo Boost puede provocar variaciones de rendimiento a lo largo del tiempo. Para un rendimiento constante y determinista, desactive Turbo Boost.

Hyperthreading

Si el hardware y el BIOS admiten hyperthreading, ESXi habilita automáticamente el hyperthreading en los hosts. Para obtener el mejor rendimiento de los cortafuegos VM-Series, desactive el hyperthreading en los hosts ESXi.

Si el entorno de implementación garantiza la habilitación de hyperthreading, asegúrese de que todos los recursos de la CPU para el cortafuegos VM-Series estén reservados desde el mismo nodo NUMA/Socket que tiene acceso a los dispositivos PCI.

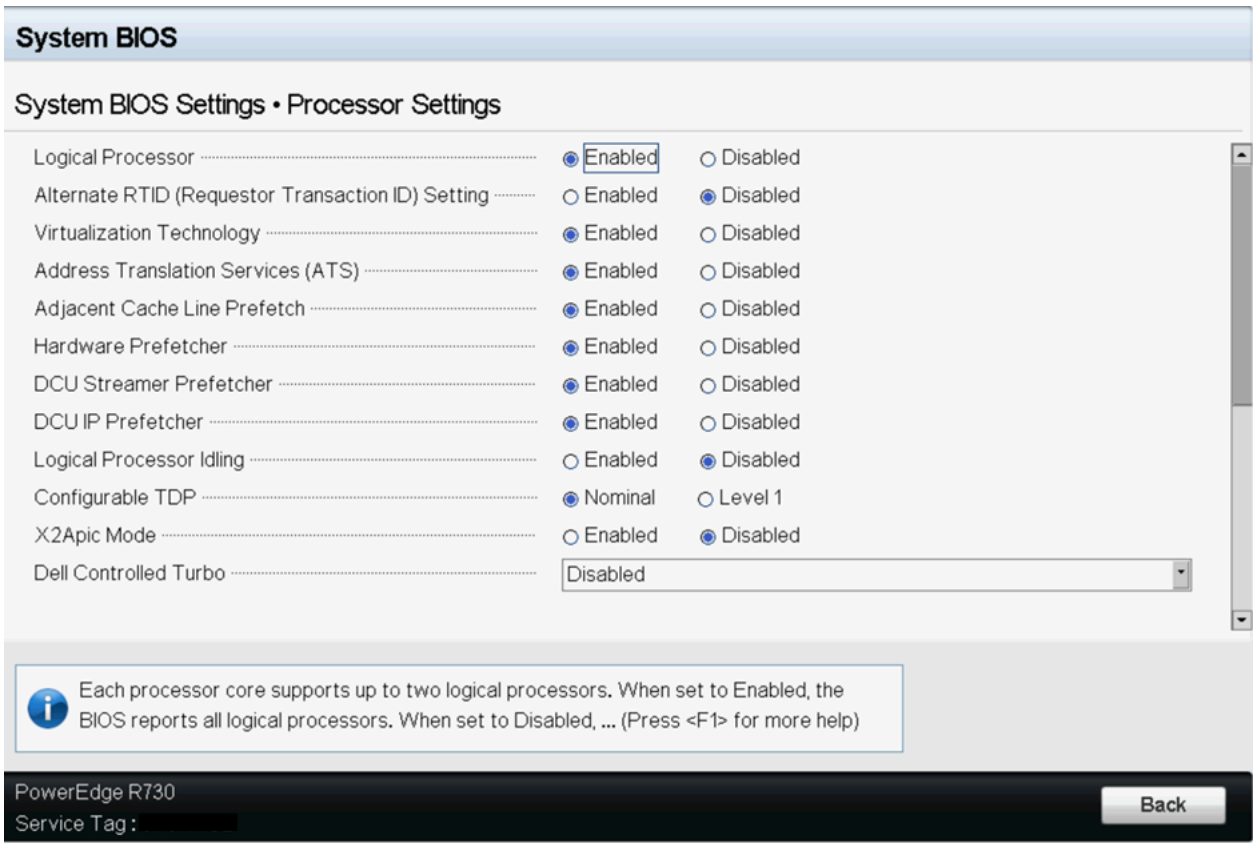
En general, configure el PA-VM como una única máquina virtual NUMA. Consulte Consideraciones sobre recursos y NUMA para más información.

Tecnología de virtualización de Intel para E/S dirigida

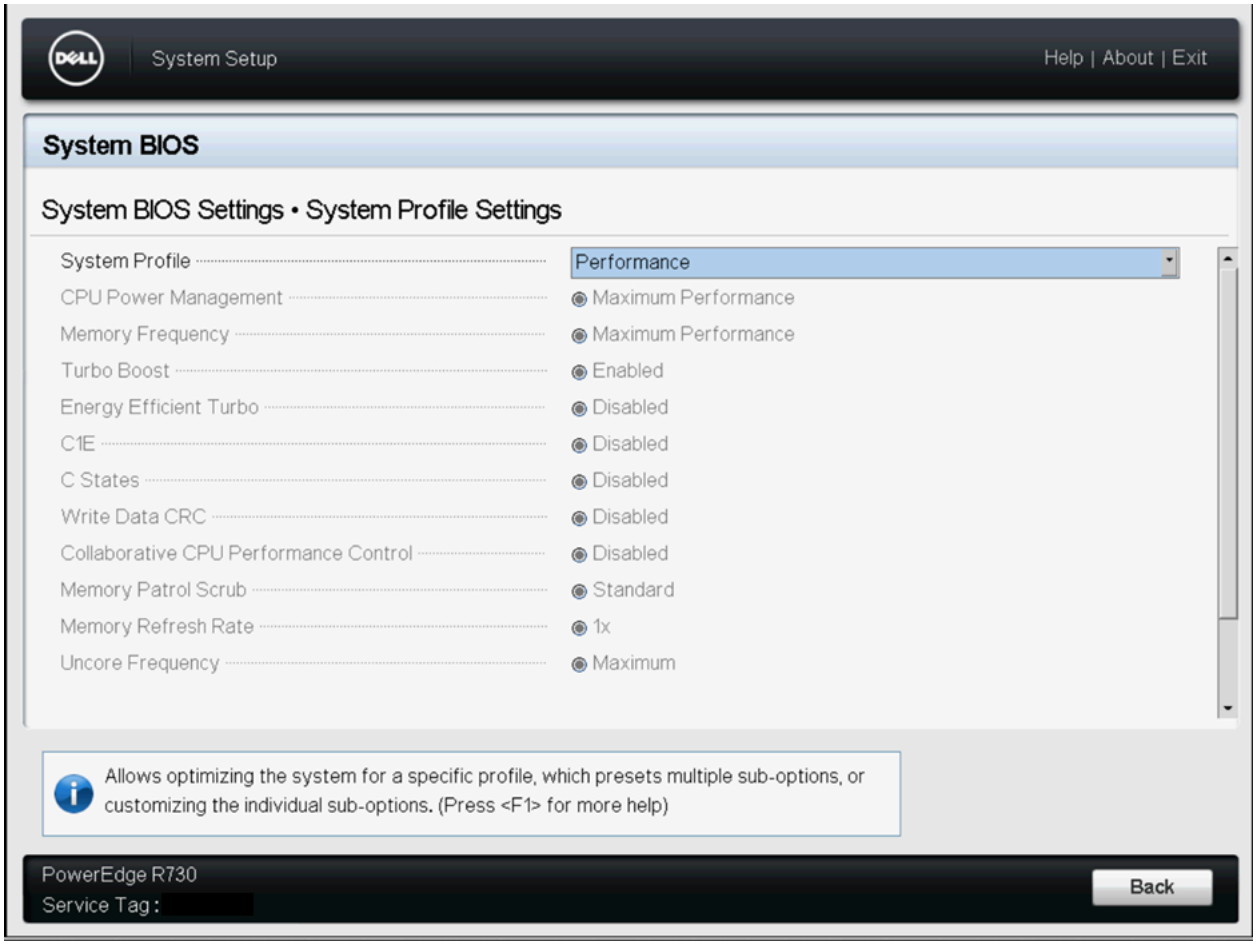
La tecnología de virtualización Intel para E/S dirigida (Intel VT-D) permite que una tarjeta LAN se dedique a un sistema invitado, lo que permite un mayor rendimiento de la red más allá del de una tarjeta LAN emulada. Habilite esta función en el BIOS. Si planea aprovechar SR-IOV para el rendimiento (recomendado), habilite la configuración del BIOS SRI-OV.

Ejemplo de configuración de BIOS

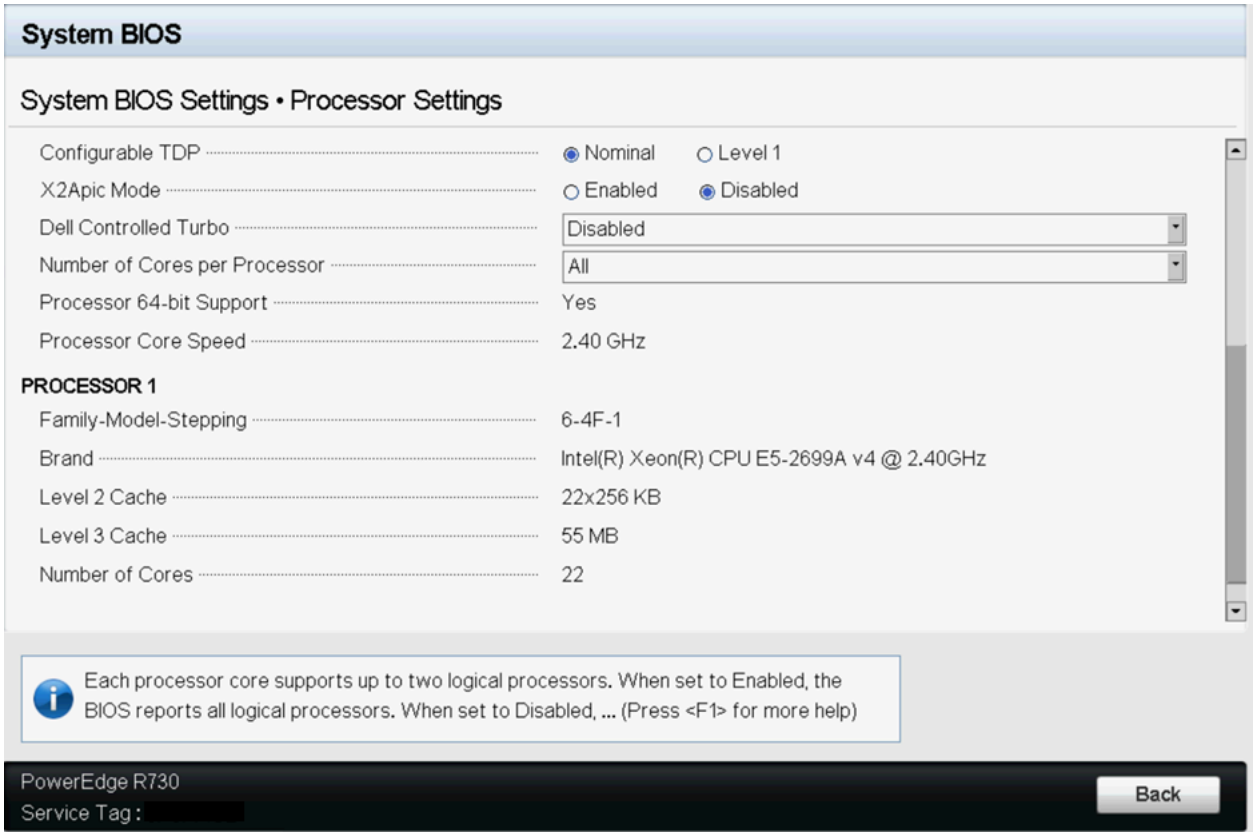
Las siguientes capturas de pantalla muestran la configuración del perfil del sistema y la configuración del procesador para un BIOS de Dell.



 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.



Configuración física

La mayoría de las tarjetas de interfaz de red (NIC) de 1GbE o 10GbE admiten una función llamada moderación de interrupciones o aceleración de interrupciones, que fusiona las interrupciones de la NIC al host para que el host no se desborde y pase todos sus ciclos de CPU procesando interrupciones. Sin embargo, para las cargas de trabajo sensibles a la latencia, el tiempo que la NIC retrasa la entrega de una interrupción para un paquete recibido, o un paquete que se ha enviado correctamente por cable, es el tiempo que aumenta la latencia de la carga de trabajo. Para obtener el mejor rendimiento en PA-VM, desactive la moderación de interrupciones. Por ejemplo, desactive la moderación de interrupciones de la NIC física en el host ESXi de la siguiente manera:

```
# esxcli system module parameters set -m ixgbe -p
 "InterruptThrottleRate=0"
```

- Cola de transmisión
- Queue Pairing (Emparejamiento de cola)

Cola de transmisión

La capa pNIC de vínculo superior de ESXi también mantiene una cola de Tx de software de paquetes en cola para la transmisión, que de forma predeterminada contiene 500 paquetes. Si la carga de trabajo es de E/S intensiva, con grandes ráfagas de paquetes de transmisión, esta cola puede desbordarse y provocar que los paquetes se abandonen en la capa de vínculo superior. El tamaño de la cola de transmisión (Tx) se puede aumentar hasta 10.000 paquetes con el siguiente comando ESXi:

 ©2024 Palo Alto Networks, Inc.

```
# esxcli system settings advanced set -i 10000 -o /Net/
MaxNetifTxQueueLen
```

Según la NIC física y la versión específica del controlador ESXi que se utiliza en el host ESXi, a veces se pueden eliminar paquetes en el controlador pNIC porque el anillo de transmisión en el pNIC es demasiado pequeño y está lleno. La mayoría de los controladores pNIC le permiten aumentar el tamaño del anillo de transmisión mediante el siguiente comando:

```
# ethtool -G vmnic0 tx 4096
```

Este comando aumenta el tamaño del anillo de Tx a 4096 entradas. El tamaño máximo que puede establecer para un controlador pNIC específico, así como el tamaño actual del anillo de Tx en efecto, se pueden determinar mediante el siguiente comando:

```
# 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
```

El ajuste de pNIC también se aplica a NSX-T, ya que ESXi es el hipervisor para las implementaciones de NSX-T.

Queue Pairing (Emparejamiento de cola)

Algunos controladores pNIC, como ixgbe de Intel y bnx2x de Broadcom, también admiten el "emparejamiento de cola", que indica a la capa de vínculo superior de ESXi que el subproceso de recepción (NetPoll) también procesará la finalización de los paquetes transmitidos en una cola de transmisión emparejada. Para ciertas cargas de trabajo de transmisión pesada, esto puede causar demoras en el procesamiento de finalización de las transmisiones, lo que hace que el anillo de transmisión de la vNIC se quede sin espacio para transmitir paquetes adicionales y obligue al controlador de la vNIC en el sistema operativo invitado a abandonar paquetes.

La desactivación del emparejamiento de colas para todas las pNIC en un host ESXi crea un subproceso independiente para procesar las finalizaciones de transmisión de pNIC. Como resultado, las finalizaciones se procesan de manera oportuna, liberando espacio en el anillo de transmisión de la vNIC para transmitir paquetes adicionales.

El comando de ESXi para deshabilitar el emparejamiento de colas es:

```
# esxcli system settings advanced set -o /Net/
NetNetqRxQueueFeatPairEnable -i 0
```

Para que esto surta efecto, debe reiniciar el host ESXi.

Si se utiliza PCI-passthrough en VM-700 en un host dedicado, no será necesario ajustar el rendimiento del controlador NIC/NIC. Sin embargo, este modo de implementación no es común.

 ©2024 Palo Alto Networks, Inc.

Configuración de NIC virtual

Si es posible, utilice SR-IOV para obtener un mejor rendimiento, como se explica en los siguientes temas:

- SR-IOV
- Combinación de VMXNET3/vSwitch y de interrupción virtual
- Habilite la compatibilidad con varias colas en Intel x710/x520

SR-IOV

- El cambio de los parámetros del módulo para un controlador SR-IOV requiere reiniciar el host ESXi.
- Deshabilite la moderación de interrupción de NIC física en el host ESXi de la siguiente manera:

```
# esxcli system module parameters set -m ixgbe -p
 "InterruptThrottleRate=0“
```

- Si habilita la compatibilidad con varias colas, también debe habilitar el ajuste de escala en el lado de recepción (RSS) para el controlador.
  - Para habilitar RSS, establezca el valor del puerto en 4.
  - Especifique los puertos en una cadena separada por comas.

  Ejemplo: configure 3 NIC con 2 puertos cada una.

```
$ 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”
```

  Ejemplo: configure RSS para un solo puerto:

```
$ vmkload_mod -u ixgbe esxcli system module parameters set -m ixgbe
 -p RSS=”0,4,0,0,0,0”
```

Combinación de VMXNET3/vSwitch y de interrupción virtual

De forma predeterminada, VMXNET3 admite un algoritmo de fusión de interrupciones (por las mismas razones por las que las NIC físicas implementan la moderación de interrupciones). Para evitar desbordar el sistema host con demasiadas interrupciones, se recopilan paquetes y se genera una sola interrupción para varios paquetes. Esto se denomina fusión de interrupciones.

La fusión de interrupciones se refiere a la cantidad de tráfico que recibe una interfaz de red, o el periodo de tiempo que pasa después de que se recibe el tráfico, antes de emitir una interrupción dura. Una interrupción demasiado temprana o demasiado frecuente da como resultado un rendimiento deficiente del sistema, ya que el kernel detiene (o "interrumpe") una tarea en ejecución para gestionar la solicitud de interrupción del hardware. Interrumpir demasiado tarde puede provocar una pérdida de tráfico, si no se retira el tráfico de la NIC en el momento adecuado dado que el tráfico que llega sobrescribe el tráfico anterior que aún espera ser recibido en el kernel. Para deshabilitar esta funcionalidad a través de cliente web de vSphere, vaya a **VM settings (Configuración de VM)** > **Options (Opciones)** > **Advanced General (General**

 ©2024 Palo Alto Networks, Inc.

avanzado) > **Configuration Parameters (Parámetros de configuración)** y añada una entrada para **`ethernetX.coalescingScheme`** con el valor **`deshabilitado`**.

Para deshabilitar la fusión de interrupciones virtuales para todas las NIC virtuales en el host (que afecta a todas las máquinas virtuales, no solo a las sensibles a la latencia), configure la opción de rendimiento de red avanzada. Vaya a **Configuration (Configuración)** > **Advanced Settings (Configuración avanzada)** > **Net (Red)** y fije **`CoalesceDefaultOn`** en **`0`** (deshabilitado).

Habilite la compatibilidad con varias colas en Intel x710/x520

Utilice ESXi 6.0.0 o posterior, con una versión de controlador ixgbe compatible con varias colas. Consulte Versiones del controlador SR-IOV en la Matriz de compatibilidad. Modifique el archivo `.vmx` o acceda a **Advanced Settings (Configuración avanzada)** para habilitar la compatibilidad con varias colas:

```
ethernetX.pnicFeatures = "4"
```

Para establecer la afinidad multinúcleo para que un vSwitch pueda superar los 300 K PPS, establezca:

```
ethernetX.pnicFeatures = "4" ethernetX.ctxPerDev = "1"
```

Ajuste **`ethernetX.ctxPerDev = "1"`**, es como un indicador binario (establecido en 1 para habilitar). Este marcador binario añade un subproceso de la CPU para procesar el tráfico solo desde el puerto **`ethernetX`**. Esto da como resultado un mejor rendimiento de la programación del tráfico.

Consideraciones sobre recursos y NUMA

NUMA significa acceso a memoria no uniforme. Los procesadores de varios núcleos tienen diseños complicados. Para abordar los problemas de rendimiento en dichos sistemas, debe conocer todos los matices de NUMA y la afinidad del procesador (CPU Pinning). Aspectos vitales a tener en cuenta:

- ¿En qué núcleos se están ejecutando nuestros subprocesos? (si el hyperthreading está habilitado, marque Hyperthreading)
- ¿En qué núcleos se ejecutan nuestras vCPU? (afinidad)
- ¿En qué socket NUMA está instalada la tarjeta NIC física?
- ¿Dónde se ha asignado la memoria? (Efectos NUMA)

  Los subprocesos que se ejecutan en cualquier socket ven un espacio de memoria unificado; por lo tanto, pueden leer/escribir en la memoria que es local para otros sockets.
- ¿Se comparte la memoria entre diferentes sockets en un nodo?
- Se necesita más tiempo para acceder a la memoria en diferentes sockets que para acceder a la memoria local.

  Los efectos NUMA ocurren cuando los subprocesos acceden de forma masiva a la memoria en un dominio NUMA diferente. Para evitar problemas de acceso a la memoria no uniforme (NUMA), evite la interconexión de ruta rápida (QPi) entre la comunicación del Socket 0 y el Socket 1.

Para máquinas virtuales sensibles a la latencia como PA-VM, VMware recomienda que no comprometa en exceso las vCPU en comparación con la cantidad de CPU físicas (procesadores) en el host ESXi. Por ejemplo, si el host tiene 8 núcleos de CPU, limite la cantidad de vCPU para su máquina virtual a 7. Esto garantiza que el programador de VMkernel de ESXi tenga más posibilidades de colocar las vCPU en pCPU que no compitan con otros contextos de programación, como las vCPU de otras máquinas virtuales o

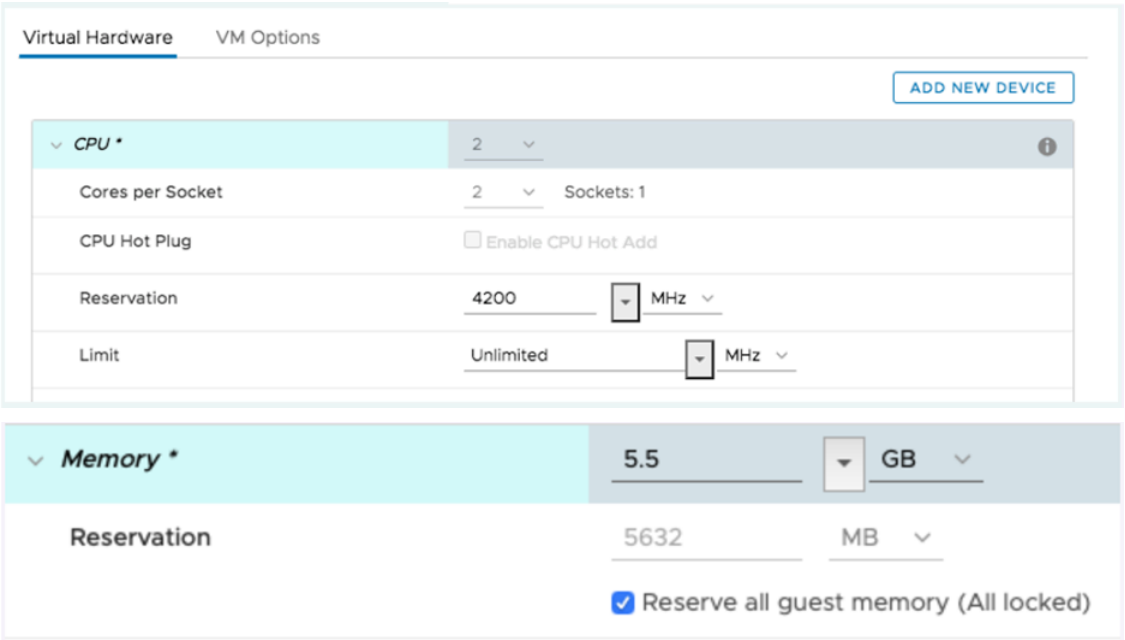
 ©2024 Palo Alto Networks, Inc.

helper worlds de ESXi. Es una práctica recomendada asegurarse de que la cantidad de vCPU que asigna a la VM no supere el número de procesos o subprocesos activos que consumen CPU en la VM.

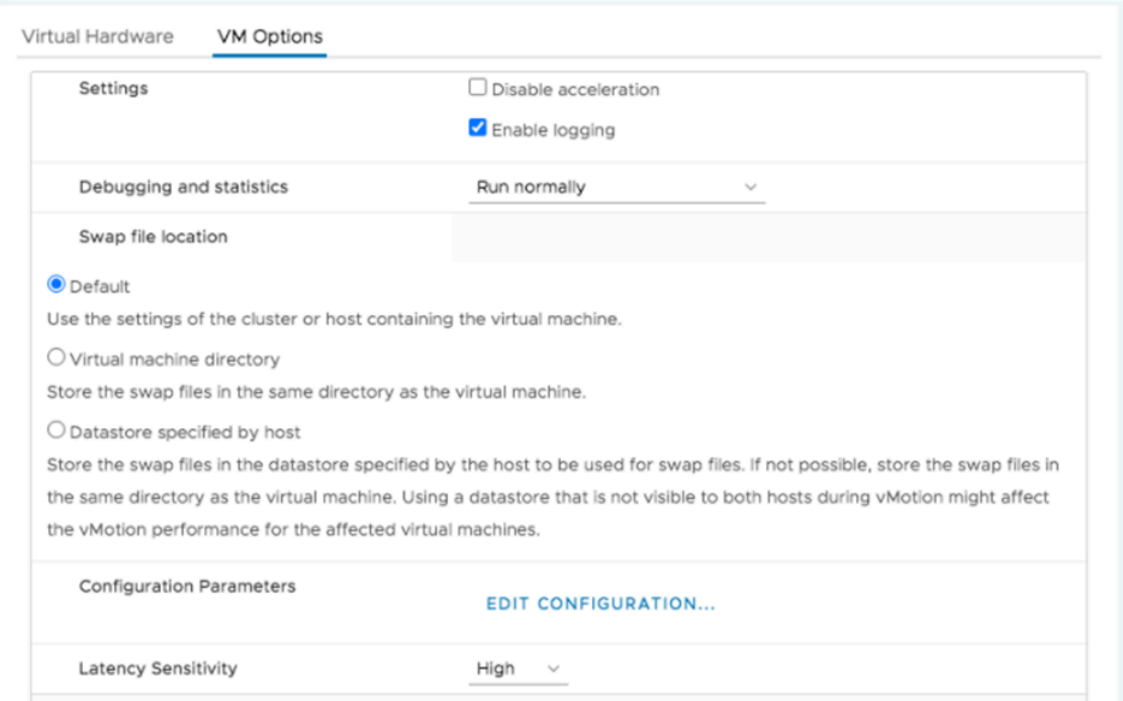
Para obtener el mejor rendimiento, todas las CPU virtuales deben programarse en el mismo nodo NUMA y toda la memoria de la máquina virtual debe caber y asignarse fuera de la memoria física local adjunta a ese nodo NUMA. Esto se puede cambiar usando la configuración de VM **`numa.nodeAffinity = 0, 1, …`** donde 0, 1, y así sucesivamente, son los números de socket.

Para asegurarse de que la máquina virtual obtenga acceso exclusivo a los recursos de la CPU, establezca la sensibilidad de latencia en Alta. Para que la nueva configuración surta efecto, la reserva de CPU de VM debe establecerse al máximo, la memoria debe reservarse y el límite de CPU debe establecerse como ilimitado.

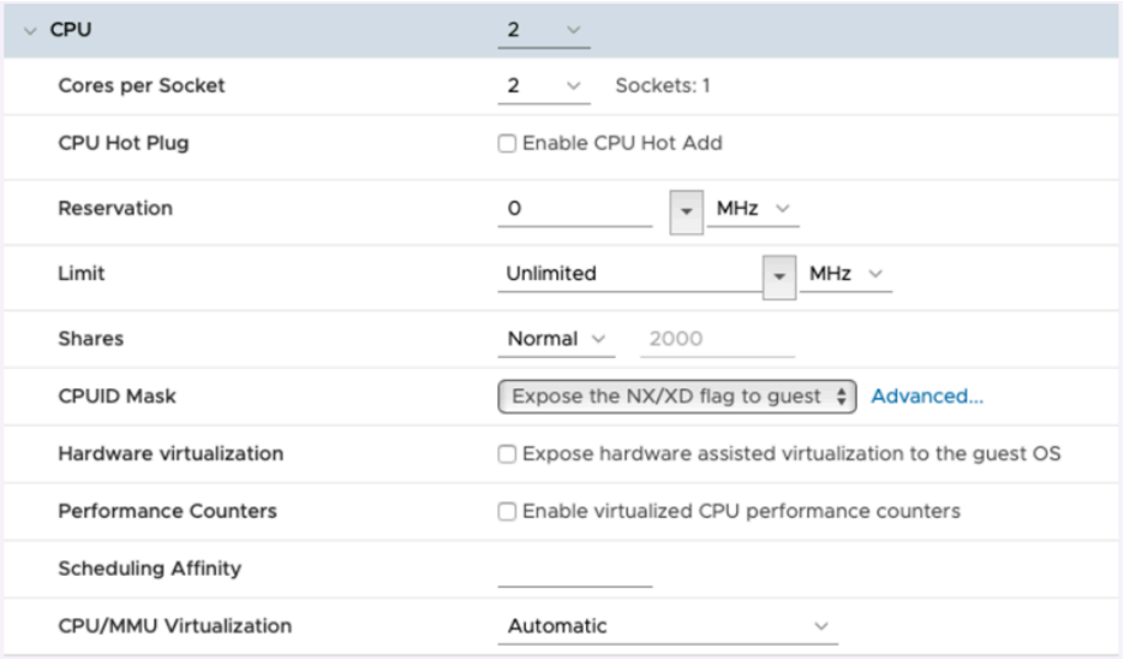
- En las versiones más recientes, utilice el cliente web de vSphere para establecer la opción de sensibilidad de latencia de VM en Alta (el valor predeterminado es Normal).
- En versiones anteriores, establezca **`sched.cpu.latencySensitivity`** en Alta.



 ©2024 Palo Alto Networks, Inc.



Además, las vCPU de VM se pueden anclar a núcleos de CPU de host mediante la configuración de VM **Host Affinity (Afinidad de host)**, para que nunca se programen en diferentes núcleos. Tenga en cuenta NUMA y hyperthreading cuando utilice la opción Host Affinity. Evite la opción Host Affinity si el sistema está sobrecargado. Para obtener más detalles, consulte Problemas potenciales con la afinidad del procesador (CPU Affinity).



Después de implementar los parámetros de ajuste, use esxtop o gráficos de CPU para verificar CPU Ready (% RDY) y Co Stop (% CSTP) para la VM. Ambos valores deben estar cerca del 0% para garantizar el acceso exclusivo a los recursos de la CPU. También puede usar esxtop para verificar el uso de NUMA y

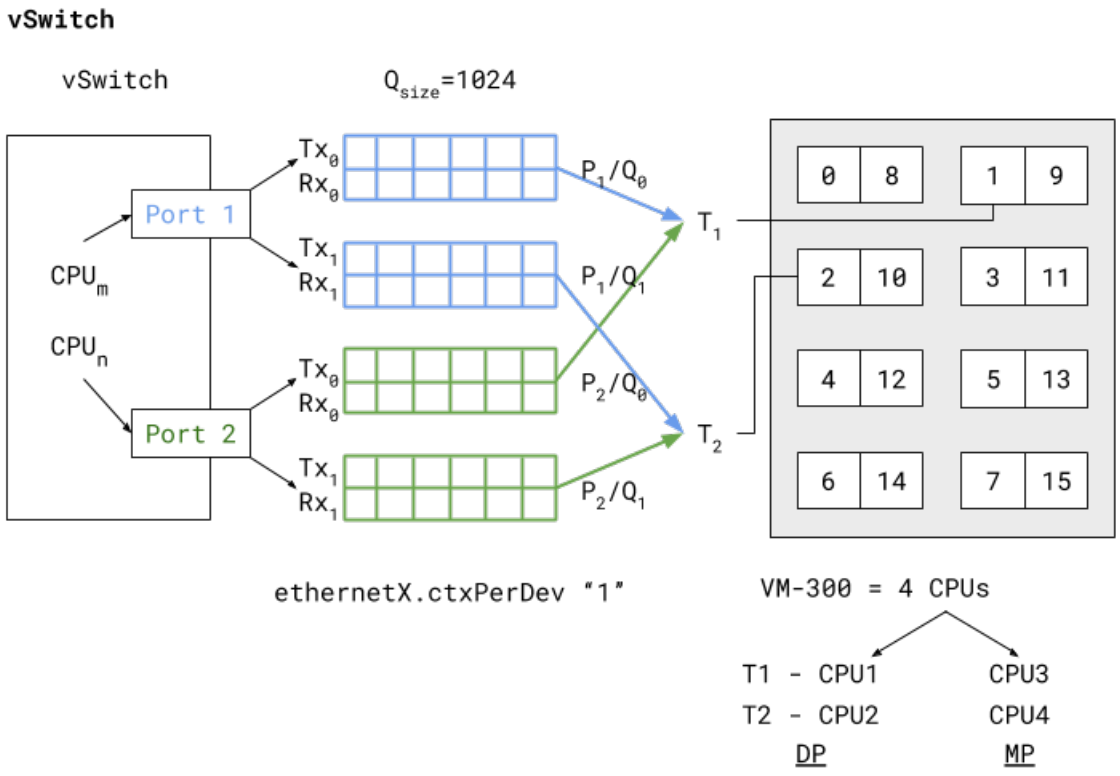
 ©2024 Palo Alto Networks, Inc.

asegurarse de que los recursos de memoria para la VM no se distribuyan entre los nodos de NUMA. Para obtener más información, consulte Interpretación de estadísticas de esxtop .

Casos de uso

Caso de uso 1: implementación de vSwitch

La siguiente imagen muestra una implementación de una PA-VM en un host ESXi donde los puertos de datos “Puerto 1” y “Puerto 2” están vinculados a eth1 y eth2 de la PA-VM. Cada puerto alberga dos pares de colas (por ejemplo, Tx0/Rx0 y Tx1/Rx1) o tiene habilitada la cola múltiple.



La habilitación de la compatibilidad con varias colas y RSS para equilibrar la carga de paquetes enviados/recibidos hacia/desde múltiples colas mejora el rendimiento del procesamiento. Basado en una lógica interna de vCPU a la asignación de puerto/cola (en este caso) los paquetes que llegan y se envían desde P1/Q0 y P2/Q0 son procesados por la tarea de plano de datos T1 que se ejecuta en (es decir, fijado a) vCPU1. La tarea T2 del plano de datos sigue una asociación similar, como se muestra en el diagrama de implementación de vSwitch anterior.

Las dos tareas del plano de datos se ejecutan en vCPU1 y vCPU2 y estas son CPU no hermanas (lo que significa que no comparten el mismo núcleo en caso de hyperthreading). Esto significa que incluso con el hyperthreading habilitado, la asignación de tareas se puede fijar a diferentes núcleos para un alto rendimiento. Además, todas estas vCPU de tareas de plano de datos pertenecen al mismo nodo (o socket) NUMA para evitar problemas de rendimiento relacionados con NUMA.

Se pueden abordar otros dos cuellos de botella de rendimiento aumentando el tamaño de las colas y dedicando una CPU virtual o subproceso a los puertos que programan el tráfico hacia y desde estos puertos. El aumento del tamaño de las colas (Qsize) creará espacio para grandes ráfagas repentinas de tráfico y evitará que se abandonen paquetes en situaciones de tráfico intenso. La adición de un subproceso de CPU dedicado (**`ethernetX.ctxPerDev = 1`**) al procesamiento de paquetes a nivel de puerto

 ©2024 Palo Alto Networks, Inc.

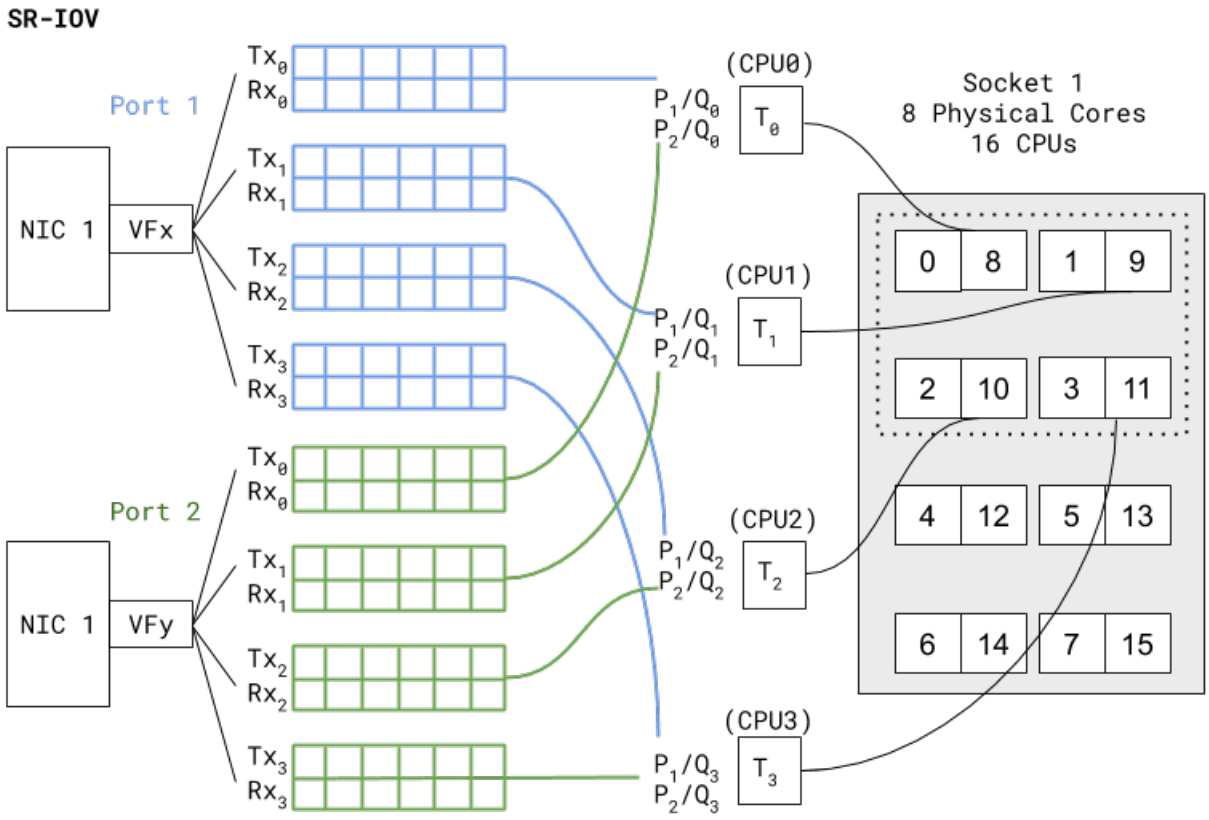
permitirá que el tráfico se procese a una mayor velocidad, lo que aumentará el rendimiento del tráfico para alcanzar la velocidad de línea.

La técnica de procesamiento de paquetes de PA-VM también determina el rendimiento. Esto se puede configurar en DPDK o PacketMMAP. DPDK usa un controlador de modo de sondeo (depende del tipo de controlador) para sondear constantemente los paquetes recibidos en las colas. Esto conduce a un mayor rendimiento. Dependiendo del período de sondeo, los paquetes observan la latencia. Si el sondeo es continuo (es decir, busy-poll un ajuste de la cli de PANOS), entonces el uso de vCPU para las tareas del plano de datos será del 100% pero producirá el mejor rendimiento. Internamente, el software utiliza un tiempo de sondeo de milisegundos para evitar la utilización innecesaria de los recursos de la CPU.

PacketMMAP, por otro lado, tiene un rendimiento más bajo que DPDK pero funciona con cualquier controlador de nivel de red. Para DPDK, el controlador vSwitch debe ser compatible con DPDK. PacketMMAP funciona con interrupciones que se generan cuando el puerto recibe un paquete y lo coloca en la cola de recepción. Esto significa que por cada paquete o grupo de paquetes, se generan interrupciones y los paquetes se vacían de la cola de recepción para su procesamiento. Esto resulta en una latencia más baja en el procesamiento de paquetes, pero un rendimiento reducido, porque las interrupciones deben procesarse cada vez, lo que genera una mayor sobrecarga de la CPU. En general, PacketMMAP tendrá una latencia de procesamiento de paquetes más baja que DPDK (sin modificación de busy-poll).

Caso de uso 2: Implementación de SR-IOV

El diagrama de SR-IOV a continuación muestra una implementación de PA-VM similar al caso de uso de vSwitch, pero en modo SR-IOV.



En SR-IOV, el puerto NIC físico compatible (se manifiesta como una función física) está esencialmente dividido en múltiples interfaces (se manifiesta como funciones virtuales). La figura anterior muestra que Port1 de NIC1 tiene una función virtual llamada VFX que está asociada como una de las interfaces del

 ©2024 Palo Alto Networks, Inc.

plano de datos PAVM, por ejemplo, eth1. Se crea una asociación similar para la función virtual de Port2 a PAVM eth2. La cadena de procesamiento de paquetes es similar a la de la implementación en el entorno vSwitch. La única diferencia es que los controladores de VF de SR-IOV deben ser compatibles con los que se utilizan en PAN-OS. Además, dado que no hay tráfico de conmutación de vSwitch interno (en el host), no es necesario establecer un subproceso dedicado para la programación del tráfico desde un puerto (es decir, **`ethernetX.ctxPerDev = 1`** no se requiere en este ajuste). Las interfaces con SR-IOV y DPDK producirán un rendimiento de procesamiento de paquetes aún mayor que el caso de uso de vSwitch.

Referencias

- Tuning VMware vCloud NFV for Data-Intensive Workloads (Ajuste de VMware vCloud NFV para cargas de trabajo con uso intensivo de datos)
- Best Practices for Performance Tuning of Telco and NFV Workloads in vSphere (Mejores prácticas para el ajuste del rendimiento de cargas de trabajo de Telco y NFV en vSphere)
- Potential Issues with CPU Affinity (Posibles problemas con la afinidad de CPU)
- Interpreting esxtop Statistics (Interpretación de estadísticas de esxtop)

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en vCloud Air

El cortafuegos VM-Series puede implementarse en un centro de datos virtual (vDC) en vCloud Air con el portal de vCloud Air, desde el portal de vCloud Director o mediante la API de vCloud Air.

- Acerca del cortafuegos VM-Series en vCloud Air
- Implementaciones compatibles con vCloud Air
- Implementación del cortafuegos VM-Series en vCloud Air

Acerca del cortafuegos VM-Series en vCloud Air

¿Dónde puedo usar esto?	¿Qué necesito?
• vCloud Air	• Licencia de cortafuegos VM-Series (BYOL) • Panorama • Plugin VM-Series

Puede implementar el cortafuegos VM-Series en un centro de datos virtual (vDC) en VMware vCloud Air mediante el portal de vCloud Air o desde el portal de vCloud Director. Y para gestionar de forma centralizada todos los cortafuegos físicos y VM-Series, puede utilizar un Panorama existente o implementar un nuevo Panorama local o en vCloud Air.

El cortafuegos VM-Series en vCloud Air requiere lo siguiente:

- Versión ESXi de la imagen de software, un archivo Open Virtualization Alliance (OVA), del sitio web de asistencia al cliente de Palo Alto Networks. En la actualidad, vCloud Air Marketplace no aloja la imagen de software.

  Para implementar de manera eficiente el cortafuegos VM-Series, incluya la imagen de software del cortafuegos en una vApp. Una vApp es un contenedor para dispositivos virtuales preconfigurados (imágenes del sistema operativo y máquinas virtuales) que se gestiona como un objeto único. Por ejemplo, si su vApp incluye un conjunto de aplicaciones de múltiples niveles y el cortafuegos VM-Series, cada vez que implemente la vApp, el cortafuegos VM-Series protegerá automáticamente el servidor web y el servidor de base de datos que se implementa con la vApp.
- Licencia y suscripciones adquiridas de un socio, distribuidor o directamente de Palo Alto Networks, en el modelo de licencia existente (BYOL); no hay disponible una licencia basada en el uso para VM-Series en vCloud Air.
- Debido a las restricciones de seguridad impuestas en vCloud Air, el cortafuegos VM-Series en vCloud Air se implementa mejor con las interfaces de capa 3 y las interfaces deben habilitarse para usar la dirección MAC asignada al hipervisor. Si no habilita la dirección MAC asignada al hipervisor, vSwitch de VMware no puede dirigir el tráfico a las interfaces del plano de datos en el cortafuegos VM-Series porque el vSwitch en vCloud Air no es compatible con el modo promiscuo o las transmisiones MAC falsificadas. El cortafuegos VM-Series no puede implementarse con interfaces tap, de capa 2 o de cable virtual.

El cortafuegos VM-Series en vCloud Air puede implementarse en una configuración de alta disponibilidad activa/pasiva. Sin embargo, el cortafuegos VM-Series en vCloud Air no admite las capacidades de supervisión de VM para máquinas virtuales que se alojan en vCloud Air.

Para obtener más información sobre vCloud Air, consulte la documentación de vCloud Air de VMware.

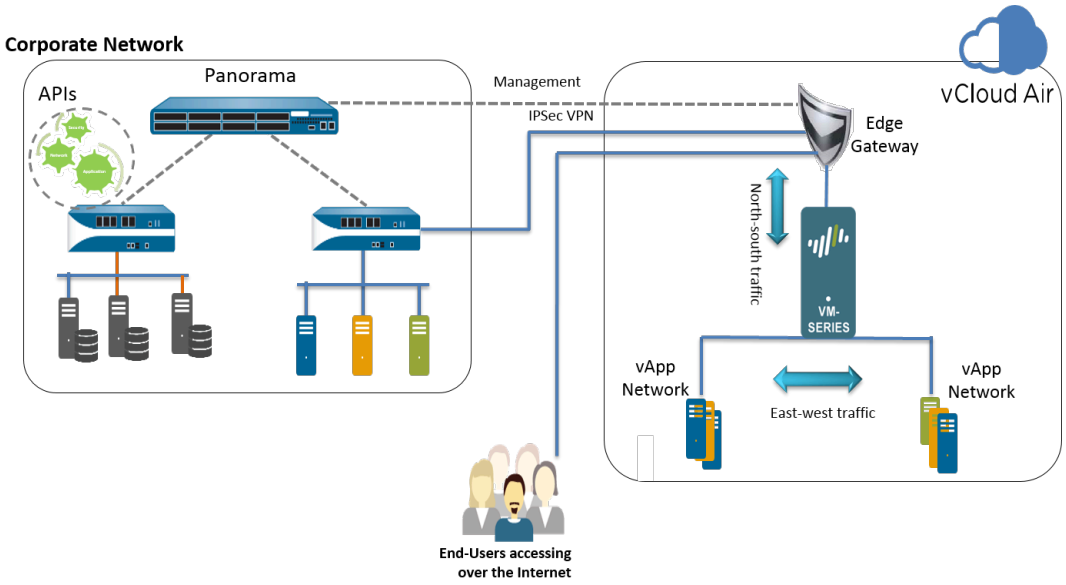
 ©2024 Palo Alto Networks, Inc.

Implementaciones compatibles con vCloud Air

Para habilitar las aplicaciones de manera segura, bloquear amenazas conocidas y desconocidas, y estar al tanto de los cambios en su entorno, puede implementar el cortafuegos VM-Series en vCloud Air con las interfaces de Capa 3 de las siguientes maneras:

- **Proteger el perímetro del centro de datos virtuales**: implemente el cortafuegos VM-Series como una máquina virtual que conecta redes aisladas y con ruta en vCloud Air. En esta implementación, el cortafuegos protege todo el tráfico vertical que atraviesa la infraestructura en vCloud Air.
- **Configurar una nube híbrida**: amplíe su centro de datos y su nube privada en vCloud Air y use una conexión VPN para habilitar la comunicación entre la red corporativa y el centro de datos. En esta implementación, el cortafuegos VM-Series usa IPSec para cifrar el tráfico y proteger a los usuarios que acceden a la nube.
- **Proteger el tráfico entre las subredes de aplicaciones en vDC**: para mejorar la seguridad, segmente su red y aísle el tráfico creando niveles de aplicación, y luego implemente el cortafuegos VM-Series para protegerse de las amenazas laterales entre las subredes y los niveles de aplicación.

La siguiente ilustración combina los tres escenarios de implementaciones e incluye a Panorama. Panorama mejora las actualizaciones de políticas, centraliza la gestión de políticas y permite una generación de informes y un almacenamiento de logs centralizados.



 ©2024 Palo Alto Networks, Inc.

Implementación del cortafuegos VM-Series en vCloud Air

Use las instrucciones de esta sección para implementar su cortafuegos VM-Series en un vDC dedicado o bajo petición en vCloud Air. Este procedimiento entiende que usted configuró su vDC, incluidas las puertas de enlace necesarias para permitir el tráfico entrante y saliente del vDC, y las redes necesarias para dirigir el tráfico de gestión y el tráfico de datos por el vDC.

STEP 1 | Obtenga el archivo OVA de VM-Series del sitio web de asistencia al cliente de Palo Alto Networks; vCloud Air Marketplace no aloja la imagen de software en la actualidad.

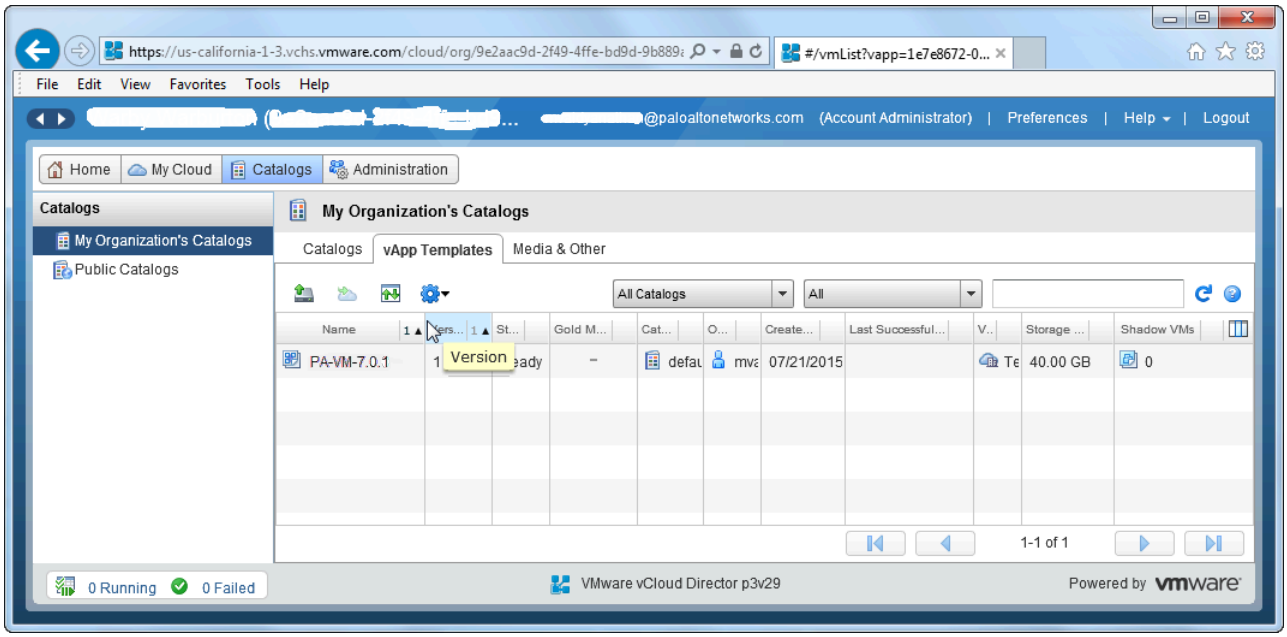
1. Vaya a: www.paloaltonetworks.com/services/support.html.
2. Filtre por **PAN-OS for VM-Series Base Images (PAN-OS para imágenes base de VM-Series)** y descargue el archivo OVA. Por ejemplo, PA-VM-ESX-9.1.0.ova.

STEP 2 | Extraiga el OVF de la imagen OVA e importe el archivo OVF en su catálogo de vCloud Air.

Al extraer la imagen OVA, asegúrese de colocar todos los archivos (.mf, .ovf, y .vmdk) en el mismo directorio.

Para obtener instrucciones sobre cómo extraer el OVF del OVA, consulte la documentación de VMware: https://www.vmware.com/support/developer/ovf/#sthash.WUp55ZyE.dpuf

Cuando importa el archivo OVF, la imagen de software para el cortafuegos VM-Series se detalla en **My Organization's Catalogs (Catálogos de mi organización)**.



 ©2024 Palo Alto Networks, Inc.

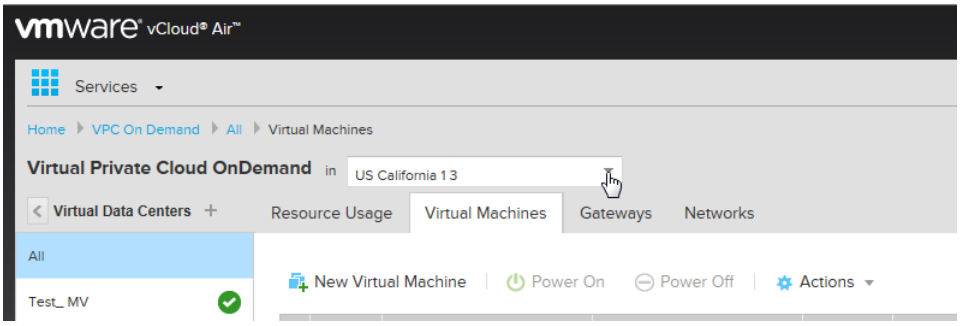
STEP 3 | Seleccione su flujo de trabajo.

Una vApp es una colección de plantillas para dispositivos virtuales preconfigurados que contienen máquinas virtuales e imágenes del sistema operativo.

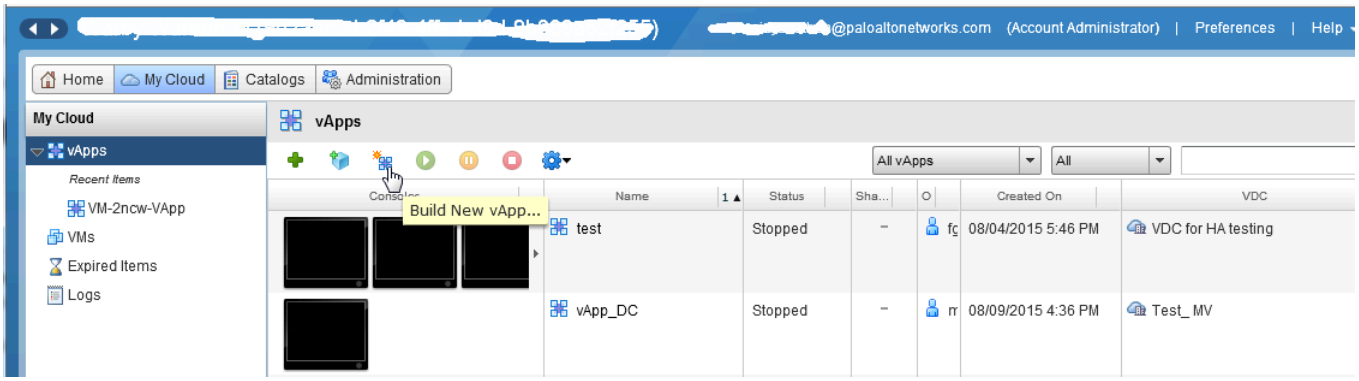
- Si desea crear un nuevo vDC y una nueva vApp que incluya el cortafuegos VM-Series, vaya al paso 4
- Si ya implementó un vDC y tiene una vAPP y ahora desea añadir el cortafuegos VM-Series a la vApp para proteger el tráfico, vaya al paso 5

STEP 4 | Cree un vDC y una vApp que incluya el cortafuegos VM-Series.

1. Inicie sesión en vCloud Air.
2. Seleccione **VPC OnDemand (VPC bajo petición)** y seleccione la ubicación en la que desea implementar el cortafuegos VM-Series.



3. Seleccione **Virtual Data Centers (Centros de datos virtuales)** y haga clic en **+** para añadir un nuevo Centro de datos virtuales.
4. Seleccione vDC, haga clic en el botón derecho y seleccione **Manage Catalogs in vCloud Director (Gestionar catálogos en vCloud Director)**. Se le redireccionará a la interfaz web de vCloud Director.
5. Cree una nueva vApp que contenga una o varias máquinas virtuales que incluyan el cortafuegos VM-Series:
   1. Select **My Cloud (Mi nube)** > **vApps** y haga clic en **Build New vApp (Crear nueva vApp)**.



   2. Seleccione **Name and Location (Nombre y ubicación)** y **Virtual Datacenter (Centro de datos virtual)** en el que se ejecutará esta vApp. De manera predeterminada, **Leases**

 ©2024 Palo Alto Networks, Inc.

(Arrendamientos) para el momento de la ejecución y el almacenamiento nunca vencen y la vApp no se detiene automáticamente.

3. **Add Virtual Machines (Añadir máquinas virtuales)**. Para añadir la imagen del cortafuegos VM-Series desde el menú desplegable **Look in: (Buscar en:)**, seleccione **My Organization's Catalog (Catálogo de mi organización)**, seleccione la imagen y haga clic en **Add (Añadir)**. Haga clic en **Next (Siguiente)**
4. Configure **Resources (Recursos)** para especificar las políticas de almacenamiento para las máquinas virtuales cuando se implementen. El cortafuegos VM-Series usa la opción **Standard (Estándar)**.
5. Configuración de **Virtual Machines (Máquinas virtuales)**. Asigne un nombre a cada una de las máquinas virtuales y seleccione la red a la que desea conectarla. Debe conectar NIC 0 (para el acceso de gestión) a la red de la ruta predeterminada; NIC 1 se utiliza para el tráfico de datos. Puede añadir NIC adicionales más tarde.
6. Revise la configuración y haga clic en **Finish (Finalizar)**.
7. Continúe al paso 6.

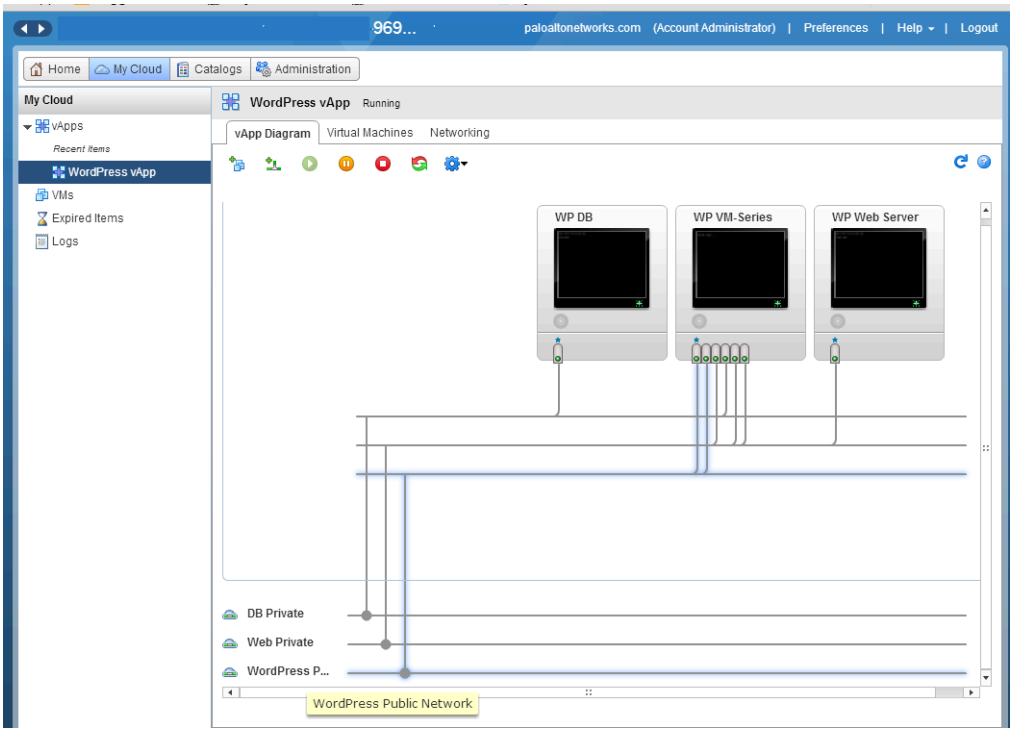
STEP 5 | Añada el cortafuegos VM-Series a una vApp.

1. Inicie sesión en vCloud Air.
2. Seleccione su **Virtual Data Center (Centro de datos virtual)** existente desde el panel izquierdo, haga clic con el botón derecho y seleccione **Manage Catalogs in vCloud Director** (Gestionar catálogos en vCloud Director). Se le redireccionará a la interfaz web de vCloud Director.
3. Seleccione **My Cloud (Mi nube)** > **vApps** y luego haga clic en el **Name (Nombre)** de la vApp en la que se incluirá el cortafuegos VM-Series.
4. Abra la vApp (doble clic en el nombre), seleccione **Virtual Machines (Máquinas virtuales)** y haga clic en ✚ para añadir una máquina virtual.
   1. En el menú desplegable **Look in: (Buscar en:)**, seleccione **My Organization's Catalog (Catálogo de mi organización)**, seleccione la imagen del cortafuegos VM-Series y haga clic en **Add (Añadir)**. Haga clic en **Next (Siguiente)**.
   2. Haga clic en **Next (Siguiente)** para omitir **Configure Resources (Configurar recursos)**. El cortafuegos VM-Series usa la opción **Standard (Estándar)** y no se debe modificar la política de almacenamiento.
   3. Introduzca un nombre en **Name (Nombre)** para el cortafuegos y para el acceso de gestión (**NIC 0)**, seleccione la red con ruta predeterminada y el **IP Mode (Modo de IP)**: estática o DHCP. Puede configurar NIC 1 y añadir NIC adicionales en el paso 6. Haga clic en **Next (Siguiente)**.
   4. Verifique cómo esta vApp se conecta a la máscara de red y dirección de puerta de enlace de vDC para las máquinas virtuales en esta vApp.
   5. Verifique que añadió el cortafuegos VM-Series y haga clic en **Finish (Finalizar)**.
   6. Continúe al paso 6.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Conecte la interfaz o las interfaces de datos del cortafuegos VM-Series a una red con ruta o aislada, como lo requiera su implementación.

1. En vCloud Director, seleccione **My Cloud (Mi nube)** > **vApps** y seleccione la vApp que acaba de crear o editar.
2. Seleccione **Virtual Machines (Máquinas virtuales)** y seleccione el cortafuegos VM-Series. Luego, haga clic con el botón derecho y seleccione **Properties (Propiedades)**.
3. Seleccione **Hardware**, desplácese hasta la sección de NIC y seleccione **NIC 1**.
4. Conecte la interfaz de la red del plan de datos a una red de vApp o a una red de VDC de la organización según sus necesidades de conectividad para el tráfico de datos al cortafuegos VM-Series. Para crear una red nueva, realice lo siguiente:
   1. En el menú desplegable Network (Red), haga clic en **Add Network (Añadir red)**.
   2. Seleccione **Network Type (Tipo de red)**, asígnele un nombre y haga clic en **OK (Aceptar)**.
   3. Verifique que la red nueva se haya conectado a la interfaz.
5. Para añadir NIC adicionales al cortafuegos, haga clic en **Add (Añadir)** y repita el paso 4 anterior. Puede adjuntar un máximo de siete interfaces del plano de datos al cortafuegos VM-Series.
6. Verifique que la interfaz de gestión del cortafuegos VM-Series esté conectada a la subred con ruta predeterminada en vDC y que al menos una interfaz del plano de datos esté conectada a la red aislada o con ruta.
   1. Seleccione **My Cloud (Mi nube)** > **vApps** y haga doble clic en el **Name (Nombre)** de la vApp que acaba de editar.
   2. Verifique la conectividad de red en **vApp Diagram (Diagrama de vApp)**.

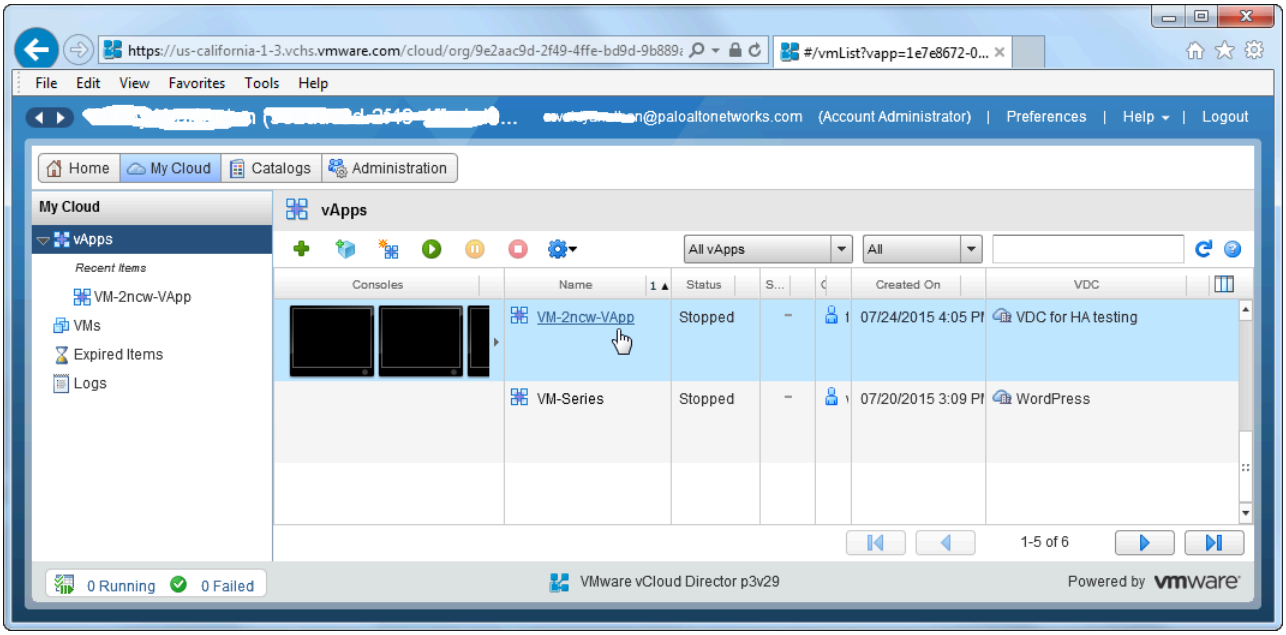


 ©2024 Palo Alto Networks, Inc.

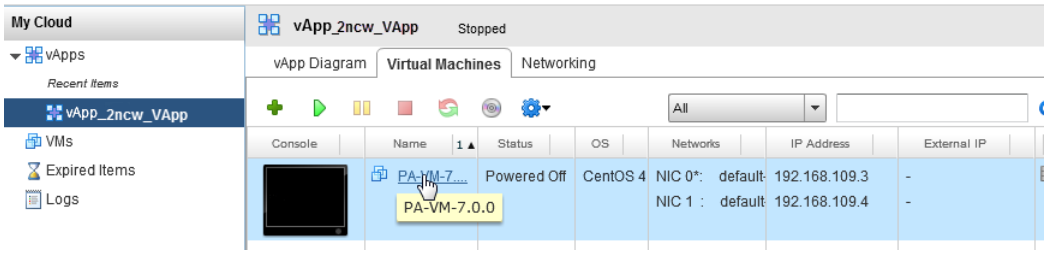
STEP 7 | (Opcional) Edite los recursos de hardware asignados para el cortafuegos VM-Series.

Solo se requiere si necesita asignar CPU, memoria o discos duros adicionales al cortafuegos.

1. Seleccione **My Cloud (Mi nube)** > **vApps** y haga doble clic en el **Name (Nombre)** de la vApp que acaba de implementar.



2. Seleccione **Virtual Machine (Máquina virtual)** y haga clic en el **Name (Nombre)** del cortafuegos VM-Series para acceder a las propiedades de la máquina virtual.



3. Añada recursos de **Hardware** adicionales para el cortafuegos VM-Series:
   - Consulte Requisitos del sistema VM-Series para ver los requisitos mínimos de la vCPU, la memoria y los requisitos de disco para su modelo VM-Series.
   - NIC: Una interfaz de gestión y hasta siete interfaces del plano de datos.

STEP 8 | Conecte el cortafuegos VM-Series.

STEP 9 | Configure una dirección IP para la interfaz de gestión del cortafuegos VM-Series.

Realice la Configuración inicial en VM-Series en ESXi.

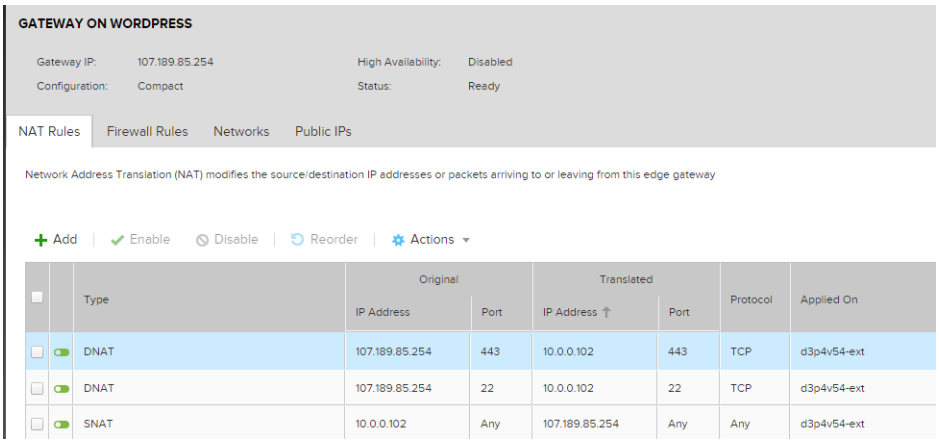
El cortafuegos VM-Series en vCloud Air es compatible con VMware Tools y usted puede Usar VMware Tools en el cortafuegos VM-Series en ESXi y vCloud Air para ver la dirección IP de gestión del cortafuegos VM-Series.

 ©2024 Palo Alto Networks, Inc.

STEP 10 | Defina reglas NAT en la puerta de enlace perimetral de vCloud Air para habilitar el acceso a Internet del cortafuegos VM-Series.

1. Seleccione **Virtual Data Centers (Centros de datos virtuales)** > **Gateways (Puertas de enlace)**, seleccione la puerta de enlace y haga doble clic para añadir **NAT Rules (Reglas de NAT)**.
2. Cree dos reglas DNAT. Una servirá para permitir el acceso SSH y otra para el acceso HTTPS a la dirección IP del puerto de gestión del cortafuegos VM-Series.
3. Cree una regla SNAT para traducir la dirección IP de origen interno para todo el tráfico iniciado desde el puerto de gestión en el cortafuegos VM-Series a una dirección IP externa.

Para enviar y recibir tráfico desde las interfaces del plano de datos en el cortafuegos, debe crear reglas DNAT y SNAT adicionales en la puerta de enlace perimetral de vCloud Air.



STEP 11 | Inicie sesión en la interfaz web del cortafuegos.

En este ejemplo, la URL para la interfaz web es https://107.189.85.254

La regla NAT en la puerta de enlace perimetral se traduce en el puerto y dirección IP externa 107.189.85.254:443 al puerto y dirección IP privada 10.0.0.102:443.

STEP 12 | Añada el código de autorización para activar las licencias en el cortafuegos.

Activación de la licencia.

STEP 13 | Configure el cortafuegos VM-Series para usar la dirección MAC asignada al hipervisor.

Direcciones MAC asignadas por el hipervisor

 ©2024 Palo Alto Networks, Inc.

STEP 14 | Configure las interfaces del plano de datos como interfaces de capa 3.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
2. Haga clic en el enlace de **ethernet 1/1** y configúrelo del siguiente modo:
   - **Tipo de interfaz: capa 3**
   - Seleccione la pestaña **Config (Configurar)** y asigne la interfaz al enrutador predeterminado.
   - En la pestaña **Config (Configuración)**, seleccione **New Zone (Nueva zona)** en el menú desplegable **Security Zone (Zona de seguridad)**. Defina una zona nueva (p. ej., untrust) y, a continuación, haga clic en **ACEPTAR**.
   - Seleccione **IPv4** y asigne una dirección IP estática.
   - En **Advanced (Avanzada)** > **Other Info (Otra información)**, amplíe el menú desplegable **Management Profile (Perfil de gestión)** y seleccione **New Management Profile (Nuevo perfil de gestión)**.
   - Introduzca un nombre en **Name (Nombre)** para el perfil, como allow_ping, y seleccione Ping en la lista de servicios permitidos; a continuación, haga clic en **OK (Aceptar)**.
   - Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.
3. Repita el proceso para cada interfaz adicional.
4. Haga clic en **Commit (Confirmar)** para guardar los cambios.

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en VMware NSX-T

El cortafuegos VM-Series se puede implementar en VMware NSX-T para proteger el tráfico Norte-Sur y Este-Oeste.

- Configuración del cortafuegos VM-Series en VMware NSX-T (norte-sur)
- Configuración del cortafuegos VM-Series en NSX-T (este-oeste)

Configuración del cortafuegos VM-Series en VMware NSX-T (norte-sur)

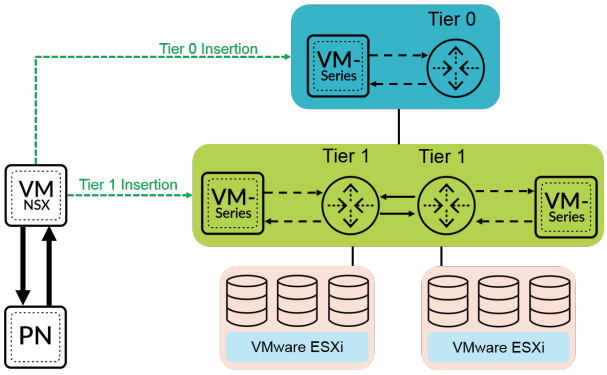
El cortafuegos VM-Series en VMware NSX-T integra los cortafuegos de Palo Alto de nueva generación y Panorama con los servidores host ESXi para proporcionar visibilidad completa y una habilitación segura de las aplicaciones de todo el tráfico norte-sur en su centro de datos definido por software de NSX-T.

Los siguientes temas ofrecen información sobre el cortafuegos VM-Series en VMware NSX-T:

- Implementaciones compatibles del cortafuegos VM-Series en VMware NSX-T (norte-sur)
- Componentes del cortafuegos VM-Series en NSX-T (norte-sur)
- Implementación del cortafuegos VM-Series en NSX-T (norte-sur)
- Amplíe la política de seguridad de NSX-V a NSX-T

Implementaciones compatibles del cortafuegos VM-Series en VMware NSX-T (norte-sur)

Puede implementar una o más instancias del cortafuegos VM-Series como servicio asociado en su centro de datos VMware NSX-T. Conecte un cortafuegos VM-Series a cualquier enrutador lógico de nivel 0 o nivel 1 para proteger el tráfico norte-sur. Puede implementar el cortafuegos VM-Series como una instancia de servicio independiente o dos cortafuegos en un par de alta disponibilidad (HA). Panorama gestiona la conexión con NSX-T Manager y los cortafuegos VM-Series implementados en su centro de datos definido por software de NSX-T.



- Inserción de nivel 0: la inserción de nivel 0 implementa un cortafuegos VM-Series en un enrutador lógico de nivel 0, que procesa el tráfico entre las redes lógicas y físicas. Cuando implemente el cortafuegos VM-Series con inserción de nivel 0, NSX-T Manager use la información de implementación que configuró en Panorama para conectar un cortafuegos a un enrutador lógico de nivel 0 en modo de conexión virtual.
- Inserción de nivel 1: la inserción de nivel 1 implementa un cortafuegos VM-Series en un enrutador lógico de nivel 1, que proporciona conexiones de enlace descendente a segmentos y una conexión de enlace ascendente a enrutadores lógicos de nivel 0. NSX-T Manager conecta los cortafuegos VM-Series implementados con inserciones de nivel 1 a un enrutador lógico de nivel 1 en modo de cable virtual.

Después de implementar el cortafuegos, configure las reglas de redirección de tráfico que envían el tráfico al cortafuegos VM-Series al cruzar un enrutador de nivel 0 o nivel 1. Las reglas de política de seguridad

 ©2024 Palo Alto Networks, Inc.

que configura en Panorama se envían a los cortafuegos VM-Series gestionados y luego se aplican al tráfico que pasa a través del cortafuegos.

Componentes del cortafuegos VM-Series en NSX-T (norte-sur)

Las siguientes tablas muestran los componentes de esta solución conjunta de Palo Alto Networks y VMware NSX-T.

Componentes de VMware	
vCenter/ESXi	El servidor vCenter es la herramienta de gestión centralizada de la familia vSphere. ESXi es un hipervisor que permite la virtualización de computo. Consulte la Matriz de compatibilidad de VMware para ver la compatibilidad de vCenter con su versión de NSX-T.
NSX-T Manager	Se debe instalar NSX-T Data Center 2.4.0 de VMware o posterior y registrar con el servidor vCenter. NSX-T Manager es necesario para implementar el cortafuegos VM-Series en los hosts ESXi dentro de un clúster ESXi.

Componentes de Palo Alto Networks	
PAN-OS	La imagen base de VM-Series (PA-VM-NST-9.1.zip) se usa para implementar el cortafuegos VM-Series en NSX-T. Los requisitos mínimos de sistema para implementar el cortafuegos VM-Series para NSX en el servidor ESXi dependen del modelo VM-Series. Consulte Modelos VM-Series para los requisitos mínimos de hardware para su modelo VM-Series.
Panorama Panorama debe estar ejecutando la misma versión o una versión más reciente que los cortafuegos que gestionará.	El cortafuegos VM-Series en NSX-T requiere Panorama 9.1. o posterior. Panorama es la herramienta de gestión centralizada de los cortafuegos de última generación de Palo Alto Networks. En esta solución, Panorama trabaja con NSX-T Manager para implementar, licenciar y gestionar de forma centralizada —configuración y políticas— en el cortafuegos VM-Series para NSX-T. Panorama debe poder conectarse a NSX-T Manager, los cortafuegos VM-Series y el servidor de actualizaciones de Palo Alto Networks.

 ©2024 Palo Alto Networks, Inc.

Componentes de Palo Alto Networks	
	Consulte la Guía del administrador de Panorama para obtener información sobre la implementación de su dispositivo Panorama.
Plugin Panorama para VMware NSX	3.0.0 o posterior
Plugin VM-Series	1.0.6 o posterior
Cortafuegos VM-Series	• Créditos Software NGFW: hasta 64 vCPU • Modelos: VM-100, VM-300, VM-500 y VM-700

Implementación del cortafuegos VM-Series en NSX-T (norte-sur)

Complete las siguientes tareas para asegurar el tráfico Norte-Sur en su entorno NSX-T con el cortafuegos VM-Series.



El siguiente procedimiento hace referencia a NSX-T Manager 3.0

- Instale el plugin de Panorama para VMware NSX
- Habilitación de la comunicación entre NSX-T Manager y Panorama
- Creación de plantillas y grupos de dispositivos en Panorama
- Configuración de definición de servicio en Panorama
- Implementación del cortafuegos VM-Series
- Dirija el tráfico al cortafuegos VM-Series
- Aplique la política de seguridad al cortafuegos VM-Series en NSX-T
- Utilice vMotion para mover el cortafuegos VM-Series entre hosts

Instale el plugin de Panorama para VMware NSX

Descargue e instale el plugin de Panorama para VMware NSX. Consulte la Matriz de compatibilidad antes de instalar o actualizar su complemento.

Si tiene una configuración de HA en Panorama, repita el proceso de instalación en cada peer Panorama. Al instalar el plugin en pares de HA de Panorama, instale el plugin en el equipo pasivo antes de hacerlo en el equipo activo. Después de instalar el complemento en el peer pasivo, pasará a un estado no funcional. La instalación del plugin en el peer activo devuelve el peer pasivo a un estado funcional.

Si tiene un Panorama independiente o dos dispositivos Panorama instalados en un par de alta disponibilidad con varios complementos instalados, es posible que los complementos no reciban información actualizada sobre la etiqueta IP si uno o más de los complementos no están configurados. Esto ocurre porque Panorama no reenviará la información de la etiqueta IP a los complementos no configurados. Además, este problema puede ocurrir si uno o más de los complementos de Panorama no están en el estado Registrado o Correcto (el estado positivo varía según cada complemento). Asegúrese de que sus complementos estén en el estado positivo antes de continuar o ejecutar los comandos que se describen a continuación.

 ©2024 Palo Alto Networks, Inc.

Si encuentra este problema, hay dos soluciones:

- Desinstale el complemento o complementos no configurados. Se recomienda que no instale un complemento que no planifique configurar de inmediato
- Puede utilizar los siguientes comandos para solventar este problema. Ejecute el siguiente comando para cada complemento no configurado en cada instancia de Panorama, para evitar que Panorama espere para enviar actualizaciones. Si no lo hace, sus cortafuegos pueden perder cierta información de la etiqueta IP.

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

  Puede cancelar este comando ejecutando:

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

Los comandos descritos no son persistentes en los reinicios y deben usarse de nuevo para cualquier reinicio posterior. Para Panorama en el par de HA, los comandos deben ejecutarse en cada Panorama.

STEP 1 | Seleccione **Panorama** > **Plugins (Complementos)**. Consulte la Matriz de compatibilidad antes de instalar o actualizar su complemento.

STEP 2 | Seleccione **Check Now (Comprobar ahora)** para recuperar una lista de actualizaciones disponibles.

STEP 3 | Seleccione **Download (Descargar)** en la columna Action (Acción) para descargar el plugin.

STEP 4 | Seleccione la versión del complemento y haga clic en **Install (Instalar)** en la columna Action (Acción) para instalar el complemento. Panorama le alertará cuando se complete la instalación.

Habilitación de la comunicación entre NSX-T Manager y Panorama

Complete el siguiente procedimiento para habilitar la comunicación entre Panorama y NSX-T Manager. Puede conectar su Panorama a hasta 16 NSX-T Managers. Si está conectando su Panorama a múltiples NSX-T Managers, debe planificar cuidadosamente la jerarquía de su grupo de dispositivos y las pilas de plantillas, y considerar cómo interactúan con los otros componentes necesarios para la implementación. Las definiciones de servicio hacen referencia a grupos de dispositivos y pilas de plantillas y envían esa información a los cortafuegos en los clústeres ESXi relacionados.

STEP 1 | (Opcional) Omita la configuración del servidor proxy, configurada en Panorama bajo **Panorama** > **Setup (Configuración)** > **Services (Servicios)** > **Proxy Server (Servidor proxy)**, para la comunicación entre Panorama y NSX-T Manager. Este comando permite que Panorama se comunique directamente con NSX-T Manager mientras mantiene la comunicación proxy para otros servicios.

1. Inicie sesión en la CLI de Panorama.
2. Ejecute el siguiente comando para habilitar o deshabilitar la omisión de proxy.

   ```
   admin@Panorama> request plugins vmware_nsx global proxy bypass
   {yes | no}
   ```

   Seleccione **yes (sí)** para habilitar la omisión de proxy y **no** para deshabilitar la omisión de proxy. Esto se establece en **no** de forma predeterminada.

STEP 2 | Inicie sesión en la interfaz web de Panorama.

Si usa una conexión segura (https) desde un navegador web, inicie sesión usando la dirección IP y la contraseña que asignó durante la configuración inicial (https://<*IP address*>).

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Configure el acceso al administrador NSX-T. Repita este procedimiento para cada NSX-T Manager al que conectará Panorama.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Managers (Administradores de servicios)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre descriptivo en **Name (Nombre)** para su NSX-T Manager.
3. (Opcional) Añada una **Description (Descripción)** para NSX-T Manager.
4. Introduzca la **NSX Manager URL (URL de NSX Manager)**, Dirección IP virtual del clúster del NSX-T Manager o FQDN, para acceder al NSX-T Manager.
5. Introduzca las credenciales de **NSX Manager Login (Inicio de sesión de NSX Manager)**: nombre de usuario y contraseña, de modo que Panorama pueda autenticarse en NSX-T Manager.
6. Haga clic en **OK (Aceptar)**.

Si modifica la contraseña de inicio de sesión de NSX-T Manager, asegúrese de actualizar la contraseña en Panorama inmediatamente. Una contraseña incorrecta interrumpe la conexión entre Panorama y NSX-T Manager.

STEP 4 | Compile los cambios realizados en Panorama.

Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

STEP 5 | Verifique el estado de conexión en Panorama.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Managers (Administradores de servicios)**.
2. Verifique el mensaje en la columna **Status (Estado)**.

   Cuando la conexión es correcta, el estado se muestra como **Registered (Registrado)**. Esto indica que Panorama y NSX-T Manager están sincronizados.

   Los mensajes de estados de error son:

   - **No connection (Sin conexión)**: No se ha podido alcanzar/establecer una conexión de red con NSX-T Manager.
   - **Invalid Credentials (Credenciales no válidas)**: Las credenciales de acceso (nombre de usuario y/o contraseña) son incorrectas.
   - **Out of sync (Sin sincronización)**: Los ajustes de configuración definidos en Panorama son diferentes de lo que se define en NSX-T Manager. Haga clic en el enlace para obtener más detalles en relación con las razones para el fallo. Por ejemplo, NSX-T Manager puede tener una definición de servicio con el mismo nombre que se definió en Panorama. Para reparar el error, use el nombre de definición de servicio detallado en el mensaje de error para validar la definición del servicio en NSX-T Manager. Hasta que se sincronice la configuración en Panorama y NSX Manager, no es posible añadir una nueva definición de servicio en Panorama.
   - **Connection Disabled (Conexión deshabilitada)**: La conexión entre Panorama y el NSX-T Manager se desactivó manualmente.

Creación de plantillas y grupos de dispositivos en Panorama

Para poder gestionar los cortafuegos VM-Series en NSX-T con Panorama, los cortafuegos deben pertenecer a un grupo de dispositivos y a una pila de plantillas. Los grupos de dispositivos le permiten

 ©2024 Palo Alto Networks, Inc.

reunir los cortafuegos que necesitan objetos y políticas similares como una unidad lógica; la configuración se define usando las fichas **Objects (Objetos)** y **Policies (Políticas)** en Panorama. Use pilas de plantillas para configurar los ajustes necesarios para que los cortafuegos VM-Series operen en la red; la configuración se define usando las pestañas **Device (Dispositivo)** y **Network (Red)** en Panorama. Cada pila de plantillas utilizada en su configuración NSX-T debe estar asociada con una definición de servicio.

Los cortafuegos implementados en NSX-T tienen dos zonas predeterminadas y dos interfaces configuradas en modo de cable virtual. Ethernet1/1 es parte de la zona **sur** y ethernet1/2 es parte de la zona **norte**. Para enviar las reglas de políticas de Panorama a los cortafuegos gestionados, debe configurar zonas e interfaces que coincidan con las del cortafuegos en la pila de plantillas correspondiente en Panorama.

STEP 1 | Añada un grupo de dispositivos o una jerarquía de grupos de dispositivos.

1. Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)** y haga clic en **Add (Añadir)**. También puede crear una jerarquía de grupos de dispositivos.
2. Introduzca un **Name (Nombre)** y una **Description (Descripción)** exclusivos para identificar el grupo de dispositivos.
3. Haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** y seleccione **Panorama** como **Commit type (Tipo de confirmación)** para guardar los cambios en la configuración que se esté ejecutando.

STEP 2 | Añada una plantilla.

1. Seleccione **Panorama** > **Templates (Plantillas)** y haga clic en **Add (Añadir)**.
2. Introduzca **Name (Nombre)** y **Description (Descripción)** para identificar la plantilla.
3. Haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** y seleccione **Panorama** como **Commit Type (Tipo de confirmación)** para guardar los cambios en la configuración que se esté ejecutando.

STEP 3 | Cree una pila de plantillas.

1. Seleccione **Panorama** > **Templates (Plantillas)** y haga clic en **Add Stack (Añadir pila)**.
2. Introduzca **Name (Nombre)** y **Description (Descripción)** para identificar la plantilla.
3. Haga clic en **Añadir** para añadir la plantilla que creó anteriormente.
4. Haga clic en **OK (Aceptar)**.
5. Haga clic en **Commit (Confirmar)** y seleccione **Commit to Panorama (Confirmar en Panorama)** para guardar los cambios en la configuración que se esté ejecutando en Panorama.

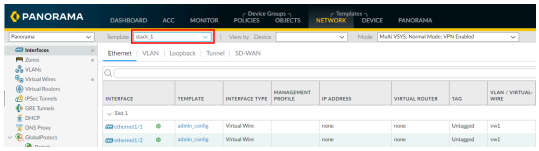
 ©2024 Palo Alto Networks, Inc.

STEP 4 | Configure el cable virtual, las interfaces y las zonas . Asegúrese de seleccionar la plantilla correcta del menú desplegable que se muestra a continuación. Los objetos que cree deben cumplir los siguientes criterios:

Si cambia el cable virtual predeterminado o los nombres de zona, el cable virtual y las zonas en Panorama deben coincidir con los nombres utilizados en el cortafuegos.

- Utilice **ethernet1/1** y **ethernet1/2**.
- El objeto del cable virtual llamado **vw1**.
- La primera zona llamada **sur**, tipo **virtual-wire** y contiene **ethernet1/1**.
- La segunda zona llamada **norte**, tipo **virtual-wire**, y contiene **ethernet1/2** .

Repita este proceso para cada plantilla en su implementación.



STEP 5 | Haga clic en **Commit (Confirmar)** y seleccione **Panorama** como **Commit Type (Tipo de confirmación)** para guardar los cambios en la configuración que se esté ejecutando.

STEP 6 | Actualice la información del servidor DNS y NTP de la pila de plantillas. Debe completar este paso si usa certificados de dispositivos en la implementación. Esto es necesario para garantizar que los cortafuegos implementados en el entorno de NSX-T tengan la información DNS correcta necesaria para llegar al servidor de certificados del dispositivo.

1. Compruebe que ha especificado la pila de plantillas correcta en el menú desplegable **Template (Plantilla)**.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y haga clic en el icono **Edit (Editar)**.
3. En la pestaña Servicios, introduzca la dirección IP de su **Primary DNS Server (Servidor DNS principal)** y de su **Secondary DNS Server (Servidor DNS secundario)**.
4. En la pestaña NTP, escriba la dirección IP del **NTP Server (Servidor NTP)**.
5. Haga clic en **OK (Aceptar)**.
6. **Commit (Confirmar)** los cambios realizados en Panorama.

Configuración de definición de servicio en Panorama

Una definición de servicio especifica la configuración para los cortafuegos VM-Series instalados en su entorno de centro de datos NSX-T. La definición del servicio debe incluir el grupo de dispositivos, una pila de plantillas y una URL de OVF.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Añada una nueva definición de servicio.

Puede crear hasta 32 definiciones de servicio en Panorama.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Definitions (Definiciones de servicio)**.
2. Seleccione **Add (Añadir)** para crear una nueva definición de servicio.
3. Introduzca un nombre descriptivo en **Name (Nombre)** para su definición de servicio.
4. (Opcional Añada una **Description (Descripción)** que identifique la función o finalidad de los cortafuegos VM-Series que se implementarán usando esta definición de servicio.

STEP 2 | Asigne un grupo de dispositivos y una pila de plantillas a la definición de servicio.

Asegúrese de Creación de plantillas y grupos de dispositivos en Panorama.

Como los cortafuegos implementados en esta solución se administran centralmente desde Panorama, debe especificar el **Device Group (Grupo de dispositivos)** y la **Template Stack (Pila de plantillas)** a los que pertenecen los cortafuegos. Todos los cortafuegos que se implementan usando esta definición de servicio pertenecen a la pila de plantillas y el grupo de dispositivos especificados.

1. Seleccione el grupo de dispositivos o jerarquía de grupo de dispositivos en la lista desplegable **Device Group (Grupo de dispositivos)**.
2. Seleccione la pila de plantillas en la lista desplegable **Template (Plantilla)**.

No se puede reutilizar una pila de plantillas o grupo de dispositivos asignados a una definición de servicio en otra definición de servicio.

STEP 3 | Especifique la ubicación del archivo OVF.

Descargue el archivo zip, descomprímalo para extraer y guardar los archivos .ovf, mf y .vmdk en el mismo directorio. Los archivos ovf y vmdk se usan para implementar cada instancia del cortafuego.

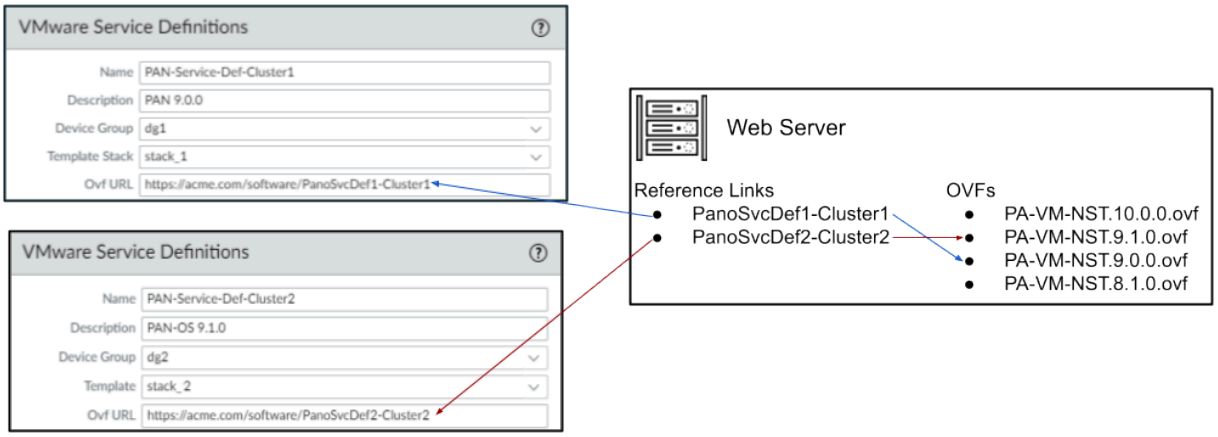
En caso necesario, modifique la configuración de seguridad para poder descargar los tipos de archivo. Por ejemplo, en el servidor IIS modifique la configuración Mime Types; en un servidor Apache, modifique el archivo .htaccess.

No cambie la ruta de acceso OVF de la definición de servicio de Panorama después de una implementación correcta de servicio NSX de cortafuegos de VM-Series. Cambiar la ruta de OVF, después de una implementación correcta del cortafuegos VM-Series, puede provocar un error en el estado de la implementación del servicio NSX. Puede resolver este error en NSX-T Manager, sin embargo, esto puede hacer que todos los cortafuegos VM-Series se vuelvan a implementar.

Se recomienda utilizar un nombre de ruta de acceso OVF con capacidad de ampliación que le permita cambiar la imagen base sin afectar a los cortafuegos implementados. En lugar de una ruta como **https://acme.com/software/PA-VM-NST.9.1.0.ovf,**, use algo como **https://acme.com/software/PanoSvcDef1-Cluster1.ovf.** El uso de una referencia de ruta estática eliminará cualquier necesidad futura de cambiar la ruta OVF. Se recomienda crear una ruta de acceso para cada definición de servicio

 ©2024 Palo Alto Networks, Inc.

de Panorama (clúster de vSphere) en la implementación y cambiar las referencias de imágenes base de PAN-OS en el servidor web según corresponda.



En **OVF URL (URL de OVF)**, añada la ubicación del servidor web que aloja el archivo ovf. Tanto http como https son protocolos admitidos.

Panorama debe tener conexión a la red con el servidor web para recuperar el archivo OVF.

Puede usar la misma versión de ovf o diferentes versiones en las definiciones de servicio. El uso de diferentes versiones de ovf en las definiciones de servicio le permite variar la versión de PAN-OS en los cortafuegos VM-Series en diferentes clústeres ESXi.

STEP 4 | Seleccione **Norte Sur** como el **Tipo de inserción** para su cortafuegos.

STEP 5 | Para recuperar automáticamente un certificado de dispositivo cuando NSX Manager implementa el cortafuegos Series-VM, configure el certificado del dispositivo.

Habilite esta opción para aplicar un certificado de dispositivo a los cortafuegos VM-Series recién implementados. Utilice esta opción únicamente cuando implemente el cortafuegos con un OVF de imagen base compatible con certificados de dispositivo. Panorama envía la información del certificado del dispositivo a NSX Manager como parte de la definición del servicio. Cuando se implementa

 ©2024 Palo Alto Networks, Inc.

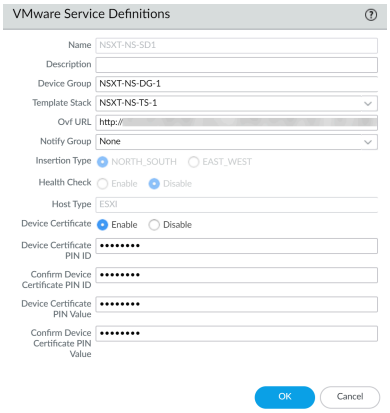
un nuevo cortafuegos en NSX, el certificado del dispositivo se instala en el cortafuegos durante el arranque.

Para obtener una lista de OVF que admiten certificados de dispositivo para el cortafuegos VM-Series en VMware NSX, consulte la Matriz de compatibilidad de Palo Alto Networks.

Si su OVF admite un certificado de dispositivo, debe Habilitar certificados de dispositivo independientemente de si está utilizando o no un certificado de dispositivo. Si su OVF no admite un certificado de dispositivo, desactive esta opción.

1. Si aún no lo ha hecho, inicie sesión en el Portal de atención al cliente y genere un PIN de registro y un ID de PIN.
2. En **Device Certificate (Certificado de dispositivo)**, haga clic en **Enable (Habilitar)**.
3. Copie el ID de PIN e introdúzcalo en el campo **Device Certificate PIN ID (ID de PIN de certificado de dispositivo)**.
4. Vuelva a introducir el ID de PIN en el campo **Confirm Device Certificate PIN ID (Confirmar ID de PIN del certificado de dispositivo)**.
5. Copie el valor de PIN e introdúzcalo en el campo **Device Certificate PIN Value (Valor de PIN del certificado de dispositivo)**.
6. Vuelva a introducir el valor del PIN en el campo **Confirm Device Certificate PIN Value (Confirmar el valor del PIN del certificado de dispositivo)**.

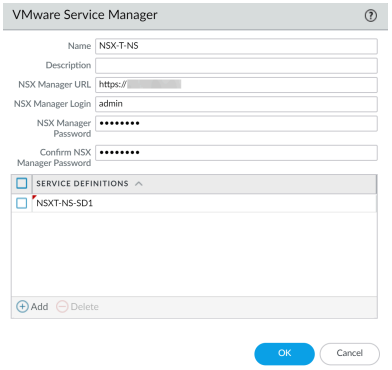
STEP 6 | Haga clic en **OK (Aceptar)** para guardar la definición de servicio.



 ©2024 Palo Alto Networks, Inc.

STEP 7 | Adjunte la definición del servicio al gestor del servicio.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Manager (Administrador de Servicio)** y haga clic en el enlace del nombre del administrador del servicio.
2. En Definiciones del servicio, haga clic en **Add (Añadir)** y seleccione su definición de servicio del menú desplegable.
3. Haga clic en **OK (Aceptar)**.

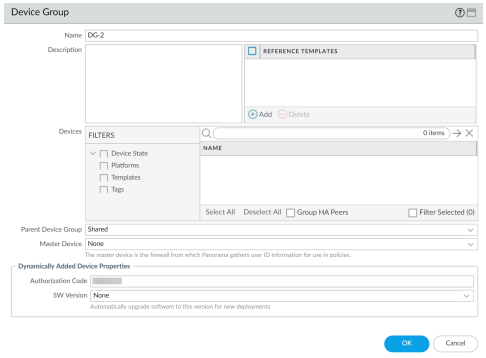


STEP 8 | Añada el código de autorización para activar la licencias de los cortafuegos.

1. Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)** y elija el grupo de dispositivos al que se asoció con la definición del servicio que acaba de crear.
2. En **Propiedades de dispositivo añadidas dinámicamente**, añada el código de autorización que recibió con el correo electrónico de cumplimiento de su pedido y, opcionalmente, seleccione Ninguno en el menú desplegable **Versión de SW**.

   Cuando se implementa un nuevo cortafuegos en NSX-T, este se añade automáticamente al grupo de dispositivos, se proporciona una licencia con el código de autorización que proporcionó y se actualiza a la versión de PAN-OS que especificó.

   En el portal de asistencia técnica, puede visualizar el número total de cortafuegos que está autorizado a implementar y la proporción del número de licencias que se han usado del número total de licencias que le ofrece su código de autorización.



STEP 9 | **Commit to Panorama (Confirmar en Panorama)**.

STEP 10 | En NSX-T Manager, verifique que la definición de servicio esté disponible.

Seleccione **System (Sistema)** > **Service Deployments (Implementaciones de servicios)** > **Catalog (Catálogo)**. La definición de servicio aparece como instancia de servicio en NSX-T Manager.

 ©2024 Palo Alto Networks, Inc.

Implementación del cortafuegos VM-Series

Después de completar la configuración en Panorama, realice el siguiente procedimiento para iniciar el cortafuegos VM-Series en su Centro de datos NSX-T.

Al implementar el cortafuegos VM-Series en NSX-T en alta disponibilidad, ambos cortafuegos se implementan en el mismo Grupo de dispositivos y Pila de plantillas.

STEP 1 | Inicie sesión en NSX-T Manager.

STEP 2 | Seleccione **System (Sistema)** > **Service Deployments (Implementaciones de servicios)** > **Deployment (Implementación)**.

STEP 3 | Seleccione su definición de servicio del menú desplegable **Partner Service (Servicio de socios)**.

STEP 4 | Haga clic en **Deploy Service (Implementar servicio)**.

STEP 5 | Introduzca un **Service Deployment Name (Nombre de implementación del servicio)** descriptivo para su cortafuegos VM-Series.

STEP 6 | Seleccione un enrutador de nivel 0 o nivel 1 en **Attachment Points (Puntos de conexión)**. NSX-T Manager conecta el cortafuegos VM-Series al enrutador seleccionado y redirecciona el tráfico que pasa a través de ese enrutador al cortafuegos VM-Series para su inspección. Debe seleccionar un enrutador sin inserción de servicios adjunto.

STEP 7 | Seleccione un **Compute Manager (Gestor de Computo)**. El gestor de cálculo es el servidor vCenter que gestiona su centro de datos.

STEP 8 | Seleccione un **Cluster (Clúster)**. Puede implementar el cortafuegos VM-Series en cualquier clúster que no incluya ningún nodo de transporte Edge.

STEP 9 | Seleccione un **Datastore (Almacén de datos)**.

STEP 10 | Configure su configuración de red.

1. Haga clic en **Edit Details (Editar detalles)** en la columna **Networks (Redes)**.
2. Seleccione la **Primary Interface Network (Red de interfaz principal)**.
3. Introduzca la **Primary Interface IP (IP de interfaz principal)**.
4. Introduzca la **Primary Gateway Address (Dirección de puerta de enlace principal)**.
5. Introduzca la **Primary Subnet Mask (Máscara de subred principal)**.
6. Haga clic en **Save (Guardar)**.

STEP 11 | NSX-T Manager rellena previamente la **Deployment Specification (Especificación de implementación)** y la **Deployment Template (Plantilla de implementación)** según el Servicio de socios que ha seleccionado.

STEP 12 | Seleccione la **Failure Policy (Política de fallos)** para Permitir o Bloquear. La política de fallos define cómo NSX-T Manager gestiona el tráfico que se dirige al cortafuegos VM-Series si el cortafuegos deja de estar disponible.

STEP 13 | Seleccione el **Deployment Mode (Modo de implementación)** para su cortafuegos VM-Series: independiente o de alta disponibilidad. Si tiene un clúster de nodos perimetrales y selecciona Alta

 ©2024 Palo Alto Networks, Inc.

disponibilidad, NSX-T Manager implementará un cortafuegos VM-Series adicional en el nodo perimetral en espera además del cortafuegos implementado en el nodo perimetral activo.

STEP 14 | Haga clic en **Save (Guardar)**para implementar el cortafuegos VM-Series.

STEP 15 | Compruebe que sus cortafuegos están conectados a Panorama.

1. Inicie sesión en Panorama.
2. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**.
3. Confirme que sus cortafuegos figuran en el grupo de dispositivos correcto y que el **Device State (Estado del dispositivo)** muestra **Connected (Conectado)**.

   El nombre del dispositivo para el cortafuegos VM-Series se muestra en Panorama como **PA-VM:** <nsx.clusterid>para la implementación de NSX-T (N-S) y como **PA-VM:** <nsx.servicevmid>para la implementación de NSX-T (E-W).

STEP 16 | Establezca una contraseña segura para la cuenta de administrador en sus cortafuegos VM-Series.

Cada cortafuegos VM-Series utiliza un nombre de usuario y una contraseña predeterminados (admin/admin), que se utilizan para el inicio de sesión inicial. Al iniciar sesión por primera vez, se le solicitará que establezca una contraseña nueva y más segura. La nueva contraseña debe tener un mínimo de ocho caracteres e incluir un mínimo de un carácter en minúsculas y otro en mayúsculas, así como un número y un carácter especial.

Puede actualizar la contraseña en cada cortafuegos de forma individual o todos a la vez a través de Panorama.

- **Panorama**: en Panorama, puede cambiar la contraseña predeterminada para todos los cortafuegos en una plantilla o eliminar el usuario administrador y crear un nuevo nombre de usuario y contraseña.
  1. Iniciar sesión en Panorama
  2. Seleccione **Device (Dispositivo)** > **Administrators (Administradores)** y seleccione el usuario **admin**.
  3. **Delete (Eliminar)** el usuario o haga clic en el usuario e introduzca una nueva contraseña.
  4. Si cambió la contraseña, haga clic en **OK (Aceptar)**.
  5. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** > **Edit Selections (Editar selecciones)** > **Force Template Values (Forzar valores de plantilla)**.
  6. Haga clic en **OK (Aceptar)**.
- **Cortafuegos**: este procedimiento debe repetirse en cada cortafuegos VM-Series.
  1. Inicie sesión en el cortafuegos VM-series utilizando el nombre de usuario y la contraseña predeterminados.
  2. Siga las indicaciones para restablecer la contraseña.

Dirija el tráfico al cortafuegos VM-Series

Complete el siguiente procedimiento para dirigir el tráfico a su cortafuegos VM-Series. Para el tráfico Norte-Sur, las reglas de redireccionamiento no tienen estado de forma predeterminada y no se pueden cambiar. Además, NSX-T crea automáticamente una regla reflexiva correspondiente para el tráfico de retorno.

 ©2024 Palo Alto Networks, Inc.

Cuando implementa el cortafuegos VM-Series para NSX-T norte-sur en modo HA, debe crear una regla de redireccionamiento de tráfico para ambos pares HA. Además, debe crear la regla de redireccionamiento para el par activo primero y el par pasivo en segundo lugar.

La regla reflexiva no aparece en la interfaz web de NSX-T.

STEP 1 | Inicie sesión en NSX-T Manager.

STEP 2 | Compruebe que esté en el modo **Policy (Política)**.

STEP 3 | Seleccione **Security (Seguridad)** > **North South Security (Seguridad Norte Sur)** > **Network Introspection (N-S) [Introspección de red (N-S)]**.

STEP 4 | Haga clic en **Add Policy (Añadir política)**.

STEP 5 | Introduzca un **Nombre**descriptivo para su política.

STEP 6 | Seleccione una instancia de servicio de cortafuegos VM-Series en el menú desplegable **Redirect To (Redirigir a)**. NSX-T Manager rellenará automáticamente el campo **Applied to (Aplicado a)** según la instancia de servicio que seleccione.

STEP 7 | Seleccione su política recién creada.

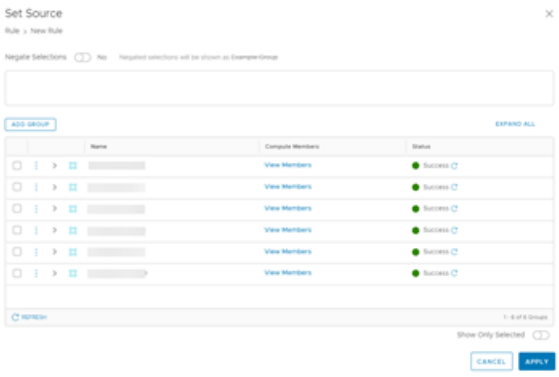
STEP 8 | Haga clic en **Add Rule (Añadir regla)**.

Si su entorno NSX-T tiene nodos perimetrales en HA activa en espera, debe crear una regla de redireccionamiento para cada nodo perimetral. NSX-T no aplica automáticamente una regla de redireccionamiento al nodo en espera en caso de una conmutación por error.

STEP 9 | Haga clic en **Name (Nombre)** e introduzca un nombre descriptivo para la regla.

STEP 10 | De forma predeterminada, la fuente se establece en Cualquiera. Complete los siguientes pasos para especificar una fuente diferente.

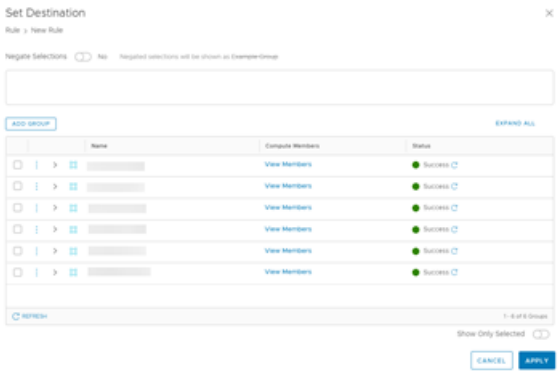
1. Haga clic en el botón editar en la columna **Source (Origen)**.
2. Seleccione el grupo o grupos que desee establecer como Origen o haga clic en Añadir grupo para crear un grupo nuevo.
3. Haga clic en **Apply (Aplicar)**.



 ©2024 Palo Alto Networks, Inc.

STEP 11 | De forma predeterminada, el destino se establece en Cualquiera. Complete los siguientes pasos para especificar un destino diferente.

1. Haga clic en el botón editar en la columna **Destination (Destino)**.
2. Seleccione el grupo o grupos para establecer como Destino o haga clic en Añadir grupo para crear un grupo nuevo.
3. Haga clic en **Apply (Aplicar)**.



STEP 12 | De forma predeterminada, cualquier servicio se redirecciona al cortafuegos. Complete los siguientes pasos para especificar ciertos servicios y protocolos.

1. Haga clic en el botón editar en la columna **Services (Servicios)**.
2. Seleccione el grupo o grupos para establecer como el Servicio o haga clic en Añadir servicio para crear un nuevo servicio.
3. Haga clic en **Apply (Aplicar)**.

STEP 13 | Seleccione **Redirect (Redireccionar)** de la lista desplegable **Action (Acción)** para enviar tráfico a su cortafuegos VM-Series.

STEP 14 | Seleccione **Enable (Habilitar)** para habilitar la regla. NSX-T Manager publica la regla de redireccionamiento que acaba de crear y crea automáticamente una regla reflexiva para el tráfico de retorno. La regla reflexiva no aparece en la interfaz web de NSX-T Manager.



STEP 15 | Si sus cortafuegos VM-Series se implementan en HA, cree otra regla para el par de HA pasivo.

Si el tráfico de retorno no se dirige al cortafuegos VM-Series, configure manualmente una regla de redireccionamiento de tráfico para el tráfico de retorno.

Aplique la política de seguridad al cortafuegos VM-Series en NSX-T

Ahora que ha implementado el cortafuegos VM-Series y ha creado reglas de redireccionamiento de tráfico para enviar tráfico al cortafuegos, puede usar Panorama para gestionar de manera centralizada las reglas de la política de seguridad en el cortafuegos VM-Series.

STEP 1 | Inicie sesión en Panorama.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Cree las reglas de política de seguridad.

De manera predeterminada, el cortafuegos crea una regla que permite la detección de reenvío bidireccional (BFD). No cree una regla que bloquee BFD. Si BFD se bloquea, NSX-T piensa que el cortafuegos no está disponible.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Prerules (Pre reglas)**.
2. Seleccione el **Grupo de dispositivos** que creó para gestionar los cortafuegos VM-Series en NSX-T en Creación de plantillas y grupos de dispositivos en Panorama.
3. Haga clic en **Add (Añadir)** e introduzca **Name (Nombre)** y **Description (Descripción)** para la regla. En este ejemplo la regla de seguridad permite todo el tráfico entre los servidores WebFrontEnd y de aplicaciones.
4. Seleccione la **Source Zone (Zona de origen)** y **Destination Zone (Zona de destino)**.
5. Para la **Source Address (Dirección de origen)** y **Destination Address (Dirección de destino)**, seleccione o escriba una dirección, grupo de dirección estática o región.

   El cortafuegos VM-Series en NSX-T no admite grupos de direcciones dinámicas para el tráfico norte-sur.
6. Seleccione la **Application (Aplicación)** que desea permitir. En este ejemplo hemos creado un **Application Group (Grupo de aplicaciones)** que incluye un grupo estático de aplicaciones específicas que se agrupan juntas.
   1. Haga clic en **Add (Añadir)** y seleccione **New Application Group (Nuevo grupo de aplicaciones)**.
   2. Haga clic en **Add (Añadir)** para seleccionar la aplicación que desea añadir al grupo.
   3. Haga clic en **OK (Aceptar)** para crear el grupo de aplicaciones.
7. Especifique la acción, **Allow (Permitir)** o **Deny (Denegar)**, para el tráfico y, opcionalmente, adjunte los perfiles de seguridad predeterminados para los antivirus, anti-spyware y protección contra vulnerabilidades en Profiles (Perfiles).
8. Haga clic en **Confirmar**, seleccione **Confirmar en Panorama**. Haga clic en **OK (Aceptar)**.

STEP 3 | Aplique las políticas a los cortafuegos VM-Series en NSX-T.

1. Haga clic en **Confirmar** > **Enviar a dispositivos** > **Editar selecciones**.
2. Seleccione el grupo de dispositivos y haga clic en **Aceptar**.
3. Seleccione **Forzar valores de plantilla**. De manera predeterminada, Panorama no anula los objetos en el cortafuegos con objetos en Panorama que comparten un nombre. Debe seleccionar Forzar valores de plantilla para enviar políticas a los cortafuegos gestionados.
4. Haga clic en **Yes (Sí)** para confirmar forzar valores de plantilla.
5. Haga clic en **OK (Aceptar)**.
6. Verifique que la confirmación se realice correctamente.

STEP 4 | (Opcional) Use la plantilla para enviar una configuración base para la configuración de red y dispositivo como, por ejemplo servidor DNS, servidor NTP, servidor Syslog y pancarta de inicio de sesión.

Si desea más información sobre el uso de plantillas, consulte la Guía del administrador de Panorama.

 ©2024 Palo Alto Networks, Inc.

Utilice vMotion para mover el cortafuegos VM-Series entre hosts

Para mantener el flujo de tráfico mientras utiliza vMotion para mover su cortafuegos VM-Series entre hosts ESXi con configuraciones de CPU homogéneas en VMware NSX-T, debe usar la CLI de PAN-OS para pausar la supervisión del heartbeat interno del cortafuegos VM-Series durante vMotion. Puede especificar el periodo de tiempo, en minutos, que se pausa la supervisión de heartbeats. La supervisión de heartbeats se puede pausar hasta por 60 minutos. Cuando el intervalo de pausa caduca o usted finaliza deliberadamente el intervalo de pausa, se reanuda la supervisión de heartbeats.

La tecnología vMotion del cortafuegos VM-Series es compatible en vSphere 6.5, 6.7 y 7.0 si los hosts ESXi tienen una configuración de CPU homogénea.

Este procedimiento no es necesario cuando se usa vMotion para mover el cortafuegos VM-Series si está ejecutando vSphere 7.0 o posterior.

STEP 1 | Inicie sesión en la CLI del cortafuegos VM-Series.

STEP 2 | Establezca el intervalo de pausa de supervisión de heartbeat mediante el siguiente comando. La pausa comienza tan pronto como se ejecuta el comando. Si vMotion tarda más de lo esperado, puede volver a ejecutar este comando para establecer un nuevo intervalo más largo que se inicie cuando el comando se vuelva a ejecutar.

```
request system heartbeat-pause set interval <pause-time-in-minutes>
```

Puede ver el tiempo restante en el intervalo de pausa usando el siguiente comando.

```
request system heartbeat-pause show interval
```

STEP 3 | (Opcional) Si completa vMotion antes de que haya transcurrido el intervalo de pausa, puede finalizar la pausa estableciendo el intervalo en cero (0).

```
request system heartbeat-pause set interval 0
```

Amplíe la política de seguridad de NSX-V a NSX-T

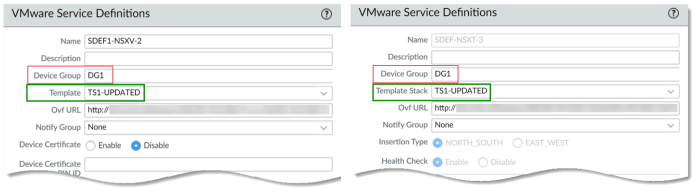
Si va a pasar de una implementación de NSX-V a una implementación de NSX-T o combina una implementación de NSX-T con una de NSX-V, puede extender su política de seguridad existente de NSX-V a NSX-T sin tener que volver a crear la reglas de política. Esto se logra aprovechando sus grupos de dispositivos existentes y compartiéndolos entre las definiciones de servicio NSX-V y NSX-T. Después de migrar su política a NSX-T, puede continuar usando VM-Series para NSX-V o eliminar su implementación de NSX-V.

STEP 1 | Instale el plugin de Panorama para VMware NSX 3.2.0 o posterior. Consulte Notas de la versión del complemento de Panorama para VMware NSX 3.2.0 antes de actualizar.

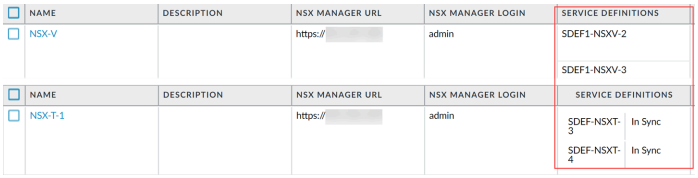
STEP 2 | Configure una definición de servicio NSX-T para cada definición de servicio NSX-V en su implementación. No cree nuevos grupos de dispositivos; en su lugar, utilice sus grupos de dispositivos NSX-V existentes. El uso de los grupos de dispositivos existentes le permite aplicar las mismas reglas de políticas de seguridad que se usan en NSX-V a los cortafuegos VM-Series implementados en NSX-T. Si tiene una política que hace referencia a una zona en particular, añada la misma pila de plantillas de su definición de servicio NSX-V a su definición de servicio NSX-T. Además, si su grupo de dispositivos hace referencia a una plantilla en particular, asegúrese de

 ©2024 Palo Alto Networks, Inc.

seleccionar la pila de plantillas que incluye la plantilla a la que se hace referencia en el grupo de dispositivos.



STEP 3 | Configure un administrador de servicios de NSX-T y asocie las definiciones de servicio de NSX-T al administrador de servicios.



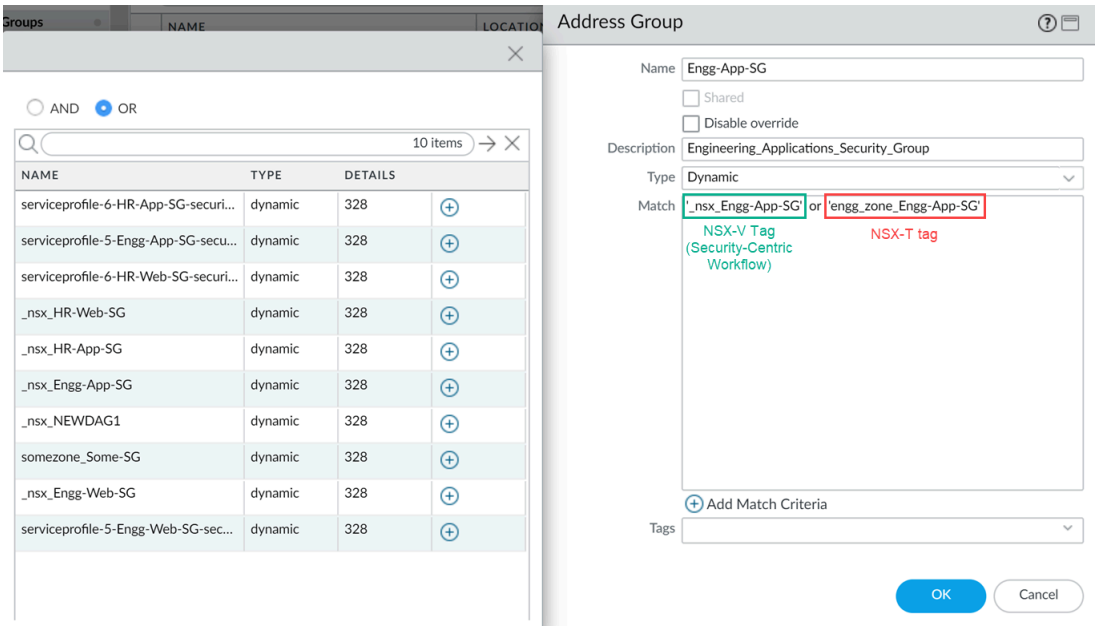
STEP 4 | Prepare su entorno NSX-T e implemente el cortafuegos VM-Series. Debe crear sus grupos de seguridad, cadenas de servicios y política de redireccionamiento del tráfico antes de iniciar el cortafuegos VM-Series.

- Implementación del cortafuegos VM-Series en NSX-T (norte-sur)
- Implementación de VM-Series mediante el flujo de trabajo basado en las operaciones

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Añada las etiquetas NSX-T a sus grupos de direcciones dinámicas existentes.

1. Seleccione **Panorama** > **Objects (Objetos)** > **Address Groups (Grupos de direcciones)**.
2. Haga clic en el nombre de un grupo de direcciones dinámicas de NSX-V existente.
3. Haga clic en **Add Match Criteria (Añadir criterios de coincidencia)** para mostrar las etiquetas de NSX-V y NSX-T.
4. Añada la etiqueta NSX-T a los grupos de direcciones dinámicas. Asegúrese de utilizar el operador **OR** entre las etiquetas.
5. Cuando haya añadido todas las etiquetas necesarias, haga clic en **OK (Aceptar)**.
6. Haga clic en **Commit (Confirmar)** para compilar los cambios.



STEP 6 | Una vez que las cargas de trabajo de su máquina virtual se hayan migrado correctamente de NSX-V a NSX-T, elimine las etiquetas NSX-V de sus grupos de direcciones dinámicas si planifica dejar de usar NSX-V. Todas las etiquetas NSX-V y las direcciones IP correspondientes se anulan del registro después de que toda la configuración relacionada con NSX-V se elimina del complemento Panorama para NSX y la configuración del cortafuegos VM-Series se elimina del NSX-V Manager.

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en NSX-T (este-oeste)

El cortafuegos VM-Series en VMware NSX-T integra los cortafuegos de Palo Alto de nueva generación y Panorama con los servidores host ESXi para proporcionar visibilidad completa y una habilitación segura de las aplicaciones de todo el tráfico Este-Oeste en su centro de datos definido por software de NSX-T.

- Componentes del cortafuegos VM-Series en NSX-T (este-oeste)
- Integración del cortafuegos VM-Series en NSX-T (este-oeste)
- Implementaciones compatibles del cortafuegos VM-Series en VMware NSX-T (este-oeste)
- Implementación de VM-Series mediante el flujo de trabajo basado en las operaciones
- Implementación de VM-Series mediante el flujo de trabajo basado en la seguridad
- Eliminar una definición de servicio de Panorama
- Migración de VM-Series en operación NSX-T a implementación basada en seguridad
- Amplíe la política de seguridad de NSX-V a NSX-T
- Utilice la migración in situ para trasladar su VM-Series de NSX-V a NSX-T

Componentes del cortafuegos VM-Series en NSX-T (este-oeste)

Las siguientes tablas muestran los componentes de esta solución conjunta de Palo Alto Networks y VMware NSX-T (este-oeste).

Componentes de VMware	
vCenter/ESXi	El servidor vCenter es la herramienta de gestión centralizada de la familia vSphere. ESXi es un hipervisor que permite la virtualización de computo. Consulte la Matriz de compatibilidad de VMware para ver la compatibilidad de vCenter con su versión de NSX-T.
NSX-T Manager	Se debe instalar NSX-T Data Center 2.5.0 de VMware o posterior y registrar con el servidor vCenter. NSX-T Manager es necesario para implementar el cortafuegos VM-Series en los hosts ESXi dentro de un clúster ESXi.

Componentes de Palo Alto Networks	
PAN-OS	PAN-OS 10.1.x y posterior.

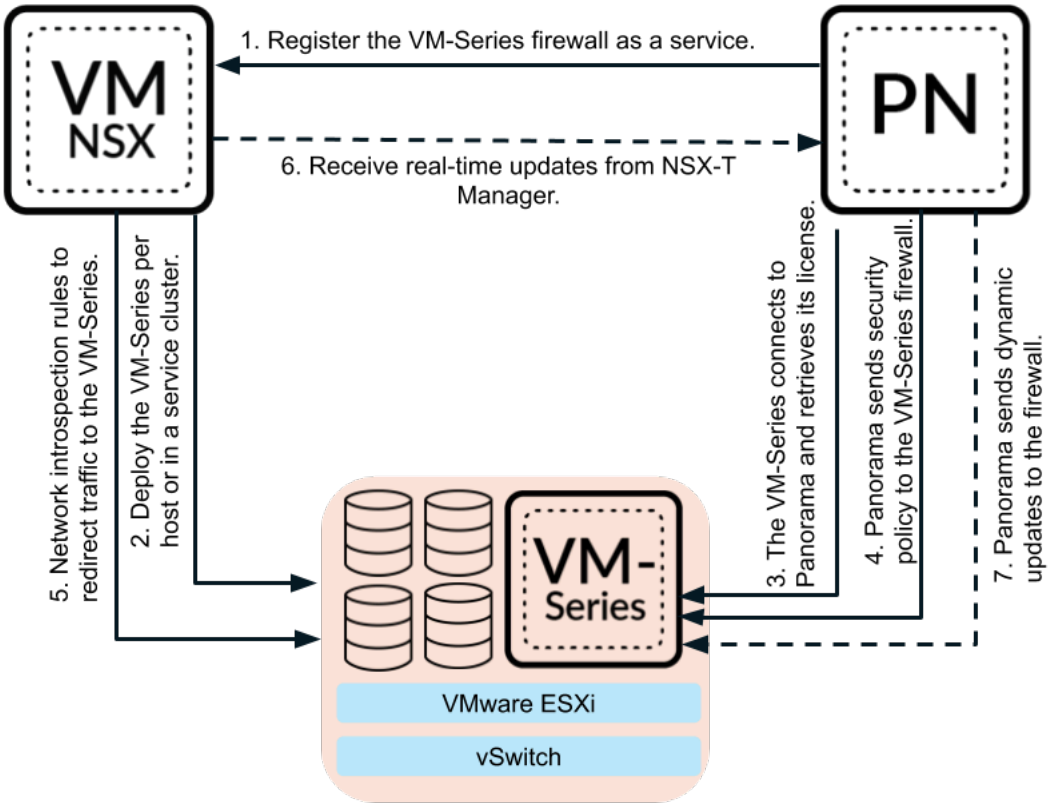
 ©2024 Palo Alto Networks, Inc.

Componentes de Palo Alto Networks	
	La imagen base de la VM-Series, por ejemplo, PA-VM-NST-10.1.0zip, es necesaria para implementar el cortafuegos VM-Series en NSX-T. Los requisitos mínimos de sistema para implementar el cortafuegos VM-Series para NSX en el servidor ESXi dependen del modelo VM-Series. Consulte Modelos VM-Series para los requisitos mínimos de hardware para su modelo VM-Series.
Panorama Panorama debe estar ejecutando la misma versión o una versión más reciente que los cortafuegos que gestionará.	El cortafuegos VM-Series en NSX-T requiere Panorama 10.1.0 y posterior para los cortafuegos que ejecutan 10.1.0 Panorama es la herramienta de gestión centralizada de los cortafuegos de última generación de Palo Alto Networks. En esta solución, Panorama trabaja con NSX-T Manager para implementar, licenciar y gestionar de forma centralizada —configuración y políticas— en el cortafuegos VM-Series para NSX-T. Panorama debe poder conectarse a NSX-T Manager, los cortafuegos VM-Series y el servidor de actualizaciones de Palo Alto Networks. Consulte la Guía del administrador de Panorama 11.1 para obtener información sobre la implementación de su dispositivo Panorama.
Plugin Panorama para VMware NSX	3.1.0 o posterior 4.0.0 o posterior para el flujo de trabajo basado en la seguridad
Plugin VM-Series	1.0.8 o posterior
Modelos de cortafuegos VM-Series	VM-100, VM-300, VM-500 y VM-700 son compatibles con NSX-T. *Antes de implementar el cortafuegos VM-Series en NSX-T, asegúrese de tener suficientes recursos de hardware ser compatible con el número de cortafuegos VM-Series en el modelo de implementación elegido (clúster de servicio o por host). Esto es crítico cuando se implementan cortafuegos grandes como el VM-700.*

 ©2024 Palo Alto Networks, Inc.

Integración del cortafuegos VM-Series en NSX-T (este-oeste)

NSX-T Manager, vCenter, Panorama y el cortafuegos VM-Series trabajan juntos para hacer frente a los desafíos de seguridad de su centro de datos NSX-T.



1. **Registre el cortafuegos VM-Series como un servicio**: utilice Panorama para conectarse a su NSX-T Manager de VMware. Panorama se comunica con NSX-T Manager utilizando la API NSX-T y establece una comunicación bidireccional. En Panorama, el Administrador de servicios se configura introduciendo la dirección IP, el nombre de usuario y la contraseña de NSX-T Manager para iniciar la comunicación.

   Después de establecer la comunicación con NSX-T Manager, configure la definición del servicio. La definición del servicio incluye la ubicación de la imagen base del cortafuegos VM-Series, el código de autorización necesario para dar licencia al cortafuegos VM-Series y los grupos de dispositivos y la pila de plantillas a los que pertenecerá el cortafuegos.

   Además, NSX-T Manager utiliza esta conexión para enviar actualizaciones sobre los cambios en el entorno NSX-T con Panorama.
2. **Implemente el cortafuegos VM-Series por host o en un clúster de servicios**: NSX-T Manager utiliza la información que se envía desde Panorama en la definición del servicio para implementar el cortafuegos VM-Series. Seleccione dónde se implementará el cortafuegos Vm-Series (en un clúster de servicios o en cada host ESXi) y cómo NSX-T proporciona una dirección IP de gestión al cortafuegos

 ©2024 Palo Alto Networks, Inc.

VM-Series (DHCP o IP estática). Cuando se inicia el cortafuegos, la API de NSX-T Manager conecta el cortafuegos VM-Series al hipervisor para que pueda recibir tráfico del vSwitch.

3. **El VM-Series se conecta a Panorama** : el cortafuegos VM-Series se conecta a Panorama para obtener su licencia. Panorama obtiene la licencia del servidor de actualizaciones de Palo Alto Networks y la envía al cortafuegos. Cuando el cortafuegos obtiene su licencia, se reinicia y vuelve a aparecer con un número de serie.

   Si Panorama no tiene acceso a Internet, no puede recuperar las licencias y enviarlas al cortafuegos, por lo que debe obtener una licencia manual para cada cortafuegos de forma individual. Si el cortafuegos VM-Series no tiene acceso a Internet, debe añadir manualmente los números de serie a Panorama para registrarlos como dispositivos gestionados, de modo que Panorama pueda enviar pilas de plantillas, grupos de dispositivos y otra información de configuración. Para obtener más información, consulte Activación de la licencia para el cortafuegos VM-Series para VMware NSX.

4. **Panorama envía una política de seguridad al cortafuegos VM-Series**: cuando el cortafuegos se vuelve a conectar a Panorama, este se añade al grupo de dispositivos y a la pila de plantillas definidas en la definición del servicio y Panorama aplica la política de seguridad adecuada a ese cortafuegos. El cortafuegos ahora está listo para proteger el tráfico en su centro de datos NSX-T.
5. **Crear reglas de introspección de red para redirigir el tráfico al cortafuegos VM-Series**: en el NSX-T Manager, cree una cadena de servicio y reglas de introspección de red que redirijan el tráfico en su centro de datos NSX-T.
6. **Enviar actualizaciones en tiempo real desde NSX-T Manager**: El NSX-T Manager envía actualizaciones en tiempo real sobre los cambios que se producen en el entorno virtual a Panorama. Estas actualizaciones incluyen cambios en la pertenencia de grupo y las direcciones IP de máquinas virtuales en grupos que envían tráfico al cortafuegos VM-Series.
7. **Panorama envía actualizaciones dinámicas**: a medida que Panorama recibe actualizaciones de NSX-T Manager, este las envía desde sus cortafuegos gestionados VM-Series. Panorama coloca las máquinas virtuales en grupos de direcciones dinámicas según los criterios que usted determine y envía la información de pertenencia a grupos de direcciones dinámicas a los cortafuegos. Esto permite que los cortafuegos apliquen la política de seguridad correcta al tráfico que fluye hacia y desde máquinas virtuales en su centro de datos NSX-T.

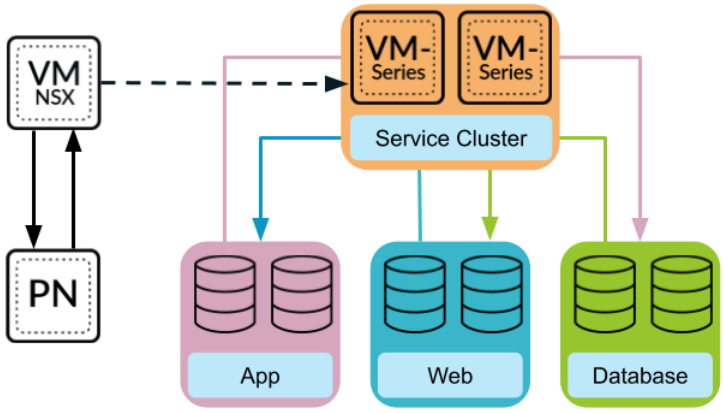
Implementaciones compatibles del cortafuegos VM-Series en VMware NSX-T (este-oeste)

Puede implementar una o más instancias del cortafuegos VM-Series como servicio asociado en su centro de datos VMware NSX-T para proteger el tráfico Este-Oeste y realizar microsegmentaciones. Para configurar el cortafuegos VM-Series para realizar la microsegmentación, puede implementar los cortafuegos en un clúster de servicios o por host.

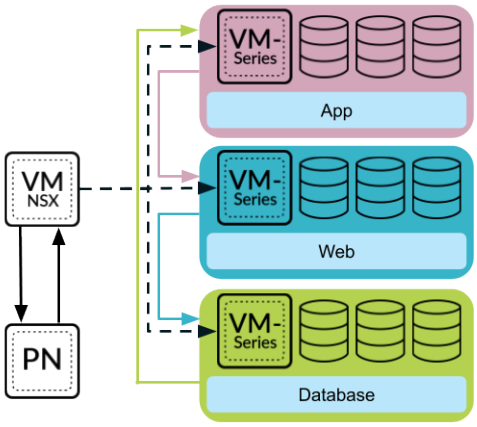
- **Clúster de servicios**: en una implementación en clúster, todos los cortafuegos VM-Series se instalan en un único clúster. El tráfico entre máquinas virtuales y grupos se redirige al clúster de VM-Series para la inspección y aplicación de políticas antes de continuar a su destino. Cuando configura una

 ©2024 Palo Alto Networks, Inc.

implementación en clúster, puede especificar un host particular dentro del clúster o seleccionar **Any (Cualquiera)** y dejar que NSX-T elija un host.



- **Basado en host**: en una implementación por host, se instala una instancia del cortafuegos VM-Series en cada host en el clúster de ESXi. El cortafuegos local inspecciona el tráfico entre invitados en el mismo host, por lo que no es necesario abandonar el host para su inspección. El cortafuegos inspecciona el tráfico que sale del host antes de llegar al vSwitch.



Después de implementar el cortafuegos, configure las reglas de redirección de tráfico que envían el tráfico al cortafuegos VM-Series. Las reglas de política de seguridad que configura en Panorama se envían a los cortafuegos VM-Series gestionados y luego se aplican al tráfico que pasa a través del cortafuegos.

Para implementar su cortafuegos VM-Series en VMware NSX-T, tiene dos opciones de flujo de trabajo: implementación basada en las operaciones y basada en la seguridad.

- Basado en las operaciones: en un flujo de trabajo basado en las operaciones, algunas partes del procedimiento de implementación se realizan en Panorama y el resto en NSX-T Manager. En Panorama, primero debe habilitar la comunicación entre Panorama y NSX-T Manager, configurar la definición del servicio e iniciar el cortafuegos VM-Series. Luego, debe iniciar sesión en NSX-T Manager para continuar con la configuración creando cadenas de servicios y reglas de dirección. Para completar su implementación de VM-Series, debe volver a Panorama para crear una política de seguridad.
- Basado en la seguridad: en un flujo de trabajo centrado en la seguridad, puede utilizar Panorama como un único panel para controlar y gestionar las operaciones de seguridad. Todo el flujo de trabajo de implementación se completa desde Panorama. El complemento Panorama para VMware NSX envía la configuración a NSX-T Manager, que crea cadenas de servicios y reglas de dirección.

 ©2024 Palo Alto Networks, Inc.

Se recomienda que seleccione un flujo de trabajo de implementación para su implementación VM-Series en NSX-T para facilitar su uso. Sin embargo, el cortafuegos VM-Series para VMware NSX-T admite el uso de ambos flujos de trabajo en el mismo complemento.

Implementación de VM-Series mediante el flujo de trabajo basado en las operaciones

Complete las siguientes tareas para implementar el cortafuegos VM-Series para proteger el tráfico Este-Oeste en su centro de datos NSX-T.

- Instale el plugin de Panorama para VMware NSX
- Habilitación de la comunicación entre NSX-T Manager y Panorama
- Creación de plantillas y grupos de dispositivos en Panorama
- Configuración de definición de servicio en Panorama
- Iniciar el cortafuegos VM-Series en NSX-T (este-oeste)
- Añadir una cadena de servicio
- Dirija el tráfico al cortafuegos VM-Series
- Aplicación de políticas de seguridad al cortafuegos VM-Series en NSX-T (este-oeste)
- Utilice vMotion para mover el cortafuegos VM-Series entre hosts

Instale el plugin de Panorama para VMware NSX

Descargue e instale el plugin de Panorama para VMware NSX. Consulte la Matriz de compatibilidad antes de instalar o actualizar su complemento.

Si tiene una configuración de HA en Panorama, repita el proceso de instalación en cada peer Panorama. Al instalar el plugin en pares de HA de Panorama, instale el plugin en el equipo pasivo antes de hacerlo en el equipo activo. Después de instalar el complemento en el peer pasivo, pasará a un estado no funcional. La instalación del plugin en el peer activo devuelve el peer pasivo a un estado funcional.

Si tiene un Panorama independiente o dos dispositivos Panorama instalados en un par de alta disponibilidad con varios complementos instalados, es posible que los complementos no reciban información actualizada sobre la etiqueta IP si uno o más de los complementos no están configurados. Esto ocurre porque Panorama no reenviará la información de la etiqueta IP a los complementos no configurados. Además, este problema puede ocurrir si uno o más de los complementos de Panorama no están en el estado Registrado o Correcto (el estado positivo varía según cada complemento). Asegúrese de que sus complementos estén en el estado positivo antes de continuar o ejecutar los comandos que se describen a continuación.

Si encuentra este problema, hay dos soluciones:

- Desinstale el complemento o complementos no configurados. Se recomienda que no instale un complemento que no planifique configurar de inmediato
- Puede utilizar los siguientes comandos para solventar este problema. Ejecute el siguiente comando para cada complemento no configurado en cada instancia de Panorama, para evitar que Panorama

 ©2024 Palo Alto Networks, Inc.

espere para enviar actualizaciones. Si no lo hace, sus cortafuegos pueden perder cierta información de la etiqueta IP.

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

Puede cancelar este comando ejecutando:

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

Los comandos descritos no son persistentes en los reinicios y deben usarse de nuevo para cualquier reinicio posterior. Para Panorama en el par de HA, los comandos deben ejecutarse en cada Panorama.

STEP 1 | Seleccione **Panorama** > **Plugins (Complementos)**.

STEP 2 | Seleccione **Check Now (Comprobar ahora)** para recuperar una lista de actualizaciones disponibles.

STEP 3 | Seleccione **Download (Descargar)** en la columna Action (Acción) para descargar el plugin.

STEP 4 | Seleccione la versión del complemento y haga clic en **Install (Instalar)** en la columna Action (Acción) para instalar el complemento. Panorama le alertará cuando se complete la instalación.

Habilitación de la comunicación entre NSX-T Manager y Panorama

Complete el siguiente procedimiento para habilitar la comunicación entre Panorama y NSX-T Manager. Puede conectar su Panorama a hasta 16 NSX-T Managers. Si está conectando su Panorama a múltiples NSX-T Managers, debe planificar cuidadosamente la jerarquía de su grupo de dispositivos y las pilas de plantillas, y considerar cómo interactúan con los otros componentes necesarios para la implementación. Las definiciones de servicio hacen referencia a grupos de dispositivos y pilas de plantillas y envían esa información a los cortafuegos en los clústeres ESXi relacionados.

STEP 1 | (Opcional) Omita la configuración del servidor proxy, configurada en Panorama bajo **Panorama** > **Setup (Configuración)** > **Services (Servicios)** > **Proxy Server (Servidor proxy)**, para la comunicación entre Panorama y NSX-T Manager. Este comando permite que Panorama se comunique directamente con NSX-T Manager mientras mantiene la comunicación proxy para otros servicios.

1. Inicie sesión en la CLI de Panorama.
2. Ejecute el siguiente comando para habilitar o deshabilitar la omisión de proxy.

   ```
   admin@Panorama> request plugins vmware_nsx global proxy bypass
   {yes | no}
   ```

   Seleccione **yes (sí)** para habilitar la omisión de proxy y **no** para deshabilitar la omisión de proxy. Esto se establece en **no** de forma predeterminada.

STEP 2 | Inicie sesión en la interfaz web de Panorama.

Si usa una conexión segura (https) desde un navegador web, inicie sesión usando la dirección IP y la contraseña que asignó durante la configuración inicial (https://<*IP address*>).

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Configure el acceso al administrador NSX-T. Repita este procedimiento para cada NSX-T Manager al que conectará Panorama.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Managers (Administradores de servicios)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre descriptivo en **Name (Nombre)** para su NSX-T Manager.
3. (Opcional) Añada una **Description (Descripción)** para NSX-T Manager.
4. Introduzca la **NSX Manager URL (URL de NSX Manager)**, Dirección IP virtual del clúster del NSX-T Manager o FQDN, para acceder al NSX-T Manager.
5. Introduzca las credenciales de **NSX Manager Login (Inicio de sesión de NSX Manager)**: nombre de usuario y contraseña, de modo que Panorama pueda autenticarse en NSX-T Manager.
6. Haga clic en **OK (Aceptar)**.

Si modifica la contraseña de inicio de sesión de NSX-T Manager, asegúrese de actualizar la contraseña en Panorama inmediatamente. Una contraseña incorrecta interrumpe la conexión entre Panorama y NSX-T Manager.

STEP 4 | Compile los cambios realizados en Panorama.

Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

STEP 5 | Verifique el estado de conexión en Panorama.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Managers (Administradores de servicios)**.
2. Verifique el mensaje en la columna **Status (Estado)**.

   Cuando la conexión es correcta, el estado se muestra como **Registered (Registrado)**. Esto indica que Panorama y NSX-T Manager están sincronizados.

   Los mensajes de estados de error son:

   - **No connection (Sin conexión)**: No se ha podido alcanzar/establecer una conexión de red con NSX-T Manager.
   - **Invalid Credentials (Credenciales no válidas)**: Las credenciales de acceso (nombre de usuario y/o contraseña) son incorrectas.
   - **Out of sync (Sin sincronización)**: Los ajustes de configuración definidos en Panorama son diferentes de lo que se define en NSX-T Manager. Haga clic en el enlace para obtener más detalles en relación con las razones para el fallo. Por ejemplo, NSX-T Manager puede tener una definición de servicio con el mismo nombre que se definió en Panorama. Para reparar el error, use el nombre de definición de servicio detallado en el mensaje de error para validar la definición del servicio en NSX-T Manager. Hasta que se sincronice la configuración en Panorama y NSX Manager, no es posible añadir una nueva definición de servicio en Panorama.
   - **Connection Disabled (Conexión deshabilitada)**: La conexión entre Panorama y el NSX-T Manager se desactivó manualmente.

Creación de plantillas y grupos de dispositivos en Panorama

Para poder gestionar los cortafuegos VM-Series para NSX-T en Panorama, los cortafuegos deben pertenecer a un grupo de dispositivos y una plantilla que forma parte de una pila de plantillas. Los

 ©2024 Palo Alto Networks, Inc.

grupos de dispositivos le permiten reunir los cortafuegos que necesitan objetos y políticas similares como una unidad lógica; la configuración se define usando las fichas **Objects (Objetos)** y **Policies (Políticas)** en Panorama. Use pilas de plantillas para configurar los ajustes necesarios para que los cortafuegos VM-Series operen en la red y los asociados; la configuración se define usando las pestañas **Device (Dispositivo)** y **Network (Red)** en Panorama. Y cada pila de plantillas con zonas usadas en su configuración de NSX-T en Panorama debe asociarse con una definición de servicio; como mínimo, debe crear una zona dentro de la pila de plantillas para que NSX-T Manager pueda redireccionar el tráfico al cortafuegos VM-Series.

Panorama es compatible con implementaciones de NSX-T Norte-Sur y NSX-T Este-Oeste al mismo tiempo. Se recomienda configurar grupos de dispositivos separados, pilas de plantillas y definiciones de servicio para NSX-T Norte-Sur y NSX-T Este-Oeste.

STEP 1 | Añada un grupo de dispositivos o una jerarquía de grupos de dispositivos.

1. Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)** y haga clic en **Add (Añadir)**. También puede crear una jerarquía de grupos de dispositivos.
2. Introduzca un **Name (Nombre)** y una **Description (Descripción)** exclusivos para identificar el grupo de dispositivos.
3. Haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** y seleccione **Panorama** como **Commit type (Tipo de confirmación)** para guardar los cambios en la configuración que se esté ejecutando.

STEP 2 | Añada una plantilla.

1. Seleccione **Panorama** > **Templates (Plantillas)** y haga clic en **Add (Añadir)**.
2. Introduzca **Name (Nombre)** y **Description (Descripción)** para identificar la plantilla.
3. Haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** y seleccione **Panorama** como **Commit Type (Tipo de confirmación)** para guardar los cambios en la configuración que se esté ejecutando.

STEP 3 | Cree una pila de plantillas.

1. Seleccione **Panorama** > **Templates (Plantillas)** y haga clic en **Add Stack (Añadir pila)**.
2. Introduzca **Name (Nombre)** y **Description (Descripción)** para identificar la plantilla.
3. Haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** y seleccione **Commit to Panorama (Confirmar en Panorama)** para guardar los cambios en la configuración que se esté ejecutando en Panorama.

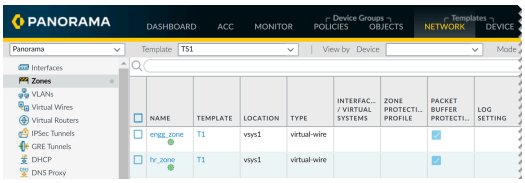
 ©2024 Palo Alto Networks, Inc.

STEP 4 | Asegúrese de Crear la(s) zona(s) para cada plantilla.

Cada zona está asignada a un perfil de servicio en NSX-T Manager. Para ser apta, una zona debe ser del tipo de cable virtual y una plantilla asociada a una definición de servicio.

Puede añadir hasta 32 zonas en cada plantilla.

1. Seleccione **Network (Red)** > **Zones (Zonas)**.
2. Seleccione la plantilla correcta en la lista desplegable **Template (Plantilla)**.
3. Seleccione **Add (Añadir)** e introduzca un **Nombre (Nombre)** de zona.
4. Establece el **Type (Tipo)** de interfaz a **Virtual Wire (Cable virtual)**.
5. Haga clic en **OK (Aceptar)**.
6. Verifique que las zonas se adjunten a la plantilla correspondiente.



7. Haga clic en **Commit (Confirmar)** y seleccione **Panorama** como **Commit Type (Tipo de confirmación)** para guardar los cambios en la configuración que se esté ejecutando.

   Panorama crea un perfil de servicio correspondiente en NSX-T Manager para cada zona calificada tras la confirmación.

STEP 5 | Actualice la información del servidor DNS y NTP de la pila de plantillas. Debe completar este paso si usa certificados de dispositivos en la implementación. Esto es necesario para garantizar que los cortafuegos implementados en el entorno de NSX-T tengan la información DNS correcta necesaria para llegar al servidor de certificados del dispositivo.

1. Compruebe que ha especificado la pila de plantillas correcta en el menú desplegable **Template (Plantilla)**.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y haga clic en el icono **Edit (Editar)**.
3. En la pestaña Servicios, introduzca la dirección IP de su **Primary DNS Server (Servidor DNS principal)** y de su **Secondary DNS Server (Servidor DNS secundario)**.
4. En la pestaña NTP, escriba la dirección IP del **NTP Server (Servidor NTP)**.
5. Haga clic en **OK (Aceptar)**.
6. **Commit (Confirmar)** los cambios realizados en Panorama.

Configuración de definición de servicio en Panorama

Una definición de servicio especifica la configuración para los cortafuegos VM-Series instalados en su entorno de centro de datos NSX-T. La definición del servicio debe incluir el grupo de dispositivos, una pila de plantillas y una URL de OVF.

STEP 1 | (Optional) Configure un grupo de notificación

Cree un grupo de notificación especificando los grupos de dispositivos a los que se debe notificar sobre los cambios en el entorno virtual. Los cortafuegos incluidos en los grupos de dispositivos especificados reciben directamente una actualización en tiempo real de los grupos de dispositivos y direcciones

 ©2024 Palo Alto Networks, Inc.

IP de VM invitados. Los cortafuegos usan esta actualización para determinar la lista más actual que constituye los grupos de direcciones dinámicas a los que se hace referencia en la política

1. Seleccione **Panorama** > **VMware** > **Grupo de notificación** y haga clic **Añadir**.
2. Dele al grupo de aplicaciones un **Name (Nombre)** descriptivo.
3. Seleccione las casillas de los grupos de dispositivos a los que se debe notificar acerca de los cambios en el entorno virtual. Si no está disponible la casilla de verificación para un grupo de dispositivos, esto significa que el grupo de dispositivos está automáticamente incluido en virtud de la jerarquía del grupo de dispositivos.
4. Haga clic en **OK (Aceptar)**.

STEP 2 | Añada una nueva definición de servicio.

Puede crear hasta 32 definiciones de servicio en Panorama.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Definitions (Definiciones de servicio)**.
2. Seleccione **Add (Añadir)** para crear una nueva definición de servicio.
3. Introduzca un nombre descriptivo en **Name (Nombre)** para su definición de servicio.
4. (Opcional Añada una **Description (Descripción)** que identifique la función o finalidad de los cortafuegos VM-Series que se implementarán usando esta definición de servicio.

STEP 3 | Asigne un grupo de dispositivos y una pila de plantillas a la definición de servicio.

Asegúrese de Creación de plantillas y grupos de dispositivos en Panorama.

Como los cortafuegos implementados en esta solución se administran centralmente desde Panorama, debe especificar el **Device Group (Grupo de dispositivos)** y la **Template Stack (Pila de plantillas)** a los que pertenecen los cortafuegos. Todos los cortafuegos que se implementan usando esta definición de servicio pertenecen a la pila de plantillas y el grupo de dispositivos especificados.

1. Seleccione el grupo de dispositivos o jerarquía de grupo de dispositivos en la lista desplegable **Device Group (Grupo de dispositivos)**.
2. Seleccione la pila de plantillas en la lista desplegable **Template (Plantilla)**.

No se puede reutilizar una pila de plantillas o grupo de dispositivos asignados a una definición de servicio en otra definición de servicio.

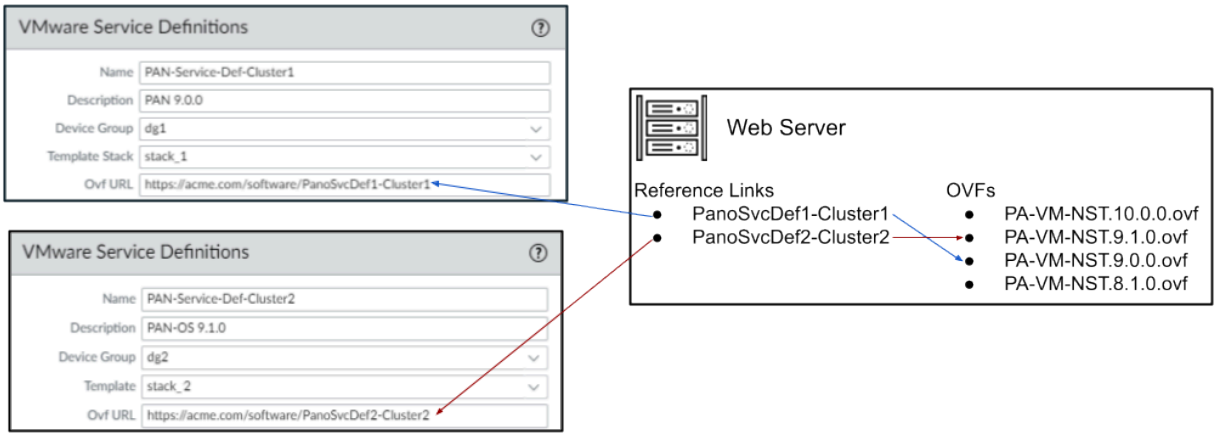
 ©2024 Palo Alto Networks, Inc.

STEP 4 | Especifique la ubicación del archivo OVF.

Descargue el archivo zip, descomprímalo para extraer y guardar los archivos .ovf, mf y .vmdk en el mismo directorio. Los archivos ovf y vmdk se usan para implementar cada instancia del cortafuego.

No cambie la ruta de acceso OVF de la definición de servicio de Panorama después de una implementación correcta de servicio NSX de cortafuegos de VM-Series. Cambiar la ruta de OVF, después de una implementación correcta del cortafuegos VM-Series, puede provocar un error en el estado de la implementación del servicio NSX. Puede resolver este error en NSX-T Manager, sin embargo, esto puede hacer que todos los cortafuegos VM-Series se vuelvan a implementar.

Se recomienda utilizar un nombre de ruta de acceso OVF con capacidad de ampliación que le permita cambiar la imagen base sin afectar a los cortafuegos implementados. En lugar de una ruta como **https://acme.com/software/PA-VM-NST.9.1.0.ovf,**, use algo como **https://acme.com/software/PanoSvcDef1-Cluster1.ovf.** El uso de una referencia de ruta estática eliminará cualquier necesidad futura de cambiar la ruta OVF. Se recomienda crear una ruta de acceso para cada definición de servicio de Panorama (clúster de vSphere) en la implementación y cambiar las referencias de imágenes base de PAN-OS en el servidor web según corresponda.



En **OVF URL (URL de OVF)**, añada la ubicación del servidor web que aloja el archivo ovf. Tanto http como https son protocolos admitidos.

Puede usar la misma versión de ovf o diferentes versiones en las definiciones de servicio. El uso de diferentes versiones de ovf en las definiciones de servicio le permite variar la versión de PAN-OS en los cortafuegos VM-Series en diferentes clústeres ESXi.

STEP 5 | (Opcional) Seleccione un **Grupo de notificación**.

STEP 6 | Seleccione **Este Oeste** como el **Tipo de inserción** para su cortafuegos.

STEP 7 | (Opcional) **Habilitar Comprobación de estado**. La comprobación de estado está habilitada de forma predeterminada en el complemento de Panorama para VMware NSX 3.2.0 y posteriores. En versiones anteriores del complemento, la comprobación de estado está deshabilitada de forma predeterminada. También llamada comprobación de estado del servicio, esta función de

 ©2024 Palo Alto Networks, Inc.

NSX-T le permite simular alta disponibilidad en caso de que falle una instancia del servicio. Cuando se configura con el cortafuegos VM-Series, si falla una instancia de servicio VM-Series, cualquier tráfico dirigido a ese cortafuegos se redirige a otra instancia de cortafuegos en el clúster (para implementaciones de clúster de servicio) o una instancia de cortafuegos en otro host (para implementaciones basadas en host).

No es posible deshabilitar o habilitar la comprobación de estado en una definición de servicio después de confirmar e implementar cortafuegos VM-Series en NSX-T. Intentar confirmar un cambio en la configuración de Comprobación de estado devuelve un error de confirmación. Para cambiar esto, debe eliminar y volver a crear su definición de servicio y volver a implementar sus cortafuegos VM-Series.

STEP 8 | Para recuperar automáticamente un certificado de dispositivo cuando NSX Manager implementa el cortafuegos Series-VM, configure el certificado del dispositivo.

Habilite esta opción para aplicar un certificado de dispositivo a los cortafuegos VM-Series recién implementados. Utilice esta opción únicamente cuando implemente el cortafuegos con un OVF de imagen base compatible con certificados de dispositivo. Panorama envía la información del certificado del dispositivo a NSX Manager como parte de la definición del servicio. Cuando se implementa un nuevo cortafuegos en NSX, el certificado del dispositivo se instala en el cortafuegos durante el arranque.

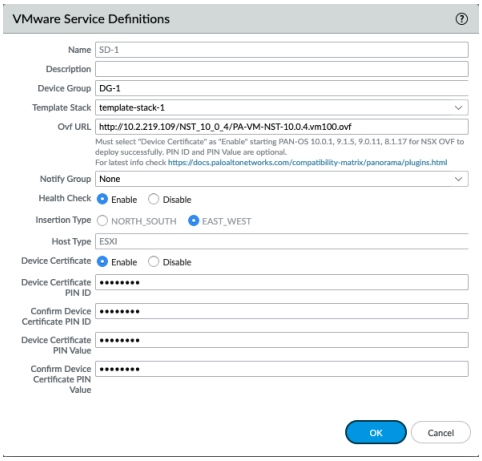
Para obtener una lista de OVF que admiten certificados de dispositivo para el cortafuegos VM-Series en VMware NSX, consulte la Matriz de compatibilidad de Palo Alto Networks.

Si su OVF admite un certificado de dispositivo, debe **Enable (Habilitar)** certificados de dispositivo independientemente de si está utilizando o no un certificado de dispositivo. Si su OVF no admite un certificado de dispositivo, desactive esta opción.

1. Si aún no lo ha hecho, inicie sesión en el Portal de atención al cliente y genere un PIN de registro y un ID de PIN.
2. En **Device Certificate (Certificado de dispositivo)**, haga clic en **Enable (Habilitar)**.
3. Copie el ID de PIN e introdúzcalo en el campo **Device Certificate PIN ID (ID de PIN de certificado de dispositivo)**.
4. Vuelva a introducir el ID de PIN en el campo **Confirm Device Certificate PIN ID (Confirmar ID de PIN del certificado de dispositivo)**.
5. Copie el valor de PIN e introdúzcalo en el campo **Device Certificate PIN Value (Valor de PIN del certificado de dispositivo)**.
6. Vuelva a introducir el valor del PIN en el campo **Confirm Device Certificate PIN Value (Confirmar el valor del PIN del certificado de dispositivo)**.

 ©2024 Palo Alto Networks, Inc.

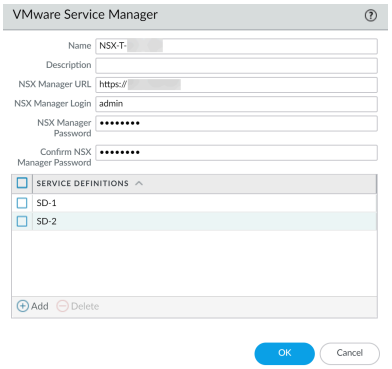
STEP 9 | Haga clic en **OK (Aceptar)** para guardar la definición de servicio.



STEP 10 | Adjunte la definición del servicio al gestor del servicio.

No es posible usar una definición de servicio en más de un administrador de servicios.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Manager (Administrador de Servicio)** y haga clic en el enlace del nombre del administrador del servicio.
2. En Definiciones del servicio, haga clic en **Add (Añadir)** y seleccione su definición de servicio del menú desplegable.
3. Haga clic en **OK (Aceptar)**.



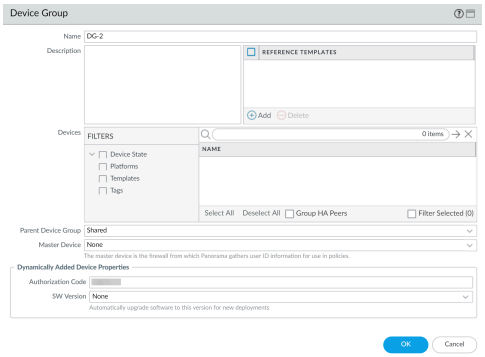
 ©2024 Palo Alto Networks, Inc.

STEP 11 | Añada el código de autorización para activar la licencias de los cortafuegos.

1. Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)** y elija el grupo de dispositivos al que se asoció con la definición del servicio que acaba de crear.
2. En **Propiedades de dispositivo añadidas dinámicamente**, añada el código de autorización que recibió con el correo electrónico de cumplimiento de su pedido y, opcionalmente, seleccione Ninguno en el menú desplegable **Versión de SW**.

   Cuando se implementa un nuevo cortafuegos en NSX-T, este se añade automáticamente al grupo de dispositivos, se proporciona una licencia con el código de autorización que proporcionó y se actualiza a la versión de PAN-OS que especificó.

   En el portal de asistencia técnica, puede visualizar el número total de cortafuegos que está autorizado a implementar y la proporción del número de licencias que se han usado del número total de licencias que le ofrece su código de autorización.



STEP 12 | **Commit to Panorama (Confirmar en Panorama)**.

STEP 13 | En NSX-T Manager, verifique que la definición de servicio esté disponible.

Seleccione **System (Sistema)** > **Service Deployments (Implementaciones de servicios)** > **Catalog (Catálogo)**. La definición de servicio aparece como instancia de servicio en NSX-T Manager.

Iniciar el cortafuegos VM-Series en NSX-T (este-oeste)

Complete el siguiente procedimiento para implementar el cortafuegos VM-Series como un servicio en su entorno NSX-T. Los campos **Deployment Specification (Especificación de implementación)** y **Deployment Template (Plantilla de implementación)** se rellenan automáticamente con información enviada desde Panorama como parte de la definición del servicio.

No edite ningún ajuste en Atributos de implementación. Estos valores se importan de Panorama y cambiarlos hace que falle la implementación.

STEP 1 | Inicie sesión en NSX-T Manager.

STEP 2 | Seleccione **System (Sistema)** > **Service Deployments (Implementaciones de servicios)** > **Deployment (Implementación)**.

STEP 3 | Seleccione su definición de servicio del menú desplegable **Partner Service (Servicio de socios)**.

STEP 4 | Haga clic en **Deploy Service (Implementar servicio)**.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Introduzca un nombre descriptivo en **Name (Nombre)** para su implementación de servicio.

STEP 6 | Seleccione el **Compute Manager (Gestor de cálculo)** (vCenter).

STEP 7 | Seleccione un **Deployment Type (Tipo de implementación)**: **Clustered (En clúster)** o **Host Based (Basado en host)**.

STEP 8 | Si seleccionó **Clustered (En clúster)** como **Deployment Type (Tipo de implementación)**, introduzca el **Clustered Deployment Count (Recuento de implementación en clúster)** para especificar el número de instancias de cortafuegos VM-Series que se van a implementar en el clúster.

STEP 9 | Seleccione un **Host** si va a iniciar VM-Series en una implementación en clúster. Seleccione un host específico del menú desplegable **Host** o **Any (Cualquiera)** para permitir que NSX-T Manager seleccione el host. Esta opción está atenuada en las implementaciones **Per host (Por host)**.

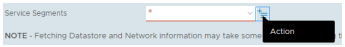
STEP 10 | Seleccione un **Data Store (Almacén de datos)** como repositorio para el cortafuegos VM-Series. En una implementación en clúster, seleccione un almacén de datos compartido si selecciona **Any (Cualquiera)** para el host, o seleccione un almacén de datos local si especificó un host en particular.

STEP 11 | Configure los ajustes de **Networks (Redes)**.

1. En la columna Redes, haga clic en **Set (Establecer)**.
2. Seleccione la **Network (Red)** para **eth0 - Management Nic**.
3. Seleccione el **Network Type (Tipo de red)**: DHCP o grupo de IP estática. Si elige Grupo de IP estática, seleccione un **IP Pool (Grupo de IP)**.
4. Marque **eth1 - Data-1 Nic**.
5. Haga clic en **Save (Guardar)**.

STEP 12 | Seleccione o configure un **Service Segment (Segmento de servicio)**. Para configurar un segmento de servicio, complete el siguiente procedimiento.

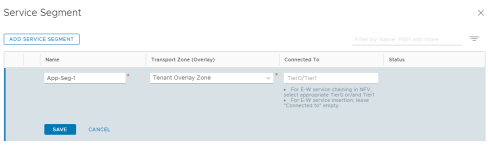
1. Haga clic en **Action (Acción)** en la columna **Service Segments (Segmentos de servicio)**.



2. Haga clic en **Add Service Segment (Añadir segmento de servicio)**.
3. Introduzca un **Name (Nombre)** descriptivo.
4. Seleccione una **Transport Zone (Overlay) [Zona de transporte (superposición)]**.

> *El cortafuegos VM-Series debe estar conectado a una zona de transporte superpuesta. Las máquinas virtuales invitadas se pueden adjuntar a una VLAN o a una zona de transporte superpuesta. El nodo de transporte que aloja las máquinas virtuales invitadas y la VM-Series debe configurarse con una zona de transporte superpuesta.*

5. Haga clic en **Save (Guardar)** y **Close (Cerrar)**.



 ©2024 Palo Alto Networks, Inc.

STEP 13 | Seleccione el **Cluster (Clúster)** donde se implementará el servicio. Debe seleccionar un clúster con **NSX Configuration (Configuración NSX)**.

STEP 14 | Haga clic en **Save (Guardar)**.

STEP 15 | Verifique que sus cortafuegos se hayan implementado correctamente.

1. Seleccione **System (Sistema)** > **Service Deployments (Implementaciones de servicio)** > **Service Instances (Instancias de servicio)**.
2. Confirme que sus cortafuegos estén en la lista y que el **Deployment Status (Estado de implementación)** muestra **Up (Activo)**.

STEP 16 | Compruebe que sus cortafuegos están conectados a Panorama.

1. Inicie sesión en Panorama.
2. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**.
3. Confirme que sus cortafuegos figuran en el grupo de dispositivos correcto y que el **Device State (Estado del dispositivo)** muestra **Connected (Conectado)**.

   El nombre del dispositivo para el cortafuegos VM-Series se muestra en Panorama como **PA-VM:** <nsx.clusterid>para la implementación de NSX-T (N-S) y como **PA-VM:** <nsx.servicevmid>para la implementación de NSX-T (E-W).

STEP 17 | Establezca una contraseña segura para la cuenta de administrador en sus cortafuegos VM-Series.

Cada cortafuegos VM-Series utiliza un nombre de usuario y una contraseña predeterminados (admin/admin), que se utilizan para el inicio de sesión inicial. Al iniciar sesión por primera vez, se le solicitará que establezca una contraseña nueva y más segura. La nueva contraseña debe tener un mínimo de ocho caracteres e incluir un mínimo de un carácter en minúsculas y otro en mayúsculas, así como un número y un carácter especial.

Puede actualizar la contraseña en cada cortafuegos de forma individual o todos a la vez a través de Panorama.

- **Panorama**: en Panorama, puede cambiar la contraseña predeterminada para todos los cortafuegos en una plantilla o eliminar el usuario administrador y crear un nuevo nombre de usuario y contraseña.

  1. Iniciar sesión en Panorama
  2. Seleccione **Device (Dispositivo)** > **Administrators (Administradores)** y seleccione el usuario **admin**.
  3. **Delete (Eliminar)** el usuario o haga clic en el usuario e introduzca una nueva contraseña.
  4. Si cambió la contraseña, haga clic en **OK (Aceptar)**.
  5. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** > **Edit Selections (Editar selecciones)** > **Force Template Values (Forzar valores de plantilla)**.
  6. Haga clic en **OK (Aceptar)**.
- **Cortafuegos**: este procedimiento debe repetirse en cada cortafuegos VM-Series.

  1. Inicie sesión en el cortafuegos VM-series utilizando el nombre de usuario y la contraseña predeterminados.
  2. Siga las indicaciones para restablecer la contraseña.

 ©2024 Palo Alto Networks, Inc.

Añadir una cadena de servicio

Una cadena de servicios es un agrupación de servicios establecidos en una secuencia lógica. Cuando el tráfico se redirige a la cadena de servicio, este se mueve a través de cada servicio en el orden que lo haya configurado.

STEP 1 | Seleccione **Security (Seguridad)** > **Network Introspection Settings (Configuración de introspección de red)** > **Service Chains (Cadenas de servicio)** > **Add Chain (Añadir cadena)**.

STEP 2 | Introduzca un **Name (Nombre)** descriptivo y una **Description (Descripción)** (opcional) para su cadena de servicio.

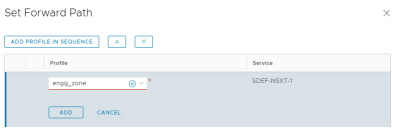
STEP 3 | Seleccione el **Service Segment (Segmento de servicio)** que aplicó cuando implementó el cortafuegos VM-Series.

STEP 4 | Establecer la ruta de reenvío. La cadena de servicio es una secuencia lógica de perfiles de servicio, por lo que el tráfico se mueve a través de los servicios en el orden especificado como ruta de reenvío.

1. Seleccione **Establecer ruta de reenvío** > **Añadir perfil en secuencia**.
2. Seleccione un perfil de servicio. La columna de servicio se cumplimenta automáticamente según el perfil de servicio que seleccione.
3. Haga clic en **Add (Añadir)**.
4. (Opcional) Si tiene otros perfiles de servicio de socios en su entorno NSX-T, haga clic en **Añadir perfil en secuencia** para añadirlos a esta cadena de servicios.

   Puede seleccionar solo un perfil de servicio por definición de servicio.

5. Haga clic en **Guardar** cuando haya terminado de añadir perfiles de servicio.



STEP 5 | En la columna Reverse Path, marque **Reenvío inversoRuta** para ver el tráfico de retorno se mueve a través de la cadena de servicio en orden inverso.

STEP 6 | (Opcional) Si se seleccionan otros perfiles de servicio de socios, establezca una ruta inversa.

Debe seleccionar el mismo perfil de servicio VM-Series establecido en la Ruta de reenvío.

1. Seleccione **Establecer ruta inversa** > **Añadir perfil en secuencia**.
2. Seleccione un perfil de servicio. La columna de servicio se cumplimenta automáticamente según el perfil de servicio que seleccione.
3. Haga clic en **Add (Añadir)**.
4. (Opcional) Si tiene otros perfiles de servicio en su entorno NSX-T, haga clic en **Agregar perfil en secuencia** para agregarlos a esta cadena de servicio.
5. Haga clic en **Guardar** cuando haya terminado de añadir perfiles de servicio.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Establezca la **Política de fallos**: **para** Permitir **o** Bloquear. Esto define la acción que NSX-T toma si un perfil de servicio falla.

STEP 8 | Haga clic en **Save (Guardar)**.

Dirija el tráfico al cortafuegos VM-Series

Configure las reglas de política para dirigir el tráfico de máquinas virtuales o grupos de máquinas virtuales al cortafuegos VM-Series.

STEP 1 | Seleccione **Security (Seguridad)** > **Network Introspection (E-W) [Introspección de red (E-O)]** > **Rules (Reglas)** > **Add Policy (Añadir política)**.

STEP 2 | Haga clic en **New Policy (Nueva política)** para dar a su política un nombre descriptivo.

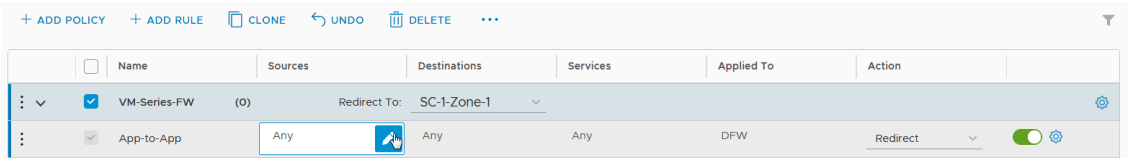
STEP 3 | Seleccione su cadena de servicio del menú desplegable **Redirect To (Redirigir a)**.

STEP 4 | Seleccione la política y haga clic en **Add Rule (Añadir regla)**.

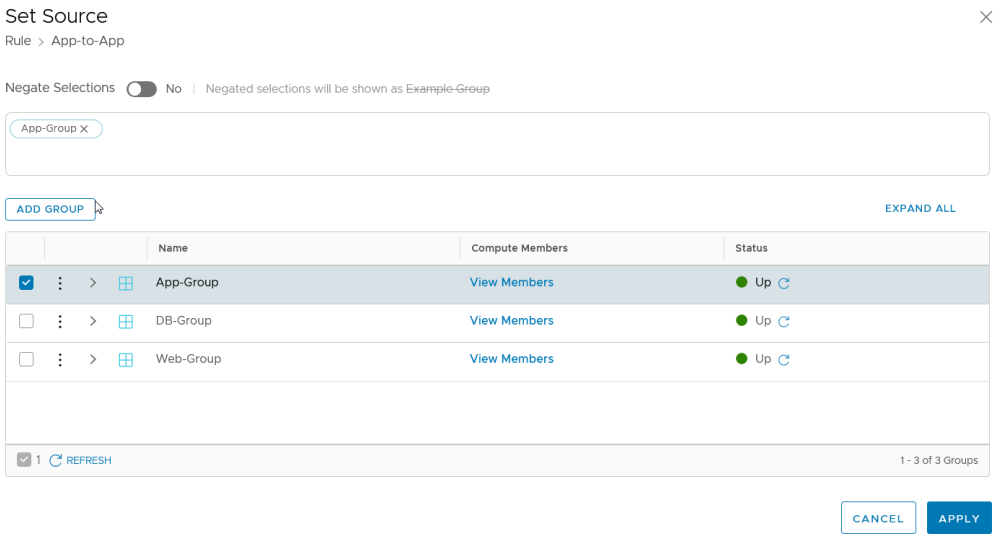
STEP 5 | Haga clic en **New Rule (Nueva regla)** para dar a su regla un nombre descriptivo.

STEP 6 | Seleccione una fuente.

1. Haga clic en el icono de lápiz en la columna de fuente para elegir un grupo de fuentes de máquinas virtuales.



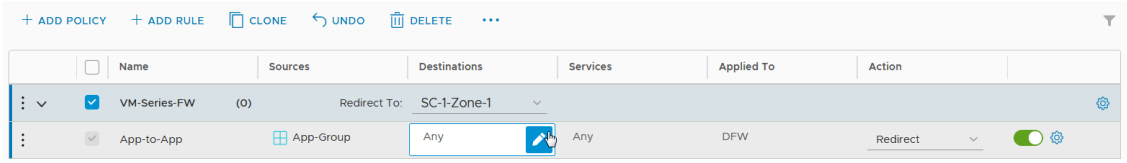
2. Verifique el grupo o grupos de fuentes.
3. Haga clic en **Apply (Aplicar)**.



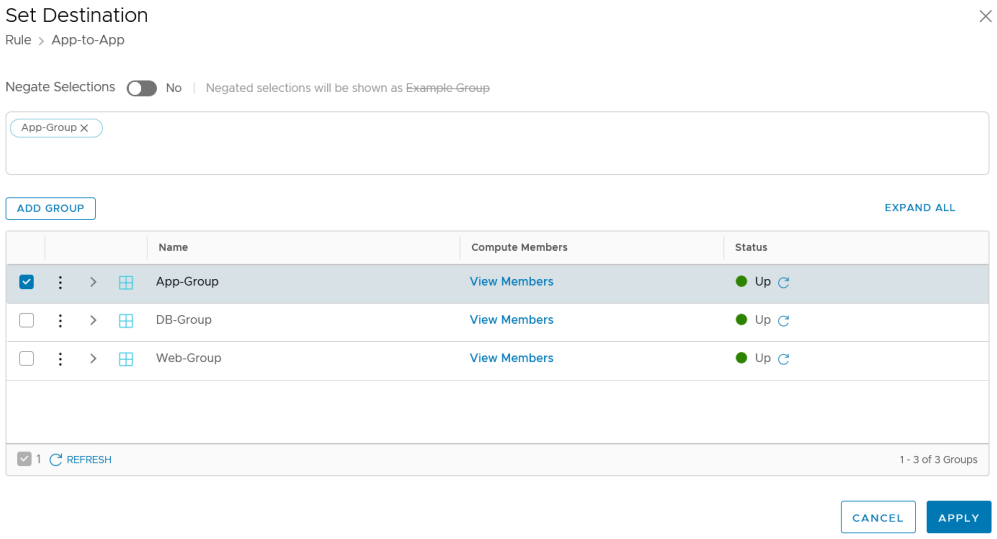
 ©2024 Palo Alto Networks, Inc.

STEP 7 | Seleccione un **Destination (Destino)**.

1. Haga clic en el icono de lápiz en la columna de destino para elegir un grupo de fuentes de máquinas virtuales.



2. Verifique el grupo o grupos de destino.
3. Haga clic en **Apply (Aplicar)**.



STEP 8 | (Opcional) Seleccione los **Services (Servicios)** a los que se aplicará la regla.

STEP 9 | Elija una de las siguientes opciones en el campo **Applied to (Aplicado a)**:

- Seleccione **DFW** para aplicar la regla a todas las NIC virtuales conectadas al conmutador lógico.
- Seleccione **Groups (Grupos)** para aplicar la regla las NIC virtuales de máquinas virtuales miembros en el grupo o grupos especificados.

STEP 10 | Seleccione la **Action (Acción)** - **Redirect (Redirigir)** o **Do Not Redirect (No redirigir)**.

STEP 11 | Haga clic en **Publish (Publicar)**.

STEP 12 | Repita este proceso para crear políticas o reglas adicionales.

Aplicación de políticas de seguridad al cortafuegos VM-Series en NSX-T (este-oeste)

Ahora que ha creado las reglas de redireccionamiento en NSX-T Manager, ahora puede usar Panorama para gestionar políticas de forma centralizada en los cortafuegos VM-Series.

Para gestionar políticas centralizadas, adjunte el grupo de direcciones dinámicas como una dirección de origen o destino en la política de seguridad y envíelo a los cortafuegos; los cortafuegos puede recuperar dinámicamente las direcciones IP de las máquinas virtuales que se incluyen en cada grupo de seguridad para garantizar que el tráfico que se origina o se dirige a las máquinas virtuales del grupo especificado cumple los requisitos.

 ©2024 Palo Alto Networks, Inc.

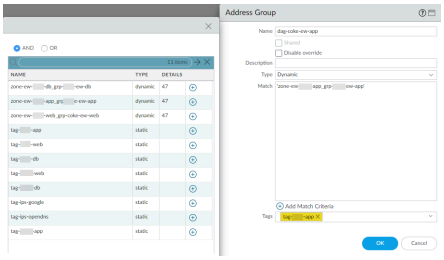
STEP 1 | Inicie sesión en Panorama.

STEP 2 | Creación de grupos de direcciones dinámicas.

1. Seleccione **Objects (Objetos)** > **Address Groups (Grupos de direcciones)**.
2. Seleccione el Grupo de dispositivos que creó para gestionar su VM-Series en el cortafuegos NSX-T de la lista desplegable **Grupo de dispositivos**.
3. Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** y una **Description (Descripción)** para el grupo de direcciones dinámicas.
4. Defina el **Type (Tipo)** como **Dynamic (Dinámico)**.
5. Agregue criterios de coincidencia a su grupo de direcciones dinámicas.

   Algunas extensiones del navegador pueden bloquear las llamadas a la API entre Panorama y NSX-T, lo que evita que Panorama reciba criterios de coincidencia. Si Panorama no muestra ningún criterio de coincidencia y usted está usando extensiones de navegador, deshabilite las extensiones y Sincronizar objetos dinámicos para completar las etiquetas disponibles para Panorama.
6. Haga clic en **Añadir criterios de coincidencia**.
7. Seleccione el **Y** u **O** operador y haga clic en el icono más (+) junto al nombre del grupo de seguridad para añadirlo al grupo de direcciones dinámicas.

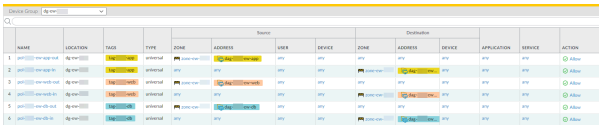
   Los grupos de seguridad que se muestran en el cuadro de diálogo de criterios de coincidencia se derivan de los grupos que ha definido en NSX-T Manager. Aquí sólo están disponibles los grupos a los que se hace referencia en las políticas de seguridad y desde los que se redirecciona el tráfico al cortafuegos VM-Series.



8. Haga clic en **OK (Aceptar)**.
9. Repita estos pasos para crear el número apropiado de grupos de direcciones dinámicas requeridos para su implementación.
10. Haga clic en **Commit (Confirmar)** para compilar los cambios.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Cree las reglas de política de seguridad.



1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Prerules (Pre reglas)**.
2. Seleccione el **Grupo de dispositivos** que creó para gestionar los cortafuegos VM-Series en NSX-T en Creación de plantillas y grupos de dispositivos en Panorama.
3. Haga clic en **Add (Añadir)** e introduzca **Name (Nombre)** y **Description (Descripción)** para la regla. En este ejemplo la regla de seguridad permite todo el tráfico entre los servidores WebFrontEnd y de aplicaciones.
4. Seleccione la **Source Zone (Zona de origen)** y **Destination Zone (Zona de destino)**. El nombre de la zona debe ser el mismo en ambas columnas.
5. En **Source Address (Dirección de origen)** y **Destination Address (Dirección de destino)**, seleccione o escriba una dirección, grupo de direcciones o región. En este ejemplo, seleccionamos un grupo de direcciones, el grupo de direcciones dinámicas que creó anteriormente.
6. Seleccione la **Application (Aplicación)** que desea permitir. En este ejemplo hemos creado un **Application Group (Grupo de aplicaciones)** que incluye un grupo estático de aplicaciones específicas que se agrupan juntas.
   1. Haga clic en **Add (Añadir)** y seleccione **New Application Group (Nuevo grupo de aplicaciones)**.
   2. Haga clic en **Add (Añadir)** para seleccionar la aplicación que desea añadir al grupo.
   3. Haga clic en **OK (Aceptar)** para crear el grupo de aplicaciones.
7. Especifique la acción, **Allow (Permitir)** o **Deny (Denegar)**, para el tráfico y, opcionalmente, adjunte los perfiles de seguridad predeterminados para los antivirus, anti-spyware y protección contra vulnerabilidades en Profiles (Perfiles).
8. Repita los pasos anteriores para crear las reglas de políticas pertinentes.
9. Haga clic en **Commit (Confirmar)** y seleccione Commit Type (Tipo de confirmación) como **Panorama**. Haga clic en **OK (Aceptar)**.

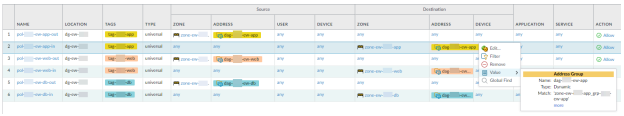
STEP 4 | Aplique las políticas a los cortafuegos VM-Series para NSX-T.

1. Haga clic en **Commit (Confirmar)** y seleccione Commit Type (Tipo de confirmación) como **Device Groups (Grupos de dispositivos)**.
2. Seleccione el grupo de dispositivos, que en este ejemplo es Grupo de dispositivos NSX-T, y haga clic en **Aceptar**.
3. Verifique que la confirmación se realice correctamente.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Valide que los miembros del grupo de direcciones dinámicas se cumplimentan en el cortafuegos VM-Series.

1. En Panorama, cambie el contexto del dispositivo para iniciar la interfaz web del cortafuegos al que envió las políticas.
2. En el cortafuegos VM-Series, seleccione **Policies (Políticas)** > **Security (Seguridad)** y elija una regla.
3. Seleccione la flecha desplegable junto al vínculo del grupo de direcciones y seleccione **Inspect (Inspeccionar)**. También puede comprobar si los criterios de coincidencia son precisos.



4. Haga clic en el vínculo **more (más)** y compruebe que se muestra la lista de direcciones IP registradas.

   La política entra en vigor para todas las direcciones IP que pertenecen a este grupo de direcciones y se muestra aquí.

STEP 6 | (Opcional) Use la plantilla para enviar una configuración base para la configuración de red y dispositivo como, por ejemplo servidor DNS, servidor NTP, servidor Syslog y pancarta de inicio de sesión.

Si desea más información sobre el uso de plantillas, consulte la Guía del administrador de Panorama.

STEP 7 | Cree un perfil de protección de zona y adjúntelo a una zona.

Un perfil de protección de la zona ofrece protección contra desbordamientos y posee la capacidad de proteger contra el análisis de puertos, los barridos de puertos y los ataques basados en paquetes. Le permite proteger el tráfico intraniveles e interniveles entre máquinas virtuales dentro de su centro de datos y el tráfico desde Internet destinado a las máquinas virtuales (cargas de trabajo) en su centro de datos.

1. Seleccione **Template (Plantilla)**.
2. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** para añadir y configurar un nuevo perfil.
3. Seleccione **Network (Red)** > **Zones (Zonas)**, haga clic en la zona predeterminada de la lista y seleccione el perfil en el menú desplegable **Zone Protection Profile (Perfil de protección de zona)**.

STEP 8 | Cree un perfil de protección DoS y adjúntelo a la regla de políticas Protección DoS .

1. Seleccione su **Device Group (Grupo de dispositivos)**.
2. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **DoS Protection (Protección DoS)** para añadir y configurar un nuevo perfil.
   - Un perfil clasificado permite la creación de un umbral que se aplica a una IP de origen única. Por ejemplo, puede configurar una calificación de sesión máxima para una dirección IP que coincidió con la política, y luego bloquear esa dirección IP única una vez que se activó el umbral.
   - Un perfil agregado permite la creación de una calificación de sesión máxima para todos los paquetes que coincidan con la política. El umbral se aplica a la nueva calificación de sesión

 ©2024 Palo Alto Networks, Inc.

para todas las direcciones IP combinadas. Una vez que el umbral se activa, afecta todo el tráfico que coincide con la política.

3. Cree una nueva regla de la política de protección DoS**Policy (Política)** > **DoS Protection (Protección DoS)** y adjunte el nuevo perfil a esta.

Utilice vMotion para mover el cortafuegos VM-Series entre hosts

Para mantener el flujo de tráfico mientras utiliza vMotion para mover su cortafuegos VM-Series entre hosts ESXi con configuraciones de CPU homogéneas en VMware NSX-T, debe usar la CLI de PAN-OS para pausar la supervisión del heartbeat interno del cortafuegos VM-Series durante vMotion. Puede especificar el periodo de tiempo, en minutos, que se pausa la supervisión de heartbeats. La supervisión de heartbeats se puede pausar hasta por 60 minutos. Cuando el intervalo de pausa caduca o usted finaliza deliberadamente el intervalo de pausa, se reanuda la supervisión de heartbeats.

La tecnología vMotion del cortafuegos VM-Series es compatible en vSphere 6.5, 6.7 y 7.0 si los hosts ESXi tienen una configuración de CPU homogénea.

Este procedimiento no es necesario cuando se usa vMotion para mover el cortafuegos VM-Series si está ejecutando vSphere 7.0 o posterior.

STEP 1 | Inicie sesión en la CLI del cortafuegos VM-Series.

STEP 2 | Establezca el intervalo de pausa de supervisión de heartbeat mediante el siguiente comando. La pausa comienza tan pronto como se ejecuta el comando. Si vMotion tarda más de lo esperado, puede volver a ejecutar este comando para establecer un nuevo intervalo más largo que se inicie cuando el comando se vuelva a ejecutar.

```
request system heartbeat-pause set interval <pause-time-in-minutes>
```

Puede ver el tiempo restante en el intervalo de pausa usando el siguiente comando.

```
request system heartbeat-pause show interval
```

STEP 3 | (Opcional) Si completa vMotion antes de que haya transcurrido el intervalo de pausa, puede finalizar la pausa estableciendo el intervalo en cero (0).

```
request system heartbeat-pause set interval 0
```

Implementación de VM-Series mediante el flujo de trabajo basado en la seguridad

Puede utilizar el flujo de trabajo basado en la seguridad para controlar y administrar su cortafuegos VM-Series para NSX-T desde Panorama. No es necesario que acceda a NSX-T Manager para crear cadenas de servicios y reglas de dirección; sin embargo, la implementación del servicio aún debe crearse en NSX-T Manager.

- Instale el plugin de Panorama para VMware NSX
- Habilitación de la comunicación entre NSX-T Manager y Panorama
- Creación de plantillas y grupos de dispositivos en Panorama
- Configuración de definición de servicio en Panorama
- Iniciar el cortafuegos VM-Series en NSX-T (este-oeste)

 ©2024 Palo Alto Networks, Inc.

- Crear grupos de direcciones dinámicas
- Crear políticas de seguridad
- Crear criterios de pertenencia a grupos de direcciones dinámicas
- Generar política de dirección
- Genere reglas de dirección

Instale el plugin de Panorama para VMware NSX

Descargue e instale el plugin de Panorama para VMware NSX. Consulte la Matriz de compatibilidad antes de instalar o actualizar su complemento.



El flujo de trabajo de la implementación basada en la seguridad requiere el complemento Panorama para VMware NSX 4.0.0. Además, debe actualizar al complemento 4.0.0 desde el complemento Panorama para VMware NSX 3.2.x

Si tiene una configuración de HA en Panorama, repita el proceso de instalación en cada peer Panorama. Al instalar el plugin en pares de HA de Panorama, instale el plugin en el equipo pasivo antes de hacerlo en el equipo activo. Después de instalar el complemento en el peer pasivo, pasará a un estado no funcional. La instalación del plugin en el peer activo devuelve el peer pasivo a un estado funcional.

Si tiene un Panorama independiente o dos dispositivos Panorama instalados en un par de alta disponibilidad con varios complementos instalados, es posible que los complementos no reciban información actualizada sobre la etiqueta IP si uno o más de los complementos no están configurados. Esto ocurre porque Panorama no reenviará la información de la etiqueta IP a los complementos no configurados. Además, este problema puede ocurrir si uno o más de los complementos de Panorama no están en el estado Registrado o Correcto (el estado positivo varía según cada complemento). Asegúrese de que sus complementos estén en el estado positivo antes de continuar o ejecutar los comandos que se describen a continuación.

Si encuentra este problema, hay dos soluciones:

- Desinstale el complemento o complementos no configurados. Se recomienda que no instale un complemento que no planifique configurar de inmediato
- Puede utilizar los siguientes comandos para solventar este problema. Ejecute el siguiente comando para cada complemento no configurado en cada instancia de Panorama, para evitar que Panorama espere para enviar actualizaciones. Si no lo hace, sus cortafuegos pueden perder cierta información de la etiqueta IP.

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

  Puede cancelar este comando ejecutando:

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

Los comandos descritos no son persistentes en los reinicios y deben usarse de nuevo para cualquier reinicio posterior. Para Panorama en el par de HA, los comandos deben ejecutarse en cada Panorama.

STEP 1 | Seleccione **Panorama** > **Plugins (Complementos)**.

STEP 2 | Seleccione **Check Now (Comprobar ahora)** para recuperar una lista de actualizaciones disponibles.

STEP 3 | Seleccione **Download (Descargar)** en la columna Action (Acción) para descargar el plugin.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Seleccione la versión del complemento y haga clic en **Install (Instalar)** en la columna Action (Acción) para instalar el complemento. Panorama le alertará cuando se complete la instalación.

Habilitación de la comunicación entre NSX-T Manager y Panorama

Complete el siguiente procedimiento para habilitar la comunicación entre Panorama y NSX-T Manager. Puede conectar su Panorama a hasta 16 NSX-T Managers. Si está conectando su Panorama a múltiples NSX-T Managers, debe planificar cuidadosamente la jerarquía de su grupo de dispositivos y las pilas de plantillas, y considerar cómo interactúan con los otros componentes necesarios para la implementación. Las definiciones de servicio hacen referencia a grupos de dispositivos y pilas de plantillas y envían esa información a los cortafuegos en los clústeres ESXi relacionados.

STEP 1 | (Opcional) Omita la configuración del servidor proxy, configurada en Panorama bajo **Panorama** > **Setup (Configuración)** > **Services (Servicios)** > **Proxy Server (Servidor proxy)**, para la comunicación entre Panorama y NSX-T Manager.

Este comando permite que Panorama se comunique directamente con NSX-T Manager mientras mantiene la comunicación proxy para otros servicios.

1. Inicie sesión en la CLI de Panorama.
2. Ejecute el siguiente comando para habilitar o deshabilitar la omisión de proxy.

   ```
   admin@Panorama> request plugins vmware_nsx global proxy bypass {yes | no}
   ```

   Seleccione **yes (sí)** para habilitar la omisión de proxy y **no** para deshabilitar la omisión de proxy. Esto se establece en **no** de forma predeterminada.

STEP 2 | Inicie sesión en la interfaz web de Panorama.

Si usa una conexión segura (https) desde un navegador web, inicie sesión usando la dirección IP y la contraseña que asignó durante la configuración inicial (https://<*IP address*>).

STEP 3 | Configure el acceso al administrador NSX-T.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Managers (Administradores de servicios)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre descriptivo en **Name (Nombre)** para su NSX-T Manager.
3. (Opcional) Añada una **Description (Descripción)** para NSX-T Manager.
4. Introduzca la **NSX Manager URL (URL de NSX Manager)**, Dirección IP virtual del clúster del NSX-T Manager o FQDN, para acceder al NSX-T Manager.
5. Introduzca las credenciales de **NSX Manager Login (Inicio de sesión de NSX Manager)**: nombre de usuario y contraseña, de modo que Panorama pueda autenticarse en NSX-T Manager.
6. Haga clic en **OK (Aceptar)**.
7. Repita este procedimiento para cada NSX-T Manager al que conectará Panorama.

Si modifica la contraseña de inicio de sesión de NSX-T Manager, asegúrese de actualizar la contraseña en Panorama inmediatamente. Una contraseña incorrecta interrumpe la conexión entre Panorama y NSX-T Manager.

STEP 4 | Compile los cambios realizados en Panorama.

Haga clic en **Commit (Confirmar)** y en **Commit to Panorama (Confirmar en Panorama)**.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Verifique el estado de conexión en Panorama.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Managers (Administradores de servicios)**.
2. Verifique el mensaje en la columna **Status (Estado)**.

   Cuando la conexión es correcta, el estado se muestra como **Registered (Registrado)**. Esto indica que Panorama y NSX-T Manager están sincronizados.

   Los mensajes de estados de error son:

   - **No connection (Sin conexión)**: No se ha podido alcanzar/establecer una conexión de red con NSX-T Manager.
   - **Invalid Credentials (Credenciales no válidas)**: Las credenciales de acceso (nombre de usuario y/o contraseña) son incorrectas.
   - **Out of sync (Sin sincronización)**: Los ajustes de configuración definidos en Panorama son diferentes de lo que se define en NSX-T Manager. Haga clic en el enlace para obtener más detalles en relación con las razones para el fallo. Por ejemplo, NSX-T Manager puede tener una definición de servicio con el mismo nombre que se definió en Panorama. Para reparar el error, use el nombre de definición de servicio detallado en el mensaje de error para validar la definición del servicio en NSX-T Manager. Hasta que se sincronice la configuración en Panorama y NSX Manager, no es posible añadir una nueva definición de servicio en Panorama.
   - **Connection Disabled (Conexión deshabilitada)**: La conexión entre Panorama y el NSX-T Manager se desactivó manualmente.

Creación de plantillas y grupos de dispositivos en Panorama

Para poder gestionar los cortafuegos VM-Series para NSX-T en Panorama, los cortafuegos deben pertenecer a un grupo de dispositivos y una plantilla que forma parte de una pila de plantillas. Los grupos de dispositivos le permiten reunir los cortafuegos que necesitan objetos y políticas similares como una unidad lógica; la configuración se define usando las fichas **Objects (Objetos)** y **Policies (Políticas)** en Panorama. Use pilas de plantillas para configurar los ajustes necesarios para que los cortafuegos VM-Series operen en la red y los asociados; la configuración se define usando las pestañas **Device (Dispositivo)** y **Network (Red)** en Panorama. Y cada pila de plantillas con zonas usadas en su configuración de NSX-T en Panorama debe asociarse con una definición de servicio que se creará más adelante; como mínimo, debe crear una zona dentro de la pila de plantillas para que NSX-T Manager pueda redireccionar el tráfico al cortafuegos VM-Series. Más adelante, asociará un grupo de dispositivos y una plantilla a la implementación de NSX-T y creará una definición de servicio.

Panorama es compatible con implementaciones de NSX-T Norte-Sur y NSX-T Este-Oeste al mismo tiempo. Debe configurar grupos de dispositivos separados, pilas de plantillas y definiciones de servicio para NSX-T Norte-Sur y NSX-T Este-Oeste.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Añada un grupo de dispositivos o una jerarquía de grupos de dispositivos.

1. Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)** y haga clic en **Add (Añadir)**. También puede crear una jerarquía de grupos de dispositivos.
2. Introduzca un **Name (Nombre)** y una **Description (Descripción)** exclusivos para identificar el grupo de dispositivos.
3. Haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** y seleccione **Panorama** como **Commit type (Tipo de confirmación)** para guardar los cambios en la configuración que se esté ejecutando.

STEP 2 | Añada una plantilla.

1. Seleccione **Panorama** > **Templates (Plantillas)** y haga clic en **Add (Añadir)**.
2. Introduzca **Name (Nombre)** y **Description (Descripción)** para identificar la plantilla.
3. Haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** y seleccione **Panorama** como **Commit Type (Tipo de confirmación)** para guardar los cambios en la configuración que se esté ejecutando.

STEP 3 | Cree una pila de plantillas y añada la plantilla recién creada.

1. Seleccione **Panorama** > **Templates (Plantillas)** y haga clic en **Add Stack (Añadir pila)**.
2. Introduzca un nombre único en **Name (Nombre)** y una descripción en **Description (Descripción)** para identificar la pila de plantillas.
3. En **Templates (Plantillas)**, haga clic en **Add (Añadir)** y seleccione la plantilla que creó en el paso 2 en el menú desplegable.
4. Haga clic en **OK (Aceptar)**.
5. Haga clic en **Commit (Confirmar)** y seleccione **Commit to Panorama (Confirmar en Panorama)** para guardar los cambios en la configuración que se esté ejecutando en Panorama.

STEP 4 | Asegúrese de Crear la(s) zona(s) para cada plantilla.

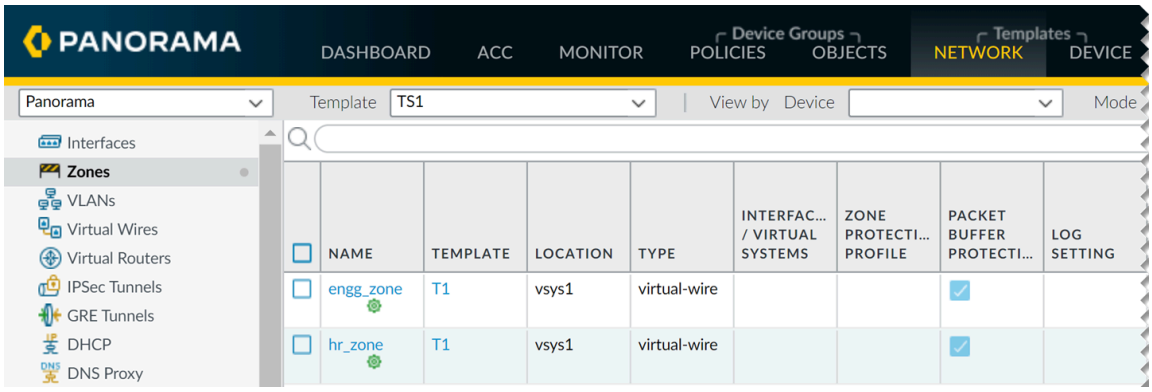
El complemento Panorama para VMware NSX asigna cada zona a un perfil de servicio en NSX-T Manager. Para clasificar, una zona debe ser del tipo de cable virtual y formar parte de una plantilla que asociará con una definición de servicio; consulte Configuración de definición de servicio en Panorama

 ©2024 Palo Alto Networks, Inc.

para obtener más información. En la mayoría de los casos de uso, una sola zona es suficiente. Sin embargo, debe crear varias zonas para varios inquilinos

Puede añadir hasta 32 zonas en cada plantilla.

1. Seleccione **Network (Red)** > **Zones (Zonas)**.
2. Seleccione la plantilla correcta en la lista desplegable **Template (Plantilla)**.
3. Seleccione **Add (Añadir)** e introduzca un **Nombre (Nombre)** de zona.
4. Establece el **Type (Tipo)** de interfaz a **Virtual Wire (Cable virtual)**.
5. Haga clic en **OK (Aceptar)**.
6. Verifique que las zonas se adjunten a la plantilla correspondiente.



7. Haga clic en **Commit (Confirmar)** y seleccione **Panorama** como **Commit Type (Tipo de confirmación)** para guardar los cambios en la configuración que se esté ejecutando.

STEP 5 | Actualice la información del servidor DNS y NTP de la pila de plantillas. Debe completar este paso si usa certificados de dispositivos en la implementación. Esto es necesario para garantizar que los cortafuegos implementados en el entorno de NSX-T tengan la información DNS correcta necesaria para llegar al servidor de certificados del dispositivo.

1. Compruebe que ha especificado la pila de plantillas correcta en el menú desplegable **Template (Plantilla)**.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y haga clic en el icono **Edit (Editar)**.
3. En la pestaña Servicios, introduzca la dirección IP de su **Primary DNS Server (Servidor DNS principal)** y de su **Secondary DNS Server (Servidor DNS secundario)**.
4. En la pestaña NTP, escriba la dirección IP del **NTP Server (Servidor NTP)**.
5. Haga clic en **OK (Aceptar)**.
6. **Commit (Confirmar)** los cambios realizados en Panorama.

Configuración de definición de servicio en Panorama

Una definición de servicio le permite registrar el cortafuegos VM-Series como servicio de seguridad asociado en NSX-T Manager. La definición del servicio debe incluir el grupo de dispositivos, una pila de plantillas y una URL de OVF.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | (Optional) Configure un grupo de notificación

Cree un grupo de notificación especificando los grupos de dispositivos a los que se debe notificar sobre los cambios en el entorno virtual. Los cortafuegos incluidos en los grupos de dispositivos especificados reciben directamente una actualización en tiempo real de los grupos de dispositivos y direcciones IP de VM invitados. Los cortafuegos usan esta actualización para determinar la lista más actual que constituye los grupos de direcciones dinámicas a los que se hace referencia en la política.

1. Seleccione **Panorama** > **VMware** > **Grupo de notificación** y haga clic **Añadir**.
2. Dele al grupo de aplicaciones un **Name (Nombre)** descriptivo.
3. Seleccione las casillas de los grupos de dispositivos a los que se debe notificar acerca de los cambios en el entorno virtual. Si no está disponible la casilla de verificación para un grupo de dispositivos, esto significa que el grupo de dispositivos está automáticamente incluido en virtud de la jerarquía del grupo de dispositivos.
4. Haga clic en **OK (Aceptar)**.

STEP 2 | Añada una nueva definición de servicio.

Puede crear hasta 32 definiciones de servicio en Panorama.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Definitions (Definiciones de servicio)**.
2. Seleccione **Add (Añadir)** para crear una nueva definición de servicio.
3. Introduzca un nombre descriptivo en **Name (Nombre)** para su definición de servicio.
4. (Opcional Añada una **Description (Descripción)** que identifique la función o finalidad de los cortafuegos VM-Series que se implementarán usando esta definición de servicio.

STEP 3 | Asigne un grupo de dispositivos y una pila de plantillas a la definición de servicio.

Asegúrese de Creación de plantillas y grupos de dispositivos en Panorama.

Como los cortafuegos implementados en esta solución se administran centralmente desde Panorama, debe especificar el **Device Group (Grupo de dispositivos)** y la **Template Stack (Pila de plantillas)** a los que pertenecen los cortafuegos. Todos los cortafuegos que se implementan usando esta definición de servicio pertenecen a la pila de plantillas y el grupo de dispositivos especificados.

1. Seleccione el grupo de dispositivos o jerarquía de grupo de dispositivos en la lista desplegable **Device Group (Grupo de dispositivos)**.
2. Seleccione la pila de plantillas en la lista desplegable **Template (Plantilla)**.

No se puede reutilizar una pila de plantillas o grupo de dispositivos asignados a una definición de servicio en otra definición de servicio.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Especifique la ubicación del archivo OVF.

Descargue el archivo zip, descomprímalo para extraer y guardar los archivos .ovf, mf y .vmdk en el mismo directorio. Los archivos ovf y vmdk se usan para implementar cada instancia del cortafuego.

No cambie la ruta de acceso OVF de la definición de servicio de Panorama después de una implementación correcta de servicio NSX de cortafuegos de VM-Series. Cambiar la ruta de OVF, después de una implementación correcta del cortafuegos VM-Series, puede provocar un error en el estado de la implementación del servicio NSX. Puede resolver este error en NSX-T Manager, sin embargo, esto puede hacer que todos los cortafuegos VM-Series se vuelvan a implementar.

En **OVF URL (URL de OVF)**, añada la ubicación del servidor web que aloja el archivo ovf. Tanto http como https son protocolos admitidos.

Puede usar la misma versión de ovf o diferentes versiones en las definiciones de servicio. El uso de diferentes versiones de ovf en las definiciones de servicio le permite variar la versión de PAN-OS en los cortafuegos VM-Series en diferentes clústeres ESXi.

STEP 5 | (Opcional) Seleccione un **Grupo de notificación**.

STEP 6 | Seleccione **Este Oeste** como el **Tipo de inserción** para su cortafuegos.

STEP 7 | (Opcional) **Habilitar Comprobación de estado**.

La comprobación de estado está habilitada de forma predeterminada. También llamada comprobación de estado del servicio, esta función de NSX-T le permite simular alta disponibilidad en caso de que falle una instancia del servicio. Cuando se configura con el cortafuegos VM-Series, si falla una instancia de servicio VM-Series, cualquier tráfico dirigido a ese cortafuegos se redirige a otra instancia de cortafuegos en el clúster (para implementaciones de clúster de servicio) o una instancia de cortafuegos en otro host (para implementaciones basadas en host).

No es posible deshabilitar o habilitar la comprobación de estado en una definición de servicio después de confirmar e implementar cortafuegos VM-Series en NSX-T. Intentar confirmar un cambio en la configuración de Comprobación de estado devuelve un error de confirmación. Para cambiar esto, debe eliminar y volver a crear su definición de servicio y volver a implementar sus cortafuegos VM-Series.

STEP 8 | Para recuperar automáticamente un certificado de dispositivo cuando NSX Manager implementa el cortafuegos Series-VM, configure el certificado del dispositivo.

Habilite esta opción para aplicar un certificado de dispositivo a los cortafuegos VM-Series recién implementados. Utilice esta opción únicamente cuando implemente el cortafuegos con un OVF de imagen base compatible con certificados de dispositivo. Panorama envía la información del certificado del dispositivo a NSX Manager como parte de la definición del servicio. Cuando se implementa

 ©2024 Palo Alto Networks, Inc.

un nuevo cortafuegos en NSX, el certificado del dispositivo se instala en el cortafuegos durante el arranque.

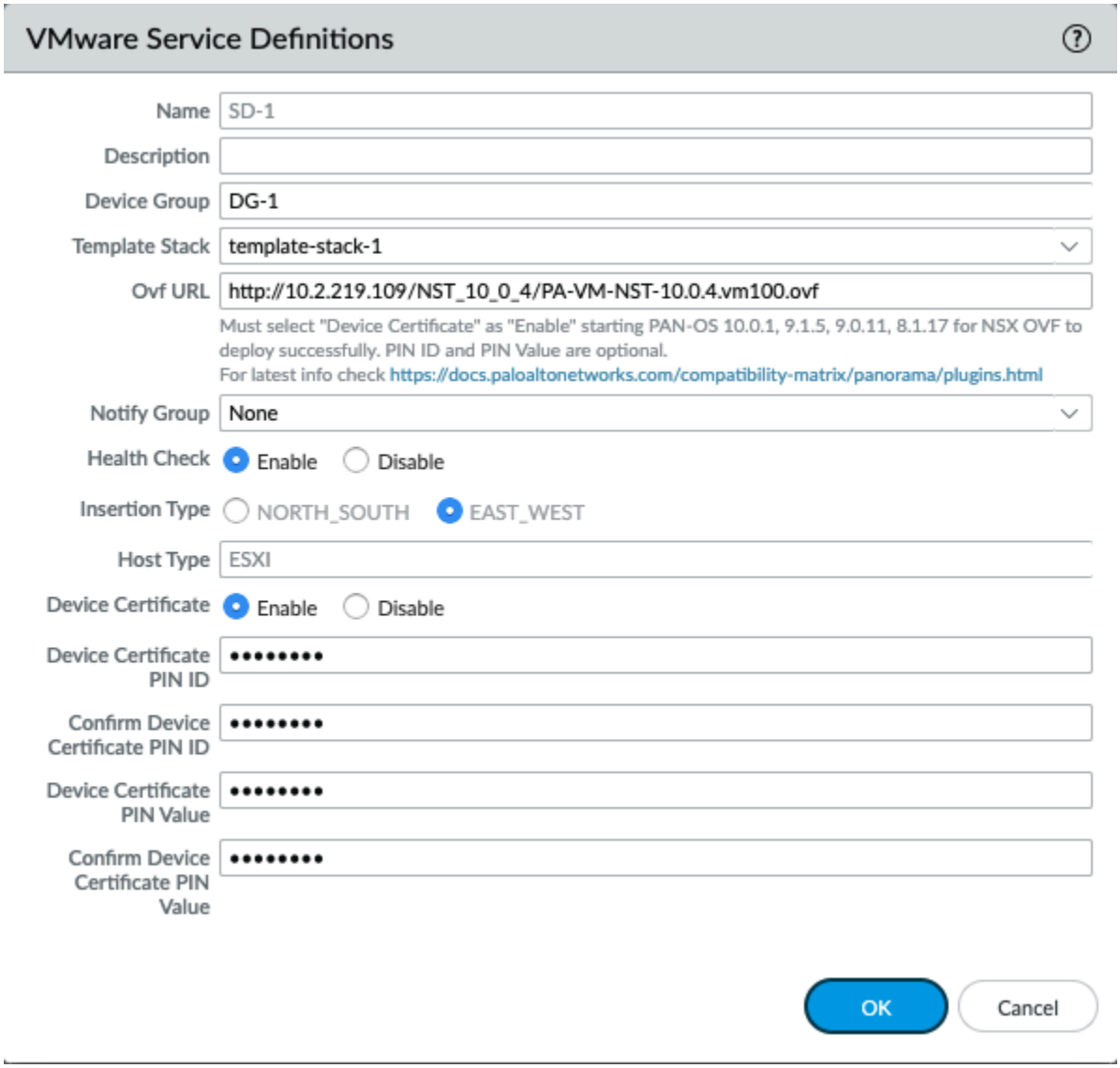
Para obtener una lista de OVF que admiten certificados de dispositivo para el cortafuegos VM-Series en VMware NSX, consulte la Matriz de compatibilidad de Palo Alto Networks.

Si su OVF admite un certificado de dispositivo, debe Habilitar certificados de dispositivo independientemente de si está utilizando o no un certificado de dispositivo. Si su OVF no admite un certificado de dispositivo, desactive esta opción.

1. Si aún no lo ha hecho, inicie sesión en el Portal de atención al cliente y genere un PIN de registro y un ID de PIN.
2. En **Device Certificate (Certificado de dispositivo)**, haga clic en **Enable (Habilitar)**.
3. Copie el ID de PIN e introdúzcalo en el campo **Device Certificate PIN ID (ID de PIN de certificado de dispositivo)**.
4. Vuelva a introducir el ID de PIN en el campo **Confirm Device Certificate PIN ID (Confirmar ID de PIN del certificado de dispositivo)**.
5. Copie el valor de PIN e introdúzcalo en el campo **Device Certificate PIN Value (Valor de PIN del certificado de dispositivo)**.
6. Vuelva a introducir el valor del PIN en el campo **Confirm Device Certificate PIN Value (Confirmar el valor del PIN del certificado de dispositivo)**.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Haga clic en **OK (Aceptar)** para guardar la definición de servicio.

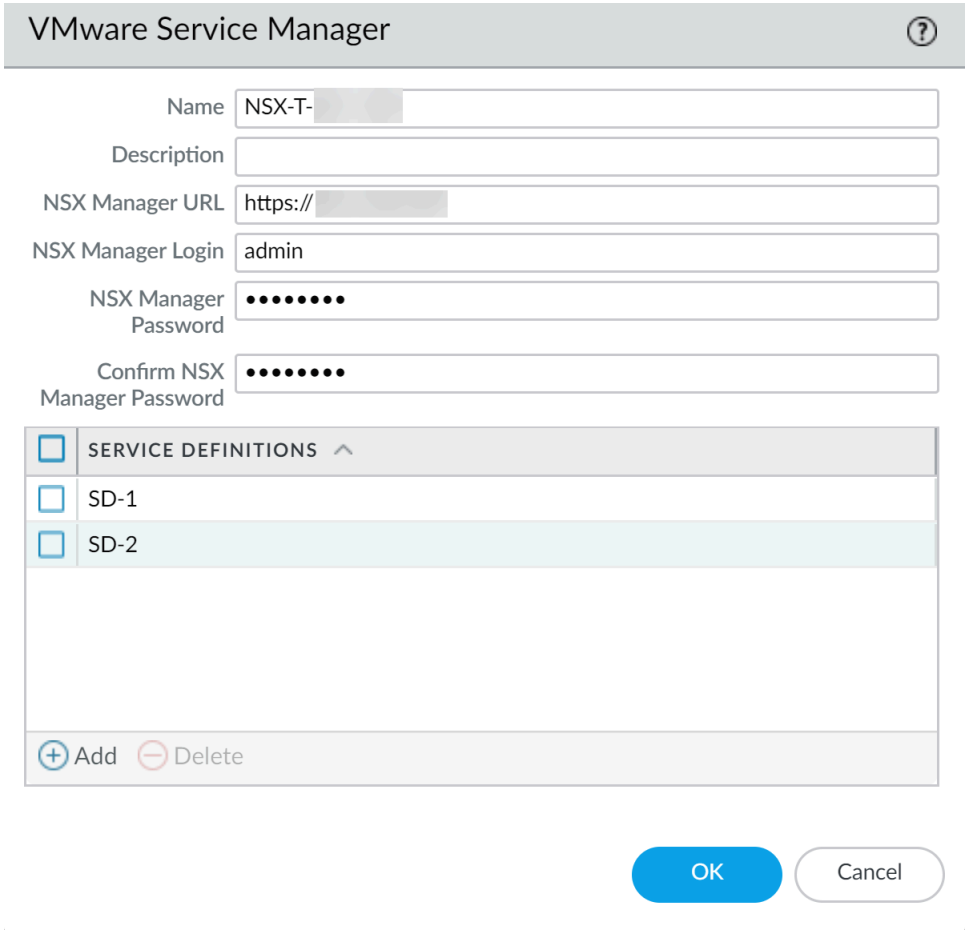


 ©2024 Palo Alto Networks, Inc.

STEP 10 | Adjunte la definición del servicio al gestor del servicio.

No es posible usar una definición de servicio en más de un administrador de servicios.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Manager (Administrador de Servicio)** y haga clic en el enlace del nombre del administrador del servicio.
2. En Definiciones del servicio, haga clic en **Add (Añadir)** y seleccione su definición de servicio del menú desplegable.
3. Haga clic en **OK (Aceptar)**.



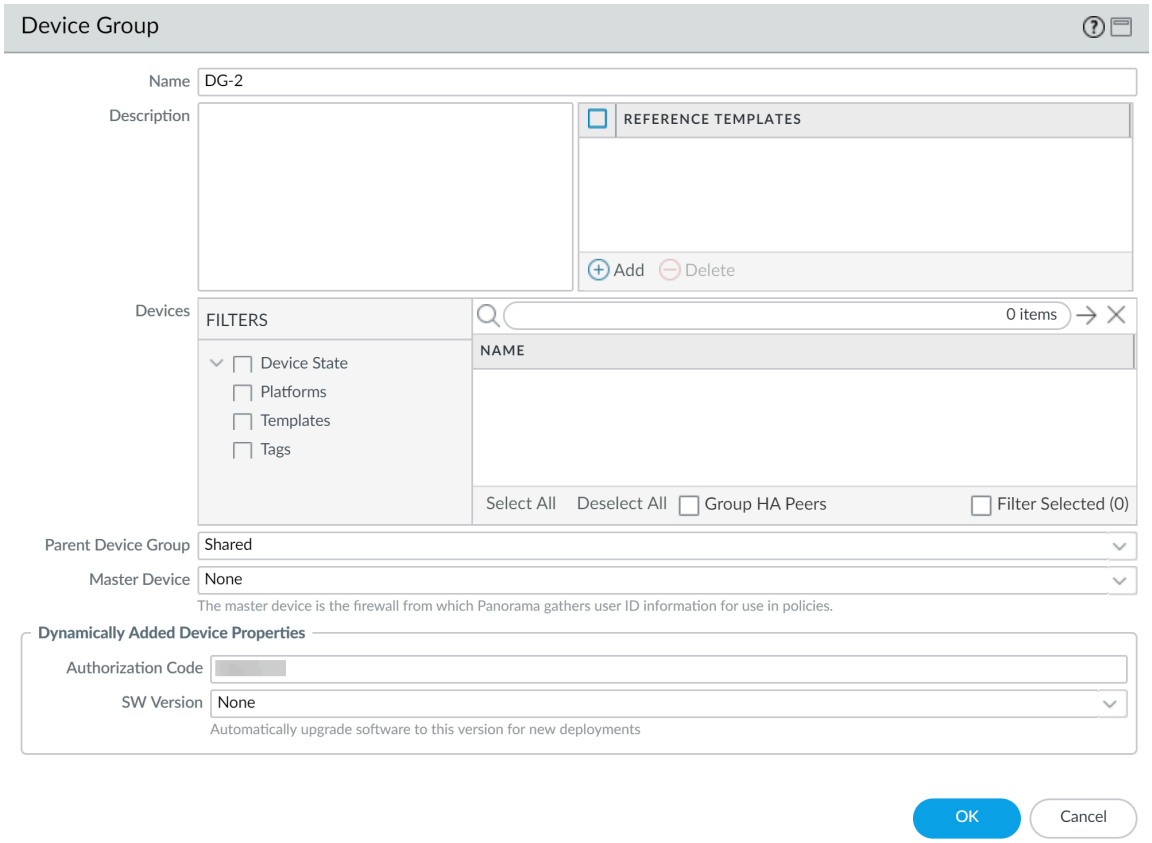
 ©2024 Palo Alto Networks, Inc.

STEP 11 | Añada el código de autorización para activar la licencias de los cortafuegos.

1. Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)** y elija el grupo de dispositivos al que se asoció con la definición del servicio que acaba de crear.
2. En **Propiedades de dispositivo añadidas dinámicamente**, añada el código de autorización que recibió con el correo electrónico de cumplimiento de su pedido y, opcionalmente, seleccione Ninguno en el menú desplegable **Versión de SW**.

   Cuando se implementa un nuevo cortafuegos en NSX-T, este se añade automáticamente al grupo de dispositivos, se proporciona una licencia con el código de autorización que proporcionó y se actualiza a la versión de PAN-OS que especificó.

   En el portal de asistencia técnica, puede visualizar el número total de cortafuegos que está autorizado a implementar y la proporción del número de licencias que se han usado del número total de licencias que le ofrece su código de autorización.



STEP 12 | **Commit to Panorama (Confirmar en Panorama)**.

 ©2024 Palo Alto Networks, Inc.

STEP 13 | En NSX-T Manager, verifique que la definición de servicio esté disponible.

Seleccione **System (Sistema)** > **Service Deployments (Implementaciones de servicios)** > **Catalog (Catálogo)**. La definición de servicio aparece como instancia de servicio en NSX-T Manager.

Iniciar el cortafuegos VM-Series en NSX-T (este-oeste)

Complete el siguiente procedimiento para implementar el cortafuegos VM-Series como un servicio en su entorno NSX-T. Los campos **Deployment Specification (Especificación de implementación)** y **Deployment Template (Plantilla de implementación)** se rellenan automáticamente con información enviada desde Panorama como parte de la definición del servicio.

No edite ningún ajuste en Atributos de implementación. Estos valores se importan de Panorama y cambiarlos hace que falle la implementación.

STEP 1 | Inicie sesión en NSX-T Manager.

STEP 2 | Seleccione **System (Sistema)** > **Service Deployments (Implementaciones de servicios)** > **Deployment (Implementación)**.

STEP 3 | Seleccione su definición de servicio del menú desplegable **Partner Service (Servicio de socios)**.

STEP 4 | Haga clic en **Deploy Service (Implementar servicio)**.

STEP 5 | Introduzca un nombre descriptivo en **Name (Nombre)** para su implementación de servicio.

STEP 6 | Seleccione el **Compute Manager (Gestor de cálculo)** (vCenter).

STEP 7 | Seleccione un **Deployment Type (Tipo de implementación)**: **Clustered (En clúster)** o **Host Based (Basado en host)**.

STEP 8 | Si seleccionó **Clustered (En clúster)** como **Deployment Type (Tipo de implementación)**, introduzca el **Clustered Deployment Count (Recuento de implementación en clúster)** para especificar el número de instancias de cortafuegos VM-Series que se van a implementar en el clúster.

STEP 9 | Seleccione un **Host** si va a iniciar VM-Series en una implementación en clúster. Seleccione un host específico del menú desplegable **Host** o **Any (Cualquiera)** para permitir que NSX-T Manager seleccione el host. Esta opción aparece atenuada en las implementaciones **Host Based (Basadas en host)**.

STEP 10 | Seleccione un **Data Store (Almacén de datos)** como repositorio para el cortafuegos VM-Series. En una implementación en clúster, seleccione un almacén de datos compartido si selecciona **Any (Cualquiera)** para el host, o seleccione un almacén de datos local si especificó un host en particular.

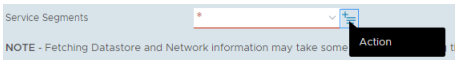
 ©2024 Palo Alto Networks, Inc.

STEP 11 | Configure los ajustes de **Networks (Redes)**.

1. En la columna Redes, haga clic en **Set (Establecer)**.
2. Seleccione la **Network (Red)** para **eth0 - Management Nic**.
3. Seleccione el **Network Type (Tipo de red)**: DHCP o grupo de IP estática. Si elige Grupo de IP estática, seleccione un **IP Pool (Grupo de IP)**.
4. Marque **eth1 - Data-1 Nic**.
5. Compruebe que ambas interfaces están marcadas.
6. Haga clic en **Save (Guardar)**.

STEP 12 | Seleccione o configure un **Service Segment (Segmento de servicio)**. Para configurar un segmento de servicio, complete el siguiente procedimiento.

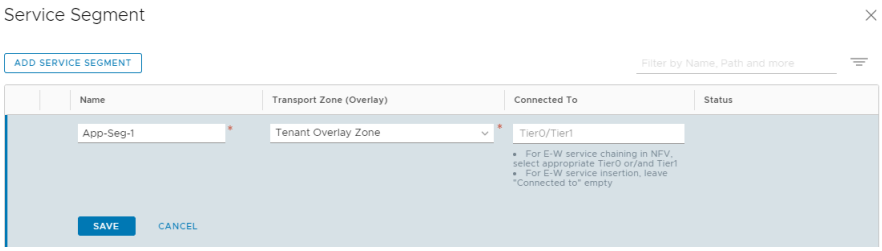
1. Haga clic en **Action (Acción)** en la columna **Service Segments (Segmentos de servicio)**.



2. Haga clic en **Add Service Segment (Añadir segmento de servicio)**.
3. Introduzca un **Name (Nombre)** descriptivo.
4. Seleccione una **Transport Zone (Overlay) [Zona de transporte (superposición)]**.

   El cortafuegos VM-Series debe estar conectado a una zona de transporte superpuesta. Las máquinas virtuales invitadas se pueden adjuntar a una VLAN o a una zona de transporte superpuesta. El nodo de transporte que aloja las máquinas virtuales invitadas y la VM-Series debe configurarse con una zona de transporte superpuesta.

5. Haga clic en **Save (Guardar)** y **Close (Cerrar)**.



STEP 13 | Seleccione el **Cluster (Clúster)** donde se implementará el servicio. Debe seleccionar un clúster con **NSX Configuration (Configuración NSX)**.

STEP 14 | Haga clic en **Save (Guardar)**.

STEP 15 | Verifique que sus cortafuegos se hayan implementado correctamente.

1. Seleccione **System (Sistema)** > **Service Deployments (Implementaciones de servicio)** > **Service Instances (Instancias de servicio)**.
2. Confirme que sus cortafuegos estén en la lista y que el **Deployment Status (Estado de implementación)** muestra **Up (Activo)**.

 ©2024 Palo Alto Networks, Inc.

STEP 16 | Compruebe que sus cortafuegos están conectados a Panorama.

1. Inicie sesión en Panorama.
2. Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**.
3. Confirme que sus cortafuegos figuran en el grupo de dispositivos correcto y que el **Device State (Estado del dispositivo)** muestra **Connected (Conectado)**.

   El nombre del dispositivo para el cortafuegos VM-Series se muestra en Panorama como **PA-VM:** <nsx.clusterid>para la implementación de NSX-T (N-S) y como **PA-VM:** <nsx.servicevmid>para la implementación de NSX-T (E-W).

STEP 17 | Establezca una contraseña segura para la cuenta de administrador en sus cortafuegos VM-Series.

Cada cortafuegos VM-Series utiliza un nombre de usuario y una contraseña predeterminados (admin/admin), que se utilizan para el inicio de sesión inicial. Al iniciar sesión por primera vez, se le solicitará que establezca una contraseña nueva y más segura. La nueva contraseña debe tener un mínimo de ocho caracteres e incluir un mínimo de un carácter en minúsculas y otro en mayúsculas, así como un número y un carácter especial.

Puede actualizar la contraseña en cada cortafuegos de forma individual o todos a la vez a través de Panorama.

- **Panorama**: en Panorama, puede cambiar la contraseña predeterminada para todos los cortafuegos en una plantilla o eliminar el usuario administrador y crear un nuevo nombre de usuario y contraseña.
  1. Iniciar sesión en Panorama
  2. Seleccione **Device (Dispositivo)** > **Administrators (Administradores)** y seleccione el usuario **admin**.
  3. **Delete (Eliminar)** el usuario o haga clic en el usuario e introduzca una nueva contraseña.
  4. Si cambió la contraseña, haga clic en **OK (Aceptar)**.
  5. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** > **Edit Selections (Editar selecciones)** > **Force Template Values (Forzar valores de plantilla)**.
  6. Haga clic en **OK (Aceptar)**.
- **Cortafuegos**: este procedimiento debe repetirse en cada cortafuegos VM-Series.
  1. Inicie sesión en el cortafuegos VM-series utilizando el nombre de usuario y la contraseña predeterminados.
  2. Siga las indicaciones para restablecer la contraseña.

Crear grupos de direcciones dinámicas

Un grupo de seguridad es un contenedor lógico que reúne invitados en múltiples hosts ESXi del clúster. Cuando crea un grupo de direcciones dinámicas que cumple con los criterios correctos y confirma los cambios, se crea un grupo de seguridad correspondiente en el NSX-T Manager. La creación de grupos de seguridad es necesaria para gestionar y proteger a los invitados.

Para que un grupo de direcciones dinámicas se convierta en un grupo de seguridad en NSX-T, debe añadir criterios de coincidencia en el grupo de direcciones dinámicas con el siguiente formato: **`'_nsxt_<dynamic-address-group-name>'`**. El nombre de dirección dinámica añadido en los criterios de coincidencia debe coincidir exactamente con el nombre del grupo de direcciones

 ©2024 Palo Alto Networks, Inc.

dinámicas. Por ejemplo, un grupo de direcciones dinámicas llamado **aplicaciones** debe incluir criterios de coincidencia **`'_nsxt_applications'`**. Además, debe incluir el grupo de direcciones dinámicas en un grupo de dispositivos en una definición de servicio, que forma parte de un administrador de servicios y está confirmado.

Cada grupo de seguridad creado a partir de un grupo de direcciones dinámico tiene el siguiente formato: **`<service-def-name>_<dynamic-address-group-name>`**. Por ejemplo, **`ServiceDef1_applications`**.



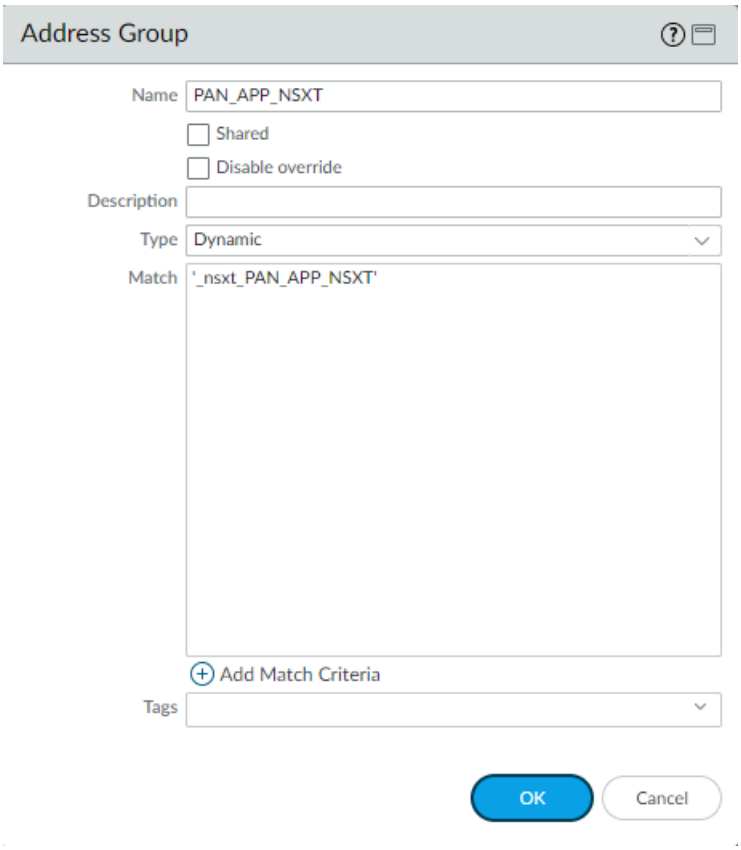
Cada grupo de direcciones dinámicas que cree debe tener un nombre único en cada grupo de dispositivos configurado en su Panorama.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Configure un grupo de direcciones dinámicas para cada grupo de seguridad requerido para su implementación.

1. Seleccione **Objects (Objetos)** > **Address Groups (Grupos de direcciones)**.
2. Compruebe que está configurando los grupos de direcciones dinámicas en un grupo de dispositivos asociado con una definición de servicio NSX-T.
3. Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** y una **Description (Descripción)** para el grupo de direcciones.
4. Defina el **Type (Tipo)** como **Dynamic (Dinámico)**.
5. Defina los criterios de coincidencia.

   Para que el grupo de direcciones dinámicas se convierta en un grupo de seguridad en NSX-T Manager, la cadena de criterios de coincidencia debe estar entre comillas simples con el prefijo _nsx_ seguido del nombre exacto del Security Group (Grupo de direcciones). Por ejemplo, ***'_nsxt_PAN_APP_NSX'****.*
6. Repita este proceso para cada grupo de seguridad que necesite.



STEP 2 | **Commit (Confirmar)** los cambios.

Crear políticas de seguridad

Cree reglas de política de seguridad que se utilizarán para generar automáticamente las reglas de dirección utilizadas en la política de dirección.

Cuando Genere reglas de dirección, tendrá la opción de generar reglas de dirección basadas en reglas previas, reglas posteriores o todas. Si selecciona Todo, el complemento de VMware para NSX crea una

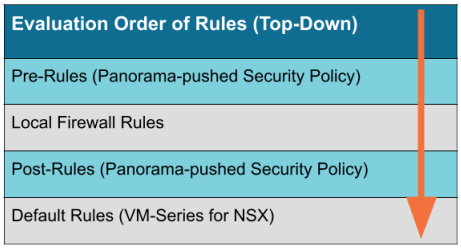
 ©2024 Palo Alto Networks, Inc.

regla de dirección para cada seguridad aplicable en las reglas anteriores y posteriores. Esto puede resultar en la creación de reglas de dirección innecesarias y dificultar la gestión de las reglas. Para ayudar a separar fácilmente sus reglas de dirección de sus reglas de seguridad, puede crear sus reglas de dirección como reglas posteriores y las reglas de seguridad como reglas anteriores.

Para generar automáticamente una regla de dirección basada en reglas de seguridad creadas en Panorama, la regla de seguridad debe cumplir con los siguientes criterios:

- Pertenecer a un grupo de dispositivos principal o secundario registrados con un Administrador de servicios NSX.
- Ser en una política de intrazona e incluir solo una zona.
- No incluye un grupo de direcciones estáticas, un rango de IP ni una máscara de red configurada para la regla.

Cuando se decida dónde definir las reglas de dirección de NSX-T en Panorama (antes o después de la base de reglas), hay que tener en cuenta el número de reglas de política de seguridad y reglas de dirección de NSX-T que creará en Panorama y el orden en el que se aplican las reglas al tráfico. Las reglas previas se aplican al tráfico antes que las reglas posteriores.



- Reglas previas: puede usar la base de reglas previas de Panorama para definir las reglas de dirección de NSX-T y las reglas de la política de seguridad del cortafuegos VM-Series. Si define las reglas de seguridad y las reglas de dirección en la misma base de reglas, debe considerar el orden de las reglas de seguridad en relación con las reglas de dirección. Cuando tiene una base de reglas grande, que incluye tanto reglas de dirección como reglas de política de seguridad, puede resultar difícil gestionar ambos tipos de reglas a medida que amplía.
- Reglas posteriores: separar las reglas de la política de seguridad que se usan para la inspección y el cumplimiento de las reglas de seguridad que se usan para generar reglas de dirección de NSX-T puede ayudarle a ampliar la implementación con una gran número de reglas. Cuando genera automáticamente sus reglas de dirección, el complemento genera una regla de dirección para cada regla en la base de reglas especificada que cumple con los criterios necesarios. Por lo tanto, al separar los dos tipos de reglas, puede evitar la generación involuntaria de reglas de dirección dudosas. Se recomienda el uso de la base de reglas de publicación para las reglas de dirección; especialmente en implementaciones con grandes cantidades de reglas de política de seguridad.

Los grupos de direcciones dinámicas de origen y destino que especifica en la regla de seguridad. Cuando genera automáticamente una regla de dirección, el lugar donde se aplica la regla (cortafuegos distribuido de NSX-T o Grupo de seguridad) depende del origen y el destino que especificó al configurar la regla de seguridad. Si ha seleccionado alguno para el origen o el destino, NSX-T Manager aplica la regla de dirección al cortafuegos distribuido. Si selecciona un grupo de direcciones dinámicas para el origen y el destino, la dirección se aplica a las VM invitadas en esos grupos de seguridad. Si crea reglas de dirección manualmente, puede especificar los grupos de seguridad donde se aplicará la regla de dirección.

Asegúrese de que la política de seguridad que se utiliza para definir las reglas de dirección no incluya grupos de direcciones dinámicas configurados como parte de un flujo de trabajo de implementación

 ©2024 Palo Alto Networks, Inc.

basado en las operaciones. Si lo hace, el origen y el destino de las reglas de dirección se enviarán a NSX-T Manager como origen-cualquiera y destino-cualquiera. Esto podría afectar el tráfico en su entorno NSX-T.

Si deshabilita una regla de seguridad que utilizará para generar automáticamente una regla de dirección, la regla de dirección también se deshabilitará.

- Utilice la base de reglas anterior para definir las reglas de dirección de NSX-T
- Utilice la base de reglas posterior para definir las reglas de dirección de NSX-T
- Aplicación de políticas de seguridad al cortafuegos VM-Series en NSX-T (este-oeste)

Utilice la base de reglas anterior para definir las reglas de dirección de NSX-T

El siguiente procedimiento describe cómo crear las reglas de la política de seguridad que se utilizarán para generar las reglas de dirección de NSX-T, y cómo crear la política de seguridad que Panorama enviará al cortafuegos VM-Series para la inspección y aplicación del tráfico.

no aplique las políticas de redireccionamiento de tráfico a no ser que comprenda el funcionamiento de las reglas en NSX-T Manager, así como en el cortafuegos VM-Series y Panorama. La política predeterminada en el cortafuegos VM-Series se define como *denegar todo* el tráfico, lo que significa que todo el tráfico que se redireccione al cortafuegos VM-Series será descartado.

Cree reglas de política de seguridad en el grupo de dispositivos asociado. Para cada regla de seguridad, establezca el Rule Type (Tipo de regla) en Intrazone (Intrazona), seleccione una zona en la pila de plantillas asociada y seleccione los grupos de direcciones dinámicas como origen y destino. La creación de una política de seguridad apta en Panorama ayuda a crear una regla de dirección correspondiente en NSX-T Manager, una vez que se genere la regla de dirección y se confirme en Panorama.

STEP 1 | En Panorama, seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Pre Rules (Pre reglas)**.

STEP 2 | Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** y **Description (Descripción)**para la regla de políticas de seguridad.

STEP 3 | Compruebe que está configurando las reglas de seguridad en un grupo de dispositivos asociado con una definición de servicio NSX-T.

STEP 4 | Establezca el tipo de regla en **intrazone (Devices with PAN-OS 6.1 or later) [intrazona (dispositivos con PAN-OS 6.1 o posterior)]**.

STEP 5 | En la pestaña Source (Origen), configure la zona de origen en la zona desde la pila de plantillas asociada a la definición del servicio. Luego, seleccione un grupo de direcciones dinámicas (grupo de seguridad NSX-T) que creó anteriormente como Source Address (Dirección de origen). No añada ningún grupo de direcciones estáticas, rangos de IP o máscaras de red como una Dirección de origen.

STEP 6 | En la pestaña Destination (Destino), Panorama no le permite establecer una zona de destino porque establece el tipo de regla en intrazona. A continuación, seleccione un grupo de direcciones dinámicas (grupo de seguridad NSX-T) que creó anteriormente como Destination Address (Dirección de destino). No agregue ningún grupo de direcciones estáticas, rangos de IP o máscaras de red como una Dirección de destino.

STEP 7 | Haga clic en **OK (Aceptar)**.

STEP 8 | Repita los pasos 1 a 7 para cada regla de dirección que necesite.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | **Commit (Confirmar)** los cambios.

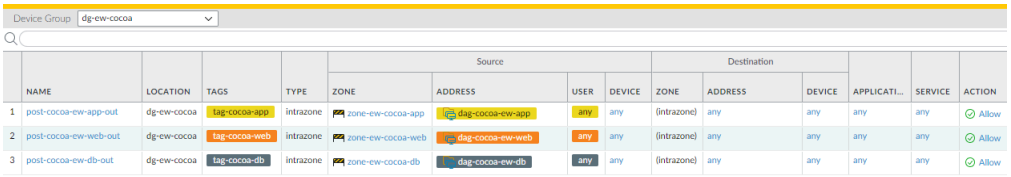
STEP 10 | Aplicación de políticas de seguridad al cortafuegos VM-Series en NSX-T (este-oeste).

Utilice la base de reglas posterior para definir las reglas de dirección de NSX-T

Cree reglas de políticas de seguridad en la base de reglas posterior para definir las reglas de dirección de NSX-T.

STEP 1 | Cree Reglas de política de seguridad.

1. En Panorama, seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Post Rules (Reglas posteriores)**.
2. Compruebe que está configurando las Reglas de la política de seguridad en un grupo de dispositivos asociado con una definición de servicio NSX-T.
3. Haga clic en el nombre de una Regla de política de seguridad para editarla.
4. Establezca el tipo de regla en **intrazone (Devices with PAN-OS 6.1 or later) [intrazona (dispositivos con PAN-OS 6.1 o posterior)]**.
5. En la pestaña Source (Origen), configure la zona de origen en la zona desde la pila de plantillas asociada a la definición del servicio. Luego, seleccione un grupo de direcciones dinámicas que creó anteriormente como la Dirección de origen. No añada ningún grupo de direcciones estáticas, rangos de IP o máscaras de red como una Dirección de origen.
6. En la pestaña Destination (Destino), Panorama no le permite establecer una zona de destino porque establece el tipo de regla en intrazona. A continuación, seleccione un grupo de direcciones dinámicas que creó anteriormente como Destination Address (Dirección de destino). No agregue ningún grupo de direcciones estáticas, rangos de IP o máscaras de red como una Dirección de destino.
7. Haga clic en **OK (Aceptar)**.
8. Repita los pasos 1 a 7 para cada regla de dirección que necesite.



STEP 2 | **Commit (Confirmar)** los cambios realizados en Panorama.

STEP 3 | Aplique reglas de política de seguridad al cortafuegos NSX-T EW SEC Centric Firewall de la serie VM-Series.

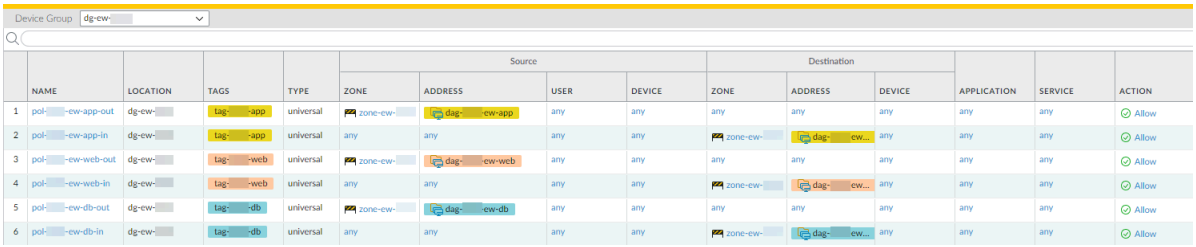
Aplicación de políticas de seguridad al cortafuegos VM-Series en NSX-T (este-oeste)

Ahora que ha definido las reglas de dirección, ahora puede usar Panorama para gestionar de forma centralizada las directivas en los cortafuegos VM-Series.

Para gestionar políticas centralizadas, adjunte el grupo de direcciones dinámicas como una dirección de origen o destino en la política de seguridad y envíelo a los cortafuegos; los cortafuegos puede recuperar dinámicamente las direcciones IP de las máquinas virtuales que se incluyen en cada grupo de seguridad para garantizar que el tráfico que se origina o se dirige a las máquinas virtuales del grupo especificado cumple los requisitos.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Cree las reglas de política de seguridad.



1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Prerules (Pre reglas)**.
2. Seleccione el **Grupo de dispositivos** que creó para gestionar los cortafuegos VM-Series en NSX-T en Creación de plantillas y grupos de dispositivos en Panorama.
3. Haga clic en **Add (Añadir)** e introduzca **Name (Nombre)** y **Description (Descripción)** para la regla. En este ejemplo la regla de seguridad permite todo el tráfico entre los servidores WebFrontEnd y de aplicaciones.
4. Seleccione la **Source Zone (Zona de origen)** y **Destination Zone (Zona de destino)**. El nombre de la zona debe ser el mismo en ambas columnas.
5. En **Source Address (Dirección de origen)** y **Destination Address (Dirección de destino)**, seleccione o escriba una dirección, grupo de direcciones o región. En este ejemplo, seleccionamos un grupo de direcciones, el grupo de direcciones dinámicas que creó anteriormente.
6. Seleccione la **Application (Aplicación)** que desea permitir. En este ejemplo hemos creado un **Application Group (Grupo de aplicaciones)** que incluye un grupo estático de aplicaciones específicas que se agrupan juntas.
   1. Haga clic en **Add (Añadir)** y seleccione **New Application Group (Nuevo grupo de aplicaciones)**.
   2. Haga clic en **Add (Añadir)** para seleccionar la aplicación que desea añadir al grupo.
   3. Haga clic en **OK (Aceptar)** para crear el grupo de aplicaciones.
7. Especifique la acción, **Allow (Permitir)** o **Deny (Denegar)**, para el tráfico y, opcionalmente, adjunte los perfiles de seguridad predeterminados para los antivirus, anti-spyware y protección contra vulnerabilidades en Profiles (Perfiles).
8. Repita los pasos anteriores para crear las reglas de políticas pertinentes.
9. Haga clic en **Commit (Confirmar)** y seleccione Commit Type (Tipo de confirmación) como **Panorama**. Haga clic en **OK (Aceptar)**.

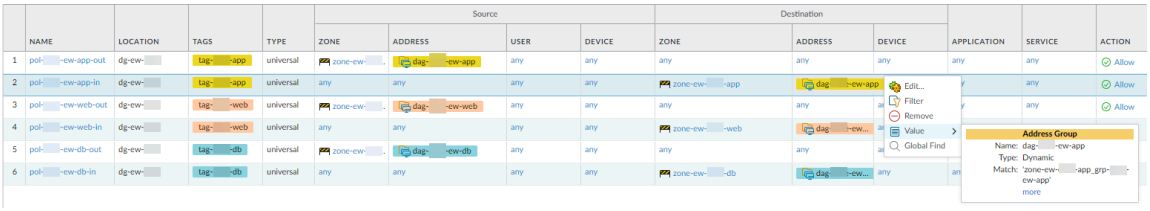
STEP 2 | Aplique las políticas a los cortafuegos VM-Series para NSX-T.

1. Haga clic en **Commit (Confirmar)** y seleccione Commit Type (Tipo de confirmación) como **Device Groups (Grupos de dispositivos)**.
2. Seleccione el grupo de dispositivos, que en este ejemplo es Grupo de dispositivos NSX-T, y haga clic en **Aceptar**.
3. Verifique que la confirmación se realice correctamente.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Valide que los miembros del grupo de direcciones dinámicas se cumplimentan en el cortafuegos VM-Series.

1. En Panorama, cambie el contexto del dispositivo para iniciar la interfaz web del cortafuegos al que envió las políticas.
2. En el cortafuegos VM-Series, seleccione **Policies (Políticas)** > **Security (Seguridad)** y elija una regla.
3. Seleccione la flecha desplegable junto al vínculo del grupo de direcciones y seleccione **Inspect (Inspeccionar)**. También puede comprobar si los criterios de coincidencia son precisos.



4. Haga clic en el vínculo **more (más)** y compruebe que se muestra la lista de direcciones IP registradas.

   La política entra en vigor para todas las direcciones IP que pertenecen a este grupo de direcciones y se muestra aquí.

STEP 4 | (Opcional) Use la plantilla para enviar una configuración base para la configuración de red y dispositivo como, por ejemplo servidor DNS, servidor NTP, servidor Syslog y pancarta de inicio de sesión.

Si desea más información sobre el uso de plantillas, consulte la Guía del administrador de Panorama.

STEP 5 | Cree un perfil de protección de zona y adjúntelo a una zona.

Un perfil de protección de la zona ofrece protección contra desbordamientos y posee la capacidad de proteger contra el análisis de puertos, los barridos de puertos y los ataques basados en paquetes. Le permite proteger el tráfico intraniveles e interniveles entre máquinas virtuales dentro de su centro de datos y el tráfico desde Internet destinado a las máquinas virtuales (cargas de trabajo) en su centro de datos.

1. Seleccione **Template (Plantilla)**.
2. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** para añadir y configurar un nuevo perfil.
3. Seleccione **Network (Red)** > **Zones (Zonas)**, haga clic en la zona predeterminada de la lista y seleccione el perfil en el menú desplegable **Zone Protection Profile (Perfil de protección de zona)**.

STEP 6 | Cree un perfil de protección DoS y adjúntelo a la regla de políticas Protección DoS .

1. Seleccione su **Device Group (Grupo de dispositivos)**.
2. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **DoS Protection (Protección DoS)** para añadir y configurar un nuevo perfil.
   - Un perfil clasificado permite la creación de un umbral que se aplica a una IP de origen única. Por ejemplo, puede configurar una calificación de sesión máxima para una dirección IP que coincidió con la política, y luego bloquear esa dirección IP única una vez que se activó el umbral.

 ©2024 Palo Alto Networks, Inc.

- Un perfil agregado permite la creación de una calificación de sesión máxima para todos los paquetes que coincidan con la política. El umbral se aplica a la nueva calificación de sesión para todas las direcciones IP combinadas. Una vez que el umbral se activa, afecta todo el tráfico que coincide con la política.

3. Cree una nueva regla de la política de protección DoS**Policy (Política)** > **DoS Protection (Protección DoS)** y adjunte el nuevo perfil a esta.

Crear criterios de pertenencia a grupos de direcciones dinámicas

En NSX-T, puede configurar los criterios de pertenencia para sus máquinas virtuales y el conjunto de IP que pertenecen a un grupo de seguridad de NSX-T (grupo de direcciones dinámicas) en el complemento de Panorama para NSX. Para cada grupo de direcciones dinámicas, debe especificar una definición de servicio y definir hasta cinco criterios de coincidencia y cada criterio incluye hasta cinco reglas de coincidencia.

Usted crea este criterio de pertenencia en el complemento y luego lo envía a NSX-T Manager. Sin embargo, este no aplica los criterios de pertenencia a las máquinas virtuales invitadas en su implementación. Debe definir y aplicar datos de pertenencia, como etiquetas, a sus máquinas virtuales invitadas en NSX-T Manager.

Las reglas que el complemento Panorama para NSX-T identifica y clasifica las máquinas virtuales en función de dos tipos de pertenencia: máquina virtual o conjunto de IP. Las claves y operadores que se pueden utilizar con cada tipo de miembro se enumeran en la siguiente tabla.

Tipo de miembro	Clave	Operador
Conjunto de IP	Tag (Etiqueta)	Igual a
Máquina virtual	• Tag (Etiqueta) • Nombre • Nombre del SO • Nombre del equipo	• Igual a • Contiene • Comienza con • Termina con • No es igual a (no se aplica con la clave de etiqueta)

*Los cambios en los criterios de pertenencia solo deben realizarse en Panorama; no realice cambios en NSX-T Manager. Si realiza cambios en NSX-T Manager, el complemento de Panorama para VMware NSX mostrará que la definición del servicio no está sincronizada. Debe hacer clic en el enlace **Out-of-Sync (No sincronizado)** para ver el motivo específico del estado de desincronización. Si la causa es un cambio en los criterios de pertenencia, realice una sincronización de configuración haciendo clic en **NSX-T Config-Sync**.*

STEP 1 | Seleccione **Panorama** > **VMware** > **NSX-T** > **Membership Criteria (Criterios de pertenencia)** > **Add (Añadir)**.

Para agregar o modificar los criterios de pertenencia a una definición de servicio, con al menos un grupo de direcciones dinámicas, puede hacer clic en el nombre de la definición de servicio en lugar de hacer clic en **Add (Añadir)**.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | En **Name (Nombre)**, seleccione una definición de servicio para los Criterios de pertenencia. La definición de servicio seleccionada debe tener el tipo de inserción East_West y debe usarse como parte de una implementación centrada en la seguridad.

STEP 3 | Haga clic en **Add (Añadir)** para especificar un grupo de direcciones dinámicas.

STEP 4 | Seleccione un **Dynamic Address Group (Grupo de direcciones dinámicas)** del menú desplegable. El menú desplegable enumera los grupos de direcciones dinámicas asociados con la definición de servicio especificada.



La interfaz de usuario del complemento muestra grupos de direcciones dinámicas y estáticas configurados en Panorama. Tenga cuidado de no seleccionar accidentalmente un grupo de direcciones estáticas al configurar los criterios de pertenencia.

STEP 5 | Haga clic en **Add (Añadir)** para definir los criterios asociados con el grupo de direcciones dinámicas elegido.

STEP 6 | Introduzca un nombre descriptivo para los **Criteria (Criterios)**.

STEP 7 | Haga clic en **Add (Añadir)** para definir una regla.

STEP 8 | Define una regla. Puede crear hasta cinco reglas.

1. Introduzca un nombre descriptivo para la regla.
2. Seleccione el **Member Type (Tipo de miembro)**: máquina virtual o conjunto de IP.
3. Seleccione la **Key (Clave)**: etiqueta, nombre, nombre del sistema operativo, nombre del equipo.
4. Seleccione el **Operator (Operador)**: igual a, contiene, comienza con, termina con, no es igual.
5. Introduzca el **Value (Valor)**.

   Si la Clave se establece en Etiqueta, el Valor es la Etiqueta. La interfaz de usuario del complemento no enumera las etiquetas, por lo que debe usar la CLI de Panorama (con NSX-T Manager 3.0.0 y posterior).

   ```
   request plugins vmware_nsx nsx_t nsxt-tags service-definition <SD_name>
   ```

6. (Opcional) Introduzca el **Scope (Alcance)**. El alcance solo se aplica con la clave **Tag (Etiqueta)**. El alcance es un valor opcional que se aplica a una etiqueta de objeto en NSX-T. El alcance se define en NSX-T Manager. Por ejemplo, si etiqueta máquinas virtuales según el sistema

 ©2024 Palo Alto Networks, Inc.

operativo, puede crear etiquetas para Windows, Linux y MacOS, y luego establecer el alcance de cada etiqueta en SO.

Para ver las etiquetas y el alcance, use la CLI de Panorama (con NSX-T Manager 3.0.0 y posterior).

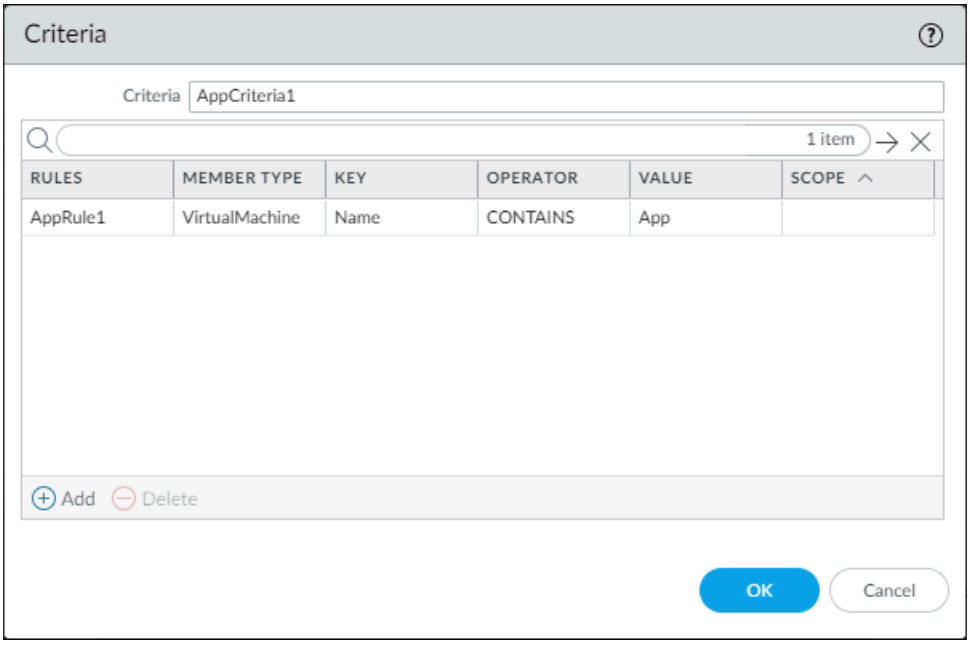
Ejecute el siguiente comando para ver la lista de etiquetas.

```
request plugins vmware_nsx nsx_t nsxt-tags service-definition <SD_name>
```

Ejecute el siguiente comando para ver el alcance asociado con la etiqueta especificada.

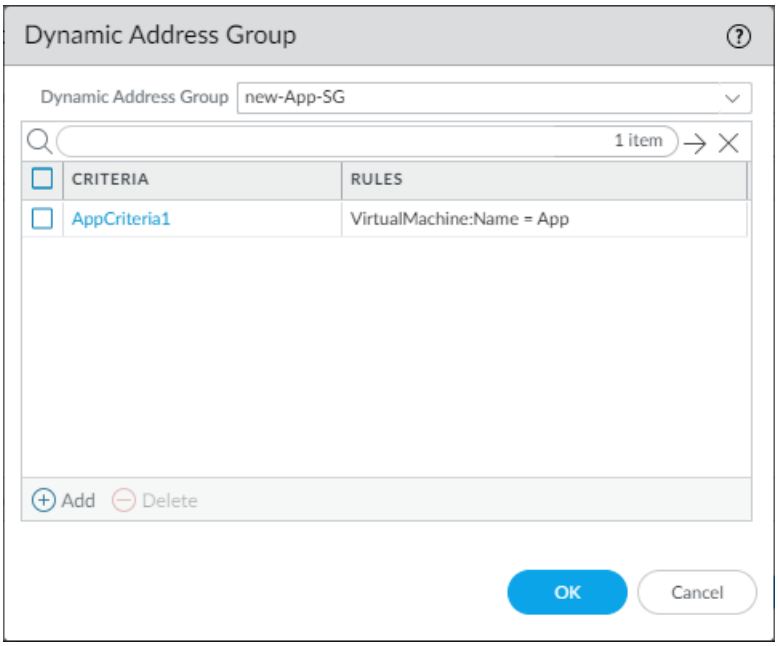
```
request plugins vmware_nsx nsx_t nsxt-scope tag <tag_value> service-definition <SD-name>
```

7. Haga clic en **OK (Aceptar)**.
8. (Opcional) haga clic en **Add (Añadir)** para crear reglas adicionales (hasta cinco en total).

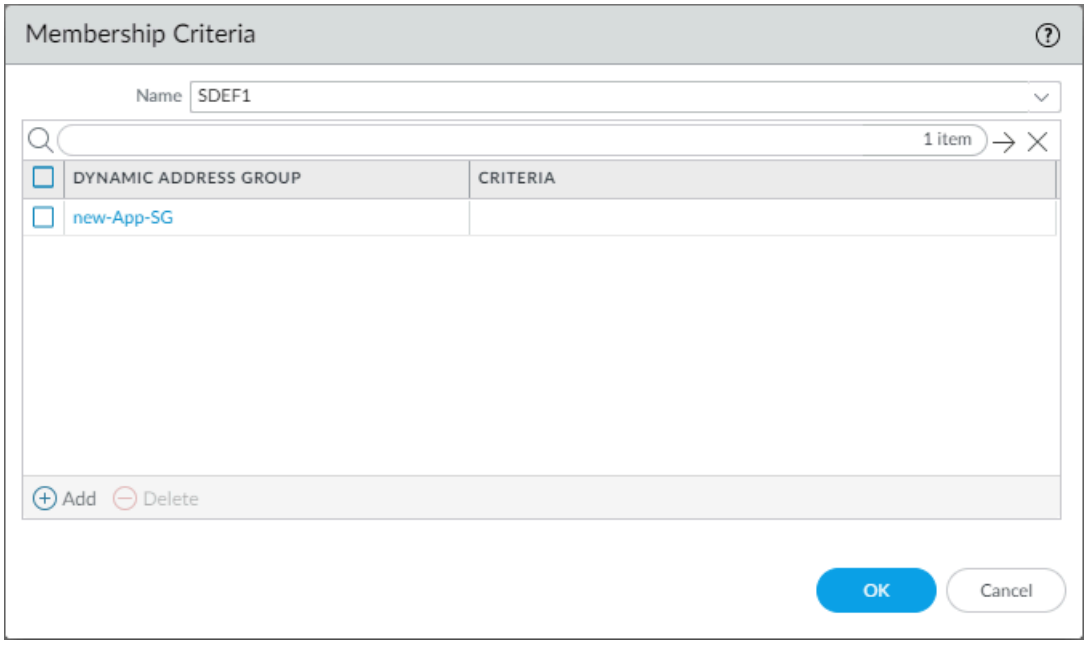


 ©2024 Palo Alto Networks, Inc.

STEP 9 | En la ventana Grupo de direcciones dinámicas, haga clic en **OK (Aceptar)** para finalizar o en **Add (Añadir)** para crear criterios y reglas adicionales (hasta cinco en total).



STEP 10 | En la ventana Criterios de pertenencia, haga clic en **OK (Aceptar)** para finalizar o en **Add (Añadir)** para especificar grupos de direcciones dinámicas adicionales.



Generar política de dirección

NSX-T utiliza la política de dirección para definir la cadena de servicio a la que se dirigirá el tráfico. Puede crear una política de dirección de forma manual o puede generar una política de dirección automáticamente.

Cuando genera una política de dirección automáticamente, el complemento de Panorama para VMware NSX-T crea una política de dirección para cada administrador de servicio especificado y las definiciones

 ©2024 Palo Alto Networks, Inc.

de servicio asociadas. De forma predeterminada, TCP estricto está deshabilitado y la Política de fallos está configurada en Permitir. La política generada automáticamente utiliza el formato de nomenclatura **`auto_<service-def-name>_<zone-name>_steering_policy`** .

Cuando TCP estricto está habilitado, el cortafuegos VM-Series hace cumplir el requisito del protocolo de enlace de tres vías. Si el cortafuegos capta tráfico a mitad de sesión (por ejemplo, debido a tráfico asimétrico) y no detecta un protocolo de enlace de tres vías, la sesión se interrumpe. Consulte la documentación de VMware NSX-T para obtener más información.

La política de fallos define lo que sucede con el tráfico si el cortafuegos VM-Series deja de funcionar. Si selecciona Permitir, el tráfico continúa hacia su destino. Si selecciona Bloquear, el tráfico se elimina.

Además, tiene la opción de seleccionar a todos sus administradores de servicios en lugar de seleccionar administradores de servicios específicos. No se recomienda elegir **All (Todos)** si alguno de sus administradores de servicios contiene definiciones de servicio basadas en las operaciones. El complemento creará una política de dirección para cada zona asociada con las definiciones de servicio basadas en las operaciones y luego la enviará a NSX-T Manager. Si elige **All (Todos)**, verifique que el administrador de servicios que selecciona cuando genera automáticamente la política de dirección incluya solo definiciones de servicio basadas en la seguridad.

Si genera automáticamente una política de dirección, también debe generar automáticamente reglas de dirección. Y si crea manualmente la política de dirección, también debe crear manualmente las reglas de dirección.

- Generación automática de políticas de dirección
- Crear manualmente una política de dirección

*Los cambios de política de dirección deben realizarse solo en Panorama; no realice cambios en NSX-T Manager. Si realiza cambios en NSX-T Manager, el complemento de Panorama para VMware NSX mostrará que la definición del servicio no está sincronizada. Debe hacer clic en el enlace **Out-of-Sync (No sincronizado)** para ver el motivo específico del estado de desincronización. Si la causa es un cambio en la política de dirección, realice una sincronización de configuración haciendo clic en **NSX-T Config-Sync (Sincronización de configuración de NSX-T)**.*

Generación automática de políticas de dirección

Utilice el siguiente procedimiento para generar automáticamente la política de dirección.

*Los siguientes pasos son para especificar administradores de servicios en lugar de seleccionar **All (Todos)**.*

STEP 1 | Seleccione **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspección de red)** > **Policy (Política)**.

STEP 2 | Haga clic en **Auto Generate (Generar automáticamente)**.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Para los **Service Managers (Administradores de servicios)**, seleccione **Select (Seleccionar)**.

> *Si selecciona **All (Todos)** en lugar de seleccionar administradores de servicios específicos, el complemento generará una política de dirección para cada definición de servicio asociada con cada administrador de servicios en su configuración. Además, asegúrese de que su administrador de servicios seleccionado incluya definiciones de servicio basadas en la seguridad.*

STEP 4 | Haga clic en **Add (Añadir)** para seleccionar el administrador de servicios.

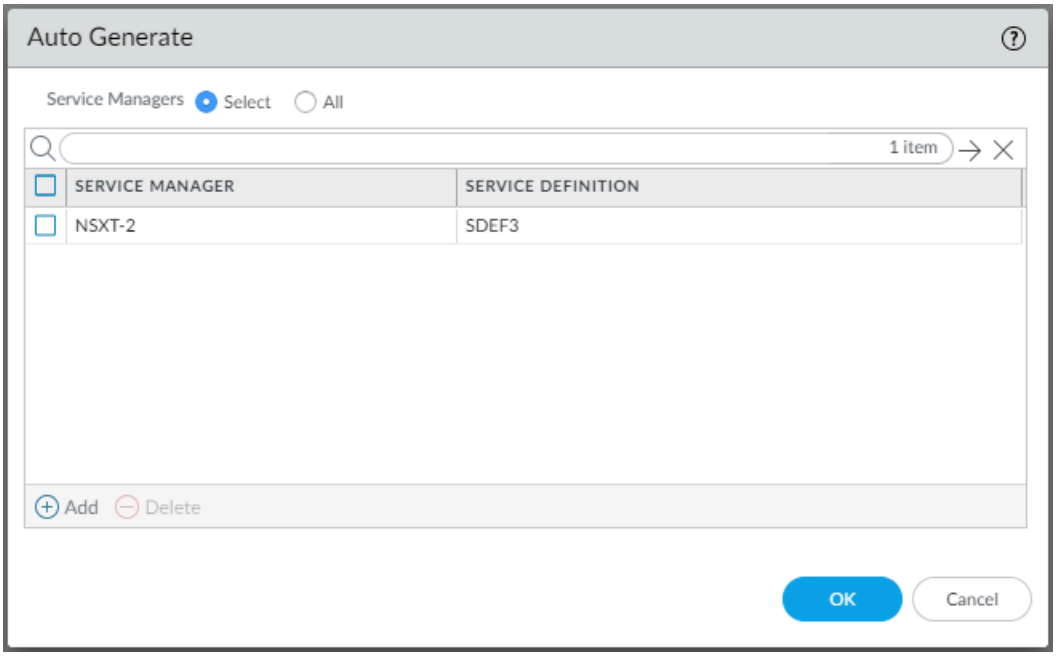
STEP 5 | Seleccione un **Service Manager (Administrador de servicios)** del menú desplegable.

STEP 6 | Haga clic en **Add (Añadir)** para seleccionar las definiciones de servicio.

STEP 7 | Seleccione la definición de servicio en el menú desplegable.

STEP 8 | Haga clic en **OK (Aceptar)** y vuelva a hacer clic en **OK (Aceptar)**.

STEP 9 | **Commit (Confirmar)** los cambios realizados en Panorama.



Crear manualmente una política de dirección

Utilice el siguiente procedimiento para crear manualmente una política de dirección.

STEP 1 | Seleccione **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspección de red)** > **Policy (Política)**.

STEP 2 | Haga clic en **Add (Añadir)**.

STEP 3 | Introduzca un **Name (Nombre)** descriptivo para su política de dirección.

> *El nombre de la política de dirección no puede incluir espacios.*

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Seleccione una **Service Definition (Definición de servicio)** en el menú desplegable.

STEP 5 | Seleccione una **Service Chain (Cadena de servicio)** de la lista desplegable.

STEP 6 | (Opcional) Habilite **TCP Strict (TCP estricto)**. Esta opción está deshabilitada de manera predeterminada.

STEP 7 | Establezca la **Política de fallos**: **Allow (Permitir)** o **Block (Bloquear)**. Permitir es el valor predeterminado.

STEP 8 | Haga clic en **OK (Aceptar)**.

STEP 9 | **Commit (Confirmar)** los cambios realizados en Panorama.



Genere reglas de dirección

Las reglas de dirección se definen en la política de dirección. Una regla define el origen y el destino del tráfico, los servicios de introspección, los objetos NSX-T a los que se aplica la regla y la política de redireccionamiento del tráfico. Puede crear reglas de dirección manualmente o generar reglas de dirección automáticamente.

Debe generar o crear una política de dirección antes de generar o crear reglas de dirección.

Para generar automáticamente una regla de dirección basada en reglas de seguridad creadas en Panorama, la regla de seguridad debe cumplir con los siguientes criterios:

- Pertenecer a un grupo de dispositivos principal o secundario registrados con un Administrador de servicios NSX.
- Ser en una política de intrazona e incluir solo una zona.
- No incluye un grupo de direcciones estáticas, un rango de IP ni una máscara de red configurada para la regla.

Las reglas de dirección generadas automáticamente usan el formato de nomenclatura **auto_<device-group-name>_<device-group-rule-name>**.

De forma predeterminada, las reglas de dirección generadas automáticamente se configuran sin que se especifique un servicio de NSX. Además, la dirección del tráfico NSX está configurada en entrada-salida, el registro está deshabilitado, el protocolo IP es ipv4-ipv6 y la acción está configurada para redireccionar.

 ©2024 Palo Alto Networks, Inc.

Después de la generación automática de reglas, puede actualizar la dirección para cambiar los valores predeterminados.

Además, tiene la opción de seleccionar a todos sus administradores de servicios en lugar de seleccionar administradores de servicios específicos. No se recomienda elegir **All (Todos)**.

Si genera automáticamente una política de dirección, también debe generar automáticamente reglas de dirección. Y si crea manualmente una política de dirección, también debe crear manualmente reglas de dirección.

- Generación automática de reglas de dirección
- Crear reglas de dirección de forma manual

*Los cambios en las reglas de dirección deben realizarse solo en Panorama; no realice cambios en NSX-T Manager. Si realiza cambios en NSX-T Manager, el complemento de Panorama para VMware NSX mostrará que la definición del servicio no está sincronizada. Debe hacer clic en el enlace **Out-of-Sync (No sincronizado)** para ver el motivo específico del estado de desincronización. Si un cambio en las reglas de dirección es la causa, realice una sincronización de configuración haciendo clic en **NSX-T Config-Sync (Sincronización de configuración de NSX-T)**.*

Generación automática de reglas de dirección

Utilice el siguiente procedimiento para generar automáticamente reglas de dirección.

Cuando genera automáticamente una regla de dirección, el lugar donde se aplica la regla (cortafuegos distribuido de NSX-T o Grupo de seguridad) depende del origen y el destino que especificó al configurar la regla de seguridad. Si ha seleccionado **Any (Cualquiera)** para el origen o el destino, NSX-T Manager aplica la regla de dirección al cortafuegos distribuido. Si selecciona un grupo de direcciones dinámicas para el origen y el destino, la dirección se aplica a las VM invitadas en esos grupos de seguridad.

Si realiza algún cambio en la configuración del grupo de dispositivos que también es parte de la configuración de la regla de dirección, como el grupo de direcciones de origen y destino que se asignan al ajuste Aplicada a en una regla de dirección, debe generar automáticamente la regla de dirección nuevamente para que se realicen los cambios.

*Los siguientes pasos son para especificar administradores de servicios en lugar de seleccionar **All (Todos)**.*

STEP 1 | Seleccione **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspección de red)** > **Rule (Regla)**.

STEP 2 | Haga clic en **Auto Generate (Generar automáticamente)**.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Seleccione el tipo de Reglas de seguridad en el menú desplegable: **All (Todas)**, solo **Pre Rulebase (Base de regla previa)** o solo **Post Rulebase (Base de regla posterior)**. Las reglas de seguridad se extraen de las definiciones de servicio especificadas en los siguientes pasos.

> *Si regenera las reglas de dirección, se eliminan todas las reglas actuales y se crean reglas nuevas en función de la base de reglas seleccionada. Si inicialmente creó reglas de dirección usando la base de reglas previa y luego regenerar las reglas de dirección usando la base de reglas posterior, solo permanecerán las reglas de dirección posteriores a la base de reglas.*

STEP 4 | Para **Type (Tipo)**, elija **Select (Seleccionar)**.

STEP 5 | Haga clic en **Add (Añadir)** para especificar los **Service Manager(s) [Administradores de servicios]** y **Service Definition(s) [Definiciones de servicios]**.

STEP 6 | Seleccione un **Service Manager (Administrador de servicios)** del menú desplegable.

STEP 7 | Haga clic en **Add (Añadir)** para seleccionar las definiciones de servicio.

STEP 8 | Haga clic en **OK (Aceptar)**.

STEP 9 | Haga clic en **OK (Aceptar)** para finalizar o en **Add (Añadir)** para especificar administradores de servicios y definiciones de servicios adicionales.

STEP 10 | (Opcional) Haga clic en una regla generada automáticamente para modificar las siguientes opciones predeterminadas.

> *Si regenera las reglas de dirección, se sobrescribirán los cambios que haya realizado en una regla de dirección generada anteriormente.*

- Habilite la **Logging (Creación de logs)** de NSX-T.
- Haga clic en **Add (Añadir)** para especificar los **NSX Services (Servicios NSX)**, como Active Directory Server, HTTPS, DNS, etc.
- **Disable (Desactivar)** la regla. Si deshabilita una regla de dirección, pero la regla de seguridad correspondiente está habilitada (**Device Group [Grupo de dispositivos]** > **Policies [Políticas]** > **Security [Seguridad]**) de políticas de grupo de dispositivos), la regla de dirección también se habilitará.
- **Applied to (Aplicado a)** le permite cambiar dónde se aplica la regla de dirección: **DFW** o **Security Group (Grupo de seguridad)**.

STEP 11 | Limpiar reglas de dirección incorrectas o no deseadas.

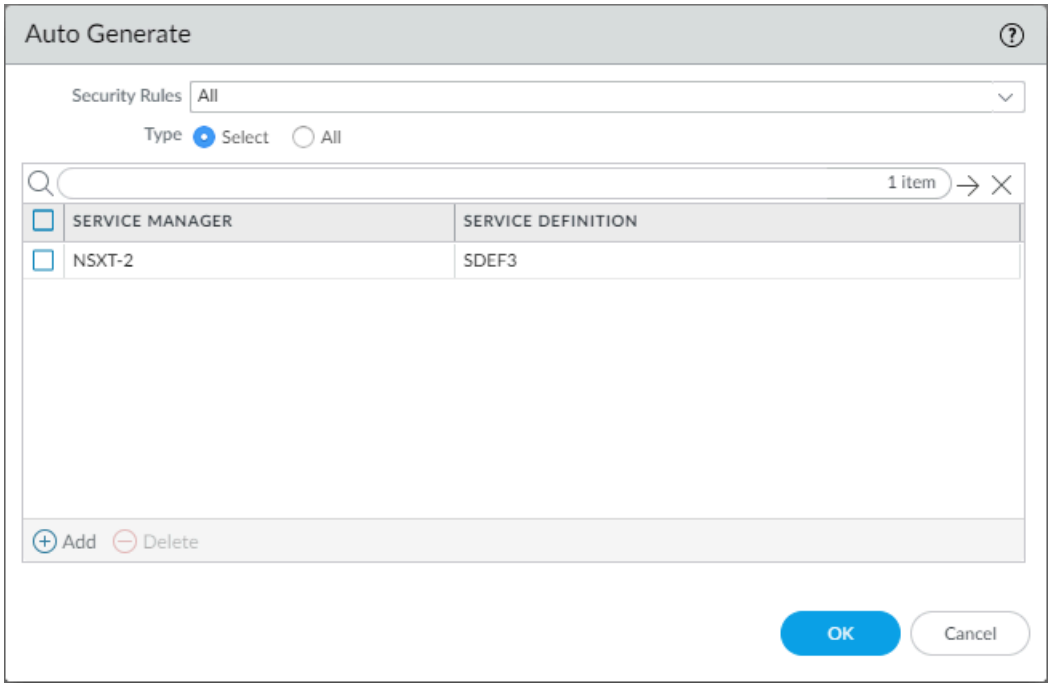
Si, por ejemplo, su grupo de dispositivos contiene reglas de seguridad en la misma base de reglas que sus reglas de dirección de NSX-T, el complemento genera reglas de seguridad basadas en esas reglas de seguridad que no son de NSX-T. Debido a que esas reglas no se refieren a un grupo de direcciones dinámicas de NSX-T, el origen y el destino de esas reglas se establecerán en Any Any (Cualquiera Cualquiera) en NSX-T Manager. Esta condición puede afectar la forma en que NSX-T Manager dirige el tráfico. Para evitar esto, debe eliminar manualmente las reglas de dirección incorrectas.

1. Seleccione las reglas de dirección incorrectas.
2. Haga clic en **Delete (Eliminar)**.

 ©2024 Palo Alto Networks, Inc.

3. Haga clic en **Yes (Sí)** para confirmar su eliminación.

STEP 12 | **Commit (Confirmar)** su configuración para enviarla a NSX-T Manager.



Crear reglas de dirección de forma manual

Utilice el siguiente procedimiento para crear reglas de dirección manualmente.

STEP 1 | Seleccione **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspección de red)** > **Rule (Regla)**.

STEP 2 | Haga clic en **Add (Añadir)**.

STEP 3 | Introduzca un **Name (Nombre)** descriptivo para la regla de dirección.

El nombre de la regla de dirección no puede incluir espacios.

STEP 4 | Seleccione una **Steering Policy (Política de dirección)** en el menú desplegable.

STEP 5 | Seleccione un **Device Group (Grupo de dispositivos)** del menú desplegable.

STEP 6 | Seleccione una **Security Rule (Regla de seguridad)** del menú desplegable.

El menú desplegable Regla de seguridad muestra las reglas de todas las reglas de seguridad en todos los grupos de dispositivos de la Definición de servicio. Asegúrese de seleccionar la regla de seguridad adecuada.

STEP 7 | Especifique la **Action (Acción)**: **Redirect (Redirigir)** o **Do Not Redirect (No redirigir)**.

STEP 8 | (Opcional) Habilite la **Logging (Creación de logs)** de NSX-T.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Especifique el **IP Protocol (Protocolo de IP)**: **ipv4-ipv6**, **ipv4** o **ipv6**.

STEP 10 | Especifique la **NSX Traffic Direction (Dirección del tráfico de NSX)**: **in-out (entrada-salida)**, **in (entrada)** o **out (salida)**.

STEP 11 | (Opcional) Haga clic en Añadir para especificar los **NSX Services (Servicios NSX)**, como Active Directory Server, HTTPS, DNS, etc.

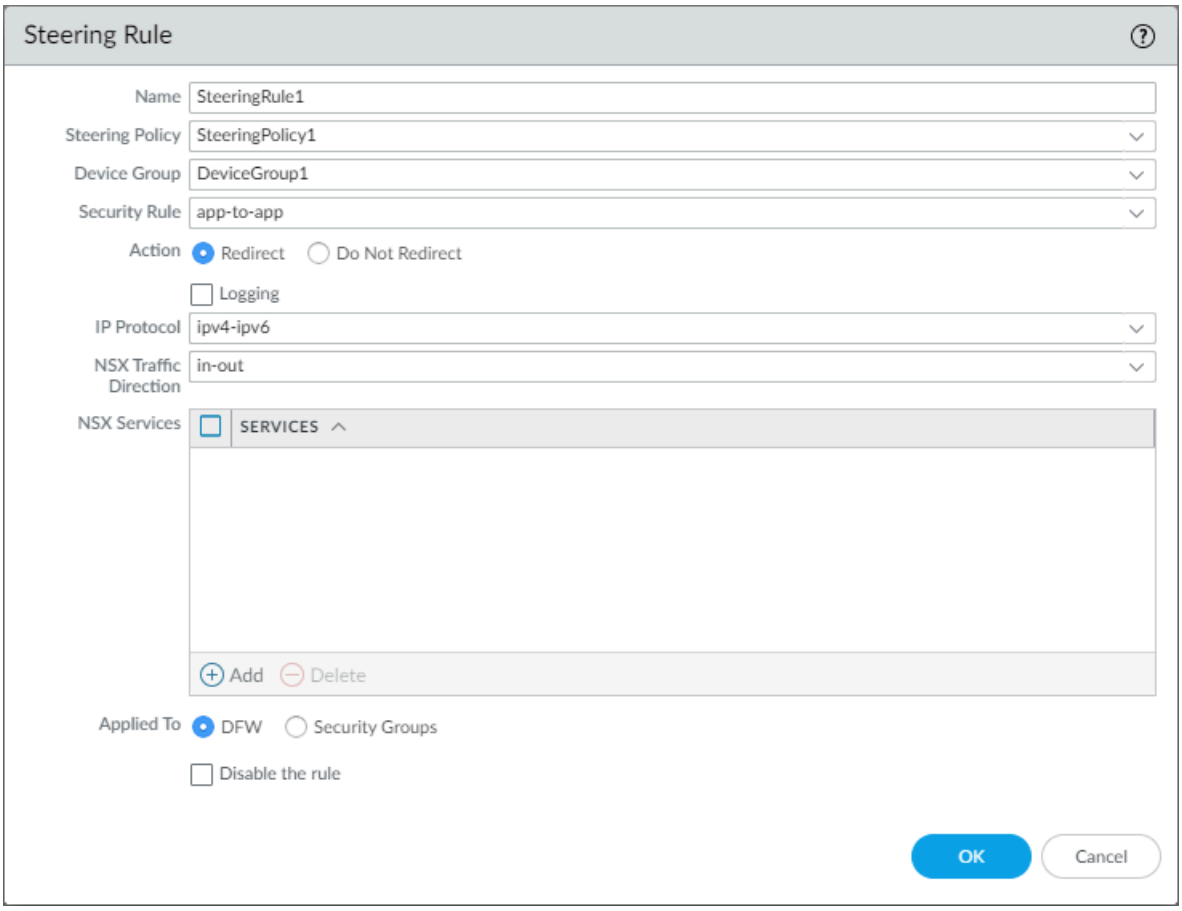
Los siguientes servicios ALG no son compatibles: FTP, TFTP, ORACLE_TNS, SUN_RPC_TCP, SUN_RPC_UDP, MS_RPC_TCP, MS_RPC_UDP, NBNS_BROADCAST, NBDG_BROADCAST.

STEP 12 | **Applied To (Aplicado a)**: **DFW** o **Security Groups (Grupos de seguridad)**. Puede seleccionar uno o más grupos de seguridad. Los grupos de seguridad se crean a partir de grupos de direcciones dinámicas configurados en Panorama. Los nombres de los grupos de seguridad tienen el siguiente formato **`<servicedefinition>_<dynamic-address-group>`**. Si selecciona DFW, la regla de dirección se aplica a todas las máquinas virtuales invitadas, independientemente de su pertenencia de seguridad.

STEP 13 | (Opcional) Desactive la regla.

STEP 14 | Haga clic en **OK (Aceptar)**.

STEP 15 | **Commit (Confirmar)** su configuración para enviarla a NSX-T Manager.



 ©2024 Palo Alto Networks, Inc.

Eliminar una definición de servicio de Panorama

Complete el siguiente procedimiento para eliminar una definición de servicio de su configuración NSX-T en Panorama.

STEP 1 | Inicie sesión en Panorama.

STEP 2 | Para una implementación basada en la seguridad, elimine las reglas de dirección y la política de dirección asociadas con la definición de servicio que se eliminará.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspección de red)** > **Rules (Reglas)**.
2. Seleccione las reglas de dirección que se van a eliminar.
3. Haga clic en **Delete (Eliminar)**.
4. Seleccione **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspección de red)** > **Policy (Política)**.
5. Seleccione la política de dirección que se eliminará.
6. Haga clic en **Delete (Eliminar)**.

STEP 3 | **Commit (Confirmar)** los cambios.

STEP 4 | Elimine los cortafuegos VM-series implementados en NSX-T que están asociados con la definición de servicio que se eliminará.

STEP 5 | Elimine los criterios de pertenencia asociados con la definición del servicio.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Membership Criteria (Criterios de pertenencia)**.
2. Seleccione los criterios que se eliminarán.
3. Haga clic en **Delete (Eliminar)**.

STEP 6 | Desvincule la definición de servicio del administrador de servicios con el que está asociada.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Service Managers (Administradores de servicios)**.
2. Introduzca el Nombre de administrador de servicios.
3. Seleccione la definición de servicio.
4. Haga clic en **Delete (Eliminar)**.
5. Haga clic en **OK (Aceptar)**.

STEP 7 | **Commit (Confirmar)** los cambios realizados en Panorama.

Migración de VM-Series en operación NSX-T a implementación basada en seguridad

Utilice el siguiente procedimiento para migrar su implementación de NSX-T basada en las operaciones a una implementación de NSX-T basada en la seguridad.

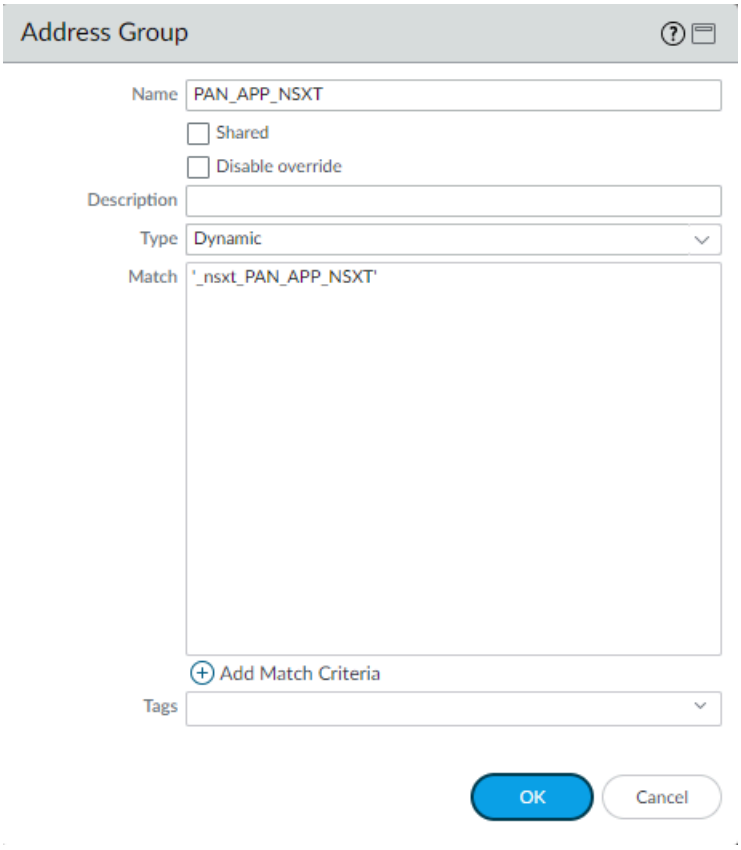
STEP 1 | Inicie sesión en Panorama.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Modifique los criterios de coincidencia de sus grupos de direcciones dinámicas para seguir el formato requerido para una implementación basada en la seguridad.

1. Seleccione **Objects (Objetos)** > **Address Groups (Grupos de direcciones)**.
2. Compruebe que está configurando los grupos de direcciones dinámicas en un grupo de dispositivos asociado con una definición de servicio NSX-T.
3. Haga clic en el nombre de un grupo de direcciones dinámicas NSX-T creado anteriormente.
4. Defina los criterios de coincidencia.

   Para que el grupo de direcciones dinámicas se convierta en un grupo de seguridad en NSX-T Manager, la cadena de criterios de coincidencia debe estar entre comillas simples con el prefijo _nsx_ seguido del nombre exacto del Security Group (Grupo de direcciones). Por ejemplo, ***'_nsxt_PAN_APP_NSX'***.
5. Repita este proceso para cada grupo de seguridad que necesite.



 ©2024 Palo Alto Networks, Inc.

STEP 3 | Establezca las reglas de seguridad para que sean las reglas de dirección de NSX-T dentro de la zona.

1. En Panorama, seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Pre Rules (Pre reglas)**.
2. Compruebe que está configurando las reglas de seguridad en un grupo de dispositivos asociado con una definición de servicio NSX-T.
3. Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** y **Description (Descripción)**para la regla de políticas de seguridad.
4. Establezca el tipo de regla en **intrazone (Devices with PAN-OS 6.1 or later) [intrazona (dispositivos con PAN-OS 6.1 o posterior)]**.
5. En la pestaña Source (Origen), configure la zona de origen en la zona desde la pila de plantillas asociada a la definición del servicio. Luego, seleccione un grupo de direcciones dinámicas que creó anteriormente como la Dirección de origen. No añada ningún grupo de direcciones estáticas, rangos de IP o máscaras de red como una Dirección de origen.
6. En la pestaña Destination (Destino), Panorama no le permite establecer una zona de destino porque establece el tipo de regla en intrazona. A continuación, seleccione un grupo de direcciones dinámicas que creó anteriormente como Destination Address (Dirección de destino). No agregue ningún grupo de direcciones estáticas, rangos de IP o máscaras de red como una Dirección de destino.
7. Haga clic en **OK (Aceptar)**.
8. Repita los pasos 1 a 7 para cada regla de dirección que necesite.
9. **Commit (Confirmar)** los cambios.

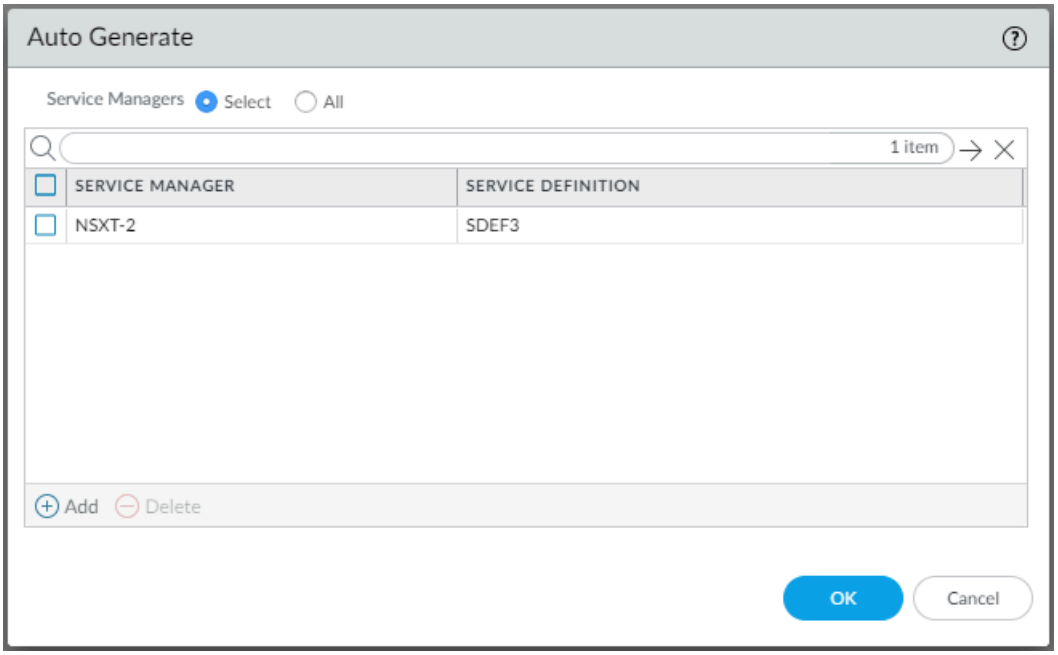
 ©2024 Palo Alto Networks, Inc.

STEP 4 | Generar automáticamente una nueva política de dirección.

Los siguientes pasos son para especificar administradores de servicios en lugar de seleccionar **All (Todos)**.

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspección de red)** > **Policy (Política)**.
2. Haga clic en **Auto Generate (Generar automáticamente)**.
3. Para los **Service Managers (Administradores de servicios)**, seleccione **Select (Seleccionar)**.

   *Si selecciona **All (Todos)** en lugar de seleccionar administradores de servicios específicos, el complemento generará una política de dirección para cada definición de servicio asociada con cada administrador de servicios en su configuración.*
4. Haga clic en **Add (Añadir)** para seleccionar el administrador de servicios.
5. Seleccione un **Service Manager (Administrador de servicios)** del menú desplegable.
6. Haga clic en **Add (Añadir)** para seleccionar las definiciones de servicio.
7. Seleccione la definición de servicio en el menú desplegable.
8. Haga clic en **OK (Aceptar)** y vuelva a hacer clic en **OK (Aceptar)**.



9. **Commit (Confirmar)** los cambios.

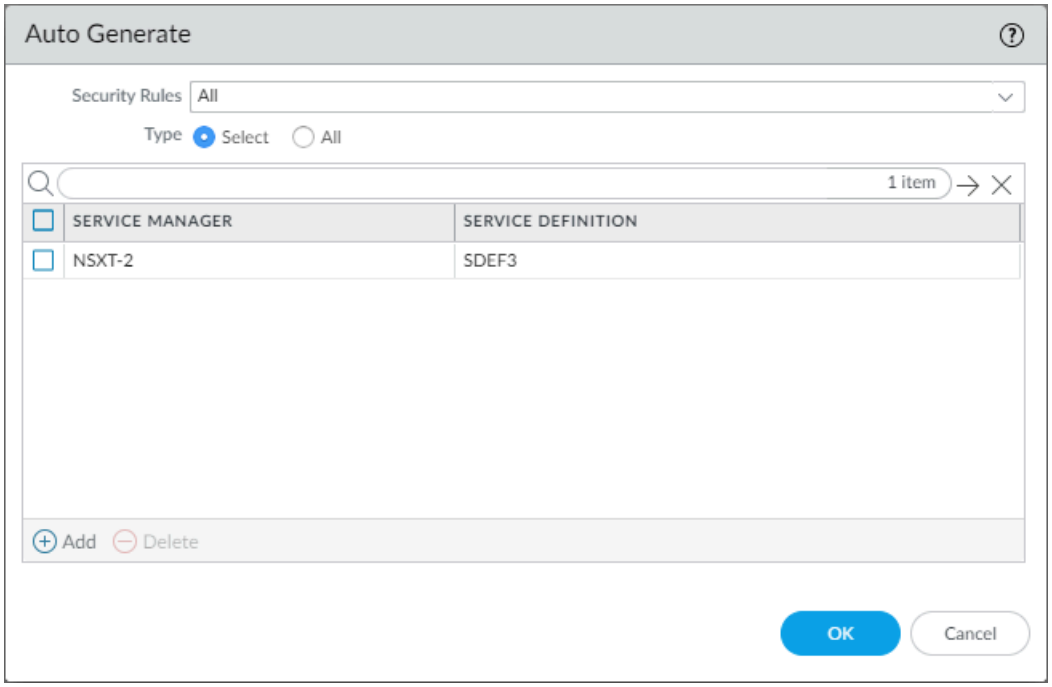
 ©2024 Palo Alto Networks, Inc.

STEP 5 | Genere nuevas reglas de dirección automáticamente.

Si genera automáticamente una política de dirección, también debe generar automáticamente reglas de dirección. Y si crea manualmente una política de dirección, también debe crear manualmente reglas de dirección.

*Los siguientes pasos son para especificar administradores de servicios en lugar de seleccionar **All (Todos)**.*

1. Seleccione **Panorama** > **VMware** > **NSX-T** > **Network Introspection (Introspección de red)** > **Rule (Regla)**.
2. Haga clic en **Auto Generate (Generar automáticamente)**.
3. Seleccione el tipo de Reglas de seguridad en el menú desplegable: **All (Todas)**, solo **Pre Rulebase (Base de regla previa)** o solo **Post Rulebase (Base de regla posterior)**. Las reglas de seguridad se extraen de las definiciones de servicio especificadas en los siguientes pasos.
4. Para **Type (Tipo)**, elija **Select (Seleccionar)**.
5. Haga clic en Añadir para especificar los **Service Manager(s) [Administradores de servicios]** y **Service Definition(s) [Definiciones de servicios]**.
6. Seleccione un **Service Manager (Administrador de servicios)** del menú desplegable.
7. Haga clic en **Add (Añadir)** para seleccionar las definiciones de servicio.
8. Haga clic en **OK (Aceptar)**.
9. Haga clic en **OK (Aceptar)** para finalizar o en **Add (Añadir)** para especificar administradores de servicios y definiciones de servicios adicionales.
10. (Opcional) Haga clic en una regla generada automáticamente para modificar las opciones predeterminadas.



STEP 6 | Crear criterios de pertenencia a grupos de direcciones dinámicas.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | **Commit (Confirmar)** los cambios realizados en Panorama.

STEP 8 | Elimine las reglas de dirección basadas en operaciones de NSX-T Manager.

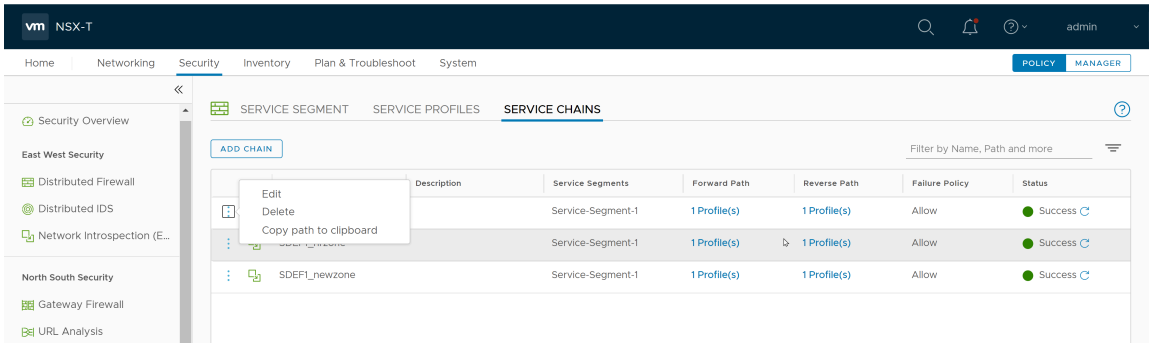
1. Inicie sesión en NSX-T Manager.
2. Seleccione **Security (Seguridad)** > **Network Introspection (E-W) [Introspección de red (E-O)]** > **Rules (Reglas)**.
3. Seleccione cada una de las reglas de dirección basadas en las operaciones.
4. Haga clic en **Delete (Eliminar)**.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Elimine la cadena de servicios basada en operaciones de NSX-T Manager.

1. Inicie sesión en NSX-T Manager.
2. Seleccione **Security (Seguridad)** > **Network Introspection Settings (Configuración de introspección de red)** > **Service Chains (Cadenas de servicio)**.
3. Haga clic en las elipses verticales.
4. Haga clic en **Delete (Eliminar)**.

 ©2024 Palo Alto Networks, Inc.



Amplíe la política de seguridad de NSX-V a NSX-T

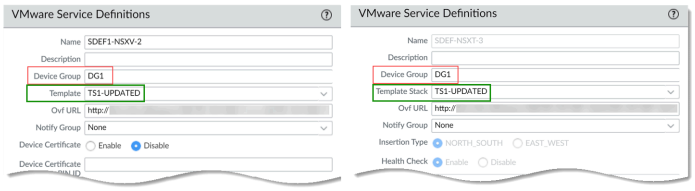
Si va a pasar de una implementación de NSX-V a una implementación de NSX-T o combina una implementación de NSX-T con una de NSX-V, puede extender su política de seguridad existente de NSX-V a NSX-T sin tener que volver a crear la reglas de política. Esto se logra aprovechando sus grupos de

 ©2024 Palo Alto Networks, Inc.

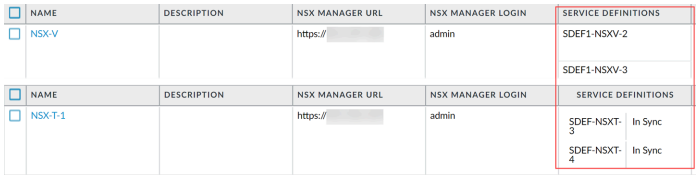
dispositivos existentes y compartiéndolos entre las definiciones de servicio NSX-V y NSX-T. Después de migrar su política a NSX-T, puede continuar usando VM-Series para NSX-V o eliminar su implementación de NSX-V.

STEP 1 | Instale el plugin de Panorama para VMware NSX 3.2.0 o posterior. Consulte Notas de la versión del complemento de Panorama para VMware NSX 3.2.0 antes de actualizar.

STEP 2 | Configure una definición de servicio NSX-T para cada definición de servicio NSX-V en su implementación. No cree nuevos grupos de dispositivos; en su lugar, utilice sus grupos de dispositivos NSX-V existentes. El uso de los grupos de dispositivos existentes le permite aplicar las mismas reglas de políticas de seguridad que se usan en NSX-V a los cortafuegos VM-Series implementados en NSX-T. Si tiene una política que hace referencia a una zona en particular, añada la misma pila de plantillas de su definición de servicio NSX-V a su definición de servicio NSX-T. Además, si su grupo de dispositivos hace referencia a una plantilla en particular, asegúrese de seleccionar la pila de plantillas que incluye la plantilla a la que se hace referencia en el grupo de dispositivos.



STEP 3 | Configure un administrador de servicios de NSX-T y asocie las definiciones de servicio de NSX-T al administrador de servicios.



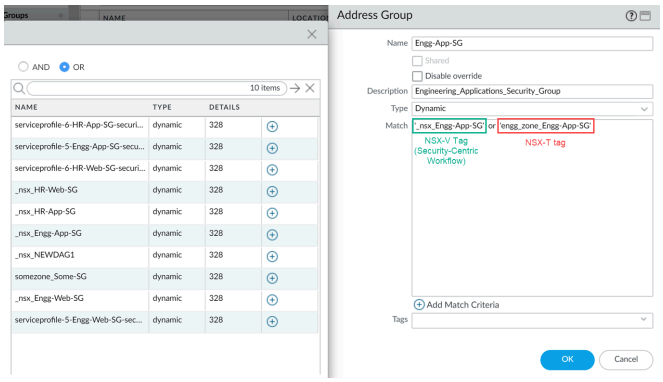
STEP 4 | Prepare su entorno NSX-T e implemente el cortafuegos VM-Series. Debe crear sus grupos de seguridad, cadenas de servicios y política de redireccionamiento del tráfico antes de iniciar el cortafuegos VM-Series.

- Implementación del cortafuegos VM-Series en NSX-T (norte-sur)
- Implementación de VM-Series mediante el flujo de trabajo basado en las operaciones

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Añada las etiquetas NSX-T a sus grupos de direcciones dinámicas existentes.

1. Seleccione **Panorama** > **Objects (Objetos)** > **Address Groups (Grupos de direcciones)**.
2. Haga clic en el nombre de un grupo de direcciones dinámicas de NSX-V existente.
3. Haga clic en **Add Match Criteria (Añadir criterios de coincidencia)** para mostrar las etiquetas de NSX-V y NSX-T.
4. Añada la etiqueta NSX-T a los grupos de direcciones dinámicas. Asegúrese de utilizar el operador **OR** entre las etiquetas.
5. Cuando haya añadido todas las etiquetas necesarias, haga clic en **OK (Aceptar)**.
6. Haga clic en **Commit (Confirmar)** para compilar los cambios.



STEP 6 | Una vez que las cargas de trabajo de su máquina virtual se hayan migrado correctamente de NSX-V a NSX-T, elimine las etiquetas NSX-V de sus grupos de direcciones dinámicas si planifica dejar de usar NSX-V. Todas las etiquetas NSX-V y las direcciones IP correspondientes se anulan del registro después de que toda la configuración relacionada con NSX-V se elimina del complemento Panorama para NSX y la configuración del cortafuegos VM-Series se elimina del NSX-V Manager.

Utilice la migración in situ para trasladar su VM-Series de NSX-V a NSX-T

Complete el siguiente procedimiento para migrar la configuración de su cortafuegos VM-Series de NSX-V a NSX-T. Al migrar su configuración, puede reutilizar políticas y grupos de direcciones dinámicas ya configurados en Panorama. Este procedimiento hace referencia a la información y los procesos publicados en la Documentación de VMware, así como a los pasos específicos de PAN.

Este procedimiento solo admite implementaciones de NSX-V centradas en operaciones. Una implementación significa que sus reglas de política para redirigir el tráfico al cortafuegos VM-Series se crearon en NSX-V Manager, no en Panorama.

Este procedimiento requiere NSX-T Manager 3.1.0 o posterior.

Se recomienda planificar el tiempo de inactividad de la seguridad mientras se realiza esta migración.

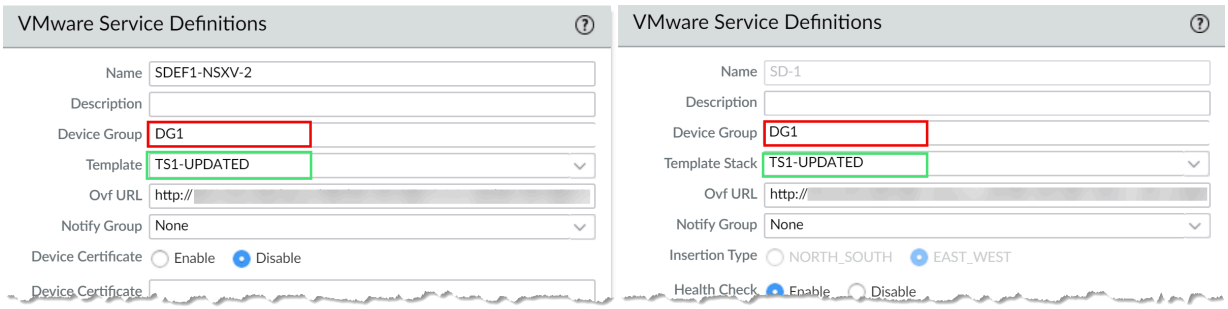
STEP 1 | Prepare sus entornos NSX-V y NSX-T para la migración basada en los pasos descritos por VMware.

 ©2024 Palo Alto Networks, Inc.

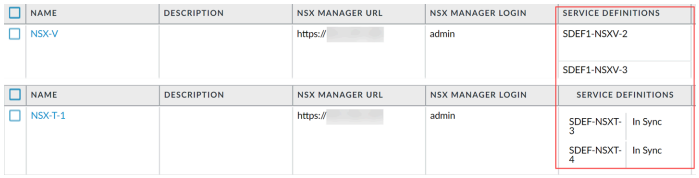
STEP 2 | Instale el plugin de Panorama para VMware NSX 3.2.0 o posterior. Consulte Notas de la versión del complemento de Panorama para VMware NSX 3.2.0 antes de actualizar.

STEP 3 | Habilitación de la comunicación entre NSX-T Manager y Panorama.

STEP 4 | Configure una definición de servicio NSX-T para cada definición de servicio NSX-V en su implementación. **No cree nuevos grupos de dispositivos**; en su lugar, utilice sus grupos de dispositivos NSX-V existentes. El uso de los grupos de dispositivos existentes le permite aplicar las mismas reglas de políticas de seguridad que se usan en NSX-V a los cortafuegos VM-Series implementados en NSX-T. Si tiene una política que hace referencia a una zona en particular, añada la misma pila de plantillas de su definición de servicio NSX-V a su definición de servicio NSX-T. Además, si su grupo de dispositivos hace referencia a una plantilla en particular, asegúrese de seleccionar la pila de plantillas que incluye la plantilla a la que se hace referencia en el grupo de dispositivos.



STEP 5 | Configure un administrador de servicios de NSX-T y asocie las definiciones de servicio de NSX-T al administrador de servicios.



STEP 6 | Verifique que su configuración de NSX-T esté presente en NSX-T Manager.

1. Inicie sesión en NSX-T Manager.
2. Seleccione **System (Sistema)** > **Service Deployments (Implementaciones de servicios)** > **Catálogo** .
3. Confirme que su definición de servicio NSX-T esté en la lista.
4. Seleccione **Security (Seguridad)** > **Network Introspection Settings (Configuración de introspección de red)** > **Service Profiles (Perfiles de servicio)**.
5. Confirme que sus zonas asociadas a su plantilla de NSX-T estén en la lista.

STEP 7 | Si aún no lo ha hecho, añada un gestor de compute en NSX-T Manager. Una vez que haya verificado que el Estado de registro y el Estado de conexión están activos, vaya a continuación.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | Importe la configuración de NSX-V a NSX-T.

STEP 9 | Desinstale la instancia de servicio de NSX-V.



Este paso resultará en una interrupción del tráfico.

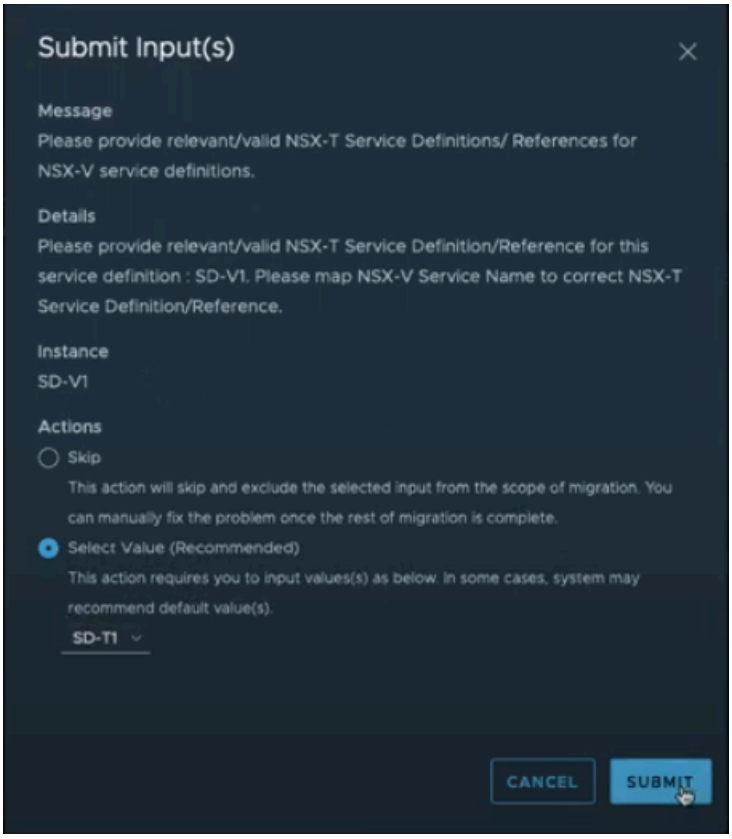
1. Inicie sesión en su cliente de vSphere.
2. Seleccione **Installation and Upgrade (Instalación y actualización)** > **Service Deployment (Implementación del servicio)**.
3. Seleccione la implementación de su servicio.
4. Haga clic en **Delete (Eliminar)**.
5. Haga clic en **Delete (Eliminar)** para confirmar.

STEP 10 | Resolver problemas de configuración en NSX-T Manager. Mientras resuelve los problemas de configuración, debe tomar acciones específicas para migrar la configuración de su cortafuegos VM-

 ©2024 Palo Alto Networks, Inc.

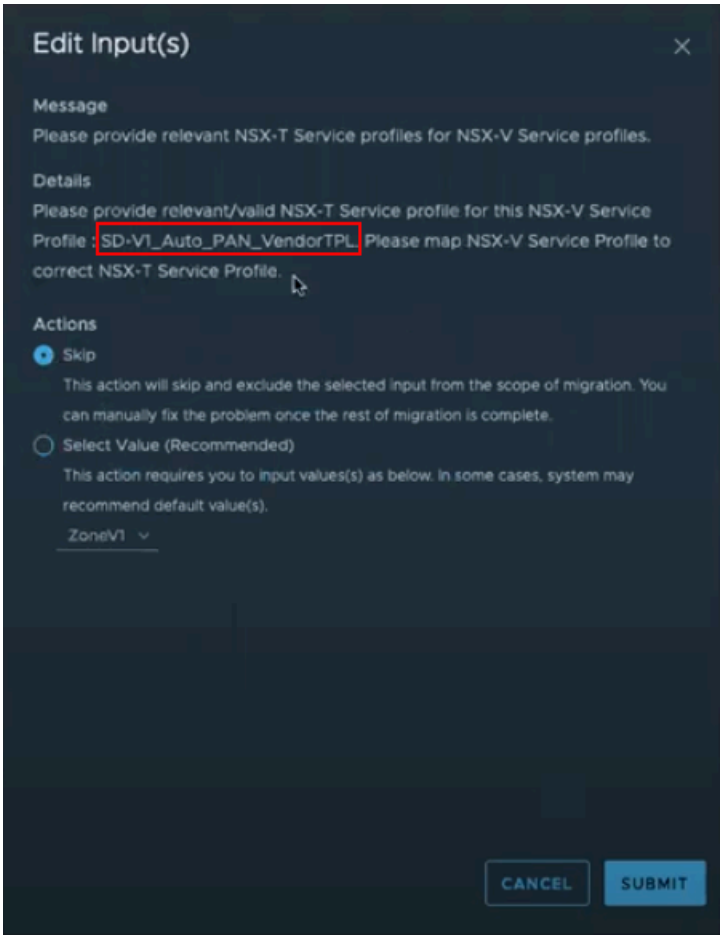
Series. En la mayoría de los casos, puede aceptar las recomendaciones presentadas por NSX-T Manager.

1. Al resolver la configuración de inserción de servicios, verifique que ha seleccionado la definición de servicio correcta que configuró previamente en Panorama para VM-Series en NSX-T.



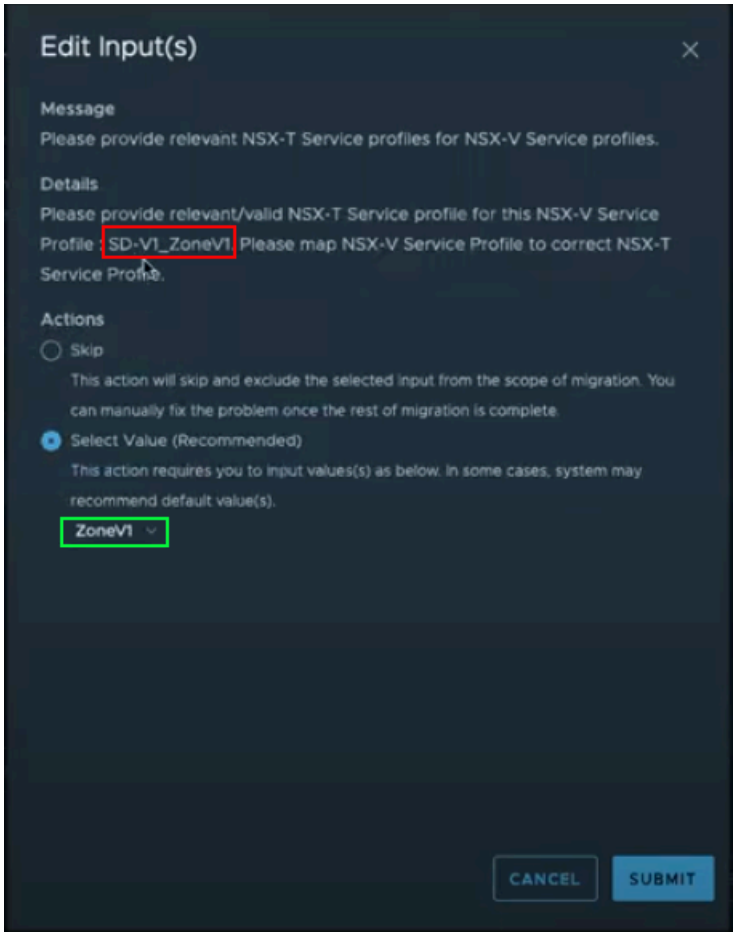
2. Continúe resolviendo la configuración restante.
3. Antes de pasar a **Migrate Configuration (Migrar configuración)**, se le pedirá que proporcione una zona de transporte para la inserción del servicio.
4. Asigne los perfiles de servicio en NSX-V a los perfiles de servicio correspondientes en NSX-T.
    1. Se puede omitir Auto_PAN_VendorTPL.

 ©2024 Palo Alto Networks, Inc.



2. Asigne el perfil de servicio NSX-T al perfil de servicio NSX-V correspondiente.

 ©2024 Palo Alto Networks, Inc.



STEP 11 | Migre la configuración.

STEP 12 | Verifique que su configuración se haya migrado correctamente.

1. Seleccione **Inventory (Inventario)** > **Groups (Grupos)** para comprobar que sus conjuntos de IP y grupos de seguridad estén presentes. Puede hacer clic en el nombre del grupo de seguridad para ver que la dirección IP correcta es parte del grupo de seguridad.
2. Seleccione **Security (Seguridad)** > **Network Introspection Settings (Configuración de introspección de red)** > **Service Segment (Segmento de servicio)** para confirmar que un segmento de servicio se ha creado.
3. Seleccione **Security (Seguridad)** > **Network Introspection Settings (Configuración de introspección de red)** > **Service Chains (Cadenas de servicio)** para confirmar que una cadena de servicio se ha creado. Haga clic en el Enlace de perfiles en las columnas de Ruta directa o Ruta inversa para ver su perfil de servicio.
4. Seleccione **Security (Seguridad)** > **Network Introspection (E-W) [Introspección de ruta (E-O)]** para confirmar que se ha creado una regla de redireccionamiento del tráfico para dirigir el tráfico al perfil de servicio del cortafuegos VM-Series.

STEP 13 | Si procede, modifique y migre perímetros.

STEP 14 | Configure y migre sus hosts.

 ©2024 Palo Alto Networks, Inc.

STEP 15 | Añada las etiquetas NSX-T a sus grupos de direcciones dinámicas existentes.

1. Seleccione **Panorama** > **Objects (Objetos)** > **Address Groups (Grupos de direcciones)**.
2. Haga clic en el nombre de un grupo de direcciones dinámicas de NSX-V existente.
3. Haga clic en **Add Match Criteria (Añadir criterios de coincidencia)** para mostrar las etiquetas de NSX-V y NSX-T.
4. Añada la etiqueta NSX-T a los grupos de direcciones dinámicas. Si selecciona no eliminar las etiquetas NSX-V, asegúrese de que utiliza el operador **OR** entre las etiquetas.
5. Cuando haya añadido todas las etiquetas necesarias, haga clic en **OK (Aceptar)**.
6. **Commit (Confirmar)** los cambios.

STEP 16 | Iniciar el cortafuegos VM-Series en NSX-T (este-oeste). No es necesario crear un nuevo segmento de servicio; en su lugar, seleccione el segmento de servicio creado durante la migración.

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en AWS

El cortafuegos VM-Series puede implementarse en la nube de Amazon Web Services (AWS) y AWS GovCloud. Se puede configurar para proteger el acceso a las aplicaciones implementadas en instancias de EC2 en una Virtual Private Cloud (VPC) en AWS.

El cortafuegos VM-Series ahora admite la suscripción a Web Proxy en entornos AWS.

- Acerca del cortafuegos VM-Series en AWS
- Implementaciones compatibles con AWS
- Implementación del cortafuegos VM-Series en AWS
- Integración de VM-Series con un balanceador de carga Gateway de AWS
- Alta disponibilidad para el cortafuegos VM-Series en AWS
- Caso de uso: Protección de las instancias de EC2 en AWS Cloud
- Caso de uso: Uso de grupos de direcciones dinámicas para proteger las nuevas instancias de EC2 en la VPC
- Caso de uso: Cortafuegos VM-Series como puertas de enlace de GlobalProtect en AWS
- Supervisión de VM en AWS
- Lista de atributos supervisados en la VPC de AWS

Acerca del cortafuegos VM-Series en AWS

Amazon Web Services (AWS) es un servicio de nube pública que le permite ejecutar sus aplicaciones en una infraestructura compartida gestionada por Amazon. Estas aplicaciones se pueden implementar en capacidades de procesamiento de tamaño variable o en instancias de EC2 en diferentes regiones de AWS y a las que los usuarios pueden acceder a través de internet.

Para ofrecer una conectividad de red consistente e instancias de EC2 fáciles de gestionar, Amazon ofrece Virtual Private Cloud (VPC). Una VPC se distribuye desde la nube pública de AWS y se asigna a un bloque CIDR desde el espacio de red privada (RFC 1918). Dentro de una VPC, puede crear subredes públicas o privadas según sus necesidades e implementar las aplicaciones en instancias de EC2 dentro de esas subredes. A continuación, para permitir el acceso a las aplicaciones dentro de la VPC, puede implementar el cortafuegos VM-Series en una instancia de EC2. El cortafuegos VM-Series se puede configurar para proteger el tráfico desde y hacia las instancias de EC2 dentro de la VPC.

El cortafuegos VM-Series está disponible en la nube AWS pública y en AWS GovCloud. Los cortafuegos VM-Series en AWS pública y AWS GovCloud son compatibles con el modelo de licencia existente (Bring Your Own License, BYOL) o con el modelo de pago por consumo (Pay-as-you-go, PAYG); el modelo con licencia basada en el uso que puede obtener de AWS Marketplace. Para obtener detalles de las licencias, consulte Licencias de cortafuegos VM-Series para nubes públicas.

*El cortafuegos VM-Series ahora es compatible con instancias basadas en ARM en **AWS Graviton 3**, **AWS Graviton 2** (ARM compute) para nubes públicas. Todas las características que estaban disponibles en entornos x86 ahora se extienden a instancias basadas en ARM, incluido el soporte de Hypervisor, DPDK que proporciona un mejor rendimiento, al tiempo que reduce los costes operativos (OPEX), el consumo de energía y las huellas. La compatibilidad con la arquitectura ARM está disponible actualmente en los modelos de licencia de AWS BYOL VM-Flex en las instancias **AWS C7gn**, **AWS R7g,** **AWS M7g** para **AWS Graviton 3** y **AWS C6gn**, **AWS R6g**, **AWS M6g** para instancias **AWS Graviton 2**, y es compatible con controladores ena.*

- Tipos de instancias EC2 de AWS
- Cortafuegos VM-Series en AWS GovCloud
- Cortafuegos VM-Series en AWS China
- Cortafuegos VM-Series en AWS Outposts
- Terminología de AWS
- Asignación de interfaz de gestión para su uso con Amazon ELB
- Ajuste del rendimiento para el cortafuegos VM-Series en AWS

Tipos de instancias EC2 de AWS

Para tipos de instancias compatibles, consulte Modelos VM-Series en instancias EC2.

Puede implementar el cortafuegos VM-Series en un tamaño de instancia de AWS con más recursos que el mínimo Requisitos del sistema VM-Series. Si elige un tamaño de instancia más grande para el modelo de cortafuegos VM-Series, aunque el cortafuegos solo usa los núcleos vCPU máximos y la memoria que se muestra en la tabla, este aprovecha el rendimiento de red más rápido que proporciona AWS. Si desea cambiar el tipo de instancia en su cortafuegos VM-Series que tiene licencia con la opción BYOL, debe

 ©2024 Palo Alto Networks, Inc.

desactivar la máquina virtual antes de cambiar el tipo de instancia para asegurarse de que su licencia sea válida. Consulte #unique_29 para saber por qué.

Para obtener orientación sobre el tamaño del cortafuegos VM-Series en AWS, consulte este artículo.

Cortafuegos VM-Series en AWS GovCloud

AWS GovCloud es una región AWS aislada que cumple con los requisitos regulatorios y de cumplimiento de las agencias y clientes del gobierno de EE.UU.

Para proteger su cargas de trabajo que contienen todas las categorías de datos de Información Controlada No Clasificada (CUI) y datos disponibles al público orientados al gobierno en la región AWS GovCloud (US), el cortafuegos VM-Series proporciona las mismas funciones de seguridad robustas en la nube pública AWS estándar y en AWS GovCloud. El cortafuegos VM-Series en AWS GovCloud y la nube pública de AWS admiten las mismas capacidades.

En AWS GovCloud, solo puede implementar cortafuegos VM-Series de forma escalable horizontalmente

El cortafuegos VM-Series en AWS GovCloud debe tener instalada la versión 5.1.1 o posterior del complemento de AWS y la versión 10.2.3 o posterior de PAN-OS. Debe asegurarse de que la versión de Panorama sea igual o superior a su versión de PAN-OS en el VM-Series.

Si el cortafuegos VM-Series en AWS GovCloud es sin conexión, debe utilizar el CSP para introducir el ID de CPU, el UUID y el código de autenticación para generar un archivo de licencia que incluya el número de serie. A continuación, puede instalar la licencia en el cortafuegos. Consulte Número de serie y formato de ID de CPU para el cortafuegos VM-Series y Licencias de cortafuegos VM-Series.

Para obtener más información, consulte AMI en AWS GovCloud para realizar la Implementación del cortafuegos VM-Series en AWS.

Cortafuegos VM-Series en AWS China

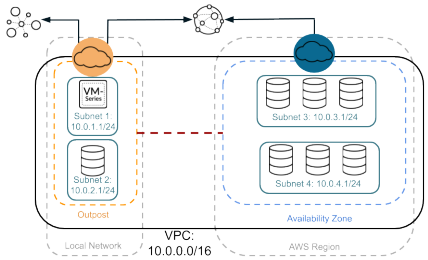
El cortafuegos VM-Series está disponible con la opción BYOL en AWS China Marketplace y está disponible en las regiones de AWS China (Pekín) y AWS China (Ningxia). Debe tener una cuenta de AWS China que sea independiente de su cuenta global de AWS para acceder a esta imagen y usar los recursos de AWS en AWS China.

Asegúrate de revisar los Requisitos del sistema para VM-Series antes del Inicio del cortafuegos VM-Series en AWS.

Cortafuegos VM-Series en AWS Outposts

Para proporcionar el mismo nivel de seguridad a las cargas de trabajo ubicadas in situ que a las cargas de trabajo ubicadas en la nube de AWS, puede instalar el cortafuegos VM-Series en AWS en un bastidor AWS Outposts de forma local. Utilice las AMI de BYOL del marketplace de AWS para su región de AWS, para implementar las instancias del cortafuegos VM-Series en las subredes de AWS Outposts.

 ©2024 Palo Alto Networks, Inc.



Consulte Registro del cortafuegos VM-Series (con código de autenticación) para crear una cuenta de asistencia técnica y registrar el cortafuegos VM-Series en el sitio web de atención al cliente de Palo Alto Networks para activar su derecho a asistencia con Palo Alto Networks.

Terminología de AWS

En este documento se da por hecho que ya conoce la red y la configuración de la VPC de AWS. Con el fin de proporcionar contexto para los términos utilizados en esta sección, a continuación presentamos una breve actualización sobre los términos de AWS (algunas definiciones se han tomado directamente del glosario de AWS) a los que se hace referencia en este documento:

Término	Description (Descripción)
EC2	Elastic Compute Cloud Un servicio web que le permite iniciar y gestionar instancias de servidores Linux/UNIX y Windows en centros de datos de Amazon.
AMI	Amazon Machine Image Una AMI proporciona la información necesaria para iniciar una instancia, que es un servidor virtual en la nube. La AMI de VM-Series es una imagen de equipo cifrada que incluye el sistema operativo necesario para crear una instancia del cortafuegos VM-Series en una instancia de EC2.
ELB	Equilibrio de carga elástico ELB es un servicio Amazon web que le ayuda a mejorar la disponibilidad y escalabilidad de sus aplicaciones dirigiendo el tráfico a través de múltiples instancias de Elastic Compute Cloud (EC2). ELB detecta las instancias EC2 insanas y redirige el tráfico a instancias sanas hasta que se restauran las instancias insanas. ELB puede enviar tráfico solamente a la interfaz primaria del siguiente instancia EC2 de carga equilibrada de salto. Por lo tanto, para utilizar el ELB con un cortafuegos VM-Series en AWS, es necesario que el cortafuegos puede utilizar la interfaz principal para el tráfico del plano de datos.
ENI	Interfaz de red elástica Una interfaz de red adicional que se puede adjuntar a una instancia EC2. Las ENI pueden incluir una dirección IP privada principal, una o más

 ©2024 Palo Alto Networks, Inc.

Término	Description (Descripción)
	direcciones IP privadas secundarias, una dirección IP pública, una dirección IP elástica (opcional), una dirección MAC, miembros de grupos de seguridad especificados, una descripción y una marca de comprobación de origen/destino.
Tipos de direcciones IP para instancias de EC2	Una instancia de EC2 puede tener diferentes tipos de direcciones IP. • Dirección IP pública. Una dirección IP que se puede enrutar a través de internet. • Dirección IP privada: Una dirección IP en el intervalo de direcciones IP privadas como se define en RFC 1918. Puede optar por asignar manualmente una dirección IP o asignar automáticamente una dirección IP dentro del rango en el bloque CIDR para la subred en la que inicia la instancia EC2. Si está asignando manualmente una dirección IP, Amazon reserva las primeras cuatro (4) direcciones IP y la última (1) dirección IP en cada subred para fines de redes IP. • Dirección IP elástica (EIP): Una dirección IP estática que ha asignado en Amazon EC2 o Amazon VPC y, a continuación, adjuntado a una instancia. Las direcciones IP elásticas están asociadas a su cuenta, no a una instancia específica. Son elásticas porque puede asignarlas, adjuntarlas, separarlas y liberarlas fácilmente a medida que cambien sus necesidades. Una instancia en una subred pública puede tener una dirección IP privada, una dirección IP pública y una dirección IP elástica (EIP); una instancia en una subred privada tendrá una dirección IP privada y, opcionalmente, tendrá un EIP.
Tipo de instancia	Las especificaciones definidas por Amazon que determinan la memoria, CPU, capacidad de almacenamiento y coste por hora de una instancia. Algunos tipos de instancias están diseñados para aplicaciones estándar, mientras que otros están diseñados para aplicaciones de uso intensivo de la memoria y la CPU, etc.
VPC	nube privada virtual Una red elástica que incluye infraestructura, plataforma y servicios de aplicaciones que comparten una seguridad e interconexión comunes.
IGW	Puerta de enlace de Internet ofrecida por Amazon. Conecta una red a internet. Puede dirigir el tráfico de las direcciones IP fuera de su VPC a la puerta de enlace de internet.
Función de IAM	Gestión de acceso e identidad Necesaria para habilitar la Alta disponibilidad para el cortafuegos VM-Series en AWS. La función de IAM define las acciones y los recursos de la API que

 ©2024 Palo Alto Networks, Inc.

Término	Description (Descripción)
	la aplicación puede usar después de asumir la función. En una conmutación por error, la función de IAM permite al cortafuegos VM-Series realizar solicitudes de API de manera segura para cambiar las interfaces del plano de datos de peer activo a peer pasivo. También es necesaria una función IAM para la supervisión de VM. Consulte Lista de atributos supervisados en la VPC de AWS.
Subredes	Un segmento del intervalo de direcciones IP de una VPC a la que se pueden adjuntar instancias de EC2. Las instancias de EC2 se agrupan en subredes en función de sus necesidades de seguridad y operativas. Hay dos tipos de subredes: • Subred privada: No se puede acceder a las instancias de EC2 en esta subred desde internet. • Subred pública: La puerta de enlace de internet está adjuntada a la subred pública, y se puede acceder a las instancias de EC2 en esta subred desde internet.
Grupos de seguridad	Un grupo de seguridad se adjunta a una ENI y especifica la lista de protocolos, puertos e intervalos de direcciones IP que tienen permiso para establecer conexiones entrantes y salientes en la interfaz. *En la VPC de AWS, los grupos de seguridad y las ACL de red controlan el tráfico entrante y saliente; los grupos de seguridad regulan el acceso a la instancia de EC2, mientras que las ACL de red regulan el acceso a la subred. Dado que está implementando el cortafuegos VM-Series, establezca reglas más permisivas en sus grupos de seguridad y ACL de red y permita al cortafuegos habilitar aplicaciones de forma segura en la VPC.*
Tablas de enrutamiento	Un conjunto de reglas de enrutamiento que controla el tráfico saliente de cualquier subred asociada a una tabla de enrutamiento. Una subred puede estar asociada a una sola tabla de enrutamiento.
Par de claves	Un conjunto de credenciales de seguridad que puede usar para demostrar su identidad de manera electrónica. El par de claves consiste en una clave privada y una pública. En el momento de iniciar el cortafuegos VM-Series, debe generar un par de claves o seleccionar uno existente para el cortafuegos VM-Series. La clave privada es obligatoria para acceder al cortafuegos en el modo de mantenimiento.
CloudWatch	Amazon CloudWatch es un servicio de supervisión que le permite recopilar y supervisar métricas para los cortafuegos VM-Series en AWS. Cuando está habilitado, los cortafuegos utilizan las API de AWS para publicar métricas de PAN-OS nativas en CloudWatch.

 ©2024 Palo Alto Networks, Inc.

Asignación de interfaz de gestión para su uso con Amazon ELB

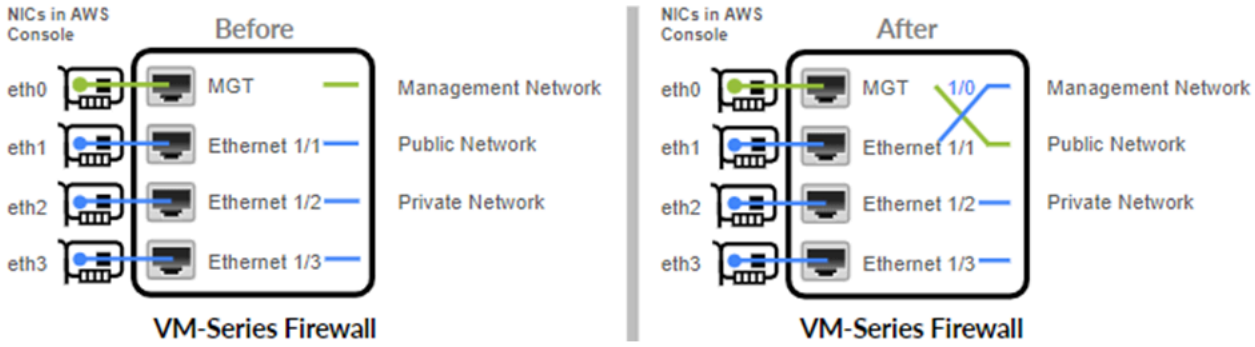
Por defecto, se asigna la interfaz de red elástica (ENI) eth0 a la interfaz MGT en el cortafuegos y se asigna ENI eth1 a ethernet 1/1 en el cortafuegos. Debido a que el ELB puede enviar tráfico solamente a la interfaz principal de la siguiente instancia EC2 de carga equilibrada, el cortafuegos VM-Series debe poder utilizar la interfaz principal para el tráfico de plano de datos.

El cortafuegos puede recibir tráfico del plano de datos en la interfaz principal en los siguientes escenarios en los que el cortafuegos VM-Series está detrás del servicio Amazon ELB:

- Los cortafuegos VM-Series protegen el tráfico de salida directamente a internet sin necesidad de utilizar un enlace VPN o un enlace de conexión directa a la red corporativa.
- El cortafuegos VM-Series protege la aplicación que se conecta a internet cuando hay exactamente un servidor backend, como un servidor web, para cada cortafuegos. Los cortafuegos VM-Series y los servidores web pueden escalar de forma lineal, en pares, detrás del ELB.

En la actualidad, para casos de uso que requieren una implementación del ELB de tipo sándwich para ampliar cortafuegos e instancias de EC2 de capa de aplicación, el intercambio de la interfaz de gestión no le permitirá implementar correctamente la solución ELB. La habilidad para intercambiar la interfaz de gestión solo resuelve parcialmente la integración con el ELB.

Para que el cortafuegos envíe y reciba tráfico del plano de datos en eth0, en vez de eth1, debe intercambiarse la asignación de los ENI en el cortafuegos, como que ENI eth0 se asigne a ethernet 1/1 y ENI eth1 se asigne a la interfaz MGT en el cortafuegos, como se muestra a continuación.



Si es posible, intercambie la interfaz de gestión antes de configurar el cortafuegos o definir las reglas de política.

El intercambio de la asignación de las interfaces asignadas permite a ELB distribuir y dirigir el tráfico a instancias sanas del cortafuegos VM-Series situadas en la mismas o diferentes zonas de disponibilidad en AWS para aumentar la capacidad y la tolerancia a los fallos.

El intercambio de interfaz solo es necesario cuando el cortafuegos VM-Series está detrás del servicio ELB de Amazon. Si su requerimiento es implementar los cortafuegos VM-Series en una configuración tradicional de alta disponibilidad, no necesita configurar el intercambio de interfaz que se describe en esta sección. Continúe a Alta disponibilidad para el cortafuegos VM-Series en AWS.

Para intercambiar las interfaces, se dispone de las siguientes opciones:

- **Al inicio**: cuando se inicia el cortafuegos, se puede introducir el comando**`mgmt-interface-swap=enable`** en el campo de **User data (Datos de usuario)** de la consola de gestión de AWS

 ©2024 Palo Alto Networks, Inc.

(consulte Inicio del cortafuegos VM-Series en AWS) o la CLI o se puede incluir el nuevo comando de operación **`mgmt-interface-swap`** en la configuración de arranque.

- **Después del inicio**: después de que inicie el cortafuegos, use la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión (comando operativo **`set system setting mgmt-interface-swap enable yes`**) en el cortafuegos.



- *Para evitar un comportamiento no predecible en el cortafuegos, elija un método para especificar coherentemente el ajuste de intercambio de interfaz; en la configuración de arranque, de la CLI del cortafuegos, o utilizando el campo **User data (Datos de usuario)** de Amazon EC2 en la consola de AWS.*
- *Asegúrese de tener acceso a la consola de AWS (consola de gestión o CLI) para visualizar la dirección IP de la interfaz eth1. Asimismo, verifique que las reglas del Grupo de seguridad de AWS permiten conexiones (HTTPS y SSH) a la nueva interfaz de gestión.*
- *Si ha configurado el cortafuegos o ha definido reglas de política antes del intercambio de interfaz, compruebe si alguna dirección IP cambia para las reglas de política de impacto eth0 o eth1.*

Ajuste del rendimiento para el cortafuegos VM-Series en AWS

Las siguientes configuraciones afectan al rendimiento:

- Las versiones 9.0.3 y anteriores de PAN-OS admiten tipos de instancia de AWS C5 y M5 que cuentan con soporte para el Adaptador de red elástico (Elastic Network Adapter) para el modo SR-IOV de forma predeterminada. Para obtener más información, consulte Elastic Network Adapter: Interfaz de red de alto rendimiento de para Amazon EC2.
- Las versiones 9.0.4 y posteriores de PAN-OS proporcionan compatibilidad con DPDK para los tipos de instancia C5 y M5 de forma predeterminada. Cuando el cortafuegos está en modo DPDK, utiliza controladores DPDK. Para obtener una lista de los controladores compatibles, consulte Controladores PacketMMAP y PDK en cortafuegos VM-Series y las notas de la versión oficial de DPDK.
- Para beneficiarse de la encapsulación de IETF RFC 8926 (Geneve) y de un rendimiento mejorado, actualice a PAN-OS 10.0.2 o posterior y consulte la Integración de VM-Series con el Balanceador de carga gateway de AWS.

Utilice la CLI de VM-Series para ver la configuración de DPDK o habilitar la E/S empaquetada.

Ver la configuración de DPDK en el cortafuegos

STEP 1 | Inicie sesión en la CLI del cortafuegos VM-Series.

STEP 2 | Vea su configuración de DPDK. Si DPDK está habilitado, el resultado es el siguiente:

```
> 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
```

 ©2024 Palo Alto Networks, Inc.

Habilitar E/S empaquetada de DPDK

STEP 1 | Inicie sesión en el cortafuegos VM-Series

STEP 2 | Habilite DPDK:

```
> set system setting dpdk-pkt-io on
```

STEP 3 | Reinicie el dispositivo.

En el cortafuegos, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y seleccione **Reboot Device (Reiniciar dispositivo)**.

 ©2024 Palo Alto Networks, Inc.

Implementaciones compatibles con AWS

El cortafuegos VM-Series protege el tráfico entrante y saliente de las instancias de EC2 dentro de la Virtual Private Cloud (VPC) de AWS. Dado que la VPC de AWS sólo admite una red IP (funciones de red de capa 3), el cortafuegos VM-Series sólo se puede implementar con interfaces de capa 3.

- Implemente el cortafuegos VM-Series para proteger las instancias de EC2 alojadas en la AWS Virtual Private Cloud.

  Si aloja sus aplicaciones en la nube de AWS, implemente el cortafuegos VM-Series para proteger y habilitar de forma segura aplicaciones para los usuarios que acceden a las mismas a través de internet. Por ejemplo, el siguiente diagrama muestra el cortafuegos VM-Series implementado en la subred de extremo a la que está adjuntada la puerta de enlace de internet. Las aplicaciones se implementan en la subred privada, que no tiene acceso directo a internet.

  Cuando los usuarios necesitan acceder a las aplicaciones en la subred privada, el cortafuegos recibe la solicitud y la dirige a la aplicación apropiada, tras verificar la política de seguridad y realizar la NAT de destino. En la ruta de retorno, el cortafuegos recibe el tráfico, aplica la política de seguridad y usa la NAT de origen para entregar el contenido al usuario. Consulte Caso de uso: Protección de las instancias de EC2 en AWS Cloud.

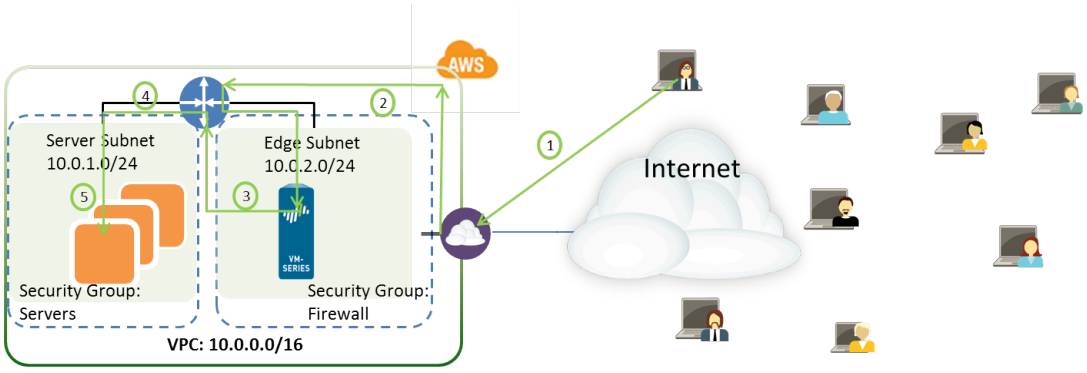


Figure 1: VM-Series para instancias de EC2

- Implemente el cortafuegos VM-Series para obtener acceso VPN entre la red corporativa y las instancias de EC2 dentro de la AWS Virtual Private Cloud.

  Para conectar su red corporativa con las aplicaciones implementadas en la AWS Cloud, puede configurar el cortafuegos como un punto de terminación para un túnel VPN de IPSec. Este túnel VPN permite a los usuarios en su red para acceder de forma segura a las aplicaciones en la nube.

  Para la gestión centralizada, la aplicación consistente de políticas en toda su red y la creación centralizada de logs e informes, también puede implementar Panorama en su red corporativa. Si necesita configurar el acceso VPN a VPC múltiples, el uso de Panorama le permite agrupar los cortafuegos por regiones y administrarlos de forma sencilla.

 ©2024 Palo Alto Networks, Inc.

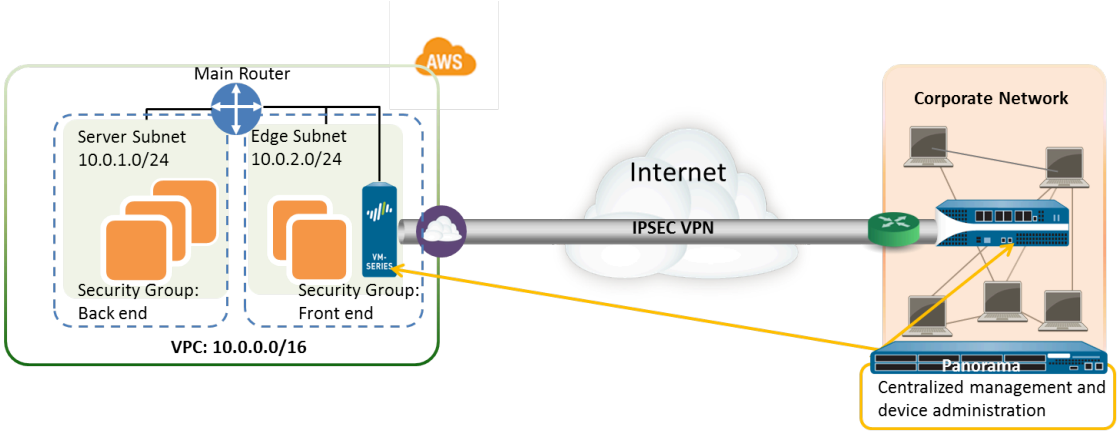


Figure 2: VM-Series para acceso VPN

- Implemente el cortafuegos VM-Series como una puerta de enlace de GlobalProtect para permitir el acceso a usuarios remotos de forma segura desde ordenadores portátiles. El agente de GlobalProtect en el portátil conecta con la puerta de enlace, y basándose en la solicitud, la puerta de enlace configura una conexión de VPN a la red corporativa o dirige la solicitud a internet. Para aplicar el cumplimiento con la seguridad para usuarios de dispositivos móviles (mediante el uso de la aplicación GlobalProtect), la puerta de enlace de GlobalProtect se usa junto con el gestor de seguridad móvil de GlobalProtect. El gestor de seguridad móvil de GlobalProtect garantiza que los dispositivos se gestionen y configuren con la configuración del dispositivo y la información de cuentas para su uso con aplicaciones y redes corporativas.

  En cada uno de los casos anteriores, puede implementar el cortafuegos VM-Series en un par de alta disponibilidad (HA) activo/pasivo. Para obtener información sobre la configuración del cortafuegos VM-Series en HA, consulte Caso de uso: Uso de grupos de direcciones dinámicas para proteger las nuevas instancias de EC2 en la VPC.

- Implemente el cortafuegos VM-Series con el servicio Amazon Elastic Load Balancing (ELB); el cortafuegos puede recibir tráfico del plano de datos en la interfaz principal en los siguientes escenarios en los que el cortafuegos VM-Series está detrás de Amazon ELB:
  - Los cortafuegos VM-Series protegen el tráfico de salida directamente a internet sin necesidad de utilizar un enlace VPN o un enlace de conexión directa a la red corporativa.
  - El cortafuegos VM-Series protege la aplicación que se conecta a internet cuando hay exactamente un servidor back-end, como un servidor web, para cada cortafuegos. Los cortafuegos VM-Series y los servidores web pueden escalar de forma lineal, en pares, detrás del ELB.

 ©2024 Palo Alto Networks, Inc.

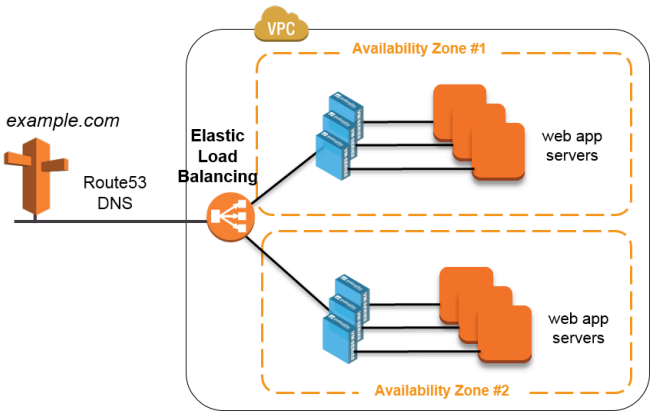


Figure 3: VM-Series con ELB

No se puede configurar el cortafuegos para enviar y recibir tráfico del plano de datos en eth0 cuando el cortafuegos está delante del ELB. El cortafuegos VM-Series debe estar detrás del Amazon ELB.

Es posible Usar de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión *o habilitarla durante el arranque. Para obtener detalles, consulte* Asignación de interfaz de gestión para su uso con Amazon ELB.

Además de los enlaces anteriores que están cubiertos conforme a la política de soporte oficial de Palo Alto Networks, Palo Alto Networks proporciona plantillas con soporte de la comunidad en el repositorio Palo Alto Networks GitHub *que le permite explorar las soluciones disponibles para iniciar rápidamente su recorrido hacia la automatización de la nube y el escalado en AWS. Consulte* AWS Transit VPC *para una implementación de concentrador y VPC suscriptor que le permite asegurar el tráfico entre los VPC, entre un VPC y un recurso de nube local/híbrida, y el tráfico saliente seguro a internet.*

 ©2024 Palo Alto Networks, Inc.

Implementación del cortafuegos VM-Series en AWS

- Obtención de la AMI
- Hoja de trabajo para la planificación de VM-Series en la VPC de AWS
- Inicio del cortafuegos VM-Series en AWS
- Inicio del cortafuegos VM-Series en AWS Outposts
- Creación de una imagen Amazon Machine Image personalizada (AMI)
- Cifrado del volumen EBS para el cortafuegos VM-Series en AWS
- Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión
- Habilitación de la supervisión de CloudWatch en el cortafuegos VM-Series
- Inicio de cortafuegos VM-Series y logs de estado en AWS

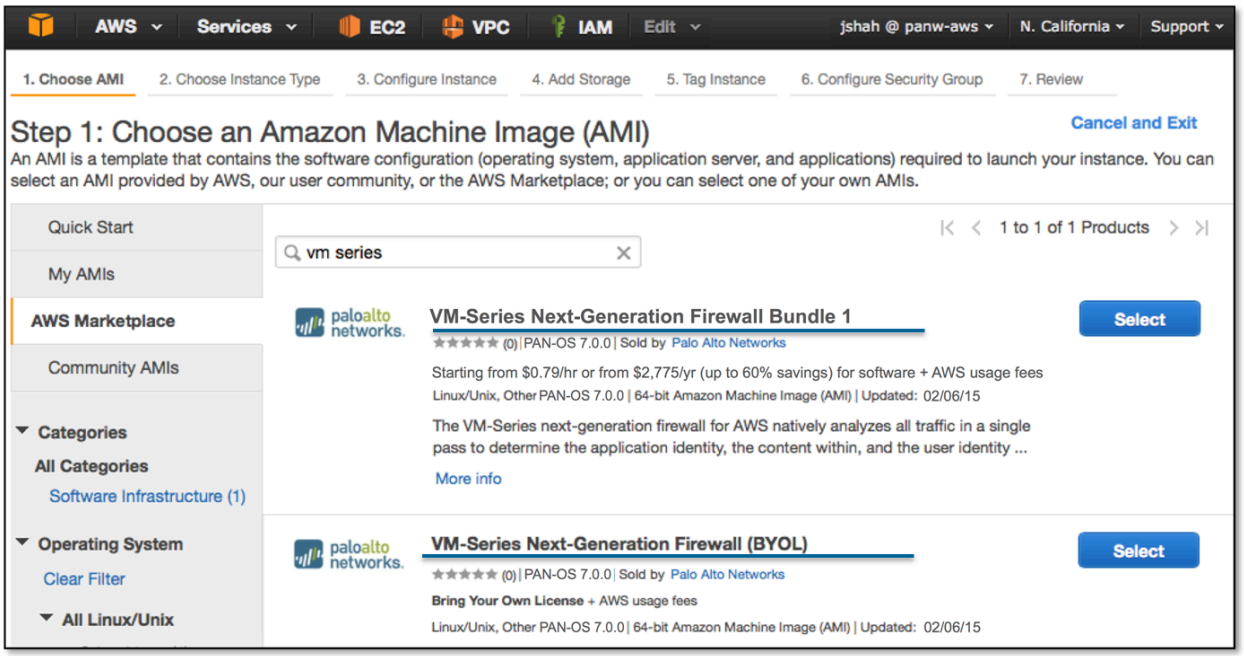
Obtención de la AMI

Obtenga la Amazon Machine Image para la nube pública de AWS y AWS GovCloud desde la perspectiva de Marketplace.

- AMI en la nube AWS pública
- AMI en AWS GovCloud
- Obtención del ID de imagen de máquina de Amazon (AMI) del cortafuegos VM-Series

AMI en la nube AWS pública

La AMI para el cortafuegos VM-Series está disponible en el AWS Marketplace para ambas opciones de tarifas Traer su propia licencia (BYOL) y Basada en uso.



 ©2024 Palo Alto Networks, Inc.

Para adquirir licencias con la opción BYOL, póngase en contacto con su ingeniero de sistemas de Palo Alto Networks o distribuidor.

AMI en AWS GovCloud

El modelo de licencia existente (Bring Your Own License, BYOL) y el modelo basado en el uso del cortafuegos VM-Series están disponibles en AWS GovCloud Marketplace.

Con una cuenta de GovCloud, puede buscar Palo Alto Networks y encontrar las AMI del cortafuegos VM-Series en Marketplace. Asegúrese de revisar los Tipos de instancia de EC2 compatibles antes de iniciar el cortafuegos. Para más detalles, consulte Inicio del cortafuegos VM-Series en AWS.

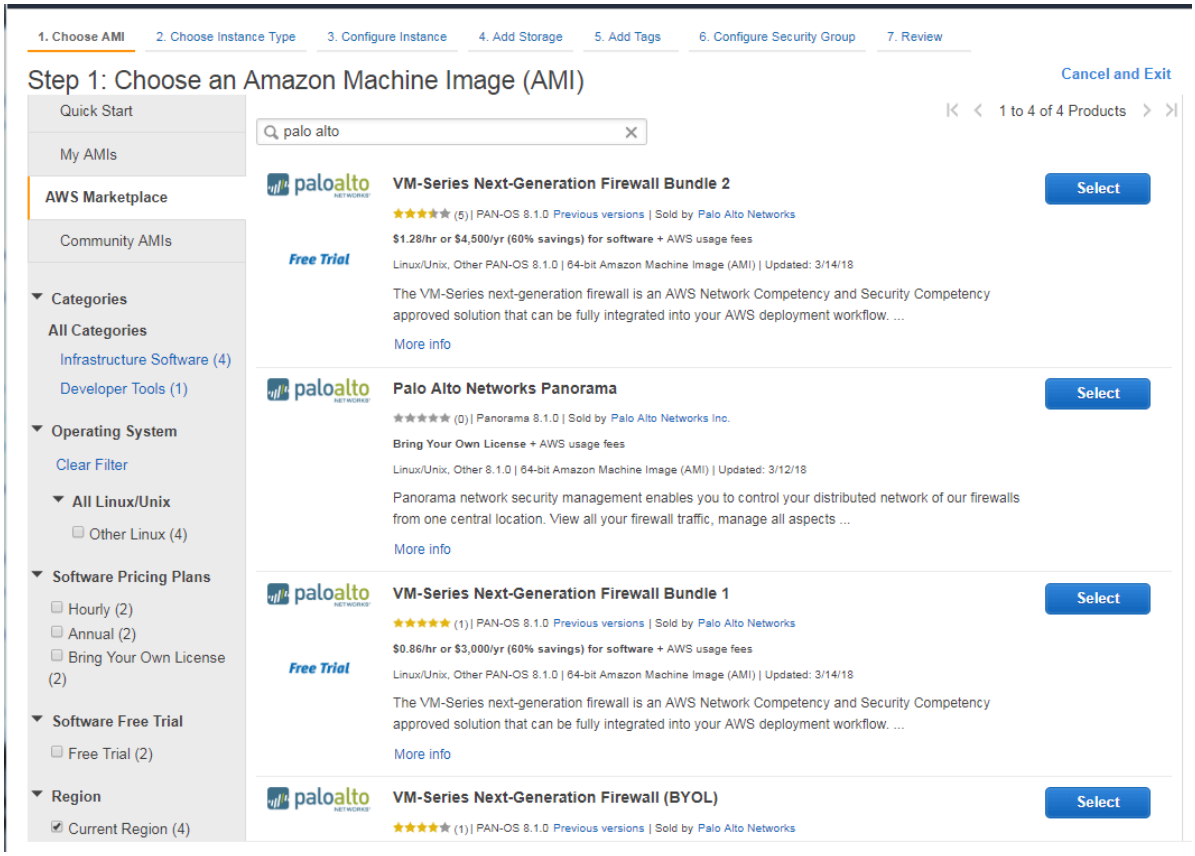


Table 1: Consulte los requisitos y limitaciones del sistema para VM-Series en AWS

Requisito	Detalles
Tipos de instancia de EC2	El tipo de instancia EC2 que seleccione debe cumplir con los Requisitos del sistema VM-Series para el modelo de cortafuegos VM-Series. Si implementa el cortafuegos VM-Series en un tipo de instancia de EC2 que no cumple estos requisitos, el cortafuegos se reiniciará en el modo de mantenimiento

 ©2024 Palo Alto Networks, Inc.

Requisito	Detalles
	Para apoyar la supervisión de VM y lograr una alta disponibilidad en AWS, el cortafuegos VM-Series deberá poder acceder directamente a los endpoints de servicio de la API de AWS sin servidores proxy entre la interfaz de gestión del cortafuegos y los endpoints de la API de AWS (como ec2.us-west-2.amazonaws.com).
Amazon Elastic Block Storage (EBS)	El cortafuegos VM-Series debe usar el volumen de almacenamiento Amazon Elastic Block Storage (EBS). La optimización de EBS ofrece una pila de configuración optimizada y capacidad dedicada y adicional para la E/S de Amazon EBS.
Redes	Dado que AWS sólo admite funciones de red de capa 3, el cortafuegos VM-Series solo se puede implementar con interfaces de capa 3. Las interfaces de capa 2, Virtual Wire, VLAN y las subinterfaces no son compatibles con los cortafuegos VM-Series implementados en la VPC de AWS.
Interfaces	Compatibilidad para un total de ocho interfaces: una interfaz de gestión y un máximo de siete interfaces de red elástica (ENI) para tráfico de datos. El cortafuegos VM-Series no es compatible con la adición en caliente de ENI; para detectar la adición o eliminación de una ENI, debe reiniciar el cortafuegos. *La instancia de EC2 que elija determinará el número total de ENI que puede habilitar. Por ejemplo, c3.8xlarge admite ocho (8) ENI.*
Derechos de asistencia y licencias	Para el modelo con licencia existente, se necesita una cuenta de asistencia y una licencia VM-Series válida para obtener el archivo Amazon Machine Image (AMI), necesario para instalar el cortafuegos VM-Series en la VPC de AWS. Las licencias necesarias para el cortafuegos VM-Series (licencia de capacidad, licencia de asistencia y suscripciones para la prevención de amenazas, filtrado de URL, WildFire, etc.) deben adquirirse en Palo Alto Networks. Para adquirir las licencias para su implementación, póngase en contacto con su representante de ventas. Consulte Licencias de cortafuegos VM-Series para nubes públicas. Para el modelo con licencia basada en el uso, se pueden adquirir los paquetes de precios anuales y por hora que se facturan directamente a AWS. Sin embargo, debe registrar el derecho de asistencia en Palo Alto Networks. Para más detalles, consulte Registro del modelo basado en el uso del cortafuegos VM-Series para nubes públicas (sin código de autenticación).

 ©2024 Palo Alto Networks, Inc.

Obtención del ID de imagen de máquina de Amazon (AMI) del cortafuegos VM-Series

Utilice las siguientes instrucciones para encontrar el ID de AMI para el cortafuegos VM-Series que coincida con la versión de PAN-OS, el tipo de licencia y la región de AWS en la que desea iniciar el cortafuegos VM-Series.

STEP 1 | Instale la CLI de AWS en el cliente que está utilizando para recuperar la ID de AMI e inicie sesión con sus credenciales de AWS.

Consulte su documentación de AWS para obtener instrucciones sobre cómo instalar la CLI.

STEP 2 | Encuentre el ID de AMI con el siguiente comando CLI.

```
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
```

Necesita sustituir el valor en los corchetes angulares <> con la información relevante como se muestra a continuación:

- Utilice el código de producto VM-Series para cada tipo de licencia. Los valores son:
  - Bundle 1—

    ```
    e9yfvyj3uag5uo5j2hjikv74n
    ```

  - Bundle 2—

    ```
    hd44w1chf26uv4p52cdynb2o
    ```

  - BYOL—

    ```
    6njl1pau431dv1qxipg63mvah
    ```

- Utilice la versión PAN-OS: 10.0. Si hay varias versiones de funciones dentro de una versión de PAN-OS, se enumeran todos los ID de AMI. Por ejemplo, en 9.0.x, verá una lista de los ID de AMI para las versiones 9.0, 9.0.3 y 9.0.5.xfr de PAN-OS, y 9.0.6 y puede usar el ID de AMI para la versión PAN-OS que necesita.
- Obtenga los detalles de la región de AWS en: https://docs.aws.amazon.com/general/latest/gr/rande.html.

Por ejemplo: Para encontrar el ID de AMI para el paquete 1 de VM-Series para PAN-OS 10.0.0 en la región de California de EE. UU., el comando CLI es:

```
 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 salida es:

```
{ "ProductCodes": [ { "ProductCodeId":
"e9yfvyj3uag5uo5j2hjikv74n", "ProductCodeType": "marketplace" } ],
"VirtualizationType": "hvm", "Hypervisor": "xen",
"ImageOwnerAlias": "aws-marketplace", "EnaSupport": true,
"SriovNetSupport": "simple", "ImageId": "ami-06f7a63d7481d0ded",
```

 ©2024 Palo Alto Networks, Inc.

```
 "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" }
```

También puede generar resultados en formato de tabla. Por ejemplo, para ver la imagen AMI para BYOL para 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 |+----------------------
+-----------------------------------------------------------------------------
+-------------+
```

Hoja de trabajo para la planificación de VM-Series en la VPC de AWS

Para facilitar la implementación, planifique las subredes de la VPC y las instancias de EC2 que quiere implementar en cada subred. Antes de empezar, use la siguiente tabla para cotejar la información de red necesaria para implementar e insertar los cortafuegos VM-Series en el flujo de tráfico de VPC:

Elemento de configuración	Valor
CIDR de VPC	
Grupos de seguridad	
CIDR de subred (pública)	
CIDR de subred (privada)	
Tabla de enrutamiento de subred (pública)	

 ©2024 Palo Alto Networks, Inc.

Elemento de configuración	Valor
Tabla de enrutamiento de subred (privada)	
Grupos de seguridad • Reglas de configuración del acceso a la gestión del cortafuegos (eth0/0) • Reglas de acceso a las interfaces del plano de datos del cortafuegos • Reglas para el acceso a las interfaces asignadas a los servidores de aplicaciones.	
Cortafuegos VM-Series detrás del ELB	
Instancia 1 de EC2 (cortafuegos VM-Series) *Sólo se requiere una EIP para la interfaz de plano de datos conectada a la subred pública.*	Subred: Tipo de instancia: IP de interfaz de gestión: EIP de interfaz de gestión: Interfaz de plano de datos eth1/1 • IP privada: • EIP (en caso necesario): • Grupo de seguridad: Interfaz de plano de datos eth1/2 • IP privada: • EIP (en caso necesario): • Grupo de seguridad:
Instancia 2 de EC2 (aplicación que se va a proteger) Repita este conjunto de valores para las aplicaciones adicionales que se implementen.	Subred: Tipo de instancia: IP de interfaz de gestión: Puerta de enlace predeterminada: Interfaz de plano de datos 1 • IP privada:

 ©2024 Palo Alto Networks, Inc.

Elemento de configuración	Valor
Requisitos para HA	Si va a implementar los cortafuegos VM-Series en una configuración de alta disponibilidad (activa/pasiva), debe asegurarse de lo siguiente: • Crear una función de IAM y asignar la función al cortafuegos VM-Series cuando implemente la instancia. Consulte Funciones de IAM para HA. • Implemente los peers de HA en la misma zona de disponibilidad de AWS. • El cortafuegos activo en el par de HA debe tener un mínimo de tres ENI: dos interfaces del plano de datos y una interfaz de gestión. El cortafuegos pasivo en el par de HA debe tener una ENI para gestión y una ENI que funcione como interfaz del plano de datos; usted configurará la interfaz del plano de datos como una interfaz de HA2. *No adjunte interfaces del planos de datos adicionales al cortafuegos pasivo en el par de HA. En una conmutación por error, las interfaces del plano de datos del cortafuegos anteriormente activo se mueven (se desasocian y luego se adjuntan) al cortafuegos ahora activo (anteriormente pasivo).*

Inicio del cortafuegos VM-Series en AWS

Si no ha registrado todavía el código de autenticación de capacidad que ha recibido con el correo electrónico de cumplimiento del pedido, con su cuenta de asistencia, consulte Registro del cortafuegos VM-Series. Una vez registrado, implemente el cortafuegos VM-Series mediante una AMI publicada en Marketplace o Creación de una imagen Amazon Machine Image personalizada (AMI) en el VPC de AWS del siguiente modo:

STEP 1 | Acceda a la consola de AWS.

Inicie sesión en la consola de AWS y seleccione el panel EC2.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configure la VPC según sus necesidades de red.

Tanto si inicia el cortafuegos VM-Series en una VPC existente o crea una nueva VPC, el cortafuegos VM-Series debe poder recibir tráfico desde las instancias de EC2 y realizar comunicaciones de entrada y salida entre la VPC e internet.

Consulte las instrucciones para crear una VPC y configurar el acceso a esta en la documentación de la VPC de AWS.

En Caso de uso: puede consultar un ejemplo con un flujo de trabajo completo: Protección de las instancias de EC2 en AWS Cloud.

1. Cree una nueva VPC o use una existente. Consulte la documentación de la Guía de inicio de AWS.
2. Compruebe que los componentes de red y seguridad están definidos adecuadamente.
   - Habilite la comunicación con internet. La VPC predeterminada incluye una puerta de enlace de internet, y si instala el cortafuegos VM-Series en la subred predeterminada, tendrá acceso a internet.
   - Cree subredes. Las subredes son segmentos de intervalos de direcciones IP asignados a la VPC en las que puede iniciar las instancias de EC2. El cortafuegos VM-Series debe pertenecer a la subred pública para que se pueda configurar su acceso a internet.
   - Cree grupos de seguridad según sea necesario para gestionar el tráfico entrante y saliente desde las instancias o subredes de EC2.
   - Añada rutas a la tabla de enrutamiento para una subred privada para garantizar que el tráfico se puede dirigir a través de subredes y grupos de seguridad en la VPC, según corresponda.
3. Si desea implementar un par de cortafuegos VM-Series en HA, debe definir las Funciones de IAM para HA antes de que pueda realizar la Configuración de la HA activa/pasiva en AWS.
4. (Opcional) Si está utilizando el arranque para realizar la configuración del cortafuegos VM-Series, consulte Arranque del cortafuegos VM-Series en AWS. Para obtener más información sobre el arranque, consulte Arranque del cortafuegos VM-Series y Seleccione un método de arranque.

STEP 3 | Inicie el cortafuegos VM-Series.

A pesar de que puede añadir interfaces de red adicionales (las ENI) al cortafuegos VM-Series cuando inicia, AWS libera la dirección IP pública asignada automáticamente para la interfaz de gestión cuando usted reinicia el cortafuegos. Por lo tanto, para garantizar la conectividad a la interfaz de gestión, debe asignar una dirección IP elástica para la interfaz de gestión antes de adjuntar interfaces adicionales al cortafuegos.

Si desea conservar la dirección EIP, puede asignar una dirección EIP a la interfaz eth 1/1 y usarla para el tráfico de gestión y el tráfico de datos. Para restringir los servicios permitidos en la interfaz o limitar

 ©2024 Palo Alto Networks, Inc.

las direcciones IP que pueden iniciar sesión en la interfaz eth 1/1, adjunte un perfil de gestión a la interfaz.

1. En el panel EC2, haga clic en **Launch Instance (Iniciar instancia)**.
2. Seleccione la AMI de VM-Series. Para obtener la AMI, consulte Obtención de la AMI.
3. Inicie el cortafuegos VM-Series en la instancia de EC2.
    1. Elija el **EC2 instance type (Tipo de instancia de EC2)** para asignar los recursos requeridos para el cortafuegos y haga clic en **Next (Siguiente)**. Consulte Requisitos del sistema VM-Series para ver los requisitos de recursos.
    2. Seleccione la VPC.
    3. Seleccione la subred pública a la que se adjuntará la interfaz de gestión de VM-Series.
    4. Seleccione **Automatically assign a public IP address (Asignar automáticamente una dirección IP pública)**. Esto le permite obtener una dirección IP de acceso público para la interfaz de gestión del cortafuegos VM-Series.

        Posteriormente, puede adjuntar una dirección IP elástica a la interfaz de gestión; a diferencia de la dirección IP pública, que deshace la asociación con el cortafuegos cuando se finaliza la instancia, la dirección IP elástica ofrece continuidad y se puede volver a adjuntar a una

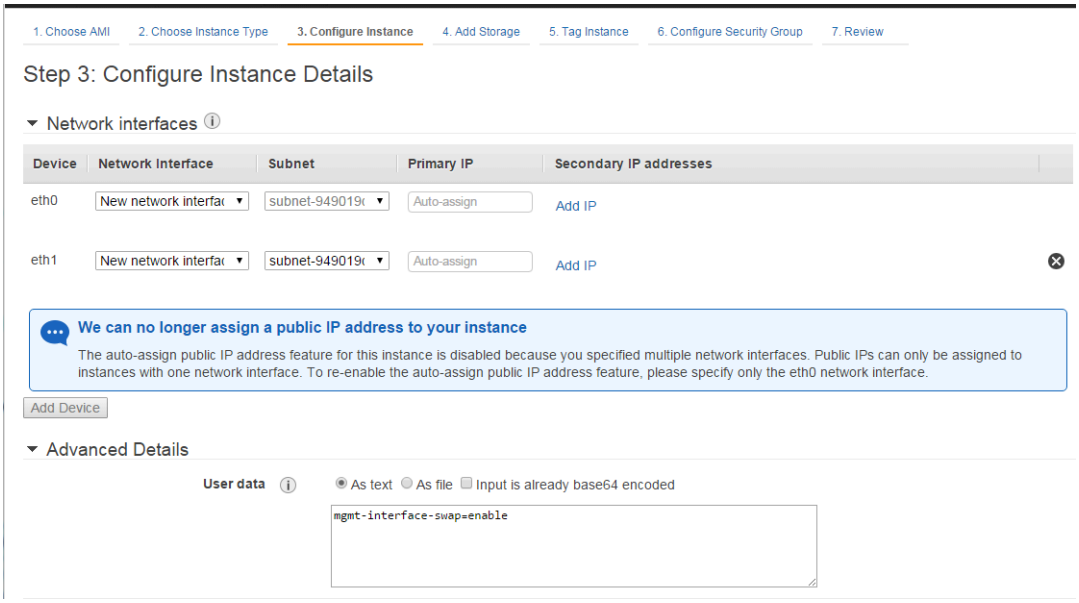
 ©2024 Palo Alto Networks, Inc.

nueva instancia (o una de sustitución) del cortafuegos VM-Series sin necesidad de volver a configurar la dirección IP, independientemente de la ubicación de referencia que tenga.

5. Seleccione **Launch as an EBS-optimized instance (Iniciar como instancia optimizada para EBS)**.
6. Añada otra interfaz de red para implementaciones con ELB, para que pueda intercambiar las interfaces de gestión y datos en el cortafuegos. El intercambio de interfaces requiere un mínimo de dos ENI (eth0 y eth1).
   - Expanda la sección de interfaces de red y haga clic en **Añadir dispositivo** para añadir otra interfaz de red.

     Asegúrese de que su VPC tiene más de una subred, para que pueda añadir ENI adicionales al inicio.

     Si inicia el cortafuegos con solo un ENI:
     - *El comando de intercambio de interfaz hará que el cortafuegos arranque en el modo de mantenimiento.*
     - *Debe reiniciar el cortafuegos cuando añade el segundo ENI.*
   - Expanda la sección Detalles avanzados y en el campo **`User data (Datos de usuario)`** introduzca **mgmt-interface-swap=enable** como texto para realizar el intercambio de interfaz durante el inicio.



Bootstrap Package (Paquete de arranque): si arranca el cortafuegos con el paquete de arranque, también puede introducir un separador de punto y coma después de **`mgmt-interface-swap = enable`**, luego introduzca **`vmseries-bootstrap -aws-s3bucket =<bucketname>`**.

User Data (Datos de usuario): si arranca con datos de usuario, introduzca un separador de punto y coma después de **`mgmt-interface-swap = enable`** e introduzca pares

 ©2024 Palo Alto Networks, Inc.

clave-valor adicionales de acuerdo con Introduzca una configuración básica como datos de usuario (AWS, Azure o GCP).

AWS Secret (Secreto de AWS): si arranca con un secreto de AWS, introduzca un separador de punto y coma después de **`mgmt-interface-swap = enable`** e introduzca el nombre del secreto como un par clave-valor, como se describe en el Paso 3 de Arranque del cortafuegos VM-Series en AWS. Por ejemplo:

7. Acepte la configuración de **Storage (Almacenamiento)** predeterminada. El cortafuegos utiliza el tipo de volumen SSD (gp2).

   La primera vez que se accede al cortafuegos se solicita este par de claves. También es necesario acceder al cortafuegos en el modo de mantenimiento.

8. (Opcional) **Tagging (Etiquetado)**. Añada una o más etiquetas para crear sus propios metadatos e identificar y agrupar el cortafuegos VM-Series. Por ejemplo, añada una etiqueta **Name (Nombre)** con un **Value (Valor)** que le ayude a recordar que las interfaces ENI se hayan intercambiado en este cortafuegos VM-Series.
9. Seleccione un **Security Group (Grupo de seguridad)** existente o cree uno nuevo. Este grupo de seguridad sirve para restringir el acceso a la interfaz de gestión del cortafuegos. Considere habilitar el acceso https y ssh como mínimo para la interfaz de gestión.
10. Si se le solicita, seleccione una opción de **SSD** adecuada para su configuración.
11. Seleccione **Review and Launch (Revisar e iniciar)**. Revise que sus selecciones son precisas y haga clic en **Launch (Iniciar)**.
12. Seleccione un par de claves existente o cree uno nuevo y acepte el descargo de responsabilidad de claves.
13. Descargue y guarde la clave privada en un lugar seguro; la extensión del archivo es `.pem`. Si pierde la clave, no se puede volver a regenerar.

    Se tardará entre 5 y 7 minutos en iniciar el cortafuegos VM-Series. Puede consultar el progreso en el panel EC2. Al completar el proceso, el cortafuegos VM-Series se muestra en la página **Instances (Instancias)** del panel EC2.

©2024 Palo Alto Networks, Inc.

STEP 4 | Configure una nueva contraseña de administración para el cortafuegos.

En la CLI del cortafuegos VM-Series, debe configurar una contraseña administrativa única para poder acceder a la interfaz web del cortafuegos. Para iniciar sesión en la CLI, necesita la clave privada que ha utilizado para iniciar el cortafuegos.

1. Use la dirección IP pública para hacer SSH en la interfaz de línea de comando (CLI) del cortafuegos VM-Series. Necesitará la clave privada que usó o creó en 3 anteriormente para acceder a la CLI.

   Si añadió un ENI adicional para admitir implementaciones con ELB, primero debe crear y asignar una dirección IP elástica al ENI para acceder a la CLI, consulte 6.

   Si utiliza PuTTY para el acceso SSH, debe convertir el formato .pem al formato .ppk. Consulte https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html
2. Introduzca el siguiente comando para iniciar sesión en el cortafuegos:

   ssh-i <*private_key.pem*> admin@<*public-ip_address*>
3. Configure una nueva contraseña usando el siguiente comando y siga las indicaciones en pantalla:

   configure

   set mgt-config users admin password
4. Si tiene una BYOL que debe activarse, configure la dirección IP del servidor DNS de modo que el cortafuegos pueda acceder al servidor de licencias de Palo Alto Networks. Introduzca el siguiente comando para configurar la dirección IP del servidor DNS:

   set deviceconfig system dns-setting servers primary <*ip_address*>
5. Confirme los cambios con el comando:

   commit
6. Finalice la sesión SSH.

STEP 5 | Apague el cortafuegos VM-Series.

1. En el panel EC2, seleccione **Instances (Instancias)**.
2. En la lista, seleccione el cortafuegos VM-Series y haga clic en **Actions (Acciones)** > **Stop (Detener)**.

STEP 6 | Cree y asigne una dirección IP elástica (Elastic IP address, EIP) a la ENI utilizada para el acceso de gestión al cortafuegos y reinicie el cortafuegos VM-Series.

1. Seleccione **Elastic IP (IP elástica)** y haga clic en **Allocate New Address (Asignar nueva dirección)**.
2. Seleccione **EC2-VPC** y haga clic en **Yes, Allocate (Sí, asignar)**.
3. Seleccione la EIP recién asignada y haga clic en **Associate Address (Asociar dirección)**.
4. Seleccione la **Network Interface (Interfaz de red)** y la **Private IP address (Dirección IP privada)** asociada con la interfaz de gestión y haga clic en **Yes, Associate (Sí, asociar)**.

STEP 7 | Cree interfaces de red virtuales y adjúntelas al cortafuegos VM-Series. Las interfaces de red virtuales se llaman Interfaces de red elásticas (ENI) en AWS y actúan como interfaces de red de plano de

 ©2024 Palo Alto Networks, Inc.

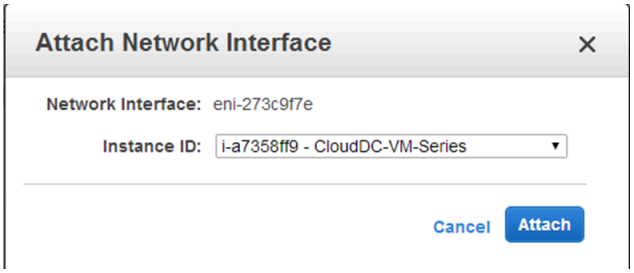
datos en el cortafuegos. Estas interfaces se usan para la gestión del tráfico de datos desde o hacia el cortafuegos.

Necesitará al menos dos ENI que permitan tráfico entrante y saliente desde o hacia el cortafuegos. Puede añadir hasta siete ENI para gestionar el tráfico de datos en el cortafuegos VM-Series; compruebe su tipo de instancia de EC2 para comprobar el número máximo que admite.

1. En el panel EC2, seleccione **Network Interfaces (Interfaces de red)** y haga clic en **Create Network Interface (Crear interfaz de red)**.
2. Introduzca un nombre descriptivo para la interfaz.
3. Seleccione la subred. Use el ID de subred para asegurarse de que ha seleccionado la subred correcta. Sólo puede adjuntar una ENI a una instancia en la misma subred.
4. Introduzca la dirección de **Private IP (IP privada)** para asignarla a la interfaz y seleccione **Auto-assign (Asignar automáticamente)** para asignar automáticamente una dirección IP dentro de las direcciones IP disponibles en la subred seleccionada.
5. Seleccione el **Security group (Grupo de seguridad)** para controlar el acceso a la interfaz de red del plano de datos.
6. Haga clic en **Yes, Create (Sí, crear)**.



7. Para adjuntar la ENI al cortafuegos VM-Series, seleccione la interfaz que acaba de crear y haga clic en **Attach (Adjuntar)**.



8. Seleccione el **Instance ID (ID de instancia)** del cortafuegos VM-Series y haga clic en **Attach (Adjuntar)**.
9. Repita los pasos anteriores para crear y adjuntar al menos una ENI más al cortafuegos.

STEP 8 | (No es necesario para el modelo con licencia basada en uso) Active las licencias en el cortafuegos VM-Series.

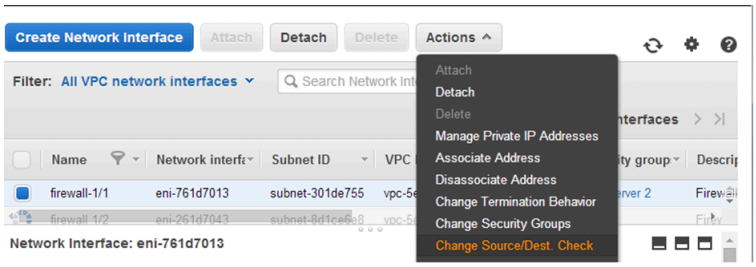
Esta tarea no se realiza en la consola de administración de AWS. Tendrá que acceder al portal de asistencia de Palo Alto Networks y a la interfaz web del cortafuegos VM-Series para activar la licencia.

Consulte Activación de la licencia.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Deshabilite la comprobación de origen/destino en todas las interfaces de red de planos de datos del cortafuegos. Si deshabilita esta opción, permite a la interfaz gestionar el tráfico de red no destinado a la dirección IP asignada a la interfaz de red.

1. En el panel EC2, seleccione la interfaz de red, por ejemplo, eth1/1, en la pestaña **Network Interfaces (Interfaces de red)**.
2. En el menú desplegable **Action (Acción)**, seleccione **Change Source/Dest. (Cambiar comprobación de origen/dest). Check (Comprobar)**.



3. Haga clic en **Disabled (Deshabilitado)** y en **Save (Guardar)** para guardar los cambios.
4. Repita los pasos 1-3 con cada interfaz de plano de datos del cortafuegos.

 ©2024 Palo Alto Networks, Inc.

STEP 10 | Configure las interfaces de red del plano de datos como interfaces de capa 3 en el cortafuegos.

Para una configuración de ejemplo, consulte los pasos 14 a 17 en Caso de uso : Protección de las instancias de EC2 en AWS Cloud.

En los servidores de aplicaciones dentro de la VPC, defina la interfaz de red de plano de datos del cortafuegos como la puerta de enlace predeterminada.

1. Si usa una conexión segura (https) desde su navegador web, inicie sesión usando la dirección EIP y la contraseña que asignó durante la configuración inicial (https://<Elastic_IP address>). Verá una advertencia de certificación; es normal. Vaya a la página web.
2. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
3. Haga clic en el enlace de **ethernet 1/1** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **capa 3**
   - En la pestaña **Config (Configurar)**, asigne la interfaz el enrutador predeterminado.
   - En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. Defina una nueva zona, por ejemplo, VM_Series_untrust, y a continuación haga clic en **OK (Aceptar)**.
   - En la pestaña **IPv4**, seleccione **Static (Estática)** o **DHCP Client (Cliente DHCP)**.

     Si usa la opción **Static (Estática)**, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para la interfaz; por ejemplo, 10.0.0.10/24.

     Asegúrese de que la dirección IP coincide con la dirección IP de la ENI que ha asignado anteriormente.

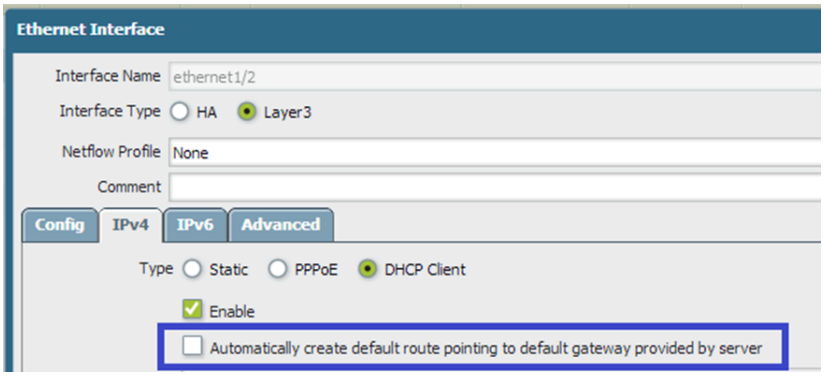
     Si usa DHCP, seleccione **DHCP Client (Cliente DHCP)**; la dirección IP privada que ha asignado a la ENI en la consola de administración de AWS se adquirirá de manera automática.
4. Haga clic en el enlace de **ethernet 1/2** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **capa 3**
   - Security Zone (Zona de seguridad): VM_Series_trust
   - **IP address (Dirección IP)**: Seleccione el botón de opción **Static (Estático)** o **DHCP Client (Cliente DHCP)**.

     Para estático, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para la interfaz. Asegúrese de que la dirección IP coincide con la dirección IP de la ENI adjuntada que ha asignado anteriormente.
5. Haga clic en **Commit (Confirmar)**. Verifique que el enlace para las interfaces esté en estado activo.



 ©2024 Palo Alto Networks, Inc.

Para DHCP, anule la selección de la casilla de verificación ***Automatically create default route to default gateway provided by server (Crear automáticamente ruta predeterminada a la puerta de enlace predeterminada proporcionada por el servidor)****. Para una interfaz adjuntada a la subred privada en la VPC, deshabilitar esta opción garantiza que el tráfico gestionado por esta interfaz no fluya directamente a la puerta de enlace de internet en la VPC.*



STEP 11 | Cree reglas NAT para permitir el tráfico entrante y saliente desde servidores implementados dentro de la VPC.

1. Seleccione **Policies (Políticas)** > **NAT** en la interfaz web del cortafuegos.
2. Cree una regla NAT para permitir el tráfico desde la interfaz de red del plano de datos en el cortafuegos a la interfaz del servidor web en la VPC.
3. Cree una regla NAT para permitir el acceso saliente para el tráfico desde el servidor web a internet.

STEP 12 | Cree políticas de seguridad para permitir/denegar el tráfico entrante y saliente desde servidores implementados dentro de la VPC.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** en la interfaz web del cortafuegos.
2. Haga clic en **Add (Añadir)** y especifique las zonas, aplicaciones y opciones de inicio de sesión que le gustaría ejecutar para restringir el tráfico de auditoría que atraviesa la red.

STEP 13 | Confirme los cambios en el cortafuegos.

Haga clic en **Commit (Confirmar)**.

STEP 14 | Compruebe que el cortafuegos VM-Series protege el tráfico y que las reglas NAT están en vigor.

1. Seleccione **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)** en la interfaz web del cortafuegos.
2. Consulte los logs para asegurarse de que las aplicaciones que atraviesan la red cumplen las políticas de seguridad que ha implementado.

Inicio del cortafuegos VM-Series en AWS Outposts

Complete este procedimiento para implementar el cortafuegos VM-Series en un bastidor AWS Outpost. Si no ha registrado todavía el código de autenticación de capacidad que ha recibido con el correo electrónico de cumplimiento del pedido, con su cuenta de asistencia, consulte Registro del cortafuegos VM-Series.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Acceda a la consola de AWS Outpost.

STEP 2 | Extienda su VPC para incluir su bastidor AWS Outpost.

El cortafuegos VM-Series debe poder recibir tráfico de las instancias EC2 y realizar comunicaciones entrantes y salientes entre la VPC e Internet.

Consulte la documentación de AWS Outpost para obtener instrucciones sobre cómo conectar su Outpost a su VPC.

1. Compruebe que los componentes de red y seguridad están definidos adecuadamente.
   - Habilite la comunicación con internet. Outpost requiere una puerta de enlace local para conectarse a su LAN local y a internet.
   - Cree una subred de Outpost.
   - Cree grupos de seguridad según sea necesario para gestionar el tráfico entrante y saliente desde las instancias o subredes de EC2.
   - Añada rutas a la tabla de enrutamiento para una subred privada para garantizar que el tráfico se puede dirigir a través de subredes y grupos de seguridad en la VPC, según corresponda.
2. Si desea implementar un par de cortafuegos VM-Series en HA, debe definir las Funciones de IAM para HA antes de que pueda Alta disponibilidad para el cortafuegos VM-Series en AWS.
3. (Opcional) Si está utilizando el arranque para realizar la configuración del cortafuegos VM-Series, consulte Arranque del cortafuegos VM-Series en AWS. Para obtener más información sobre el arranque, consulte Arranque del cortafuegos VM-Series.

STEP 3 | Inicie el cortafuegos VM-Series.

A pesar de que puede añadir interfaces de red adicionales (las ENI) al cortafuegos VM-Series cuando inicia, AWS libera la dirección IP pública asignada automáticamente para la interfaz de gestión cuando usted reinicia el cortafuegos. Por lo tanto, para garantizar la conectividad a la interfaz de gestión, debe asignar una dirección IP elástica para la interfaz de gestión antes de adjuntar interfaces adicionales al cortafuegos.

Si desea conservar la dirección EIP, puede asignar una dirección EIP a la interfaz eth 1/1 y usarla para el tráfico de gestión y el tráfico de datos. Para restringir los servicios permitidos en la interfaz o limitar

 ©2024 Palo Alto Networks, Inc.

las direcciones IP que pueden iniciar sesión en la interfaz eth 1/1, adjunte un perfil de gestión a la interfaz.

1. En el panel EC2, haga clic en **Launch Instance (Iniciar instancia)**.
2. Seleccione la AMI de VM-Series. Para obtener la AMI, consulte Obtención de la AMI.
3. Inicie el cortafuegos VM-Series en la instancia de EC2.
    1. Elija el **EC2 instance type (Tipo de instancia de EC2)** para asignar los recursos requeridos para el cortafuegos y haga clic en **Next (Siguiente)**. Consulte Requisitos del sistema VM-Series para ver los requisitos de recursos.
    2. Seleccione la VPC.
    3. Seleccione la subred pública en Outpost a la que se adjuntará la interfaz de gestión de VM-Series.
    4. Seleccione **Automatically assign a public IP address (Asignar automáticamente una dirección IP pública)**. Esto le permite obtener una dirección IP de acceso público para la interfaz de gestión del cortafuegos VM-Series.

       Posteriormente, puede adjuntar una dirección IP elástica a la interfaz de gestión; a diferencia de la dirección IP pública, que deshace la asociación con el cortafuegos cuando se finaliza la instancia, la dirección IP elástica ofrece continuidad y se puede volver a adjuntar a una

 ©2024 Palo Alto Networks, Inc.

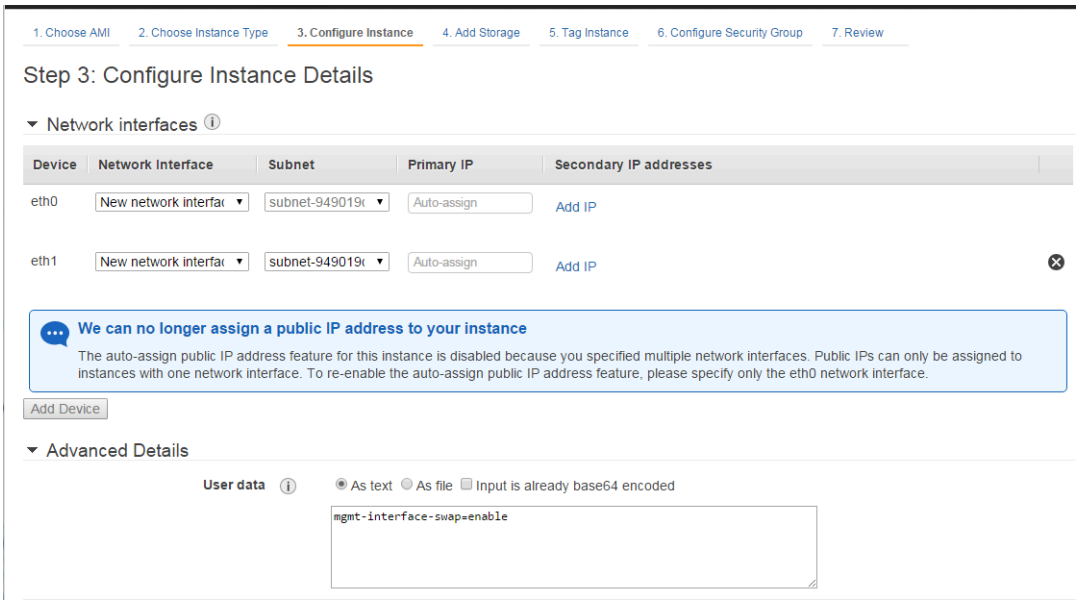
nueva instancia (o una de sustitución) del cortafuegos VM-Series sin necesidad de volver a configurar la dirección IP, independientemente de la ubicación de referencia que tenga.

5. Seleccione **Launch as an EBS-optimized instance (Iniciar como instancia optimizada para EBS)**.
6. Añada otra interfaz de red para implementaciones con ELB, para que pueda intercambiar las interfaces de gestión y datos en el cortafuegos. El intercambio de interfaces requiere un mínimo de dos ENI (eth0 y eth1).
   - Expanda la sección de interfaces de red y haga clic en **Añadir dispositivo** para añadir otra interfaz de red.

     Asegúrese de que su VPC tiene más de una subred, para que pueda añadir ENI adicionales al inicio.

     Si inicia el cortafuegos con solo un ENI:
     - *El comando de intercambio de interfaz hará que el cortafuegos arranque en el modo de mantenimiento.*
     - *Debe reiniciar el cortafuegos cuando añade el segundo ENI.*
   - Expanda la sección Advanced Details (Detalles avanzados) y en el campo User data (Datos de usuario) introduzca **`mgmt-interface-swap=enable`** como texto para realizar el intercambio de interfaz durante el inicio.

     *Si está iniciando el cortafuegos, también puede introducir **`vmseries-bootstrap-aws-s3bucket =<bucketname>`** con un separador de coma después de **`mgmt-interface-swap=enable`**.*



7. Acepte la configuración de **Storage (Almacenamiento)** predeterminada. El cortafuegos utiliza el tipo de volumen SSD (gp2)

   La primera vez que se accede al cortafuegos se solicita este par de claves. También es necesario acceder al cortafuegos en el modo de mantenimiento.

 ©2024 Palo Alto Networks, Inc.

8. (Opcional) **Tagging (Etiquetado)**. Añada una o más etiquetas para crear sus propios metadatos e identificar y agrupar el cortafuegos VM-Series. Por ejemplo, añada una etiqueta **Name (Nombre)** con un **Value (Valor)** que le ayude a recordar que las interfaces ENI se hayan intercambiado en este cortafuegos VM-Series.
9. Seleccione un **Security Group (Grupo de seguridad)** existente o cree uno nuevo. Este grupo de seguridad sirve para restringir el acceso a la interfaz de gestión del cortafuegos. Considere habilitar el acceso https y ssh como mínimo para la interfaz de gestión.
10. Si se le solicita, seleccione una opción de **SSD** adecuada para su configuración.
11. Seleccione **Review and Launch (Revisar e iniciar)**. Revise que sus selecciones son precisas y haga clic en **Launch (Iniciar)**.
12. Seleccione un par de claves existente o cree uno nuevo y acepte el descargo de responsabilidad de claves.
13. Descargue y guarde la clave privada en un lugar seguro; la extensión del archivo es `.pem`. Si pierde la clave, no se puede volver a regenerar.

    Se tardará entre 5 y 7 minutos en iniciar el cortafuegos VM-Series. Puede consultar el progreso en el panel EC2. Al completar el proceso, el cortafuegos VM-Series se muestra en la página **Instances (Instancias)** del panel EC2.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Configure una nueva contraseña de administración para el cortafuegos.

En la CLI del cortafuegos VM-Series, debe configurar una contraseña administrativa única para poder acceder a la interfaz web del cortafuegos. Para iniciar sesión en la CLI, necesita la clave privada que ha utilizado para iniciar el cortafuegos.

1. Use la dirección IP pública para hacer SSH en la interfaz de línea de comando (CLI) del cortafuegos VM-Series. Necesitará la clave privada que usó o creó en 3 anteriormente para acceder a la CLI.

   Si añadió un ENI adicional para admitir implementaciones con ELB, primero debe crear y asignar una dirección IP elástica al ENI para acceder a la CLI, consulte 6.

   Si utiliza PuTTY para el acceso SSH, debe convertir el formato .pem al formato .ppk. Consulte https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html
2. Introduzca el siguiente comando para iniciar sesión en el cortafuegos:

   ssh-i <*private_key.pem*> admin@<*public-ip_address*>
3. Configure una nueva contraseña usando el siguiente comando y siga las indicaciones en pantalla:

   configure

   set mgt-config users admin password
4. Si tiene una BYOL que debe activarse, configure la dirección IP del servidor DNS de modo que el cortafuegos pueda acceder al servidor de licencias de Palo Alto Networks. Introduzca el siguiente comando para configurar la dirección IP del servidor DNS:

   set deviceconfig system dns-setting servers primary <*ip_address*>
5. Confirme los cambios con el comando:

   commit
6. Finalice la sesión SSH.

STEP 5 | Apague el cortafuegos VM-Series.

1. En el panel EC2, seleccione **Instances (Instancias)**.
2. En la lista, seleccione el cortafuegos VM-Series y haga clic en **Actions (Acciones)** > **Stop (Detener)**.

STEP 6 | Cree y asigne una dirección IP elástica (Elastic IP address, EIP) a la ENI utilizada para el acceso de gestión al cortafuegos y reinicie el cortafuegos VM-Series.

1. Seleccione **Elastic IP (IP elástica)** y haga clic en **Allocate New Address (Asignar nueva dirección)**.
2. Seleccione **EC2-VPC** y haga clic en **Yes, Allocate (Sí, asignar)**.
3. Seleccione la EIP recién asignada y haga clic en **Associate Address (Asociar dirección)**.
4. Seleccione la **Network Interface (Interfaz de red)** y la **Private IP address (Dirección IP privada)** asociada con la interfaz de gestión y haga clic en **Yes, Associate (Sí, asociar)**.

STEP 7 | Cree interfaces de red virtuales y adjúntelas al cortafuegos VM-Series. Las interfaces de red virtuales se llaman Interfaces de red elásticas (ENI) en AWS y actúan como interfaces de red de plano de

 ©2024 Palo Alto Networks, Inc.

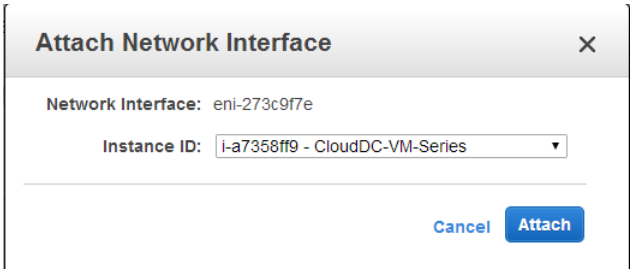
datos en el cortafuegos. Estas interfaces se usan para la gestión del tráfico de datos desde o hacia el cortafuegos.

Necesitará al menos dos ENI que permitan tráfico entrante y saliente desde o hacia el cortafuegos. Puede añadir hasta siete ENI para gestionar el tráfico de datos en el cortafuegos VM-Series; compruebe su tipo de instancia de EC2 para comprobar el número máximo que admite.

1. En el panel EC2, seleccione **Network Interfaces (Interfaces de red)** y haga clic en **Create Network Interface (Crear interfaz de red)**.
2. Introduzca un nombre descriptivo para la interfaz.
3. Seleccione la subred. Use el ID de subred para asegurarse de que ha seleccionado la subred correcta. Sólo puede adjuntar una ENI a una instancia en la misma subred.
4. Introduzca la dirección de **Private IP (IP privada)** para asignarla a la interfaz y seleccione **Auto-assign (Asignar automáticamente)** para asignar automáticamente una dirección IP dentro de las direcciones IP disponibles en la subred seleccionada.
5. Seleccione el **Security group (Grupo de seguridad)** para controlar el acceso a la interfaz de red del plano de datos.
6. Haga clic en **Yes, Create (Sí, crear)**.



7. Para adjuntar la ENI al cortafuegos VM-Series, seleccione la interfaz que acaba de crear y haga clic en **Attach (Adjuntar)**.



8. Seleccione el **Instance ID (ID de instancia)** del cortafuegos VM-Series y haga clic en **Attach (Adjuntar)**.
9. Repita los pasos anteriores para crear y adjuntar al menos una ENI más al cortafuegos.

STEP 8 | (No es necesario para el modelo con licencia basada en uso) Active las licencias en el cortafuegos VM-Series.

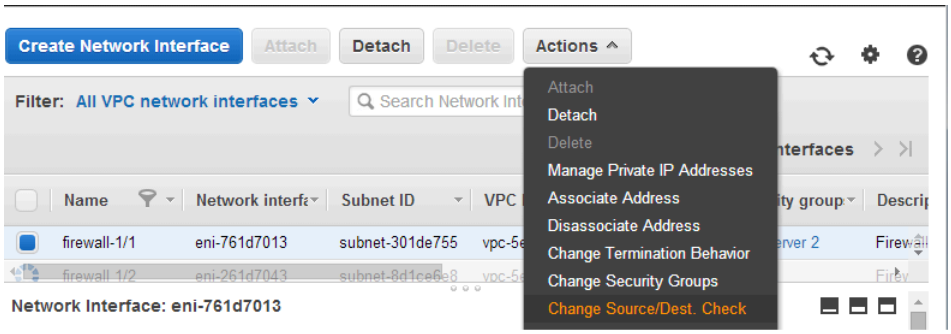
Esta tarea no se realiza en la consola de administración de AWS. Tendrá que acceder al portal de asistencia de Palo Alto Networks y a la interfaz web del cortafuegos VM-Series para activar la licencia.

Consulte Activación de la licencia.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Deshabilite la comprobación de origen/destino en todas las interfaces de red de planos de datos del cortafuegos. Si deshabilita esta opción, permite a la interfaz gestionar el tráfico de red no destinado a la dirección IP asignada a la interfaz de red.

1. En el panel EC2, seleccione la interfaz de red, por ejemplo, eth1/1, en la pestaña **Network Interfaces (Interfaces de red)**.
2. En el menú desplegable **Action (Acción)**, seleccione **Change Source/Dest. (Cambiar comprobación de origen/dest). Check (Comprobar)**.



3. Haga clic en **Disabled (Deshabilitado)** y en **Save (Guardar)** para guardar los cambios.
4. Repita los pasos 1-3 con cada interfaz de plano de datos del cortafuegos.

 ©2024 Palo Alto Networks, Inc.

STEP 10 | Configure las interfaces de red del plano de datos como interfaces de capa 3 en el cortafuegos.

Para una configuración de ejemplo, consulte los pasos 14 a 17 en Caso de uso : Protección de las instancias de EC2 en AWS Cloud.

En los servidores de aplicaciones dentro de la VPC, defina la interfaz de red de plano de datos del cortafuegos como la puerta de enlace predeterminada.

1. Si usa una conexión segura (https) desde su navegador web, inicie sesión usando la dirección EIP y la contraseña que asignó durante la configuración inicial (https://<Elastic_IP address>). Verá una advertencia de certificación; es normal. Vaya a la página web.
2. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
3. Haga clic en el enlace de **ethernet 1/1** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **capa 3**
   - En la pestaña **Config (Configurar)**, asigne la interfaz el enrutador predeterminado.
   - En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. Defina una nueva zona, por ejemplo, VM_Series_untrust, y a continuación haga clic en **OK (Aceptar)**.
   - En la pestaña **IPv4**, seleccione **Static (Estática)** o **DHCP Client (Cliente DHCP)**.

     Si usa la opción **Static (Estática)**, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para la interfaz; por ejemplo, 10.0.0.10/24.

     Asegúrese de que la dirección IP coincide con la dirección IP de la ENI que ha asignado anteriormente.

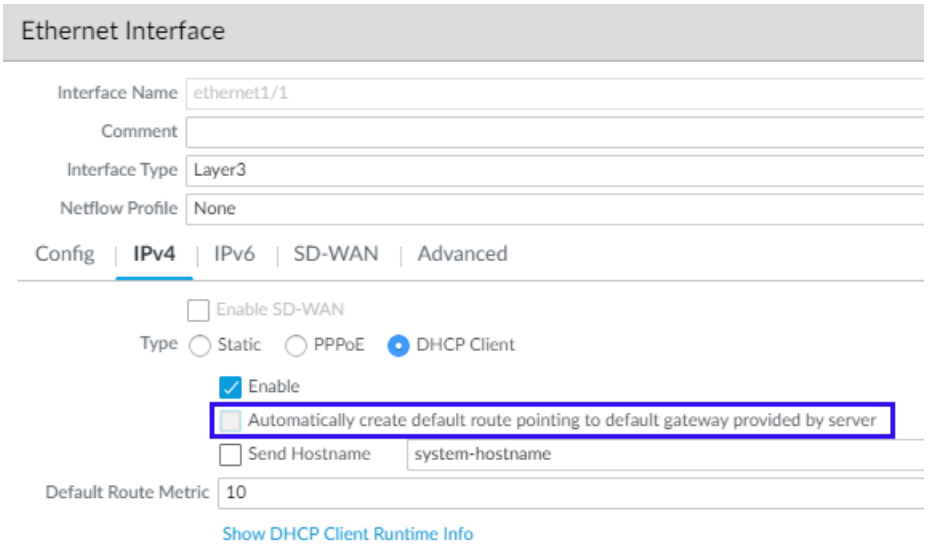
     Si usa DHCP, seleccione **DHCP Client (Cliente DHCP)**; la dirección IP privada que ha asignado a la ENI en la consola de administración de AWS se adquirirá de manera automática.
4. Haga clic en el enlace de **ethernet 1/2** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **capa 3**
   - Security Zone (Zona de seguridad): VM_Series_trust
   - **IP address (Dirección IP)**: Seleccione el botón de opción **Static (Estático)** o **DHCP Client (Cliente DHCP)**.

     Para estático, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para la interfaz. Asegúrese de que la dirección IP coincide con la dirección IP de la ENI adjuntada que ha asignado anteriormente.
5. Haga clic en **Commit (Confirmar)**. Verifique que el enlace para las interfaces esté en estado activo.



 ©2024 Palo Alto Networks, Inc.

Para DHCP, anule la selección de la casilla de verificación ***Automatically create default route to default gateway provided by server (Crear automáticamente ruta predeterminada a la puerta de enlace predeterminada proporcionada por el servidor)****. Para una interfaz adjuntada a la subred privada en la VPC, deshabilitar esta opción garantiza que el tráfico gestionado por esta interfaz no fluya directamente a la puerta de enlace de internet en la VPC.*



STEP 11 | Cree reglas NAT para permitir el tráfico entrante y saliente desde servidores implementados dentro de la VPC.

1. Seleccione **Policies (Políticas)** > **NAT** en la interfaz web del cortafuegos.
2. Cree una regla NAT para permitir el tráfico desde la interfaz de red del plano de datos en el cortafuegos a la interfaz del servidor web en la VPC.
3. Cree una regla NAT para permitir el acceso saliente para el tráfico desde el servidor web a internet.

STEP 12 | Cree políticas de seguridad para permitir/denegar el tráfico entrante y saliente desde servidores implementados dentro de la VPC.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** en la interfaz web del cortafuegos.
2. Haga clic en **Add (Añadir)** y especifique las zonas, aplicaciones y opciones de inicio de sesión que le gustaría ejecutar para restringir el tráfico de auditoría que atraviesa la red.

STEP 13 | Confirme los cambios en el cortafuegos.

Haga clic en **Commit (Confirmar)**.

STEP 14 | Compruebe que el cortafuegos VM-Series protege el tráfico y que las reglas NAT están en vigor.

1. Seleccione **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)** en la interfaz web del cortafuegos.
2. Consulte los logs para asegurarse de que las aplicaciones que atraviesan la red cumplen las políticas de seguridad que ha implementado.

 ©2024 Palo Alto Networks, Inc.

Creación de una imagen Amazon Machine Image personalizada (AMI)

Una AMI de VM-Series personalizada le brinda la consistencia y flexibilidad para implementar un cortafuegos VM-Series con la versión de PAN-OS que desea usar en su red en lugar de limitarse a usar solo una AMI que se publica en AWS public Marketplace o en AWS GovCloud Marketplace. El uso de una AMI personalizada acelera el proceso de implementación de un cortafuegos con la versión PAN-OS de su elección porque reduce el tiempo para aprovisionar el cortafuegos con una AMI publicada en AWS public o AWS GovCloud Marketplace, y luego realiza actualizaciones de software para obtener a la versión de PAN-OS que desea utilizar en su red o para la cual está cualificado.

Puede crear una AMI personalizada con las licencias BYOL, Paquete 1 o Paquete 2. El proceso de creación de una AMI personalizada requiere que elimine toda la configuración del cortafuegos y la restablezca a los valores predeterminados de fábrica, por lo que en este flujo de trabajo iniciará una nueva instancia del cortafuegos desde AWS Marketplace en lugar de usar un cortafuegos existente que esté completamente configurado.

Al crear una AMI personalizada con una versión BYOL del cortafuegos, primero debe activar la licencia en el cortafuegos para poder acceder y descargar las actualizaciones de software de PAN-OS para actualizar su cortafuegos, y luego desactivar la licencia en el cortafuegos antes de reiniciar el cortafuegos a los valores predeterminados de fábrica y crear la AMI personalizada. Si no desactiva la licencia, perderá la licencia que aplicó en esta instancia de cortafuegos.

STEP 1 | Implemente el cortafuegos VM-Series desde Marketplace.

Consulte 3

STEP 2 | (Solo para BYOL) Active la licencia.

STEP 3 | Instale actualizaciones de software y actualice el cortafuegos a la versión de PAN-OS que planifica usar.

STEP 4 | (Solo para BYOL) Desactive la licencia.

STEP 5 | Realice un restablecimiento de datos privados.

Un restablecimiento de datos privados elimina todos los registros y restaura la configuración predeterminada.

Los discos del sistema no se borran, por lo que las actualizaciones de contenido del paso 4 están intactas.

1. Acceda a la CLI del cortafuegos.
2. Elimine todos los registros y restaure la configuración predeterminada.

```
        solicitud de restablecimiento de datos privados del
sistema
```

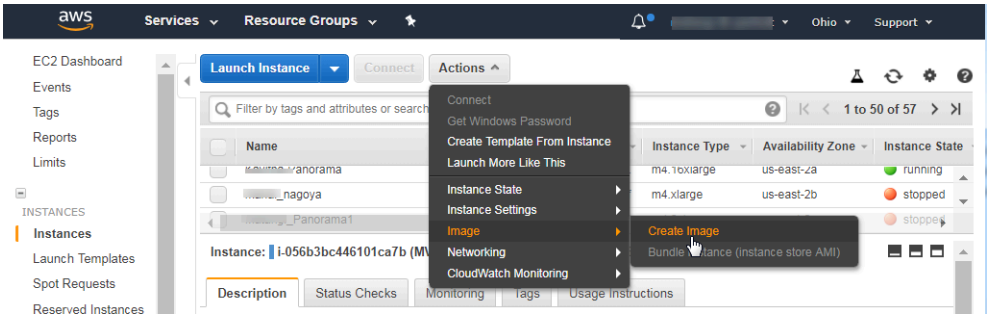
Introduzca **y** para confirmar.

El cortafuegos se reinicia para inicializar la configuración predeterminada.

 ©2024 Palo Alto Networks, Inc.

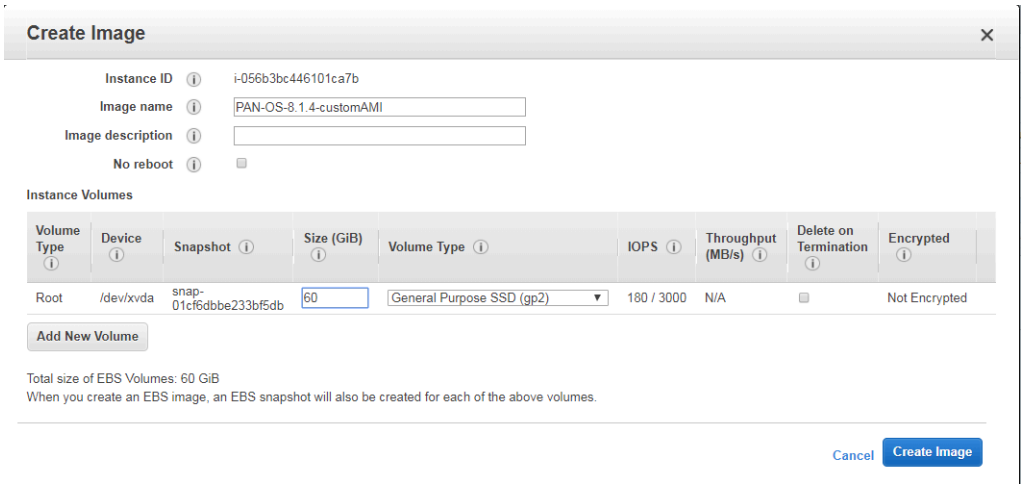
STEP 6 | Cree el AMI personalizado.

1. Inicie sesión en la consola de AWS y seleccione el panel EC2.
2. Debe **Stop (Detener)** el cortafuegos VM-Series.
3. Seleccione la instancia del cortafuegos VM-Series y haga clic en **Image (Imagen)** > **Create Image (Crear imagen)**.



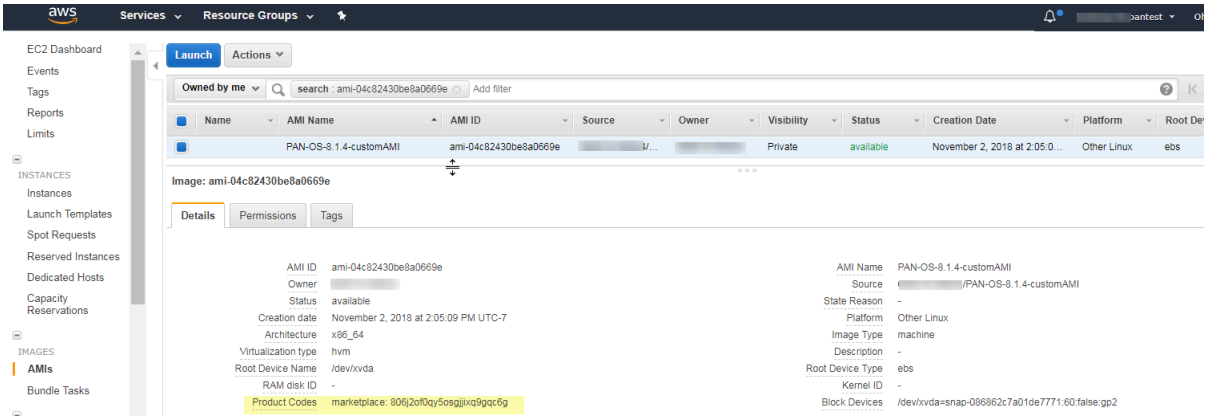
4. Introduzca un nombre de imagen personalizado y haga clic en **Create Image (Crear imagen)**.

   El espacio en disco mínimo requerido es de 60 GB.



5. Verifique que se haya creado la AMI personalizada y que tenga el código de producto correcto.
   1. En el panel EC2, seleccione **AMI**.
   2. Seleccione la AMI que acaba de crear. Dependiendo de si seleccionó una AMI con las opciones de licencia BYOL, Paquete 1 o Paquete 2, debería ver una de los siguientes **Product Codes (Códigos de producto)** en los detalles:
      - BYOL: 6njl1pau431dv1qxipg63mvah
      - Paquete 1: 6kxdw3bbmdeda3o6i1ggqt4km
      - Paquete 2: 806j2of0qy5osgjjixq9gqc6g

 ©2024 Palo Alto Networks, Inc.



STEP 7 | Cifrado del volumen EBS para el cortafuegos VM-Series en AWS.

STEP 8 | Configure la contraseña de administración para el cortafuegos.

Consulte 4

Cifrado del volumen EBS para el cortafuegos VM-Series en AWS

El cifrado EBS está disponible para todos Tipos de instancias EC2 de AWS en los que puede implementar el cortafuegos VM-Series. Para almacenar de forma segura datos en el cortafuegos VM-Series en AWS, primero debe crear una instancia EC2 respaldada por EBS a partir de una imagen de la serie VM-Series que se publique en AWS público o en el Marketplace de GovCloud, o a partir de una AMI personalizada. Durante la creación de instancias, seleccione la opción de cifrar el volumen de EBS con una clave AWS KMS (Servicio de gestión de claves). Puede elegir usar la clave maestra predeterminada para su cuenta de AWS o cualquier clave de KMS que haya creado previamente con el Servicio de gestión de claves de AWS.

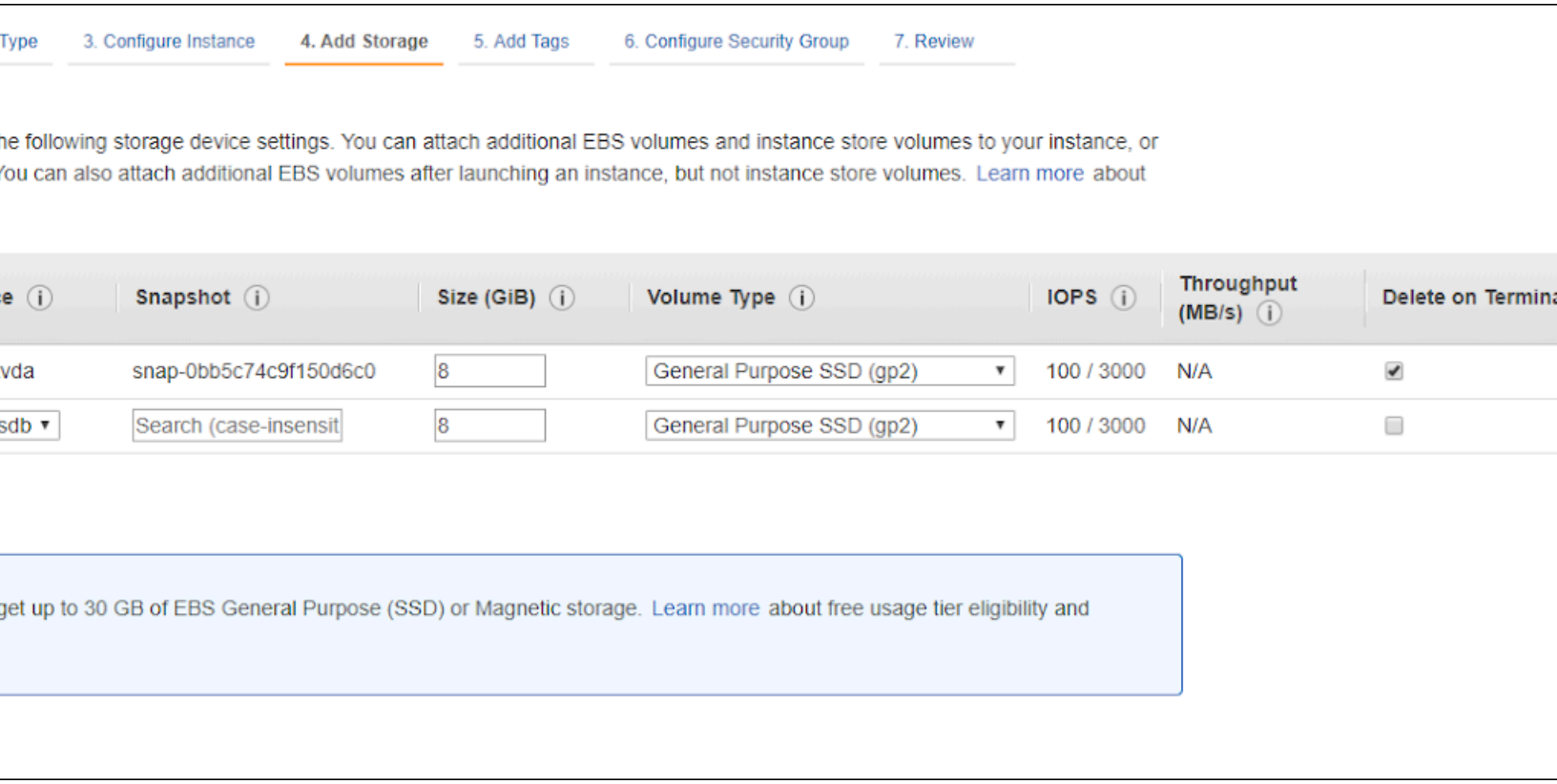
STEP 1 | Cree una clave de cifrado en AWS u omita este paso si desea usar la clave maestra predeterminada para su cuenta.

Utilizará esta clave para cifrar el volumen EBS en el cortafuegos. Tenga en cuenta que la clave es específica de la región.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Para cifrar un volumen EBS:

1. Inicie una instancia de AWS EC2.
2. Especifique sus volúmenes de EBS: si está usando una AMI sin cifrar, las propiedades de cifrado aparecerán como `No cifradas`.
3. Seleccione una clave AWS KMS para cifrar el volumen. Puede seleccionar la misma clave KMS para cada volumen que desee crear, o puede usar una clave KMS diferente para cada volumen.



4. Seleccione **Revisar** e inicie la instancia. Su instancia se iniciará con un volumen cifrado de Amazon EBS que utiliza la clave KMS que seleccionó.

Para obtener información sobre cómo cifrar volúmenes EBS existentes, consulte Cifrar un volumen EBS existente.

Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión

Si no intercambia la interfaz de gestión (MGT) con la interfaz del plano de datos (ethernet 1/1) cuando se implementa el cortafuegos, puede utilizar la CLI para habilitar el cortafuegos y recibir tráfico del plano de datos en la interfaz principal tras iniciar el cortafuegos.

STEP 1 | Complete los pasos 1 a 7 en Inicio del cortafuegos VM-Series en AWS.

Antes de proceder, verifique que el cortafuegos tiene un mínimo de dos ENI (eth0 y eth1). Si inicia el cortafuegos con solo un ENI, el comando de intercambio de interfaces hará que el cortafuegos se inicie en el modo de mantenimiento.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | En el panel de EC2, visualice la dirección IP de la interfaz eth1 y verifique que las reglas del grupo de seguridad de AWS permiten conexiones (HTTPS y SSH) a la nueva interfaz de gestión (eth1).

STEP 3 | Inicie sesión en la CLI del cortafuegos VM-Series e introduzca el comando siguiente:

```
set system setting mgmt-interface-swap enable yes
```

STEP 4 | Confirme que desea intercambiar la interfaz y utilice la interfaz del plano de datos eth1 como interfaz de gestión.

STEP 5 | Reinicie el cortafuegos para que se produzca el intercambio. Utilice el comando siguiente:

```
request restart system
```

STEP 6 | Verifique que se hayan intercambiado las interfaces. Utilice el comando siguiente:

```
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
```

Habilitación de la supervisión de CloudWatch en el cortafuegos VM-Series

El cortafuegos VM-Series en AWS puede publicar métricas PAN-OS nativas en AWS CloudWatch, que puede usar para supervisar los cortafuegos. Estas métricas le permiten evaluar el rendimiento y los patrones de uso que puede usar para tomar medidas para iniciar o finalizar instancias de los cortafuegos VM-Series.

Los cortafuegos usan las API de AWS para publicar la métrica en un *espacio de nombres* , que es la ubicación en AWS donde las métricas se recopilan en un intervalo de tiempo especificado. Cuando configura los cortafuegos para publicar métricas en AWS CloudWatch, hay dos espacios de nombres donde puede ver las métricas: el espacio de nombres primario recopila y añade la métrica seleccionada para todas las instancias configuradas para usar el espacio de nombres, y el espacio de nombres secundario que se crea automáticamente con el sufijo `_dimensiones` le permite filtrar las métricas utilizando el nombre de host y los metadatos de ID de instancia de AWS (o *dimensiones*) y obtener visibilidad sobre el uso y el rendimiento de los cortafuegos VM-Series individuales.

Puede supervisar la métrica en CloudWatch o crear políticas de escalado automático para activar alarmas y tomar medidas para implementar manualmente una nueva instancia del cortafuegos cuando la métrica supervisada alcance un valor de umbral. Consulte la documentación de AWS CloudWatch y grupos de escalado automático (ASG) para las recomendaciones sobre cómo establecer las condiciones de alarma para una acción de ampliación o reducción.

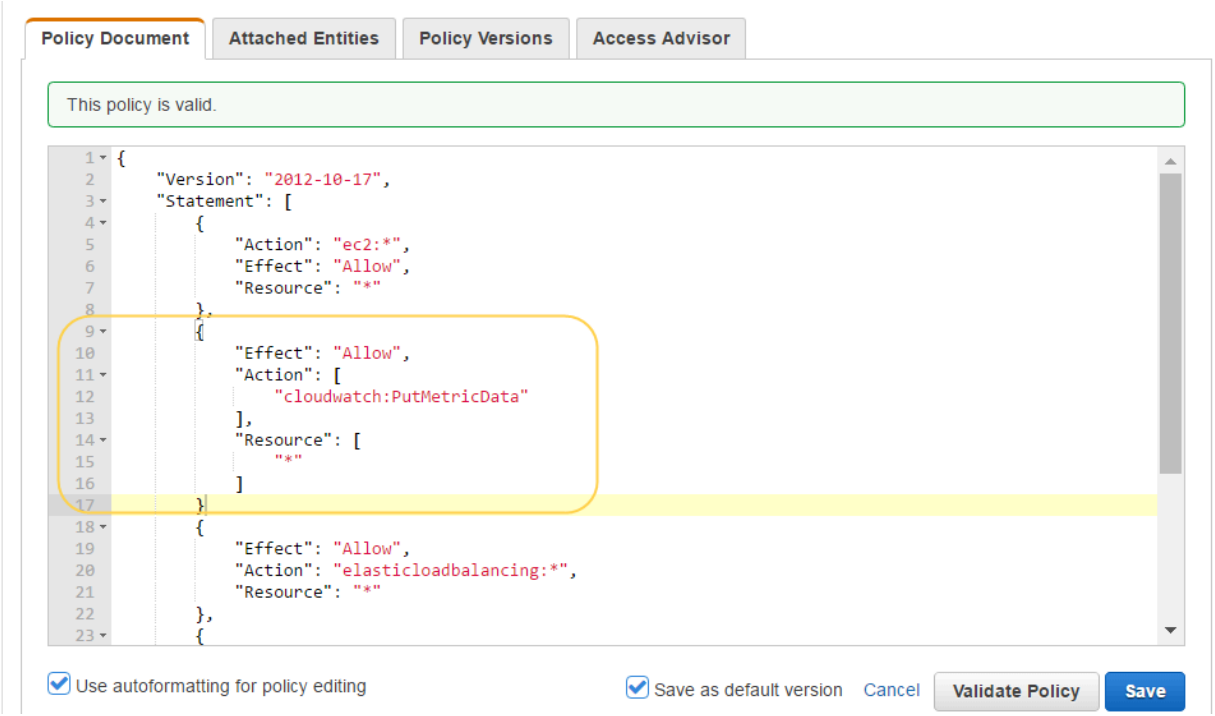
Para obtener una descripción de las métricas de PAN-OS que puede publicar en CloudWatch, consulte Métricas personalizadas de PAN-OS publicadas para la supervisión.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Asigne los permisos adecuados para la función de usuario de gestión de identidad y acceso (IAM) que utiliza para implementar el cortafuegos VM-Series en AWS.

Si usted inicia una nueva instancia del cortafuegos VM-Series o actualiza un cortafuegos VM-Series existente en AWS, la función IAM asociada a su instancia debe tener permisos para publicar las métricas en CloudWatch.

1. En la consola de AWS, seleccione IAM.
2. Edite la función IAM para otorgar los siguientes permisos:



Puede copiar y pegar los permisos aquí:

```
 { "Version": "2012-10-17", "Statement": [ { "Effect":
"Allow", "Action": [ "cloudwatch:PutMetricData" ],
"Resource": [ "*" ] } ] }
```

STEP 2 | Habilite CloudWatch en el cortafuegos VM-Series en AWS.

1. Inicie sesión en la interfaz web del cortafuegos VM-Series
2. Seleccione **Device (Dispositivo)** > **VM-Series**.
3. En la configuración de AWS CloudWatch, haga clic en **Edit (Editar)** (⚙) y seleccione **Enable CloudWatch Monitoring (Habilitar la supervisión de CloudWatch)**.

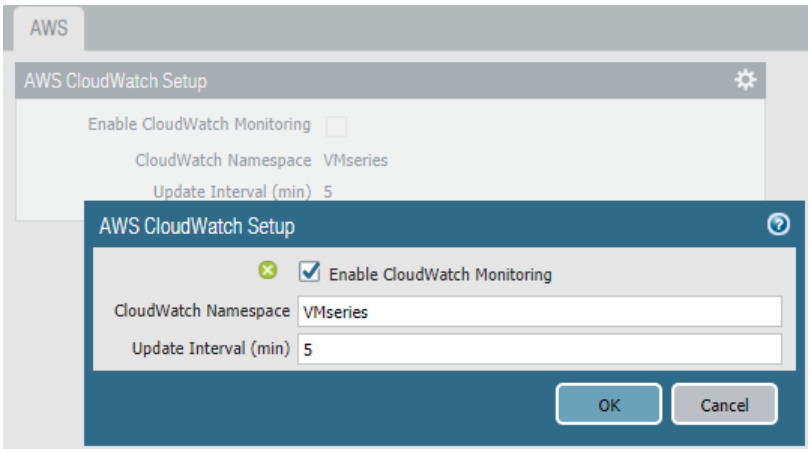
   1. Introduzca el **CloudWatch Namespace (Espacio de nombres de CloudWatch)** en el cual el cortafuegos puede publicar métricas. El espacio de nombre no puede comenzar con **AWS**.

      Las métricas agregadas para todos los cortafuegos VM-Series en un par de HA o implementación de escalado automático se publican en el espacio de nombres que introdujo anteriormente. El espacio de nombres con el sufijo `_dimensiones` que se crea automáticamente le permite filtrar y ver métricas para un cortafuegos VM-Series

 ©2024 Palo Alto Networks, Inc.

específico utilizando el nombre de host o los metadatos de ID de instancia de AWS adjuntos al cortafuegos.

2. Establezca el **Update interval (Intervalo de actualización)** a un valor entre 1-60 minutos. Esta es la frecuencia con la que el cortafuegos publica las métricas en CloudWatch. El valor predeterminado es de 5 minutos.



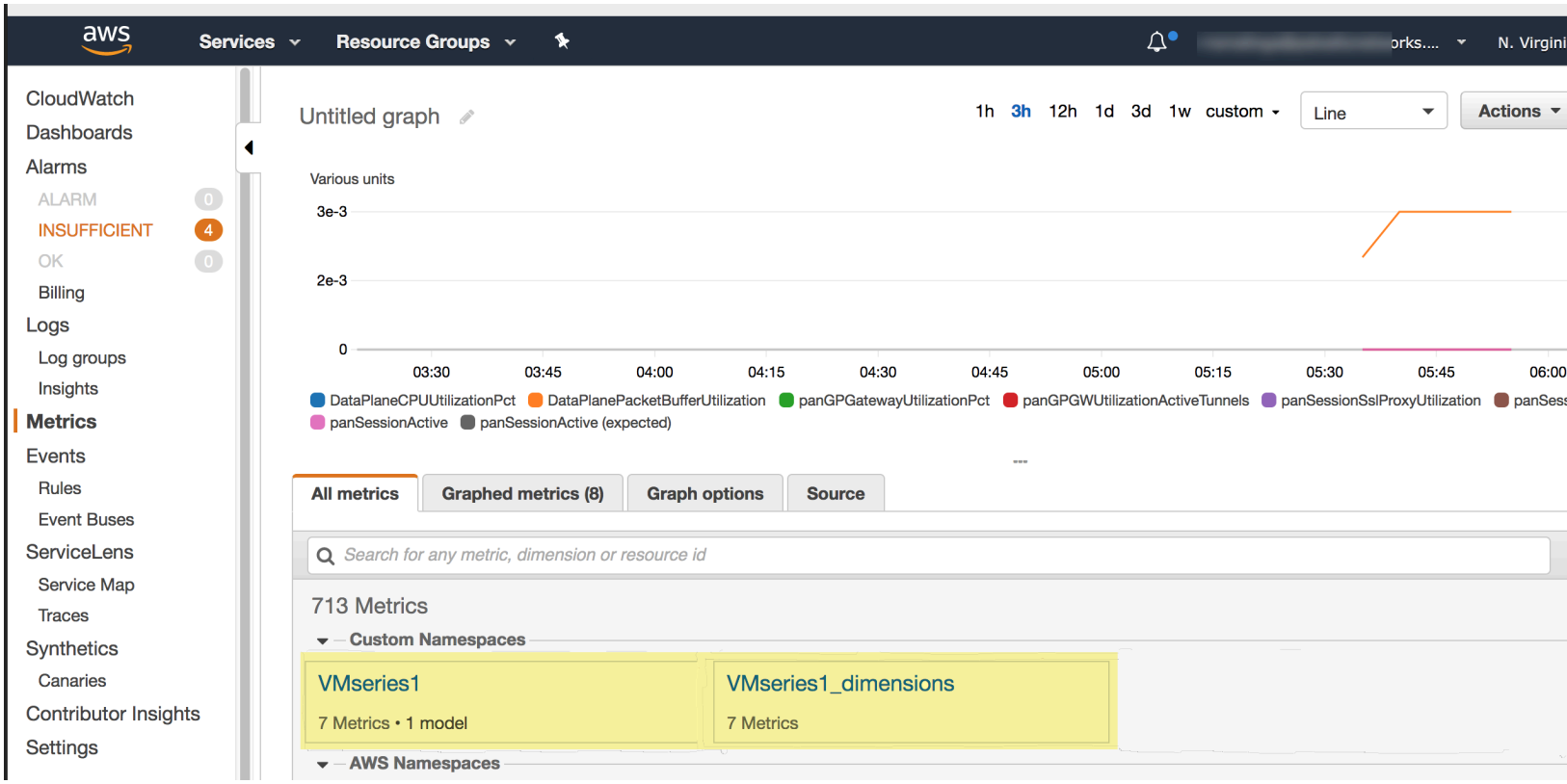
4. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

   Hasta que el cortafuegos comience a publicar las métricas en CloudWatch, no puede configurar alarmas para las métricas PAN-OS.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Compruebe que pueda ver las métricas en CloudWatch.

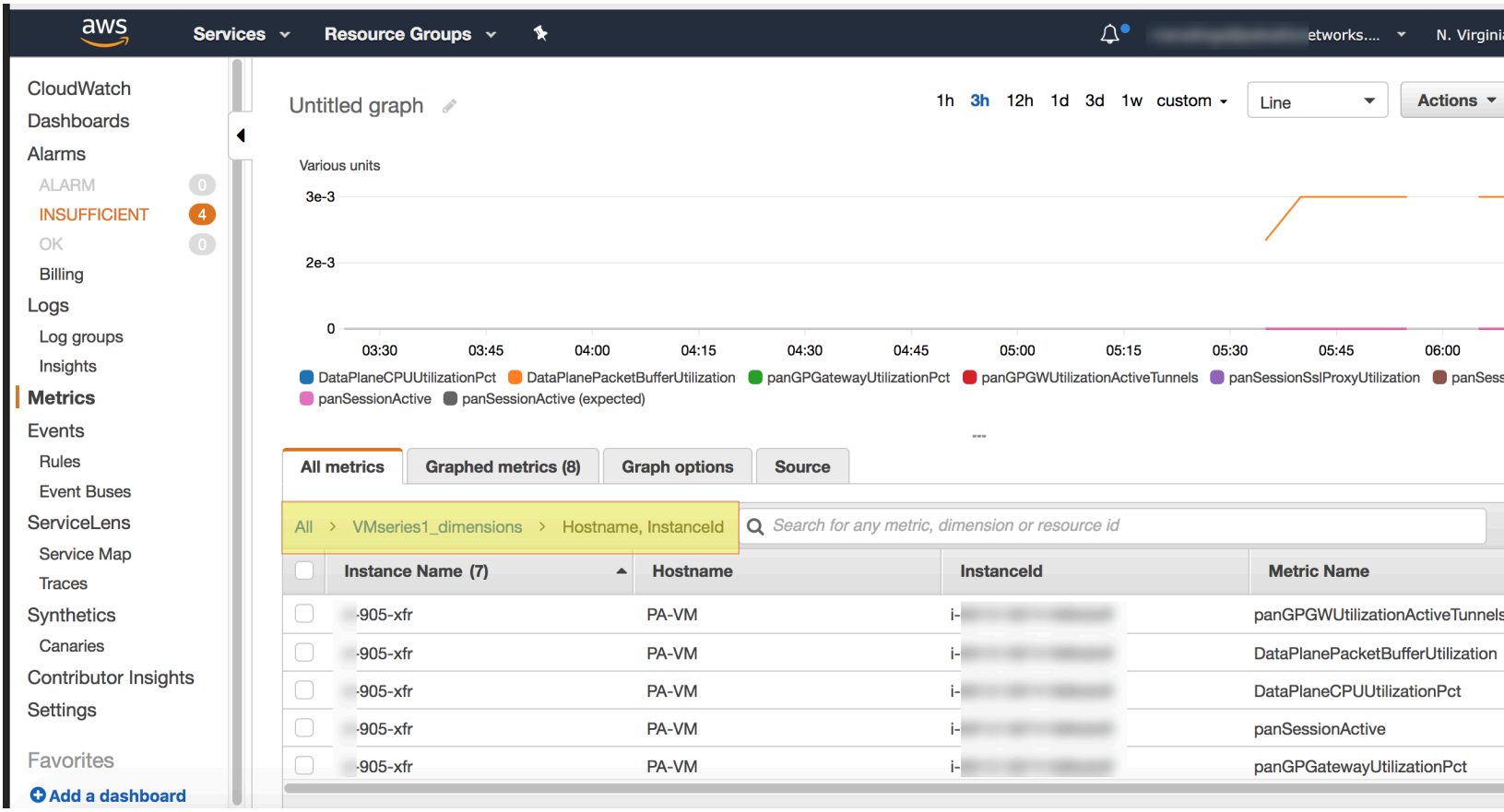
1. En la consola de AWS, seleccione **CloudWatch** > **Metrics (Métricas)** para ver las métricas de CloudWatch por categoría.
2. En el menú desplegable Métricas personalizadas, seleccione el espacio de nombres.



3. Compruebe que pueda ver las métricas de PAN-OS en la lista de visualización.

   Para filtrar por nombre de host o ID de instancia de AWS de un cortafuegos específico, seleccione `_dimensiones`.

 ©2024 Palo Alto Networks, Inc.



STEP 4 | Configure alarmas y acciones para métricas PAN-OS en CloudWatch.

Consulte la documentación de AWS: http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html

Un cortafuegos VM-Series con configuración de arranque tardará entre 7 y 9 minutos en estar disponible para el servicio. Por lo tanto, aquí hay algunos ejemplos sobre cómo configurar alarmas que activan el escalado automático para el cortafuegos VM-Series:

- Si ha implementado 2 instancias de los cortafuegos VM-Series como puertas de enlace de Global Protect que protegen a los usuarios remotos, use la métrica Túneles activos de la puerta de enlace de GlobalProtect. Puede configurar una alarma para cuando el número de túneles activos sea superior a 300 durante 15 minutos; puede implementar 2 nuevas instancias del cortafuegos VM-Series, que se arrancan y configuran para funcionar como puertas de enlace de Global Protect.
- Si está utilizando el cortafuegos para asegurar sus cargas de trabajo en AWS, use la métrica Utilización de la sesión para ampliar o reducir horizontalmente el cortafuegos según el uso de los recursos. Puede configurar una alarma para cuando la métrica de utilización de la sesión sea superior al 60 % durante 15 minutos, para implementar una instancia del cortafuegos de instancia VM-Series. Y al contrario, si la Utilización de la sesión es inferior al 50 % durante 30 minutos, finalice una instancia del cortafuegos VM-Series.

Inicio de cortafuegos VM-Series y logs de estado en AWS

Para ayudar en la depuración de problemas de implementación, el cortafuegos VM-Series proporciona logs del sistema durante el inicio del sistema. Una vez que el sistema se inicia correctamente, el cortafuegos

 ©2024 Palo Alto Networks, Inc.

puede generar mensajes de estado para los eventos del sistema y puede informar acerca de cambios en los recursos del sistema como informe de estado. Los mensajes se registran en la consola del cortafuegos VM-Series en /dev/ttyS0 and /dev/tty0.

Si configura correctamente su entorno, también puede usar el servicio AWS CloudWatch para ver los logs de los cortafuegos VM-Series implementados en AWS.

- Ver logs del cortafuegos VM-Series en CloudWatch
- Mensajes del sistema del cortafuegos VM-Series

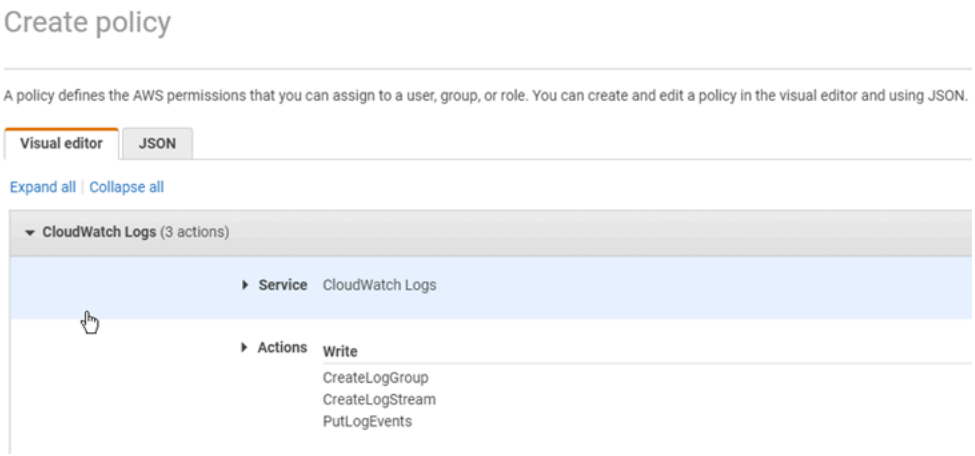
Ver logs del cortafuegos VM-Series en CloudWatch

Para ver los logs del cortafuegos VM-Series en CloudWatch, el cortafuegos debe, como mínimo, ejecutar la versión del complemento VM-Series que admite mensajes del sistema, como se indica en la Matriz de compatibilidad.

- Asegúrese de que su entorno de AWS esté actualizado y que Boto3 esté disponible.
- Debe crear una función y política de IAM que permita que los cortafuegos VM-Series creen un grupo de log y una secuencia de logs en CloudWatch, y escriban eventos de log en la secuencia de logs.

  Para asegurarse de que CloudWatch pueda mostrar logs del cortafuegos VM-Series, su rol de IAM debe incluir una política que permita las siguientes acciones:

  ```
  "logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents"
  ```



- Asegúrese de que la versión del complemento de VM-Series admite logs de inicio y de estado del cortafuegos, como se especifica en la Matriz de compatibilidad.

El complemento de VM-Series incluye un script de generación de logs que se conecta al servicio AWS CloudWatch.

1. El script crea el grupo de logs **PaloAltoNetworksFirewalls**. Todas las instancias del cortafuegos VM-Series en su implementación usan este grupo de logs.
2. El script crea una secuencia de log exclusiva para su cortafuegos VM-Series. Cada uno de sus cortafuegos configura CloudWatch y tiene su propia secuencia de logs basada en el ID de instancia del cortafuegos.
3. Cuando se registra un evento, el mensaje del log y la marca de tiempo se envían al grupo de logs utilizando la secuencia de logs del cortafuegos.

 ©2024 Palo Alto Networks, Inc.

Mensajes del sistema del cortafuegos VM-Series

Para ayudar en la depuración, el cortafuegos VM-Series proporciona mensajes del sistema durante el inicio del sistema. una vez iniciado el sistema, el cortafuegos puede generar mensajes de estado para informar acerca del estado del sistema. Los eventos o errores de estado críticos siempre se informan, y puede habilitar mensajes periódicos de estado para registrar el estado del sistema en el intervalo que elija.

- Formato de mensaje
- Mensajes de inicio del sistema
- Mensajes de estado
- Mensajes periódicos de estado

Formato de mensaje

El formato del mensaje de registro es el siguiente:

```
Nivel de rlog: Recurso: Estado: Detalles
```

- **Log level (Nivel de log)**
  - CRÍTICO
  - ERROR
  - INFO

  Cada evento CRÍTICO o de ERROR tiene un MSGID único en los logs. Si ha habilitado Mensajes periódicos de estado, el MSGID le ayuda a distinguir los nuevos mensajes CRITICAL o ERROR de los problemas no resueltos que haya visto antes.

  ```
  Nivel de rlog: Recurso: Estado: MSGID: Detalles
  ```

  Un mensaje de ERROR de estado incluirá un código de error. Por ejemplo:

  ```
  ERROR: HA : INACTIVA: MSGID: Estado HA <>
  ```
- **Recurso**
  - BOOTSTRAP
  - CONTENIDO
  - HA
  - INTERFAZ
  - LICENCIA
  - INTERFAZGESTIÓN
  - PANORAMA
  - PANOS
  - PERIODIC_STATUS
  - SISTEMA

 ©2024 Palo Alto Networks, Inc.

- **State (Estado)**
  - INICIO/LISTO
  - COMPLETO/FALLO
  - ACTIVA/INACTIVA
  - CORRECTO/INCORRECTO
- **Details (Detalles)**: los detalles generalmente se transmiten desde el recurso.

Mensajes de inicio del sistema

La siguiente lista está ordenada libremente según los eventos de inicio del sistema. Sin embargo, el orden puede cambiar a medida que se producen eventos.

- **Base OS start and network initialization (Inicio del sistema operativo base e inicialización de la red)**

  ```
  INFO: SISTEMA: INICIO: Cortafuegos de Palo Alto Networks inicializando
  ```

- **PAN-OS bootstrap (Arranque de PAN-OS)**

  ```
  INFO: BOOTSTRAP : COMPLETO: Cortafuegos arrancado correctamente
  ```

  O

  ```
  ERROR: BOOTSTRAP : FALLO: MSGID: Fallo/Error de arranque del cortafuegos - <>
  ```

- **Management interface swap (Intercambio de interfaz de gestión)** (si procede)

  ```
  INFO: INTERFAZGESTIÓN: COMPLETO: Intercambio de interfaz de cortafuegos configurado
  ```

  O

  ```
  ERROR: INTERFAZGESTIÓN: MSGID: COMPLETO: Fallo de intercambio de interfaz de cortafuegos <>
  ```

- **PAN-OS start (Inicio de PAN-OS)**

  ```
  INFO: PANOS: INICIO: Versión de cortafuegos <x,yz> Iniciando
  ```

  O

  ```
  CRITICAL: PANOS: FALLO: MSGID: El cortafuegos no pudo iniciar la versión <x,yz>
  ```

  ```
  INFO: SISTEMA: INICIO: Cortafuegos de Palo Alto Networks inicializando
  ```

 ©2024 Palo Alto Networks, Inc.

- **Load license (Cargar licencia)**

  ```
  INFO: LICENCIA: COMPLETO: Cortafuegos con licencia cargada
  correctamente <model>
  ```

  O

  ```
  CRITICAL: LICENCIA: FALLO: MSGID: El cortafuegos no ha podido obtener
  la licencia <reason>
  ```

- **Load content (Cargar contenido)**

  ```
  INFO: CONTENIDO: COMPLETO: Versión de contenido de cortafuegos <>
  cargada.
  ```

  O

  ```
  ERROR: CONTENIDO: FALLO: MSGID: Error al cargar la versión <> de
  contenido de cortafuegos.
  ```

- **Dataplane processes up, and auto commit (procesos de plano de datos activos y con confirmación automática)**

  ```
  INFO: CONFIRMAR: COMPLETO: Trabajo de confirmación automática
  correcto.Licencia de cortafuegos - <model>
  ```

  O

  ```
  CRITICAL: CONFIRMAR: FALLO: Fallo de trabajo de confirmación
  automática <reason>.
  ```

- **Panorama registration, Panorama connected (Registro de Panorama, panorama conectado)** (si procede)

  ```
  INFO: PANORAMA: COMPLETO: Conectado a Panorama <IP>
  ```

  O

  ```
  ERROR: PANORAMA: FALLO: MSGID: Error al conectarse a Panorama <IP>
  ```

- **System ready and interfaces up (Sistema listo e interfaces activas)**

  ```
  INFO: SISTEMA: LISTO: Cortafuegos listo para procesar el tráfico.
  Licencia de cortafuegos - <model>
  ```

Mensajes de estado

Los mensajes de estado informan el estado de un recurso. Después de un inicio del sistema correcto, todos los eventos de estado del sistema se establecen como Up (Activos) y se informan los cambios de estado posteriores. Como se menciona en Formato de mensaje, los mensajes de estado que indican ERROR incluirán un código de estado. En los mensajes de ejemplo a continuación, <> es un marcador de posición para el código de estado.

Si un administrador realiza un apagado intencionado, el apagado no se informa.

 ©2024 Palo Alto Networks, Inc.

- **CloudLoggingConnectionFailed**

  Si no hay logs de CloudWatch (debido a un fallo de conexión), puede verificar el log de PAN-OS `vm_cloud_logging.log`.

- **Data path interface failure (Fallo de interfaz de ruta de datos)**

  Mensaje: `ERROR: INTERFAZ: INACTIVA: MSGID: La interfaz <> dejó de estar activa`

- **HA interface failure (Fallo de interfaz de HA)**: este mensaje se aplica a un solo cortafuegos; no implica nada sobre el estado del par de HA. Por ejemplo, el estado del cortafuegos principal puede estar UP (ACTIVO) cuando el secundario está inactivo.

  `INFO: HA : ACTIVO: Estado HA <>`

  O

  `ERROR: HA : INACTIVA: MSGID: Estado HA <>`

- **Peer HA interface failure (Fallo de interfaz de para de HA)**: este mensaje es el estado del par en el par de HA.

  `ERROR: PEER_HA: ACTIVO: Estado de par de HA <>`

  O

  `ERROR: PEER_HA: INACTIVA: MSGID: Estado de par de HA <>`

- **Panorama Connectivity (Conectividad de Panorama)**

  `ERROR: PANORAMA: INACTIVA: MSGID: Conectividad <IP> de Panorama perdida`

  O

  `INFO: PANORAMA: ACTIVO: Panorama <IP> conectado`

Mensajes periódicos de estado

Cuando no hay cambios de estado, puede optar por generar un mensaje de estado periódico. De forma predeterminada, el intervalo de generación de logs en la nube es 0 (sin mensajes).

Por ejemplo, si su estado permanece activo, el mensaje es:

`INFO: PERIODIC_STATUS: CORRECTO: Todos los recursos en buen estado`

Si existen fallos de estado no resueltos, el mensaje periódico las vuelve a imprimir. Como se menciona en Formato de mensaje, el MSGID le ayuda a distinguir entre errores cuando está visualizando los logs periódicos.

`INFO: PERIODIC_STATUS: INCORRECTO : Recursos en mal estado`

`ERROR: INTERFAZ: INACTIVA: MSGID: Interfaz ethernet1/2 inactiva`

 ©2024 Palo Alto Networks, Inc.

- **Set the periodic interval from 10 to 300 seconds (Establecer el intervalo periódico de 10 a 300 segundos)**
  - **CLI:**

    solicitar intervalo de generación de logs en la nube de complementos vm_series <seconds>
  - **XML API:**

```
api/?type=op&cmd=<request>   <plugins>     <vm_series>
       <cloud-logging>         <interval>seconds</interval>
       </cloud-logging>      </vm_series>    </plugins> </
request>
```

- **Mostrar el intervalo de generación de logs en la nube**: utilice la CLI para mostrar el intervalo actual en segundos.

  mostrar intervalo generación de logs en la nube de complementos vm_series
- **Disable periodic logging (Desactivar generación de logs periódica)** : utilice la CLI para desactivar la generación de logs periódica.

  solicitar el intervalo 0 de generación de logs en la nube de complementos vm_series

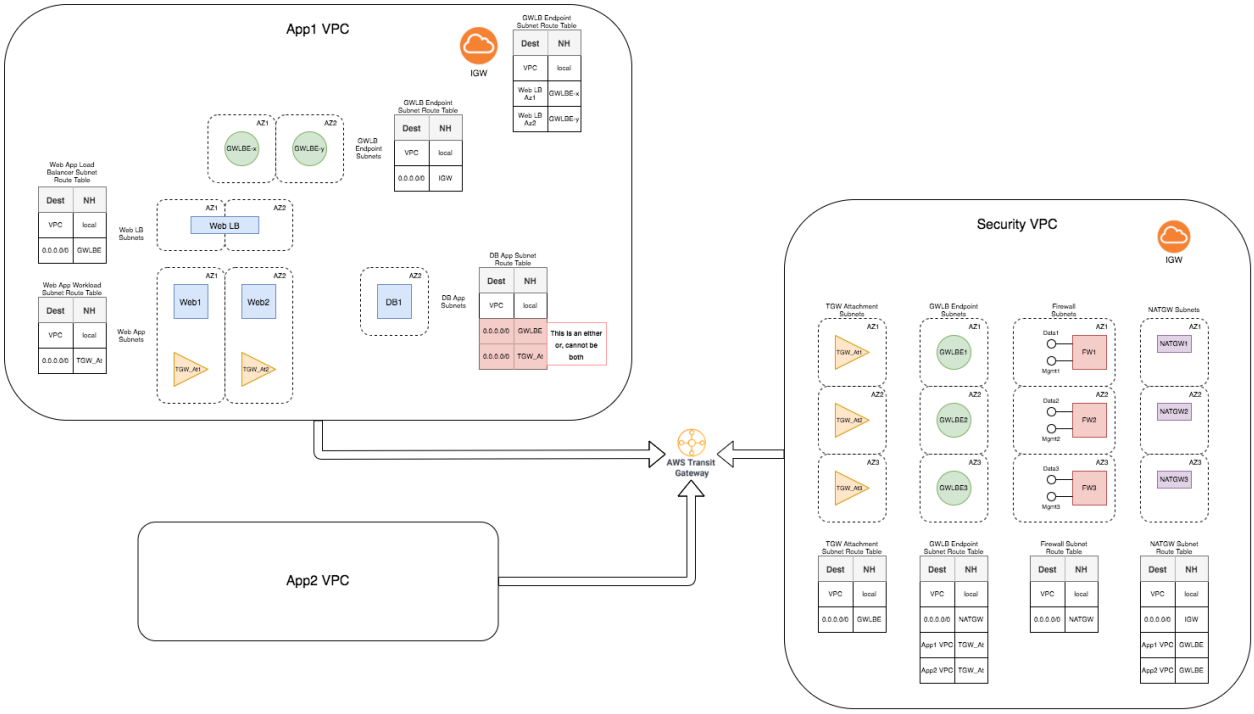
 ©2024 Palo Alto Networks, Inc.

Implementaciones orquestadas de Panorama en AWS

El complemento de Panorama para AWS 3.0.1 o posterior organiza las implementaciones del cortafuegos VM-Series en AWS y habilita políticas de seguridad para cortafuegos gestionados. AWS Orchestration se ha diseñado como un modelo plug and play para configurar implementaciones de seguridad en AWS. Simplifica la implementación de la solución Gateway Load Balancer (GWLB) existente al reunir toda la configuración en una pantalla en Panorama. Panorama permite que el complemento gestione su implementación y configure los recursos. Este complemento también realiza la gestión del cortafuegos al generar la configuración básica necesaria para que el tráfico fluya para la implementación. Cuando configure las políticas, el complemento dará servicio a los flujos de entrada, salida y Este/Oeste para todos los protocolos de tráfico. Utilice este complemento para configurar, implementar y gestionar sus implementaciones de seguridad.

La imagen a continuación destaca la topología de la implementación de la VPC de seguridad. Aquí, todos los recursos de seguridad se implementan en la VPC de seguridad gestionada por el complemento. La solución GWLB se aprovecha para redirigir el tráfico de sus aplicaciones a la pila de cortafuegos.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

Como parte de la configuración de la infraestructura en la nube de AWS, el complemento crea la VPC de seguridad con edpoints de GWLB, cortafuegos,y tablas de enrutamiento y subredes de puerta de enlace de NAT. El complemento no crea AWS Transit Gateway (TGW).

El cortafuegos VM-Series puede inspeccionar el tráfico enrutado entre las VPC.

El flujo de tráfico entrante que se origina en la VPC de aplicación fluye a través de la IGW y se redirige al endpoint de GWLB en función de la ruta de borde. El tráfico entra a través del endpoint de GWLB a los cortafuegos en la VPC de seguridad para su inspección. Después de la inspección, el tráfico se devuelve al endpoint de GWLB y se dirige a la aplicación original.

Para el tráfico saliente y Este-Oeste, esta solución aprovecha la TGW. Cuando crea una TGW, el complemento crea archivos adjuntos de TGW y tablas de rutas en la VPC de seguridad. Debe adjuntar su VPC de aplicación a la TGW utilizada en la configuración de VPC de seguridad. También debe dirigir el tráfico Saliente y de Este-Oeste a la TGW añadiendo rutas a las tablas de enrutamiento asociadas con sus subredes de carga de trabajo. Debe modificar la tabla de enrutamiento de adjuntos de la VPC de seguridad para dirigir el tráfico este-oeste y saliente al adjunto de VPC de seguridad.

El complemento supervisa los adjuntos de TGW para saber si hay adjuntos de VPC recién añadidos y eliminados. Cuando el complemento detecta un adjunto nuevo o existente, este realiza los cambios necesarios en la VPC de seguridad para garantizar que el cortafuegos inspeccione el tráfico que entra en TGW antes de enviarlo de vuelta a la TGW. Estos cambios incluyen añadir rutas a la tabla de enrutamiento de la puerta de enlace NAT para dirigir el tráfico saliente de vuelta al endpoint del GWLB y a la tabla de enrutamiento del endpoint del GWLB para devolver el tráfico a la TGW después de la inspección. El complemento actualiza la tabla de rutas del adjunto de la TGW para garantizar que el tráfico que vuelve de la VPC de seguridad a la TGW se envía al adjunto de la aplicación adecuado. El tráfico de la VPC de aplicación se dirige a la TGW a través del enrutamiento. Cuando el tráfico llega al adjunto de TGW en la VPC de seguridad, la tabla de rutas de adjuntos envía el tráfico a la VPC de seguridad. Desde allí, se dirige al endpoint de GWLB Endpoint existente y luego al cortafuegos para su inspección. El tráfico saliente fluye hacia la dirección de destino original a través de la puerta de enlace NAT. El tráfico Este-Oeste se envía de regreso a la TGW donde la tabla de enrutamiento dirige el tráfico a la dirección de destino original.

- Preparación para una implementación de AWS organizada
- Organice una implementación del cortafuegos VM-Series en AWS
- Ver el estado de implementación
- Flujo de tráfico y configuraciones

Preparación para una implementación de AWS organizada

Complete las siguientes tareas en AWS y Panorama antes de orquestar un cortafuegos VM-Series en AWS.

- **AWS**
  - Las implementaciones organizadas por Panorama en AWS requieren dos zonas de disponibilidad y admiten hasta seis zonas de disponibilidad.
  - Cree un perfil de instancia o usuario de AWS para una cuenta de AWS específica con acceso mediante programación y los permisos necesarios para permitir que el complemento cree recursos en la VPC de seguridad.

    Para la cuenta de seguridad:una cuenta de AWS con un perfil de usuario o instancia que tiene los permisos necesarios para lanzar recursos de AWS, como VPC, instancias de máquina virtual,

 ©2024 Palo Alto Networks, Inc.

balanceador de carga de AWS, las puertas de enlace de NAT y los endpoints. El complemento necesita que el perfil de usuario o instancia existente tenga el siguiente conjunto de permisos para declarar válido la función de IAM. El hipervínculo CFT en **Security Account (Cuenta de seguridad)** crea una directiva con los siguientes permisos.

```
"Statement":[ { "Effect": "Allow", "Action": "ec2:*", "Resource":
 "*" }, { "Effect": "Allow", "Action": "elasticloadbalancing:*",
 "Resource": "*" }, { "Effect": "Allow", "Action":
 "cloudwatch:*", "Resource": "*" }, { "Effect": "Allow",
 "Action": "autoscaling:*", "Resource": "*" }, { "Effect":
 "Allow", "Action": "sts:assumerole", "Resource": "*" },
 { "Effect": "Allow", "Action": "cloudformation:*", "Resource":
 "*" }, { "Effect": "Allow", "Action": [ "iam:Get*", "iam:List*",
 "iam:PassRole" ], "Resource": "*" }, { "Effect": "Allow",
 "Action": "ram:*", "Resource": "*" } ] },
```

Los siguientes permisos pormenorizados admiten a sus requisitos y permisos de seguridad. Estos permisos proporcionan una explicación detallada de las llamadas a la API realizadas desde el complemento. Los permisos se pormenorizan para admitir todas las acciones a las que se llamará desde el CFT y el código de back-end del complemento, tanto para la VPC de seguridad como para la VPC de aplicación entre cuentas.

Los siguientes permisos no se implementan en el complemento de AWS para Panorama versión 3.0.1 porque la lista de permisos detallada supera el límite de tamaño de la política de AWS. Para las políticas en línea, puede añadir tantas políticas como desee para un usuario, función o grupo, pero el tamaño total agregado de la política por entidad no puede superar estos límites: el tamaño de la política de usuario no puede superar los 2048 caracteres, el tamaño de la política de función no puede superar los 10240 caracteres y el tamaño de la política de grupos no puede superar los 5120 caracteres. Debido a estas limitaciones y al tiempo de validación del back-end, debe utilizar los permisos mencionados anteriormente.

```
{ "Version": "2012-10-17", "Statement":
 [ { "Sid": "VisualEditor0", "Effect": "Allow",
 "Action": [ "ec2:AuthorizeSecurityGroupIngress",
 "cloudwatch:PutMetricData", "ec2:Describe*",
 "cloudwatch:DeleteAlarms", "autoscaling:DescribePolicies",
 "ec2:DeleteVpcEndpoints", "ec2:AttachInternetGateway",
 "ec2:AcceptTransitGatewayVpcAttachment",
 "autoscaling:ExecutePolicy", "ec2:DeleteRouteTable",
 "sts:GetSessionToken", "cloudformation:DescribeStackEvents",
 "ec2:RevokeSecurityGroupEgress", "ec2:CreateRoute",
 "ec2:CreateInternetGateway", "cloudformation:UpdateStack",
 "ec2:DeleteInternetGateway", "iam:ListRolePolicies",
 "autoscaling:TerminateInstanceInAutoScalingGroup",
 "iam:ListPolicies", "ec2:DisassociateTransitGatewayRouteTable",
 "iam:GetRole", "iam:GetPolicy", "ec2:CreateTags",
 "elasticloadbalancing:CreateTargetGroup",
 "ec2:RunInstances", "ec2:DisassociateRouteTable",
 "ec2:CreateVpcEndpointServiceConfiguration",
 "ec2:CreateTransitGatewayRoute",
 "ec2:CreateTransitGatewayVpcAttachment",
 "elasticloadbalancing:DescribeAccountLimits",
```

 ©2024 Palo Alto Networks, Inc.

```
"elasticloadbalancing:AddTags", "cloudformation:DeleteStack",
"cloudwatch:DescribeAlarms", "ec2:DeleteNatGateway",
"ram:AssociateResourceShare",
"autoscaling:DeleteAutoScalingGroup", "ec2:CreateSubnet",
"elasticloadbalancing:ModifyLoadBalancerAttributes",
"iam:GetRolePolicy", "ec2:ModifyVpcEndpoint",
"ec2:DisassociateAddress",
"autoscaling:DescribeAutoScalingInstances",
"ec2:ModifyVpcEndpointServicePermissions",
"ec2:CreateNatGateway", "ec2:CreateVpc",
"ec2:ModifySubnetAttribute", "iam:PassRole",
"autoscaling:DescribeScalingActivities",
"sts:DecodeAuthorizationMessage",
"autoscaling:DescribeLoadBalancerTargetGroups",
"iam:ListAttachedGroupPolicies",
"ec2:DeleteLaunchTemplateVersions", "sts:GetServiceBearerToken",
"iam:ListAccessKeys", "ram:DisassociateResourceShare",
"ec2:ReleaseAddress", "ec2:DeleteLaunchTemplate",
"elasticloadbalancing:CreateLoadBalancer",
"ec2:AcceptVpcEndpointConnections", "iam:ListGroupPolicies",
"iam:ListRoles", "elasticloadbalancing:DeleteTargetGroup",
"ram:AssociateResourceSharePermission",
"ec2:CreateLaunchTemplate",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DeleteListener",
"ram:UpdateResourceShare", "iam:GetPolicyVersion",
"ec2:DeleteSubnet", "ec2:ModifyVpcEndpointServiceConfiguration",
"ec2:CreateTransitGatewayRouteTable",
"ec2:ModifyTransitGateway",
"cloudformation:DescribeStackResource",
"ec2:AssociateRouteTable",
"elasticloadbalancing:DeleteLoadBalancer",
"elasticloadbalancing:DescribeLoadBalancers",
"logs:CreateLogStream", "ec2:GetLaunchTemplateData",
"ec2:DeleteTransitGatewayVpcAttachment",
"autoscaling:DescribeAutoScalingGroups",
"iam:ListAttachedRolePolicies", "logs:GetLogEvents",
"autoscaling:UpdateAutoScalingGroup",
"ec2:AssociateTransitGatewayRouteTable",
"elasticloadbalancing:ModifyTargetGroupAttributes",
"autoscaling:SetDesiredCapacity",
"cloudformation:DescribeStackResources", "ec2:CreateRouteTable",
"ec2:DetachInternetGateway", "cloudformation:DescribeStacks",
"ec2:DeleteTransitGatewayRouteTable", "sts:AssumeRole",
"ec2:DeleteTransitGatewayRoute", "iam:GetUserPolicy",
"iam:ListGroupsForUser", "ec2:DeleteVpc", "iam:GetGroupPolicy",
"ec2:AssociateAddress", "autoscaling:CreateAutoScalingGroup",
"ram:AcceptResourceShareInvitation",
"ec2:DeleteTags", "logs:DescribeLogStreams",
"ec2:DeleteVpcEndpointServiceConfigurations",
"autoscaling:DeletePolicy", "elasticloadbalancing:RemoveTags",
"elasticloadbalancing:CreateListener",
"elasticloadbalancing:DescribeListeners",
"autoscaling:PutScalingPolicy", "ec2:CreateSecurityGroup",
"iam:ListAttachedUserPolicies", "ec2:ModifyVpcAttribute",
"ec2:ModifyInstanceAttribute",
```

 ©2024 Palo Alto Networks, Inc.

```
 "ec2:GetTransitGatewayRouteTableAssociations",
 "ram:DeleteResourceShare", "ec2:AuthorizeSecurityGroupEgress",
 "ec2:ModifyTransitGatewayVpcAttachment",
 "iam:GetInstanceProfile",
 "ram:DisassociateResourceSharePermission",
 "elasticloadbalancing:DescribeTags", "ec2:DeleteRoute",
 "iam:ListUserPolicies", "logs:PutLogEvents",
 "ec2:AllocateAddress", "ec2:CreateLaunchTemplateVersion",
 "cloudwatch:PutMetricAlarm", "cloudformation:CreateStack",
 "ec2:CreateVpcEndpoint", "ec2:DeleteSecurityGroup",
 "ec2:StartVpcEndpointServicePrivateDnsVerification",
 "ec2:ModifyLaunchTemplate", "iam:ListUsers",
 "ram:CreateResourceShare" ], "Resource": "*" } ] }
```

Para la cuenta de aplicación:una cuenta de AWS distinta de la Cuenta de seguridad que aloja a TGW o a las aplicaciones que deben protegerse. Dentro de esta cuenta debe crear un RoleARN con los siguientes permisos.

```
{ "Version": "2012-10-17", "Statement": [ { "Action":
 [ "ec2:Describe*", "ec2:DisassociateTransitGatewayRouteTable",
 "ec2:CreateTransitGatewayRoute",
 "ec2:CreateTransitGatewayRouteTable",
 "ec2:AssociateTransitGatewayRouteTable",
 "ec2:DeleteTransitGatewayRouteTable",
 "ec2:DeleteTransitGatewayRoute",
 "ec2:GetTransitGatewayRouteTableAssociations" ], "Resource":
 "*", "Effect": "Allow" }, { "Action": [ "iam:Get*",
 "iam:List*" ], "Resource": "*", "Effect": "Allow" } ] }
```

- **Dedicated CIDR block (Bloque CIDR dedicado)**: un bloque CIDR reservado para la VPC de seguridad. El complemento gestiona este bloque CIDR, usándolo para lanzar cortafuegos, balanceadores de carga y otros recursos de implementación para la VPC de seguridad.
- **AWS transit gateway (Puerta de enlace de transito de AWS)**: cree una TGW y asegúrese de que el usuario de AWS seleccionado tenga permiso para configurar los recursos de TGW.

La cuenta de AWS debe tener las dos funciones de IAM siguientes:

- AWSServiceRoleForElasticLoadBalancing
- AWSServiceRoleForAutoScaling

- **Panorama**
  - **Panorama Plugin for AWS (Complemento de Panorama para AWS)**: versión 3.0.1 o posterior.
  - **VM-Series Plugin (Complemento VM-Series)**: versión 2.0.6 o posterior.
  - **PanOS**: Versión 10.0.5 o posterior.
  - Cree una clave de API de licencia válida configurada en Panorama para eliminar la licencia de los cortafuegos.
  - Cree una función de IAM en el complemento en **Panorama** > **Plugins (Complementos)** > **AWS** > **Setup (Configuración)** > **IAM Roles (Funciones de IAM)**. Esta configuración necesita la clave de acceso y la clave secreta asociadas con el usuario que creó en su cuenta de AWS.

 ©2024 Palo Alto Networks, Inc.

Configuración de funciones de IAM para el complemento de AWS en Panorama

Con el complemento de AWS versión 3.0.1 o posterior, puede usar funciones de IAM para permitir que Panorama autentique y recupere metadatos en los recursos implementados dentro de su (s) cuenta (s) de AWS. Cuando su Panorama no está implementado en AWS, tiene dos opciones. Puede proporcionar las credenciales de IAM a largo plazo para las cuentas de AWS o configurar Asumir rol en AWS para permitir el acceso a los recursos de AWS definidos dentro de la misma cuenta de AWS o entre cuentas. Se recomienda Asumir rol como la opción más segura.

STEP 1 | Para validar las credenciales de usuario de AWS creadas para la VPC de seguridad, vaya a **Panorama** > **Plugins (Complementos)** > **AWS** > **Setup (Configuración)** > **IAM Roles (Funciones de IAM)**.

STEP 2 | Haga clic en **Add (Añadir)** e introduzca los siguientes detalles en **Security Account Detail (Detalle de la cuenta de seguridad)**.

- Escriba un nombre para la función de IAM y una descripción opcional.
- Introduzca la clave de acceso de AWS y la clave secreta para validar los permisos. Vuelva a introducir la clave secreta para confirmar la clave de acceso secreta.
- Seleccione un tipo de cuenta:**Instance Profile (Perfil de instancia)** o **AWS Account Credentials (Credenciales de cuenta de AWS)**. Si su Panorama se implementa en AWS, puede elegir adjuntar un perfil de instancia con los permisos correctos a su Panorama o añadir las credenciales asociadas con la función de IAM en Panorama. Si su Panorama no se implementa en AWS, debe introducir las credenciales para la función de IAM localmente en Panorama.

STEP 3 | En **Application Account Details (Detalles de la cuenta de la aplicación)**, busque y seleccione los RoleARN necesarios para proporcionar permisos válidos a la cuenta de seguridad para acceder a los recursos de la VPC de aplicación.

El estado de validez de la supervisión y la implementación están codificados por colores para facilitar la identificación.

- Válido (verde): indica que la clave secreta y la clave de acceso son válidas. Además, todas los RoleARN introducidos para el acceso a la cuenta de la aplicación tienen permisos válidos para realizar las acciones necesarias.
- Parcialmente válido (naranja): indica que la clave secreta y la clave de acceso son válidas, pero que uno o más RoleARNs especificados para el acceso a la cuenta de la aplicación no tienen permisos válidos para realizar las acciones necesarias. Haga clic en el hipervínculo de estado para abrir el IAM y ver qué RoleARNs específicos no cumplen.
- No válido (rojo): indica que la clave secreta y la clave de acceso introducidas no son válidas o no tienen permisos para realizar la acción necesaria.
- Confirmación requerida (gris): indica que se requiere una confirmación para la función.
- Validando (gris): indica que el complemento está intentando conectarse a AWS para verificar los requisitos necesarios. Si este estado continúa durante más de unos segundos, compruebe si se ha establecido la conexión con AWS.

Solo se permiten las funciones de IAM con estado verde o naranja para una configuración de implementación posterior.

 ©2024 Palo Alto Networks, Inc.

Organice una implementación del cortafuegos VM-Series en AWS

Complete el siguiente procedimiento para organizar la implementación de un cortafuegos VM-Series en AWS.

Las implementaciones de Panorama en AWS con un perfil de instancia no se admiten cuando se implementan detrás de un proxy.

STEP 1 | Entre en la interfaz web de Panorama.

STEP 2 | Instale el complemento Panorama para AWS 3.0.1 o posterior.

Para actualizar el complemento de Panorama para AWS a la versión 3.0.1, primero debe actualizar el complemento a la versión 2.0.2. Una vez instale la versión 3.0.1 del complemento de AWS, no podrá cambiar a la versión 2.0.x o anterior.

Si tiene una configuración de HA en Panorama, repita el proceso de instalación/actualización en cada par de Panorama.

Si actualmente tiene instalado un complemento de Panorama para cualquier plataforma en la nube, la instalación (o desinstalación) de un complemento adicional requiere un reinicio de Panorama para que pueda confirmar los cambios.

STEP 3 | Configuración de funciones de IAM para el complemento de AWS en Panorama

STEP 4 | Seleccione **Panorama** > **Plugins (Complementos)** > **AWS** > **Deployments (Implementaciones)** para **Add (Añadir)** una nueva implementación.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Escriba los detalles genéricos de la implementación en la pestaña **General**.

- Escriba un **Name (Nombre)** y una **Description (Descripción)** opcional para identificar la implementación en Panorama y la nube de AWS.
- Seleccione una **IAM Role (Función de IAM)** en el menú desplegable. La lista muestra las funciones de IAM que tienen permisos de implementación válidos o parcialmente válidos.

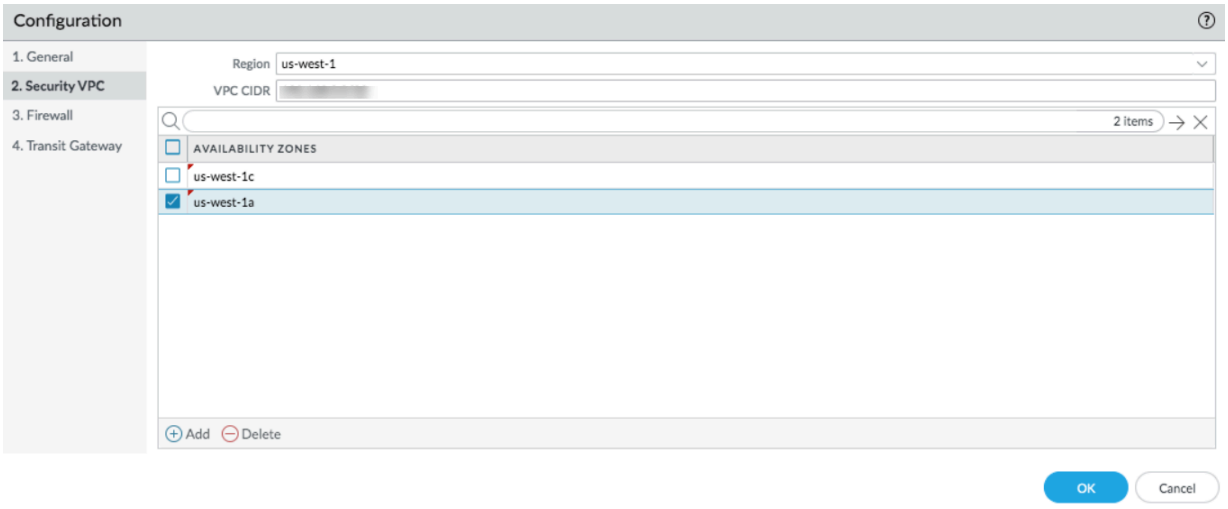
Una vez que se ha creado una función de IAM y se ha añadido a la implementación, puede editar la información de IAM (como la clave secreta y la clave de acceso). Sin embargo, no podrá editar el nombre de la función de IAM. Para cambiar el nombre, deberá eliminar el IAM y crear otro.



 ©2024 Palo Alto Networks, Inc.

STEP 6 | Introduzca la información relacionada con la VPC de seguridad en la pestaña **Security VPC (VPC de seguridad)**.

- Seleccione la **Region (Región)** de AWS en la que desea ejecutar la implementación. La lista muestra regiones basadas en la función de IAM seleccionada.
- Introduzca un valor de **VPC CIDR (CIDR de VPC)** para crear recursos en la VPC de seguridad. Este CIDR será gestionado por el complemento de AWS.
- Seleccione dos o más **Availability Zones (Zonas de disponibilidad)** de la lista rellenada previamente y siga los mismos criterios en AWS. Esta lista se rellena en función de la región seleccionada.



STEP 7 | Seleccione **Firewall (Cortafuegos)** > **Image (Imagen)** e introduzca los siguientes detalles.

- **License Type (Tipo de licencia)**:los tipos de licencia estándar **Bring Your Own License (Traer su propia licencia)** (BYOL), **Pay As you Go-Marketplace-Bundle1**, y **Pay As you Go-Marketplace-Bundle2** se proporcionan como opciones en el menú desplegable (según las regiones elegidas). Si selecciona **Bring Your Own License (Traer su propia licencia)**, prepárese para introducir un código de autenticación de licencia.

  Los paquetes 1 y 2 de pago por uso no se pueden usar con una imagen personalizada de AMI.

- (Opcional: aparece solo si elige el tipo de licencia **Bring Your Own License (Traer su propia licencia)** **License Authcode (Código de autenticación de licencia)**: introduzca el código

 ©2024 Palo Alto Networks, Inc.

de autenticación de su BYOL. Este código de autenticación determina qué tipos de instancia aparecen en el menú desplegable **Instance Type (Tipo de instancia)**.

- **Instance Type (Tipo de instancia)**:elija los tipos de instancias compatibles del menú desplegable. Esta lista se deriva del código de autenticación de la licencia.
- **Image Type (Tipo de imagen)**: seleccione Marketplace Image (Imagen de Marketplace) o Custom Image (Imagen personalizada).

  Si selecciona **Marketplace Image (Imagen de Marketplace)**, seleccione en el menú desplegable, **PanOS Version (Versión de PanOS)** 10.0.5 o posterior compatible con las regiones seleccionadas al configurar la VPC de seguridad.

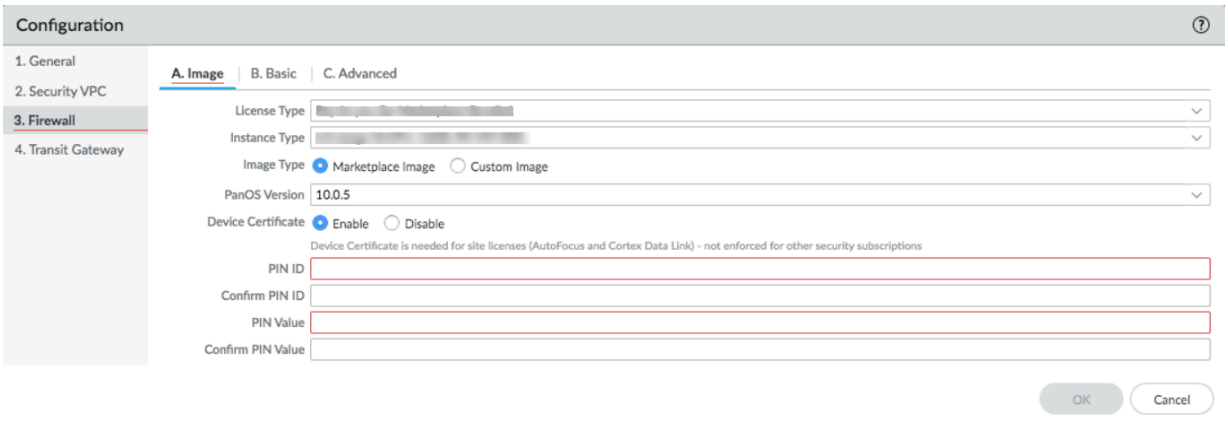
  Si selecciona **Custom Image (Imagen personalizada)**, introduzca el ID de Amazon Machine Image (AMI) y seleccione una versión de PanOS 10.0.5 o posterior.
- **Device Certificate (Certificado de dispositivo)**: el certificado de dispositivo se genera en el Portal de atención al cliente y le permite recuperar los derechos de licencia del sitio para AutoFocus o Cortex Data Link. Seleccione **Disable (Deshabilitar)** si no está utilizando estas licencias. Para configurar el PIN del certificado del dispositivo, seleccione **Enable (Habilitar)** e introduzca la siguiente información:

  PIN ID (ID de PIN): introduzca el ID de PIN.

  Confirm PIN ID (Confirmar ID de PIN): vuelva a introducir el ID de PIN.

  PIN Value (Valor del PIN): introduzca el PIN.

  Confirm VM PIN Value (Confirmar valor de PIN de MV): vuelva a introducir el PIN.



 ©2024 Palo Alto Networks, Inc.

STEP 8 | Seleccione **Firewall (Cortafuegos)** > **Basic (Básico)** e introduzca los siguientes detalles.

- **AWS Key Name (Nombre de clave de AWS)**: el nombre de una clave SSH que utilizará para iniciar sesión en los cortafuegos después de su implementación. Esta clave se inicia en el cortafuegos y se puede usar para depurar cuando el cortafuegos está en funcionamiento.
- **Existing Device Group (Grupo de dispositivos existentes)**: si selecciona **No**, el complemento crea el formato del nombre del grupo de dispositivos. Si selecciona **Yes (Sí)**, seleccione un **Device Group (Grupo de dispositivos)** existente de la lista desplegable.
- **Primary Panorama IP (IP principal de Panorama)**: la dirección IP del panorama que está utilizando. El menú desplegable muestra las direcciones IP públicas y privadas en la interfaz de gestión. Seleccione una dirección IP en el menú desplegable.

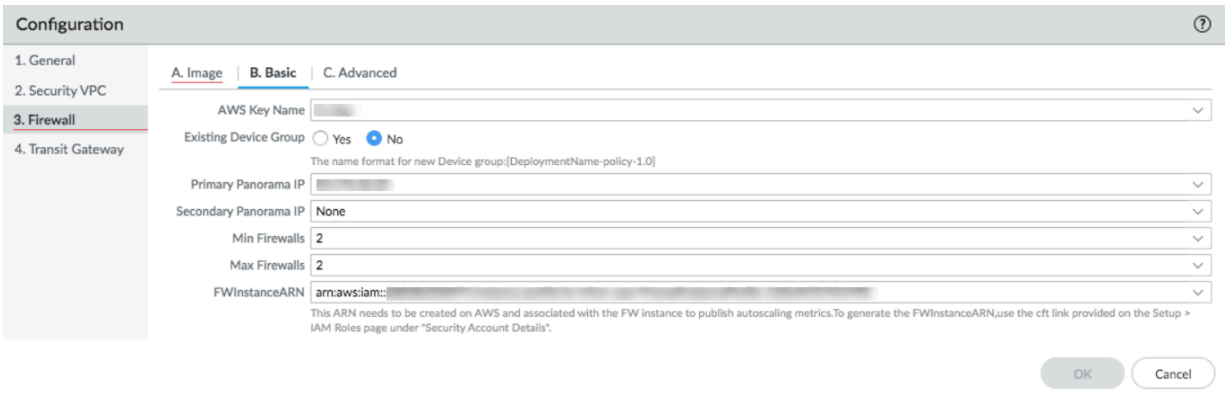
  *Si implementó Panorama detrás de un proxy, debe introducir manualmente la IP pública del Panorama principal en **Panorama** > **Setup (Configuración)** > **Interfaces** .*

  Si se utiliza la IP privada de Panorama, es posible que sea necesario agregar rutas a las tablas de rutas de AWS para las subredes de cortafuegos implementadas en complementos y la subred Panorama existente, con el fin de facilitar la conectividad entre los cortafuegos recién implementados y Panorama.
- **Secondary Panorama IP (IP secundaria de Panorama)**: si tiene una HA de Panorama, el menú desplegable enumera las direcciones IP en la interfaz de gestión del dispositivo secundario. Seleccione una dirección IP en el menú desplegable.

  Si el Panorama secundario tiene una dirección IP pública, es posible que no aparezca en el menú desplegable. En este caso, debe añadir manualmente la dirección IP del Panorama secundario.
- **Min Firewalls (Cortafuegos mínimos)**: el número mínimo de cortafuegos en un grupo de Escalado automático (ASG). Un valor entre 1 y 25.
- **Max Firewalls (Cortafuegos máximos)**: el número máximo de cortafuegos en un grupo de escalado automático (ASG). Un valor entre 2 y 25.
- **FirewallInstanceARN**: en el menú desplegable, seleccione el ARN de asumir función creado en la nube de AWS asociado a la instancia de cortafuegos para publicar métricas de escalado

 ©2024 Palo Alto Networks, Inc.

automático. El menú desplegable muestra solo las funciones ARN que ha introducido en la página **Setup (Configuración)** > **IAM Roles (Funciones de IAM)**.



 ©2024 Palo Alto Networks, Inc.

STEP 9 | (Opcional) Seleccione **Firewall (Cortafuegos)** > **Advanced (Avanzado)** e introduzca los siguientes detalles.

- **Autoscaling Metric (Métrica de escalado automático)**: elija una métrica en el menú desplegable: Porcentaje de utilidad de CPU de plano de datos (predeterminado), Sesiones activas, Porcentaje de utilidad de búfer de paquetes de plano de datos o Porcentaje de utilidad de sesión.
- **Scale In Threshold (Umbral de reducción horizontal)**: permite seleccionar un valor para el umbral de reducción horizontal. El valor depende de la métrica que ha seleccionado.
- **Scale Out Threshold (Umbral de ampliación horizontal)**: permite elegir un valor para el umbral de ampliación horizontal. El valor depende de la métrica que ha seleccionado.
- **Scale Out Threshold (Umbral de ampliación horizontal)**: permite elegir un valor para el umbral de ampliación horizontal. El valor depende de la métrica que ha seleccionado.
- **Jumbo Frame (Tramas gigantes)**: desactivado de forma predeterminada. Solo puede habilitar esta opción al preparar la implementación inicial. Seleccione **Enable (Habilitar)** para habilitar la compatibilidad con tramas gigantes en el cortafuegos.



STEP 10 | Seleccione si desea conectarse a una **Transit Gateway (Puerta de enlace de tránsito)** para gestionar el enrutamiento del tráfico en la VPC de seguridad y la VPC de aplicaciones.

- Seleccione si desea **Connect to TGW (Conectar aTGW)**. Si selecciona **Yes (Sí)**, prepárese para introducir un ID de TGW al que desee asociar la VPC de seguridad.

  Esta configuración solo es necesaria para los flujos de tráfico salientes o Este-Oeste.

- (Opcional) Seleccione un **TGW ID (ID de TGW)** al que desee asociar la VPC de seguridad.

  *Debe compartir la TGW si desea usarlas en todas las cuentas. Puede compartirlo mediante el **Resource Access Manager (Gestor de acceso de recursos)** (RAM) en AWS. Cree RAM basada en la cuenta donde se encuentra la TGW.*

- Seleccione **Application Account Names (Nombres de cuenta de aplicación)**. Si la TGW y la VPC de seguridad están en la misma cuenta, seleccione una cuenta de aplicación con la que desee compartir la TGW. El complemento crea la RAM en la Cuenta de seguridad para compartir la

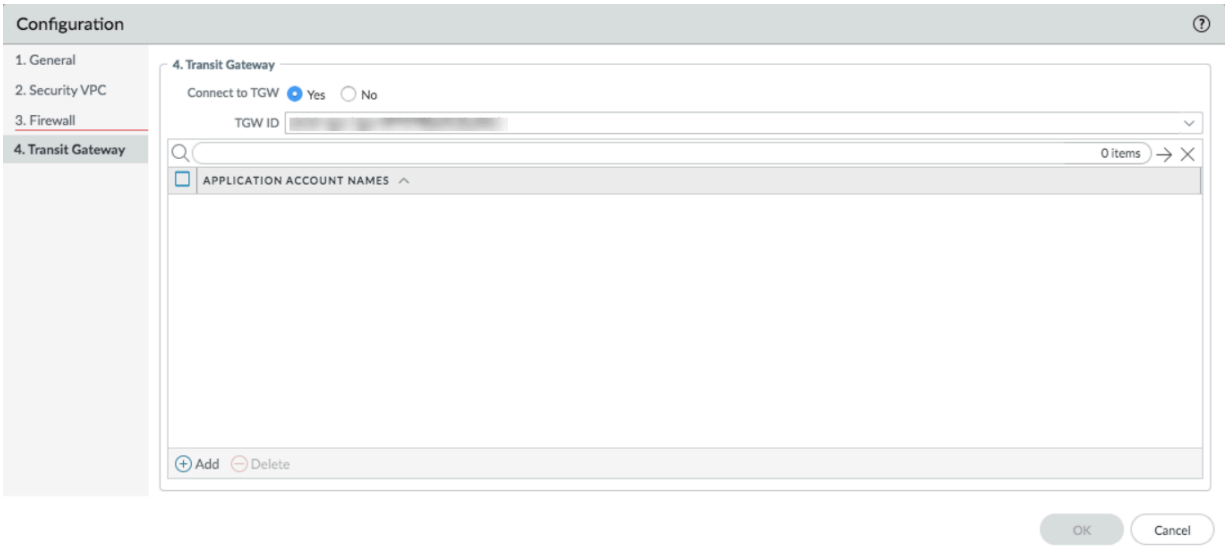
 ©2024 Palo Alto Networks, Inc.

TGW entre las cuentas de aplicación que ha seleccionado. Debe aceptar la invitación para RAM en la cuenta que seleccione aquí.

Si la puerta de enlace del tránsito (TGW) y la VPC de seguridad están en la misma cuenta, seleccione una cuenta de aplicación con la que desee compartir TGW. Si la TGW está en una cuenta de aplicación, asegúrese de que la TGW se comparte en el Gestor de acceso de recursos (RAM).

Si la TGW está en una cuenta de aplicación (que no sea la cuenta de seguridad):

1. Asegúrese de que la TGW esté compartida con la Cuenta de seguridad.
2. Utilice el hipervínculo de CFT en **Setup (Configuración)** > **IAM Roles (Funciones de IAM)** > **Application Account Details (Detalles de la cuenta de aplicación)**. Desde el CFT, puede crear el RAM para la TGW mencionada.
3. En la Cuenta de seguridad, asegúrese de ir al RAM en la consola de AWS y aceptar la solicitud para compartir la TGW.



STEP 11 | Seleccione **Commit (Confirmar)** para añadir la implementación y enviar a los cortafuegos.

 ©2024 Palo Alto Networks, Inc.

Ver el estado de implementación

Si hay una entrada en la columna **Deployment Status (Estado de la implementación)**, haga clic en el hipervínculo para ver los detalles de la implementación.

Los posibles mensajes de estado son:

- **Commit changes (Confirmar cambios)**:ha añadido una implementación por primera vez, pero aún no ha confirmado los cambios.

  Cada cambio de configuración para la implementación debe estar confirmado para que el complemento pueda recoger sus cambios.

- **Deploying (Implementación)**: el complemento está implementando o actualizando la implementación. Para obtener más información, haga clic en el hipervínculo para ver el estado detallado.
- **Failure (Fallo)**: la implementación ha fallado. Haga clic en el hipervínculo y vea el **Detailed Status (Estado detallado)** para la Pila de seguridad.
- **No Deployed (No implementado)**:el complemento está listo para implementar la configuración, pero la implementación no ha comenzado.
- **Success (Correcto)**: el complemento ha implementado correctamente la Pila de seguridad y los cortafuegos se han conectado a Panorama. Los cortafuegos pueden pasar el tráfico.
- **Warning (Advertencia)**: la implementación ha finalizado correctamente, pero algo externo a la implementación ha fallado. Por ejemplo, es posible que vea este mensaje:

  ```
  Los cortafuegos no se han conectado después de 20 minutos de la finalización de la implementación.
  ```

  Haga clic en el hipervínculo y vea la Pila de seguridad.

Una vez que se realiza la implementación, el complemento le permite modificar un cierto subconjunto de parámetros. Una vez realizados los cambios, debe realizar una confirmación antes de hacer clic en el botón **Redeploy (Volver a implementar)**. Cuando se produce una actualización, el complemento se asegura de que la configuración de Panorama esté creada y sea precisa. Vuelve a implementar el CFT para aplicar cualquier cambio, y adjuntar o desconectarse del TGW configurado (si se modificó esta configuración).

- **Deploy (Implementar)**: después de confirmar la configuración inicial, seleccione **Deploy (Implementar)** para iniciar la implementación.
- **Redeploy (Volver a implementar)**: modifique una implementación, confirme los cambios y seleccione **Redeploy (Volver a implementar)**.

  *Debe confirmar los cambios en la implementación antes de hacer clic en **Redeploy (Volver a implementar)**.*

- **Undeploy (Eliminar implementación)**: elimine una implementación, pero mantenga la configuración para que se pueda volver a implementar más adelante.

*Para quitar una implementación existente y su configuración, marque una implementación y seleccione **Delete (Eliminar)** en la parte inferior de la página de **Deployments (Implementaciones)**.*

 ©2024 Palo Alto Networks, Inc.

Estado detallado

Para acceder al **Detailed Status (Estado detallado)**,haga clic en el hipervínculo en la columna **Deployment Status (Estado de implementación)**. A partir del estado detallado, puede aprender dónde aplicar la configuración, ver el mensaje de error de un error de pila o ver el estado de implementación cuando se está implementando.

- **Name (Nombre)**: el nombre de la implementación.
- **Status (Estado)**: consulte el Deployment Status (Estado de implementación) para obtener la descripción de cada estado.
- **Detail (Detalle)**: detalles sobre la implementación seleccionada en **Deployment Status (Estado de implementación)**. Por ejemplo, si la implementación se realizó correctamente, muestra la fecha y hora de la implementación, o si hubo un error de pila, muestra un mensaje de error.
- **Policy Device Group (Política de grupo de dispositivos)**: el complemento puede crear una política de grupo de dispositivos para su implementación o puede elegir un grupo de dispositivos existente para que actúe como la política de grupo de dispositivos para una implementación específica.
- **Config Device Group (Configuración de grupo de dispositivos)**: el complemento crea una configuración de grupo de dispositivos como elemento secundario de la política de grupo de dispositivos. El complemento coloca la información de configuración de la implementación en la configuración de grupo de dispositivos, lo que garantiza que la política de grupo de dispositivos permanezca intacta si quita la implementación.

  No coloque información de políticas en la config del grupo de dispositivos.

- **Template Stack (Pila de plantillas)**: muestra la pila de plantillas asociada al cortafuegos VM-Series. Cualquier configuración personalizada se aplica a esta pila de plantillas.
- **External IP (IP externa)**: muestra las direcciones IP públicas de las puertas de enlace NAT de la VPC de seguridad, una para cada zona de disponibilidad. Las direcciones IP públicas salientes se utilizan para todo el tráfico saliente de la implementación y para el tráfico saliente de la interfaz de gestión del cortafuegos VM-Series.

  Para permitir que los cortafuegos se conecten a Panorama, las direcciones IP públicas salientes deben estar en la lista blanca del grupo de seguridad de Panorama.

- **CloudFormation Link (Enlace de CloudFormation)**: este vínculo abre la consola de AWS para mostrar la pila actual en la sección Servicios de Cloud Formation. Puede ver dónde se implementa la pila y depurar problemas con la implementación.
- **CloudWatch Link (Enlace de CloudWatch)**:este enlace abre la consola de AWS para mostrar los registros de **PaloAltoNetworkFirewalls (Cortafuegos de PaloAltoNetwork)** y los grupos de registros relacionados con el cortafuegos.
- **AutoScalingGroup Link (Enlace de AutoScalingGroup)**: este vínculo abre la consola de AWS para mostrar los detalles del ASG asociado con la implementación y la lista de instancias en el ASG. Puede ver los logs asociados a estas instancias en **CloudWatch Link (Enlace de CloudWatch)**.
- **Endpoint Service Name (Nombre del servicio de endpoint)**: el nombre del endpoint de GWLB creado como parte de la implementación. Por ejemplo, com.amazonaws.vpce.us-east-1.vpce-svc-0d00ebcb0000dc000.
- **Cloudformation Stack Name (Nombre de la pila de Cloudformation)**: por ejemplo, mynw-aws2-virgexstdg0-c0b0f.

 ©2024 Palo Alto Networks, Inc.

Flujo de tráfico y configuraciones

El complemento implementa y gestiona la VPC de seguridad. El complemento actualiza las tablas de rutas de la VPC de seguridad en función de los adjuntos descubiertos en AWS Transit Gateway.

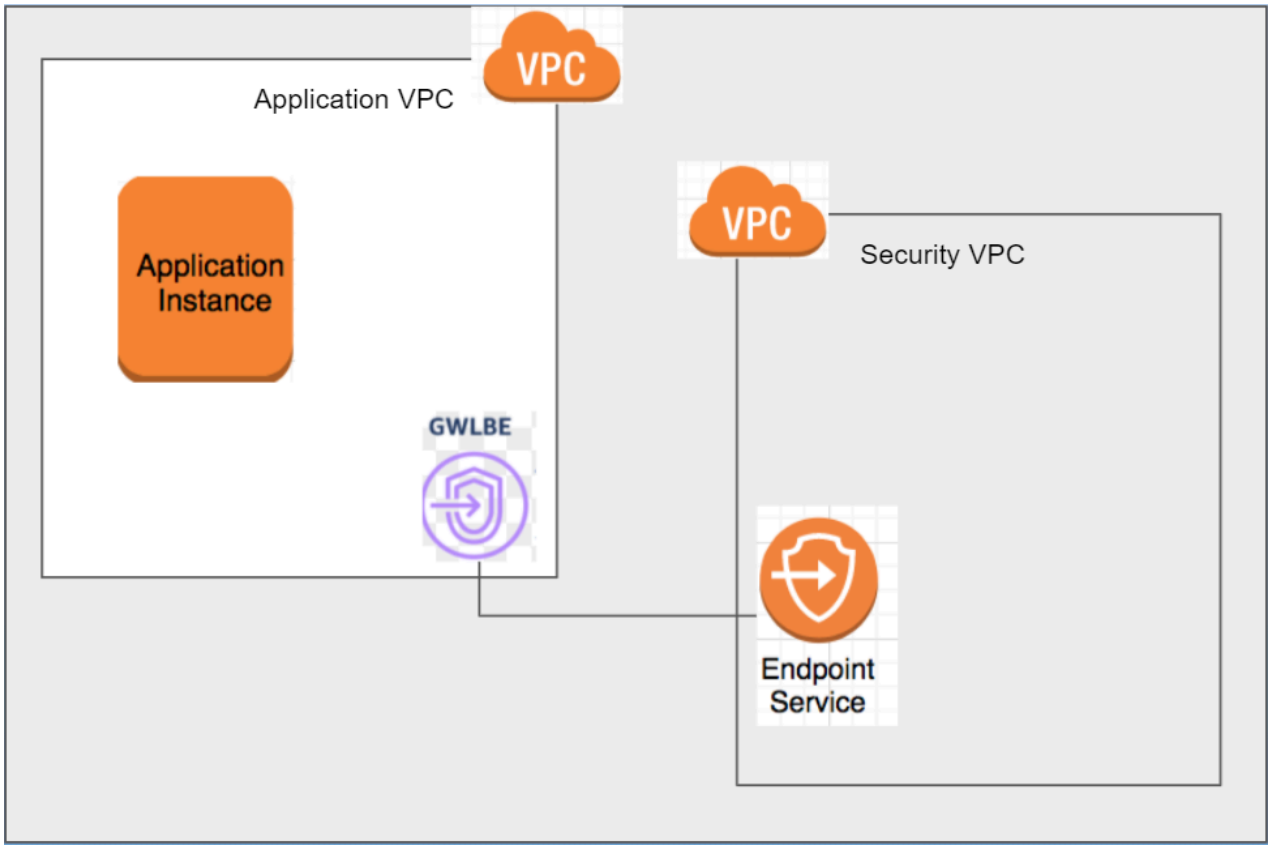
Flujo de tráfico entrante

Table 2: Combinaciones de flujo de tráfico entrante

	Aplicación	Tipo de trafico
1	En cuenta de seguridad	Entrante
2	En la cuenta de la aplicación	Saliente cruzado

Caso de uso: Tráfico entrante: la aplicación está en la Cuenta de seguridad

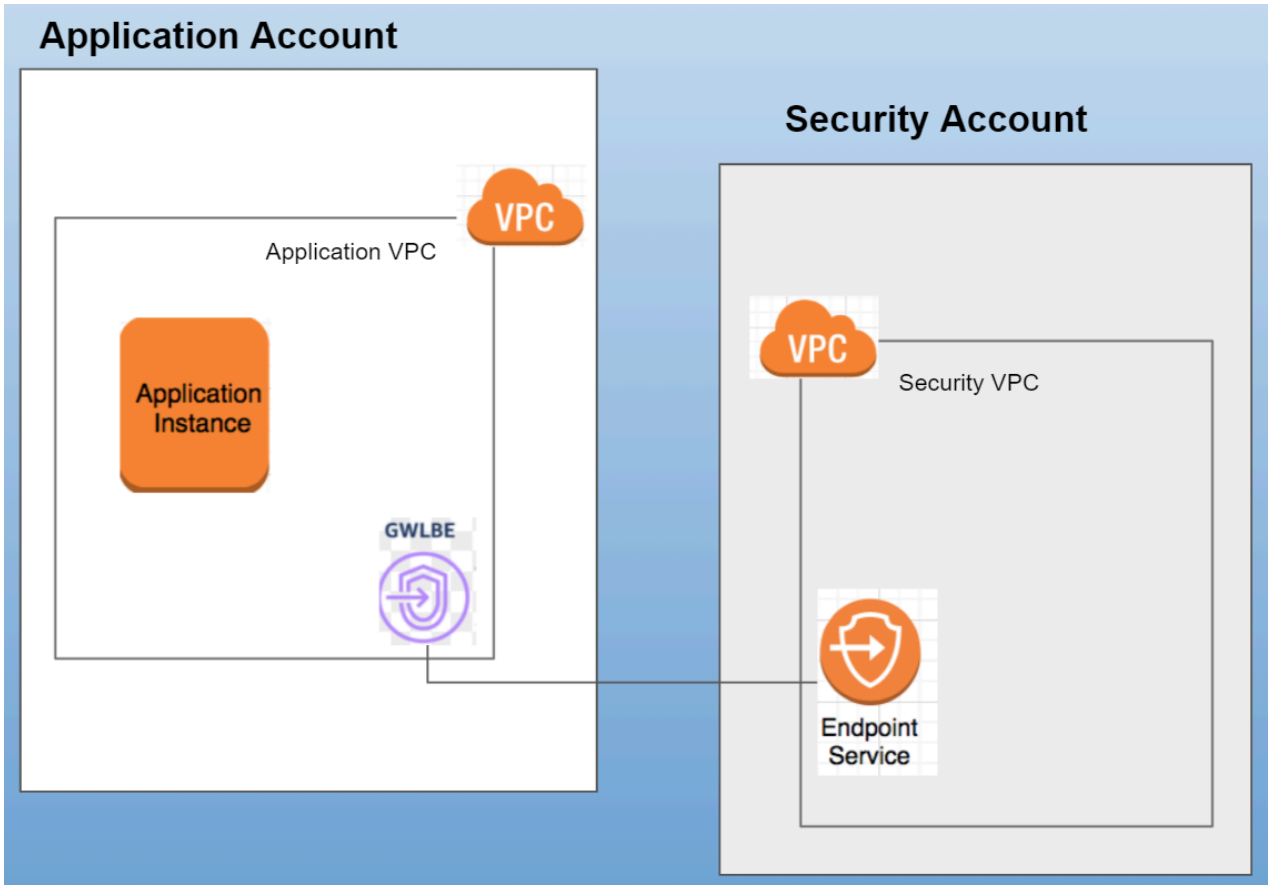
El complemento crea un Endpoint de servicio de VPC en la Cuenta de seguridad. Los Endpoints de GWLB deben estar asociados con el Servicio de endpoint de la VPC.



 ©2024 Palo Alto Networks, Inc.

Caso de uso: Tráfico entrante: la aplicación está en otra Cuenta de aplicación

Cuando la aplicación está en una cuenta diferente, en la consola de AWS, en el panel de navegación, seleccione **Endpoint Services (Servicios de endpoint)** y seleccione su Servicio de endpoints. Seleccione **Actions (Acciones)** > **Add Principal (Añadir principal)** para permitir principales. Por ejemplo, **`arn: aws: iam :: AccountNumber: root`**. Los Endpoints de GWLB deben estar asociados con el Servicio de endpoint de la VPC.



 ©2024 Palo Alto Networks, Inc.

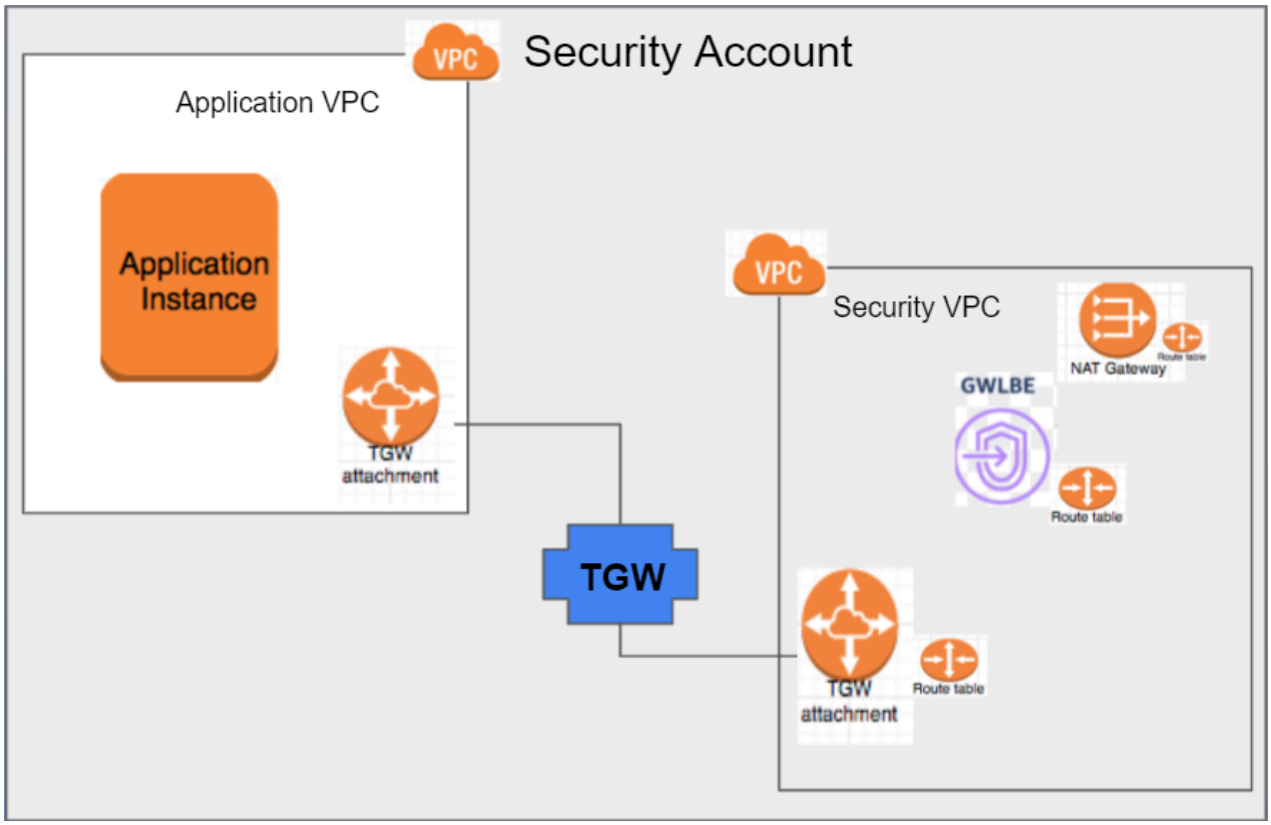
Flujo de tráfico saliente y este-oeste

Table 3: Combinaciones de flujo de tráfico saliente

	Transit Gateway	Aplicación	Tipo de trafico
1	En cuenta de seguridad	En cuenta de seguridad	Saliente
2	En cuenta de seguridad	En la cuenta de la aplicación	Saliente
3	En la cuenta de la aplicación	En la cuenta de la aplicación	Saliente cruzado
4	En la cuenta de la aplicación	En cuenta de seguridad	Saliente cruzado

Caso de uso: Tráfico saliente: Transit Gateway y la aplicación están en la cuenta de seguridad

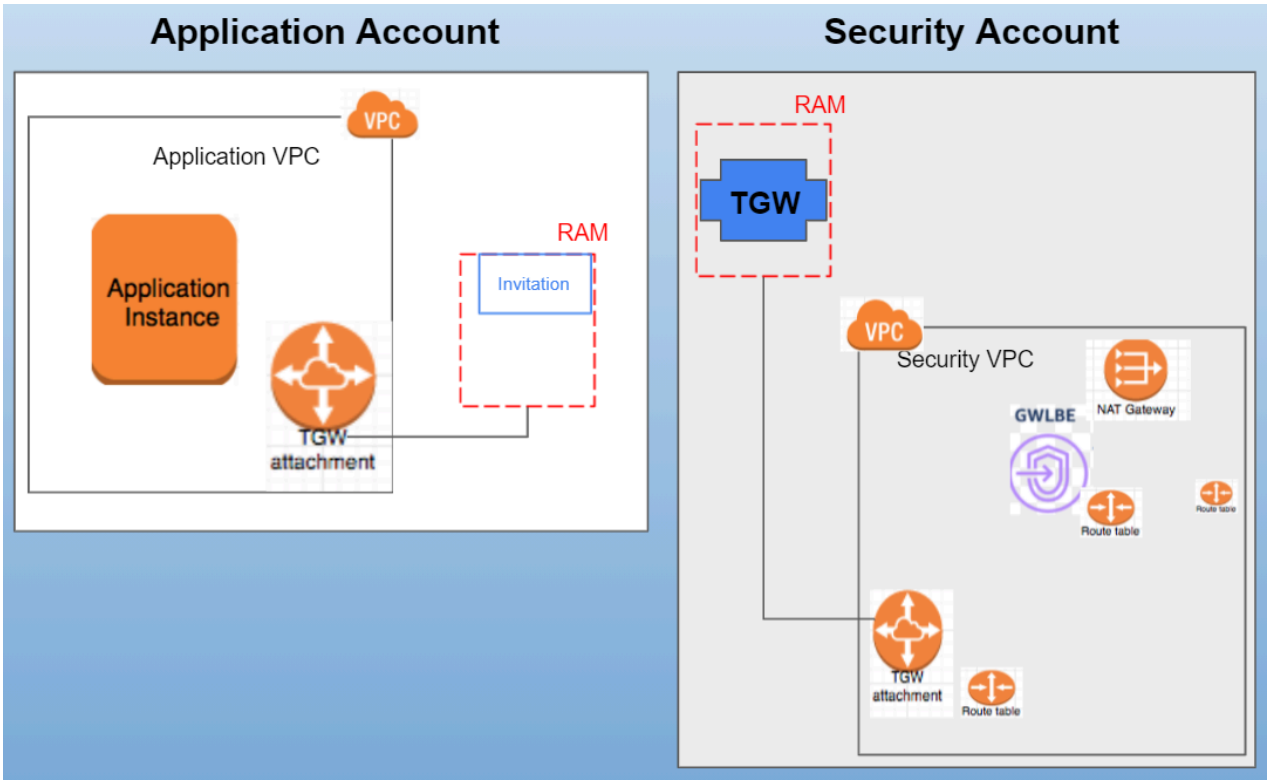
El complemento busca los adjuntos en la TGW configurada. Cuando el complemento detecta un adjunto nuevo o existente, realiza las modificaciones necesarias en la tabla de rutas en los componentes de la VPC de seguridad.



 ©2024 Palo Alto Networks, Inc.

Caso de uso: Tráfico saliente: Transit Gateway está en la cuenta de seguridad y la aplicación está en la cuenta de la aplicación

Cuando la TGW está en la Cuenta de seguridad, para proteger las aplicaciones que no están en la Cuenta de seguridad, la TGW se comparte entre estas aplicaciones mediante el Gestor de accesos a recursos, o Resource Access Manager, (RAM) en la consola de AWS. Puede elegir las cuentas con las que desea compartir la TGW desde la interfaz de usuario del complemento. Una vez que la implementación esté en estado de **Deploying (Implementación)**, controle el RAM en la cuenta de la aplicación en busca de una invitación para compartir recursos.



Caso de uso: Tráfico saliente: Transit Gateway y la aplicación están en la cuenta de la Aplicación

Cuando la TGW está en la cuenta de la aplicación, debe compartirse con la Cuenta de seguridad mediante el RAM. Para crear un adjunto de TGW y una tabla de ruta, se debe añadir un RoleARN de esta cuenta a la función de IAM usada para esta implementación. Utilice el hipervínculo CFT en **Setup (Configuración)** > **Application Account (Cuenta de la aplicación)** para configurar los requisitos previos de la cuenta de la aplicación.

©2024 Palo Alto Networks, Inc.

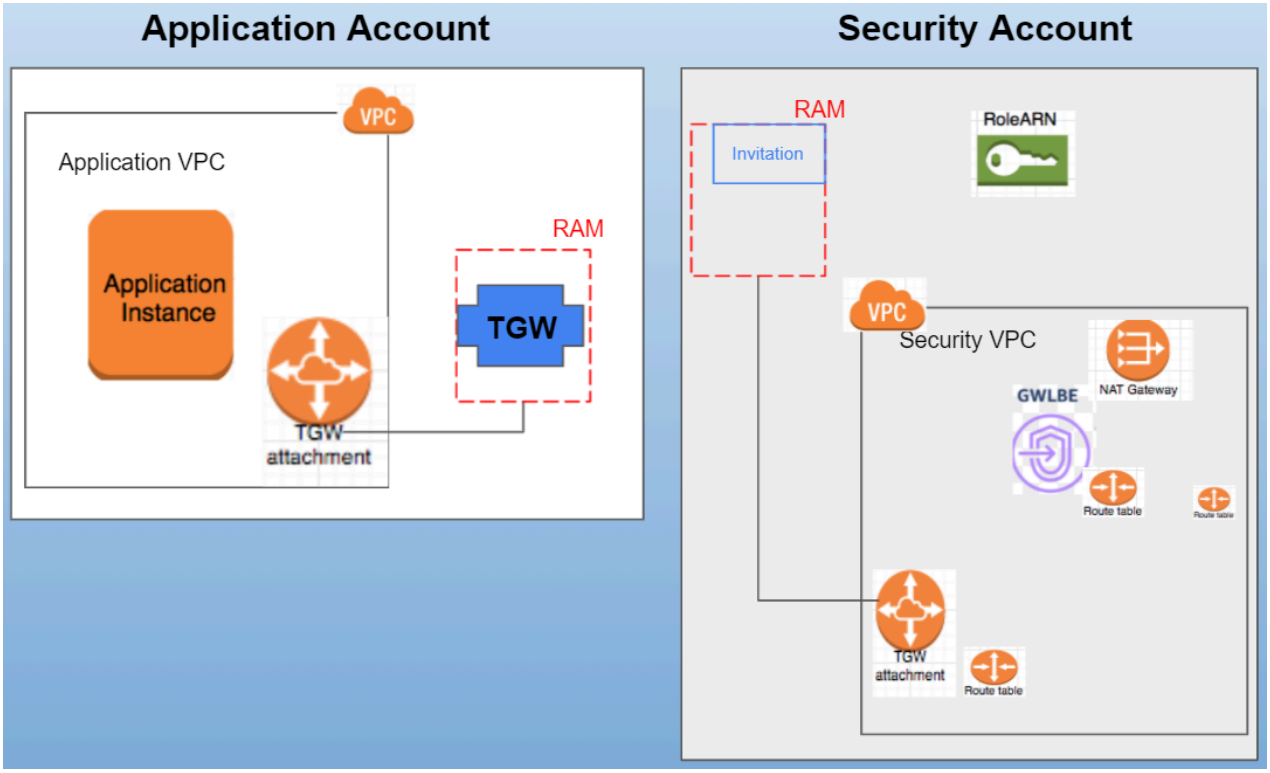


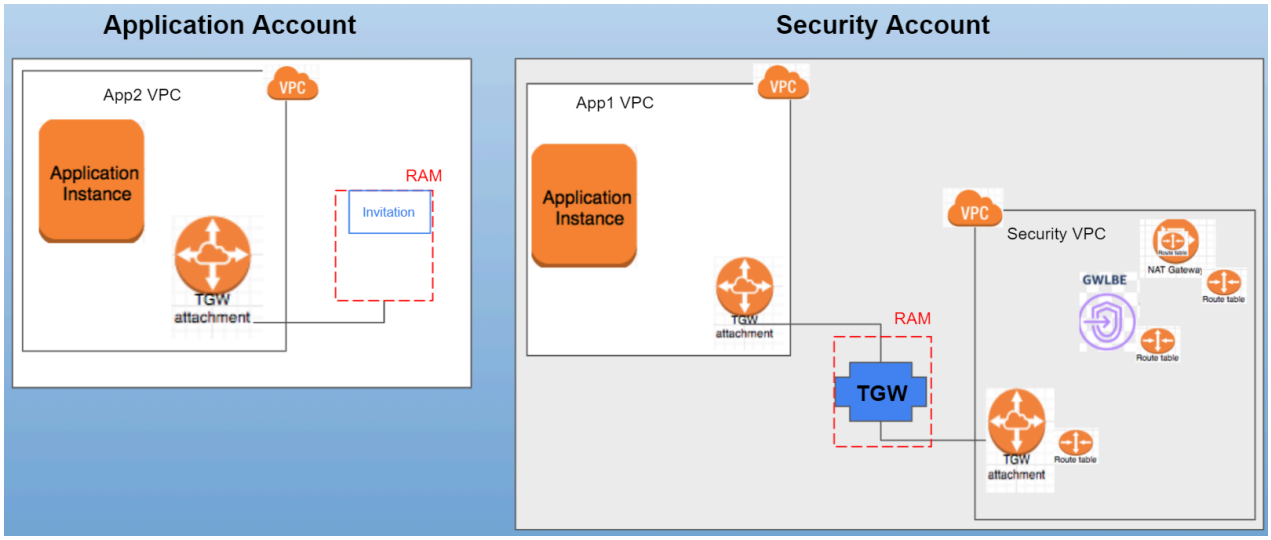
Table 4: Combinaciones de flujo de tráfico este-oeste

	Transit Gateway	Aplicación 1	Aplicación 2	Tipo de trafico
1	En cuenta de seguridad	En cuenta de seguridad	En cuenta de seguridad	Este oeste
2 (aplicación de varias cuentas)	En cuenta de seguridad	En cuenta de seguridad	En la cuenta de la aplicación	Este oeste
3	En la cuenta de la aplicación	En la cuenta de la aplicación	En la cuenta de la aplicación	Cruce este-oeste
4 (aplicación de varias cuentas)	En la cuenta de la aplicación	En la cuenta de la aplicación	En cuenta de seguridad	Cruce este-oeste

Caso de uso: Tráfico este-oeste: Transit Gateway y Application1 están en la cuenta de seguridad y Application2 está en la cuenta de seguridad

©2024 Palo Alto Networks, Inc.

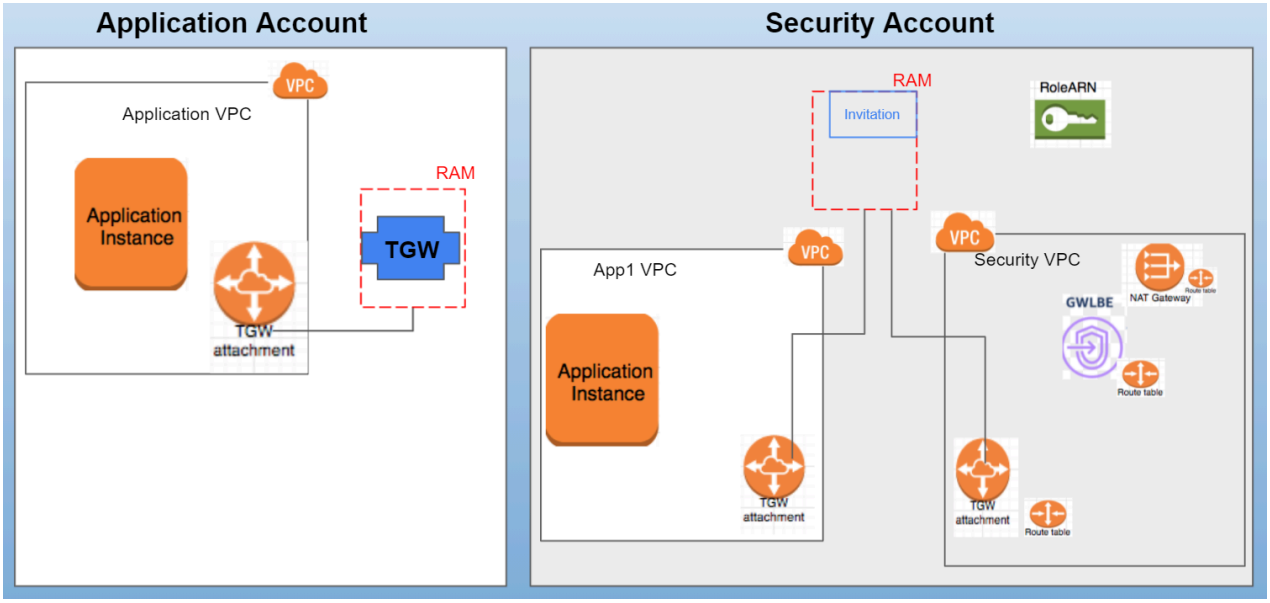
Cuando la TGW está en la Cuenta de seguridad, para proteger las aplicaciones que no están en la Cuenta de seguridad, la TGW se comparte entre estas aplicaciones mediante el Gestor de accesos a recursos, o Resource Access Manager, (RAM) en la consola de AWS. Puede elegir las cuentas con las que desea compartir la TGW desde la interfaz de usuario del complemento. Una vez que la implementación esté en estado de **Deploying (Implementación)**, controle el RAM en la cuenta de la aplicación en busca de una invitación para compartir recursos.



Caso de uso: Tráfico este-oeste: Transit Gateway y Application1 están en la cuenta de la aplicación y Application2 está en la cuenta de seguridad

Cuando la TGW está en la cuenta de la aplicación, debe compartirse con la Cuenta de seguridad mediante el RAM. Para crear un adjunto de TGW y una tabla de ruta, se debe añadir un RoleARN de esta cuenta a la función de IAM usada para esta implementación. Utilice el hipervínculo CFT en **Setup (Configuración)** > **Application Account (Cuenta de la aplicación)** para configurar los requisitos previos de la cuenta de la aplicación.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

Integración de VM-Series con un balanceador de carga Gateway de AWS

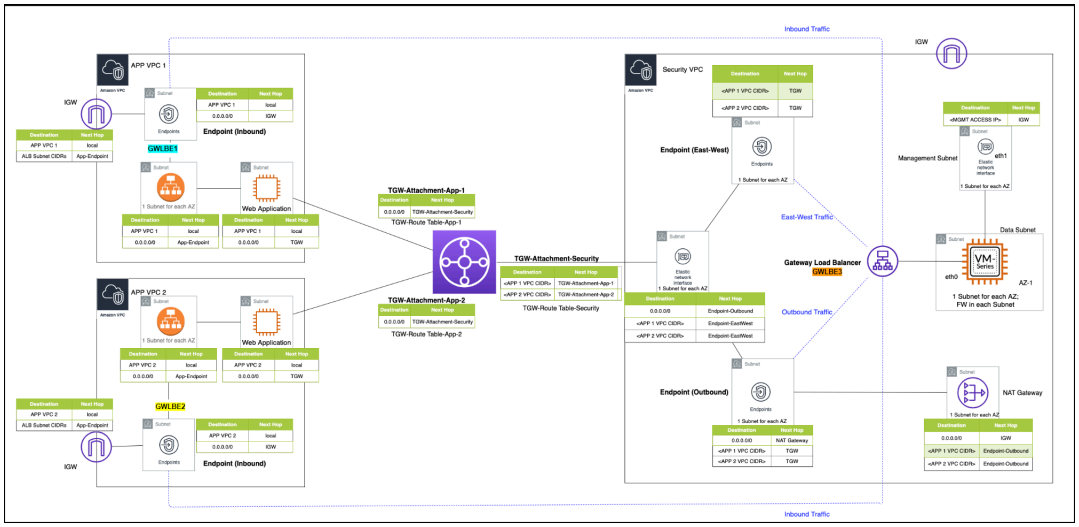
El Balanceador de carga Gateway de AWS (GWLB) es un servicio gestionado por AWS que le permite implementar una pila de cortafuegos VM-Series y operar de forma que se pueda ampliar horizontalmente y tolerar los fallos. A continuación puede exponer el GWLB de AWS con la pila de cortafuegos como un servicio de endpoint de VPC para la inspección del tráfico y la prevención de amenazas. Al crear endpoints del balanceador de carga Gateway (GWLBE) para el servicio de endpoint de VPC, puede insertar fácilmente una pila de cortafuegos VM-Series de escalado automático en las rutas de tráfico saliente, este-oeste y de entrada de sus aplicaciones. Los cortafuegos VM-Series y el GWLB utilizan la encapsulación GENEVE para mantener intactos los encabezados y la carga útil de los paquetes de tráfico, lo que brinda una visibilidad completa de la identidad de la fuente para sus aplicaciones.

Cuando se integra con un GWLB, un cortafuegos VM-Series que recibe tráfico encapsulado de GENEVE no puede finalizar el tráfico de túnel IPsec.

El cortafuegos VM_series admite el descifrado cuando se implementa detrás de un GWLB para casos de uso de reenvío y entrada, incluidos TLS1.2 y TLS1.3 que utilizan cifrados DHE/ECDHE.

La imagen a continuación describe cómo la integración de GWLB con VM-Series simplifica sus entornos de AWS Transit Gateway (TGW). Adjunta una VPC de seguridad centralizada a su puerta de enlace de tránsito. La VPC de seguridad centralizada incluye un GWLB para realizar un escalado y equilibrar la carga del tráfico en la pila de cortafuegos VM-Series.

La implementación del cortafuegos VM-Series detrás de una GWLB requiere que configure la Puerta de enlace de tránsito de AWS.



Para asegurarse de que el cortafuegos VM-Series pueda inspeccionar el tráfico que se enruta entre los adjuntos de VPC, debe habilitar el modo de dispositivo en el adjunto de VPC de la puerta de enlace de

 ©2024 Palo Alto Networks, Inc.

tránsito para la VPC de seguridad que contiene el cortafuegos VM-Series. Puede habilitar el modo de dispositivo mediante el comando:

```
modify-transit-gateway-vpc-attachment --transit-gateway-attachment-id
 <value> --options ApplianceModeSupport=enable
```

Para obtener más instrucciones, consulte Habilitación del modo de dispositivo.

Esto garantiza que el tráfico bidireccional se enrute simétricamente: tanto el tráfico de solicitud como el de respuesta se dirigen al mismo endpoint de puerta de enlace en la VPC del cortafuegos, y GWLB mantendrá la persistencia en el mismo cortafuegos VM-Series para su inspección antes de continuar hacia el destino correcto.

Cuando se implementa con un balanceador de carga Gateway, puede utilizar el cortafuegos VM-Series para proteger:

- Tráfico de entrada: tráfico que se origina fuera de la VPC y se destina a los recursos dentro de la VPC de su aplicación, como los servidores web. Los cortafuegos VM-Series evitan que el malware y las vulnerabilidades se introduzcan en la red con el tráfico permitido por los grupos de seguridad de AWS.
- Tráfico saliente: tráfico que se origina en las VPC de la aplicación y se destina a recursos externos en internet. Los cortafuegos VM-Series protegen los flujos de tráfico saliente al garantizar que las cargas de trabajo en las VPC de la aplicación se conecten a los servicios permitidos (como Windows Update) y categorías de URL permitidas, y evitan la filtración de información confidencial. Además, los perfiles de seguridad de los modelos VM-Series evitan que el malware y las vulnerabilidades se introduzcan en la red en el tráfico de retorno.
- Tráfico este-oeste: en un entorno de puerta de enlace de tránsito, el tráfico este-oeste se refiere al tráfico entre las VPC, como el tráfico entre las cargas de trabajo de origen y destino en dos VPC de aplicación distintas. Los cortafuegos VM-Series protegen los flujos de tráfico de este a oeste frente a la propagación de malware.

Para proteger el tráfico entrante a las VPC de su aplicación:

1. Cree puntos de conexión GWLBE (GWLBE1 y GWLBE2 en la figura anterior) con subredes independientes asociadas en sus VPC radiales. Asegúrese de tener subredes independientes para los endpoints de GWLB, ALB y la aplicación, y el adjunto de Transit Gateway dentro de la VPC de la aplicación.
2. Añada tablas de enrutamiento en la VPC de la aplicación (además de la ruta local de la VPC) de la siguiente manera:
    1. Tabla de enrutamiento con asociación de perímetro de IGW: añada un enrutamiento destinado a ALB con destino como GWLBE.
    2. Tabla de enrutamiento con asociación de subred ALB: añada una ruta destinada a 0.0.0.0/0 con destino como GWLBE.
    3. Tabla de enrutamiento con asociación de subred GWLBE: añada una ruta destinada a 0.0.0.0/0 con destino como IGW.

Con estas rutas en su lugar, el tráfico entrante que llega a la IGW de VPC se enruta hacia GWLBE. El GWLBE reenvía el tráfico a GWLB, que a su vez envía el tráfico al cortafuegos VM-Series en la VPC de seguridad para su inspección. El cortafuegos envía el tráfico de solicitud de vuelta a la VPC GWLBE de la aplicación, que luego reenvía el tráfico a la aplicación a través de ALB. ALB envía a esta solicitud el tráfico de respuesta a la aplicación de GWLBE, que a continuación envía el tráfico a GWLB. El GWLB

 ©2024 Palo Alto Networks, Inc.

a su vez envía el tráfico al cortafuegos VM-Series. Después de inspeccionar el tráfico de respuesta, el cortafuegos envía el tráfico de respuesta a la aplicación GWLBE, que a su vez envía el tráfico a IGW.

Para proteger el tráfico saliente de las VPC de la aplicación:

1. Cree un GWLBE (GWLBE3 en la figura anterior) en la VPC de cortafuegos centralizada. Asegúrese de que tiene subredes independientes para el endpoint de GWLB, conexión de Transit Gateway, puerta de enlace de NAT dentro de la VPC de seguridad.
2. Cree una puerta de enlace de NAT en la VPC de seguridad.
3. Añada tablas de enrutamiento de la siguiente manera:
    1. Tabla de enrutamiento con asociación de subred de aplicación: añada una ruta destinada a 0.0.0.0/0 con destino como TGW. Esto se suma a la ruta local de la VPC.
    2. Tablas de enrutamiento en la VPC de seguridad:
        - Tabla de enrutamiento con asociación de subred de conexión de TGW: además de la ruta local de la VPC, añada la ruta destinada a 0.0.0.0/0 con destino como GWLBE3.
        - Tabla de enrutamiento con asociación de subred GWLBE: además de la ruta local de la VPC, añada la ruta destinada a 0.0.0.0/0 con destino como puerta de enlace de NAT. Añada la ruta destinada a los CIDR de la VPC de la aplicación con destino como TGW.
        - Tabla de enrutamiento con asociación de subred de puerta de enlace NAT: además de la ruta local de la VPC, añada la ruta destinada a 0.0.0.0/0 con destino como IGW. Añada la ruta destinada a los CIDR de la VPC de aplicación con destino como GWLBE3.
    3. Añada las tablas de enrutamiento de Transit Gateway de la siguiente manera:
        - Tabla de enrutamiento con asociación App1-1 VPC TGW-Attachment: añada una ruta destinada a 0.0.0.0/0 con ID de datos conexión como datos de conexión TGW de la VPC de seguridad.
        - Tabla de enrutamiento con asociación App2-2 VPC TGW-Attachment: añada una ruta destinada a 0.0.0.0/0 con ID de conexión como conexión TGW de la VPC de seguridad.
        - Tabla de enrutamiento con asociación TGW-Attachment de la VPC de seguridad: (a) Añada una ruta destinada a App-1 VPC CIDR con ID de conexión como conexión TGW de VPC Application-1. (b) Añada una ruta destinada a App-2 VPC CIDR con ID de conexión como conexión TGW de VPC Application-2.

Con esta configuración implementada, el tráfico saliente iniciado desde Application(App1) se envía a TGW y TGW lo reenvía a la subred de la VPC de seguridad. El tráfico entonces se enruta a Security GWLBE (GWLBE3), que envía el tráfico al cortafuegos VM-Series para su inspección a través de GWLB. El cortafuegos VM-Series envía el tráfico de vuelta a GWLBE3 después de la inspección y GWLBE3 reenvía el tráfico a la puerta de enlace de NAT que envía el tráfico a través de IGW. Del mismo modo, el tráfico de respuesta pasa a través de la puerta de enlace de NAT a GWLBE3, el cortafuegos VM-Series y TGW, después de lo cual se enruta de regreso a la aplicación.

El tráfico Este-Oeste también se gestiona con las rutas y la configuración descritas en los pasos anteriores. Cuando el tráfico se envía de App1 a App2, el tráfico pasa a través de TGW que enruta el tráfico a GWLBE3. El GWLBE3 reenvía el tráfico al cortafuegos VM-Series a través de GWLB. El cortafuegos VM-Series envía el paquete de vuelta a GWLBE3 después de la inspección. GWLBE3 luego reenvía el paquete a App2 a través de TGW. El tráfico de respuesta de App-2 a App-1 tomará la ruta inversa.



Se recomienda tener todas las subredes en la misma zona de disponibilidad (AZ) para evitar cargos de tráfico entre zonas.

 ©2024 Palo Alto Networks, Inc.

Integración manual de VM-Series con un balanceador de carga Gateway

Consulte los siguientes temas para integrar manualmente el cortafuegos VM-Series con un balanceador de carga de puerta de enlace de AWS.

- Habilite la integración de VM-Series con un balanceador de carga Gateway
- Integre manualmente VM-Series con un balanceador de carga Gateway
- (Opcional) Asociar un endpoint VPC con una interfaz de VM-Series
- (Opcional) Habilitar el enrutamiento de superposición para la VM-Series en AWS

Habilite la integración de VM-Series con un balanceador de carga Gateway

Al integrar el cortafuegos VM-Series con un GWLB, primero debe habilitar el cortafuegos VM-Series para procesar correctamente el tráfico redirigido al cortafuegos por los endpoints de GWLB. Puede habilitar esta funcionalidad mediante la CLI de cortafuegos VM-Series, a través del paquete de arranque de VM-Series o el campo de datos de usuario en la consola de AWS.

La implementación de cortafuegos VM-Series con un GWLB requiere:

- PAN-OS 10.0.2 o posterior
- Complemento de VM-Series 2.0.2 o posterior
- Panorama 10.0.2 o posterior si usa Panorama para gestionar sus cortafuegos

En la tabla siguiente se enumeran los comandos necesarios para habilitar la inspección de tráfico GWLB con un endpoint de VPC. Los comandos de operación se pueden usar en un archivo de arranque init-cfg.txt o en el campo de datos de usuario en la consola de AWS.

Parámetro de arranque	Comando de la CLI	Description (Descripción)
op-command-modes=mgmt-interface-swap	op-command-modes=mgmt-interface-swap *Este comando requiere que el cortafuegos se reinicie antes de que surta efecto.*	Intercambia eth0 y eth1. GWLB de forma predeterminada, envía el tráfico solo a Eth0 de sus instancias de destino. Al intercambiar, Eth0 se convierte en la interfaz de datos y eth1 se convierte en la interfaz de gestión.
plugin-op-commands=aws-gwlb-inspect:enable	request plugins vm_series aws gwlb inspect enable <yes/no>	Permite que el cortafuegos VM-Series procese el tráfico que pasa a través de un GWLB.

Integre manualmente VM-Series con un balanceador de carga Gateway

Complete el siguiente procedimiento para integrar manualmente su cortafuegos VM-Series en AWS con un GWLB.

©2024 Palo Alto Networks, Inc.

Si asocia puntos de enlace de VPC a una interfaz o subinterfaces a través de datos de usuario durante el arranque y su archivo bootstrap.xml no incluye la configuración de la interfaz, puede configurar las interfaces después de iniciar el cortafuegos.

STEP 1 | Configure la VPC de seguridad. Consulte la Documentación de AWS para obtener más información sobre cómo crear su VPC de seguridad.

- Cree dos subredes: una para gestión y otra para datos.
- Cree dos grupos de seguridad: uno para la gestión del cortafuegos y otro para los datos.
- Los grupos de seguridad de la subred de gestión deben permitir https y ssh para el acceso de gestión.
- Asegúrese de que el o los grupos de seguridad en su VPC de datos permitan paquetes encapsulados con el protocolo GENEVE (puerto UDP 6081).
- Si su implementación incluye una puerta de enlace de tránsito y tráfico que se moverá entre VPC, debe habilitar el modo de dispositivo en el adjunto de VPC de seguridad.

El grupo de destino del GWLB no puede utilizar HTTP para las comprobaciones de estado porque el cortafuegos VM-Series no permite el acceso con un protocolo no seguro. En su lugar, utilice otro protocolo como HTTPS o TCP.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Inicie el cortafuegos VM-Series.

1. En el panel EC2, haga clic en **Launch Instance (Iniciar instancia)**.
2. Seleccione la AMI de VM-Series de Palo Alto. Para obtener la AMI, consulte Obtención de la AMI.
3. Inicie el cortafuegos VM-Series en la instancia de EC2.
   1. Elija el **EC2 instance type (Tipo de instancia de EC2)** para asignar los recursos requeridos para el cortafuegos y haga clic en **Next (Siguiente)**. Consulte Requisitos del sistema para VM-Series, para conocer los requisitos de recursos.
   2. Seleccione la VPC de seguridad.
   3. Seleccione la subred de datos para adjuntar a eth0.
   4. Añada otra interfaz de red para que eth1 actúe como interfaz de gestión después del intercambio de interfaz. El intercambio de interfaces requiere un mínimo de dos ENI (eth0 y eth1).
      - Expanda la sección Interfaces de red y haga clic en **Add Device (Añadir dispositivo)** para añadir otra interfaz de red y configurar la subred de gestión a esta interfaz.

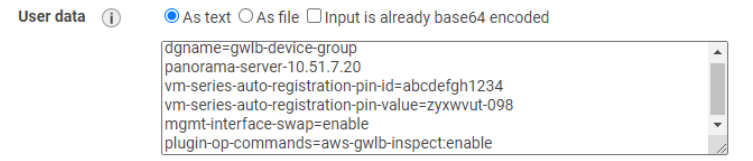
        Asegúrese de que su VPC tiene más de una subred, para que pueda añadir ENI adicionales al inicio.

        Si inicia el cortafuegos con solo un ENI:
        - *El comando de intercambio de interfaz hará que el cortafuegos arranque en el modo de mantenimiento.*
        - *Debe reiniciar el cortafuegos cuando añade el segundo ENI.*
      - Expanda la sección Advanced Details (Detalles avanzados) y en el campo **User data (Datos de usuario)** introduzca como texto para realizar el intercambio de interfaz durante el inicio.

        `mgmt-interface-swap=enable`

        `plugin-op-commands=aws-gwlb-inspect:enable`

        Si configura el tipo de destino en la dirección IP de una interfaz específica en el cortafuegos VM-Series, no necesita habilitar el intercambio de interfaz de gestión.

   5. Acepte la configuración de **Storage (Almacenamiento)** predeterminada. El cortafuegos utiliza el tipo de volumen SSD (gp2).
   6. Si se le solicita, seleccione una opción de **SSD** adecuada para su configuración.
   7. (Opcional) **Tagging (Etiquetado)**. Añada una o más etiquetas para crear sus propios metadatos e identificar y agrupar el cortafuegos VM-Series. Por ejemplo, añada una etiqueta

 ©2024 Palo Alto Networks, Inc.

Name (Nombre) con un **Value (Valor)** que le ayude a recordar que las interfaces ENI se hayan intercambiado en este cortafuegos VM-Series.

8. Seleccione el **Security Group (Grupo de seguridad)** de datos para eth0 (interfaz de datos). Habilite el tráfico en el puerto UDP 6081.

   Si habilita las verificaciones de estado en el cortafuegos, no puede utilizar HTTP. En su lugar, utilice otro protocolo como HTTPS o TCP.

9. Seleccione **Review and Launch (Revisar e iniciar)**. Revise que sus selecciones son precisas y haga clic en **Launch (Iniciar)**.

10. Seleccione un par de claves existente o cree uno nuevo y acepte el descargo de responsabilidad de claves.

    La primera vez que se accede al cortafuegos se solicita este par de claves. También es necesario acceder al cortafuegos en el modo de mantenimiento.

11. Descargue y guarde la clave privada en un lugar seguro; la extensión del archivo es `.pem`. Si pierde la clave, no se puede volver a regenerar.

    Se tardará entre 5 y 7 minutos en iniciar el cortafuegos VM-Series. Puede consultar el progreso en el panel EC2. Al completar el proceso, el cortafuegos VM-Series se muestra en la página **Instances (Instancias)** del panel EC2.

STEP 3 | Adjunte el grupo de seguridad de gestión a eth1 (interfaz de gestión). Permita ssh y https. Consulte la Documentación de AWS para obtener más información.

STEP 4 | Cree y asigne una dirección IP elástica (EIP) a la ENI utilizada para el acceso de gestión (eth1) al cortafuegos.

1. Seleccione **Elastic IP (IP elástica)** y haga clic en **Allocate New Address (Asignar nueva dirección)**.
2. Seleccione **EC2-VPC** y haga clic en **Yes, Allocate (Sí, asignar)**.
3. Seleccione la EIP recién asignada y haga clic en **Associate Address (Asociar dirección)**.
4. Seleccione la **Network Interface (Interfaz de red)** y la **Private IP address (Dirección IP privada)** asociada con la interfaz de gestión y haga clic en **Yes, Associate (Sí, asociar)**.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Configure una nueva contraseña de administración para el cortafuegos.

En la CLI del cortafuegos VM-Series, debe configurar una contraseña administrativa única para poder acceder a la interfaz web del cortafuegos. Para iniciar sesión en la CLI, necesita la clave privada que ha utilizado para iniciar el cortafuegos.

1. Use la EIP para hacer SSH en la interfaz de línea de comando (CLI) del cortafuegos VM-Series. Necesitará la clave privada que utilizó o creó anteriormente y que utiliza el nombre de usuario **admin (administrador)** para acceder a la CLI.

   Si utiliza PuTTY para el acceso SSH, debe convertir el formato .pem al formato .ppk. Consulte https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html
2. Introduzca el siguiente comando para iniciar sesión en el cortafuegos:

   ssh-i <*private_key.pem*> admin@<*public-ip_address*>
3. Configure una nueva contraseña usando el siguiente comando y siga las indicaciones en pantalla:

   configure

   set mgt-config users admin password
4. Si tiene una BYOL que debe activarse, configure la dirección IP del servidor DNS de modo que el cortafuegos pueda acceder al servidor de licencias de Palo Alto Networks. Introduzca el siguiente comando para configurar la dirección IP del servidor DNS:

   set deviceconfig system dns-setting servers primary <*ip_address*>
5. Confirme los cambios con el comando:

   commit
6. Finalice la sesión SSH.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Configure la interfaz de red del plano de datos como una interfaz de capa 3 en el cortafuegos.

En los servidores de aplicaciones dentro de la VPC, defina la interfaz de red de plano de datos del cortafuegos como la puerta de enlace predeterminada.

1. Si usa una conexión segura (https) desde su navegador web, inicie sesión usando la dirección EIP y la contraseña que asignó durante la configuración inicial (https://<Elastic_IP address>). Verá una advertencia de certificación; es normal. Vaya a la página web.
2. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
3. Haga clic en el enlace de **ethernet 1/1** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **capa 3**
   - En la pestaña **Config (Configuración)**, asigne la interfaz al enrutador virtual predeterminado.
   - En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. Defina una nueva zona y deje los campos restantes con valores predeterminados y, a continuación, haga clic en **OK (Aceptar)**.
   - En la pestaña **IPv4**, seleccione **DHCP Client (Cliente DHCP)**.

     Si usa DHCP, seleccione **DHCP Client (Cliente DHCP)**; la dirección IP privada que ha asignado a la ENI en la consola de administración de AWS se adquirirá de manera automática.
   - En la pestaña Avanzada, cree un perfil de gestión para habilitar el servicio HTTP como parte de la creación de perfiles de gestión y permitir sondeos de comprobación de estado desde GWLB.
   - (Opcional) En la pestaña IPv6, seleccione **Enable IPv6 on this Interface (Habilitar IPv6 en esta interfaz)** y seleccione **DHCPv6 Client (Cliente DHCPv6)**.

     La VM-Series para AWS detrás de un GWLB solo admite IPv6 como parte de AWS Dualstack, lo que significa que los clientes se comunican con los balanceadores de carga mediante direcciones IPv4 e IPv6. IPv6 solo no es compatible con AWS GWLB. Consulte la Documentación de AWS para obtener más información.

     Además, debe crear una política de seguridad que permita el tráfico IPv6.
4. Haga clic en **Commit (Confirmar)**. Verifique que el estado del enlace para la interfaz está en activo.

STEP 7 | Cree políticas de seguridad para permitir/denegar el tráfico.

Dado que VM-Series trata el tráfico como intrazona cuando se integra con un GWLB, una regla intrazona predeterminada permite todo el tráfico. Se recomienda anular la regla intrazona predeterminada con una acción de denegación para el tráfico que no coincide con ninguna de las otras reglas de la política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** en la interfaz web del cortafuegos.
2. Haga clic en **Add (Añadir)** y especifique las zonas de seguridad, aplicaciones y opciones de inicio de sesión que le gustaría ejecutar para restringir el tráfico de auditoría que atraviesa la red.

STEP 8 | Haga clic en **Commit (Confirmar)** para confirmar los cambios en el cortafuegos.

 ©2024 Palo Alto Networks, Inc.

Integración de VM-Series con WAN en la nube de AWS

AWS Cloud WAN es un servicio de redes de área extensa gestionadas (WAN) que le permite crear una red unificada que interconecta entornos de nube y locales. Proporciona un panel centralizado para conectar VPC locales, sucursales, centros de datos y Amazon a través de la red global de AWS e incluso otros proveedores de nube.

Implementar una WAN en la nube le permite emplear cortafuegos de nueva generación (NGFW) y sistemas de prevención de intrusión (IPS) para inspeccionar el tráfico de red como parte de una estrategia de defensa en profundidad. Esto a menudo se hace usando una VPC de seguridad separada y centralizada donde se configuran los dispositivos de seguridad y el tráfico se enruta hacia dentro y hacia fuera usando WAN en la nube. Tener un VPC de seguridad separado proporciona una manera simplificada y centralizada de gestionar la inspección de seguridad.

Cloud WAN ayuda con la conectividad dentro de AWS a través de AWS Network Manager, una interfaz que gestiona centralmente su red global. Una red global es una red privada única que actúa como contenedor a nivel de raíz para sus objetos de red y puede contener puertas de enlace de tránsito y una red central. La red central consiste en políticas de red, archivos adjuntos como VPC y tablas de rutas de puertas de enlace de tránsito.

Cloud WAN permite la asignación de VPC a segmentos y al punto de conexión regional para sus archivos adjuntos como se define en la política. Se pueden definir políticas para la redirección de tráfico entre segmentos iguales o diferentes para que un cortafuegos los inspeccione.

Puede utilizar los servicios WAN en la nube para:

- Implementar un VPC de seguridad detrás de GWLB en un segmento de seguridad y redirigir el tráfico que llega desde los archivos adjuntos de la nube a VPC, antes de reenviarlo al destino.
- Recopile logs y gestione actividades como el escalado automático, la recopilación de TAG, etc., en cortafuegos gestionados por Panorama.
- Filtrar e inspeccionar el tráfico hacia/desde Internet utilizando el tráfico norte-sur.
- Inspeccionar el tráfico para la comunicación entre VPC

AWS Cloud WAN se puede implementar utilizando dos métodos:

- **Federación de puertas de enlace de tránsito con WAN en la nube**: en este método se sustituyen las conexiones de pares de puertas de enlace de tránsito creadas estáticamente por WAN en la nube. Mientras federa las puertas de enlace de tránsito con WAN en la nube, tendrá que registrar las puertas de enlace de tránsito utilizando el Administrador de red de AWS y crear la interconexión entre las puertas de enlace de tránsito y crear archivos adjuntos a las puertas de enlace de tránsito y, a continuación, aplicar la configuración de WAN en la nube.
- **Solo WAN en la nube**: en este método WAN en la nube se utiliza para toda la conectividad y las puertas de enlace de tránsito se eliminan.

Consideraciones antes de implementar WAN en la nube de AWS:

- La conexión entre puertas de enlace de tránsito y WAN en la nube es compatible en la misma región y no entre regiones.
- WAN en la nube no admite la integración nativa con AWS Direct Connect.
- Para los casos de uso que requieren conexiones VPN de sitio a sitio de AWS a través de Direct Connect utilizando direcciones IP privadas, asegúrese de conectar WAN en la nube con una puerta de enlace de tránsito.

 ©2024 Palo Alto Networks, Inc.

- Mientras implementa WAN en la nube junto con las puertas de enlace de tránsito, asegúrese de que el ASN de la puerta de enlace de tránsito sea diferente del ASN utilizado para los bordes de la red central de WAN en la nube.
- Mientras crea la red central, asegúrese de añadir todas las regiones a las que están configuradas sus VPC en la sección Ubicaciones periféricas en la configuración de política de red central. También necesitará crear segmentos y añadir el tipo de segmento (Dev, Prod, Gestión o Seguridad) al que pertenecen estas regiones, bajo el nombre del segmento.

Casos de uso

Puede utilizar Cloud WAN para enrutar el tráfico entre:

- Las VPC en el mismo segmento y en la misma región (adjuntos aislados).
- Las VPC en diferentes segmentos de la misma región.
- Las VPC en el mismo segmento en diferentes regiones (adjuntos aislados).
- Las VPC en diferentes segmentos en diferentes regiones.

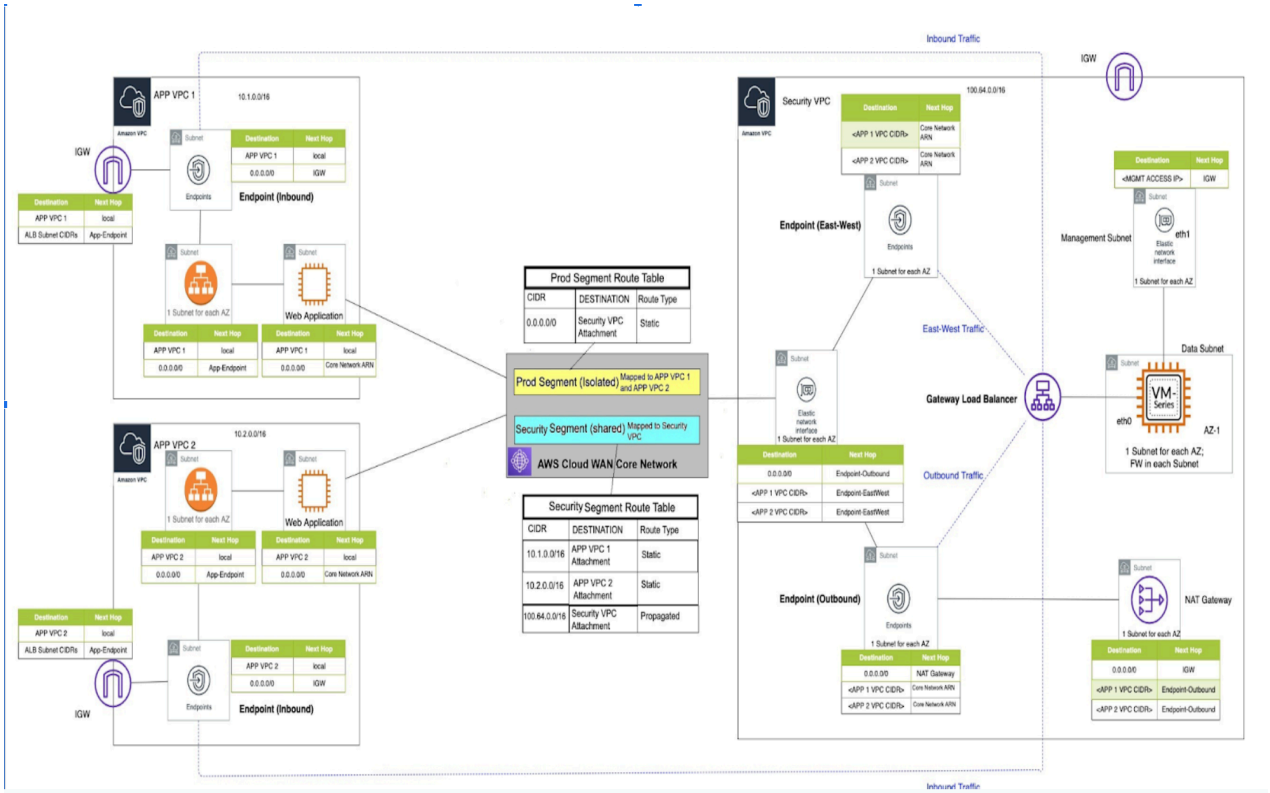
Implementar la WAN en la nube de AWS

Consideremos un caso de uso en el que las VPC están en el mismo segmento y en la misma región (adjuntos aislados). Para configurar esta configuración, implemente el cortafuegos VM-Series detrás de un GWLB similar a la Integración de VM-Series con un balanceador de carga Gateway de AWS. Puede implementar el cortafuegos VM-Series detrás del GWLB en un VPC de seguridad, que está directamente conectado a una WAN en la nube o a través de una pasarela de tránsito con un adjunto de WAN en la nube.

Para migrar completamente fuera de la puerta de enlace de tránsito, debe conectar sus VPC directamente a la WAN en la nube.

El tráfico de salida de la VPC de producción se enruta a la WAN en la nube, que luego se enruta a la VPC de seguridad para su inspección y se envía a través de la puerta de enlace NAT y la puerta de enlace interna. En la dirección inversa, el tráfico de la VPC de seguridad llega al segmento de seguridad y, a continuación, según la configuración de enrutamiento, se envía al archivo adjunto de la VPC.

 ©2024 Palo Alto Networks, Inc.

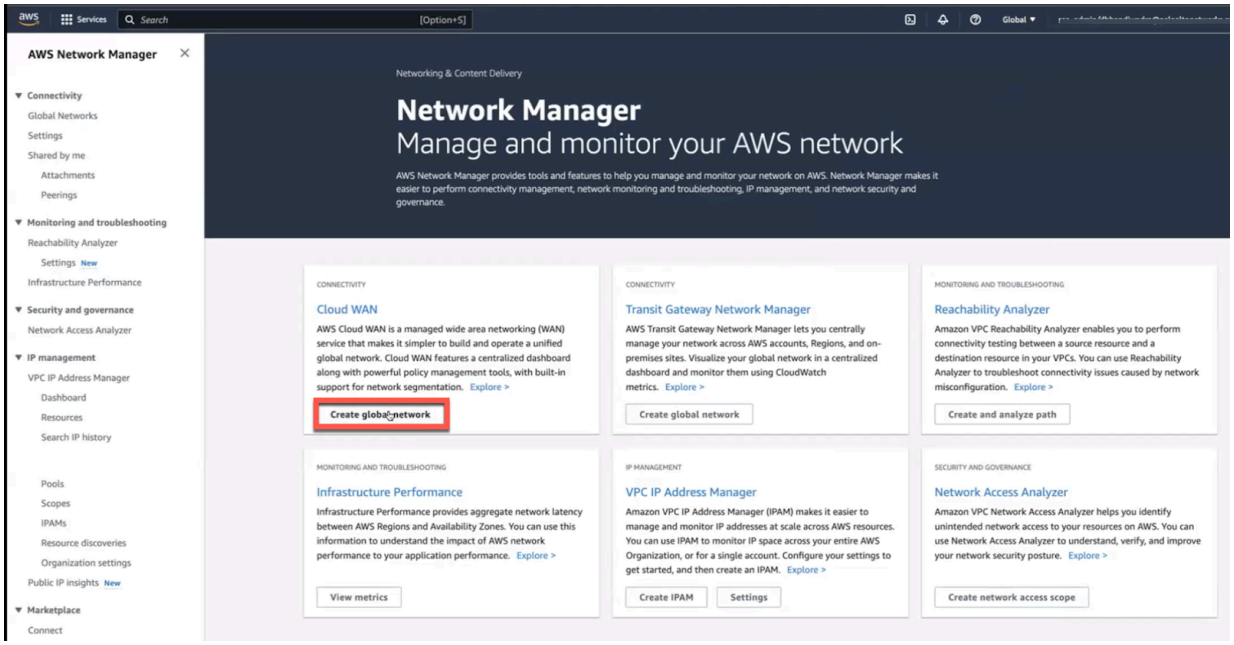


Para inspeccionar el tráfico entre las VPC en el mismo segmento y la misma región con implementación de **WAN en la nube de AWS (sólo)**, ejecute las siguientes tareas:

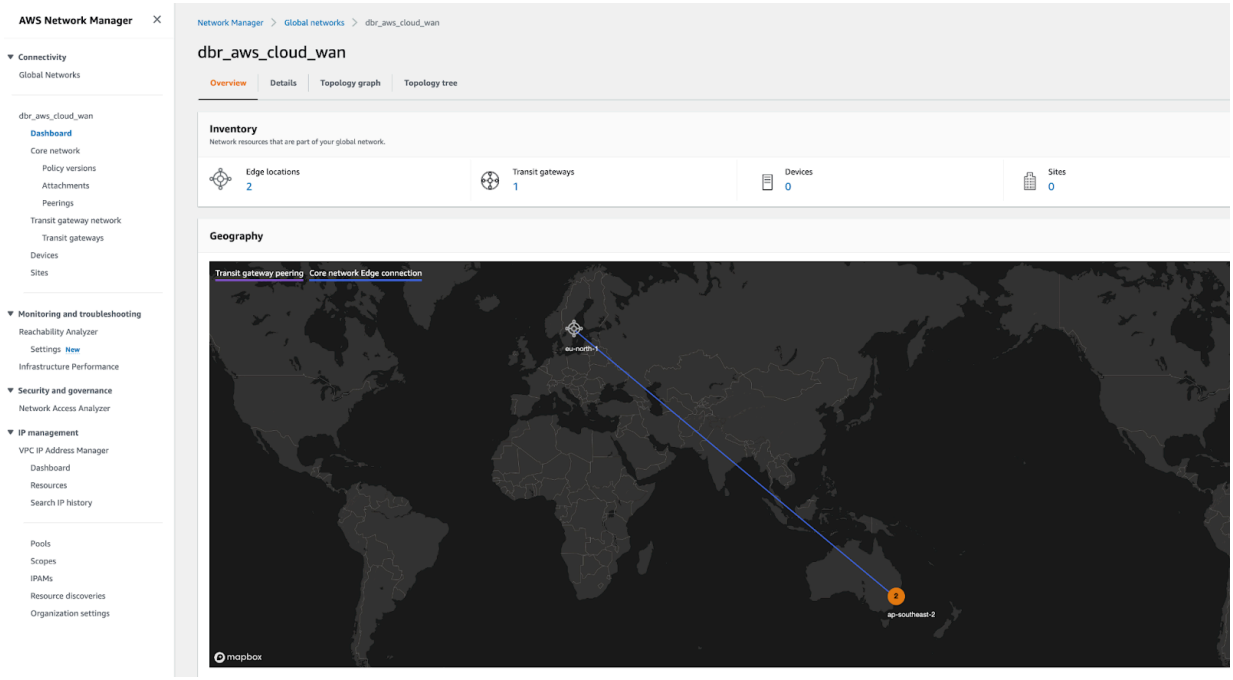
 ©2024 Palo Alto Networks, Inc.

1. Inicie sesión en AWS Network Manager y **Crear red global**.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.



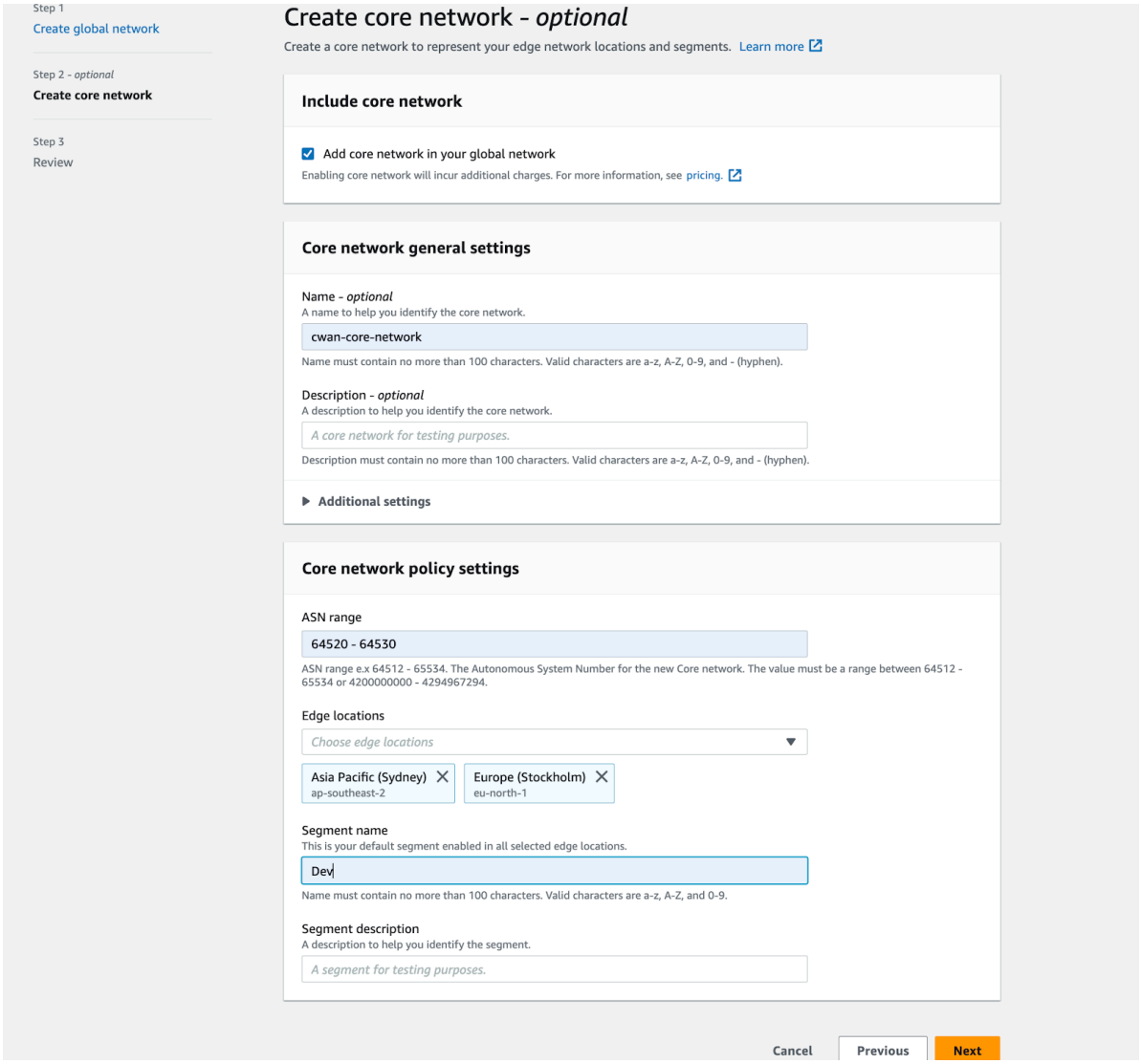
 ©2024 Palo Alto Networks, Inc.

2. Cree una red central y una política de red central.

   Utilice la consola WAN de nube de AWS para crear una versión de política de red central después de estas tareas:

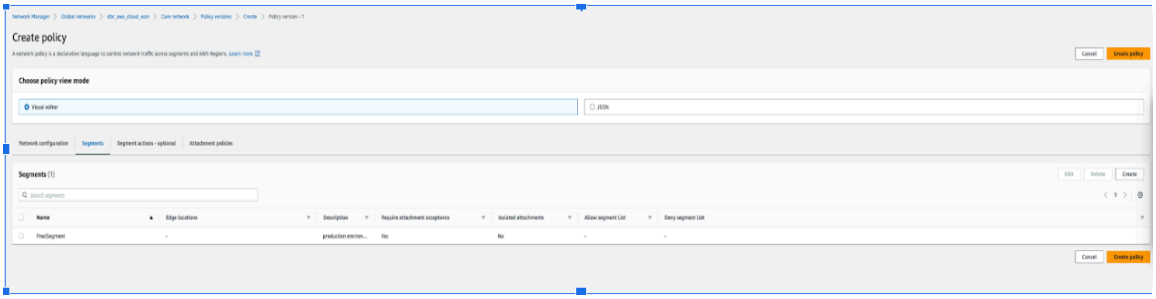
   - Configure los ajustes de red.

 ©2024 Palo Alto Networks, Inc.

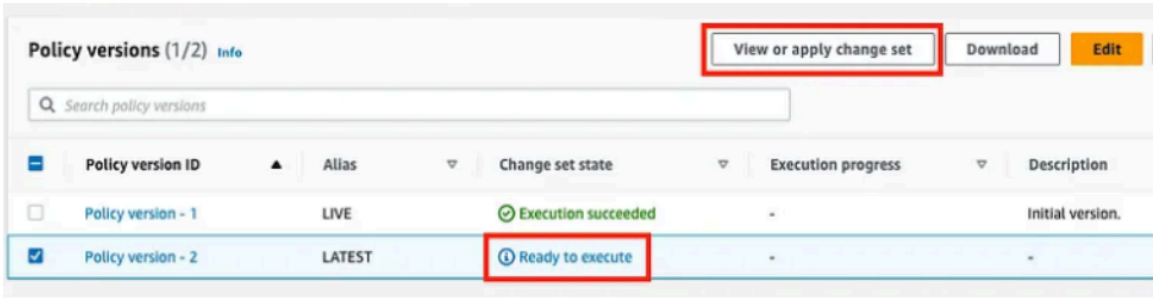


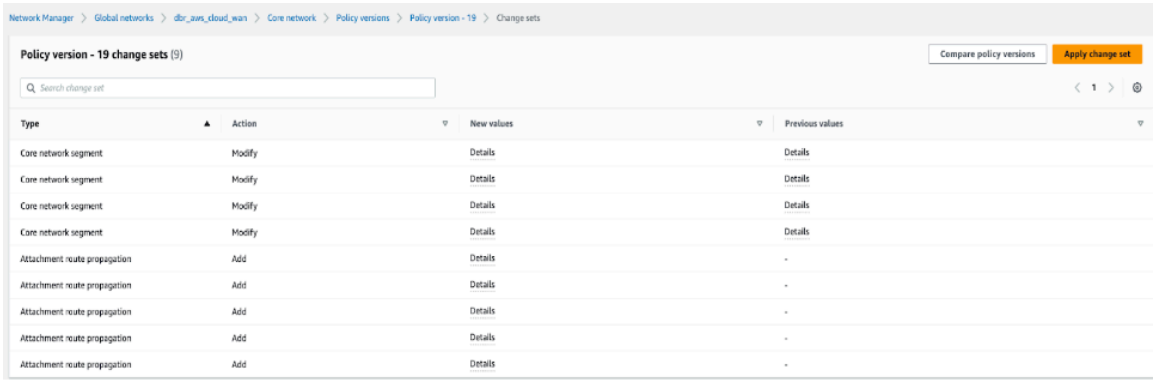
 ©2024 Palo Alto Networks, Inc.

- Para editar una versión de política, haga clic en **Versiones de política**, seleccione la política necesaria y haga clic en **Editar**. Haga los cambios necesarios y haga clic en **Crear política**.



- Después de que el estado del conjunto de cambios de la versión de política cambie a **Listo para ejecutar**, ejecute la política haciendo clic en **Ver o aplicar conjunto de cambios**. Alternativamente, haga clic en **Comparar versión de política** para ver el documento JSON.

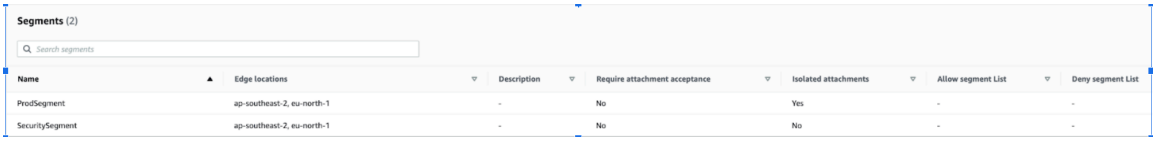




- • Cree segmentos de políticas de red dentro de su red central.

  Mientras configura las versiones de políticas, asegúrese de añadir las aplicaciones: APP VPC 1 (10.1.0.0/16) y APP VPC 2 (10.2.0.0/16) en el segmento Prod y el cortafuegos, y VPC de seguridad (100.64.0.0/16), en el segmento de seguridad.

©2024 Palo Alto Networks, Inc.

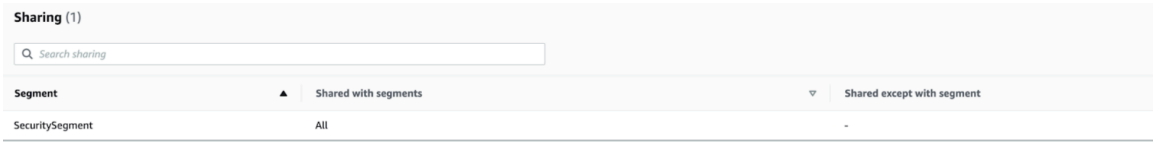


Segments (2)

Search segments

Name	Edge locations	Description	Require attachment acceptance	Isolated attachments	Allow segment List	Deny segment List
ProdSegment	ap-southeast-2, eu-north-1	-	No	Yes	-	-
SecuritySegment	ap-southeast-2, eu-north-1	-	No	No	-	-

- Cree acciones para compartir segmentos y rutas de segmentos.



Sharing (1)

Search sharing

Segment	Shared with segments	Shared except with segment
SecuritySegment	All	-

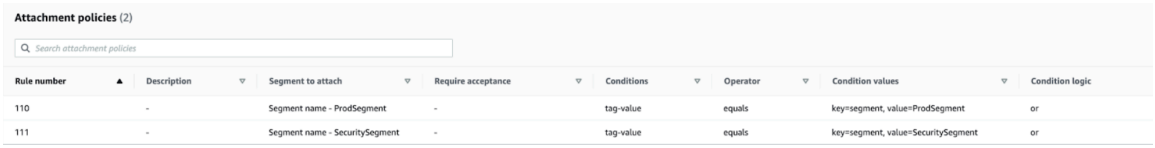


Routes (3)

Search routes

Segment	Destination CIDR block	Destination
ProdSegment	0.0.0.0/0	attachment-0853fd8b1c1a3ed87
SecuritySegment	10.1.0.0/16	attachment-04fd636bdaaf4f6e0
SecuritySegment	10.2.0.0/16	attachment-0ffa029e9effa9ba2

- Cree archivos adjuntos.



Attachment policies (2)

Search attachment policies

Rule number	Description	Segment to attach	Require acceptance	Conditions	Operator	Condition values	Condition logic
110	-	Segment name - ProdSegment	-	tag-value	equals	key=segment, value=ProdSegment	or
111	-	Segment name - SecuritySegment	-	tag-value	equals	key=segment, value=SecuritySegment	or

Puede seleccionar añadir etiquetas como Prod Segment (valor) al Segmento (clave). Estas etiquetas se reflejan solo después de agregar los segmentos en la WAN de nube.

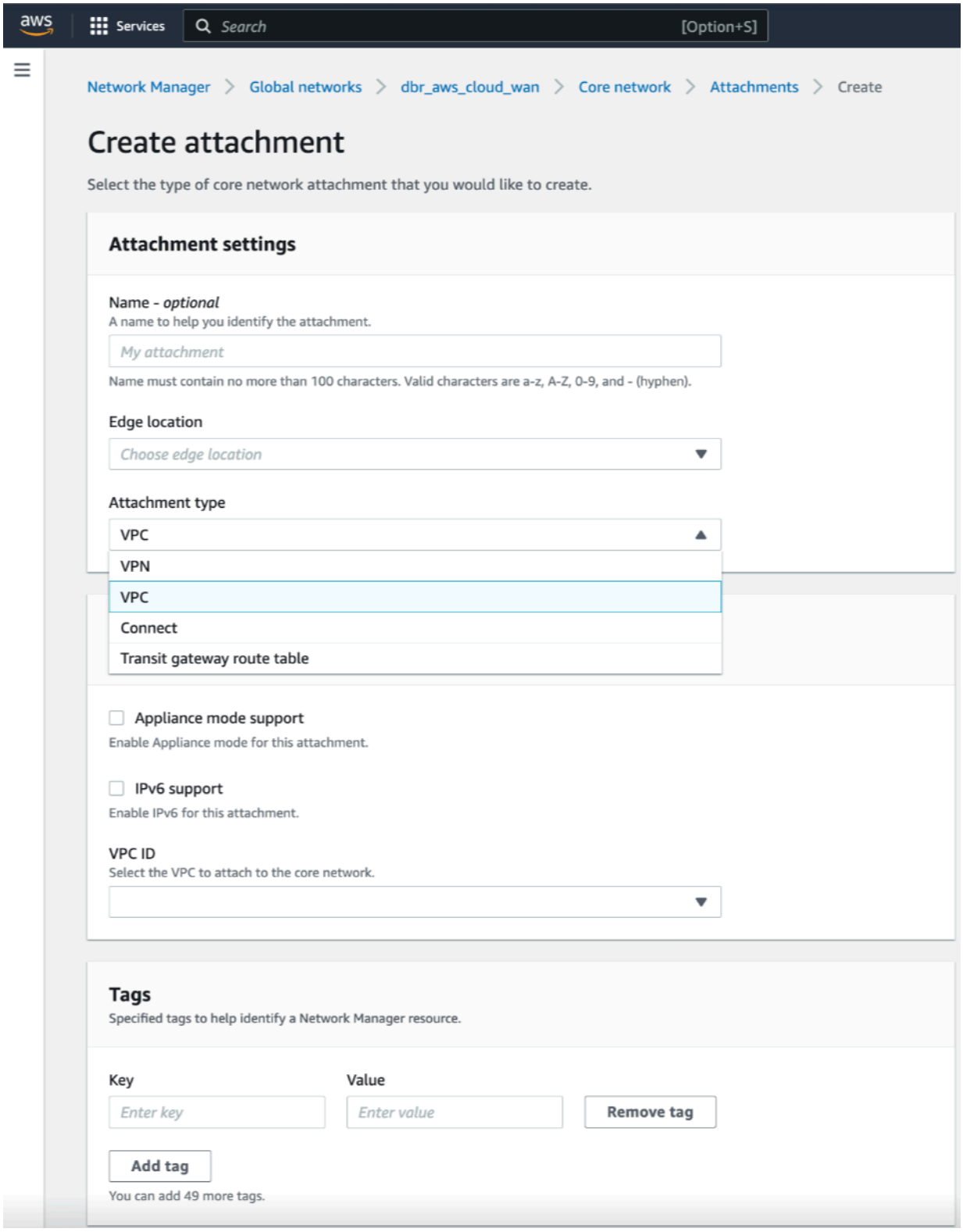
©2024 Palo Alto Networks, Inc.

3. Cree un archivo adjunto.



- *Utilice VPC o la tabla de rutas de puerta de enlace de tránsito como tipo de archivo adjunto mientras crea un archivo adjunto.*
- *Para asegurarse de que el cortafuegos VM-Series pueda inspeccionar el tráfico que se enruta entre los adjuntos de VPC, debe habilitar el modo de dispositivo en el adjunto de VPC para la VPC de seguridad que contiene el cortafuegos VM-Series.*

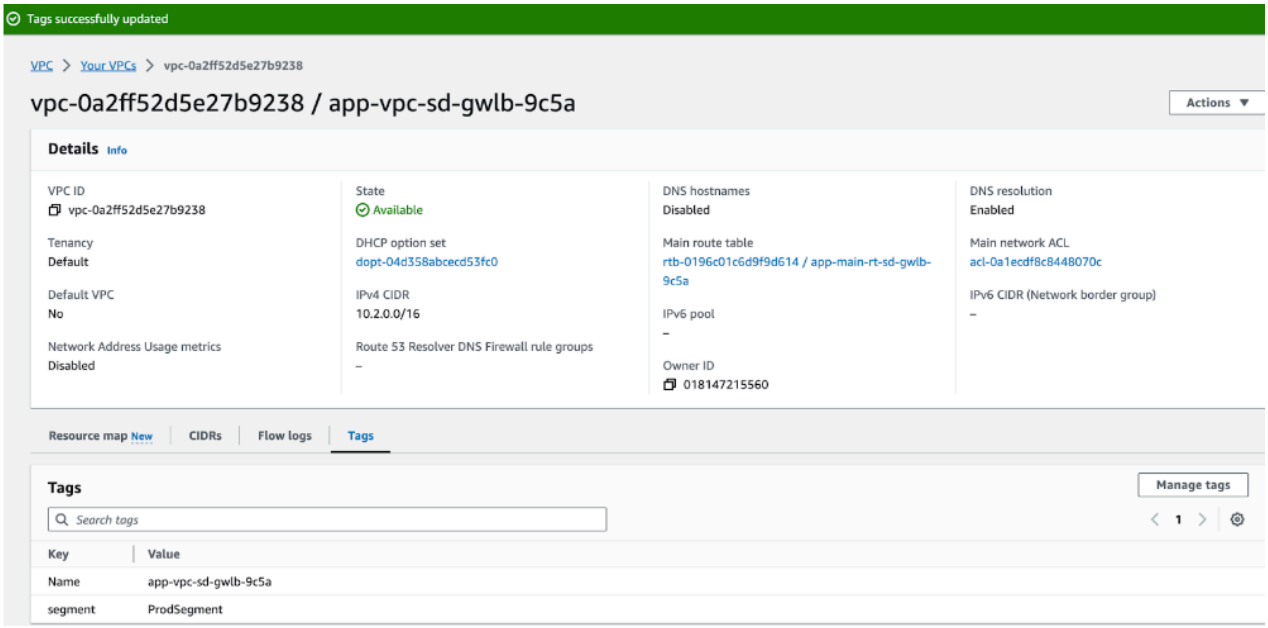
 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

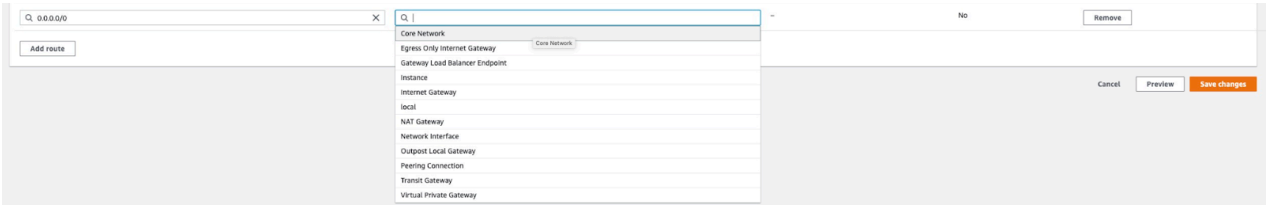
4. Actualizar tablas de rutas de las VPC.

   Ahora que las construcciones de WAN en la nube necesarias están en su lugar, las VPC deben ajustarse para facilitar el reenvío de paquetes hacia la red central. Las instancias de aplicación y cortafuegos o las respectivas VPC deben etiquetarse de manera similar a la del segmento. Añada etiquetas específicas al archivo adjunto para que coincida con el archivo adjunto creado durante laCreación de archivos adjuntos de políticas del paso 2.

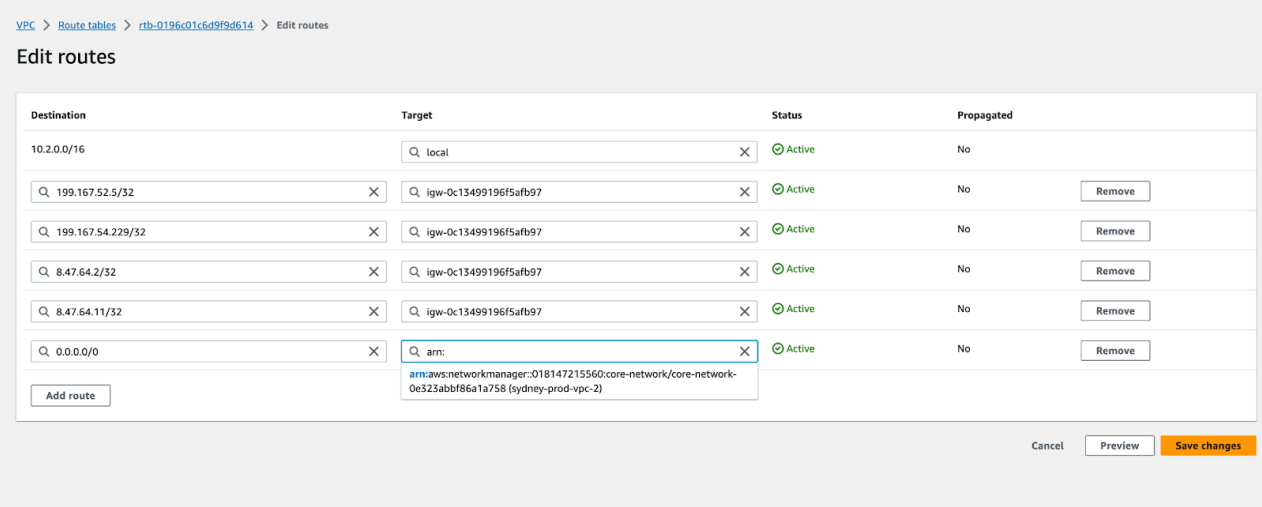


Para permitir la comunicación entre las VPC adjuntas y la red central, es necesario actualizar las tablas de rutas de las VPC desde la ruta de puerta de enlace de tránsito de destino existente hasta el ARN de la red central correspondiente, como se muestra a continuación.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

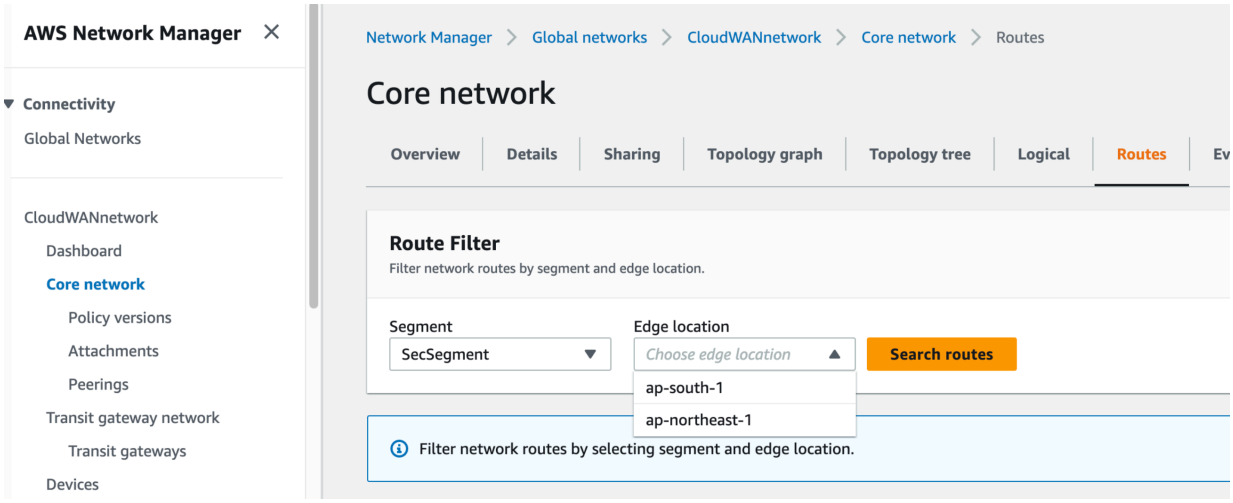
Guía de paquetes

Los siguientes pasos describen un recorrido de paquetes cuando una instancia EC2 en Application VPC 1 se comunica con una instancia EC2 en Application VPC 2:

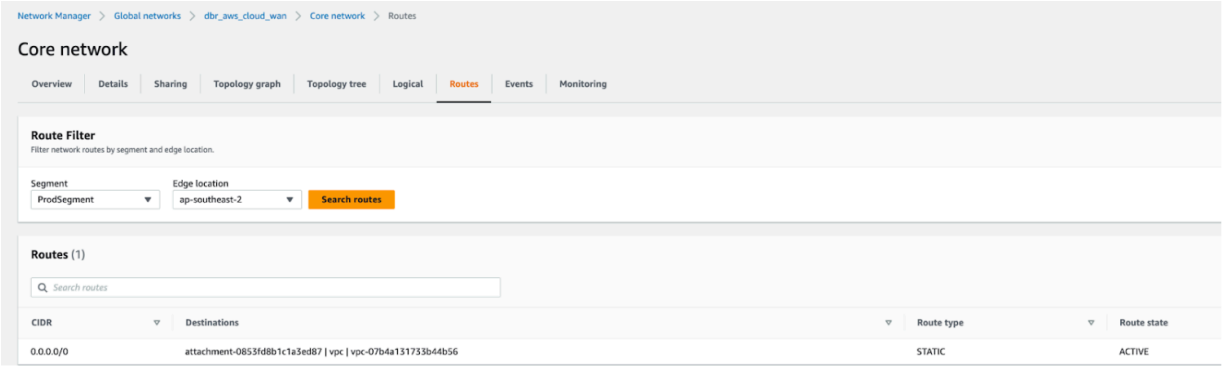
- Cuando un cliente en APP VPC 1(10.1.0.0/16) inicia una conexión a un servidor en APP VPC 2 (10.2.0.0/16), realiza una búsqueda en la tabla de rutas de VPC (App Subnet). El paquete empareja la entrada de ruta predeterminada con el ARN de la red central como destino y el paquete se enruta a la red central.

 ©2024 Palo Alto Networks, Inc.

- Cuando el paquete llega a la red central, realiza una búsqueda en la tabla de rutas del segmento Prod porque APP VPC 1 está asociada con el segmento Prod. El paquete empareja la entrada predeterminada con el adjunto de seguridad como destino y el paquete se enruta a la VPC de seguridad.



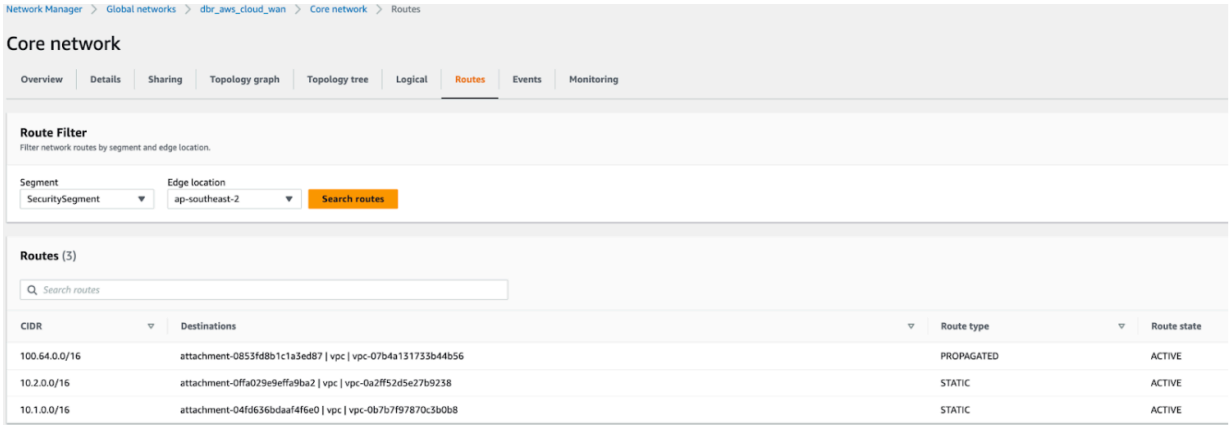
 ©2024 Palo Alto Networks, Inc.



- Cuando el paquete llega al adjunto de VPC de seguridad (100.64.0.0/16), realiza una búsqueda en la tabla de rutas VPC (CWAN Subnet). El paquete coincide con la ruta predeterminada con el endpoint 1 del cortafuegos como destino y el paquete se enruta a un cortafuegos, a través del endpoint del cortafuegos, para su inspección.
- El cortafuegos inspecciona el tráfico, lo compara con su política de seguridad y lo permite pasar. El cortafuegos enruta el paquete de vuelta al endpoint del cortafuegos, donde realiza una consulta en la tabla de rutas VPC (subred de cortafuegos). El paquete empareja la entrada de ruta predeterminada con el ARN de la red central como destino y el paquete se enruta a la red central.
- Cuando el paquete llega a la red central, realiza una búsqueda en la tabla de rutas de seguridad compartida porque la VPC de seguridad está asociada con el segmento de seguridad. El paquete

 ©2024 Palo Alto Networks, Inc.

empareja la entrada APP VPC 2 CIDR(10.2.0.0/16) con el adjunto APP VPC 2 como el destino y el paquete se enruta a APP VPC 2.



- Cuando el paquete llega a APP VPC 2, realiza una búsqueda en la tabla de rutas VPC (CWAN Subnet). El paquete empareja la entrada VPC CIDR con local como destino y el paquete se enruta a Instancia.

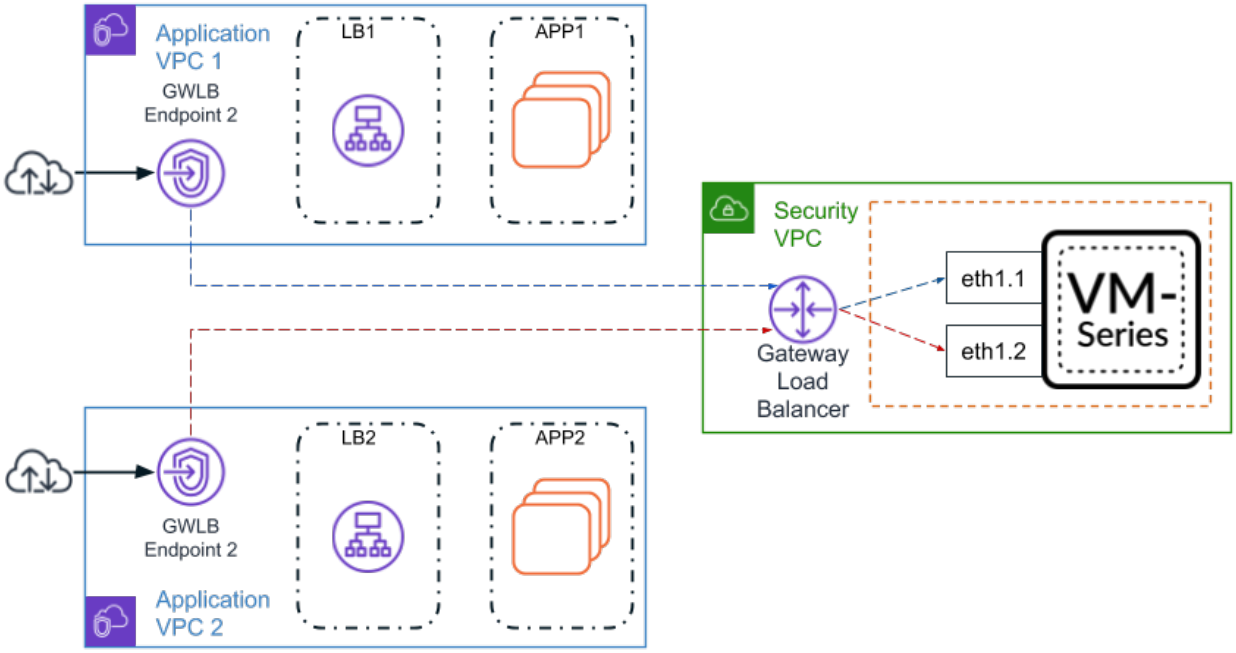
El tráfico de retorno traza la misma ruta en la dirección opuesta.

Asociar un endpoint VPC con una interfaz de VM-Series

Puede asociar uno o más endpoints de VPC con una interfaz o subinterfaz del cortafuegos VM-Series. Puede proporcionar una aplicación de políticas coherente asociando todos los endpoints en una única VPC a la misma subinterfaz en el cortafuegos. O, si su implementación tiene VPC con direcciones IP superpuestas, puede asociar endpoints en diferentes VPC con diferentes subinterfaces para la aplicación de políticas diferenciadas.

No es obligatorio asociar una VPC a una interfaz o subinterfaz para integrar el cortafuegos VM-Series con una GWLB.

 ©2024 Palo Alto Networks, Inc.



Puede configurar interfaces y asociar una VPC con interfaces de cortafuegos mediante los siguientes métodos:

- Incluya la configuración de la interfaz en su archivo `bootstrap.xml` y los comandos de asociación como parte del archivo `init-cfg.txt` o datos de usuario de AWS.
- Después de implementar el cortafuegos, configure manualmente sus interfaces y use la CLI del cortafuegos para asociar sus VPC con interfaces.

Puede asociar varios endpoints de VPC a una única interfaz en el cortafuegos VM-Series. Sin embargo, debe asociar cada endpoint de VPC de forma individual. Por ejemplo, para asociar el endpoint 1 de la VPC y el endpoint 2 de la VPC con la subinterfaz ethernet1/1.2, debe ejecutar el comando de asociación por separado para cada endpoint de la VPC.

La siguiente tabla describe los comandos utilizados para asociar una VPC con una interfaz. Puede incluir el comando de operación en su archivo `init-cfg.txt` o en los datos de usuario de AWS.

Parámetro de arranque	Comando de la CLI	Description (Descripción)
plugin-op-commands= aws-gwlb-associate-vpce:<vpce-id>@ethernet<subinterface>	request plugins vm_series aws gwlb associate vpc-endpoint <vpce-id> interface <subinterface>	Asocia un endpoint de VPC con una interfaz o subinterfaz en el cortafuegos. La interfaz especificada se asigna a una zona de seguridad.
—	request plugins vm_series aws gwlb disassociate vpc-endpoint <vpce-id> interface <subinterface>	Desasocia un endpoint de VPC con una interfaz o subinterfaz en el cortafuegos. La interfaz especificada se asigna a una zona de seguridad.

 ©2024 Palo Alto Networks, Inc.

Parámetro de arranque	Comando de la CLI	Description (Descripción)
—	show plugins vm_series aws gwlb	Muestra el estado operativo del cortafuegos en relación con su implementación GWLB. No muestra la configuración del cortafuegos. Por ejemplo, si configura una asociación a una interfaz que no existe, esa asociación se configura pero no forma parte del estado operativo. Por lo tanto, no se muestra.

Al asociar un endpoint de VPC mediante el archivo bootstrapping init-cfg.txt o la fecha de usuario de AWS, puede enumerar varias interfaces o subinterfaces juntas. Todos los comandos deben estar en una sola línea en una lista separada por comas sin espacios, como se muestra en el siguiente ejemplo.

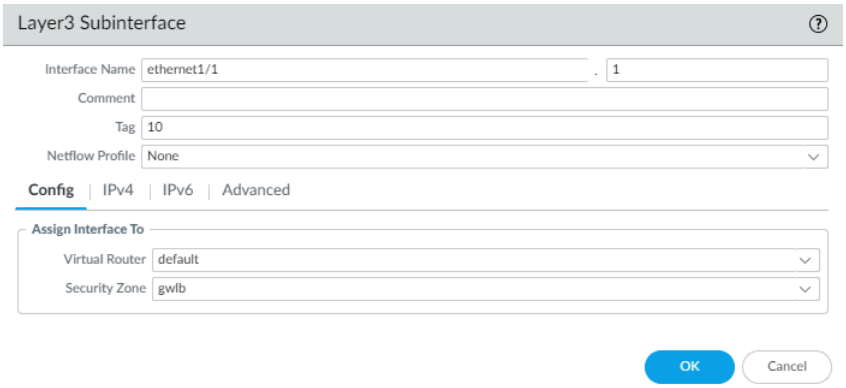
```
plugin-op-commands=aws-gwlb-inspect:enable,aws-gwlb-associate-
vpce:vpce-0913731043b5c0ebc@ethernet1/1.1,aws-gwlb-associate-
vpce:vpce-08207ccb4cb23a1de@ethernet1/1.1,aws-gwlb-associate-
vpce:vpce-07b66cca88821d6e1@ethernet1/1.2,aws-gwlb-associate-
vpce:vpce-0a9a583fdb928492b@ethernet1/1.3
```

Si utiliza subinterfaces para separar el tráfico, cree una subinterfaz para cada VPC y asóciela a una VPC.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Configure la subinterfaz.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Seleccione **Network (Red)** > **Interface (Interfaz)**.
3. Resalte **ethernet1/1** y haga clic en **Add Subinterface (Añadir subinterfaz)**.
4. Introduzca un sufijo numérico (1 a 9999) para identificar la subinterfaz.
5. Introduzca una **VLAN Tag (etiqueta VLAN)** (de 1 a 4094) para la subinterfaz. Este campo es obligatorio pero no se utiliza la VLAN.
6. Seleccione **Virtual Router (Enrutador virtual)** como predeterminado.
7. Seleccione una **Security Zone (Zona de seguridad)**.
8. En la pestaña **IPv4**, fije el **Type (Tipo)** en **DHCP Client (Cliente DHCP)**.
9. Haga clic en **OK (Aceptar)**.
10. Repita este comando para cada endpoint de la nube privada virtual (VPC).



STEP 2 | Asocie la interfaz con un endpoint de VPC.

1. Inicie sesión en la CLI del cortafuegos.
2. Ejecute el siguiente comando:

   request plugins vm_series aws gwlb associate vpc-endpoint <vpce-id> interface <subinterface>

   Por ejemplo:

   request plugins vm_series aws gwlb associate vpc-endpoint vpce-02c4e6g8ha97h7e39 interface ethernet1/1.4

   Puede encontrar el ID del endpoint de la VPC en la consola de AWS.

3. Repita este comando para cada interfaz y asociación de endpoint de VPC.

STEP 3 | Verifique su interfaz a las asociaciones de endpoints de VPC.

show plugins vm_series aws gwlb

```
GWLB habilitado: Enrutamiento de superposición real: False
 ------------------------------------------------------------ VPC
 endpoint Interface
```

 ©2024 Palo Alto Networks, Inc.

```
-------------------------------------------------------------
vpce-0aeb1a919bd4ae609 ethernet1/1.1 vpce-0294375bfe413f04a
ethernet1/1.2
```

STEP 4 | Si es necesario, puede utilizar el siguiente comando para desvincular un endpoint de VPC de una interfaz.

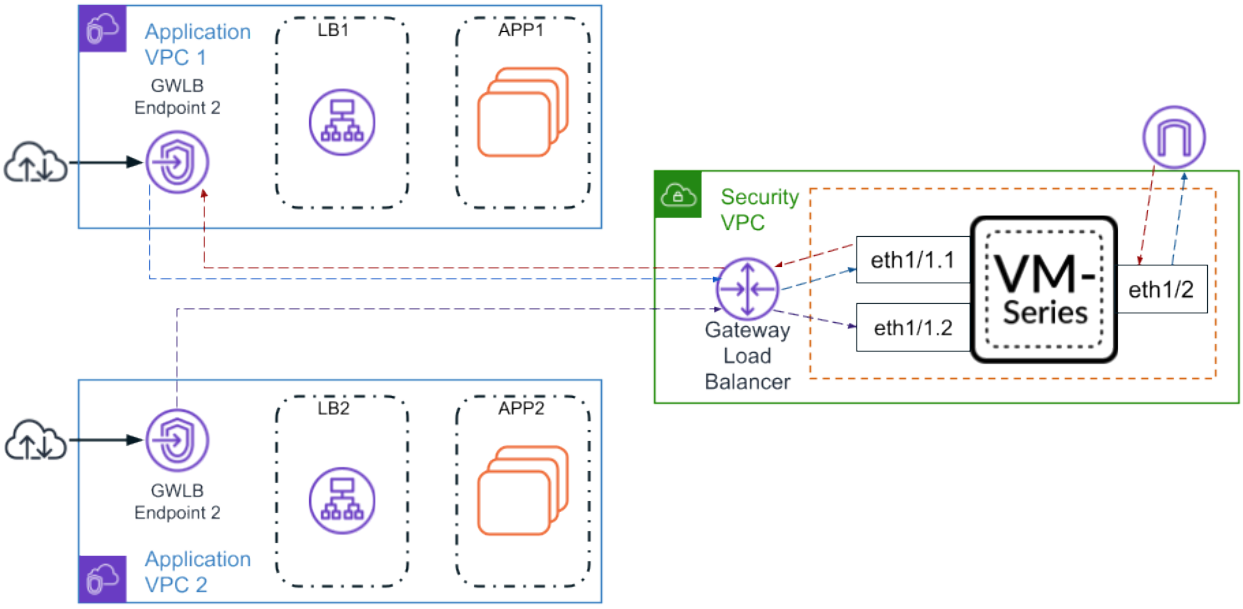
request plugins vm_series aws gwlb disassociate vpc-endpoint <vpce-id> interface <subinterface>

Habilitar el enrutamiento de superposición para la VM-Series en AWS

El enrutamiento excesivo requiere PAN-OS 10.0.5 o posterior.

Mediante el uso del enrutamiento por superposición en la integración del cortafuegos VM-Series, AWS GWLB le permite utilizar la política de dos zonas para inspeccionar el tráfico que sale (salida) de su entorno de AWS. Esto permite que los paquetes salgan del cortafuegos VM-Series a través de una interfaz diferente a la que ingresaron.

Cuando se configura el enrutamiento de superposición, el cortafuegos VM-Series puede realizar una búsqueda de ruta de capa 3 en el encabezado interno de un paquete. Si el destino es el mismo que la interfaz de entrada, el paquete se dirigirá normalmente. Todos los paquetes futuros en la sesión se tratan como vwire; como si el enrutamiento de superposición no estuviese habilitado. Si el paquete va a un destino saliente, el cortafuegos VM-Series desencapsula el paquete y lo reenvía a la puerta de enlace IGW o NAT. Cuando el paquete regresa, el cortafuegos VM-Series vuelve a aplicar la encapsulación.



Utilice el siguiente procedimiento para habilitar el enrutamiento de superposición.

STEP 1 | Antes de comenzar, asegúrese de crear diferentes subredes para las interfaces trust y untrust.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Integre manualmente VM-Series con un balanceador de carga Gateway.

STEP 3 | (Opcional) Asociar un endpoint VPC con una interfaz de VM-Series.

STEP 4 | Utilice el comando CLI de enrutamiento de superposición. Este comando de la CLI no es necesario si ha incluido el comando de operación de enrutamiento de superposición en los datos de usuario de AWS o en el archivo de arranque init-cfg.txt.

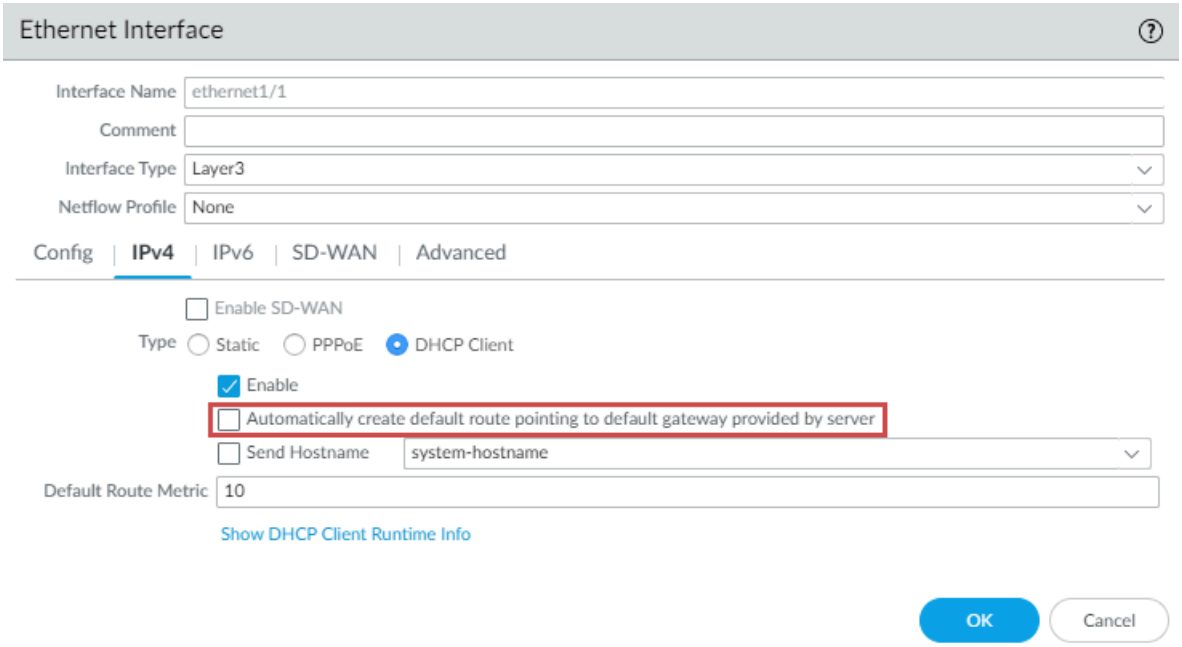
1. Inicie sesión en la interfaz de línea de comandos del cortafuegos VM-Series.
2. Ejecute el siguiente comando.

```
request plugins vm_series aws gwlb overlay-routing enable yes
```

STEP 5 | Inicie sesión en la interfaz web del cortafuegos.

STEP 6 | Deshabilitar **Automatically create default route pointing to default gateway provided by server (Crear automáticamente ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor)** en la interfaz de confianza trust (entrada).

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet**.
2. Haga clic en su interfaz trust y luego en la pestaña IPv4.
3. Anule la selección en **Automatically create default route pointing to default gateway provided by server (Crear automáticamente ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor)**.
4. Haga clic en OK (Aceptar).



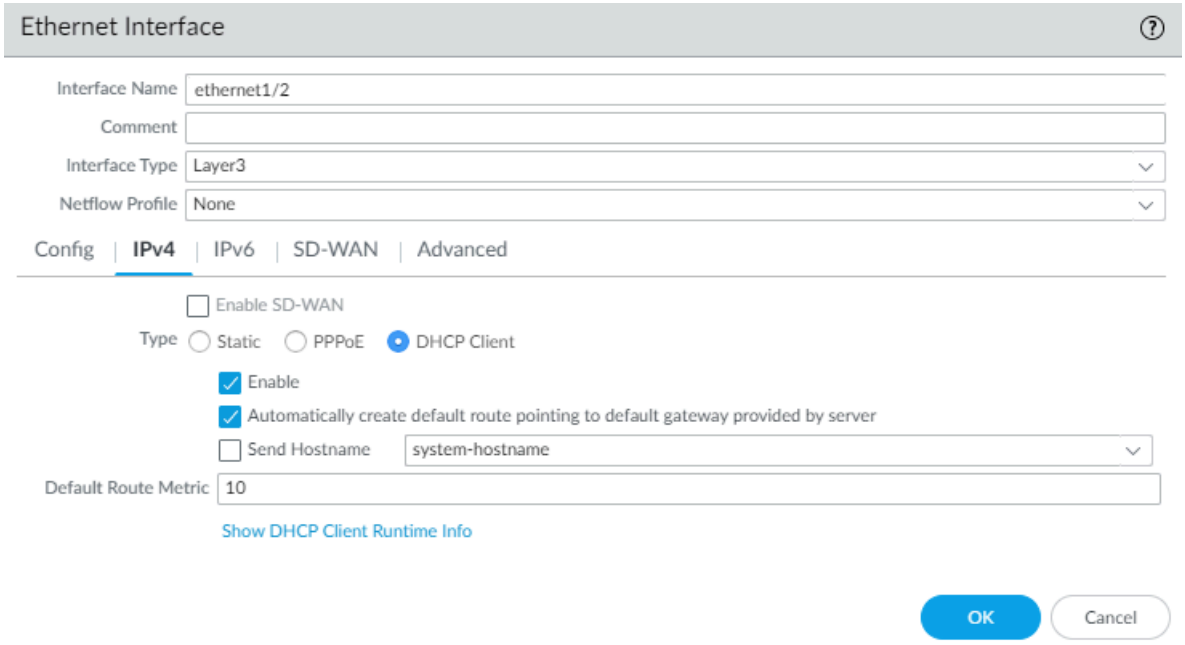
STEP 7 | Configure la interfaz Ethernet 1/2.

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet**.
2. Seleccione **Interface Type (Tipo de interfaz)—Layer3 (Capa 3)**.
3. En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. Esta zona actuará como su zona de

 ©2024 Palo Alto Networks, Inc.

desconfianza untrust y dirigirá el tráfico saliente fuera de su VPC de seguridad. Defina la nueva zona, como VM-Series-untrust y, a continuación, haga clic en **OK (Aceptar)**.

4. En la pestaña **IPv4**, seleccione **DHCP Client (Cliente DHCP)**.
5. Seleccione **Automatically create default route pointing to default gateway provided by server (Crear automáticamente ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor)**.
6. Haga clic en **OK (Aceptar)**.



STEP 8 | Configurar un router virtual.

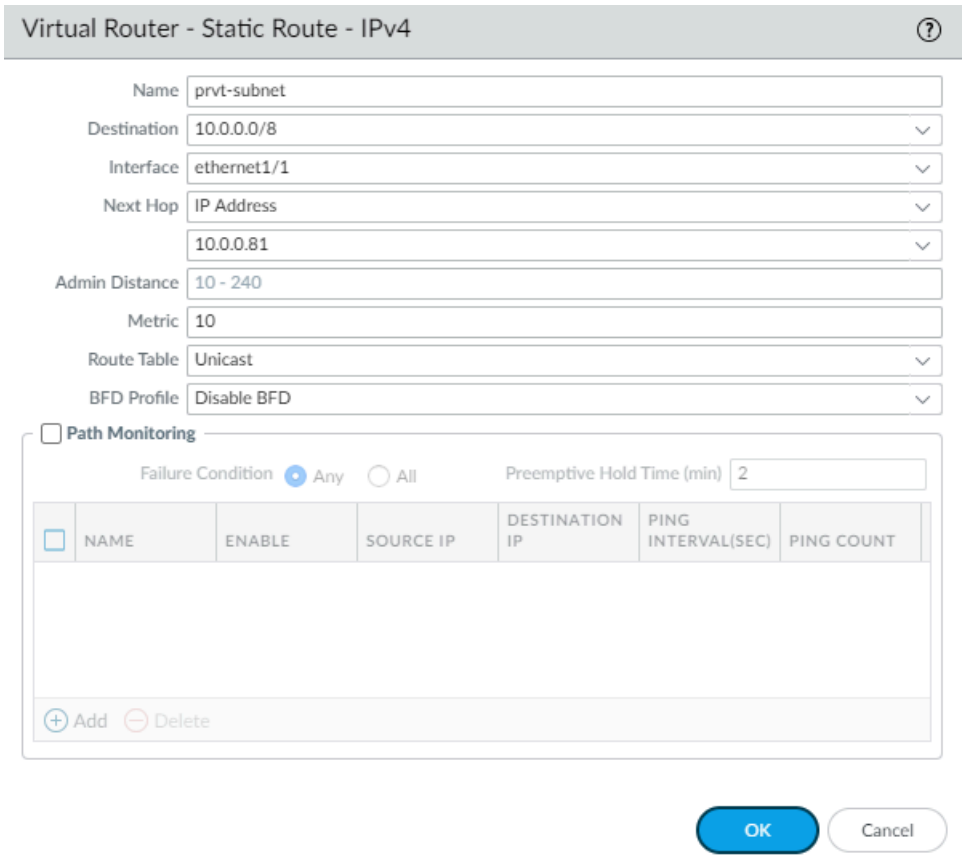
1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** > **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** descriptivo para el sistema virtual.
3. En **Interfaces,**, seleccione **Add (Añadir)** Ethernet1/1, cualquier subinterfaces bajo Ethernet1/1 y Ethernet1/2.
4. Haga clic en **Static Routes (Rutas estáticas)** > **Add (Añadir)**.
   1. Introduzca un nombre descriptivo para la ruta estática.
   2. Como el **Destination (Destino)**, introduzca la dirección IP privada de la subred de la VPC de la aplicación.
   3. Seleccione la interfaz trust (entrada) en el menú desplegable **Interface (Interfaz)**.
   4. En **Next Hop (Siguiente salto)**, seleccione Dirección IP e introduzca la dirección IP de la puerta de enlace de la interfaz trust. Puede encontrar la dirección IP de la puerta de enlace

 ©2024 Palo Alto Networks, Inc.

en **Network (Red)** > **Interfaces** > **Ethernet** > **Dynamic-DHCP Client (Cliente DHCP dinámico)**.



5. Haga clic en **OK (Aceptar)**.



5. Asegúrese de que las rutas estáticas puedan llegar a todas las VPC de aplicaciones de la implementación. Puede realizar algunas rutas agregadas grandes (que cubran todos los RFC1918) o rutas específicas de la VPC de la aplicación. Si utiliza subinterfaces, no es necesario

 ©2024 Palo Alto Networks, Inc.

enrutar de nuevo a la subinterfaz. La comprobación de salida solo busca la interfaz coincidente en lugar de la subinterface correspondiente.

6. Haga clic en **OK (Aceptar)**.

STEP 9 | Cree una directiva NAT para la salida de tráfico Ethernet1/2.

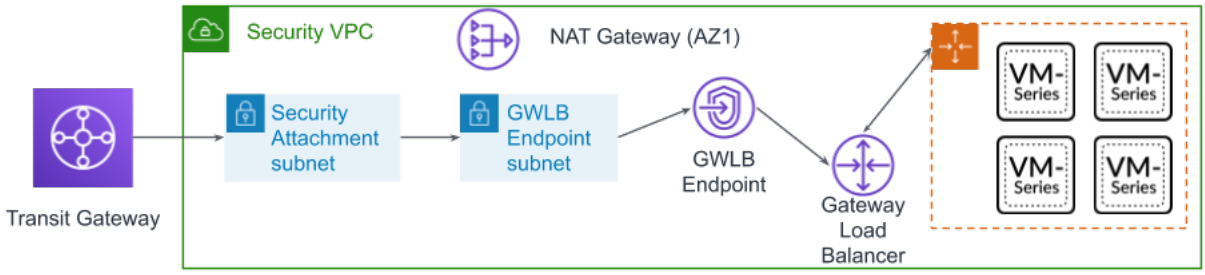
1. Seleccione **Policies (Políticas)** > **NAT** > **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** descriptivo para la regla de política NAT.
3. Seleccione **ipv4** en el menú desplegable **NAT Type (Tipo de NAT)**.
4. En la pestaña **Original Packet (Paquete original)**, establezca la **Source Zone (Zona de origen)** en cualquiera y la **Destination Zone (Zona de destino)** en la zona untrust (salida).
5. En la pestaña **Translated Packet (Paquete traducido)**, establezca los siguientes parámetros.
   - Tipo de traducción: Dynamic IP and Port
   - Address Type: Interface Address
   - Interfaz: Seleccione su puerto de desconfianza untrust (salida) en el menú desplegable.
   - IP address: ninguno
6. Haga clic en **OK (Aceptar)**.

STEP 10 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

Grupo de escalado automático de VM-Series con el balanceador de carga Gateway de AWS

La plantilla de escalado automático de Palo Alto Networks para AWS le ayuda a integrar y configurar el cortafuegos VM-Series con un GWLB para proteger las aplicaciones implementadas en AWS. La plantilla aprovecha las características de escalabilidad de AWS para incrementar de forma independiente y automática los cortafuegos VM-Series implementados en AWS para satisfacer los incrementos en la demanda de recursos de carga de trabajo de las aplicaciones.

*Estas plantillas son **compatibles con la comunidad**.*



Esta solución proporciona una plantilla de VPC de seguridad y una plantilla de aplicación. La plantilla de VPC de seguridad implementa el grupo de escalado automático de cortafuegos VM-series, una subred GWLBE, GWLBE, GWLB, una subred de datos adjuntos de seguridad y una puerta de enlace NAT para cada zona de disponibilidad. Descargue las plantillas de CloudFormation del Repositorio de GitHub de Palo Alto Networks.

 ©2024 Palo Alto Networks, Inc.

La plantilla de escalado automático de VM-Series para la integración con GWLB de AWS incluye los siguientes componentes básicos:

Componente	Description (Descripción)
Componentes PAN	• Panorama 10.0.2 o posterior • PAN-OS 10.0.2 o posterior • Complemento de VM-Series 2.0.2 o posterior instalado en Panorama
Plantilla de cortafuegos (Plantilla compatible con la comunidad)	Según el número de zonas de disponibilidad (AZ) que elija, la plantilla `firewall-new-vpc-v3.0.template` implementará lo siguiente: *La plantilla admite un máximo de cuatro AZ.* • Subredes para la gestión Lambda, adjuntos de puerta de enlace de tránsito, endpoints GWLB y puertas de enlace NAT, así como subredes de confianza. • Tablas de enrutamiento para cada subred • Adjuntos de puerta de enlace de tránsito y tablas de enrutamiento • Puertas de enlace de internet y NAT • Un grupo de escalado automático con un cortafuegos VM-Series por AZ. • Un GWLB y un endpoint de GWLB en cada AZ. El CIDR de VPC para la plantilla de cortafuegos debe ser superior a /23. Debido a las muchas variaciones en un entorno de producción que incluye, entre otros, un número específico de componentes, como subredes, zonas de disponibilidad, tablas de enrutamiento y grupos de seguridad. Debe implementar `firewall-new-vpc-v3.0.template` en una nueva VPC. *La plantilla de escalado automático de VM-Series para AWS no implementa una puerta de enlace de tránsito o Panorama. Debe implementar una puerta de enlace de tránsito y Panorama antes de iniciar firewall-new-vpc-v3.0.template.*
Plantilla de aplicación (Plantilla compatible con la comunidad)	Según el número de zonas de disponibilidad (AZ) que seleccione, la plantilla `panw-aws-app-v3.0.` implementa lo siguiente: *La plantilla admite un máximo de cuatro AZ.* • Subredes para Lambda, adjuntos de puerta de enlace de tránsito, endpoints de GWLB, balanceadores de carga de aplicaciones. • Tablas de enrutamiento para cada subred, así como una tabla de enrutamiento de entrada asociada con la puerta de enlace de internet para dirigir el tráfico de entrada al endpoint de GWLB.

 ©2024 Palo Alto Networks, Inc.

Componente	Description (Descripción)
	• Un balanceador de carga de aplicación • Una puerta de enlace de internet • Un grupo de escalado automático con una instancia de Ubuntu por zona de disponibilidad. El CIDR de VPC para la plantilla de aplicación debe ser superior a /23. *La plantilla de la aplicación está destinada a utilizarse como ejemplo para validar la plantilla de seguridad.*
Funciones Lambda	AWS Lambda proporciona una automatización sólida basada en eventos sin la necesidad de un software de orquestación complejo. Además de implementar los componentes descritos en las filas anteriores, `firewall-new-vpc-v3.0.template` realiza las siguientes funciones: • Añade o elimina una interfaz (ENI) cuando se inicia o desactiva un cortafuegos. • Elimina todos los recursos asociados cuando usted elimina una pila o finaliza una instancia. • Elimina un cortafuegos como dispositivo gestionado de Panorama cuando se produce un evento de escalado horizontal. • Desactiva la licencia cuando un evento de escalado horizontal resulta en la desactivación de un cortafuegos. • Supervisa la puerta de enlace de tránsito periódicamente para detectar nuevos datos adjuntos o separados, y actualiza las tablas de enrutamiento según corresponda en la VPC de seguridad.
Archivos Bootstrap El archivo bootstrap.xml proporcionado en el repositorio de GitHub se proporciona solo para pruebas y evaluaciones. Para una implementación de producción, debe modificar las credenciales de muestra en bootstrap.xml	Esta solución requiere el archivo init-cfg.txt y el archivo bootstrap.xml para que el cortafuegos VM-Series tenga la configuración básica para gestionar el tráfico. • El archivo `init-cfg.txt` incluye el comando operacional mgmt-interface-swap para permitir que el cortafuegos reciba tráfico del plano de datos en su interfaz principal (eth0). Esta solución de escalado automático requiere el intercambio del plano de datos y las interfaces de gestión para permitir que el GWLB reenvíe el tráfico web al nivel de escalado automático de los cortafuegos VM-Series. • El archivo `bootstrap.xml` habilita la conectividad básica para las interfaces de red del cortafuegos y permite que el cortafuegos se conecte al espacio de nombres del AWS CloudWatch que coincida con el nombre de pila que introduzca al iniciar la plantilla.

 ©2024 Palo Alto Networks, Inc.

Componente	Description (Descripción)
antes de su inicio.	

Si necesita eliminar estas plantillas de AWS, siempre elimine primero la plantilla de la aplicación. Si intenta eliminar la plantilla de cortafuegos, la eliminación fallará.

- Antes de iniciar las plantillas
- Inicio de la plantilla del cortafuegos
- Inicio de la plantilla de la aplicación

Antes de iniciar las plantillas

Antes de iniciar las plantillas para integrar un grupo de escalado automático de cortafuegos VM-Series con un GWLB de AWS, debe completar el siguiente procedimiento.

STEP 1 | Asegúrese de tener lo siguiente antes de comenzar.

- Obtenga el código de autenticación para un paquete que admita el número de cortafuegos que pueden ser necesarios para su implementación. Debe guardar este código de autenticación en un archivo de texto llamado `authcodes` (sin extensiones), y poner el archivo `authcodes` en la carpeta `/licencia` del paquete de arranque.
- Descargue los archivos necesarios para iniciar la plantilla del Balanceador de carga de puerta de enlace de MV-Series del repositorio GitHub.
- Cree una puerta de enlace de tránsito. Esta puerta de enlace de tránsito conecta sus VPC de seguridad y aplicaciones.
  - Tome nota del ID de la puerta de enlace de tránsito; lo necesitará más adelante cuando implemente la plantilla.
  - Debe añadir una ruta 0.0.0.0/0 a la tabla de enrutamiento del adjunto de la aplicación que apunta al adjunto de seguridad para proteger el tráfico este-oeste y de salida.
  - Asegúrese de que **Default route table association (Asociación de tabla de ruta predeterminada)** y **Default route table propagation (Propagación de tabla de ruta predeterminada)** estén deshabilitadas.
- El enrutamiento entre dominios sin clases (CIDR) de VPC recomendado para el cortafuegos y las plantillas de aplicaciones debe ser superior a /23.

El grupo de destino de la puerta de enlace GWLB no puede utilizar HTTP para las comprobaciones de estado porque el cortafuegos VM-Series no permite el acceso con un protocolo no seguro. En su lugar, utilice HTTPS o TCP.

STEP 2 | Implemente Panorama 10.0.2 y configure lo siguiente.

Panorama debe permitir direcciones IP públicas de AWS. El cortafuegos VM-Series accede a Panorama utilizando la dirección IP externa de la puerta de enlace NAT creada por la plantilla.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Descarga e instalación del complemento VM-Series en Panorama.

1. Seleccione **Panorama** > **Plugins (Complementos)** y utilice **Check Now (Comprobar ahora)** para buscar paquetes de complementos nuevos. El complemento VM-Series se llama `vm_series`.
2. Consulte las notas de las versiones del complemento para comprobar cuál aporta actualizaciones útiles para su caso.
3. Seleccione la versión apropiada del complemento y haga clic en **Download (Descargar)** en la columna Action (Acción).
4. Haga clic en **Install (Instalar)** en la columna Action (Acción). Panorama muestra un aviso cuando termina la instalación.
5. Para ver el complemento, seleccione **Device (Dispositivo)** > **VM-Series**.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Configure la plantilla.

1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Templates (Plantillas)** y haga clic en **Add (Añadir)**.
   1. Introduzca un **Name (Nombre)** descriptivo.
   2. Haga clic en **OK (Aceptar)**.
3. Configure el enrutador virtual.
   1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
   2. Asegúrese de haber seleccionado la plantilla que creó anteriormente en el menú desplegable **Template (Plantilla)**.
   3. Haga clic en **Add (Añadir)**.
   4. Utilice el siguiente formato para nombrar el enrutador virtual: VR-<tempstackname>.
   5. Habilite ECMP en el enrutador virtual.
   6. Haga clic en **OK (Aceptar)**.
4. Configure la interfaz y cree la zona.
   1. Seleccione **Network (Red)** > **Interfaces** y haga clic en **Add Interface (Añadir interfaz)**.
   2. Seleccione **Slot 1 (Ranura 1)** y, a continuación, seleccione el nombre de la interfaz (por ejemplo, Ethernet 1/1).
   3. Establezca **Interface Type (Tipo de interfaz)** en Capa 3.
   4. En la pestaña **Config (Configuración)**, seleccione **New Zone (Nueva zona)** en el menú desplegable **Security Zone (Zona de seguridad)**. En el cuadro de diálogo Zone, defina un **nombre** para la nueva zona, por ejemplo, Internet, y a continuación haga clic en **OK**.
   5. En el menú desplegable **Virtual Router (Enrutador virtual)**, seleccione el enrutador virtual que creó anteriormente.
   6. Seleccione **IPv4** y haga clic en **DHCP Client (Cliente DHCP)**.
   7. Haga clic en **OK (Aceptar)**.
5. Cree un perfil de gestión que permita que HTTPS en la interfaz creada anteriormente admita las comprobaciones de estado.
   1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Interface Mgmt (Gestión de interfaz)** y haga clic en **Add (Añadir)**.
   2. Seleccione los protocolos que la interfaz permitirá para el tráfico de gestión: **Ping**, **Telnet**, **SSH**, **HTTP**, **HTTP OCSP**, **HTTPS** o **SNMP**.

      *No habilite **HTTP** ni **Telnet** porque esos protocolos realizan transmisiones de texto sin cifrar y, por lo tanto, no son seguros.*
6. Asigne el perfil de gestión de interfaz a una interfaz.
   1. Seleccione **Network (Red)** > **Interfaces**, seleccione el tipo de interfaz (**Ethernet**, **VLAN**, **Loopback [Bucle invertido]** o **Tunnel [Túnel]**) y seleccione la interfaz.
   2. Seleccione **Advanced (Avanzado)** > **Other info (Otra información)** y seleccione el **Management Profile (Perfil de gestión)** de la interfaz que acaba de añadir.
   3. Haga clic en **OK (Aceptar)**.
7. Configure el servidor DNS y el tiempo de actualización del FQDN.

 ©2024 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y haga clic en el icono edición.
2. Establezca el **Primary DNS Server (Servidor DNS primario)** en 169.254.169.253. Esta es la dirección DNS de AWS.
3. Establezca el **Minimum FQDN Refresh Time (Tiempo mínimo de actualización de FQDN)** en 60 segundos.
4. Haga clic en **OK (Aceptar)**.

8. Haga clic en **Commit (Confirmar)** para compilar los cambios. Esto es necesario antes de continuar con el siguiente paso.
9. Cree un administrador.
    1. Seleccione **Device (Dispositivo)** > **Administrators (Administradores).**
    2. Introduzca `pandemo` como el **Name (Nombre)**.
    3. Establezca la **Password (Contraseña)** en `demopassword` y elija **Confirm (Confirmar)**.
    4. Haga clic en **OK (Aceptar)**.
10. Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 5 | Configure una pila de plantillas y añada la plantilla a la pila de plantillas.

1. Seleccione **Panorama** > **Templates (Plantillas)** y haga clic en **Add Stack (Añadir pila)**.
2. Introduzca un nombre único en **Name (Nombre)** para identificar la pila.
3. Haga clic en **Add (Añadir)** y seleccione la plantilla.
4. Haga clic en **OK (Aceptar)** para guardar la pila de plantillas.

STEP 6 | Cree el **Device Group (Grupo de dispositivos)**.

1. Seleccione **Panorama** > **Device Groups (Grupos de dispositivos)**.
2. Haga clic en **Add (Añadir)**.
3. Introduzca un **Name (Nombre)** descriptivo.
4. Haga clic en **OK (Aceptar)**.
5. Añada una regla previa de seguridad para permitir todo.
    1. Asegúrese de haber seleccionado el grupo de dispositivos que creó anteriormente en el menú desplegable **Device Group (Grupo de dispositivos)**.
    2. Seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Pre-rules (Reglas previas)** y haga clic en **Add (Añadir)**.
    3. Introduzca un **Name (Nombre)** descriptivo.
    4. En **Source (Origen)**, **User (Usuario)**, **Destination (Destino)**, **Application (Aplicación)** y **Service/URL Category (Categoría de servicio/URL)**, seleccione cualquiera.
    5. En **Actions (Acciones)**, seleccione **Allow (Permitir)**.
    6. Haga clic en **OK (Aceptar)**.
6. Haga clic en **Commit (Confirmar)** para compilar los cambios.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Añada la clave API de desactivación de licencia para el cortafuegos a Panorama.

1. Inicie sesión en el portal de atención al cliente.
2. Seleccione **Products (Productos)** > **Assets (Activos)** > **API Key Management (Gestión de clave de API)**.
3. Copie la clave de API.
4. Use la CLI para instalar la clave de API copiada en el paso anterior.

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

STEP 8 | Después de implementar Panorama, debe abrir los siguientes puertos como se describe a continuación en el grupo de seguridad de Panorama en AWS.

- **Puerto 443 (HTTPS)**: Desde la implementación inicial de la plantilla de cortafuegos, deje HTTPS abierto para que Lambda pueda conectarse a Panorama.

  Cuando asegure el puerto 443, especifique un rango de dirección IP desde el cual permitirá las conexiones, así como las EIP asignados a las puertas de enlace NAT. El número de puertas de enlace NAT en su implementación depende del número de zonas de disponibilidad que configure. Para encontrar las EIP de puerta de enlace NAT en AWS, vaya a **VPC** > **NAT Gateways (Puertas de enlace NAT)**. Anote la información de EIP para el grupo de seguridad para HTTPS.

  Además, para permitir que Panorama libere la licencia de cortafuegos después de la eliminación de la pila, debe permitir el tráfico del rango CIDR de la región donde implementó la plantilla de cortafuegos. Puede encontrar el CIDR para su región en este enlace.
- **Puerto 3978**: Puerto 3978 debe poder recibir tráfico de cualquier dirección IP.

Inicio de la plantilla del cortafuegos

Este flujo de trabajo describe cómo implementar la plantilla del cortafuegos.

STEP 1 | Modifique el archivo `init-cfg.txt` y cárguelo a la carpeta `/ config`.

Debido a que utiliza Panorama para arrancar los cortafuegos VM-Series, su archivo `init-cfg.txt` debería modificarse de la siguiente manera. No se necesita ningún archivo `bootstrap.xml`.

Asegúrese de utilizar los nombres de grupo de dispositivos y plantillas que creó anteriormente en el archivo 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
```

Su archivo init-cfg.txt debe incluir **`plugin-op-commands=aws-gwlb-inspect:enable`**. Esto es necesario al integrar el cortafuegos VM-Series con un GWLB.

Debe añadir el PIN de registro automático del certificado de dispositivo al archivo init-cfg.txt para instalar automáticamente un certificado de dispositivo cuando se implementa su instancia de cortafuegos VM-Series.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Añada el código de autenticación de la licencia en la carpeta `/license` del paquete de arranque.

1. Use un editor de texto para crear un nuevo archivo de texto llamado **`authcodes`** (sin extensión).
2. Añada el código de autenticación para sus licencias BYOL a este archivo y guárdelo. El código de autenticación debe representar un paquete y debe admitir el número de cortafuegos que puedan ser necesarios para su implementación. Si utiliza códigos de autenticación individuales, en vez de un paquete, el cortafuegos solo recupera la clave de licencia para el primer código de autenticación en el archivo.

STEP 3 | Cargue el código Lambda para la plantilla de cortafuegos (`panw-aws-zip`) y la plantilla de aplicación (`app.zip`) a un depósito S3. Puede usar el mismo depósito S3 que usa para el proceso de arranque.

Si la pila de aplicaciones es gestionada por una cuenta diferente a la del cortafuegos, use la cuenta de la aplicación para crear otro depósito s3 en la misma región de AWS que la plantilla del cortafuegos y copie `app.zip` a ese depósito s3.

STEP 4 | Seleccione la plantilla del cortafuegos.

1. En la Consola de administración de AWS, seleccione **CloudFormation** > **Create Stack (Crear pila)**.
2. Seleccione **Upload (Cargar)** la plantilla del cortafuegos más reciente desde el repositorio Git, para elegir la plantilla de cortafuegos para implementar los recursos que inicia la plantilla. Haga clic en Open (Abrir) y Next (Siguiente).
3. Especifique el nombre de la pila. El nombre de pila le permite identificar de manera única todos los recursos que se implementan utilizando esta plantilla.

STEP 5 | Introduzca un **Name (Nombre)** descriptivo para su pila. El nombre debe tener 28 caracteres o menos.

STEP 6 | Configure los parámetros para la VPC.

1. Introduzca el número de zonas de disponibilidad y seleccione la región en el menú desplegable de zonas de disponibilidad.
2. Busque el ID de AMI para el cortafuegos VM-Series e introdúzcalo. Asegúrese de que el ID de AMI coincida con la región de AWS, la versión de PAN-OS y la opción de licencia de BYOL o PAYG que optó por utilizar. Consulte Obtener los ID de Amazon Machine Image para obtener más información.
3. Seleccione el **Key Pair (Par de claves)** EC2 (desde el menú desplegable) para iniciar el cortafuegos. Para iniciar sesión en los cortafuegos, debe proporcionar el nombre de este par de claves y la clave privada asociada a él.
4. Seleccione **Yes (Sí)** si quiere **Enable Debug Log (Habilitar log de depuración)**. La habilitación del log de depuración genera logs más detallados que ayudan a resolver problemas con la implementación. Estos logs se generan utilizando el nombre de la pila y se guardan en AWS CloudWatch.

De forma predeterminada, la plantilla utiliza la utilización de la CPU como parámetro de escalado para los cortafuegos VM-Series. Las métricas PAN-OS personalizadas se publican automáticamente en el espacio de nombres de CloudWatch que coincide con el nombre de la pila que especificó anteriormente.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Especifique el nombre de la(s) bucket(s) de Amazon S3.

1. introduzca el nombre del bucket S3 que contiene el paquete de arranque.

   Si el depósito de arranque no está configurado correctamente o si introduce incorrectamente el nombre del depósito, el proceso de arranque falla y no puede iniciar sesión en el cortafuegos. Los controles de estado para los balanceadores de carga también fallan.
2. Introduzca el nombre del bucket S3 que contiene el archivo panw-aws.zip. Como se mencionó anteriormente, puede usar un depósito S3 para los códigos Bootstrap y Lambda.

STEP 8 | Especifique las claves para habilitar el acceso de la API al cortafuegos y a Panorama.

1. Introduzca la clave que debe usar el cortafuegos para autenticar las llamadas de la API. La clave predeterminada se basa en el archivo de muestra y solo se debe usar para probar y evaluar. Para una implementación de producción, debe crear un inicio de sesión de PAN-OS por separado, solo para la llamada de la API y generar una clave asociada.
2. Introduzca la clave de API para permitir que AWS Lambda haga llamadas de la API a Panorama. Para una implementación de producción, debe crear un inicio de sesión diferente solo para la llamada API y generar una clave asociada.

STEP 9 | Añada su(s) número(s) de cuenta de AWS. Debe proporcionar el número de cuenta que ha utilizado para implementar cualquier VPC que esté conectada a su GWLB. Añada estos valores como una lista separada por comas. Puede añadir números de cuenta adicionales después de implementar la plantilla.

Para ubicar su número de cuenta, haga clic en su nombre de usuario de AWS en la parte superior derecha de la consola de AWS y seleccione **My Security Credentials (Mis credenciales de seguridad)**.

STEP 10 | Introduzca el ID de la puerta de enlace de tránsito. El ID de la puerta de enlace de tránsito es necesaria para proteger el tráfico de salida y este-oeste. Si no introduce un ID de puerta de enlace de tránsito, la plantilla asume que los cortafuegos integrados con GWLB solo deben inspeccionar el tráfico de entrada.

STEP 11 | Introduzca el CIDR para la VPC de seguridad.

STEP 12 | Revise la configuración de la plantilla e inicie la plantilla.

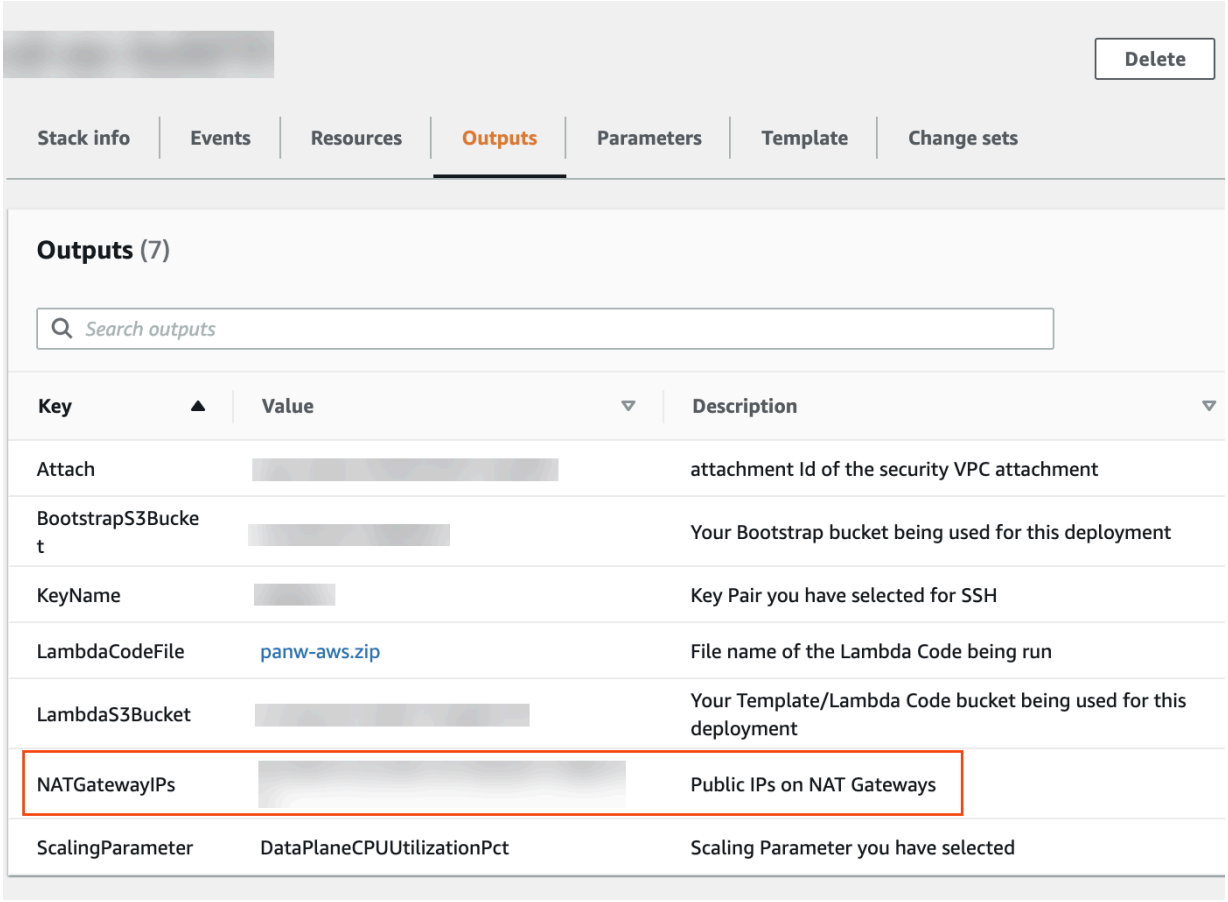
1. Seleccione **I acknowledge that this template might cause AWS CloudFormation to create IAM resources (Entiendo que esta plantilla podría causar que AWS CloudFormation cree recursos de IAM]**.
2. Haga clic en **OK (Aceptar)** para iniciar la plantilla. Se muestra el evento CREATE_IN_PROGRESS.
3. Cuando se realiza una implementación correcta, el estado se actualiza a CREATE_COMPLETE.

STEP 13 | Verifique que la plantilla haya iniciado todos los recursos requeridos.

STEP 14 | Cree reglas que permitan las direcciones IP de la puerta de enlace NAT en el grupo de seguridad donde se implementa el dispositivo Panorama. Esto es necesario para permitir que los cortafuegos se

 ©2024 Palo Alto Networks, Inc.

conecten a Panorama. Se puede encontrar la lista de direcciones IP de la puerta de enlace NAT en la salida de la pila de seguridad CFT.



 ©2024 Palo Alto Networks, Inc.

1. Acceda a la consola VPC de AWS.
2. Seleccione **Security Groups (Grupos de seguridad)** en el panel de navegación.
3. Seleccione la seguridad donde se implementa Panorama.
4. Seleccione **Actions (Acciones)** > **Edit Inbound Rules (Editar reglas de entrada)** > **Add rule (Añadir regla)**.
5. Añada reglas que permitan las direcciones IP de la puerta de enlace de NAT para la regla TCP personalizada para el intervalo de puertos 3978.
6. Haga clic en **Save rules (Guardar reglas)**.

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	

Inicio de la plantilla de la aplicación

Complete el siguiente procedimiento para iniciar la plantilla de la aplicación.

STEP 1 | Cree un deposito S3 desde el que iniciará la plantilla de la aplicación.

- Si se trata de una implementación de cuentas cruzadas, cree un nuevo depósito.
- Si hay una cuenta, puede crear un nuevo depósito o usar el depósito S3 que creó anteriormente (puede usar un depósito para todo).

STEP 2 | Cargue el archivo app.zip en el depósito S3.

STEP 3 | Seleccione la plantilla de inicio de aplicación que desea que inicie.

1. En la consola de administración de AWS, seleccione **CloudFormation** > **CreateStack**
2. Seleccione Upload a template to Amazon S3 (Cargar una plantilla a Amazon S3), para seleccionar la plantilla de aplicación para implementar los recursos que la plantilla inicia dentro de la misma VPC que los cortafuegos, o a una VPC diferente. Haga clic en **Open (Abrir)** y **Next (Siguiente)**.
3. Especifique el nombre de la pila. El nombre de pila le permite identificar de manera única todos los recursos que se implementan utilizando esta plantilla.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Seleccione las zonas de disponibilidad (AZ) que abarcará su configuración en Seleccionar lista de AZ.

STEP 5 | Introduzca un **VPC Name (Nombre de VPC)** descriptivo.

STEP 6 | Configure los parámetros de Lambda.

1. Introduzca el nombre del depósito S3 donde se almacena app.zip.
2. Introduzca el nombre del archivo zip.

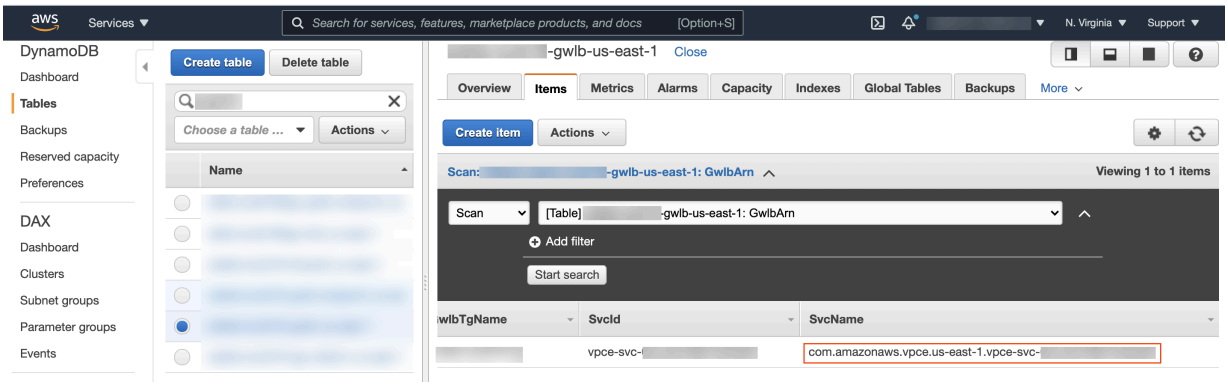
STEP 7 | Seleccione el tipo de instancia EC2 para el servidor web Ubuntu iniciado por esta plantilla.

STEP 8 | Introduzca su par de claves de Amazon EC2.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Introduzca el nombre de la configuración del servicio (Nombre del servicio) para el endpoint GWLB en la VPC de seguridad.

1. Seleccione **DynamoDB** en el menú desplegable **Services (Servicios)** en la consola de AWS.
2. Seleccione **Tables (Tablas)** y busque su tabla de VPC de seguridad. El nombre de la tabla será <stack name>-gwlb-<region>. Por ejemplo, cft-deployment-gwlb-us-east-1.
3. Haga clic en la pestaña Elementos y copie el Nombre del servicio.
4. Pegue el nombre del servicio en los parámetros de configuración de la plantilla de la aplicación.



 ©2024 Palo Alto Networks, Inc.

STEP 10 | Introduzca el ID de la puerta de enlace de tránsito. Esta es la misma puerta de enlace de tránsito que creó antes de implementar la plantilla de cortafuegos.

STEP 11 | Revise la configuración de la plantilla e inicie la plantilla.

STEP 12 | Una vez implementada la aplicación, debe añadir una ruta a la tabla de enrutamiento de la puerta de enlace de tránsito para habilitar la inspección del tráfico de salida y de este a oeste.

1. Inicie sesión en la consola de VPC de AWS.
2. Seleccione **Transit Gateway Route Tables (Tablas de enrutamiento de la puerta de enlace de tránsito)** y elija la tabla de enrutamiento de la puerta de enlace de tránsito. Esta tabla de enrutamiento la ha creado la plantilla y se denomina **<app-stack-name>-<region>-PANWAppAttRt**.
3. Seleccione **Routes (Rutas)** y haga clic en **Create static route (Crear ruta estática)**.
4. Introduzca 0.0.0.0/0 en el campo **CIDR**.
5. En el menú desplegable **Choose attachment (Elegir adjunto)**, seleccione el adjunto de VPC de cortafuegos VM-Series.
6. Haga clic en **Create static route (Crear ruta estática)**.

STEP 13 | (Opcional) Cree un host bastión (también conocido como un cuadro de salto) para acceder al servidor web creado por la plantilla de la aplicación.

1. Cree una subred pública en la VPC de su aplicación.
2. Añada un enrutamiento a esta subred desde su dirección IP hasta la puerta de enlace de internet.
3. Cree una nueva instancia EC2 en la subred pública con una dirección IP pública..
4. Cree un grupo de seguridad para esta instancia EC2 que permita el acceso SSH desde su dirección IP.

Habilitar la resiliencia de sesión en el VM-Series para AWS

La resiliencia de la sesión permite que el cortafuegos VM-Series mantenga la continuidad de la sesión durante un evento de fallo. El AWS Gateway Load Balancer (GWLB) puede detectar y cancelar el registro de cortafuegos en mal estado de la serie VM-Series implementados en un clúster escalable horizontalmente detrás del GWLB. Con la capacidad de resiliencia de sesión habilitada, la GWLB puede rehacer las sesiones de tráfico existentes que fluyen hacia un VM-Series en mal estado y redirigir el tráfico a un cortafuegos VM-Series en buen estado.

Para mantener las sesiones conmutando por error a cortafuegos saludables de la serie VM-Series, debe implementar una caché de Redis accesible a sus cortafuegos VM-Series: ElastiCache para Redis para AWS. La caché de Redis mantiene la información de sesión. Cuando el balanceador de carga detecta un cortafuegos VM-Series en mal estado, el balanceador de carga reequilibra el tráfico a un cortafuegos VM-Series en buen estado. El cortafuegos en buen estado VM-Series accede a la caché de Redis para obtener información de sesión y continúa inspeccionando y reenviando el tráfico existente.

Su balanceador de carga debe cumplir con los siguientes requisitos para soportar la resiliencia de sesión.

- Su balanceador de carga debe ser un balanceador de carga de puerta de enlace.
- Debe establecer **Volver a equilibrar flujo existente** en **Activado** para permitir que el GWLB rehaga flujos existentes. Consulte la Documentación de AWS para obtener más información.
- Habilite el **Cifrado en tránsito** para cifrar las conexiones a la caché Redis mediante TLS.

 ©2024 Palo Alto Networks, Inc.

Su instancia de ElastiCache para Redis debe cumplir los siguientes requisitos para admitir la resiliencia de la sesión en el cortafuegos VM-Series.

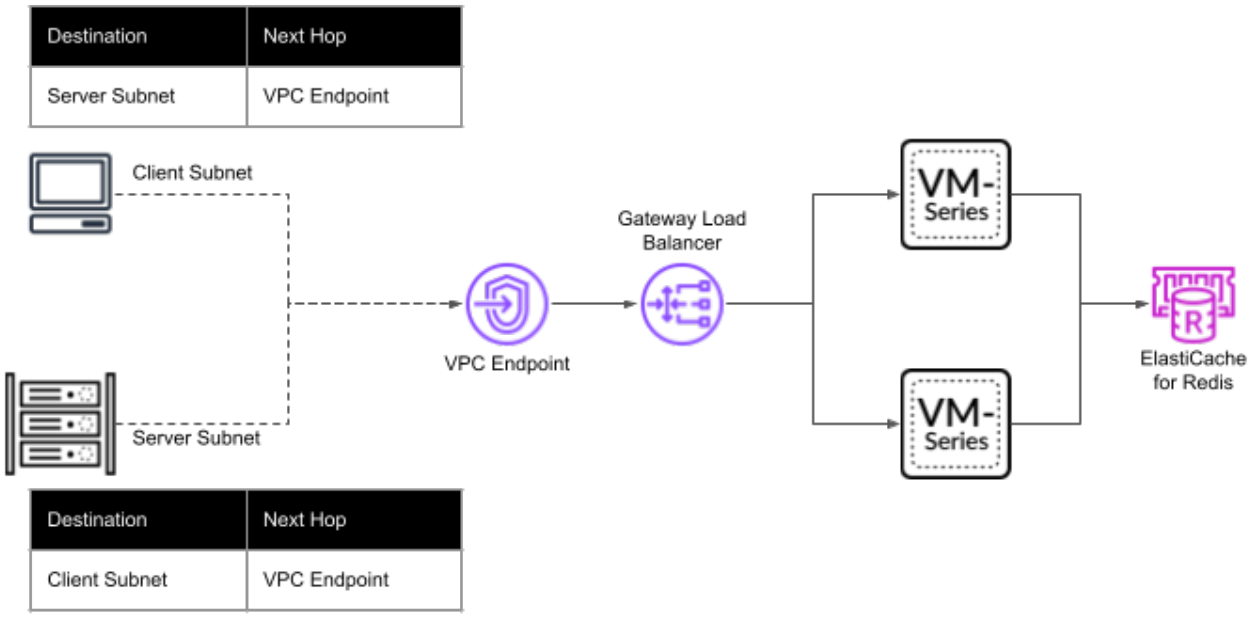
- Nivel estándar
- Implemente la caché de Redis en la misma región y zona que las instancias del cortafuegos VM-Series.
- Asegúrese de que su interfaz de gestión de cortafuegos pueda acceder a su instancia de ElastiCache. Por ejemplo, tenga ambos dispositivos en el mismo VPC.

Al dimensionar su Memorystore para Redis, utilice las siguientes pautas.

- Base el tamaño de la caché de Redis en el número máximo de sesiones admitidas por la instancia del cortafuegos VM-Series. Consulte Límites máximos basados en nivel y memoria hasta el máximo de sesiones para su cortafuegos.
- Cada entrada redis por sesión utiliza aproximadamente 128 bytes. Por lo tanto, un cortafuegos VM-Series que admite 10.000.000 de sesiones requiere aproximadamente 1,3 GB de almacenamiento. Y un clúster de 10 cortafuegos VM-Series requiere al menos 13 GB.
- Utilice la siguiente fórmula para calcular los requisitos de redis.

  (128 x <number of sessions>) x 10^{-9} = requiere tamaño de caché de Redis por cortafuegos

Antes de habilitar la capacidad de resiliencia de la sesión, revise el blog de AWS sobre Flujos de tráfico existentes.



 ©2024 Palo Alto Networks, Inc.

La resiliencia de la sesión no se puede habilitar en las instancias de cortafuegos VM-Series existentes; solo en las nuevas instancias de implementación.

Habilite la resiliencia de sesión en el cortafuegos VM-Series pasando la configuración como parte de un archivo init-cfg.txt de arranque o en el campo de datos de usuario. Antes de comenzar, asegúrese de tener la siguiente información.

Campo	Descripción
`op-command-modes=mgmt-interface-swap`	Permite intercambiar la interfaz de gestión (MGT) con la interfaz de plano de datos (ethernet 1/1) al implementar el cortafuegos. Para obtener más detalles, consulte Asignación de interfaz de gestión para su uso con Amazon ELB.
`plugin-op-commands=` 1. `set-sess-ress:True` 2. `aws-gwlb-inspec:enable`	1. Activa la resiliencia de la sesión. 2. Habilita el cortafuegos VM-Series para procesar el tráfico que pasa a través de una GWLB
`redis-endpoint=`	Proporcione la dirección IP o FQDN y el puerto de su endpoint de ElastiCache Redis
`redis-auth=`	(opcional) El código de autenticación que usa su cortafuegos VM-Series para conectarse con el endpoint de Redis

STEP 1 | Implemente su instancia de ElastiCache para Redis.

STEP 2 | Prepara sus archivos de arranque.

```
op-command-modes=mgmt-interface-swap plugin-op-commands=set-
sess-ress:True, aws-gwlb-inspect:enable redis-endpoint=<redis-IP-
address:port> redis-auth=<redis-auth-code>
```

STEP 3 | Arranque sus cortafuegos.

 ©2024 Palo Alto Networks, Inc.

Alta disponibilidad para el cortafuegos VM-Series en AWS

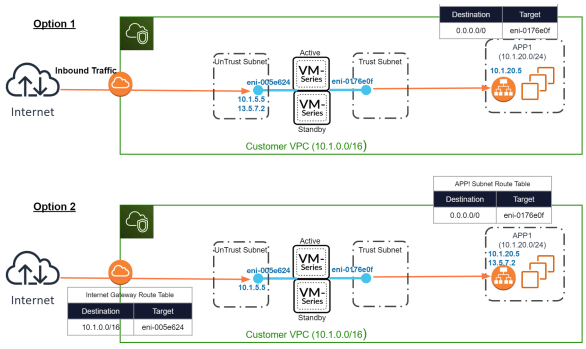
El cortafuegos VM-Series en AWS acepta solamente HA activa/pasiva; si se implementa con Amazon Elastic Load Balancing (ELB), no acepta HA (en este caso, el ELB proporciona capacidades de conmutación de fallos).

- Descripción general de HA en AWS
- Funciones de IAM para HA
- Enlaces de HA
- Sondeos de heartbeat y mensajes de saludo
- Prioridad y preferencia de dispositivos
- Temporizadores de HA
- Configuración de HA activa/pasiva en AWS mediante una IP secundaria
- Configuración de HA activa/pasiva en AWS mediante Interface Move
- Migración de HA activa/pasiva en AWS

Descripción general de HA en AWS

Para asegurar la redundancia, puede implementar cortafuegos VM-Series en AWS en una configuración de alta disponibilidad (HA) activa/pasiva. El peer activo sincroniza continuamente su información de sesión y configuración con el peer pasivo configurado de manera idéntica. Una conexión de latido entre los dos dispositivos garantiza la conmutación por error si falla el dispositivo activo. Hay dos opciones para implementar el cortafuegos VM-Series en AWS en HA: movimiento de IP secundaria y movimiento de interfaz de plano de datos (ENI).

Tiene dos opciones para asegurarse de que todo el tráfico a sus aplicaciones que se conectan a internet pase a través del cortafuegos. Puede configurar la dirección IP pública de la aplicación en la interfaz Untrust (E1/2 en la ilustración anterior) del cortafuegos VM-Series, o puede configurar el enrutamiento de entrada de AWS. La capacidad de enrutamiento de entrada de AWS le permite asociar tablas de ruta con la puerta de enlace de Internet de AWS y añadir reglas de ruta para redirigir el tráfico de la aplicación a través del cortafuegos VM-Series. Esta redirección garantiza que todo el tráfico de Internet pase a través del cortafuegos sin tener que reconfigurar los endpoints de la aplicación.



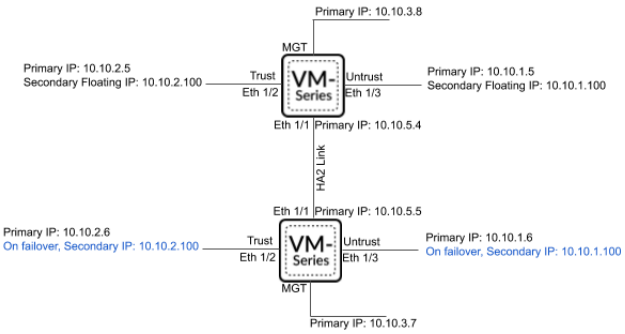
Movimiento de IP secundaria

Cuando el par activo deja de funcionar, el par pasivo detecta este fallo y se activa. Además, activa las llamadas de la API a la infraestructura de AWS para mover las direcciones IP secundarias configuradas

 ©2024 Palo Alto Networks, Inc.

desde las interfaces del plano de datos del par que ha fallado a sí mismo. Además, AWS actualiza las tablas de rutas para garantizar que el tráfico se dirija a la instancia de cortafuegos activa. Estas dos operaciones garantizan que las sesiones de tráfico de entrada y saliente se restauren después de la conmutación por error. Esta opción le permite aprovechar DPDK para mejorar el rendimiento de sus instancias de cortafuegos VM-Series y proporciona un mejor tiempo de conmutación por error que el HA de movimiento de interfaz, a la vez que es compatible con todas las funciones proporcionadas por el movimiento de interfaz.

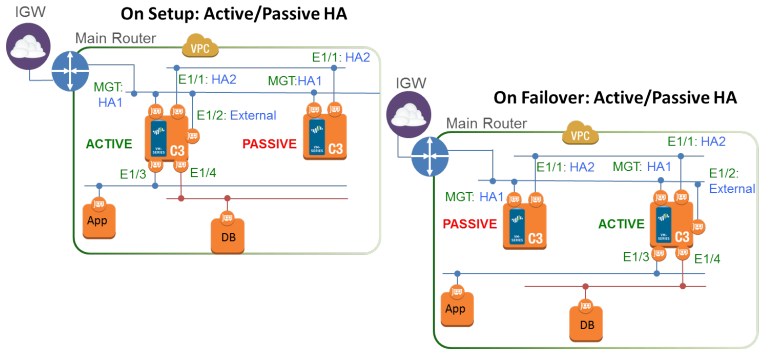
La HA de cambio de IP secundaria requiere el complemento VM-Series 2.0.1 o posterior.



Ahora puede configurar hasta cuatro direcciones IP por interfaz SD-WAN para lograr la conmutación por error de alta disponibilidad en configuraciones activas/pasivas de su entorno de nube pública AWS. Puede lograrlo configurando una segunda dirección IP flotante en las interfaces SD-WAN. La IP flotante en la interfaz SD-WAN de la zona externa debe coincidir con la de la zona interna. Esta función solo es compatible con PAN-OS 11.1.0 y versiones posteriores y solo con direcciones IPv4.

Movimiento de Interfaz de plano de datos

Cuando el par activo deja de funcionar, el par pasivo detecta el fallo y se activa. Además, activa llamadas API a la infraestructura de AWS para mover todas las interfaces de plano de datos (ENI) del par que ha fallado a sí mismo.



 ©2024 Palo Alto Networks, Inc.

Funciones de IAM para HA

AWS requiere que todas las solicitudes de API se firmen criptográficamente con las credenciales emitidas por ellos. Para habilitar los permisos de API para cortafuegos VM-Series que se implementarán como par HA, debe crear una política y vincular esa política a una función en el Servicio de gestión de identidad y acceso (IAM) de AWS. El papel debe vincularse a los cortafuegos VM-Series al iniciarse. La política otorga a la función de IAM permisos para iniciar las acciones de API necesarias para mover interfaces o direcciones IP secundarias del par activo al par pasivo cuando se activa la conmutación por error.

Para instrucciones detalladas sobre la creación de políticas, consulte la documentación de AWS en Creación de políticas gestionadas del cliente. Para obtener instrucciones detalladas sobre cómo crear una función de IAM, cómo definir qué cuentas o servicios de AWS pueden asumir la función, cómo definir qué acciones y recursos de API puede usar la aplicación luego de asumir la función, consulte la documentación de AWS sobre Funciones de IAM para Amazon EC2.

La función de IAM, que se configura en la consola de AWS, debe tener los permisos para las siguientes acciones y recursos (como mínimo):

Las siguientes acciones, permisos y recursos de IAM son necesarios para habilitar la HA. Para habilitar la supervisión de AWS Cloudwatch, consulte Habilitación de la supervisión de CloudWatch en el cortafuegos VM-Series

para la acción de IAM necesaria.

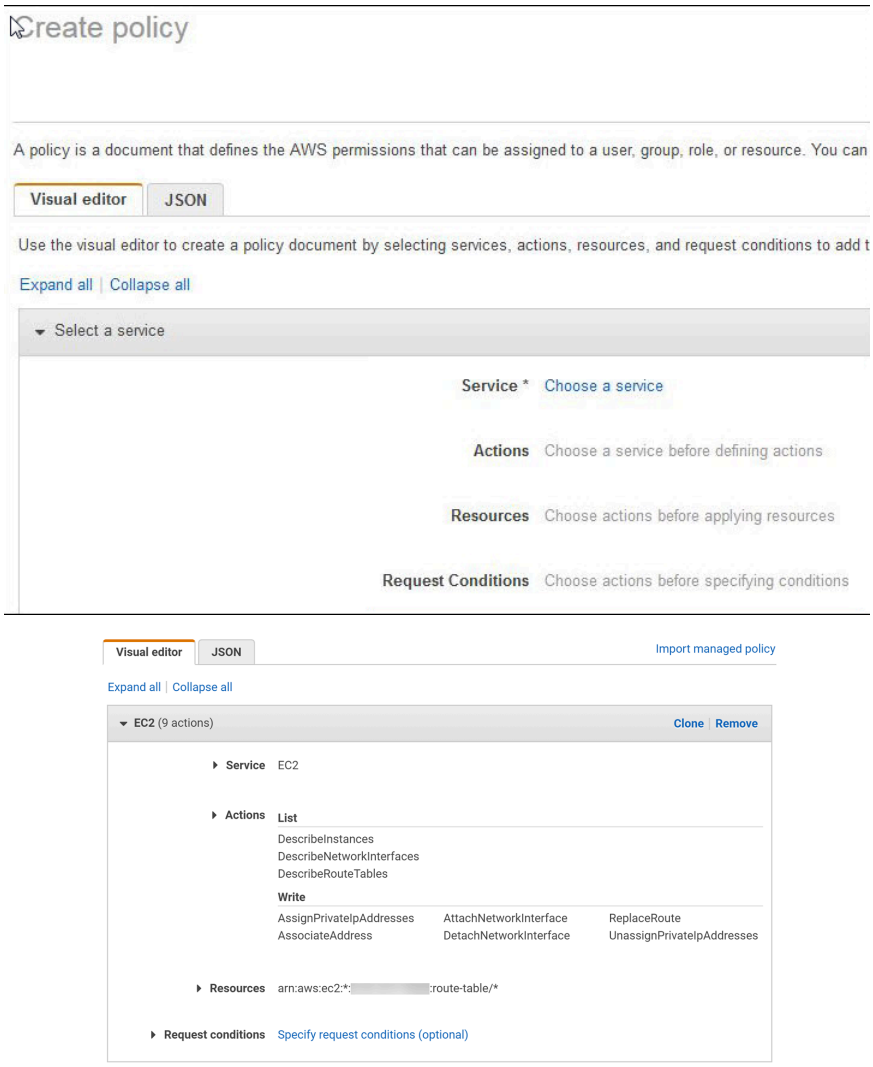
Acción, permiso o recurso de IAM	Description (Descripción)	Movimiento de interfaz	Movimiento de IP secundaria
AttachNetworkInterface	Para obtener permiso para adjuntar una ENI a una instancia.	✓	✓
DescribeNetworkInterfaces	Para obtener los parámetros de ENI con el fin de adjuntar una interfaz a la instancia.	✓	✓
DetachNetworkInterface	Para obtener permiso para desconectar la ENI de la instancia EC2.	✓	✓
DescribeInstances	Para dar permiso para obtener información sobre las instancias de EC2 en la VPC.	✓	✓
AssociateAddress	Para obtener permisos para mover direcciones IP públicas asociadas con las direcciones IP primarias de la interfaz pasiva a la activa.		✓
AssignPrivateIpAddresses	Para permisos para asignar direcciones IP secundarias y direcciones IP públicas asociadas a interfaces en el par pasivo.		✓

©2024 Palo Alto Networks, Inc.

Acción, permiso o recurso de IAM	Description (Descripción)	Movimiento de interfaz	Movimiento de IP secundaria
DescribeRouteTables	Para obtener permiso para recuperar todas las tablas de enrutamiento asociadas a las instancias del cortafuegos VM-Series.		✓
ReplaceRoute	Para obtener permisos para actualizar las entradas de la tabla de enrutamiento de AWS.		✓
GetPolicyVersion	Para obtener permiso para recuperar información sobre la versión de la política de AWS.		✓
GetPolicy	Para obtener permiso para recuperar información sobre políticas de AWS.		✓
ListAttachedRolePolicies	Para obtener permiso para recuperar la lista de todas las políticas administradas adjuntas a un rol de IAM específico.		✓
ListRolePolicies	Para obtener permiso para recuperar una lista de los nombres de las políticas en línea integradas en un rol de IAM específico.		✓
GetRolePolicy	Para obtener permiso para recuperar una política en línea especificada incrustada en una función de IAM especificada.		✓
política	Para obtener permiso para acceder al Nombre de recurso de Amazon (ARN) de la política de IAM.		✓
función	Para obtener permiso para acceder al ARN de las funciones de IAM.		✓
tabla de enrutamiento	Para obtener permiso para acceder a la tabla de enrutamiento Nombre de recurso de Amazon (ARN) para actualizarla tras una conmutación por error.		✓
Comodín (*)	En el campo ARN use * como comodín.	✓	✓

 ©2024 Palo Alto Networks, Inc.

La siguiente captura de pantalla muestra la configuración de gestión de acceso para la función de IAM descrita anteriormente para el HA de IP secundaria:



Los permisos mínimos que necesita para la alta disponibilidad (HA) de movimiento de la interfaz son:

{ "Version":"2012-10-17", "Statement":[{ "Sid":"VisualEditor0", "Effect":"Allow", "Action": ["ec2:AttachNetworkInterface", "ec2:DetachNetworkInterface", "ec2:DescribeInstances", "ec2:DescribeNetworkInterfaces"], "Resource":"*" }]}

Los permisos mínimos que necesita para la alta disponibilidad (HA) de movimiento de la IP secundaria son:

{ "Statement": [{ "Action": ["ec2:AttachNetworkInterface", "ec2:DetachNetworkInterface", "ec2:DescribeInstances", "ec2:DescribeNetworkInterfaces", "ec2:AssignPrivateIpAddresses", "ec2:AssociateAddress", "ec2:DescribeRouteTables"], "Effect": "Allow", "Resource": ["*"], "Sid": "VisualEditor0" }, { "Action": "ec2:ReplaceRoute", "Effect": "Allow", "Resource": "arn:aws:ec2:*:*:route-table/*", "Sid": "VisualEditor1" }], "Version": "2012-10-17"}

 ©2024 Palo Alto Networks, Inc.

Enlaces de HA

Los dispositivos en un par de HA usan enlaces HA para sincronizar datos y mantener información de estado. en AWS, el cortafuegos VM-Series usa los siguientes puertos:

- **Enlace de control**: El enlace de HA1 se utiliza para intercambiar saludos, heartbeats e información de estado de HA, así como la sincronización del plano de gestión para el enrutamiento e información de User-ID. Este enlace también se utiliza para sincronizar cambios de configuración en el dispositivo activo o pasivo con su peer.

  El puerto de gestión se utiliza para HA1. Puertos TCP 28769 y 28260 para una comunicación con texto claro; puerto 28 para una comunicación cifrada (SSH sobre TCP).

- **Enlace de datos**: El enlace de HA2 se utiliza para sincronizar sesiones, reenviar tablas, asociaciones de seguridad de IPSec y tablas de ARP entre dispositivos de un par de HA. El flujo de datos del enlace de HA2 siempre es unidireccional (excepto en la conexión persistente de HA2); fluye desde el dispositivo activo al dispositivo pasivo.

  Ethernet1/1 debe asignarse como el enlace HA2; esto es necesario para implementar el cortafuegos VM-Series en AWS en HA. El enlace de datos de HA puede configurarse para utilizar IP (número de protocolo 99) o UDP (puerto 29281) como transporte.

El cortafuegos VM-Series en AWS no admite los enlaces de backup para HA1 ni HA2.

Sondeos de heartbeat y mensajes de saludo

Los cortafuegos utilizan mensajes de saludo y latido para comprobar que el peer responde y está operativo. Los mensajes de saludo se envían desde un peer al otro en el *intervalo de saludo* configurado para verificar el estado del dispositivo. El heartbeat es un ping ICMP para el peer de HA a través del enlace de control y el peer responde al ping para establecer que los dispositivos están conectados y responden. Si desea información detallada sobre los temporizadores de HA que activan una conmutación por error, consulte Temporizadores de HA. (Los temporizadores de HA para el cortafuegos VM-Series son los mismos que para los cortafuegos serie PA-5200).

Prioridad y preferencia de dispositivos

A los dispositivos de un par de HA se les puede asignar un valor de *prioridad de dispositivo* para indicar una preferencia por el dispositivo que debería asumir el papel activo y gestionar el tráfico en una conmutación por error. Si necesita utilizar un dispositivo específico del par de HA para proteger de manera activa el tráfico, debe habilitar el comportamiento de preferencia en ambos cortafuegos y asignar un valor de prioridad de dispositivo para cada dispositivo. El dispositivo con el valor numérico más bajo y, por lo tanto, *mayor prioridad*, se designará como activo y gestionará todo el tráfico de la red. El otro dispositivo estará en un estado pasivo y sincronizará información de configuración y estado con el dispositivo activo, de manera que esté listo para pasar al estado activo en el caso de producirse un fallo.

De manera predeterminada, la preferencia está deshabilitada en los cortafuegos y debe habilitarse en ambos dispositivos. Cuando se habilita, el comportamiento de preferencia permite que el cortafuegos con la *mayor prioridad* (valor numérico más bajo) vuelva a estar activo cuando se recupere de un fallo. Cuando se produce una preferencia, el evento se registra en los logs del sistema.



No se recomienda la preferencia para HA en el cortafuegos VM-Series en AWS.

 ©2024 Palo Alto Networks, Inc.

Temporizadores de HA

Los temporizadores de alta disponibilidad (HA) se utilizan para detectar un fallo de cortafuegos y activar una conmutación por error. Para reducir la complejidad al configurar temporizadores de HA, puede seleccionar uno de los tres perfiles: **Recommended (Recomendado)**, **Aggressive (Agresivo)** y **Advanced (Avanzado)**. Estos perfiles cumplimentan automáticamente los valores óptimos del temporizador de HA para la plataforma de cortafuegos específica con el fin de habilitar una implementación de HA más rápida.

Utilice el perfil **Recommended (Recomendado)** para ajustes comunes del temporizador de conmutación por error y el perfil **Aggressive (Agresivo)** para ajustes más rápidos del temporizador de conmutación por error. El perfil **Advanced (Avanzado)** le permite personalizar los valores del temporizador para que se adapten a sus requisitos de red.

Temporizador de HA en VM-Series de AWS	Valores predeterminados para los perfiles Recomendado/Agresivo
Tiempo de espera de promoción	2000/500 ms
Intervalo de saludo	8000/8000 ms
Intervalo de heartbeat	2000/1000 ms
Número máximo de flaps	3/3
Tiempo de espera para ser preferente	1/1 min
Tiempo de espera activo tras fallo de supervisor	0/0 ms
Tiempo de espera ascendente principal adicional	500/500 ms

Configuración de HA activa/pasiva en AWS mediante una IP secundaria

Complete el siguiente procedimiento para implementar nuevos cortafuegos VM-Series como un par de HA con direcciones IP secundarias.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Antes de implementar los cortafuegos VM-Series para su par HA, asegúrese de lo siguiente:

- Consulte la Hoja de trabajo de planificación de VPC para asegurarse de que su VPC esté preparada para el cortafuegos VM-Series.
- La HA de cambio de IP secundaria requiere el complemento VM-Series 2.0.1 o posterior.
- Implemente los pareja de HA en la misma zona de disponibilidad de AWS.

  A partir del complemento 2.0.3 de VM-Series, puede implementar los pares HA en diferentes zonas de disponibilidad. Aunque no se recomienda este tipo de implementación, se admite.
- Cree una función de IAM y asigne la función al cortafuegos VM-Series cuando implemente las instancias.
- Los cortafuegos activos y pasivos deben tener al menos cuatro interfaces cada uno: una interfaz de gestión, una interfaz HA2, una interfaz untrust y una interfaz trust. Además, las interfaces trust y no trust en el cortafuegos activo deben asignar una dirección IP secundaria.

  La interfaz de administración debe utilizarse como la interfaz HA1.
- Compruebe que los componentes de red y seguridad están definidos adecuadamente.
  - Habilitar la comunicación a Internet desde la interfaz de gestión (al menos `udp/53` y `tcp/443`). La VPC predeterminada incluye una puerta de enlace de internet, y si instala el cortafuegos VM-Series en la subred predeterminada, tendrá acceso a internet.
  - Cree subredes. Las subredes son segmentos de intervalos de direcciones IP asignados a la VPC en las que puede iniciar las instancias de EC2. El cortafuegos VM-Series debe pertenecer a la subred pública para que se pueda configurar su acceso a internet.
  - Cree un grupo de seguridad de datos que incluya las interfaces de datos del cortafuegos. Además, configure la seguridad para permitir todo el tráfico (0.0.0.0/0), de modo que los cortafuegos apliquen la seguridad. Esto es necesario para mantener las sesiones existentes durante la conmutación por error.
  - Añada rutas a la tabla de enrutamiento para una subred privada para garantizar que el tráfico se puede dirigir a través de subredes y grupos de seguridad en la VPC, según corresponda.
- Si está arrancando el cortafuegos, cree el depósito de S3 necesario que contenga los archivos de arranque requeridos.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Implementación del cortafuegos VM-Series en AWS.

1. Si sus cortafuegos VM-Series no tienen instalado el complemento de VM-Series 2.0.1 o posterior, actualice el complemento antes de continuar.
2. Configure ethernet 1/1 como la interfaz HA2 en cada par de HA.
   1. Abra la consola de Amazon EC2.
   2. Seleccione Interfaz de red y luego seleccione su interfaz de red.
   3. Seleccione **Actions (Acciones)** > **Manage IP Addresses (Administrar direcciones IP).**
   4. Deje el campo en blanco para permitir que AWS asigne una dirección IP dinámicamente o introduzca una dirección IP dentro del rango de subred para el cortafuegos VM-Series.
   5. Haga clic en **Yes (Sí)** y **Update (Actualizar)**.
   6. Seleccione **Actions (Acciones)** > **Cambiar comprobación de Origen/Dest. (Cambiar comprobación de origen/destino)** y seleccione **Disable (Desactivar)**.
   7. Repita este proceso en el segundo par de HA (para que sea pasivo).
3. Añada una dirección IP secundaria a las interfaces de su plano de datos en el par de HA (para que sea activo).
   1. Seleccione **Network Interface (Interfaz de red)** y luego seleccione su interfaz de red.
   2. Seleccione **Actions (Acciones)** > **Manage IP Addresses (Administrar direcciones IP)** > **IPv4 Addresses (Direcciones IPv4)** > **Assign new IP (Asignar nueva IP)**.
   3. Deje el campo en blanco para permitir que AWS asigne una dirección IP dinámicamente o introduzca una dirección IP dentro del rango de subred para el cortafuegos VM-Series.
   4. Haga clic en **Yes (Sí)** y **Update (Actualizar)**.
4. Asocie una dirección IP elástica (pública) en la instancia principal con la interfaz no fiable del par activo.
   1. Seleccione **Elastic IPs (IP elásticas)** y luego elija la dirección de IP elástica para asociar.
   2. Seleccione **Actions (Acciones)** > **Associate Elastic IP (Asociar IP elástica)**.
   3. En **Resource Type (Tipo de recurso)**, seleccione **Network Interface (Interfaz de red)**.
   4. Seleccione la interfaz de red con la que asociar la Dirección IP elástica.
   5. Haga clic en **Associate (Asociar)**.
5. Para la inspección del tráfico saliente, añada una entrada a la tabla de enrutamiento de subred que establezca el siguiente salto como la interfaz trust del cortafuegos.
   1. Seleccione **VPC** > **Route Tables (Tablas de enrutamiento)**.
   2. Elija su tabla de enrutamiento de subred.
   3. Seleccione **Actions (Acciones)** > **Edit routes (Editar rutas)** > **Add route (Añadir ruta)**.
   4. Introduzca el bloque CIDR o la dirección IP de **Destination (Destino)**.
   5. Para **Target (Destino)**, introduzca la interfaz de red de la interfaz trust del cortafuegos.
   6. Haga clic en **Save routs (Guardar rutas)**.
6. Para utilizar AWS Ingress Routing, cree una tabla de enrutamiento y asóciela a la puerta de enlace de Internet. Luego añada una entrada con el siguiente salto configurado como la interfaz untrust del cortafuegos activo.

 ©2024 Palo Alto Networks, Inc.

1. Seleccione **Route Tables (Tablas de enrutamiento)** > **Create route table (Crear tabla de enrutamiento)**.
2. (Opcional) Introduzca una **Name tag (Etiqueta de nombre)** descriptiva para su tabla de enrutamiento.
3. Haga clic en **Create (Crear)**.
4. Haga clic en su tabla de enrutamiento y seleccione **Actions (Acciones)** > **Edit edge associations (Editar asociaciones perimetrales)**.
5. Seleccione **Internet gateways (Puertas de enlace de Internet)** y elija su puerta de enlace de Internet de VPC.
6. Haga clic en **Save (Guardar)**.
7. Haga clic en su tabla de enrutamiento y seleccione **Actions (Acciones)** > **Edit routes (Editar rutas)**.
8. Para el **Target (Destino)**, seleccione **Network Interface (Interfaz de red)** y elija la interfaz untrust del cortafuegos activo.
9. Haga clic en **Save routs (Guardar rutas)**.

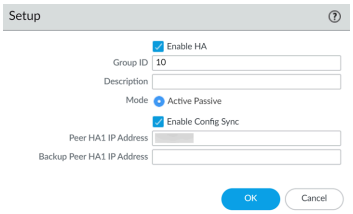
STEP 3 | Configure las interfaces en el cortafuegos. Debe configurar el enlace de datos HA2 y al menos dos interfaces de Capa 3 para sus interfaces trust y untrust. Complete este flujo de trabajo en el primer par de HA y luego repita los pasos en el segundo par de HA.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Seleccione **Red** > **Interfaces** > **Ethernet** y haga clic en su interfaz untrust. En este ejemplo, la interfaz HA2 es 1/1, la interfaz trust es ethernet 1/2 y la interfaz untrust es ethernet 1/3.
3. Haga clic en el enlace de **ethernet 1/1** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **HA**
4. Haga clic en el enlace de **ethernet 1/2** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **capa 3**
   - En la pestaña **Config (Configurar)**, asigne la interfaz el enrutador predeterminado.
   - En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. Defina una zona nueva, por ejemplo trust-zone, y a continuación haga clic en **Aceptar**.
   - En la pestaña **IPv4**, seleccione **DHCP Client (Cliente DHCP)**.
   - Marque **Enable (Habilitar)**.
   - En la interfaz untrust, marque **Automatically create default route pointing to default gateway provided by server (Crear ruta predeterminada automáticamente que apunte a la puerta de enlace predeterminada proporcionada por el servidor)**. Esta opción indica al cortafuegos que cree una ruta estática a una puerta de enlace predeterminada.
   - Repita estos pasos para ethernet 1/3.
5. Repita los pasos anteriores en el par pasivo.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Habilitar HA.

1. Seleccione **Dispositivo** > **Alta disponibilidad** > **General**.
2. Edite los ajustes de la configuración.
3. Introduzca la dirección IP privada del par pasivo en el **Campo de dirección IP del par HA1**.
4. Haga clic en **OK (Aceptar)**.



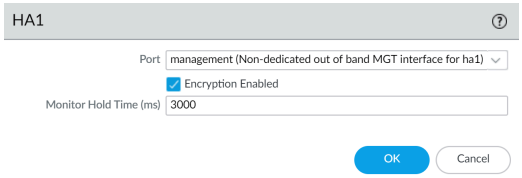
5. Edite la **Election Settings (Configuración de elección)** para especificar un cortafuegos específico para que sea el par activo. Introduzca un valor numérico más bajo de **Device Priority (Prioridad de dispositivo)** en el cortafuegos activo. Si ambos cortafuegos tienen el mismo valor de prioridad de dispositivo, el cortafuegos con el valor MAC más bajo en el control de HA1 será el cortafuegos activo.

   No se recomienda habilitar la función de preferencia.

6. Haga clic en **OK (Aceptar)**.
7. **Commit (Confirmar)** los cambios.
8. Repita los pasos anteriores en el par pasivo.

STEP 5 | Configure el Enlace de control (HA1) para usar el puerto de gestión.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la sección Control Link (HA1) (Enlace de control).

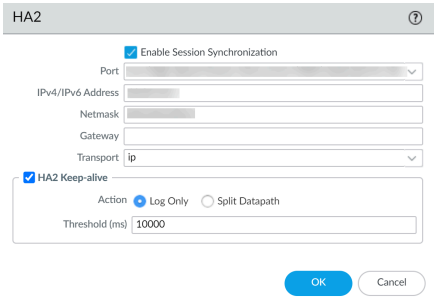


2. (Opcional) Seleccione **Encryption Enabled (Cifrado habilitado)** para proteger la comunicación de HA entre los peers. Para habilitar el cifrado, debe exportar la clave de HA desde un dispositivo e importarla al dispositivo peer.
   1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **Certificates (Certificados)**.
   2. Seleccione **Export HA key (Exportar clave de HA)**. Guarde la clave de HA en una ubicación de red a la que pueda acceder el dispositivo peer.
   3. En el dispositivo peer, desplácese hasta **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** y seleccione **Import HA key (Importar clave de HA)** para desplazarse hasta la ubicación donde guardó la clave e importarla en el dispositivo peer.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Configure el Enlace de datos (HA2) para usar ethernet1/1.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite la sección Enlace de datos (HA2).
2. Seleccione el **Port (Puerto)** ethernet1/1.
3. Introduzca la dirección IP para ethernet1/1. Esta dirección IP debe ser la misma que asignó a la ENI en el panel EC2.
4. Introduzca la **Netmask (Máscara de red)**.
5. Introduzca una dirección IP de **Gateway (Puerta de enlace)** si las interfaces de HA1 están en subredes separadas.
6. Seleccione **IP** o **UDP** para **Transport (Transporte)**. Utilice **IP** si necesita transporte de Capa 3 (número de protocolo de IP 99). Utilice **UDP** si desea que el cortafuegos calcule la suma de comprobación de todo el paquete y no solamente el encabezado, como en la opción IP (puerto UDP 29281).



7. (Opcional) Modifique el **Threshold (Umbral)** para los paquetes **HA2 Keep-alive (Conexión persistente de HA2)**. De manera predeterminada, **HA2 Keep-alive (Conexión persistente de HA2)** Conexión persistente de HA2) está habilitada para la supervisión del enlace de datos de HA2 entre los peers. Si ocurre un fallo y se supera este umbral (el valor predeterminado es 10000 ms), se producirá la acción definida. Se generará un mensaje de log de sistema crítico cuando se produzca un fallo de conexión persistente de HA2.

*Puede configurar la opción **HA2 keep-alive (Conexión persistente de HA2)** en ambos dispositivos o solamente un dispositivo del par de HA. Si habilita esta opción en un solo dispositivo, solamente ese dispositivo enviará los mensajes de conexión persistente.*

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Cuando termine de configurar la HA en ambos cortafuegos, verifique que los dispositivos están emparejados en la HA activo/pasivo.

1. Acceda al **Panel** de ambos dispositivos y visualice el widget de Alta disponibilidad.
2. En el par de HA activo, haga clic en **Sincronizar con el par**.
3. Confirme que los cortafuegos estén emparejados y sincronizados.
   - En el cortafuegos pasivo: el estado del cortafuegos local debería mostrar **Pasivo** y la **Config. en ejecución** debería mostrar como sincronizada.
   - En el cortafuegos activo: el estado del cortafuegos local debe mostrar **Activo** y la **Config. en ejecución** debe aparecer como Sincronizada.
4. Desde la interfaz de línea de comandos del cortafuegos, ejecute los siguientes comandos:
   - Para verificar la disposición de la conmutación por error:

     ```
     show plugins vm_series aws ha state
     ```
   - Para mostrar la asignación de IP secundaria:

     ```
     show plugins vm_series aws ha ips
     ```

Configuración de HA activa/pasiva en AWS mediante Interface Move

Complete el siguiente procedimiento para configurar HA activo-pasivo usando el modo de movimiento de interfaz.

STEP 1 | Asegúrese de cumplir los requisitos previos.

Para implementar un par de cortafuegos VM-Series en HA en la nube de AWS, debe asegurarse de lo siguiente:

- Seleccione la función de IAM que creó al iniciar el cortafuegos VM-Series en una instancia de EC2; no puede asignar la función a una instancia que ya se esté ejecutando. Consulte Roles de IAM para HA.

  Para obtener instrucciones detalladas sobre cómo crear un rol de IAM, cómo definir qué cuentas o servicios de AWS pueden asumir el rol y cómo definir qué acciones y recursos de API puede usar la aplicación después de asumir el rol, consulte la documentación de AWS

  .
- DPDK no es compatible con el cortafuegos VM-Series en AWS en una implementación de HA de movimiento de interfaz. Si tiene el complemento VM-Series 2.0.1 o posterior en sus cortafuegos, debe desactivar DPDK.

  La desactivación de DPDK requiere que el cortafuegos se reinicie. Si está utilizando bootstrapping para implementar el cortafuegos VM-Series, puede evitar reiniciar el cortafuegos mediante la

 ©2024 Palo Alto Networks, Inc.

deshabilitación de DPDK en el archivo initi-cfg.txt utilizando **`op-cmd-dpdk-pkt-io=off`**. Consulte Arranque del cortafuegos VM-Series en AWS para obtener más información.

- El cortafuegos activo en el par de alta disponibilidad (HA) debe tener como mínimo tres ENI: dos interfaces del plano de datos y una interfaz de administración.

  El cortafuegos pasivo en el par de alta disponibilidad debe tener un ENI para la administración y un ENI que funcione como interfaz del plano de datos; se configurará la interfaz del plano de datos como una interfaz de ha2.

  No conecte interfaces del plano de datos adicionales al cortafuegos pasivo en el par de alta disponibilidad. En una conmutación por error, las interfaces del plano de datos del cortafuegos anteriormente activo se mueven (se desasocian y luego se adjuntan) al cortafuegos ahora activo (anteriormente pasivo).

- Los peers de HA deben implementarse en la misma zona de disponibilidad de AWS. Si bien VM-Series HA en Zonas de disponibilidad en AWS no es una solución recomendada, es compatible.

STEP 2 | Inicio del cortafuegos VM-Series en AWS.

STEP 3 | (Complemento VM-Series 2.0.1 o posterior) Deshabilite DPDK en los cortafuegos activo y pasivo. DPDK está habilitado de forma predeterminada y el modo HA de movimiento de interfaz no es compatible con DPDK, por lo que debe deshabilitarlo; habilitando el paquete MMAP.

1. Inicie sesión en la CLI del cortafuegos pasivo.
2. Deshabilite DPDK usando el siguiente comando. La ejecución de este comando reinicia el cortafuegos.

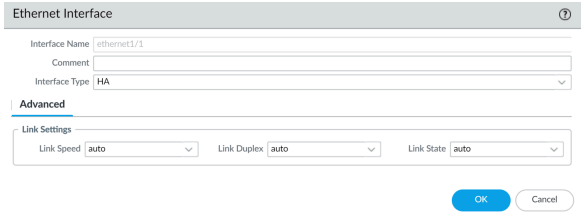
   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

STEP 4 | Habilitar HA.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la sección Setup (Configuración).
2. Seleccione **Enable HA (Habilitar HA)**.

STEP 5 | Configure ethernet 1/1 como una interfaz de HA. Esta interfaz debe utilizarse para la comunicación de HA2.

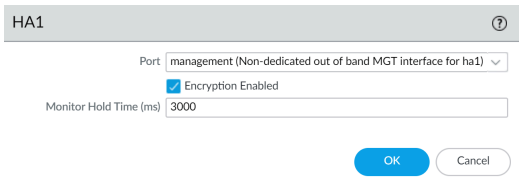
1. Seleccione **Network (Red)** > **Interfaces**.
2. Confirme que el enlace esté en estado activo en ethernet1/1.
3. Haga clic en el enlace para ethernet1/1 y configure el **Interface Type (Tipo de interfaz)** a HA.



 ©2024 Palo Alto Networks, Inc.

STEP 6 | Configure el Enlace de control (HA1) para usar el puerto de gestión.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la sección Control Link (HA1) (Enlace de control).

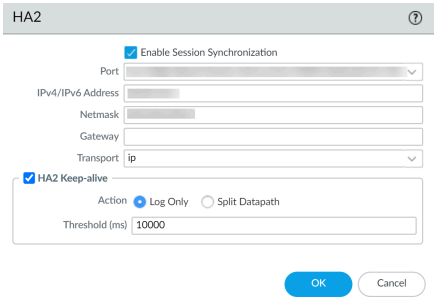


2. (Opcional) Seleccione **Encryption Enabled (Cifrado habilitado)** para proteger la comunicación de HA entre los peers. Para habilitar el cifrado, debe exportar la clave de HA desde un dispositivo e importarla al dispositivo peer.

   1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **Certificates (Certificados)**.
   2. Seleccione **Export HA key (Exportar clave de HA)**. Guarde la clave de HA en una ubicación de red a la que pueda acceder el dispositivo peer.
   3. En el dispositivo peer, desplácese hasta **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** y seleccione **Import HA key (Importar clave de HA)** para desplazarse hasta la ubicación donde guardó la clave e importarla en el dispositivo peer.

STEP 7 | Configure el Enlace de datos (HA2) para usar ethernet1/1.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite la sección Enlace de datos (HA2).
2. Seleccione el **Port (Puerto)** ethernet1/1.
3. Introduzca la dirección IP para ethernet1/1. Esta dirección IP debe ser la misma que asignó a la ENI en el panel EC2.
4. Introduzca la **Netmask (Máscara de red)**.
5. Introduzca una dirección IP de **Gateway (Puerta de enlace)** si las interfaces de HA1 están en subredes separadas.
6. Seleccione **IP** o **UDP** para **Transport (Transporte)**. Utilice **IP** si necesita transporte de Capa 3 (número de protocolo de IP 99). Utilice **UDP** si desea que el cortafuegos calcule la suma de comprobación de todo el paquete y no solamente el encabezado, como en la opción IP (puerto UDP 29281).



7. (Opcional) Modifique el **Threshold (Umbral)** para los paquetes **HA2 Keep-alive (Conexión persistente de HA2)**. De manera predeterminada, **HA2 Keep-alive (Conexión persistente de HA2)** Conexión persistente de HA2) está habilitada para la supervisión del enlace de datos

 ©2024 Palo Alto Networks, Inc.

de HA2 entre los peers. Si ocurre un fallo y se supera este umbral (el valor predeterminado es 10000 ms), se producirá la acción definida. Se generará un mensaje de log de sistema crítico cuando se produzca un fallo de conexión persistente de HA2.

> *Puede configurar la opción **HA2 keep-alive (Conexión persistente de HA2)** en ambos dispositivos o solamente un dispositivo del par de HA. Si habilita esta opción en un solo dispositivo, solamente ese dispositivo enviará los mensajes de conexión persistente.*

STEP 8 | Establezca la prioridad de dispositivo y habilite la preemption.

Utilice esta configuración si desea asegurarse de que un dispositivo específico es el dispositivo activo preferido. Para obtener más información, consulte Prioridad de dispositivo y preferencia.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la sección Election Settings (Configuración de elección).
2. Establezca el valor numérico de **Device Priority (Prioridad de dispositivo)**. Asegúrese de establecer un valor numérico más bajo en el dispositivo al que desee asignar una mayor prioridad.

   > *Si ambos cortafuegos tienen el mismo valor de prioridad de dispositivo, el cortafuegos con la dirección MAC más baja en el enlace de control de HA1 será el dispositivo activo.*
3. Seleccione **Preemptive (Preferente)**.

   Debe habilitar la preferencia tanto en el dispositivo activo como en el pasivo.
4. Modifique los temporizadores de conmutación por error. De manera predeterminada, el perfil del temporizador de HA se establece como el perfil **Recommended (Recomendado)** y es adecuado para la mayoría de implementaciones de HA.

STEP 9 | (Opcional) Modifique el tiempo de espera antes de que se active la conmutación por error.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la Configuración Activa/Pasiva.
2. Modifique el **Monitor fail hold up time (Tiempo de espera ascendente tras fallo de supervisor)** a un valor entre 1 y 60 minutos; el valor predeterminado es 1 minuto. Este es el intervalo de tiempo durante el cual el cortafuegos permanecerá activo después de un fallo de enlace. Use esta configuración para evitar una conmutación por error de HA iniciada por flaps ocasionales de los dispositivos vecinos.

STEP 10 | Configuración de la dirección IP del peer de HA.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la sección Setup (Configuración).
2. Introduzca la dirección IP del puerto de HA1 en el peer. Esta es la dirección IP asignada a la interfaz de gestión (ethernet 0/0), que también es el enlace de HA1 en el otro cortafuegos.
3. Configure el número de **Group ID (ID de grupo)** entre 1 y 63. A pesar de que este valor no se utiliza en el cortafuegos VM-Series en AWS, no puede dejar el campo en blanco.

STEP 11 | Configure el otro peer.

Repita los pasos del 3 al 9 en el peer de HA.

 ©2024 Palo Alto Networks, Inc.

STEP 12 | Cuando termine de configurar ambos dispositivos, verifique que los dispositivos están emparejados en la HA activa/pasiva.

1. Acceda a **Dashboard (Panel)** de ambos dispositivos y visualice el widget **High Availability (Alta disponibilidad)**.
2. En el dispositivo activo, haga clic en el enlace **Sync to peer (Sincronizar en el peer)**.
3. Confirme que los dispositivos están emparejados y sincronizados, como se muestra a continuación:
   - En el dispositivo pasivo: El estado del dispositivo local debería mostrarse como **passive (pasivo)** y la configuración está **synchronized (sincronizada)**.
   - En el dispositivo activo: El estado del dispositivo local debería mostrarse como **active (activo)** y la configuración está **synchronized (sincronizada)**.

STEP 13 | Verifique que la conmutación por error se produzca de manera correcta.

1. Verifique el modo HA.

   ```
   show plugins vm_series aws ha failover-mode
   ```
2. Verifique que el modo de E/S de paquetes esté configurado para MMAP de paquetes.

   ```
   show system setting dpdk-pkt-io
   ```
3. Apague el peer de HA activo.
   1. En el panel EC2, seleccione **Instances (Instancias)**.
   2. En la lista, seleccione el cortafuegos VM-Series y haga clic en **Actions (Acciones)** > **Stop (Detener)**.
4. Verifique que el peer pasivo asuma la función de peer activo y que las interfaces del plan de datos se movieron al peer de HA ahora activo.

Migración de HA activa/pasiva en AWS

Ambos modos de alta disponibilidad son compatibles, lo que le permite migrar entre cada modo si su implementación lo requiere. Debido a que el modo de movimiento de interfaz no es compatible con DPDK, debe deshabilitarlo en el cortafuegos VM-Series antes de completar la migración. La desactivación de DPDK requiere que reinicie el cortafuegos VM-Series, lo que afectará cualquier sesión de tráfico en el cortafuegos activo.

- Migración de HA activa/pasiva en AWS al modo de IP secundaria
- Migración de HA activa/pasiva en AWS al modo Interface Move

Migración de HA activa/pasiva en AWS al modo de IP secundaria

Complete el siguiente procedimiento para migrar su par de HA de cortafuegos VM-Series existente de HA de movimiento de interfaz a HA de IP secundaria.

La HA de cambio de IP secundaria requiere el complemento VM-Series 2.0.1 o posterior.

STEP 1 | Actualización del plugin de VM-Series en el par HA pasivo y luego en el par activo.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Cree una dirección IP secundaria para todas las interfaces de datos en el par activo.

1. Inicie sesión en la consola EC2 de AWS.
2. Seleccione **Network Interface (Interfaz de red)** y luego seleccione su interfaz de red.
3. Seleccione **Actions (Acciones)** > **Manage IP Addresses (Administrar direcciones IP)** > **IPv4 Addresses (Direcciones IPv4)** > **Assign new IP (Asignar nueva IP)**.
4. Deje el campo en blanco para permitir que AWS asigne una dirección IP dinámicamente o introduzca una dirección IP dentro del rango de subred para el cortafuegos VM-Series.
5. Haga clic en **Yes (Sí)** y **Update (Actualizar)**.

STEP 3 | Asocie una dirección IP elástica secundaria (pública) con la interfaz no trust del par activo.

1. Inicie sesión en la consola EC2 de AWS.
2. Seleccione **Elastic IPs (IP elásticas)** y luego elija la Dirección de IP elástica para asociar.
3. Seleccione **Actions (Acciones)** > **Associate Elastic IP (Asociar IP elástica)**.
4. En **Resource Type (Tipo de recurso)**, seleccione **Network Interface (Interfaz de red)**.
5. Seleccione la interfaz de red con la que asociar la Dirección IP elástica.
6. Haga clic en **Associate (Asociar)**.

STEP 4 | Cree una tabla de enrutamiento que apunte a la subred que contiene la interfaz trust.

1. Seleccione **Route Tables (Tablas de enrutamiento)** > **Create route table (Crear tabla de enrutamiento)**.
2. (Opcional) Introduzca una **Name tag (Etiqueta de nombre)** descriptiva para su tabla de enrutamiento.
3. Seleccione su**VPC**.
4. Haga clic en **Create (Crear)**.
5. Seleccione **Subnet Associations (Asociaciones de subred)** > **Edit subnet associations (Editar asociaciones de subred)**.
6. Seleccione la casilla de verificación **Associate (Asociar)** para la subred que contiene la interfaz trust.
7. Haga clic en **Save (Guardar)**.

STEP 5 | Actualice las funciones de IAM con acciones y permisos adicionales necesarios para migrar a HA de movimiento de IP secundaria.

Acción, permiso o recurso de IAM	Description (Descripción)
AssociateAddress	Para obtener permisos para mover direcciones IP públicas asociadas con las direcciones IP primarias de la interfaz pasiva a la activa.
AssignPrivateIpAddresses	Para obtener permisos para mover direcciones IP secundarias y direcciones IP públicas asociadas de la interfaz pasiva a la activa.

 ©2024 Palo Alto Networks, Inc.

Acción, permiso o recurso de IAM	Description (Descripción)
UnassignPrivateIpAddress	Para permisos para anular la asignación de direcciones IP secundarias y direcciones IP públicas asociadas de interfaces en el par activo.
DescribeRouteTables	Para obtener permiso para recuperar todas las tablas de enrutamiento asociadas a las instancias del cortafuegos VM-Series.
ReplaceRoute	Para obtener permiso para actualizar las entradas de la tabla de enrutamiento de AWS.
GetPolicyVersion	Para obtener permiso para recuperar información sobre la versión de la política de AWS.
GetPolicy	Para obtener permiso para recuperar información sobre políticas de AWS.
ListAttachedRolePolicies	Para obtener permiso para recuperar la lista de todas las políticas administradas adjuntas a un rol de IAM específico.
ListRolePolicies	Para obtener permiso para recuperar una lista de los nombres de las políticas en línea integradas en un rol de IAM específico.
GetRolePolicy	Para obtener permiso para recuperar una política en línea especificada incrustada en una función de IAM especificada.
política	Para obtener permiso para acceder al Nombre de recurso de Amazon (ARN) de la política de IAM.
función	Para obtener permiso para acceder al ARN de las funciones de IAM.
tabla de enrutamiento	Para obtener permiso para acceder al ARN de la tabla de enrutamiento.
Comodín (*)	En el campo ARN use * como comodín.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Cree nuevas interfaces (ENI) en el cortafuegos pasivo en la misma subred que las interfaces de datos del cortafuegos activo.

No asigne direcciones IP secundarias a estas nuevas interfaces.

1. Abra la consola de Amazon EC2.
2. Seleccione **Network Interfaces (Interfaces de red)** > **Create Network Interfaces (Crear interfaces de red)**.
3. Introduzca un **Name (Nombre)** descriptivo para su nueva interfaz.
4. En **Subnet (Subred)**, seleccione la subred de la interfaz untrust del cortafuegos activo.
5. En **Private IP (IP privada)**, deje el campo en blanco para permitir que AWS asigne una dirección IP de forma dinámica o introduzca una dirección IP dentro del rango de subred para la interfaz untrust del cortafuegos activo.
6. En **Security groups (Grupos de seguridad)**, seleccione uno o más grupos de seguridad.
7. Seleccione **Yes (Sí)** y **Create (Crear)**.
8. Seleccione **Actions (Acciones)** > **Change Source/Dest. Check (Cambiar comprobación de origen/destino)** y seleccione **Disable (Desactivar)**.
9. Repita estos pasos para la subred de la interfaz trust del cortafuegos activo.

STEP 7 | Adjunte las nuevas ENI a la instancia de cortafuegos pasivo. Debe adjuntar estas ENI al cortafuegos pasivo en el orden correcto porque el método de HA de IP secundaria se basa en el índice de interfaz de red asignado por AWS. Por ejemplo, si eth1/2 en el cortafuegos activo es parte de la subred A y eth1/3 es parte de la subred B, entonces debe conectar la interfaz que es parte de la subred A y la interfaz que es parte de la subred B. En este ejemplo, AWS ha asignado un valor de índice de 2 a eth1/2 y un valor de 3 a eth1/3. Esta indexación debe mantenerse para que la conmutación por error se produzca correctamente.

1. Para adjuntar las ENI creadas anteriormente, seleccione la interfaz untrust que creó y haga clic en **Attach (Adjuntar)**.
2. Seleccione el ID de instancia del cortafuegos pasivo y haga clic en **Attach (Adjuntar)**.
3. Repita estos pasos para la interfaz trust.

STEP 8 | Inicie sesión en la interfaz pasiva y configure las interfaces para obtener sus direcciones IP a través de DHCP.

1. Inicie sesión en la interfaz web del cortafuegos VM-series pasivo.
2. Seleccione **Network (Red)** > **Interfaces**.
3. Haga clic en la primera interfaz de datos.
4. Seleccione **IPv4**.
5. Seleccione **DHCP Client (Cliente DHCP)**.
6. Solo en la interfaz untrust, seleccione **Automatically create default route pointing to default gateway provided by server (Crear ruta predeterminada automáticamente que apunte a la puerta de enlace predeterminada proporcionada por el servidor)**.
7. Haga clic en OK (Aceptar).
8. Repita este proceso para cada interfaz de datos.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Si ha configurado políticas de NAT en el cortafuegos VM-Series que hacen referencia a las direcciones IP privadas de las interfaces de datos, esas políticas deben actualizarse para hacer referencia a las direcciones IP secundarias recién asignadas.

1. Acceda a la interfaz web del cortafuegos VM-Series activo.
2. Seleccione **Policies (Políticas)** > **NAT**.
3. Haga clic en la regla de política de NAT que desea modificar y luego en **Translated Packet (Paquete traducido)**.
4. En **Translated Address (Dirección traducida)**, haga clic en Añadir e introduzca la dirección IP secundaria creada en AWS.
5. Elimine la dirección IP principal.
6. Haga clic en **OK (Aceptar)**.
7. Repita estos pasos según sea necesario.
8. Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 10 | Habilite el modo de conmutación por error de HA de IP secundaria.

1. Acceda a la CLI del cortafuegos VM-Series en el par activo.
2. Ejecute el siguiente comando.

   ```
   request plugins vm_series aws ha failover-mode secondary-ip
   ```
3. Confirme los cambios.
4. Confirme su modo HA ejecutando el siguiente comando.

   ```
   show plugins vm_series aws ha failover-mode
   ```
5. Repita este comando en el par pasivo.

STEP 11 | Cuando termine de configurar la HA en ambos cortafuegos, verifique que los dispositivos están emparejados en la HA activo/pasivo.

1. Acceda al **Panel** de ambos dispositivos y visualice el widget de Alta disponibilidad.
2. En el par de HA activo, haga clic en **Sincronizar con el par**.
3. Confirme que los cortafuegos estén emparejados y sincronizados.
   - En el cortafuegos pasivo: el estado del cortafuegos local debería mostrar **Pasivo** y la **Config. en ejecución** debería mostrar como sincronizada.
   - En el cortafuegos activo: el estado del cortafuegos local debe mostrar **Activo** y la **Config. en ejecución** debe aparecer como Sincronizada.
4. Desde la interfaz de línea de comandos del cortafuegos, ejecute los siguientes comandos:
   - Para verificar la disposición de la conmutación por error:

     ```
     show plugins vm_series aws ha state
     ```
   - Para mostrar la asignación de IP secundaria:

     ```
     show plugins vm_series aws ha ips
     ```

 ©2024 Palo Alto Networks, Inc.

Migración de HA activa/pasiva en AWS al modo Interface Move

Complete el siguiente procedimiento para migrar su par de HA de cortafuegos VM-Series existente de HA de IP secundaria a HA de movimiento de interfaz.

STEP 1 | Deshabilite la compatibilidad con DPDK en el par HA pasivo. El modo HA de movimiento de interfaz no admite DPDK, por lo que se debe desactivar; habilitando el paquete MMAP.

1. Inicie sesión en la CLI del cortafuegos pasivo.
2. Deshabilite DPDK usando el siguiente comando. La ejecución de este comando reinicia el cortafuegos.

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

STEP 2 | Desactive la compatibilidad con DPDK en el par HA activo.

1. Inicie sesión en la CLI del cortafuegos activo.
2. Deshabilite DPDK usando el siguiente comando. La ejecución de este comando reinicia el cortafuegos.

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

   El reinicio del cortafuegos afectará al tráfico.

STEP 3 | Cambie el modo HA en el par activo del modo de IP secundaria al modo de movimiento de interfaz.

1. Acceda a la CLI del cortafuegos VM-Series en el par activo.
2. Ejecute el siguiente comando.

   ```
   request plugins vm_series aws ha failover-mode interface-move
   ```
3. Confirme los cambios.
4. Confirme su modo HA ejecutando el siguiente comando.

   ```
   show plugins vm_series aws ha failover-mode
   ```
5. Repita este comando en el par pasivo.

STEP 4 | Elimine las interfaces de datos de la instancia de cortafuegos pasivo.

1. Inicie sesión en la consola EC2 de AWS.
2. Seleccione **Network Interfaces (Interfaces de red)**.
3. Seleccione una interfaz de datos en la instancia de cortafuegos pasivo y haga clic en **Delete (Eliminar)**.
4. En la ventana **Delete Network Interface (Eliminar interfaz de red)**, haga clic en **Yes, Delete (Sí, eliminar)**.
5. Repita este proceso para cada interfaz de datos en la instancia de cortafuegos pasivo.

 ©2024 Palo Alto Networks, Inc.

Utilice AWS Secrets Manager para almacenar certificados VM-Series

Puede integrar administradores de claves nativos de la nube para almacenar certificados. Las claves privadas utilizadas para los certificados no se almacenan en el disco duro de un cortafuegos, por lo que se eliminan los problemas de seguridad. Los administradores conservan los certificados y las claves privadas en el almacenamiento en la nube. El cortafuegos usa AWS Secrets Manager para recuperar los certificados y las claves privadas del almacenamiento en la nube y los utiliza para funciones como el descifrado e IPSec.

Solo se admiten los cortafuegos VM-Series para permitir la recuperación de certificados a través de AWS Secrets Manager. Si utiliza certificados de AWS Secrets Manager, no puede cambiar a una versión anterior de PAN-OS.

Para el descifrado de entrada y salida, cargue los certificados en el administrador de claves nativo y proporcione los permisos de acceso necesarios al NGFW.

Un cortafuegos NGFW en una nube pública puede usar AWS Secrets Manager para almacenar certificados. En tales casos, se configuran las políticas de gestión de acceso necesarias, utilizando PAN-OS o la CLI, para las mismas instancias.

Para entornos que utilizan el escalado automático, una instancia se inicia en un estado con los certificados necesarios recuperados y lista para descifrar el tráfico sin configuración manual adicional.

Cuando un certificado se actualiza en la nube, debe volver a importarse como un nuevo certificado en el cortafuegos. Deberá asignar funciones de IAM a una instancia para permitir que la instancia recupere certificados del almacén de AWS Secrets Manager. La función de IAM debe tener **Obtener** permiso para Secretos de AWS Secrets Manager.

Todos los certificados se eliminan cuando cambia una clave maestra y luego se vuelven a recuperan al confirmar. Cuando la configuración se sincroniza con el cortafuegos pasivo en alta disponibilidad (HA), el daemon de administración descarga automáticamente el certificado en el cortafuegos pasivo. Como resultado, el certificado en sí no está sincronizado.

STEP 1 | En la Consola de administración de AWS, cree una función de IAM o seleccione una función que se haya creado anteriormente. La función de IAM que utilice debe tener privilegios de lectura/escritura

STEP 2 | Seleccione la política de **IAM Role (Función de IAM)** en la sección **Instances (Instancias)** de la consola de AWS para ver el **Secrets Manager**.

STEP 3 | En la pestaña **Permissions (Permisos)**, seleccione **Secrets Manager**. Utilizará esta pantalla para ver las claves públicas y privadas.

STEP 4 | En la pantalla **Secrets (Secretos)**, seleccione el nombre del archivo de secretos asociado con la función de IAM.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | En el campo **Secret (Secreto)**, seleccione **Key/value (Clave/valor)** para mostrar la clave pública y privada. Ambas claves deberían ser iguales. Además, las claves públicas o privadas deben coincidir con el formato previsto por AWS en Secrets Manager. Si el formato no coincide, la recuperación de la clave falla.

La opción **Rotation configuration (Configuración rotación)** debe estar **Deshabilitada.** Esta característica no es compatible.

STEP 6 | Vuelva a su grupo de recursos y seleccione el cortafuegos VM-Series. Haga clic en **Identity (Identidad) > User Assigned (Asignada por el usuario)** y añada la **Managed Identity (Identidad gestionada)**.

STEP 7 | Vuelva a Secrets Manager y seleccione **Certificates (Certificados)**. Importe su certificado.

STEP 8 | Inicie sesión en al cortafuegos VM-Series.

STEP 9 | Seleccione **Device (Dispositivo) > Certificate Management (Gestión de certificados) > Certificates (Certificados) > Import (Importar)**.

STEP 10 | En **Cloud (Nube)**, introduzca el nombre del certificado y establezca el formato de archivo.

STEP 11 | Seleccione **Cloud (Nube)**, elija **AWS** en el menú desplegable **Cloud Platform (Plataforma en la nube)**:

1. Introduzca el **Certificate Name (Nombre del certificado)**; cópielo del campo **Certificate Name (Nombre del certificado)** en **AWS Secrets Manager > Secrets (Secretos)**.
2. Seleccione **AWS** para la **Cloud Platform (Plataforma en la nube)**.
3. Introduzca el **Cloud Secret Name (Nombre secreto de la nube)**; copie esto del campo **Secret name (Nombre secreto)** en **AWS Secrets Manager > Secrets (Secretos)**.
4. Puede especificar el **Algorithm (Algoritmo)** en la pantalla de **Información del certificado**. Seleccione el algoritmo para su configuración, ya sea **RSA** o **DSA de curva elíptica**. De forma predeterminada, el algoritmo está configurado para utilizar **RSA**. Configure el certificado para usar el **Certificado de reenvío fiable**, **Certificado de reenvío no fiable**o **CA raíz de confianza**. De forma alternativa, puede seleccionar todos los algoritmos para el certificado.
5. Haga clic en **OK (Aceptar)**.
6. Confirme los cambios.

 ©2024 Palo Alto Networks, Inc.

STEP 12 | Verifique que el certificado se haya añadido correctamente:

1. Seleccione **Device (Dispositivo) > Certificate Management (Gestión de certificados) > Certificates (Certificados)**.
2. Su nuevo certificado deberá aparecer en la lista.

Los detalles del certificado no se muestran en la pantalla **Certificates (Certificados)**

. Para ver esta información en la CLI, utilice el comando:

```
show shared certificate <cert-name>
```

Los detalles del certificado no se muestran en la pantalla **Certificates (Certificados)**

. Para ver esta información en la CLI, utilice el comando:

```
show shared certificate
```

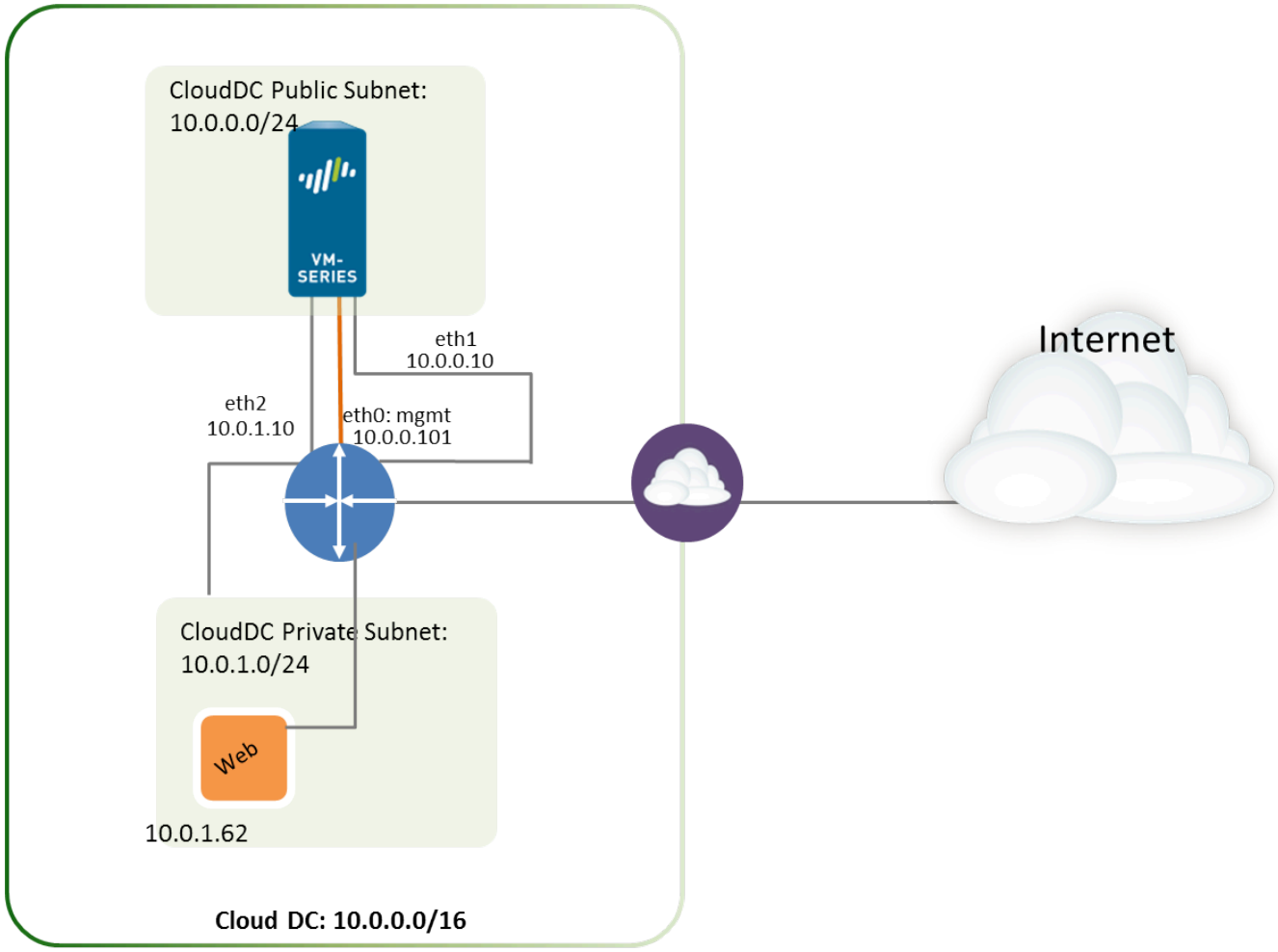
<cert-name>

Puede confirmar la configuración de la integración de certificados en Panorama. Utilice la ventana **Certificado de dispositivo** para determinar si se utiliza el certificado. Tenga en cuenta que debido a que los datos no se almacenan en la configuración en curso (el disco duro), todos los campos de la tabla **Certificados de dispositivos** están vacíos, excepto el campo **Uso** (si está configurado) y el **Nombre secreto de la nube**.

 ©2024 Palo Alto Networks, Inc.

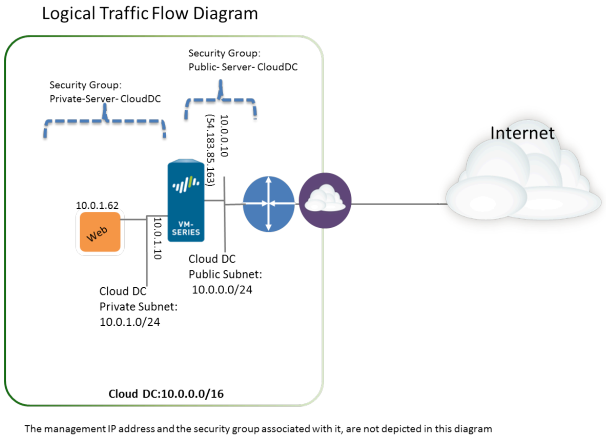
Caso de uso: Protección de las instancias de EC2 en AWS Cloud

En este ejemplo, la VPC se implementa en la red 10.0.0.0/16 con dos subredes /24: 10.0.0.0/24 y 10.0.1.0/24. El cortafuegos VM-Series se iniciará en la subred 10.0.0.0/24 a la que se ha adjuntado la puerta de enlace de internet. La subred 10.0.1.0/24 es una subred privada que alojará las instancias de EC2 que necesitan la protección del cortafuegos VM-Series; cualquier servidor en esta subred privada usa NAT para una dirección IP enrutable (que es una dirección IP elástica) para acceder a internet. Use la Hoja de trabajo para la planificación de VM-Series en la VPC de AWS para planificar el diseño de la VPC; la grabación de los intervalos de subred, las interfaces de red y las direcciones IP asociadas para las instancias de EC2 y los grupos de seguridad facilitará y optimizará el proceso de configuración.



La siguiente imagen ilustra el flujo lógico de tráfico hacia y desde el servidor web a internet. El tráfico hacia y desde el servidor web se envía a la interfaz de datos del cortafuegos VM-Series adjunto a la subred privada. El cortafuegos aplica políticas y procesos de tráfico entrante y saliente hacia y desde la puerta de enlace de internet del VPC. La imagen muestra también los grupos de seguridad adjuntos a las interfaces de datos.

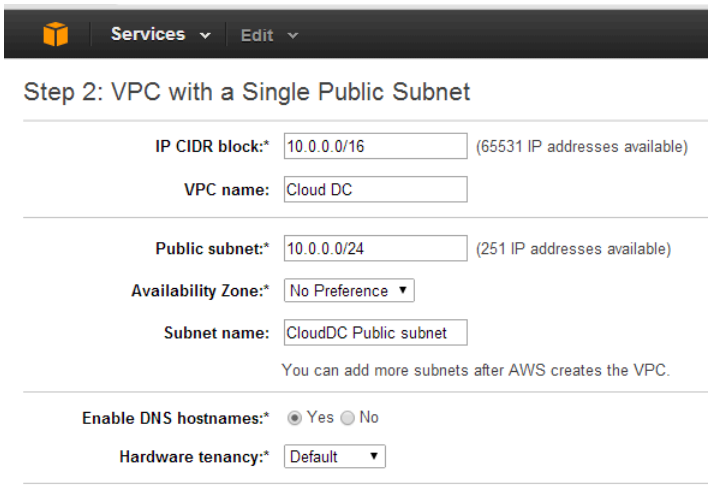
 ©2024 Palo Alto Networks, Inc.



STEP 1 | Cree una nueva VPC con una subred pública (o seleccione una VPC existente).

1. Inicie sesión en la consola de AWS y seleccione el panel **VPC**.
2. Compruebe que ha seleccionado el área geográfica correcta (región de AWS). La VPC se implementará en la región seleccionada actualmente.
3. Seleccione **Start VPC Wizard (Iniciar asistente de VPC)** y seleccione **VPC with a Single Public Subnet (VPC con una subred pública sencilla)**.

   En este ejemplo, el bloque CIDR de IP para la VPC es 10.0.0.0/16, el nombre de la VPC es Cloud DC, la subred pública es 10.0.0.0/24 y el nombre de la subred es Cloud DC Public subnet. Creará una subred privada después de crear la VPC.



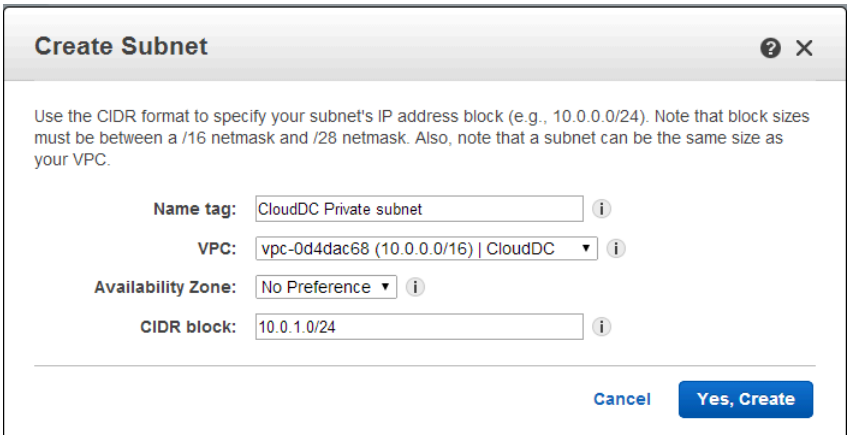
4. Haga clic en **Create VPC (Crear VPC)**.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Cree una subred privada.

Seleccione **Subnets (Subredes)** y haga clic en **Create a Subnet (Crear una subred)**. Introduzca la información.

En este ejemplo, **Name tag (Etiqueta de nombre)** para la subred es Web/DB Server Subnet, se crea en la VPC del Cloud Datacenter y se asigna un bloque CIDR de 10.0.1.0/24.



 ©2024 Palo Alto Networks, Inc.

STEP 3 | Cree una nueva tabla de enrutamiento para cada subred.

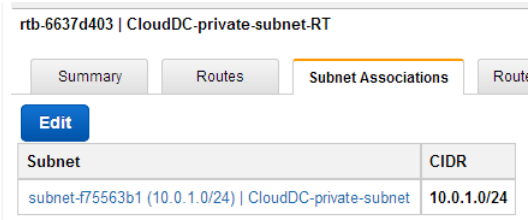
Aunque se crea automáticamente una tabla de enrutamiento en la VPC, recomendamos crear nuevas tablas de enrutamiento en lugar de modificar la tabla de enrutamiento predeterminada.

Para dirigir el tráfico saliente desde cada subred, en un punto posterior de este flujo de trabajo añadirá las rutas a la tabla de enrutamiento asociada a cada subred.

1. Seleccione **Route Tables (Tablas de enrutamiento)** > **Create Route Table (Crear tabla de enrutamiento)**.
2. Añada un nombre en **Name (Nombre)**, por ejemplo, CloudDC-public-subnet-RT, seleccione la **VPC** que creó en el Paso 1 y haga clic en **Yes, Create (Sí, crear)**.
3. Seleccione la tabla de enrutamiento, haga clic en **Subnet Associations (Asociaciones de subred)** y seleccione la subred pública.



4. Seleccione **Create Route Table (Crear tabla de enrutamiento)**.
5. Añada un nombre en **Name (Nombre)**, por ejemplo, CloudDC-private-subnet-RT, seleccione la **VPC** que creó en el Paso 1 y haga clic en **Yes, Create (Sí, crear)**.
6. Seleccione la tabla de enrutamiento, haga clic en **Subnet Association (Asociaciones de subred)** y seleccione la subred privada.



STEP 4 | Cree grupos de seguridad para restringir el acceso a internet entrante/saliente a las instancias de EC2 en la VPC.

De manera predeterminada, AWS no permite la comunicación entre interfaces que no pertenezcan al mismo grupo de seguridad.

Seleccione **Security Groups (Grupos de seguridad)** y haga clic en el botón **Create Security Group (Crear grupo de seguridad)**. En este ejemplo, hemos creado tres grupos de seguridad con las siguientes reglas para acceso entrante:

- CloudDC-Management, que especifica los protocolos y las direcciones IP de origen que pueden conectarse a la interfaz de gestión en el cortafuegos VM-Series. Necesita SSH y HTTPS como

 ©2024 Palo Alto Networks, Inc.

mínimo. En este ejemplo, se habilitan SSH, ICMP, HTTP y HTTPS en las interfaces de red adjuntas a este grupo de seguridad.

La interfaz de gestión (eth 0/0) del cortafuegos VM-Series se asignará a CloudDC-management-sg.

- Public-Server-CloudDC, que especifica las direcciones IP que se pueden conectar a través de HTTP, FTP y SSH en la VPC. Este grupo permite el tráfico desde la red externa al cortafuegos.

  La interfaz del plano de datos eth 1/1 del cortafuegos VM-Series se asignará a Public-Server-CloudDC.

- Private-Server-CloudDC, con acceso muy limitado. Sólo permite que las instancias de EC2 en la misma subred se comuniquen entre sí y con el cortafuegos VM-Series.

  La interfaz del plano de datos eth1/2 del cortafuegos VM-Series y la aplicación en la subred privada se adjuntarán a este grupo de seguridad.

  La siguiente captura de pantalla muestra los grupos de seguridad para este caso de uso.

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 | Implemente el cortafuegos VM-Series.

Sólo la interfaz de red principal que actuará como la interfaz de gestión se adjuntará y configurará para el cortafuegos durante el primer inicio. Las interfaces de red necesarias para la gestión del tráfico de datos se añadirán en el Paso 6.

Ver Paso 3 en Inicio del cortafuegos VM-Series en AWS.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Cree y adjunte las interfaces de red virtual, denominadas interfaces de red elásticas (ENI), al cortafuegos VM-Series. Estas ENI se usan para la gestión del tráfico de datos desde o hacia el cortafuegos.

1. En el panel EC2, seleccione **Network Interfaces (Interfaces de red)** y haga clic en **Create Network Interface (Crear interfaz de red)**.
2. Introduzca un nombre descriptivo para la interfaz.
3. Seleccione la subred. Use el ID de subred para asegurarse de que ha seleccionado la subred correcta. Sólo puede adjuntar una ENI a una instancia en la misma subred.
4. Introduzca la dirección de **Private IP (IP privada)** que quiere asignar a la interfaz o seleccione **Auto-assign (Asignar automáticamente)** para asignar automáticamente una dirección IP dentro de las direcciones IP disponibles en la subred seleccionada.
5. Seleccione el **Security group (Grupo de seguridad)** para controlar el acceso a la interfaz de red.
6. Haga clic en **Yes, Create (Sí, crear)**.

   En este ejemplo, se crean dos interfaces con la siguiente configuración:

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

   - Para Eth1/1 (VM-Series-Untrust)
     - Subred: 10.0.0.0/24
     - IP privada:10.0.0.10
     - Grupo de seguridad: Servidor público CloudDC
   - Para Eth1/2 (VM-Series-Trust)
     - Subred: 10.0.1.0/24
     - IP privada: 10.0.1.10
     - Grupo de seguridad: Servidor privado CloudDC
7. Para adjuntar la ENI al cortafuegos VM-Series, seleccione la interfaz que acaba de crear y haga clic en **Attach (Adjuntar)**.



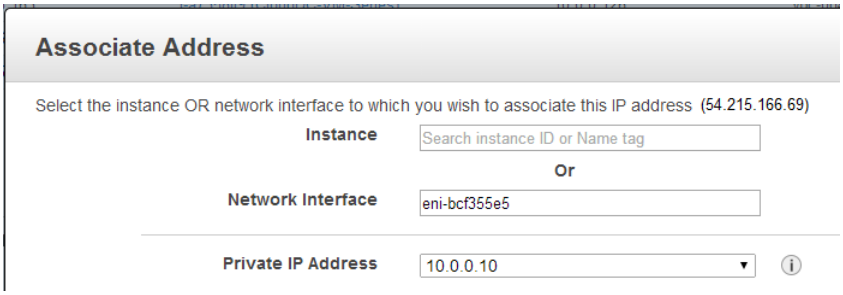
8. Seleccione el **Instance ID (ID de instancia)** del cortafuegos VM-Series y haga clic en **Attach (Adjuntar)**.
9. Repita los pasos 7 y 8 para adjuntar la otra interfaz de red.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Cree una dirección IP elástica y conéctela a la interfaz de red de plano de datos del cortafuegos que requiere acceso directo a internet.

En este ejemplo, VM-Series_Untrust se asigna a una EIP. La EIP asociada a la interfaz es la dirección IP de acceso público para el servidor web en la subred privada.

1. Seleccione **Elastic IP (IP elástica)** y haga clic en **Allocate New Address (Asignar nueva dirección)**.
2. Seleccione **EC2-VPC** y haga clic en **Yes, Allocate (Sí, asignar)**.
3. Seleccione la EIP recién asignada y haga clic en **Associate Address (Asociar dirección)**.
4. Seleccione la **Network Interface (Interfaz de red)** y **Private IP address (Dirección IP privada)** asociada con la interfaz y haga clic en **Yes, Associate (Sí, asociar)**.



En este ejemplo, la configuración es:

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-...

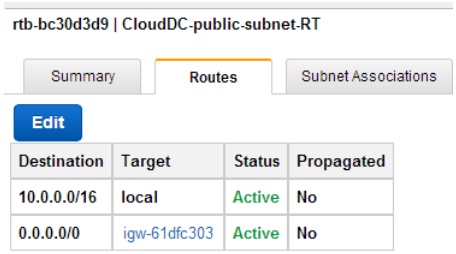
STEP 8 | Deshabilite la comprobación de Origen/Destino en cada interfaz de red adjuntada al cortafuegos VM-Series. Deshabilitar este atributo permite a la interfaz gestionar el tráfico de red no destinado a su dirección IP.

1. Seleccione la interfaz de red en la pestaña **Network Interfaces (Interfaces de red)**.
2. En el menú desplegable **Action (Acción)**, seleccione **Change Source/Dest. (Cambiar comprobación de origen/dest). Check (Comprobar)**.
3. Haga clic en **Disabled (Deshabilitado)** y en **Save (Guardar)** para guardar los cambios.
4. Repita los pasos 1-3 para interfaces de red adicionales, firewall-1/2 en este ejemplo.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | En la tabla de enrutamiento asociada a la subred pública (desde el paso 3), añada una ruta predeterminada a la puerta de enlace de internet para la VPC.

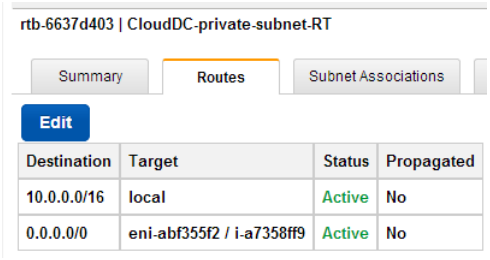
1. Desde el panel VPC, seleccione **Route Tables (Tablas de enrutamiento)** y busque la tabla de enrutamiento asociada a la subred pública.
2. Seleccione la tabla de enrutamiento, seleccione **Routes (Rutas)** y haga clic en **Edit (Editar)**.
3. Añada una ruta para reenviar paquetes desde esta subred a la puerta de enlace de internet. En este ejemplo, 0.0.0.0 indica que todo el tráfico desde o hacia esta subred usará la puerta de enlace de internet adjuntada a la VPC.



STEP 10 | En la tabla de enrutamiento asociada a la subred pública, añada una ruta predeterminada para enviar tráfico al cortafuegos VM-Series.

Añadir esta ruta permite el reenvío de tráfico desde instancias de EC2 en esta subred privada al cortafuegos VM-Series.

1. Desde el panel VPC, seleccione **Route Tables (Tablas de enrutamiento)** y busque la tabla de enrutamiento asociada a la subred privada.
2. Seleccione la tabla de enrutamiento, seleccione **Routes (Rutas)** y haga clic en **Edit (Editar)**.
3. Añada una ruta para reenviar paquetes desde esta subred a la interfaz de red del cortafuegos VM-Series que reside en la misma subred. En este ejemplo, 0.0.0.0/0 indica que todo el tráfico desde y hacia esta subred usará eni-abf355f2 (ethernet 1/2, que es CloudDC-VM-Series-Trust) en el cortafuegos VM-Series.



Por cada servidor web o de base de datos implementado en una instancia de EC2 en la subred privada, debe definir una ruta predefinida a la dirección IP del cortafuegos VM-Series de forma que el cortafuegos es la puerta de enlace predeterminada para el servidor.

Realice los pasos 11 a 16 en el cortafuegos VM-Series.

 ©2024 Palo Alto Networks, Inc.

STEP 11 | Configure una nueva contraseña de administración para el cortafuegos.

Se necesita una herramienta SSH como PuTTY para acceder a la CLI en el cortafuegos y cambiar la contraseña administrativa predeterminada. No puede acceder a la interfaz web hasta que haga SSH y cambie la contraseña predeterminada.

1. Use la dirección IP pública que ha configurado en el cortafuegos para hacer SSH en la interfaz de línea de comando (CLI) del cortafuegos VM-Series.

   Necesitará la clave privada que usó o creó en Inicio del cortafuegos serie VM en AWS, pasos 3-12 para acceder a la CLI.
2. Introduzca el siguiente comando para iniciar sesión en el cortafuegos:

   ssh-i <*private_key_name*> admin@<*public-ip_address*>
3. Configure una nueva contraseña usando el siguiente comando y siga las indicaciones en pantalla:

   configure

   set mgt-config users admin password

   commit
4. Finalice la sesión SSH.

STEP 12 | Acceda a la interfaz web del cortafuegos VM-Series.

Abra un navegador web e introduzca la EIP de la interfaz de gestión. Por ejemplo: https://54.183.85.163

STEP 13 | Active las licencias del cortafuegos VM-Series. Este paso solo se requiere para la licencia BYOL; las licencias basadas en uso se activan de manera automática.

Consulte Activación de la licencia.

 ©2024 Palo Alto Networks, Inc.

STEP 14 | En el cortafuegos VM-Series, configure las interfaces de red del plano de datos en el cortafuegos como interfaces de capa 3.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
2. Haga clic en el enlace de **ethernet 1/1** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **capa 3**
   - Seleccione la pestaña **Config (Configurar)** y asigne la interfaz al enrutador predeterminado.
   - En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione Nueva zona. Defina una zona nueva (p. ej., untrust) y, a continuación, haga clic en OK (Aceptar).
   - Seleccione IPv4, seleccione **DHCP Client (Cliente DHCP)**; la adquisición de la dirección IP privada que asignó a la interfaz de red en la consola de administración de AWS se realizará automáticamente.
   - En la pestaña **Advanced (Avanzada)** > **Other Info (Otra información)**, amplíe el menú desplegable Perfil de gestión y seleccione **New Management Profile (Nuevo perfil de gestión)**.
   - Introduzca un **Name (Nombre)** para el perfil, como allow_ping, y seleccione **Ping** en la lista de servicios permitidos; a continuación, haga clic en **OK (Aceptar)**.
   - Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.
3. Haga clic en el enlace de **ethernet 1/2** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **capa 3**
   - Seleccione la pestaña **Config (Configurar)** y asigne la interfaz al enrutador predeterminado.
   - En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. Defina una zona nueva (p. ej., trust) y, a continuación, haga clic en **OK** (Aceptar).
   - Seleccione **IPv4**, seleccione **DHCP Client (Cliente DHCP)**.
   - En la pestaña **IPv4**, anule la selección de la casilla de verificación **Automatically create default route to default gateway provided by server (Crear automáticamente ruta predeterminada a la puerta de enlace predeterminada proporcionada por el servidor)**. Para una interfaz adjuntada a la subred privada en la VPC, deshabilitar esta opción garantiza que el tráfico gestionado por esta interfaz no fluya directamente a la IGW en la VPC.
   - En **Advanced (Avanzada)** > **Other Info (Otra información)**, amplíe el menú desplegable Perfil de gestión y seleccione el perfil allow_ping que ha creado anteriormente.
   - Haga clic en **OK (Aceptar)** para guardar la configuración de interfaz.
4. Haga clic en **Commit (Confirmar)** para guardar los cambios. Verifique que el estado de enlace para la interfaz está en activo . Si el estado de enlace no está activo, reinicie el cortafuegos.

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

 ©2024 Palo Alto Networks, Inc.

STEP 15 | En el cortafuegos VM-Series, cree las reglas NAT de destino y NAT de origen para permitir el tráfico entrante y saliente desde y hacia las aplicaciones implementadas en la VPC.

1. Seleccione **Policies (Políticas)** > **NAT**.
2. Cree una regla NAT de destino que envíe el tráfico desde el cortafuegos hasta el servidor web.
   1. Haga clic en **Add (Añadir)** e introduzca un Nombre para la regla. Por ejemplo, NAT2WebServer.
   2. En la pestaña **Original Packet (Paquete original)**, realice las siguientes selecciones:
      - **Source Zone (Zona de origen)**: untrust (donde se origina el tráfico)
      - **Destination Zone (Zona de destino)**: untrust (la zona para la interfaz del plano de datos del cortafuegos con la que se asocia la EIP para el servidor web).
      - **Source Address (Dirección de origen)**: Cualquiera
      - **Destination Address (Dirección de destino)**: 10.0.0.10
      - En la pestaña **Translated Packet (Paquete traducido)**, seleccione la casilla de verificación Destination Address Translation (Traducción de dirección de destino) y

 ©2024 Palo Alto Networks, Inc.

establezca la **Translated Address (Dirección traducida)** a 10.0.1.62, que es la dirección IP privada del servidor web.

3. Haga clic en **OK (Aceptar)**.

			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. Cree una regla NAT de origen para permitir el acceso para el tráfico saliente desde el servidor web a internet.

   1. Haga clic en **Add (Añadir)** e introduzca un Nombre para la regla. Por ejemplo, NAT2External.
   2. En la pestaña **Original Packet (Paquete original)**, realice las siguientes selecciones:
      - **Source Zone** (Zona de origen): trust (donde se origina el tráfico)
      - **Destination Zone (Zona de destino)**: untrust (la zona para la interfaz del plano de datos del cortafuegos con la que se asocia la EIP para el servidor web).
      - **Source Address (Dirección de origen)**: Cualquiera
      - **Destination Address (Dirección de destino)**: Cualquiera
   3. En la pestaña **Translated Packet (Paquete traducido)**, seleccione lo siguiente en la sección Traducción de dirección de origen:
      - **Translation Type (Tipo de traducción)**: Dynamic IP and Port
      - **Tipo de dirección**: Dirección traducida
      - **Translated Address (Dirección traducida)**: 10.0.0.10 (la interfaz del plano de datos del cortafuegos en la zona no fiable.)
   4. Haga clic en **OK (Aceptar)**.

			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. Haga clic en **Commit (Confirmar)** para guardar las políticas NAT.

STEP 16 | En el cortafuegos VM-Series, cree políticas de seguridad para gestionar el tráfico.

En lugar de introducir una dirección IP estática para el servidor web, use un grupo de direcciones dinámicas. Los grupos de direcciones dinámicas le permiten crear políticas que se adapten automáticamente a los cambios, de modo que no tenga que actualizar la política cuando inicie los servidores web adicionales en la subred. Para obtener detalles, consulte Caso de uso: Uso de grupos de direcciones dinámicas para proteger las nuevas instancias de EC2 en la VPC.

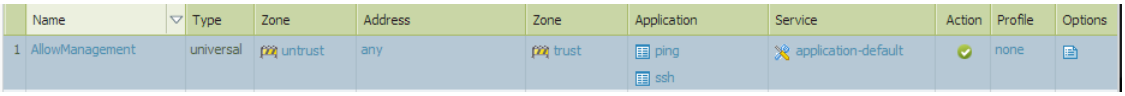
1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.

   En este ejemplo, tenemos cuatro reglas. Una regla que permite el acceso a la gestión del tráfico del cortafuegos, una regla que permite el tráfico entrante al servidor web, una tercera regla

 ©2024 Palo Alto Networks, Inc.

para permitir el acceso a internet al servidor web y en la última regla se modifica una regla predeterminada intrazona predefinida para registrar todo el tráfico denegado.

2. Cree una regla para permitir el acceso a la gestión al cortafuegos.
   1. Haga clic en **Add (Añadir)** e introduzca un nombre en **Name (Nombre)** para la regla. Compruebe que el **Rule Type (Tipo de regla)** es universal.
   2. En la pestaña **Source (Origen)**, seleccione untrust como la **Source Zone (Zona de origen)**.
   3. En la pestaña **Destination (Destino)**, añada trust como la **Destination Zone (Zona de destino)**.
   4. En la pestaña **Applications (Aplicaciones)**, **Add (Añada)** ping y ssh.
   5. En la pestaña **Actions (Acciones)**, establezca **Action (Acción)** como Allow (Permitir).
   6. Haga clic en **OK (Aceptar)**.



3. Cree una regla para permitir el tráfico entrante al servidor web.
   1. Haga clic en **Add (Añadir)** e introduzca en **Name (Nombre)** un nombre para la regla y verifique que **Rule Type (Tipo de regla)** es universal.
   2. En la pestaña **Source (Origen)**, seleccione untrust como la **Source Zone (Zona de origen)**.
   3. En la pestaña **Destination (Destino)**, añada trust como la **Destination Zone (Zona de destino)**.
   4. En la pestaña **Applications (Aplicaciones)**, haga clic en **Add** (Añadir) para añadir la navegación web.
   5. En la pestaña **Service/URL Category (Categoría de URL/servicio)**, compruebe que el servicio está establecido como predeterminado de la aplicación.
   6. En la pestaña **Actions (Acciones)**, establezca **Action (Acción)** como Allow (Permitir).
   7. En la sección Configuración de perfiles de la pestaña **Actions (Acciones)**, seleccione **Profiles (Perfiles)** y, a continuación, adjunte los perfiles predeterminados para antivirus, antispyware y protección contra vulnerabilidades.
   8. Haga clic en **OK (Aceptar)**.



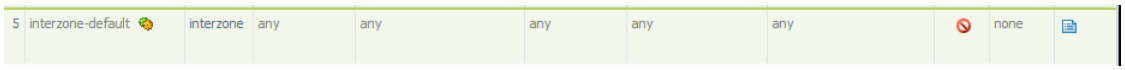
4. Cree una regla para permitir el acceso a internet al servidor web.
   1. Haga clic en **Add (Añadir)** e introduzca en **Name (Nombre)** un nombre para la regla y verifique que Rule Type (Tipo de regla) es universal.
   2. En la pestaña **Source** (Origen), seleccione trust como la **Source Zone (Zona de origen)**.
   3. En la sección Dirección de origen de la pestaña **Source (Origen)**, añada 10.0.1.62, la dirección IP del servidor web.
   4. En la pestaña **Destination (Destino)**, añada untrust como la **Destination Zone (Zona de destino)**.
   5. En la pestaña **Service/URL Category (Categoría de URL/servicio)**, compruebe que el servicio está establecido como **application-default (Predeterminado de la aplicación)**.
   6. En la pestaña **Actions (Acciones)**, establezca **Action (Acción)** como Allow (Permitir).

 ©2024 Palo Alto Networks, Inc.

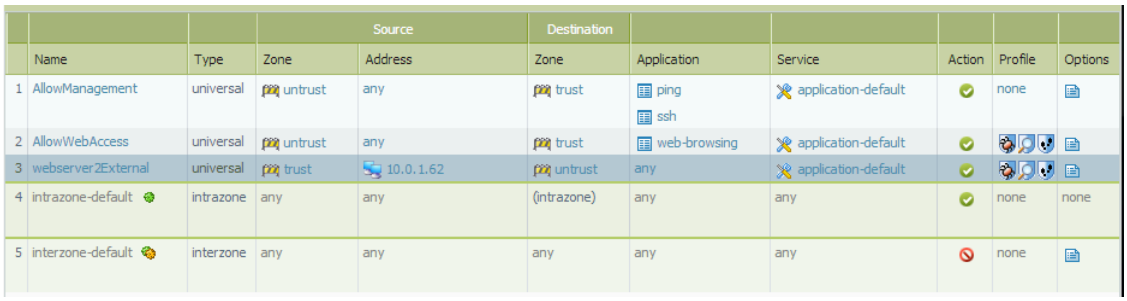
7. En la sección Configuración de perfiles de la pestaña **Actions (Acciones)**, seleccione **Profiles (Perfiles)** y, a continuación, adjunte los perfiles predeterminados para antivirus, antispyware y protección contra vulnerabilidades.
8. Haga clic en **OK (Aceptar)**.



5. Modifique la regla predeterminada entre zonas para registrar todo el tráfico denegado. Esta regla predeterminada entre zonas se evalúa cuando no se define explícitamente ninguna otra regla para buscar coincidencias de tráfico en zonas diferentes.
   1. Seleccione la regla **interzone-default** y haga clic en **Override (Cancelar)**.
   2. En la pestaña **Actions (Acciones)**, seleccione **Log at session end (Log al finalizar sesión)**.
   3. Haga clic en **OK (Aceptar)**.



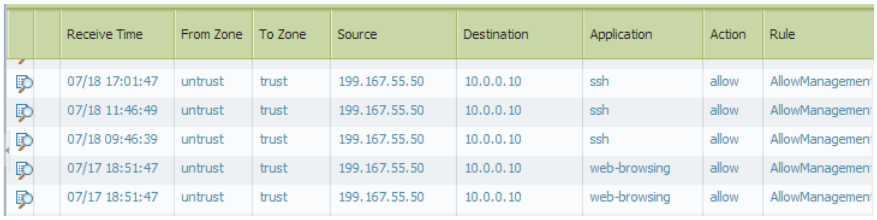
6. Revise el conjunto completo de reglas de seguridad definidas en el cortafuegos.
7. Haga clic en **Commit (Confirmar)** para guardar las políticas.



 ©2024 Palo Alto Networks, Inc.

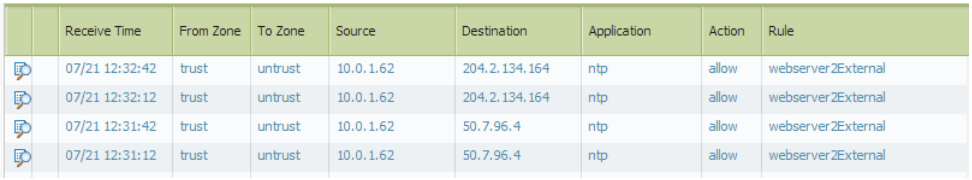
STEP 17 | Compruebe que el cortafuegos VM-Series está protegiendo el tráfico.

1. Inicie un navegador web e introduzca la dirección IP del servidor web.
2. Inicie sesión en la interfaz web del cortafuegos VM-Series y compruebe que puede ver los logs de tráfico de las sesiones en **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)**.
   - Tráfico entrante en el servidor web (llega a la instancia de EC2 en la VPC de AWS):



		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

   - Tráfico saliente del servidor web (instancia de EC2 en la VPC de AWS):



		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

   Ha implementado correctamente el cortafuegos VM-Series como una puerta de enlace de la nube.

 ©2024 Palo Alto Networks, Inc.

Caso de uso: Uso de grupos de direcciones dinámicas para proteger las nuevas instancias de EC2 en la VPC

En un entorno dinámico como la VPC de AWS, donde inicia las nuevas instancias de EC2 bajo demanda, la carga de trabajo administrativa de la gestión de la política de seguridad puede ser excesiva. El uso de grupos de direcciones dinámicas en la política de seguridad aporta agilidad y evita las interrupciones en los servicios o brechas en la protección.

En este ejemplo, puede usar la fuente de información de la VM en el cortafuegos para supervisar una VPC y usar grupos de direcciones dinámicas en la política de seguridad para detectar y proteger instancias EC2. Al iniciar las instancias de EC2, el grupo de direcciones dinámicas coteja las direcciones IP de todas las instancias que coinciden con los criterios definidos para la pertenencia al grupo y, a continuación, se aplica la política de seguridad del grupo. La política de seguridad en este ejemplo permite el acceso a internet a todos los miembros del grupo.

En lugar de usar la fuente de información de la VM en el cortafuegos, puede optar por usar Panorama como el punto central de comunicación con sus VPC. Usando el plugin de AWS en Panorama, puede recuperar la asignación de dirección IP a etiqueta y registrar la información en cortafuegos gestionados en los que configura notificaciones. Para obtener más detalles sobre esta opción, consulte Supervisión de VM con el plugin de AWS en Panorama.

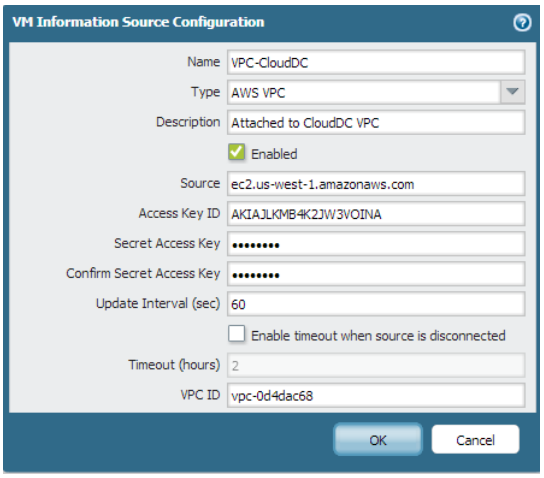
Este flujo de trabajo en la siguiente sección asume que ha creado la VPC de AWS e implementado el cortafuegos VM-Series y algunas aplicaciones en instancias EC2. Para obtener instrucciones sobre la configuración de la VPC para VM-Series, consulte Caso de uso: Protección de las instancias de EC2 en AWS Cloud.

STEP 1 | Configure el cortafuegos para supervisar la VPC.

1. Seleccione **Device (Dispositivo)** > **VM Information Sources (Fuentes de información de equipo virtual)**.
2. Haga clic en **Add (Añadir)** y especifique la siguiente información:
   1. Un **Name (Nombre)** para identificar la VPC que quiere supervisar. Por ejemplo, VPC-CloudDC.
   2. En **Type (Tipo)** establezca el tipo como VPC de AWS.
   3. En **Source (Origen)**, introduzca la URI de la VPC. La sintaxis es **`ec2.<your_region>.amazonaws.com`**
   4. Añada las credenciales necesarias para que el cortafuegos firme digitalmente las llamadas de la API realizadas por los servicios de AWS. Necesitará lo siguiente:
      - **Access Key ID (ID de clave de acceso)**: Introduzca la cadena de texto alfanumérico que identifica de forma exclusiva al usuario propietario o con autorización de acceso a la cuenta de AWS.
      - **Secret Access Key (Clave de acceso secreta)**: Introduzca la contraseña y confirme la entrada.
   5. (**Opcional**) Modifique el **Update interval (Intervalo de actualización)** a un valor entre 5-600 segundos. De manera predeterminada, el cortafuegos sondea cada 5 segundos.

 ©2024 Palo Alto Networks, Inc.

Las llamadas de la API se ponen en cola y recuperan cada 60 segundos, de modo que las actualizaciones pueden tardar hasta 60 segundos, más el intervalo de sondeo configurado.



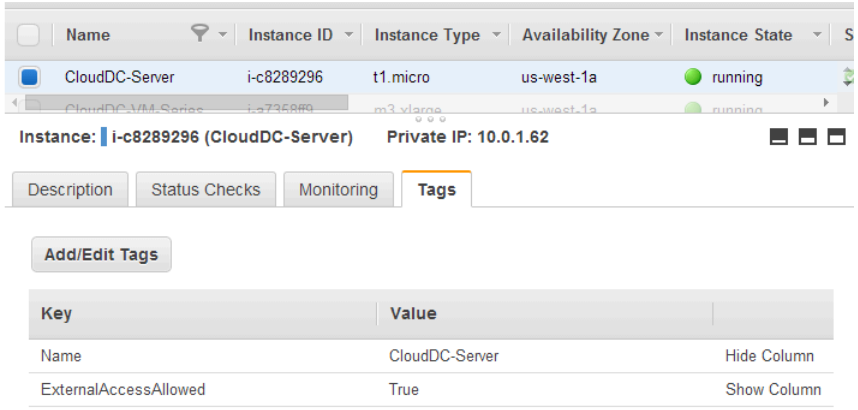
6. Introduzca el **VPC ID (ID de la VPC)** que se muestra en el panel VPC en la consola de administración de AWS.
7. Haga clic en **OK (Aceptar)** y seleccione **Commit (Confirmar)** los cambios.
8. Compruebe que el **Status (Estado)** de conexión aparezca como conectado

STEP 2 | Etiquete las instancias de EC2 en la VPC.

Para obtener una lista de etiquetas que el cortafuegos VM-Series puede supervisar, consulte Lista de atributos supervisados en la VPC de AWS.

Una etiqueta es un par nombre-valor. Puede etiquetar las instancias de EC2 en el panel EC2 de la consola de administración de AWS o usando la API de AWS o la CLI de AWS.

En este ejemplo, usamos el panel EC2 para añadir la etiqueta:

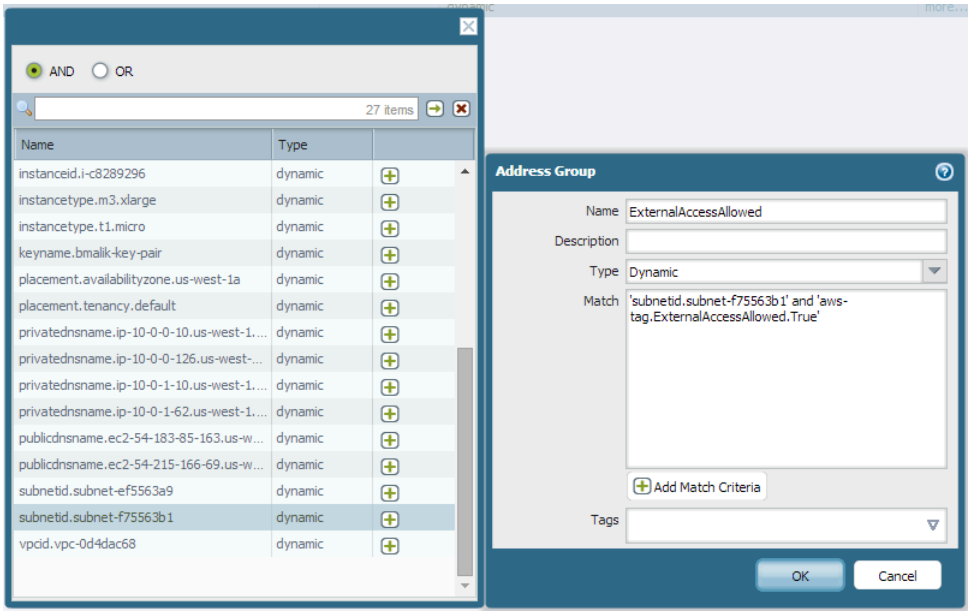


 ©2024 Palo Alto Networks, Inc.

STEP 3 | Cree un grupo de direcciones dinámicas en el cortafuegos.

Vea el tutorial para obtener información detallada de la función.

1. Seleccione **Object (Objeto)** > **Address Groups (Grupos de direcciones)**.
2. Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** y una **Description (Descripción)** para el grupo de direcciones.
3. Defina el **Type (Tipo)** como **Dynamic (Dinámico)**.
4. Defina los criterios de coincidencia.
   1. Haga clic en **Add Match Criteria (Añadir criterios de coincidencia)** y seleccione el operador **And (Y)**.
   2. Seleccione los atributos de filtrado o búsqueda de coincidencias. En este ejemplo, se selecciona la etiqueta ExternalAccessAllowed que acaba de crear y el ID de subred de la subred privada de la VPC.



5. Haga clic en **OK (Aceptar)**.
6. Haga clic en **Commit (Confirmar)**.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Uso del grupo de direcciones dinámicas en una política de seguridad.

Para crear una regla que permita el acceso a internet a cualquier servidor web que pertenezca al grupo de direcciones dinámicas llamado ExternalServerAccess.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Haga clic en **Add (Añadir)** e introduzca en **Name (Nombre)** un nombre para la regla y verifique que **Rule Type (Tipo de regla)** es universal.
3. En la pestaña **Source** (Origen), seleccione trust como la **Source Zone (Zona de origen)**.
4. En la sección Dirección de origen de la pestaña **Source (Origen)**, **Add (Añada)** el grupo ExternalServerAccess que acaba de crear.
5. En la pestaña **Destination (Destino)**, añada untrust como la **Destination Zone (Zona de destino)**.
6. En la pestaña **Service/URL Category (Categoría de URL/servicio)**, compruebe que el servicio está establecido como **application-default (Predeterminado de la aplicación)**.
7. En la pestaña **Actions (Acciones)**, establezca **Action (Acción)** como Allow (Permitir).
8. En la sección Configuración de perfiles de la pestaña **Actions (Acciones)**, seleccione **Profiles (Perfiles)** y, a continuación, adjunte los perfiles predeterminados para antivirus, antispyware y protección contra vulnerabilidades.
9. Haga clic en **OK (Aceptar)**.

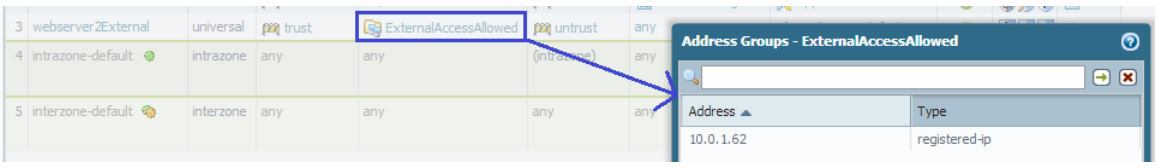


10. Haga clic en **Commit (Confirmar)**.

STEP 5 | Comprobar que los miembros del grupo de direcciones dinámicas se han añadido al cortafuegos.

La política entra en vigor para todas las direcciones IP que pertenecen a este grupo de direcciones y se muestra aquí.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione la regla.
2. Seleccione la flecha desplegable junto al vínculo del grupo de direcciones y seleccione **Inspect (Inspeccionar)**. También puede comprobar si los criterios de coincidencia son precisos.
3. Haga clic en el vínculo **more (más)** y compruebe que se muestra la lista de direcciones IP registradas.



 ©2024 Palo Alto Networks, Inc.

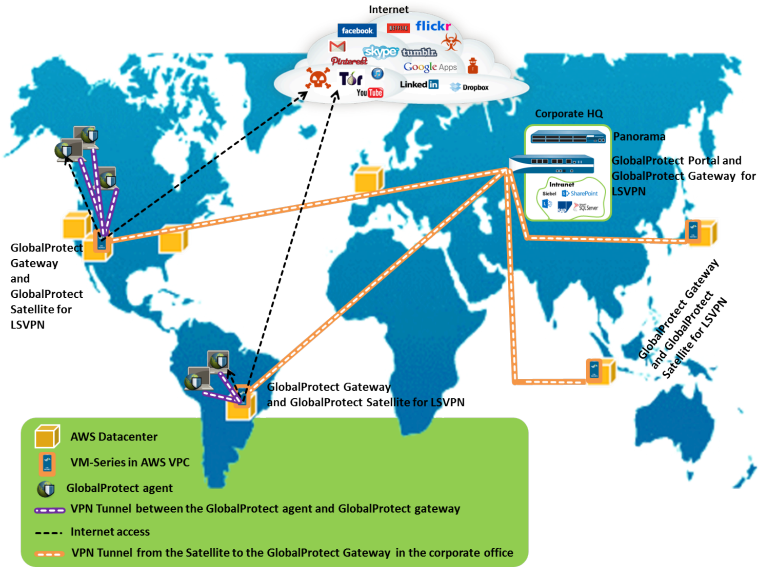
Caso de uso: Cortafuegos VM-Series como puertas de enlace de GlobalProtect en AWS

La protección de los usuarios de dispositivos móviles ante amenazas y aplicaciones de riesgo suele consistir en una compleja combinación de adquisición y configuración de la seguridad e infraestructura de TI, aseguramiento del ancho de banda y los requisitos de tiempo de actividad en todo el mundo sin salirse del presupuesto.

El cortafuegos VM-Series en AWS combina la seguridad y la logística de TI necesarias para proteger de forma consistente y fiable los dispositivos móviles de usuarios en regiones donde no está presente. Al implementar un cortafuegos VM-Series en la nube AWS, puede implementar rápida y fácilmente GlobalProtect™ en cualquier región sin el gasto o la logística de TI que suelen ser necesarias para establecer esta infraestructura usando sus propios recursos.

Para reducir al mínimo la latencia, seleccione las regiones de AWS más cercanas a sus usuarios, implemente los cortafuegos VM-Series en las instancias de EC2 y configure los cortafuegos como puertas de enlace de GlobalProtect. Con esta solución, las puertas de enlace de GlobalProtect en la nube de AWS aplican políticas de seguridad para el tráfico de internet, de modo que no haya que desviarlo por la red corporativa. Asimismo, para el acceso a recursos en la red corporativa, el cortafuegos VM-Series en AWS aprovecha la funcionalidad LSVPN para establecer túneles de IPSec de nuevo en el cortafuegos de la red corporativa.

Para una implementación sencilla y una gestión centralizada de esta, use Panorama para configurar los componentes de GlobalProtect usados en esta solución. De manera opcional, para garantizar el uso seguro de los dispositivos móviles (smartphones y tablets) en su red, use el gestor de seguridad móvil para configurar y gestionar dispositivos móviles.



- Componentes de la infraestructura de GlobalProtect
- Implementación de gateways de GlobalProtect en AWS

©2024 Palo Alto Networks, Inc.

Componentes de la infraestructura de GlobalProtect

Para bloquear las aplicaciones inseguras y proteger a los usuarios móviles contra el software malintencionado, debe configurar la infraestructura de GlobalProtect que incluye el portal de GlobalProtect, la puerta de enlace de GlobalProtect y la aplicación GlobalProtect. Asimismo, para acceder a los recursos corporativos, debe configurar una conexión de VPN de IPSec entre los cortafuegos VM-Series en AWS y el cortafuegos de la sede corporativa mediante LSVPN (una implementación de VPN de concentrador y radio).

- El agente o la aplicación de GlobalProtect se instala en cada sistema de usuario final que se use para acceder a aplicaciones y recursos corporativos. El agente se conecta primero al portal para obtener información sobre las puertas de enlace y, a continuación, establece una conexión de VPN segura con la puerta de enlace de GlobalProtect. La conexión de VPN entre el sistema de usuario final y la puerta de enlace garantiza la privacidad de los datos.
- El portal de GlobalProtect proporciona las funciones de gestión para la infraestructura de GlobalProtect. Todos los sistemas de usuarios finales reciben información de configuración desde el portal, incluida la información sobre las puertas de enlace disponibles, así como certificados de cliente que pueden ser necesarios para conectarse a las puertas de enlace de GlobalProtect. En este caso de uso, el portal de GlobalProtect es un cortafuegos basado en hardware que se implementa en la sede corporativa.
- La puerta de enlace de GlobalProtect y la aplicación de políticas basadas en aplicaciones, usuarios, contenido, dispositivos y estado de dispositivos. En este caso de uso, los cortafuegos VM-Series en AWS funcionan como las puertas de enlace de GlobalProtect. La puerta de enlace de GlobalProtect analiza posible software malintencionado y otras amenazas en las solicitudes de los usuarios, y si la política lo permite, envía la solicitud a internet o a la red corporativa a través del túnel de IPSec (a la puerta de enlace de LSVPN).
- Para LSVPN, debe configurar el portal de GlobalProtect, la puerta de enlace de GlobalProtect para LSVPN (concentrador) y los satélites de GlobalProtect (radios).

  En este caso de uso, el cortafuegos basado en hardware en la oficina corporativa se implementa como el portal de GlobalProtect y la puerta de enlace de LSVPN. Los cortafuegos VM-Series en AWS están configurados para funcionar como satélites de GlobalProtect. Los satélites y la puerta de enlace de GlobalProtect están configurados para establecer un túnel de IPSec que finaliza en la puerta de enlace. Cuando un usuario de un dispositivo móvil solicita una aplicación o recurso alojado en la red corporativa, el cortafuegos VM-Series dirige la solicitud a través del túnel de IPSec.

Implementación de gateways de GlobalProtect en AWS

Para proteger a los usuarios de dispositivos móviles, además de implementar y configurar las puertas de enlace de GlobalProtect en AWS, necesita configurar el resto de componentes necesarios para esta solución integrada. La siguiente tabla enumera el flujo de trabajo recomendado:

- Implemente el cortafuegos VM-Series en AWS.

  Consulte Implementación del cortafuegos VM-Series en AWS.

 ©2024 Palo Alto Networks, Inc.

- Configure el cortafuegos en la sede corporativa.

  En este caso de uso, el cortafuegos está configurado como el portal de GlobalProtect y la puerta de enlace de LSVPN.

  - Configure el portal de GlobalProtect.
  - Configure el portal de GlobalProtect para LSVPN.
  - Configure el portal para la autenticación de satélites de LSVPN.
  - Configure la puerta de enlace de GlobalProtect para LSVPN.

- Configure una plantilla en Panorama para la configuración de los cortafuegos VM-Series en AWS como puertas de enlace de GlobalProtect y satélites de LSVPN.

  Para gestionar fácilmente esta implementación distribuida, use Panorama para configurar los cortafuegos en AWS.

  - Cree plantillas en Panorama.

  A continuación, use los siguientes enlaces para definir la configuración en las plantillas.

  - Configure el cortafuegos como una puerta de enlace de GlobalProtect.
  - Prepare el satélite para unirse a la LSVPN.

- Cree grupos de dispositivos en Panorama para definir las políticas de acceso a la red y las reglas de acceso a internet y aplíquelas a los cortafuegos en AWS.

  Consulte Creación de grupos de dispositivos.

- Aplique las plantillas y los grupos de dispositivos a los cortafuegos VM-Series en AWS y compruebe que los cortafuegos están correctamente configurados.

- Implementación del software de cliente de GlobalProtect.

  Cada sistema de usuario final necesita el agente o aplicación de GlobalProtect para conectarse a la puerta de enlace de GlobalProtect.

  Consulte Implementación del software de cliente de GlobalProtect.

 ©2024 Palo Alto Networks, Inc.

Supervisión de recursos en AWS

A medida que implementa o finaliza los recursos en la nube pública de AWS, puede usar el plugin de Panorama para AWS o usar las fuentes de información del recurso en AWS en el cortafuegos para aplicar uniformemente las reglas de la política de seguridad en estas cargas de trabajo. Consulte la matriz de compatibilidad para obtener información de la versión del complemento de Panorama.

El complemento de Panorama en AWS se ha diseñado para el escalado y le permite supervisar hasta 1000 VPC de AWS en la nube pública de AWS. Con este complemento, use Panorama como apoyo para sondear sus cuentas de AWS por etiquetas y a continuación distribuir los metadatos (asignación de dirección IP a etiquetas) a muchos cortafuegos en un grupo de dispositivos. Debido a que Panorama se comunica con sus cuentas de AWS para recuperar información de recursos en AWS, puede optimizar el número de llamadas de la API realizadas al entorno de nube. Cuando usa Panorama y el plugin de AWS, puede centralizar la recuperación de etiquetas y la gestión de la política de seguridad para garantizar políticas uniformes para arquitecturas híbridas y nativas de la nube. Consulte Supervisión de recursos en AWS con el complemento de AWS en Panorama.

Si no posee Panorama o cuenta con una implementación más simple y desea supervisar 10 VPC o menos, puede usar la fuente de información de VM en el cortafuegos (hardware o VM-Series) para supervisar las cargas de trabajo de AWS. Puede usar los metadatos, que recupera el cortafuegos, en grupos de direcciones dinámicas y hacer referencia a ellos en las políticas de seguridad para proteger las cargas de trabajo de su VM a medida que inician o se detienen, y las direcciones IP cambian con frecuencia. Consulte Caso de uso: Uso de grupos de direcciones dinámicas para proteger las nuevas instancias de EC2 en el VPC.

Supervisión de recursos en AWS con el complemento de AWS en Panorama

A medida que implementa o finaliza recursos en la nube pública de AWS, necesita una manera de actualizar de forma sincrónica la política de seguridad en sus cortafuegos de Palo Alto Networks®, de modo que pueda proteger estas instancias EC2. Para habilitar esta capacidad en Panorama, debe instalar el plugin de AWS en Panorama y habilitar la comunicación de API entre Panorama y su VPC de AWS. Panorama puede recopilar un conjunto predefinido de atributos (o elementos de metadatos) como etiquetas para sus recursos AWS y registrar la información en sus cortafuegos de Palo Alto Networks®. Si hace referencia a estas etiquetas en los Grupos de direcciones dinámicas y las coteja con las reglas de la política de seguridad, puede aplicar la política de forma sistemática en todos los recursos implementados en las cuentas AWS.

- Configuración del complemento de AWS para la supervisión en Panorama
- Lista de atributos supervisados en la VPC de AWS

Configuración del plugin AWS para la supervisión de VM en Panorama

Para encontrar todas las cargas de trabajo de la máquina virtual que su organización implementó en la nube pública de AWS, debe instalar el plugin de AWS en Panorama y configurar las *definiciones de supervisión* que permiten que Panorama se autentique en sus VPC de AWS y recupere información de la VM en las cargas de trabajo. Panorama recupera la dirección IP de las VM que están en ejecución (dirección IP pública, y direcciones IP privadas principal y secundaria) y las etiquetas asociadas. Para obtener una lista de los elementos de metadatos que admite Panorama, consulte Lista de atributos supervisados en la VPC de AWS.

 ©2024 Palo Alto Networks, Inc.

Después de que Panorama recupere los atributos, para enviar la información de la máquina virtual de Panorama a los cortafuegos, debe añadir los cortafuegos (hardware o VM-Series) como dispositivos gestionados en Panorama y agrupar los cortafuegos en uno o más grupos de dispositivos. A continuación, puede especificar los grupos de dispositivos que forman parte del *grupo de notificación*, que es un elemento de configuración en una definición de monitorización, que Panorama usa para registrar la asignación de direcciones IP a etiquetas que recupera de AWS.

Finalmente, para aplicar uniformemente las políticas de seguridad en las instancias EC2, debe configurar los grupos de direcciones dinámicas y hacer referencia a ellos en las reglas de la política que permiten o deniegan el tráfico a las direcciones IP de las VM. Para optimizar su configuración y gestionar las políticas y los objetos centralmente en Panorama, puede definir los grupos de direcciones dinámicas y las reglas de la política de seguridad, y enviarlos a los cortafuegos en lugar de gestionar los grupos de direcciones dinámicas y las reglas de la política de seguridad localmente en cada cortafuegos.

El complemento de AWS versión 3.0.1 o posterior supervisa instancias EC2 de hasta 1000 VPC en la nube pública de AWS, AWS GovCloud y AWS China. Sin embargo, debido a que Panorama no se puede implementar en AWS China, el rol de IAM no es compatible con perfiles de instancia en AWS China; debe proporcionar las credenciales de AWS.

Al configurar la definición de supervisión, asegúrese de adjuntar el DG principal al grupo de notificación del complemento y de que todos los DG secundarios estén desconectados del grupo de notificación.

Para asegurarse de que la DAU propague todas las etiquetas IP de las DG principales a las DG secundarias que están conectadas al cortafuegos, ejecute el comando debug dau settings device-group recursive yes en la CLI de Panorama

- Planificación de la lista de comprobación para la supervisión de VM en AWS
- Roles y permisos de IAM para Panorama
- Instalar o actualizar el complemento de AWS
- Configuración del plugin AWS para la supervisión de VM

Planificación de la lista de comprobación para la supervisión de VM en AWS

Para que Panorama interactúe con las API de AWS y recopile información en sus instancias EC2, debe crear una función de IAM y asignar las políticas que conceden los permisos requeridos para autenticarse a AWS y acceder a las instancias EC2 en su VPC. Puede agregar 100 roles IAM para gestionar hasta 1000 VPC en Panorama.

- Recopile la ID de la VPC.
- Etiquete las instancias de EC2 en AWS. Puede etiquetar (definir un par de nombre-valor) las instancias EC2 en el panel EC2 de la consola de gestión de AWS o usando la API de AWS o la CLI de AWS. Consulte Lista de atributos supervisados en la VPC de AWS para acceder a la lista de atributos compatibles.
- Busque direcciones IP duplicadas en las VPC en las que habilitará la supervisión. Si tiene direcciones IP duplicadas en las VPC de AWS, los metadatos se anexarán o intercambiarán, y esto podría causar resultados inesperados en la aplicación de la política.

  Las direcciones IP duplicadas se escriben en el archivo plugin_aws_ret.log a que puede acceder desde la CLI de Panorama.

 ©2024 Palo Alto Networks, Inc.

- Revise los requisitos para Panorama y los cortafuegos gestionados:
  - Requisitos mínimos del sistema: dispositivo virtual Panorama o dispositivo Panorama basado en hardware.

<table>
<tr><th colspan="5">Requisitos mínimos de Panorama</th></tr>
<tr><td rowspan="4">Recursos del sistema</td><td>Memoria</td><td>CPU</td><td>Número de VPC supervisadas</td><td>Número de Etiquetas registradas</td></tr>
<tr><td>16GB</td><td>4</td><td>1-100</td><td rowspan="3">Panorama 9.1 o posterior con complemento de AWS 2.0 (o posterior) se prueba para recuperar 10.000 direcciones IP con 13 etiquetas para cada una, o 5000 direcciones IP con 25 etiquetas para cada una, y registrarlas correctamente en los cortafuegos incluidos en un grupo de dispositivos. La longitud de la etiqueta (incluye nombre y valor) para cada instancia EC2 se asume que es de 64 bytes por etiqueta. Por ejemplo, la etiqueta del nombre de la instancia EC2 es aws.ec2.tag.Name.prod-web-app-4523-lvss6j.</td></tr>
<tr><td>32 GB</td><td>8</td><td>100-500</td></tr>
<tr><td>64 GB</td><td>16</td><td>500-1000</td></tr>
<tr><td>Versión OS de Panorama</td><td colspan="4">10.0.5 o posterior</td></tr>
<tr><td>Versión de complemento de AWS</td><td colspan="4">3.0.1 o posterior</td></tr>
<tr><td>Licencias</td><td colspan="4">Licencia de asistencia técnica activa y una licencia de gestión de dispositivos en panorama para gestionar los cortafuegos.
Los cortafuegos de última generación también deben tener una licencia de asistencia técnica válida.</td></tr>
<tr><td>Roles y permisos para recuperar metadatos en las instancias EC2</td><td colspan="4">Consulte Roles y permisos de IAM para Panorama</td></tr>
</table>

  - Debe añadir los cortafuegos como dispositivos gestionados en Panorama y crear grupos de dispositivos, de modo que pueda configurar Panorama para notificar a estos grupos con la información de la VM que recupera. Los grupos de dispositivos pueden incluir cortafuegos serie VM o sistemas virtuales en los cortafuegos del hardware.
  - Si sus dispositivos Panorama poseen una configuración de alta disponibilidad, debe instalar manualmente la misma versión del plugin de AWS en ambos pares de Panorama. Además, si

 ©2024 Palo Alto Networks, Inc.

está utilizando perfiles de instancia, debe adjuntar el mismo perfil de instancia a ambos pares de Panorama.

Configure el plugin de AWS en el par activo de Panorama únicamente. Después de confirmarlo, la configuración se sincronizará con el par pasivo de Panorama. Solo el par activo de Panorama sondea las cuentas a AWS que configuró para la supervisión de VM.

- Configure las credenciales/permisos necesarios para firmar digitalmente las llamadas de la API a los servicios de AWS.

  Puede elegir si desea proporcionar las credenciales a largo plazo, ID de clave de acceso y clave secreta de acceso, que permiten el acceso a los recursos dentro de cada cuenta de AWS, o configurar una opción de Asumir la función en AWS para permitir el acceso a los recursos de AWS definidos dentro de la misma cuenta o cuentas cruzadas de AWS. Con Asumir función, debe configurar una relación de confianza y definir los permisos mientras crea la función. Esto es especialmente útil en una implementación de cuentas cruzadas donde la cuenta de consulta no tiene permisos para ver o gestionar datos de la cuenta consultada. Para que el plugin de Panorama se autentique correctamente en la VPC y recupere las etiquetas, debe configurar la función Asumir para usar la API del Servicio de token de seguridad (STS) de AWS para cualquier servicio de AWS. Y un usuario de la cuenta de consulta debe tener permisos STS para consultar la función Asumir y obtener las credenciales de seguridad temporales para acceder a los recursos. Si su Panorama se ha implementado en AWS, puede optar por utilizar un perfil de instancia en lugar de proporcionar las credenciales de AWS para el rol de IAM. El perfil de la instancia incluye la información del rol y las credenciales asociadas que Panorama necesita para firmar digitalmente llamadas API a los servicios de AWS. Consulte Roles y permisos de IAM para Panorama para más información.

Roles y permisos de IAM para Panorama

Con el complemento de AWS, puede usar funciones de IAM o perfiles de instancia para permitir que Panorama autentique y recupere metadatos en los recursos implementados dentro de su (s) cuenta (s) de AWS.

- Cuando su Panorama no está implementado en AWS, tiene dos opciones. Puede proporcionar las credenciales de IAM a largo plazo para las cuentas de AWS que desea supervisar, o configurar Asumir rol en AWS para permitir el acceso a recursos de AWS definidos dentro de la misma cuenta de AWS o entre cuentas. Se recomienda Asumir rol como la opción más segura.
- Cuando su Panorama se implementa en AWS, además de las dos opciones enumeradas anteriormente, también puede añadir un perfil de instancia que permita que el rol de IAM se transfiera a la instancia EC2. Puede usar un perfil de instancia donde todos sus recursos supervisados y Panorama estén alojados dentro de la misma cuenta, o un perfil de instancia con Asumir Rol para el acceso entre cuentas cruzadas donde su Panorama y los recursos supervisados se implementan en diferentes cuentas de AWS. Si utiliza el perfil de instancia, no introduzca sus credenciales de AWS en Panorama.

Opción 1: Función de IAM con credenciales a largo plazo	
Roles y permisos requeridos	Las credenciales de AWS asociadas con la cuenta de AWS que tiene las instancias de VPC/EC2 que desea supervisar.

 ©2024 Palo Alto Networks, Inc.

	El formato JSON para los permisos mínimos asociados al rol IAM con credenciales a largo plazo es el siguiente: `{ “Version”: “2012-10-17", “Statement”: [{ “Sid”: “VisualEditor0”, “Effect”: “Allow”, “Action”: [“elasticloadbalancing:DescribeLoadBalancerAttributes”, “elasticloadbalancing:DescribeLoadBalancers”, “elasticloadbalancing:DescribeTags”, “ec2:DescribeInstances”, “ec2:DescribeNetworkInterfaces”, “ec2:DescribeVpcs”, “ec2:DescribeVpcEndpoints”, “ec2:DescribeSubnets”], “Resource”: “*” }] }`
Entradas en Panorama	Introduzca el **Access Key ID (ID de clave de acceso)** y la **Secret Access Key (Clave de acceso secreta)** para el usuario en **Panorama** > **Plugins (Complementos)** > **AWS** > **Setup (Configuración)** > **IAM Role (Rol IAM)**.
Opción 2: Función de IAM con Asumir rol	
Roles y permisos requeridos	Si bien puede usar esta opción para supervisar VPC dentro de la misma cuenta o entre cuentas, se recomienda esta opción para habilitar el acceso de cuentas cruzadas asumiendo un rol que le permita acceder a los recursos a los que normalmente tiene acceso. Para asumir un rol desde una cuenta diferente, ese rol debe confiar en su cuenta de AWS y debe estar definido como una entidad fiable en su política de confianza «trust». Además, un usuario que quiera acceder a un rol en una cuenta diferente debe tener una política con acceso seguro al servicio de token (STS) que especifique el ARN del rol. **En la cuenta 1 que desea supervisar:** • Cree un rol de IAM con los permisos necesarios. Para la supervisión de VM, necesita los siguientes permisos. `{ “Version”: “2012-10-17", “Statement”: [{ “Sid”: “VisualEditor0”, “Effect”: “Allow”, “Action”: [“elasticloadbalancing:DescribeLoadBalancerAttributes”, “elasticloadbalancing:DescribeLoadBalancers”, “elasticloadbalancing:DescribeTags”, “ec2:DescribeInstances”, “ec2:DescribeNetworkInterfaces”, “ec2:DescribeVpcs”, “ec2:DescribeVpcEndpoints”, “ec2:DescribeSubnets”], “Resource”: “*” }] }` • Copie el ARN del rol. • Cree un usuario y añada el ID de cuenta para la cuenta 2 como entidad de confianza. Esto proporciona a la Cuenta 2 los permisos para usar este rol para acceder a los recursos dentro de su Cuenta 1. **En la Cuenta 2 que requiere acceso a la cuenta 1**

 ©2024 Palo Alto Networks, Inc.

	• Adjunte la siguiente política con permisos STS y modifique el ARN de rol para que coincida con lo que creó en la cuenta 1. `{ "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource":"arn:aws:iam::012347211234:role/ PAN-OS-assume-role" } }`
Entradas en Panorama	• Introduzca el **Access Key ID (ID de clave de acceso)** y **Secret Access Key (Clave de acceso secreta)** para el usuario en la cuenta 2 en **Panorama** > **Plugins (Complementos)** > **AWS** > **Setup (Configuración)** > **IAM Role (Rol IAM)**. • Introduzca el **Role ARN (ARN de rol)** para la cuenta 1 de AWS que desea supervisar en el **Panorama** > **Plugins (Complementos)** > **AWS** > **Monitoring Definitions (Definiciones de supervisión)**.
Opción 3: Perfil de instancia	
Roles y permisos requeridos	Solo cuando Panorama se implementa como una instancia EC2 en AWS *Tenga en cuenta que cuando utiliza la consola de gestión de AWS para crear una función de IAM, la consola crea automáticamente un perfil de instancia con el mismo nombre que la función. Dado que la función y el perfil de instancia tienen el mismo nombre, cuando se lanza su Panorama (instancia EC2) con una función de IAM, se asocia el perfil de instancia del mismo nombre.* Cuando Panorama y los recursos que desea supervisar están todos en una sola cuenta de AWS. Cree un rol de IAM con AmazonEC2ReadOnlyAccess.
Entradas en Panorama	Seleccione **Instance Profile (Perfil de instancia)** como la opción en **Panorama** > **Plugins (Complementos)** > **AWS** > **Setup (Configuración)** > **IAM Role (Rol IAM)**.
Opción 4: Perfil de instancia con Asumir rol	
Roles y permisos requeridos	Use el perfil de instancia con Asumir rol cuando Panorama y los recursos que desea supervisar se implementan en las cuentas de AWS. Para HA de Panorama, asegúrese de adjuntar el mismo perfil de instancia a ambos pares de Panorama. **En la cuenta 1, donde se implementan sus instancias EC2:** • Cree un rol de IAM. • Para este rol, añada el ID de cuenta de AWS (Cuenta 2) donde su Panorama se implementa como una entidad de confianza. • Adjunte las políticas JSON como se detalló anteriormente para la Supervisión de VM.

 ©2024 Palo Alto Networks, Inc.

	• Copie el ARN de rol. Este rol es necesario para que Panorama recupere metadatos en sus instancias EC2 o clústeres de EKS. **En la cuenta 2, donde se implementa su Panorama:** • Cree un rol de IAM y adjunte la política JSON (con la política STS y el ARN de recursos que obtuvo de la Cuenta 1). • Para cada cuenta de AWS adicional que desee supervisar, copie la misma política STS y modifique el ARN de rol.
Entradas en Panorama	• Seleccione **Instance Profile (Perfil de instancia)** como opción en **Panorama** > **Plugins (Complementos)** > **AWS** > **Setup (Configuración)** > **IAM Role (Rol IAM)** • Introduzca el **Role ARN (ARN de rol)** para la cuenta de AWS que desea supervisar en el **Panorama** > **Plugins (Complementos)** > **AWS** > **Monitoring Definitions (Definiciones de supervisión)**. Por ejemplo, la cuenta 1 en este ejemplo.

Instalar o actualizar el complemento de AWS

Para comenzar a supervisar sus instancias EC2 en AWS, consulte la Matriz de compatibilidad para el Complemento de Panorama para AWS y las versiones del complemento para VM-Series necesarias para admitir la supervisión de máquinas virtuales.

Para actualizar un complemento de Panorama anterior para la versión de AWS a una versión posterior (por ejemplo, pasar de la versión 1.0 a la versión 4.0), primero debe actualizar a las versiones de complemento de Panorama y VM-Series requeridas para la versión más reciente (actualmente, 4.0), luego instalarlo como se indica a continuación para realizar una actualización.

Después de instalar el complemento de AWS más reciente (por ejemplo, v4.0), no podrá cambiar a una versión anterior (por ejemplo, v2.0).

Si tiene una configuración de HA en Panorama, repita el proceso de instalación/actualización en cada par de Panorama.

Instale o desinstale los complementos durante una periodo de mantenimiento planificado.

Si actualmente tiene instalado un complemento de Panorama para cualquier plataforma en la nube, la instalación (o desinstalación) de un complemento adicional requiere un reinicio de Panorama para que confirme los cambios.

Si tiene un Panorama independiente o dos dispositivos Panorama instalados en un par de alta disponibilidad con varios complementos instalados, es posible que los complementos no reciban información actualizada sobre la etiqueta IP si uno o más de los complementos no están configurados. Esto ocurre porque Panorama no reenviará la información de la etiqueta IP a los complementos no configurados. Además, este problema puede ocurrir si uno o más de los complementos de Panorama no están en el estado Registrado o Correcto (el estado positivo varía según cada complemento). Asegúrese de que sus complementos estén en el estado positivo antes de continuar o ejecutar los comandos que se describen a continuación.

 ©2024 Palo Alto Networks, Inc.

Si encuentra este problema, hay dos soluciones:

- Desinstale el complemento o complementos no configurados. Se recomienda que no instale un complemento que no planifique configurar de inmediato
- Puede utilizar los siguientes comandos para solventar este problema. Ejecute el siguiente comando para cada complemento no configurado en cada instancia de Panorama, para evitar que Panorama espere para enviar actualizaciones. Si no lo hace, sus cortafuegos pueden perder cierta información de la etiqueta IP.

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

  Puede cancelar este comando ejecutando:

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

Los comandos descritos no son persistentes en los reinicios y deben usarse de nuevo para cualquier reinicio posterior. Para Panorama en el par de HA, los comandos deben ejecutarse en cada Panorama.

STEP 1 | Inicie sesión en la interfaz web de Panorama, seleccione **Panorama** > **Plugins (complementos)** y haga clic en **Check Now (Comprobar ahora)** para obtener la versión de complemento de **AWS** que es compatible con la supervisión de máquinas virtuales.

STEP 2 | **Download and Install (Descargar e instalar)** el complemento.

Después de realizar la instalación correctamente, Panorama se actualiza y el plugin de AWS se muestra en la pestaña **Panorama** > **Plugins (Complementos)**.

*En el widget de información general del **Dashboard (Panel)** de Panorama, puede verificar el complemento de Panorama para la versión de AWS que está instalada.*

STEP 3 | (Panorama en HA) **Commit (Confirmar)** > **Commit to Panorama (Confirmar con Panorama)**.

Si su Panorama está en HA, confirme los cambios en la configuración de Panorama para asegurarse de que las etiquetas estén registradas en el par de Panorama para una conmutación por error.

Configuración del plugin AWS para la supervisión de VM

Para comenzar a supervisar las máquinas virtuales en su implementación de nube pública de AWS, después de instalar el plugin de AWS, debe crear una definición de monitorización. Esta definición especifica la función de IAM autorizada a acceder a las instancias EC2 en la VPC de AWS que desea supervisar y el grupo de notificación que incluye los cortafuegos a los que Panorama debe enviar todas las asignaciones de dirección IP a etiqueta que recupera. Para aplicar la política, debe crear grupos de direcciones dinámicas y hacer referencia a ellas en la política de seguridad. Los grupos de direcciones dinámicas le permiten filtrar las etiquetas que desea supervisar, de modo que el cortafuegos pueda obtener las direcciones IP públicas y privadas registradas para cada etiqueta y permitir o denegar el acceso al tráfico hacia y desde las cargas de trabajo basado en las reglas de la política que defina.

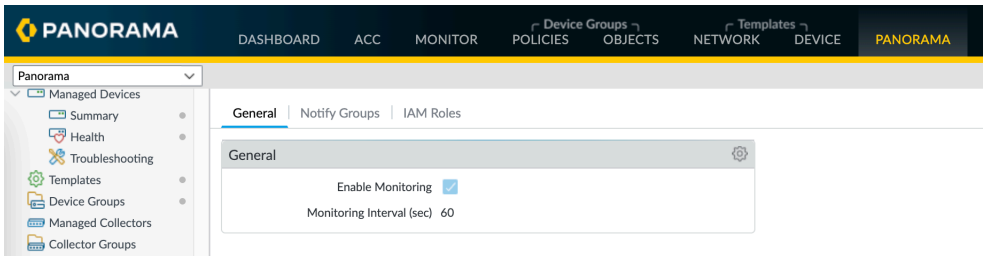
STEP 1 | Inicie sesión en la interfaz web de Panorama.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configure los siguientes objetos para habilitar la supervisión de VM en AWS.

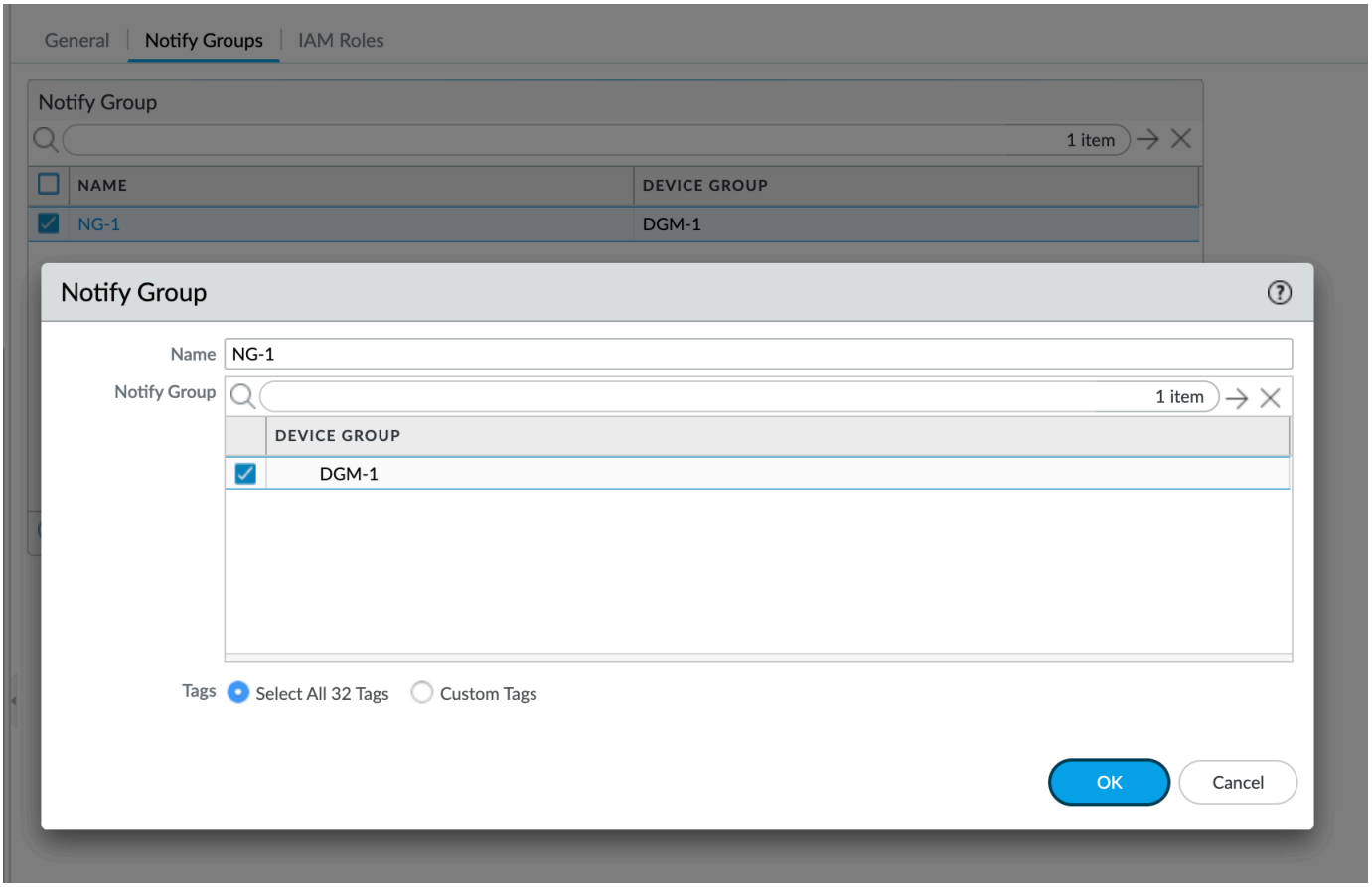
- Verifique que la supervisión se habilite en el complemento. Es necesario habilitar esta configuración para que Panorama se comunique con la nube pública de AWS a fin de supervisar las VM.

  La casilla de verificación **Enable Monitoring (Habilitar supervisión)** está en **Panorama** > **Plugins (Plugins)** > **AWS** > **Setup (Configuración)** > **General**.



- Añadir un grupo de notificación.

  1. Seleccione **Panorama** > **Plugins (Complementos)** > **AWS** > **Setup (Configuración)** > **Notify Groups (Grupos de notificación)** > **Add (Añadir)**.



  2. Introduzca un **Name (Nombre)** para identificar el grupo de cortafuegos al que Panorama envía la información de VM que recupera.
  3. Seleccione los **Device Groups (Grupos de dispositivos)**, que son un grupo de cortafuegos o sistemas virtuales, al que Panorama enviará la información de la VM (asignación de dirección IP a etiqueta) que recupera de la VPC de AWS. Los cortafuegos usan esta actualización para determinar la lista de miembros más actual que constituye los grupos de direcciones dinámicas a

 ©2024 Palo Alto Networks, Inc.

los que se hace referencia en la política. Si usa el complemento de Panorama para Azure y AWS, puede dirigirse al mismo cortafuegos o sistema virtual con etiquetas de ambos entornos.

Analice detalladamente sus grupos de dispositivos.

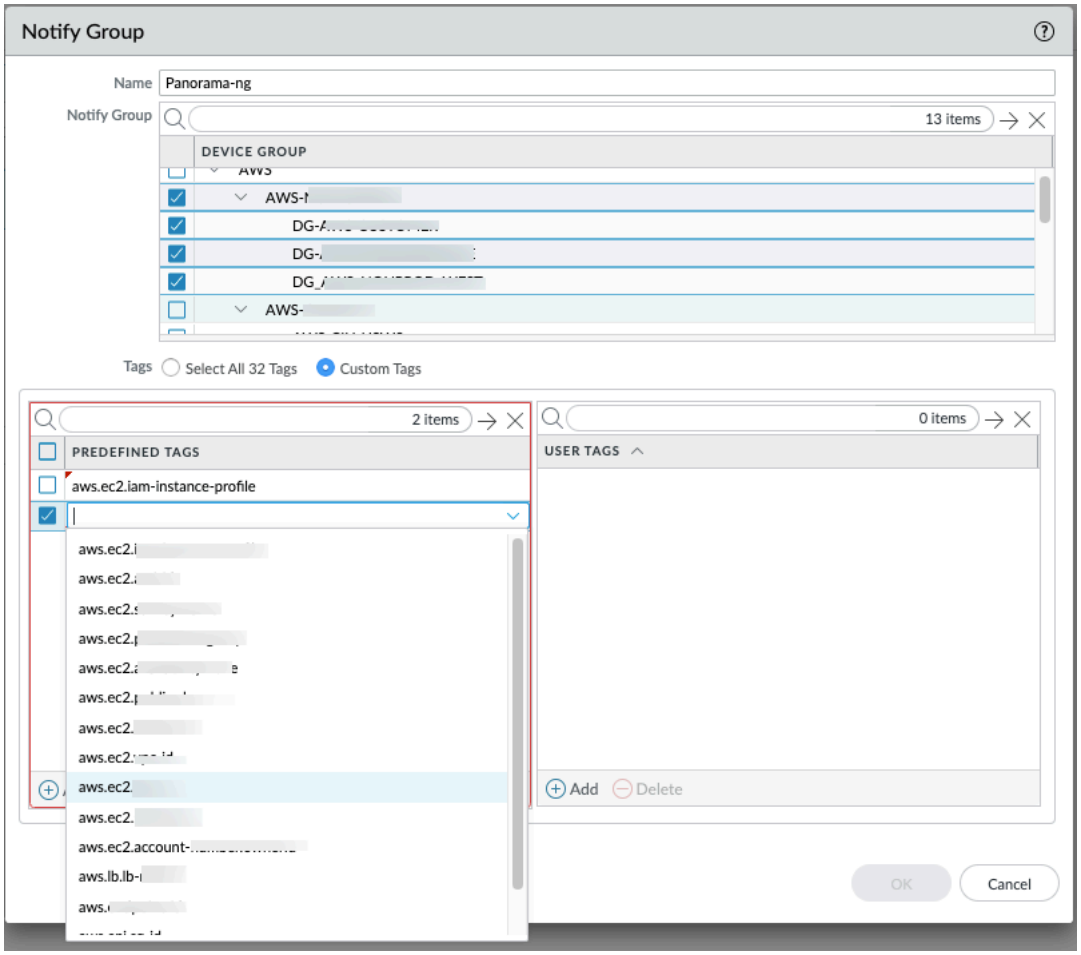
- *Debido a que la definición de monitorización puede incluir únicamente un grupo de notificación, asegúrese de seleccionar todos los grupos de dispositivos relevantes dentro de su grupo de notificación. Si desea eliminar el registro de las etiquetas que Panorama envió a un cortafuegos en un grupo de notificación, debe eliminar la definición de monitorización.*
- *Para eliminar el registro de las etiquetas de todos los sistemas virtuales en un cortafuegos habilitado para varios sistemas virtuales, debe añadir cada sistema virtual a un grupo de dispositivos separado en Panorama y asignar los grupos de dispositivos al grupo de notificación. Si asigna todos los sistemas virtuales a un grupo de dispositivos, Panorama registrará las etiquetas en un solo sistema virtual en el cortafuegos.*

4. Seleccione las etiquetas que desea recuperar de las VPC de AWS.

   Usted puede **Select All 32 Tags (Seleccionar todas las 32 etiquetas)** (el valor predeterminado) o elegir las **Custom Tags (Etiquetas personalizadas)** que desea recuperar para sus instancias. Con la opción de etiquetas personalizadas, puede **Add (Añadir)** las etiquetas predefinidas y las etiquetas definidas por el usuario que desea utilizar como criterios de coincidencia en la política de seguridad. Si está supervisando una gran cantidad de instancias de EC2, la reducción del número de etiquetas que recupera asegura un uso más eficiente de la CPU y la memoria en su

 ©2024 Palo Alto Networks, Inc.

Panorama. Consulte Planificación de la lista de comprobación para la supervisión de VM en AWS para obtener directrices.

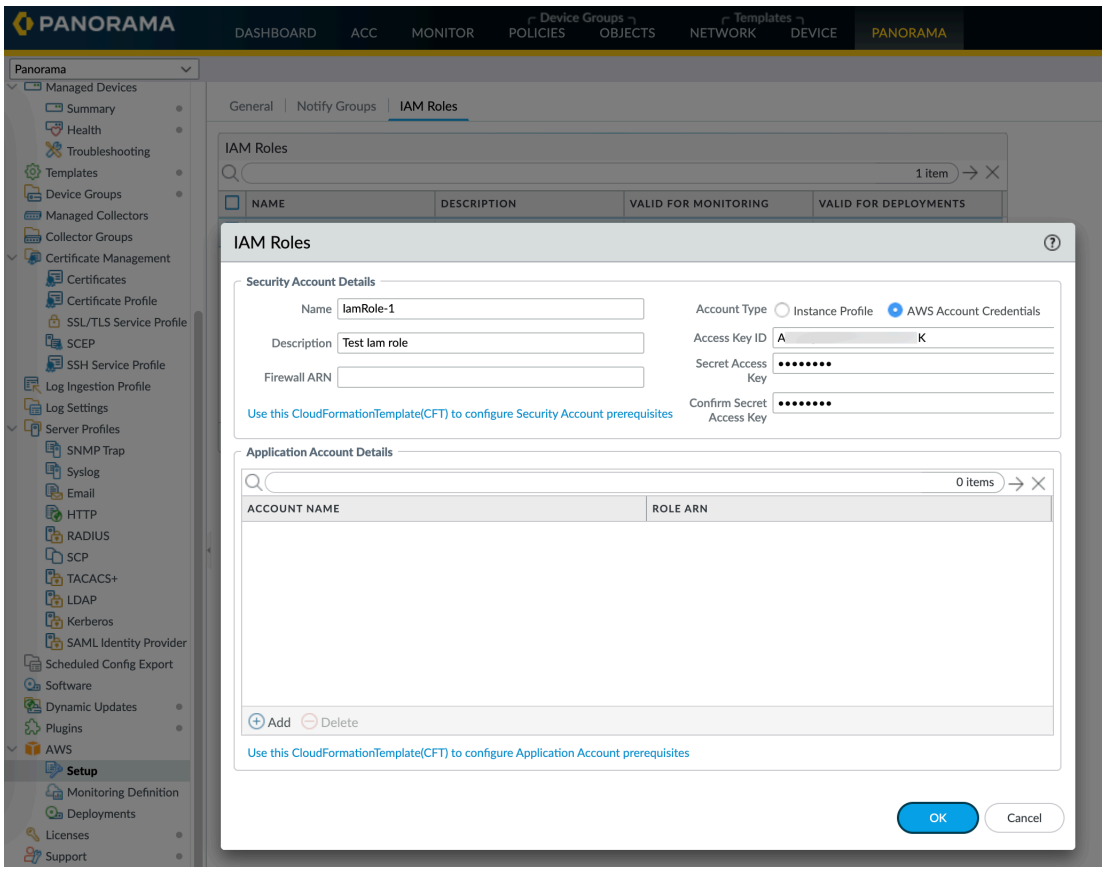


- Añada una función de IAM.

  Una función de IAM es una entidad que le permite delegar el acceso, de modo que Panorama pueda realizar solicitudes de servicio en su nombre a los recursos de AWS (máquinas virtuales que se implementan en instancias EC2).

  1. Seleccione **Panorama** > **Plugins (Complementos)** > **AWS** > **Setup (Configuración)** > **IAM Role (Función de IAM)** > **Add (Añadir)**.

 ©2024 Palo Alto Networks, Inc.



2. Introduzca un **Name (Nombre)** y, opcionalmente, una **Description (Descripción)** para identificar la función de IAM.
3. Seleccione el tipo de cuenta: **Instance Profile (Perfil de instancia)** o **AWS Account Credentials (Credenciales de cuenta de AWS)**. Si su Panorama se implementa en AWS, puede elegir adjuntar un perfil de instancia con los permisos correctos a su Panorama o añadir las

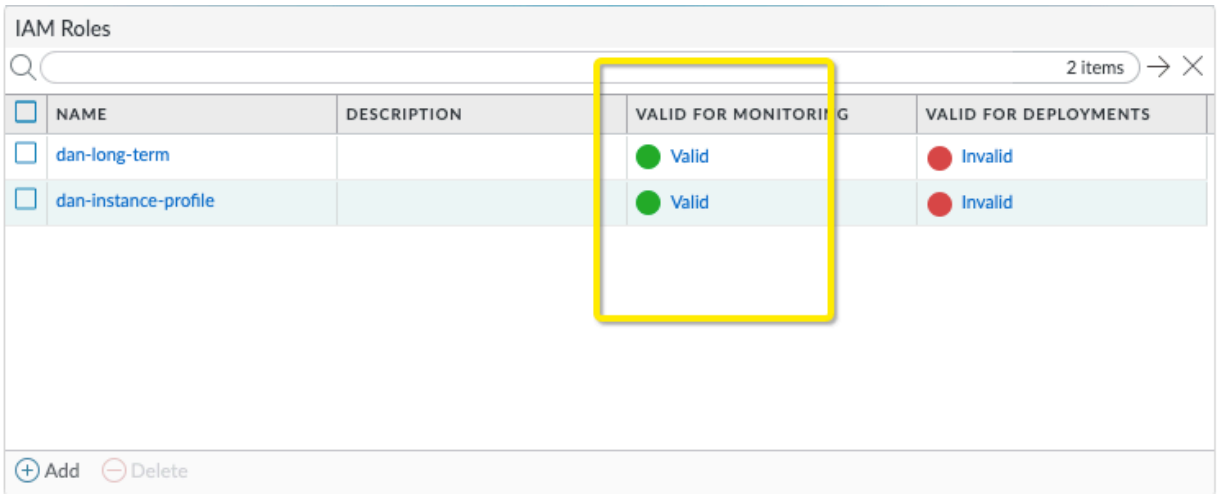
 ©2024 Palo Alto Networks, Inc.

credenciales asociadas con el rol de IAM en Panorama. Si su Panorama no se implementa en AWS, debe introducir las credenciales para el rol de IAM localmente en Panorama.

4. (solo para credenciales de cuenta de AWS) Introduzca la **Secret Access Key (Clave de acceso secreta)** y vuelva a introducirla para confirmar, y haga clic en **OK (Aceptar)**.

(Solo para AWS GovCloud), debe establecer la región de AWS que ejecuta el comando de operación (op-comando). A continuación se muestra un ejemplo para establecer la región de AWS mediante el comando de operación (op-command):

```
request plugins aws set-aws-region region <aws-govcloud-region>
```



STEP 3 | Cree una **Monitoring Definition (definición de supervisión)** para cada VPC que desea supervisar.

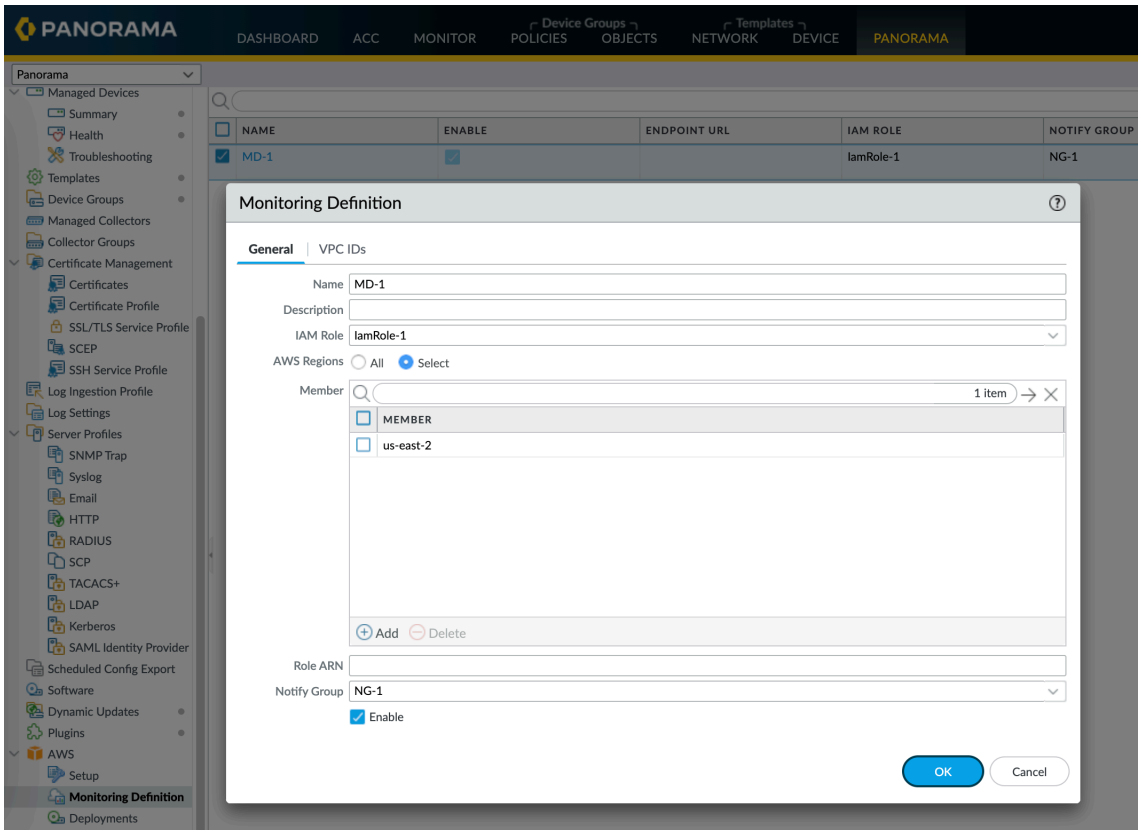
Cuando añade una nueva definición de monitorización, se habilita de manera predeterminada.

- Seleccione **Panorama** > **Plugins (Complementos)** > **AWS** > **Monitoring Definition (Definición de supervisión)** > **General**, para **Add (Añadir)** una nueva definición.
- Introduzca un **Name (Nombre)** y, opcionalmente, una **Description (Descripción)** para identificar la VPC de AWS para la que usa esta definición.
- Seleccione la **IAM Role (Función de IAM)**, luego **Add (Añadir)** la **VPC ID (ID de VPC)** desde el panel de control de VPC en la consola de gestión de AWS, y **Notify Group (Grupo de notificación)**.
- Seleccione **AWS Regions (Regiones de AWS)**:
  - **All (Todas)**: seleccione todas las regiones de AWS.
  - **Select (Seleccionar)**: seleccione regiones específicas de AWS. Busque regiones de AWS desde la barra de búsqueda de **Member (Miembro)** o seleccione **Add (Añadir)** nuevas regiones.
- (Opcional) Introduzca la **Role ARN (Función ARN)**, si ha configurado el encadenamiento de funciones y las funciones IAM con credenciales temporales que tienen permisos para usar la API de

 ©2024 Palo Alto Networks, Inc.

AWS STS para acceder a los recursos de AWS con la misma cuenta o cuenta cruzada. El ARN de rol debe pertenecer a la VPC que desea supervisar.

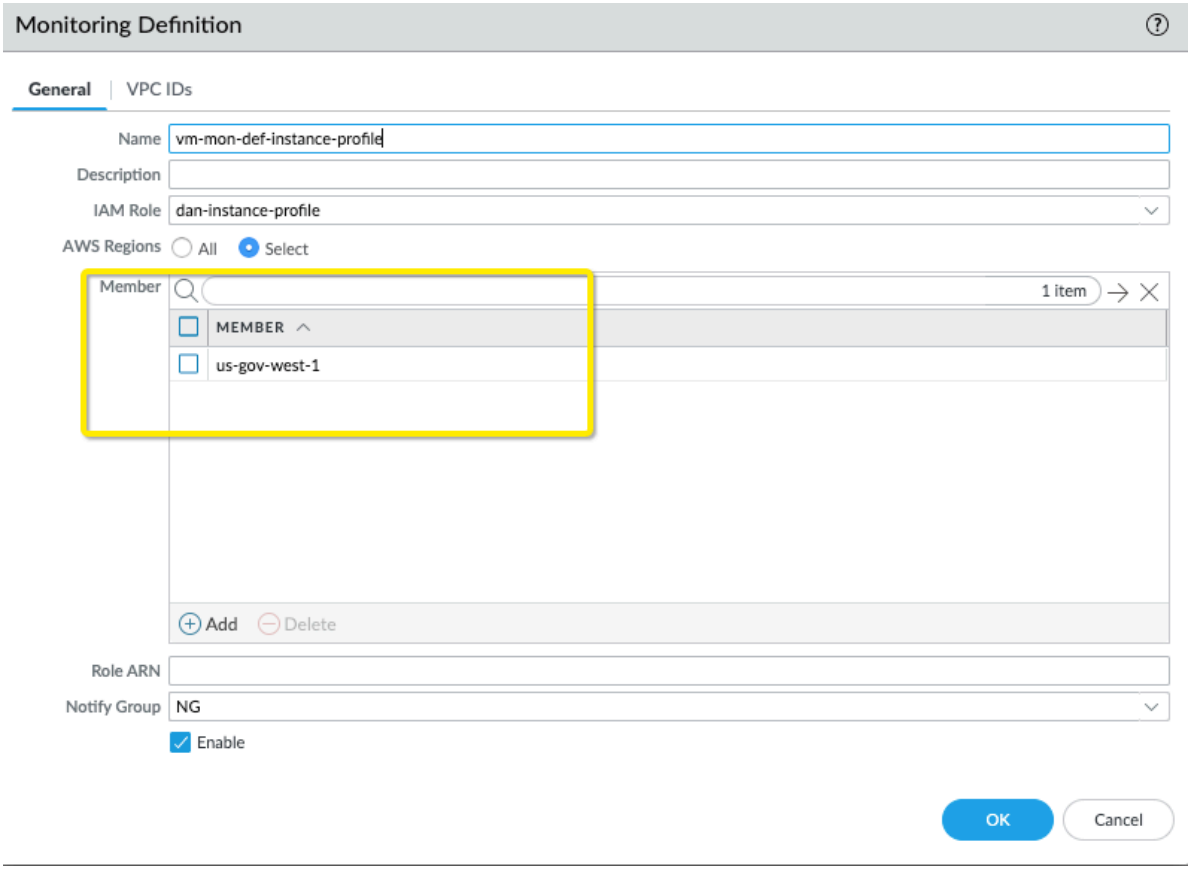
- Seleccione un **Notify Group (Grupo de notificación)** y luego **Enable (Habilitar)** la supervisión.



(Solo para AWS GovCloud), configure la región de AWS en la definición de supervisión mediante la **CLI** y luego **confirme** los cambios. Ejecute el siguiente comando en la CLI:

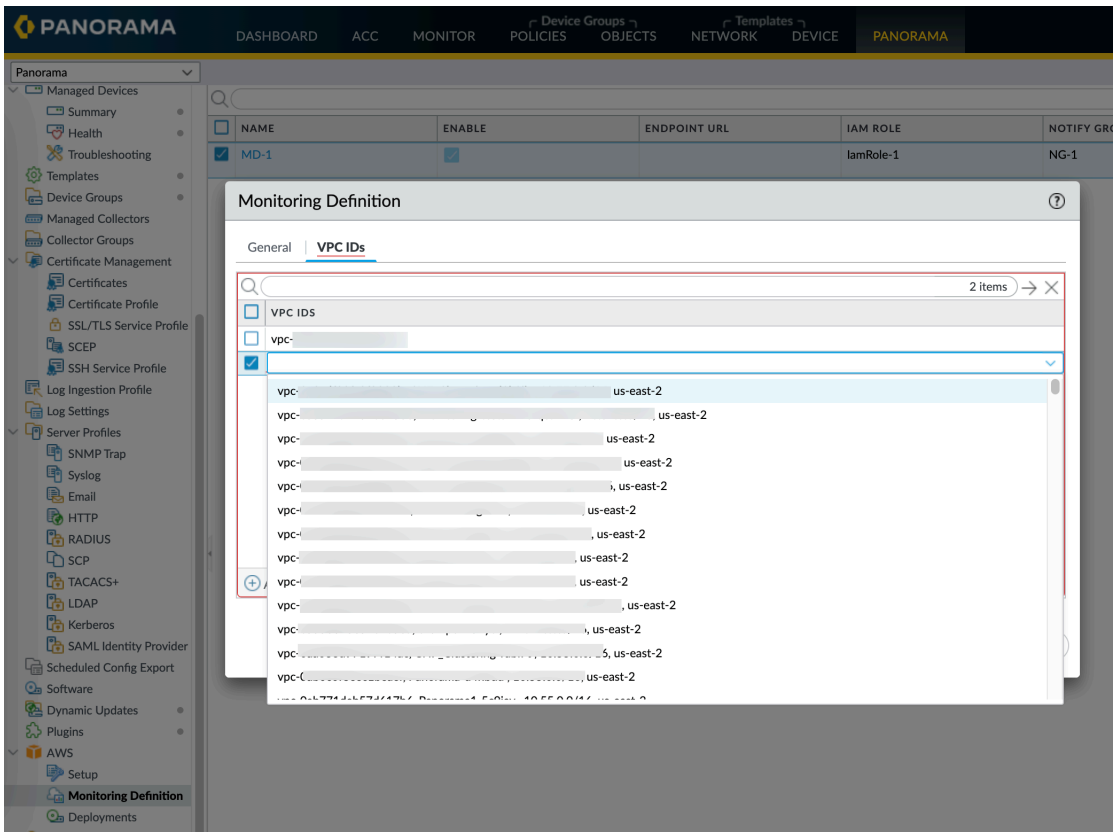
```
set plugins aws monitoring-definition <vm-mon-name> aws-regions
<aws-govcloud-region>
```

 ©2024 Palo Alto Networks, Inc.



- En la pestaña **VPC IDs (ID de VPC)**, añada los ID de VPC desde el panel de control de VPC en la consola de administración de AWS.

 ©2024 Palo Alto Networks, Inc.



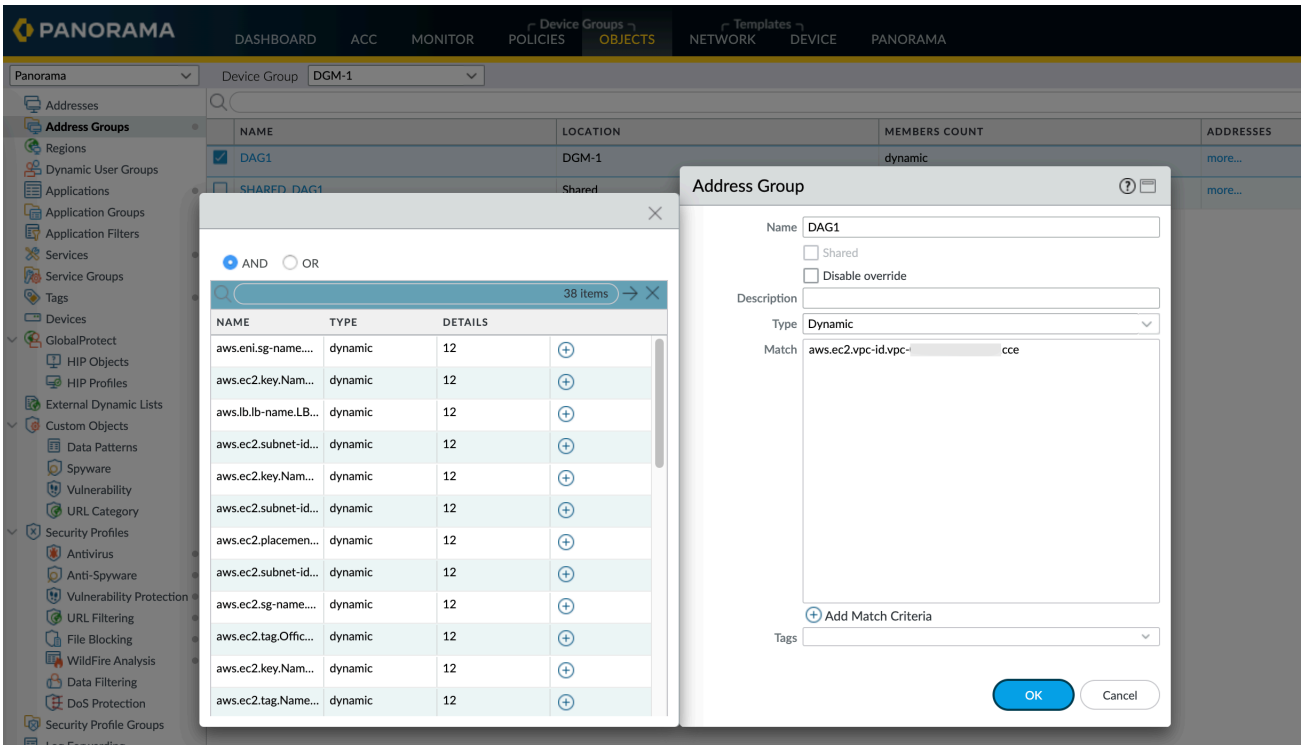
STEP 4 | Haga clic en **Commit (Confirmar)** para confirmar los cambios realizados en Panorama.

Compruebe que el estado de la definición de monitorización se muestre como Success (Correcto). Si falla, compruebe que introdujo la ID de la VPC de AWS correctamente y proporcionó las ID y claves correctas para autorizar el acceso.

*Haga clic en **Validate (Validar)** para verificar que Panorama pueda autenticarse utilizando el rol y las claves de IAM y para comunicarse con las VPC de AWS que introdujo anteriormente.*

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Compruebe que puede ver la información de la VM en Panorama y defina los criterios de coincidencia para los grupos de direcciones dinámicas.



Durante una conmutación por error de HA, la instancia de Panorama activada recientemente intenta reconectarse a la nube de AWS y recuperar las etiquetas de todas las definiciones de supervisión. Si Panorama no puede volver a conectarse ni siquiera con una de las definiciones de supervisión que ha configurado y habilitado, Panorama genera un mensaje de log del sistema

```
No se pueden procesar cuentas después del cambio de alta
 disponibilidad; se requiere la intervención del usuario.
```

Si esto sucede, debe iniciar sesión en Panorama y verificar las definiciones de supervisión para corregir credenciales no válidas o eliminar cuentas no válidas. A pesar de que Panorama está desconectado de la nube de AWS, todas las etiquetas que se recuperaron de las definiciones de supervisión antes de la conmutación por error se retienen y los cortafuegos pueden continuar aplicando la política en esa lista de direcciones IP. Panorama elimina todas las etiquetas asociadas a las cuentas únicamente cuando elimina una definición de servicio. Se recomienda que para supervisar este problema, configure el reenvío de logs a un destino HTTPS orientado a la acción desde Panorama, de modo que pueda actuar de inmediato.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Sepa dónde encontrar los logs relacionados con el complemento de AWS en Panorama para la resolución de problemas.

- Use el comando CLI **`less plugins-log`** para ver una lista de todos los logs disponibles

  `less plugins-log plugin_aws_ret.log` muestra logs relacionados con la dirección IP y la recuperación de etiquetas.

  `less plugins-log plugin_aws_proc.log` muestra logs relacionados con el procesamiento de la dirección IP registrada y las etiquetas.

  `less plugins-log plugin_aws.log` muestra logs relacionados con la configuración de complementos y daemons de AWS.

Utilice **`show plugins aws vm-mon-status`** para conocer el estado de las definiciones de supervisión.

```
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
```

 ©2024 Palo Alto Networks, Inc.

Lista de atributos supervisados en la VPC de AWS

A medida que proporciona o modifica máquinas virtuales en su VPC de AWS, tiene dos maneras de supervisar estas instancias y recuperar las etiquetas para usarlas como criterio de coincidencia en grupos de direcciones dinámicas.

- **Fuente de información de la VM:** en un cortafuegos de última generación, puede supervisar hasta 32 etiquetas: 14 pares de clave-valor predefinidos y 18 pares de clave-valor definidos por el usuario (etiquetas).
- **Plugin de AWS en Panorama**: el plugin de Panorama para AWS le permite conectar Panorama a su VPC de AWS en la nube pública y recuperar la asignación de dirección IP a etiqueta para sus máquinas virtuales. Panorama registra la información de la VM en los cortafuegos gestionados de Palo Alto Networks® que configuró para las notificaciones. Con el plugin, Panorama puede recuperar un total de 32 etiquetas para cada máquina virtual, 11 etiquetas predefinidas y hasta 21 etiquetas definidas por el usuario.



La longitud máxima del valor de la etiqueta (nombre y valor incluidos) debe ser de 116 caracteres o menos. Si una etiqueta tiene más de 116 caracteres, Panorama no recupera la etiqueta y la registra en los cortafuegos.

Atributos supervisados en el AWS-VPC		Fuente de información de la VM en el cortafuegos	Complemento de AWS en Panorama
ID de AMI	ImageId.<ImageId string>	Sí	Sí
Arquitectura	Arquitectura.<Architecture string>	Sí	No
Zona de disponibilidad	AvailabilityZone.<string>	Sí	Sí
Sistema operativo invitado	GuestOS.<guest OS name>	Sí	No
Perfil de instancia IAM	Iam-instance-profile.<instanceProfileArn>	No	Sí
ID de instancia	InstanceId.<InstanceId string>	Sí	No
Estado de instancia	InstanceState.<instance state>	Sí	No
Tipo de instancias	InstanceType.<instance type>	Sí	No
Nombre de clave	KeyName.<KeyName string>	Sí	Sí

©2024 Palo Alto Networks, Inc.

Atributos supervisados en el AWS-VPC		Fuente de información de la VM en el cortafuegos	Complemento de AWS en Panorama
Owner ID El valor de este atributo se recibe de la ENI.	Número de cuenta.<OwnerId>	No	Sí
Colocación Arrendamiento, nombre del grupo	Placement.Tenancy.<string> Placement.GroupName.<string>	Sí	Sí
Nombre DNS privado	PrivateDnsName.<Private DNS Name>	Sí	No
Nombre DNS público	PublicDnsName.<Public DNS Name>	Sí	Sí
ID de subred	SubnetID.<subnetID string>	Sí	Sí
ID de grupo de seguridad	Sg-id.<sg-xxxx>	No	Sí
Nombre del grupo de seguridad	Sg-name.<SecurityGroupName>	No	Sí
ID de VPC	VpcId.<VpcId string>	Sí	Sí
Etiqueta (clave, valor)	aws-tag.<key>.<value>	Sí; Se admiten hasta 18 etiquetas definidas por el usuario como máximo. Las etiquetas definidas por el usuario se ordenan alfabéticamente y las primeras 18 etiquetas están	Sí; Se admiten hasta 21 etiquetas definidas por el usuario como máximo. Las etiquetas definidas por el usuario se ordenan alfabéticamente y las primeras 21 etiquetas se pueden usar en Panorama y los cortafuegos.

©2024 Palo Alto Networks, Inc.

Atributos supervisados en el AWS-VPC		Fuente de información de la VM en el cortafuegos	Complemento de AWS en Panorama
		disponibles para usarlas en los cortafuegos.	

Permisos de IAM requeridos para supervisar la VPC de AWS

Para habilitar la Supervisión de VM las credenciales de inicio de sesión de AWS del usuario vinculadas a la Clave de acceso de AWS y a la Clave de acceso secreto deben tener permisos para los atributos detallados anteriormente. Estos privilegios permiten que el cortafuegos inicie llamadas de la API para supervisar las máquinas virtuales en la VPC de AWS.

La política de IAM asociada con el usuario debe tener un acceso de solo lectura global, como AmazonEC2ReadOnlyAccess, o debe incluir permisos individuales para todos los atributos supervisados. El siguiente ejemplo de política de IAM detalla los permisos para iniciar las acciones de API y supervisar los recursos en la VPC de AWS:

```
{ “Version”: “2012-10-17", “Statement”: [ { “Sid”:
 “VisualEditor0”, “Effect”: “Allow”, “Action”:
 [ “elasticloadbalancing:DescribeLoadBalancerAttributes”,
 “elasticloadbalancing:DescribeLoadBalancers”,
 “elasticloadbalancing:DescribeTags”, “ec2:DescribeInstances”,
 “ec2:DescribeNetworkInterfaces”, “ec2:DescribeVpcs”,
 “ec2:DescribeVpcEndpoints”, “ec2:DescribeSubnets” ], “Resource”:
 “*” } ] }
```

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en KVM

Kernel-based Virtual Machine (KVM) es un módulo de virtualización de código abierto para servidores que ejecutan distribuciones Linux. El cortafuegos VM-Series se puede implementar en un servidor Linux que ejecute el hipervisor KVM.

En esta guía se asume que ya utiliza infraestructura de TI basada en Linux y dispone de lo necesario para el uso de herramientas de Linux y herramientas de Linux. Las instrucciones solo hacen referencia a la implementación del cortafuegos VM-Series en KVM.

- VM-Series en KVM: Especificaciones y requisitos previos
- Implementaciones compatibles en KVM
- Instalación del cortafuegos VM-Series en KVM
- Ajuste de rendimiento de VM-Series para KVM
- Descarga tráfico inteligente

VM-Series en KVM: especificaciones y requisitos previos

- Opciones para conectar el VM-Series en la red
- Requisitos previos de la serie VM en KVM

Table 5: Requisitos del sistema para VM-Series en KVM

Requisitos	Description (Descripción)
Recursos de hardware	Consulte Requisitos del sistema VM-Series para ver los requisitos mínimos de hardware para su modelo VM-Series.
Versiones de software	Consulte las versiones de software KVM compatibles en la Matriz de compatibilidad. *El cortafuegos VM-Series ahora es compatible con instancias basadas en ARM en el hipervisor **KVM** para nubes privadas. Todas las características que estaban disponibles en entornos x86 ahora se extienden a instancias basadas en ARM, incluido el soporte de Hypervisor, DPDK que proporciona un mejor rendimiento, al tiempo que reduce los costes operativos (OPEX), el consumo de energía y las huellas. El soporte de arquitectura ARM está actualmente disponible en KVM como créditos de NGFW de software*
Controladores SR-IOV	Consulte los controladores de Versiones del controlador PacketMMAP en la Matriz de compatibilidad.
Controladores DPDK	Consulte Versiones del controlador DPDK en la matriz de compatibilidad. Si utiliza uno de los controladores NIC compatibles en VM-Series en KVM, DPDK está habilitado de forma predeterminada.
Interfaces de red: Tarjetas de interfaz de red y puentes de software	VM-Series en KVM admite un máximo de 25 interfaces: 1 interfaz de gestión y un máximo de 24 interfaces de red para tráfico de datos. VM-Series implementado en KVM admite conmutadores virtuales basados en software como el puente Linux o el puente Open vSwitch, así como conectividad directa a PCI-passthrough o a un adaptador compatible con SR-IOV. Si planifica establecer la conectividad mediante PCI-passthrough o SR-IOV, no puede configurar un vSwitch en el puerto físico utilizado para el PCI-passthrough o SR-IOV. Para comunicarse con el host y otras máquinas virtuales de la red, el cortafuegos VM-Series debe tener acceso exclusivo al puerto físico y a las funciones virtuales asociadas (associated virtual functions, VF) en esa interfaz.

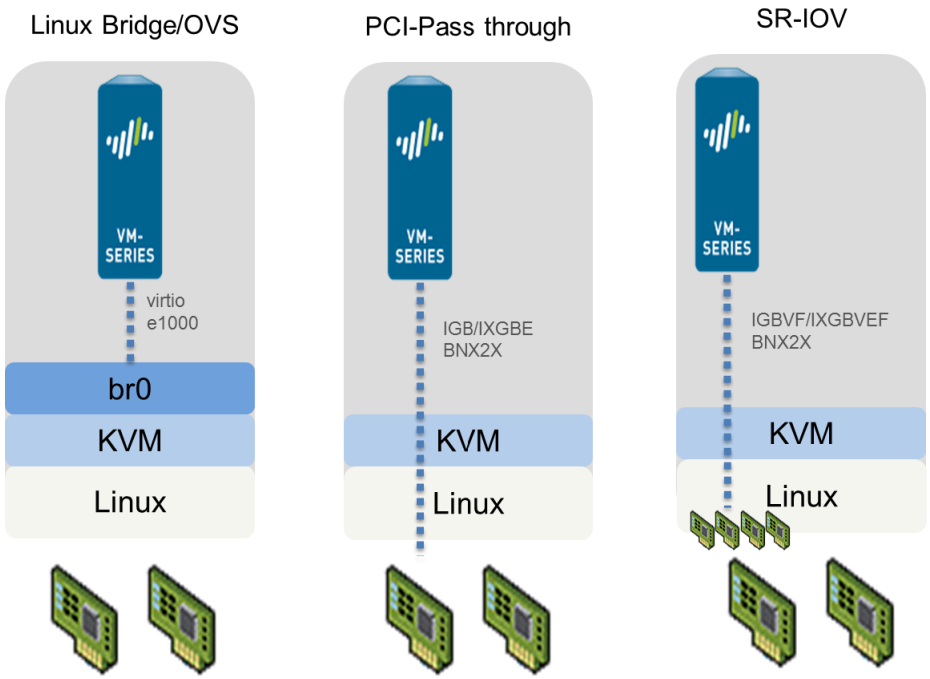
 ©2024 Palo Alto Networks, Inc.

Requisitos	Description (Descripción)

	• En el puente Linux y OVS, son compatibles los controladores e1000 y Virtio; no es compatible el controlador predeterminado rtl8139.
	• En cuanto a la compatibilidad de PCI-passthrough/SR-IOV, se han probado las siguientes tarjetas de red para el cortafuegos VM-Series:
	  • Tarjeta de red 1G basada en Intel 82576: Compatibilidad con SR-IOV en todas las distribuciones de Linux compatibles; compatible con PCI-passthrough.
	  • Tarjeta de red 10G basada en Intel 82599: Compatibilidad con SR-IOV en todas las distribuciones de Linux compatibles; compatible con PCI-passthrough.
	  • NIC Intel X710 10 G: Compatibilidad con SR-IOV en todas las distribuciones de Linux compatibles; compatible con envío PCI
	  • NIC Intel X722 10 G: Compatibilidad con SR-IOV en todas las distribuciones de Linux compatibles; compatible con envío PCI
	  • Tarjeta de red 10G basada en Broadcom 57112 y 578xx: Compatibilidad con SR-IOV en todas las distribuciones de Linux compatibles; no compatible con PCI-passthrough.
	  • NIC Mellanox ConnectX5 10G/25G/50G/100G: Compatibilidad con SR-IOV en todas las distribuciones de Linux compatibles.
	  • Consulte Versiones del controlador PacketMMAP en la Matriz de compatibilidad
	  Las interfaces compatibles con SR-IOV asignadas al cortafuegos VM-Series deben configurarse como interfaces de capa 3 o como interfaces HA.
	• Para ARM, el cortafuegos VM-Series se ha probado para tarjetas de red Mellanox, Intel I350 Gigabit NIC, X710, 10G y 40G.

 ©2024 Palo Alto Networks, Inc.

Opciones para conectar el VM-Series en la red



- Con un puente Linux u OVS, el tráfico de datos usa el puente de software para conectar invitados en el mismo host. Para la conectividad externa, el tráfico de datos usa la interfaz física a la que se ha conectado el puente.
- Con el envío PCI, el tráfico de datos pasa directamente entre el invitado y la interfaz física a la que está conectada. Cuando la interfaz se conecta a un invitado, no está disponible para el host o para otros invitados en el host.
- Con SR-IOV, el tráfico de datos pasa directamente entre el invitado y la función virtual a la que está conectada.

Requisitos previos de la serie VM en KVM

Antes de instalar el cortafuegos VM-Series en el servidor Linux, consulte las siguientes secciones:

- Preparación del servidor Linux
- Preparación de la implementación del cortafuegos VM-Series

Preparación del servidor Linux

Antes de instalar el cortafuegos VM-Series en KVM, verifique que tiene un entorno Linux en funcionamiento y que su infraestructura de red admite la conectividad que requiere la implementación que seleccionó.

- Verificar la compatibilidad con Linux
- Verificar la infraestructura de redes
- Instalar herramientas de software Mellanox
- Habilite las funciones virtuales para las NIC de Mellanox CX5 en el cortafuegos VM-Series en KVM
- Verificar la configuración del host

©2024 Palo Alto Networks, Inc.

Verificar la compatibilidad con Linux

Compruebe que tenga el entorno correcto para respaldar su instalación.

- Compruebe la versión de distribución de Linux. Para obtener una lista de versiones compatibles, consulte VM-Series para KVM en la Matriz de compatibilidad.
- Compruebe que ha instalado y configurado las herramientas y paquetes de KVM necesarios para crear y gestionar máquinas virtuales, como Libvirt.
- Si quiere usar un controlador de disco SCSI para acceder al disco en el que el cortafuegos VM-Series almacena los datos, debe usar virsh para conectar el controlador virtio-scsi al cortafuegos VM-Series. A continuación, puede modificar la plantilla XML del cortafuegos VM-Series para habilitar el uso del controlador virtio-scsi. Para obtener instrucciones, consulte Habilitación del uso de un controlador SCSI.

KVM en Ubuntu 12.04 no admite el controlador virtio-scsi.

Verificar la infraestructura de redes

Compruebe que ha configurado la infraestructura de red para enviar el tráfico entre los invitados y el cortafuegos VM-Series y asegúrese de tener conectividad con un servidor externo de Internet. El cortafuegos VM-Series puede conectar usando un puente Linux, Open vSwitch, envío PCI o una tarjeta de red compatible con SR-IOV.

- Asegúrese de que el estado del enlace para cada interfaz que planifica usar sea Activo; a veces debe abrir la interfaz manualmente.
- Si usa un puente Linux u OVS, compruebe que tiene configurados los puentes necesarios para enviar o recibir tráfico desde y hacia el cortafuegos. De lo contrario, cree puentes y compruebe que estén activos antes de iniciar la instalación del cortafuegos.
- Si utiliza SR-IOV o PCI-passthrough, verifique el ID de PCI de todas las interfaces. Para ver la lista, use el siguiente comando:

  `Virsh nodedev-list –tree`

  Consulte Comprobación de PCI-ID para la ordenación de interfaces de red en el cortafuegos VM-Series.
- Si utiliza SR-IOV o envío PCI, compruebe que las extensiones de virtualización (VT-d/IOMMU) están habilitadas en la BIOS. Por ejemplo, para habilitar IOMMU, `intel_iommu=on` debe estar definido en `/etc/grub.conf`. Consulte las instrucciones en la documentación suministrada por el proveedor del sistema.
- Si usa envío PCI, asegúrese de que el cortafuegos VM-Series tiene acceso exclusivo a las interfaces que tiene pensado adjuntarle.

  Para permitir el acceso exclusivo, debe desconectar manualmente las interfaces del servidor Linux.

  `Virsh nodedev-detach <pci id of interface>`

  Por ejemplo:

  `Virsh nodedev-detach pci_0000_07_10_0`

  En algunos casos, es posible que deba editar `/etc/libvirt/qemu.conf` y anular el comentario`Relax_acs_check = 1`.

 ©2024 Palo Alto Networks, Inc.

- Si usa SR-IOV, compruebe que la capacidad de funcionamiento virtual esté habilitada para el puerto en el que tiene pensado usar la tarjeta de red. Con SR-IOV, un único puerto Ethernet (función física) se puede dividir en varias funciones virtuales múltiples. Un invitado se puede asignar a una o varias funciones virtuales.

  Habilite las funciones virtuales de la siguiente forma:

  1. Crear un nuevo archivo en esta ubicación: `/etc/modprobe.d/`
  2. Utilice vi para editar el archivo para que las funciones sean persistentes:

     `vim /etc/modprobe.d/igb.conf`
  3. Habilitar el número de funciones virtuales requeridas:

     `options igb max_vfs=4`

     En el ejemplo a continuación, después de guardar los cambios y reiniciar el servidor Linux, cada interfaz (o función física) tendrá 4 funciones virtuales.

  Consulte la documentación suministrada por el proveedor de red para ver detalles sobre el número concreto de funciones virtuales compatibles y las instrucciones para habilitar las funciones virtuales.

Instalar herramientas de software Mellanox

Si está utilizando una tarjeta Mellanox CX5, instale las herramientas de software Mellanox en el host. Antes de la instalación, verifique la compatibilidad con Linux y su infraestructura de red.

STEP 1 | Desde el host, descargue el paquete de Mellanox OpenFabric Enterprise Distribution para Linux (MLNX_OFED) para su versión de SO desde el siguiente enlace:

https://www.mellanox.com/products/infiniband-drivers/linux/mlnx_ofed

STEP 2 | Ejecute el comando de instalación:

`mlnxofedinstall`

Si tiene instalados todos los paquetes de requisitos previos, el comando anterior instala todos los paquetes MLNX_OFED. Continúe al Paso 3.

Si su entorno no tiene los paquetes necesarios, el instalador enumera todos los paquetes que se deben instalar. Después de instalar los paquetes, vuelva a ejecutar el comando de instalación y continúe al Paso 3.

STEP 3 | Reinicie el host.

STEP 4 | Compruebe el estado de las herramientas de software 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
```

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Asegúrese de que Mellanox esté actualizado en la lista PCI:

```
Controlador Ethernet # lspci | grep Mellanox 3b:00.0: Controlador
 Ethernet Mellanox Technologies MT28800 Family [ConnectX-5 Ex]
 3b:00.1: Mellanox Technologies MT28800 Family [ConnectX-5 Ex]
```

Habilite las funciones virtuales para las NIC de Mellanox CX5 en el cortafuegos VM-Series en KVM

Instale las herramientas de software de Mellanox antes de habilitar las funciones virtuales en las NIC de Mellanox Cx5.

STEP 1 | Asegúrese de que las herramientas de software de Mellanox (mst) están iniciadas.

STEP 2 | Habilitar el número de funciones virtuales requeridas. Por ejemplo:

```
mlxconfig -d /dev/mst/mt4121_pciconf0 set SRIOV_EN=1 NUM_OF_VFS=4
```

Después de guardar los cambios y reiniciar el servidor Linux, cada interfaz (o función física) del ejemplo anterior tendrá 4 funciones virtuales. Consulte la documentación suministrada por el proveedor de red para ver detalles sobre el número concreto de funciones virtuales compatibles y las instrucciones para habilitar las funciones virtuales.

Es posible que vea el siguiente mensaje de error la primera vez que habilita las funciones virtuales en las NIC de Mellanox Cx5:

```
[ 1429.841162] mlx5_core 0000:3b:00.1:
 mlx5_port_module_event:1025:(pid 0): Evento de módulo
 de puerto [error]: módulo 1, error de cable, uno o
 más puertos de red se han apagado debido a un fallo de
 alimentación o un corte no anunciado en la ranura PCIe.
 Consulte el manual de usuario de la tarjeta para conocer
 las especificaciones de energía o póngase en contacto con
 el soporte de Mellanox
```

Para resolver el problema, introduzca la siguiente secuencia de comandos en el servidor Linux:

```
# mlxconfig -d <dev> set ADVANCED_POWER_SETTINGS=1 #
 mlxconfig -d <dev> set DISABLE_SLOT_POWER_LIMITER=1 #
 reboot
```

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Verifique el estado de las funciones virtuales.

```
# cat /sys/class/net/enp59s0f1/device/sriov_numvfs
```

(Opcional) Si las funciones virtuales no están configuradas correctamente (el estado es 0 o está vacío), ejecute el siguiente comando:

```
# echo 4 > /sys/class/net/enp59s0f1/device/sriov_numvfs
```

STEP 4 | Enumere los dispositivos PCI para que coincidan con precisión con el número de funciones virtuales cargadas en la función física correspondiente para Mellanox:

```
Controlador Ethernet # lspci | grep Mellanox 3b:00.0: Controlador
 Ethernet Mellanox Technologies MT28800 Family [ConnectX-5 Ex]
 3b:00.1: Controlador Ethernet Mellanox Technologies MT28800
 Family [ConnectX-5 Ex] 3b:00.2: Controlador Ethernet Mellanox
 Technologies MT28800 Family [ConnectX-5 Ex Virtual Function]
 3b:00.3: Controlador Ethernet Mellanox Technologies MT28800
 Family [ConnectX-5 Ex Virtual Function] 3b:00.4: Controlador
 Ethernet Mellanox Technologies MT28800 Family [ConnectX-5
 Ex Virtual Function] 3b:00.5: Controlador Ethernet Mellanox
 Technologies MT28800 Family [ConnectX-5 Ex Virtual Function]
 3b:00.6: Controlador Ethernet Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex Virtual Function] 3b:00.7: Controlador Ethernet
 Mellanox Technologies MT28800 Family [ConnectX-5 Ex Virtual
 Function] 3b:01.0: Controlador Ethernet Mellanox Technologies
 MT28800 Family [ConnectX-5 Ex Virtual Function] 3b:01.1: Mellanox
 Technologies MT28800 Family [ConnectX-5 Ex Virtual Function]
```

Verificar la configuración del host

Configure el host para obtener el máximo rendimiento de la VM-Series. Consulte el Ajuste de rendimiento de VM-Series para KVM para obtener información sobre cómo configurar cada opción a continuación.

- **Habilite DPDK**. DPDK permite que el host procese los paquetes más rápido eludiendo el kernel de Linux. En cambio, las interacciones con NIC se realizan utilizando controladores y bibliotecas DPDK. Para usar DPDK con el cortafuegos VM-Series se requiere Open vSwitch.
- **Habilite SR-IOV**. La virtualización de E/S de raíz única (SR-IOV) permite que un único dispositivo físico PCIe bajo un único puerto raíz parezca ser múltiples dispositivos físicos separados para el hipervisor o el invitado.
- **Habilite el soporte de colas múltiples para NIC**. Virtio-net de colas múltiples permite que el rendimiento de la red escale con el número de vCPU y permite el procesamiento paralelo de paquetes a través de la creación de múltiples colas TX y RX.
- **Aislamiento de recursos de CPU en un nodo NUMA**. Puede mejorar el rendimiento del VM-Series en KVM aislando los recursos de la CPU de la máquina virtual invitada en un nodo de acceso a la memoria no uniforme (NUMA) único.

 ©2024 Palo Alto Networks, Inc.

Preparación de la implementación del cortafuegos VM-Series

- Adquiera el modelo VM-Series y registre el código de autorización en el sitio web de asistencia al cliente de Palo Alto Networks. Consulte Creación de una cuenta de asistencia técnica y Registro del cortafuegos VM-Series.
- Obtenga la imagen qcow2 y guárdela en el servidor Linux. Se recomienda copiar la imagen en la carpeta: /var/lib/libvirt/qemu/images.

  Si tiene pensado implementar más de una instancia del cortafuegos VM-Series, haga el número necesario de copias de la imagen. Dado que cada instancia del cortafuegos VM-Series mantiene un vínculo con la imagen .qcow2 que se usó para la implementación del cortafuegos, para evitar problemas de daños de los datos, compruebe que cada imagen sea independiente y la use una única instancia del cortafuegos.

 ©2024 Palo Alto Networks, Inc.

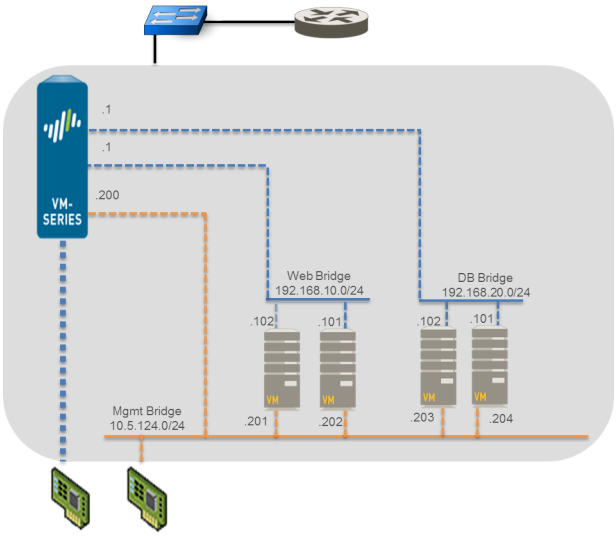
Implementaciones compatibles en KVM

Puede implementar una única instancia del cortafuegos VM-Series por host Linux (inquilino único) o instancias múltiples de cortafuegos VM-Series en un host Linux. El cortafuegos VM-Series se puede implementar con interfaces virtual wire, de capa 2 o de capa 3. Si tiene previsto usar interfaces compatibles con SR-IOV en el cortafuegos VM-Series, sólo puede configurar las interfaces como interfaces de capa 3.

- Protección del tráfico en un host único
- Protección del tráfico en una serie de hosts Linux

Protección del tráfico en un host único

Para proteger el tráfico de dispositivo a dispositivo en invitados de un servidor Linux, el cortafuegos VM-Series se puede implementar con interfaces de cable virtual, de capa 2 o de capa 3. La siguiente ilustración muestra el cortafuegos con interfaces de capa 3, donde el cortafuegos y otros invitados en el servidor están conectados mediante el uso de puentes Linux. En esta implementación, todo el tráfico entre los servidores web y los servidores de bases de datos se dirige a través de cortafuegos; el tráfico que atraviesa sólo los servidores de bases de datos o sólo los servidores web es procesado por el puente y no se dirige a través del cortafuegos.

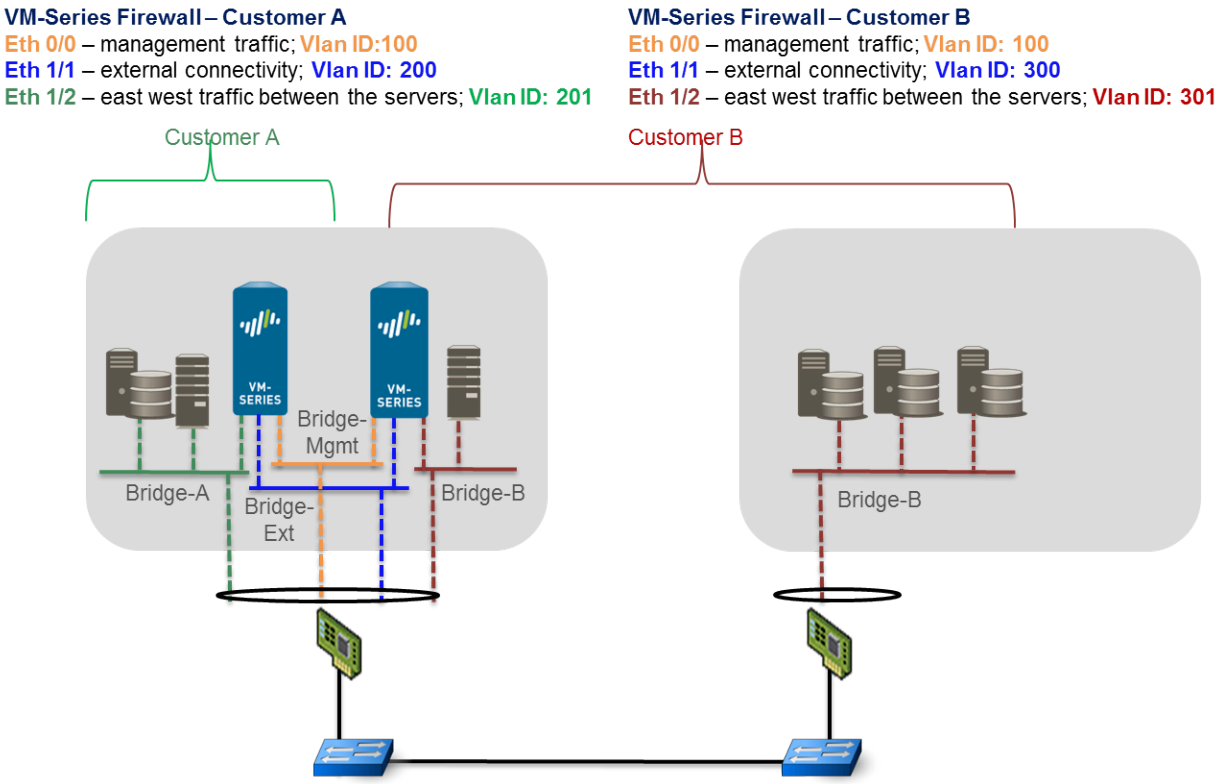


Protección del tráfico en una serie de hosts Linux

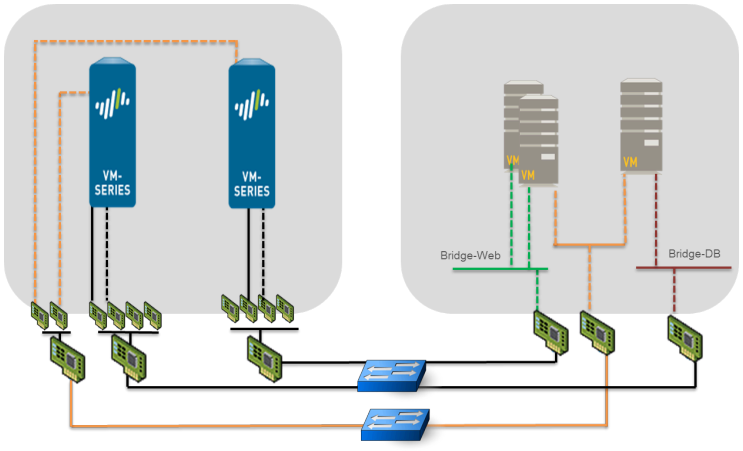
Para proteger sus cargas de trabajo, se puede implementar más de una instancia de cortafuegos VM-Series en un host Linux. Si, por ejemplo, quiere aislar el tráfico para departamentos o clientes separados, puede usar etiquetas VLAN

para aislar lógicamente el tráfico de red y dirigirlo al cortafuegos VM-Series apropiado. En el siguiente ejemplo, un host Linux aloja el cortafuegos VM-Series para dos clientes, Cliente A y Cliente B, y la carga de trabajo para el Cliente B se reparte a través de dos servidores. Para aislar el tráfico y dirigirlo al cortafuegos VM-Series configurado para cada cliente, se usan VLAN.

©2024 Palo Alto Networks, Inc.



En otra variación de esta implementación, se implementan un par de cortafuegos VM-Series en una configuración de alta disponibilidad. Los cortafuegos VM-Series de la siguiente ilustración se implementan en un servidor Linux con adaptadores compatibles SR-IOV. Con SR-IOV, un único puerto Ethernet (función física) se puede dividir en varias funciones virtuales múltiples. Cada función virtual adjunta al cortafuegos VM-Series se configura como una interfaz de capa 3. El equipo activo en el equipo HA protege el tráfico que se dirige hacia él desde invitados que están implementados en un servidor Linux diferente.



 ©2024 Palo Alto Networks, Inc.

Instalación del cortafuegos VM-Series en KVM

La API libvirt que se usa para gestionar KVM incluye varias herramientas que le permiten crear y gestionar máquinas virtuales. Para instalar el cortafuegos VM-Series en KVM, puede seguir uno de estos métodos.

- virt-manager: implementa la VM-Series utilizando el administrador de máquinas virtuales virt-manager. Virt-manager proporciona un práctico asistente para ayudarle en el proceso de instalación.
- virsh: implementa la VM-Series utilizando la línea de comandos KVM. Cree un archivo XML que defina la instancia de máquina virtual y el archivo XML de arranque que define la configuración inicial del cortafuegos. Luego instale el cortafuegos montando una imagen ISO como un CD-ROM.
- virt-install: otra opción para implementar el cortafuegos VM-Series utilizando la línea de comandos KVM. Utilice esta opción para crear la definición para el cortafuegos VM-Series e instálelo.

Este documento proporciona los pasos para instalar el cortafuegos VM-Series en KVM utilizando virt-manager y virsh.

- Instalación del cortafuegos VM-Series en Hyper-V
- Instalación del cortafuegos VM-Series utilizando un archivo ISO
- Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión en KVM
- Habilitación del uso de un controlador SCSI
- Comprobación de PCI-ID para la ordenación de interfaces de red en el cortafuegos VM-Series

Instalación del cortafuegos VM-Series en Hyper-V

Utilice el siguiente procedimiento que utiliza virt-manager para instalar el cortafuegos VM-Series en un servidor que ejecuta KVM en RHEL.

- Aprovisionamiento del cortafuegos VM-Series en un host KVM
- Realización de la configuración inicial del cortafuegos VM-Series en KVM

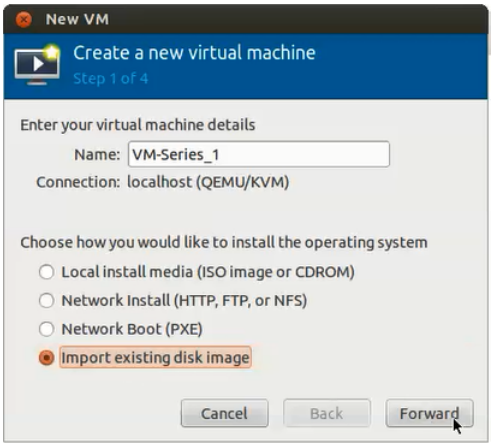
Aprovisionamiento del cortafuegos VM-Series en un host KVM

Use las siguientes instrucciones para aprovisionar el host KVM para el cortafuegos VM-Series.

©2024 Palo Alto Networks, Inc.

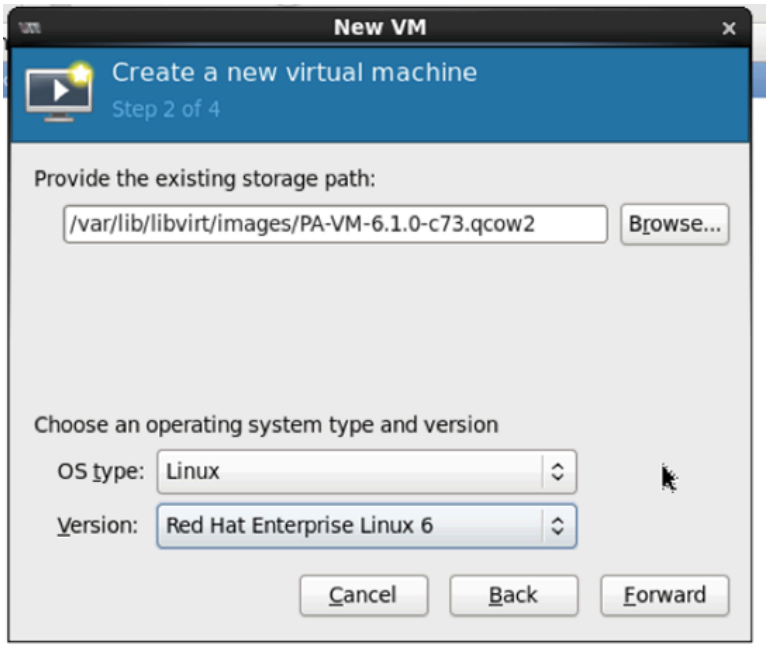
STEP 1 | Cree una nueva máquina virtual y añada el cortafuegos VM-Series para la imagen KVM en virt-mgr.

1. En Virt-manager, seleccione **Create a new virtual machine (Crear una nueva máquina virtual)**.
2. Añada un nombre descriptivo en **Name (Nombre)** para el cortafuegos VM-Series.



3. Seleccione **Import existing disk image (Importar imagen de disco existente)**, navegue hasta la imagen y establezca **OS Type (Tipo de sistema operativo)**: Linux y **Version (Versión)**: Red Hat Enterprise Linux 6.

Si lo prefiere, puede dejar OS Type (Tipo de sistema operativo) y Version (Versión) como Generic (Genérico).

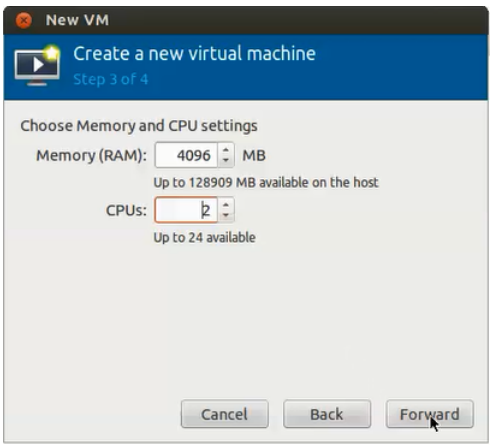


4. Para añadir adaptadores de red a las interfaces de datos:

 ©2024 Palo Alto Networks, Inc.

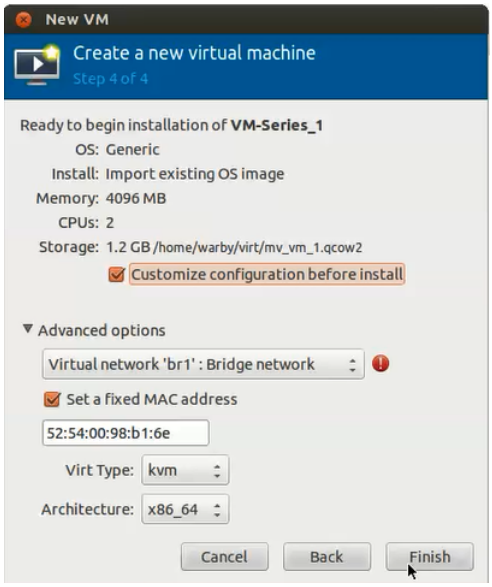
STEP 2 | Configure los ajustes de memoria y CPU.

1. Establezca la **Memory (Memoria)** a la memoria mínima basada en los Requisitos del sistema VM-Series de su modelo VM-Series.
2. Establezca la **CPU** en las CPU mínimas según el Requisitos del sistema para VM-Series modelo de VM-Series.



STEP 3 | Habilite la personalización de la configuración y seleccione el puente de la interfaz de gestión.

1. Seleccione **Customize configuration before install (Personalizar configuración antes de la instalación)**.
2. En Advanced Options (Opciones avanzadas), seleccione el puente para la interfaz de gestión y acepte la configuración predeterminada.



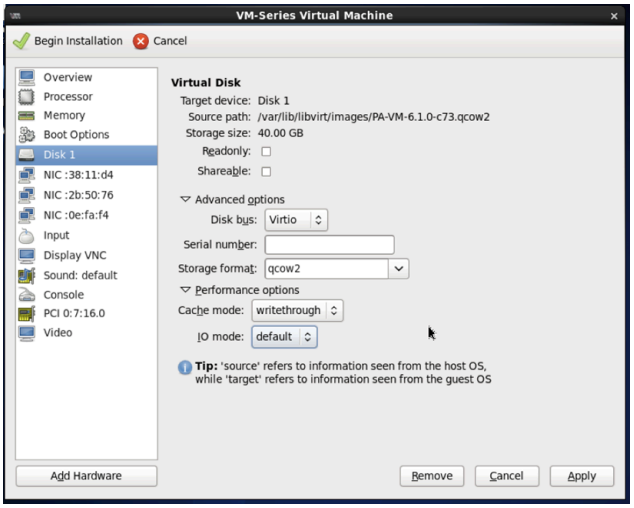
 ©2024 Palo Alto Networks, Inc.

STEP 4 | Configure los ajustes del disco virtual.

1. Seleccione **Disk (Disco)**, expanda las opciones avanzadas y seleccione **Storage format (Formato de almacenamiento)**: qcow2; **Disk Bus (Bus de disco)**: Virtio o IDE, en función de su configuración.

   Si desea utilizar un bus de disco SCSI, consulte Habilitación del uso de un controlador SCSI.

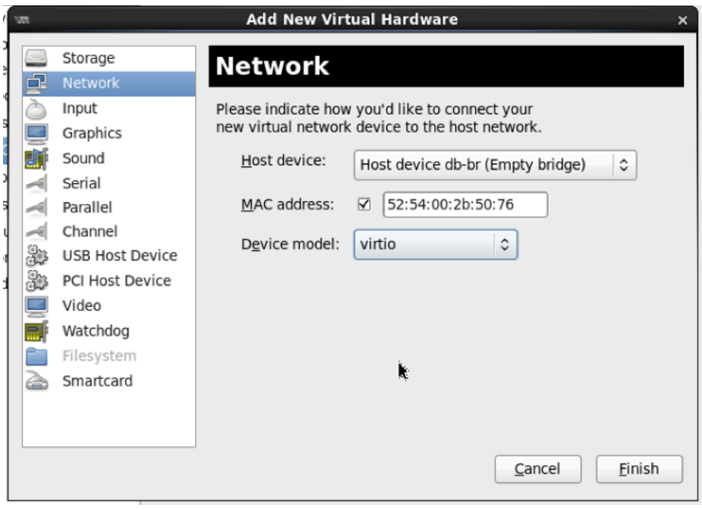
2. Expanda las opciones de Performance (Rendimiento) y configure **Cache mode (Modo de caché)** como **writethrough**. Esta configuración mejora el tiempo de instalación y la velocidad de ejecución en el cortafuegos VM-Series.



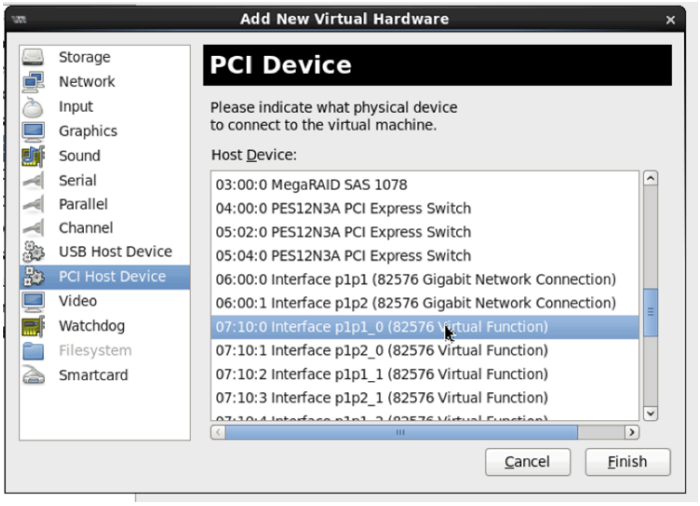
 ©2024 Palo Alto Networks, Inc.

STEP 5 | Configure los adaptadores de red.

1. Seleccione **Add Hardware (Añadir hardware)Network (Red)** si está usando un puente de software como un puente Linux u Open vSwitch.
2. En **Host Device (Dispositivo host)**, introduzca el nombre del puente o selecciónelo de la lista desplegable.
3. Para especificar el controlador, establezca **Device Model (Modelo de dispositivo)** en e-1000 o virtio. Estos son los únicos tipos de interfaces virtuales compatibles.



4. Seleccione **Add Hardware (Añadir hardware)** > **PCI Host Device (Dispositivo host PCI)** para envío PCI o un dispositivo compatible con SR-IOV.

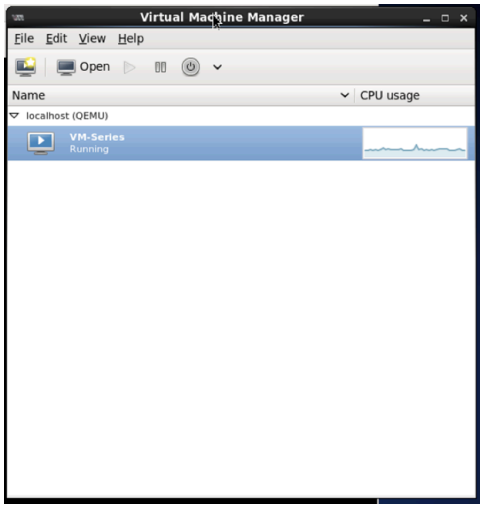


5. En la lista **Host Device (Dispositivo host)**, seleccione la interfaz en la tarjeta o la función virtual.
6. Haga clic en **Apply (Aplicar)** o **Finish (Finalizar)**.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Haga clic en **Begin Installation (Iniciar instalación)** Begin Installation. Espere entre 5 y 7 minutos a que se complete la instalación.

De manera predeterminada, la plantilla XML del cortafuegos VM-Series se crea y almacena en etc/libvirt/qemu.



STEP 7 | (Opcional) Arranque el cortafuegos VM-Series

Si está utilizando bootstrapping para realizar la configuración del cortafuegos VM-Series en KVM, consulte Arranque del cortafuegos VM-Series en KVM. Para obtener más información sobre el arranque, consulte Arranque del cortafuegos VM-Series.

STEP 8 | Defina la configuración de acceso a la red para la interfaz de gestión.

1. Abra una conexión a la consola.
2. Inicie el cortafuegos con nombre de usuario/contraseña: admin/admin.
3. Introduzca el modo de configuración con el siguiente comando:

```
configure
```

4. Use los siguientes comandos para configurar la interfaz de gestión:

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>
   ```

   donde <*Firewall-IP*> es la dirección IP que quiere asignar a la interfaz de gestión, <*netmask*> es la máscara de subred, <*gateway-IP*> es la dirección IP de la puerta de enlace de la red e <*DNS-IP*> es la dirección IP del servidor DNS.

3. ```
   commit
   ```

 ©2024 Palo Alto Networks, Inc.
   ```

STEP 9 | Verifique los puertos del host que se asignarán a la interfaz en el cortafuegos VM-Series. Para verificar el orden de las interfaces en el host Linux, consulte Comprobación de PCI-ID para la ordenación de interfaces de red en el cortafuegos VM-Series.

Para asegurarse de que el tráfico sea gestionado por la interfaz correcta, use el siguiente comando para identificar qué puertos en el host se asignan a los puertos en el cortafuegos 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
 0000:00:11.1
```

STEP 10 | Acceda a la interfaz web del cortafuegos VM-Series, configure las interfaces y defina las reglas de seguridad y las reglas NAT para habilitar de forma segura las aplicaciones que quiere proteger.

Consulte la Guía del administrador de PAN-OS.

Realización de la configuración inicial del cortafuegos VM-Series en KVM

Utilice la consola del dispositivo virtual en el servidor KVM para configurar el acceso de red al cortafuegos VM-Series. De forma predeterminada, el cortafuegos VM-Series usa DHCP para obtener una dirección IP para la interfaz de gestión. Sin embargo, puede asignar una dirección IP estática. Después de completar la configuración inicial, acceda a la interfaz web para completar otras tareas de configuraciones. Si tiene Panorama para la gestión centralizada, consulte la Guía del administrador de Panorama para obtener más información sobre cómo gestionar el dispositivo mediante Panorama.

Si utiliza el arranque para realizar la configuración de su cortafuegos de la serie VM-Series en KVM, consulte Arrancar el cortafuegos VM-Series en KVM.

Para obtener más información sobre el arranque, consulte Arranque del cortafuegos serie VM.

STEP 1 | Obtenga la información necesaria de su administrador de red.

- Dirección IP para el puerto MGT
- Máscara de red
- Puerta de enlace predeterminada
- Dirección IP de servidor DNS

STEP 2 | Acceda a la consola del cortafuegos VM-Series.

1. Seleccione la pestaña **Console (Consola)** en el servidor KVM para el cortafuegos VM-Series o haga clic en el botón derecho del cortafuegos VM-Series y seleccione **Open Console (Abrir consola)**.
2. Pulse Intro para acceder a la pantalla de inicio de sesión.
3. Introduzca el nombre de usuario/contraseña predeterminados (admin/admin) para iniciar sesión.
4. Introduzca **`configure`** para pasar al modo de configuración.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Defina la configuración de acceso a la red para la interfaz de gestión.

Introduzca los siguientes comandos:

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> Máscara de
 red <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

STEP 4 | Confirme los cambios y salga del modo de configuración.

Introduzca **commit (confirmar)**.

Introduzca **exit (salir)**.

Instalación del cortafuegos VM-Series utilizando un archivo ISO

Cree manualmente la definición XML del cortafuegos VM-Series y, a continuación, utilice virsh para importar la definición como una ISO. Virsh es la herramienta más potente que permite la gestión completa de la máquina virtual.

- Uso de un archivo ISO para implementar el cortafuegos VM-Series
- Archivo XML de muestra para el cortafuegos serie VM

Uso de un archivo ISO para implementar el cortafuegos VM-Series

Si quiere pasar una secuencia de comandos al cortafuegos VM-Series durante el inicio, puede montar un CD-ROM con un archivo ISO. El archivo ISO le permite definir un archivo XML de arranque que incluya los parámetros de configuración inicial para el puerto de gestión del cortafuegos. El cortafuegos VM-Series en el primer inicio comprueba el archivo **bootstrap-networkconfig.xml** y usa los valores definidos en el mismo.

Si se encuentra un solo error en el análisis del archivo de arranque, el cortafuegos VM-Series rechazará toda la configuración en este archivo y se iniciará con los valores predeterminados.

STEP 1 | Cree el archivo XML y defínalo como una instancia de máquina virtual.

Para un archivo de muestra, consulte Archivo XML de muestra para el cortafuegos VM-Series.

En este ejemplo, el cortafuegos VM-Series se llama PAN_Firewall_DC1.

Por ejemplo:

```
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
```

 ©2024 Palo Alto Networks, Inc.

```
 ------------------------------------------- -
 PAN_Firewall_DC1_bootstp shut off
```

STEP 2 | Cree el archivo XML de arranque.

Puede definir los parámetros de configuración inicial en este archivo y asígnele el nombre bootstrap-networkconfig.

Si no quiere incluir un parámetro, por ejemplo, panorama-server-secondary. Elimine la línea entera del archivo. Si deja el campo de dirección IP vacío, el archivo no se analizará correctamente.

Use el siguiente ejemplo como plantilla para el archivo bootstrap-networkconfig. El archivo bootstrap-networkconfig puede incluir solamente los siguientes parámetros:

```
<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 | Cree el archivo ISO. En este ejemplo, usamos mkisofs.

Guarde el archivo ISO en el directorio de imágenes (/var/lib/libvirt/image) o el directorio qemu (/etc/libvirt/qemu) para asegurarse de que el cortafuegos tiene acceso de lectura al archivo ISO.

Por ejemplo:

```
# mkisofs -J -R -v -V "Bootstrap" -A "Bootstrap" -ldots -l -
allow-lowercase -allow-multidot -o <iso-filename> bootstrap-
networkconfig.xml
```

STEP 4 | Adjunte el archivo ISO en el CD-ROM.

Por ejemplo:

```
# virsh -q attach-disk <vm-name> <iso-filename> sdc --type cdrom --
mode readonly –persistent\
```

Archivo XML de muestra para el cortafuegos serie VM

```
<?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
```

 ©2024 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>
```

*Para modificar el número de vCPU asignadas en el cortafuegos VM-Series, modifique el valor **2** a **4** o **8** vCPU en esta línea del archivo XML de muestra:*

```
<vcpu placement="static">2</vcpu>
```

Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión en KVM

De forma predeterminada, el cortafuegos VM-Series asigna la primera interfaz (eth0) como interfaz de gestión. Sin embargo, en algunas implementaciones, la primera interfaz debe estar preasignada a una dirección IP pública. Por lo tanto, la interfaz de gestión debe asignarse a una interfaz diferente. La asignación de una dirección IP pública a la interfaz de gestión es un riesgo para la seguridad.

Alternativamente, puede habilitar el intercambio de la interfaz de gestión como parte del Componentes de archivo de init-cfg.txt *cuando se realiza el bootstrapping o arranque.*

STEP 1 | Inicie sesión en la CLI del cortafuegos VM-Series e introduzca el comando siguiente:

```
set system setting mgmt-interface-swap enable yes
```

STEP 2 | Confirme que desea intercambiar la interfaz y utilice la interfaz del plano de datos eth1 como interfaz de gestión.

STEP 3 | Reinicie el cortafuegos para que se produzca el intercambio. Utilice el comando siguiente:

```
request restart system
```

STEP 4 | Verifique que se hayan intercambiado las interfaces. Utilice el comando siguiente:

```
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
```

Habilitación del uso de un controlador SCSI

Si quiere que el cortafuegos VM-Series use el tipo de bus de disco SCSI para acceder al disco virtual, use las siguientes instrucciones para adjuntar el controlador virtio scsi al cortafuegos y, a continuación, habilite el uso del controlador virtio-scsi.

 ©2024 Palo Alto Networks, Inc.

KVM en Ubuntu 12.04 no es compatible con el controlador virtio-scsi; el controlador virtio-scsi solo se puede habilitar en el cortafuegos VM-Series que se ejecuta en RHEL o CentOS.

Este proceso requiere virsh porque Virt manager no es compatible con el controlador virtio-scsi.

STEP 1 | Cree un archivo XML para el controlador SCSI. En este ejemplo, se llama 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>
```

Asegúrese de que la ranura usada para el controlador virtio-scsi no crea conflicto con otro dispositivo.

STEP 2 | Asocie este controlador con la plantilla XML del cortafuegos VM-Series.

```
[root@localhost~]# virsh attach-device --config <VM-Series_name> /
root/virt-scsi.xmlDispositivo conectado correctamente
```

STEP 3 | Habilite el uso del controlador SCSI en el cortafuegos.

```
[root@localhost~]# virsh attach-disk <VM-Series_name>/var/
lib/libvirt/images/PA-VM-6.1.0-c73.qcow2 sda --cache none --
persistent Disco conectado correctamente
```

STEP 4 | Modifique la plantilla XML en el cortafuegos VM-Series. En la plantilla XML debe cambiar el disco de destino y el bus de disco usados por el cortafuegos.

De manera predeterminada, la plantilla XML se almacena en 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>
```

Comprobación de PCI-ID para la ordenación de interfaces de red en el cortafuegos VM-Series

Independientemente de que use interfaces virtuales (puente Linux/OVS) o dispositivos PCI (envío PCI o un adaptador compatible con SR-IOV) para la conectividad con el cortafuegos VM-Series, este trata la interfaz como un dispositivo PCI. La asignación de una interfaz en el cortafuegos VM-Series se basa en PCI-ID, un valor que combina el bus, dispositivo o ranura y función de la interfaz. Las interfaces se ordenan empezando por el PCI-ID más bajo, lo que significa que la interfaz de gestión (eth0) del cortafuegos se asigna a la interfaz con el PCI-ID más bajo.

Por ejemplo, puede asignar cuatro interfaces al cortafuegos VM-Series: tres interfaces virtuales del tipo virtio y e1000, y la cuarta es un dispositivo PCI. Para ver el PCI-ID de cada interfaz, introduzca el

 ©2024 Palo Alto Networks, Inc.

comando **virsh dumpxml $ domain <*name of the VM-Series firewall*>** en el host Linux para ver la lista de interfaces adjuntas al cortafuegos VM-Series. En el resultado, compruebe la siguiente configuración de red:

```
<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>
```

En este caso, el PCI-ID de cada interfaz es el siguiente:

- El primer PCI-ID de interfaz virtual es 00:03:00
- El segundo PCI-ID de interfaz virtual es 00:10:00
- El tercer PCI-ID de interfaz virtual es 00:06:00
- El cuarto PCI-ID de interfaz virtual es 00:07:00

Por lo tanto, en el cortafuegos VM-Series, la interfaz con PCI-ID de 00:03:00 se asigna como eth0 (interfaz de gestión), la interfaz con PCI-ID 00:06:00 se asigna como eth1 (ethernet1/1), la interfaz con PCI-ID 00:07:00 es eth2 (ethernet1/2) y la interfaz con PCI-ID 00:10:00 es eth3 (ethernet1/3).

Configurar el protocolo de control de agregación de enlaces

La agregación de enlaces implica configurar un *grupo de interfaces de agregación de enlaces* y configurar el *Protocolo de control de agregación de enlaces*. Un grupo de interfaz de agregación utiliza la agregación de enlaces IEEE 802.1AX para combinar varias interfaces de Ethernet en una sola interfaz virtual que conecta el cortafuegos a otro dispositivo de red o cortafuegos. Este grupo de agregación aumenta el ancho de banda entre pares al equilibrar la carga de tráfico en las interfaces combinadas. También proporciona redundancia; cuando una interfaz falla, las interfaces restantes continúan manteniendo el tráfico.

Por defecto, la detección de fallos de interfaz es automática solo en la capa física, entre peers conectados directamente. Sin embargo, si habilita el protocolo de control de agregación de enlaces, la detección de fallos es automática en la capa física y de enlace de datos, independientemente de si los pares están conectados directamente. LACP también permite la conmutación por error automática a interfaces en espera si configura reservas activas.

Para configurar un grupo de interfaces de agregación y LACP, consulte Configurar un grupo de interfaces de agregación.

Crear una interfaz de Ethernet de agregación con Panorama

No añada máquinas virtuales de Panorama asociadas con funciones virtuales desde la misma función física a la misma interfaz de Ethernet de agregación. Hacerlo crea un bucle. Crear una interfaz de Ethernet de agregación:

 ©2024 Palo Alto Networks, Inc.

Configurar una interfaz de Ethernet de agregación:

1. Seleccione **Network (Red)>Interfaces>Ethernet** y **Add Aggregate Group (Añadir grupo de agregación)**.
2. En el campo adyacente a **Interface Name (Nombre de interfaz) de solo lectura,** introduzca un número para identificar el grupo de agregación. El intervalo es de 1 al número máximo de grupos de interfaz de agregación admitidos por el cortafuegos.
3. Para el **Interface Type (Tipo de interfaz)**, seleccione **HA**, **Virtual Wire**, **Layer 2 (Capa 2)** o **Layer 3 (Capa 3)**.
4. Configure los parámetros restantes para el **Interface Type** que seleccionó.
5. Confirme los cambios.

Después de crear la interfaz de agregación, agregue enlaces a ella.

Agregar enlaces a la interfaz de Ethernet de agregación

Para añadir enlaces a la interfaz de Ethernet de agregación:

STEP 1 | En Panorama, agregue una interfaz de Ethernet para actuar como oyente en modo pasivo para el par. Seleccione **Network (Red) > Interface (Interfaz)**.

STEP 2 | Seleccione una interfaz de Ethernet para actuar como un par.

STEP 3 | En la pantalla **Aggregate Ethernet Interface (Interfaz de Ethernet de agregación)**, seleccione **LACP**.

STEP 4 | Haga clic en **Enable LACP (Habilitar LACP)**.

STEP 5 | Asegúrese de que el modo es **Passive (Pasivo)**.

STEP 6 | Haga clic en **OK (Aceptar)**.

STEP 7 | Confirme los cambios en Panorama.

STEP 8 | Confirme el cambio de configuración. Haga clic en **Yes (Sí)**.

Crear la interfaz de Ethernet de agregación usando la CLI

Utilice los siguientes comandos de la CLI para crear una interfaz de Ethernet de agregación:

```
admin@PA-VM# set network interface aggregate-ethernet ae1 ae1 <value>
 Aggregate interface name: ae1 - ae16
```

Por ejemplo,

```
admin@PA-VM# set network interface aggregate-ethernet ae1
```

Asociar una interfaz secundaria usando la CLI

Utilice los siguientes comandos de la CLI para asociar una interfaz secundaria:

```
admin@PA-VM# set network interface ethernet ethernet1/1 aggregate-
group ae1 aggregate-ethernet ae1 <value> Aggregate interface group
```

 ©2024 Palo Alto Networks, Inc.

Por ejemplo,

```
set network interface ethernet ethernet1/1 aggregate-group ae1
```

Mostrar la configuración de la interfaz con la CLI

Utilice los siguientes comandos de la CLI para mostrar la configuración de la interfaz:

```
admin@PA-VM> show interface all total configured hardware
 interfaces: 4 name id speed/duplex/state mac address
 ------------------------------------------------------------------------------
 ethernet1/1 16 10000/full/up ba:db:ee:fb:ad:30 ethernet1/2
 17 10000/full/up 52:54:00:ce:8a:f5 ethernet1/3 18 10000/full/
up ba:db:ee:fb:ad:30 ae1 48 [n/a]/[n/a]/up ba:db:ee:fb:ad:30
 aggregation groups: 1 ae1 members: ethernet1/1 ethernet1/3 total
 configured logical interfaces: 2 name id vsys zone forwarding
 tag address ------------------- ----- ---- ----------------
 ------------------------ ------ ------------------ ethernet1/2 17 1
 trust vr:default 0 192.168.20.196/24 ae1 48 1 untrust vr:default 0
 192.168.10.110/24
```

Mostrar la configuración de la interfaz de Ethernet de agregación mediante la CLI

Utilice los siguientes comandos de la CLI para mostrar la configuración de la interfaz de Ethernet de agregación:

```
admin@PA-VM> show interface ae1
 ------------------------------------------------------------------------------
 Name: ae1, ID: 48 Link status: Runtime link speed/duplex/
state: [n/a]/[n/a]/up Configured link speed/duplex/state:
 auto/auto/auto MAC address: Port MAC address ba:db:ee:fb:ad:30
 Aggregate group members: 2 ethernet1/1 ethernet1/3
 Operation mode: layer3 Untagged sub-interface support: no
 ------------------------------------------------------------------------------
 Name: ae1, ID: 48 Operation mode: layer3 Virtual router default
 Interface MTU 1500 Interface IP address: 192.168.10.110/24
 Interface management profile: ae-mgmt-profile ping: yes telnet:
 no ssh: yes http: yes https: yes snmp: no response-pages: no
 userid-service: no Service configured: Zone: untrust, virtual
 system: vsys1 Adjust TCP MSS: no Ignore IPv4 DF: no Policing: no
 ------------------------------------------------------------------------------
 ------------------------------------------------------------------------------
 Physical port counters read from MAC:
 ------------------------------------------------------------------------------
 rx-broadcast 0 rx-bytes 7874426 rx-multicast 0 rx-unicast 151353
 tx-broadcast 0 tx-bytes 9320 tx-multicast 0 tx-unicast 130
 ------------------------------------------------------------------------------
 Hardware interface counters read from CPU:
 ------------------------------------------------------------------------------
 bytes received 3920 bytes transmitted 7406 packets received
 40 packets transmitted 123 receive incoming errors 0
 receive discarded 0 receive errors 0 packets dropped 0
 ------------------------------------------------------------------------------
 Logical interface counters read from CPU:
 ------------------------------------------------------------------------------
```

 ©2024 Palo Alto Networks, Inc.

```
 bytes received 7854114 bytes transmitted 7700 packets received
 150927 packets transmitted 130 receive errors 0 packets dropped
 150614 packets dropped by flow state check 0 forwarding errors 0 no
 route 0
```

Configurar la agregación de enlaces en el Switch utilizando la CLI

Active la agregación de enlaces en el switch:

```
int eth1/4 channel-group 1 mode on int eth1/8 channel-group 1 mode on
```

Verifique la configuración:

```
show running-config interface Ethernet 1/4 interface Ethernet 1/4 no
 lldp transmit no lldp receive no switchport Channel-group 1 mode on
 show running-config interface Ethernet 1/8 interface Ethernet 1/8 no
 lldp transmit no lldp receive no switchport Channel-group 1 mode on
```

 ©2024 Palo Alto Networks, Inc.

Ajuste de rendimiento de VM-Series para KVM

El cortafuegos VM-Series para KVM es un dispositivo de alto rendimiento pero puede requerir el ajuste del hipervisor para lograr los mejores resultados. Esta sección describe algunas de las prácticas recomendadas y recomendaciones para facilitar el mejor rendimiento del cortafuegos dVM-Series.

Por defecto, KVM utiliza un puente de linux para redes de máquinas virtuales. Sin embargo, el mejor rendimiento en un entorno virtual se realiza con interfaces de E/S dedicadas (PCI passthrough o SR-IOV). Si se requiere un conmutador virtual, utilice un conmutador virtual optimizado para el rendimiento (como Open vSwitch con DPDK).

- Instalación de KVM y Open vSwitch en Ubuntu 16.04.1 LTS
- Habilitación de Open vSwitch en KVM
- Integración de Open vSwitch con DPDK
- Habilitación de SR-IOV en KVM
- Habilitación del modo de acceso VLAN con SR-IOV
- Habilitación del soporte de múltiples colas para NIC en KVM
- Aislamiento de recursos de CPU en un nodo NUMA en KVM

Instalación de KVM y Open vSwitch en Ubuntu 16.04.1 LTS

Para facilitar la instalación, se recomienda utilizar Ubuntu 16.04.1 LTS como plataforma de hipervisor de KVM.

STEP 1 | Instale KVM y OVS.

1. Inicie sesión en la CLI de Ubuntu.
2. Ejecute los siguientes comandos:

```
$ sudo apt-get install qemu-kvm libvirt-bin ubuntu-vm-builder
 bridge-utils $ sudo apt-get install openvswitch-switch
```

STEP 2 | Verifique y compare las versiones de paquetes relevantes.

Ejecute los siguientes comandos:

```
$ 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
```

Habilitación de Open vSwitch en KVM

Habilite OVS modificando la configuración de red de la definición del XML invitado.

Modifique la definición del XML invitado de la siguiente manera.

 ©2024 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> [...]
```

Integración de Open vSwitch con DPDK

Para integrar Open vSwitch (OVS) con DPDK, debe instalar los componentes necesarios y, luego, configurar OVS. DPDK está habilitado de forma predeterminada en el cortafuegos VM-Series para KVM.

- Instalación de QEMU, DPDK y OVS en Ubuntu
- Configuración de OVS y DPDK en el host
- Edición del archivo de configuración de cortafuegos VM-Series

Instalación de QEMU, DPDK y OVS en Ubuntu

Antes de poder habilitar DPDK en OVS, debe instalar QEMU 2.5.0, DPDK 2.2.0 y OVS 2.5.1. Complete los siguientes procedimientos para instalar los componentes.

STEP 1 | Inicie sesión en el la CLI del host KVM.

STEP 2 | Instale QEMU 2.5.0 ejecutando los siguientes comandos:

```
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 | Instalar dpdk-2.2.0.

1. Ejecute los siguientes comandos:

   ```
   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. Cambiar `CONFIG_RTE_APP_TEST=y` to **`CONFIG_RTE_APP_TEST=n`**
3. Cambiar `CONFIG_RTE_BUILD_COMBINE_LIBS=n` to **`CONFIG_RTE_BUILD_COMBINE_LIBS=y`**
4. Ejecute el siguiente comando:

   ```
   vi GNUmakefile
   ```

5. Cambiar `ROOTDIRS-y := lib drivers app` to **`ROOTDIRS-y := lib drivers`**
6. Ejecute el siguiente comando:

   ```
   make install T=x86_64-native-linuxapp-gcc
   ```

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Instale OVS 2.5.1 ejecutando los siguientes comandos:

```
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
```

Configuración de OVS y DPDK en el host

Después de instalar los componentes necesarios para admitir OVS y DPDK, debe configurar el host para usar OVS y DPDK.

STEP 1 | Inicie sesión en el la CLI del host KVM.

STEP 2 | Si está sustituyendo o reconfigurando una configuración existente de OVS-DPDK, ejecute los siguientes comandos para restablecer cualquier configuración anterior. Repita el comando para cada interfaz.

```
rm /usr/local/var/run/openvswitch/<interface-name>
```

STEP 3 | Configure páginas grandes iniciales para OVS.

```
echo 16384 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```

STEP 4 | Monte páginas grandes para QEMU:

```
mkdir /dev/hugepages mkdir /dev/hugepages/libvirt mkdir /dev/
hugepages/libvirt/qemu mount -t hugetlbfs hugetlbfs /dev/hugepages/
libvirt/qemu
```

STEP 5 | Utilice el siguiente comando para eliminar cualquier daemon OVS existente actualmente.

```
killall ovsdb-server ovs-vswitchd
```

STEP 6 | Cree directorios para el daemon OVS.

```
mkdir -p /usr/local/etc/openvswitch
mkdir -p /usr/local/var/run/openvswitch
```

STEP 7 | Borre directorios antiguos.

```
rm -f /var/run/openvswitch/vhost-user*
rm -f /usr/local/etc/openvswitch/conf.db
```

STEP 8 | Inicialice la base de datos de configuración.

```
ovsdb-tool create /usr/local/etc/openvswitch/conf.db\
```

 ©2024 Palo Alto Networks, Inc.

```
/usr/local/share/openvswitch/vswitch.ovsschema
```

STEP 9 | Cree un servidor de base de datos 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 | Inicialice OVS.

```
ovs-vsctl --no-wait init
```

STEP 11 | Inicie el servidor de base de datos.

```
export DB_SOCK=/usr/local/var/run/openvswitch/db.sock
```

STEP 12 | Instale el módulo igb_uio (controlador de dispositivo de red) para 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 | Habilite DPDK en interfaces usando PCI-ID o el nombre de interfaz.

```
./dpdk_nic_bind.py --bind=igb_uio <your first data interface>
./dpdk_nic_bind.py --bind=igb_uio <your second data interface>
```

STEP 14 | Inicie el daemon OVS en modo DPDK. Puede cambiar el número de núcleos para ovs-vswitchd. Al cambiar -c 0x1 a -c 0x3, puede tener dos núcleos que ejecuten este daemon.

```
ovs-vswitchd --dpdk -c 0x3 -n 4 -- unix:$DB_SOCK --pidfile --
detach
echo 50000 > /sys/kernel/mm/hugepages/hugepages-2048kB/
nr_hugepages
```

STEP 15 | Cree el puente OVS y conecte los puertos al puente 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
```

 ©2024 Palo Alto Networks, Inc.

STEP 16 | Cree puertos DPDK vhost user para 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 | Establezca el número de colas de hardware de la NIC utilizada por el host.

```
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-rxqs=8
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-txqs=8
```

STEP 18 | Establezca la máscara de CPU utilizada para OVS.

```
ovs-vsctl set Open_vSwitch . other_config:pmd-cpu-mask=0xffff
```

STEP 19 | Establezca los permisos necesarios para los puertos DPDK vhost user. En el siguiente ejemplo, 777 se usa para otorgar permisos de lectura, escritura y ejecutables.

```
chmod 777 /usr/local/var/run/openvswitch/vhost-user1
chmod 777 /usr/local/var/run/openvswitch/vhost-user2
chmod 777 /dev/hugepages/libvirt/qemu
```

Edición del archivo de configuración de cortafuegos VM-Series

Edite el archivo de configuración XML del cortafuegos VM-Series para admitir OVS y DPDK. Puede acceder al archivo de configuración XML o después de implementar el cortafuegos VM-Series. Si hace esto después de implementar el cortafuegos, asegúrese de deshabilitar el cortafuegos antes de realizar cambios. Los valores que se encuentran a continuación son ejemplos, sus valores para cada parámetro variarán en función de su modelo VM-Series.

STEP 1 | Inicie sesión en el la CLI del host KVM.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Modifique el archivo de configuración XML del cortafuegos VM-Series.

1. Abra el archivo de configuración XML con **virsh edit $*<your-vm-series-name>***.
2. Establece el respaldo de memoria para la hugepage. Asegúrese de proporcionar suficiente memoria para admitir el modelo de cortafuegos VM-Series que está implementando en el host. Consulte Requisitos del sistema VM-Series para más información.

```
<memory unit='KiB'></memory> <currentMemory
 unit='KiB'>12582912 6291456</currentMemory> <memoryBacking>
 <hugepages/>
```

3. Establezca los indicadores de CPU necesarios para la VM.

```
<cpu mode='host-model'>
```

4. Habilite el uso compartido de memoria entre la VM y el host.

```
<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. Configure los puertos de usuario DPDK vhost como las interfaces de red del cortafuegos VM-Series. Además, establezca el número de colas virtuales virtio que el host proporciona al cortafuegos VM-Series.

```
<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>
```

Habilitación de SR-IOV en KVM

La virtualización de E/S de raíz única (SR-IOV) permite que un único dispositivo físico PCIe bajo un único puerto raíz parezca ser múltiples dispositivos físicos separados para el hipervisor o el invitado. Para habilitar SR-IOV en un invitado KVM, defina un conjunto de dispositivos de función virtual (VF) asociados con una NIC física y asigne automáticamente dispositivos VF desde el grupo a las ID de PCI.

Para SR-IOV con interfaces de red Intel 10 GB (controlador ixgbe), la versión del controlador debe ser 4.2.5 o posterior para admitir múltiples colas para cada interfaz NIC. Consulte la Matriz de compatibilidad para la compatibilidad de los controladores PacketMMAP y DPDK con la versión PAN-OS.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Defina una red para un grupo de VF.

1. Genere un archivo XML con texto similar al siguiente ejemplo. Cambie el valor de `pf dev` al `ethdev` correspondiente a la función física de su dispositivo SR-IOV.

   ```
   <network> <name>passthrough</name> <forward mode='hostdev'
    managed='yes'> <pf dev='eth3'/> </forward> </network>
   ```

2. Guarde el archivo XML.
3. Ejecute los siguientes comandos:

   ```
   $ virsh net-define <path to network XML file>  $ virsh net-
   autostart passthrough $ virsh net-start passthrough
   ```

STEP 2 | Para asegurarse de que el cortafuegos VM-Series se inicie en modo DPDK, edite la configuración XML de la máquina virtual invitada en el hipervisor KVM para añadir lo siguiente:

```
<cpu mode='host-passthrough' check='none'/>
```

Esto garantiza que los indicadores de la CPU estén expuestos.

Para comprobar que los indicadores de la CPU estén expuestos en la máquina virtual:

```
cat /proc/cpuinfo
```

En el resultado de los `indicadores` para PAN-OS 11.1 o posterior con DPDK 18.11, necesita los indicadores `AVX` o `AES`, y `SSE`.

STEP 3 | Después de definir e iniciar la red, modifique la definición del XML de invitado para especificar la red.

```
<interface type='network'> <source network='passthrough'> </
interface>
```

Cuando el huésped comienza, se asigna automáticamente una VF al invitado.

STEP 4 | Añada la dirección MAC de multidifusión al host.

Cuando se habilita SR-IOV, el tráfico de multidifusión se filtra mediante el PF. Este filtrado causa que las aplicaciones que confían en la multidifusión, como OSPF, fallen. Para evitar este filtrado, debe añadir manualmente las direcciones MAC de multidifusión al host usando el siguiente comando:

```
#ip maddress add <multicast-mac> dev <interface-name>
```

Habilitación del modo de acceso VLAN con SR-IOV

Los cortafuegos VM-Series en KVM pueden funcionar en modo de acceso VLAN para admitir casos de uso en los que se implementa como una función de red virtual (VNF) que ofrece seguridad como servicio en un entorno de centro de datos/nube de múltiples inquilinos. En el modo de acceso VLAN, cada VNF tiene interfaces de red virtual (VNI) dedicadas para cada red y envía y recibe paquetes a y desde las funciones virtuales (VF) de SR-IOV sin etiquetas VLAN; debe habilitar esta capacidad en las funciones

 ©2024 Palo Alto Networks, Inc.

físicas y virtuales en el hipervisor host. Cuando activa el modo de acceso VLAN en el cortafuegos VM-Series, el cortafuegos puede enviar y recibir tráfico sin etiquetas VLAN en todas sus interfaces de plano de datos. Además, si configura las políticas de QoS, el cortafuegos puede aplicar QoS en la interfaz de acceso y proporcionar un tratamiento diferenciado del tráfico en una implementación de múltiples inquilinos.

De forma predeterminada, el cortafuegos VM-Series en KVM funciona en modo troncal VLAN.

STEP 1 | En el sistema host, configure la función física y virtual para operar en modo de acceso VLAN.

`ip link set [inf_name] vf [vf_num] vlan [vlan_id]`.

Para obtener el mejor rendimiento en el cortafuegos VM-Series, asegúrese de:

- *Habilitar la fijación de CPU. Consulte* Aislamiento de recursos de CPU en un nodo NUMA en KVM.
- *Deshabilite la Protección de reproducción, si ha configurado Túneles IPSec.*

  En la interfaz web del cortafuegos, seleccione ***Network (Red)*** *>* ***IPSec Tunnels (Túneles IPSec)*** *seleccione un túnel IPSec, haga clic en* ***General*** *y seleccione* ***Show Advanced Options (Mostrar opciones avanzadas)*** *y deshabilite* ***Enable Replay Protection (Habilitar protección de reproducción)***.

STEP 2 | Acceda a la CLI en el cortafuegos VM-Series.

STEP 3 | Habilite el modo de acceso VLAN.

`request plugins vm-series vlan-mode access-mode on`

`on` habilita el modo de acceso VLAN; para usar el modo troncal VLAN, introduzca **`request plugins vm-series vlan-mode access-mode off`**.

STEP 4 | Reinicie el cortafuegos.

Introduzca **`solicitar reinicio del sistema`** .

STEP 5 | Verifique la configuración del modo VLAN.

`show plugins vm-series vlan-mode`

Habilitación del soporte de múltiples colas para NIC en KVM

Modifique la definición del XML invitado para habilitar multi-queue virtio-net. Virtio-net de colas múltiples permite que el rendimiento de la red escale con el número de vCPU y permite el procesamiento paralelo de paquetes a través de la creación de múltiples colas TX y RX.

Modifique la definición del XML invitado. Introduzca un valor de 1 a 256 para N para especificar el número de colas. Para obtener los mejores resultados, haga coincidir el número de colas con la cantidad de núcleos del plano de datos configurados en la máquina virtual.

 ©2024 Palo Alto Networks, Inc.

```
<interface type='network'> <source network='default'/> <model
 type='virtio'/> <driver name='vhost' queues='N'/> </interface>
```

Aislamiento de recursos de CPU en un nodo NUMA en KVM

Puede mejorar el rendimiento del VM-Series en KVM aislando los recursos de la CPU de la máquina virtual invitada en un nodo de acceso a la memoria no uniforme (NUMA) único. En KVM, puede ver la topología NUMA **virsh**. El siguiente ejemplo es de un sistema NUMA de dos nodos:

STEP 1 | Consulte la topología NUMA. En el siguiente ejemplo, hay dos nodos NUMA (sockets), cada uno con una CPU de cuatro núcleos con hyperthreading habilitado. Todos los ID de CPU de número par pertenecen a un nodo y todos los ID de CPU de número impar pertenecen al otro nodo.

```
% 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 | Fije vCPUs en un invitado KVM a vCPU físicas específicas, use el **cpuset** atributo en la definición de xml invitado. En este ejemplo, las 8 CPU virtuales se fijan a las CPU físicas en el primer nodo NUMA. Si no desea fijar explícitamente las vCPU, puede omitir el bloque**cputune**, en cuyo caso, todas las vCPU se fijarán al rango de CPU especificadas en cpuset, pero no se asignarán explícitamente.

```
<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>
```

 ©2024 Palo Alto Networks, Inc.

Descarga tráfico inteligente

El servicio de Descarga de tráfico inteligente (ITO) enruta los primeros paquetes de un flujo al cortafuegos para su inspección a fin de determinar si el resto de los paquetes del flujo deben inspeccionarse o descargarse. Esta decisión se basa en la política o en si el flujo se puede inspeccionar (por ejemplo, el tráfico cifrado no se puede inspeccionar). Al inspeccionar únicamente los flujos que pueden beneficiarse de la inspección de seguridad, la carga general en el cortafuegos se reduce en gran medida y el rendimiento del cortafuegos VM-Series aumenta sin sacrificar la seguridad.

Descarga de tráfico inteligente: Compatibilidad con la Capa 3 (enrutamiento estático y dinámico)

Intelligent Traffic Offload (ITO) es una suscripción de seguridad de cortafuegos VM-Series. Cuando ITO se configura en el VM-Series con la infraestructura NVIDIA Bluefield DPU compatible en su proceso subyacente, este aumenta la capacidad de rendimiento del cortafuegos.

En versiones anteriores, ITO requería que se implementara el cortafuegos VM-Series en Modo de cable virtual. Esta limitación impedía las implementaciones en modo de Capa 3 que admitían enrutamiento estático o dinámico. Esta versión elimina esa limitación, ya que le permite implementar el cortafuegos VM-Series con descarga de tráfico inteligente para el tráfico L3 compatible con enrutamiento estático y dinámico.

Con el enrutamiento dinámico, se obtiene un enrutamiento L3 estable, de alto rendimiento y alta disponibilidad a través de listas de filtrado basadas en perfiles y mapas de ruta condicionales que se pueden utilizar en enrutadores lógicos. Estos perfiles proporcionan una granularidad más detallada para filtrar rutas para cada protocolo de enrutamiento dinámico y mejorar la redistribución a través de varios protocolos. Cuando se combina con NAT para IPv4, puede ampliar la política de seguridad para proteger los dispositivos de los usuarios finales de la exposición a amenazas externas.

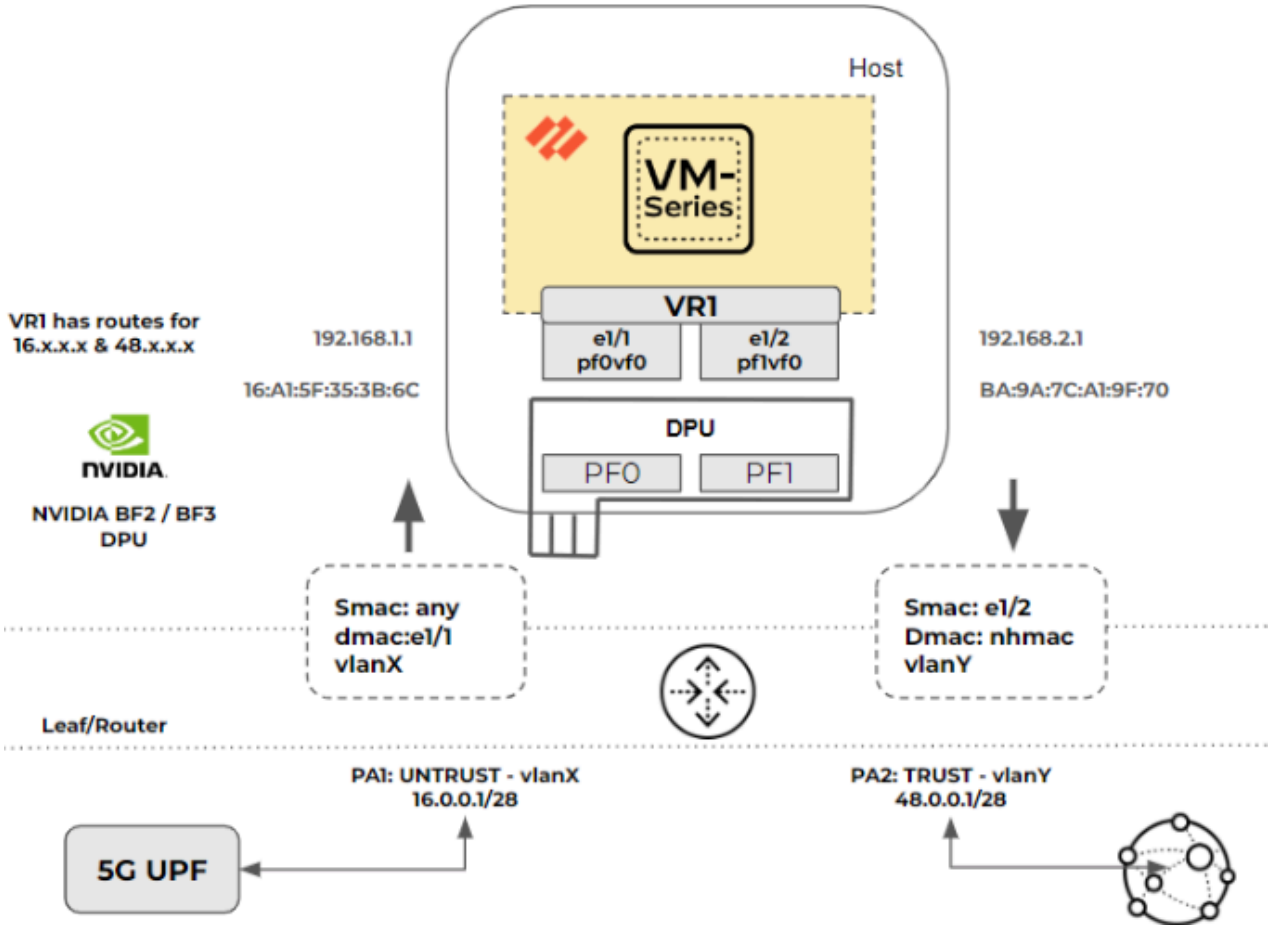
Además, puede utilizar la descarga de tráfico inteligente para NAT (IPv4). La misma limitación anterior, que requería que implementara el cortafuegos VM-Series en modo de cable virtual, ahora se ha eliminado en esta versión, lo que le permite implementar el cortafuegos con una suscripción ITO mediante NAT para la seguridad perimetral. Ahora puede implementar su suscripción de ITO en el modo de Capa 3 que admite NAT para IPv4, lo que proporciona características de seguridad sólidas que evitan que los dispositivos de los usuarios finales estén expuestos a amenazas externas.

La compatibilidad con NAT se extiende a NAT44 y DIPP para ambas implementaciones con descarga de tráfico inteligente (basada en DPU) y software de corte para la inspección del tráfico.

El nuevo modo de Capa 3 realmente amplía su capacidad de aprovechar la seguridad dentro de sus centros de datos, confiando en cortafuegos para conmutar y enrutar el tráfico a los dominios de red.

La siguiente figura muestra cómo funciona el flujo de paquetes en el modo de capa 3. Muestra el host utilizando NVIDIA BlueField DPU y ramificación/enrutador.

 ©2024 Palo Alto Networks, Inc.



En la figura anterior, el flujo de paquetes tiene las siguientes características:

- Las interfaces e1/1 y e1/2 están configuradas en modo de Capa 3.
- VR1 se configura con rutas estáticas o dinámicas al enrutador de capa 3 5G o un UPF y al enrutador del par de Internet.
- Se admite el tráfico etiquetado y sin etiquetar. El enrutador y la DPU o NIC pueden estar en modo de acceso o troncal.

Este es el proceso de flujo de paquetes para el modo de Capa 3:

1. El paquete se envía desde el UPF 5G (enrutador de Capa 3) a la ramificación/enrutador de Capa 3.
2. El paquete llega al puerto del enrutador PA1 que está conectado a DPU y SmartNIC PF0 y que está programado para agregar una etiqueta vlanX a los paquetes.
3. El paquete llega al puerto DPU pf0vf0 y se entrega al VM-Series con o sin quitar la VLAN.
4. El cortafuegos se está ejecutando en modo L3. Este encuentra el siguiente salto del paquete y su dirección MAC.
5. El cortafuegos actualiza la DPU y SmartNIC a través de gRPC con la nueva MAC de destino y vlanY, si es necesario.
6. El paquete etiquetado con vlanY llega al puerto PA2 del enrutador desde el puerto PF1 de DPU/SmartNIC.
7. Si el paquete no estaba etiquetado, el puerto PA2 del enrutador puede agregar la etiqueta vlanY.

 ©2024 Palo Alto Networks, Inc.

8. El paquete se envía a la dirección del siguiente salto y se entrega al par de Internet. En el caso del enrutamiento dinámico, con cualquier actualización de ruta, el VM-Series actualiza la DPU con la nueva dirección MAC del siguiente salto.

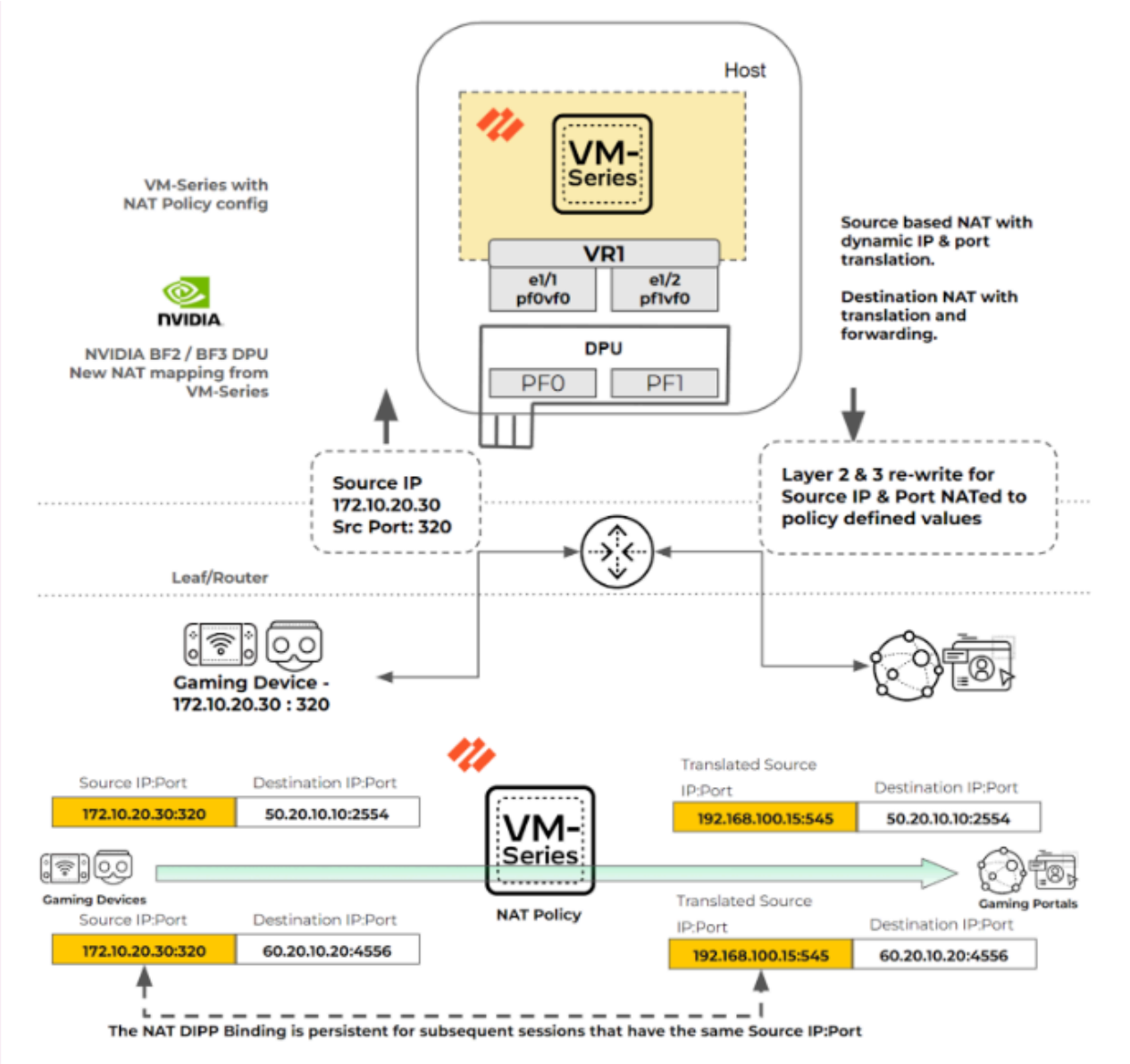
Descarga de tráfico inteligente: Compatibilidad con NAT para Virtual Wire y L3

Por lo general, en las implementaciones de 5G y ciertos entornos empresariales de hiperescala, el NGFW virtual de la serie VM-Series protege el perímetro de Internet o el tráfico norte-sur. En este tipo de implementaciones, puede aprovechar el modo NAT para asegurarse de que los dispositivos de los usuarios finales no estén expuestos a Internet.

Palo Alto Networks proporciona soporte NAT con capacidades ITO tanto en modo de implementación de cable virtual (vWire) como de capa 3. Ahora puede configurar varios modos de NAT con IPv4, como NAT de origen con traducción dinámica de puertos e IP, traducción de puertos NAT de destino y reenvío.

La siguiente imagen ilustra cómo funciona esto desde el punto de vista del flujo de paquetes. Ilustra los puertos de origen y destino para dispositivos de juego a través de portales de juegos.

 ©2024 Palo Alto Networks, Inc.



Así es como se configura la política NAT:

- La VM-Series tiene la política NAT configurada para realizar la asignación de NAT de origen para IP y puerto a IP dinámica y puerto.
- La política NAT definida también puede realizar la traducción y el reenvío de puertos e IP de destino.

Este es el proceso de flujo de paquetes cuando se configura una política NAT:

1. El paquete se envía desde el dispositivo 5G a través del enrutador 5G UPF o de Capa 3 con una dirección IP y puerto de origen 172.10.20.30:320.
2. El paquete llega al cortafuegos VM-Series, donde se define la política NAT para realizar la traducción de NAT de origen a dirección IP dinámica y puerto. La IP de origen: El puerto 172.10.20.30:320 se traduce a 192.168.100.15:545.
3. El cortafuegos VM-Series realiza una reescritura de capa 2 y capa 3 en el paquete en función de la política NAT definida, que puede ser NAT de origen con traducción dinámica de direcciones IP y puertos o NAT de destino con traducción y reenvío de puertos.

 ©2024 Palo Alto Networks, Inc.

4. El cortafuegos VM-Series actualiza la DPU y SmartNIC a través de gRPC con la traducción NAT.
5. El DIPP de SNAT mantiene la persistencia mediante la conservación del enlace de una dirección IP de origen privado y un par de puertos a una dirección IP de origen pública (traducida) específica y un par de puertos para sesiones posteriores con la misma dirección IP de origen original y el mismo par de puertos. En este caso, 172.10.20.30:320 y su dirección traducida 192.168.100.15:545 son persistentes para múltiples direcciones IP de destino:Puertos.

Descarga de tráfico inteligente: Requisitos

ITO requiere un cortafuegos VM-Series y una DPU BlueField-2 instalados en el mismo host físico x86. Se admite la alta disponibilidad activa/pasiva para los cortafuegos VM-Series.

Puede implementar solo un cortafuegos VM-Series y una DPU BlueField-2 por host.

- Conmutador de red con 2 puertos de 100 GB/s disponibles (4 para HA).

  Si desea utilizar VLAN, asegúrese de que su conmutador sea compatible.
- Requisitos de hardware del host físico X86.
  - Mínimo 64 GB de RAM disponible (64 GB para servidor / 56 GB para cortafuegos VM-Series)
  - Mínimo 8 núcleos físicos
  - Bluefield-2 SmartNIC MBF2M516A-CEEOT con dos puertos de 100GB/s instalados en la ranura PCI-e 3 o 4
  - Un SFP de 100 GigE certificado para cada puerto de la DPU BlueField2, según lo recomendado por la Guía del usuario de la DPU NVIDIA BlueField Ethernet.
- Requisitos de software de host X86:
  - Ubuntu 18.04, con la versión del kernel 4.15.0-20
  - Versión de flujo de arranque binario de Bluefield: 5.3-1.0.0.1

    Acepte el Acuerdo de licencia de usuario final para iniciar la descarga.
- Máquina virtual para el cortafuegos VM-Series.
  - PAN-OS 11.0 o posterior.
  - Complemento de VM-Series 2.1.0 o posterior.
  - Para autorizar a la descarga de tráfico inteligente, cree un perfil de implementación de software NGFW para 10.0.4 y superior, con un mínimo de 8 vCPU y el servicio de descarga de tráfico inteligente. El perfil puede incluir otros servicios de seguridad.

    Con PAN-OS 10.1.1 o posterior y el complemento de VM-Series 2.1.1 o posterior, para autorizar la descarga de tráfico inteligente, cree un perfil de implementación de software NGFW para 10.0.4 y posterior, con un mínimo de ocho (8) CPU virtuales y el Servicio de descarga de tráfico inteligente. El perfil puede incluir otros servicios de seguridad.

Descarga de tráfico inteligente: Interfaces

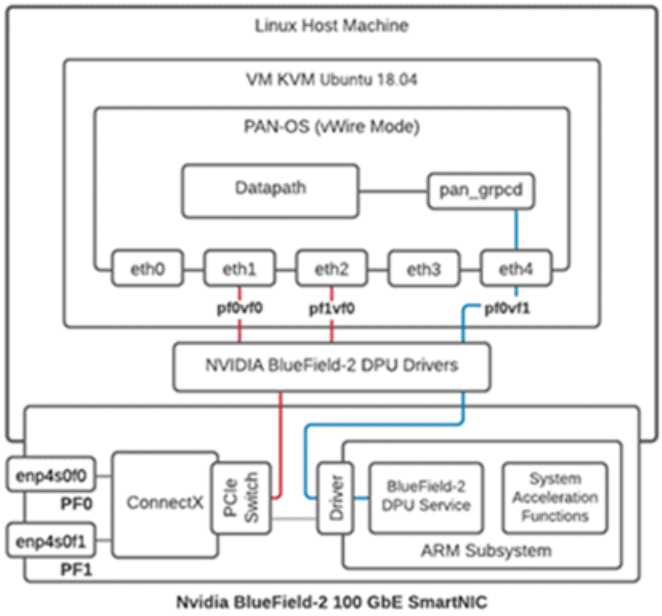
Una implementación de descarga de tráfico inteligente conecta tres tipos de interfaces:

 ©2024 Palo Alto Networks, Inc.

- Interfaces virtuales PAN-OS:
  - eth0: interfaz de gestión
  - eth1, eth2: plano de datos
  - eth3: Interfaz de HA
  - eth4: interfaz gRPC
- Interfaces físicas de DUPU BlueField-2 (creadas a partir del sistema operativo host).
- Interfaces físicas del host para los puertos de DPU BlueField-2 de 100 GB (creados a partir del sistema operativo host).

Las interfaces PAN-OS se conectan a la DPU BlueField-2 a través de las funciones virtuales (VF) de SR-IOV que crea en el host físico.

En la siguiente figura, los dos puertos DPU BlueField-2 se muestran como funciones físicas PF0 y PF1. Estos PF se pueden observar desde el lado del host como enp4s0f0 y enp4s0f1, y se dividen en múltiples funciones virtuales (VF) para la funcionalidad SR-IOV.



- La primera función virtual para cada PF debe ser el puerto de datos (eth1: pf0vf0).
- Se requiere un función virtual adicional para el canal de control de la interfaz cliente/servidor de gRPC (eth4: pf0v1).
- Las FV del lado del host son las siguientes:
  - enp4s0f0 está representada por pf0vf0 y pf1vf0 en la DPU BlueField-2 y se utilizan para datos.
  - enp4s0f1 está representada por pf0vf1 y se utiliza para el tráfico de control de gRPC.

Descarga de tráfico inteligente: Escalabilidad

Las limitaciones de capacidad de ampliación actuales de la DPU NVIDIA BlueField-2 son las siguientes:

- Capacidad de la mesa de sesiones: 500.000 sesiones
- Tasa de actualización de la tabla de sesiones: 7000 sesiones/segundo

 ©2024 Palo Alto Networks, Inc.

- Conexiones por segundo: 20.000
- Tasa de horquilla de descarga: aprox. 90 Gbps para paquetes de 1500 bytes

Si el tráfico de descarga a la DPU BlueField-2 supera las 7.000 sesiones por segundo, o la tabla de sesiones de descarga está llena, el tráfico aún fluye a través del cortafuegos VM-Series y se inspecciona. Cuando las sesiones por segundo caen por debajo de 7.000, se reanuda la descarga de tráfico inteligente a la DPU Bluefield-2.

La HA activa / pasiva es compatible con los cortafuegos VM-Series que se ejecutan en hosts físicos con configuraciones idénticas.

La descarga de tráfico inteligente no admite la configuración de sesión *de envejecimiento acelerado.*

Descarga de tráfico inteligente: High Availability

La alta disponibilidad activa/pasiva es compatible con ambos modos de implementación, Vwire y Capa 3, para un par de cortafuegos VM-Series.

- Los cortafuegos deben instalarse en hosts físicos con la DPU BlueField-2 configurada como se especifica en Descarga de tráfico inteligente: Requisitos.
- Para la interfaz HA2 (consulte las figuras en Flujo de paquetes activo y Flujo de paquetes pasivo), utilice la misma interfaz Mellanox (cx-3, cx-4 o cx-5) en ambos hosts.

  Las interfaces de alta disponibilidad se pueden configurar en cualquier NIC de otro proveedor compatible con los cortafuegos de software.
- (opcional) Para soportar la conmutación de tráfico, los hosts deben estar en VLAN independientes para que pueda usar etiquetas de VLAN para seleccionar la principal.

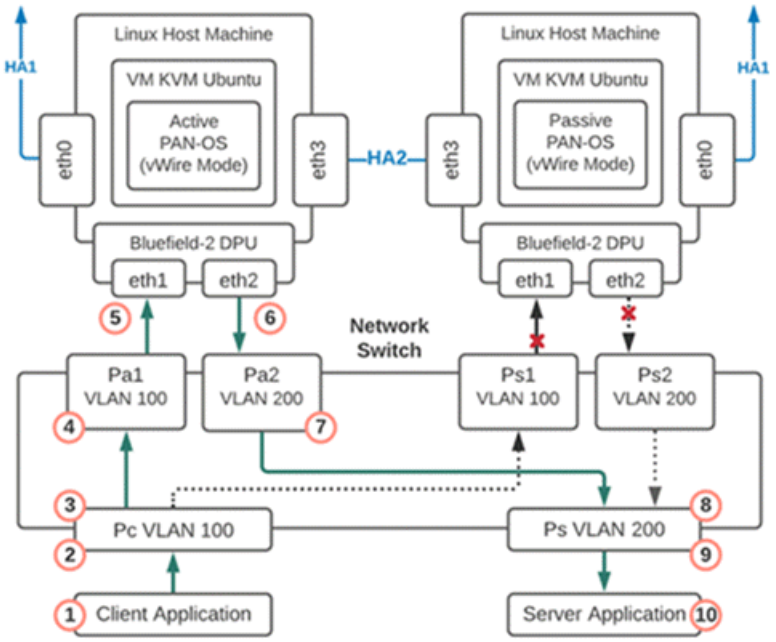
La descarga inteligente del tráfico en el VM-Series en alta disponibilidad se centra en la disponibilidad del cortafuegos VM-Series. Cada cortafuegos mantiene una tabla de sesiones y cada DPU BlueField-2 mantiene una tabla de flujo. La configuración de HA sincroniza la tabla de sesión activa, lo que garantiza que se refleje en el cortafuegos pasivo durante el tiempo de ejecución. La tabla de sesiones almacena tanto las sesiones que requieren inspección como las que están marcadas para su descarga.

HA utiliza la interfaz PAN-OS eth3, que se encuentra en una NIC en el cortafuegos VM-Series. Eth3 se utiliza para seleccionar el cortafuegos activo y sincronizar las tablas de sesiones del cortafuegos VM-Series en el par activo/pasivo.

Flujo de paquetes activo

En el siguiente diagrama se muestran los pasos del flujo de paquetes activo para una configuración de alta disponibilidad en un modo de implementación vWire que utiliza una configuración de VLAN opcional. La configuración de alta disponibilidad y el flujo de paquetes seguirán siendo similares para el modo de implementación de capa 3.

 ©2024 Palo Alto Networks, Inc.



1. El paquete se envía desde la aplicación cliente al conmutador de red.
2. El paquete llega al puerto del conmutador que está programado para añadir una etiqueta VLAN 100 a los paquetes.
3. Los paquetes etiquetados solo pueden ir al puerto Pa1 ya que la interfaz para el puerto Ps1 está inactiva porque ese cortafuegos está en modo pasivo.
4. El paquete llega al puerto Pa1 y la VLAN 100 se elimina del paquete y el paquete se entrega al cortafuegos eth1.
5. El cortafuegos se ejecuta en modo vWire, por lo que el cortafuegos procesa el paquete y luego envía eth2.

   Si el cortafuegos se está ejecutando en modo L3, encontrará el siguiente salto del paquete y su dirección MAC. A continuación, el cortafuegos actualizará la DPU y SmartNIC a través de gRPC con la nueva MAC y VLAN de destino, si es necesario.
6. El paquete llega al puerto Pa2 y se añade la VLAN 200.
7. El paquete se envía al puerto Pa2 y solo se puede entregar al puerto Ps porque el otro puerto Ps2 de la VLAN 200 está inactivo.
8. El paquete llega al puerto Ps y la etiqueta VLAN 200 se elimina.
9. El paquete se envía por el puerto Ps sin etiqueta VLAN
10. El paquete se entrega al servidor.

Evento de conmutación por error

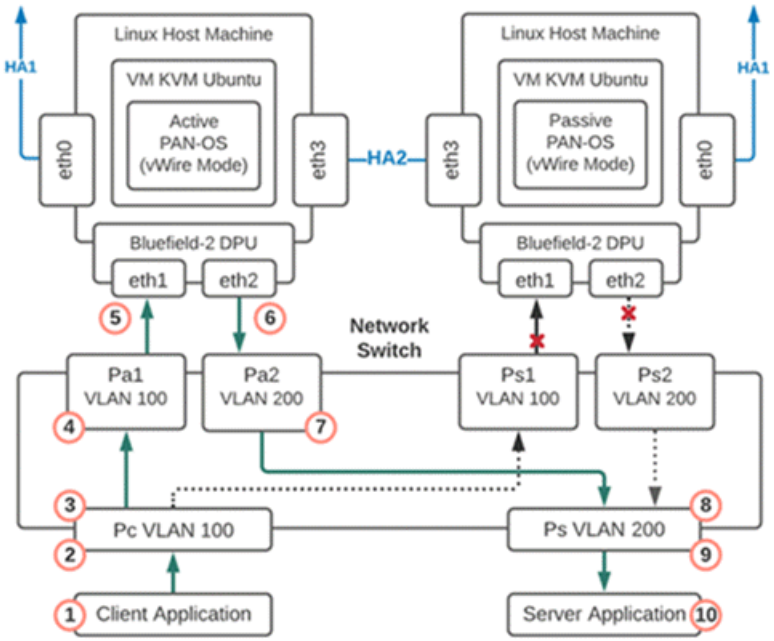
Un evento de conmutación por error ocurre cuando hay una notificación del cortafuegos activo VM-Series o el cortafuegos pasivo detecta que el activo no responde. Cuando esto sucede, las conexiones de red a los puertos Pa1 y Pa2 se desactivan y las conexiones de red a los puertos Ps1 y Ps2 se activan.

Flujo de paquetes pasivo

Cuando el cortafuegos VM-Series está en estado pasivo, la DPU BlueField-2 en el miembro pasivo está activa, pero no pasa tráfico hasta que se produce una conmutación por error y el cortafuegos VM-Series

 ©2024 Palo Alto Networks, Inc.

coubicado se activa. El siguiente diagrama recorre el flujo de paquetes pasivo para una configuración de alta disponibilidad que usa una configuración de VLAN opcional.



1. El paquete se envía desde la aplicación cliente al conmutador de red.
2. El paquete llega al puerto del conmutador que está programado para añadir una etiqueta VLAN 100 a los paquetes.
3. Los paquetes etiquetados solo pueden ir al puerto Ps1 porque la interfaz para el puerto Pa1 está inactiva y ese cortafuegos ahora ha pasado de pasivo a activo.
4. El paquete llega al puerto Ps1 y la VLAN 100 se elimina del paquete, y el paquete se entrega al cortafuegos eth1.
5. El cortafuegos se ejecuta en modo vWire, por lo que el cortafuegos procesa el paquete y luego envía eth2.

   Si el cortafuegos se está ejecutando en modo L3, encontrará el siguiente salto del paquete y su dirección MAC. A continuación, el cortafuegos actualizará la DPU y SmartNIC a través de gRPC con la nueva MAC y VLAN de destino, si es necesario
6. El paquete llega al puerto Ps2 y se añade la VLAN 200.
7. El paquete se envía al puerto Ps2 y solo se puede entregar al puerto Ps porque el otro puerto Pa2 de la VLAN 200 está inactivo.
8. El paquete llega al puerto Ps y la etiqueta VLAN 200 se elimina.
9. El paquete se envía por el puerto Ps sin etiqueta VLAN.
10. El paquete se entrega al servidor.

Instalación de la DPU BlueField-2

Instale la DPU BlueField-2 en el host físico antes de instalar el cortafuegos VM-Series:

1. Instale la DPU BlueField-2 en la máquina host como se indica en la Guía del usuario de la NVIDIA DPU BlueField Ethernet.

 ©2024 Palo Alto Networks, Inc.

2. Instale los controladores BlueField como se indica en la Guía de inicio rápido del software NVIDIA DPU BlueField-2.

Instale el cortafuegos VM-Series

La instalación estándar de KVM en el cortafuegos VM-Series instala PAN-OS. Siga los pasos de instalación en las siguientes secciones.

- VM-Series en KVM: especificaciones y requisitos previos
- Instalación del cortafuegos VM-Series en Hyper-V o Instalación del cortafuegos VM-Series utilizando un archivo ISO

Habilitar funciones virtuales

Como se mencionó en Descarga de tráfico inteligente: Interfaces las funciones virtuales (VF), conecte las interfaces PAN-OS a la DPU BlueField-2.

El número máximo de funciones virtuales VF por puerto es 2. Necesita un total de tres: dos para la ruta de datos y uno para la interfaz de gestión.

STEP 1 | Habilite las funciones virtuales en la máquina host.

- De forma predeterminada, la DPU BlueField-2 usa la primera VF para la ruta de datos, es decir, enp4s0f0v0 y enp4s0f1v0 en el siguiente ejemplo.
- La otra VF, enp4s0f0v1, se utiliza para la interfaz de gestión del servicio que se ejecuta en la tarjeta BlueField-2 (no se debe confundir con la interfaz de gestión del cortafuegos 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
```

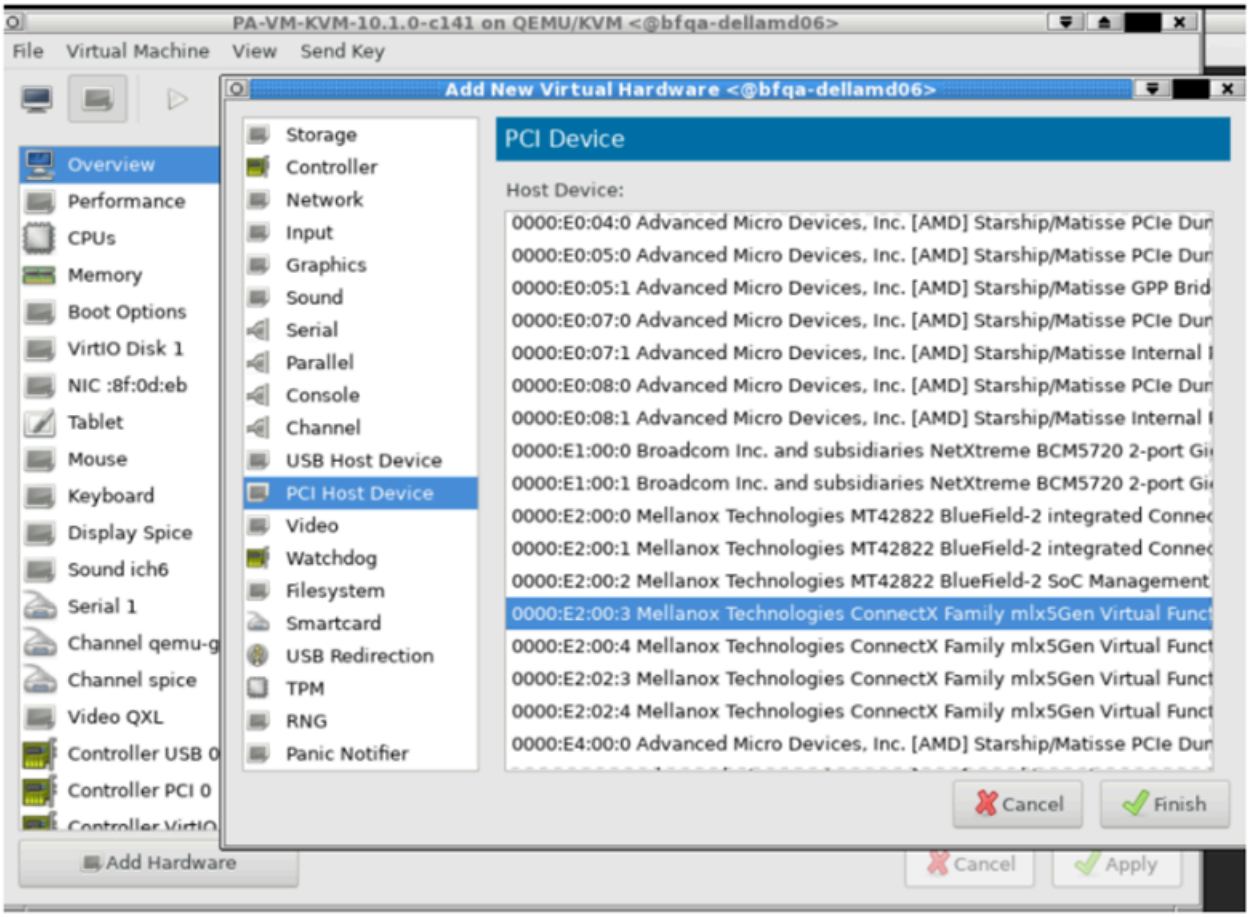
$ echo 2 > **/sys/class/net/enp4s0f1/device/sriov_numvfs**

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Asigne las VF al cortafuegos VM-Series desde el hipervisor KVM.

El PAN-OS invitado no se iniciará a menos que se asignen VF a la VM.

1. Apague la máquina virtual.
2. En KVM, use virt-manager para añadir la VF a la VM.
   - Seleccione Añadir hardware, seleccione VF0 de PF1 y haga clic en Finalizar.
   - Seleccione Añadir hardware, seleccione VF0 de PF0 y haga clic en Finalizar.
   - Seleccione Añadir hardware, seleccione VF1 de PF0 y haga clic en Finalizar.



Compruebe el sistema DPU BlueField-2

La DPU BlueField-2 se comunica primero con el host cuando el controlador Rshim está instalado en el host. El Rshim proporciona una interfaz tty (accesible a través de minicom) y una interfaz de red llamada tmfifo_net0. Con la interfaz tmfifo_net0, puede acceder a la DPU BlueField-2 desde el host. El controlador Rshim se ejecuta en el sistema operativo Hypervisor x86 y, de hecho, la instalación de OFED instala un controlador Rshim de forma predeterminada.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Inicie sesión en la máquina host.

```
$ ssh user@<host-ip-address>
```

```
$ password:
```

STEP 2 | Si la interfaz de red del host para el controlador Rshim no tiene una dirección IP, debe crear una.

```
$ ip addr add dev tmfifo_net0 192.168.100.1/24
```

STEP 3 | Desde la máquina host, inicie sesión en el subsistema BlueField-2 DPU.

```
$ ssh ubuntu@192.168.100.2
```

```
$ password: <fake-password>
```

Si es su primer inicio de sesión, el sistema le solicita que reemplace la contraseña predeterminada por una nueva.

STEP 4 | Cambie la contraseña predeterminada en la DPU BlueField-2.

Inicie sesión en BlueField-2 DPU con el nombre de usuario inicial como **ubuntu** y la contraseña **ubuntu**.

Una vez que inicie sesión, el sistema le solicitará que configure una nueva contraseña.

```
ADVERTENCIA: Su contraseña ha caducado. ¡Debe cambiar su contraseña
 ahora e iniciar sesión nuevamente! Cambiar la contraseña para
 ubuntu. Contraseña actual: ***** Nueva contraseña: ***** Vuelva a
 escribir la nueva contraseña: ***** passwd: contraseña actualizada
 correctamente
```

Cierre sesión e inicie sesión con su nueva contraseña.

STEP 5 | Compruebe la versión del software.

```
$ ofed_info -s
```

Esto debería devolver la siguiente versión o posterior:

```
$ MLNX_OFED_LINUX-5.3-0.3.3
```

STEP 6 | Compruebe que la DPU Bluefield 2 esté en el modo correcto.

El modo correcto es el modo de propiedad de la función de CPU incorporada. Consulte la documentación del Modo de propiedad de la función de CPU integrada para obtener instrucciones sobre cómo comprobar y configurar el modo.

 ©2024 Palo Alto Networks, Inc.

Instale o actualice el software BlueField Bootstream

Siga estos pasos para asegurarse de tener el último software de flujo de arranque de Bluefield (BFB) para la DPU BlueField-2. El BFB incluye el sistema operativo BlueField y otro software como controladores e interfaces de red.

STEP 1 | Descargue el paquete BFB en el host físico de la DPU BlueField-2.

Obtenga la última versión del controlador para el sistema operativo que se ejecuta en los núcleos DPI ARM en el sitio web de NVIDIA; debe aceptar el acuerdo de licencia de usuario final para descargar.

STEP 2 | Instale el BFB desde la ubicación de inicio de Rshim en el host físico.

Tenga en cuenta que el nombre de archivo a continuación (la cadena que comienza con **DOCA** y finaliza con **.bfb**) no contiene espacios. Introduzca el comando en una sola línea.

```
$ 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 | Inicie sesión en la DPU BlueField-2.

Utilice la nueva contraseña que creó en Compruebe el sistema DPU BlueField-2.

```
$ ssh ubuntu@192.168.100.2
```

```
$ password:
```

STEP 4 | Aplique la actualización de firmware en la DPU BlueField-2.

Introduzca el siguiente comando en una sola línea.

```
$ sudo /opt/mellanox/mlnx-fw-updater/firmware/mlxfwmanager_sriov_dis_aarch64_41686
```

STEP 5 | Apague y encienda el sistema.

Cierre la sesión de la DPU BlueField-2 y vuelva al host Linux.

```
$ ipmitool chassis power cycle
```

STEP 6 | Inicie sesión en la DPU BlueField-2.

```
$ ssh ubuntu@192.168.100.2
```

```
$ password:
```

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Inicie el servicio opof (descarga abierta) en la DPU BlueField-2. opof es un servicio independiente en este momento.

Las VF deben existir antes de iniciar opof.

```
$ opof_setup_highavail
$ service opof restart
```

STEP 8 | Verifique que el servicio opof se esté ejecutando sin problemas.

```
$ service opof status
```

Instalar o actualizar el paquete Debian

Si la versión del paquete Debian es anterior a la 1.0.4, debe actualizar.

STEP 1 | En la DPU BlueField-2, verifique la versión del paquete opof.

```
$ opof -v
```

Si es anterior a 1.7.4, debe actualizarse.

Si es anterior a 1.0.4, debe actualizarse.

STEP 2 | Añada el repositorio de NViIDIA para paquetes.

```
$ cd /etc/apt/sources.list.d
```

Introduzca cada comando `wget` todo en una línea. No hay espacios en las 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 | En la DPU BlueField-2, compruebe el paquete Debian en el repositorio.

```
$ apt buscar opof
```

```
Ordenando... Búsqueda de texto completo realizada... Done opof/now
 1.0.4 arm64 [installed,local] Nvidia Firewall Open Offload Daemon
```

STEP 4 | En ARM, desinstale el paquete Debian obsoleto.

```
$ apt eliminar opof
```

STEP 5 | Instale el nuevo paquete Debian.

```
$ apt instalar opof
```

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Configure y reinicie el servicio opof.

```
$ opof_setup
$ service opof restart
```

STEP 7 | Verifique que el servicio opof se esté ejecutando sin problemas.

```
$ service opof status
```

Ejecute la Descarga de tráfico inteligente

Esta solución requiere una suscripción al servicio de descarga de tráfico inteligente y un mínimo de 8 núcleos físicos en el host físico para obtener el mejor rendimiento. Por ejemplo, en un VM-Series de 10 vCPU de forma predeterminada, PAN-OS asigna 2 núcleos para la descarga inteligente de tráfico, 2 núcleos para los procesos de gestión y los 4 núcleos restantes para el procesamiento del plano de datos.

- Configurar la Descarga de tráfico inteligente en el cortafuegos VM-Series
- Configurar el servicio de descarga de tráfico inteligente en la DPU BlueField-2
- Iniciar o reiniciar el servicio de descarga de tráfico inteligente
- Obtener el estado y el estado del servicio

Configure la descarga de tráfico inteligente en el cortafuegos VM-Series

Siga estos pasos para habilitar la descarga de tráfico inteligente en PAN-OS.

STEP 1 | Abra la VM de PAN-OS. Esto supone que ya tiene una instancia de VM creada y la está reiniciando.

$ **virsh start <vm-name>**

STEP 2 | Utilice SSH para iniciar sesión en la interfaz de administración del cortafuegos VM-Series.

$ **ssh admin@<panos-management-IP-address>**

```
$ admin@PA-VM>
```

STEP 3 | Verifique que Intelligent Traffic Offload esté instalado y tenga licencia.

admin@PA-VM> **show intelligent-traffic-offload**

```
Descarga inteligente de tráfico:   Configuración           :
 Habilitada   Operación habilitada        : Verdadero   Paquete
 de número mínimo        : 8   Tasa mínima                 :
 95   Envejecimiento TCP              : 12-   Envejecimiento
 UDP               : 20
```

`Configuración: habilitada` significa que Intelligent Traffic Outload tiene licencia.

`Operación habilitada: Verdadero` significa que ha reiniciado un dispositivo configurado.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Habilitar la descarga de tráfico inteligente.

Utilice el siguiente comando para habilitar ITO.

admin@PA-VM> **set session offload yes**

También puede usar **set session offload no** para deshabilitar la ITO sin reiniciar el sistema.

*Utilice el comando **set session offload** sin reiniciar cuando habilite la función por primera vez. Sin embargo, si decide deshabilitar ITO más adelante, debe reiniciar. Además, si elige habilitar ITO después de implementar el cortafuegos, debe reiniciar. En el caso de entornos de ITO sin DPU o de software de corte, no es necesario reiniciar.*

STEP 5 | Validar la descarga de tráfico inteligente.

admin@PA-VM> **show session info | match offload**

```
Descarga de sesiones de hardware: Verdadero
```

Para ver contadores globales, use el siguiente comando:

admin@PA-VM> **show counter global | match flow_offload**

Configurar el servicio de descarga de tráfico inteligente en la DPU BlueField-2

El servicio se debe compilar como se describe en Configurar la descarga de tráfico inteligente en el cortafuegos VM-Series.

STEP 1 | Desde la máquina host, inicie sesión en el complejo DPU BlueField-2.

$ **ssh ubuntu@192.168.100.2**

```
$ password: <fake-password> $ ubuntu> sudo -i
```

STEP 2 | Configure la configuración preliminar en el sistema operativo DPU BlueField-2.

root@bf2SmartNIC:~# **opof_setup_highavail**

```
[ INFO ] No num of hugepages specified, use 2048 [ INFO ] No gRPC
 port specified, use pf0vf1
```

Iniciar o reiniciar el servicio de descarga de tráfico inteligente

Si el servicio de ITO se está ejecutando en una DPU, es probable que el servicio se inicie automáticamente. Para verificar el estado, ejecute el siguiente comando:

$ service opof status

Si el servicio opof no se está ejecutando, introduzca el siguiente comando para iniciar el controlador:

$ service opof start

Para reiniciar el servicio, ejecute el siguiente comando:

$ service opof restart

 ©2024 Palo Alto Networks, Inc.

Obtener estado y salud del servicio

Utilice opof para obtener el estado y la salud del servicio. Cada comando tiene su propia ayuda en la línea de comandos, por ejemplo: **$ opof -h**

- Consultar una sesión:

  $ opof query -i <session_id>
- Estadísticas de descarga del servicio de consultas:

  $ opof stats

Solución de problemas de la DPU BlueField-2

Utilice el siguiente procedimiento para apagar y encender el sistema.

1. Para apagar y encender el sistema, cierre la sesión de la DPU BlueField-2 y vuelva al sistema operativo del host Linux.

   $ ipmitool chassis power cycle
2. Si las interfaces no aparecen después del ciclo de energía, inicie sesión en la DPU BlueField-2 e introduzca:

   $ / sbin / mlnx_bf_configure
3. Vuelva al sistema operativo host e introduzca:

   $ sudo /etc/init.d/openibd restart

Descarga de tráfico inteligente: Resolución de problemas de tráfico

Validar flujos de tráfico

El tráfico de datos puede generarse desde el cliente y consumirse a través de la configuración de descarga de tráfico inteligente por un servidor. IPERF3 se puede utilizar para generar tráfico, como se explica en Ejecutar pruebas de IPERF3. Una vez que se inicia el tráfico, los primeros paquetes del flujo se envían al PA-VM, que decide si el flujo debe descargarse o no.

Se debe definir unapolítica de anulación de la aplicación para identificar los flujos de descarga. Un flujo de TCP establece el indicador FIN/RST en un paquete de control y lo envía a la PA-VM. Cuando la PA-VM decide descargar el flujo, use show session all para mostrar los flujos descargados. Use **<flowID>** para proporcionar información sobre el estado del flujo. Un flujo descargado tiene el estado `Descarga: sí`.

Los contadores de flujo no se actualizan mientras los paquetes subsiguientes del flujo están en el estado de descarga y pasan por la DPU BlueField-2. Una vez que se completa el flujo, el servicio de descarga activa un temporizador de vencimiento (vencimiento de TCP configurado desde la CLI). Cuando el temporizador expira, el servicio recopila las estadísticas de flujo actualizadas y las envía al cortafuegos VM-Series. Luego, el cortafuegos actualiza sus contadores de sesiones de flujo y **muestra el ID de sesión <flowID>** y devuelve los valores actualizados.

Contadores de sesiones

Utilice el siguiente comando para ver los contadores de sesiones.

admin@PA-VM > **show counter global | match flow_offload**

 ©2024 Palo Alto Networks, Inc.

Las columnas de salida para cada contador son:

Nombre del contador | Valor | Tasa | Severidad | Categoría | Aspecto | Descripción.

- Valor: número de ocurrencias desde el inicio del sistema.
- Tasa: frecuencia de cambio del contador.
- Severidad: información, advertencia, caída. Se utiliza para la asistencia técnica.
- Categoría: flujo (un componente de una sesión).
- Aspecto: descarga para un flujo completo.

Nombre del contador	Description (Descripción)
flow_offload_rcv_cpu	Número de paquetes recibidos por la CPU con sesión descargada
flow_offload_session_update	Número de veces que es necesario actualizar la sesión
flow_offload_session_insert	Número de sesiones insertadas en el dispositivo de descarga
flow_offload_session_delete	Número de sesiones eliminadas del dispositivo de descarga
flow_offload_delete_msg_failed	Número de mensajes de eliminación a GRPC que fallaron
flow_offload_add_msg_failed	Número de mensajes de sesión a GRPC que fallaron
flow_offload_session_verify	Número de mensajes de verificación al dispositivo de descarga
flow_offload_verify_msg_failed	Número de mensajes de verificación a GRPC que fallaron
flow_offload_update_session_stat	HW indica antigüedad del flujo
flow_offload_missing_session_stat	No se puede encontrar la sesión para las estadísticas
flow_offload_invalid_session	Descargar ID de sesión no válida
flow_offload_del_session_fail	Descargar Eliminar sesión no válida
flow_offload_add_session_fail	Descargar Añadir sesión ha fallado
flow_offload_get_session_fail	Fallo de obtención de sesión de descarga
flow_offload_grpc_fail	No fue posible realizar la llamada de grpc de descarga
flow_offload_active_session	Número de sesiones descargadas activas
flow_offload_aged_session	Número de sesiones descargadas obsoletas
flow_offload_session	Número de sesiones descargadas

 ©2024 Palo Alto Networks, Inc.

Ejecutar pruebas de IPERF3

Iperf3 es una aplicación opcional sencilla para generar tráfico que es eficaz para ejecutar pruebas de tráfico de datos. Para ejecutar el servidor como un servicio, use **`iperf3 -s -D`**. De forma predeterminada, la aplicación espera paquetes en el puerto de destino TCP/UDP 5201, pero el puerto se puede cambiar.

- Flujo único: para flujos iperf3 únicos, introduzca:

```
iperf3 -c <server-ip-address> -t 60
```

- Múltiples flujos: para iniciar 20 flujos simultáneos durante 60 segundos, introduzca:

```
iperf3 -c <ip of server> -P 20 -t 60
```

Validación de logs de descarga de tráfico inteligente

Puede utilizar los logs del cortafuegos VM-Series para validar la conectividad entre el cliente ITO que se ejecuta en el cortafuegos y el servicio de descarga en la DPU BlueField-2. La salida de log prevista para una descarga correcta es la siguiente.

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
```

Resolución de problemas de OPOF

También puede ver los registros del servicio de descarga para validar la conectividad:

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 (límite: 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:
 0000:03:00.1 (socket 0) May 21 18:40:38 localhost.localdomain
```

 ©2024 Palo Alto Networks, Inc.

```
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]: Escucha del servidor en: 169.254.33.51:3443
```

Los registros muestran que Intelligent Traffic Offload se está comunicando con el cortafuegos VM-Series de VM PA-VM a través del `servidor que escucha` la dirección IP, y usted ve los VF junto con otros detalles de los parámetros de DPDK. También se adjunta un log de la adición de un flujo de un flujo TCP que se descarga.

 ©2024 Palo Alto Networks, Inc.

Descarga basada en software de corte

Si su entorno no es compatible con DPU o requiere un cortafuegos de nueva generación basado en contenedores y el tipo de tráfico tiene flujos descargables, puede aprovechar la descarga basada en software de corte. Con el fin de configurar el software de corte, su cortafuegos (PAN-OS) se puede configurar para implementar software de corte en el software para realizar descargas.

El software de corte es capaz de comprender el tráfico GTP-U y, por lo tanto, ayudará a aumentar el rendimiento gestionado para los casos de uso de seguridad 5G. Con el software de corte habilitado, dentro de la GTPU, la sesión interna completa la inspección de paquetes L7 y luego sigue la ruta de datos del software de corte existente. Evita las operaciones innecesarias y aprovecha la caché para completar la operación, mejorando así la gestión del rendimiento y el rendimiento del cortafuegos de software.

Al utilizar el software de corte, tenga en cuenta:

- El software de corte está desactivado de forma predeterminada en los cortafuegos de software. Puede habilitar esta función mediante el arranque o la CLI en los VM y CN-Series.
- En la serie VM-Series, puede utilizar el software de corte y el ITO simultáneamente.
- Para las actualizaciones a la versión actual con ITO habilitado, habilite la descarga de sesión con software de corte mediante la CLI después de la actualización.
- En los cortafuegos basados en software, si planea usar software de corte, necesita un mínimo de 6 núcleos.
- Puede utilizar el software de corte en los cortafuegos basados en software implementados en un entorno local, como KVM o ESXi, o en una nube pública, como AWS, Azure o GCP

Configuración de la descarga basada en el software de corte para una máquina virtual implementada mediante la CLI

Utilice la CLI para habilitar el software de corte en el cortafuegos VM-Series sin compatibilidad con hardware. El software de corte está desactivado de forma predeterminada.

1. Acceda al cortafuegos VM-Series como administrador.
2. Utilice el comando CLI **set session sw-cut-thru yes** para habilitar la función software cut-through.
3. Para deshabilitar la función software cut-through, introduzca **set session sw-cut-thru no**.

Configurar la descarga basada en software de corte utilizando el arranque, bootstrap.

Para configurar el software de corte mediante bootstrap, añada lo siguiente en el archivo **init-cfg.txt**:

plugin-op-commands=sw_cut_through:enable

Para deshabilitar el software de corte mediante bootstrap:

plugin-op-commands=sw_cut_through disable



*Para mostrar el estado del software de corte, utilice **show session info | match "Software Cut Through" (Mostrar información de sesión | hacer coincidir con "Software de corte"**.*

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en Hyper-V

El cortafuegos VM-Series se puede implementar en un servidor que ejecuta Microsoft Hyper-V. Hyper-V viene empaquetado como un hipervisor independiente o como un complemento/función para Windows Server.

- Implementaciones compatibles con Hyper-V
- Requisitos del sistema en Hyper-V
- Servicios de integración de Linux
- Instalación del cortafuegos serie VM en Hyper-V

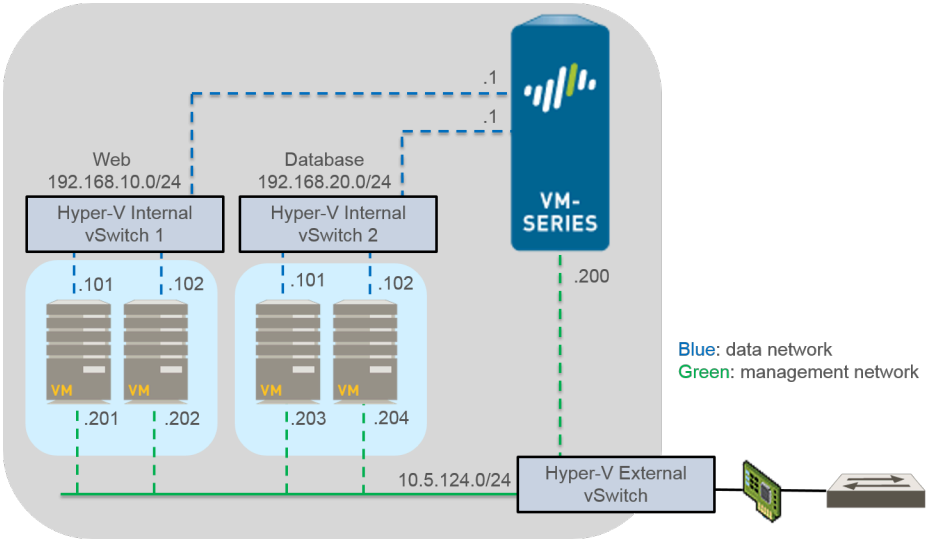
Implementaciones compatibles con Hyper-V

Puede implementar una o varias instancias del cortafuegos VM-Series en hosts ejecutando Hyper-V. La ubicación del cortafuegos VM-Series dependerá de la topología de su red. VM-Series acepta implementaciones de interfaces tap, virtual wire, Layer 2 y Layer 3.

- Protección del tráfico en un host Hyper-V único
- Protección del tráfico en hosts Hyper-V múltiples

Protección del tráfico en un host Hyper-V único

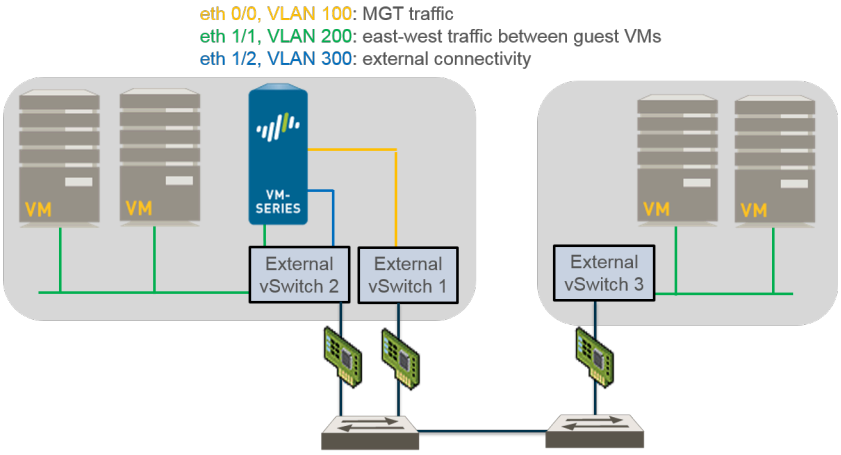
El cortafuegos VM-Series se implementa en un host Hyper-V único junto con otros VM invitados. En el ejemplo siguiente, el cortafuegos VM-Series tiene una interfaz Layer 3 y VM-Series y otros VM invitados se conectan con vSwitches de Hyper-V. Todo el tráfico entre los servidores web y los servidores de bases de datos se dirige a través del cortafuegos. El tráfico solamente a través de las servidores de bases de datos o solamente servidores web se procesa con el vSwitch externo y no se dirige a través del cortafuegos.



Protección del tráfico en hosts Hyper-V múltiples

Puede implementar su cortafuegos VM-Series para proteger el tráfico de host Hyper-V múltiples. En el ejemplo siguiente, el VM-Series se implementa en modo Layer 2 para proteger el tráfico a y desde VM invitados. Un cortafuegos VM-Series protege el tráfico entre cuatro VM invitados desplegados en dos hosts Hyper-V. Se usa el etiquetado VLAN para aislar lógicamente el tráfico y dirigirlo al cortafuegos. Además, el tráfico de gestión se desacopla del tráfico restante con la colocación de su propio vSwitch.

©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

Requisitos del sistema en Hyper-V

El VM-Series necesita una asignación mínima de recursos en el host Hyper-V, para cumplir con los requisitos que se citan a continuación y garantizar un funcionamiento óptimo.

- La CPU del host debe ser una CPU Intel o AMD de 64-bits x86 con extensión de virtualización.
- Consulte Requisitos del sistema VM-Series para ver los requisitos mínimos de hardware para su modelo VM-Series.
- Mínimo de dos adaptadores de red. El cortafuegos VM-Series acepta adaptadores de red sintéticos, que ofrecen mejor rendimiento que los adaptadores de red emulados. Hyper-V acepta hasta ocho adaptadores de red sintéticos.
- Consulte la matriz de compatibilidad para obtener información sobre las versiones de Windows Server compatibles.

  Hyper-V Server no tiene una interfaz de usuario gráfica nativa; toda la configuración se hace a través de PowerShell. Sin embargo, puede usar el gestor de Hyper-V en una máquina virtual para gestionar el cortafuegos. Si usa el plugin de la función de Hyper-V, podrá gestionar el cortafuegos usando el gestor de Hyper-V o PowerShell.
- El cortafuegos de la serie VM admite SR-IOV/PCI-Passthrough.

  DPDK solo es compatible con dispositivos SRIOV de Nvidia/Mellanox (Mlx5). No se admite el modo troncal con SR-IOV.

 ©2024 Palo Alto Networks, Inc.

Servicios de integración de Linux

Servicios de integración de Linux (LIS) es un paquete de controladores y servicios que mejoran el rendimiento de máquinas virtuales basadas en Linux en Hyper-V. El cortafuegos VM-Series es compatible con los siguientes servicios para mejorar la integración entre el host y la máquina virtual:

- **Apagado correcto**: Le permite realizar un apagado correcto del cortafuegos VM-Series desde la interfaz de gestión de Hyper-V sin tener que iniciar sesión en el invitado.
- **Heartbeat al gestor de Hyper-V**: Proporciona monitorizado heartbeat del estado de funcionamiento de los VM invitados desde la interfaz de gestión de Hyper-V.
- **Visibilidad de dirección IP de gestión de cortafuegos**: Le permite utilizar el gestor de Hyper-V para visualizar la dirección IP asignada a la interfaz de gestión del cortafuegos.

 ©2024 Palo Alto Networks, Inc.

Instalación del cortafuegos serie VM en Hyper-V

Use las instrucciones de esta sección para implementar su cortafuegos VM-Series en un host Hyper-V. Se necesita una cuenta de soporte de Palo Alto Networks y una licencia de VM-Series válida para descargar el archivo de imagen de VHDX e instalar el VM-Series en el host Hyper-V. Si no ha registrado todavía el código de autenticación de capacidad que ha recibido con el correo electrónico de cumplimiento del pedido, con su cuenta de asistencia técnica, consulte Registro del cortafuegos VM-Series. Después de completar el registro, continúe realizando las siguientes tareas:

- Antes de comenzar
- Ajuste de rendimiento del cortafuegos VM-Series en Hyper-V
- Provisión de cortafuegos VM-Series en un host Hyper-V con gestor de Hyper-V
- Provisión de cortafuegos VM-Series en un host Hyper-V con PowerShell
- Configuración inicial del cortafuegos VM-Series

Antes de comenzar

Antes de instalar y configurar su cortafuegos VM-Series, conozca y contabilice los siguientes elementos, según sea necesario, cuando configure su cortafuegos VM-Series:

- Tipos de conmutadores virtuales
- Replicación de dirección IP

Tipos de conmutadores virtuales

Antes de instalar el VM-Series, debe crear los vSwitches necesarios para proporcionar conectividad externa para el acceso de gestión y para dirigir el tráfico a y desde las máquinas virtuales que protege el cortafuegos. Hyper-V le permite crear tres tipos de vSwitches:

- **vSwitch externo**: Se conecta a un adaptador de red físico y proporciona al vSwitch acceso a una red física.
- **vSwitch interno**: Pasa el tráfico entre las máquinas virtuales y el host Hyper-V. Este tipo de vSwitch no proporciona conectividad a una conexión de red física.
- **vSwitch privado**: Pasa el tráfico solamente entre las máquinas virtuales y el host Hyper-V.

Se necesita un vSwitch externo para instalar el cortafuegos VM-Series. Otros vSwitches conectados al cortafuegos VM-Series pueden ser de cualquier tipo y dependerá de la topología de su red.

Replicación de dirección IP

Si está implementando el cortafuegos VM-Series con interfaces habilitadas en modo Layer 3, asegúrese de habilitar el uso de las direcciones MAC asignadas al hipervisor, de modo que el hipervisor y cortafuegos pueden manejar los paquetes correctamente. De forma alternativa, utilice el gestor de Hyper-V para habilitar la replicación de direcciones MAC en el adaptador de red virtual para la interfaz del plano de datos del cortafuegos. Para obtener más información, consulte Direcciones MAC asignadas por el hipervisor.

Si está implementando el cortafuegos VM-Series con interfaces habilitadas en modo Layer 2 o modo virtual-wire, debe habilitar la replicación de direcciones MAC en el adaptador de red virtual de Hyper-V para cada interfaz del plano de datos del cortafuegos. Este ajuste es necesario para asegurarse de que los

 ©2024 Palo Alto Networks, Inc.

paquetes enviados por el VM-Series no son descartados por el adaptador de red virtual si la dirección MAC no coincide con la dirección MAC de la interfaz saliente.

Ajuste de rendimiento del cortafuegos VM-Series en Hyper-V

El cortafuegos VM-Series para Hyper-V es un dispositivo de alto rendimiento pero puede requerir el ajuste del hipervisor para lograr los mejores resultados. Esta sección describe algunas de las prácticas recomendadas y recomendaciones para facilitar el mejor rendimiento del cortafuegos dVM-Series.

- Deshabilitación de colas de máquina virtual
- Aislamiento de recursos de CPU en un nodo NUMA

Deshabilitación de colas de máquina virtual

Palo Alto Networks recomienda deshabilitar las colas de máquina virtual (virtual machine queues, VMQ) para todas las NIC en el host de Hyper-V. Esta opción es propensa a errores de configuración y puede reducir el rendimiento de red cuando está habilitada.

STEP 1 | Inicie sesión en Hyper-V Manager y seleccione su máquina virtual.

STEP 2 | Seleccione **Settings (Configuración)** > **Hardware** > **Network Adapter (Adaptador de red)** > **Hardware Acceleration (Aceleración de hardware)**.

STEP 3 | En la cola de la máquina virtual, retire la selección de **Enable virtual machine queue (Habilitar cola de máquina virtual)**.

STEP 4 | Haga clic en **Apply (Aplicar)** para guardar sus cambios y **OK (Aceptar)** para salir de la configuración de VM.

Aislamiento de recursos de CPU en un nodo NUMA

Puede mejorar el rendimiento de VM-Series para Hyper-V aislando los recursos de la CPU de la máquina virtual invitada en un solo nodo de acceso a la memoria no uniforme (NUMA). Puede ver la configuración NUMA de su VM en Hyper-V Manager seleccionando **Settings (Configuración)** > **Hardware** > **Processor (Procesador)** > **NUMA**.

Provisión de cortafuegos VM-Series en un host Hyper-V con gestor de Hyper-V

Utilice estas instrucciones para implementar el cortafuegos VM-Series en Hyper-V utilizando el gestor de Hyper-V.

STEP 1 | Descargue el archivo VHDX.

Registre su cortafuegos VM-Series y obtenga el archivo VHDX.

1. Vaya a https://www.paloaltonetworks.com/services/support.
2. Filtre por **PAN-OS for VM-Series Base Images (PAN-OS para imágenes base de VM-Series)** y descargue el archivo VHDX. Por ejemplo, PA-VM-HPV-7.1.0.vhdx.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configure el vSwitch o vSwitches que necesitará.

Para crear un vSwitch:

1. En el gestor de Hyper-V, seleccione el host y seleccione **Action (Acción)** > **Virtual Switch Manager (Gestor de conmutadores virtuales)** para abrir la ventana del gestor de conmutadores virtuales.
2. Bajo **Create virtual switch (Crear conmutador virtual)**, seleccione el tipo de vSwitch (externo, interno o privado) para su creación y haga clic en **Create virtual switch (Crear conmutador virtual)**.

STEP 3 | Instale el cortafuegos.

1. En el gestor de Hyper-V, seleccione el host y seleccione **Action (acción)** > **New (Nuevo)** > **Virtual Machine (Máquina virtual)**. Configure los siguientes ajustes en el asistente de nueva máquina virtual:
   1. Elija un **Name (Nombre)** y **Location (Ubicación)** para el cortafuegos VM-Series. El cortafuegos VM-Series guarda el archivo VHDX en la ubicación especificada.
   2. Elija **Generation 1 (Generación 1)**. Es la opción por defecto y la única versión compatible.
   3. Para **Startup Memory (Memoria de inicio)**, asigne la memoria basada en los Requisitos del sistema VM-Series de su modelo VM-Series.

      No habilite la memoria dinámica; el cortafuegos VM-Serie necesita asignación de memoria estática.

   4. Configure **Networking**. Seleccione un vSwitch externo para conectar la interfaz de gestión en el cortafuegos.
   5. Para conectar el **Virtual Hard Disk (Disco duro virtual)**, seleccione **Use an existing virtual hard disk (Usar un disco duro virtual existente)** y navegue hasta el archivo VHDX descargado anteriormente.
   6. Revise el resumen y haga clic en **Finish (Finalizar)**.
2. Asigne las CUP virtuales al cortafuegos.
   1. Seleccione el VM creado y vaya a **Action (acción)** > **Settings (Configuración)**.
   2. Seleccione **Processor (Procesador)** e introduzca la cantidad mínima de CPU basada en los Requisitos del sistema VM-Series de su modelo VM-Series .
   3. Haga clic en **OK (Aceptar)**.

STEP 4 | Conecte al menos un adaptador de red para la interfaz del plano de datos en el cortafuegos.

1. Seleccione **Settings (Configuración)** > **Hardware** > **Add Hardware (Añadir hardware)** y seleccione **Hardware type (Tipo de hardware)** para su adaptador de red.

   No son compatibles adaptadores de red heredados y SR-IOV. Si se selecciona, el cortafuegos VM-Series se reiniciará en el modo de mantenimiento.

2. Haga clic en **OK (Aceptar)**.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | (Opcional) Habilite la replicación de direcciones MAC en Hyper-V si no está utilizando Layer 3 con dirección MAC asignada al hipervisor.

1. Haga doble clic en el adaptador de red virtual del plano de datos y haga clic en **Ajustes avanzados**.
2. Haga clic en **Enable MAC address spoofing (Habilitar duplicación de direcciones MAC)** seleccione la casilla y haga clic en **Apply (Aplicar)**.

STEP 6 | Inicie el cortafuegos.

Seleccione el cortafuegos de la lista **Virtual Machines (Máquinas virtuales)** y vaya a **Action (Acción)** > **Start (Iniciar)** para iniciar el cortafuegos.

Provisión de cortafuegos VM-Series en un host Hyper-V con PowerShell

Utilice estas instrucciones para implementar el cortafuegos VM-Series en Hyper-V utilizando PowerShell.

STEP 1 | Descargue el archivo VHDX.

Registre su cortafuegos VM-Series y obtenga el archivo VHDX.

1. Vaya a https://www.paloaltonetworks.com/services/support.
2. Filtre por **PAN-OS for VM-Series Base Images (PAN-OS para imágenes base de VM-Series)** y descargue el archivo VHDX. Por ejemplo, PA-VM-HPV-7.1.0.vhdx**.**

STEP 2 | Configure el vSwitch o vSwitches que necesitará.

Cree un vSwitch utilizando los comando siguientes. Asigne un nombre al vSwitch y elija el tipo de conmutador.

```
> New-VMSwitch -Name <"switch-name"> -SwitchType <switch-type>
```

STEP 3 | Instale el cortafuegos VM-Series.

1. Cree la nueva máquina virtual y establezca la memoria en función de los Requisitos del sistema VM-Series de su modelo VM-Series.

```
> NEW-VM -Name <vm-name> -MemoryStartupBytes 4GB -
VHDPath <file-path-to-vhdx>
```

2. Establezca el recuento del procesador en función de los requisitos del sistema de VM-Series de su modelo VM-Series.

```
> SET-VMProcessor –VMName <vm-name> –Count 2
```

STEP 4 | Conecte al menos un adaptador de red para la interfaz de gestión del cortafuegos.

Conecte el adaptador de red por defecto creado durante la creación del VM para el vSwitch de gestión.

```
> connect-VMNetworkAdapter -vmname <vm-name> -Name <"network-
adapter-name"> -SwitchName <"management-vswitch">
```

 ©2024 Palo Alto Networks, Inc.

STEP 5 | (Opcional) Habilite la replicación de direcciones MAC en Hyper-V si no está utilizando Layer 3 con dirección MAC asignada al hipervisor.

```
> Set-VMNetworkAdapter -vmname <vm-name> -Name <"network-adapter-name"> -MacAddressSpoofing On
```

STEP 6 | Inicie el cortafuegos.

Por ejemplo:

```
> Start-VM -vmname <vm-name>
```

Configuración inicial del cortafuegos VM-Series

Use estas instrucciones para realizar la configuración inicial de su cortafuegos VM-Series. De forma predeterminada, el cortafuegos VM-Series usa DHCP para obtener una dirección IP para la interfaz de gestión. Sin embargo, puede asignar una dirección IP estática. Después de completar la configuración inicial, acceda a la interfaz web para completar otras tareas de configuración. Si usa Panorama para la gestión central, consulte la Guía del administrador de Panorama para saber más sobre la gestión del dispositivo mediante Panorama.

Si está utilizando bootstrapping para realizar la configuración del cortafuegos VM-Series en Hyper-V, consulte Arranque del cortafuegos VM-Series en Hyper-V. Para obtener más información sobre el arranque, consulte Arranque del cortafuegos serie VM.

STEP 1 | Obtenga la información necesaria de su administrador de red.

- Dirección IP de puerto de gestión
- Máscara de red
- Puerta de enlace predeterminada
- Dirección IP de servidor DNS

STEP 2 | Acceda a la consola del cortafuegos VM-Series.

1. En el gestor de Hyper-V, seleccione el cortafuegos VM-Series y haga clic en **Conectar** en la lista de acciones.
2. Inicie sesión en el cortafuegos con el nombre de usuario y contraseña por defecto: **admin/admin**
3. Acceda al modo de configuración con el siguiente comando: **configure**

STEP 3 | Defina la configuración de acceso a la red para la interfaz de gestión.

Introduzca los siguientes comandos:

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> Máscara de
 red <netmask>
```

 ©2024 Palo Alto Networks, Inc.

```
default-gateway <gateway-IP> dns-settingservers primary <DNS-IP>
```

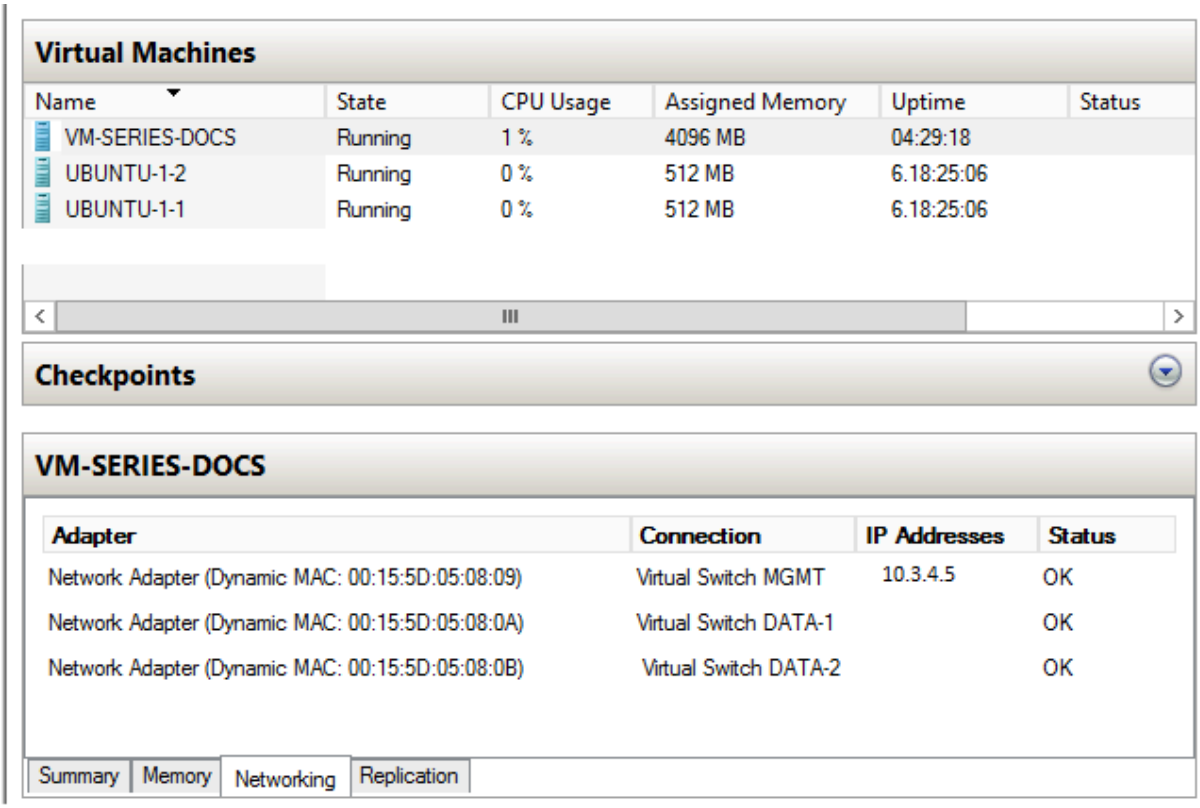
donde <*Firewall-IP*> es la dirección IP que quiere asignar a la interfaz de gestión, <*netmask*> es la máscara de subred, <*gateway-IP*> es la dirección IP de la puerta de enlace de la red e <*DNS-IP*> es la dirección IP del servidor DNS.

STEP 4 | Confirme los cambios y salga del modo de configuración.

1. Introduzca **commit (confirmar)**.
2. Introduzca **exit (salir)**.

STEP 5 | Verifique que puede ver la dirección IP de la interfaz de gestión del gestor de Hyper-V.

1. Seleccione el cortafuegos VM-Series de la lista de **Virtual Machines (Máquinas virtuales)**.
2. Seleccione **Networking**. El primer adaptador de red que se muestra en la lista se utiliza para el acceso de gestión al cortafuegos; los posteriores adaptadores de la lista se utilizan como interfaces del plano de datos del cortafuegos.



STEP 6 | Verifique el acceso a la red para los servicios externos requeridos para la gestión del cortafuegos, como el servidor de actualizaciones de Palo Alto Networks.

1. Compruebe la utilidad del ping para verificar la conectividad de red al servidor de actualizaciones de Palo Alto Networks como se muestra en el siguiente ejemplo. Verifique que la

 ©2024 Palo Alto Networks, Inc.

resolución DNS se produzca y la respuesta incluya la dirección IP del servidor de actualización; el servidor de actualización no responde a una solicitud de 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
```

Cuando haya comprobado la resolución DNS, pulse Ctrl+C para detener la solicitud de ping.

2. Use el siguiente comando de la CLI para recuperar información sobre el derecho a la asistencia técnica para el cortafuegos desde el servidor de actualizaciones de Palo Alto Networks:

```
request support check
```

Si tiene conectividad, el servidor de actualizaciones responde con el estado de asistencia para el cortafuegos.

STEP 7 | (Opcional) Verifique que su configuración de trama gigante en VM-Series no supera la MTU máxima aceptada en Hyper-V.

VM-Series tiene un tamaño de MTU por defecto de 9216 bytes cuando se habilitan las tramas gigantes. Sin embargo, el tamaño máximo de MTU aceptado por el adaptador de red físico del host Hyper-V es de 9000 o 9014 bytes, dependiendo de las capacidades del adaptador de red. Para verificar la MTU configurada en Hyper-V:

1. En Windows Server 2012 R2, abra el **Control Panel (Panel de control)** y vaya a **Network and Internet (Red e Internet)** > **Network and Sharing Center (Red y Centro compartido)** > **View network status and tasks (Ver estado de red y tareas)**.
2. Haga clic en un adaptador de red o conmutador virtual de la lista.
3. Haga clic en **Properties (Propiedades)**.
4. Haga clic en **Configure (Configurar)**.
5. En la pestaña Avanzados, seleccione **Jumbo Packet (Paquete Jumbo)** de la lista.
6. Seleccione 9000 o 9014 bytes del menú desplegable Valor.
7. Haga clic en **OK (Aceptar)**.

Si ha habilitado las tramas gigantes de Hyper-V, habilite de tramas gigantes en el cortafuegos VM-Series y seleccione el tamaño de MTU para que se corresponda con lo configurado en el host Hyper-V.

STEP 8 | Acceda a la interfaz web del cortafuegos VM-Series, configure las interfaces y defina las reglas de seguridad y las reglas NAT para habilitar de forma segura las aplicaciones que quiere proteger.

Consulte la Guía del administrador de PAN-OS.

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en Azure

El cortafuegos VM-Series en Azure incorpora las funciones de seguridad del cortafuegos de nueva generación de Palo Alto Networks como máquina virtual en el Azure Marketplace. El cortafuegos VM-Series proporciona un conjunto completo de funcionalidades de seguridad para garantizar que las cargas de trabajo y los datos de su máquina virtual estén protegidos, y las capacidades que habilita el cortafuegos son diferentes de las funciones de seguridad nativas como los grupos de seguridad, los cortafuegos de la aplicación web y los cortafuegos nativos basados en puertos.

En Azure, el cortafuegos VM-Series está disponible en el modelo BYOL (traer su propia licencia) o en el modelo PAYG de pago por consumo horario. Microsoft Azure permite implementar el cortafuegos para proteger sus cargas de trabajo dentro de la red virtual en la nube, para poder implementar una solución de nube pública o poder ampliar la infraestructura de TI local para crear una solución híbrida.

- Acerca del cortafuegos VM-Series en Azure
- Implementaciones compatibles con Azure
- Implementación del cortafuegos VM-Series desde Azure Marketplace (plantilla de soluciones)
- Implementación del cortafuegos VM-Series desde Azure China Marketplace (plantilla de soluciones)
- Implementaciones organizadas de Panorama en Azure
- Creación de una imagen personalizada de VM-Series para Azure
- Uso de las recomendaciones del centro de seguridad de Azure para proteger sus cargas de trabajo
- Implementación del cortafuegos serie VM en Azure Stack
- Implementación del cortafuegos VM-Series en Azure Stack HCI
- Habilitación de Application Insights de Azure en el cortafuegos VM-Series
- Supervisión de VM en Azure
- Configuración de la HA activo/pasivo en Azure
- Uso de la plantilla ARM para implementar el cortafuegos VM-Series
- Implementación de la plantilla VM-Series y Azure Application Gateway
- Servicios seguros de Kubernetes en Azure

Acerca del cortafuegos VM-Series en Azure

El cortafuegos VM-Series en Azure debe implementarse en una red virtual (VNet) utilizando el modo de implementación de Gestor de recursos. Puede implementar el cortafuegos VM-Series en la nube pública estándar de Azure, Azure China y Azure Government: incluido DoD en Azure Government, que cumple con los requisitos de seguridad para los datos del nivel 5 de impacto del Departamento de defensa (DoD) y los altos estándares de FedRAMP.

El cortafuegos VM-Series en el marketplace para las regiones de la nube pública de Azure, Azure Government y Azure DoD es compatible con el modelo de Bring Your Own License (BYOL) y la opción Pay-As-You-Go (PAYG) por hora (licencias basadas en uso). Para obtener detalles de la licencia, consulte Tipos de licencia: cortafuegos VM-series y mire la lista de regiones compatibles con Azure en las que puede implementar el cortafuegos VM-Series.

Para Azure China, el cortafuegos VM-Series solo está disponible en la opción BYOL. Consulte Implementación del cortafuegos VM-Series desde Azure China Marketplace (plantilla de soluciones) para el flujo de trabajo.

Además, puede implementar el cortafuegos VM-Series en Azure Stack, la solución de nube privada de Microsoft que le permite usar los servicios de Azure en el centro de datos de su organización. Con Azure Stack, puede desarrollar una solución de nube híbrida que unifique su implementación pública de Azure con su configuración local de Azure Stack. Puede descargar la oferta BYOL del cortafuegos VM-Series en Azure Marketplace y ponerla a la disposición de sus inquilinos en Azure Stack. Para obtener instrucciones, consulte Implementación del cortafuegos VM-Series en Azure Stack.

- Azure Networking y el cortafuegos VM-Series
- Integración del centro de seguridad de Azure
- Plantillas de cortafuegos VM-Series en Azure
- Requisitos mínimos del sistema para VM-Series en Azure
- Soporte para alta disponibilidad (HA) en VM-Series en Azure

Azure Networking y el cortafuegos VM-Series

La infraestructura de Azure VNet no necesita máquinas virtuales para disponer de una interfaz de red en cada subred. La arquitectura incluye una tabla de rutas internas (denominadas rutas) que conecta directamente todas las máquinas virtuales dentro de VNet de modo que el tráfico se envíe automáticamente a una máquina virtual en cualquier subred. Para una dirección de destino fuera de VNet, el tráfico se envía a la puerta de enlace de Internet por defecto o a una puerta de enlace VPN, si así se configura. Para dirigir el tráfico a través del cortafuegos VM-Series, debe crear rutas definidas por el usuario (UDR) para especifican el siguiente salto para el tráfico que sale de una subred. Este ruta obliga a que el tráfico destinado a otra subred vaya al cortafuegos VM-Series en vez de utilizar la rutas del sistema para acceder directamente a la máquina virtual en otra subred. Por ejemplo, en una aplicación de dos niveles con un nivel web y un nivel de base de datos, puede configurar la UDR para que se dirija el tráfico desde la subred web a la subred DB a través del cortafuegos VM-Series.

 ©2024 Palo Alto Networks, Inc.

En Azure, las UDR son solamente para el tráfico que sale de una subred. No se pueden crear rutas definidas por el usuario para especificar el modo en que el tráfico entra en una subred desde Internet o para dirigir el tráfico a máquinas virtuales dentro de una subread. Las UDR le permiten dirigir el tráfico saliente a una interfaz en el cortafuegos VM-Series de modo que siempre pueda garantizar que el cortafuegos también protege el tráfico a Internet.

Para documentación acerca de Microsoft Azure, consulte https://azure.microsoft.com/en-us/documentation/.

Las plantillas de solución para implementar el cortafuegos VM-Series disponibles en Azure Marketplace, tienen tres interfaces de red. Para Configuración de la HA activo/pasivo en Azure, deberá añadir una interfaz adicional para el enlace HA2. Si desea personalizar la plantilla, utilice las plantillas ARM disponibles en el repositorio GitHub.

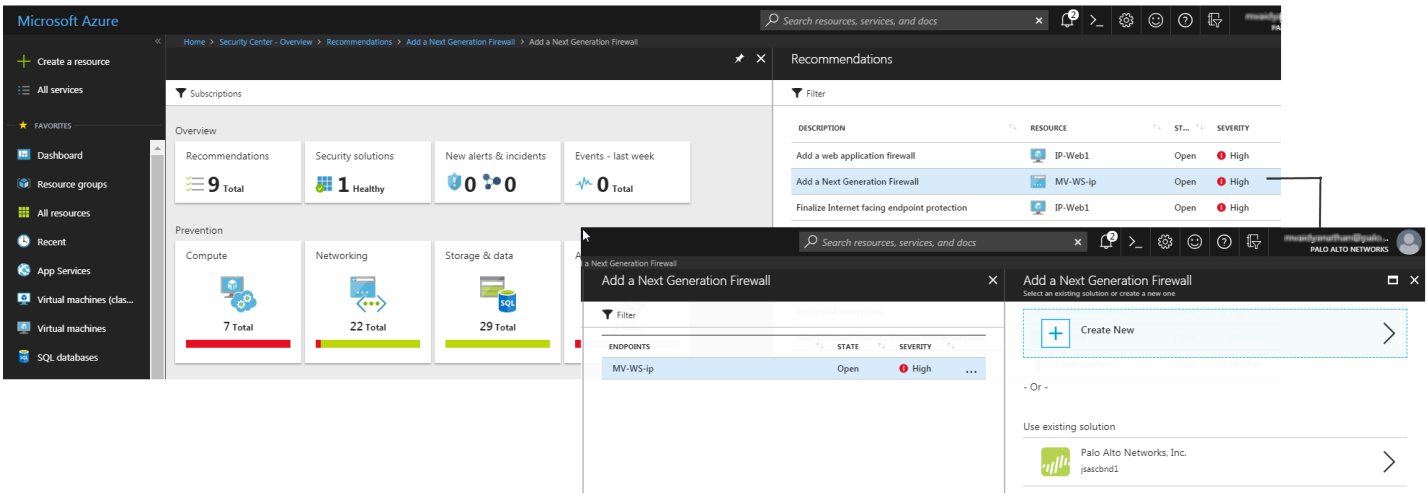
Integración del centro de seguridad de Azure

Microsoft ha puesto en desuso el soporte ofrecido por el Centro de seguridad de Azurepara las soluciones de seguridad de socios y lo ha sustituido con Azure Sentinel.

El cortafuegos VM-Series está integrado con el centro de seguridad de Azure para brindar una vista unificada a fin de supervisar y alertar sobre la postura de seguridad de sus cargas de trabajo de Azure. En el centro de seguridad de Azure, el cortafuegos VM-Series está disponible como una solución de seguridad de socio que protege sus cargas de trabajo de Azure de amenazas y mitiga las brechas en la protección de su propiedad comercial e intelectual en la nube pública. Para permitir esta integración y mostrar logs como alertas de seguridad directamente en el panel del centro de seguridad de Azure, el cortafuegos VM-Series en Azure incluye un perfil predeterminado de reenvío de logs.

Para comenzar, debe habilitar el centro de seguridad de Azure en su suscripción de Azure. Tiene dos formas en las que puede habilitar esta integración:

- **Implementar un cortafuegos VM-Series basado en una recomendación en el panel del centro de seguridad de Azure.**



Cuando el panel del centro de seguridad de Azure le recomienda implementar un cortafuegos VM-Series para proteger una carga de trabajo expuesta a internet, solo puede implementar el cortafuegos en un nuevo grupo de recursos o en un grupo de recursos existente que esté vacío. Esto se debe a que, actualmente, Azure no le permite implementar un dispositivo con varias NIC en un grupo de

 ©2024 Palo Alto Networks, Inc.

recursos existente. Por lo tanto, después de implementar el cortafuegos VM-Series, debe configurarlo manualmente para que esté en la ruta de tráfico de la carga de trabajo que necesita proteger.

Cuando implemente el cortafuegos desde el centro de seguridad de Azure, el cortafuegos se inicia con tres interfaces de red: gestión, orientación externa (no confiable) y orientación interna (confiable), y una ruta definida por el usuario (user defined route, UDR) que envía todo el tráfico saliente de la subred confiable a la interfaz confiable del cortafuegos de modo que el tráfico de Internet siempre lo inspeccione el cortafuegos. La configuración predeterminada incluye dos ejemplos de reglas de la política de seguridad: la regla de *salida predeterminada* permite todo el tráfico desde la zona fiable a la zona no fiable en el puerto predeterminado de la aplicación, y la regla de *entrada predeterminada* permite todo el tráfico de la navegación web desde la zona no fiable a la zona fiable, luego de inspeccionar el tráfico con los perfiles predeterminados de seguridad de protección de vulnerabilidades, antivirus y antispyware. El cortafuegos también reenvía todos los archivos que se interceptan con la regla de entrada o salida a la nube pública de WildFire para su análisis. Ambas reglas incluyen un perfil de filtrado de URL que bloquea todo el tráfico a las categorías de URL extremistas, desconocidas, malware, phishing, DNS dinámico y de infracción de derechos de autor. Además de estos perfiles de seguridad, ambas reglas de política de seguridad están habilitadas para registrar al final de la sesión y reenviar logs de envíos de amenazas y Wildfire como alertas de seguridad al panel de Azure Security Center.

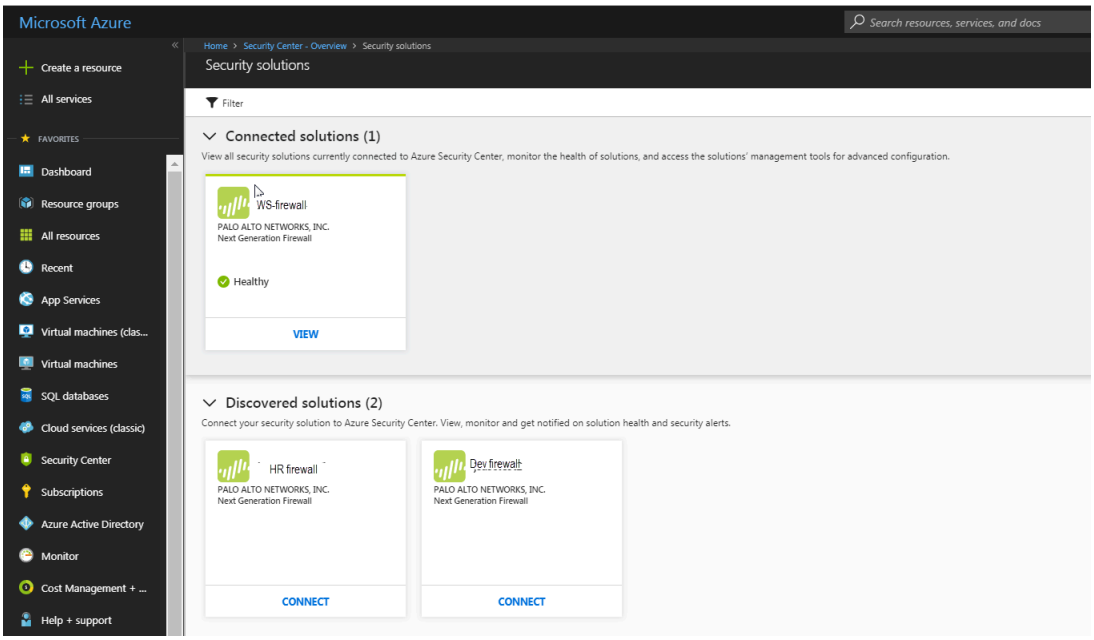
Para hacer un uso práctico de esta integración y Implementación de un cortafuegos VM-Series basado en una recomendación del centro de seguridad de Azuredentro del mismo grupo de recursos que las cargas de trabajo que desea proteger, puede organizar una carga de trabajo con una dirección IP pública que esté expuesta a Internet. Cuando el centro de seguridad de Azure detecta el riesgo de seguridad, genera la recomendación de implementar un cortafuegos de última generación y puede implementar el cortafuegos VM-Series en un nuevo grupo de recursos en el que podrá añadir cargas de trabajo después. Debe eliminar la carga de trabajo que montó para activar la recomendación.

- **Seleccionar un cortafuegos VM-Series que ya implementó para proteger sus cargas de trabajo**. Si tiene un nivel estándar de suscripción al centro de seguridad de Azure, el centro de seguridad de Azure detecta y muestra todos los cortafuegos VM-Series existentes que implementó desde Azure Marketplace o usando una implementación personalizada con la CLI de Azure, PowerShell o una

 ©2024 Palo Alto Networks, Inc.

plantilla ARM. Los cortafuegos de su suscripción de Azure se agrupan en Soluciones de seguridad en el panel de Azure Security Center.

Microsoft Azure no admite la detección de cortafuegos existentes con la suscripción de nivel Gratuito.



Para Conexión de un cortafuegos VM-Series existente desde el centro de seguridad de Azure, debe configurar una máquina virtual Linux y configurar el reenvío de Syslog para reenviar logs de cortafuegos en el formato de evento común como alertas a Azure Security Center. La configuración adicional permite una vista de panel de cristal único para supervisar todos los activos de Azure.

Reenviar un gran volumen de logs al centro de seguridad de Azure puede resultar en un costo adicional de su suscripción.

Plantillas de cortafuegos VM-Series en Azure

Puede implementar el cortafuegos VM-Series en Azure utilizando plantillas. Palo Alto Networks brinda dos tipos de plantillas: plantillas de solución y plantillas ARM.

- **Plantillas de solución en Azure Marketplace**: Las plantillas de solución disponibles en Azure Marketplace le permiten implementar el cortafuegos VM-Series utilizando el portal de Azure. Puede utilizar un grupo de recursos y la cuenta de almacenaje existentes (o crear otros nuevos) para implementar el cortafuegos VM-Series con la siguiente configuración por defecto:
  - VNet CIDR 10.8.0.0/16; puede personalizar el CIDR para un rango diferente de direcciones IP privadas.
  - Tres subredes: 10.8.0.0/24 (gestión), 10.8.1.0/24 (no fiable), 10.8.2.0/24 (fiable)
  - Tres interfaces de red, una en cada subred. Si personaliza el CIDR de VNet, los rangos de subredes se asignan a sus cambios.

  Para usar la plantilla de la solución, consulte Implementación del cortafuegos VM-Series desde Azure Marketplace (plantilla de soluciones); para Azure China, consulte Implementación del cortafuegos VM-Series desde Azure China Marketplace (plantilla de soluciones).

 ©2024 Palo Alto Networks, Inc.

- **Plantillas ARM en el repositorio GitHub**: Además de las implementaciones basadas en Marketplace, Palo Alto Networks proporciona plantillas de gestor de recursos de Azure en el repositorio GitHub para simplificar el proceso de implementación del cortafuegos VM-Series en Azure.
  - Use la plantilla ARM para implementar el cortafuegos VM-Series: la plantilla ARM incluye dos archivos JSON (un archivo de plantillas y un archivo de parámetros) para ayudarle a implementar y provisionar todos los recursos dentro de VNet en un operación simple y coordinada. Estas plantillas se proporcionan bajo una política de soporte "tal cual está, mejor opción".

    Si desea utilizar Azure CLI para localizar todas las imágenes disponibles de Palo Alto Networks, necesitará los siguientes detalles para completar el comando (show vm-image list):

    - *Editor: paloaltonetworks*
    - *Oferta: vmseries-flex*
    - *SKU: byol, bundle1, bundle2*
    - *Versión: 10.0.0 o la más reciente*
  - Implemente la plantilla VM-Series y Azure Application Gateway para admitir una arquitectura de seguridad de ampliación que protege sus aplicaciones web orientadas a internet utilizando dos cortafuegos VM-Series entre un par de balanceadores de carga Azure (externos e internos) VM-Series y Azure Application Gateway. Esta plantilla actualmente no está disponible para Azure China.
  - Use la plantilla ARM para implementar el cortafuegos VM-Series en un grupo de recursos existente, por ejemplo, cuando desee Configuración de la HA activo/pasivo en Azure.

Además de las plantillas ARM anteriores que están cubiertas en la política de soporte oficial de Palo Alto Networks, Palo Alto Networks proporciona plantillas compatibles con la comunidad en el repositorio de GitHub de Palo Alto Networks que le permite explorar las solucionar disponibles para iniciar rápidamente su recorrido hacia el escalado y la automatización de la nube en Azure.

Requisitos mínimos del sistema para VM-Series en Azure

Debe implementar el cortafuegos VM-Series solamente en el modo de Gestor de recursos de Azure (ARM); el modo clásico (implementaciones basadas en la gestión de servicio) no es compatible. El cortafuegos VM-Series en Azure debe cumplir los siguientes requisitos:

- Máquinas virtuales Linux de Azure de los siguientes tipos: Modelos compatibles.

  Estos tipos incluyen soporte para redes aceleradas (SR-IOV).
- Para la memoria, disco y los núcleos CPU necesarios para implementar el cortafuegos VM-Series, consulte Requisitos del sistema VM-Series.

  Puede añadir un disco adicional de 40 GB hasta 8TB para almacenamiento de registros. El cortafuegos VM-series usa discos gestionados de Azure donde estén disponibles; no utiliza el disco temporal que Azure proporciona con algunos tipos de instancia.

 ©2024 Palo Alto Networks, Inc.

- Hasta ocho interfaces de red (NIC). Es necesaria una interfaz principal para el acceso de gestión y hasta siete interfaces para el tráfico de datos.

  En Azure, debido a que una máquina virtual no requiere una interfaz de red en cada subred, puede configurar el cortafuegos VM-Series con tres interfaces de red (una para tráfico de gestión y dos para tráfico del plano de datos. Para crear reglas de políticas basadas en zonas, además de la interfaz de gestión, necesita al menos dos interfaces de plano de datos para poder asignar una interfaz del plano de datos a la zona *fiable*, y la otra interfaz del plano de datos a la zona *no fiable*. Para una implementación de alta disponibilidad, necesitará otra interfaz para el enlace de HA2 entre los equipos de HA.

  Debido a que Azure VNet es una red Layer3, el cortafuegos VM-Series de Azure es compatible solamente con interfaces Layer3.

Soporte para alta disponibilidad (HA) en VM-Series en Azure

Para garantizar la disponibilidad, puede Configuración de la HA activo/pasivo en Azure en una configuración tradicional con sincronización de sesión o usar una arquitectura de escala que utilice balanceadores de carga nativos de la nube como Azure Application Gateway o Azure Load Balancer, para distribuir el tráfico a través de un conjunto de instancias saludables del cortafuegos. Para obtener detalles, consulte Implementación de la plantilla VM-Series y Azure Application Gateway.

VM-Series en permisos de entidad de servicio de Azure

Para que Panorama interactúe con las API de Azure y recopile información sobre sus cargas de trabajo, debe crear una aplicación de Azure Active Directory y una entidad de servicio que tenga los permisos necesarios para autenticarse con Azure AD y acceder a los recursos en su suscripción.

Para crear la aplicación de Active Directory y la entidad de servicio, siga las instrucciones en Cómo: Utilice el portal para crear una aplicación de Azure AD y una entidad de servicio que pueda acceder a los recursos. Durante el proceso de generación de la aplicación, hay un paso para "Asignar la aplicación a la función" y asignar una función de IAM de "lector" a la aplicación.

Si no cuenta con los permisos necesarios para crear y registrar la aplicación de AD, solicite a su administrador de suscripción o de Azure AD que cree una Entidad de servicio.

Una vez que se haya registrado la aplicación, registre estos valores para poder introducirlos en el complemento de Panorama para Azure más adelante:

- ID de aplicación
- Clave secreta (regístrela cuando cree la clave secreta; la clave secreta no es visible una vez que abandone la página).
- ID de inquilino

Permisos

La siguiente tabla enumera las funciones integradas mínimas requeridas y los permisos granulares si desea personalizar la función.

Para asistencia técnica	Permisos
Alta disponibilidad de Azure	Consulte Configuración de la HA activo/pasivo en Azure.

 ©2024 Palo Alto Networks, Inc.

Para asistencia técnica	Permisos
Azure Application Insights Habilitación de Application Insights de Azure en el cortafuegos VM-Series	**"Microsoft.Authorization/*/read",** **"Microsoft.Network/networkInterfaces/*",** **"Microsoft.Network/networkSecurityGroups/*",** **"Microsoft.Network/virtualNetworks/*",** **"Microsoft.Compute/virtualMachines/read"**
Supervisión de Azure Configuración del plugin Azure para la supervisión en Panorama	Requiere una función mínima de **Reader (Lector)** para la Entidad de servicio. Como alternativa, puede añadir los siguientes permisos personalizados: **"Microsoft.Compute/virtualMachines/read",** **"Microsoft.Network/networkInterfaces/read",** **"Microsoft.Network/virtualNetworks/read",** **"Microsoft.Network/virtualNetworks/subnets/read",** **"Microsoft.Network/applicationGateways/read",** **"Microsoft.Network/locations/serviceTags/read",** **"Microsoft.Network/loadBalancers/read",** **"Microsoft.Network/publicIPAddresses/read",** **"Microsoft.Resources/subscriptions/resourcegroups/read"**
Panorama Orchestrated Deployments Cree una función personalizada y asóciela a Active Directory	**"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",**

 ©2024 Palo Alto Networks, Inc.

Para asistencia técnica	Permisos
	"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",

 ©2024 Palo Alto Networks, Inc.

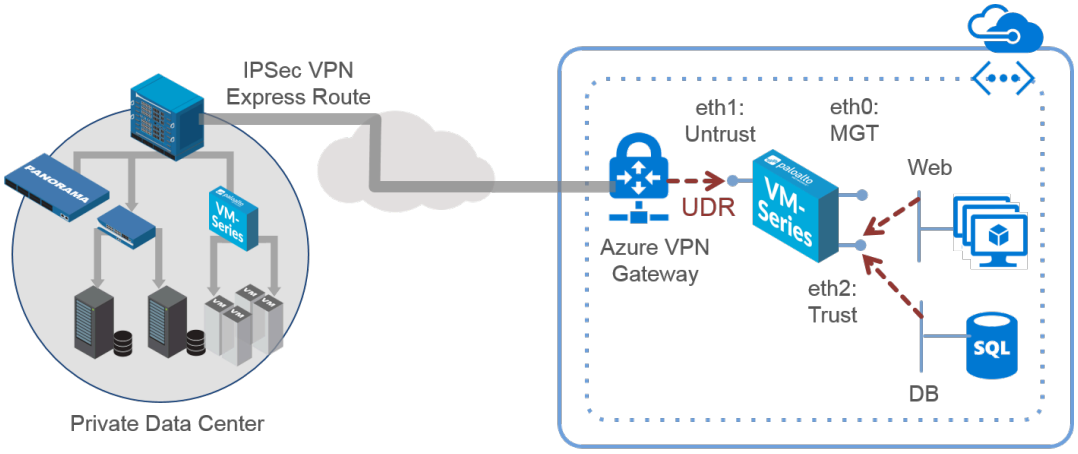
Para asistencia técnica	Permisos
	"Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
	"Microsoft.Network/locations/serviceTags/read",
	"Microsoft.Network/applicationGateways/read", "Microsoft.Network/networkInterfaces/read",
	"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"

©2024 Palo Alto Networks, Inc.

Implementaciones compatibles con Azure

Utilice el cortafuegos VM-Series en Azure para proteger a sus usuarios de red en los siguientes escenarios:

- **Híbrido y VNet a VNet**: el cortafuegos VM-Series en Azure le permite ampliar con seguridad su centro de datos/nube privada en Azure utilizando IPSec y ExpressRoute. Para mejorar la seguridad de su centro de datos, si ha segmentado su red e implementado sus cargas de trabajo en VNets separadas, puede proteger el flujo de trafico entre VNets con un túnel IPSec y las políticas que permiten el tráfico de aplicaciones.



- **Inter-Subnet**: El cortafuegos VM-Series puede dirigir a sus servidores en una VNet y protege contra amenazas laterales para el tráfico inter-subred entre aplicaciones en una arquitectura multinivel.
- **Puerta de enlace**: El cortafuegos VM-Series sirve como puerta de enlace VNet para proteger implementaciones que se conectan a Internet en la red virtual de Azure (VNet). El cortafuegos VM-Series garantiza el tráfico destinado a los servidores en la VNet y protege contra amenazas laterales para el tráfico inter-subred entre aplicaciones en una arquitectura multinivel.
- **GlobalProtect**: utilice la infraestructura de Azure para implementar de forma rápida y sencilla el cortafuegos VM-Series como GlobalProtect™ y ampliar la política de seguridad de puertas de enlace a usuarios y dispositivos remotos, independientemente de su ubicación.

Puede continuar con la Implementación del cortafuegos VM-Series desde Azure Marketplace (plantilla de solución), Implementación del cortafuegos VM-Series en Azure Stack, Implementación del cortafuegos VM-Series en Azure Stack HCI o Organice una implementación del cortafuegos VM-Series en Azure.

También puede obtener información sobre las Plantillas del cortafuegos VM-Series en Azure que puede utilizar para implementar el cortafuegos.

Para obtener más información sobre el arranque, consulte Arranque del cortafuegos VM-Series en Azure y Arranque del cortafuegos VM-Series en Azure Stack HCI.

©2024 Palo Alto Networks, Inc.

Implementación del cortafuegos VM-Series desde Azure Marketplace (plantilla de soluciones)

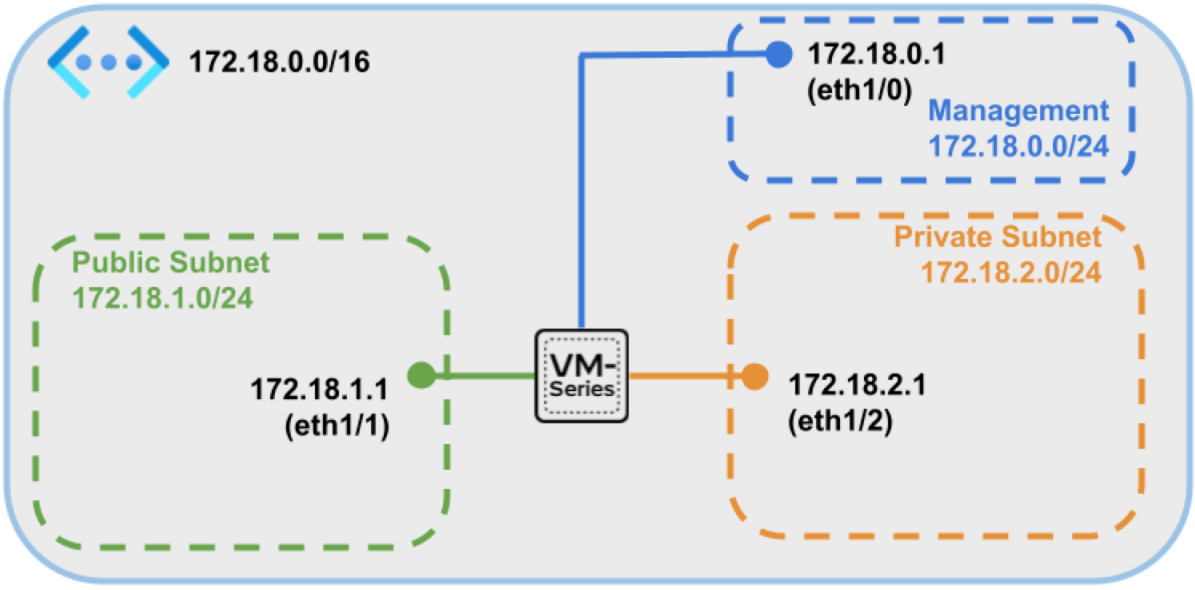
Ahora puede implementar plantillas de solución VM-series en Azure Marketplace en una topología y no necesita restringirse a implementaciones de cortafuegos único. Deberá implementar los recursos en un grupo de recursos vacío y puede especificar una etiqueta que se aplicará a todos los recursos creados por la plantilla.

Palo Alto Networks ahora es compatible con los siguientes tipos de implementaciones con licencias BYOL o PAYG:

- Cortafuegos VM-Series único.
  - Cortafuegos único de dos interfaces
  - Cortafuegos único una interfaz
- Alta resiliencia con balanceadores de carga (LB)
  - Cortafuegos común con LB
  - Cortafuegos entrante dedicado con LB público
  - Conjunto de cortafuegos dedicados saliente y este-oeste con ILB
  - Conjuntos de cortafuegos de entrada y salida dedicados con LB e ILB públicos

Cortafuegos VM-series único

Para arquitecturas simples con requisitos de rendimiento predecibles, puede implementar un único cortafuegos de nueva generación junto con componentes de red básicos como VNet y subredes de gestión, privadas y públicas (solo para implementación de dos interfaces).



Alta resiliencia con balanceadores de carga

 ©2024 Palo Alto Networks, Inc.

El uso de alta resiliencia con LB le permite implementar un conjunto de 2-4 cortafuegos con balanceo de carga para soportar la resiliencia del grado de producción para diferentes escenarios de tráfico.

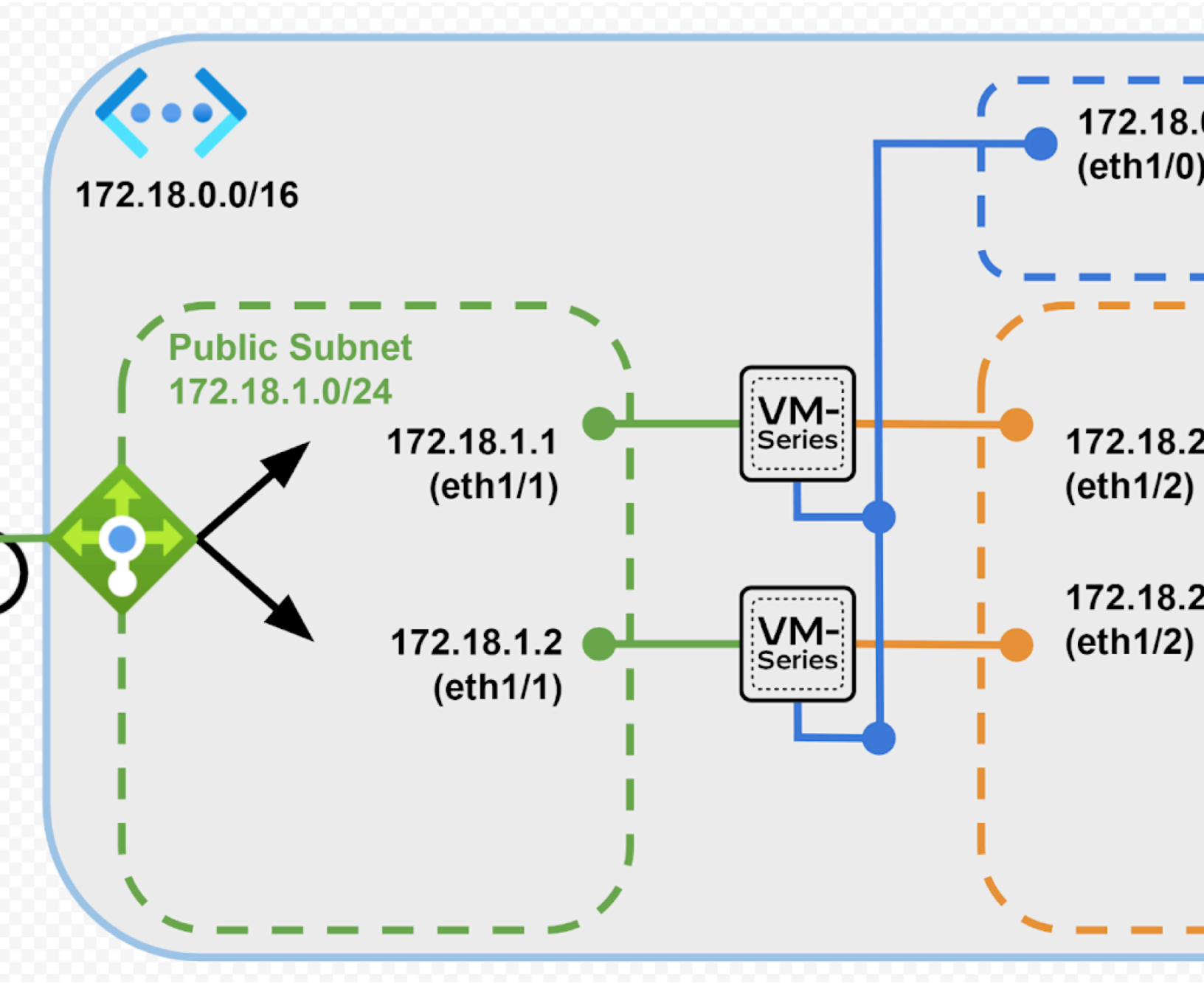
Conjunto de cortafuegos común con balanceadores de carga

Con esta arquitectura de implementación puede implementar:

- 1 VNet y 3 subredes: gestión, privada y pública
- 1 equilibrador de carga interno y 1 público
- 2 cortafuegos VM-Series de nueva generación

Esta arquitectura es adecuada para implementaciones pequeñas y pruebas de concepto, y tiene un conjunto de 2 cortafuegos intercalados entre un balanceador de carga interno y público con tráfico entrante y saliente que pasa a través de ambos cortafuegos. El conjunto de cortafuegos es un recurso compartido y tiene opciones ampliables limitadas.

 ©2024 Palo Alto Networks, Inc.



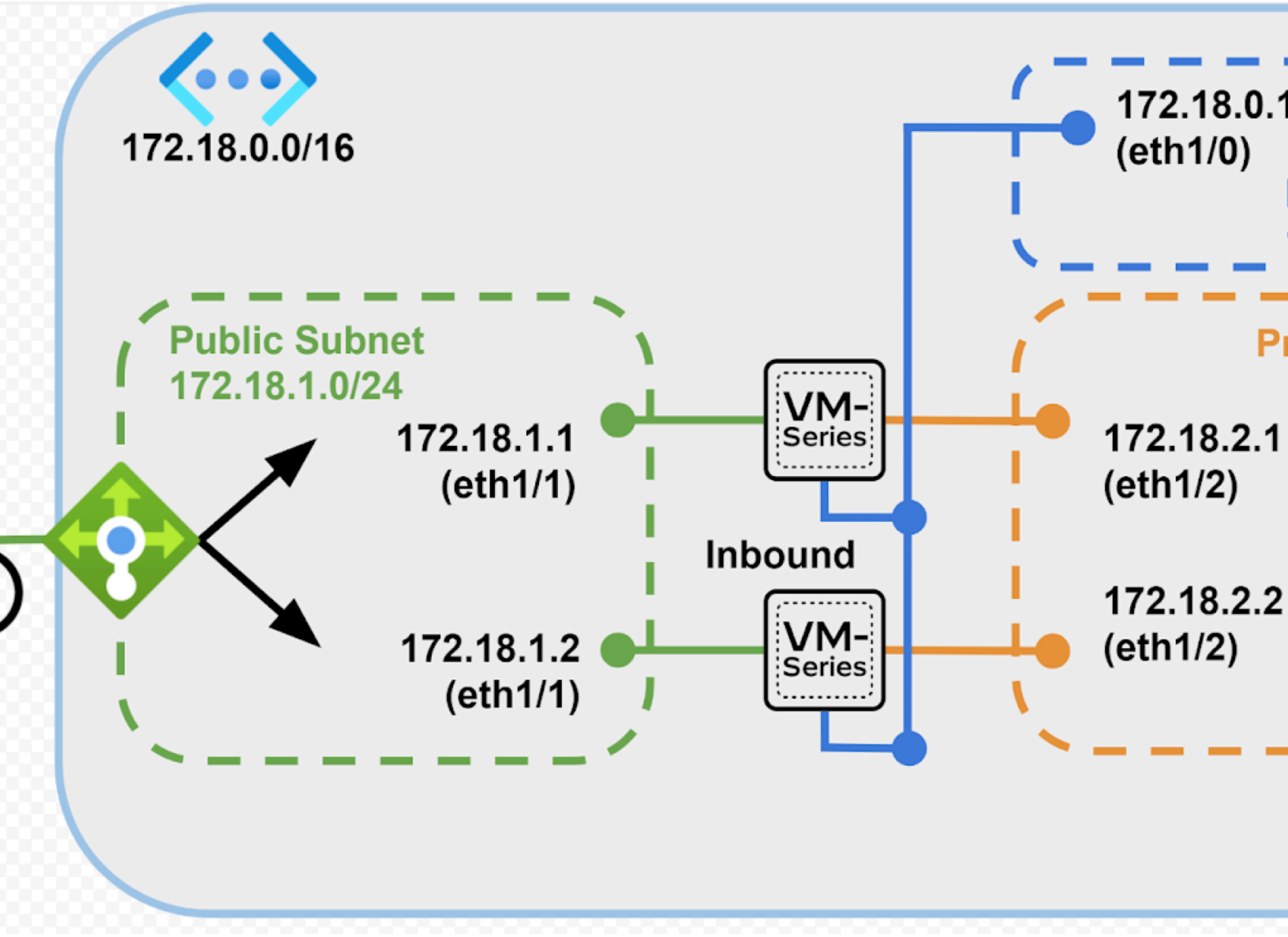
Cortafuegos entrante dedicado con ILB

Con esta arquitectura de implementación puede implementar:

- 1 VNet y 3 subredes: gestión, privada y pública
- 1 balanceador de carga público
- 2 cortafuegos VM-Series de nueva generación

Esta arquitectura es adecuada para implementaciones de producción y soporta dos cortafuegos detrás de un balanceador de carga público con solo tráfico entrante fluyendo a través de ambos cortafuegos. Esta arquitectura ofrece una mayor ampliación y resiliencia operativa y reduce las posibilidades de un alto uso del ancho de banda del tráfico de acceso entrante.

 ©2024 Palo Alto Networks, Inc.



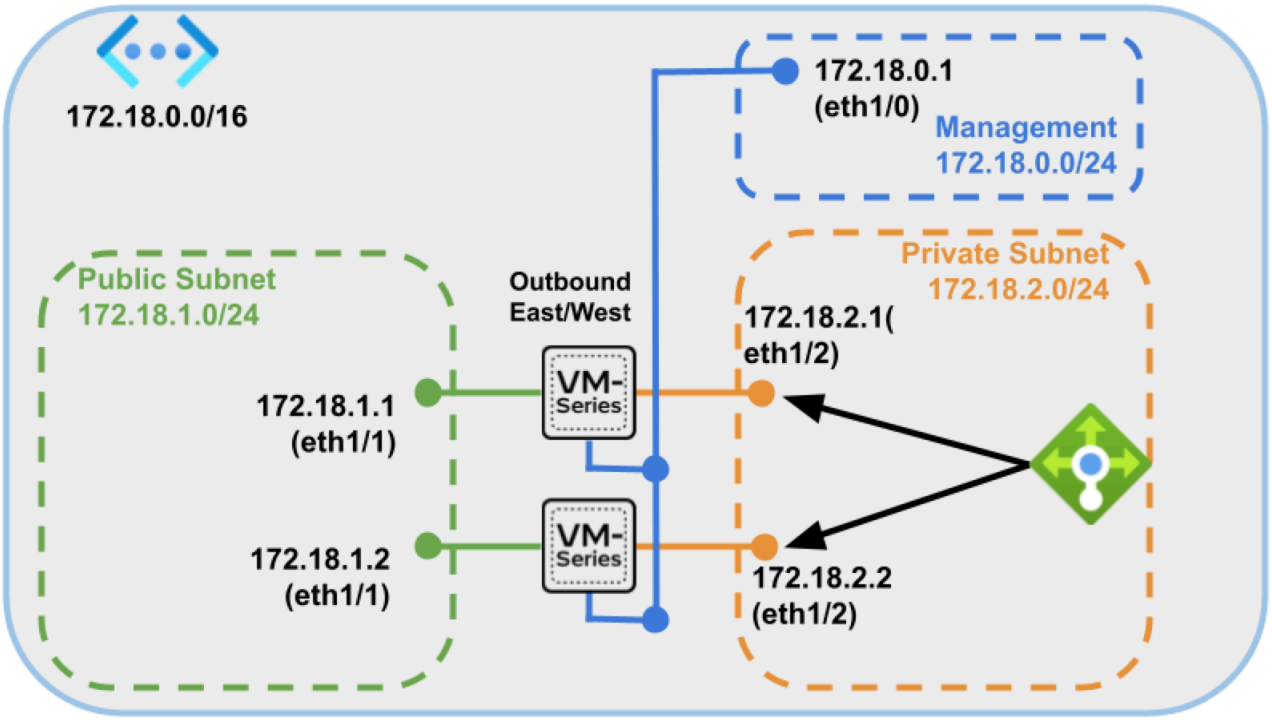
Conjunto dedicado de cortafuegos saliente y este-oeste con ILB

Con esta arquitectura de implementación puede implementar:

- 1 VNet y 3 subredes: gestión, privada y pública
- 1 balanceador de carga interno
- 2 cortafuegos VM-Series de nueva generación

La arquitectura dedicada saliente y este-oeste coloca un conjunto de 2 cortafuegos frente a un balanceador de carga interno con solo tráfico saliente fluyendo a través de ambos cortafuegos. El modelo separa los flujos de tráfico saliente, este-oeste y de retorno a través de un conjunto de cortafuegos común, lo que permite una mayor ampliación de las cargas de tráfico saliente. Palo Alto Networks recomienda este modelo para sus implementaciones de producción.

 ©2024 Palo Alto Networks, Inc.



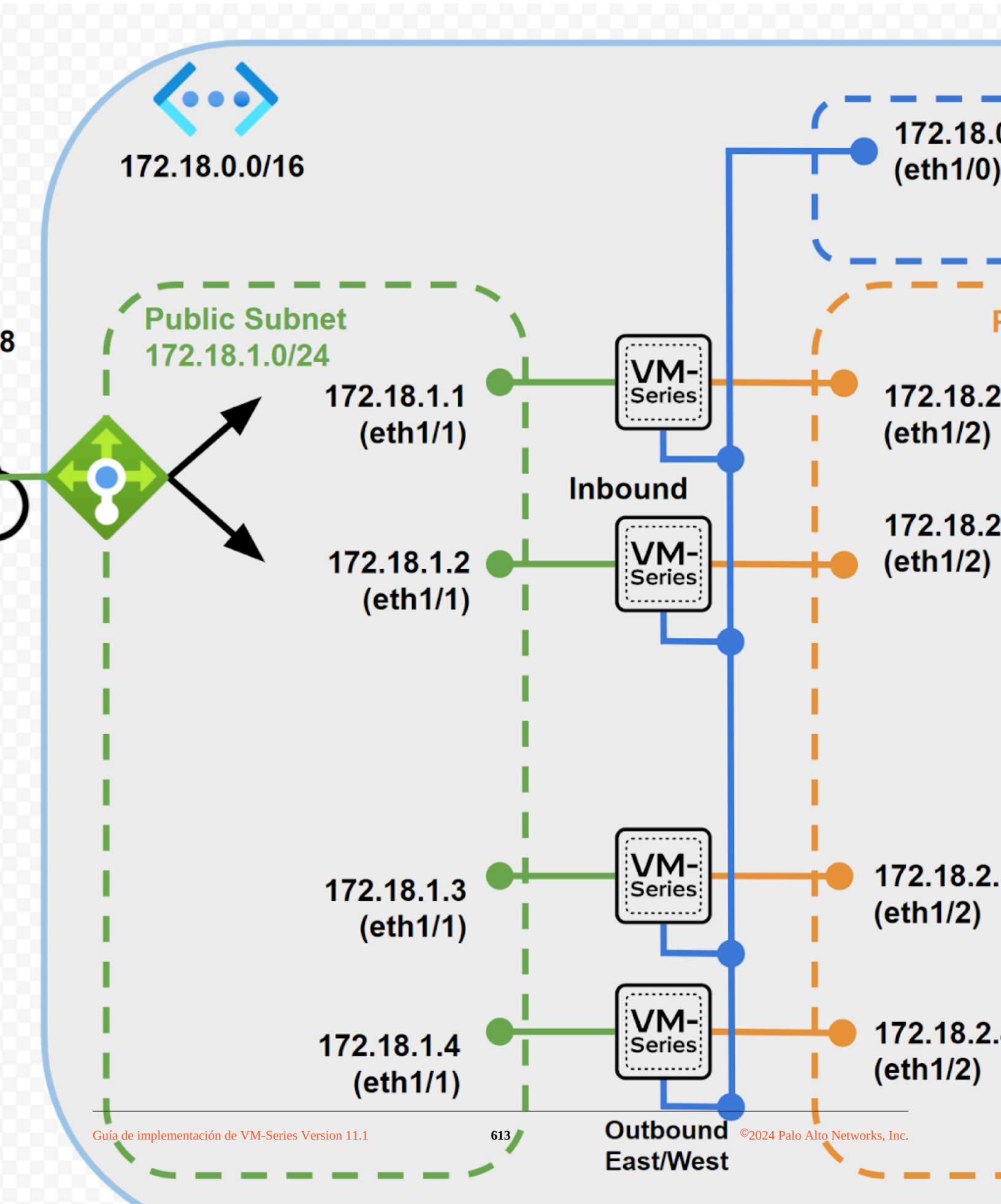
Conjuntos de cortafuegos dedicados de entrada, salida y este-oeste con LB e ILB públicos

Con esta arquitectura de implementación puede implementar:

- 1 VNet y 3 subredes: gestión, privada y pública
- 1 balanceador de carga interno
- 4 cortafuegos VM-Series de nueva generación

La arquitectura dedicada de entrada, salida y este-oeste implementa un conjunto de 4 cortafuegos, 2 de los cuales están dirigidos por un balanceador de carga público para flujos entrantes y los otros 2 están dirigidos por un balanceador de carga interno, para flujos salientes y este-oeste. Esta arquitectura combina los beneficios de todas las arquitecturas anteriores en una sola plantilla.

 ©2024 Palo Alto Networks, Inc.



©2024 Palo Alto Networks, Inc.

Implemente la plantilla de solución de Azure para un único cortafuegos VM-Series

Las siguientes instrucciones describen cómo implementar la plantilla de soluciones para el cortafuegos VM-Series que está disponible en Azure® Marketplace y Azure Government Marketplace. Para usar las plantillas personalizables del Gestor de recursos de Azure (Azure Resource Manager, ARM) disponibles en el repositorio de GitHub, consulte Uso de la plantilla ARM para implementar el cortafuegos VM-Series.

STEP 1 | Configure una cuenta de Azure.

1. Si todavía no tiene una, cree una cuenta de Microsoft®.
2. Inicie sesión en el portal de Azure (**`https://portal.azure.com`** o **`https://portal.azure.us`**) utilizando las credenciales de su cuenta de Microsoft.

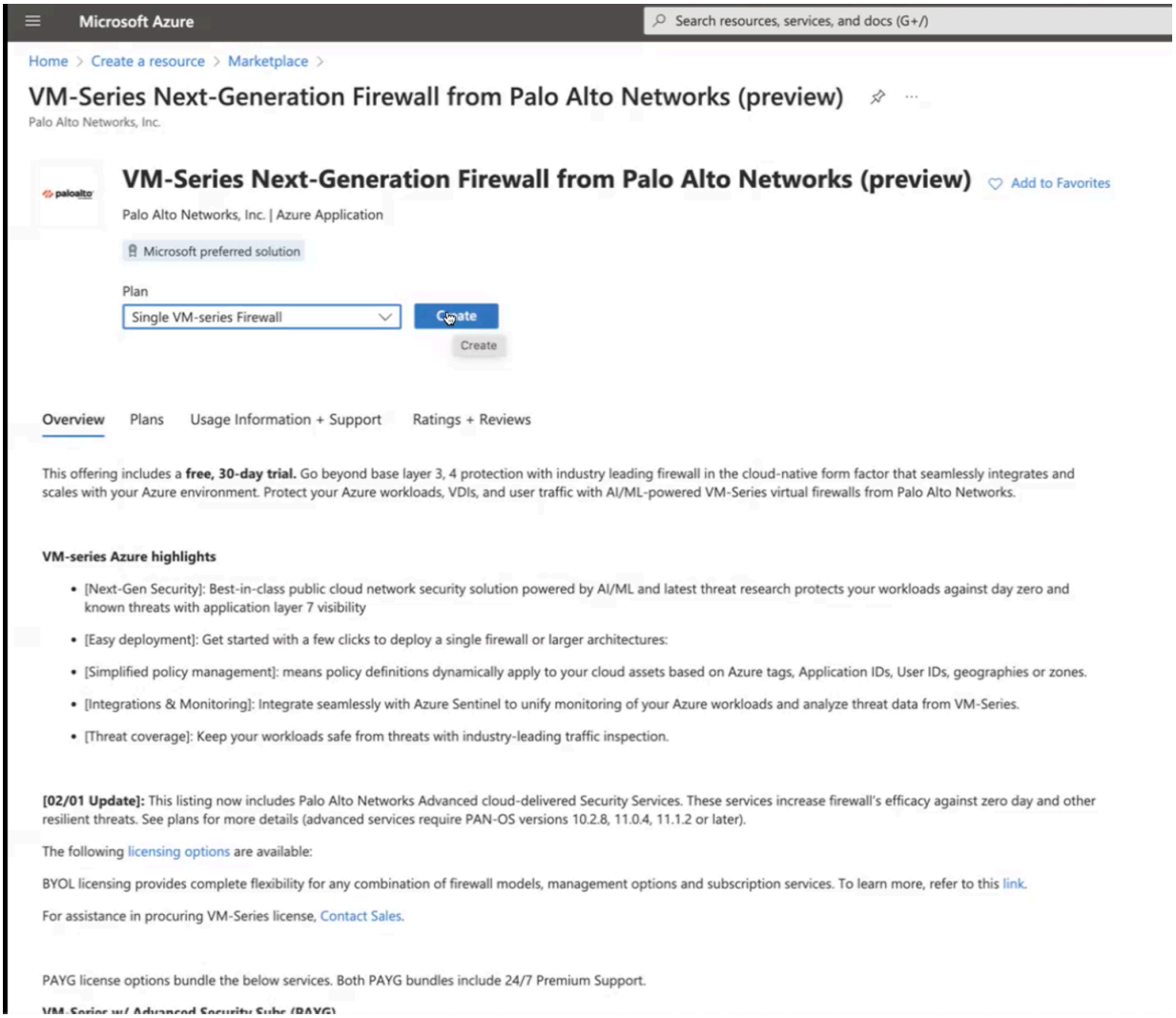
   *Si está utilizando una suscripción de prueba, puede ser necesario abrir una solicitud de soporte (**Help + Support [Ayuda + soporte]** > **New Support Request [Nueva solicitud de soporte]**) para incrementar la cuota de núcleos VM asignados.*

STEP 2 | Busque la plantilla de solución VM-Series en Azure Marketplace, haga clic en **Create a resource (Crear un recurso)** y seleccione **VM-Series Next Generation Firewall from Palo Alto (Cortafuegos VM-Series de nueva generación de Palo Alto)**.

1. Seleccione **Marketplace** > **Virtual Machines (Máquinas virtuales)**.
2. Busque Palo Alto Networks® y aparecerá una lista de ofertas de cortafuegos VM-Series. Para conocer las diferencias entre los modelos Licencia existente (bring your own license, BYOL) y Pago por consumo (pay as you go, PAYG), consulte Licencias de cortafuegos VM-Series para nubes públicas.
3. Seleccione el cortafuegos único de nueva generación VM-Series para **Create (Crear)** un nuevo cortafuegos VM-Series.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Implemente el cortafuegos.



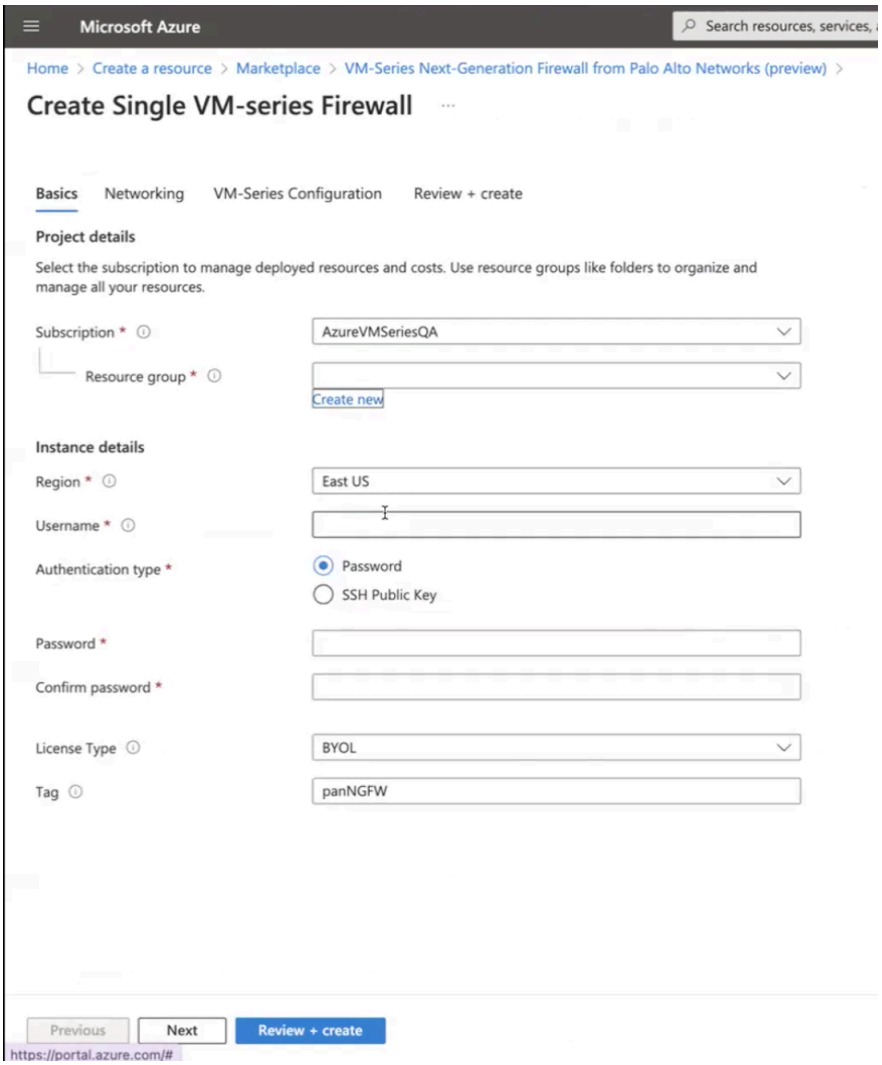
1. Configure los ajustes básicos para el cortafuegos.
   1. Seleccione su **Subscription (Suscripción)** de Azure.
   2. Cree un grupo de recursos nuevo o seleccione uno existente que esté vacío. El grupo de recursos contendrá todos los recursos asociados con el cortafuegos VM-Series para esta implementación.

      Azure eliminó la opción de seleccionar un grupo de recursos existente para las soluciones de Marketplace que permiten varios controladores de interfaz de red (network interface controllers, NIC). Para implementar el cortafuegos en un grupo de recursos existente, use la plantilla ARM en el Repositorio GitHub o su propia plantilla ARM personalizada.
   3. Seleccione la **Region (Región)** de Azure en la que se está implementando el cortafuegos.
   4. Introduzca un **Username (Nombre de usuario)** para el administrador del cortafuegos.
   5. Seleccione el **Authentication type (Tipo de autenticación)**: contraseña o clave pública SSH.

 ©2024 Palo Alto Networks, Inc.

Debe habilitar la autenticación de clave SSH si planea usar el cortafuegos en el modo operativo FIPS-CC. Aunque puede implementar el cortafuegos VM-Series con un nombre de usuario y contraseña, no podrá autenticarse con el nombre de usuario y la contraseña después de cambiar el modo operativo a FIPS-CC. Después del restablecimiento al modo FIPS-CC, debe usar la clave SSH para iniciar sesión y, continuación, podrá configurar un nombre de usuario y contraseña que podrá usar para iniciar sesión posteriormente en la interfaz web del cortafuegos. Para obtener detalles sobre la creación de la clave SSH, consulte la Documentación de Azure.

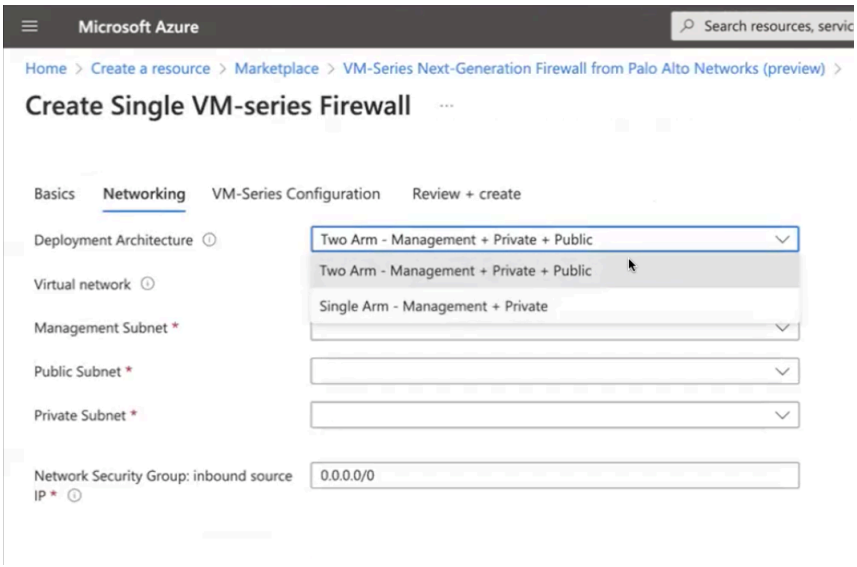
6. Introduzca una **Password (Contraseña)** (de hasta 31 caracteres) o copie y pegue una **SSH public key (Clave pública SSH)** para proteger el acceso administrativo al cortafuegos.
7. Confirme la contraseña.
8. Seleccione el **License Type (Tipo de licencia)**.
9. Introduzca la **Tag (Etiqueta)** de implementación que especificó al crear el grupo de recursos.
10. Haga clic en **Next (Siguiente)**.



2. Configure redes.

 ©2024 Palo Alto Networks, Inc.

1. Seleccione una red virtual (Virtual Network, VNet) existente de Azure o cree una nueva, e introduzca el espacio de direcciones IP para la VNet.
2. Configure las subredes para las interfaces de red: puede elegir una configuración de una sola interfaz con subredes de gestión y confianza, o una configuración de dos interfaces con subredes de gestión, trust y untrust.



   Si usa subredes predeterminadas, debe revisar la configuración. Si usa una VNet existente, debe haber definido tres subredes: una para cada una de las interfaces confiable, no confiable y de gestión. Si crea una nueva Vnet, verifique o cambie los prefijos de cada subred.
3. Introduzca la dirección IP de origen o el rango de IP (incluya el bloque de CIDR) para el acceso a la VNet. **Network Security Group: inbound source IP (Grupo de seguridad de redes: IP de origen entrante)** le permite restringir el acceso entrante a Azure VNet.

   Restrinja el acceso al cortafuegos. Asegúrese de suministrar un bloque CIDR que corresponda a sus direcciones IP o red de gestión dedicadas. No haga que la red de origen permitida sea más grande de lo necesario y nunca configure la fuente permitida como 0.0.0.0/0. Verifique su dirección IP antes de configurarla en la plantilla para asegurarse de que no se bloquea.
4. Haga clic en **Next (Siguiente)**.

3. Defina el acceso de gestión al cortafuegos.
   1. Utilice la variable por defecto ((nueva) fwMgmtPublicIP)) para asignar una **Public IP address (Dirección de IP pública)** a la interfaz de gestión (`eth0`) del cortafuegos.

      Azure accelerated networking no es compatible con la interfaz de gestión.
   2. Introduzca un prefijo para acceder el cortafuegos utilizando un nombre de DNS. Debe combinar el prefijo introducido con el sufijo que se muestra en la pantalla

 ©2024 Palo Alto Networks, Inc.

para acceder a la interfaz web del cortafuegos. Por ejemplo: **<*yourname*><*your-region*>.cloudapp.azure.com**

3. Seleccione la **VM-Series Version (Versión de VM-Series)** más reciente.
4. Introduzca un nombre de pantalla para identificar el cortafuegos VM-Series en el grupo de recursos.

4. Añada la información para configurar el cortafuegos en el inicio. Seleccione la **VM-Series Version (Versión de VM-Series**, el **Virtual machine size (Tamaño de máquina virtual)** y la **Availability Option (Opción de disponibilidad)**.

   1. Seleccione **sí** si desea **Enable Bootstrap (Habilitar el arranque)**. Consulte Arranque del cortafuegos VM-Series en Azure. Seleccione una de las dos opciones siguientes en **Utilizar archivo Bootstrap:**

      1. Proporcionar archivo de arranque
      2. Proporcionar parámetros de arranque: añada información adicional relacionada con Panorama primario, Panorama secundario, DG, pila de plantillas, etc.

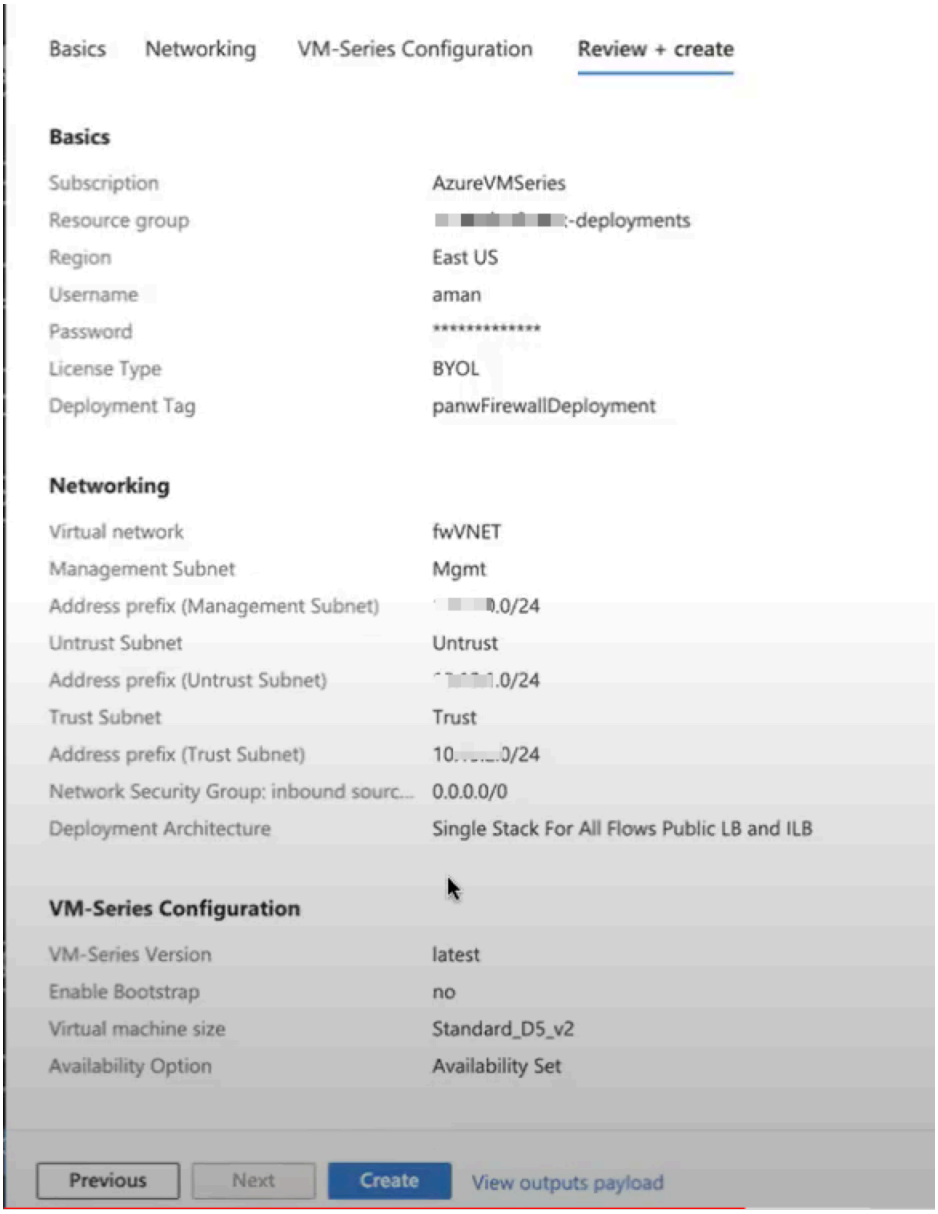
   2. Introduzca el **Storage Account Name (Nombre de la cuenta de almacenamiento)** que contiene el Paquete de arranque.
   3. Introduzca la **Storage Account Access Key (Clave de acceso de la cuenta de almacenamiento)**. Este cortafuegos necesita la clave de acceso para autenticarse en la cuenta de almacenamiento y acceder a los archivos almacenados dentro de ella.
   4. Añada el **File share name (Nombre del recurso compartido de archivos)** en el que cargó los archivos requeridos para el arranque del cortafuegos. La cuenta de almacenamiento debe

 ©2024 Palo Alto Networks, Inc.

estar en la misma región en la que implementa el cortafuegos y debe tener la estructura correcta de carpetas para el arranque.

5. Seleccione la capa de máquina virtual Azure y el tamaño para cumplir con sus necesidades. Utilice el enlace **Change size (Cambiar tamaño)** para ver los tipos de instancia compatibles y para ver los Requisitos mínimos del sistema para VM-Series en Azure.

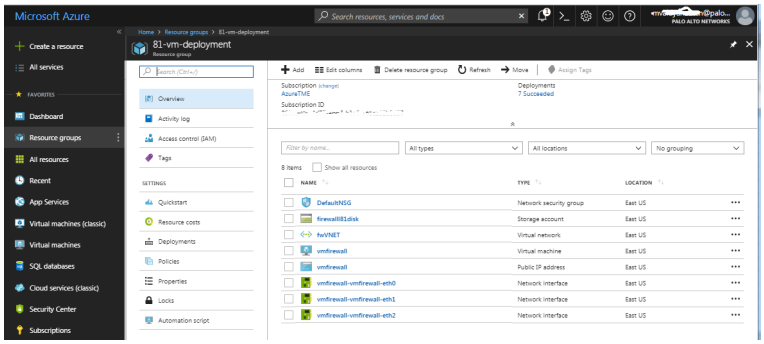
5. Revise el resumen y haga clic en **OK (Aceptar)**. Acepte los términos de uso y la política de privacidad y haga clic en **Create (Crear)** para iniciar el cortafuegos.



6. Verifique que se ha implementado con éxito el cortafuegos VM-Series.

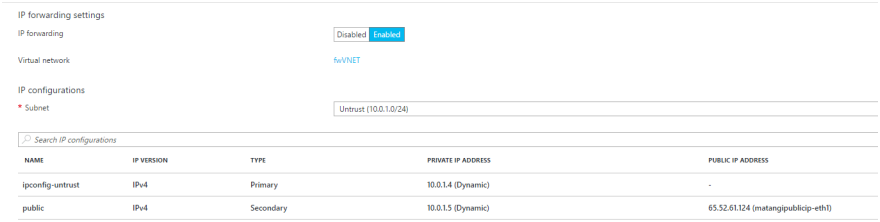
1. Haga clic en **Dashboard (Panel)** > **Resource Groups (Grupos de recursos)** y seleccione el grupo de recursos.
2. Seleccione su grupo de recursos y consulte la **Overview (Descripción general)** para obtener el estado detallado en el que se implementaron los recursos correctamente.

 ©2024 Palo Alto Networks, Inc.



STEP 4 | Adjunte una dirección IP pública para la interfaz no fiable del cortafuegos VM-Series. Cuando crea una nueva dirección IP pública, obtiene una del bloque de direcciones IP que posee Microsoft, por lo que no puede elegir una específica. El número máximo de direcciones IP públicas que puede asignar a una interfaz se basa en su suscripción a Azure.

1. En el portal Azure, seleccione la interfaz de red para la que desea añadir una dirección IP pública (como la interfaz **eth1**).
2. Seleccione **IP Configurations (Configuraciones de IP)** > **Add (Añadir)** y para la dirección IP pública, seleccione **Enabled (Habilitada)**. Cree una nueva dirección IP pública o seleccione una que tenga disponible.
3. Verifique que puede ver la dirección IP secundaria asociada con la interfaz.

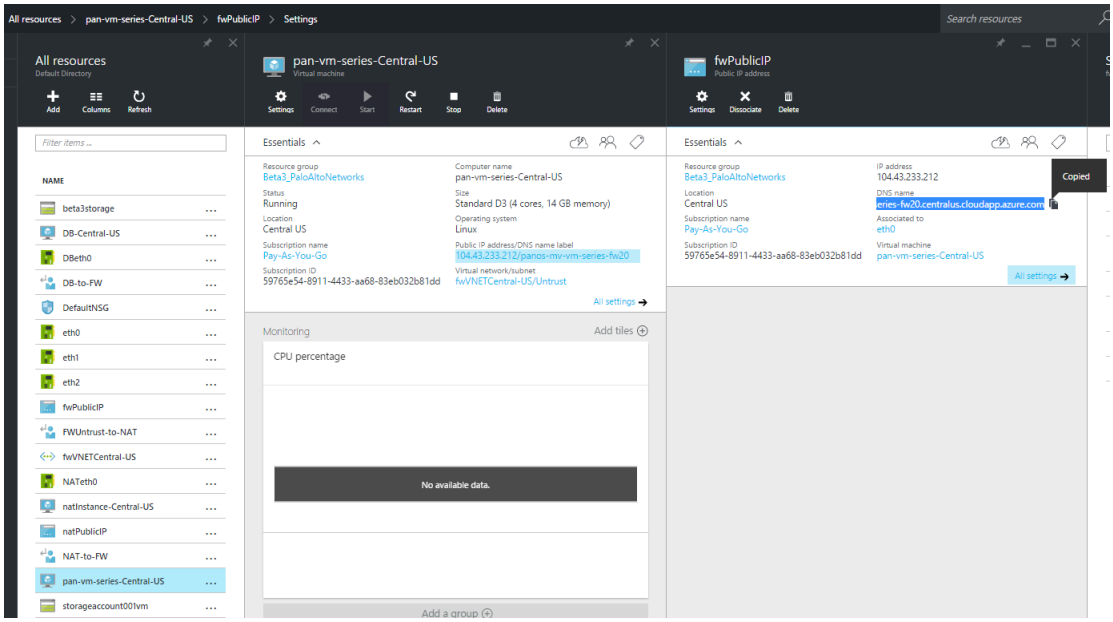


Cuando conecta una dirección IP secundaria a una interfaz de red, el cortafuegos VM-Series no adquiere automáticamente la dirección IP privada asignada a la interfaz. Necesitará configurar manualmente la dirección IP privada utilizando la interfaz web de cortafuegos VM-Series. Consulte Configure las interfaces de red del plano de datos como interfaces de capa 3 en el cortafuegos.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Inicie sesión en la interfaz web del cortafuegos.

1. En el portal de Azure, en **All Resources (Todos los recursos)**, seleccione el cortafuegos VM-Series y visualice el nombre de DNS completo para el cortafuegos.



1. Mediante una configuración segura (https) desde su navegador web, inicie sesión en el nombre de DNS para el cortafuegos.
2. Introduzca el nombre de usuario/contraseña definido en el archivo de parámetros. Aparecerá una advertencia de certificados pero no hay problema, continúe a la página web.

STEP 6 | Active las licencias del cortafuegos VM-Series.

Para la versión BYOL

1. Cree una cuenta de asistencia técnica.
2. Registre el cortafuegos VM-Series (con código de autenticación).
3. En la interfaz web del cortafuegos, seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y seleccione **Activate feature using authentication code (Activar función usando el código de actualización)**.
4. Introduzca el código de autenticación de capacidad (*auth-code*) que registró en el portal de asistencia técnica. El cortafuegos se conectará con el servidor de actualización

 ©2024 Palo Alto Networks, Inc.

(`updates.paloaltonetworks.com`), descargará la licencia y se reiniciará automáticamente.

5. Vuelva a iniciar sesión en la interfaz web y confirme lo siguiente en el **Dashboard (Panel)**:
   - Se muestra un número de serie válido en **Serial# (Nº de serie)**.

     Si aparece el término `Unknowhn (Desconocido)`, significa que el cortafuegos no tiene licencia. Para ver logs de tráfico en el cortafuegos, debe instalar una licencia de capacidad válida.
   - El **VM Mode (Modo VM)** se muestra como Microsoft Azure.

Para la versión PAYG

1. Cree una cuenta de asistencia técnica.
2. Registro del modelo basado en el uso del cortafuegos VM-Series para nubes públicas (sin código de autenticación).

STEP 7 | Configure las interfaces de red del plano de datos como interfaces de capa 3 en el cortafuegos.

Si aloja varios sitios web o servicios con diferentes direcciones IP y certificados SSL en un único servidor, es posible que necesite configurar más de una dirección IP en las interfaces de cortafuegos VM-Series.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
2. Haga clic en **ethernet 1/1** y configúrelo del siguiente modo:
   - Establezca **Interface Type (Tipo de interfaz)** a **Layer3 (Capa 3)** (predeterminado).
   - En la pestaña **Config (Configurar)**, asigne la interfaz el enrutador predeterminado.
   - También en la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. Defina una zona nueva denominada **`UnTrust`** y haga clic en **OK (Aceptar)**.
   - En la pestaña **IPv4**, seleccione **DHCP Client (Cliente DHCP)** si planea asignar solo una dirección IP en la interfaz; el cortafuegos adquirirá automáticamente la dirección IP privada asignada en la plantilla ARM. Si planifica asignar más de una dirección IP, seleccione **Static (Estática)** e introduzca manualmente las direcciones IP primarias y secundarias asignadas a la interfaz en el portal de Azure.
   - Deshabilite (desmarque) **Automatically create default route to default gateway provided by server (Crear automáticamente ruta predeterminada a la puerta de enlace predeterminada proporcionada por el servidor)** para asegurarse de que el tráfico gestionado por esta interfaz no fluya directamente a la puerta de enlace predeterminada en la vNet.
3. Haga clic en **ethernet 1/2** y configúrelo del siguiente modo:
   - Establezca **Interface Type (Tipo de interfaz)** a **Layer3 (Capa 3)** (predeterminado).
   - Establezca **Security Zone (Zona de seguridad)** como **Trust (Confiable)**.
   - Configure la **IP address (Dirección IP)** como **DHCP Client (Cliente DHCP)** o **Static (Estática)**.
   - Deshabilite (desmarque) **Automatically create default route to default gateway provided by server (Crear automáticamente ruta predeterminada a la puerta de enlace predeterminada proporcionada por el servidor)** para asegurarse de que el tráfico

 ©2024 Palo Alto Networks, Inc.

gestionado por esta interfaz no fluya directamente a la puerta de enlace predeterminada en la vNet.

4. Haga clic en **Commit (Confirmar)** para confirmar los cambios y verifique que el enlace para la interfaz esté en estado activo.
5. Añada una ruta estática en el enrutador virtual del cortafuegos VM-Series para las redes que necesita el cortafuegos para el enrutamiento.

   Por ejemplo, añada una ruta predeterminada a las subredes de destino para los servidores que protege el cortafuegos:

   - Seleccione **Network (Red)** > **Virtual Router (Enrutador virtual)** > **default (predeterminado)** >
   - Seleccione **Static Routes (Rutas estáticas)** > **IPv4** y añada la dirección IP del siguiente salto para los servidores de destino. Puede establecer x.x.x.1 como la dirección IP del siguiente salto para todo el tráfico (destinado a 0.0.0.0/0 desde ethernet1/1 de la interfaz).

STEP 8 | Configure el cortafuegos para su implementación específica.

- **Puerta de enlace**: Implemente un balanceador de carga externo delante de la zona No confiable.
- **Híbrido y entre VNet**: Implemente una puerta de enlace VPN de Azure o una máquina virtual NAT delante de la zona No confiable.
- **Entre subredes**: En el cortafuegos VM-Series, añada una regla de política de seguridad intra-zona para permitir el tráfico basado en las subredes conectadas con la interfaz Confiable.
- **GlobalProtect™**: Implemente una máquina virtual NAT delante de la zona No confiable.

STEP 9 | Dirija el tráfico al cortafuegos VM-Series.

1. Para garantizar que el cortafuegos VM-Series proteja todo el tráfico dentro del grupo de recursos de Azure, configure rutas estáticas en el cortafuegos.
2. Configure las rutas definidas por el usuario para dirigir todo el tráfico a través de las interfaces en el cortafuegos VM-Series. Para más información, consulte la documentación de Azure sobre UDRs.

   Las rutas definidas por el usuario de las subredes internas deben enviar todo el tráfico a través de la interfaz Confiable. Las rutas definidas por el usuario del lado No confiable dirigen todo el tráfico desde Internet a través de la interfaz No confiable en el cortafuegos VM-Series. El tráfico de Internet puede provenir de Azure Application Gateway o balanceador de carga Azure, o a través de la puerta de enlace VPN de Azure; en el caso de una implementación híbrida que conecta su red local con la nube de Azure.

STEP 10 | Para publicar las métricas de PAN-OS® en Azure Application Insights, consulte Habilitación de Application Insights de Azure en el cortafuegos VM-Series.

Implemente la plantilla de solución Azure para cortafuegos de alta resiliencia VM-Series con balanceadores de carga

Todas las interfaces de cortafuegos VM-Series deben tener asignada una dirección IPv4 cuando se implementan en un entorno de nube pública. Las direcciones IPv6 no son compatibles.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Configure una cuenta de Azure.

1. Si todavía no tiene una, cree una cuenta de Microsoft®.
2. Inicie sesión en el portal de Azure (**`https://portal.azure.com`** o **`https://portal.azure.us`**) utilizando las credenciales de su cuenta de Microsoft.

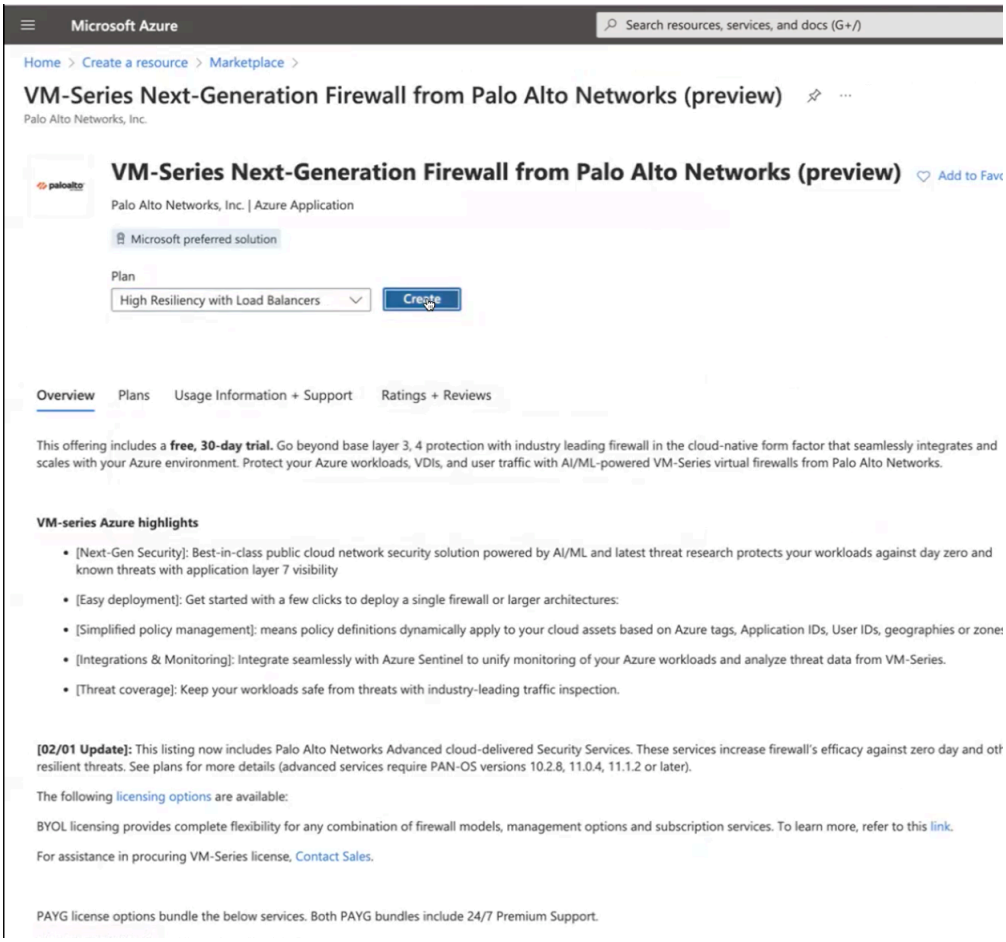
   *Si está utilizando una suscripción de prueba, puede ser necesario abrir una solicitud de soporte (**Help + Support [Ayuda + soporte]** > **New Support Request [Nueva solicitud de soporte]**) para incrementar la cuota de núcleos VM asignados.*

STEP 2 | Busque la plantilla de solución VM-Series en Azure Marketplace, haga clic en **Create a resource (Crear un recurso)** y seleccione **VM-Series Next Generation Firewall from Palo Alto (Cortafuegos VM-Series de nueva generación de Palo Alto)**.

1. Seleccione **Marketplace** > **Virtual Machines (Máquinas virtuales)**.
2. Busque Palo Alto Networks® y aparecerá una lista de ofertas de cortafuegos VM-Series. Para conocer las diferencias entre los modelos Licencia existente (bring your own license, BYOL) y Pago por consumo (pay as you go, PAYG), consulte Licencias de cortafuegos VM-Series para nubes públicas.
3. Seleccione Alta resiliencia con balanceadores de carga para **Create (Crear)** un nuevo cortafuegos VM-Series.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Implemente el cortafuegos.



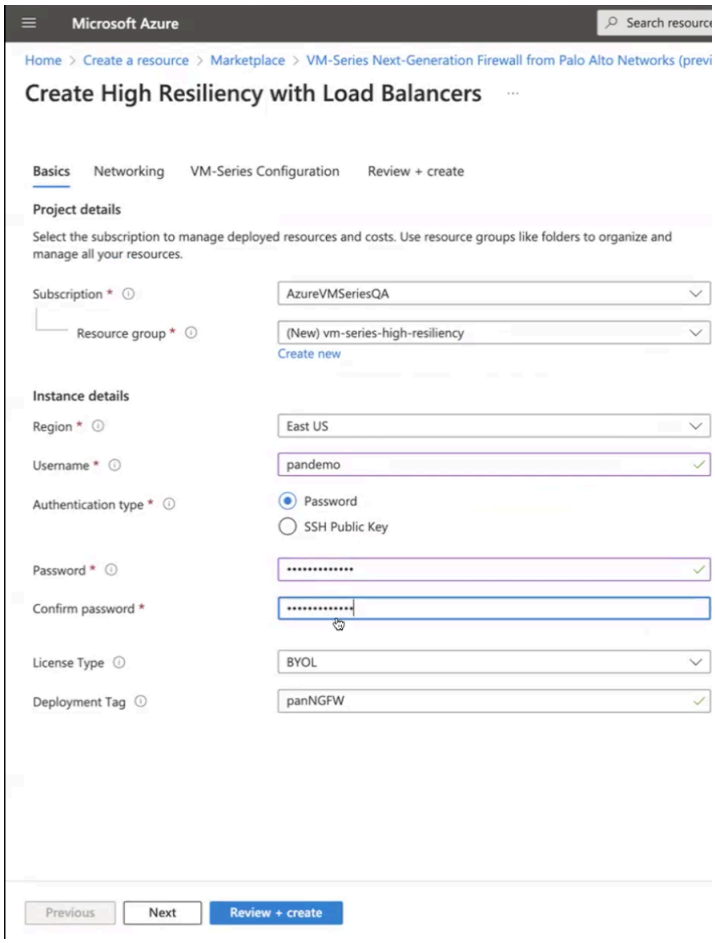
1. Configure los ajustes básicos para el cortafuegos.
   1. Seleccione su **Subscription (Suscripción)** de Azure.
   2. Cree un grupo de recursos nuevo o seleccione uno existente que esté vacío. El grupo de recursos contendrá todos los recursos asociados con el cortafuegos VM-Series para esta implementación.

      Azure eliminó la opción de seleccionar un grupo de recursos existente para las soluciones de Marketplace que permiten varios controladores de interfaz de red (network interface controllers, NIC). Para implementar el cortafuegos en un grupo de recursos existente, use la plantilla ARM en el Repositorio GitHub *o su propia plantilla ARM personalizada.*
   3. Seleccione la **Region (Región)** de Azure en la que se está implementando el cortafuegos.
   4. Introduzca un **Username (Nombre de usuario)** para el administrador del cortafuegos.
   5. Seleccione el **Authentication type (Tipo de autenticación)**: contraseña o clave pública SSH.

 ©2024 Palo Alto Networks, Inc.

Debe habilitar la autenticación de clave SSH si planea usar el cortafuegos en el modo operativo FIPS-CC. Aunque puede implementar el cortafuegos VM-Series con un nombre de usuario y contraseña, no podrá autenticarse con el nombre de usuario y la contraseña después de cambiar el modo operativo a FIPS-CC. Después del restablecimiento al modo FIPS-CC, debe usar la clave SSH para iniciar sesión y, continuación, podrá configurar un nombre de usuario y contraseña que podrá usar para iniciar sesión posteriormente en la interfaz web del cortafuegos. Para obtener detalles sobre la creación de la clave SSH, consulte la Documentación de Azure.

6. Introduzca una **Password (Contraseña)** (de hasta 31 caracteres) o copie y pegue una **SSH public key (Clave pública SSH)** para proteger el acceso administrativo al cortafuegos.
7. Confirme la contraseña.
8. Seleccione el **License Type (Tipo de licencia)**.
9. Introduzca la **Tag (Etiqueta)** de implementación que especificó al crear el grupo de recursos.
10. Haga clic en **Next (Siguiente)**.



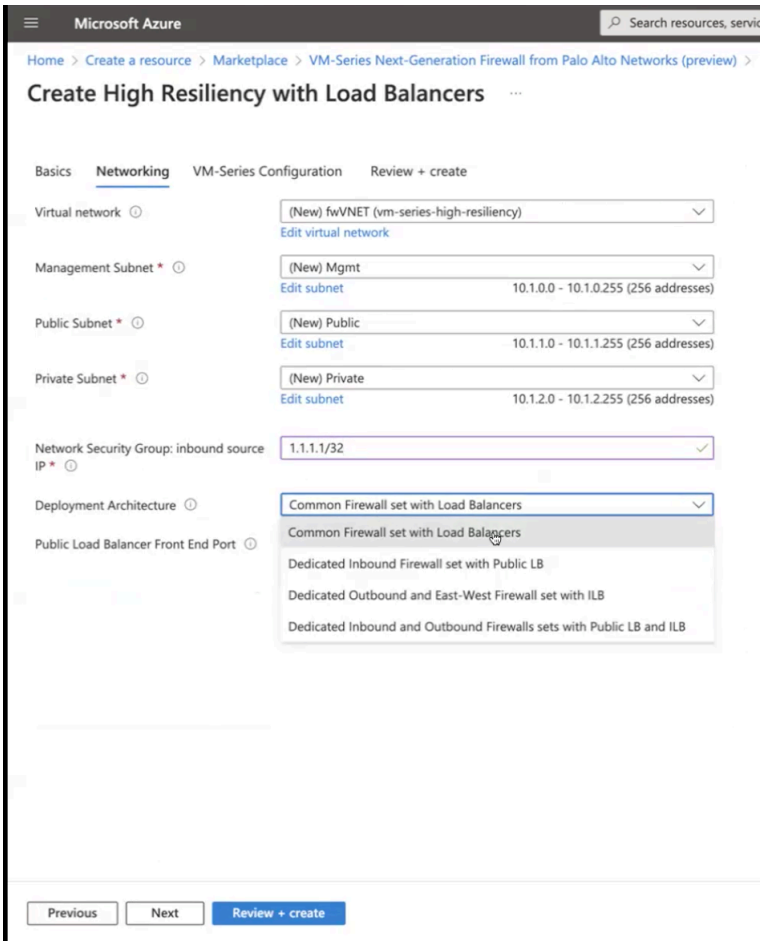
2. Configure redes.
    1. Seleccione una red virtual (Virtual Network, VNet) existente de Azure o cree una nueva, e introduzca el espacio de direcciones IP para la VNet.
    2. Configure las subredes para las interfaces de red.

 ©2024 Palo Alto Networks, Inc.

Si usa subredes predeterminadas, debe revisar la configuración. Si usa una VNet existente, debe haber definido tres subredes: una para cada una de las interfaces confiable, no confiable y de gestión. Si crea una nueva Vnet, verifique o cambie los prefijos de cada subred.

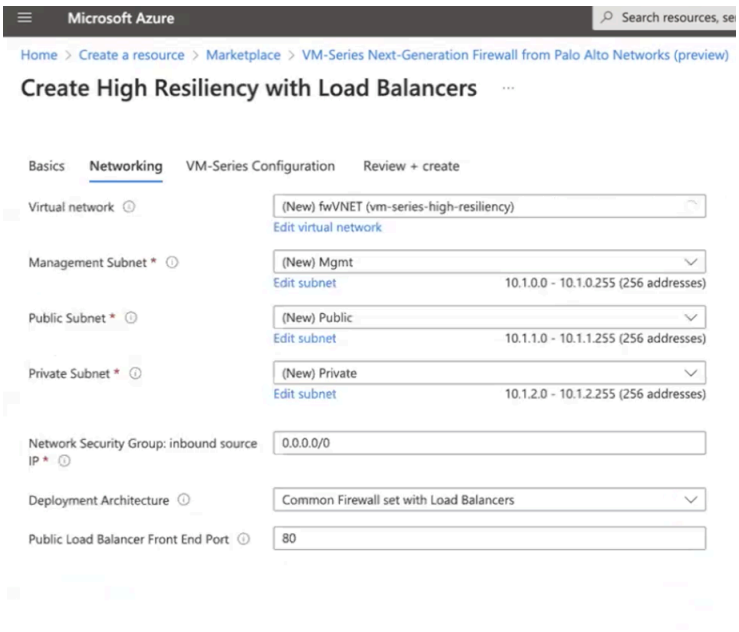
3. Introduzca la dirección IP de origen o el rango de IP (incluya el bloque de CIDR) para el acceso a la VNet. **Network Security Group: inbound source IP (Grupo de seguridad de redes: IP de origen entrante)** le permite restringir el acceso entrante a Azure VNet.

   Restrinja el acceso al cortafuegos. Asegúrese de suministrar un bloque CIDR que corresponda a sus direcciones IP o red de gestión dedicadas. No haga que la red de origen permitida sea más grande de lo necesario y nunca configure la fuente permitida como 0.0.0.0/0. Verifique su dirección IP antes de configurarla en la plantilla para asegurarse de que no se bloquea.



4. Seleccione la arquitectura de implementación e introduzca el número de puerto Front End del balanceador de carga público (no aplicable para salidas dedicadas).

 ©2024 Palo Alto Networks, Inc.



5. Haga clic en **Next (Siguiente)**.

3. Defina el acceso de gestión al cortafuegos.

   1. Utilice la variable por defecto ((nueva) fwMgmtPublicIP)) para asignar una **Public IP address (Dirección de IP pública)** a la interfaz de gestión (`eth0`) del cortafuegos.

      Azure accelerated networking no es compatible con la interfaz de gestión.

   2. Introduzca un prefijo para acceder el cortafuegos utilizando un nombre de DNS. Debe combinar el prefijo introducido con el sufijo que se muestra en la pantalla

 ©2024 Palo Alto Networks, Inc.

para acceder a la interfaz web del cortafuegos. Por ejemplo: **<*yourname*><*your-region*>.cloudapp.azure.com**

3. Seleccione la **VM-Series Version (Versión de VM-Series)** más reciente.
4. Introduzca un nombre de pantalla para identificar el cortafuegos VM-Series en el grupo de recursos.

4. Añada la información para configurar el cortafuegos en el inicio. Seleccione la **VM-Series Version (Versión de VM-Series**, el **Virtual machine size (Tamaño de máquina virtual)** y la **Availability Option (Opción de disponibilidad)**.

   1. Seleccione **sí** si desea **Enable Bootstrap (Habilitar el arranque)**. Consulte Arranque del cortafuegos VM-Series en Azure. Seleccione una de las dos opciones siguientes en **Utilizar archivo Bootstrap:**

      1. Proporcionar archivo de arranque
      2. Proporcionar parámetros de arranque: añada información adicional relacionada con Panorama primario, Panorama secundario, DG, pila de plantillas, etc.

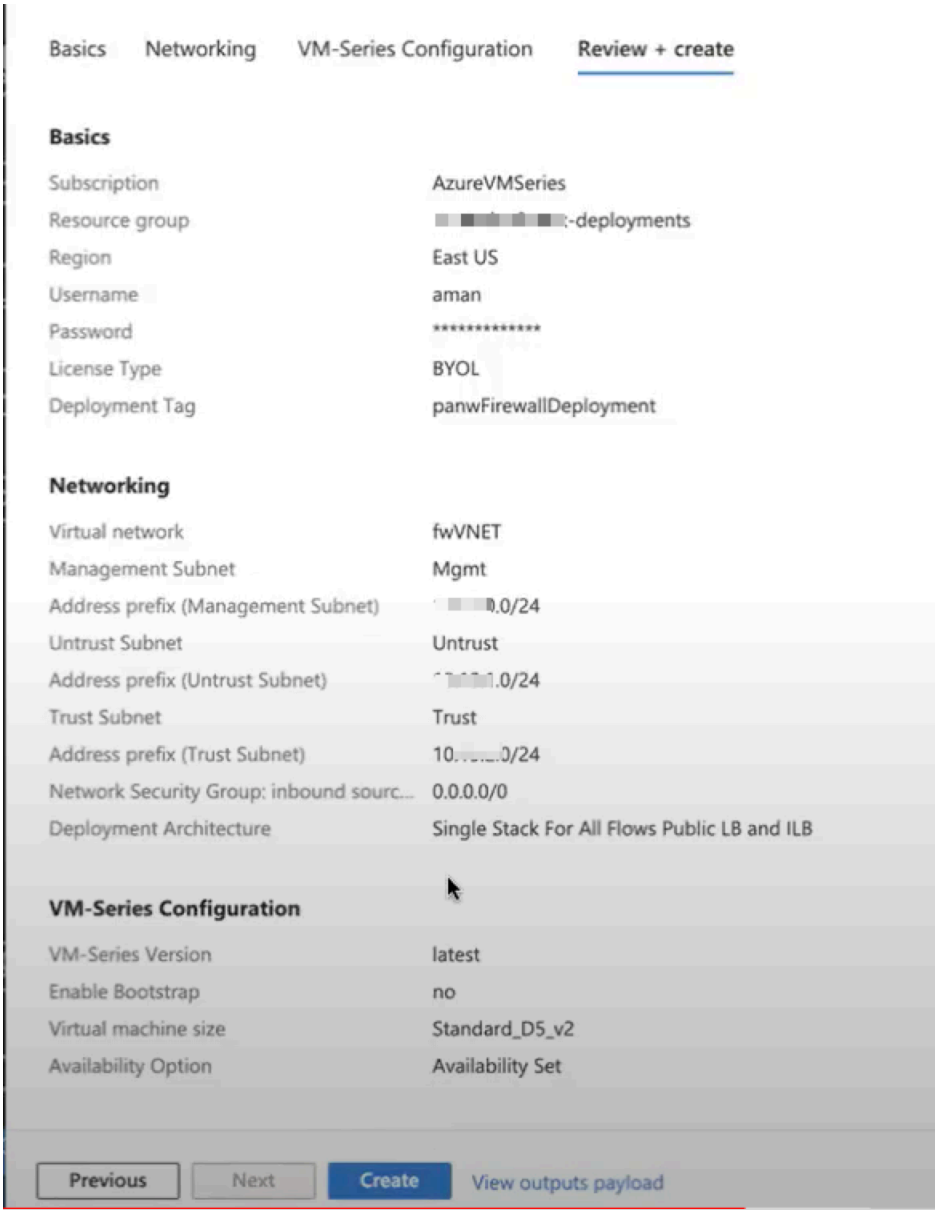
   2. Introduzca el **Storage Account Name (Nombre de la cuenta de almacenamiento)** que contiene el Paquete de arranque.
   3. Introduzca la **Storage Account Access Key (Clave de acceso de la cuenta de almacenamiento)**. Este cortafuegos necesita la clave de acceso para autenticarse en la cuenta de almacenamiento y acceder a los archivos almacenados dentro de ella.
   4. Añada el **File share name (Nombre del recurso compartido de archivos)** en el que cargó los archivos requeridos para el arranque del cortafuegos. La cuenta de almacenamiento debe

 ©2024 Palo Alto Networks, Inc.

estar en la misma región en la que implementa el cortafuegos y debe tener la estructura correcta de carpetas para el arranque.

5. Seleccione la capa de máquina virtual Azure y el tamaño para cumplir con sus necesidades. Utilice el enlace **Change size (Cambiar tamaño)** para ver los tipos de instancia compatibles y para ver los Requisitos mínimos del sistema para VM-Series en Azure.

5. Revise el resumen y haga clic en **OK (Aceptar)**. Acepte los términos de uso y la política de privacidad y haga clic en **Create (Crear)** para iniciar el cortafuegos.



6. Compruebe que ha implementado correctamente el cortafuegos VM-Series siguiendo los pasos descritos en Implemente la plantilla de solución de Azure para un único cortafuegos VM-Series.

La siguiente es una interfaz de muestra y definiciones de zona del cortafuegos VM-Series de alta resiliencia con LB

 ©2024 Palo Alto Networks, Inc.

- Configuración de la primera interfaz Ethernet como interfaz de Capa 3 con configuración de cliente DHCP y especificación de no crear una ruta predeterminada automáticamente.

```
set network interface ethernet ethernet1/1 layer3 dhcp-client
 create-default-route no
```

- Configuración de la segunda interfaz Ethernet de manera similar a una interfaz de Capa 3 con cliente DHCP, y sin crear una ruta predeterminada.

```
set network interface ethernet ethernet1/2 layer3 dhcp-client
 create-default-route no
```

- Creación de una zona denominada *pública* y asignación de Ethernet1/1 a esta zona. Esta interfaz gestionará el tráfico considerado como *público*.

```
set zone public network layer3 ethernet1/1
```

- Creación de otra zona llamada *privada* y asignación de Ethernet1/2 a esta zona, destinada al tráfico interno *privado*.

```
set zone private network layer3 ethernet1/2
```

- Configuración de un enrutador virtual llamado 'Private-VR' y asignación de Ethernet1/2 a este enrutador virtual.

```
set network virtual-router Private-VR interface ethernet1/2
```

- Del mismo modo, configuración de otro enrutador virtual 'Public-VR' y asignación de Ethernet1/1 a este enrutador.

```
set network virtual-routing-table Public-VR interface ethernet1/1
```

- Definición de una ruta estática en *Private-VR* para llegar a Internet a través de la *Public-VR*.

```
set network virtual-router Private-VR routing-table ip static-route
 Internet nexthop next-vr Public-VR
```

- Establecimiento del destino del tráfico de Internet en todas las IP (0.0.0.0/0) en la *Private-VR*.

```
set network virtual-router Private-VR routing-table ip static-route
 Internet destination 0.0.0.0/0
```

- Adición de rutas específicas para las sondas de estado de Azure Load Balancer a través de una IP e interfaz específicas.

```
set network virtual-router Private-VR routing-table ip static-route
 AzureLBHealthProbe nexthop ip-address <private-subnet-gateway>
 set network virtual-router Private-VR routing-table ip static-
route AzureLBHealthProbe interface ethernet1/2 set network virtual-
router Private-VR routing-table ip static-route AzureLBHealthProbe
 destination 168.63.129.16/32
```

 ©2024 Palo Alto Networks, Inc.

- Definición de una ruta a una red virtual a través de una interfaz y dirección IP especificadas.

```
set network virtual-router Private-VR routing-table ip static-
route tovnet nexthop ip-address 10.2.2.1 set network virtual-
router Private-VR routing-table ip static-route tovnet interface
 ethernet1/2 set network virtual-router Private-VR routing-table ip
 static-route tovnet destination 10.1.0.0/16
```

- Configuración de rutas en *Public-VR* para reenviar todo el tráfico dirigido a Internet a través de una IP especificada.

```
set network virtual-router Public-VR routing-table ip static-
route Internet nexthop ip-address 10.2.1.1 set network virtual-
router Public-VR routing-table ip static-route Internet interface
 ethernet1/1 set network virtual-router Public-VR routing-table ip
 static-route Internet destination 0.0.0.0/0
```

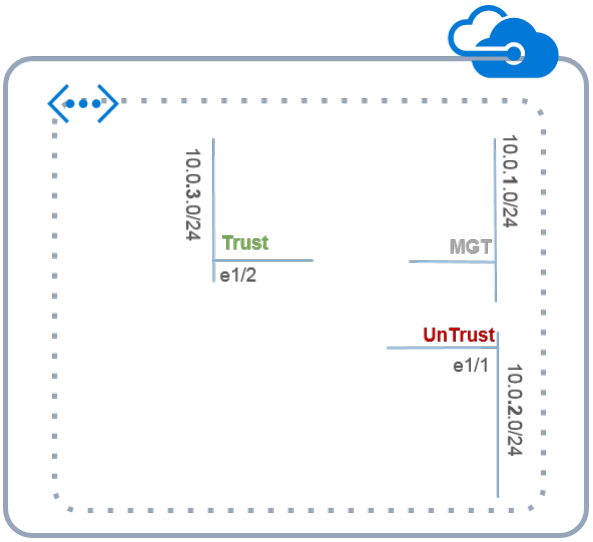
- Definición de rutas en *Public-VR* para el tráfico destinado a rangos de IP privados que se encaminarán a *Private-VR*.

```
set network virtual-router Public-VR routing-table ip static-route
 rfc1918-1 nexthop next-vr Private-VR set network virtual-router
 Public-VR routing-table ip static-route rfc1918-1 destination
 10.0.0.0/8 set network virtual-router Public-VR routing-table
 ip static-route rfc1918-2 nexthop next-vr Private-VR set network
 virtual-router Public-VR routing-table ip static-route rfc1918-2
 destination 172.16.0.0/12 set network virtual-router Public-VR
 routing-table ip static-route rfc1911-3 nexthop next-vr Private-VR
```

 ©2024 Palo Alto Networks, Inc.

Implementación del cortafuegos VM-Series desde Azure China Marketplace (plantilla de soluciones)

Las siguientes instrucciones muestran cómo implementar la plantilla de soluciones para el cortafuegos VM-Series que está disponible en Azure China Marketplace. Azure China Marketplace solo es compatible con el modelo BYOL del cortafuegos VM-Series. Puede implementar el cortafuegos en un grupo de recursos existente que esté vacío o en un nuevo grupo de recursos. La red virtual predeterminada en la plantilla es 10.0.0.0/16 y despliega un cortafuegos VM-Series que tiene 3 interfaces de red, una de gestión y dos interfaces del plano de datos, como se muestra a continuación. Para usar las plantillas de ARM personalizables disponibles en el repositorio de GitHub, consulte Uso de la plantilla ARM para implementar el cortafuegos VM-Series.



STEP 1 | Configure una cuenta de Azure.

1. Cree una cuenta de Microsoft.
2. Inicie sesión en el portal de Azure (**`https://portal.azure.com`**) utilizando las credenciales de su cuenta de Microsoft.

   *Si está utilizando una suscripción de prueba, puede ser necesario abrir una solicitud de soporte (**Help + Support [Ayuda + soporte]** > **New Support Request [Nueva solicitud de soporte]**) para incrementar la cuota de núcleos VM asignados.*

©2024 Palo Alto Networks, Inc.

STEP 2 | Encuentre la plantilla de soluciones VM-Series en Azure Marketplace.

1. Busque Palo Alto Networks en Azure China marketplace (https://market.azure.cn). Se muestra la oferta para las diferentes versiones de PAN-OS de los cortafuegos VM-Series.



2. Seleccione una oferta y haga clic en **Immediate deployment of (Implementación inmediata de)**.

STEP 3 | Implemente el cortafuegos.

1. Seleccione su **Subscription (Suscripción)** de Azure.
2. Seleccione un grupo de recursos para mantener todos los recursos asociados con el cortafuegos VM-Series en esta implementación.

   Puede implementar el cortafuegos VM-Series en un nuevo grupo de recursos o un grupo de recursos existente que esté vacío. Para implementar el cortafuegos en un grupo de recursos existente que cuenta con otros recursos, use la plantilla ARM en el Repositorio GitHub o su propia plantilla ARM personalizada. Asegúrese de que los recursos existentes coincidan con los valores de los parámetros que proporciona en la plantilla ARM.

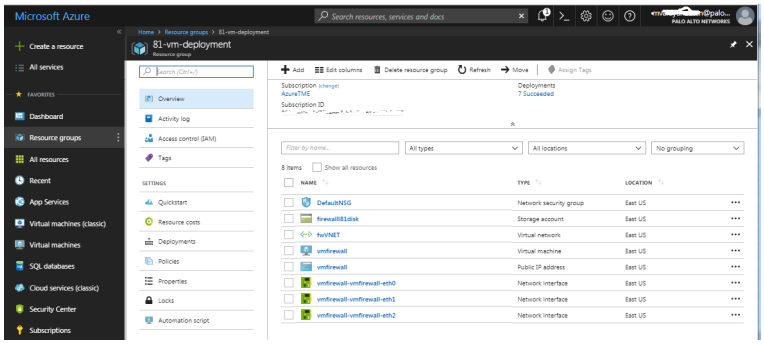
   1. Si crea un nuevo grupo de recursos, introduzca un nombre para el grupo de recursos y seleccione la región de Azure China donde desea implementar el cortafuegos.
   2. Si selecciona un grupo de recursos existente, seleccione la región de Azure China para este grupo de recursos y seleccione la implementación completa.
3. Configure los ajustes básicos para el cortafuegos.
   1. Introduzca el nombre de la cuenta de almacenamiento para una cuenta existente o cree una nueva.
   2. Introduzca el nombre del contenedor de almacenamiento blob en el cual se copiará y guardará la imagen vhd del cortafuegos.
   3. Introduzca un nombre DNS para acceder a la dirección IP pública en la interfaz de administración (eth0) del cortafuegos. Para acceder a la interfaz web del

 ©2024 Palo Alto Networks, Inc.

cortafuegos, debe combinar el prefijo que introduce con el sufijo, por ejemplo <yourDNSname><china_region>.cloudapp.azure.com.

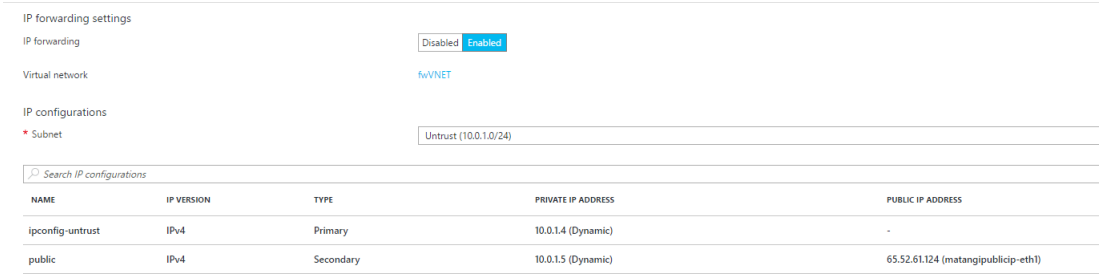
4. Introduzca un **Username (Nombre de usuario)** para el administrador del cortafuegos.
5. Introduzca una **Password (Contraseña)** para asegurar el acceso administrativo al cortafuegos.
6. Seleccione la capa de máquina virtual Azure y el tamaño para cumplir con sus necesidades. Consulte Requisitos mínimos del sistema para VM-Series en Azure.
7. Introduzca un **VmName** que es un nombre utilizado para identificar al cortafuegos VM-Series en el grupo de recursos.
8. Use **PublicIPAddressName** para etiquetar la interfaz de gestión del cortafuegos dentro del grupo de recursos. Microsoft Azure vincula el nombre DNS que definió con este nombre para que pueda acceder a la interfaz de gestión en el cortafuegos desde internet público.
9. Introduzca **Name (Nombre)** para identificar el emisor. El **IP Address Prefix (Prefijo de dirección IP)** predeterminado para la red virtual es 10.0.0.0/16. Puede cambiar esto para cumplir con sus necesidades de direcciones IP.
10. Configure las subredes para las interfaces de red. Si usa una red virtual existente, debe haber definido tres subredes, una para cada una de las interfaces de gestión, fiable y no fiable. Si crea una nueva Vnet, verifique o cambie los prefijos de cada subred. Las subredes predeterminadas son 10.0.1.0/24, 10.0.2.0/24 y 10.0.3.0/24. Puede asignar estas subredes a las interfaces de gestión, fiable y no fiable como desee.

4. Revise el resumen, acepte los términos de uso y la política de privacidad, y haga clic en **Immediate deployment (Implementación inmediata)** para implementar el cortafuegos. La implementación puede tardar 20 minutos y puede usar el enlace en la página para verificar el progreso.
5. Verifique que se ha implementado con éxito el cortafuegos VM-Series.
   1. Inicie sesión en el portal de Azure China (https://portal.azure.cn) utilizando las credenciales de su cuenta de Microsoft.
   2. Seleccione **Dashboard (Panel)** > **Resource Groups (Grupo de recursos)**, seleccione el grupo de recursos.
   3. Seleccione en **All Settings (Todos los ajustes)** > **Deployments (Implementaciones)** > **Deployment History (Historial de implementaciones)** para el estado detallado



STEP 4 | Adjunte una dirección IP pública para la interfaz no fiable del cortafuegos VM-Series. Esto le permite acceder a la interfaz desde internet público y es útil para cualquier aplicación o servicio que se encuentre en internet.

1. En el portal Azure, seleccione la interfaz de red para la que desea agregar una dirección IP pública. Por ejemplo, la interfaz eth1.
2. Seleccione **IP Configurations (Configuraciones de IP)** > **Add (Añadir)** y para la dirección IP pública, seleccione **Enabled (Habilitado)**. Cree una nueva dirección IP pública o seleccione una que tenga disponible.
3. Verifique que puede ver la dirección IP secundaria asociada con la interfaz.

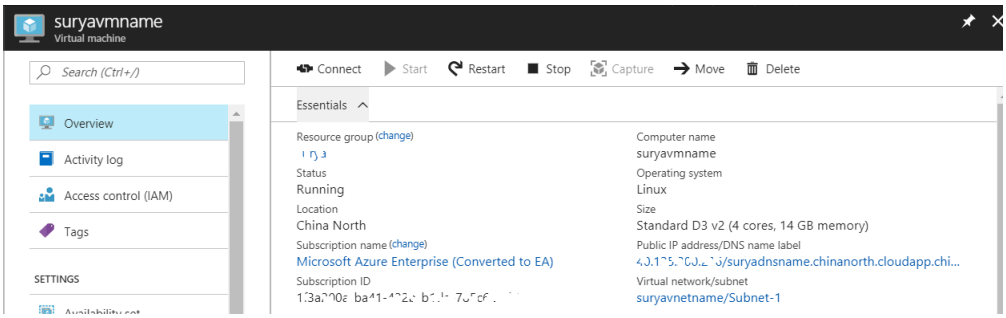


Cuando conecta una dirección IP secundaria a una interfaz de red, el cortafuegos VM-Series no adquiere automáticamente la dirección IP privada asignada a la interfaz. Necesitará configurar manualmente la dirección IP privada utilizando la interfaz web de cortafuegos VM-Series. Consulte Configure las interfaces de red del plano de datos como interfaces de capa 3 en el cortafuegos.

Cada interfaz en el cortafuegos VM-Series en Azure puede tener una dirección IP dinámica (predeterminada) o estática privada, y múltiples direcciones IP públicas (estáticas o dinámicas) asociadas a ella. El número máximo de direcciones IP públicas que puede asignar a una interfaz se basa en su suscripción a Azure. Cuando crea una nueva dirección IP pública, obtiene una del bloque de direcciones IP que posee Microsoft, por lo que no puede elegir una específica.

STEP 5 | Inicie sesión en la interfaz web del cortafuegos.

1. En el portal de Azure, en **All Resources (Todos los recursos)**, seleccione el cortafuegos VM-Series y visualice el nombre de DNS completo para el cortafuegos.



2. Utilizando una configuración segura (https) desde su navegador web, inicie sesión en el nombre de DNS para el cortafuegos.
3. Introduzca el nombre de usuario/contraseña definido anteriormente. Verá una advertencia de certificación; es normal. Vaya a la página web.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Active las licencias del cortafuegos VM-Series.

1. Cree una cuenta de asistencia técnica.
2. Registre el cortafuegos VM-Series (con código de autenticación).
3. En la interfaz web del cortafuegos, seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y seleccione **Activate feature using authentication code (Activar función usando el código de actualización)**.
4. Introduzca el código de autenticación de capacidad que registró en el portal de asistencia técnica. El cortafuegos se conectará con el servidor de actualización (updates.paloaltonetworks.com), descargará la licencia y se reiniciará automáticamente.
5. Vuelva a iniciar sesión en la interfaz web y confirme lo siguiente en el **Dashboard (Panel)**:
   - Se muestra un número de serie válido en **Serial# (Nº de serie)**.

     Si aparece el término Desconocido, significa que el dispositivo no tiene licencia. Para ver logs de tráfico en el cortafuegos, debe instalar una licencia de capacidad válida.
   - El **VM Mode (Modo VM)** se muestra como Microsoft Azure.

STEP 7 | Configure las interfaces de red del plano de datos como interfaces de capa 3 en el cortafuegos.

Si aloja varios sitios web o servicios con diferentes direcciones IP y certificados SSL en un único servidor, es posible que necesite configurar más de una dirección IP en las interfaces de cortafuegos VM-Series.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
2. Haga clic en el enlace de **ethernet 1/1** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: Capa3 (predeterminado).
   - En la pestaña Config (Configurar), asigne la interfaz el enrutador predeterminado.
   - En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione Nueva zona. Defina una zona nueva denominada Untrust y haga clic en OK (Aceptar).
   - En la pestaña **IPv4**, seleccione **DHCP Client (Cliente DHCP)** si planifica asignar solo una dirección IP en la interfaz. Se adquirirá automáticamente la dirección IP privada en la plantilla ARM. Si planifica asignar más de una dirección IP, seleccione **Static (Estática)** e introduzca manualmente las direcciones IP primarias y secundarias asignadas a la interfaz en el portal de Azure.
   - Anule la selección de la casilla de verificación **Automatically create default route to default gateway provided by server (Crear automáticamente ruta predeterminada a la puerta de enlace predeterminada proporcionada por el servidor)**. La desactivación de esta opción garantiza que el tráfico gestionado por esta interfaz no fluya directamente a la puerta de enlace predeterminada en la red virtual.
3. Haga clic en el enlace de **ethernet 1/2** y configúrelo del siguiente modo:
   - Establezca **Interface Type (Tipo de interfaz)** a Capa3 (predeterminado).
   - **Security Zone (Zona de seguridad)**: Fiable
   - **IP address (Dirección IP)**: Seleccione **DHCP Client (Cliente DHCP)** o **Static (Estática)**.
   - Anule la selección de la casilla de verificación **Automatically create default route to default gateway provided by server (Crear automáticamente ruta predeterminada a la**

 ©2024 Palo Alto Networks, Inc.

puerta de enlace predeterminada proporcionada por el servidor). La desactivación de esta opción garantiza que el tráfico gestionado por esta interfaz no fluya directamente a la puerta de enlace predeterminada en la red virtual.

4. Haga clic en **Commit (Confirmar)**. Verifique que el enlace para la interfaz esté en estado activo.

STEP 8 | Configure el cortafuegos para su implementación específica.

- Puerta de enlace: Implemente un balanceador de carga externo delante de la zona No fiable.
- Híbrido y Entre VNet: Implemente una puerta de enlace VPM de Azure o una máquina virtual NAT delante de la zona No fiable.
- Entre subredes: En el cortafuegos VM-Series, añada una regla de política de seguridad intra-zona para permitir el tráfico basado en las subredes adjuntadas a la interfaz Fiable.
- GlobalProtect: Implemente una máquina virtual NAT delante de la zona No fiable.

STEP 9 | Dirija el tráfico al cortafuegos VM-Series.

1. Para garantizar que el cortafuegos VM-Series proteja todo el tráfico dentro del grupo de recursos de Azure, configure rutas estáticas en el cortafuegos.
2. Configure los UDR para dirigir todo el tráfico a través de las interfaces en el cortafuegos VM-Series. Para más información, consulte la documentación de Azure sobre UDRs.

   Las UDR de las subredes internas deben enviar todo el tráfico a través de la interfaz Fiable. Las UDR del lado No fiables dirigen todo el tráfico desde Internet a través de la interfaz No fiable en el cortafuegos VM-Series. El tráfico de Internet puede llegar de Azure Application Gateway o Azure Load Balancer, o a través de la puerta de enlace VPN de Azure; en el caso de una implementación híbrida que conecta su red local con la nube de Azure.

 ©2024 Palo Alto Networks, Inc.

Implementaciones organizadas de Panorama en Azure

El complemento de Panorama para Azure implementa, configura y supervisa de forma centralizada su estrategia de seguridad en la nube de Azure. Organiza las implementaciones de VM-Series en su red de Azure para que pueda habilitar políticas de seguridad para cortafuegos gestionados. El complemento conecta con la implementación de Azure ARM y las páginas de Azure Monitor, lo que proporciona visibilidad del estado de la implementación, el uso y el rendimiento de sus cortafuegos VM-Series.

En Azure, el complemento organiza la implementación de recursos de Azure, como balanceadores de carga, subredes y puertas de enlace NAT, así como conjuntos de escalado automático de cortafuegos VM-Series. En Panorama, el complemento configura automáticamente los grupos de dispositivos de Panorama, las pilas de plantillas y las políticas NAT. Lee las etiquetas de sus recursos de Azure y luego habilita de manera centralizada las políticas basadas en etiquetas en un grupo de cortafuegos.

El complemento de Panorama puede organizar implementaciones en una o más regiones de su entorno de Azure. Una implementación puede consistir en una pila de hubs o una pila de entrada o ambas, según el tráfico que se debe proteger para su implementación:

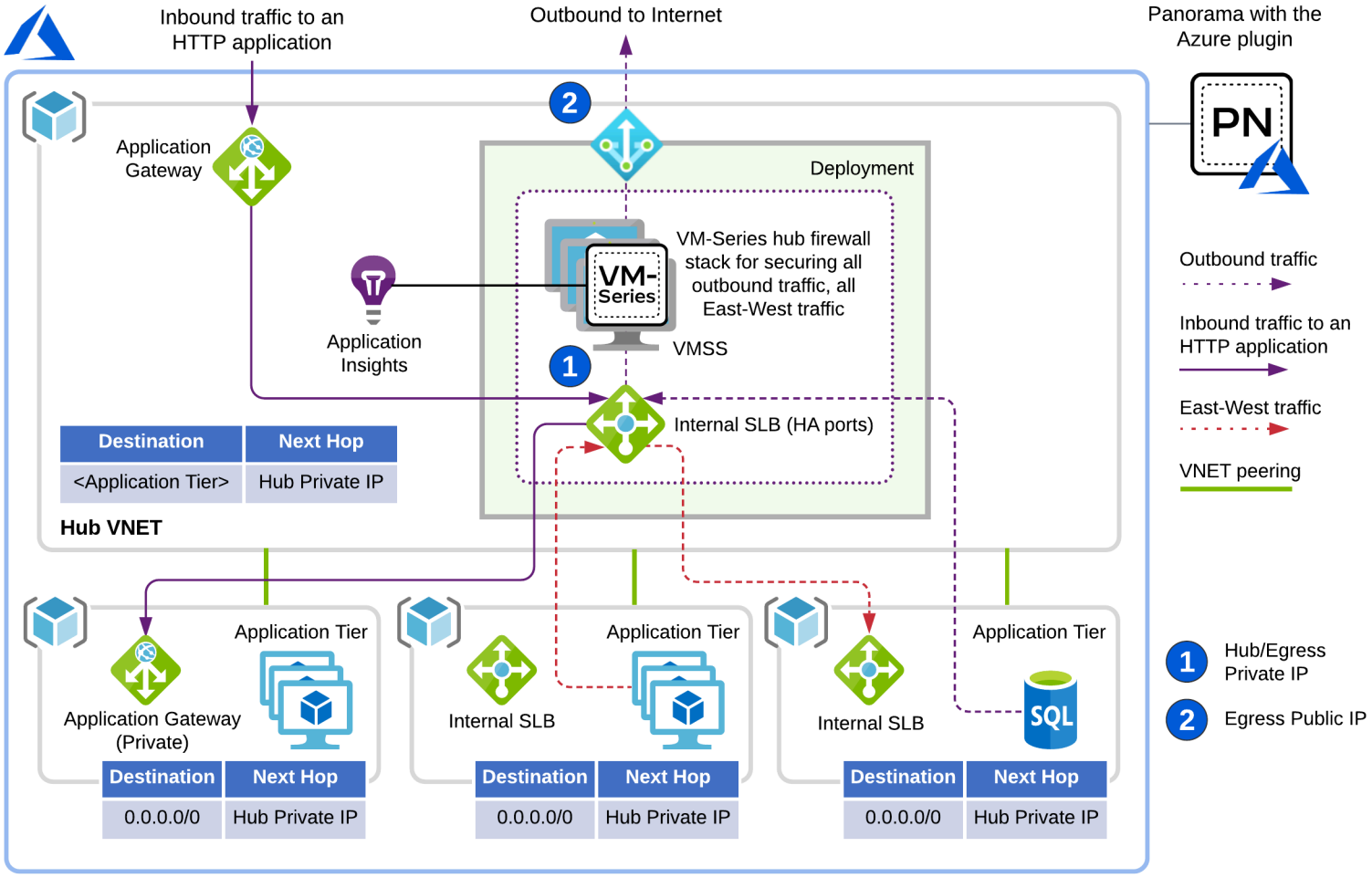
- Una pila de *cortafuegos de hub* protege el tráfico saliente y este-oeste entre las cargas de trabajo de su aplicación.
- Una pila de *cortafuegos de entrada* protege el tráfico hacia y desde sus aplicaciones orientadas al público.

Puede configurar el número de cortafuegos en cada pila. Tiene la opción de configurar un número estático de cortafuegos en su implementación o un rango para que VMSS lo use para el escalado. Ambas pilas en la implementación crean un VMSS de cortafuegos VM-Series y cada una puede ampliar hasta 25 cortafuegos.

Pila de hubs

Una implementación usa una pila de hubs y aprovecha el balanceador de carga estándar interno de Azure (con puertos HA) para realizar un escalado y balancear la carga en un conjunto de cortafuegos. A continuación, puede usar la dirección IP privada del balanceador de carga estándar (**2**, "IP privada de Hub/salida" en la siguiente figura) para enrutar el tráfico a los cortafuegos para inspección y prevención de amenazas. La pila de Hub protege el tráfico de salida y de Este a Oeste de sus aplicaciones.

 ©2024 Palo Alto Networks, Inc.



Para proteger su tráfico saliente y el tráfico Este-Oeste, añada reglas de ruta en las redes virtuales de su aplicación para redirigir el tráfico a la pila de Hub para su inspección.

Pila de entrada

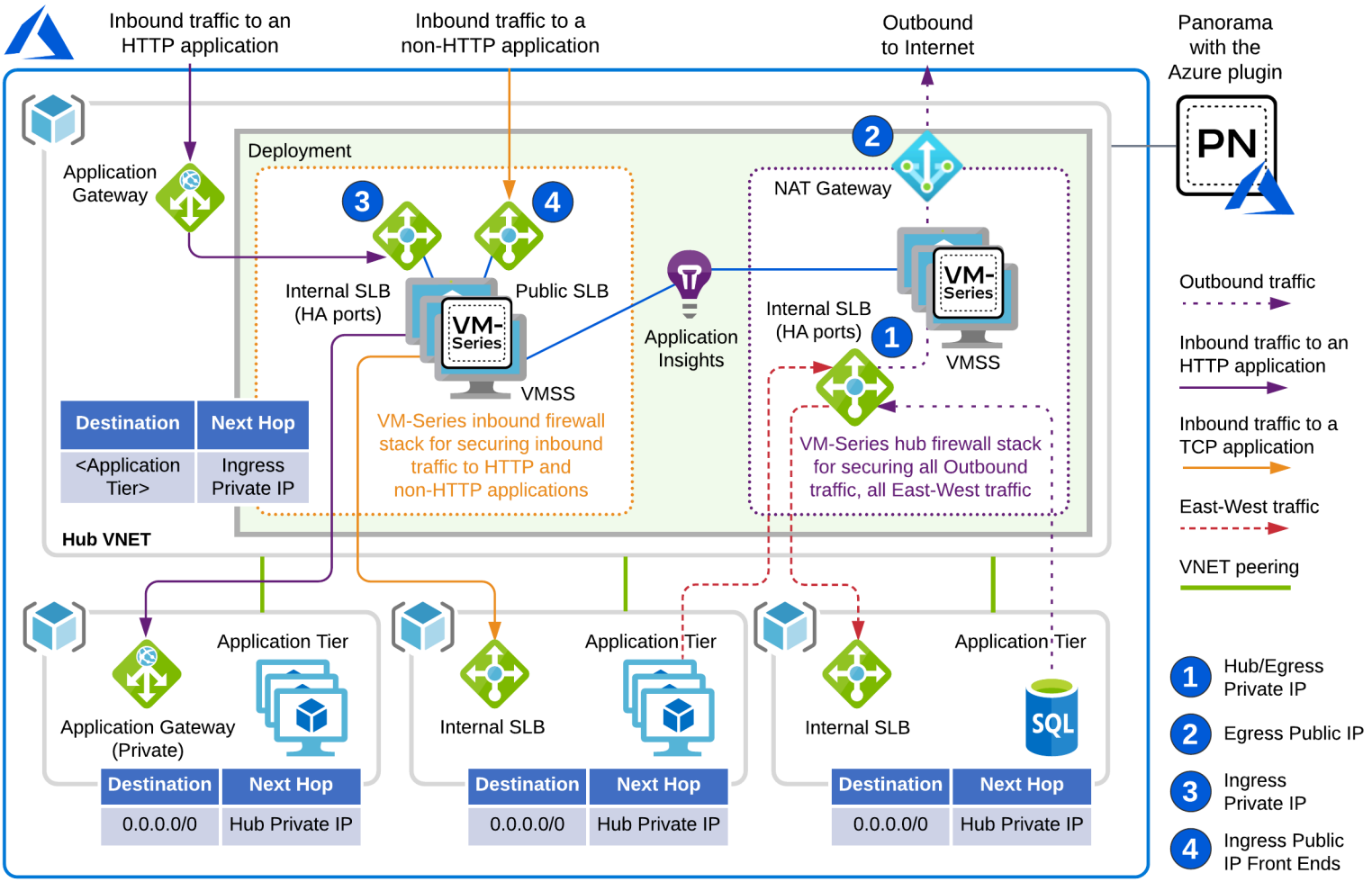
Una pila de cortafuegos de entrada realiza el escalado de forma independiente y añade visibilidad y seguridad al tráfico de entrada de sus aplicaciones.

Cada pila entrante puede proteger hasta 10 aplicaciones.

Para proteger su tráfico HTTP de entrada, añada UDR en las tablas de enrutamiento de subred de Application Gateway para enrutar todo el tráfico a la pila de entrada (**3**, IP privada de entrada en la siguiente figura). Para proteger el tráfico de entrada no HTTP, utilice el complemento de Panorama para crear entradas de front-end para los endpoints de su aplicación (**4**, Front-ends de entrada de IP pública en la siguiente figura). Para habilitar la inspección, el complemento de Panorama crea automáticamente reglas de balanceador de carga en el balanceador de carga estándar público de Azure y reglas NAT en los cortafuegos.

Si solo tiene tráfico de entrada HTTP/HTTPS, puede omitir la pila de entrada y proteger ese tráfico solo con la pila del hub.

 ©2024 Palo Alto Networks, Inc.



Consulte Preparación para una implementación organizada y Organice una implementación del cortafuegos VM-Series en Azure.

Preparación para una implementación organizada

Complete las siguientes tareas antes de organizar un cortafuegos VM-Series en Azure.

- Requisitos previos de configuración
- Permisos de orquestación
- Cree una función personalizada y asóciela a Active Directory
- Encuentre su nombre de Azure Directory Domain

Requisitos previos de configuración

Complete las siguientes tareas básicas en Panorama y Azure.

©2024 Palo Alto Networks, Inc.

- Azure
  - Cree una entidad de servicio para permitir que el complemento realice llamadas a la API.
  - Planifique un bloque CIDR específicamente dedicado a la VNet de tránsito del cortafuegos VM-Series. El complemento gestiona este bloque CIDR y lo usa para implementar la red virtual de cortafuegos inicial y realizar actualizaciones futuras a nuevas pilas de plantillas.

    El rango CIDR mínimo es /22.
- Panorama
  - Asegúrese de tener una clave API de licencia válida configurada en Panorama. Esto permite que el complemento gestione la eliminación de las licencias en los eventos de escalado automático. Consulte Instalación de una clave de API de desactivación de licencia.
  - Instale la última versión del complemento de VM-Series en Panorama para permitir que la configuración de Application Insight se añada a la pila de plantillas.
- Regiones de Azure cualificadas

  Las implementaciones orquestadas en panorama se admiten en todas las regiones que admitan el cortafuegos VM-Series. Las siguientes regiones han cualificado; si implementa en una región no incluida en la lista y encuentra un problema, póngase en contacto con la asistencia técnica.
  - Oeste de EE. UU.
  - Oeste de EE.UU. 2
  - Centro Norte de EE. UU.
  - Este de EE. UU.
  - Este de EE.UU. 2
  - Europa Occidental
  - Alemania Centro-Oeste
  - Emiratos Árabes Unidos Norte
  - India Occidental
  - Sureste de Australia

Mientras planifica su implementación, tenga en cuenta que si actualmente está ejecutando un complemento de Panorama para la versión 2.x de Azure, no se permite la actualización a la versión actual. Junto con esto, una vez que se instala la versión actual, no se permite el cambio a la versión 2.x del complemento. Consulte el complemento de Panorama para Azure en la Matriz de compatibilidad.

Permisos de orquestación

El es un archivo JSON de muestra con permisos para la función de Implementador de plantillas. En la sección **`AssignableScopes`**, incluya todas las suscripciones relevantes que se deben consultar, incluida la suscripción en la que se implementa la implementación y CADA suscripción que contenga una red virtual de aplicación que esté emparejada con la red virtual del cortafuegos VM-Series donde existan recursos protegidos .

```
{ "Name": "Template Deployment", "IsCustom": true,
 "Description": "Manage template deployments.",    "Actions":
 [ "Microsoft.Resources/subscriptions/resourcegroups/*",
```

 ©2024 Palo Alto Networks, Inc.

```
 "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}", . . . ] }
```

Cree una función personalizada y asóciela a Active Directory

STEP 1 | Para crear un Active Directory en Azure, vaya a Azure Active Directory y haga clic en **App registrations (Registros de la aplicación)** a la izquierda. Cree una función personalizada con los permisos que requiere el complemento.

A continuación se incluye un ejemplo de JSON.

1. Haga clic en **Add (Añadir)** y proporcione un nombre. Seleccione la función creada a partir del archivo JSON anterior, deje "Asignar acceso a" como usuario de Active Directory y luego seleccione el directorio activo creado en el primer paso y haga clic en Guardar.
2. Seleccione el tipo.

   No modifique nada en la URI de redirección.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Cree una función personalizada con los permisos que requiere el complemento.

Consulte Permisos de orquestación.

1. Inicie sesión en la CLI de Azure.

```
az login
```

2. Cree una función personalizada a partir del archivo en Permisos de orquestación.

```
az role definition create --role-definition <role-json-file>
```

STEP 3 | Asocie la función con el Active Directory que creó en el Paso 1. Puede utilizar la consola o la CLI.

Debe repetir este paso en cada suscripción definida en la sección ***`assignableScope`*** *de la función personalizada en* Permisos de orquestación.

Consola

1. En el portal de Azure, vaya a **Subscriptions (Suscripciones)** y seleccione su suscripción.
2. A la izquierda, seleccione **Access Control (IAM) [Control de acceso (IAM)]** y luego **Role Assignments (Asignaciones de funciones)** en la barra superior.
3. Seleccione **Add (Añadir)** y elija **add role assignment (añadir asignación de funciones)**.
   - Seleccione la función que creó en el Paso 3 y deje "Asignar acceso a" como usuario de Active Directory.
   - Seleccione el directorio activo creado en el Paso 1 y haga clic en **Save (Guardar)**.

CLI:

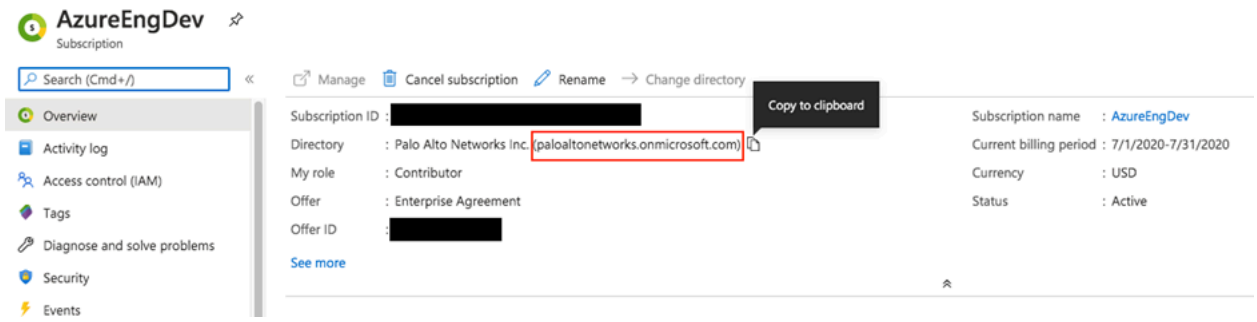
En el siguiente comando, **`<role-name>`** hace referencia al nombre en el archivo JSON de muestra, en el ejemplo anterior, **`Implementación de plantilla`**.

```
az ad sp create-for-rbac --name <name-of-service-principal> --role
 <role-name> --output json
```

Encuentre su nombre de Azure Directory Domain

Para que el complemento proporcione vínculos a su implementación de Azure y la instancia de Application Insights en el portal de Azure, debe identificar el dominio de directorio para su suscripción, como se muestra a continuación:

 ©2024 Palo Alto Networks, Inc.



Organice una implementación del cortafuegos VM-Series en Azure

Puede crear un máximo de diez implementaciones organizadas. Además, cada implementación orquestada admite hasta 100 aplicaciones de front-end.

Azure China y Azure Government no son compatibles.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Añada una entidad de servicio.

Incorpore sus credenciales de entidad de servicio creadas para otorgar permisos al complemento de Panorama para realizar las llamadas API necesarias para organizar su implementación.

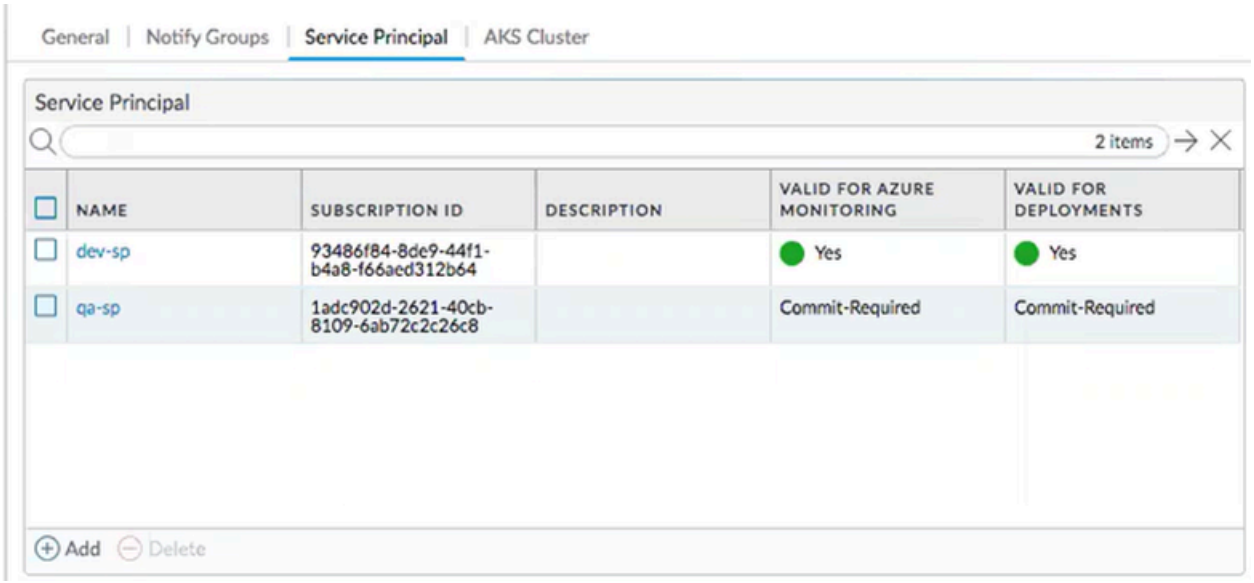
1. Seleccione **Setup (Configuración)** > **Service Principal (Entidad de servicio)** > **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** y, una **Description (Descripción)** opcional para identificar la cuenta de servicio.
3. Introduzca la **Subscription ID (ID de suscripción)** para la suscripción de Azure que desea supervisar.

   Debe iniciar sesión en su portal de Azure para obtener la ID de esta suscripción.
4. Introduzca el **Client ID (ID del cliente)**. El ID del cliente de la aplicación asociada a su aplicación de Azure Active Directory.
5. Introduzca el **Client Secret (Secreto del cliente)** y vuelva a introducirla para confirmarlo.
6. Introduzca la **Tenant ID (ID de inquilino)**.

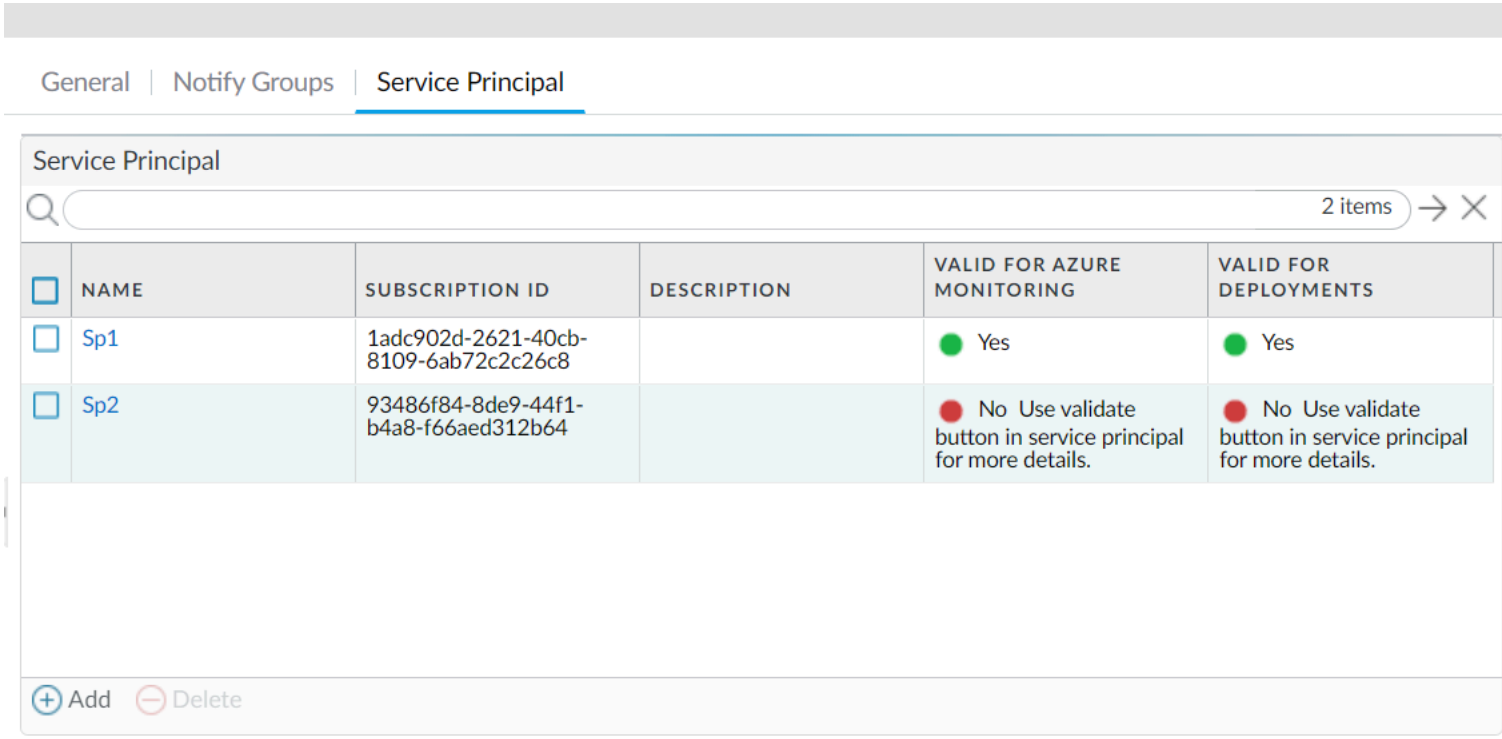
   La ID de inquilino es la ID del directorio que guardó cuando configuró la aplicación de Active Directory.
7. Haga clic en **Validate (Validar)** para comprobar que las claves y las ID que introdujo sean válidas y que Panorama se puede comunicar con la suscripción a Azure usando la API.

   Puede tardar hasta un minute en validar. Puede actualizar la página para comprobar su progreso.
8. Cuando la entidad de servicio sea válida, confirme sus cambios.

   La confirmación garantiza que la entidad de servicio esté disponible cuando configure la implementación.



 ©2024 Palo Alto Networks, Inc.



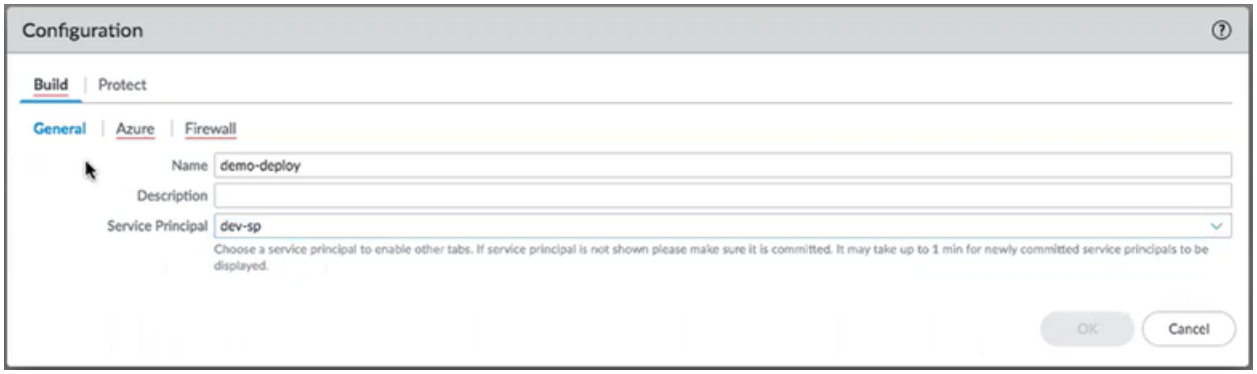
 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configure su implementación de Azure.

1. Seleccione **Deployments (Implementaciones)** y **Add (Añadir)** una configuración.
2. Seleccione **Build (Compilación)** > **General**.
   - Proporcione un **Name (Nombre)** y una **Description (Descripción)** opcional.
   - Seleccione una entidad de servicio de la lista desplegable.

     Debe seleccionar una entidad de servicio válida para habilitar la pestaña **Azure** .

     Si no ve la entidad de servicio, vuelva al Paso 1 y asegúrese de que la entidad de servicio sea válida y esté confirmada.



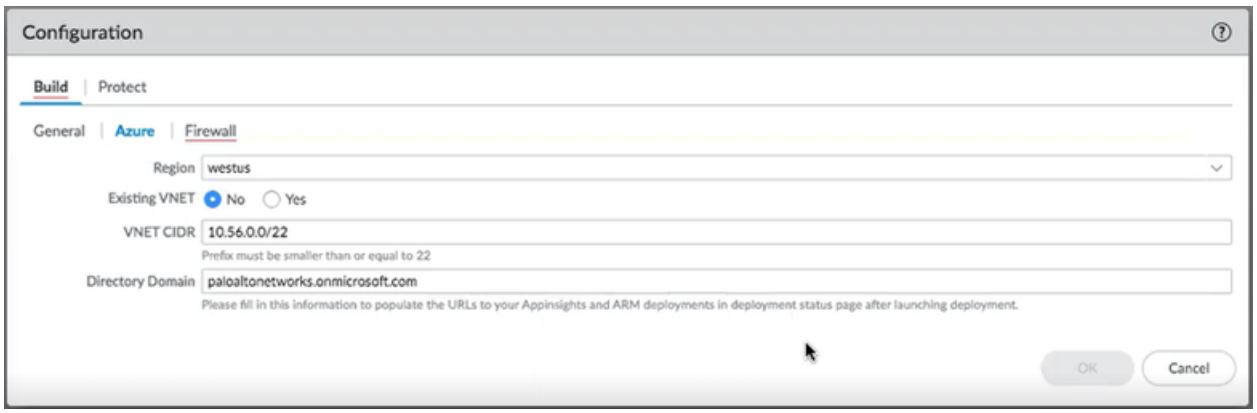
3. En la pestaña **Build (Compilación)** > **Azure**, seleccione una región.

   La lista desplegable es dinámica: enumera todas las regiones que tienen una imagen de cortafuegos de nueva generación VM-Series de Palo Alto Networks.

   - **Existing VNET (VNET existente)**.
     - Seleccione **No** para crear una nueva red virtual.

       El complemento utiliza CIDR de VNET y Dominio de directorio para crear una VNET para usted.
     - Seleccione **Yes (Sí)** para indicar una red virtual existente.
   - **VNET CIDR (CIDR de VNET)**: introduzca su rango de CIDR. El prefijo debe ser menor o igual a /22. Por ejemplo, 192.168.0.0/22.
   - **Directory Domain (Dominio del directorio)**: consulte Encuentre su nombre de Azure Directory Domain. Esta cadena es parte de la URL de todos los recursos de la suscripción y ayuda al complemento a que se vincule con las implementaciones.

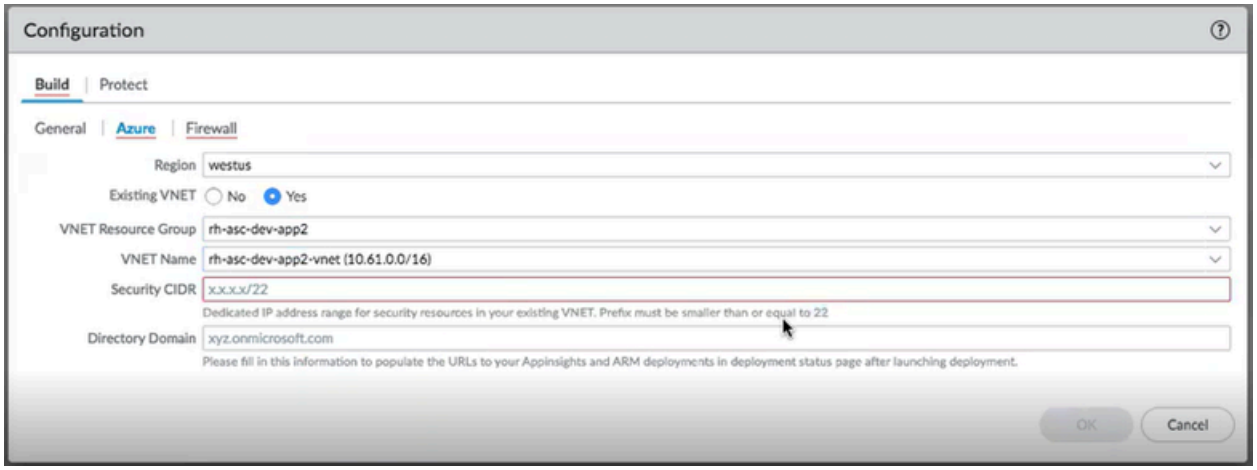
 ©2024 Palo Alto Networks, Inc.



Si selecciona **Yes (Sí)**, el complemento solicita el grupo de recursos de VNET, el nombre de VNET, el CIDR de seguridad y el Dominio de directorio.

- **VNET Resource Group (Grupo de recursos de VNET)**: elija de una lista de todos los grupos de recursos en la región seleccionada.
- **VNET Name (Nombre de VNET)**: elija de una lista de redes virtuales en su grupo de recursos elegido.
- **Security CIDR (CIDR de seguridad)**: introduzca su rango de CIDR. El prefijo debe ser menor o igual a /22. Por ejemplo, 192.168.0.0/22.
- **Directory Domain (Dominio del directorio)**: consulte Encuentre su nombre de Azure Directory Domain. Esta cadena es parte de la URL de todos los recursos de la suscripción y ayuda al complemento a que se vincule con las implementaciones.

El Grupo de recursos de VNET y el nombre de VNET ayudan al complemento a localizar su VNET existente. Todo lo que implementa el complemento entra en un grupo de recursos que gestiona el complemento.



 ©2024 Palo Alto Networks, Inc.

STEP 3 | Configure las pilas de cortafuegos VM-Series para su implementación.

Puede implementar la pila de Hub para proteger el tráfico saliente / este-oeste. Puede implementar la pila de entrada para proteger el tráfico de entrada. También puede implementar ambas pilas si es necesario proteger todos los flujos de tráfico.

Los parámetros de configuración son los mismos para ambas pilas.

- **License Type (Tipo de licencia)**: seleccione BYOL, Paquete 1 o Paquete 2.
- **License Authcode (Código de autorización de licencia)**: (solo BYOL). Introduzca el código de autenticación enviado en su carta de bienvenida.
- **VM Size (Tamaño de VM)**
  - La lista desplegable muestra los tamaños de VM que se correlacionan con el código de autenticación que introdujo.
  - Paquete 1 o Paquete 2: elija cualquier tamaño de máquina virtual (VM).

Grupo de dispositivos existente: el grupo de dispositivos debe ser único tanto en las pilas como en las implementaciones. Es decir, necesita un grupo de dispositivos dedicado independiente para cada pila en cada implementación.

Si selecciona **No**, el complemento crea un grupo de dispositivos.

Si selecciona **Yes (Sí)**, seleccione un grupo de dispositivos existente de la lista desplegable.

- **Min Firewalls (Cortafuegos mín.)**: un valor entre 1 y 25 para un VMSS.
- **Max firewalls (Máx. cortafuegos)**: un valor entre 1 y 25 para un VMSS.

STEP 4 | Seleccione **Build (Compilación)** > **Firewall (Cortafuegos)** > **Basic (Básico)** para configurar la información común a ambas Pilas.

Para **Image Type (Tipo de imagen)**, seleccione **Marketplace Image (Imagen de Marketplace)** o **Custom Image (Imagen personalizada)**.

- **Image Resource Group (Grupo de recursos de imágenes)**: (solo imagen personalizada) elija el grupo de recursos que contiene su imagen personalizada. Para una imagen personalizada, la lista

 ©2024 Palo Alto Networks, Inc.

muestra todos los grupos de recursos que contienen una imagen de la región que seleccionó en el Paso 2. b.

- **Image (Imagen)**: (solo imagen personalizada) la lista desplegable muestra todas las imágenes del grupo de recursos seleccionado.
- **Software Version (Versión de software)**: (imagen de Marketplace) solo se muestran las versiones de software válidas. Consulte la Matriz de compatibilidad para conocer la versión mínima de PAN-OS.
- **Username (Nombre de usuario)**: el nombre de usuario del administrador para el cortafuegos que crea. El nombre debe ser legal tanto para el cortafuegos VM-Series como para Azure. Consulte ¿Cuáles son los requisitos de nombre de usuario al crear una VM?
- **Password (Contraseña)**: la contraseña de administrador para el cortafuegos que crea. La contraseña debe cumplir los requisitos de caracteres y longitud (31 caracteres) tanto para el cortafuegos VM-Series como para Azure. Consulte ¿Cuáles son los requisitos de contraseña al crear una VM?.
- **Confirm Password (Confirmar contraseña)**: vuelva a introducir su contraseña.
- **Primary Panorama IP (IP principal de Panorama)**: especifique la dirección IP de Panorama que el cortafuegos puede usar para conectarse a Panorama cuando se inicia. Elija entre la dirección IP pública o privada que se muestra en la lista desplegable, o escriba la dirección IP de Panorama.
- **Secondary Panorama IP (IP secundaria de Panorama)**: (solo si Panorama está en la configuración de HA). Especifique la IP secundaria de Panorama que el cortafuegos puede usar para conectarse a Panorama cuando se inicia. Elija de la lista desplegable o escriba la IP correcta.
- **Configure Device Certificate PIN (Configurar el PIN del certificado del dispositivo)**. Puesto que estos valores están cifrados, debe introducir y confirmar cada valor.
  - **Device Certificate PIN ID (ID del PIN del certificado del dispositivo)**: el ID del certificado del dispositivo.
  - **Confirm Device Certificate PIN ID (Confirmar el ID del PIN del certificado del dispositivo)**
  - **Device Certificate PIN Value (Valor del PIN del certificado del dispositivo)**: el valor del PIN del certificado.
  - **Confirm Device Certificate PIN Value (Confirmar el valor del PIN del certificado del dispositivo)**

STEP 5 | Seleccione **Build (Compilación)** > **Firewall (Cortafuegos)** > **Advanced (Avanzados)**, valores predeterminados opcionales.

Marque **Advanced (Avanzados)** para editar los valores predeterminados.

- **Autoscaling Metric (Métrica de escalado automático)**: el valor predeterminado es el porcentaje de utilidad de CPU del plano de datos.
- **Scale In Threshold (Escala en umbral)**: acepte el valor predeterminado o defina una escala en el umbral.
- **Scale Out Threshold (Umbral de ampliación horizontal)**: acepte el valor predeterminado o defina un escalado en el umbral.
- **Jumbo Frame (Tramas gigantes)**: desactivado de forma predeterminada.

Haga clic en **OK (Aceptar)** y en confirmar para aplicar los cambios. Actualice la página hasta que vea el botón **Deploy (Implementar)** y haga clic en **Deploy (Implementar)** para iniciar la implementación.

 ©2024 Palo Alto Networks, Inc.

Una vez que comienza la implementación, la información se escribe en la página **Deployments (Implementaciones)**.

La implementación tarda entre 15 y 20 minutos en completarse.

Si hay una entrada en la columna **Deployment Status (Estado de la implementación)**, haga clic en el hipervínculo para ver los detalles de la implementación.

Los posibles mensajes de estado son:

- **Commit changes (Confirmar cambios)**:ha añadido una implementación por primera vez, pero aún no ha confirmado los cambios.

  Cada cambio de configuración para la implementación debe estar confirmado para que el complemento pueda recoger sus cambios.
- **Deploying (Implementación)**: el complemento está implementando o actualizando la implementación. Para obtener más información, haga clic en el hipervínculo para ver el estado detallado.
- **Failure (Fallo)**: la implementación ha fallado. Haga clic en el hipervínculo y vea el **Detailed Status (Estado detallado)** para la Pila de seguridad.
- **No Deployed (No implementado)**:el complemento está listo para implementar la configuración, pero la implementación no ha comenzado.
- **Success (Correcto)**: el complemento ha implementado correctamente la Pila de seguridad y los cortafuegos se han conectado a Panorama. Los cortafuegos pueden pasar el tráfico.
- **Warning (Advertencia)**: la implementación ha finalizado correctamente, pero algo externo a la implementación ha fallado. Por ejemplo, es posible que vea este mensaje:

  ```
  Los cortafuegos no se han conectado después de 20 minutos de la finalización de la implementación.
  ```

  Haga clic en el hipervínculo y vea la Pila de seguridad.

Una vez que se realiza la implementación, el complemento le permite modificar un cierto subconjunto de parámetros. Una vez realizados los cambios, debe realizar una confirmación antes de hacer clic en

 ©2024 Palo Alto Networks, Inc.

el botón **Redeploy (Volver a implementar)**. Cuando se produce una actualización, el complemento se asegura de que la configuración de Panorama esté creada y sea precisa.

- **Deploy (Implementar)**: después de confirmar la configuración inicial, seleccione **Deploy (Implementar)** para iniciar la implementación.
- **Redeploy (Volver a implementar)**: modifique una implementación, confirme los cambios y seleccione **Redeploy (Volver a implementar)**.

  *Debe confirmar los cambios en la implementación antes de hacer clic en **Redeploy (Volver a implementar)**.*
- **Undeploy (Eliminar implementación)**: elimine una implementación, pero mantenga la configuración para que se pueda volver a implementar más adelante.

*Para quitar una implementación existente y su configuración, marque una implementación y seleccione **Delete (Eliminar)** en la parte inferior de la página de **Deployments (Implementaciones)**.*

STEP 6 | Seleccione **Azure** > **Deployments (Implementaciones)** para ver el estado de la implementación.

- La columna Grupo de recursos muestra los grupos de recursos que ha creado el complemento.
- La interfaz de gestión del cortafuegos utiliza la IP de acceso del cortafuegos para conectarse a Panorama. Debe incluir esta dirección en la lista de permitidos para asegurarse de que Panorama pueda conectarse con Panorama para obtener la configuración necesaria.

  Si Panorama se implementa en una nube pública, asegúrese de añadir la IP de acceso al cortafuegos al grupo de seguridad de Panorama.

  Consulte Puertos usados para Panorama para determinar qué puertos debe abrir para permitir el tráfico.
- Abra el enlace en la columna **Deployment Status (Estado de la implementación)** para obtener detalles adicionales para cada pila.
  - **Hub-Stack (Pila de hub)**: la IP pública de la pila de hub coincide con la IP de acceso al cortafuegos en el resumen de implementación porque la puerta de enlace NAT es la misma para el tráfico de salida de la implementación y el tráfico de gestión de los cortafuegos.

    Todo el tráfico saliente y este-oeste debe enrutarse a la **Egress Private IP (IP privada de salida)** para su inspección. Puede dirigir el tráfico a esta dirección si configuró las UDR.
  - **Inbound-Stack (Pila de entrada)**: la IP privada es la dirección del balanceador de carga interno de Azure que se encuentra frente a los cortafuegos. Puede dirigir el tráfico a esta dirección si está configurando las UDR.
- Siga los vínculos para ver la información de implementación y Application Insights en Azure.
- Los detalles de la implementación pueden mostrar mensajes de errores de Éxito, Advertencia y Error

STEP 7 | Configure la protección de entrada para aplicaciones TCP/UDP backend.

El balanceador de carga público que se encuentra al frente de la pila de cortafuegos de entrada es el punto de entrada para cualquier aplicación UDP o TCP backend. Añada la siguiente configuración

 ©2024 Palo Alto Networks, Inc.

para permitir que el complemento gestione el balanceador de carga necesario y la configuración del cortafuegos para enrutar a su aplicación de backend.

1. Seleccione **Azure** > **Deployments (Implementaciones)** y seleccione su implementación.
2. Seleccione la pestaña **Protect (Proteger)** y haga clic en **Add (Añadir)**.
3. Proporcione la aplicación **Name (Nombre)** y elija un **Protocol (Protocolo)**.

   Introduzca los detalles de protección:

   - **Frontend IP Type (Tipo de IP de frontend)**: selecciona una de las siguientes opciones: Nueva IP pública, Frontend existente e IP pública existente.

     Si selecciona Frontend existente, el **Frontend Name (Nombre de frontend)** enumera todas las interfaces conocidas en el balanceador de carga.
   - **Resource Group (Grupo de recursos)**: (solo IP pública existente) en la lista desplegable, seleccione el grupo de recursos donde se encuentra la dirección IP de su interfaz deseada.
   - Nombre de IP: (solo IP pública existente) se usa para asignar la IP a una interfaz en el balanceador de carga, configurar el balanceador de carga y crear una regla NAT.
   - **Frontend Port (Puerto frontend)**: añade el puerto de interfaz de usuario que debe configurarse para recibir tráfico en el balanceador de carga público.
   - **Backend IP (IP de backend)**: añade la dirección IP de su aplicación de backend.
   - **Backend Port (Puerto de backend)**: añade el puerto en el que su aplicación backend espera recibir tráfico.

   Haga clic en **OK (Aceptar)**.
4. **Commit (Confirmar)** para añadir la configuración en el balanceador de carga y enviarla a los cortafuegos.

 ©2024 Palo Alto Networks, Inc.

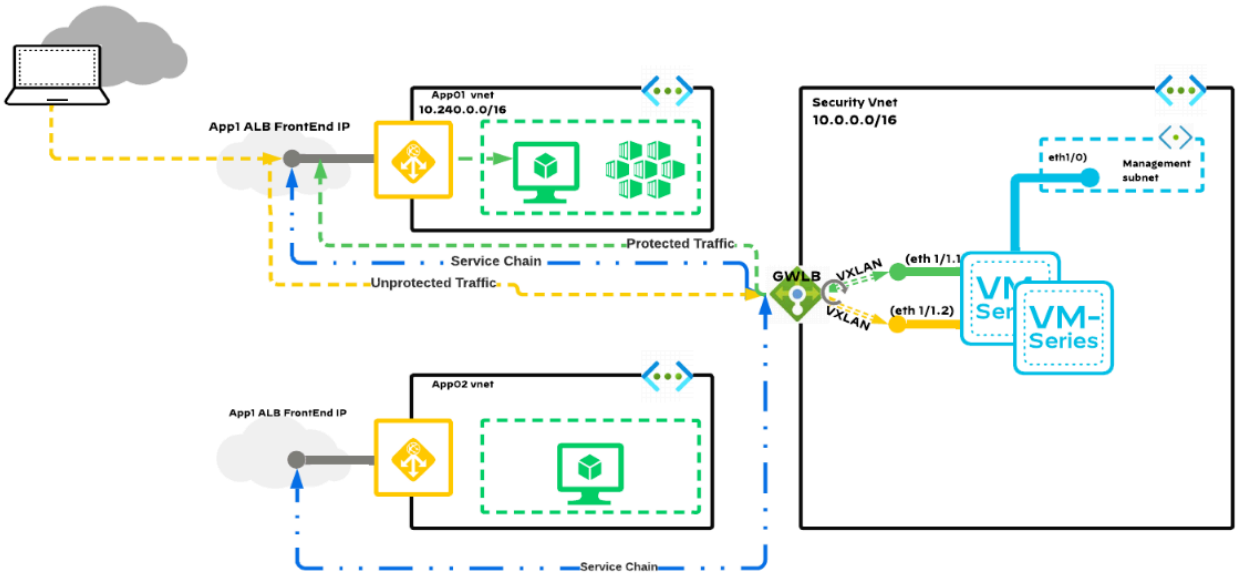
Implementar el VM-Series con el balanceador de carga de gateway de Azure

Ahora puede implementar el cortafuegos VM-Series para Azure en integración con el balanceador de carga de puerta de enlace de Azure (GWLB). La protección del tráfico de entrada requiere una visibilidad completa de la identidad de la fuente de tráfico mientras viaja a su destino en la nube. Cuando los cortafuegos VM-Series se implementan detrás de un balanceador de carga estándar público, las direcciones IP de origen del tráfico entrante se reemplazan con la dirección IP del balanceador de carga. Como resultado, la identidad de origen de la aplicación se ofusca u oculta. Al implementar los cortafuegos VM-Series detrás de Azure GWLB, los encabezados de los paquetes de tráfico y la carga útil se mantienen intactos, lo que proporciona una visibilidad completa de la identidad de la fuente a medida que viaja a su destino. Cuando la integración de Azure GWLB está habilitada, VM-Series usa paquetes VXLAN para inspeccionar el paquete interno de tráfico y aplicar directivas a ese paquete.

Cuando se implementan detrás de Azure GWLB, los cortafuegos VM-Series pueden aplicar políticas de seguridad basadas en zonas. Puede segmentar el tráfico con destino a la red virtual y a Internet mediante la asignación de una zona de confianza al tráfico con destino a la red virtual y una zona no fiable para el tráfico con destino a Internet.

Con esta integración, puede implementar el cortafuegos VM-Series como back-end en Azure GWLB en todas las regiones compatibles.

 ©2024 Palo Alto Networks, Inc.



La integración del cortafuegos VM-Series con Azure GWLB requiere PAN-OS 10.1.4 o posterior y el complemento VM-Series 2.1.4 o posterior.

Siga las prácticas recomendadas para no superponer los CIDR usados por diferentes redes virtuales.

STEP 1 | Implemente el cortafuegos VM-Series detrás de Azure GWLB mediante la plantilla ARM.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | (Opcional) Añada instancias de cortafuegos VM-Series adicionales detrás del GWLB implementado en el Paso 1.

1. Cree una máquina virtual con la CLI de Microsoft Azure.

   Proporcione los parámetros de entrada en el siguiente comando de muestra.

```
az vm create \ --resource-group <myResourceGroup> \ --
name <myPA-VM> \ --vnet-name secVnet \ --subnet Subnet-
mgmt \ --public-ip-sku Standard \ --size Standard_DS3_V2
 \ --nsg networkSecurityGroup1 \ --admin-username
 <username> \ --admin-password <password> \ --image
 paloaltonetworks:vmseries-flex:bundle1:10.1.4 \ --plan-
name bundle1 \ --plan-product vmseries-flex \ --plan-
publisher paloaltonetworks \ --custom-data "storage-
```

 ©2024 Palo Alto Networks, Inc.

```
account=<myStorageAccountName>,access-key=<myAccessKey>,file-
share=<FileName>,share-directory=<SharedDirectoryName>"
```

El archivo `init-cfg.txt` es necesario para arrancar el cortafuegos VM-Series. Este proporciona la información básica que el cortafuegos necesita para conectarse a su red. El archivo `init-cfg.txt` en la carpeta de arranque incluye la siguiente información.

- *Para implementar la solución con puertos predeterminados:*

  ```
  plugin-op-commands=azure-gwlb-inspect:enable
  ```

- *Para implementar la solución con puertos personalizados, use el comando de muestra en el archivo `init-cfg.txt`, si se usa el campo de datos personalizados para definir los ID de VNI y la información del puerto. Debe definir los identificadores VNI internos y externos en el rango de 800 a 1000.*

  ```
  plugin-op-commands=azure-gwlb-inspect:enable
  +internal-port-<internalport>+external-port-
  <externalport>+internal-vni-<internalvni>+external-
  vni-<internalvni>
  ```

  Si elige usar puertos personalizados, use estos comandos de muestra para configurar el GWLB.

  ```
  az network lb address-pool tunnel-interface
   add --resource-group <myResourceGroup> --lb-
  name <myGatewayLoadBalancer> --address-pool
   <myBackendPool> --type external --protocol
   vxlan --identifier <VNI> --port <port> az
   network lb address-pool tunnel-interface
   add --resource-group <myResourceGroup> --lb-
  name <myGatewayLoadBalancer> --address-pool
   <myBackendPool> --type internal --protocol vxlan
   --identifier <VNI> --port <port>
  ```

  Para obtener más información, consulte Datos personalizados y Cloud-init en Máquinas virtuales en Azure.

2. Cree NIC en la subred de datos.

   ```
   az network nic create -g <myResourceGroup> --vnet-name secVnet
    --subnet Subnet-data -n <myDataNIC> --accelerated-networking
    true --ip-forwarding true
   ```

3. Detenga la máquina virtual creada en el Paso 1.

   ```
   az vm deallocate -n <myPA-VM> -g <myResourceGroup>
   ```

 ©2024 Palo Alto Networks, Inc.

4. Añadir la NIC creada en el Paso 2 a la máquina virtual.

```
az vm nic add -g <myResourceGroup> --vm-name <myPA-VM> --nics
 <myDataNIC>
```

5. Añada la máquina virtual al grupo de direcciones de back-end de GWLB.

```
az network nic ip-config address-pool add --address-
pool BackendPool1 --ip-config-name ipconfig1 --nic-name
 <myDataNIC> --resource-group <myResourceGroup> --lb-name
 securityLB
```

6. Inicie la máquina virtual.

```
az vm start -n <myPA-VM> -g <myResourceGroup>
```

7. Conéctese al cortafuegos mediante SSH. Introduzca lo siguiente en la CLI del cortafuegos para verificar si el GWLB está habilitado.

```
show plugins vm_series azure gwlb
```

(Opcional) Si no arranca el cortafuegos, los **datos de usuario** se utilizan para configurar los puertos y los ID de VNI. Utilice los siguientes comandos de muestra en la CLI del cortafuegos para habilitar o deshabilitar GWLB, configurar puertos personalizados e ID de VNI, y ver el estado de GWLB y la asignación de ID de puerto/VNI.

Los números de puerto y los ID de VNI deben coincidir con los del grupo de direcciones de back-end de GWLB.

```
request plugins vm_series azure gwlb inspect enable yes request
 plugins vm_series azure gwlb parameters internal-port 2000
```

 ©2024 Palo Alto Networks, Inc.

```
external-port 2001 internal-vni 800 external-vni 801 show plugins
vm_series azure gwlb
```

Salida de muestra:

```
GWLB enabled : True Internal Tunnel Port: 2000 Internal Tunnel VNI:
 800 External Tunnel Port: 2001 External Tunnel VNI: 801
```

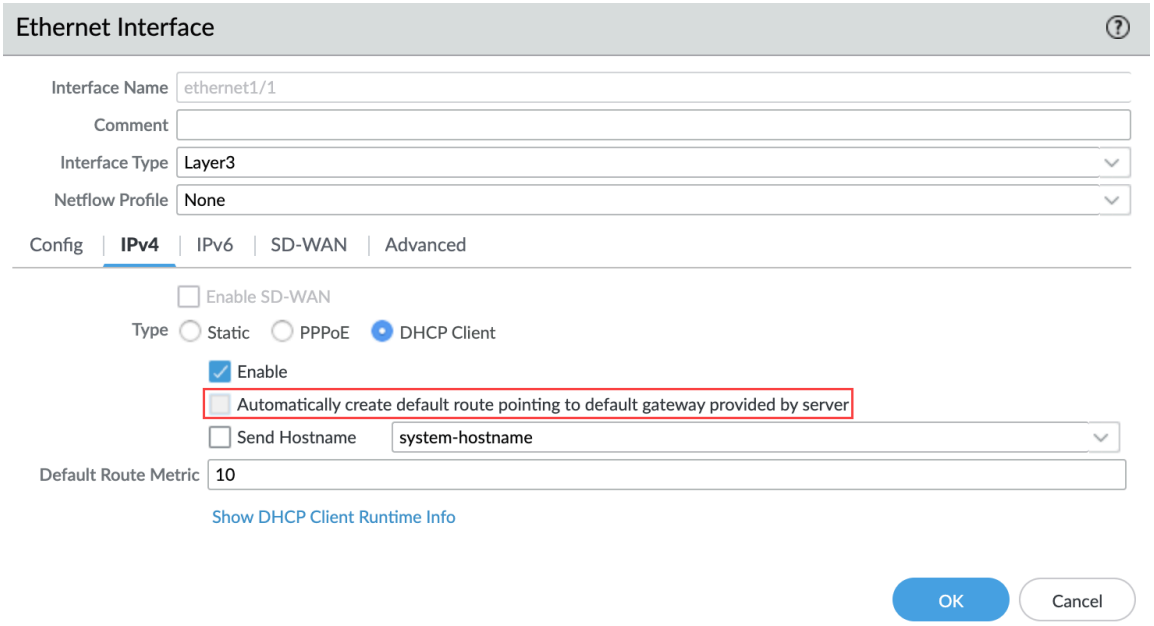
(Configuración de arranque manual) Si no arrancó el cortafuegos VM-Series con GWLB en el Paso 1 o en los Pasos 2.1 a 2.7, realice los siguientes procesos manuales.

1. Configure manualmente las interfaces de red del plano de datos como interfaces de capa 3 en el cortafuegos.
   1. En la interfaz web del cortafuegos VM-Series, seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
   2. Haga clic en **ethernet 1/1** y configúrelo del siguiente modo:
      - Establezca**Interface Type (Tipo de interfaz)** en **Layer3 (Capa 3)** (predeterminado).
      - En la pestaña **Config (Configuración)**, asigne la interfaz a un enrutador virtual

        .
      - También en la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. Defina una zona interna y externa, luego haga clic en **On (Aceptar)**.
      - En la pestaña **IPv4**, seleccione **DHCP Client (Cliente DHCP)**.
      - Deshabilite **Automatically create default route to default gateway provided by server (Crear automáticamente ruta predeterminada a la puerta de enlace predeterminada**

 ©2024 Palo Alto Networks, Inc.

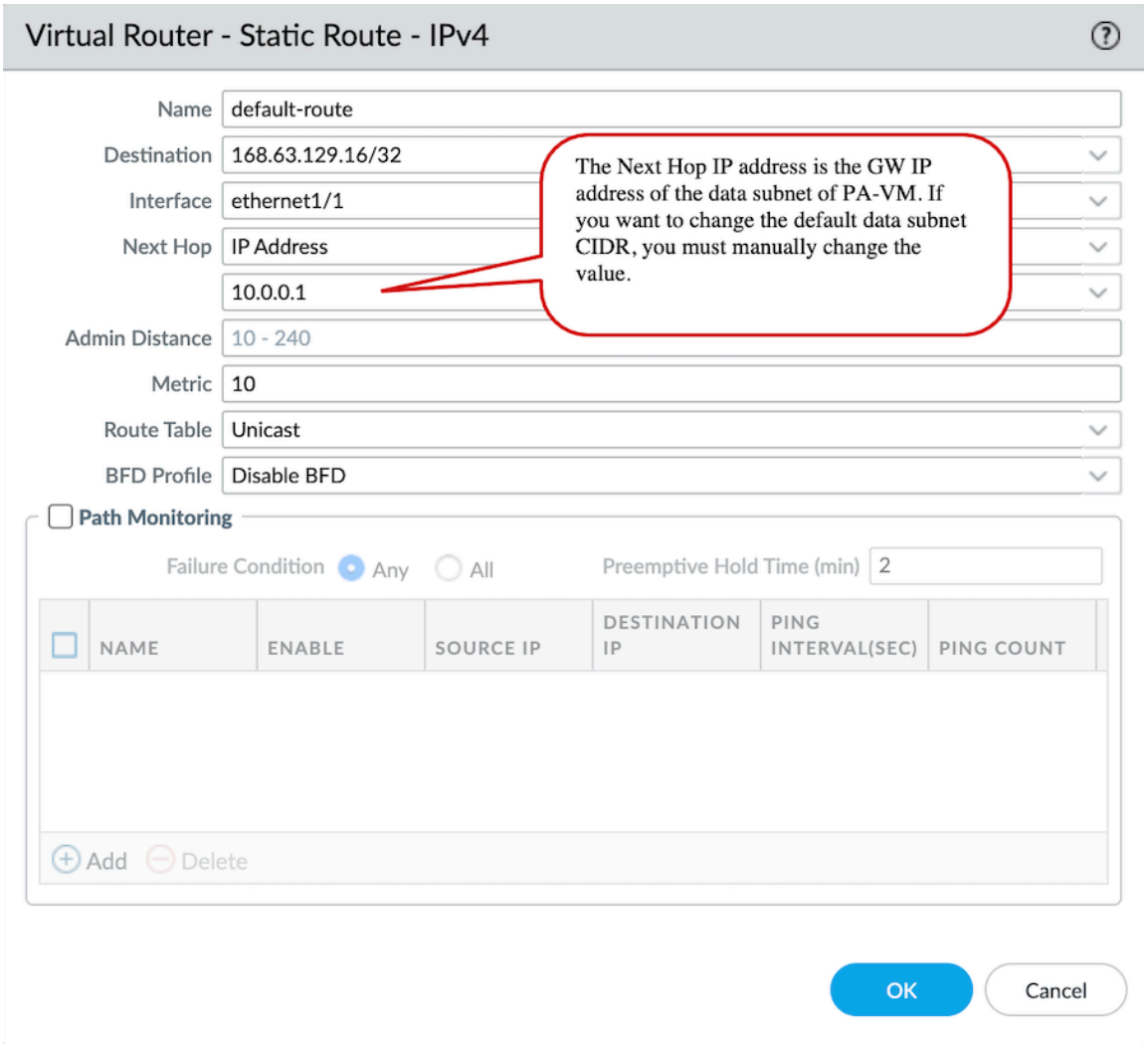
proporcionada por el servidor) para asegurarse de que el tráfico gestionado por esta interfaz no fluya directamente a la puerta de enlace predeterminada en la vNet.



3. En la pestaña **Advanced (Avanzado)**, cree un perfil de gestión para permitir que el cortafuegos reciba verificaciones de estado.
4. Haga clic en **Commit (Confirmar)** para confirmar los cambios y verifique que el enlace para la interfaz esté en estado activo.

2. Cree una ruta estática en el cortafuegos VM-Series.
   1. En la interfaz web del cortafuegos VM-Series, seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual asociado con la interfaz de datos.
   2. Seleccione **Static Routes (Rutas estáticas)** y haga clic en **Add (Añadir)**.
   3. Configure la ruta estática.

 ©2024 Palo Alto Networks, Inc.

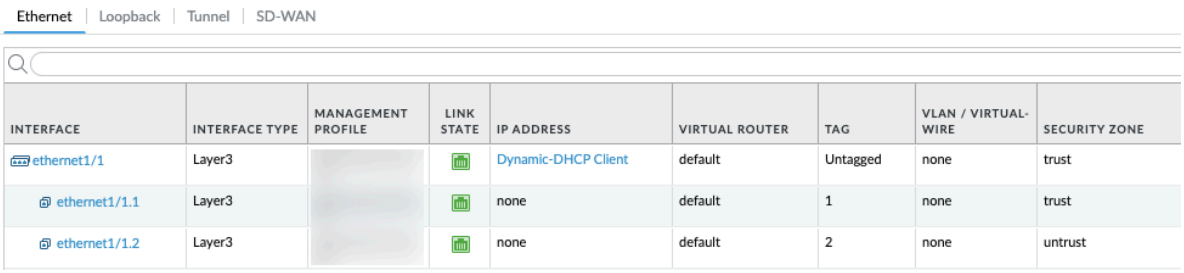


 ©2024 Palo Alto Networks, Inc.

4. Haga clic en **OK (Aceptar)**.
5. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

3. Cree dos subinterfaces en eth1/1 para aplicar políticas de seguridad basadas en zonas.
   1. En la interfaz web del cortafuegos VM-Series, seleccione **Network (Red)** > **Interface (Interfaz)**.
   2. Resalte **ethernet1/1** y haga clic en **Add Subinterface (Añadir subinterfaz)**.
   3. Introduzca un sufijo numérico (1 a 9999) para identificar la subinterfaz.
   4. Introduzca una **VLAN Tag (etiqueta VLAN)** para la subinterfaz. Este campo es obligatorio pero no se utiliza la VLAN.

      El ID/puerto de VNI para el túnel interno se asigna a la etiqueta VLAN 1 y el túnel externo se asigna a la etiqueta VLAN 2. La etiqueta VLAN 1 y la etiqueta VLAN 2 siempre deben asignarse a la zona interna (de confianza) y a la zona externa (no fiable) respectivamente.
   5. Seleccione el **Virtual Router (Enrutador virtual)** asociado a la interfaz de datos.
   6. Seleccione una **Security Zone (Zona de seguridad)**.
   7. En la pestaña **IPv4**, defina el **Type (Tipo)** en **DHCP Client (Cliente DHCP)**.
   8. Haga clic en **OK (Aceptar)**.
   9. Repita este comando para la segunda subinterfaz.
   10. **Commit (Confirmar)** para confirmar los cambios.



 ©2024 Palo Alto Networks, Inc.

Creación de una imagen personalizada de VM-Series para Azure

Puede crear una imagen del cortafuegos VM-Series personalizada para usarla más adelante en su implementación de Azure. Una imagen personalizada le ofrece la flexibilidad y la coherencia para implementar el cortafuegos VM-Series con la versión de PAN-OS que desea usar en lugar de estar restringido a usar solo una imagen disponible a través del marketplace de Azure. Además, su imagen personalizada puede incluir el contenido más reciente y las actualizaciones de antivirus.

La creación de una imagen personalizada requiere que elimine todos los datos privados, configuración de usuario, usuarios, configuración de complementos, etc., antes de crear el VHD. Además, complete el siguiente procedimiento para preparar y crear una imagen personalizada.

Si el cortafuegos VM-Series utilizado para crear su imagen personalizada se implementó con un tipo de disco premium, cualquier cortafuegos VM-Series implementado con la imagen personalizada debe implementarse con el mismo tipo de disco premium. Sin embargo, si crea una imagen usando un cortafuegos implementado con un tipo de disco estándar, puede implementar el cortafuegos usando un tipo de disco estándar o premium.

STEP 1 | Inicie sesión en Azure.

STEP 2 | Implementación del cortafuegos VM-Series desde Azure Marketplace.

STEP 3 | (Solo licencia BYOL) Active su licencia.

STEP 4 | Actualización del cortafuegos VM-Series a PAN-OS 10.0.3. La actualización a PAN-OS 10.0.3 también actualiza el complemento de VM-Series a 2.0.3.

STEP 5 | Acceda a la interfaz de línea de comandos del cortafuegos VM-Series a través de SSH con el nombre de usuario y la contraseña proporcionados en la plantilla de Azure Marketplace.

STEP 6 | Verifique que su cortafuegos VM-Series tenga las versiones correctas de PAN-OS, complemento de VM-Series, contenido y antivirus.

```
show system info
```

Si está utilizando PAN-OS 10.1, asegúrese de actualizar el complemento VM-Series a la versión 2.1.7 o superior y, si está utilizando PAN-OS 10.2.0, asegúrese de que está utilizando el complemento VM-Series a 3.0.3 o superior.

STEP 7 | (Solo licencia BYOL) Desactive su licencia.

STEP 8 | Realice un restablecimiento de datos privados en el cortafuegos VM-Series. Este comando requiere que el cortafuegos se reinicie. Debe esperar a que el cortafuegos VM-Series se reinicie por completo antes de continuar; el reinicio puede tardar de cinco a siete minutos.

```
solicitud de restablecimiento de datos privados del sistema
```

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Cree una nueva imagen VHD a partir de la instancia de VM-Series.

1. Inicie sesión en la CLI de Azure.
2. Compruebe que esté utilizando la suscripción correcta.

   ```
   az account set --subscription <subscription-id>
   ```

3. Ejecute los siguientes comandos para generalizar la máquina virtual, lo que le permitirá crear imágenes para varias implementaciones y crear el nuevo VHD.

   ```
   az vm deallocate --resource-group <myResourceGroup> --name
   <myVM>
   ```

   ```
   az vm generalize --resource-group <myResourceGroup> --name
   <myVM>
   ```

   ```
   az image create --resource-group <myResourceGroup> --name
   <myImage> --source <resource-id-of-VM>
   ```

STEP 10 | Cree un nuevo cortafuegos VM-Series a partir de su imagen personalizada.

```
az vm create --resource-group <myResourceGroup> --name <myNewVM>
--image <myImage> --admin-username <newUser> --admin-password
<newPassword> --plan-name byol --plan-product vmseries-flex --plan-
publisher paloaltonetworks --size Standard_DS2_v2
```

STEP 11 | Después de implementar un cortafuegos VM-Series con su imagen personalizada, compruebe su implementación.

1. Debe iniciar sesión en el cortafuegos con las credenciales proporcionadas al abrir la máquina virtual desde la imagen personalizada.
2. Después de iniciar sesión correctamente, verifique que su cortafuegos esté ejecutando la versión correcta de PAN-OS y que tiene las versiones de contenido y antivirus correctas.

   ```
   show system info
   ```

STEP 12 | (Opcional) Copie la imagen personalizada en otra región.

```
az image copy –source-resource-group <source-rg> –source-object-name
<pa-vm-image-name> –target-location <target-region> –target-resource-
group <destination-rg>
```

 ©2024 Palo Alto Networks, Inc.

Uso de las recomendaciones del centro de seguridad de Azure para proteger sus cargas de trabajo

Microsoft ha puesto en desuso el soporte ofrecido por el Centro de seguridad de Azure*para las soluciones de seguridad de socios y lo ha sustituido con* Azure Sentinel.

Cuando implementa nuevas cargas de trabajo en su suscripción a Azure que está habilitada para el centro de seguridad de Azure, el centro de seguridad de Azure le permite proteger estas cargas de trabajo de dos maneras. En un flujo de trabajo, el centro de seguridad de Azure le recomienda implementar una nueva instancia del cortafuegos VM-Series para proteger una carga de trabajo de aplicación orientada a internet. En el otro flujo de trabajo, el centro de seguridad de Azure descubre los cortafuegos VM-Series (soluciones de seguridad del socio) que implementó en la suscripción a Azure y debe realizar una configuración adicional para conectar el cortafuegos VM-Series al centro de seguridad de Azure para poder ver alertas en el panel. Consulte Integración del centro de seguridad de Azure para obtener detalles de la integración, y las ventajas y desventajas de cada flujo de trabajo:

- Implementación de un cortafuegos VM-Series basado en una recomendación del centro de seguridad de Azure
- Conexión de un cortafuegos VM-Series existente desde el centro de seguridad de Azure

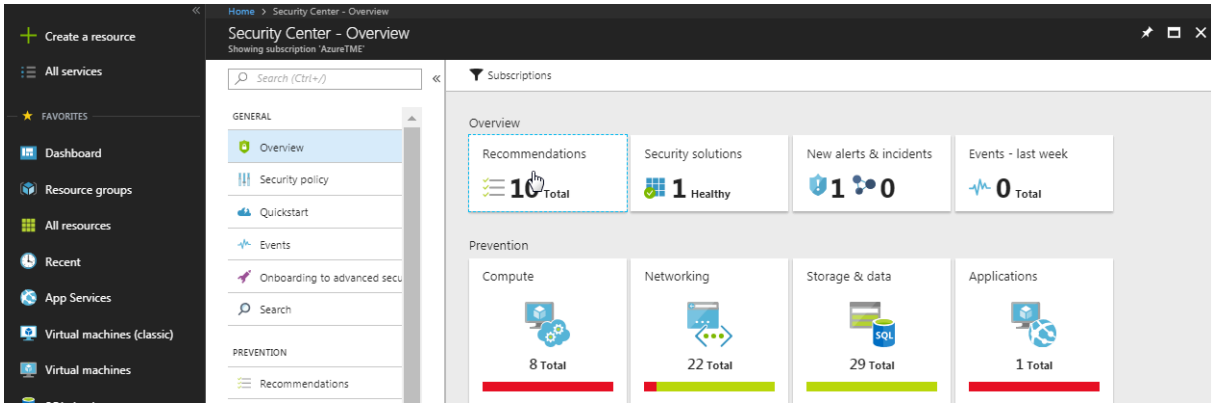
Implementación de un cortafuegos VM-Series basado en una recomendación del centro de seguridad de Azure

El centro de seguridad de Azure escanea sus recursos de Azure y proporciona recomendaciones para proteger las cargas de trabajo que requieren un cortafuegos de última generación. La recomendación se muestra en el panel y puede implementar una nueva instancia del cortafuegos VM-Series de Azure marketplace o puede usar la CLI de Azure, Powershell o una plantilla ARM. La ventaja de una implementación personalizada usando la CLI de Azure, Powershell o una plantilla ARM es que puede implementar el cortafuegos VM-Series en el mismo grupo de recursos que la carga de trabajo que desea proteger. Cuando implementa el cortafuegos VM-Series usando Azure marketplace, Azure requiere que implemente el cortafuegos en un nuevo grupo de recursos o solo en un grupo de recursos vacío. Por lo tanto, la implementación de Marketplace requiere que garantice que el tráfico desde la carga de trabajo que desea proteger se dirija al cortafuegos en un grupo de recursos diferente.

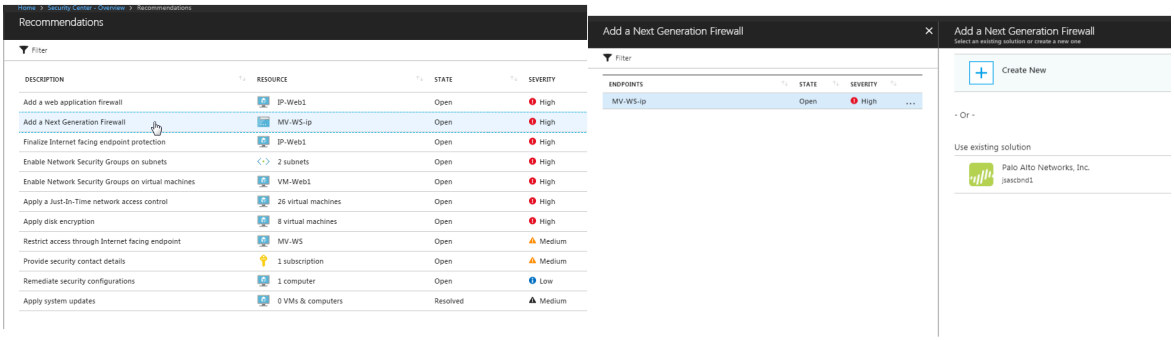
STEP 1 | Inicie sesión en su portal de Azure y acceda al panel del centro de seguridad.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Seleccione **Recommendations (Recomendaciones)**.



STEP 3 | Seleccione **Add a Next Generation Firewall (Añadir un cortafuegos de última generación)** y seleccione la carga de trabajo que desea proteger.



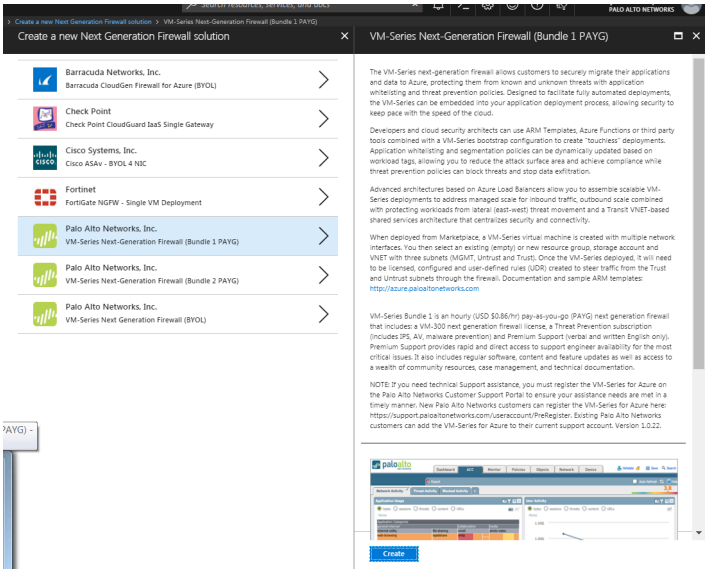
STEP 4 | Elija si desea implementar una nueva instancia del cortafuegos VM-Series o usar una instancia existente del cortafuegos VM-Series.

Para usar este flujo de trabajo, monte una carga de trabajo con una dirección IP pública expuesta a internet e implemente una instancia del cortafuegos VM-Series en un nuevo grupo de recursos. A

 ©2024 Palo Alto Networks, Inc.

continuación, elimine la carga de trabajo que montó e implemente las cargas de trabajo de producción en el grupo de recursos en el que implementó el cortafuegos VM-Series.

- Para **Create New (Crear nuevo)**, consulte Implementación del cortafuegos VM-Series desde Azure Marketplace (plantilla de soluciones).
- Para **Use existing solution (Usar solución existente)**, seleccione el cortafuegos VM-Series que implementó previamente.



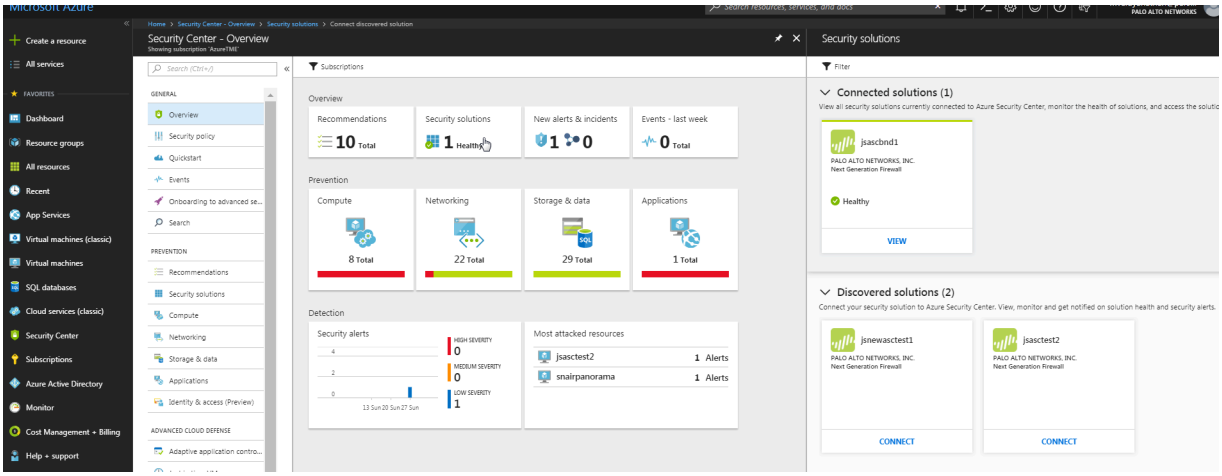
Conexión de un cortafuegos VM-Series existente desde el centro de seguridad de Azure

Cuando el centro de seguridad de Azure detecta que implementó el cortafuegos VM-Series en la suscripción a Azure, muestra el cortafuegos como una solución de seguridad. Entonces, podrá conectar el cortafuegos VM-Series al centro de seguridad usando el formato de evento común (Common Event Format, CEF) en Syslog y ver los logs del cortafuegos como alertas en el panel del centro de seguridad.

STEP 1 | Inicie sesión en su portal de Azure y acceda al panel del centro de seguridad.

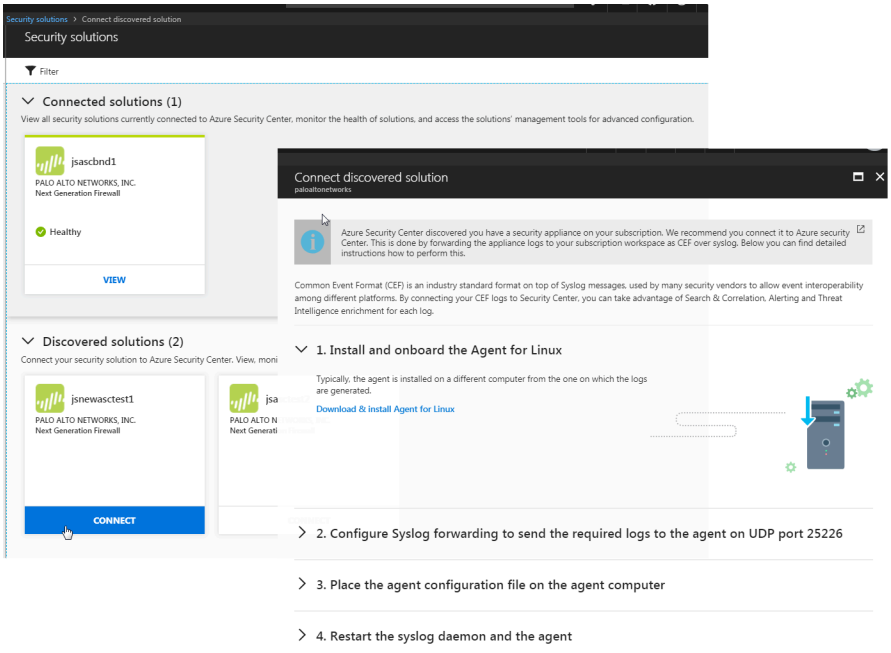
 ©2024 Palo Alto Networks, Inc.

STEP 2 | Seleccione Security Solutions (Soluciones de seguridad) para ver todos los cortafuegos VM-Series disponibles en esta suscripción a Azure.



STEP 3 | Expanda las soluciones que se detectaron y seleccione la instancia del cortafuegos VM-Series en el mismo grupo de recursos que la carga de trabajo que desea proteger y haga clic en **Connect (Conectar)**.

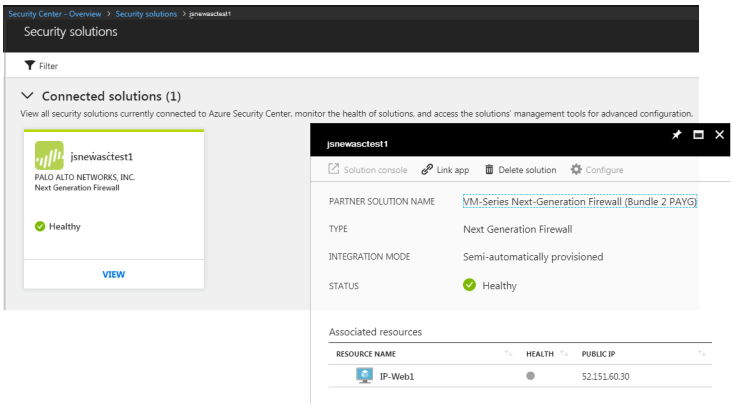
Para ver los logs del cortafuegos como alertas en el panel del centro de seguridad, debe realizar el proceso de cuatro pasos que se muestra en la pantalla.



 ©2024 Palo Alto Networks, Inc.

STEP 4 | Tras conectar correctamente el cortafuegos VM-Series al centro de seguridad, el cortafuegos VM-Series muestra la lista de soluciones conectadas.

Haga clic en View (Ver) para verificar que el cortafuegos proteja la carga de trabajo que desea proteger.



Uso de Panorama para reenviar logs al centro de seguridad de Azure

Si usa Panorama para administrar sus cortafuegos, puede usar plantillas y grupos de dispositivos para reenviar logs del cortafuegos al centro de seguridad de Azure. Con el perfil de reenvío de logs predeterminado del centro de seguridad de Azure, los logs de envío de WildFire y amenazas de gravedad baja, media, alta o crítica generados en el cortafuegos se muestran como alertas de seguridad en el panel del centro de seguridad de Azure. De modo que pueda centrarse y triangular las alertas de manera más eficaz, puede configurar filtros de log detallados a fin de solo reenviar logs de su interés o reenviar únicamente logs de gravedad alta y crítica. También puede conectar de manera selectiva el perfil de reenvío de logs con algunas reglas de política de seguridad de acuerdo con sus necesidades de seguridad y aplicaciones.

Para habilitar la integración del centro de seguridad de Azure de Panorama, use el siguiente flujo de trabajo.

STEP 1 | Añada el cortafuegos como dispositivo gestionado en Panorama.

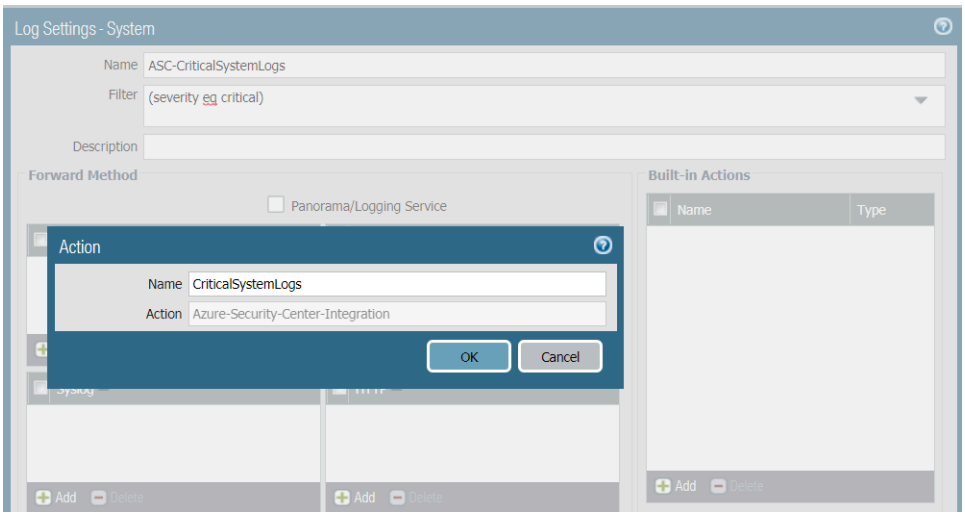
STEP 2 | Desde Panorama, cree una plantilla y un grupo de dispositivos para aplicar la configuración de reenvío de logs en los cortafuegos que reenviarán logs al centro de seguridad de Azure.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Especifique los tipos de logs que se reenviarán al servicio de registro de logs.

La forma en que habilita el reenvío depende del tipo de log. Para los logs generados según una coincidencia de política, use un perfil de reenvío de logs dentro de un grupo de dispositivos, y para los demás tipos de logs, use la configuración de Log Settings (Ajustes de logs) dentro de una plantilla.

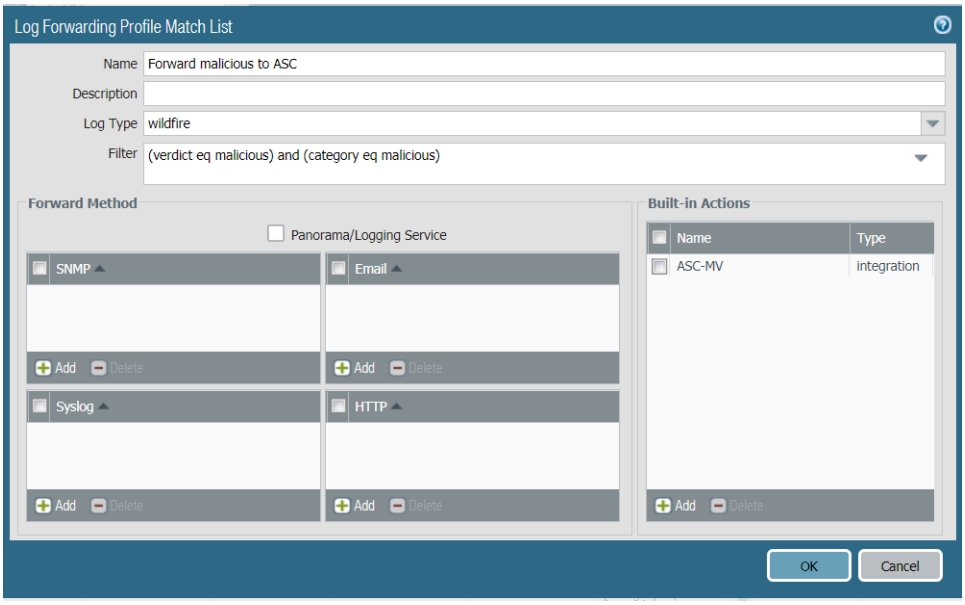
1. Configure el reenvío de logs del sistema, configuración, ID de usuario y coincidencia HIP.
   1. Seleccione **Device (Dispositivo)** > **Log Settings (Configuración de log)**.
   2. Seleccione la **Template (Plantilla)** que contiene los cortafuegos a los que desea reenviar logs al servicio de registro de logs.
   3. Para cada tipo de log que desea reenviar al servicio de registro de logs, haga clic en **Add (Añadir)** para añadir un filtro de lista de coincidencia. Brinde un nombre en **Name (Nombre)** y, opcionalmente defina un **Filter (Filtro)**.
   4. Haga clic en **Add (Añadir)** para añadir acciones integradas e introduzca un nombre en **Name (Nombre)**. La acción de integración del centro de seguridad de Azure se seleccionará automáticamente. Haga clic en **OK (Aceptar)**.



   5. Haga clic en **OK (Aceptar)**.
2. Configure el reenvío de todos los demás tipos de logs que se generan cuando se produce una coincidencia de política como los logs de autenticación, filtrado de datos, filtrado de URL, envío de WildFire, amenaza y tráfico. Para reenviar estos logs, debe crear y adjuntar un perfil de reenvío de logs a cada regla de política para la cual desea reenviar logs.
   1. Seleccione **Device Group (Grupo de dispositivos)** y, luego, **Objects (Objetos)** > **Log Forwarding (Reenvío de logs)** para **Add (Añadir)** un perfil. En la lista de coincidencia del perfil de reenvío de logs, añada cada tipo de log que desea reenviar.

 ©2024 Palo Alto Networks, Inc.

2. Seleccione **Add (Añadir)** para añadir acciones integradas que permitan que los cortafuegos del grupo de dispositivos reenvíen los logs al centro de seguridad de Azure.



3. Cree reglas de política de seguridad básicas en el grupo de dispositivos que acaba de crear y seleccione **Actions (Acciones)** para adjuntar el perfil de reenvío de logs que creó para el reenvío de logs al centro de seguridad de Azure. Hasta que el cortafuegos tenga interfaces y zonas y una política de seguridad básica, no permitirá pasar el tráfico, y solo se registrará el tráfico que coincida con una regla de la política de seguridad (de manera predeterminada).
4. Por cada regla que cree, seleccione **Actions (Acciones)** y seleccione el perfil de reenvío de logs que permite que el cortafuegos reenvíe logs al centro de seguridad de Azure.

STEP 4 | Confirme los cambios en Panorama y aplíquelos en la plantilla y el grupo de dispositivos que creó.

STEP 5 | Verifique que los logs del cortafuegos se reenvían al centro de seguridad de Azure.

1. Inicie sesión en el portal de Azure, seleccione **Azure Security Center (Centro de seguridad de Azure)**.
2. Verifique que puede ver los logs del cortafuegos como alertas de seguridad en el panel del centro de seguridad de Azure.

 ©2024 Palo Alto Networks, Inc.

Implementación del cortafuegos serie VM en Azure Stack

Puede implementar el cortafuegos VM-Series en Azure Stack para proteger el tráfico seguro dentro de la subred entre las aplicaciones en una arquitectura de varios niveles y tráfico saliente desde los servidores en su implementación de Azure Stack. Si desea usar el cortafuegos VM-Series como una puerta de enlace que protege el tráfico entrante destinado a los servidores en su implementación de Azure Stack, debe implementar un dispositivo NAT delante del cortafuegos que recibe tráfico entrante y lo reenvía al cortafuegos. El dispositivo NAT es necesario debido a que Azure Stack no puede asignar una dirección IP pública a una interfaz que no sea principal en una máquina virtual, como el cortafuegos VM-Series.

El cortafuegos VM-Series en Azure Stack no admite el arranque, Azure Application Insights o la integración con el centro de seguridad de Azure.

A diferencia de la nube pública de Azure, no cuenta con una plantilla de soluciones para implementar el cortafuegos VM-Series en Azure Stack. Por lo tanto, debe usar una plantilla ARM para implementar el cortafuegos VM-Series. Para comenzar, puede usar una plantilla ARM de muestra admitida por la comunidad en GitHub y desarrollar su propia plantilla ARM para las implementaciones de producción.

STEP 1 | Descargue elementos de Marketplace de Azure a Azure Stack.

Para implementar un cortafuegos VM-Series en Azure Stack, debe acceder a la oferta BYOL de la imagen de PAN-OS del cortafuegos VM-Series (8.1 o posterior). Puede descargar la imagen directamente de Azure Marketplace a Azure Stack en una implementación conectada.

STEP 2 | Acceda al portal de Azure Stack.

El operador de Azure Stack (un proveedor de servicios o un administrador en su organización) debe proporcionar la URL correcta para acceder al portal.

STEP 3 | Implemente el cortafuegos VM-Series.

Azure Stack no brinda una plantilla de soluciones para el cortafuegos VM-Series. Por lo tanto, debe hacer referencia a la imagen que descargó en el paso anterior en una plantilla ARM para implementar el cortafuegos VM-Series. Para comenzar, puede implementar la plantilla ARM de muestra disponible en GitHub bajo la política admitida por la comunidad:

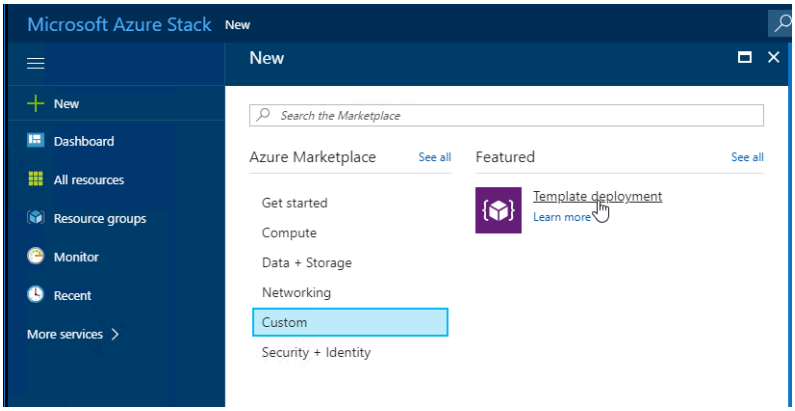
1. Obtenga la plantilla de muestra de Azure Stack en GitHub.
   - Seleccione azurestackdeploy.json para ver el contenido.
   - Haga clic en Raw (Sin formato) y copie el contenido del archivo JSON.
2. Implemente la plantilla de muestra de GitHub.

   Puede implementar el cortafuegos en un grupo de recursos existente que esté vacío o en un nuevo grupo de recursos. La VNet predeterminada en la plantilla es 192.168.0.0/16 e implementa un cortafuegos VM-Series con tres interfaces de red; una interfaz de gestión en la subred 192.168.0.0/24 y dos interfaces del plano de datos en las subredes 192.168.1.0/24 y 192.168.2.0/24. Puede personalizar estas subredes para que se adapten a sus necesidades.

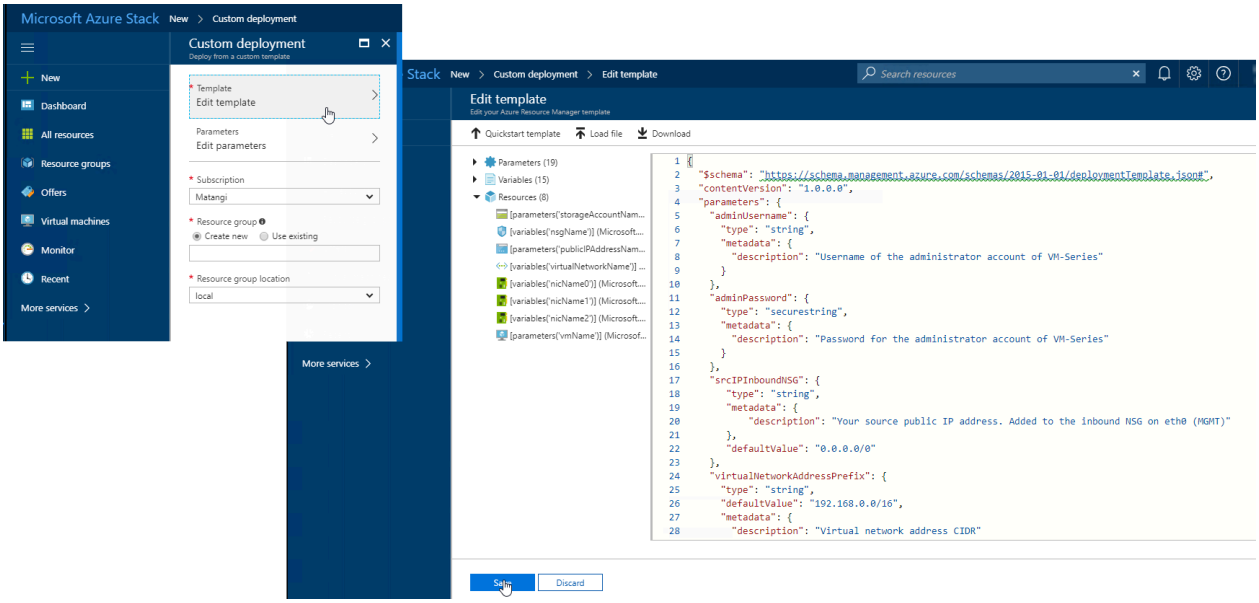
   - Inicie sesión en el portal de Azure Stack.

 ©2024 Palo Alto Networks, Inc.

- Seleccione **New (Nuevo)** > **Custom (Personalizado)** > **Template deployment (Implementación de plantillas)**.

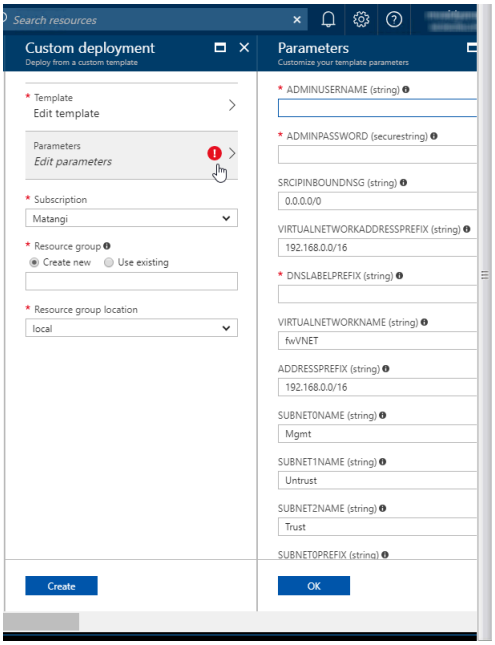


- **Edit template (Editar plantilla)**, elimine todo el contenido existente en la plantilla, pegue el contenido en la plantilla JSON que copió previamente y haga clic en **Save (Guardar)**.

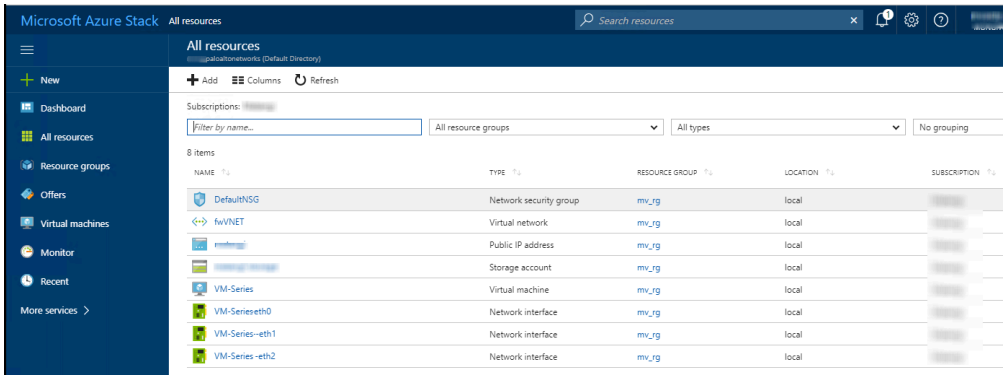


 ©2024 Palo Alto Networks, Inc.

- **Edit parameters (Editar parámetros)**, introduzca los valores de los parámetros requeridos y modifique los valores predefinidos si debe hacerlo. Luego, haga clic en **OK (Aceptar)**.



- Seleccione la **Subscription (Suscripción)** que desea usar y haga clic en **OK (Aceptar)**.
- Seleccione un **Resource Group (Grupo de recursos)** existente que esté vacío o cree uno nuevo y haga clic en **OK (Aceptar)**.
- Haga clic en **Create (Crear)**. Un nueva imagen en el panel muestra el progreso de la implementación de la plantilla.



 ©2024 Palo Alto Networks, Inc.

STEP 4 | Siguientes pasos:

1. Inicie sesión en la interfaz web del cortafuegos.

   Utilizando una configuración segura (https) desde su navegador web, inicie sesión en el nombre de DNS para el cortafuegos. Introduzca el nombre de usuario/contraseña definido anteriormente. Verá una advertencia de certificación; es normal. Vaya a la página web.

2. Active las licencias del cortafuegos VM-Series.

   1. Cree una cuenta de asistencia técnica y Registre el cortafuegos VM-Series (con código de autorización)
   2. En la interfaz web del cortafuegos, seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y seleccione **Activate feature using authentication code (Activar función usando el código de actualización)**.
   3. Introduzca el código de autenticación de capacidad que registró en el portal de asistencia técnica. El cortafuegos se conectará con el servidor de actualización (updates.paloaltonetworks.com), descargará la licencia y se reiniciará automáticamente.
   4. Vuelva a iniciar sesión en la interfaz web del **Dashboard (Panel)** y confirme que se muestra un **Serial# (Número de serie)** válido.

      El **VM Mode (Modo VM)** se muestra como Microsoft Azure.

      Si aparece el término Desconocido, significa que el dispositivo no tiene licencia. Para ver logs de tráfico en el cortafuegos, debe instalar una licencia de capacidad válida.

STEP 5 | #unique_470/unique_470_Connect_42_idd11a757e-7f39-4222-a807-21829428b7a8

 ©2024 Palo Alto Networks, Inc.

Implementación del cortafuegos VM-Series en Azure Stack HCI

Puede implementar el cortafuegos VM-Series en Azure Stack HCI dentro de la arquitectura de red definida por software (SDN). Azure Stack HCI es una solución de clúster de infraestructura hiperconvergente (HCI) que aloja cargas de trabajo virtualizadas de Windows y Linux, y su almacenamiento en un entorno híbrido que combina infraestructura local con servicios en la nube de Azure. Para obtener más información, consulte Descripción general de la solución Azure Stack HCI.

Puede implementar el cortafuegos VM-Series en Azure Stack HCI y proteger el tráfico entrante, el tráfico saliente y el tráfico este-oeste entre varias vNET. El tráfico del cortafuegos VM-Series está anclado a una interfaz activa con una interfaz de gestión fuera de banda, donde las aplicaciones internas y el tráfico entrante se enrutan a través de tablas de rutas para forzar el tráfico a través del balanceador de carga del cortafuegos para el tráfico este-oeste y norte-sur, para proporcionar micro segmentación interna y un perímetro de seguridad. La pasarela SDN permite que el tráfico entre y salga de la SDN interna a través de la vNet del Hub.

Realice los siguientes pasos para implementar el cortafuegos VM-Series en SDN de Azure Stack HCI:

1. Para empezar, necesitará lo siguiente:
   - Uno o más servidores del Catálogo Azure Stack HCI y la suscripción de Azure.
   - Licencias del sistema operativo para sus máquinas virtuales de carga de trabajo, por ejemplo, Windows Server. Consulte Activar las VM de Windows Server.
   - Una conexión a Internet para cada servidor del clúster que puede conectarse a través del tráfico saliente HTTPS a endpoints conocidos de Azure al menos cada 30 días. Consulte Requisitos de conectividad de Azure para obtener más información.
   - Para clústeres extendidos a través de varios sitios:
     - Al menos una conexión de 1 Gb entre sitios (se prefiere una conexión RDMA de 25 GB)
     - Al menos cuatro servidores (dos en cada sitio)
     - Una latencia promedio de 5 ms ida y vuelta entre sitios, si desea realizar una replicación síncrona donde la escritura ocurre simultáneamente en ambos sitios.
   - Para utilizar la infraestructura SDN, necesita un disco duro virtual (VHD) para que el sistema operativo Azure Stack HCI cree máquinas virtuales (VM) de controlador, multiplexor y puerta de enlace de red en la red de gestión (consulte Planificar la implementación de controlador de red, implementar balanceador de carga de software de SDN e Implementación de puerta de enlace de SDN).

   Para obtener más información, consulte Qué necesita para Azure Stack HCI.
2. Cree un clúster de Azure Stack HCI utilizando cualquiera de los métodos siguientes:
   - Con Windows Admin Center. Para obtener más información, consulte Crear un clúster de Azure Stack HCI con Windows Admin Center.
   - Con Windows Powershell. Para obtener más información, consulte Crear un clúster de Azure Stack HCI con Windows PowerShell.
3. Registre el clúster Azure Stack HCI con Azure para supervisar, asistencia técnica, facturación y servicios híbridos.

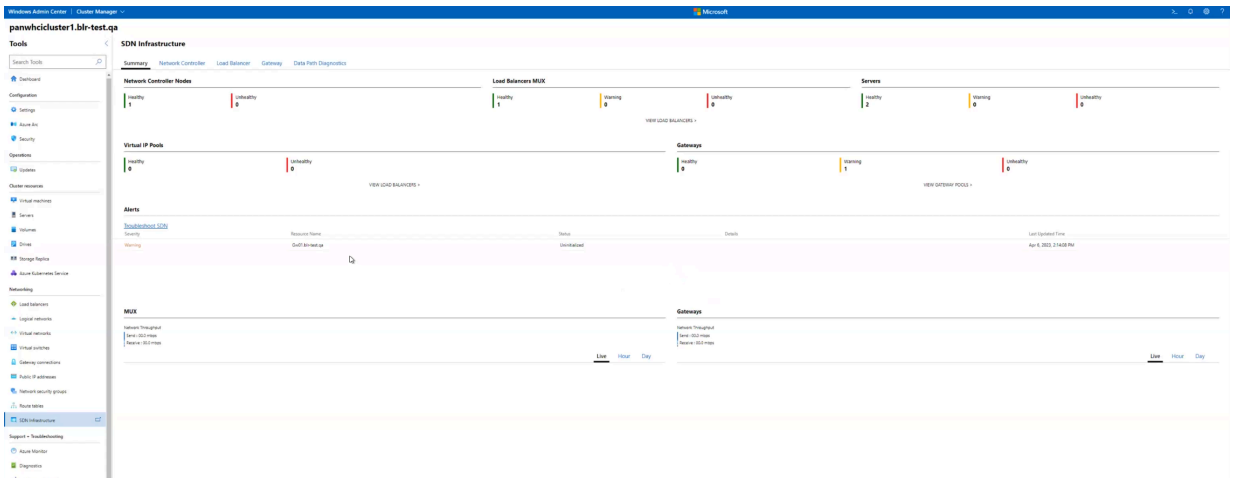
 ©2024 Palo Alto Networks, Inc.

4. Implemente la infraestructura de SDN utilizando cualquiera de los métodos siguientes:
   - Implementación mediante Windows Admin Center
   - Implementación mediante SDN Express
   - Implementación durante la creación de clúster

   Este documento considera la opción de Windows Admin Center para la implementación de cortafuegos VM-Series.

   Después de implementar correctamente la infraestructura SDN, vaya al panel Infraestructura SDN del Windows Admin Center y asegúrese de que todos los nodos del servidor estén en buen estado.

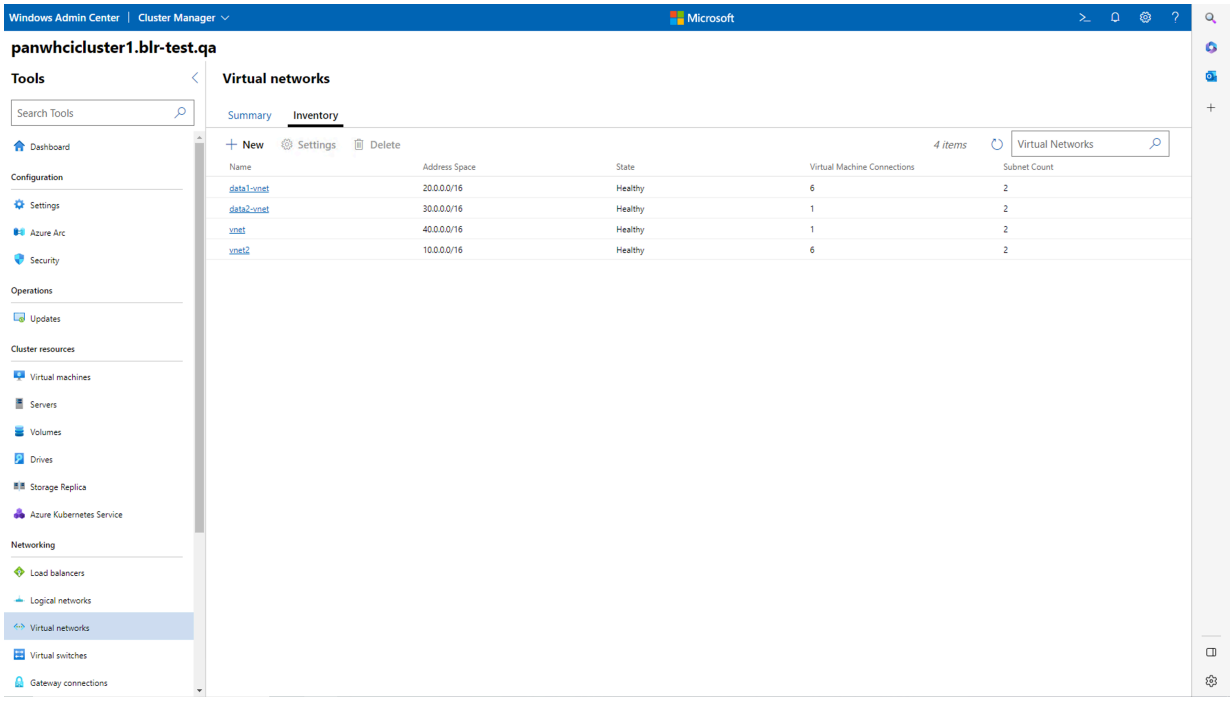
 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

5. Después de implementar la infraestructura SDN, cree una red virtual de virtualización de red Hyper-V (HNV).

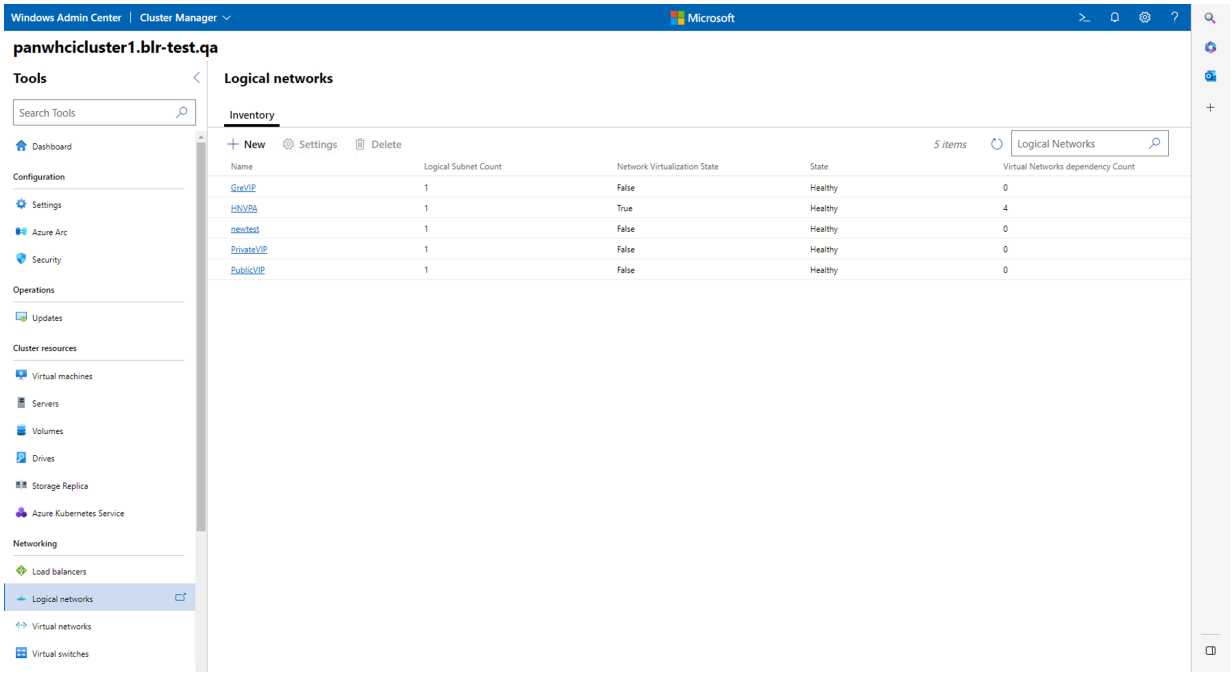
 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

Al modelar una red basada en VLAN como una red lógica SDN, puede aplicar políticas de red a las cargas de trabajo que están adjuntas a estas redes. Para obtener más información, consulte Administración lógica de redes de inquilinos.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

6. Implemente el cortafuegos VM-Series.

   Descargue el archivo VHDX. Registre su cortafuegos VM-Series y obtenga el archivo VHDX.

   - Vaya a https://www.paloaltonetworks.com/services/support.
   - Filtre por **PAN-OS for VM-Series Base Images (PAN-OS para imágenes base de VM-Series)** y descargue el archivo VHDX. Por ejemplo, PA-VM-HPV-7.1.0.vhdx.

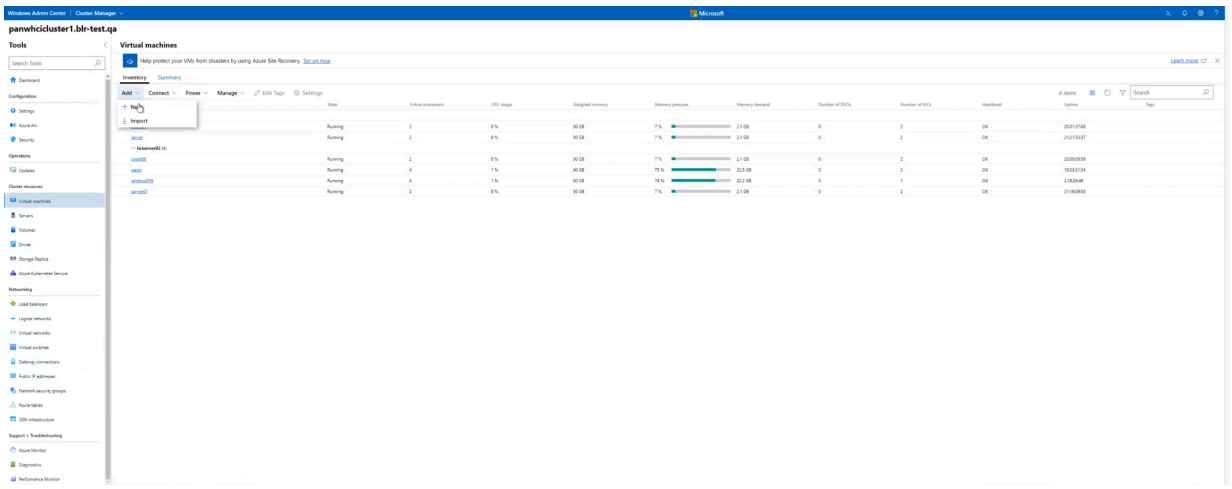
 ©2024 Palo Alto Networks, Inc.

7. Lleve a cabo los siguientes pasos para instalar el cortafuegos VM-Series en Azure Stack HCI:

   Añada una máquina virtual.

   1. Vaya al **Windows Admin Center** > **Gestor de clústeres** y seleccione el clúster.
   2. Vaya a **Virtual Machines (Máquinas virtuales)** > **Add (Añadir)**> **New (Nueva)**.

 ©2024 Palo Alto Networks, Inc.

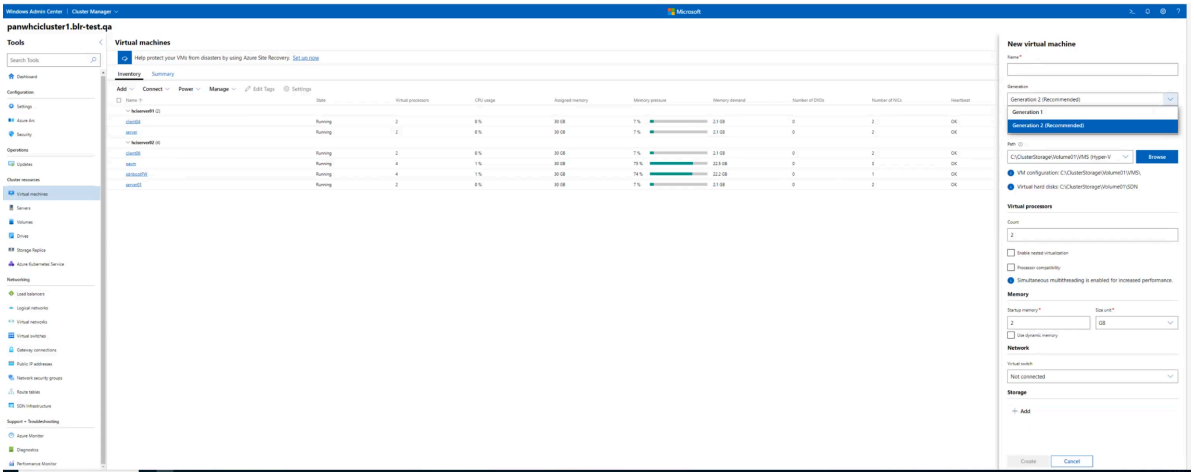


 ©2024 Palo Alto Networks, Inc.

Configure los siguientes ajustes en el asistente de **Nueva máquina virtual**:

- Introduzca el **Nombre** del cortafuegos VM-Series.
- Seleccione Generación 1. Es la opción por defecto y la única versión compatible.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

- Seleccione el **host** y la **ruta** del cortafuegos VM-Series. Examine el archivo de imagen VHD/VHDX FW.

  Nota: Debe almacenar el VHD/VHDX en la ubicación `C:/ClusterStorage/Volúmenes`.
- Para Memoria de inicio, asigne la memoria basada en los Requisitos del sistema VM-Series de su modelo VM-Series.
- Para configurar la conexión en red, en el menú desplegable **Red virtual**, seleccione **vNet**.

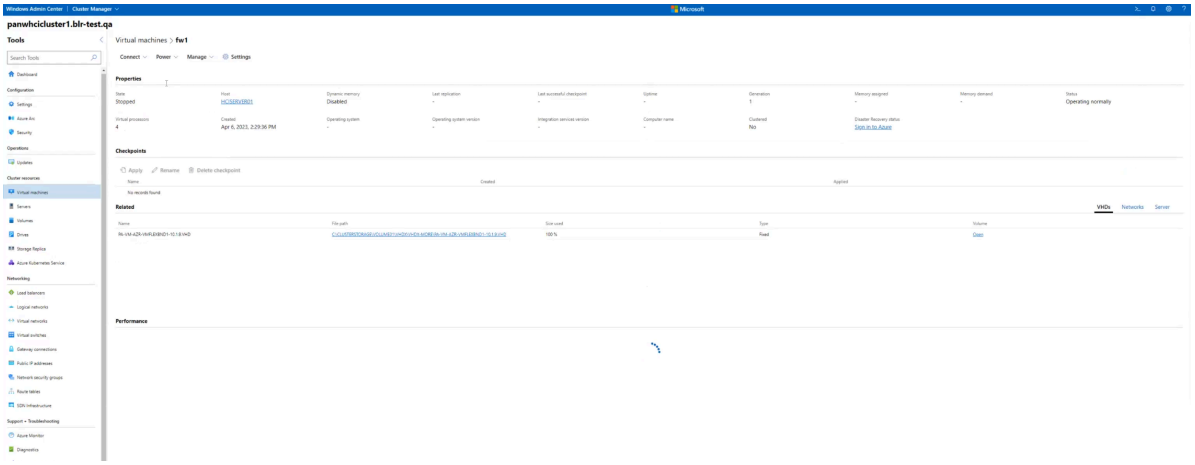
  Se crea un conmutador virtual convergente (vSwitch) mientras aparece el clúster Azure Stack HCI.

  - Seleccione **Conmutador virtual** > **Modo de aislamiento** > **Red virtual** > **Subred virtual**.
  - Haga clic en **Añadir dirección IP** e introduzca la dirección IP de la interfaz de gestión.
  - Seleccione **Grupo de seguridad de red** (opcional).
- Para conectar el Disco duro virtual, seleccione **Usar un disco duro virtual existente** y navegue hasta el archivo VHDX descargado anteriormente en el **Paso 6**.
- Haga clic en **Create (Crear)**.

 ©2024 Palo Alto Networks, Inc.

8. Después de instalar correctamente el cortafuegos VM-Series en el clúster, puede añadir más **Adaptadores de red** para el tráfico de datos. Realice lo siguiente para añadir un **Adaptador de red**:
   - Seleccione su VM, vaya a **Settings (Configuración)** > **Network (Red)**.

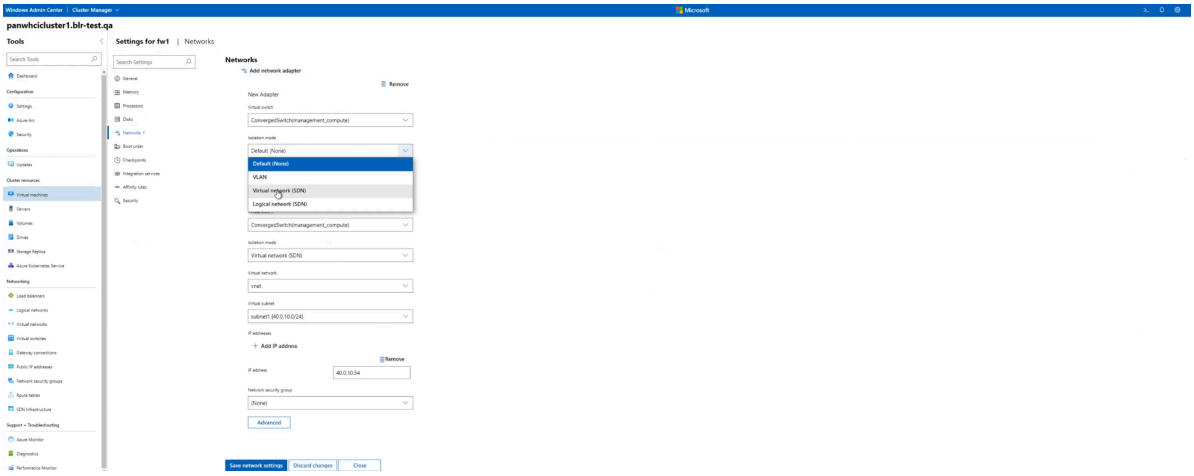
 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

- Haga clic en **Añadir adaptador de red**.

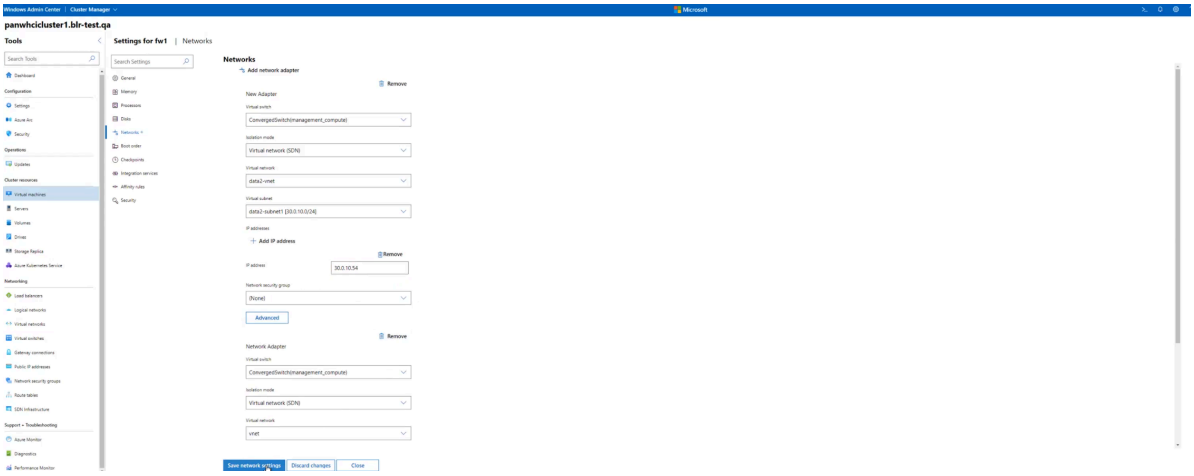
 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

- Seleccione **Conmutador virtual** > **Modo de aislamiento** > **Red virtual** > **Subred virtual**.
- Haga clic en **Añadir dirección IP** e introduzca la dirección IP de la interfaz de datos.
- Seleccione **Grupo de seguridad de red** (opcional).
- Haga clic en **Guardar configuración de red**.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

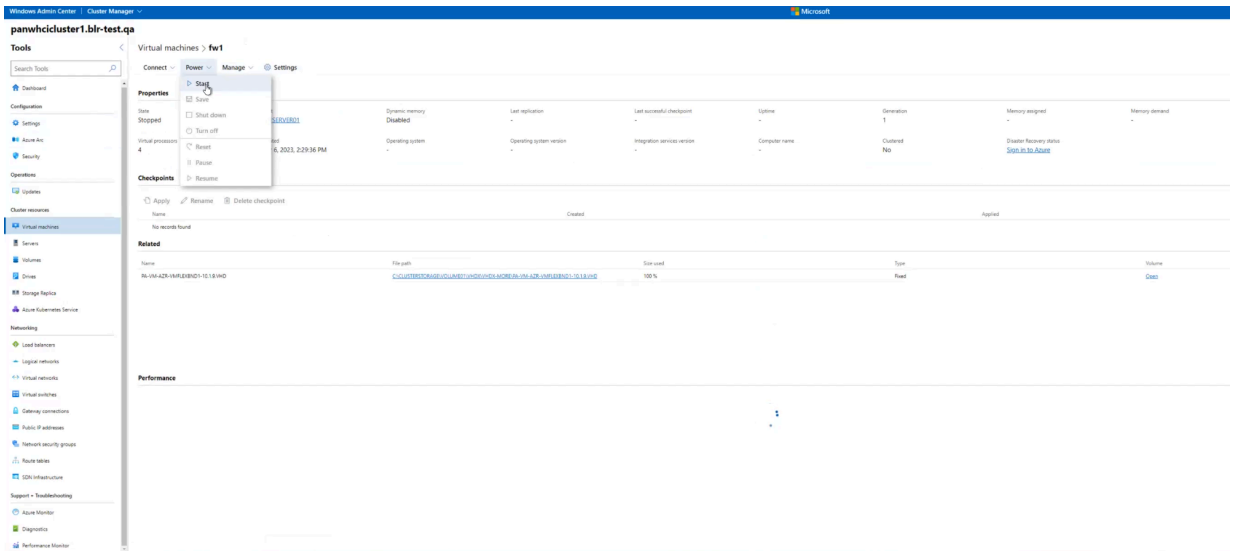
Conecte al menos un adaptador de red para la interfaz de datos en el cortafuegos. Puede crear y añadir más **adaptadores de red** siguiendo los mismos pasos anteriores.

9. (Opcional) Habilite la suplantación de dirección MAC si no está usando la Capa 3 con dirección MAC.
   1. Haga doble clic en el adaptador de red virtual del plano de datos y haga clic en **Ajustes avanzados**.
   2. Haga clic en **Enable MAC address spoofing (Habilitar duplicación de direcciones MAC)** seleccione la casilla y haga clic en **Apply (Aplicar)**.
10. Arranque del cortafuegos VM-Series en Azure Stack HCI.

 ©2024 Palo Alto Networks, Inc.

11. Inicie el cortafuegos.

 ©2024 Palo Alto Networks, Inc.



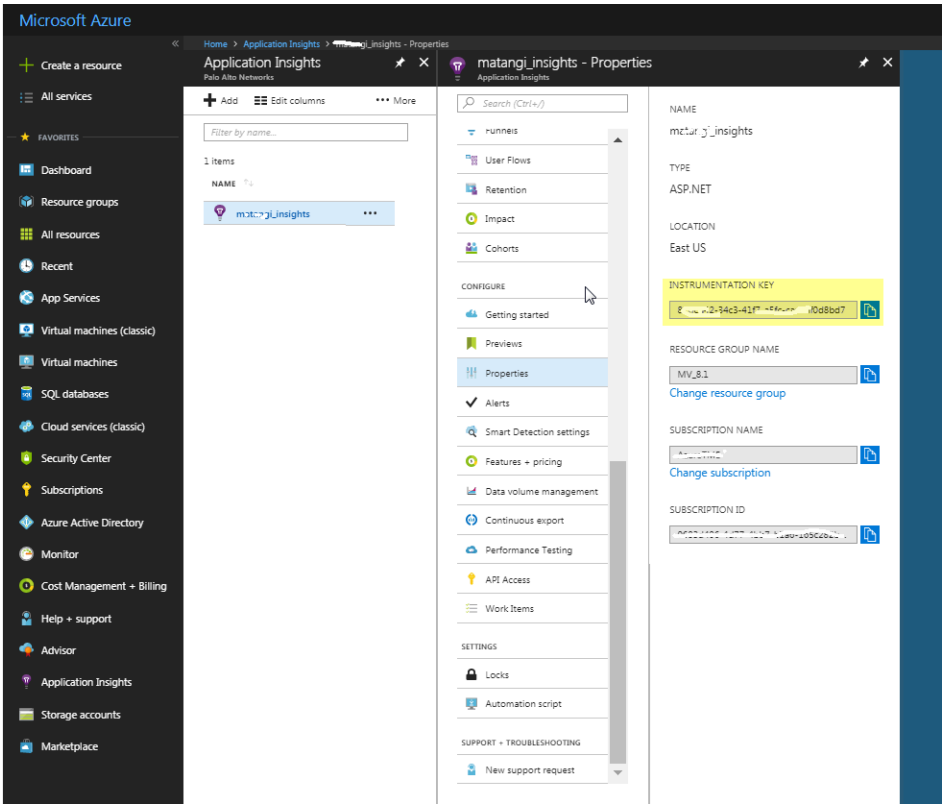
 ©2024 Palo Alto Networks, Inc.

Habilitación de Application Insights de Azure en el cortafuegos VM-Series

El cortafuegos VM-Series en Azure puede publicar métricas PAN-OS personalizas de manera nativa en Azure Application Insights que puede usar para supervisar los cortafuegos directamente desde el portal de Azure. Estas métricas le permiten evaluar el rendimiento y los patrones de uso del cortafuegos que puede usar para configurar alarmas y tomar medidas para automatizar eventos como el inicio o la finalización de instancias de los cortafuegos VM-Series. Consulte Métricas personalizadas de PAN-OS publicadas para la supervisión para obtener una descripción de las métricas que están disponibles.

STEP 1 | En el portal de Azure, cree su instancia de Application Insights para supervisar el cortafuegos y copie la **Instrumentation Key (Clave de instrumentación)** en **Configure (Configurar)** > **Properties (Propiedades)**.

El cortafuegos necesita esta clave para autenticarse en la instancia de Application Insights y publicar las métricas en ella. Consulte VM-Series en permisos de entidad de servicio de Azure para ver los permisos necesarios.

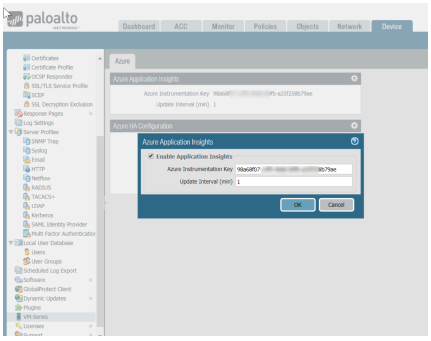


 ©2024 Palo Alto Networks, Inc.

STEP 2 | Permita que el cortafuegos publique métricas en su instancia de Application Insights.

1. Inicie sesión en al cortafuegos VM-Series de Azure.
2. Seleccione **Device (Dispositivo)** > **VM-Series** > **Azure**.
3. Edite **Azure Application Insights** e introduzca la clave de instrumentación que copió anteriormente.

   El intervalo predeterminado para publicar métricas es cinco minutos. Puede cambiarlo para que varíe de 1 a 60 minutos.



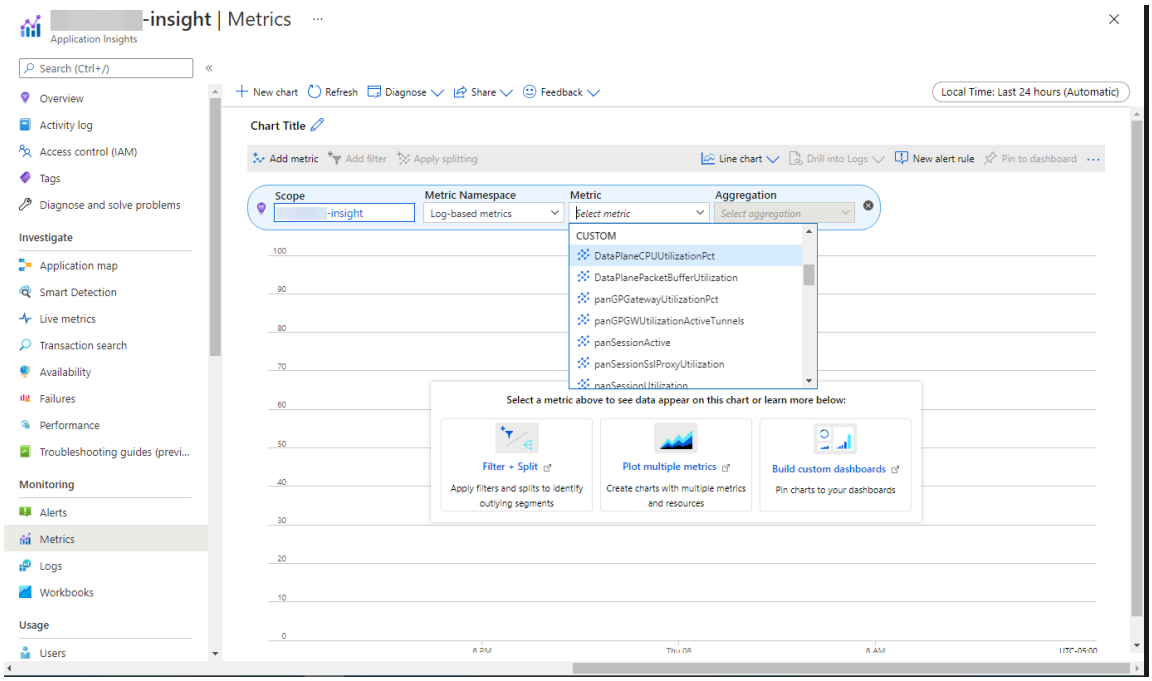
4. Haga clic en **Commit (Confirmar)** para compilar los cambios.

   El cortafuegos genera un log del sistema para registrar si la autenticación en Azure Application Insights se realizó correctamente o si falló.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Verifique que puede ver las métricas en el panel de Azure Application Insights.

1. En el portal de Azure, seleccione la instancia de Application Insights y seleccione **Monitoring (Supervisión)** > **Metrics (Métricas)** para ver las métricas personalizadas de PAN-OS.



2. Seleccione las métricas en las que desea supervisar las tendencias y activar alertas. Consulte la documentación de Microsoft Azure para obtener detalles sobre la exploración de métricas en Application Insights.

Implementación de Application Insights mediante espacio de trabajo

A partir del complemento de Azure 4.2.0, Azure recomienda implementar Application Insights mediante espacios de trabajo y planea finalizar el soporte técnico para Application Insights clásico a partir de febrero de 2024. No es obligatorio migrar Application Insights al espacio de trabajo al actualizar al complemento

 ©2024 Palo Alto Networks, Inc.

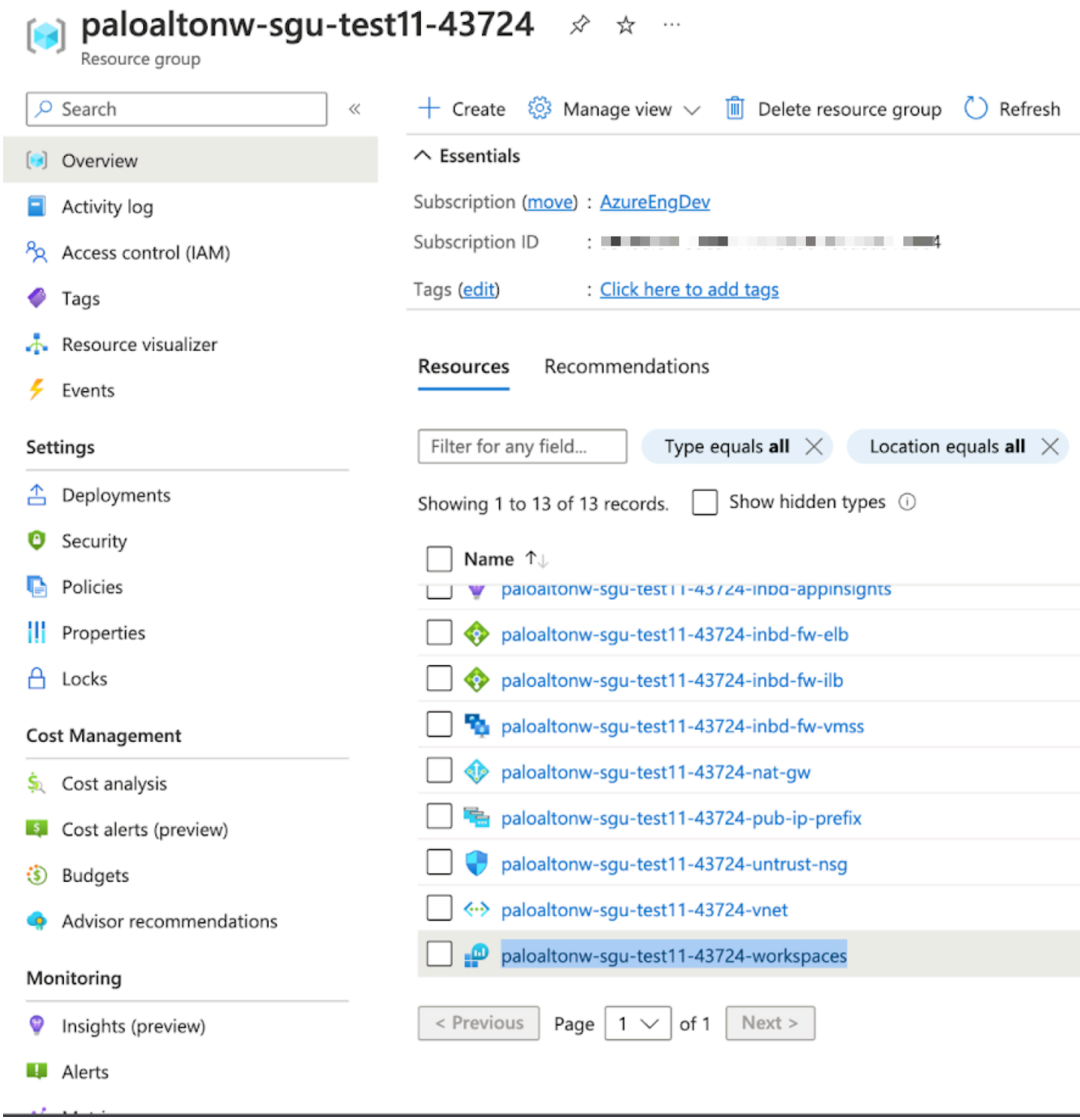
de Azure 4.2.0. Sin embargo, se recomienda, ya que tendrá que migrar Application Insights antes de febrero de 2024.

Consideraciones antes de actualizar al complemento de Azure 4.2.0:

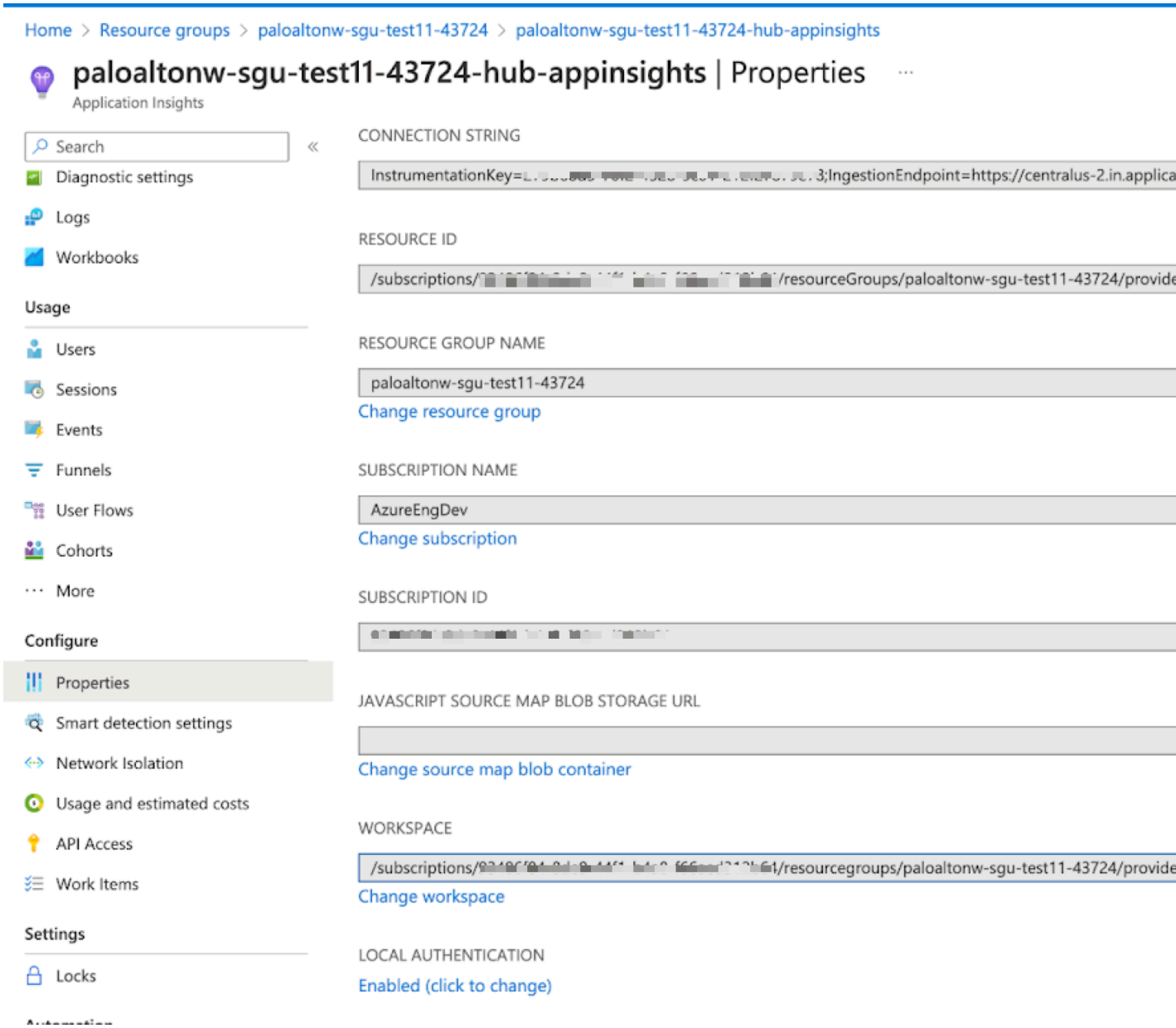
- Se recomienda que migre Application Insights antes de actualizar al complemento de Azure 4.2.0.
- Si no desea migrar ahora, pero desea actualizar el complemento de Azure, entonces:
  - Puede conservar la implementación existente y crear una nueva implementación para abrir el espacio de trabajo de Application Insights. También puede aprovechar la nueva implementación para soluciones de escalado automático.
  - Puede anular la implementación de la implementación existente y volver a implementarla, lo que crearía el espacio de trabajo de Application Insights.
  - Puede volver a implementar una implementación existente, lo que mostrará el espacio de trabajo de Application Insights.

La implementación de Application Insights mediante espacios de trabajo requiere la creación de un grupo de recursos y asociar el espacio de trabajo con él. Se recomienda nombrar su espacio de trabajo como Espacios de trabajo-<resource_group_name>. Si implementa tanto el hub como la pila de entrada, deberá crear dos Application Insights y ambos deben estar asociados al mismo espacio de trabajo.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

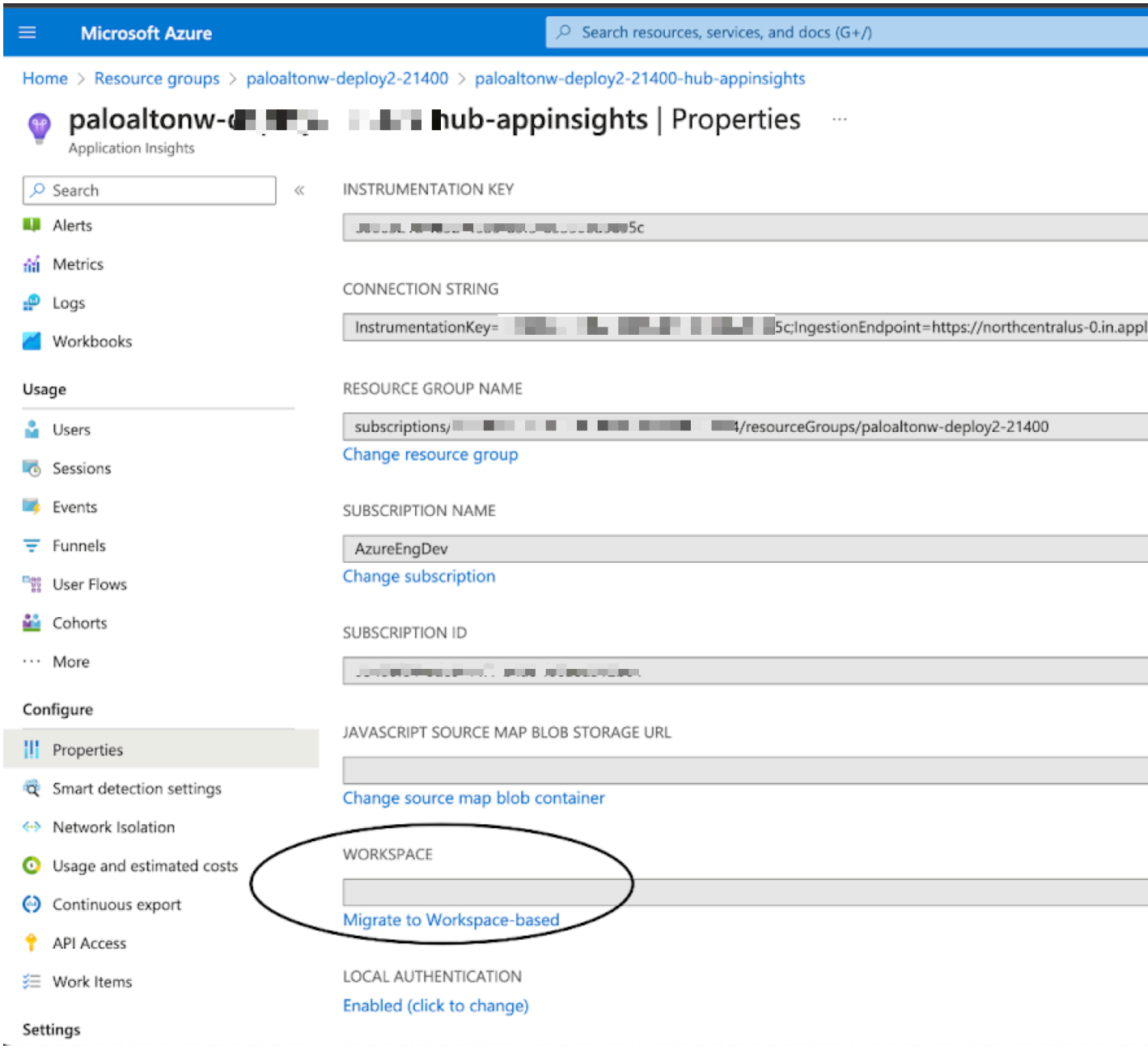


Migración manual de Application Insights

Para **migrar manualmente** su Application Insights existente, deberá comprobar si su Application Insights actual es clásico o de espacio de trabajo. Para comprobar el método de implementación de Application Insights:

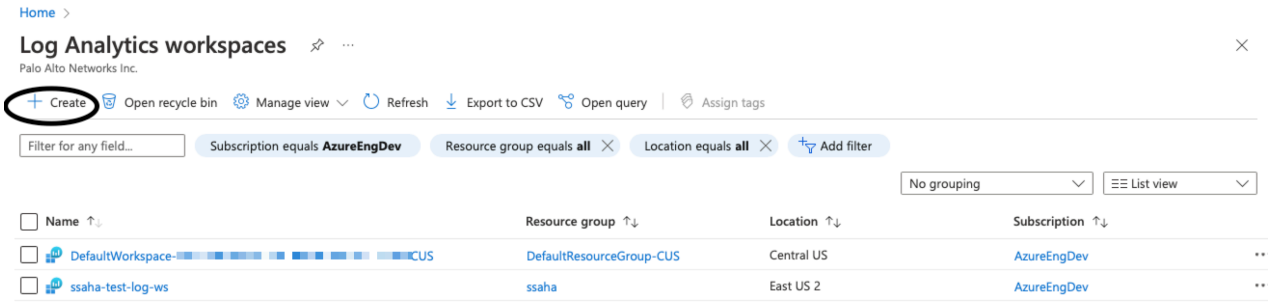
Vaya al Portal de Azure # Grupo de recursos # Application Insights # Propiedades. Si Application Insight es clásico, el valor del campo del espacio de trabajo aparecerá vacío y el enlace **Migrar a un espacio de trabajo**estará disponible.

 ©2024 Palo Alto Networks, Inc.



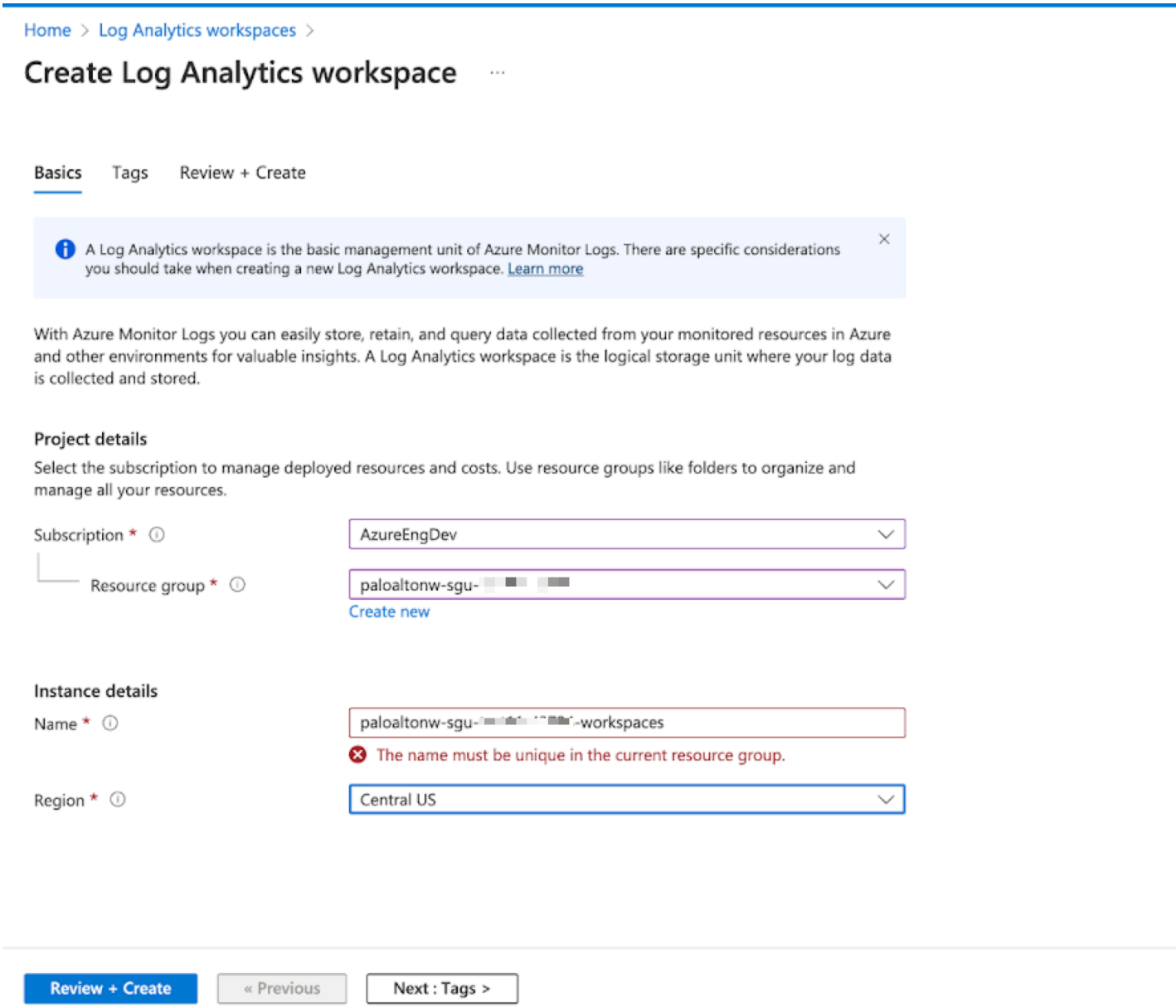
Para migrar Application Insights, busque el espacio de trabajo de Log Analytics en el portal de Azure y haga clic en **Crear** para crear un espacio de trabajo de Log Analytics.

 ©2024 Palo Alto Networks, Inc.



Seleccione la suscripción y el grupo de recursos asociados a la implementación actual. Al asignar un nombre al espacio de trabajo, utilice la convención 'resource_group_name-workspaces'. El espacio de trabajo se puede asociar a Application Insights de la pila de hub o a Application Insights de la pila de entrada. Asegúrese de que la región sea coherente con la región de implementación y haga clic en **Revisar + Crear.**

 ©2024 Palo Alto Networks, Inc.



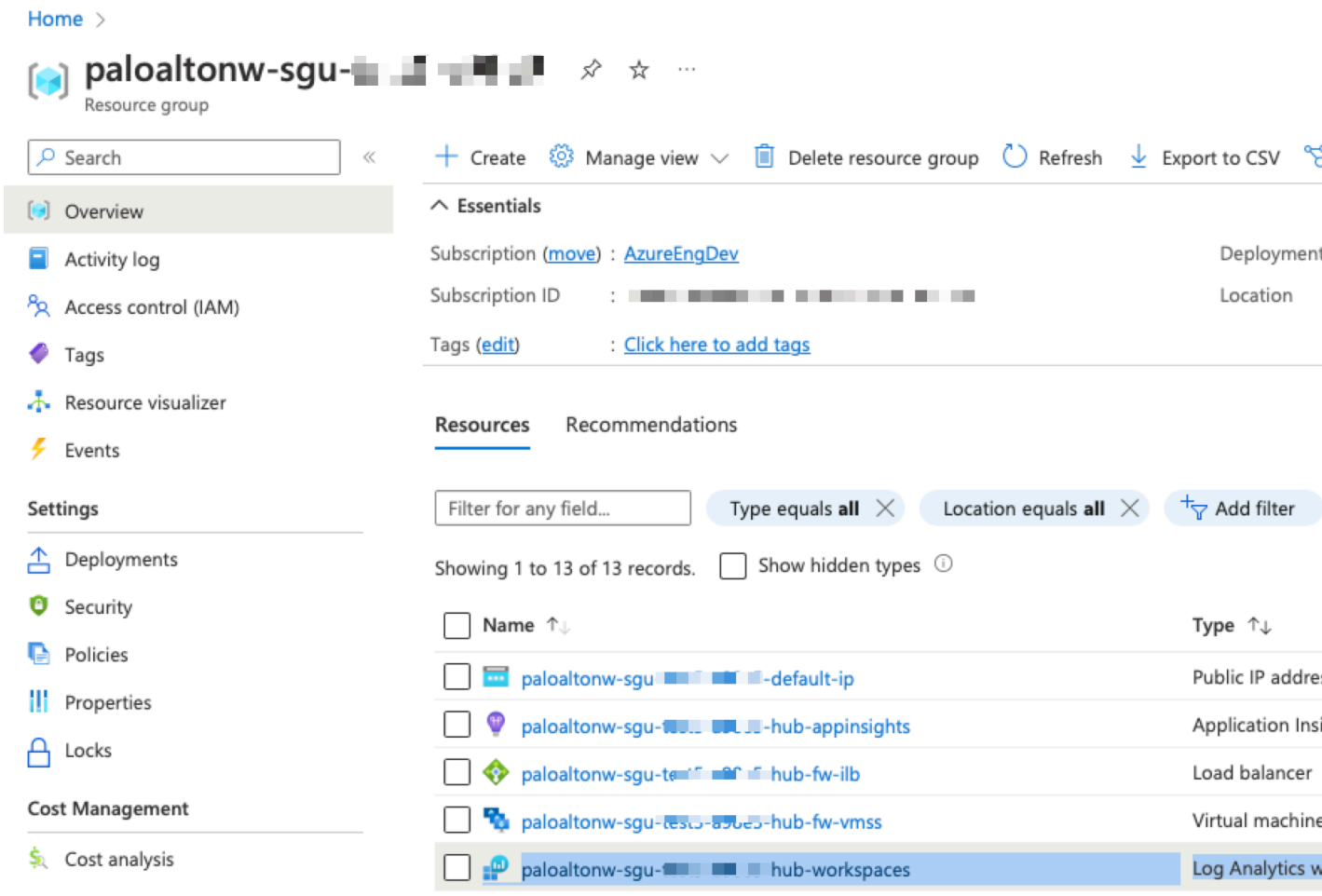
Una vez que el espacio de trabajo se ha creado correctamente, aparece en el grupo de recursos.

Haga clic en el enlace de **Migrar a un espacio de trabajo** en la pestaña Propiedad de Application Insights. Aparece el espacio de trabajo recién creado.

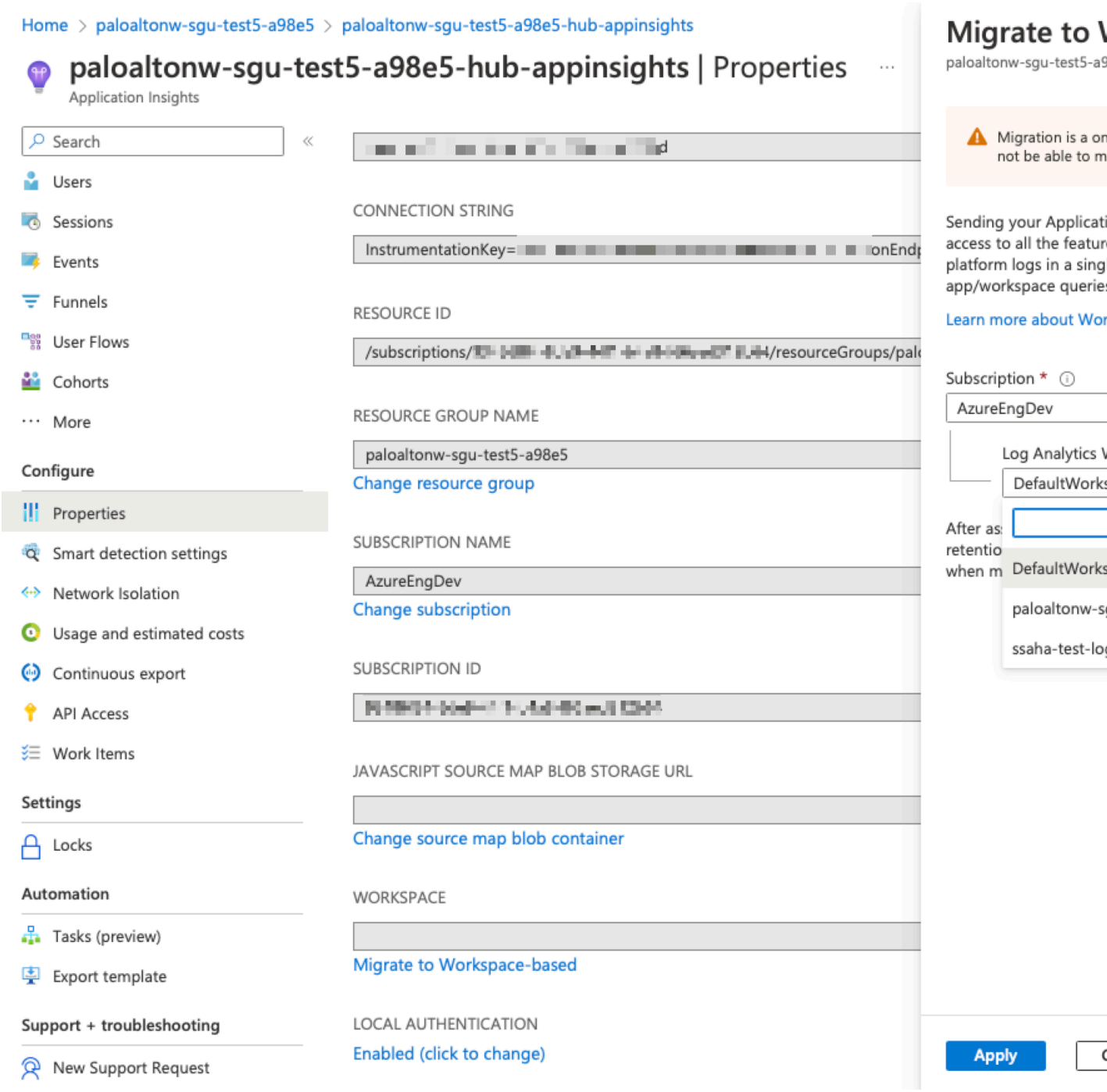
Seleccione el espacio de trabajo y haga clic en **Aplicar**.

Nota: La migración es irreversible y el recurso no se puede revertir a Application Insights clásico una vez migrado.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.



Eliminación de Application Insights

Elimine primero la instancia de Application Insights y, a continuación, elimine el espacio de trabajo junto con otros recursos del grupo de recursos al que está asociada la implementación.

Cambiar a una versión anterior

No se permite el cambio a una versión anterior, ya que deberá implementar Application Insights mediante el método clásico, que no se recomienda.

 ©2024 Palo Alto Networks, Inc.

Supervisión en Azure

La supervisión en Microsoft® Azure® le permite actualizar dinámicamente las reglas de la política de seguridad para aplicar de manera uniforme la política de seguridad en todos los activos implementados dentro de su suscripción a Azure. Para habilitar esta capacidad, debe instalar el Complemento de Panorama para Azure y habilitar la comunicación de API entre Panorama y sus suscripciones de Azure. A continuación, Panorama podrá recopilar la asignación de dirección IP a etiqueta en todos los activos de Azure, y enviar o distribuir la información de los recursos de Azure a sus cortafuegos de Palo Alto Networks®.

- Acerca de la supervisión en Azure
- Configuración del plugin Azure para la supervisión en Panorama
- Atributos supervisados con el plugin Panorama en Azure

Acerca de la supervisión en Azure

A medida que implementa o finaliza máquinas virtuales en la nube pública de Azure, puede usar el complemento de Panorama para Azure para aplicar de manera coherente las reglas de política de seguridad en estas cargas de trabajo.

El plugin de Panorama en Azure se diseña para el escalamiento y le permite supervisar hasta 100 suscripciones de Azure en la nube pública de Azure. Con este plugin, usa Panorama como apoyo para sondear sus suscripciones de etiquetas y distribuye los metadatos (asignación de dirección IP a etiquetas) a varios cortafuegos en un grupo de dispositivos. Debido a que Panorama se comunica con sus suscripciones de Azure para recuperar información de recursos de Azure, puede optimizar el número de llamadas de la API realizadas al entorno de nube. A pesar de que puede definir la política de seguridad localmente en el cortafuegos, el uso de Panorama y el complemento le facilita la centralización de la gestión de la política de seguridad y garantiza políticas coherentes para arquitecturas híbridas y nativas de la nube.

Consulte la información de versión del Complemento de Panorama en la Matriz de compatibilidad.

Configuración del plugin Azure para la supervisión en Panorama

Para encontrar todas las cargas de trabajo que su organización haya implementado en la nube de Azure, debe instalar el complemento de Azure en Panorama y configurar las *definiciones de supervisión* que permiten que Panorama se autentique en sus suscripciones a Azure y recupere información en las cargas de trabajo de Azure. Panorama recupera la dirección IP privada principal de los recursos de Azure y las etiquetas asociadas. Para obtener una lista de los elementos de metadatos que admite Panorama, consulte Atributos supervisados con el complemento de Panorama en Azure.

Después de que Panorama recupere los atributos, para enviar la información de recursos de Panorama a los cortafuegos, debe añadir los cortafuegos (hardware o VM-Series) como dispositivos gestionados en Panorama y agrupar los cortafuegos en uno o más grupos de dispositivos. A continuación, puede especificar los grupos de dispositivos que forman parte del *grupo de notificación*, que es un elemento de configuración en una definición de monitorización, que Panorama usa para registrar la asignación de direcciones IP a etiquetas que recupera de Azure.

Finalmente, para aplicar uniformemente las políticas de seguridad en las cargas de trabajo de Azure, debe configurar los grupos de direcciones dinámicas y hacer referencia a ellos en las reglas de la política que permiten o deniegan el tráfico a las direcciones IP de los recursos de Azure. Para optimizar su

 ©2024 Palo Alto Networks, Inc.

configuración y gestionar las políticas y los objetos centralmente en Panorama, puede definir los grupos de direcciones dinámicas y las reglas de la política de seguridad, y enviarlos a los cortafuegos en lugar de gestionar los grupos de direcciones dinámicas y las reglas de la política de seguridad localmente en cada cortafuegos.

El complemento de Azure supervisa los recursos de Azure en la nube pública de Azure. Azure China o Azure Government no son compatibles.

- Lista de comprobación para planificar la supervisión de VM con el plugin de Azure
- Instalación del complemento de Azure
- Configuración del complemento de Azure para la supervisión

Lista de comprobación para planificar la supervisión con el complemento de Azure

- Configure la aplicación de Active Directory y una entidad de servicio para habilitar el acceso a la API. Para que Panorama interactúe con las API de Azure y recopile información en sus cargas de trabajo, debe crear una entidad de servicio para Azure Active Directory. Esta entidad de servicio tiene los permisos necesarios para autenticarse en Azure AD y acceder a los recursos en su suscripción.

  Para completar la configuración, debe tener permisos para registrar una aplicación con su inquilino de Azure AD y asignar la aplicación a una función en su suscripción. Si no tiene los permisos necesarios, solicite al administrador de Azure AD o de su suscripción que cree una entidad de servicio con un rol de lector de IAM o los permisos personalizados indicados en VM-Series en permisos de entidad de servicio de Azure.
- Asegúrese de que la ID de suscripción sea única en las entidades de servicio. Panorama le permite usar solo una entidad de servicio para supervisar una suscripción a Azure. Puede supervisar hasta 100 suscripciones a Azure con 100 recursos de entidades de servicio. A partir del complemento panorama para Azure versión 3.2.0, puede supervisar hasta 500 suscripciones de Azure. Tome nota de los tiempos de procesamiento descritos en la tabla a continuación.

	Número de suscripciones				
	100	**200**	**300**	**400**	**500**
Utilización de los recursos del sistema	• CPU: 22 % • Memoria: 0,025 / 1024 = 8987 MB	• CPU: 23,8 % • Memoria: 0,025 / 1024 = 8987 MB	• CPU: 31,8 % • Memoria: 0,025 / 1024 = 8987 MB	• CPU: 28,6 % • Memoria: 0,025 / 1024 = 8987 MB	• CPU: 39,2 % • Memoria: 0,025 / 1024 = 8987 MB
Tiempo promedio para procesar todas las definiciones de supervisión	1 hora, 15 minutos	2 horas, 30 minutos	3 horas, 30 minutos	4 horas	5 horas
Tiempo medio de procesamiento	5 minutos	10 minutos	15 minutos	20 minutos	25 minutos

 ©2024 Palo Alto Networks, Inc.

	Número de suscripciones				
	100	200	300	400	500
de actualización de etiqueta					

La información de la tabla anterior se capturó en una instancia con 8 vCPU y 32 GB de memoria.

- Panorama puede enviar hasta 8000 asignaciones de direcciones IP a etiquetas al cortafuegos o sistema virtual asignado a un grupo de dispositivos. Revise los requisitos para Panorama y los cortafuegos gestionados:
  - Requisitos mínimos del sistema (consulte la información del complemento de Panorama en la Matriz de compatibilidad):

    Dispositivo virtual Panorama o dispositivo Panorama basado en hardware que ejecuta Panorama 8.1.3 o posterior, con una licencia de asistencia técnica activa y una licencia de gestión de dispositivos para gestionar los cortafuegos.

    Cortafuegos de última generación con licencia que ejecutan PAN-OS 8.0 o 8.1.
  - Debe añadir los cortafuegos como dispositivos gestionados en Panorama y crear grupos de dispositivos, de modo que pueda configurar Panorama para notificar a estos grupos con la información que recupera. Los grupos de dispositivos pueden incluir cortafuegos serie VM o sistemas virtuales en los cortafuegos del hardware.
  - El número de etiquetas que el complemento de Panorama puede recuperar y registrar es el siguiente:

    En las instancias de Panorama 8.1.3 o posterior que gestiona cortafuegos ejecutando PAN-OS 8.1.3 o inferior, los cortafuegos o sistemas virtuales incluidos dentro de un grupo de dispositivos pueden tener 7.000 direcciones IP con 10 etiquetas cada una, o 6.500 direcciones IP con 15 etiquetas cada una.

    En las instancias de Panorama 8.1.3 o posteriores que gestionan cortafuegos que ejecutan PAN-OS 8.0.x, pueden tener 2500 direcciones IP con 10 etiquetas cada una.
    - Si sus dispositivos Panorama poseen una configuración de alta disponibilidad, debe instalar manualmente la misma versión del complemento de Azure en ambos pares de Panorama.

      Configure el complemento de Azure únicamente en el peer Panorama activo. Después de confirmarlo, la configuración se sincronizará con el par pasivo de Panorama. Solo el par activo de Panorama sondea las suscripciones de Azure que configuró para la supervisión.

Instalación del complemento de Azure

Para comenzar la supervisión en Azure, debe descargar e instalar el complemento de Azure en Panorama. Si tiene una configuración de HA en Panorama, repita el proceso de instalación en cada peer Panorama.

Si instaló un complemento de Panorama, el proceso de instalación (o desinstalación) de otro complemento requiere que Panorama se reinicie para permitirle confirmar los cambios. Por lo tanto, instale complementos adicionales durante una ventana de mantenimiento planificado para permitir un reinicio.

 ©2024 Palo Alto Networks, Inc.

Si tiene un Panorama independiente o dos dispositivos Panorama instalados en un par de alta disponibilidad con varios complementos instalados, es posible que los complementos no reciban información actualizada sobre la etiqueta IP si uno o más de los complementos no están configurados. Esto ocurre porque Panorama no reenviará la información de la etiqueta IP a los complementos no configurados. Además, este problema puede ocurrir si uno o más de los complementos de Panorama no están en el estado Registrado o Correcto (el estado positivo varía según cada complemento). Asegúrese de que sus complementos estén en el estado positivo antes de continuar o ejecutar los comandos que se describen a continuación.

Si encuentra este problema, hay dos soluciones:

- Desinstale el complemento o complementos no configurados. Se recomienda que no instale un complemento que no planifique configurar de inmediato
- Puede utilizar los siguientes comandos para solventar este problema. Ejecute el siguiente comando para cada complemento no configurado en cada instancia de Panorama, para evitar que Panorama espere para enviar actualizaciones. Si no lo hace, sus cortafuegos pueden perder cierta información de la etiqueta IP.

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

  Puede cancelar este comando ejecutando:

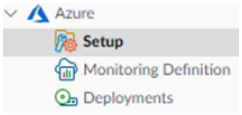
  ```
  request plugins dau plugin-name <plugin-name> unblock-device-push no
  ```

Los comandos descritos no son persistentes en los reinicios y deben usarse de nuevo para cualquier reinicio posterior. Para Panorama en el par de HA, los comandos deben ejecutarse en cada Panorama.

STEP 1 | Inicie sesión en la interfaz web de Panorama, seleccione **Panorama** > **Plugins (Complementos)** y haga clic en **Check Now (Comprobar ahora)** para obtener la lista de complementos disponibles.

STEP 2 | Seleccione **Download (Descargar)** e **Install (Instalar)** para descargar e instalar el complemento.

Después de realizar la instalación correctamente, Panorama se actualiza y el complemento de Azure se muestra en la pestaña **Panorama**.



STEP 3 | Reinicie Panorama.

Seleccione **Panorama** > **Setup (Configuración)** > **Operations (Operaciones)** > **Reboot Panorama (Reiniciar Panorama)**

Configuración del complemento de Azure para la supervisión

Para comenzar a supervisar los recursos en su implementación de nube pública de Azure, después de instalar el complemento de Azure, debe crear una definición de monitorización. Esta definición especifica la entidad de servicio autorizada a acceder a los recursos en la suscripción de Azure que desea supervisar y el grupo de notificación que incluye los cortafuegos a los que Panorama debe enviar todas las asignaciones de dirección IP a etiqueta que recupera. Para aplicar la política, debe crear grupos de direcciones dinámicas y hacer referencia a ellas en la política de seguridad. Los grupos de direcciones dinámicas le permiten filtrar las etiquetas que desea supervisar, de modo que el cortafuegos pueda obtener las direcciones IP

 ©2024 Palo Alto Networks, Inc.

privadas principales registradas para cada etiqueta, y permitir o denegar el acceso al tráfico hacia y desde las cargas de trabajo basado en las reglas de la política que define.

STEP 1 | Inicie sesión en la interfaz web de Panorama.

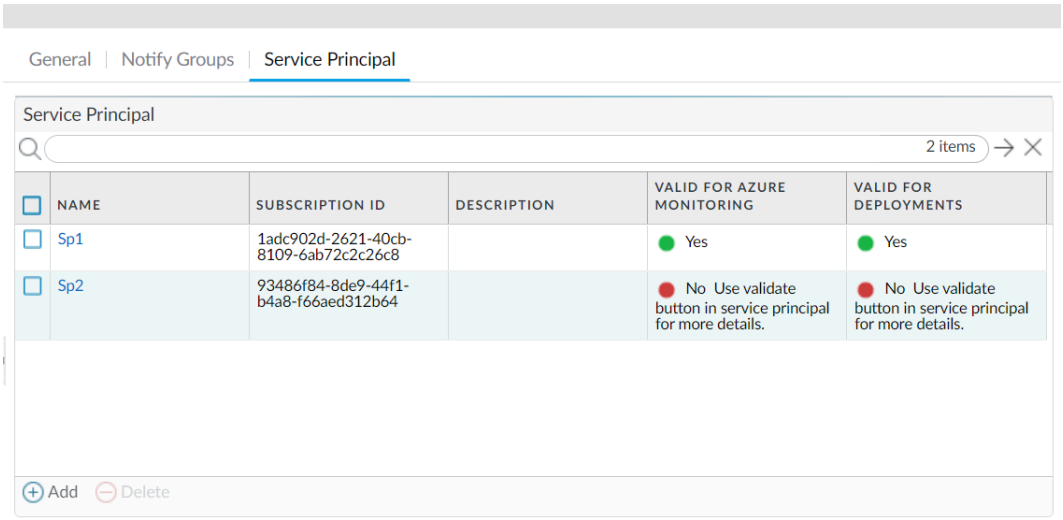
 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configure los siguientes objetos para habilitar la supervisión en Azure.

- Añada una Entidad de servicio.

  La entidad de servicio es la cuenta de servicio que creó en el portal de Azure. Esta cuenta se adjunta a Azure AD y tiene permisos limitados de acceso y supervisión de los recursos en su suscripción a Azure.

  1. Seleccione **Panorama** > **Plugins (Complementos)** > **Azure** > **Setup (Configuración)** > **Service Principal (Entidad de servicio)** > **Add (Añadir)**.

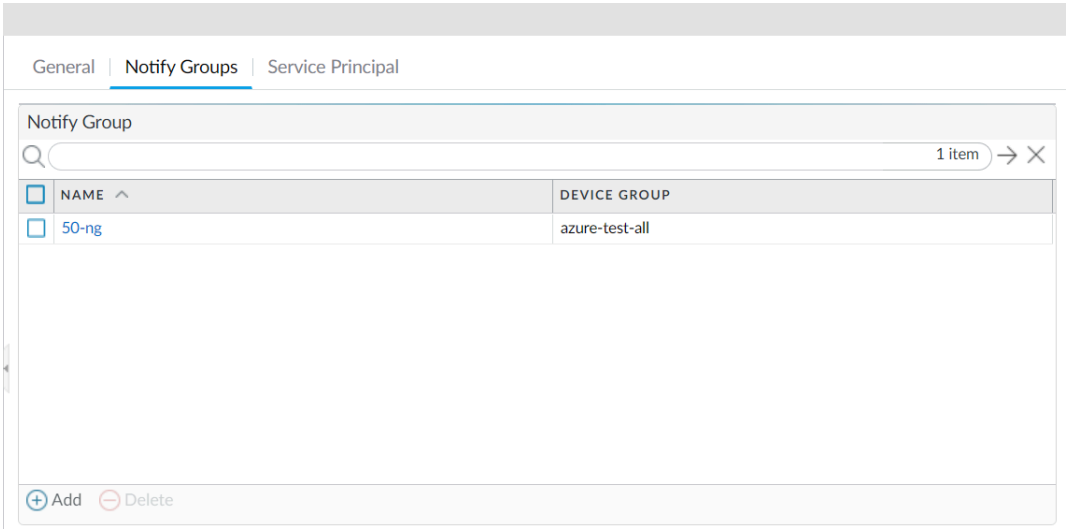


  2. Introduzca un **Name (Nombre)** y, opcionalmente, una **Description (Descripción)** para identificar la cuenta de servicio.
  3. Introduzca la **Subscription ID (ID de suscripción)** para la suscripción de Azure que desea supervisar. Debe iniciar sesión en su portal de Azure para obtener la ID de esta suscripción.
  4. Introduzca el **Client Secret (Secreto del cliente)** y vuelva a introducirla para confirmarlo.
  5. Introduzca la **Tenant ID (ID de inquilino)**. La ID de inquilino es la ID del directorio que guardó cuando configuró la aplicación de Active Directory.
  6. Haga clic en **Validate (Validar)** para comprobar que las claves y las ID que introdujo sean válidas y que Panorama se puede comunicar con la suscripción a Azure usando la API.

- Añadir un grupo de notificación.

  1. Seleccione **Panorama** > **Plugins (Complementos)** > **Azure** > **Setup (Configuración)** > **Notify Groups (Grupos de notificación)** > **Add (Añadir)**.

 ©2024 Palo Alto Networks, Inc.



Al configurar la definición de supervisión, asegúrese de adjuntar el DG principal al grupo de notificación del complemento y de que todos los DG secundarios estén desconectados del grupo de notificación.

Para asegurarse de que la DAU propague todas las etiquetas IP de las DG principales a las DG secundarias que están conectadas al cortafuegos, ejecute el comando debug dau settings device-group recursive yes en la CLI de Panorama

2. Introduzca un **Name (Nombre)** y, opcionalmente, una **Description (Descripción)** para identificar el grupo de cortafuegos al que Panorama envía la información que recupera.
3. Seleccione los **Device Groups (Grupos de dispositivos)**, que son un grupo de cortafuegos o sistemas virtuales, al que Panorama enviará la información (asignación de dirección IP a etiqueta) que recupera de la VPC de Azure. Los cortafuegos usan esta actualización para

 ©2024 Palo Alto Networks, Inc.

determinar la lista de miembros más actual que constituye los grupos de direcciones dinámicas a los que se hace referencia en la política.

4. Seleccione la opción **Seleccionar todas las etiquetas** o **Etiquetas personalizadas**.

   Le permite especificar las etiquetas que prefiere y generar las etiquetas necesarias. Debe introducir la clave de la etiqueta de usuario para configurar las etiquetas de usuario.

   Por ejemplo:

   Si la máquina virtual (VM) en la nube de Azure está etiquetada como **`UserID`**con un valor **`SampleValue,`** introduzca **`UserID`**en las etiquetas de usuario. A continuación, puede ver que **`azure.tag.UserID.SampleValue`** se rellena como la etiqueta de usuario.

   Debe pensar detenidamente sus Grupos de dispositivos porque una Definición de supervisión puede incluir solo un grupo de notificación, asegúrese de seleccionar todos los Grupos de dispositivos relevantes dentro de su grupo de notificación. Si desea eliminar el registro de las etiquetas que Panorama envió a un cortafuegos en un grupo de notificación, debe eliminar la definición de monitorización.

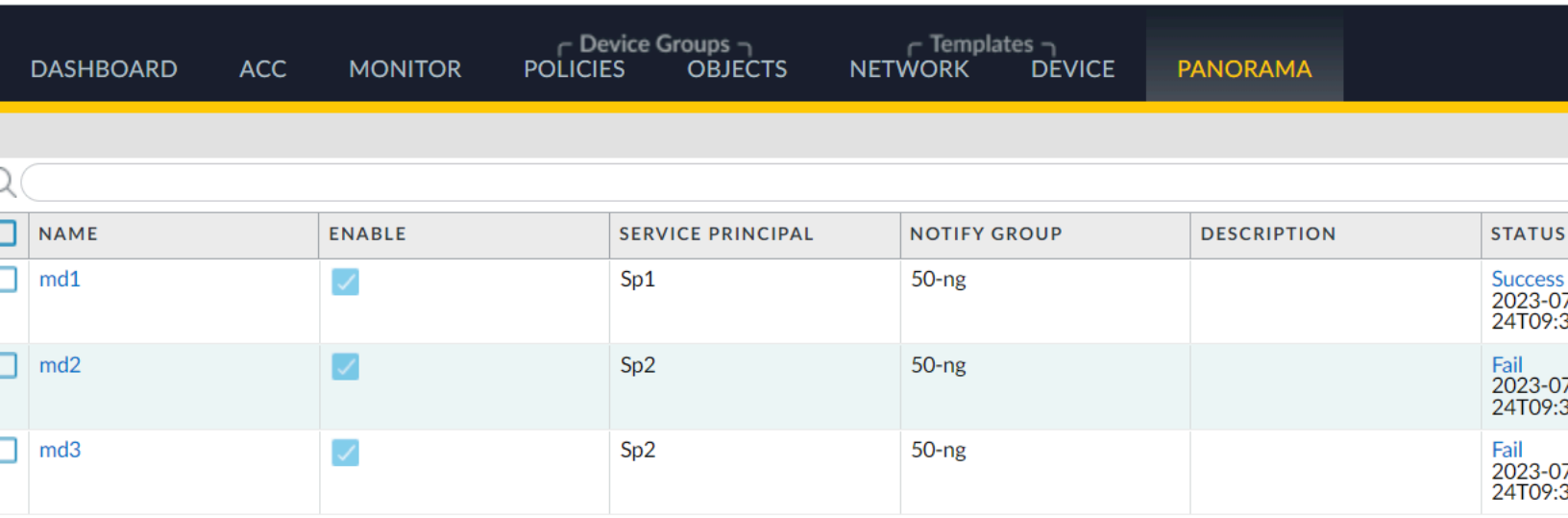
   Para eliminar el registro de las etiquetas de todos los sistemas virtuales en un cortafuegos habilitado para varios sistemas virtuales, debe añadir cada sistema virtual a un grupo de dispositivos separado en Panorama y asignar los grupos de dispositivos al grupo de notificación. Panorama registrará las etiquetas de solo un sistema virtual si asigna todos los sistemas virtuales a un grupo de dispositivos.

5. Haga clic en **OK (Aceptar)**.
6. Verifique que la supervisión se habilite en el complemento. Es necesario habilitar esta configuración para que Panorama se comunique con la nube pública de Azure para supervisar.

   La casilla de verificación **Enable Monitoring (Habilitar supervisión)** está en **Panorama** > **Plugins (Complementos)** > **Azure** > **Setup (Configuración)** > **General**.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Cree una **Monitoring Definition (Definición de monitorización)**.



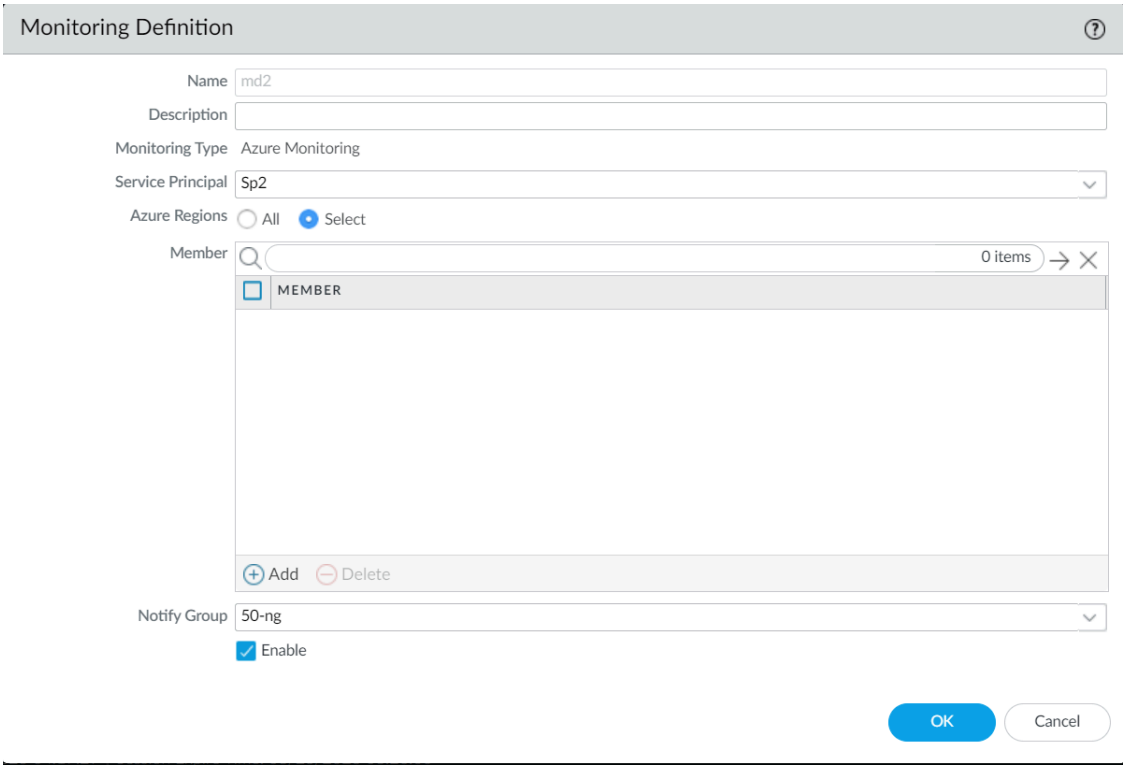
Cuando añade una nueva definición de supervisión, esta se habilita de forma predeterminada.

- Select **Panorama** > **Plugins (Complementos)** > **Azure** > **Monitoring Definition (Definición de supervisión)** para **Add (Añadir)** una nueva definición.
- Introduzca un **Name (Nombre)** y, opcionalmente, una **Description (Descripción)** para identificar la suscripción a Azure para la que usa esta definición.
- Seleccione **Service Principal (Entidad de servicio)** y **Notify Group (Grupo de notificación)**.

  Panorama requiere las claves y las ID que especifica en la configuración de la entidad de servicio para generar un token de portador de Azure, que se usa en el encabezado de la llamada a la API para recopilar información en sus cargas de trabajo.

  - *El complemento Panorama para Azure 5.1.0 admite una entidad de servicio para varias definiciones de supervisión.*
  - *El complemento Panorama para Azure 5.0.0 o una versión anterior no admite una entidad de servicio para varias definiciones de supervisión.*
- Seleccione las **Regiones de Azure**

 ©2024 Palo Alto Networks, Inc.



.

No hay dos definiciones de supervisión que puedan tener exactamente la misma ***Entidad de servicio*** *y* ***Región*** *configuradas. El complemento fallará la operación de* ***confirmación*** *para las definiciones de supervisión que tengan la misma* ***Entidad de servicio*** *y* ***Región*** *Configuradas.*

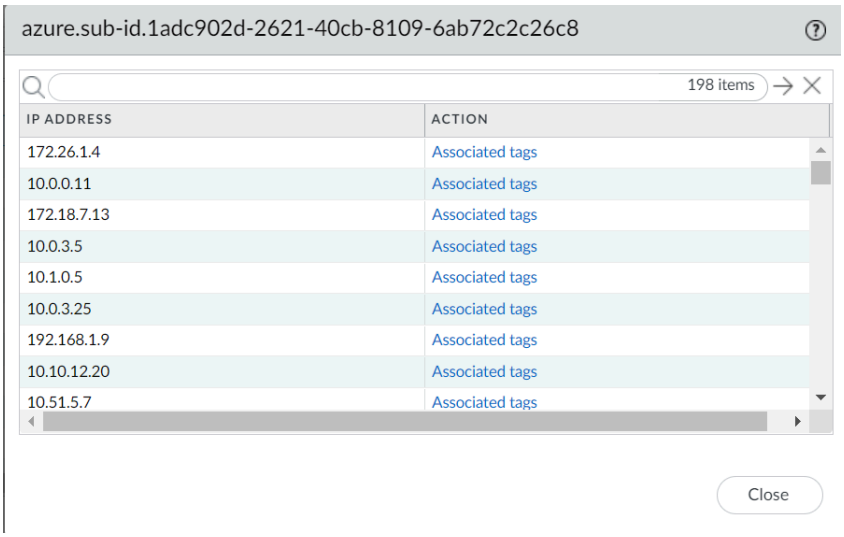
 ©2024 Palo Alto Networks, Inc.

STEP 4 | Haga clic en **Commit (Confirmar)** para confirmar los cambios realizados en Panorama.

Compruebe que el estado de la definición de monitorización se muestre como Success (Correcto). Si falla, compruebe que introdujo la ID de la suscripción a Azure correctamente y proporcionó las ID y claves correctas para la entidad de servicio.

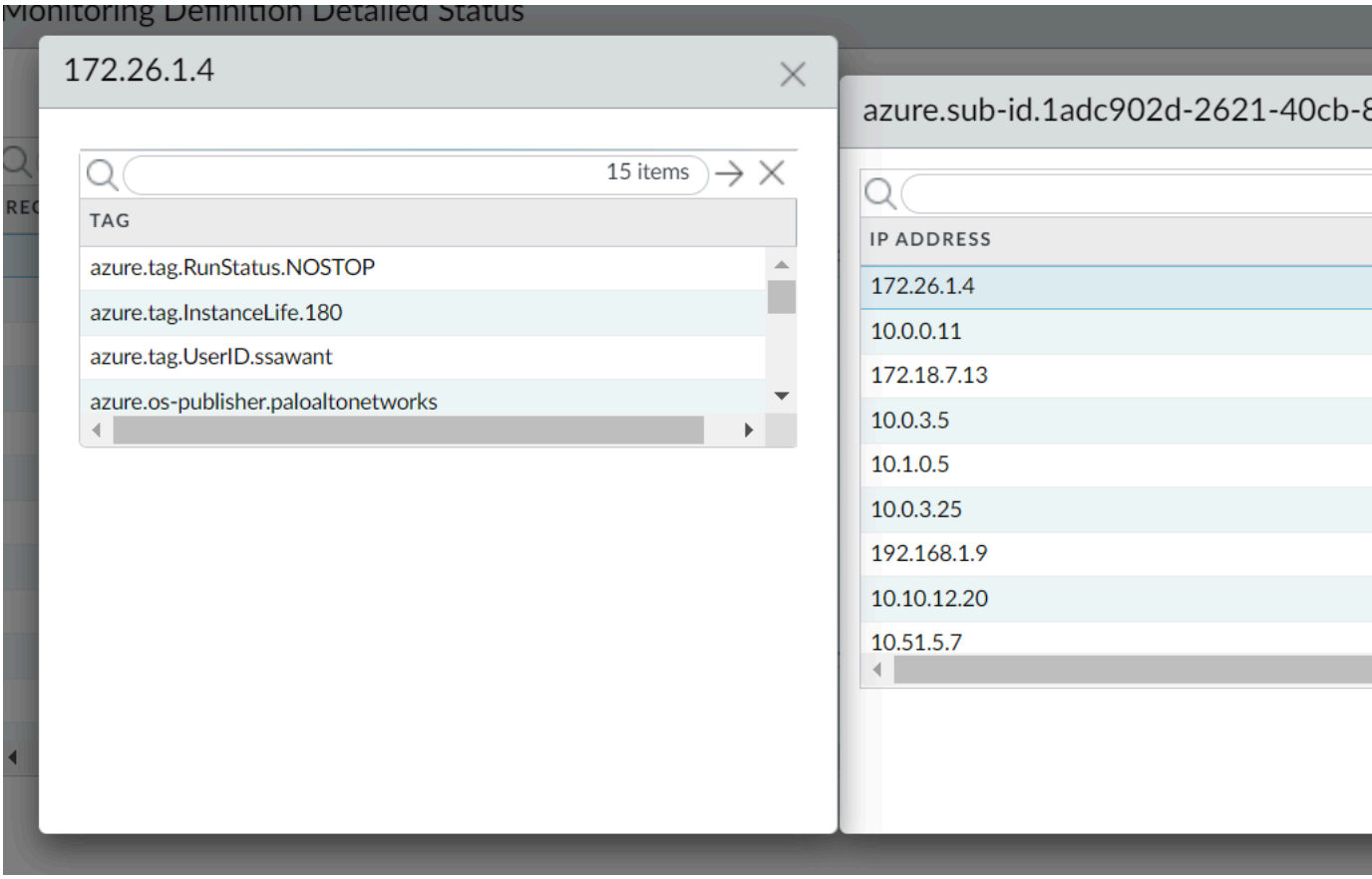
Puede seleccionar una definición de supervisión y hacer clic en el **Panel** para ver los detalles de la etiqueta de una definición de supervisión.

El filtro de ubicación en el cuadro de diálogo **Estado detallado de la definición de supervisión** filtra los detalles del panel por ubicación.



haga clic en **más** para ver la dirección IP de la etiqueta y, a continuación, vaya a **Etiquetas asociadas** para ver todas las etiquetas asociadas con esta dirección IP.

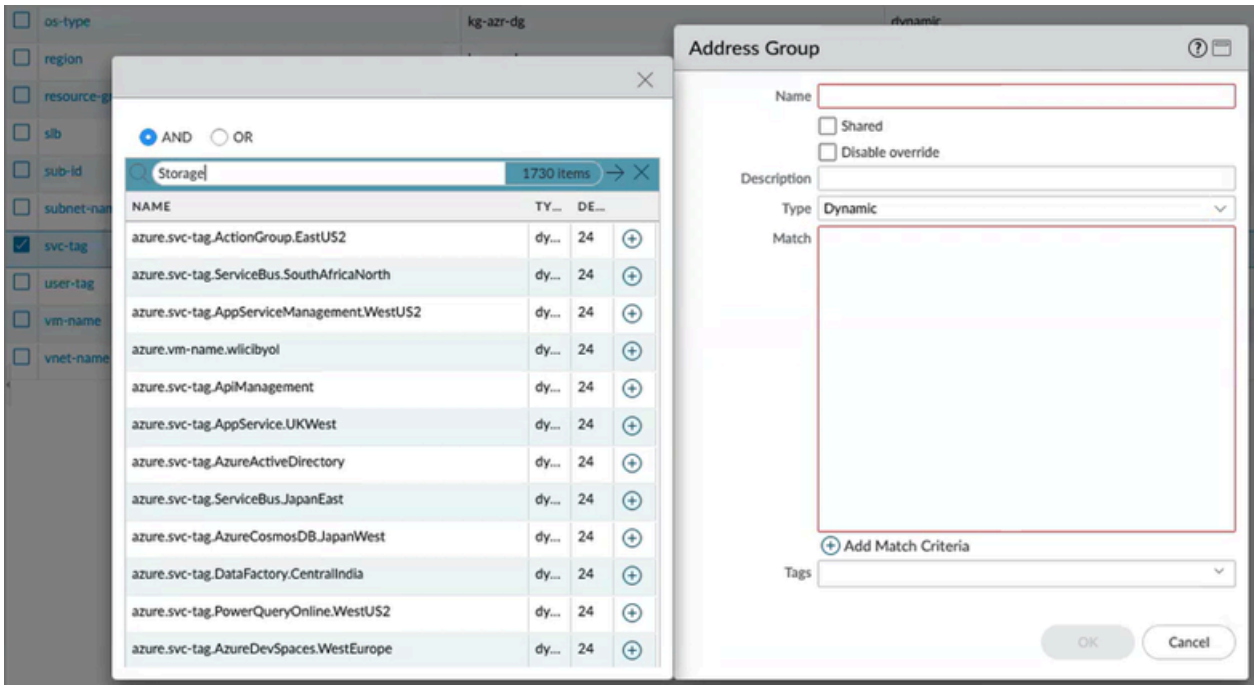
 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

STEP 5 | Compruebe que puede ver la información en Panorama y defina los criterios de coincidencia para los Grupos de direcciones dinámicas.

Algunas extensiones del navegador pueden bloquear las llamadas a la API entre Panorama y Azure, lo que evita que Panorama reciba criterios de coincidencia. Si Panorama no muestra ningún criterio de coincidencia y usted está usando extensiones de navegador, deshabilite las extensiones y Sincronizar objetos dinámicos para completar las etiquetas disponibles para Panorama.



 ©2024 Palo Alto Networks, Inc.

Durante una conmutación por error de HA, la instancia de Panorama activada recientemente intenta reconectarse a la nube de Azure y recuperar las etiquetas de todas las definiciones de supervisión. Si hay un error al volver a conectar incluso una definición de supervisión, Panorama genera un mensaje de log del sistema

```
No es posible procesar las suscripciones después
 del cambio de alta disponibilidad; se requiere la
 intervención del usuario.
```

Cuando vea este error, debe iniciar sesión en Panorama y solucionar el problema, por ejemplo, quitar una suscripción no válida o proporcionar credenciales válidas, y confirmar los cambios para permitir que Panorama vuelva a conectarse y recuperar las etiquetas de todas las definiciones de supervisión. Incluso cuando Panorama esté desconectado de la nube de Azure, los cortafuegos tienen la lista de todas las etiquetas que se recuperaron antes de la conmutación por error y pueden continuar aplicando la política en esa lista de direcciones IP. Panorama elimina todas las etiquetas asociadas a las suscripciones únicamente cuando elimina una definición de servicio. Se recomienda que para supervisar este problema, configure el reenvío de logs a un destino HTTPS *orientado a la acción desde Panorama, de modo que pueda actuar de inmediato.*

Atributos supervisados con el plugin Panorama en Azure

Cuando usa el plugin Panorama para Azure, Panorama recopila el siguiente conjunto de atributos o elementos de metadatos en las máquinas virtuales en su implementación de Microsoft® Azure®. Panorama puede recuperar un total de 32 etiquetas para cada máquina virtual, 11 etiquetas predefinidas, y hasta 21 etiquetas definidas por el usuario.

La longitud máxima de una etiqueta es de 127 caracteres. Si una etiqueta tiene más de 127 caracteres, Panorama no recupera la etiqueta y la registra en los cortafuegos. Además, las etiquetas no deberían incluir caracteres especiales no sean ASCII, como { o ".

Se admiten hasta 21 etiquetas definidas por el usuario como máximo. Las etiquetas definidas por el usuario se ordenan alfabéticamente y las primeras 21 etiquetas se pueden usar en Panorama y los cortafuegos.

El complemento Panorama en Azure versión 3.0 o posterior admite las siguientes etiquetas:

- **Balanceador de carga**

  Etiquetas del balanceador de carga para cada puerta de enlace de aplicaciones y balanceador de carga estándar (direcciones IP públicas y privadas). Cada balanceador de carga tiene etiquetas predefinidas para el grupo de recursos, el nombre del balanceador de carga y la región, y admite hasta 21 etiquetas definidas por el usuario específicas para el balanceo de carga.
- **Subred/VNET**

  Etiquetas de subred/VNET para cada subred y VNET en su suscripción. Cada etiqueta de subred y VNET está asociada con el rango CIDR de IP completo, por lo que puede crear políticas basadas en un

 ©2024 Palo Alto Networks, Inc.

rango CIDR en lugar de direcciones IP individuales. El complemento consulta cada subred y VNET en su suscripción y crea etiquetas para ellos.

Los siguientes atributos se supervisan en todos los complementos de Panorama para las versiones de Azure:

Atributos supervisados en la VPC de Azure	Ejemplo
Nombre de la VM	azure.vm-name
Tipo de sistema operativo	azure.os-type
Editor del sistema operativo	azure.os-publisher
Oferta de sistema operativo	azure.os-offer
SKU DEL SISTEMA OPERATIVO	azure.os-sku.
Región de Azure	azure.region
Nombre del grupo de recursos	azure.resource-group
Nombre de grupo de seguridad de red	azure.nsg-name
ID de suscripción	azure.sub-id
Balanceador de carga	azure.slb
Puerta de enlace de aplicaciones	azure.appgw
Nombre de la red virtual	azure.vnet-name
Nombre de subred	azure.subnet-name
Etiqueta de servicio	azure.svg-tag
Etiquetas definidas por el usuario	azure.tag.key.value

Supervisión de etiqueta de servicio

El complemento Panorama en la versión 3.0 de Azure admite etiquetas de servicio. Por ejemplo, **`azure.svg-tag`**.

Las etiquetas de servicio de Azure simplifican la seguridad de las máquinas virtuales de Azure y las redes virtuales de Azure porque le permiten limitar el acceso a la red solo a los servicios de Azure que desea utilizar. Una etiqueta de servicio representa un grupo de prefijos de direcciones IP para un servicio de Azure específico. Por ejemplo, una etiqueta puede representar todas las direcciones IP de almacenamiento.

 ©2024 Palo Alto Networks, Inc.

El complemento realiza una llamada a la API diaria (a las 5:00 am UTC) para recuperar todas las etiquetas de servicio del Portal de Azure, analiza la carga útil para formar asignaciones de servicios IP y almacena las asignaciones en la base de datos del complemento. Las asignaciones se pasan a configd, luego a Panorama. Si la llamada a la API no devuelve información del servicio, el complemento forma las asignaciones de servicios IP a partir del contenido de **`service_tags_public.json`**. Los logs del complemento informan el origen de las asignaciones del servicio IP, la recuperación diaria o el archivo JSON.

El complemento también actualiza las etiquetas de servicio para una nueva instalación del complemento, confirma eventos y la adición o eliminación de la definición de monitorización.

A continuación, se muestra un ejemplo de la asignación de servicios IP:

```
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
```

 ©2024 Palo Alto Networks, Inc.

Configuración de la HA activo/pasivo en Azure

Puede configurar un par de cortafuegos VM-Series en Azure en una configuración de alta disponibilidad (HA) activa/pasiva. Para alta disponibilidad en Azure, debe implementar ambos miembros de HA de cortafuegos dentro del mismo Grupo de recursos de Azure y debe instalar la misma versión de Plugin VM-Series en ambos miembros de HA.

- Configuración de HA activa/pasiva en Azure (tráfico norte-sur y este-oeste): si tiene una aplicación que se conecta a Internet implementada en su infraestructura de Azure y necesita proteger el tráfico norte-sur, necesita una dirección IP flotante para proteger el tráfico durante una conmutación por error. Esta dirección IP flotante, que permite la conectividad externa, siempre está conectada al par activo. En la conmutación por error, el proceso de desconexión de la dirección IP y la vuelta a conectarse al par ahora activo puede llevar unos minutos.
- Configuración de HA activa/pasiva en Azure (solo tráfico este-oeste): si sus requisitos de acceso y seguridad de las aplicaciones están contenidos en la infraestructura de Azure y solo necesita proteger el tráfico este-oeste, no necesita una dirección IP flotante. En cambio, la implementación de HA reconfigura automáticamente las UDR en las tablas de enrutamiento de Azure para proporcionar un tiempo de conmutación por error más rápido.

Para habilitar HA en el cortafuegos VM-Series en Azure, debe crear una aplicación de Azure Active Directory y una entidad de servicio que incluya los permisos que se enumeran en la siguiente tabla.

Tipo de alta disponibilidad de Azure	Permisos	Alcance de la función
Movimiento de HA de IP secundaria	**"Microsoft.Authorization/*/read""Microsoft.Compute/virtualMachines/read""Microsoft.Network/networkInterfaces/*""Microsoft.Network/networkSecurityGroups/*""Microsoft.Network/virtualNetworks/join/action""Microsoft.Network/virtualNetworks/subnets/join/action"** Los siguientes permisos son necesarios solo si ha asignado una dirección IP pública a cualquiera de sus interfaces de datos. Se recomienda la interfaz de SKU estándar. **"Microsoft.Network/publicIPAddresses/join/action""Microsoft.Network/publicIPAddresses/**	• Red virtual en la que se implementan las máquinas virtuales (VM) • Dos cortafuegos VM-Series • NIC de ambos cortafuegos VM-Series • Grupo de seguridad de red • Direcciones IP públicas de los cortafuegos VM-Series

 ©2024 Palo Alto Networks, Inc.

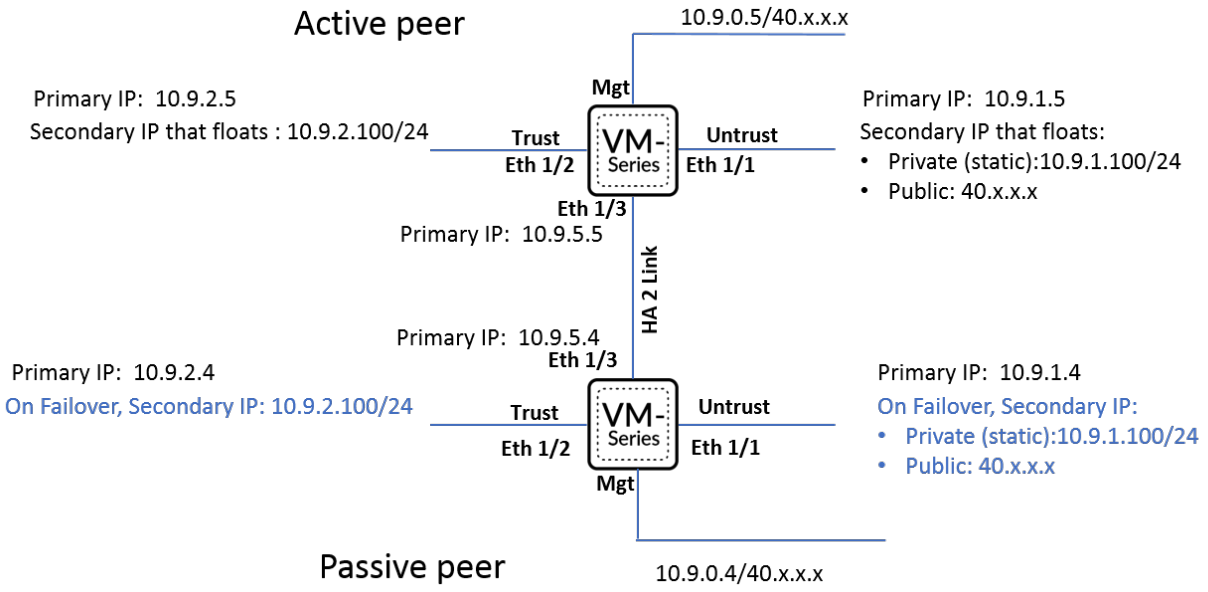
Tipo de alta disponibilidad de Azure	Permisos	Alcance de la función
	read""Microsoft.Network/publicIPAddresses/write"	
UDR HA	**"Microsoft.Authorization/*/read""Microsoft.Compute/virtualMachines/read""Microsift.Network/routeTables/*"**	• Dos cortafuegos VM-Series • NIC de ambos cortafuegos VM-Series • Tablas de ruta asociadas con UDR
Movimiento de IP secundaria y UDR	**"Microsoft.Authorization/*/read""Microsoft.Compute/virtualMachines/read""Microsoft.Network/networkInterfaces/*""Microsoft.Network/networkSecurityGroups/*""Microsoft.Network/routeTables/*""Microsift.Network/virtualNetworks/join/action""Microsoft.Network/virtualNetworks/subnets/join/action"** Los siguientes permisos son necesarios solo si ha asignado una dirección IP pública a cualquiera de sus interfaces de datos. Se recomienda la interfaz de SKU estándar. **"Microsoft.Network/publicIPAddresses/join/action""Microsoft.Network/publicIPAddresses/read""Microsoft.Network/publicIPAddresses/write"**	• Red virtual en la que se implementan las máquinas virtuales (VM) • Dos cortafuegos VM-Series • NIC de ambos cortafuegos VM-Series • Grupo de seguridad de red • Direcciones IP públicas de los cortafuegos VM-Series • Tablas de ruta asociadas con UDR

Configuración de HA activa/pasiva en Azure (tráfico norte-sur y este-oeste)

Si desea asegurar el tráfico norte-sur a sus aplicaciones en su infraestructura de Azure, use este flujo de trabajo con direcciones IP flotantes que pueden moverse rápidamente de un par a otro. Debido a que no puede mover la dirección IP asociada con la interfaz principal del cortafuegos en Azure, debe asignar una dirección IP secundaria que pueda funcionar como una dirección IP flotante. Cuando el cortafuegos activo se desactiva, la dirección IP flotante pasa del cortafuegos activo al pasivo, de modo que el cortafuegos pasivo puede proteger el tráfico sin problemas tan pronto como se convierta en el par activo. Además de la

 ©2024 Palo Alto Networks, Inc.

dirección IP flotante, los equipos en HA también necesitan Enlaces de HA, un enlace de control (HA1) y un enlace de datos (HA2), para sincronizar los datos y mantener la información de estado.



- Configuración de los cortafuegos para habilitar HA
- Configure la HA activa/pasiva en el cortafuegos VM-Series en Azure

Configuración de los cortafuegos para habilitar HA

Reúna los siguientes detalles para configurar HA en los cortafuegos VM-Series en Azure.

- Configure la aplicación de Active Directory y un y principal del servicio para habilitar el acceso a la API programática .
  - Para que el cortafuegos interactúe con las API de Azure, debe crear un Principal de servicio de Active Directory de Azure. Esta entidad de servicio tiene los permisos necesarios para autenticarse en Azure AD y acceder a los recursos dentro de su suscripción. Para completar esta configuración, debe tener permisos para registrar una aplicación con su inquilino de Azure AD y asignar la aplicación a un función en su suscripción. Si no tiene los permisos necesarios, solicite al administrador de Azure AD o de su suscripción que cree una entidad de servicio. Consulte la tabla anterior para los permisos necesarios. Copie los siguientes detalles para usar más adelante en este flujo de trabajo:
    - **ID del cliente**: la ID de la aplicación asociada con el Active Directory (en el portal de Azure, haga clic en **Home (Inicio)** > **Azure Active Directory [Active Directory de Azure]** > **App registrations [Registros de la aplicación]**, seleccione su aplicación y copie el ID).

 ©2024 Palo Alto Networks, Inc.

- **ID de inquilino**: el ID de directorio asociado con Active Directory (en el portal de Azure, haga clic en **Home [Inicio]** > **Azure Active Directory [Active Directory de Azure]** > **Properties [Propiedades]** > **Directory ID [ID de directorio]**, seleccione la aplicación y copie el ID).

- **ID de suscripción de Azure**: la suscripción de Azure en la que ha implementado los cortafuegos. Debe iniciar sesión en su portal de Azure para obtener la ID de esta suscripción.
- **Nombre del grupo de recursos**: el nombre del grupo de recursos en el que ha implementado los cortafuegos que desea configurar como pares de alta disponibilidad. Ambos cortafuegos deben estar en el mismo grupo de recursos.
- **Clave secreta**: la clave de autenticación asociada con la aplicación de Active Directory (en el portal de Azure Portal, haga clic en **Home [Inicio]** > **Azure Active Directory [Active Directory de Azure]** > **Certificates & secrets [Certificados y secretos]**, copie el **Value [Valor]** en **Client secrets (Secretos del cliente]**. Si no tiene una clave secreta, cree una primero y luego copie el valor). Para iniciar sesión como la aplicación, debe proporcionar tanto el valor clave como el ID de la aplicación.

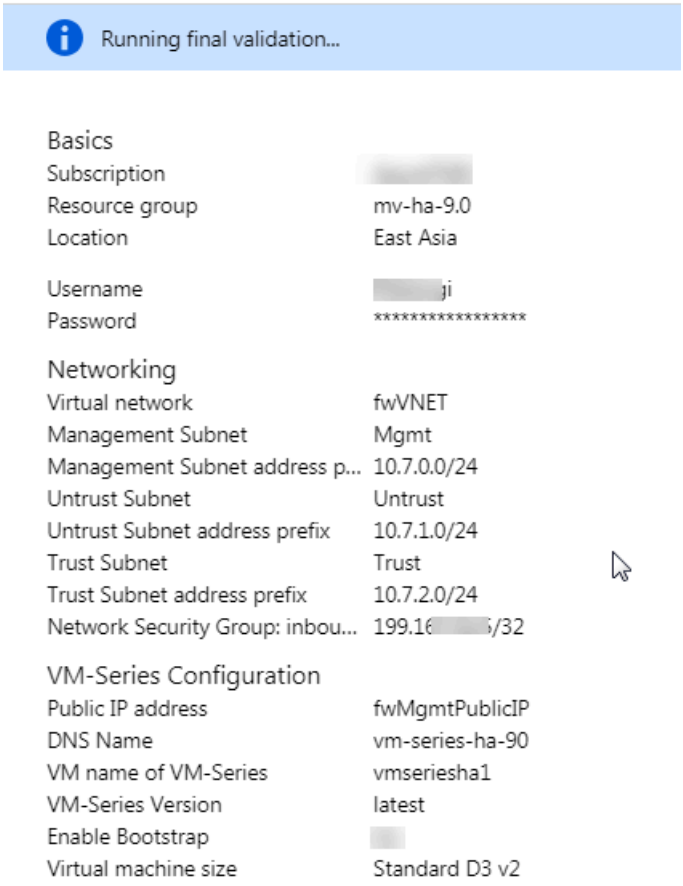
- Sepa dónde obtener las plantillas que necesita para implementar los cortafuegos VM-Series dentro del mismo Grupo de recursos de Azure.

  Para una configuración de alta disponibilidad, ambos pares de HA deben pertenecer al mismo Grupo de recursos de Azure. Si implementa la primera instancia del cortafuegos desde Azure Marketplace y debe usar su plantilla ARM personalizada o la plantilla de GitHub de muestra de Palo Alto Networks para implementar la segunda instancia del cortafuegos en el grupo de recursos existente. El motivo por

 ©2024 Palo Alto Networks, Inc.

el que necesita una plantilla personalizada o la plantilla de muestra de Palo Alto Networks es porque Azure no admite la capacidad de implementar el cortafuegos en un grupo de recursos que no esté vacío.

Copie la información de implementación para la primera instancia de cortafuegos. Por ejemplo:



- Haga coincidir el **VM Name of VM-Series (Nombre VM del cortafuegos VM-Series** como se muestra en la captura de pantalla anterior con el **Hostname (Nombre de host)** en la interfaz web del cortafuegos. Debe añadir el mismo nombre en **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**, porque el nombre de host del cortafuegos se utiliza para desencadenar la conmutación por error.

- Planifique la configuración de la interfaz de red en los cortafuegos VM-Series en Azure.

  Para configurar alta disponibilidad (HA), debe implementar ambos pares de HA dentro del mismo Grupo de recursos de Azure y ambos cortafuegos deben tener el mismo número de interfaces de red. Se requiere un mínimo de cuatro interfaces de red en cada par de HA:

  - **Interfaz de gestión (eth0)**: dirección IP privada y pública asociada con la interfaz principal. La dirección IP pública permite el acceso a la interfaz web del cortafuegos y al acceso SSH.

    Puede utilizar la interfaz IP privada en la interfaz de gestión como la dirección IP del par HA1 para la comunicación de enlace de control entre los pares activo/pasivo de HA. Si desea una interfaz

 ©2024 Palo Alto Networks, Inc.

dedicada HA1, debe adjuntar una interfaz de red adicional en cada cortafuegos, y esto significa que necesita cinco interfaces en cada cortafuegos.

- **Interfaz untrust (eth1 / 1)**: dirección IP privada principal con máscara de red /32 y configuración de IP secundaria con una dirección IP privada (cualquier máscara de red) y una dirección IP pública.

  En una conmutación por error, cuando el par pasivo pasa al estado activo, la dirección IP pública asociada con la configuración de IP secundaria se separa del par anteriormente activo y se une al par HA ahora activo.
- **Interfaz trust (eth1 / 2)**: direcciones IP privadas primarias y secundarias. En una conmutación por error, cuando el par pasivo pasa al estado activo, la dirección IP privada secundaria se separa del par previamente activo y se une al par HA ahora activo.
- **HA2 (eth 1/3)**: dirección IP privada principal. La interfaz HA2 es el enlace de datos que utilizan los equipos en HA para sincronizar sesiones, reenviar tablas, asociaciones de seguridad IPSec y tablas ARP.

Interface (Interfaz)	Equipo de cortafuegos activo	Equipo de cortafuegos pasivo	Description (Descripción)
Fiable	Dirección de IP secundaria	—	La interfaz de confianza del equipo activo requiere una configuración de IP secundaria que pueda flotar hacia el otro par durante una conmutación por error. Esta configuración de IP secundaria en la interfaz de confianza debe ser una dirección IP privada con la máscara de red de los servidores que protege. En caso de una conmutación por error, el plugin VM-Series llama a la API de Azure para desconectar esta dirección IP privada secundaria del miembro activo y adjuntarla al pasivo. La conexión de esta dirección IP al miembro ahora activo garantiza que el cortafuegos pueda recibir tráfico en la IP flotante en la interfaz untrust y enviarla a la IP flotante en la interfaz trust y a las cargas de trabajo.
No fiable	Dirección de IP secundaria	—	La interfaz untrust del cortafuegos requiere una configuración de IP secundaria que incluya una dirección IP privada estática con una máscara de red para la subred untrust y una dirección IP pública para acceder a los servidores de servicios de backend o las cargas de trabajo a través de Internet. En caso de una conmutación por error, el plugin VM-Series llama a la API de Azure para separar la configuración de IP secundaria del miembro activo y adjuntarla al pasivo antes de que pase al estado activo. Este proceso de flotación de la configuración de IP secundaria permite que el cortafuegos ahora activo continúe procesando el tráfico entrante que está destinado a las cargas de trabajo.

 ©2024 Palo Alto Networks, Inc.

Interface (Interfaz)	Equipo de cortafuegos activo	Equipo de cortafuegos pasivo	Description (Descripción)
HA2	Añada un NIC al cortafuegos desde la consola de administración de Azure.	Añada un NIC al cortafuegos desde la consola de administración de Azure.	En los miembros activo y pasivo, añada un enlace dedicado de HA2 para habilitar la sincronización de la sesión. La interfaz predeterminada para HA1 es la interfaz de gestión, y usted puede optar por usar la interfaz de gestión en lugar de añadir una interfaz adicional al cortafuegos. Para habilitar el flujo de datos a través del enlace HA2, debe añadir una interfaz de red adicional en el portal de Azure y configurar la interfaz para HA2 en el cortafuegos.

Configure la HA activa/pasiva en el cortafuegos VM-Series en Azure

En este flujo de trabajo, implementa la primera instancia del cortafuegos VM-Series utilizando la plantilla de solución de cortafuegos VM-Series en Azure marketplace, y la segunda instancia del cortafuegos utilizando la plantilla GitHub de muestra.

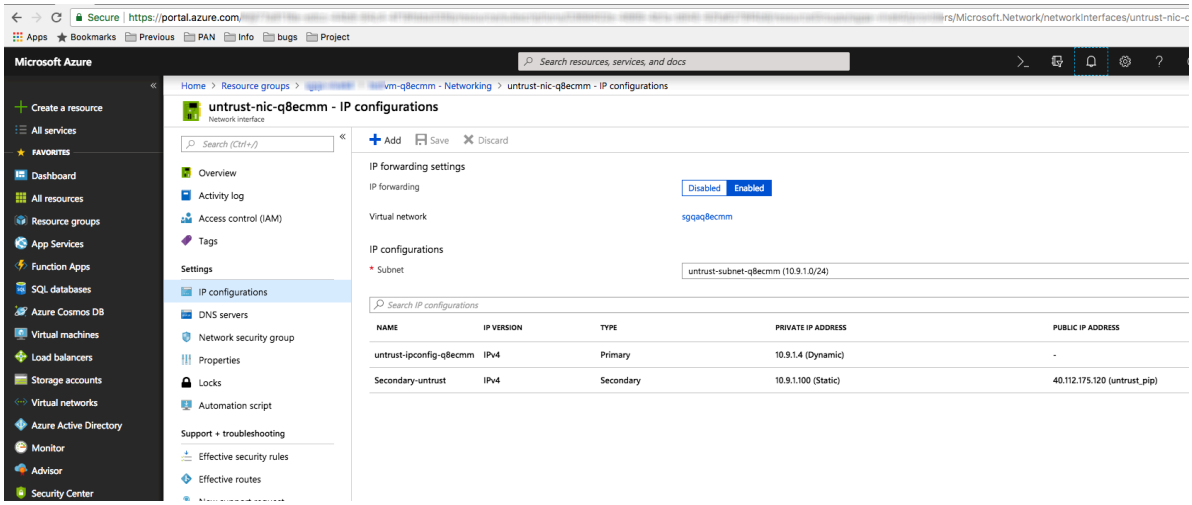
La clave de autenticación (secreto de cliente) asociada con la aplicación de Active Directory necesaria para configurar el cortafuegos VM-Series en una configuración de alta disponibilidad, se cifra con la versión 1.0.4 del plugin VM-Series en el cortafuegos y en Panorama. Debido a que la clave está Cifrada en la versión 1.0.4 del plugin VM-Series, debe instalar la misma versión del plugin en Panorama y los cortafuegos VM-Series gestionados para poder gestionar de manera centralizada los servidores de seguridad de Panorama.

Ahora puede configurar hasta cuatro direcciones IP por interfaz SD-WAN para lograr la conmutación por error de alta disponibilidad en configuraciones activas/pasivas de su entorno de nube pública de Azure. Puede lograrlo configurando una segunda dirección IP flotante en las interfaces SD-WAN. La IP flotante en la interfaz SD-WAN de la zona externa debe coincidir con la de la zona interna. Esta función solo es compatible con PAN-OS 11.1.0 y versiones posteriores y solo con direcciones IPv4.

©2024 Palo Alto Networks, Inc.

STEP 1 | Implemente el cortafuegos VM-Series utilizando una plantilla de solución y configure las interfaces de red para HA.

1. Añada una configuración de IP secundaria a la interfaz untrust en el cortafuegos.



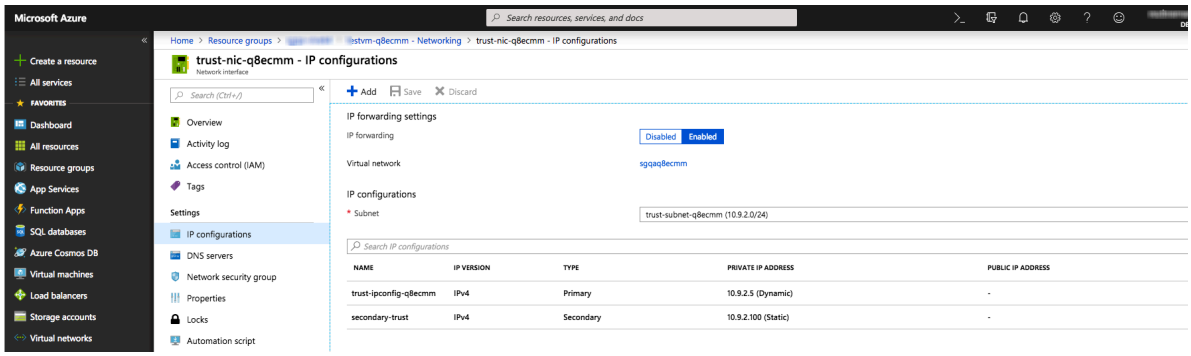
Debe adjuntar la configuración de IP secundaria, con una dirección IP privada (cualquier máscara de red) y una dirección IP pública, al cortafuegos que será designado como el miembro activo. La configuración de IP secundaria siempre permanece con el miembro de HA activo y se mueve de un equipo a otro cuando se produce una conmutación por error.

En este flujo de trabajo, este cortafuegos será designado como el miembro activo. El miembro de HA activo tiene un valor numérico más bajo para prioridad del dispositivo que configura como parte

 ©2024 Palo Alto Networks, Inc.

de la configuración de HA en el cortafuegos, y este valor indica una preferencia por cuál cortafuegos asume el rol de equipo activo.

2. Añada una configuración de IP secundaria a la interfaz trust en el cortafuegos.



La configuración de IP secundaria para la interfaz trust solo requiere una dirección IP privada estática. Esta dirección IP se mueve desde el cortafuegos activo al cortafuegos pasivo en caso de

 ©2024 Palo Alto Networks, Inc.

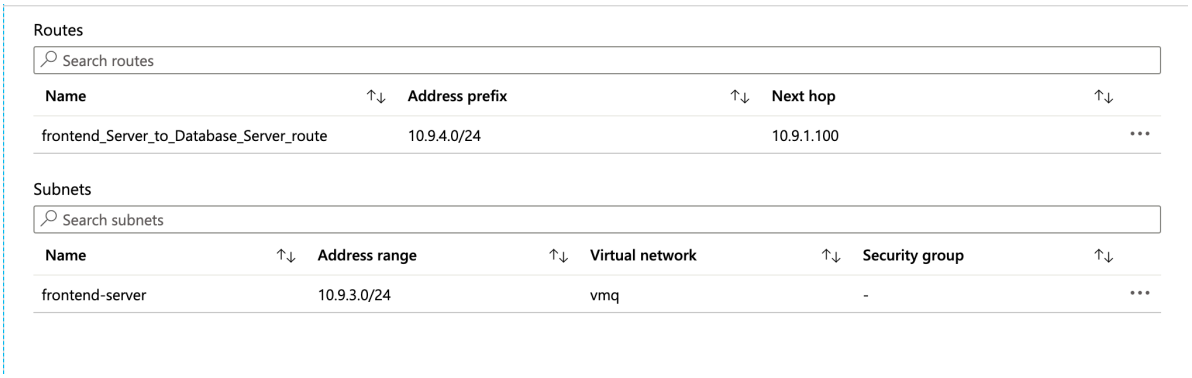
fallo, de modo que el tráfico fluye desde untrust a la interfaz trust y a las subredes de destino que el cortafuegos protege.

3. Conecte una interfaz de red para la comunicación de HA2 entre los miembros en HA del cortafuegos.
   1. Añada una subred dentro de la red virtual.
   2. Crear y adjuntar una interfaz de red al cortafuegos.
4. Configure su tabla de rutas en Azure.

   Su próximo salto debe apuntar a la dirección IP flotante como se muestra aquí:



 ©2024 Palo Alto Networks, Inc.



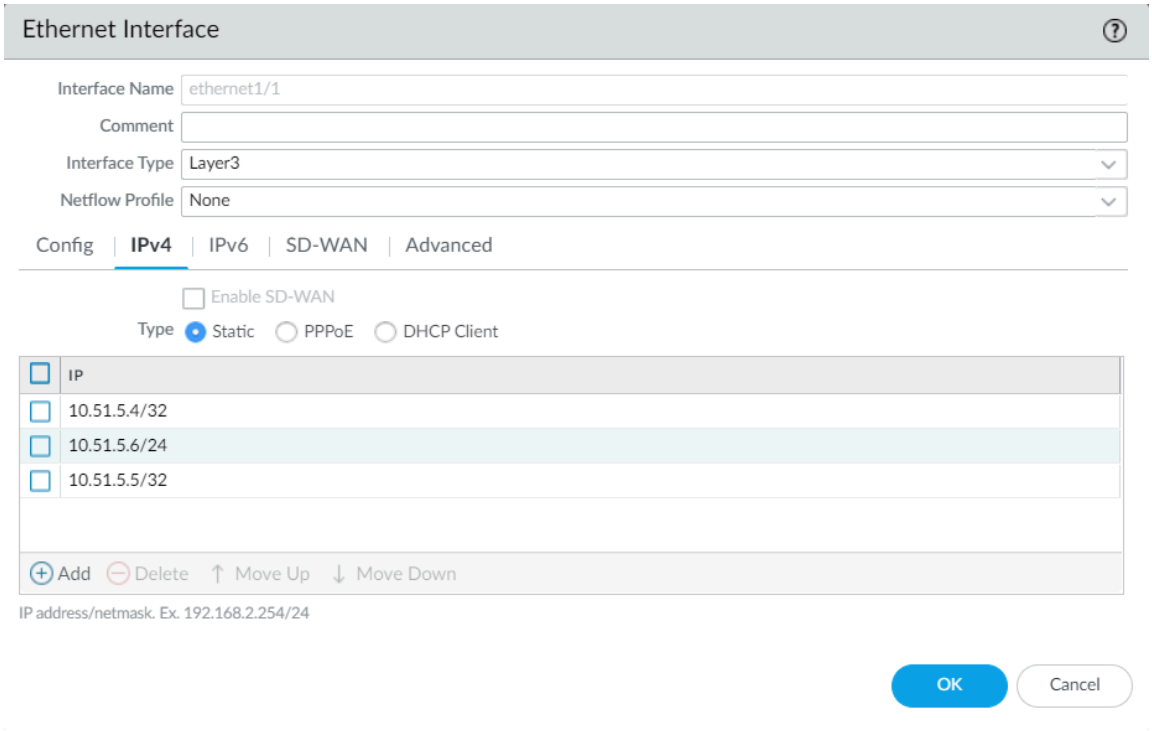
 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configure las interfaces en el cortafuegos.

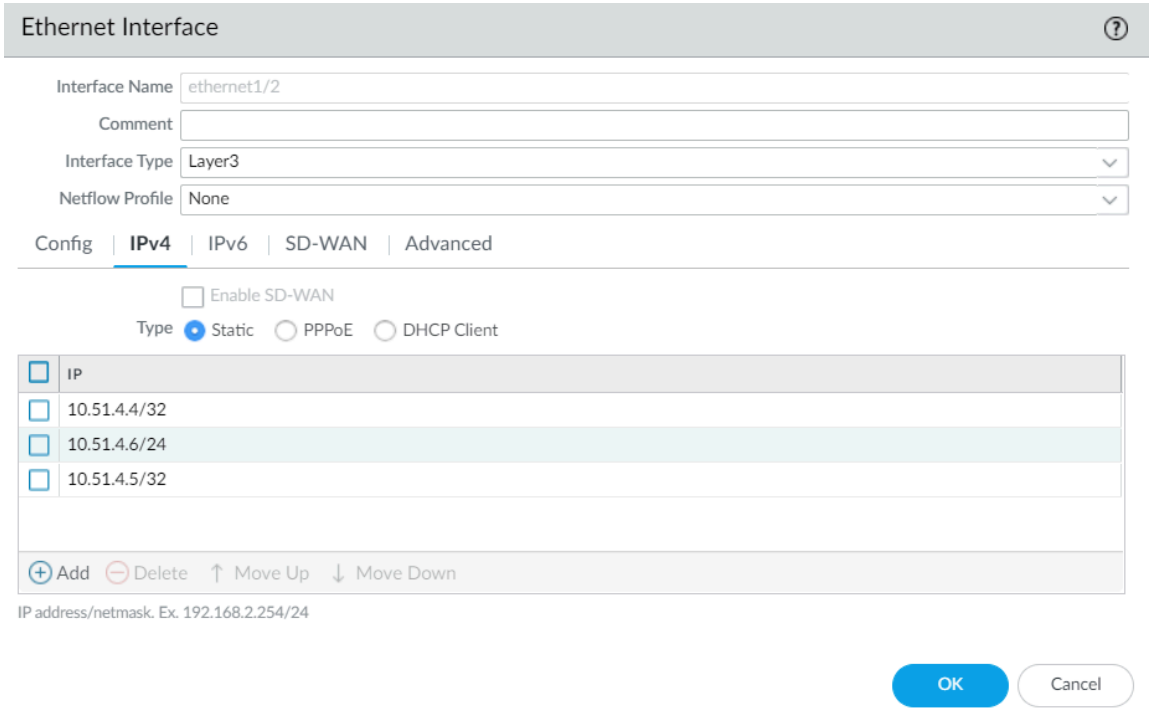
Complete estos pasos en el miembro de HA activo, antes de implementar y configurar el miembro de HA pasivo.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Configure ethernet 1/1 como la interfaz untrust y ethernet 1/2 como la interfaz trust.

   Seleccione **Network (Red)** > **Interfaces** y configure de la siguiente forma:



 ©2024 Palo Alto Networks, Inc.



3. Configure ethernet 1/3 como la interfaz de HA.

   Para configurar el enlace HA2, seleccione la interfaz y establezca el **Interface Type (Tipo de interfaz)** en **AH**. Ajuste la velocidad del enlace y dúplex a automático.



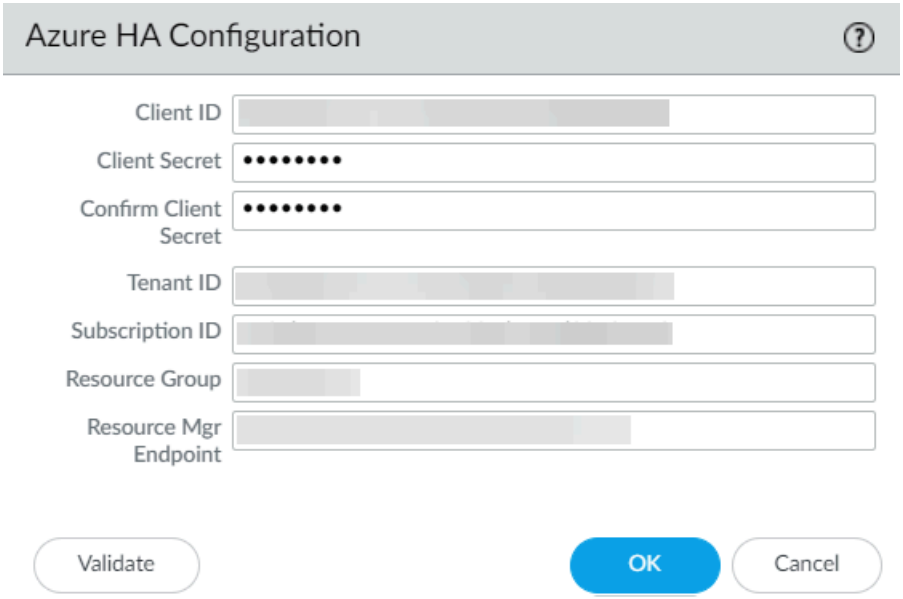
 ©2024 Palo Alto Networks, Inc.

STEP 3 | Configure el plugin VM-Series para autenticarse en el grupo de recursos de Azure en el que ha implementado el cortafuegos.

Configure la configuración de Azure HA en el plugin de VM-Series.

Para cifrar el secreto del cliente, use el plugin VM-Series versión 1.0.4 o posterior. Si usa Panorama para gestionar sus cortafuegos, debe instalar la versión 1.0.4 o posterior del plugin VM-Series.

1. Seleccione **Device (Dispositivo)** > **VM-Series** para habilitar el acceso programático entre el plugin del cortafuegos y los recursos de Azure.



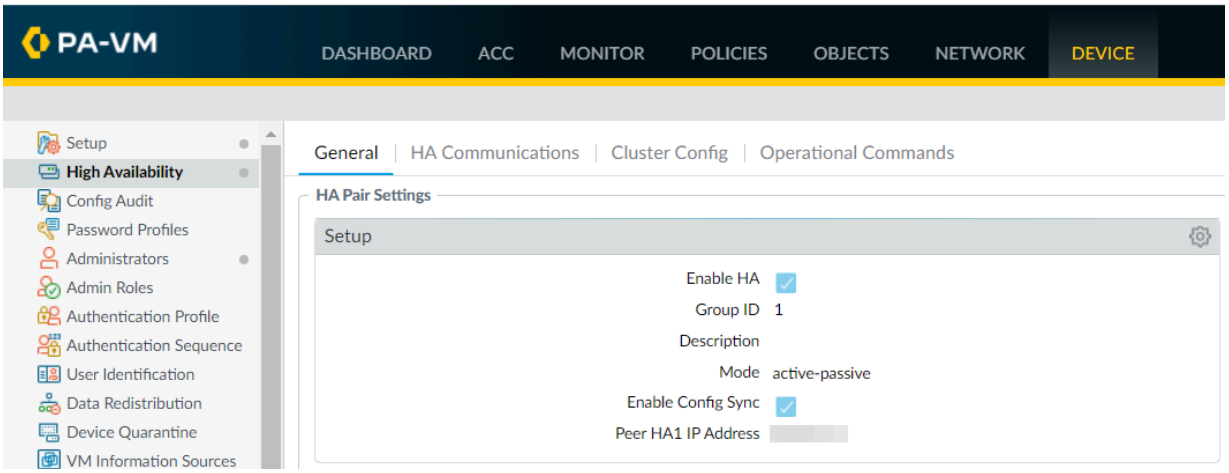
2. Introduzca la **Client ID (ID de cliente)**. La ID del cliente es la ID de la aplicación asociada a su aplicación de Azure Active Directory.
3. Introduzca el **Client Secret (Secreto del cliente)** y vuelva a introducirla para confirmarlo.
4. Introduzca la **Tenant ID (ID de inquilino)**. La ID de inquilino es la ID del directorio que guardó cuando configuró la aplicación de Active Directory.
5. Introduzca la **Subscription ID (ID de suscripción)** para la suscripción de Azure que desea supervisar.
6. Introduzca el nombre del **Resource Group (Grupo de recursos)**.
7. (Solo para implementaciones de Azure Stack) Introduzca la URL del **Resource Mgr Endpoint (Endpoint del gestor de recursos)**. Este campo es obligatorio SOLO para implementaciones de Azure Stack. No introduzca un valor para este campo si usa una implementación normal de Azure Cloud; La conmutación por error de alta disponibilidad (HA) no se realizará correctamente si especifica la dirección la URL del **Resource Mgr Endpoint (Endpoint del gestor de recursos)** para una implementación normal de Azure Cloud.

   Este campo está disponible en el complemento VM-Series 2.1.2 y posterior.

8. Haga clic en **Validate (Validar)** para comprobar que las claves y las ID que introdujo son válidas y que el plugin VM-Series se puede comunicar con los recursos de Azure usando la API.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Habilitar HA.



1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **HA**.
2. Introduzca la **Peer HA1 IP Address (Dirección IP de HA1 del peer)** como la dirección IP privada del equipo pasivo.
3. (Opcional) Edite el enlace de control (HA1). Si no planifica usar la interfaz de gestión para el enlace de control y ha añadido una interfaz adicional (por ejemplo, ethernet 1/4), edite esta sección para seleccionar la interfaz que se usará para la comunicación de HA1.
4. Edite el enlace de datos (HA2) para usar **Port (Puerto)** Ethernet 1/3 y añada la dirección IP de este equipo y la dirección IP de la **Gateway (Puerta de enlace)** para la subred. Al elegir el modo de transporte, tenga en cuenta que UPD es el único modo de transporte compatible con entornos de Azure. Al elegir el modo de transporte, tenga en cuenta que UPD es el único modo de transporte compatible con entornos de Azure.

STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 6 | Configure el miembro HA pasivo dentro del mismo Grupo de recursos de Azure.

1. Implemente la segunda instancia del cortafuegos.
   - Descargue la plantilla personalizada y el archivo de parámetros de GitHub.
   - Inicie sesión en el portal de Azure.
   - Busque la **custom template (plantilla personalizada)** y seleccione **Deploy from a custom template (Implementar desde una plantilla personalizada)**.
   - Seleccione **Build your own template in the editor (Crear su propia plantilla en el editor)** > **load File (Cargar archivo)**.
   - Seleccione el **azuredeploy.json** que descargó anteriormente, y seleccione **Save (Guardar)**.
   - Complete las entradas, acepte los términos y elija **Purchase (Comprar)**.

     Asegúrese de hacer coincidir las siguientes entradas con la de la instancia de cortafuegos que ya implementó: suscripción de Azure, nombre del grupo de recursos, ubicación del grupo

 ©2024 Palo Alto Networks, Inc.

de recursos, nombre de la red virtual existente en la que desea implementar el cortafuegos, VNet CIDR, Nombres de subred, CIDR de subred e inicie la dirección IP para las subredes de gestión, trust y untrust.

2. Repita el Paso 1 y Paso 2para configurar las interfaces y configurar el cortafuegos como el equipo HA pasivo.
3. Omita el Paso 3 y complete la Habilitación de HA (Paso 5). En Paso 4 modifique las direcciones IP según corresponda para este miembro HA pasivo.

STEP 7 | Cuando termine de configurar ambos cortafuegos, verifique que los dispositivos están emparejados en la HA activo/pasivo.

1. Acceda al **Dashboard** de ambos dispositivos y visualice el widget High Availability.
2. En el cortafuegos activo, haga clic en el enlace **Sync to peer**.
3. Confirme que los cortafuegos están emparejados y sincronizados, como se muestra a continuación:
   - En el cortafuegos pasivo: el estado del cortafuegos local debería mostrar **passive (pasivo)** y la **Running Config (Config. en ejecución)** debería mostrar **synchronized (sincronizada)**.
   - En el cortafuegos activo: El estado del cortafuegos local debería mostrar **active (activo)** y **Running Config (Config. en ejecución)** debería mostrar **synchronized (sincronizada)**.
4. En el equipo pasivo, verifique que la configuración del plugin VM-Series ahora esté sincronizada.

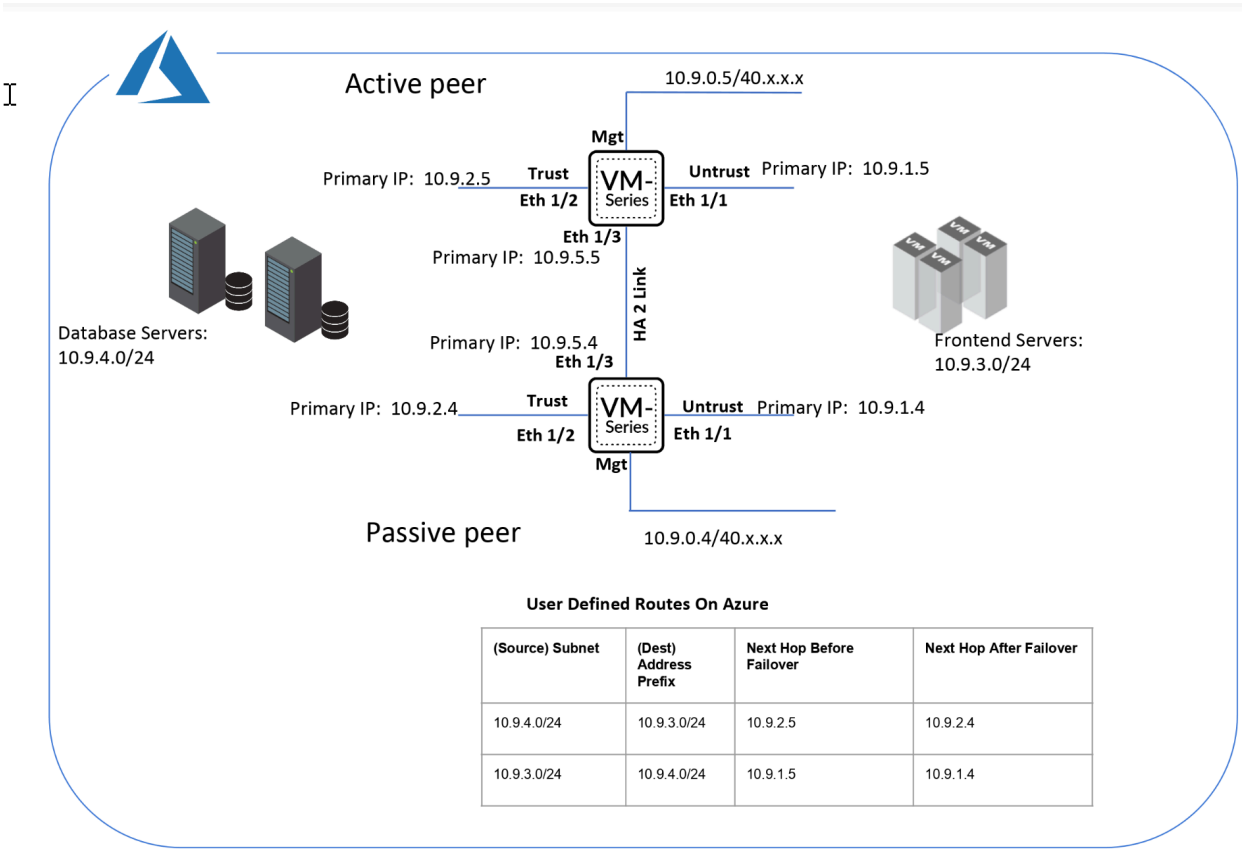
   Seleccione **Device (Dispositivo)** > **VM-Series** y valide que puede ver la configuración de Azure HA que había omitido durante la configuración del equipo pasivo.

Configuración de HA activa/pasiva en Azure (solo tráfico este-oeste)

Si todos sus recursos están implementados dentro de la infraestructura de Azure y no necesita aplicar seguridad para el tráfico norte sur a la red virtual de Azure, puede implementar un par de cortafuegos VM-Series en una configuración de alta disponibilidad (HA) activa/pasiva sin direcciones IP flotantes. Los pares de HA continuarán necesitando Enlaces de HA, un enlace de control (HA1) y un enlace de datos (HA2), para sincronizar los datos y mantener la información de estado.

Debe tener la versión 1.0.9 o posterior de Plugin VM-Series y debe implementar ambos miembros de HA del cortafuegos en el mismo grupo de recursos de Azure.

 ©2024 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

- Configuración de los cortafuegos para habilitar HA
- Configure la HA activa/pasiva en el cortafuegos VM-Series en Azure

Configuración de los cortafuegos para habilitar HA

Reúna los siguientes detalles para configurar HA en los cortafuegos VM-Series en Azure.

- Configure la aplicación de Active Directory y un y principal del servicio para habilitar el acceso a la API programática .
  - Para que el cortafuegos interactúe con las API de Azure, debe crear un Principal de servicio de Active Directory de Azure. Esta entidad de servicio tiene los permisos necesarios para autenticarse en Azure AD y acceder a los recursos dentro de su suscripción. Para completar esta configuración, debe tener permisos para registrar una aplicación con su inquilino de Azure AD y asignar la aplicación a un función en su suscripción. Si no tiene los permisos necesarios, solicite al administrador de Azure AD o de su suscripción que cree una entidad de servicio. Consulte la tabla

 ©2024 Palo Alto Networks, Inc.

anterior para los permisos necesarios. Copie los siguientes detalles para usar más adelante en este flujo de trabajo:

- **ID del cliente**: la ID de la aplicación asociada con el Active Directory (en el portal de Azure, haga clic en **Home (Inicio)** > **Azure Active Directory [Active Directory de Azure]** > **App registrations [Registros de la aplicación]**, seleccione su aplicación y copie el ID).
- **ID de inquilino**: el ID de directorio asociado con Active Directory (en el portal de Azure, haga clic en **Home [Inicio]** > **Azure Active Directory [Active Directory de Azure]** > **Properties [Propiedades]** > **Directory ID [ID de directorio]**, seleccione la aplicación y copie el ID).
- **ID de suscripción de Azure**: la suscripción de Azure en la que ha implementado los cortafuegos. Debe iniciar sesión en su portal de Azure para obtener la ID de esta suscripción.
- **Nombre del grupo de recursos**: el nombre del grupo de recursos en el que ha implementado los cortafuegos que desea configurar como pares de alta disponibilidad. Ambos cortafuegos deben estar en el mismo grupo de recursos.
- **Clave secreta**: la clave de autenticación asociada con la aplicación de Active Directory (en el portal de Azure Portal, haga clic en **Home [Inicio]** > **Azure Active Directory [Active Directory de Azure]** > **Certificates & secrets [Certificados y secretos]**, copie el **Value [Valor]** en **Client secrets (Secretos del cliente]**. Si no tiene una clave secreta, cree una primero y luego copie el valor). Para iniciar sesión como la aplicación, debe proporcionar tanto el valor clave como el ID de la aplicación.

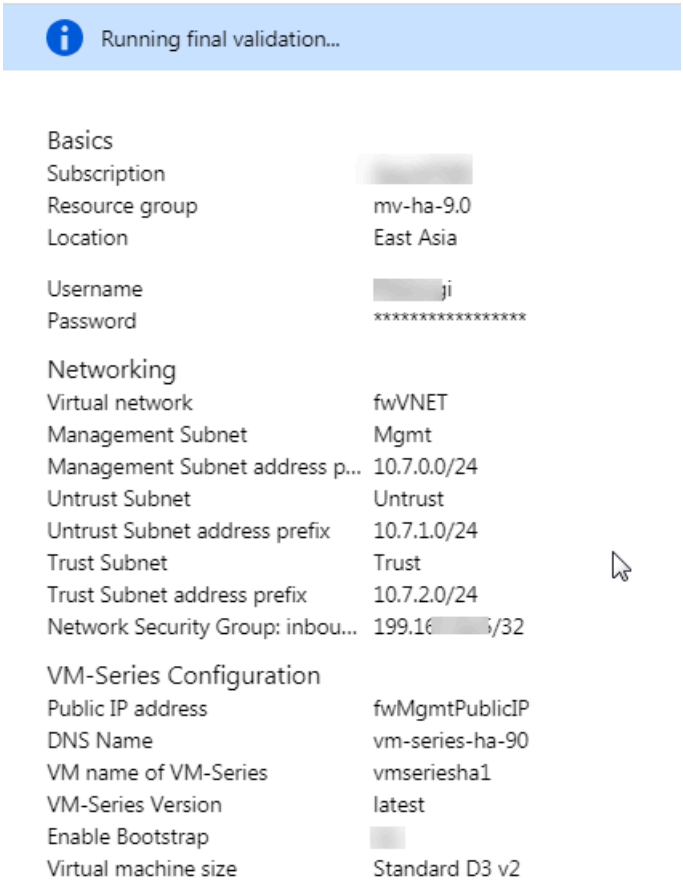
- Sepa dónde obtener las plantillas que necesita para implementar los cortafuegos VM-Series dentro del mismo Grupo de recursos de Azure.

  Para una configuración de alta disponibilidad, ambos pares de HA deben pertenecer al mismo Grupo de recursos de Azure. Si implementa la primera instancia del cortafuegos desde Azure Marketplace y debe usar su plantilla ARM personalizada o la plantilla de GitHub de muestra de Palo Alto Networks para implementar la segunda instancia del cortafuegos en el grupo de recursos existente. El motivo por

 ©2024 Palo Alto Networks, Inc.

el que necesita una plantilla personalizada o la plantilla de muestra de Palo Alto Networks es porque Azure no admite la capacidad de implementar el cortafuegos en un grupo de recursos que no esté vacío.

Copie la información de implementación para la primera instancia de cortafuegos. Por ejemplo:



- Haga coincidir el **VM Name of VM-Series (Nombre VM del cortafuegos VM-Series** como se muestra en la captura de pantalla anterior con el **Hostname (Nombre de host)** en la interfaz web del cortafuegos. Debe añadir el mismo nombre en **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**, porque el nombre de host del cortafuegos se utiliza para desencadenar la conmutación por error.

- Planifique la configuración de la interfaz de red en los cortafuegos VM-Series en Azure.

  Para configurar alta disponibilidad (HA), debe implementar ambos pares de HA dentro del mismo Grupo de recursos de Azure y ambos cortafuegos deben tener el mismo número de interfaces de red. Se requiere un mínimo de cuatro interfaces de red en cada par de HA:

  - **Interfaz de gestión (eth0)**: dirección IP privada y pública asociada con la interfaz principal. La dirección IP pública permite el acceso a la interfaz web del cortafuegos y al acceso SSH.

    Puede utilizar la interfaz IP privada en la interfaz de gestión como la dirección IP del par HA1 para la comunicación de enlace de control entre los pares activo/pasivo de HA. Si desea una interfaz

 ©2024 Palo Alto Networks, Inc.

dedicada HA1, debe adjuntar una interfaz de red adicional en cada cortafuegos, y esto significa que necesita cinco interfaces en cada cortafuegos.

- **Interfaz untrust (eth1/1)**: dirección IP privada principal con máscara de red /32.

  En la conmutación por error, cuando el par pasivo pasa al estado activo, el complemento de VM-Series envía automáticamente el tráfico a la dirección IP privada principal del par pasivo. Las UDR de Azure habilitan el flujo de tráfico.
- **Interfaz de confianza (eth1/2)**: dirección IP privada principal. En la conmutación por error, cuando el par pasivo pasa al estado activo, el complemento de VM-Series envía automáticamente el tráfico a la dirección IP privada principal del par pasivo.
- **HA2 (eth 1/3)**: dirección IP privada principal. La interfaz HA2 es el enlace de datos que utilizan los equipos en HA para sincronizar sesiones, reenviar tablas, asociaciones de seguridad IPSec y tablas ARP.

Interface (Interfaz)	Equipo de cortafuegos activo	Equipo de cortafuegos pasivo	Description (Descripción)
HA2	Añada un NIC al cortafuegos desde la consola de administración de Azure.	Añada un NIC al cortafuegos desde la consola de administración de Azure.	En los miembros activo y pasivo, añada un enlace dedicado de HA2 para habilitar la sincronización de la sesión. La interfaz predeterminada para HA1 es la interfaz de gestión, y usted puede optar por usar la interfaz de gestión en lugar de añadir una interfaz adicional al cortafuegos. Para habilitar el flujo de datos a través del enlace HA2, debe añadir una interfaz de red adicional en el portal de Azure y configurar la interfaz para HA2 en el cortafuegos.

Configure la HA activa/pasiva en el cortafuegos VM-Series en Azure

En este flujo de trabajo, implementa la primera instancia del cortafuegos VM-Series utilizando la plantilla de solución de cortafuegos VM-Series en Azure marketplace, y la segunda instancia del cortafuegos utilizando la plantilla GitHub de muestra.

 ©2024 Palo Alto Networks, Inc.

La clave de autenticación (secreto de cliente) asociada con la aplicación de Active Directory necesaria para configurar el cortafuegos VM-Series en una configuración de alta disponibilidad, se cifra con la versión 1.0.9 del complemento de VM-Series en el cortafuegos y en Panorama. Debido a que la clave está cifrada en la versión 1.0.9 del complemento de VM-Series, debe instalar la misma versión del plugin en Panorama y los cortafuegos VM-Series gestionados para poder gestionar de manera centralizada los servidores de seguridad de Panorama.

STEP 1 | Implemente el cortafuegos VM-Series utilizando una plantilla de solución y configure las interfaces de red para HA.

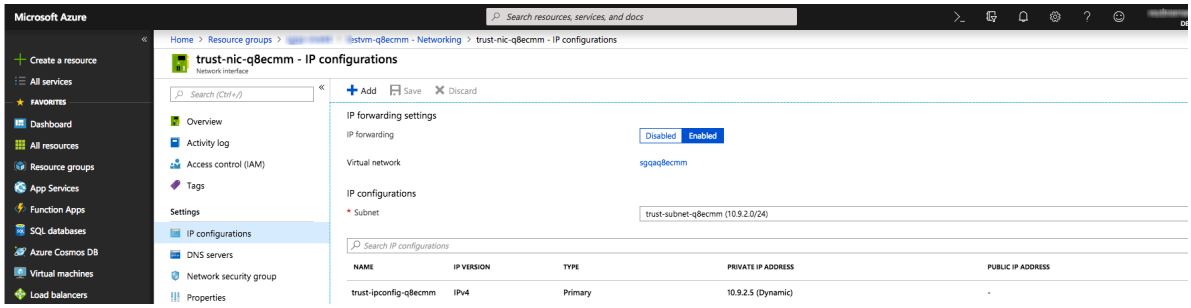
Para proteger el tráfico este-oeste dentro de una red virtual de Azure, solo necesita una dirección IP principal para las interfaces trust y untrust del cortafuegos. Cuando se produce una conmutación por error, la UDR cambia y la ruta apunta a la dirección IP principal del par que pasa al estado activo.

1. Añadir una configuración de IP principal a la interfaz de confianza del miembro activo del cortafuegos.

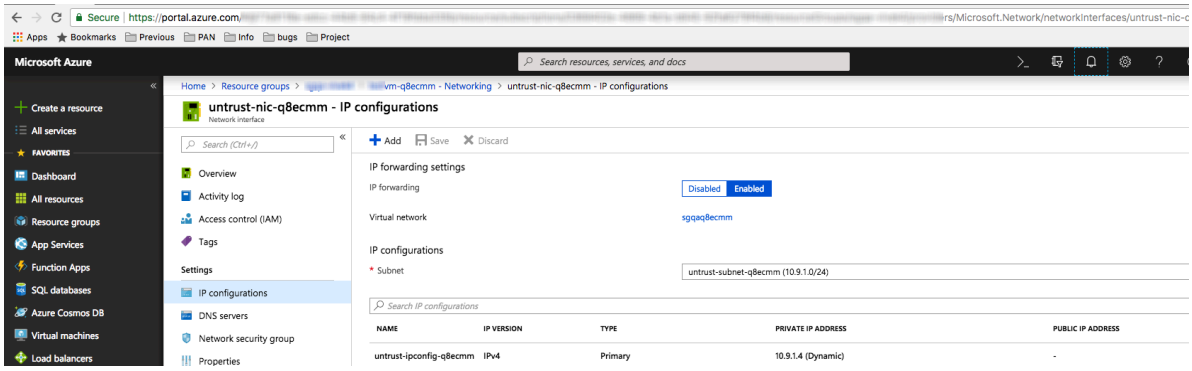
   En este flujo de trabajo, este cortafuegos se designará como el miembro activo. El miembro de HA activo tiene un valor numérico más bajo para prioridad del dispositivo que configura como parte de

 ©2024 Palo Alto Networks, Inc.

la configuración de HA en el cortafuegos, y este valor indica una preferencia por cuál cortafuegos asume el rol de equipo activo.



2. Añada una configuración de IP principal a la interfaz untrust (no confiable) del miembro activo del cortafuegos.

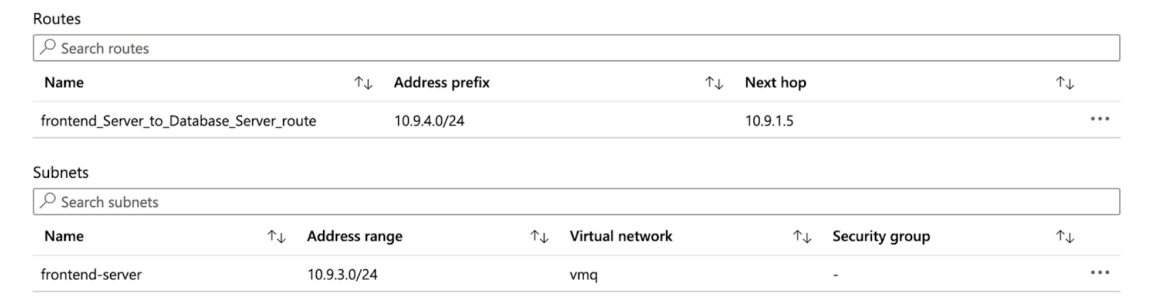


 ©2024 Palo Alto Networks, Inc.

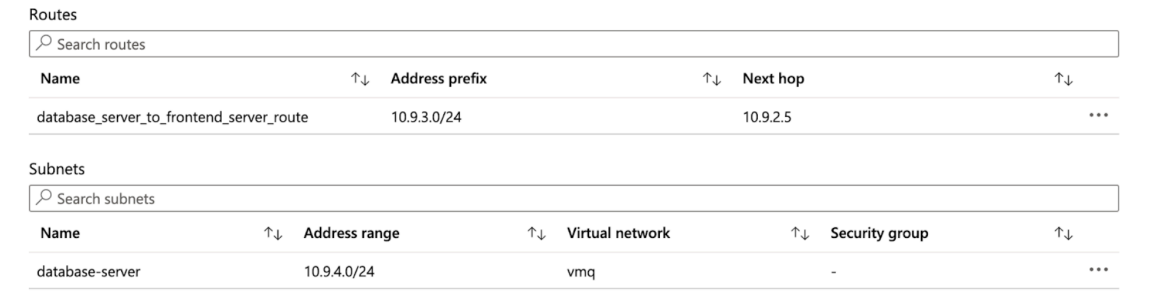
3. Conecte una interfaz de red para la comunicación HA2 entre los miembros HA del cortafuegos.
   1. Añada una subred dentro de la red virtual.
   2. Crear y adjuntar una interfaz de red al cortafuegos.
4. Establezca su tabla de rutas en Azure.

   Cree una ruta al siguiente salto de la dirección IP principal de las interfaces trust y untrust del miembro activo del cortafuegos.

Example with Frontend Server to Database Server Route :



Example with Database Server to Frontend Server route:



Después de la conmutación por error, el próximo salto para la ruta del servidor de la base de datos al servidor Frontend cambiará de 10.9.2.5 a 10.9.2.4. Del mismo modo, el próximo salto para la ruta del servidor Frontend al servidor de la base de datos cambiará de 10.9.1.5 a 10.9.1.4.

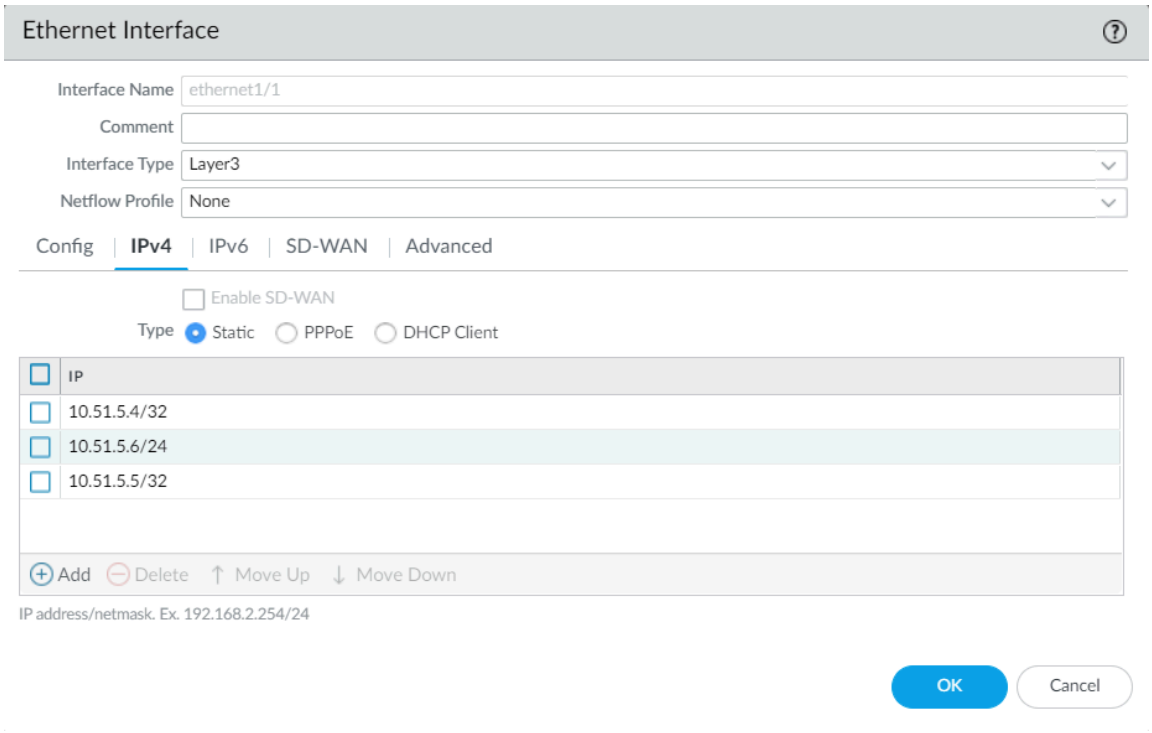
 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configure las interfaces en el cortafuegos.

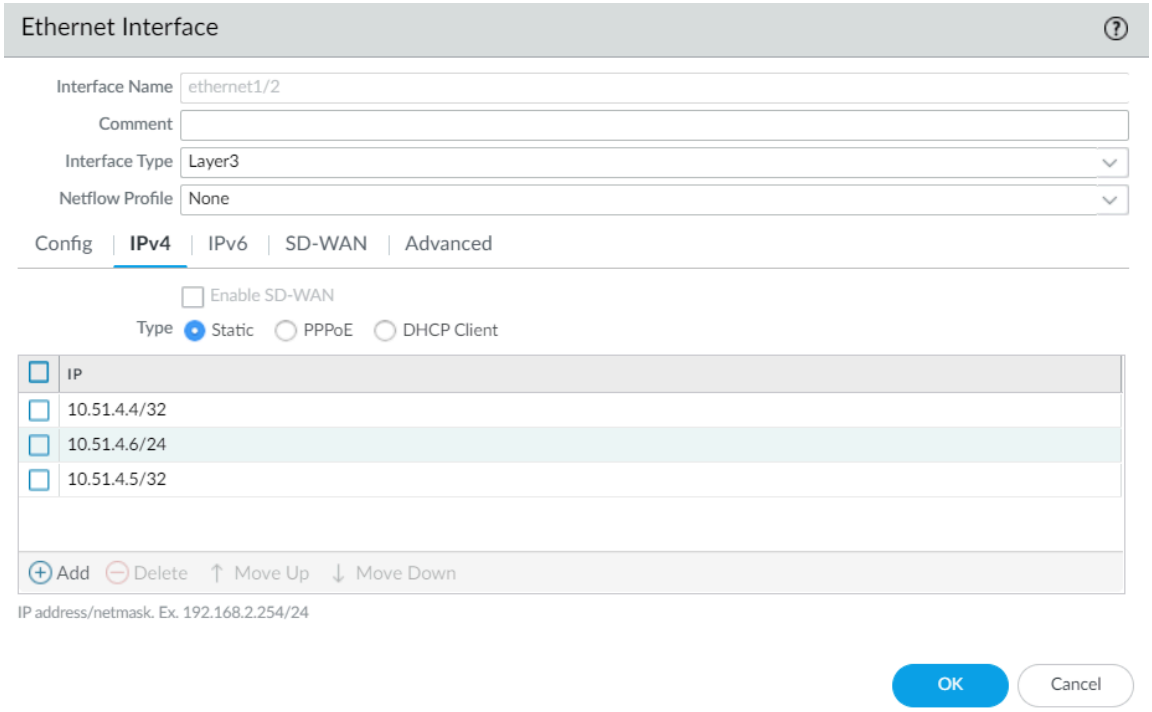
Complete estos pasos en el miembro de HA activo, antes de implementar y configurar el miembro de HA pasivo.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Configure ethernet 1/1 como la interfaz untrust y ethernet 1/2 como la interfaz untrust.

   Seleccione **Network (Red)** > **Interfaces** y configure de la siguiente forma:



 ©2024 Palo Alto Networks, Inc.



3. Configure ethernet 1/3 como la interfaz de HA.

   Para configurar el enlace HA2, seleccione la interfaz y establezca el **Interface Type (Tipo de interfaz)** en **AH**. Ajuste la velocidad del enlace y dúplex a automático.



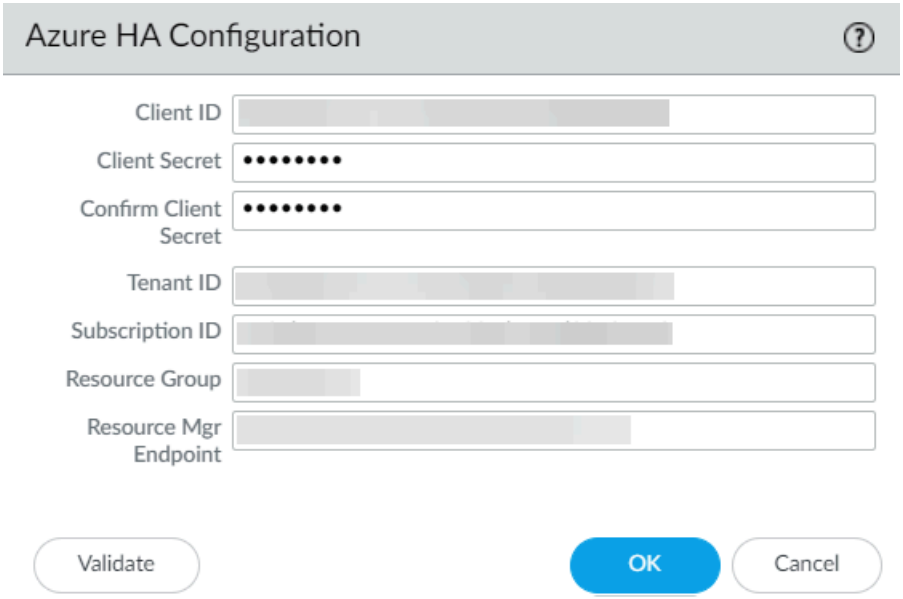
 ©2024 Palo Alto Networks, Inc.

STEP 3 | Configure el plugin VM-Series para autenticarse en el grupo de recursos de Azure en el que ha implementado el cortafuegos.

Configure la configuración de Azure HA en el plugin de VM-Series.

Para cifrar el secreto del cliente, use el plugin VM-Series versión 1.0.4 o posterior. Si usa Panorama para gestionar sus cortafuegos, debe instalar la versión 1.0.4 o posterior del plugin VM-Series.

1. Seleccione **Device (Dispositivo)** > **VM-Series** para habilitar el acceso programático entre el plugin del cortafuegos y los recursos de Azure.



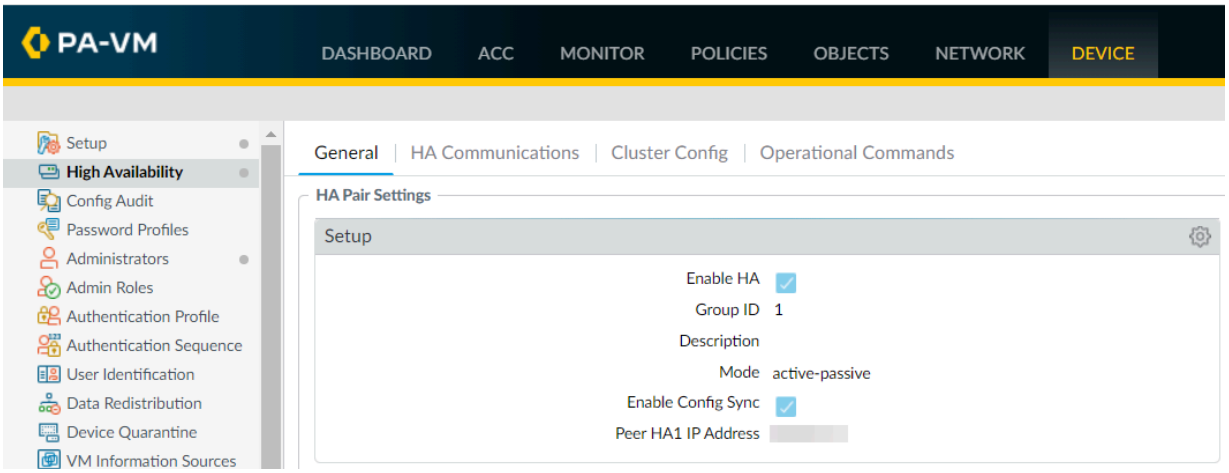
2. Introduzca la **Client ID (ID de cliente)**. La ID del cliente es la ID de la aplicación asociada a su aplicación de Azure Active Directory.
3. Introduzca el **Client Secret (Secreto del cliente)** y vuelva a introducirla para confirmarlo.
4. Introduzca la **Tenant ID (ID de inquilino)**. La ID de inquilino es la ID del directorio que guardó cuando configuró la aplicación de Active Directory.
5. Introduzca la **Subscription ID (ID de suscripción)** para la suscripción de Azure que desea supervisar.
6. Introduzca el nombre del **Resource Group (Grupo de recursos)**.
7. (Solo para implementaciones de Azure Stack) Introduzca la URL del **Resource Mgr Endpoint (Endpoint del gestor de recursos)**.

   Este campo está disponible en el complemento VM-Series 2.1.2 y posterior.

8. Haga clic en **Validate (Validar)** para comprobar que las claves y las ID que introdujo son válidas y que el plugin VM-Series se puede comunicar con los recursos de Azure usando la API.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Habilitar HA.



1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **HA**.
2. Introduzca la **Peer HA1 IP Address (Dirección IP de HA1 del peer)** como la dirección IP privada del equipo pasivo.
3. (Opcional) Edite el enlace de control (HA1). Si no planifica usar la interfaz de gestión para el enlace de control y ha añadido una interfaz adicional (por ejemplo, ethernet 1/4), edite esta sección para seleccionar la interfaz que se usará para la comunicación de HA1.
4. Edite el enlace de datos (HA2) para usar **Port (Puerto)** Ethernet 1/3 y añada la dirección IP de este equipo y la dirección IP de la **Gateway (Puerta de enlace)** para la subred.

STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 6 | Configure el miembro HA pasivo dentro del mismo Grupo de recursos de Azure.

1. Implemente la segunda instancia del cortafuegos.
   - Descargue la plantilla personalizada y el archivo de parámetros de GitHub.
   - Inicie sesión en el portal de Azure.
   - Busque la **custom template (plantilla personalizada)** y seleccione **Deploy from a custom template (Implementar desde una plantilla personalizada)**.
   - Seleccione **Build your own template in the editor (Crear su propia plantilla en el editor)** > **load File (Cargar archivo)**.
   - Seleccione el **azuredeploy.json** que descargó anteriormente, y seleccione **Save (Guardar)**.
   - Complete las entradas, acepte los términos y elija **Purchase (Comprar)**.

     Asegúrese de hacer coincidir las siguientes entradas con la de la instancia de cortafuegos que ya implementó: suscripción de Azure, nombre del grupo de recursos, ubicación del grupo de recursos, nombre de la red virtual existente en la que desea implementar el cortafuegos,

 ©2024 Palo Alto Networks, Inc.

VNet CIDR, Nombres de subred, CIDR de subred e inicie la dirección IP para las subredes de gestión, trust y untrust.

2. Repita el Paso 1 y Paso 2para configurar las interfaces y configurar el cortafuegos como el equipo HA pasivo.
3. Omita el Paso 3 y complete la Habilitación de HA (Paso 5). En Paso 4 modifique las direcciones IP según corresponda para este miembro HA pasivo.

STEP 7 | Cuando termine de configurar ambos cortafuegos, verifique que los dispositivos están emparejados en la HA activo/pasivo.

1. Acceda al **Dashboard** de ambos dispositivos y visualice el widget High Availability.
2. En el cortafuegos activo, haga clic en el enlace **Sync to peer**.
3. Confirme que los cortafuegos están emparejados y sincronizados, como se muestra a continuación:
   - En el cortafuegos pasivo: el estado del cortafuegos local debería mostrar **passive (pasivo)** y la **Running Config (Config. en ejecución)** debería mostrar **synchronized (sincronizada)**.
   - En el cortafuegos activo: El estado del cortafuegos local debería mostrar **active (activo)** y **Running Config (Config. en ejecución)** debería mostrar **synchronized (sincronizada)**.
4. En el equipo pasivo, verifique que la configuración del plugin VM-Series ahora esté sincronizada.

   Seleccione **Device (Dispositivo)** > **VM-Series** y valide que puede ver la configuración de Azure HA que había omitido durante la configuración del equipo pasivo.

 ©2024 Palo Alto Networks, Inc.

Utilice Azure Key Vault para almacenar certificados VM-Series

Puede integrar administradores de claves nativos de la nube para almacenar certificados. Las claves privadas utilizadas para los certificados no se almacenan en el disco duro de un cortafuegos, por lo que se eliminan los problemas de seguridad. Los administradores conservan los certificados y las claves privadas en el almacenamiento en la nube. El cortafuegos utiliza Azure Key Vault para recuperar los certificados y las claves privadas del almacenamiento en la nube y los usa para características como el descifrado e IPSec.

Solo se admiten cortafuegos VM-Series para habilitar la recuperación de certificados a través de Azure Key Vault. Si usa certificados de Key Vault, no puede cambiar a una versión anterior de PAN-OS.

Para el descifrado de entrada y salida, cargue los certificados en el administrador de claves nativo y proporcione los permisos de acceso necesarios al cortafuegos NGFW. Un NGFW en una nube pública puede usar Key Vault para almacenar certificados. En tales casos, se configuran las políticas de gestión de acceso necesarias, utilizando PAN-OS o la CLI, para las mismas instancias.

Para entornos que utilizan el escalado automático, una instancia se inicia en un estado con los certificados necesarios recuperados y lista para descifrar el tráfico sin configuración manual adicional.

Cuando un certificado se actualiza en la nube, debe volver a importarse como un nuevo certificado en el cortafuegos. Deberá asignar funciones de IAM a una instancia para permitir que la instancia recupere certificados del almacén de Azure Key Vault. La función de IAM debe tener el permiso **Obtener** para secretos en Azure Key Vault.

Puede recuperar certificados del almacén de certificados de Key Vault, no de su sección Secretos. PEM es el único formato compatible. PKCS12 o certificado encadenado no es compatible.

Todos los certificados se eliminan cuando cambia una clave maestra y luego se vuelven a recuperan al confirmar. Cuando la configuración se sincroniza con el cortafuegos pasivo en alta disponibilidad (HA), el daemon de administración descarga automáticamente el certificado en el cortafuegos pasivo. Como resultado, el certificado en sí no está sincronizado.

STEP 1 | Descargar un certificado.

STEP 2 | Cree un Key Vault en Azure en el mismo grupo de recursos donde está implementado su cortafuegos VM-Series. Utilice Key Vault donde almacenó el certificado (clave pública y privada) en formato PEM.

Cargue el certificado y la clave privada juntos en formato **.pem**.

STEP 3 | Después de crear Key Vault, en **Access Policies (Políticas de acceso)**, haga clic en **Create (Crear)** y añada la Identidad gestionada.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Vuelva a su grupo de recursos y seleccione el cortafuegos VM-Series. Haga clic en **Identity (Identidad) > User Assigned (Asignada por el usuario)** y añada la **Managed Identity (Identidad gestionada)**.

Los permisos en la identidad gestionada también se deben proporcionar a Key Vault.

STEP 5 | Vuelva a Key Vault y seleccione **Certificates (Certificados)**. Importe el archivo PEM de su certificado.

Los certificados deben permanecer en formato PEM en **Key Vault > Certificados**.

STEP 6 | Inicie sesión en al cortafuegos VM-Series.

STEP 7 | Seleccione **Device (Dispositivo) > Certificate Management (Gestión de certificados) > Certificates (Certificados) > Import (Importar)**.

Si desea importar un certificado **ECDSA**, modifique la clave privada:

----Begin EC PRIVATE KEY----

&

----END EC PRIVATE KEY----

Para

----BEGIN PRIVATE KEY----

&

----END PRIVATE KEY----

Si desea importar un certificado **PEM** , modifique la clave privada:

----BEGIN PRIVATE KEY----

&

----END PRIVATE KEY----

STEP 8 | En **Cloud (Nube)**, introduzca el nombre del certificado y establezca el formato de archivo en **PEM**.

STEP 9 | Seleccione **Cloud (Nube)** como **Tipo de certificado**, luego configure los siguientes campos:

1. Introduzca el **Certificate Name (Nombre del certificado)**; cópielo de Key Vault en el portal de Azure.
2. Seleccione **Azure** en el menú desplegable **Cloud Platform (Plataforma en la nube)**.
3. Introduzca el **Azure Key Vault URI (URI de almacén de claves de Azure)** para especificar la ubicación del almacén Key Vault; cópielo de Key Vault en el portal de Azure.
4. Introduzca el **Cloud Secret Name (Nombre secreto de la nube)**. Esto se usa para almacenar el certificado en Azure Key Vault.
5. Puede especificar el **Algorithm (Algoritmo)** en la pantalla de **Información del certificado**. Seleccione el algoritmo para su configuración, ya sea **RSA** o **DSA de curva elíptica**. De forma predeterminada, el algoritmo está configurado para utilizar **RSA**. Configure el certificado para

 ©2024 Palo Alto Networks, Inc.

usar el **Certificado de reenvío fiable**, **Certificado de reenvío no fiable**o **CA raíz de confianza**. De forma alternativa, puede seleccionar todos los algoritmos para el certificado.

6. Haga clic en **OK (Aceptar)**.
7. Confirme los cambios.

STEP 10 | Verifique que el certificado se haya añadido correctamente:

1. Seleccione **Device (Dispositivo) > Certificate Management (Gestión de certificados) > Certificates (Certificados)**.
2. Su nuevo certificado deberá aparecer en la lista.

Los detalles del certificado no se muestran en la pantalla **Certificates (Certificados)**

. Para ver esta información en la CLI, utilice el comando:

```
show shared certificate
```

<cert-name>

Puede confirmar la configuración de la integración de certificados en Panorama. Utilice la ventana **Certificado de dispositivo** para determinar si se utiliza el certificado. Tenga en cuenta que debido a que los datos no se almacenan en la configuración en curso (el disco duro), todos los campos de la tabla **Certificados de dispositivos** están vacíos, excepto el campo **Uso** (si está configurado) y el **Nombre secreto de la nube**.

 ©2024 Palo Alto Networks, Inc.

Uso de la plantilla ARM para implementar el cortafuegos VM-Series

Además de las implementaciones basadas en Marketplace, Palo Alto Networks proporciona un repositorio GitHub que aloja muestras de plantillas ARM que se pueden descargar y personalizar para sus necesidades. Las plantillas ARM son archivos JSON que describen los recursos necesarios para recursos individuales, tales como interfaces de red, una máquina virtual completa o, incluso, una pila de aplicaciones completa con múltiples máquinas virtuales.

Las plantillas ARM son para usuarios avanzados y Palo Alto Networks proporciona la plantilla ARM bajo la política admitida por la comunidad. Para obtener información sobre las plantillas ARM, consulte la documentación de Microsoft sobre plantillas ARM.

Para simplificar la implementación de todos los recursos necesarios, la plantilla de muestra de dos niveles (https://github.com/PaloAltoNetworks/azure/tree/master/two-tier-sample) incluye dos archivos json:

- **Archivo de plantilla**: El azureDeploy.json es el recurso principal que implementa todos los componentes dentro del grupo de recursos.
- **Archivo de parámetros**: azureDeploy.parameters.json es el archivo que incluye los parámetros necesarios para implementar con éxito el cortafuegos VM-Series en la VNet. Incluye detalles como el nivel y tamaño de la máquina virtual, el nombre de usuario y la contraseña para el cortafuegos, el nombre del contenedor de almacenaje para el cortafuegos. Puede personalizar este archivo para su implementación de Azure VNet.

Para ayudarle a implementar el cortafuegos como una puerta de enlace para aplicaciones orientadas a internet, la plantilla proporciona el cortafuegos VM-Series, un servidor de base de datos y un servidor web. La VNet utiliza el espacio de dirección IP no enrutable privado 192.168.0.0/16. Puede modificar la plantilla para usar 172.16.0.0/12, o 10.0.0.0/8.

La plantilla ARM también proporciona las reglas definidas por el usuario necesarias y las marcas de envío de IP para permitir que el cortafuegos VM-Series proteja el grupo de recursos de Azure. Para las cinco subredes: Fiable, No fiable, Web, DB y NAT, incluidas en la plantilla, hay cinco tablas de rutas, una para cada subred con reglas definidas por el usuario para la transmisión de tráfico al cortafuegos VM-Series y la máquina virtual NAT.

Para las cuatro subredes —Fiable, No fiable, Web y DB— incluidas en la plantilla, hay cuatro tablas de rutas, una para cada subred con reglas definidas por el usuario para dirigir el tráfico al cortafuegos VM-Series.

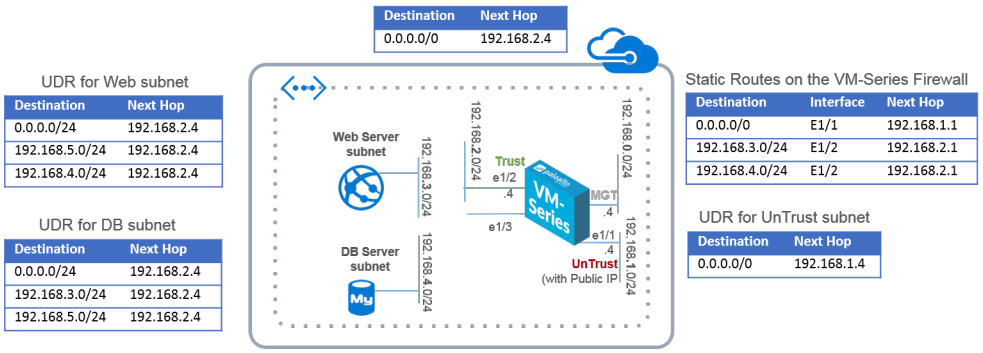


Figure 4: Implementación del cortafuegos VM-Series con la plantilla ARM

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Descargue la plantilla ARM de muestra de dos niveles del repositorio GitHub.

Descargue y guarde los archivos en un cliente local: https://github.com/PaloAltoNetworks/azure/tree/master/two-tier-sample

STEP 2 | Cree un Grupo de recursos en Azure..

1. Inicie sesión en la CLI de Azure con el comando: **`az login`**

   Si necesita ayuda, consulte la documentación de Azure sobre la instalación de la CLI, o para obtener detalles sobre cómo acceder a la CLI en Azure Government o Azure China.
2. Cree un grupo de recursos.

STEP 3 | Implemente la plantilla ARM.

1. Abra el archivo de parámetros con un editor de texto y modifique los valores para su implementación:

   *En Azure China, debe editar la ruta de la cuenta de almacenamiento que aloja la imagen VHD requerida para implementar el cortafuegos VM-Series. En la sección de variables del archivo de plantilla, busque el parámetro llamado **userImageNameURI** y sustituya el valor con la ubicación donde guardó la imagen VHD.*
2. Implemente la plantilla en el grupo de recursos creado.

   ```
   az deployment group create --name <YourResourceGroupName> --
   resource-group <YourResourceGroupName> --parameters '@<path-
   to-template-parameter-azureDeploy.json>'
   ```
3. Compruebe el progreso/estado de la implementación desde la CLI de Azure:

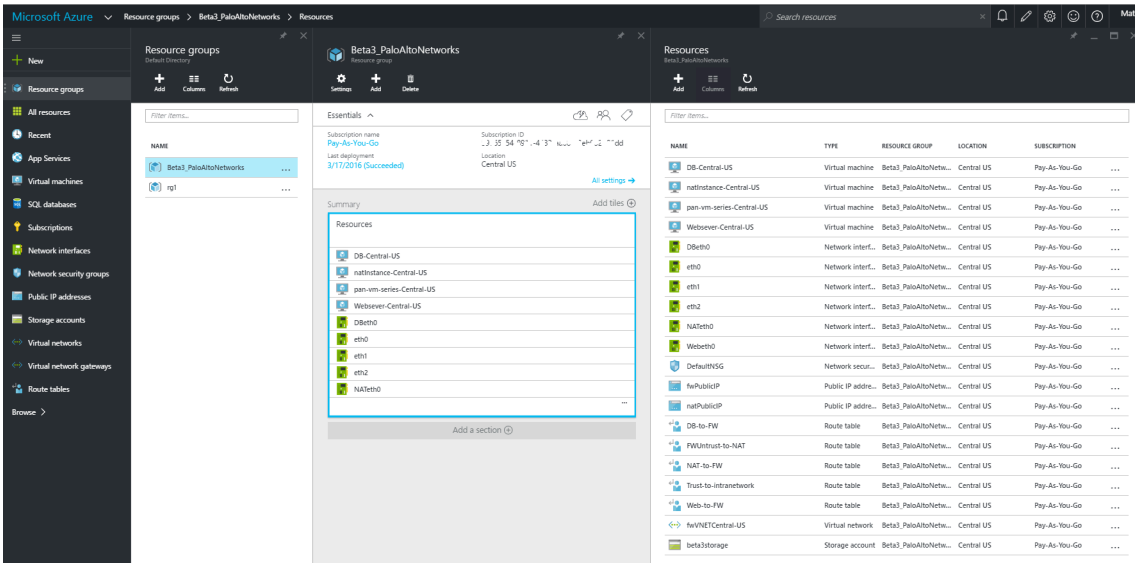
   ```
   azure deployment group show <YourResourceGroupName>
   ```

 ©2024 Palo Alto Networks, Inc.

Cuando se ha implementado la plantilla correctamente, el `ProvisioningState está ejecutándose`.

*Si `ProvisioningState ha fallado`, debe comprobar los errores en el portal de Azure en **Resource Group (Grupo de recursos)** > **Events (Eventos)** Filtre solamente los eventos de la última hora, seleccione los eventos más recientes, y explore para encontrar los errores.*

4. Verifique que se ha implementado con éxito el cortafuegos VM-Series.
   1. Seleccione **Dashboard (Panel)** > **Resource Groups (Grupo de recursos)**, seleccione el grupo de recursos.
   2. Seleccione en **All Settings (Todos los ajustes)** > **Deployments (Implementaciones)** > **Deployment History (Historial de implementaciones)** para el estado detallado.



El espacio de la dirección en VNet utiliza el prefijo 192.168, que se define en la plantilla ARM.

5. Adjunte una dirección IP pública a la interfaz de no fiable en el cortafuegos.

STEP 4 | Configure el cortafuegos como puerta de enlace de VNet para proteger su implementación con conexión a Internet.

1. Inicie sesión en la dirección IP de la interfaz de gestión del cortafuegos.
2. Configure las interfaces de red del plano de datos como interfaces de Capa 3 en el cortafuegos (**Network (Red)** > **Interfaces** > **Ethernet**).
3. Añada reglas estáticas al enrutador virtual del cortafuegos. Para dirigir el tráfico a través del cortafuegos en este ejemplo, necesita tres rutas estáticas en el cortafuegos (**Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, seleccione el enrutador y haga clic en **Static Routes (Rutas estáticas)**:
   1. Dirija todo el tráfico saliente través de la zona No fiable, ethernet1/1 al enrutador de Azure en 192.168.1.1.

 ©2024 Palo Alto Networks, Inc.

2. Dirija todo el tráfico entrante destinado a la subred del servidor web través de la zona Fiable, ethernet1/2 al enrutador de Azure en 192.168.2.1.
3. Dirija todo el tráfico entrante destinado a la subred del servidor de base de datos a través de la zona Fiable, ethernet1/2 al enrutador de Azure en 192.168.2.1.

4. Cree reglas de política de seguridad (**Policies (Políticas)** > **Security (Seguridad)**) para permitir el tráfico entrante y saliente del cortafuegos. También necesita reglas de política de seguridad para permitir el tráfico apropiado de la subred de servidor web a la subred de servidor de base de datos y viceversa.
5. Haga clic en **Commit (Confirmar)** para confirmar los cambios en el cortafuegos.
6. Compruebe que el cortafuegos VM-Series está protegiendo el tráfico [**Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)**].

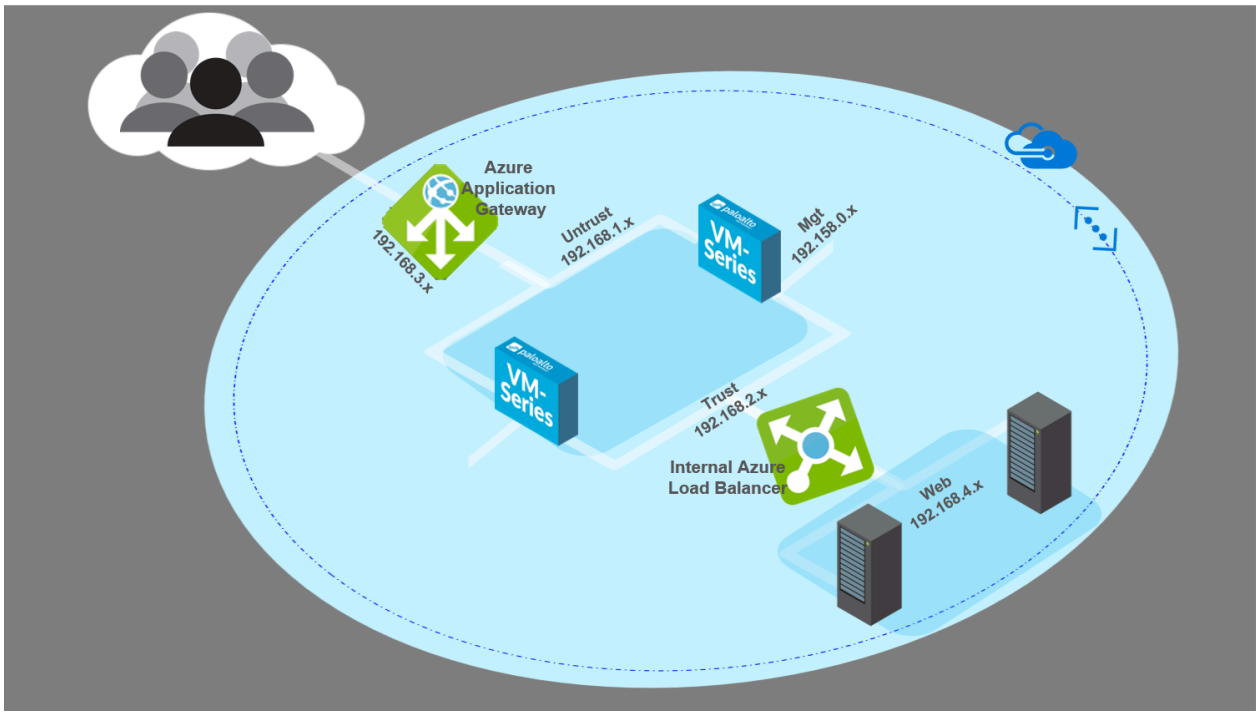
 ©2024 Palo Alto Networks, Inc.

Implementación de la plantilla VM-Series y Azure Application Gateway

La plantilla VM-Series y Azure Application Gateway es un kit de inicio que puede usar para implementar cortafuegos VM-Series para asegurar cargas de trabajo web para implementaciones orientadas a Internet en Microsoft Azure (actualmente no disponible para Azure China).

Esta plantilla implementa dos cortafuegos VM-Series entre un par de balanceadores de carga Azure (externos e internos). El balanceador de carga externo es una Azure Application Gateway, que es un balanceador de carga HTTP (Capa 7) que también sirve como puerta de enlace orientada a Internet, que recibe tráfico y lo distribuye a través del cortafuegos VM-Series en el balanceador de carga interno. El balanceador de carga interno es un balanceador Azure Load Balancer (Capa 4) que enfrenta a un par de servidores web. La plantilla es compatible con las versiones de BYOL y Azure Marketplace del cortafuegos VM-Series.

A medida que aumenta la demanda en sus cargas de trabajo web y usted aumenta la capacidad para el nivel del servidor web, puede implementar manualmente cortafuegos VM-Series adicionales para proteger su nivel de servidor web.

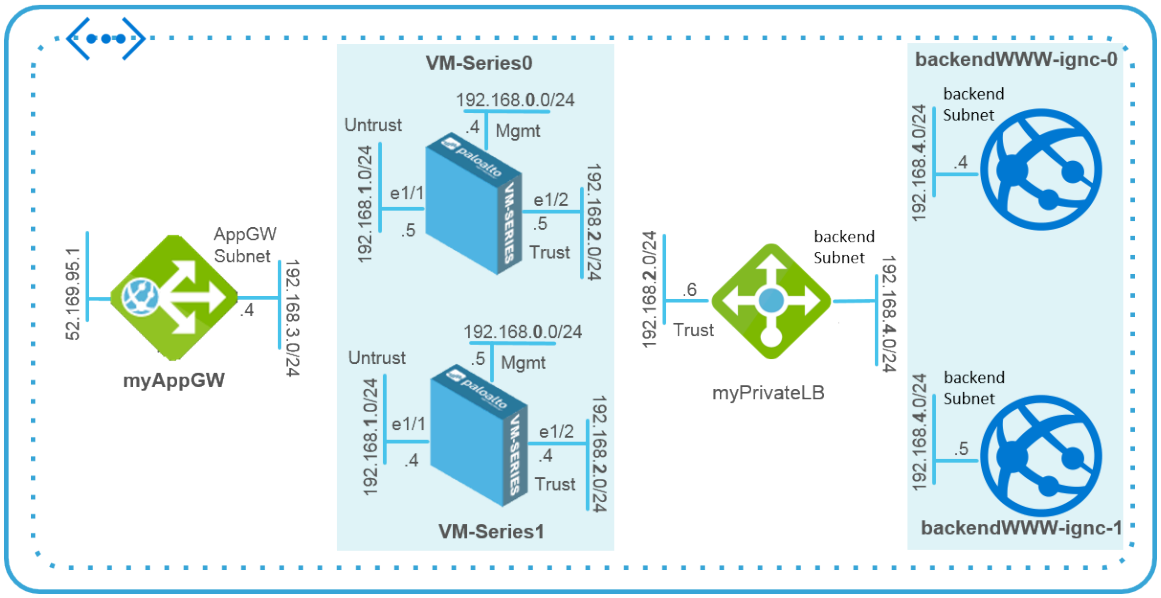


- Plantilla VM-Series y Azure Application Gateway
- Comience a usar la plantilla VM-Series y Azure Application Gateway

 ©2024 Palo Alto Networks, Inc.

Plantilla VM-Series y Azure Application Gateway

La plantilla VM-Series y Azure Application Gateway ejecuta Azure Application Gateway (balanceador de carga de Capa 7) y un balanceador de carga de Azure (Capa 4). Un par de cortafuegos VM-Series en un conjunto de disponibilidad y un par de servidores web de muestra que ejecutan Apache2 en Ubuntu de otro conjunto de disponibilidad están anidados entre la puerta de enlace de la aplicación y el balanceador de carga. Los conjuntos de disponibilidad brindan protección contra interrupciones planificadas y no planificadas. El siguiente diagrama de topología muestra los recursos que implementa la plantilla:



Puede usar una cuenta de almacenamiento nueva o una existente y un grupo de recursos en el cual implementar todos los recursos para esta solución dentro de una ubicación de Azure. No proporciona valores predeterminados para el nombre del grupo de recursos y el nombre de la cuenta de almacenamiento, debe introducir un nombre para ellos. A pesar de que puede crear una nueva o utilizar una red virtual existente, la plantilla crea una red virtual predeterminada llamada *vnet-FW* con el bloque CIDR 192.168.0.0/16, y asigna cinco subredes (192.168.1.0/24 - 192.168.5.0/24) para implementar Azure Application Gateway, los cortafuegos VM-Series, el balanceador de carga Azure y los servidores web. Cada cortafuegos VM-Series se implementa con tres interfaces de red: ethernet0/1 en la subred Gestión (192.168.0.0/24), ethernet1/1 en la subred Untrust (192.168.1.0/24) y ethernet1/2 en la subred Trust (192.168. 2.0 / 24).

La plantilla crea un Grupo de seguridad de red (NSG) que permite el tráfico entrante desde cualquier dirección IP de origen en los puertos 80, 443 y 22. También implementa el par de cortafuegos VM-Series y el par de servidores web en sus respectivos Conjuntos de disponibilidad para garantizar que al menos una instancia de cada uno esté disponible durante un periodo de mantenimiento planificado o no planificado. Cada conjunto de disponibilidad está configurado para usar tres dominios de fallos y cinco dominios de actualización.

Azure Application Gateway actúa como un servicio de proxy inverso, que finaliza una conexión de cliente y reenvía las solicitudes a los servidores web de backend. Azure Application Gateway está configurado con un escucha HTTP y utiliza una sonda de estado predeterminada para comprobar que la dirección IP del cortafuegos VM-Series (para ethernet1/1) es saludable y puede recibir tráfico.

 ©2024 Palo Alto Networks, Inc.

La plantilla no proporciona una solución de escalado automático; debe planificar sus necesidades de capacidad y luego desplegar recursos adicionales para Adaptación de la plantilla *para su implementación.*

Los cortafuegos VM-Series no están configurados para recibir y asegurar el tráfico web destinado a los servidores web. Por lo tanto, como mínimo, debe configurar el cortafuegos con una ruta estática para enviar tráfico desde los cortafuegos VM-Series al enrutador predeterminado, configurar la política NAT de destino para devolver el tráfico a la dirección IP del balanceador de carga y configurar la reglas de políticas de seguridad. La regla de políticas NAT también es necesaria para que el cortafuegos envíe respuestas a las sondas de estado de la escucha HTTP en Azure Application Gateway. Para ayudarlo con una configuración básica del cortafuegos, el repositorio GitHub incluye un archivo de configuración de muestra llamado *appgw-sample.xml* que puede usar para comenzar.

Comience a usar la plantilla VM-Series y Azure Application Gateway

La Plantilla VM-Series y Azure Application Gateway inicia todos los recursos que necesita para implementar y proteger sus cargas de trabajo web para las implementaciones de Internet en Microsoft Azure, excepto Azure China. Esta sección proporciona detalles sobre cómo implementar la plantilla, configurar los cortafuegos para el enrutamiento y proteger el tráfico destinado a los servidores web, y ampliar las capacidades y recursos que esta plantilla proporciona para satisfacer sus necesidades de implementación.

- Implementación de la plantilla en Azure
- Parámetros de la plantilla serie VM y Azure Application Gateway
- Archivos de configuración de muestra
- Adaptación de la plantilla

Comience a usar la plantilla y Azure Application Gateway

¿Dónde puedo usar esto?	¿Qué necesito?
• Microsoft Azure • Microsoft Azure Stack • Azure® Marketplace • Azure Government Marketplace	❑ Licencia de (PAYG o BYOL) ❑ Complemento de ❑ Panorama ❑ Complemento de Panorama para Azure.

La plantilla de y Azure Application Gateway inicia todos los recursos que necesita para implementar y proteger sus cargas de trabajo web para las implementaciones de Internet en Microsoft Azure, excepto Azure China. Esta sección proporciona detalles sobre cómo implementar la plantilla, configurar los cortafuegos para el enrutamiento y proteger el tráfico destinado a los servidores web, y ampliar las capacidades y recursos que esta plantilla proporciona para satisfacer sus necesidades de implementación.

Implementación de la plantilla en Azure

Use las siguientes instrucciones para implementar la plantilla en Azure.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Implemente la plantilla.

Actualmente no está disponible para la implementación en Azure China.

1. Acceda a la plantilla desde https://github.com/PaloAltoNetworks/azure-applicationgateway
2. Haga clic en **Deploy to Azure (Implementar en Azure)**.
3. Complete los detalles para implementar la plantilla. Consulte Parámetros de la plantilla y Azure Application Gateway para una descripción y los valores predeterminados, si los hay, para cada parámetro.

   Como mínimo, debe elegir la **Azure Subscription (Suscripción Azure)**, **Resource Group (Grupo de recursos)**, **Location (Ubicación)**, **Storage Account Name (Nombre de la cuenta**

 ©2024 Palo Alto Networks, Inc.

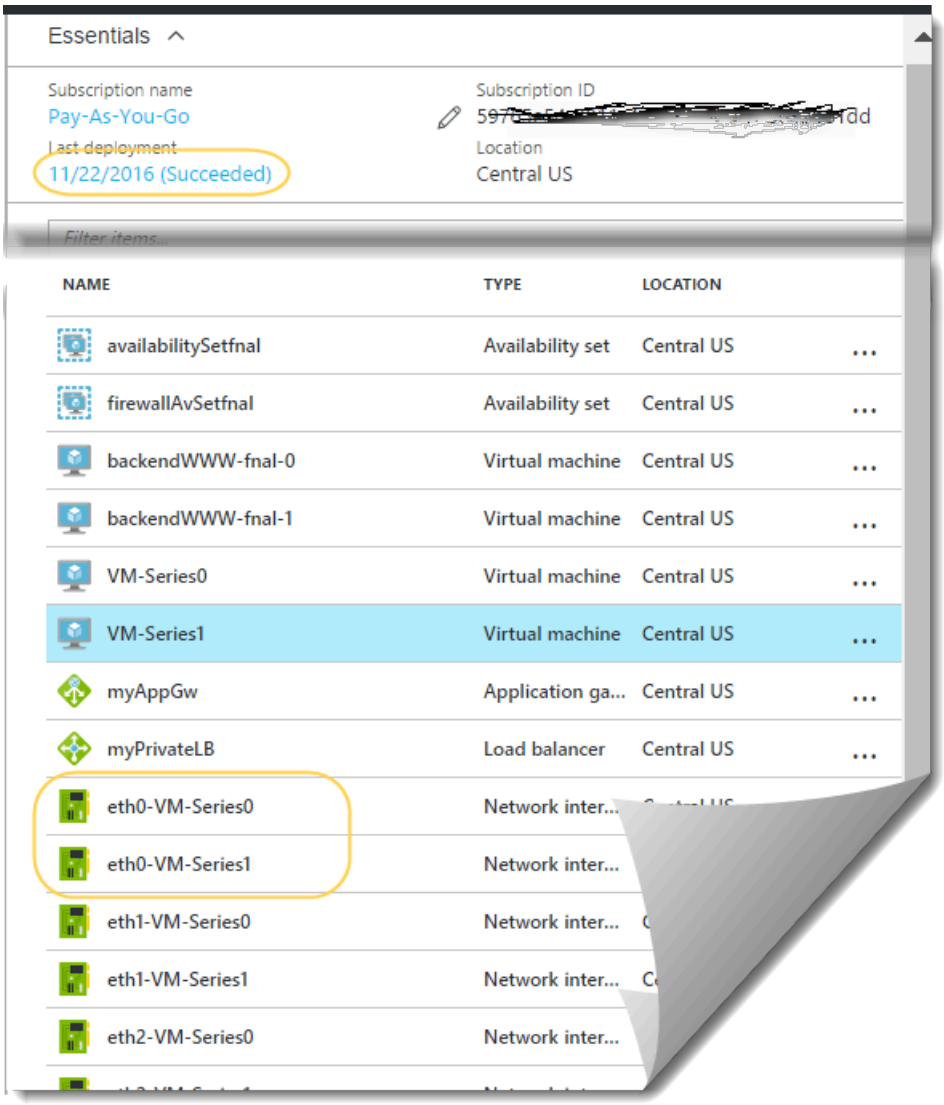
de almacenamiento)y **Username/password (Nombre de usuario y contraseña)** o **SSH Key (Clave SSH)** para la cuenta administrativa en los cortafuegos .

4. Haga clic en **Purchase (Comprar)** para aceptar los términos e implementar los recursos.

   Si se presentan errores de validación, haga clic para ver los detalles y corregirlos.

5. En el Portal de Azure, verifique que haya implementado con éxito los recursos de la plantilla, incluidos los cortafuegos .

   1. Seleccione **Dashboard (Panel)** > **Resource Groups (Grupo de recursos)**, seleccione el grupo de recursos.
   2. Seleccione **Overview (Descripción general)** para revisar todos los recursos que se han implementado. El estado de implementación debería mostrar **Succeeded (Realizado)**.



   3. Tenga en cuenta la dirección IP pública o el nombre DNS asignado a **eth0-VM-Series0** y **eth0-VM-Series1** para acceder a la interfaz de gestión de los cortafuegos .

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Inicie sesión en los cortafuegos.

1. Utilizando una conexión segura (HTTPS) desde su navegador web, inicie sesión en la dirección IP de eth0-0 o el nombre de DNS para el cortafuegos.
2. Introduzca el nombre de usuario/contraseña definido en el archivo de parámetros. Verá una advertencia de certificación; es normal. Vaya a la página web.

STEP 3 | Configure el cortafuegos .

Puede configurar el cortafuegos manualmente o importar el Archivo de configuración de muestra proporcionado en el Repositorio GitHub y personalícelo de acuerdo a sus necesidades de seguridad.

- **Configure el cortafuegos manualmente**: Debes hacer lo siguiente como mínimo:

1. Configure las interfaces de red del plano de datos como interfaces de Capa 3 en el cortafuegos (**Network (Red)** > **Interfaces** > **Ethernet**).
2. Añada una regla estática al enrutador virtual en el cortafuegos. Esta regla estática especifica la dirección IP de la interfaz no fiable del cortafuegos como la dirección de siguiente salto para cualquier tráfico destinado a ethernet1 / 1. (**Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, seleccione el enrutador y haga clic en **Static Routes (Rutas estáticas**).
3. Cree reglas de política de seguridad (**Policies (Políticas)** > **Security (Seguridad)**) para permitir el tráfico entrante y saliente del cortafuegos.
4. Añada políticas NAT (**Policies (Políticas)** > **NAT**). Cree NAT de destino y reglas NAT de origen en el cortafuegos para enviar tráfico a los servidores web y de vuelta al cliente que inició la solicitud.

   La regla NAT de destino es para todo el tráfico que llega a la interfaz No fiable del cortafuegos. Esta regla traduce la dirección IP de destino en el paquete a la del balanceador de carga interno, de modo que todo el tráfico se dirige al balanceador de carga interno y en los servidores web de backend.

   La regla NAT de origen es para todo el tráfico del servidor web de backend y destinada a la interfaz No fiable en el cortafuegos. Esta regla traduce la dirección de origen a la dirección IP de la interfaz trust en el cortafuegos.
5. **Commit (Confirmar)** los cambios.

   - **Importe el archivo de configuración de muestra:**
6. Descargue y guarde el Archivo de configuración de muestra en un cliente local.
7. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**, haga clic en **Import named configuration snapshot (Importar instantánea de configuración con**

 ©2024 Palo Alto Networks, Inc.

nombre), seleccione **Browse (Examinar)** para buscar el archivo de configuración de muestra que ha guardado a nivel local y haga clic en **OK (Aceptar)**.

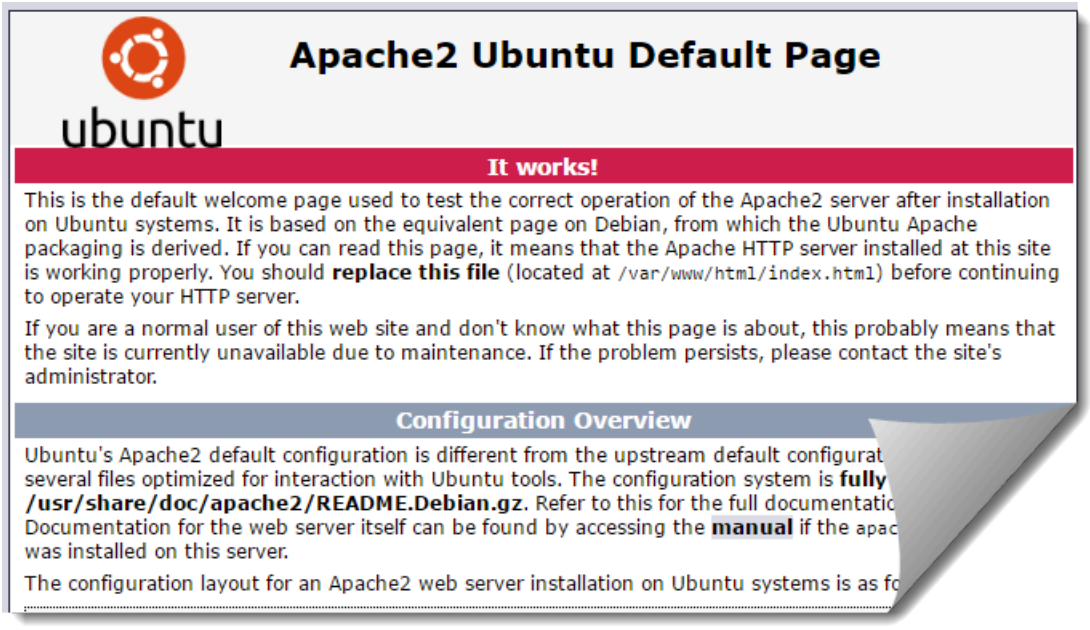
8. Haga clic en **Load named configuration snapshot (Cargar instantánea de configuración con nombre)**, seleccione el **Name (Nombre)** del archivo de configuración de muestra que ha importado y haga clic en **OK (Aceptar)**.
9. Cambie la dirección IP de los objetos de dirección y la ruta estática para que coincida con la dirección IP del bloque CIDR que utilizó. Actualice los objetos de dirección para usar las direcciones IP privadas para eth1-0 y eth1-1.
10. Importante Cree una nueva cuenta de usuario administrador. Seleccione **Device (Dispositivo)** > **Administrators (Administradores)** y seleccione **Add (Añadir)** una nueva cuenta.
11. Modifique el **Hostname (Nombre de host)** en el widget Configuración general en **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Administración)**.
12. Seleccione **Commit (Confirmar)** sus cambios y cierre la sesión. La confirmación sobrescribe la configuración en ejecución con el archivo de configuración de muestra y las actualizaciones que acaba de realizar. Al confirmar, el nombre de host y la cuenta de usuario administrativo que especificó al implementar la plantilla se sobrescriben. Ahora deberá iniciar sesión utilizando la nueva cuenta de usuario y contraseña de administrador.
    - **Inicie sesión en el cortafuegos**: Utilice las credenciales que creó y elimine la cuenta administrativa "pan demo" importada como parte del archivo de configuración de muestra.

STEP 4 | Inicie sesión y configure la otra instancia del cortafuegos .

Consulte el paso Configurar el cortafuegos .

STEP 5 | Verifique que haya configurado los cortafuegos correctamente.

Desde su navegador web, use HTTP para acceder a la dirección IP o nombre DNS de la puerta de enlace de la aplicación. Debería poder ver la página web predeterminada de Apache 2 Ubuntu.



Si ha utilizado el cortafuegos de la configuración de muestra, inicie sesión en el cortafuegos y vea los Logs de tráfico generados al iniciar la sesión en **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)**.

 ©2024 Palo Alto Networks, Inc.

Parámetros de la plantilla serie VM y Azure Application Gateway

La siguiente tabla detalla los parámetros requeridos y opcionales y los valores predeterminados, si los hubiera.

Parámetros	Description (Descripción)
Grupo de recursos	Crear nuevo o usar existente (sin predeterminado).
Suscripción	El tipo de suscripción de Azure que usará para cubrir el coste de los recursos implementados con la plantilla.
Ubicación	Seleccione la ubicación de Azure a la que desea implementar la plantilla (sin predeterminada).
Grupo de seguridad de red	
Nombre de grupo de seguridad de red	El grupo de seguridad de red limita las direcciones IP de origen a partir de las cuales se puede acceder a los cortafuegos y servidores web VM-Series. Valor predeterminado: nsg-mgmt
Grupo de seguridad de redes: IP de orig. entrante	Las direcciones IP de origen que pueden iniciar sesión en el puerto de gestión de las VM implementadas por la plantilla. El valor predeterminado 0.0.0.0/0 significa que puede iniciar sesión en el puerto de administración del cortafuegos desde cualquier dirección IP.
Cuenta de almacenamiento	
Nombre de la cuenta de almacenamiento	Cree un nuevo o introduzca el nombre de una cuenta de almacenamiento existente (sin valor predeterminado). El nombre debe ser totalmente único.
Tipo de la cuenta de almacenamiento	Elija entre almacenamiento estándar y premium y sus necesidades de replicación de datos para la redundancia local, redundancia de zona y redundancia geográfica con acceso de lectura. La opción predeterminada es almacenamiento con redundancia local (LRS). Las otras opciones son Standard GRS, Premium LRS y Standard RAGRS.
VNet	
Red virtual	Cree una nueva o introduzca el nombre de una red virtual existente. El nombre predeterminado para la VNet es vnet-FW
Prefijo de dirección de red virtual	192.168.0.0/16

 ©2024 Palo Alto Networks, Inc.

Parámetros	Description (Descripción)
Azure Application Gateway	
Nombre de puerta de enlace de la aplicación	myAppGw
Nombre DNS de la puerta de enlace de la aplicación	Introduzca un nombre DNS global único para Azure Application Gateway.
Nombre y prefijo de la subred de la puerta de enlace de la aplicación	El nombre predeterminado es AppGWSubnet y el prefijo de la subred es 192.168.3.0/24.
balanceador de carga Azure y servidores web	
Nombre del balanceador de carga interno	myPrivateLB
Nombre y prefijo de la subred del balanceador de carga interno	El nombre predeterminado es backendSubnet y el prefijo de subred es 192.168.4.0/24.
Tamaño de VM de Backend	El tamaño predeterminado es la VM Azure estándar de nivel D1. Use el menú desplegable de la plantilla para ver las otras opciones de Azure VM disponibles para los servidores web de backend.
Cortafuegos	
Modelo de cortafuegos	Elija entre BYOL o PAYG (paquete 1 o paquete 2, cada paquete incluye el VM-300 y un conjunto de suscripciones).
Nombre y tamaño de cortafuegos VM	El nombre predeterminado para el cortafuegos es VM-Series, y el tamaño predeterminado es D3 Azure VM de nivel estándar. Use el menú desplegable en la plantilla para ver las otras opciones de Azure VM disponibles para los cortafuegos VM-Series
Nombre y prefijo de la subred de gestión	La subred de administración para los cortafuegos VM-Series y los servidores web implementados en esta solución. El nombre predeterminado es Mgmt y el prefijo de la subred es 192.168.0.0/24.
Nombre de la dirección IP pública de Mgmt	Introduzca un nombre de host para acceder a la interfaz de administración en cada cortafuegos. Los nombres deben ser globalmente únicos.

 ©2024 Palo Alto Networks, Inc.

Parámetros	Description (Descripción)
Nombre y prefijo de subred Fiable	La subred a la que eth1/1 en el cortafuegos VM-Series está conectado; esta subred conecta el cortafuegos VM-Series a la puerta de enlace de la aplicación Azure. El cortafuegos recibe tráfico web destinado a los servidores web en eth1/1. El nombre predeterminado es Fiable y el prefijo de la subred es 192.168.2.0/24.
Nombre de subred No fiable	La subred a la que se conecta eth1/2 en el cortafuegos VM-Series. El cortafuegos recibe tráfico web de ida y vuelta en esta interfaz. El nombre predeterminado es No fiable y el prefijo de la subred es 192.168.1.0/24. El nombre debe ser totalmente único.
Nombre de usuario	Introduzca el nombre de usuario para la cuenta administrativa en los cortafuegos VM-Series y los servidores web.
Tipo de autenticación	Debe introducir una contraseña para autenticación o usar una clave pública SSH (no predeterminada).

Archivos de configuración de muestra

Para ayudarle a comenzar, el Repositorio GitHub contiene un archivo de configuración de muestra llamado *appgw-sample.xml* que incluye las siguientes reglas/objetos:

- **Objetos de dirección**: Dos objetos de dirección, `firewall-untrust-IP` y `internal-load-balancer-IP`, que deberá modificar para que coincidan con las direcciones IP en su configuración. Debe modificar estos objetos de dirección para usar las direcciones IP privadas asignadas a eth1-VM-Series0 y eth1-VM-Series1 en el portal de Azure.
- **Ruta estática**: El enrutador virtual predeterminado en el cortafuegos tiene una ruta estática a 192.168.1.1 y esta dirección IP es precisa si usa los valores predeterminados de la plantilla. Si ha cambiado el CIDR de la subred No fiable, deberá actualizar la dirección IP para que coincida con su configuración. Todo el tráfico proveniente de los servidores web de backend, destinados a la puerta de enlace de la aplicación, usa esta dirección IP como el siguiente salto para entregar paquetes a la interfaz no fiable en el cortafuegos.
- **Regla de políticas NAT**: La regla de políticas NAT habilita NAT de destino y NAT de origen.
  - La regla de NAT de destino es para todo el tráfico que llega a la interfaz no fiable del cortafuegos (ethernet1 / 2), que es el objeto de dirección IP no fiable del cortafuegos. Esta regla traduce la dirección IP de destino en el paquete a la del balanceador de carga interno, de modo que todo el tráfico se dirige al balanceador de carga interno y, por lo tanto, a los servidores web de backend.
  - La regla NAT de origen es para todo el tráfico del servidor web backend y está destinada a la interfaz de red no fiable en el cortafuegos. Esta regla traduce la dirección de origen a la dirección IP de la interfaz fiable en el cortafuegos (ethernet1 / 2).
- **Regla de políticas de seguridad**: Dos reglas de políticas de seguridad se definen en el archivo de configuración de muestra. La primera regla permite todo el tráfico entrante de navegación web y genera un log al inicio de una sesión en el cortafuegos. La segunda regla bloquea el resto del tráfico y genera

 ©2024 Palo Alto Networks, Inc.

un log al inicio y al final de una sesión en el cortafuegos. Puede usar estos logs para supervisar todo el tráfico a los servidores web en esta implementación.

- **Credenciales del usuario administrativo**: El archivo de configuración de muestra incluye un nombre de usuario y contraseña para iniciar sesión en el cortafuegos, que está configurado como pandemo/demopassword. Después de importar la configuración de muestra, debe cambiar la contraseña por una contraseña fuerte y personalizada o crear una nueva cuenta de administrador y eliminar la cuenta pandemo.

Adaptación de la plantilla

A medida que evolucionan sus necesidades, puede definir sus necesidades de capacidad y ampliar la plantilla para su escenario de implementación. Estas son algunas maneras de desarrollar la plantilla inicial para satisfacer sus necesidades de capacidad planificadas:

- Implemente cortafuegos VM-Series adicionales detrás de Azure Application Gateway. Puede instalar manualmente más cortafuegos VM-Series en el mismo conjunto de disponibilidad o iniciar un nuevo conjunto de disponibilidad e implementar manualmente cortafuegos VM-Series adicionales.
- Configure los cortafuegos VM-Series más allá de la configuración básica proporcionada en el archivo de configuración de muestra del repositorio GitHub.
- Habilite el equilibrio de carga HTTPS (descarga de SSL) en Azure Application Gateway. Para más información, consulte la documentación de Azure.
- Añada o reemplace los servidores web de muestra incluidos con la plantilla.

 ©2024 Palo Alto Networks, Inc.

Servicios seguros de Kubernetes en Azure

Para proteger los servicios de Azure Kubernetes, primero debe instalar el complemento de Azure en Panorama y configurar una implementación de Servicios seguros de Kubernetes en Azure de Azure. El complemento de Azure para Panorama es compatible con la supervisión de máquinas virtuales basada en etiquetas y el Servicios seguros de Kubernetes en Azure, protege el tráfico de entrada para los clústeres de Azure Kubernetes Services (AKS) y supervisa el tráfico saliente desde los clústeres de AKS. La Implementación organizada de Panorama le permite aprovechar las métricas de escalado automático de Azure y los umbrales de ampliación y reducción, para gestionar los picos de demanda de recursos de carga de trabajo de la aplicación gracias a que escala de manera independiente los cortafuegos VM-Series.

Para proteger el tráfico de entrada para su clúster AKS, primero debe Servicios seguros de Kubernetes en Azure. La Implementación organizada de Panorama funciona con Servicios seguros de Kubernetes en Azure para recopilar información acerca de su red y recursos, y luego crear un nivel de escaldo automático de cortafuegos VM-Series para implementaciones Servicios seguros de Kubernetes en Azure. Consulte la Matriz de compatibilidad de Palo Alto Networks para verificar las versiones mínimas de SO, complemento y plantilla necesarios para proteger clústeres de AKS.

Palo Alto Networks proporciona una plantilla AKS que implementa un clúster de Azure Kubernetes Service (AKS) en una nueva red virtual de Azure. El complemento de Azure en Panorama le ayuda a configurar una conexión que puede supervisar las cargas de trabajo del clúster de Azure Kubernetes, recolectando servicios que ha indicado como "balanceador de carga interno" y creando etiquetas que puede usar en grupos de direcciones dinámicas. Puede aprovechar los grupos de direcciones dinámicas de Panorama para aplicar la política de seguridad en el tráfico entrante enrutado a los servicios que se ejecutan en su clúster de AKS.

- ¿Cómo funciona el complemento de Panorama para Azure Secure Kubernetes Services?
- Proteger un clúster AKS

¿Cómo funciona el complemento de Panorama para Azure Secure Kubernetes Services?

Puede usar cortafuegos VM-Series para proteger el tráfico entrante para los clústeres del Servicio Kubernetes de Azure (AKS). El cortafuegos VM-Series solo puede proteger los servicios expuestos por un balanceador de carga (como un balanceador de carga de Azure). El tráfico saliente solo se puede supervisar.

Este capítulo revisa los diferentes componentes que permiten que el complemento de Azure para Panorama se conecte a un clúster AKS.

- Requisitos
- Un ejemplo de topología de hub y spoke para proteger los clústeres de AKS
- Enrutamiento definido por el usuario
- Comunicación del clúster AKS
- Grupos de direcciones dinámicas con etiquetas de Kubernetes

 ©2024 Palo Alto Networks, Inc.

Requisitos

Esta solución requiere los siguientes componentes. Consulte la información del complemento de Panorama en la Matriz de compatibilidad para conocer los requisitos mínimos de versión.

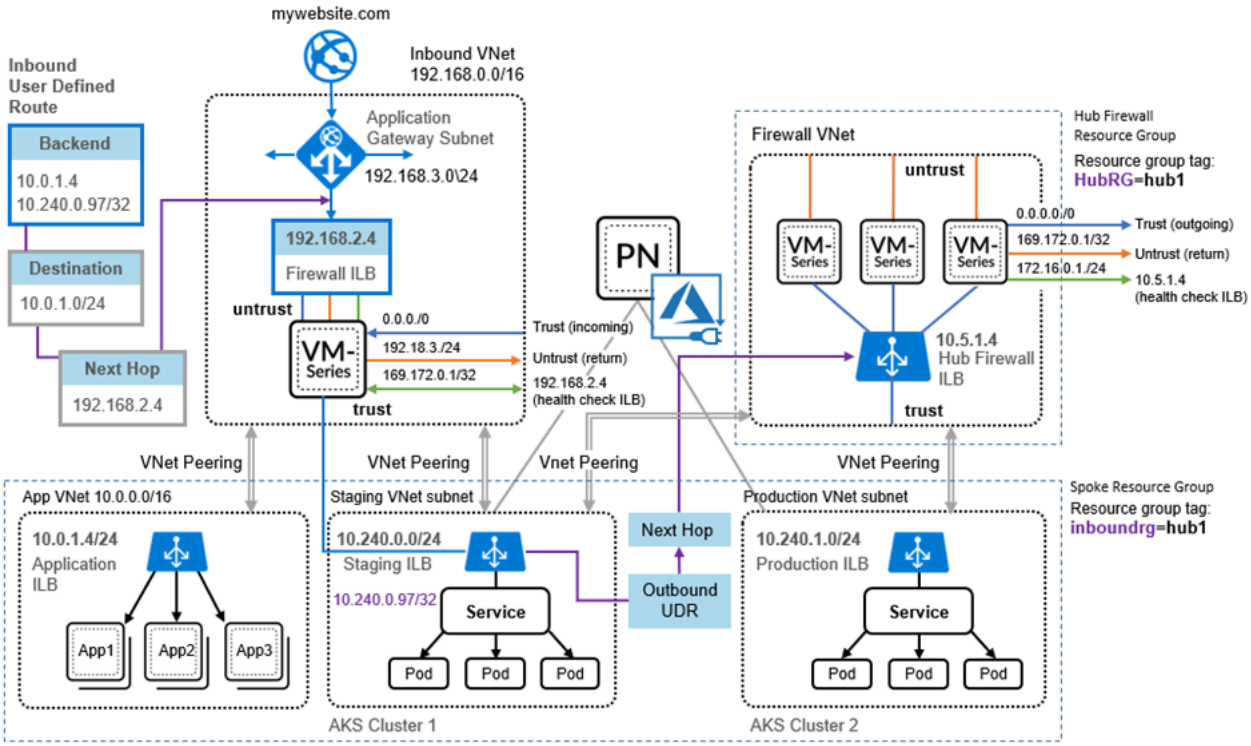
- Cortafuegos VM-Series.
- Panorama: la versión de Panorama debe ser igual o superior a la versión PAN-OS del VM-Series.
- Complemento de Panorama para Azure.
- Una Implementación orquestada de Panorama.
- Plantilla Azure AKS versión 1.0. Esta plantilla crea un clúster de AKS.

  Debe habilitar AKS Advanced Networking (CNI) para el clúster.

  Una implementación de AKS requiere redes avanzadas para configurar el emparejamiento de redes virtuales para las redes virtuales de hub and spoke (consulte Un ejemplo de topología de hub y spoke para proteger los clústeres de AKS).

Un ejemplo de topología de hub y spoke para proteger los clústeres de AKS

El siguiente diagrama ilustra un ejemplo de implementación de escalado automático que protege el tráfico entrante para los clústeres AKS de Azure. Revisemos algunos de los componentes.



- **Infraestructura de escalado automático**: las plantillas de escalado automático de Azure crean la infraestructura de mensajería y la arquitectura básica de hub y spoke.
- **Clústeres AKS**: la plantilla AKS de Palo Alto Networks crea un clúster AKS en una nueva red virtual. Dado el nombre del grupo de recursos de Spoke, la plantilla etiqueta el clúster VNet y AKS con el nombre del grupo de recursos de Spoke, por lo que el complemento de escalado automático de Azure para Panorama puede descubrir el grupo de recursos. El complemento de Azure para Panorama consulta

 ©2024 Palo Alto Networks, Inc.

las direcciones IP del servicio en el almacenamiento provisional de ILB para obtener información sobre los servicios de clúster de AKS.

Solo se puede asociar un conjunto de escala de cortafuegos de Spoke con un clúster de AKS; si expone varios servicios en un único clúster de AKS, estos deben estar protegidos por el mismo Spoke.

Para cada grupo de recursos, cree un grupo de direcciones basado en subred. En el diagrama anterior, por ejemplo, cree un grupo de direcciones para 10.240.0.0/24 (AKS Cluster 1).

- **Emparejamiento de VNet**: debe configurar manualmente el Emparejamiento de VNet para comunicarse con otras redes virtuales en la misma región.

  El emparejamiento entre regiones no es compatible.

  Puede usar otras herramientas de automatización para implementar clústeres AKS. Si implementa en una red virtual existente (la red virtual de cortafuegos de hub, por ejemplo), debe configurar manualmente el emparejamiento de red virtual en los grupos de recursos de hub y spoke entrantes y salientes, y etiquetar manualmente el clúster VNet y AKS con el nombre del grupo de recursos.

- **Rutas y reglas definidas por el usuario**: debe configurar manualmente rutas y reglas definidas por el usuario (consulte Enrutamiento definido por el usuario). En el diagrama anterior, el tráfico entrante se puede redirigir, de acuerdo con las reglas de UDR, al Cortafuegos ILB para su inspección. El tráfico saliente que sale de un clúster AKS se redirige al ILB del cortafuegos del Hub con reglas de enrutamiento definidas por el usuario de Azure (UDR). La solución asume Permitir todo como una política predeterminada para que la orquestación de Kubernetes funcione tal como está, pero para aplicar la política puede usar una lista de permitidos y una lista de denegados para permitir o boquear el tráfico saliente.

Enrutamiento definido por el usuario

Debe crear manualmente el enrutamiento y las reglas de enrutamiento definidas por el usuario para controlar el tráfico entrante o saliente.

Entrante

En el diagrama anterior, el tráfico entrante desde la puerta de enlace de aplicaciones se dirige al grupo de backend y, según las reglas de UDR, se redirige al cortafuegos ILB. Por ejemplo, cree una UDR que apunte a la subred de la red virtual para que el tráfico de los servicios de Kubernetes apunte al ILB del cortafuegos.

Saliente

En el conjunto de cortafuegos del Hub, para cada clúster AKS que se protege, debe crear rutas estáticas para el CIDR de subred del clúster, con el siguiente salto como la dirección de puerta de enlace de la subred trust de la VNet del Hub.

Todo el tráfico saliente para un clúster AKS se dirige al cortafuegos del Hub establecido con una sola regla UDR.

 ©2024 Palo Alto Networks, Inc.

Comunicación del clúster AKS

El complemento de Panorama para Azure solo puede comunicarse con el nodo del controlador AKS para un clúster AKS específico. Para el tráfico saliente de AKS, el siguiente salto es el ILB del cortafuegos del Hub. Dado que el tráfico saliente se supervisa, debe Permitir todo el tráfico. Los siguientes temas hacen énfasis en las prácticas comunes que le pueden ayudar a establecer la conectividad. Téngalos en cuenta cuando planifique sus redes y subredes.

- Crear autenticación de clúster de AKS
- Utilice un grupo de direcciones para identificar el tráfico
- Añada el grupo de direcciones de subred a la política de nivel superior
- Evite la interrupción de la aplicación cuando se emparejan la carga de trabajo y las redes virtuales de clúster de AKS

Crear autenticación de clúster de AKS

Cuando conecta el clúster de AKS en el complemento de Azure para Panorama, debe introducir un token de autorización secreto. Use los comandos de Kubernetes para realizar los siguientes pasos.

STEP 1 | Crear un ClusterRole.

STEP 2 | Crear un ClusterRoleBinding.

1. Crear un archivo `.yaml` para el ClusterRoleBinding. Por ejemplo, cree un archivo de texto llamado `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. Use Azure Cloud Shell para aplicar el enlace de rol `crb.yaml`.

   kubectl apply -f crb.yaml

3. Vea la cuenta de servicio que acaba de crear.

   kubectl get serviceaccounts

STEP 3 | Guarde la credencial de la cuenta de servicio en un archivo `.json`.

1. En su máquina local, cambie al directorio en el que desea guardar la credencial.
2. Utilice los comandos kubectl para crear el token.

   MY_SA_TOKEN=‘kubectl get serviceaccounts default -o jsonpath=’{.secrets[0].name}’‘

3. Ver el nombre del token.

   $ echo $MY_SA_TOKEN

4. Mostrar la credencial.

   kubectl get secret $MY_SA_TOKEN -o json

Necesita el token cuando conecte el clúster de AKS en el complemento de Azure para Panorama , en el Paso 3.d.

 ©2024 Palo Alto Networks, Inc.

Utilice un grupo de direcciones para identificar el tráfico

Para crear cierta granularidad para el tráfico saliente supervisado, cree un grupo de direcciones específicamente para la subred de la red virtual del clúster de AKS (por ejemplo, 10.240.0.97/32 en el diagrama anterior). Luego puede escribir reglas que permitan el tráfico entrante o de retorno en lugar de usar Permitir todo.

Si crea un grupo de direcciones, tenga cuidado de mantener la comunicación entre el controlador AKS y cualquier nodo de trabajo. Consulte Añada el grupo de direcciones de subred a la política de nivel superior.

Si se interrumpe la comunicación, el tráfico de la aplicación puede perderse o la implementación de su aplicación puede tener problemas.

Añada el grupo de direcciones de subred a la política de nivel superior

Para mantener la conectividad, el grupo de direcciones debe ser parte de la política de nivel superior en Panorama. Puede configurar el grupo de direcciones del clúster o iniciar el clúster para configurar el grupo de direcciones del clúster.

*Añada el grupo de direcciones a la política de nivel superior **antes de** configurar el emparejamiento de red virtual o* Enrutamiento definido por el usuario.

Evite la interrupción de la aplicación cuando se emparejan la carga de trabajo y las redes virtuales de clúster de AKS

Si un clúster de AKS coexiste con cargas de trabajo de máquina virtual que se ejecutan en redes virtuales separadas, y la red virtual está emparejada con el spoke de carga de trabajo (entrante) y el Hub (saliente), debe crear grupos de direcciones para diferenciar las cargas de trabajo y el tráfico AKS, y añadir el grupo de direcciones a la Política de nivel superior tal y como se ha descrito anteriormente.

Grupos de direcciones dinámicas con etiquetas de Kubernetes

Al supervisar un recurso de clúster de AKS, el complemento de Azure genera automáticamente las siguientes etiquetas IP para los servicios de AKS.

```
aks.<aks cluster name>.<aks service name>
```

Las etiquetas no se generan para nodos, pods u otros recursos.

Si el servicio AKS tiene alguna etiqueta, la etiqueta es como la siguiente (una por etiqueta):

```
aks.<aks cluster name>.svc.<label>.<value>
```

Si se define una etiqueta labelSelector para un clúster, el complemento genera la siguiente etiqueta IP:

```
aks_<labelSelector>.<aks cluster name>.<aks service name>
```

 ©2024 Palo Alto Networks, Inc.

Proteger un clúster AKS

Para permitir que Panorama se conecte a los balanceadores de carga en un clúster de Azure Kubernetes Services (AKS), debe habilitar el complemento de Azure en Panorama para establecer una conexión con su clúster AKS. Luego, debe configurar los grupos de dispositivos y las plantillas a las que pertenecen los cortafuegos para que Panorama pueda enviar objetos de configuración y reglas de política a sus cortafuegos gestionados.

- Antes de comenzar
- Use la plantilla para implementar un clúster de AKS
- Conecte el clúster de AKS en el complemento de Azure para Panorama
- Configurar el emparejamiento de red virtual
- Redirigir el tráfico a un cortafuegos ILB
- Aplicar política al servicio de AKS relevante
- Implementar y proteger los servicios de AKS

Antes de comenzar

Para proteger AKS, primero debe implementar la solución Azure Auto Scaling disponible en GitHub.

Para proteger una aplicación web que se ejecuta como un servicio dentro de un clúster de Kubernetes, debe planificar las redes virtuales, las subredes y las UDR. Los cortafuegos VM-Series y Panorama le proporcionan seguridad y visibilidad de sus servicios de Kubernetes.

- ❑ Revise "¿Cómo funciona el complemento de Panorama para Azure Secure Kubernetes Services?".
- ❑ Debe tener AKS advanced networking para usar la plantilla AKS de Palo Alto Networks.
- ❑ Diseñe sus subredes AKS **antes** de implementar clústeres de AKS. Revisar Un ejemplo de topología de hub y spoke para proteger los clústeres de AKS y Comunicación del clúster AKS.
  - ❑ La plantilla crea un solo clúster de AKS (Servicio) como muestra. Debe especificar los rangos de CIDR para la red virtual, la subred de la red virtual y el servicio. Los rangos de CIDR no deben superponerse
  - ❑ Dimensione sus subredes según sus requisitos. Evite rangos innecesariamente grandes, ya que pueden afectar el rendimiento.
  - ❑ Consulte Enrutamiento definido por el usuario. Especifique rutas específicas de UDR en lugar de rutas amplias específicas de subred.
- ❑ Planifique cómo quiere emparejar sus redes virtuales. Si está emparejando clústeres de AKS, asegúrese de haber leído Comunicación del clúster AKS
- ❑ Piense en las formas en que desea identificar el tráfico.
  - ❑ Si planifica utilizar un grupo de direcciones en el tráfico saliente de AKS, consulte Añada el grupo de direcciones de subred a la política de nivel superior.
  - ❑ Si tiene nombres de servicio o etiquetas que no son únicos en los espacios de nombres, utilice el selector de etiquetas para filtrar una etiqueta y un espacio de nombres para obtener un resultado único.

 ©2024 Palo Alto Networks, Inc.

Use la plantilla para implementar un clúster de AKS

La plantilla de Azure AKS es una muestra que aprovisiona un clúster en una nueva red virtual.

STEP 1 | En GitHub, vaya a PaloAltoNetworks/azure-aks y localice el paquete de compilación en el repositorio.

STEP 2 | Descomprima el paquete de compilación. Edite los archivos `azuredeploy.json` y `parameters.json` para su propia implementación y guárdelos.

STEP 3 | Emita los siguientes comandos de Azure CLI para implementar la plantilla.

```
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 | Implemente sus aplicaciones o servicios en el clúster de AKS.

1. Anote su archivo YAML de servicio para que el tipo sea balanceador de carga y anótelo como service.beta.kubernetes.io/azure-load-balancer-internal: "true". Por ejemplo:

   ```
     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 no lo ha hecho, debe crear la autenticación del clúster de AKS antes de continuar.
3. Implemente su servicio en su clúster de AKS.

   Por ejemplo, puede implementar su aplicación a través de kubectl:

   `kubectl apply -f myapplication.yaml`

   Para ver una muestra, consulte: https://github.com/Azure-Samples/azure-voting-app-redis/blob/master/azure-vote-all-in-one-redis.yaml
4. Use kubectl para obtener la IP del servicio para el servicio implementado.

   `kubectl get services -o wide`

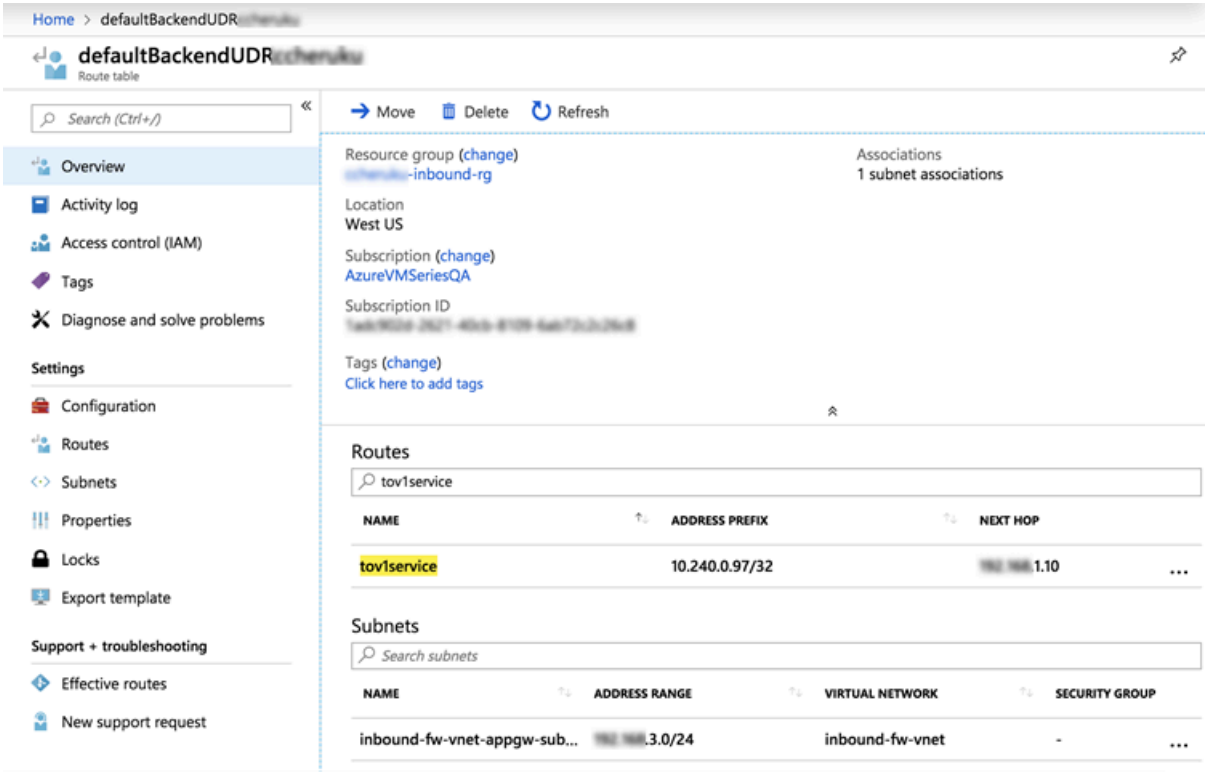
NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE	SELECTOR
azure-vote-back	ClusterIP	10.0.77.21	<none>	6379/TCP	2d23h	app=azure-vote-back
azure-vote-front	LoadBalancer	10.0.18.189	10.240.0.97	80:31937/TCP	2d23h	app=azure-vote-front
kubernetes	ClusterIP	10.0.0.1	<none>	443/TCP	2d23h	<none>

   En la columna EXTERNAL-IP 10.240.0.97 es para el ILB, de acuerdo con su anotación en Paso a. Use el IP de servicio para crear una ruta definida por el usuario en Azure.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Cree una regla UDR para apuntar su servicio al cortafuegos ILB detrás de la puerta de enlace de la Aplicación.

En Azure, vaya a su grupo de recursos de spoke de entrada, vea la tabla de rutas y añada una nueva ruta basada en la IP del servicio de destino. En la siguiente pantalla, el valor en la columna tov1service **ADDRESS PREFIX (PREFIJO DE DIRECCIÓN)** es la IP del servicio.



Conecte el clúster de AKS en el complemento de Azure para Panorama

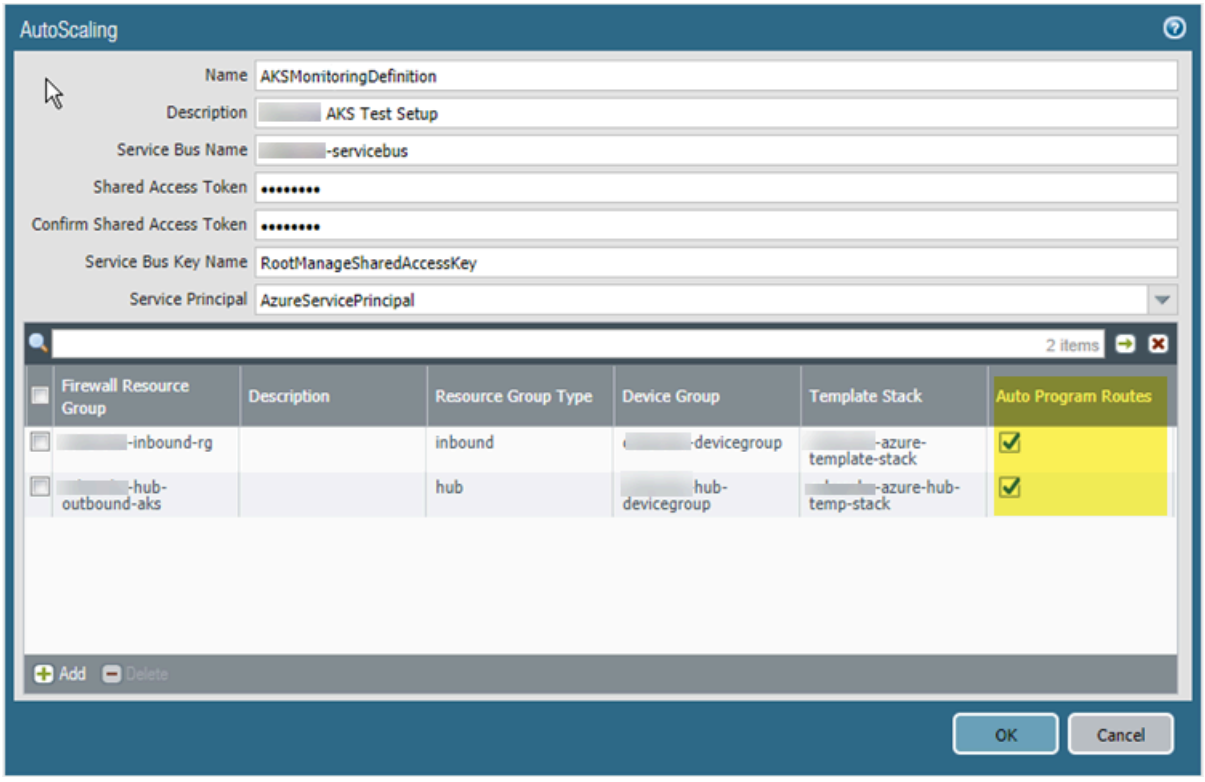
Esta tarea asume que ha implementado una implementación organizada de Panorama y que ha creado plantillas, pilas de plantillas y grupos de dispositivos.

Consulte la ayuda en línea de Panorama para obtener más información sobre cómo completar cada formulario.

STEP 1 | Seleccione **Panorama** > **Azure** > **Deployments (Implementaciones)** para ver la definición de supervisión que creó cuando configuró la implementación. Como se muestra a continuación, si **Auto**

 ©2024 Palo Alto Networks, Inc.

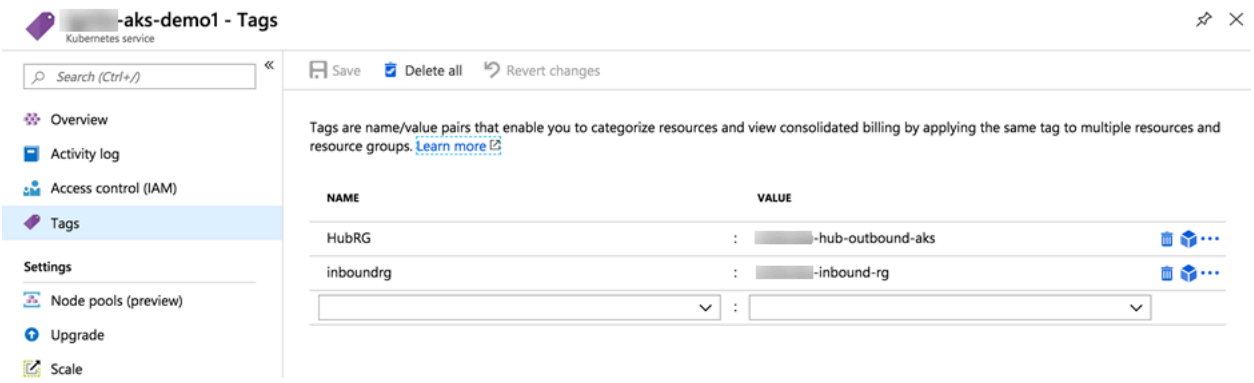
Program Routes (Programar rutas automáticamente) está habilitado, las rutas del cortafuegos están programadas para usted.



 ©2024 Palo Alto Networks, Inc.

STEP 2 | En AKS, etiquete sus Grupos de recursos. Las etiquetas son pares de nombre/valor.

1. Seleccione **Home (Inicio)** > **Resource groups (Grupos de recursos)** y seleccione un grupo de recursos.
2. Seleccione **Tags (Etiquetas)** y defina pares de nombre/valor. Como se muestra en la siguiente figura, los nombres de las etiquetas deben ser inboundgrouprg y HubRG:
   - inboundgrouprg: el nombre del grupo de recursos spoke
   - HubRG: el nombre del grupo de recursos hub



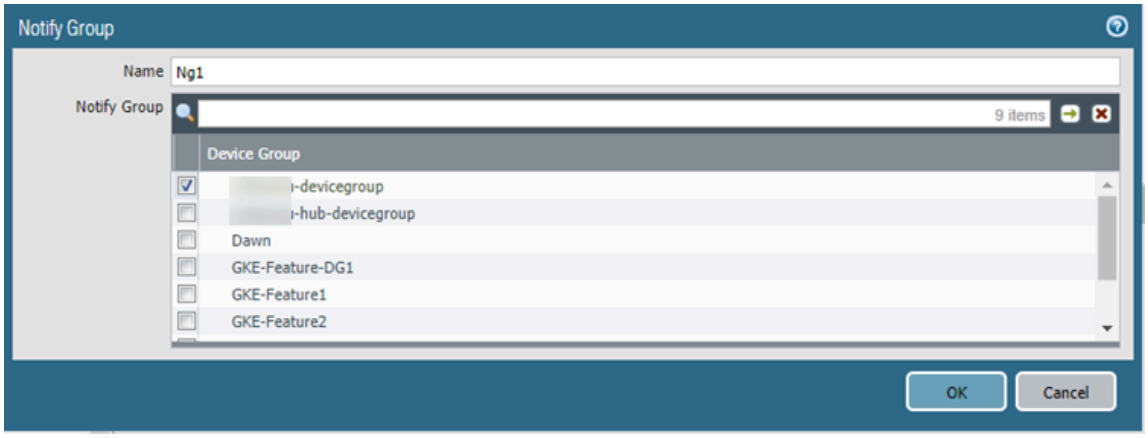
La plantilla toma el nombre del grupo de recursos de Spoke como parámetro y etiqueta el clúster de VNet y de AKS con el nombre del grupo de recursos Spoke para que pueda ser descubierto por el complemento de Panorama para Azure.

Las plantillas implementan recursos en redes virtuales independientes. Si implementa manualmente el clúster y el servicio de AKS en la misma red virtual que el conjunto de cortafuegos de Spoke, debe crear manualmente etiquetas para el nombre del grupo de recursos de spoke.

 ©2024 Palo Alto Networks, Inc.

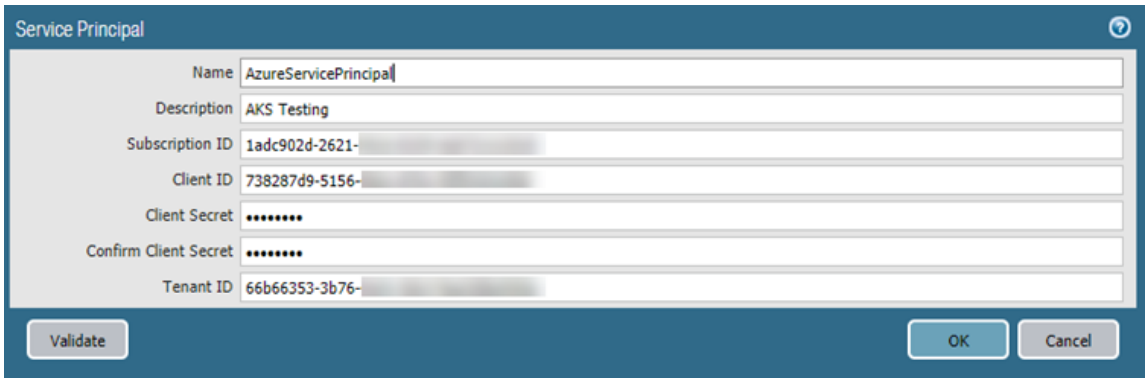
STEP 3 | En Panorama, seleccione **Panorama** > **Azure** > **Setup (Configuración).**

1. En la pestaña **General**, habilite la supervisión.
2. En la pestaña **Notify Groups (grupos de notificación)**, seleccione **Add (Añadir)** un grupo de notificación y seleccione los grupos de dispositivos que se notificarán.



3. En la pestaña **Service Principal (Entidad de servicio)**, seleccione **Add (Añadir)** y **Validate (Validar)** una entidad de servicio.

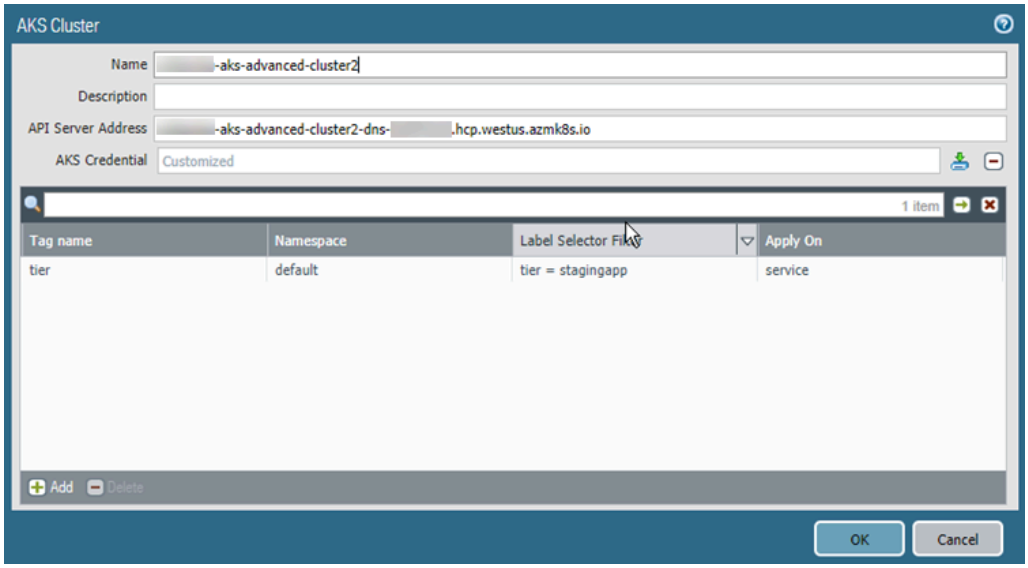
   Utilice la entidad de servicio que creó para la implementación organizada.



4. En la pestaña **AKS Cluster (Clúster de AKS)**, seleccione **Add (Añadir)** un clúster de AKS.
   - Introduzca el nombre exacto del clúster de AKS.
   - Introduzca la dirección del servidor API. Para buscar la dirección en Azure, vea su servicio AKS y seleccione Descripción general.
   - Cargue el archivo JSON de credenciales de AKS (consulte Crear autenticación de clúster de AKS).
5. Complete los campos restantes y seleccione **Add (Añadir)** una o más etiquetas.

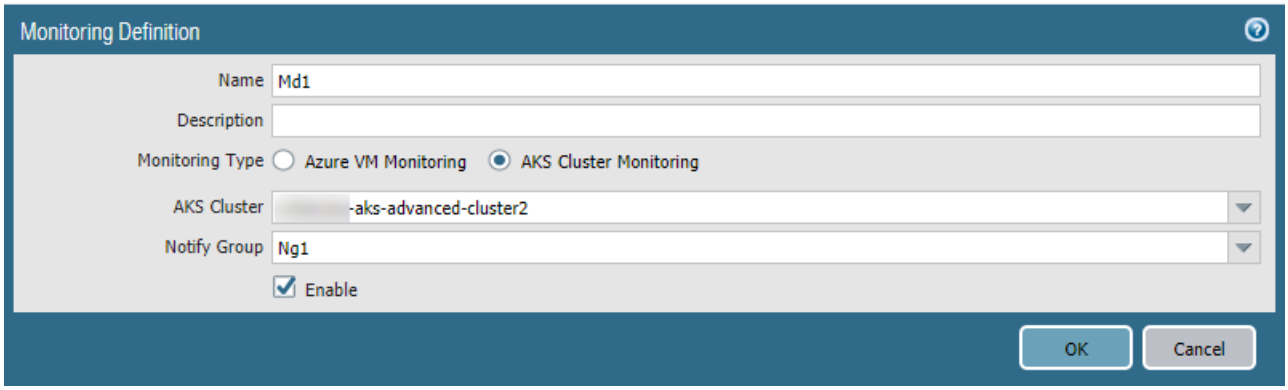
   Si tiene nombres de servicio o etiquetas que no son únicos en los espacios de nombres, utilice el selector de etiquetas para filtrar una etiqueta y un espacio de nombres para obtener un resultado único.

 ©2024 Palo Alto Networks, Inc.



STEP 4 | Seleccione **Panorama** > **Azure** > **Monitoring Definition (Definición de supervisión)**

1. Añada una Definición de monitorización.
2. Introduzca un nombre y una descripción, y seleccione **AKS Cluster Monitoring (supervisión de clúster de AKS)**.
3. Seleccione un **AKS Cluster (Clúster de AKS)** y un **Notify Group (Grupo de notificación)**, marque **Enable (Habilitar)** y haga clic en **OK (Aceptar)**.



Configurar el emparejamiento de red virtual

Si planea usar un grupo de direcciones para identificar el tráfico, asegúrese de añadir el grupo de direcciones de subred a su política Panorama de nivel superior antes de configurar el emparejamiento.

Después de implementar un clúster de AKS, configure el Emparejamiento de VNet desde la red virtual entrante a su clúster y desde su clúster a la red virtual del cortafuegos.

Redirigir el tráfico a un cortafuegos ILB

Debe crear manualmente rutas definidas por el usuario (UDR) y reglas de enrutamiento para redirigir el tráfico a un ILB específico. Por ejemplo, vea cómo el diagrama en "¿Cómo funciona el complemento de Panorama para Azure Secure Kubernetes Services?" representa una UDR de entrada.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Cree reglas de enrutamiento de URL que redirijan el tráfico web al grupo de servidores backend apropiado.

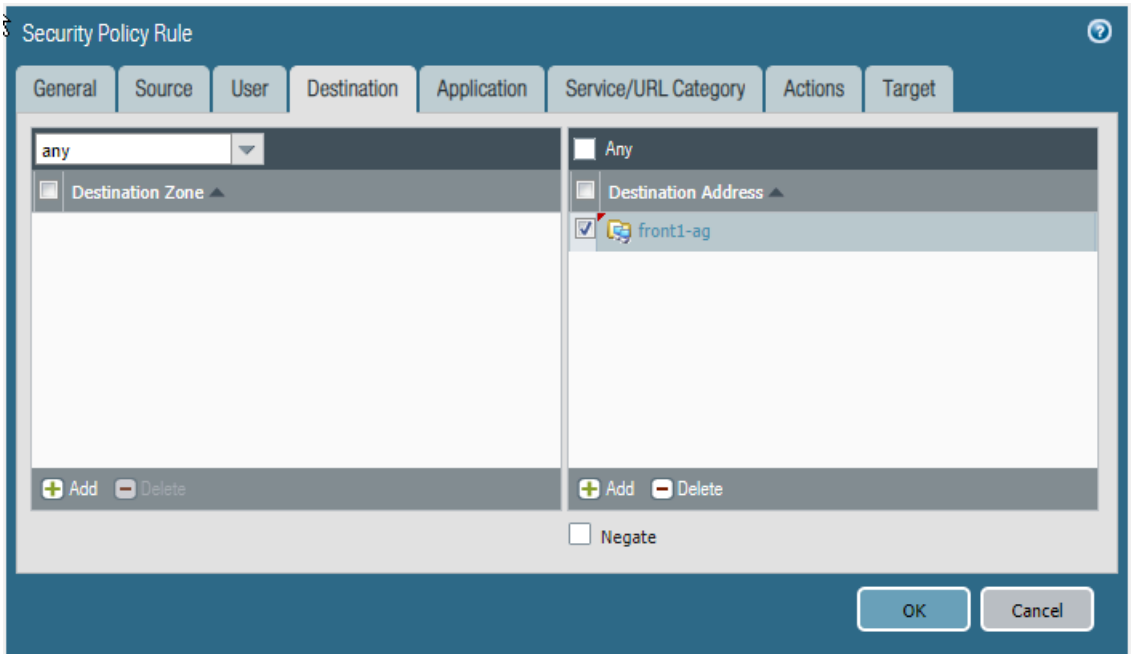
STEP 2 | Actualice las reglas de UDR para la subred de la puerta de enlace de la aplicación para añadir una ruta para el CIDR del servicio, con el siguiente salto como el balanceador de carga del cortafuegos de entrada del grupo de recursos de cortafuegos de Spoke.

Aplicar política al servicio de AKS relevante

STEP 1 | En Panorama, seleccione Políticas.

STEP 2 | En la lista **Device Group (Grupo de dispositivos)**, seleccione el grupo de dispositivos para su servicio de AKS.

STEP 3 | **Add (Añadir)** una regla de política de seguridad. Complete el formulario y, en la pestaña **Destination (Destino)** debe **Add (Añadir)** la dirección de destino o el grupo de direcciones.



Implementar y proteger los servicios de AKS

Estos pasos describen cómo puede proteger el tráfico entrante y saliente que atraviesa los servicios de Kubernetes mediante el cortafuegos VM-Series y el complemento de Azure para Panorama.

STEP 1 | En el entorno de implementación de la aplicación, cree un archivo YAML para la aplicación o use un archivo que ya exista. El siguiente es un archivo YAML de aplicación de muestra:

```
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:
           requests:             cpu: 100m             memory:
 128Mi           limits:               cpu: 250m             memory:
 256Mi         ports:          - containerPort: 6379           name:
```

 ©2024 Palo Alto Networks, Inc.

```
 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 | Edite su archivo YAML para etiquetar los servicios de Kubernetes.

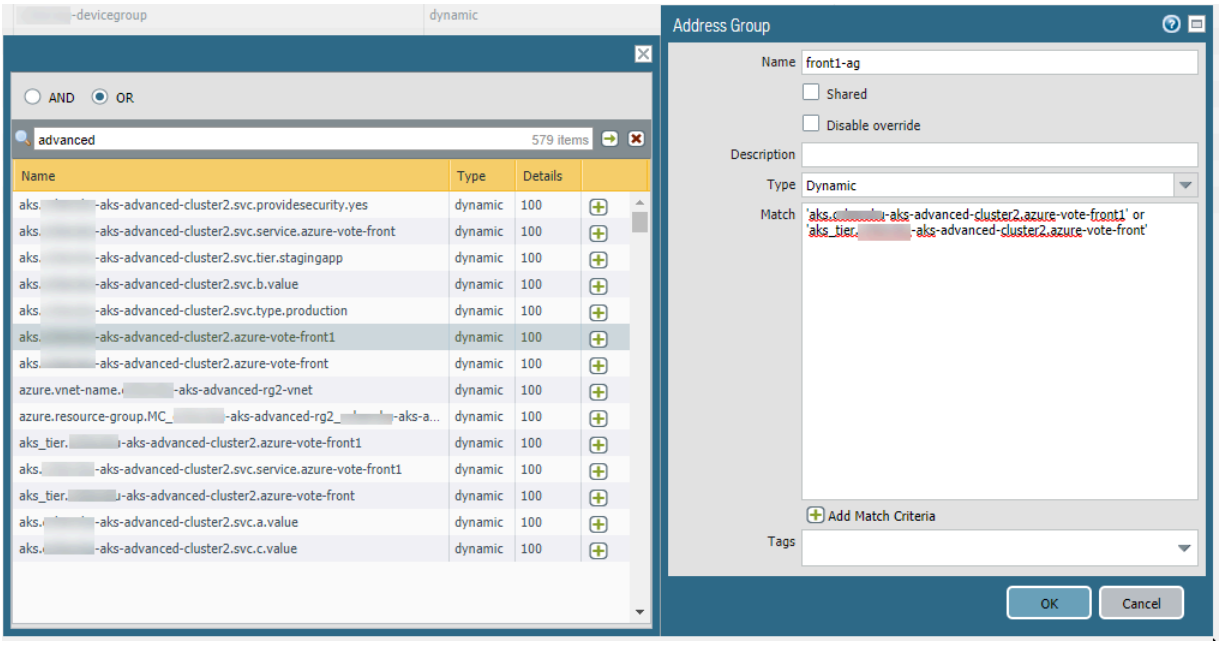
Las etiquetas permiten crear la asignación de etiqueta a IP correspondiente cuando utiliza el complemento de Panorama para que AKS se conecte al clúster. Por ejemplo, en el archivo de muestra anterior, busque las etiquetas de la aplicación en los metadatos del servicio. Estos son: **`azure-vote-back`** y **`azure-vote-front`**.

STEP 3 | En su clúster de AKS, aplique el archivo YAML.

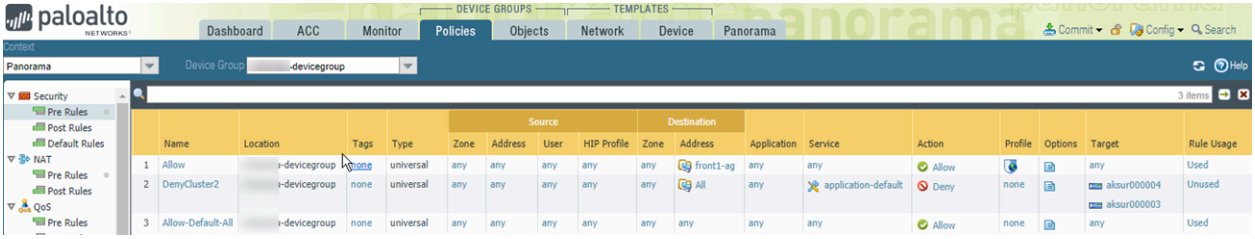
 ©2024 Palo Alto Networks, Inc.

STEP 4 | En Panorama, cree un Grupo de direcciones utilizando una etiqueta de grupo de recursos.

1. En la pestaña **Objects (Objetos)**, seleccione un grupo de dispositivos de la lista **Device Group (Grupo de dispositivos)**.
2. Seleccione **Address Group (Grupos de direcciones)** y luego **Add (Añadir)** un Grupo de direcciones.
   1. Especifique un nombre y seleccione el tipo **Dynamic (Dinámico)**.
   2. **Add (Añadir)** direcciones. Añadir genera una ventana que enumera las direcciones detectadas. Rellenar la lista puede llevar varios minutos.
   3. Puede elegir una o más direcciones para los Criterios de coincidencia. Seleccione AND u OR para la relación de criterios.
   4. Si tiene muchas direcciones, introduzca una cadena en el cuadro de búsqueda para filtrar la salida, como se muestra en la siguiente figura.
   5. En la lista de direcciones, haga clic en + para incluir la dirección en los criterios de coincidencia del grupo de direcciones.
   6. Cuando se complete el criterio de coincidencia, haga clic en **OK (Aceptar)**.



STEP 5 | Mostrar política utilizando el grupo de direcciones.



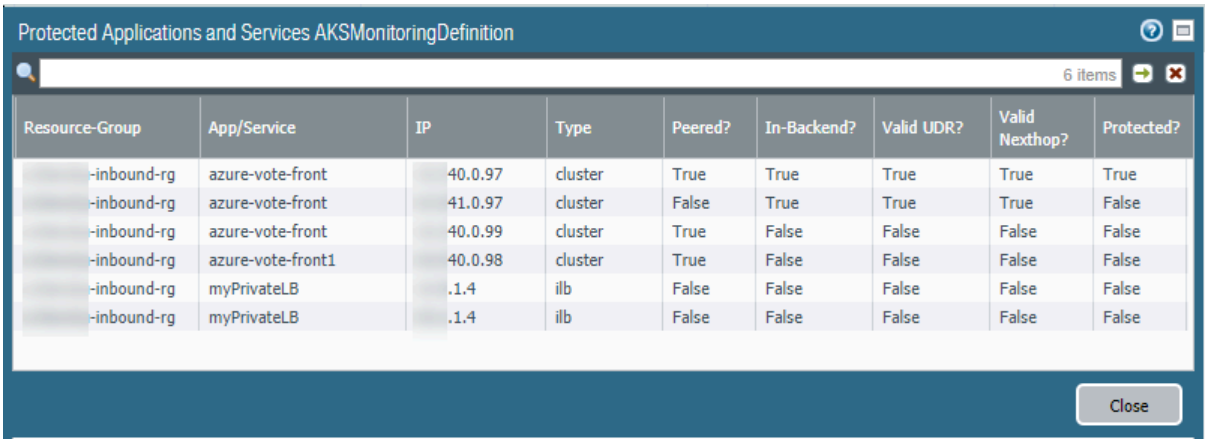
 ©2024 Palo Alto Networks, Inc.

STEP 6 | Ver servicios AKS seguros.

En **Panorama** > **Azure** > **Deployments (Implementaciones)**, vea su definición de supervisión y, en la columna Acción, seleccione el enlace **Protected Applications and Services (Aplicaciones y servicios protegidos)**.

La columna **Protected? (¿Protegida?)** resume el estado de seguridad de sus grupos de recursos. La ventana puede tardar varios minutos en completarse. Si tiene muchos grupos de recursos, introduzca una cadena en el cuadro de búsqueda para filtrar el resultado.

Este resultado se basa en la configuración del grupo de recursos de Azure; no consulta al grupo de dispositivos o la pertenencia de la pila de plantillas.



 ©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en OpenStack

El cortafuegos VM-Series para OpenStack le permite proporcionar una entrega de aplicaciones segura junto con seguridad, rendimiento y visibilidad de la red.

- Cortafuegos VM-Series para OpenStack
- Componentes de VM-Series para la solución OpenStack
- Plantilla Heat para una implementación básica de puerta de enlace
- Plantillas Heat para encadenamiento de servicios y escalado de servicios
- Instalación del cortafuegos VM-Series en una implementación de puerta de enlace básica
- Instalación del cortafuegos VM-Series con encadenamiento y escalado de servicios

Implementaciones VM-Series en OpenStack

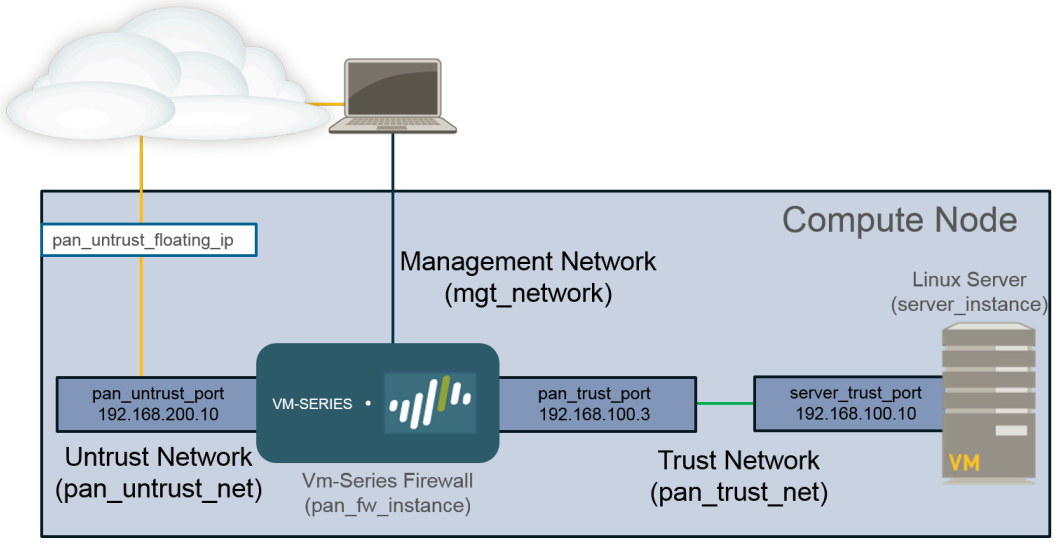
Las plantillas de orquestación Heat proporcionadas por Palo Alto Networks le permiten implementar el cortafuegos VM-Series de forma individual, mediante el encadenamiento de servicios o dinámicamente con la ampliación del servicio.

- Gateway básico
- Encadenamiento de servicios y Escalado de servicios

Gateway básico

El cortafuegos VM-Series para OpenStack le permite implementar el cortafuegos VM-Series en el hipervisor KVM que se ejecuta en un nodo de cálculo en su entorno OpenStack. Esta solución utiliza plantillas de orquestación Heat y arranques para implementar el cortafuegos VM-Series y un servidor Linux. El cortafuegos VM-Series protege el servidor Linux implementado mediante la inspección del tráfico que entra y sale del servidor. Los archivos de arranque de muestra permiten que el cortafuegos VM-Series arranque con una configuración básica para gestionar el tráfico.

Estos archivos de plantillas heat y los archivos de arranque se combinan para crear dos máquinas virtuales, el servidor de seguridad VM-Series y el servidor Linux, en una configuración de red similar a la que se muestra a continuación.



Encadenamiento de servicios y Escalado de servicios

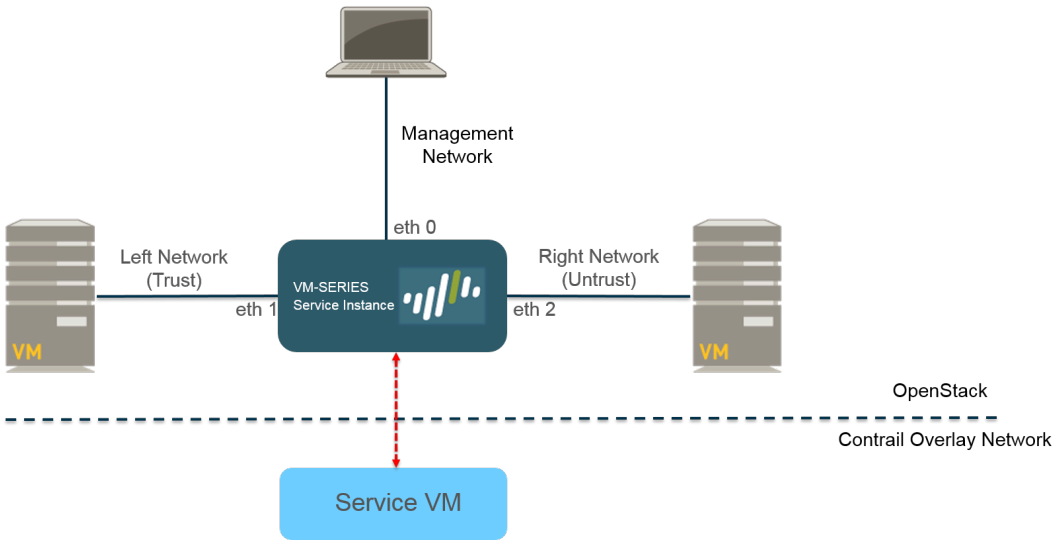
OpenStack Queens no es compatible con la implementación del cortafuegos VM-Series a través del encadenamiento o el escalado del servicio.

El encadenamiento de servicios es una característica de Contrail que implementa un cortafuegos VM-Series como una instancia de servicio en su entorno OpenStack. Una cadena de servicio es un conjunto de máquinas virtuales de servicio, como cortafuegos o balanceadores de carga, y cada máquina virtual en la cadena de servicio es una instancia de servicio. La escalabilidad del servicio le permite implementar dinámicamente instancias adicionales del cortafuegos VM-Series. OpenStack, a través del uso de

 ©2024 Palo Alto Networks, Inc.

la utilización de la CPU o las métricas de bytes entrantes por segundo recopiladas por Ceilometer, implementa o cierra instancias adicionales del cortafuegos VM-Series para satisfacer las necesidades actuales de su red.

El cortafuegos VM-Series en la solución OpenStack aprovecha las plantillas de la orquestación heat para configurar e implementar los componentes necesarios para el encadenamiento y el escalado de los servicios. Las plantillas heat proporcionadas por Palo Alto Networks crean una plantilla de servicio, instancia de servicio y política de servicio (para dirigir el tráfico al cortafuegos VM-Series) para implementar dos servidores Linux y la instancia de servicio de cortafuegos VM-Series entre ellos.



 ©2024 Palo Alto Networks, Inc.

Componentes de VM-Series para la solución OpenStack

El cortafuegos VM-Series en un entorno OpenStack ha sido probado con los siguientes componentes.

Componente	Description (Descripción)
Software	Consulte la Matriz de compatibilidad para obtener detalles sobre las versiones de software compatibles.
Recursos de hardware VM-Series	Consulte Requisitos del sistema VM-Series para ver los requisitos mínimos de hardware para su modelo VM-Series. En OpenStack, los factores definen la CPU, la memoria y la capacidad de almacenamiento de una instancia de procesamiento. Cuando configure su plantilla Heat, elija el factor de procesamiento que cumpla o supere los requisitos de hardware para el modelo VM-Series.
Fuel Master	Fuel es una herramienta de implementación y gestión basada en la interfaz de usuario web para OpenStack.
Controlador OpenStack	Este nodo ejecuta la mayoría de los servicios de OpenStack compartidos, como API y programación. Además, la UI de Horizon se ejecuta en este nodo.
Procesamiento de OpenStack	El nodo de procesamiento contiene las máquinas virtuales, incluido el cortafuegos VM-Series, en la implementación de OpenStack. El nodo de procesamiento que aloja VM-Series debe cumplir los siguientes criterios: • Tipo de instancia OS :: Nova :: Servidor • Permitir la configuración de al menos tres interfaces • Aceptar la imagen VM-Series qcow2 • Aceptar el parámetro de sabor de cálculo *Instale el nodo de cálculo OpenStack en un servidor dedicado porque el cortafuegos VM-Series no es compatible con la virtualización anidada.*
Controlador contrail	El nodo del controlador Contrail es un controlador de red definido por software que se utiliza para la gestión, control y análisis de la red virtualizada. Proporciona información de enrutamiento a los nodos de cálculo y puerta de enlace. Además, el controlador Contrail proporciona el soporte necesario para el encadenamiento del servicio y el escalado del servicio.
Puerta de enlace de Contrail	El nodo de puerta de enlace de Contrail proporciona conectividad IP a redes externas desde redes virtuales. Los túneles MPLS sobre GRE de

 ©2024 Palo Alto Networks, Inc.

Componente	Description (Descripción)
	las máquinas virtuales finalizan en el nodo de la puerta de enlace, donde los paquetes se desencapsulan y se envían a sus destinos en redes IP.
Ceilometer (Telemetría OpenStack)	En el caso del cortafuegos VM-Series para OpenStack, Ceilometer supervisa la utilización de la CPU para el escalado del servicio. Cuando la utilización de la CPU cumple los umbrales definidos, se despliega o se cierra una nueva instancia de servicio del cortafuegos VM-Series.
Archivos de plantilla de orquestación Heat	Palo Alto Networks proporciona una plantilla Heat de ejemplo para implementar el cortafuegos VM-Series. Esta plantilla se compone de una plantilla principal y una plantilla de entorno. Estos archivos crean una instancia de VM-Series con una interfaz de gestión y dos interfaces de datos. En una implementación de puerta de enlace básica, la plantilla crea una instancia de servidor Linux con una interfaz. La interfaz del servidor se conecta a la red privada creada por la plantilla. En una implementación de encadenamiento de servicio o escalado de servicio, las plantillas inician instancias de dos servidores Linux con un servidor conectado a cada interfaz de datos del cortafuegos.
Archivos de arranque del cortafuegos VM-Series	Los archivos de arranque del cortafuegos VM-Series constan de un archivo init-cfg.txt, un archivo bootstrap.xml y códigos de autenticación VM-Series. Junto con los archivos de plantilla Heat, Palo Alto Networks proporciona un archivos init-cfg.txt y bootstrap.xml de muestra. Debe proporcionar sus propios códigos de autenticación para otorgar la licencia a su cortafuegos VM-Series y activar cualquier suscripción. Consulte Arranque del cortafuegos VM-Series para obtener más información acerca de los archivos de arranque VM-Series.

 ©2024 Palo Alto Networks, Inc.

Plantilla Heat para una implementación básica de puerta de enlace

El archivo de plantilla heat incluye los siguientes cuatro archivos para ayudarlo a iniciar el cortafuegos VM-Series en KVM en OpenStack. Los cuatro archivos son necesarios para implementar el cortafuegos VM-Series y el servidor Linux.

- **pan_basic_gw.yaml**: Define los recursos creados para admitir el cortafuegos VM-Series y el servidor Linux en el nodo de cálculo, como interfaces y direcciones IP.
- **pan_basic_gw_env.yaml**: Define el entorno en el que se encuentran el cortafuegos VM-Series y los servidores Linux. Muchos parámetros en el archivo pan_basic_gw.yaml hacen referencia a los parámetros definidos en este archivo, como el sabor de la VM-Series y los servidores Linux.
- **init-cfg.txt**: Incluye el comando de operación para habilitar DHCP en la interfaz de la gestión del cortafuegos.
- **bootstrap.xml**: Proporciona la configuración básica para el cortafuegos VM-Series. El archivo bootstrap.xml configura las interfaces de datos y las direcciones IP. Estos valores deben coincidir con los valores correspondientes en el archivo pan_basic_gw.yaml.

  Además, el archivo bootstrap.xml incluye una regla NAT denominada untrust2trust. Esta regla traduce el puerto fiable en el servidor al puerto no fiable del cortafuegos VM-Series.

Tiene dos opciones para pasar archivos de arranque a OpenStack: inyección de archivos (archivos de personalidad) o datos de usuario.

La inyección de archivos ya no es compatible a partir de OpenStack Queens; debes usar datos de usuario en su lugar.

La siguiente tabla describe los recursos que crea el archivo de plantilla pan_basic_gw.yaml y proporciona el valor predeterminado, si corresponde.

Recurso	Description (Descripción)
pan_fw_instance	Cortafuegos VM-Series con una interfaz de gestión y dos interfaces de datos.
server_instance	Un servidor Linux con una sola interfaz.
pan_trust_net	Una conexión a la red interna a la que están conectadas la interfaz fiable del cortafuegos y la interfaz fiable del servidor.
pan_trust_subnet	Subred conectada a la interfaz fiable en el cortafuegos (pan_trust_net) y tiene un valor CIDR de 192.168.100.0/24.
pan_untrust_net	Red no fiable a la que está conectado el puerto no fiable del cortafuegos.

©2024 Palo Alto Networks, Inc.

Recurso	Description (Descripción)
pan_untrust_subnet	Subred conectada a la interfaz no confiable del cortafuegos (pan_untrust_net) y tiene un valor CIDR de 192.168.200.0/24.
allow_ssh_https_icmp_secgroup	Grupo de seguridad que permite TCP en los puertos 22 y 443, y tráfico ICMP.
pan_untrust_port	El puerto no fiable del cortafuegos VM-Series desplegado en el modo Capa 3. La plantilla Heat proporciona una dirección IP predeterminada de 192.168.200.10 a este puerto. Si cambia esta dirección IP en la plantilla heat, deberá cambiar la dirección IP en el archivo bootstrap.xml.
pan_untrust_floating_ip	Una dirección IP flotante asignada desde public_network.
pan_untrust_floating_ip_assoc	Esto asocia pan_untrust_floating_ip a pan_untrust_port.
pan_trust_port	El puerto fiable del modo de Capa 3 del cortafuegos VM-Series.
server_trust_port	El puerto fiable del modo Capa 3 del servidor Linux. La plantilla Heat proporciona una dirección IP predeterminada de 192.168.100.10 a este puerto. Si cambia esta dirección IP en la plantilla heat, deberá cambiar la dirección IP en el archivo bootstrap.xml.

El archivo pan_basic_gw.yaml hace referencia a pan_basic_gw_env.yaml de muchos de los valores necesarios para crear los recursos necesarios para implementar el cortafuegos VM-Series y el servidor Linux. El archivo de entorno de la plantilla heat contiene los siguientes parámetros.

Parámetros	Description (Descripción)
mgmt_network	La interfaz de gestión del cortafuegos VM-Series se adjunta a la red especificada en este parámetro. La plantilla no crea la red de gestión; usted debe crear esto antes de implementar las plantillas heat. El valor predeterminado es mgmt_ext_net.
public_network	Direcciones que el clúster de OpenStack y las máquinas virtuales en el clúster usan para comunicarse con la red externa o pública. La red pública proporciona direcciones IP virtuales para endpoints públicos, que se utilizan para conectarse a las API de servicios de OpenStack. La plantilla no crea la red pública; usted debe crear esto antes de implementar las plantillas heat. El valor predeterminado es public_net.

 ©2024 Palo Alto Networks, Inc.

Parámetros	Description (Descripción)
pan_image	Este parámetro especifica la imagen base de la VM-Series utilizada por la plantilla de Heat cuando se implementa el cortafuegos VM-Series. El valor predeterminado es pa-vm-7.1.4.
pan_flavor	Este parámetro define los recursos de hardware asignados al cortafuegos VM-Series. El valor predeterminado es m1.medium. Este valor cumple con los Requisitos del sistema para VM-Series en KVM descrito en el capítulo Configuración del cortafuegos VM-Series en KVM.
server_image	Este parámetro indica a la plantilla Heat qué imagen usar para el servidor Linux. El valor predeterminado es Ubuntu-14.04.
server_flavor	Este parámetro define los recursos de hardware asignados al servidor Linux. El valor predeterminado es m1.small.
server_key	La clave del servidor se usa para acceder al servidor Linux a través de ssh. El valor predeterminado es server_key. Puede cambiar este valor introduciendo una nueva clave de servidor en el archivo de entorno.

 ©2024 Palo Alto Networks, Inc.

Plantillas Heat para encadenamiento de servicios y escalado de servicios

OpenStack Queens no es compatible con la implementación del cortafuegos VM-Series a través del encadenamiento o el escalado del servicio.

El archivo de entorno de la plantilla heat define los parámetros específicos de la instancia de cortafuegos VM-Series desplegada mediante el encadenamiento del servicio o el escalado del servicio. Los parámetros definidos en el archivo de entorno se dividen en las secciones que se describen a continuación. Hay dos versiones de las plantillas heat para el servicio de encadenamiento, vwire y L3, y una para el escalado de servicio.

El encadenamiento de servicios requiere los archivos de la plantilla heat y dos archivos bootstrap para iniciar la instancia del servicio de cortafuegos VM-Series y dos servidores Linux en las redes izquierda y derecha.

- **Archivos de plantilla**: esta plantilla define los recursos creados para admitir el cortafuegos VM-Series y dos servidores Linux, como interfaces y direcciones IP.
  - service_chaining_template_vm.yaml for vwire deployments.
  - service_chaining_template_L3.yaml for L3 deployments.
  - service_scaling_template.yaml for service scaling deployments.
- **Archivo de entorno**: Este archivo de entorno define el entorno en el que se encuentran el cortafuegos VM-Series y los servidores Linux. Muchos parámetros de la plantilla hacen referencia a los parámetros definidos en este archivo, como el factor de la serie VM y los nombres de los servidores Linux.
  - service_chaining_env_vm.yaml para implementaciones de vwire.
  - service_chaining_env_L3.yaml para implementaciones L3.
  - service_scaling_env.yaml para implementaciones de escalado de servicios.
- **service_instance.yaml**: (Escalado de servicio solamente) Esta es una plantilla heat anidada que sirve de referencia para Service_Scaling_template.yaml para implementar la instancia de servicio. Proporciona la información necesaria para implementar instancias de servicio para eventos de escalado.
- **init-cfg.txt**: Proporciona la información mínima requerida para iniciar un cortafuegos VM-Series. El archivo init-cfg.txt proporcionado solo incluye el comando operativo para habilitar DHCP en la interfaz de gestión del cortafuegos.
- **<file_name>_bootstrap.xml**: Proporciona la configuración básica para el cortafuegos VM-Series. El archivo bootstrap.xml configura las interfaces de datos. Estos valores deben coincidir con los valores correspondientes en los archivos de plantillas heat.

Para obtener más información sobre los archivos init-cfg.txt y bootstrap.xml, consulte Archivos de configuración de arranque.

Las siguientes tablas describen los parámetros del archivo de entorno.

- Red virtual
- Máquina virtual
- Plantilla de servicio

 ©2024 Palo Alto Networks, Inc.

- Instancia de servicio
- IPAM
- Política de servicio
- Alarma

Red virtual

Los parámetros de configuración de red virtual en el archivo de entorno de la plantilla heat definen la red virtual que conecta el cortafuegos VM-Series y los dos servidores Linux desplegados por la plantilla heat.

Red virtual (configuración de VN)	
management_network	La interfaz de gestión del cortafuegos VM-Series se adjunta a la red especificada en este parámetro.
left_vn o left_network	Nombre de la red virtual izquierda.
right_vn o right_network	Nombre de la red virtual derecha.
left_vn_fqdn	Nombre de dominio completo de la red virtual izquierda.
right_vn_fqdn	Nombre de dominio completo de la red virtual derecha
route_target	Edite este valor para que la configuración del objetivo de ruta coincida con la de su puerta de enlace externa.

Máquina virtual

Los parámetros de la máquina virtual definen los servidores Linux izquierdo y derecho. El nombre de la tupla del puerto se define aquí y la plantilla Heat hace referencia al mismo. En Contrail, una tupla de puertos es un conjunto ordenado de interfaces de red virtuales conectadas a la misma máquina virtual. Con una tupla de puertos, puede crear puertos y pasar esa información cuando crea una instancia de servicio. La plantilla heat crea los puertos izquierdo, derecho y de gestión y los añade a la tupla de puertos. La tupla de puertos se vincula a la instancia del servicio. Cuando inicia la instancia de servicio utilizando las plantillas heat, la tupla de puertos asigna la máquina virtual del servicio a la máquina virtual implementada en OpenStack.

Máquina virtual (VM Config)	
factor	El factor de las máquinas virtuales izquierda y derecha. El valor predeterminado es m1.small.
left_vm_image r right_vm_image o image	El nombre de la imagen del software para las máquinas virtuales izquierda y derecha. Cambie este valor para que coincida con el nombre de archivo de la imagen que cargó.

 ©2024 Palo Alto Networks, Inc.

Máquina virtual (VM Config)	
	El valor predeterminado es TestVM, que es una imagen predeterminada proporcionada por OpenStack.
svm_name	El nombre puesto al cortafuegos VM-Series.
left_vm_name y right_vm_name	El nombre de las máquinas virtuales izquierda y derecha.
port_tuple_name	El nombre de la tupla de puertos utilizada por los dos servidores Linux y el cortafuegos VM-Series.
server_key	La clave del servidor se utiliza para acceder a máquinas virtuales a través de SSH. El valor predeterminado es server_key. Puede cambiar este valor introduciendo una nueva clave de servidor en el archivo de entorno.

Plantilla de servicio

La plantilla de servicio define los parámetros de la instancia del servicio, como la imagen del software, el factor de la máquina virtual, el tipo de servicio y las interfaces. Las plantillas de servicio se configuran dentro del alcance de un dominio y se pueden usar en todos los proyectos dentro del dominio especificado.

Plantilla de servicio (ST Config)	
S_Tmp_name	El nombre de la plantilla de servicio.
S_Tmp_version	La versión de la plantilla de servicio. El valor predeterminado es 2. No cambie este parámetro porque la plantilla de servicio versión 2 es necesaria para apoyar tuplas de puertos.
S_Tmp_service_mode	El modo de servicio es el modo de red utilizado por la instancia de servicio de cortafuegos VM-Series. Para la plantilla de red L3, el valor predeterminado es dentro de la red. Para la plantilla de cable virtual, el valor predeterminado es transparente.
S_Tmp_service_type	El tipo de servicio implementado por la plantilla. El valor predeterminado es cortafuegos y no se debe cambiar cuando se implementa el cortafuegos VM-Series.
S_Tmp_image_name	Este parámetro especifica la imagen base de la VM-Series utilizada por la plantilla de Heat cuando se implementa el cortafuegos VM-Series. Edite este parámetro para que coincida con el nombre de la imagen del cortafuegos VM-Series cargada en su entorno OpenStack.
S_Tmp_flavor	Este parámetro define los recursos de hardware asignados al cortafuegos VM-Series. El valor predeterminado es m1.large.

 ©2024 Palo Alto Networks, Inc.

Plantilla de servicio (ST Config)	
S_Tmp_interface_type_mgmt S_Tmp_interface_type_left S_Tmp_interface_type_right	Los parámetros definen el tipo de interfaz para las interfaces de gestión, izquierda y derecha.
Dominio	El dominio al que está vinculada esta plantilla de servicio. El valor predeterminado es default-domain.

Instancia de servicio

La porción de instancia de servicio del archivo de entorno de la plantilla de heat proporciona el nombre de la instancia individual implementada por la plantilla heat y la plantilla de servicio.

Instancia de servicio (Configuración de SI)	
S_Ins_name	El nombre de la instancia del servicio. Este es el nombre de la instancia de cortafuegos VM-Series en Contrail.
S_Ins_fq_name	El nombre completo de la instancia del servicio.

IPAM

La gestión de direcciones IP (IP address management, IPAM) proporciona la información de la dirección IP para las interfaces de la instancia del servicio. Cambia estos parámetros para que se adapten mejor a su entorno.

IPAM (configuración de IPAM)	
NetIPam_ip_prefix_mgmt	El prefijo IP de la interfaz de gestión en el cortafuegos VM-Series. El valor predeterminado es 172.2.0.0.
NetIPam_ip_prefix_len_mgmt	La longitud del prefijo IP de la interfaz de gestión en el cortafuegos VM-Series. El valor predeterminado es /24.
NetIPam_ip_prefix_left	El prefijo IP de la interfaz izquierda en el cortafuegos VM-Series. El valor predeterminado es 10.10.1.0.
NetIPam_ip_prefix_len_left	La longitud del prefijo IP de la interfaz izquierda en el cortafuegos VM-Series. El valor predeterminado es /24.
NetIPam_ip_prefix_right	El prefijo IP de la interfaz derecha en el cortafuegos VM-Series. El valor predeterminado es 10.10.2.0.
NetIPam_ip_prefix_len_right	La longitud del prefijo IP de la interfaz derecha en el cortafuegos VM-Series. El valor predeterminado es /24.

 ©2024 Palo Alto Networks, Inc.

IPAM (configuración de IPAM)	
NetIPam_addr_from_start_true	Este parámetro determina cómo se asignan las direcciones IP a las máquinas virtuales en las subredes descritas anteriormente. Si es verdadero, cualquier VM nueva toma la siguiente dirección IP disponible. Si es falso, a cualquier VM nueva se le asigna una dirección IP de forma aleatoria. El valor predeterminado es verdadero.

Política de servicio

La política de servicio define las reglas y políticas de redireccionamiento de tráfico que señalan el tráfico que pasa entre las máquinas virtuales izquierda y derecha a la instancia de servicio de cortafuegos VM-Series.

Política de servicio (Configuración de política)	
policy_name	El nombre de la política de servicio en Contrail que redireccione el tráfico a través del cortafuegos VM-Series. Para la plantilla L3, el valor predeterminado es PAN_SVM_policy-L3. Para la plantilla de cable virtual, el valor predeterminado es PAN_SVM_policy-vw.
policy_fq_name	El nombre completo de la política de servicio.
simple_action	La acción predeterminada de Contrail se aplica al tráfico que va a la instancia del servicio de cortafuegos VM-Series. El valor predeterminado es aprobado porque el cortafuegos VM-Series aplicará su propia política de seguridad al tráfico.
Protocol	Los protocolos permitidos por Contrail para pasar al cortafuegos VM-Series. El valor predeterminado es cualquiera.
src_port_end y src_port_start	Use este parámetro para especificar puertos de origen que deberían estar asociados a la regla de la política. Puede introducir un solo puerto, una lista de puertos separados por comas o un rango de puertos en formato <port>-<port>. El valor predeterminado es -1 en las plantillas heat proporcionadas; es decir, cualquier puerto de origen.
dirección	Este parámetro define la dirección del tráfico permitido por Contrail para pasar al cortafuegos VM-Series. El valor predeterminado es <> o tráfico bidireccional.
dst_port_end y dst_port_start	Use este parámetro para especificar los puertos de destino que deberían asociarse a la regla de la política. Puede introducir un solo puerto, una lista de puertos separados por comas o un rango de puertos en formato <port>-<port>.

 ©2024 Palo Alto Networks, Inc.

Política de servicio (Configuración de política)	
	El valor predeterminado es -1 en las plantillas heat proporcionadas; es decir, cualquier puerto de destino.

Alarma

Los parámetros de alarma se usan en el servicio de escalado y no están incluidos en los archivos de entorno de encadenamiento de servicios. Estos parámetros definen los umbrales utilizados por Contrail para determinar cuándo debería tener lugar el escalado. Este conjunto de parámetros solo lo usa la plantilla heat de escalado de servicios.

El tiempo predeterminado configurado bajo los parámetros de enfriamiento tiene como objetivo permitir que el cortafuegos tenga el tiempo suficiente para iniciarse. Si cambia los valores de enfriamiento, deje suficiente tiempo para que cada nueva instancia de cortafuegos se inicie.

Alarma	
meter_name	La métrica supervisada por Ceilometer y utilizada por contrail para determinar cuándo se debe desplegar o eliminar un cortafuegos adicional de la VM-Series. La plantilla heat usa la utilización de la CPU o bytes por segundo como métricas para el escalado del servicio.
cooldown_initial	La cantidad de tiempo que Contrail espera antes de iniciar una instancia de servicio adicional después de que se inicia la instancia de servicio inicial. El valor predeterminado es 1200 segundos.
cooldown_scaleup	La cantidad de tiempo que Contrail espera entre el inicio de la instancia de servicio adicional, después del primer inicio de la instancia de ampliación de servicio. El valor predeterminado es 1200 segundos.
cooldown_scaledown	La cantidad de tiempo que Contrail espera entre el cierre de instancias de servicio adicional, después de que la primera instancia de ampliación de servicio se cierra. El valor predeterminado es 1200 segundos.
period_high	El intervalo durante el cual la carga promedio de la CPU se calcula como alta antes de activar una alarma. El valor predeterminado es 300 segundos.
period_low	El intervalo durante el cual la carga promedio de la CPU se calcula como baja antes de activar una alarma. El valor predeterminado es 300 segundos.
threshold_high	El valor de la utilización de la CPU en porcentaje o en bytes por segundo a los que hace referencia Contrail antes de iniciar un evento de ampliación. El valor predeterminado es 40 % de utilización de la CPU o 2800 bytes por segundo.
threshold_low	El valor de la utilización de la CPU en porcentaje o en bytes por segundo a los que hace referencia Contrail antes de iniciar un evento de reducción. El

 ©2024 Palo Alto Networks, Inc.

Alarma	
	valor predeterminado es 20 % de utilización de la CPU o 12000 bytes por segundo.

 ©2024 Palo Alto Networks, Inc.

Instalación del cortafuegos VM-Series en una implementación de puerta de enlace básica

Complete los siguientes pasos para preparar las plantillas heat, los archivos de arranque y las imágenes de software necesarias para implementar el cortafuegos VM-Series en OpenStack. Después de preparar los archivos, implemente el cortafuegos VM-Series y el servidor Linux.

STEP 1 | Descargue la plantilla Heat y los archivos bootstrap de arranque.

Descargue el paquete de plantilla Heat del Repositorio GitHub.

STEP 2 | Descargue la imagen base de VM-Series.

1. Inicie sesión en el Sitio web de asistencia al cliente de Palo Alto Networks.
2. Seleccione **Software Updates (Actualizaciones de software)** y seleccione **PAN-OS for VM-Series KVM Base Images (Pan OS para imágenes base KVM de VM-Series)** del menú desplegable **Filter By (Filtrar por)**.
3. Descargue el archivo **qcow2** de VM-Series para KVM.

STEP 3 | Descargue Ubuntu 14.04 y suba la imagen al controlador OpenStack.

La plantilla Heat necesita una imagen Ubuntu para iniciar el servidor Linux.

1. Descargue Ubuntu 14.04.
2. Inicie sesión en la UI de Horizon.
3. Seleccione **Project (Proyecto)** > **Compute (Calcular)** > **Images (Imágenes)** > **Create Image (Crear imagen)**.
4. **Name (Nombre)** la imagen Ubuntu 14.04 para hacer coincidir el parámetro en el archivo pan_basic_gw_env.yaml.
5. Fije la fuente de imagen en el **Image File (Archivo de imagen)**.
6. Haga clic en **Choose file (Elija archivo)** y navegue hasta su archivo de imagen de Ubuntu.
7. Establezca el Formato para que coincida con el formato de archivo de su imagen de Ubuntu.
8. Haga clic en **Create Image (Crear imagen)**.

STEP 4 | Suba la imagen base de VM-Series para KVM al controlador OpenStack.

1. Inicie sesión en la UI de Horizon.
2. Seleccione **Project (Proyecto)** > **Compute (Calcular)** > **Images (Imágenes)** > **Create Image (Crear imagen)**.
3. En **Name (Nombre)**, asigne un nombre a la imagen para que coincida con de la imagen de su plantilla Heat.
4. Fije la fuente de imagen en el **Image File (Archivo de imagen)**.
5. Haga clic en **Choose file (Elija archivo)** y navegue hasta su archivo de imagen VM-Series.
6. Establezca el Formato en **QCOW2-QEMU Emulator (Emulador QCOW2-QEMU)**.
7. Haga clic en **Create Image (Crear imagen)**.

©2024 Palo Alto Networks, Inc.

STEP 5 | Cargue los archivos de arranque. Tiene dos opciones para pasar archivos de arranque a OpenStack: inyección de archivos (archivos de personalidad) o datos de usuario. Para pasar los archivos de arranque utilizando datos de usuario, debe colocar los archivos en una tar ball (archivo .tgz) y codificar esa tar ball con base64.

La inyección de archivos ya no es compatible a partir de OpenStack Queens; debes usar datos de usuario en su lugar.

- Para la inyección de archivos, cargue init-cfg.txt, bootstrap.xml y sus códigos de autenticación VM-Series en su controlador OpenStack o en un servidor web al que pueda acceder el controlador OpenStack.
- Si utiliza el método de **`-- datos de usuario`** para pasar el paquete de arranque a la unidad de configuración, puede usar el siguiente comando para crear la tar ball y codificarla (archivo .tgz) con base64:

```
tar -cvzf <file-name>.tgz config/ license software content base64
 -i <in-file> -o <outfile>
```

STEP 6 | Edite la plantilla pan_basic_gw.yaml para apuntar a los archivos de arranque y a los códigos de autenticación.

- Si está utilizando archivos personalizados, especifique la ruta del archivo o la dirección del servidor web para la ubicación de sus archivos en personalidad. Quite la marca de comentario de las líneas que no esté usando.

```
  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 está utilizando datos de usuario, especifique la ruta del archivo o la dirección del servidor web para la ubicación de sus archivos en user_data. Si tienes más de uno

```
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
```

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Edite el archivo de la plantilla pan_basic_gw_env.yaml para adaptarlo a su entorno. Asegúrese de que los valores de gestión y red pública coincidan con los que creó en su entorno OpenStack. Establezca pan_image para que coincida con el nombre que asignó al archivo de imagen base de la VM-Series. También puede cambiar su clave de servidor aquí.

```
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 | Implemente la plantilla Heat.

1. Ejecute el comando **`source openrc`**
2. Ejecute el comando **`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 | Compruebe que el cortafuegos VM-Series se implementa correctamente.

Puede usar los siguientes comandos para verificar el estado de creación de la pila.

- Verifique el estado de la pila con **`heat stack-list`**
- Consulte una lista detallada de eventos que ocurrieron durante la creación de la pila con **`heat event-list`**
- Vea detalles sobre tu pila con **`heat stack-show`**

STEP 10 | Compruebe que el cortafuegos VM-Series esté inspeccionando bidireccionalmente el tráfico que accede a los servidores Linux.

1. Inicie sesión en el cortafuegos.
2. Seleccione **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)** para ver la sesión SSH.

 ©2024 Palo Alto Networks, Inc.

Instalación del cortafuegos VM-Series con encadenamiento y escalado de servicios

Complete los siguientes pasos para preparar las plantillas heat, los archivos de arranque y las imágenes de software necesarias para implementar el cortafuegos VM-Series. Después de preparar los archivos, implemente el servicio de cortafuegos VM-Series y dos servidores Linux.

OpenStack Queens no es compatible con la implementación del cortafuegos VM-Series a través del encadenamiento o el escalado del servicio.

STEP 1 | Descargue la plantilla Heat y los archivos bootstrap de arranque.

Descargue el paquete de plantilla Heat del Repositorio GitHub.

STEP 2 | Descargue la imagen base de VM-Series.

1. Inicie sesión en el Sitio web de asistencia al cliente de Palo Alto Networks.
2. Seleccione **Software Updates (Actualizaciones de software)** y seleccione **PAN-OS for VM-Series KVM Base Images (Pan OS para imágenes base KVM de VM-Series)** del menú desplegable **Filter By (Filtrar por)**.
3. Descargue el archivo **qcow2** de VM-Series para KVM.

STEP 3 | Descargue Ubuntu 14.04 y suba la imagen al controlador OpenStack.

Para el encadenamiento de servicios, puede usar la imagen predeterminada proporcionada por OpenStack llamada TestVM. Omita este paso si usa TestVM. Para el escalado de servicios se requiere una imagen de Ubuntu.

1. Descargue Ubuntu 14.04.
2. Inicie sesión en la UI de Horizon.
3. Seleccione **Project (Proyecto)** > **Compute (Calcular)** > **Images (Imágenes)** > **Create Image (Crear imagen)**.
4. **Name (Nombre)** la imagen Ubuntu 14.04 para hacer coincidir el parámetro en el archivo pan_basic_gw_env.yaml.
5. Fije la fuente de imagen en el **Image File (Archivo de imagen)**.
6. Haga clic en **Choose file (Elija archivo)** y navegue hasta su archivo de imagen de Ubuntu.
7. Establezca el Formato para que coincida con el formato de archivo de su imagen de Ubuntu.
8. Haga clic en **Create Image (Crear imagen)**.

Se requiere una clave de servidor cuando se utiliza una imagen de Ubuntu. Asegúrese de que la clave del servidor se añade al archivo de entorno.

©2024 Palo Alto Networks, Inc.

STEP 4 | Suba la imagen base de VM-Series para KVM al controlador OpenStack.

1. Inicie sesión en la UI de Horizon.
2. Seleccione **Project (Proyecto)** > **Compute (Calcular)** > **Images (Imágenes)** > **Create Image (Crear imagen)**.
3. En **Name (Nombre)**, asigne un nombre a la imagen para que coincida con de la imagen de su plantilla Heat.
4. Fije la fuente de imagen en el **Image File (Archivo de imagen)**.
5. Haga clic en **Choose file (Elija archivo)** y navegue hasta su archivo de imagen VM-Series.
6. Establezca el Formato en **QCOW2-QEMU Emulator (Emulador QCOW2-QEMU)**.
7. Haga clic en **Create Image (Crear imagen)**.

STEP 5 | Cargue los archivos de arranque. Los archivos deben cargarse en la estructura de carpetas descrita aquí. La plantilla heat usa esta estructura de carpetas para localizar los archivos de arranque.

1. Inicie sesión en el controlador OpenStack.
2. Cree la siguiente estructura de carpetas:

   /root/bootstrap/config/

   /root/bootstrap/license/
3. Use SCP o FTP para añadir los archivos init-cfg.txt y bootstrap.xml a la carpeta config y añada los códigos de autenticación de la VM-Series a la carpeta de licencia.

STEP 6 | Edite el archivo de entorno de plantilla para adaptarlo a su entorno. Verifique que los nombres de las imágenes en el archivo de entorno coincidan con los que dio a los archivos cuando los cargó.

```
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
```

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Edite los archivos de plantilla para apuntar a los archivos de arranque y a los códigos de autenticación. En Personality (Personalidad), especifique la ruta del archivo a la ubicación de sus archivos. Quite la marca de comentario de las líneas que no esté usando.

```
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 | Suba los archivos de plantilla heat.

1. Inicie sesión en el controlador OpenStack.
2. Use SCP o FTP para añadir el archivo de plantilla heat y el archivo de entorno.

STEP 9 | Implemente la plantilla Heat.

1. Ejecute el comando **`source openrc`**
2. Ejecute el comando **`heat stack-create <stack-name> -f <template> -e ./<env-template>`**

STEP 10 | Compruebe que el cortafuegos VM-Series se implementa correctamente.

Puede usar los siguientes comandos para verificar el estado de creación de la pila.

- Verifique el estado de la pila con **`heat stack-list`**
- Consulte una lista detallada de eventos que ocurrieron durante la creación de la pila con **`heat event-list`**
- Vea detalles sobre tu pila con **`heat stack-show`**

STEP 11 | Compruebe que el cortafuegos VM-Series esté inspeccionando bidireccionalmente el tráfico entre los servidores Linux.

1. Inicie sesión en el cortafuegos.
2. Seleccione **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)** para ver la sesión SSH.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en Google Cloud Platform

Puede implementar un cortafuegos VM-Series en una instancia de Google Compute Engine en Google Cloud Platform.

- Implementaciones admitidas en Google Cloud Platform
- Preparación para configurar el cortafuegos VM-Series en la nube pública de Google
- Implementación del cortafuegos VM-Series en Google Cloud Platform
- Supervisión de VM con el complemento de Panorama para GCP
- Escalado automático del cortafuegos VM-Series en Google Cloud Platform
- Configurar HA activa/pasiva en Google Cloud Platform

Acerca del cortafuegos VM-Series en Google Cloud Platform

Los cortafuegos VM-Series cuentan con funciones de última generación para Google® Cloud Platform (GCP™).

Para maximizar el rendimiento, los cortafuegos VM-Series en GCP admiten bibliotecas del kit de desarrollo del plano de datos (Data Plane Development Kit, DPDK), que proporcionan el procesamiento rápido de paquetes y mejoran el rendimiento de la red sobre la base de combinaciones específicas de licencias del cortafuegos VM-Series y tamaños de máquinas virtuales (Virtual Machine, VM) de Google Cloud Platform.

- Google Cloud Platform y el cortafuegos VM-Series
- Requisitos mínimos del sistema para el cortafuegos VM-Series

Google Cloud Platform y el cortafuegos VM-Series

La integración del cortafuegos VM-Series con Google Cloud Platform (GCP) le permite implementar el cortafuegos VM-Series como una máquina virtual (virtual machine, VM) que se ejecuta en una instancia de Google Compute Engine. Este proceso se simplifica cuando Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace.

Tras implementar el cortafuegos VM-Series, puede configurar los siguientes servicios opcionales:

- Habilitar la supervisión de Google Stackdriver en el cortafuegos VM-Series: desde el cortafuegos, envíe las métricas de PAN-OS al servicio de Google Stackdriver.
- Habilitar la supervisión de VM para registrar cambios de VM en Google Cloud Platform: configure una fuente de información de VM que supervise la zona específica de GCP que contiene sus instancias. Los metadatos supervisados de VM pueden incluir propiedades predefinidas de GCP (como la ID de proyecto) y propiedades definidas por el usuario (como etiquetas y etiquetas de red).

Requisitos mínimos del sistema para el cortafuegos VM-Series

Debe seleccionar una licencia de cortafuegos VM-Series para nubes públicas y un método de licencia: licencia existente (Bring Your Own License, BYOL) o pago por consumo (Pay-as-you-go, PAYG). Para implementar un cortafuegos VM-Series en una instancia de Google Compute Engine, debe elegir un tipo de máquina que admita los requisitos del sistema de VM-Series para su licencia.

Una única instancia de Google Compute Engine admite hasta ocho interfaces de red. Si desea configurar ocho interfaces, seleccione un tipo de máquina n1-standard-8 o más grande.

Capacidad	BYOL	Paquetes 1 y 2	
		PAYG	Marketplace
Cortafuegos VM-100	✓		
Cortafuegos VM-200	✓		

©2024 Palo Alto Networks, Inc.

Capacidad	BYOL	Paquetes 1 y 2	
		PAYG	Marketplace
Cortafuegos VM-300	✓	✓	✓
Cortafuegos VM-1000-HV	✓		
Cortafuegos VM-500	✓		
Cortafuegos VM-700	✓		

El cortafuegos VM-Series admite los tipos de máquina estándar predefinidos que se enumeran a continuación. Puede elegir un tipo de máquina con mayor rendimiento o crear su propio tipo personalizado de máquina si los requisitos del recurso son compatibles con la licencia de su cortafuegos VM-Series.

- n1-standard-4
- n1-standard-8
- n1-standard-16
- n2-standard-4
- n2-standard-8
- n2-standard-16
- n2-standard-32

Tipos de máquinas personalizadas:

- e2-standard-4
- e2-standard-8
- e2-standard-16
- e2-standard-32

©2024 Palo Alto Networks, Inc.

Implementaciones admitidas en Google Cloud Platform

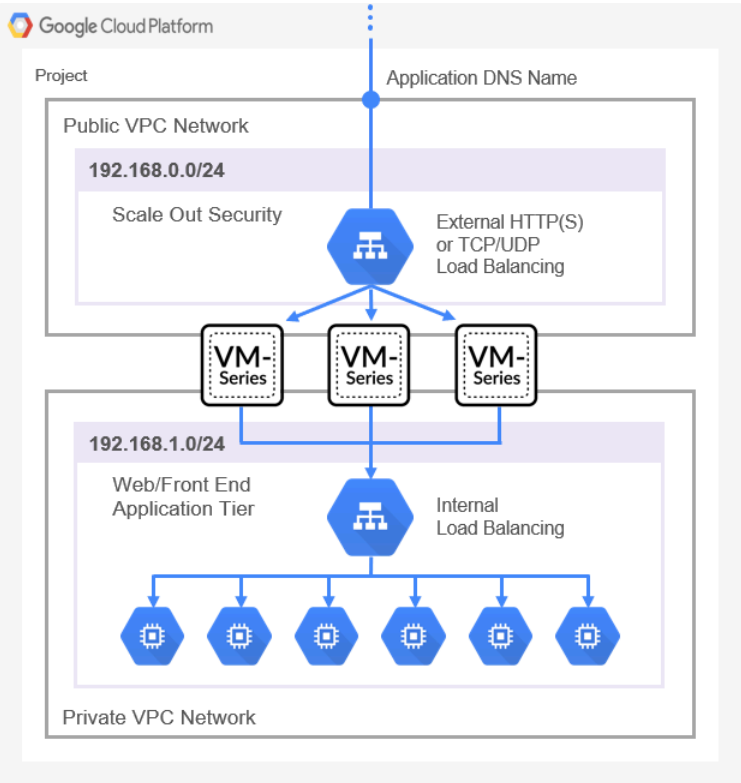
Puede implementar el cortafuegos VM-Series en una instancia de Google® Compute Engine en una red de su nube pública privada (VPC). Los tipos de implementaciones son los siguientes:

- Puerta de enlace de Internet
- Puerta de enlace de segmentación
- VPN IPSec híbrida

Puerta de enlace de Internet

El cortafuegos VM-Series asegura el tráfico vertical desde y hacia Internet para proteger las aplicaciones de amenazas conocidas y desconocidas. Un proyecto de Google puede tener hasta cinco redes VPC. Para acceder a un ejemplo común de una puerta de enlace de internet, consulte los ejemplos de configuración de Google.

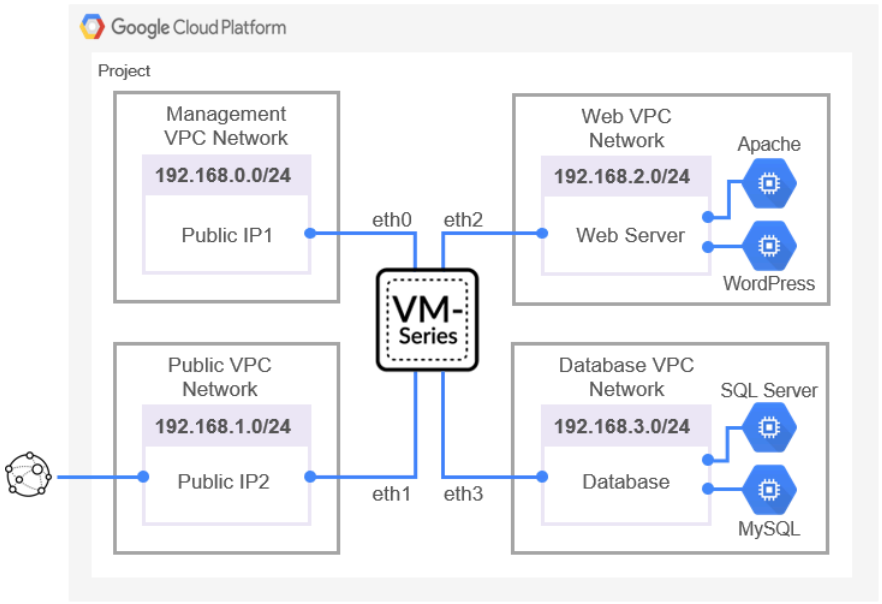
En entornos de nube pública, una práctica común es usar una arquitectura de ampliación (consulte la figura a continuación) en lugar de VM más grandes y con mayor rendimiento. Esta arquitectura (a veces denominada implementación *sándwich*) evita un punto único de falla y le permite añadir o eliminar cortafuegos según sea necesario.



Puerta de enlace de segmentación

Una puerta de enlace de segmentación protege el tráfico horizontal entre las nubes privadas virtuales (virtual private clouds, VPC) para asegurar el cumplimiento de la protección de datos y el acceso a la aplicación. La siguiente figura muestra un cortafuegos que protege el tráfico horizontal y vertical.

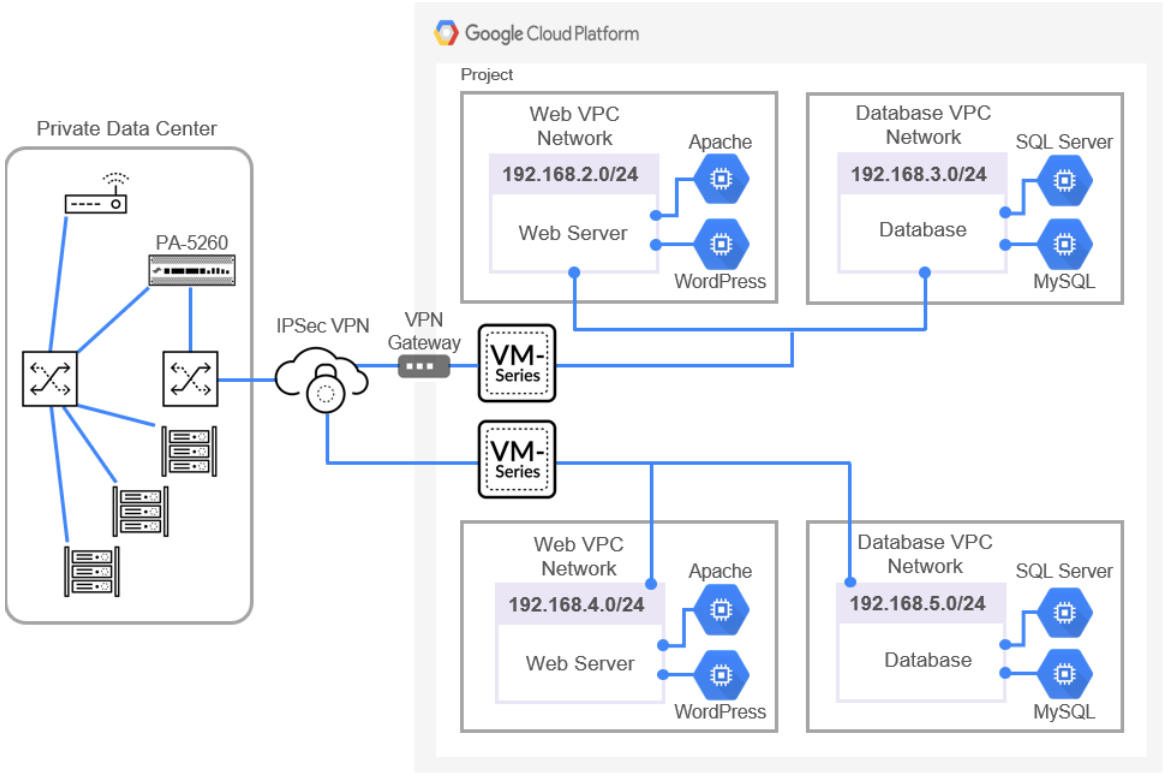
©2024 Palo Alto Networks, Inc.



VPN IPSec híbrida

El cortafuegos VM-Series sirve como un punto de finalización de VPN de IPSec, lo que permite las comunicaciones seguras desde y hacia las aplicaciones alojadas en Google Cloud Platform (GCP).

La implementación en la figura a continuación muestra una VPN de sitio a sitio desde una red local a un cortafuegos VM-Series implementado en GCP y una conexión IPSec desde una red local a una puerta de enlace de VPN de Google Cloud.



 ©2024 Palo Alto Networks, Inc.

Cree una imagen personalizada del cortafuegos VM-Series para Google Cloud Platform

Palo Alto Networks publica versiones de imagen base del cortafuegos de VM-Series o versiones secundarias con correcciones críticas (como PAN-OS 11.0) en Google Cloud Platform (GCP) Marketplace. Estas versiones están disponibles cuando implementa un cortafuegos VM-Series desde GCP Marketplace. Sin embargo, es posible que deba implementar una versión de PAN-OS que sea anterior o posterior a la versión de Marketplace.

Para implementar una versión del cortafuegos VM-Series que no está disponible en Marketplace, puede crear una imagen del cortafuegos VM-Series personalizada con una licenciaBYOL.

Los pasos básicos para crear un cortafuegos personalizado a partir de una instancia de cortafuegos son los siguientes:

- Implemente un nuevo cortafuegos desde GCP Marketplace.
- Active su licencia de cortafuegos, descargue la versión de software PAN-OS que desee en su cortafuegos, use Actualización dinámica para actualizar el contenido de sus **Applications and Threats (Aplicaciones y amenazas)** , y desactive la licencia del cortafuegos.
- Realce un restablecimiento de datos privados desde la consola de GCP.
- Cree una imagen personalizada desde el cortafuegos actualizado.

STEP 1 | Antes de crear su imagen personalizada, revise sus cuentas, planifique y cree las redes para la implementación del cortafuegos VM-Series, para la implementación del cortafuegos VM-Series y planifique sus interfaces de red.

STEP 2 | Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace

No es posible crear una imagen desde un cortafuegos existente. Comenzar a partir del GCP Marketplace garantiza que se pueda obtener una licencia para su imagen personalizada.

STEP 3 | (Solo BYOL) Activar la licencia.

1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y active la licencia.

   El cortafuegos se reinicia cuando se completa el proceso de licencia.
2. Inicie sesión en el cortafuegos.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Actualice a su versión de PAN-OS preferida e instale actualizaciones de software.

1. Seleccione **Device (Dispositivo)** > **Software** > **Check Now (Comprobar ahora)** y descargue la versión de PAN-OS requerida.

   Si no ve la versión que desea, descárguela del sitio web de atención al cliente de Palo Alto Networks de la siguiente manera.

   1. Inicie sesión y seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)**.

      En la lista **Filter By (Filtrar por)**, elija PAN-OS para VM-Series.
   2. Seleccione una versión de PAN-OS y descárguela a su máquina local.
   3. En su cortafuegos VM-Series, seleccione **Device (Dispositivo)** > **Software** y **Upload (Cargar)** para cargar su versión de PAN-OS desde su máquina local a su dispositivo.
2. Instale la versión seleccionada.
3. Actualice la versión del software PAN-OS:
4. Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y actualice sus **Applications and Threats (Aplicaciones y amenazas)** y cualquier otro contenido que desee incluir en su imagen base.

STEP 5 | (Solo BYOL) desactivar la máquina virtual del cortafuegos.



Si no desactiva la licencia, perderá la licencia que aplicó en su instancia de cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y, en **License Management (Gestión de licencias)**, seleccione **Deactivate VM (Desactivar máquina virtual)**.
2. Seleccione **Complete Manually (Completar manualmente)**y **Export (Exportar)** el token de licencia.
3. Vuelva al sitio web de Servicio de atención al cliente de Palo Alto Networks, seleccione **Assets (Activos)** > **VM-Series Auth-Codes (Códigos de autenticación de VM-Series)** > **Deactivate License(s) [Desactivar licencia(s)]** y cargue el token de licencia.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Realice un restablecimiento de datos privados.

Un restablecimiento de datos privados elimina todos los registros y restaura la configuración predeterminada.

Los discos del sistema no se borran, por lo que las actualizaciones de contenido del 4 están intactas.

1. Acceda a la CLI del cortafuegos y manténgala activa.
2. Desde la consola de GCP, elimine las claves SSH de su cortafuegos VM-Series.
   1. Seleccione **Compute Engine** > **VM Instances (Instancias de VM)** y seleccione el nombre de su instancia.
   2. En la vista **Details (Detalles)** , seleccione **EDIT (EDITAR)**.
   3. En **SSH Keys (Claves SSH)**, haga clic en el enlace **Show and edit (Mostrar y editar)** y haga clic en **X** para eliminar las claves SSH.
   4. Haga clic en **Save (Guardar)** para guardar sus cambios.
3. (Opcional) Exporte una copia de la configuración.
4. En la CLI, solicite un restablecimiento de datos privados.

   ```
   solicitud de restablecimiento de datos privados del sistema
   ```

   Introduzca **y** para confirmar.

   El cortafuegos se reinicia para inicializar la configuración predeterminada.
5. Desde la consola de GCP, seleccione **Compute Engine** > **VM instances (Instancias de VM)** y **STOP (DETENER)** el cortafuegos.

STEP 7 | Cree una imagen personalizada en la consola de GCP.

Estos pasos se basan en la Creación, eliminación y desuso de imágenes personalizadas.

1. Seleccione **Compute Engine** > **Images (Imágenes)** > **Create Image (Crear imagen)**.
2. Asigne un nombre a su imagen y seleccione la **Google-managed key (Clave gestionada por Google)** (consulte Claves de cifrado gestionadas por Google).
3. Seleccione **Disk (Disco)** para el origen y para el **Source disk (Disco de origen)**, seleccione la máquina virtual del cortafuegos VM-Series detenida y haga clic en **Create (Crear)**.
4. (Opcional) Cuando la imagen se haya completado, haga clic en el enlace **Equivalent REST (REST equivalente)** y, desde la **REST response (Respuesta REST)**, copie el enlace selfLink. Este es el enlace de URI para cualquier tipo de canal de CI/CD que necesite.

   Por ejemplo: `projects/my-vpc-vpcID/global/images/pa-vm-8-1-9`

   Al usar este enlace, apunta directamente a su imagen para que pueda usarla en una plantilla o un script. Por ejemplo:

   ```
   sourceImage: https://www.googleapis.com/compute/v1/projects/
   {{project}}/global/images/pa-vm-8-1-9}
   ```

 ©2024 Palo Alto Networks, Inc.

Preparación para configurar los cortafuegos VM-Series en la nube pública de Google

El proceso para Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace requiere tareas de preparación.

Si está implementando utilizando Google Marketplace, debe crear las redes y subredes de su proyecto, y planificar las redes y las asignaciones de direcciones IP para las interfaces del cortafuegos VM-Series por adelantado. Durante la implementación, debe seleccionar entre las redes y subredes existentes.

Consulte los siguientes temas cuando planifique su implementación:

- Requisitos generales
- Instalación del complemento VM-Series en Panorama
- Instalación del complemento de Panorama para GCP
- Prepárese para implementar desde GCP Marketplace

Requisitos generales

Los componentes de esta lista de comprobación son comunes para implementar un cortafuegos VM-Series que gestiona directamente o con Panorama. Se aplican requisitos adicionales para el complemento de Panorama para servicios como la supervisión de Stackdriver, la supervisión de VM, el escalado automático o la protección de las implementaciones de Kubernetes.

Consulte siempre la Matriz de compatibilidad para la información del complemento Panorama para nubes públicas. Esta versión requiere el siguiente software:

- **Cuenta GCP**: debe tener una cuenta de usuario de GCP con una dirección de correo electrónico enlazada y debe conocer el nombre de usuario y la contraseña de esa dirección de correo electrónico.
- **SDK de Google Cloud**: si no lo ha hecho, instale SDK de Google Cloud, que incluye las API de Google Cloud, gcloud y otras herramientas de línea de comandos. Puede utilizar la interfaz de línea de comandos para implementar la plantilla de cortafuegos y otras plantillas.
- **PAN-OS en cortafuegos VM-Series en GCP**: cortafuegos VM-Series que ejecutan una versión de PAN-OS disponible en Google Marketplace.
  - **Cortafuegos VM-Series**: los cortafuegos VM-Series que desee gestionar desde Panorama deben implementarse en Google Cloud Platform mediante una imagen de Palo Alto Networks de Google Marketplace. Los cortafuegos deben cumplir con Requisitos mínimos del sistema para el cortafuegos VM-Series.
  - **Licencias VM-Series**: debe obtener una licencia de un cortafuegos VM-Series para obtener un número de serie. Se requiere un número de serie para añadir un cortafuegos VM-Series como dispositivo gestionado de Panorama. Si está utilizando el complemento de Panorama para GCP para implementar cortafuegos VM-Series, debe proporcionar un código de autenticación BYOL. Google Marketplace gestiona la facturación de su servicio, pero los cortafuegos que implemente se conectarán directamente con el servidor de licencias de Palo Alto Networks.
  - **Complemento de VM-Series en el cortafuegos**: los cortafuegos VM-Series que ejecutan PAN-OS 9.0 y versiones posteriores incluyen el Complemento de VM-Series, que gestiona la integración con

 ©2024 Palo Alto Networks, Inc.

nubes públicas y privadas. Como se muestra en la Matriz de compatibilidad, el Complemento de VM-Series tiene una versión mínima que corresponde a cada versión de PAN-OS.

Cuando hay una actualización importante de PAN-OS, la versión del complemento de VM-Series se actualiza automáticamente. Para versiones menores, depende de usted determinar si es necesaria una actualización del complemento de VM-Series y, de ser así, realizar una actualización manual. Consulte Instalación del complemento VM-Series en Panorama.

- **Panorama ejecutado en modo de gestión** : un dispositivo físico o virtual de Panorama que ejecuta una versión de PAN-OS que es igual o posterior a los cortafuegos gestionados. No es necesario implementar instancias virtuales en GCP.
  - Debe tener una versión con licencia de Panorama.
  - Panorama debe tener acceso de red a las VPC en las que están implementadas las máquinas virtuales que desea gestionar.
  - Si su idea es gestionar máquinas virtuales implementadas en GCP, o configurar funciones como el escalado automático, sus versiones de PAN-OS y del Complemento de VM-Series deben cumplir con los requisitos de Nube pública para ser compatible con el complemento de Panorama para GCP.
  - Complemento de VM-Series en Panorama. Consulte Instalación del complemento VM-Series en Panorama
- **Complemento de Panorama para GCP versión 2.0.0**: el complemento de GCP gestiona las interacciones necesarias para otorgar licencias, arrancar y configurar cortafuegos implementados con las plantillas de supervisión de VM o Auto Scaling. El complemento GCP, junto con las plantillas de supervisión de VM o Auto Scaling, usa pilas de plantillas de plantillas de Panorama y grupos de dispositivos para programar reglas NAT que dirigen el tráfico a los cortafuegos gestionados VM-Series.

  Consulte Instalación del complemento de Panorama para GCP.

Instalación del complemento VM-Series en Panorama

En Panorama, instale o actualice a la versión del complemento de VM-Series que admita las funciones de GCP que desea configurar, como se detalla en la tabla Matriz de compatibilidad para Nubes públicas.

Instalación inicial: debido a que el complemento de VM-Series es opcional en Panorama, la primera vez que instale debe descargar el complemento de VM-Series desde el Portal de asistencia técnica, luego vaya a **Panorama** > **Device Deployment (Implementación de dispositivos)** > **Plugins (Complementos)** para cargar e instalar.

Actualización: vaya a **Panorama** > **Device Deployment (Implementación de dispositivo)** > **Plugins (Complementos)** y haga clic en **Check Now (Comprobar ahora)**. Instale una versión que cumpla con los requisitos de la tabla Matriz de compatibilidad para Nubes públicas.

Instalación del complemento de Panorama para GCP

El complemento de Panorama para GCP es necesario si desea utilizar Panorama para gestionar las implementaciones de supervisión de VM o escalado automático creadas con plantillas de Palo Alto Networks. Instale la versión del complemento de VM-Series que admita las funciones de GCP que desea configurar, como se detalla en la tabla Matriz de compatibilidad para Nubes públicas.



No puede actualizar el complemento de Panorama para GCP de la versión 1.0.0 a la versión 2.0.x. Si ha instalado la versión 1.0.0, elimínela antes de instalar 2.0.x.

 ©2024 Palo Alto Networks, Inc.

Si tiene un Panorama independiente o dos dispositivos Panorama instalados en un par de alta disponibilidad con varios complementos instalados, es posible que los complementos no reciban información actualizada sobre la etiqueta IP si uno o más de los complementos no están configurados. Esto ocurre porque Panorama no reenviará la información de la etiqueta IP a los complementos no configurados. Además, este problema puede ocurrir si uno o más de los complementos de Panorama no están en el estado Registrado o Correcto (el estado positivo varía según cada complemento). Asegúrese de que sus complementos estén en el estado positivo antes de continuar o ejecutar los comandos que se describen a continuación.

Si encuentra este problema, hay dos soluciones:

- Desinstale el complemento o complementos no configurados. Se recomienda que no instale un complemento que no planifique configurar de inmediato
- Puede utilizar los siguientes comandos para solventar este problema. Ejecute el siguiente comando para cada complemento no configurado en cada instancia de Panorama, para evitar que Panorama espere para enviar actualizaciones. Si no lo hace, sus cortafuegos pueden perder cierta información de la etiqueta IP.

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

  Puede cancelar este comando ejecutando:

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

Los comandos descritos no son persistentes en los reinicios y deben usarse de nuevo para cualquier reinicio posterior. Para Panorama en el par de HA, los comandos deben ejecutarse en cada Panorama.

STEP 1 | Verifique su instalación de Panorama.

En Panorama, asegúrese de que su versión de PAN-OS cumpla con los requisitos necesarios para admitir el escalado automático de GCP.

STEP 2 | Eliminación del complemento de Panorama para GCP v1.0.

Si tiene instalado el complemento de Panorama v1.0, debe eliminarlo.

STEP 3 | Instalación del complemento de Panorama para GCP.

Seleccione **Panorama** > **Plugins (Complementos)** y escriba **`gcp`** en la barra de búsqueda. **Instale** la versión del complemento que admita las funciones que desea configurar (consulte la tabla Matriz de compatibilidad para Nubes públicas).

Después de la instalación, puede ver el complemento en la lista **General Information (Información general)** de la consola de Panorama. Vea **Panorama** > **Google Cloud Platform** y verá las interfaces **Setup (Configuración)**, **Monitoring Definition (Definición de monitorización)** y **AutoScaling (Escalado automático)**.

STEP 4 | (Opcional) Si sus dispositivos Panorama poseen una configuración de alta disponibilidad, debe instalar manualmente la misma versión del complemento de Google en ambos pares de Panorama.

Configure el complemento de Google en el par activo de Panorama únicamente. Después de confirmarlo, la configuración se sincroniza con el par pasivo de Panorama. Solo el par activo de Panorama sondea las máquinas virtuales de Google que ha configurado para la supervisión de VM.

 ©2024 Palo Alto Networks, Inc.

Prepárese para implementar desde GCP Marketplace

Revise estos requisitos para garantizar que cuenta con las cuentas y los permisos apropiados antes de utilizar Google Marketplace para implementar el cortafuegos en una instancia de Google Compute Engine (GCE).

- Cuentas y permisos generales
- Recursos de Google disponibles
- Métodos de autenticación de Google
- Par de claves SSH

Cuentas y permisos generales

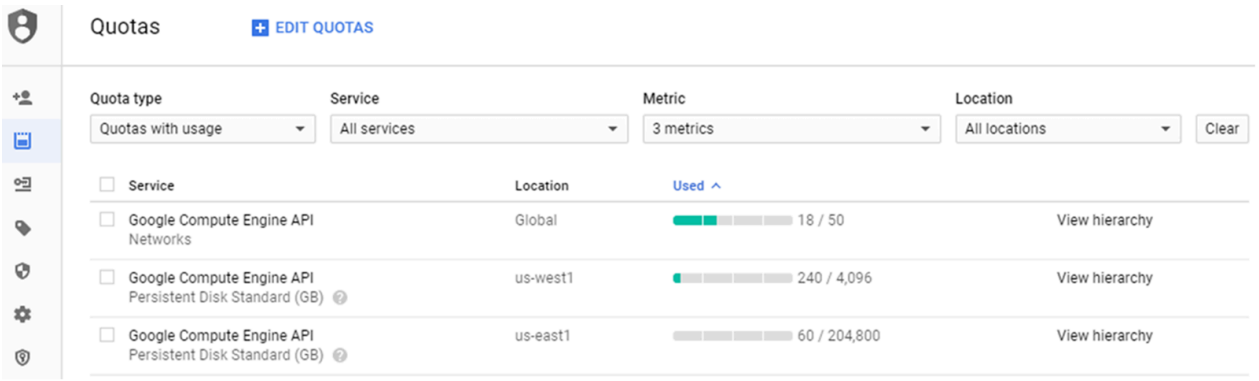
- Tanto usted, como los usuarios a los que dé permiso, deben tener las siguientes funciones o permisos de gestión de identidad y acceso (Identity and Access Management, IAM) equivalentes mínimos para conectarse al cortafuegos VM-Series:
  - **Visor de Compute**: El Visor de Compute le permite obtener y mostrar una lista de los recursos de Compute Engine sin poder leer los datos almacenados en esos recursos.
  - **Visor de objetos de almacenamiento**: te permite arrancar con un depósito de almacenamiento de Google en el mismo proyecto.

  > *Los usuarios de su organización pueden tener permisos de IAM o funciones predefinidos que son más permisivos de lo necesario. Asegúrese de restringir adecuadamente el acceso al cortafuegos VM-Series.*

  También puede restringir el acceso con cuentas de servicio, como se describe en Métodos de autenticación de Google.
- **Escritor de métricas de supervisión**: requerido para Stackdriver.

Recursos de Google disponibles

Su proyecto tiene suficientes recursos para implementar el cortafuegos VM-Series como una instancia de Google Compute Engine. Si implementa una solución de Marketplace de GCP, determine si la solución implementa otras VM además del cortafuegos. En Google Cloud Console, seleccione **IAM & admin (IAM y administración)** > **Quotas (Cuotas)** para revisar las cuotas de recursos para su proyecto, y las redes y el espacio en el disco utilizados. Si se agotan sus recursos, puede solicitar a Google que asigne más a su organización.



 ©2024 Palo Alto Networks, Inc.

Métodos de autenticación de Google

GCP admite varias maneras de conectarse a una instancia. Puede autenticarse con una cuenta de servicio o un par de claves SSH.

1. **Cuentas de servicio**: las Cuentas de servicio se aplican a las aplicaciones o a las VM, no a los usuarios finales. Por lo general, se usan para controlar el acceso cuando usa programas o secuencias de comandos, o accede al cortafuegos desde la línea de comandos de gcloud. Si usa las cuentas de servicio de Google para autenticar instancias o aplicaciones, debe conocer la dirección de correo electrónico de las cuentas. Consulte Creación y gestión de claves de la cuenta del servicio.

   Es necesario utilizar una cuenta de servicio si desea conectarse al cortafuegos VM-Series desde fuera del proyecto, ya sea desde un proyecto diferente o desde la línea de comandos. Por ejemplo, si desea habilitar un cortafuegos físico de última generación para supervisar su cortafuegos VM-Series, debe guardar la información de la cuenta de servicio del cortafuegos VM-Series en un archivo JSON. En el cortafuegos físico, puede cargar el archivo cuando configura la conexión.

   1. Seleccione **IAM & Admin (IAM y administración)** > **Service accounts (Cuentas de servicio)** y elija **+Create Service Account (+Crear cuenta de servicio)**.

      Introduzca el nombre y la descripción de la cuenta de servicio y haga clic en **Create (Crear)**.
   2. Seleccione un tipo de función en el menú desplegable y, a la derecha, seleccione un nivel de acceso adecuado.

      Por ejemplo, seleccione Proyecto> Editor. Puede seleccionar varias funciones para una cuenta de servicio. Cuando haya terminado, haga clic en **Continue (Continuar)**.
   3. Otorgue permiso a usuarios específicos para acceder a esta cuenta de servicio. Seleccione miembros de la columna **Permissions (Permisos)** a la derecha para otorgarles permiso para acceder a las funciones en el paso anterior.
2. **Claves SSH**: si implementa el cortafuegos VM-Series desde Marketplace, debe proporcionar una clave de Open SSH en formato RSA para los metadatos de la instancia de Google Compute Engine.

   El cortafuegos VM-Series solo acepta una clave por implementación.

   Durante la implementación, debe pegar la clave pública en la implementación de Marketplace, como se describe en Par de claves SSH. Tras la implementación, puede usar la clave privada de SSH en el cortafuegos para configurar la cuenta de administrador. Para añadir usuarios, consulte Gestión de administradores de cortafuegos.

Puede autenticarse de varias formas:

- **Crear cuentas de servicio para instancias**: puede crear una cuenta de servicio para una instancia o grupo de instancias específico y otorgar permisos específicos, que a su vez se pueden otorgar a los usuarios.

 ©2024 Palo Alto Networks, Inc.

- **Usar la cuenta de servicio predeterminada para su proyecto**: si usa la consola de Google Cloud Platform (GCP™), inicie sesión con su dirección de correo electrónico y podrá acceder a una instancia GCE según los permisos o las funciones que el administrador del proyecto asignó a su cuenta.

  Cada instancia de Google Compute Engine creada con Google Cloud Console o la herramienta de línea de comandos de gcloud tiene una cuenta de servicio predeterminada con el nombre en formato de dirección de correo electrónico:

  `<project-number>-compute@developer.gserviceaccount.com`

  Para ver el nombre de la cuenta de servicio de la instancia del cortafuegos, vea los detalles de la instancia y desplácese hasta la parte inferior (consulte la cuenta de servicio predeterminada de Compute Engine).

  La cuenta de servicio predeterminada puede gestionar la autenticación a las máquinas virtuales en el mismo proyecto como un cortafuegos VM-Series. Los ámbitos de acceso permiten que el cortafuegos inicie las llamadas a la API para las VM en un proyecto de Google Cloud.
- **Usar permisos de IAM y la API de Google:** si usa las API del SDK de Google y gcloud, debe llamar a las API para la autenticación.
  - Generalmente, use el SDK de Google cuando desee gestionar el cortafuegos desde una línea de comandos o ejecutar una secuencia de comandos para configurar el cortafuegos.
  - Debe acceder a las API de Google si una máquina virtual a la que se conecta tiene una imagen personalizada con aplicaciones que requieren las API de Google.

Par de claves SSH

Cuando implementa el cortafuegos VM-Series desde Google Marketplace, necesita un par de claves SSH para autenticarse con el cortafuegos VM-Series.

Cree el par de claves según la documentación de su generador de claves. No edite el archivo de clave pública. De lo contrario, se arriesga a introducir caracteres ilegales.

El cortafuegos VM-Series gestiona la autenticación de manera diferente a las instancias de GCE. Después de la implementación, primero inicie sesión con el usuario **`admin`**. El nombre de usuario predeterminado del cortafuegos VM-Series se acepta solo una vez. Después de iniciar sesión correctamente, debe configurar un nombre de usuario y una contraseña de administrador para la interfaz web del VM-Series; (consulte Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace).

El campo **SSK Key (Clave SSH)** de la interfaz de implementación de Google Marketplace muestra el siguiente marcador:

`admin:ssh-rsa your-SSH-key`

`admin` es el nombre de usuario del administrador del cortafuegos VM-Series es necesario para iniciar sesión en el cortafuegos por primera vez. Añada el prefijo **`admin:`** en el campo Marketplace cuando Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace.

No puede iniciar sesión en el cortafuegos VM-Series si no proporciona toda la clave pública o si su clave tiene caracteres ilegales cuando pega la clave en el campo **SSH key (Clave SSH)** de Marketplace. Cuando introduce la clave SSH en el cortafuegos VM-Series por primera vez, la clave pública se transfiere al cortafuegos.

 ©2024 Palo Alto Networks, Inc.

Si la clave pública está dañada, debe eliminar la implementación y empezar de nuevo. Cualquier red y subred permanece, pero las reglas del cortafuegos deben volver a crearse.

STEP 1 | Cree un par de claves SSH y almacene el par de claves SSH en la ubicación predeterminada para su sistema operativo que se menciona en Ubicación de una clave SSH.

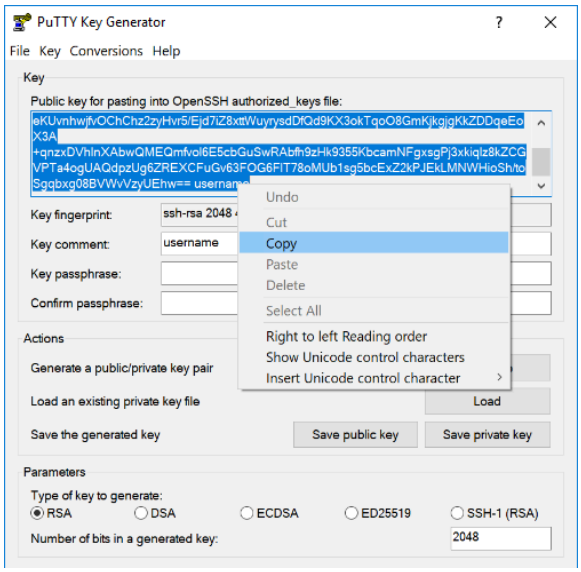
- **Linux o MacOS**: utilice `ssh-keygen` para crear el par de claves en su directorio .ssh.
- **Windows**: utilice PuTTYgen para crear el par de claves.

  El contenido en el campo **Key comment (Comentario sobre la clave)** no es relevante para el cortafuegos VM-Series; puede aceptar el valor predeterminado (la fecha de creación de la clave) o introducir un comentario que ayude a recordar el nombre del par de claves. Use el botón **Save private key (Guardar clave privada)** para almacenar la clave privada en su directorio .ssh.

STEP 2 | Seleccione la clave pública completa.

- **Linux o MacOS**: abra la clave pública en un editor de texto y copie la clave pública.
- **Windows**: debe usar el generador de claves de PuTTY para ver la clave pública. Inicie PuTTYgen, haga clic en **Load (Cargar)** y busque la clave privada que guardó en su directorio .ssh.

  En PuTTYgen, desplácese hacia abajo para asegurarse de seleccionar la clave completa, haga clic derecho y seleccione Copy (Copiar).



 ©2024 Palo Alto Networks, Inc.

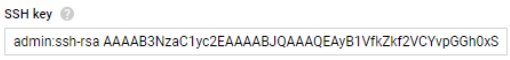
STEP 3 | Introduzca la clave pública en el campo de la clave SSH como se detalla a continuación.

1. En el campo **SSH key (Clave SSH)** de Marketplace, elimine el texto del marcador e introduzca:

   `admin:`

   Asegúrese de que no existan espacios adicionales después de los dos puntos.

2. Inserte el cursor después de **`admin:`** y seleccione **Paste as plain text (Pegar como texto)**. La clave debe estar en una sola línea, como se muestra a continuación:

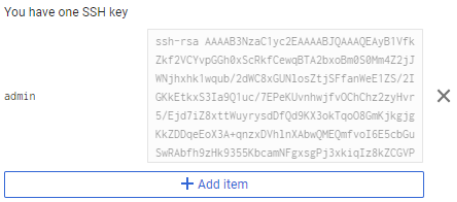
3. Mueva el cursor al final de la clave, añada un espacio y escriba: **`admin`**

   El contenido final del campo **SSH key (Clave SSH)** debe ser:

   `admin:ssh-rsa` [KEY] **`admin`**

STEP 4 | Revisa la clave.

Después de la implementación y antes de intentar iniciar sesión en el cortafuegos, vea la instancia de gestión y compruebe la clave en busca de saltos de línea y espacios adicionales:



Si toda la clave está en una línea y el formato es **`admin:ssh-rsa`** [KEY] **`admin`**, ya ha terminado.

STEP 5 | (opcional) Si algo está mal, debe sustituir la clave.

1. Haga clic en la **X** para eliminar la clave y haga clic en **+ Add item (+ Añadir elemento)**.
2. Introduzca la clave como se describe en el Paso 3. Ahora el campo **SSH key (Clave SSH)** debe mostrar:

   `admin:ssh-rsa` [KEY] **`admin`**
3. Haga clic en **Guardar** para introducir la implementación actualizada.
4. Vuelva a comprobar la clave.

Planificación de red de la nube privada virtual (VPC)

Antes de realizar la implementación desde Google Market, planifique las Redes de VPC (denominadas *redes*), subredes (también conocidas como *subredes*) y reglas de cortafuegos de Google. Debe crear redes y subredes antes de comenzar con Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace.

La página de implementación de Marketplace muestra únicamente redes y subredes que existen cuando inicia la implementación. Si falta una red, debe salir de la implementación, crear la red y comenzar nuevamente.

 ©2024 Palo Alto Networks, Inc.

- **Redes de VPC**: debe crear una red personalizada específicamente para cada interfaz de red del cortafuegos VM-Series.
  - Consulte Licencias de cortafuegos VM-Series para nubes públicas para determinar el número de interfaces de red necesarias en función de su licencia de cortafuegos VM-Series. Como mínimo, configure las tres redes y subredes de VPC necesarias para el inicio del cortafuegos VM-Series.
  - Un proyecto de GCP tiene una red predeterminada con configuraciones preestablecidas y reglas de cortafuegos; puede eliminar la red predeterminada, si no la utiliza.
  - De manera predeterminada, existen hasta cinco redes en un proyecto. Su administrador de GCP puede solicitar redes adicionales para su proyecto.
  - Para conectarse a la interfaz de gestión, debe crear una regla del cortafuegos de GCP que permita el acceso. Puede realizarlo durante la implementación si selecciona **Enable GCP Firewall rule for connections to Management interface (Habilitar regla en el cortafuegos de GCP para las conexiones con la interfaz de gestión)** y proporcionar un bloque CIDR para la **Source IP in GCP Firewall rule for connections to Management Interface (IP de origen en la regla del cortafuegos de GCP para conexiones con la interfaz de gestión)**.

    Asegúrese de que sus redes incluyan todas las instancias que desea proteger.

- **Subredes**: una instancia de Compute Engine puede admitir hasta ocho interfaces de capa 3 en una sola instancia. Las interfaces de gestión, fiables y no fiables, consumen tres interfaces y puede crear hasta cinco interfaces adicionales para el plano de datos. Por lo general, las interfaces del plano de datos representan redes de aplicaciones.
- **Direcciones IP**: cuando crea subredes de interfaz, proporciona intervalos de Direcciones IP y tiene la opción de habilitar una dirección externa cuando implementa una subred.
  - Cuando crea una subred de red, debe especificar un rango de direcciones IP. Este rango se utiliza para la red interna, por lo que no puede superponerse con otras subredes.
  - Durante la implementación, puede optar por habilitar una dirección IP externa al crear una interfaz de red. De manera predeterminada, recibe una dirección IP efímera. No puede proporcionar una dirección IP estática reservada durante la implementación, pero puede ascender la dirección efímera a una dirección IP estática después de completar el proceso de implementación (consulte Promoción de una dirección IP efímera externa).

Planificación de interfaz de red

Cuando realice la implementación desde Google Cloud Platform Marketplace, la implementación predeterminada del cortafuegos VM-Series tiene tres interfaces: la interfaz del plano de gestión y las interfaces del plano de datos fiable y no fiable. Puede definir instancias del plano de datos adicionales, en función de los recursos informáticos disponibles en su máquina virtual (VM); consulte Licencias de cortafuegos VM-Series para nubes públicas.

Durante la implementación, podrá asignar un nombre a estas interfaces.

Orden de interfaces

Cuando realice la implementación con Marketplace, el orden de las interfaces de red está predefinido. La interfaz de gestión se asigna a eth0, no fiable a eth1 y fiable a eth2. Marketplace usa este orden porque la asignación de la interfaz de gestión a eht0 y la interfaz no fiable a eth1 es necesaria si debe intercambiar la interfaz de gestión para garantizar el equilibrio de las cargas.

 ©2024 Palo Alto Networks, Inc.

Interfaz de gestión

La primera interfaz de red que añade se asigna a eth0 en el cortafuegos e incluye la opción de habilitar el reenvío de IP. Use esta interfaz de red para gestionar el cortafuegos VM-Series. Por lo general, esta interfaz tiene una dirección IP externa.



Solo se requiere una dirección de IP externa si la interfaz del plano de datos está conectada a la subred pública. En el momento de la creación, puede recibir una dirección IP efímera y ascenderla a una dirección IP estática después de completar la implementación (consulte Promoción de una dirección IP efímera externa*).*

Interfaces del plano de datos (fiable, no fiable)

Cuando lleva a cabo implementaciones desde Marketplace, el orden en el que añade interfaces está predeterminado.

- Configure la interfaz no fiable después de la interfaz de gestión. Este orden implica que la interfaz no fiable se asigna a eth1. Las interfaces no fiables generalmente se conectan a la subred pública y tienen una dirección IP externa.

  Solo se requiere una dirección de IP externa si la interfaz del plano de datos está conectada a la subred pública. En el momento de la creación, puede recibir una dirección IP efímera, luego promoverla a una dirección IP estática, como se analizó en Promoción de una dirección IP efímera externa.

- La interfaz fiable debe estar después de la interfaz no fiable, de modo que se asigne a eth2. La interfaz fiable con frecuencia no tiene una dirección IP externa. Puede añadir interfaces del plano de datos adicionales después de la interfaz fiable.

Interfaces del plano de datos adicionales

Planee interfaces para las aplicaciones que desea proteger, como servidores web, bases de datos y otras aplicaciones en su red. Puede crear hasta cinco interfaces del plano de datos adicionales, además de las tres que son necesarias para iniciar su cortafuegos. Asegúrese de que las aplicaciones que desea proteger se encuentren en redes que se conectan al cortafuegos VM-Series.

 ©2024 Palo Alto Networks, Inc.

Implementación del cortafuegos VM-Series en Google Cloud Platform

Para implementar el cortafuegos VM-Series con la plantilla de GCP marketplace, primero debe crear una red de VPC para cada interfaz en el cortafuegos. Después de implementar el cortafuegos desde Google Marketplace, puede iniciar sesión en el cortafuegos para ajustar la configuración para que funcione dentro de su configuración de VPC de GCP. También puede habilitar la supervisión para recopilar métricas que le permitan mejorar la gestión de recursos o crear reglas de políticas de seguridad que se adapten automáticamente a los cambios en el entorno de su aplicación.

- Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace
- Intercambio de interfaces de gestión para el equilibrio de carga de Google Cloud Platform
- Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión
- Habilitación de la supervisión de Google Stackdriver en el cortafuegos VM-Series
- Habilitación de supervisión de VM para el registro de cambios de VM en Google Cloud Platform (GCP)
- Uso de grupos de direcciones dinámicas para proteger instancias dentro de la VPC
- Uso de plantillas personalizadas o la CLI de gcloud para implementar el cortafuegos VM-Series

Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace

Puede usar Google® Cloud Platform Marketplace para implementar el cortafuegos VM-Series en una licencia de capacidad fija de vCPU (Modelos VM-Series). Las imágenes con licencia disponibles en las nubes públicas son:

- Paquete 1 de cortafuegos VM-Series de última generación
- Paquete 2 de cortafuegos VM-Series de última generación
- Cortafuegos VM-Series de última generación (BYOL)

Consulte Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace para obtener más información sobre estas opciones de licencia.

Marketplace implementa una instancia del cortafuegos VM-Series con un mínimo de una interfaz de gestión y dos interfaces del plano de datos (fiable y no fiable). Puede añadir interfaces del plano de datos adicionales para hasta cinco instancias de Compute Engine en su nube privada virtual (VPC).

Antes de implementar el cortafuegos VM-Series, debe crear o seleccionar un proyecto en su organización y crear las redes y subredes que se conectarán con el cortafuegos, como se describe en Planificación de redes de VPC y Planificación de interfaz de red.

No puede conectar varias interfaces de red a la misma red de VPC. Cada interfaz que crea debe tener una red dedicada con al menos una subred. Asegúrese de que sus redes incluyan las instancias del plano de datos adicionales que crea.

STEP 1 | Seleccione un método de arranque.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Localice la lista de cortafuegos VM-Series en Marketplace.

1. Inicie sesión en Google Cloud Console.
2. En el menú Products and Services (Productos y servicios), seleccione **Marketplace**.
3. Busque **`VM-Series`**.
4. Seleccione una de las opciones de licencia del cortafuegos VM-Series.

STEP 3 | Haga clic en **Launch on Compute Engine (Iniciar en Compute Engine)**.

STEP 4 | Nombre la instancia y seleccione los recursos.

1. Introduzca el **Deployment Name (Nombre de la implementación)** (este nombre de muestra en el gestor de implementaciones). El nombre debe ser único y no puede entrar en conflicto con ninguna otra implementación del proyecto.
2. Seleccione una **Zone (Zona)**. Consulte Regiones y zonas para acceder a una lista de las zonas compatibles.
3. Seleccione el **Machine Type (Tipo de máquina)** según los Requisitos del sistema para VM-Series para su licencia y los Requisitos mínimos del sistema para el cortafuegos VM-Series en Google Cloud Platform.

STEP 5 | **Especifique los metadatos de instancia**.

Las opciones **Bootstrap Bucket (Depósito de arranque)** y **Interface Swap (Intercambio de interfaces)** afectan a la configuración inicial la primera vez que se reinicia el cortafuegos VM-Series.

1. **Bootstrap Bucket (Depósito de arranque)** (Opcional): si planea usar un archivo de arranque, introduzca el nombre de un depósito de almacenamiento o la ruta a una carpeta dentro del depósito de almacenamiento que contiene el paquete de arranque. Necesita permiso para acceder al depósito de almacenamiento. Por ejemplo:

   `vmseries-bootstrap-gce-storagebucket=<bucketname>`

   O

   `vmseries-bootstrap-gce-storagebucket=<bucketname/directoryname>`

   Si elige iniciar con metadatos personalizados, continúe al Paso 6.
2. **Interface Swap (Intercambio de interfaces)** (Opcional): intercambie la interfaz de gestión (eth0) y la primera interfaz del plano de datos (eth1) durante la implementación. El intercambio de interfaz solo es necesario cuando implementa el cortafuegos VM-Series detrás del balanceador de carga de HTTP(S) de Google Cloud Platform. Para más detalles, consulte Intercambio de interfaces de gestión para el equilibrio de carga de Google Cloud Platform.
3. **SSH key (Clave SSH)**: pegue la clave pública de un par de claves SSH. Siga las instrucciones para su sistema operativo en Par de claves SSH para crear, copiar y pegar la clave. Los usuarios

 ©2024 Palo Alto Networks, Inc.

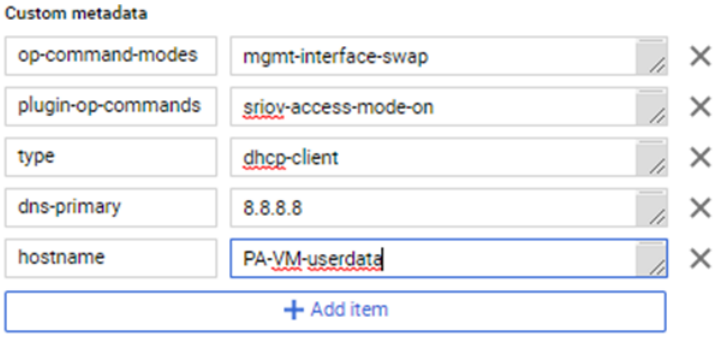
de Windows deben ver la clave en PuTTY, copiarla de la interfaz del usuario y pegarla en la implementación de Marketplace.

Si la clave no se formatea adecuadamente, el cortafuegos VM-Series no le permite iniciar sesión. Debe eliminar la implementación y comenzar nuevamente.

4. Haga clic en **More (Más)** para revelar opciones adicionales de metadatos. Las opciones **blockProjectKeys** y **enableSerialConsole** son propiedades de la instancia; puede cambiar estos valores de metadatos tras una implementación correcta.
   - **blockProjectKeys** (Opcional): si bloquea las claves del proyecto, podrá usar solo la clave SSH pública que brindó para acceder a la instancia.
   - **enableSerialConsole** (Opcional): interactuar con la consola de serie le permite supervisar la creación de instancias y realizar tareas de depuración interactivas.

STEP 6 | **Especifique metadatos personalizados**.

Si elige iniciar con metadatos personalizados, añada cualquier par clave-valor que no haya añadido en el Paso 5. Consulte Componentes de archivo de init-cfg.txt para obtener la lista de pares clave-valor. Por ejemplo:



STEP 7 | **Configure el disco de inicio**.

1. **Boot disk type (Tipo de disco de arranque)**: seleccione disco SSD persistente o disco estándar persistente. Consulte las opciones de almacenamiento.
2. Introduzca el **Boot disk size (Tamaño del disco de arranque)**; 60 GB es el tamaño mínimo. Puede editar el tamaño de disco más adelante, pero debe detener la VM para hacerlo.

STEP 8 | Configure la interfaz de gestión.

1. **Management VPC Network name (Nombre de la red de VPC de gestión)**: seleccione una red existente
2. **Management Subnet name (Nombre de la subred de gestión)**: seleccione una subred existente.
3. **Enable External IP for Management interface (Habilitar IP externa para la interfaz de gestión)** (Opcional): si habilita esta opción, puede usar la dirección IP asignada a la interfaz de gestión del cortafuegos VM-Series para usar SSH a fin de acceder a la interfaz web del cortafuegos VM-Series.
4. **Enable GCP Firewall rule for connections to Management interface (Habilitar regla en el cortafuegos de GCP para las conexiones con la interfaz de gestión)** (Opcional): esta opción

 ©2024 Palo Alto Networks, Inc.

crea automáticamente una regla Allow (Permitir) en el cortafuegos de GCP para una dirección IP de origen externo que proporcione.

5. **Source IP in GCP Firewall rule for connections to Management Interface (IP de origen en la regla del cortafuegos de GCP para conexiones con la interfaz de gestión)**: si selecciona **Enable GCP Firewall rule for connections to Management interface (Habilitar regla en el cortafuegos de GCP para las conexiones con la interfaz de gestión)**, introduzca una dirección IP de origen o un bloque CIDR.
   - No use 0.0.0.0/0. Proporcione una dirección IP o un bloque CIDR que corresponda a sus direcciones IP o red de gestión dedicadas. No configure el rango de la red de origen en un valor mayor al necesario.
   - Verifique la dirección para asegurarse de que no se bloquea.

STEP 9 | Configure la interfaz del plano de datos no fiable.

1. **Untrust VPC Network name (Nombre de la red de VPC no fiable)**: seleccione una red existente.
2. **Untrust Subnet name (Nombre de la subred no fiable)**: seleccione una subred existente.
3. **Enable External IP for Untrust (Habilitar IP externa para interfaces no fiables)**: permita que GCP brinde una dirección IP efímera que actúe como dirección IP externa.

STEP 10 | Configure la interfaz del plano de datos fiable.

1. **Trust VPC Network name (Nombre de la red de VPC fiable)**: seleccione una red existente.
2. **Trust Subnet name (Nombre de la subred fiable)**: seleccione una subred existente.
3. **Enable External IP for Trust (Habilitar IP externa para interfaces fiables)**: permita que GCP proporcione una dirección IP efímera que actúe como dirección IP externa.

STEP 11 | Configure interfaces adicionales. Debe introducir el número de interfaces del plano de datos que desea añadir; el valor predeterminado es 0 (ninguno). La página de implementación muestra siempre los campos de cinco planos de datos adicionales enumerados del 4 al 8.

1. **Additional Dataplane interfaces (Interfaces adicionales del plano de datos)**: introduzca el número de instancias adicionales del plano de datos.

   Si este número es 0 (predeterminado), se ignoran los números del plano de datos 4 a 8 incluso si completa los campos de la interfaz. Si, por ejemplo, especifica 2 y completa la información de las tres interfaces, solo se crearán las dos primeras.

2. **Additional Dataplane # VPC name (Nombre de la VPC del número del plano de datos adicional)**: seleccione una red existente.
3. **Dataplane # Subnet name (Nombre de la subred del número del plano de datos)**: seleccione una subred que exista.
4. **Enable External IP for dataplane # interface (Habilitar IP externa para la interfaz del número del plano de datos)**: permita que GCP proporcione una dirección IP efímera que actúe como dirección IP externa.

STEP 12 | Haga clic en **Deploy (Implementar)** para implementar la instancia.

STEP 13 | Use el gestor de implementación de Google Cloud para ver y gestionar su implementación.

 ©2024 Palo Alto Networks, Inc.

STEP 14 | Use la CLI para modificar la contraseña de administrador en el cortafuegos.

1. Inicie sesión en el cortafuegos VM-Series desde la línea de comandos. En su herramienta SSH, conéctese a la IP externa para la interfaz de gestión y especifique la ruta a su clave privada.

   Usuarios de Windows: Use PuTTY para conectarse al cortafuegos VM-Series y realizar las instrucciones en la línea de comandos. Para especificar la ruta a la clave privada, seleccione **Connection (Conexión)** > **SSH** > **Auth (Autenticación)**. En **Private key file for authentication (Archivo de clave privada para autenticación)**, haga clic en **Browse (Examinar)** para seleccionar su clave privada.
2. Introduzca el modo de configuración:

   ```
   VMfirewall> configure
   ```
3. Introduzca el siguiente comando:

   ```
   VMfirewall # set mgt-config users admin password
   ```
4. Introduzca y confirme una nueva contraseña para el administrador.
5. Confirme su contraseña nueva:

   ```
   VMfirewall # commit
   ```
6. Regrese al modo de comando:

   ```
   VMfirewall # exit
   ```
7. (Opcional) Si implementó un archivo de arranque para el intercambio de interfaces, use el siguiente comando para ver la asignación de interfaces:

   ```
   VMfirewall> debug show vm-series interfaces all
   ```

STEP 15 | Acceda a la interfaz web del cortafuegos VM-Series.

1. En un navegador, cree una conexión segura (https) con la dirección IP para la interfaz de gestión.

   Si recibe un error de red, compruebe si tiene una regla en el cortafuegos de GCP que permita la conexión.
2. Cuando se le solicite, introduzca el nombre de usuario (admin) y la contraseña de administrador que especificó desde la CLI.
3. (Opcional) Si realizó un arranque, verifique la realización del arranque.

   Si se producen problemas, busque la información del log en el cortafuegos VM-Series. Seleccione **Monitor (Supervisar)** > **System (Sistema)** y, en el campo de búsqueda manual, introduzca **`description contains 'bootstrap'`** y busque un mensaje en los resultados que indique que el arranque se realizó con éxito.

Después de iniciar sesión en el cortafuegos, puede añadir administradores y crear interfaces, zonas, reglas NAT y reglas de la política, al igual que lo haría en un cortafuegos físico.

Intercambio de interfaces de gestión para el equilibrio de carga de Google Cloud Platform

Debido a que el equilibrio de cargas interno puede enviar tráfico solamente a la interfaz principal de la siguiente instancia de Google compute Engine de carga equilibrada, el cortafuegos VM-Series debe poder utilizar eth0 para el tráfico del plano de datos.

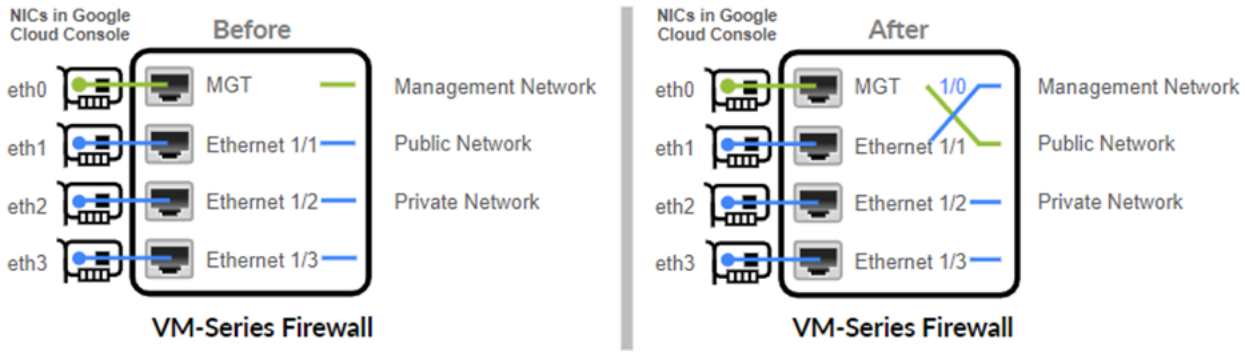
 ©2024 Palo Alto Networks, Inc.

El cortafuegos puede recibir tráfico del plano de datos en eth0 si el cortafuegos VM-Series está detrás de la interfaz del equilibrio de cargas interno de Google Cloud Platform.

- Los cortafuegos VM-Series protegen el tráfico de salida directamente a Internet sin necesidad de utilizar un enlace VPN o un enlace de conexión directa a la red corporativa.
- El cortafuegos VM-Series protege la aplicación que se conecta a internet cuando hay exactamente un servidor back-end, como un servidor web, para cada cortafuegos. Los cortafuegos VM-Series y los servidores web pueden escalar de forma lineal, en pares, detrás de la dirección del equilibrio de cargas interno de Google.

Para que el cortafuegos envíe y reciba tráfico del plano de datos en eth0, en vez de eth1, debe intercambiar la asignación de la interfaz de red del equilibrio de cargas interno dentro del cortafuegos, de modo que eth0 se asigne a ethernet 1/1 y eth1 se asigne a la interfaz MGT en el cortafuegos.

Si es posible, intercambie la asignación de la interfaz de gestión antes de configurar el cortafuegos y definir reglas de política.



El intercambio de la asignación de las interfaces asignadas permite a Google Cloud Platform distribuir y dirigir el tráfico a instancias en buen estado del cortafuegos VM-Series situadas en zonas diferentes o en las mismas zonas.

Intercambio de la interfaz de gestión

Puede intercambiar las interfaces cuando lo desee, o puede configurar el cortafuegos una vez creado.

En la creación: cuando implementa el cortafuegos VM-Series, puede habilitar el intercambio de interfaces de dos maneras.

- Google Cloud Console: en el formulario Create Instance (Crear instancia), introduzca un par clave-valor en el campo **Metadata (Metadatos)**, donde **`mgmt-interface-swap`** es la clave y **`enable`** es el valor.
- Archivo de arranque: cree un archivo de arranque que incluya el comando operativo **`mgmt-interface-swap`** en la configuración de arranque, como se describe en Arranque del cortafuegos VM-Series en Google Cloud Platform. En el formulario Create Instance (Crear instancia), introduzca un par clave-valor en el campo **Metadata (Metadatos)** para habilitar la opción de arranque.

Desde el cortafuegos VM-Series: inicie sesión en el cortafuegos y Use la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión. En el modo operativo, ejecute el siguiente comando:

```
set system setting mgmt-interface-swap enable yes
```

 ©2024 Palo Alto Networks, Inc.

- *Elija un método para especificar la configuración de intercambio de interfaces: el archivo de configuración de arranque, la CLI del cortafuegos o el campo **Metadata (Metadatos)** de la instancia de Google Compute Engine (que se accede desde Google Cloud Console). El uso de un método garantiza un comportamiento predecible en el cortafuegos.*

  Desde Google Cloud Console no es posible confirmar si ha intercambiado eth0 y eth1. Luego del intercambio, debe recordar que el equilibrio de cargas esté en eth0 y que la interfaz de gestión del cortafuegos sea eth1 de modo que pueda configurar el equilibrio de cargas de Google Cloud Platform, y cree reglas de políticas de seguridad para proteger el equilibrio de cargas de uno o más cortafuegos VM-Series.
- *Si configuró el cortafuegos VM-Series antes del intercambio, compruebe si algún cambio en la dirección IP para eth0 y eth1 afecta a las reglas de política.*

Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión

Esta tarea solo es necesaria si su arquitectura coloca el cortafuegos VM-Series detrás del balanceador de carga interno de Google Cloud Platform.

Si no especificó los metadatos para intercambiar la interfaz de gestión (management interface, MGT) con la interfaz del plano de datos cuando implementó el cortafuegos, puede utilizar la CLI para habilitar el cortafuegos a fin de recibir tráfico del plano de datos en la interfaz principal.

STEP 1 | Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace.

Antes de continuar, verifique que el cortafuegos tiene un mínimo de dos interfaces de red (eth0 y eth1). Si inicia el cortafuegos con solo una interfaz, el comando de intercambio de interfaces hará que el cortafuegos se inicie en el modo de mantenimiento.

STEP 2 | En Google Cloud Console, consulte los detalles de la instancia de VM para verificar las direcciones IP de la interfaz de red de la interfaz eth1 y verifique que las reglas de seguridad permitan las conexiones (HTTPS y SSH) en la interfaz de gestión nueva (eth1).

STEP 3 | Inicie sesión en la CLI del cortafuegos VM-Series e introduzca el comando siguiente:

```
set system setting mgmt-interface-swap enable yes
```

Puede ver la asignación predeterminada desde la interfaz de la línea de comandos. Los resultados son similares a lo siguiente:

```
> debug show vm-series interfaces all Interface_name Base-
OS_port   mgt              eth0   Ethernet1/1      eth1
   Ethernet1/2      eth2
```

STEP 4 | Confirme que desea intercambiar la interfaz (utilice la interfaz del plano de datos eth1 como interfaz de gestión).

STEP 5 | Reinicie el cortafuegos para que se produzca el intercambio:

```
request restart system
```

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Verifique que se hayan intercambiado las interfaces:

```
debug show vm-series interfaces all
```

Habilitación de la supervisión de Google Stackdriver en el cortafuegos VM-Series

Un cortafuegos VM-Series en una instancia de Google® Compute Engine puede publicar métricas PAN-OS personalizadas en Google Stackdriver. Estas métricas le permiten evaluar el rendimiento y los patrones de uso, de modo que pueda gestionar los recursos de su cortafuegos según corresponda.

- Permisos de Google Stackdriver
- Habilitar Google Stackdriver

Permisos de Google Stackdriver

Los requisitos de autenticación varían en función de si puede usar la cuenta de servicio predeterminada para realizar la autenticación o si necesita usar las API de Google para autenticarse.

Puede realizar la autenticación de dos maneras:

- **Usar la cuenta de servicio predeterminada para la instancia del cortafuegos VM-Series**: si usa la consola de Google Cloud Platform (GCP™), inicie sesión con su dirección de correo electrónico y podrá acceder a la instancia según los permisos o las funciones que el administrador del proyecto asignó a su cuenta.
- **Usar permisos de IAM y la API de Google:** si usa las API del SDK de Google y gcloud, debe llamar a las API para la autenticación. Generalmente, use el SDK de Google cuando desee gestionar el cortafuegos desde una línea de comandos o ejecutar una secuencia de comandos para configurar el cortafuegos.

Cada instancia de Google Compute Engine creada con Google Cloud Console o la herramienta de la línea de comandos gcloud tiene una cuenta de servicios predeterminada con el nombre en formato de dirección de correo electrónico:

```
<project-number>-compute@developer.gserviceaccount.com
```

Para ver el nombre de la cuenta de servicios para la instancia del cortafuegos, consulte los detalles de la instancia y desplácese hasta abajo (consulte la cuenta de servicio predeterminada de Compute Engine).

La cuenta de servicio predeterminada puede gestionar la autenticación para supervisar las VM en el mismo proyecto como un cortafuegos VM-Series.

- Los ámbitos de acceso predeterminados permiten que el cortafuegos inicie las llamadas a la API para supervisar las VM en un proyecto de Google Cloud.
- No necesita acceder a las API de Google salvo que una de las máquinas virtuales supervisadas tenga una imagen personalizada con las aplicaciones que requieren las API de Google.

Si desea configurar la supervisión desde un cortafuegos físico o un cortafuegos VM-Series en un proyecto diferente, debe usar las API de Google para la autenticación. Hay dos requisitos previos:

- Las API de Google deben estar instaladas.
- Su cuenta debe tener las funciones de escritor de métricas de supervisión y visor de cuentas de Stackdriver.

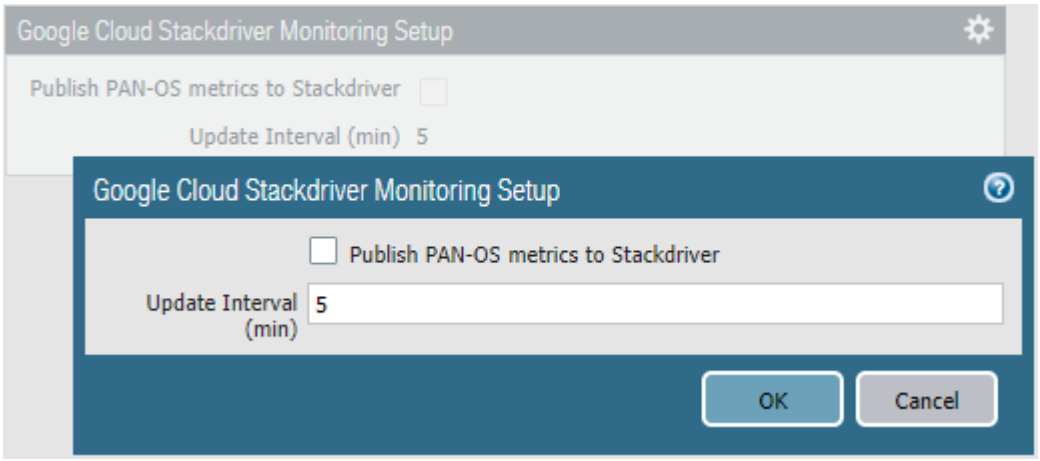
 ©2024 Palo Alto Networks, Inc.

Habilitar Google Stackdriver

Para obtener una descripción de las métricas de PAN-OS que puede publicar en Google Stackdriver, consulte Métricas personalizadas de PAN-OS publicadas para la supervisión.

STEP 1 | Implemente las métricas de PAN-OS desde un cortafuegos VM-Series en una instancia de Google Compute Engine a Stackdriver.

1. Inicie sesión en la interfaz web del cortafuegos VM-Series.
2. Seleccione **Device (Dispositivo)** > **VM-Series**. En la configuración de supervisión de Google Cloud Stackdriver, haga clic en **Edit** ( ).
   1. Consulte **Publicación de métricas de PAN-OS en Stackdriver**.



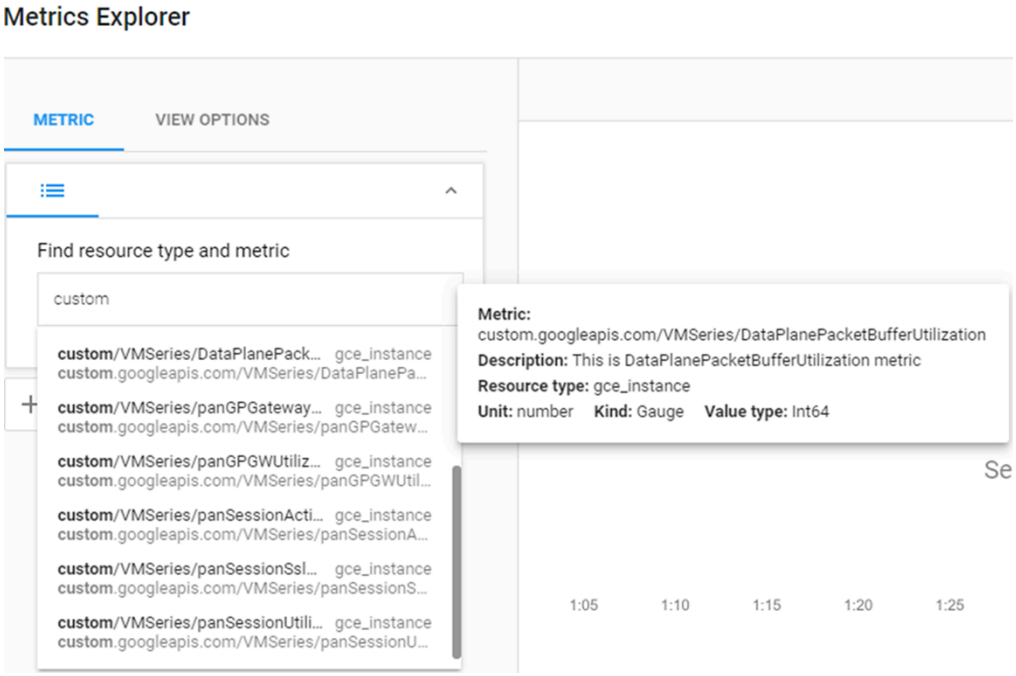
   2. Especifique el **Update Interval (Intervalo de actualización)** (el intervalo es de 1 a 60 minutos; el valor predeterminado es de 5). Esta es la frecuencia con la que el cortafuegos publica las métricas en Stackdriver.
   3. Haga clic en **OK (Aceptar)**.
3. Haga clic en **Commit (Confirmar)** para compilar los cambios.

   Espere hasta que el cortafuegos comience a publicar las métricas en Stackdriver antes de configurar alarmas para las métricas de PAN-OS.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Compruebe que pueda ver las métricas en Stackdriver.

1. En Google Cloud Console, seleccione **Products and Services (Productos y servicios)** > **Monitoring (Supervisión)**.
2. En Stackdriver, seleccione **Resources (Recursos)** > **Metrics Explorer (Explorador de métricas)**.
3. En la sección Find resource type and metric (Buscar tipo y métrica del recurso), introduzca **`custom`** en el campo de búsqueda para filtrar las métricas de PAN-OS.



STEP 3 | Configure alertas y acciones para métricas PAN-OS en Stackdriver. Consulte Inicio rápido de la supervisión para Google Compute Engine e Introducción de Stackdriver a las alertas.

Habilitación de supervisión de VM para el registro de cambios de VM en Google Cloud Platform (GCP)

Puede habilitar cortafuegos que ejecuten PAN-OS 9.0 (virtuales o físicos) para supervisar las cargas de trabajo de la aplicación en instancias de Google Compute Engine. La supervisión de VM le permite controlar un conjunto predefinido de elementos de metadatos o atributos en el cortafuegos VM-Series. En la Guía del administrador de PAN-OS 9.1, consulte Atributos supervisados en máquinas virtuales en plataformas en la nube.

Si tiene conocimientos sobre cómo añadir, mover y eliminar máquinas virtuales dentro de un VPC de Google, puede crear reglas de la política de seguridad que automáticamente se adapten a los cambios en su entorno de aplicación. A medida que implementa o mueve máquinas virtuales, el cortafuegos recopila atributos (o elementos de metadatos). Puede usar estos metadatos para la coincidencia de políticas o para definir grupos de direcciones dinámicas (consulte Uso de grupos de direcciones dinámicas para proteger instancias dentro de la VPC).

 ©2024 Palo Alto Networks, Inc.

Puede configurar hasta diez fuentes de información de VM en cada cortafuegos o sistema virtual en un cortafuegos con capacidad para varios sistemas virtuales. Los orígenes de información también se pueden enviar con plantillas de Panorama.

Para realizar la supervisión de VM, debe tener el escritor de métricas de supervisión con función de IAM.

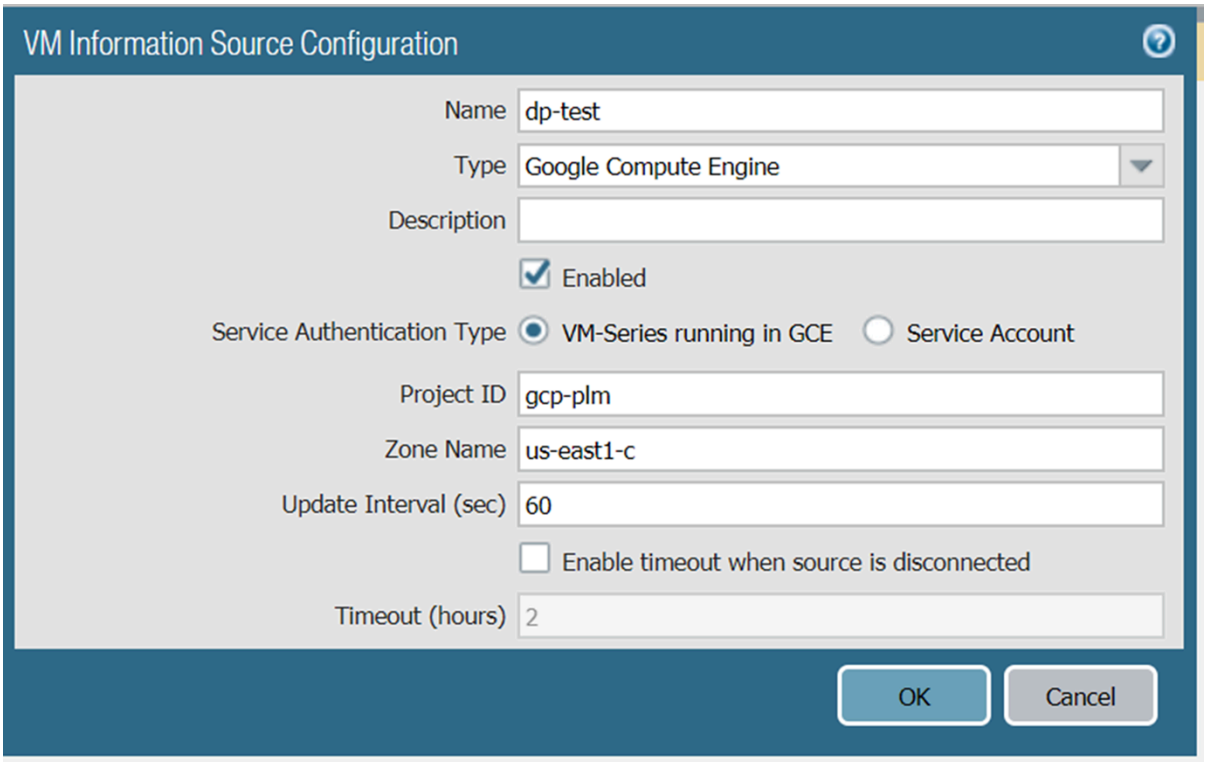
STEP 1 | Inicie sesión en el controlador implementado.

STEP 2 | Habilite la supervisión de VM.

1. Seleccione **Device (Dispositivo)** > **VM Information Sources (Fuentes de información de equipo virtual)**.
2. Haga clic en **Add (Añadir)** para añadir una fuente de información de VM e introduzca la siguiente información:
   - Especifique un **Name (Nombre)** para identificar la instancia que desea supervisar.
   - Seleccione el **Type (Tipo)** de Google Compute Engine.
   - Seleccione **Enabled (Habilitado)**.
   - Elija el **Service Authentication Type (Tipo de autenticación del servicio)**.
     - Si selecciona **VM-Series running in GCE (VM-Series que se ejecuta en GCE)**, realizará la autenticación con la cuenta de servicio predeterminada que se generó cuando se creó la instancia. Esto forma parte de los metadatos de la instancia.
     - Si desea supervisar desde un cortafuegos fuera del proyecto actual, seleccione **Service Account (Cuenta de servicio)**. Debe cargar las credenciales de la cuenta de servicio en formato JSON. Consulte Creación y gestión de claves de la cuenta del servicio.
   - (Opcional) Modifique el **Update interval (Intervalo de actualización)** a un valor entre 5-600 segundos. De manera predeterminada, el cortafuegos sondea cada 5 segundos.

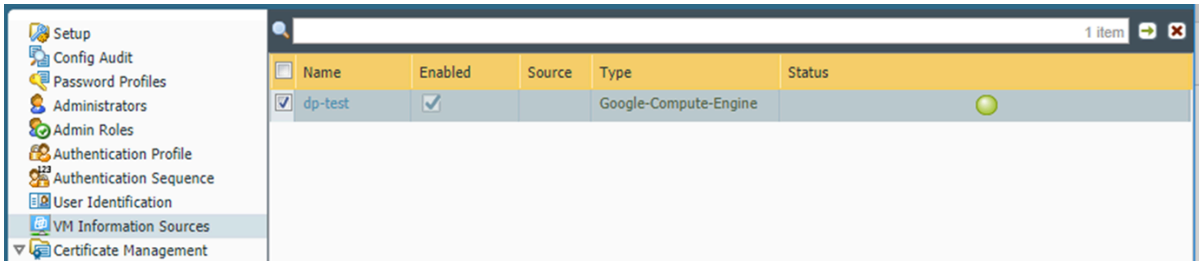
 ©2024 Palo Alto Networks, Inc.

Las llamadas de la API se ponen en cola y recuperan cada 60 segundos, de modo que las actualizaciones pueden tardar hasta 60 segundos, más el intervalo de sondeo configurado.



- (Opcional) Para cambiar el número de horas antes del tiempo de espera, seleccione **Enable timeout when the source is disconnected (Habilitar tiempo de espera cuando el origen está desconectado)** e introduzca el tiempo de espera (horas) antes de que la conexión al origen supervisado se cierre (el intervalo es de 2 a 10; el valor predeterminado es de 2).

  Si el cortafuegos no puede acceder al host y se alcanza el límite especificado, el cortafuegos cierra la conexión al origen.
- Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.



STEP 3 | Comprobar el estado de conexión.

Si el estado de conexión está pendiente o desconectado, compruebe que el origen está operativo y que el cortafuegos puede acceder al origen. Si usa un puerto diferente al puerto de gestión (Management, MGT) para la comunicación con el origen supervisado, debe cambiar la ruta de servicio (seleccione **Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]**, haga clic en **Service Route Configuration [Configuración de ruta de servicios]** y modifique la **Source Interface [Interfaz de origen]** para el servicio **VM Monitor [Supervisor de VM]**).

 ©2024 Palo Alto Networks, Inc.

Uso de grupos de direcciones dinámicas para proteger instancias dentro de la VPC

En un entorno dinámico como Google® Cloud Platform (GCP™), donde inicia las nuevas instancias a demanda, la sobrecarga administrativa de la gestión de la política de seguridad puede ser excesiva. El uso del uso de grupos de direcciones dinámicas en la política aporta agilidad y evita las interrupciones en los servicios o brechas de seguridad.

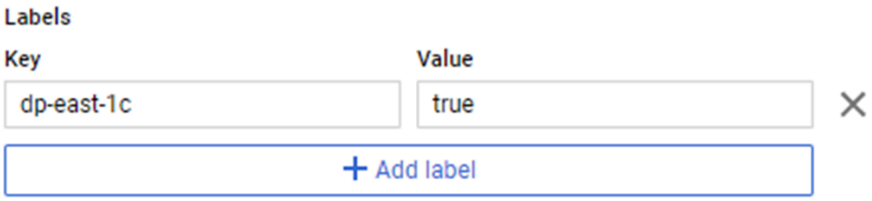
Este flujo de trabajo asume que implementó un cortafuegos VM-Series, configuró algunas aplicaciones en las instancias, y habilitó la supervisión de Google Stackdriver.

STEP 1 | Configure el cortafuegos para supervisar la VPC.

STEP 2 | Etiquete instancias en la VPC.

Una etiqueta es un par nombre-valor. Puede etiquetar recursos desde Google Cloud Console, desde las llamadas a la API de Google o desde Google Cloud Shell. En esta tarea etiquetamos instancias, pero estas etiquetas se pueden aplicar a muchos recursos como se describe en Etiquetado de recursos.

También puede añadir etiquetas desde el navegador de instancias.

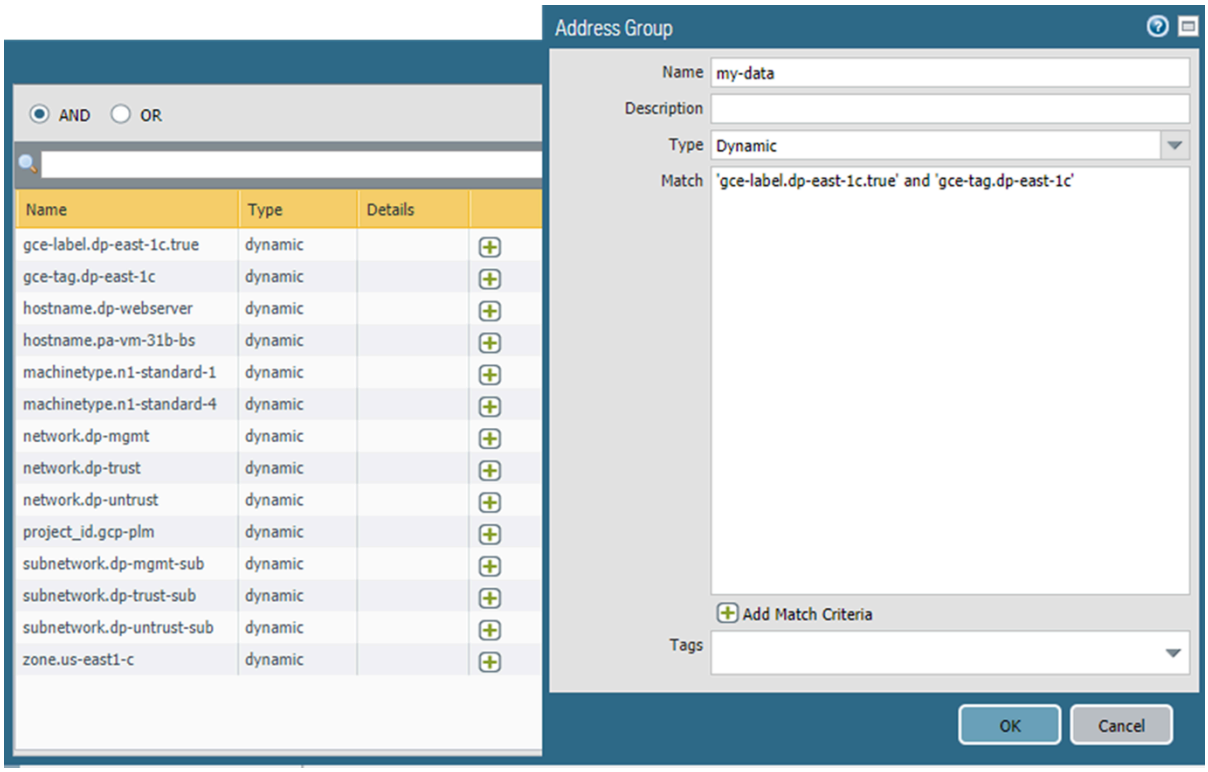


Las etiquetas que crea respaldan su estrategia para diferenciar sus recursos de manera que sean útiles para su política de seguridad.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Cree un grupo de direcciones dinámicas en el cortafuegos.

1. Seleccione **Objects (Objetos)** > **Address Groups (Grupos de direcciones)**.
2. Haga clic en **Add (Añadir)** para añadir un grupo de direcciones dinámicas y especificar un **Name (Nombre)** y una **Description (Descripción)**.
3. Configure **Type (Tipo)** en **Dynamic (Dinámico)**.
4. Defina los criterios de coincidencia.
   1. Haga clic en **Add Match Criteria (Añadir criterios de coincidencia)** y seleccione el operador **And (Y)**.
   2. Seleccione los atributos de filtrado o búsqueda de coincidencias.



5. Haga clic en **OK (Aceptar)**.
6. Haga clic en **Commit (Confirmar)**.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Use el grupo de direcciones dinámicas en una regla de política de seguridad.

Cree una regla que permita el acceso a Internet a cualquier servidor web que pertenezca al grupo de direcciones dinámicas llamado my-data.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Haga clic en **Add (Añadir)** para añadir una regla y en **Name (Nombre)** para introducir un nombre para la regla, y verifique que **Rule Type (Tipo de regla)** sea `universal`.
3. En la pestaña **Source** (Origen), seleccione trust como la **Source Zone (Zona de origen)**.
4. En la sección Source Address (Dirección de origen), haga clic en **Add (Añadir)** para añadir su nueva grupo my-data.
5. En la pestaña **Destination (Destino)**, añada untrust como la **Destination Zone (Zona de destino)**.
6. En la pestaña **Service/URL Category (Categoría de URL/servicio)**, compruebe que el servicio está establecido como **application-default (Predeterminado de la aplicación)**.
7. En la pestaña **Actions (Acciones)**, establezca **Action (Acción)** como Allow (Permitir).
8. En la sección Profile Settings (Configuración de perfiles),establezca el **Profile Type (Tipo de perfil)** en **Profiles (Perfiles)** y, a continuación, adjunte los perfiles predeterminados para antivirus, antispyware y protección contra vulnerabilidades.
9. Haga clic en **OK (Aceptar)**.
10. Haga clic en **Commit (Confirmar)**.

STEP 5 | Comprobar que los miembros del grupo de direcciones dinámicas se han añadido al cortafuegos.

La política entra en vigor para todas las direcciones IP que pertenecen a este grupo de direcciones y se muestra aquí.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione la regla.
2. Seleccione **Inspect (Inspeccionar)** en la lista desplegable. También puede comprobar si los criterios de coincidencia son precisos.
3. Haga clic en **more (más)** para comprobar que se muestra la lista de direcciones IP registradas.

Uso de plantillas personalizadas o la CLI de gcloud para implementar el cortafuegos VM-Series

Las imágenes de la VM-Series oficiales publicadas en Google Cloud Platform Marketplace están disponibles en el proyecto **`paloaltonetworksgcp-public`**. Debe conocer la ruta segura a estas imágenes si desea llamarlas desde la línea de comando **`gcloud`** o haga referencia a ellas en una plantilla que haya escrito o adaptado.

- BYOL: vmseries-byol-<*version*>
- PAYG Bundle 1: vmseries-bundle1-<*version*>
- PAYG Bundle 2: vmseries-bundle2-<*version*>

Use la CLI de gcloud para buscar los nombres y el proyecto de la imagen actual:

```
gcloud compute images list --project paloaltonetworksgcp-public
 --no-standard-images   NAME PROJECT FAMILY DEPRECATED STATUS
```

 ©2024 Palo Alto Networks, Inc.

```
   vmseries-bundle1-810 paloaltonetworksgcp-public READY   vmseries-
bundle2-810 paloaltonetworksgcp-public READY   vmseries-byol-810
 paloaltonetworksgcp-public READY
```

Añada la marca **`--uri`** para ver las rutas de la imagen:

```
  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
```

Por ejemplo, descargue la plantilla gcp-two-tier de https://github.com/PaloAltoNetworks.

Esta plantilla separa el nombre de la imagen (que incluye la versión de PAN-OS) de la ruta del URL. En `two-tier-template.py` la variable *image* espera el nombre de la imagen; por ejemplo: *vmseries-byol-810*. `vm-series-template.py` usa los valores de *COMPUTE_URL_BASE* y *sourceImage* para construir la ruta.

Habilite la resiliencia de sesión en VM-Series para GCP

La resiliencia de la sesión permite que el cortafuegos VM-Series mantenga la continuidad de la sesión durante un evento de fallo. El balanceador de carga de red (NLB) de GCP puede detectar y cancelar el registro de cortafuegos VM-Series en mal estado implementados en un clúster escalable horizontalmente detrás de él. Con la resiliencia de sesión habilitada, el NLB repite las sesiones de tráfico existentes que fluyen hacia un VM-Series en mal estado y redirige el tráfico a un cortafuegos VM-Series en buen estado. Esto permite que un clúster de cortafuegos VM-Series continúe inspeccionando sesiones de aplicaciones de larga duración, incluso en el caso de fallos del dispositivo VM-Series.

La inspección de tráfico de los flujos de tráfico repetidos es únicamente de Capa 4. El cortafuegos VM-Series inspecciona el tráfico en sesiones nuevas hasta la Capa 7.

Para mantener las sesiones que conmutan por error a cortafuegos VM-Series en buen estado, debe implementar una caché accesible de nivel estándar deMemorystore para Redis para sus cortafuegos VM-Series. La caché de Redis mantiene la información de sesión. Cuando el balanceador de carga detecta un cortafuegos VM-Series en mal estado, el balanceador de carga reequilibra el tráfico a un cortafuegos VM-Series en buen estado. El cortafuegos en buen estado VM-Series accede a la caché de Redis para obtener información de sesión y continúa inspeccionando y reenviando el tráfico existente.

Su balanceador de carga debe cumplir con los siguientes requisitos para soportar la resiliencia de sesión.

- Su balanceador de carga debe ser un balanceador de carga de red de paso interno.
- Debe configurar la persistencia de la conexión del balanceador de carga en nodos en mal estado en **NEVER_PERSIST.**

Su instancia de Memorystore para Redis debe cumplir los siguientes requisitos para admitir la resiliencia de sesión en el cortafuegos VM-Series.

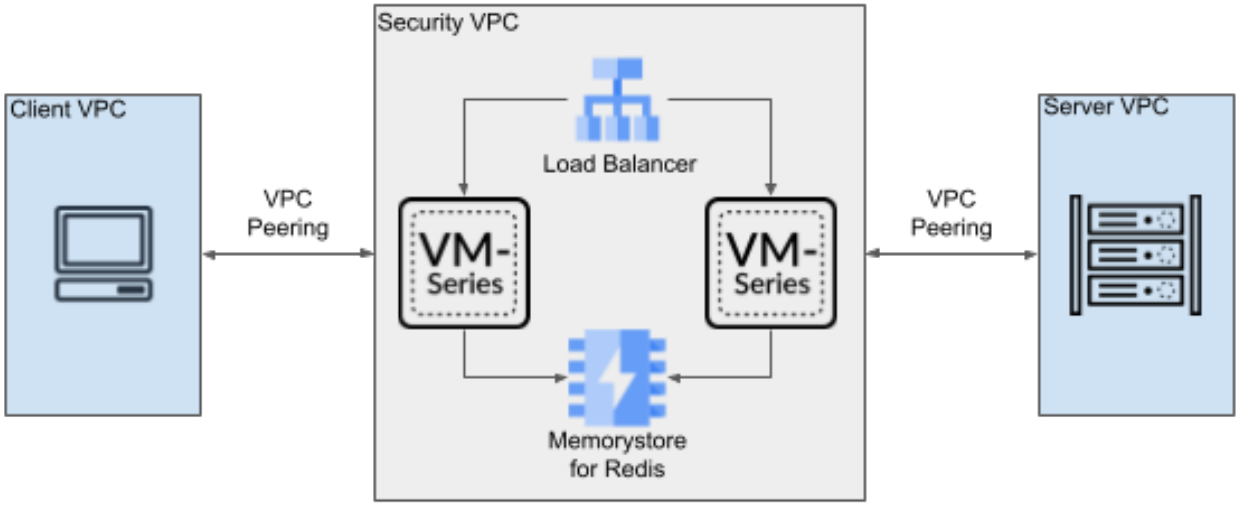
 ©2024 Palo Alto Networks, Inc.

- Nivel estándar
- Implemente la caché de Redis en la misma región y zona que las instancias del cortafuegos VM-Series.
- En el menú desplegable Red, seleccione la red VPC asociada con la interfaz de gestión del cortafuegos VM-Series.
- Habilite **AUTH** para limitar el acceso solo a usuarios fiables.
- Habilite el **Cifrado en tránsito** para cifrar las conexiones a la caché Redis mediante TLS.

Al dimensionar su Memorystore para Redis, utilice las siguientes pautas.

- Base el tamaño de la caché de Redis en el número máximo de sesiones admitidas por la instancia del cortafuegos VM-Series. Consulte Límites máximos basados en nivel y memoria hasta el máximo de sesiones para su cortafuegos.
- Cuando la resiliencia de la sesión está habilitada, el número máximo de sesiones tiene un límite del 70 % de la cantidad indicada en el enlace anterior. Por ejemplo, si su cortafuegos admite hasta 10.000.000 de sesiones, el máximo es 7.000.000 con resiliencia de sesión.
- Cada entrada redis por sesión utiliza aproximadamente 128 bytes. Por lo tanto, un cortafuegos VM-Series que admite 10.000.000 de sesiones requiere aproximadamente 1,3 GB de almacenamiento. Y un clúster de 10 cortafuegos VM-Series requiere al menos 13 GB.
- Utilice la siguiente fórmula para calcular los requisitos de redis.

  (128 x <number of sessions>) x 10^{-9} = requiere tamaño de caché de Redis por cortafuegos



La resiliencia de la sesión no se puede habilitar en las instancias de cortafuegos VM-Series existentes; solo en las nuevas instancias de implementación.

Habilite la resiliencia de sesión en el cortafuegos VM-Series pasando la configuración como parte de un archivo init-cfg.txt de arranque o en el campo de datos de usuario.

©2024 Palo Alto Networks, Inc.

Parámetro de arranque	Description (Descripción)
`op-command-modes=mgmt-interface-swap`	Le permite intercambiar la interfaz de gestión (MGT) con la interfaz del plano de datos (ethernet 1/1) al implementar el cortafuegos. Para obtener más detalles, consulte Intercambio de interfaces de gestión para el equilibrio de carga de Google Cloud Platform.
`plugin-op-commands=set-sess-ress:True`	Habilita la resiliencia de la sesión.
`redis-endpoint=`	Proporcione la dirección IP o FQDN y el puerto de su endpoint de Redis.
`redis-auth=`	Opcional El código de autenticación que usa el cortafuegos VM-Series para conectarse con el endpoint de Redis.
`redis-certificate=`	OpcionalLa cadena del certificado de CA raíz utilizada para conectarse al endpoint de Redis. El certificado debe ser una cadena codificada en base64 con codificación utf-8.

STEP 1 | Implemente su caché de Redis.

STEP 2 | Prepare su archivo de arranque.

```
op-command-modes=mgmt-interface-swap plugin-op-commands=set-sess-ress:True redis-endpoint=<redis-IP-address:port> redis-auth=<redis-auth-code> redis-certificate=
```

STEP 3 | Arranque sus cortafuegos VM-Series.

STEP 4 | Inicie sesión en el cortafuegos.

STEP 5 | Cree un objeto de dirección para la dirección IP del front-end del balanceador de carga.

1. Seleccione **Objects (Objetos)** > **Address (Dirección)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** descriptivo.
3. Establezca el Tipo en Máscara de red IP e introduzca la dirección IP del front-end del balanceador de carga.
4. Haga clic en **OK (Aceptar)**.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Cree una interfaz de bucle invertido para enviar paquetes de verificación de estado al balanceador de carga.

1. Seleccione **Networking (Redes)** > **Interfaces** > **Loopback (Bucle invertido)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** descriptivo.
3. En la pestaña **Config (Configuración)**, configure el **Virtual router (Enrutador virtual)** como predeterminado y la **Security Zone (Zona de seguridad)** como su zona de confianza.
4. En la pestaña **IPv4**, agregue el objeto de dirección que creó anteriormente.
5. Haga clic en **OK (Aceptar)**.

STEP 7 | Crear un perfil de gestión.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Interface Mgmt (Gestión de interfaz)** y haga clic en **Add (Añadir)**.
2. Habilite Ping, SSH, HTTPS y SNMP.

   No habilite HTTP ni Telnet porque esos protocolos realizan transmisiones de texto sin cifrar y, por lo tanto, no son seguros.
3. Haga clic en **OK (Aceptar)**.

STEP 8 | Añada su perfil de gestión a su interfaz de bucle invertido.

1. Seleccione **Network (Red)Interfaces**, seleccione su interfaz de bucle invertido..
2. Seleccione **Advanced (Avanzado)** > **Other (Otra)** información y seleccione la interfaz Perfil de gestión que acaba de añadir.
3. Haga clic en **OK (Aceptar)**.

STEP 9 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

 ©2024 Palo Alto Networks, Inc.

Supervisión de VM con el complemento de Panorama para GCP

El complemento de Panorama para Google Cloud Platform (GCP) versión 2.0.0 le permite crear una configuración de supervisión de VM que se autentica con un proyecto de GCP y supervisa los cortafuegos VM-Series y otras máquinas virtuales implementadas en él. Una vez que establece una conexión con su proyecto, el complemento puede recuperar la comunicación de dirección IP a etiqueta entre los activos de Panorama y GCP. Las etiquetas pueden ser atributos predefinidos, etiquetas definidas por el usuario para las máquinas virtuales y etiquetas de red definidas por el usuario (consulte Revisión y creación de etiquetas).

El complemento de Panorama para GCP recupera las direcciones IP internas y externas de las máquinas virtuales en ejecución y, periódicamente, recupera asignaciones de IP a etiqueta de las máquinas virtuales en VPC de GCP conectadas.

Puede utilizar etiquetas para organizar las máquinas virtuales en grupos de direcciones dinámicas y luego hacer referencia a sus etiquetas en las reglas de la política de seguridad que permiten o bloquean el tráfico a direcciones IP de máquinas virtuales específicas. Para ejecutar la política de seguridad de manera coherente, puede enviar reglas a sus cortafuegos VM-Series.

- Configuración de supervisión de VM con el complemento de Panorama para GCP

Configuración de supervisión de VM con el complemento de Panorama para GCP

Este tema describe los pasos para preparar sus activos GCP para la supervisión de VM, revisar los elementos necesarios de Panorama y describe cómo configurar la supervisión de VM en el complemento de Panorama para Google Cloud Platform (GCP).

- Configuración de activos de GCP para la supervisión de VM
- Revisión y creación de etiquetas
- Configuración de supervisión de VM con el complemento de Panorama para GCP
  - Prepare Panorama para configurar la supervisión de máquinas virtuales
  - Configuración de la supervisión de VM

Configuración de activos de GCP para la supervisión de VM

Puede supervisar los cortafuegos VM-Series que ha implementado desde el GCP marketplace, los cortafuegos que ha implementado con plantillas de cortafuegos de escalado automático, las instancias de GCE que ha creado desde la consola de GCP o la línea de comandos de gcloud, u otras máquinas virtuales implementadas en GCP. Si implementa las VM de PAN-OS desde el Marketplace, siga las instrucciones en Configuración del cortafuegos VM-Series en Google Cloud Platform .

Revisión de las funciones de IAM

Asegúrese de tener los siguientes permisos mínimos para las tareas de supervisión de VM:

 ©2024 Palo Alto Networks, Inc.

- En la consola GCP, cree cuentas de servicio para su proyecto y otorgue el permiso al propietario o editor del proyecto.

  La creación de una cuenta de servicio no se puede automatizar. Si no tiene permiso para crear una cuenta de servicio, puede pedirle a un administrador que la cree y le asigne una función adecuada.
- Ver sus cuentas de servicio: solo lectura.
- Ver máquinas virtuales de PAN-OS implementadas desde Google Marketplace: Visor de Compute.
- Asignar una etiqueta definida por el usuario a una instancia: Propietario, editor del proyecto o Administrador de la instancia.

Crear una cuenta de servicio

Antes de usar el complemento de GCP en Panorama para configurar la supervisión de VM, debe usar la consola de GCP para crear cuentas de servicio que otorgan permisos para acceder a su proyecto de GCP, cortafuegos VM-Series implementados dentro de él, cualquier otra VM que desea que Panorama gestione y las redes y subredes relacionadas. El complemento de GCP para Panorama recupera los atributos predefinidos para los activos de Google, las etiquetas de VM definidas por el usuario y las etiquetas de red definidas por el usuario.

Desde el complemento de Panorama para GCP versión 3.1.0 o posterior, en una configuración de VPC compartida, puede crear cuentas de servicio para proyectos host y otorgar permisos a los proyectos de servicio. Para obtener más información, consulta cómo crear una cuenta de servicio entre proyectos en GCP. Las credenciales de esta cuenta de servicio deben usarse en la definición de supervisión para recuperar etiquetas para varios proyectos de servicio adjuntos.

Cada proyecto tiene una cuenta de servicio predeterminada que se creó de forma automática cuando se creó el proyecto. Si crea una cuenta de servicio separada específicamente para la supervisión de máquinas virtuales, tendrá un mayor control de los usuarios y sus funciones. Puede configurar hasta 100 cuentas de servicio por proyecto.

STEP 1 | En la consola de Google Cloud Platform, seleccione el proyecto que desea supervisar.

STEP 2 | Seleccione **IAM & Admin (IAM y administrador)** > **Service accounts (Cuentas de servicio)** y elija **+Create Service Account (+Crear cuenta de servicio)**.

Introduzca el nombre y la descripción de la cuenta de servicio y haga clic en **Create (Crear)**.

STEP 3 | Seleccione un tipo de función en el menú desplegable y, a la derecha, seleccione un nivel de acceso adecuado.

Por ejemplo, seleccione Proyecto> Editor. Puede seleccionar varias funciones para una cuenta de servicio.

Cuando haya terminado, haga clic en **Continue (Continuar)**.

STEP 4 | Otorgue permiso a usuarios específicos para acceder a esta cuenta de servicio. Seleccione miembros de la columna **Permissions (Permisos)** a la derecha para otorgarles permiso para acceder a las funciones en el paso anterior.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | (Opcional) Haga clic en **+CREATE KEY (+CREAR CLAVE)** para crear una credencial que le permita autenticarse con la CLI de Google Cloud para acceder a los cortafuegos VM-Series, redes y otras máquinas virtuales asociadas con esta cuenta de servicio.

La clave se descarga automáticamente. Asegúrese de guardarla en un lugar seguro. El formato JSON de la clave privada que se genera es el siguiente:

```
{ "type": "service_account", "project_id": "gcp-xxx",
 "private_key_id": "<private-key-id>", "private_key": "-----BEGIN
 PRIVATE KEY-----<private-key-value>-----END PRIVATE KEY-----
\n", "client_email": "<client-email>", "client_id": "<client-
id>", "auth_uri": "<auth-uri>", "token_uri": "<token-uri>",
 "auth_provider_x509_cert_url": "<auth-provider-x509-cert-url>",
 "client_x509_cert_url": "<client-x509-cert-url>" }
```

Revisión y creación de etiquetas

"Etiqueta" es un término general para atributos predefinidos, etiquetas definidas por el usuario y etiquetas de red definidas por el usuario.

- Las etiquetas predefinidas (atributos) se crean automáticamente para las VM de Google. Cuando configura la supervisión de VM, puede optar por supervisar los 8 atributos predefinidos, o puede crear una lista personalizada de atributos para supervisar.
- Puede definir sus propias etiquetas para las etiquetas de máquinas virtuales y etiquetas de redes.

Etiquete las máquinas virtuales y las redes para que pueda identificarlas y agruparlas para que pueda estructurar reglas que apliquen la política de seguridad. Puede etiquetar cualquier VM implementada en su proyecto de Google, por ejemplo, un cortafuegos VM-Series, un servidor web, un servidor de aplicaciones o un balanceador de carga.

- Las etiquetas deben estar asociadas a una máquina virtual. Esto también se aplica a redes y subredes.
- Si hay varias direcciones IP asociadas con una instancia (por ejemplo, si etiquetó las interfaces trust y untrust del cortafuegos VM-Series), Panorama genera varios conjuntos de información de etiquetas.

El número total de etiquetas que el complemento de Panorama puede recuperar y registrar depende de la versión de PAN-OS que Panorama esté ejecutando y de la versión de los cortafuegos VM-Series gestionados.

La zona de Google, la región de Google, el nombre de la VPC y el nombre de la subred se utilizan para etiquetar interfaces de red en máquinas virtuales con múltiples interfaces específicas de la interfaz de red.

Atributos predefinidos

El complemento de Google Cloud Platform para Panorama recupera las siguientes etiquetas predefinidas de cualquier máquina virtual gestionada:

- **ID del proyecto**: por ejemplo: google.project-id.myProjectId.

  Para encontrar la información de su proyecto en la consola de Google, seleccione su proyecto y luego seleccione **IAM & Admin (IAM y Administrador)** > **Settings (Configuración)**.
- **Cuenta de servicio**: su cuenta de servicio en forma de dirección de correo electrónico. Por ejemplo: google.svc-accnt.sa-name@project-id.iam.gserviceaccount.com.

  Para encontrar su cuenta de servicio, consulte los detalles de la instancia de VM.

 ©2024 Palo Alto Networks, Inc.

- **Nombre de VPC**: el nombre de la red VPC para una VM gestionada. Por ejemplo: google.vpc-name.myvnet.
- **Nombre de subred**: el nombre de una subred que creó para una interfaz de VM gestionada. Por ejemplo, para la interfaz untrust del cortafuegos VM-Series, el nombre de la subred que creó para la interfaz untrust: google.subnet-name-untrust.web.
- **SKU de SO**: el sistema operativo que eligió cuando implementó la VM gestionada. Por ejemplo: google.os-sku.centos-7.

  Este atributo no es compatible si la máquina virtual usa una imagen personalizada.

- **Zona de Google**: la zona que seleccionó cuando implementó la VM. Por ejemplo: google.zone.us-east1-c.
- **Región de Google**: la región que contiene la zona que seleccionó. Por ejemplo: google.region.us-east1.
- **Nombre del grupo de instancias**: por ejemplo: google.instance-group.myInstanceGroup. Para ver o crear un grupo de instancias en la consola de Google, seleccione **Compute Engine** > **Instance Group (Grupo de instancias)**.

Etiquetas definidas por el usuario

Panorama utiliza hasta 16 etiquetas definidas por el usuario. Si tiene más de 16 etiquetas, Panorama ordena las etiquetas definidas por el usuario alfabéticamente y utiliza las primeras 16 etiquetas.

Revise los requisitos de Google para los pares clave-valor de etiquetas: Las claves tienen una longitud mínima de 1 carácter y una longitud máxima de 63 caracteres, y no pueden estar vacías. Los valores pueden estar vacíos y tener una longitud máxima de 63 caracteres.

Para crear o ver etiquetas en la consola de GCP, vaya a **Compute Engine** > **VM Instances (Instancias de VM)** y seleccione **Show Info Panel (Mostrar panel de información)**. Seleccione una o más máquinas virtuales y en el panel **Info (Información)**, seleccione **Labels (Etiquetas)**. Haga clic en **+Add a label (+Añadir una etiqueta)**, añada una clave y un valor, y haga clic en **Save (Guardar)**.

Etiquetas de red definidas por el usuario

Panorama utiliza hasta 8 etiquetas de red definidas por el usuario. Si tiene más de 8 etiquetas, Panorama ordena las etiquetas definidas por el usuario alfabéticamente y utiliza las primeras 8 etiquetas.

Tenga en cuenta que Google limita las etiquetas de red de la siguiente manera:

- Máximo 63 caracteres por etiqueta.
- Puede utilizar letras minúsculas, números y guiones; una etiqueta debe comenzar con una letra minúscula y finalizar con un número o una letra minúscula.

Para crear o ver etiquetas de red en la consola de GCP, vaya a **Compute Engine** > **VM Instances (Instancias de VM)** y seleccione una instancia. Debe **Edit (Editar)** la instancia y desplazarse hacia abajo hasta **Network Tags (Etiquetas de red)**, introduzca las etiquetas (separadas por comas) y seleccione **Save (Guardar)**. Consulte Configuración de etiquetas de red.

Configuración de supervisión de VM con el complemento de Panorama para GCP

Después de etiquetar sus activos de GCP y crear cuentas de servicio, ponga sus activos a disposición de Panorama para que pueda configurar la supervisión de VM.

 ©2024 Palo Alto Networks, Inc.

Prepare Panorama para configurar la supervisión de máquinas virtuales

Siga estos pasos para permitir que Panorama gestione y supervise sus activos de GCP. Cualquier VM implementada en GCP puede ser un dispositivo gestionado en Panorama.

STEP 1 | En Panorama, añada los cortafuegos VM-Series y otras VM asociadas con su proyecto de GCP como dispositivos gestionados.

STEP 2 | Añada un grupo de dispositivos y asígnele dispositivos gestionados. Un grupo de dispositivos es un grupo de cortafuegos o sistemas virtuales que desea gestionar como un grupo.

Una máquina virtual puede ser miembro de un solo Grupo de dispositivos. Planifique sus grupos de dispositivos con cuidado.

STEP 3 | Añada una plantilla. Nombre la plantilla y acepte la VPC predeterminada.

STEP 4 | Añada una pila de plantillas. Debe **Add (Añadir)** la pila, **Add (Añadir)** la plantilla que acaba de crear y seleccione sus dispositivos.

STEP 5 | Confirme los cambios.

Configuración de la supervisión de VM

STEP 1 | Si aún no lo ha hecho, Instalación del complemento de Panorama para GCP.

STEP 2 | Inicie sesión en la interfaz web de Panorama y seleccione **Panorama** > **Google Cloud Platform**.

STEP 3 | Configuración de la supervisión de VM.

1. Configure los ajustes generales.
   1. Seleccione **Panorama** > **Google Cloud Platform** > **Setup (Configuración)** > **General**. Para editar la configuración, haga clic en el engranaje.
      - Marque **Enable Monitoring (Habilitar supervisión)** para permitir la supervisión de VM en todos los proyectos para los que configure una cuenta de servicio.
      - introduzca el **Monitoring Interval (Intervalo de supervisión)** en segundos. Este es el período de tiempo entre eventos de recuperación de etiquetas.
2. **Add (Añadir)** un grupo de notificación. Un grupo de notificación es una lista de Grupos de dispositivos a los que Panorama envía asignaciones y actualizaciones de dirección IP a etiqueta.

   Un proyecto solo puede tener un grupo de notificación.

   1. **Select Panorama (Seleccione Panorama)** > **Google Cloud Platform** > **Setup (Configuración)** > **Notify Group (Grupo de notificación)** y haga clic en **Add (Añadir)**.
   2. Introduzca un **Name (Nombre)** para identificar el grupo de cortafuegos al que Panorama envía la información de VM (asignaciones de dirección IP a etiqueta) que recupera.
   3. Seleccione los **Device Groups (Grupos de dispositivos)** a los que Panorama enviará la información de la VM (asignaciones de dirección IP a etiqueta) recuperada de su proyecto. Los cortafuegos VM-Series utilizan la actualización para determinar la lista de miembros

 ©2024 Palo Alto Networks, Inc.

actual para los Grupos de direcciones dinámicas a los que se hace referencia en la política de seguridad.

Planifique sus grupos de dispositivos con cuidado.

4. Seleccione etiquetas predefinidas o personalizadas.
   - **Select All 8 Predefined Tags (Seleccionar las 8 etiquetas predefinidas)**: elija esta opción para seleccionar todos los atributos (etiquetas) predefinidos.
   - **Custom tags (Etiquetas personalizadas)**: elija esta opción para crear listas de etiquetas para atributos predefinidos, etiquetas definidas por el usuario y etiquetas de red definidas por el usuario.
5.
   - Asegúrese de incluir todos los grupos de dispositivos relevantes en un solo grupo de notificación.
   - Si desea eliminar el registro de las etiquetas que Panorama envió a un cortafuegos en un grupo de notificación, debe eliminar la definición de monitorización.
   - Para registrar las etiquetas en todos los sistemas virtuales en un cortafuegos habilitado para varios sistemas virtuales, debe añadir cada sistema virtual a un Grupo de dispositivos independiente en Panorama y asignar los Grupos de dispositivos al grupo de notificación. Panorama registrará las etiquetas a un solo sistema virtual, si asigna todos los sistemas virtuales a un Grupo de dispositivos.

3. **Add (Añadir)** credencial de cuenta de servicio de GCP.
   - Nombre la credencial de la cuenta de servicio.
   - (Opcional) Introduzca una descripción de la cuenta de servicio.
   - **Examine** para cargar el archivo JSON generado cuando creó la cuenta de servicio.

   En la configuración de VPC compartida, debe crear cuentas de servicio para proyectos host y otorgar permisos a los proyectos de servicio. Puede utilizar estas cuentas de servicio en el complemento de GCP. Esto le permitirá recuperar etiquetas que forman parte de proyectos de servicio adjuntos al proyecto host.

   Debe utilizar la interfaz web de Panorama. No puede usar la CLI para añadir una cuenta de servicio

   Solo puede usar una cuenta de servicio para una credencial. No cree varias credenciales a partir de un solo archivo JSON.

Después de añadir la credencial de la cuenta de servicio, puede validar la credencial desde la línea de comando de Panorama:

```
request plugins gcp validate-service-account <svc-acct-credential-name>
```

STEP 4 | Cree una **Monitoring Definition (Definición de monitorización)**.

Una definición de monitorización consiste en la credencial de cuenta de servicio para su proyecto y un grupo de notificación. Todos los activos de red de su proyecto se supervisan y las etiquetas recuperadas

 ©2024 Palo Alto Networks, Inc.

se envían a los Grupos de dispositivos que enumera en su definición de supervisión. Cuando añade una nueva definición de monitorización, esta se habilita de manera predeterminada.

Un proyecto puede tener una única definición de monitorización, y una definición de monitorización puede incluir solo un grupo de notificación.

1. Seleccione **Panorama** > **Google Cloud Platform** > **Monitoring Definition (Definición de monitorización)** y haga clic en Añadir.
2. Debe **Name (Nombrar)** la definición de monitorización.
3. Introduzca una **Description (Descripción)** opcional para el proyecto y los activos que está supervisando.
4. Seleccione la credencial de la **Service Account (Cuenta de servicio)** que creó en el paso anterior.
5. Seleccione un **Notify Group (Grupo de notificación)**.
6. Elija **Enable (Habilitar)** la supervisión de los elementos asociados con esta cuenta de servicio.

STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar los cambios realizados en Panorama.

Compruebe que el estado de la definición de monitorización se muestre como Success (Correcto). Si falla, compruebe que introdujo la ID de la VPC de AWS correctamente y que proporcionó las ID y claves correctas para autorizar el acceso.

STEP 6 | Compruebe que puede ver la información de la VM en Panorama y defina los criterios de coincidencia para los grupos de direcciones dinámicas.

Durante una conmutación por error de HA, el Panorama secundario intenta reconectarse a Google Cloud Platform y recuperar etiquetas de todas las definiciones de supervisión. Si hay un error al volver a conectar incluso una definición de supervisión, Panorama genera un mensaje de registro del sistema:

```
No es posible procesar las suscripciones después del cambio de HA;
 requiere la intervención del usuario.
```

Si ve este error, solucione el problema en Panorama. Por ejemplo, elimine una suscripción no válida o proporcione credenciales válidas) y confirme los cambios para permitir que Panorama se vuelva a conectar y recupere las etiquetas de todas las definiciones de monitorización.

Incluso cuando Panorama esté desconectado de Google Cloud Platform, los cortafuegos tienen la lista de todas las etiquetas que se recuperaron antes de la conmutación por error y pueden continuar aplicando la política en esa lista de direcciones IP. Cuando elimina una definición de monitorización, Panorama elimina todas las etiquetas asociadas a las máquinas virtuales registradas. Se recomienda configurar la acción orientada de reenvío de logs a un destino HTTPS desde Panorama, de modo que pueda tomar medidas de inmediato.

 ©2024 Palo Alto Networks, Inc.

Escalado automático del cortafuegos VM-Series en Google Cloud Platform

El complemento de Panorama para Google Cloud Platform (GCP) versión 2.0.0 le ayuda a implementar el cortafuegos VM-Series en la GCP y permite que Panorama gestione los cortafuegos VM-Series que garantizan la supervisión de la VM o las implementaciones de escalado automático en GCP. Si se usa Panorama para gestionar de forma centralizada las políticas y cortafuegos, es posible aumentar la eficiencia operativa a la hora de gestionar y mantener una red distribuida de cortafuegos.

Si Panorama mantiene sus grupos de instancias gestionados de GCP, puede crear políticas de habilitación de aplicaciones que protegen y controlan la red.

La implementación del escalado automático admite el uso de una configuración de red de VPC compartida o emparejamiento de red de VPC para crear una red VPC común en la que un proyecto host contiene redes de VPC compartidas y los cortafuegos VM-Series, y un proyecto de servicio contiene una implementación de aplicación basada en vm o en contenedor (un clúster de Kubernetes). Palo Alto Networks proporciona plantillas para ayudarle a implementar los cortafuegos VM-Series en el proyecto host e implementar una aplicación de muestra opcional en el proyecto de servicio.

Las licencias BYOL y PAYG se pueden utilizar para los cortafuegos VM-Series. Durante la concesión de licencias, las instancias de cortafuegos VM-Series se comunican directamente con el servidor de licencias de Palo Alto Networks.

Si elige BYOL, su implementación puede desactivar las instancias de licencia en respuesta a un evento de reducción vertical. Si la información de implementación de un cortafuegos VM-Series está configurada en el complemento de Panorama para GCP y el cortafuegos se elimina automáticamente, Panorama detecta el estado del cortafuegos y automáticamente anula el registro del cortafuegos.

- Componentes de escalado automático para Google Cloud Platform
- Implementar plantillas de escalado automático de GCP 2

Componentes de escalado automático para Google Cloud Platform

Las implementaciones típicas de escalado automático de GCP usan un proyecto host y un proyecto de servicio y forman una red VPC común entre los dos. El complemento de Panorama para GCP puede proteger una implementación de escalado automático en un solo proyecto con VPC de servicio y host, o proyectos de servicio y host en una configuración de red de VPC compartida o VPC emparejada, donde el proyecto host contiene los cortafuegos VM-Series y las redes de VPC compartidas, y el proyecto de servicio contiene la implementación de su aplicación. Si su aplicación se implementa en un clúster de Kubernetes, se requiere una VPC emparejada.

- Requisitos de escalado automático
- Prepárese para implementar las plantillas de escalado automático

Requisitos de escalado automático

- **Requisitos generales**: asegúrese de que su entorno cumpla con los requisitos básicos.

©2024 Palo Alto Networks, Inc.

- **Complemento de Panorama para GCP**: si aún no lo ha hecho, Instalación del complemento de Panorama para GCP.

  Si ha instalado anteriormente el complemento Panorama para GCP versión 1.0.0, elimínelo antes de instalar 2.0.X. No puede actualizar.

- **Plantillas de escalado automático de Palo Alto Networks versión 1.0**: Palo Alto Networks proporciona las plantillas para implementar instancias del cortafuegos VM-Series en el proyecto host, y configurar e implementar una aplicación de muestra en un proyecto de servicio. Consulte Acerca de las plantillas de escalado automático para obtener más información sobre las plantillas.

  Descargar las plantillas de GitHub. El archivo zip contiene archivos zip independientes para el cortafuegos y las plantillas de la aplicación.

Prepárese para implementar las plantillas de escalado automático

Complete las siguientes tareas antes de implementar las plantillas de escalado automático.

- Prepare un proyecto host y las cuentas de servicio necesarias
- Obtenga una clave API de licencia
- Configure el complemento de Panorama para GCP para proteger una implementación de escalado automático
- Prepare un paquete de arranque de cortafuegos VM-Series para escalado automático

Prepare un proyecto host y las cuentas de servicio necesarias

Necesita un proyecto de host y un proyecto de servicio para formar la topología de VPC compartida que admita el cortafuegos y las plantillas de aplicación. Puede crear un nuevo proyecto host o preparar un proyecto existente para que actúe como su host.

Para configurar la nube privada virtual (VPC) compartida, un administrador de la organización debe otorgar al administrador del proyecto host la función de Administrador de la VPC compartida. El administrador de la VPC compartida puede habilitar un proyecto para que actúe como host y otorgar la función de administrador del proyecto de servicio al administrador del proyecto de servicio. Revise la documentación de GCP sobre las funciones de los Administradores e la IAM.

STEP 1 | En la consola de GCP, cree un proyecto de GCP para que actúe como host. Si desea utilizar un proyecto existente, vaya al siguiente paso.

Para crear un nuevo proyecto, seleccione su organización o **No organization (Sin organización)**, haga clic en **New project (Nuevo proyecto)** y complete la información de su proyecto. Tenga en cuenta que esta es su única oportunidad de **EDIT (EDITAR)** el ID del proyecto.

El SDK de Google Cloud debe estar instalado y configurado para que pueda autenticarse con su proyecto host desde la CLI. Utilizará la interfaz de línea de comandos para implementar la plantilla de cortafuegos y la plantilla de la aplicación, y para adjuntar el proyecto de servicio al proyecto host.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Habilite las API y los servicios necesarios para el escalado automático. Las API requeridas son:

- API de Cloud Pub/Sub
- API de Cloud Deployment Manager
- API de Cloud Storage
- API de Compute Engine
- API de Grupo de instancias administrado de Google Compute Engine
- API de Actualizador de grupo de instancias de Google Compute Engine
- API de Grupos de instancias de Google Compute Engine
- API de Kubernetes Engine
- API de Stackdriver
- API de Stackdriver Logging
- API de Stackdriver Monitoring

Puede habilitar las API desde la Consola de GCP o la CLI de GCP, como se muestra a continuación.

Habilitación de las API desde la consola de GCP

1. Seleccione el proyecto host y, en el menú de navegación, seleccione **APIs & Services (API y servicios)**.
2. Busque y vea cada API solicitada.
3. Debe **ENABLE (HABILITAR)** cualquier API que no muestre el estado "API habilitada".

Habilitación de las API desde la CLI

1. En la CLI, vea su configuración para asegurarse de que está en el proyecto correcto.

```
gcloud config list
```

   Si no es así, defina el proyecto de la siguiente manera:

```
gcloud config set project <project-name>
```

2. Emita los siguientes comandos para habilitar las API necesarias.

```
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
```

 ©2024 Palo Alto Networks, Inc.

```
enable logging.googleapis.com gcloud services enable
monitoring.googleapis.com
```

3. Compruebe que las API necesarias estén habilitadas.

```
gcloud services list --enabled
```

STEP 3 | Cree una cuenta de servicio para implementar el cortafuegos VM-Series y asigne las funciones de IAM necesarias para realizar un escalado automático de un servicio o un clúster de Kubernetes.

Cuando configura las plantillas de cortafuegos, añade la dirección de correo electrónico de esta cuenta de servicio al archivo `.yaml` del cortafuegos VM-Series. Dentro del proyecto host, la plantilla utiliza las credenciales de esta cuenta de servicio para crear una nube privada virtual host con subredes,

 ©2024 Palo Alto Networks, Inc.

implementar cortafuegos VM-Series en la VPC, configurar métricas personalizadas de Stackdriver, crear un tema de Pub/Sub y más.

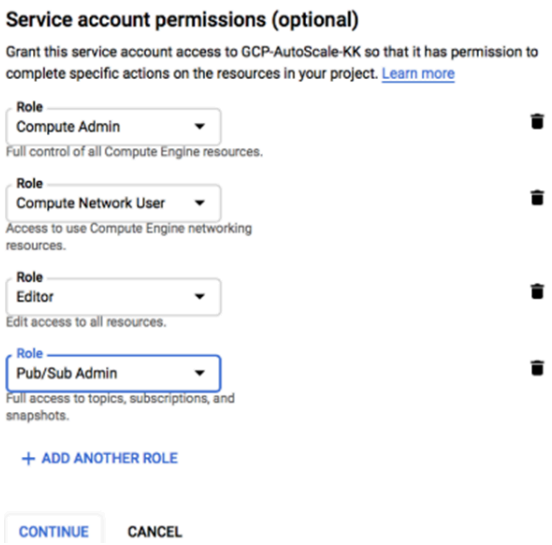
1. En la consola de GCP, seleccione **IAM & Admin (Administrador e IAM)** > **Service accounts (Cuentas de servicio)** y seleccione **+CREATE SERVICE ACCOUNT (+ CREAR CUENTA DE SERVICIO)**.

   Complete los detalles de la cuenta de servicio y haga clic en **CREATE (CREAR)**.

2. Dé permiso a la cuenta de servicio para realizar un escalado automático de los recursos en este proyecto.

   Seleccione un tipo de función en el menú desplegable y, a la derecha, seleccione un nivel de acceso adecuado. Por ejemplo, seleccione Proyecto> Editor. Puede seleccionar varias funciones para una cuenta de servicio.

   - ❑ Compute Engine > Administrador de Compute
   - ❑ Compute Engine > Usuario de la red de Compute
   - ❑ Pub/Sub > Administrador
   - ❑ Supervisión > Escritor de métricas de supervisión
   - ❑ Stackdriver > Editor de cuentas de Stackdriver
   - ❑ Almacenamiento > Administrador de almacenamiento
   - ❑ (Solo GKE) Kubernetes > Administrador de clúster de Kubernetes Engine
   - ❑ (Solo GKE) Kubernetes > Visor de Kubernetes Engine

   Seleccione **Continue (Continuar)** cuando haya finalizado la adición de funciones.

3. Haga clic en **+CREATE KEY (+CREAR CLAVE)** para crear una clave para la cuenta de servicio de host.

   - (Opcional) Añada direcciones de correo electrónico para otorgar a otros usuarios o administradores acceso a esta cuenta de servicio.
   - Haga clic en JSON para descargar la clave privada en formato JSON.
   - Guarde la llave en un lugar seguro. Necesitará esta clave cuando Implementar plantillas de escalado automático de GCP.

 ©2024 Palo Alto Networks, Inc.

4. Haga clic en **DONE (LISTO)**.

STEP 4 | Cree una cuenta de servicio que un administrador de Panorama pueda utilizar para interactuar con este proyecto host.

1. En la consola de GCP, seleccione **IAM & Admin (IAM y administrador)** > **Service accounts (Cuentas de servicio)** y seleccione **+CREATE SERVICE ACCOUNT (+ CREAR CUENTA DE SERVICIO)**.
2. Complete los detalles de la cuenta de servicio y haga clic en **CREATE (CREAR)**.
3. .Otorgar acceso a la cuenta de servicio.

   Seleccione un tipo de función en el menú desplegable y, a la derecha, seleccione un nivel de acceso adecuado. Por ejemplo, seleccione Proyecto> Editor. Puede seleccionar varias funciones para una cuenta de servicio.

   - ❑ Compute Engine > Visor de Compute
   - ❑ Deployment Manager > Visor
   - ❑ Pub/Sub > Administrador

   Haga clic en **CONTINUE (CONTINUAR)**.
4. Haga clic en **+CREATE KEY (+CREAR CLAVE)** para crear una clave para la cuenta de servicio de host.

   - (Opcional) Añada direcciones de correo electrónico para otorgar a otros usuarios o administradores acceso a esta cuenta de servicio.
   - Seleccione JSON para descargar la clave privada en formato JSON.
   - Guarde la llave en un lugar seguro. Necesitará esta clave cuando Configure el complemento de Panorama para GCP para proteger una implementación de escalado automático.

STEP 5 | (opcional) En la CLI, compruebe que puede comunicarse con su nuevo proyecto de host.

1. Configure su proyecto en el proyecto host que acaba de crear.

   ```
   gcloud set project <your-autoscale-host-project-name>
   ```
2. Cree una configuración para el escalado automático. Su nueva configuración se activa automáticamente a menos que desactive la activación.

   ```
   gcloud config configurations create <CONFIGURATION_NAME> gcloud config list
   ```

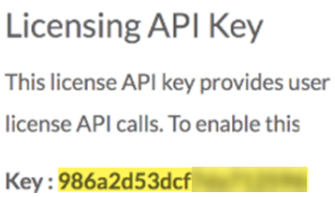
Obtenga una clave API de licencia

Necesita una clave de API de licencia para que Panorama pueda otorgar y retirar la licencia de los activos gestionados en GCP.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Inicie sesión en el Support portal (Portal de atención al cliente) y seleccione **Assets (Activos)** > **Licensing API (API de licencias)** y haga clic en **Enable (Habilitar)**. Se muestra la clave.

Solo un superusuario puede ver el enlace Habilitar para generar esta clave. Consulte Cómo habilitar, regenerar y ampliar la clave API de licencias.



STEP 2 | Seleccione la clave y cópiela.

STEP 3 | Desde el CLI, haga una conexión SSH a Panorama y ejecute el siguiente comando, sustituyendo <key> con la clave de API que copió del portal de atención al cliente:

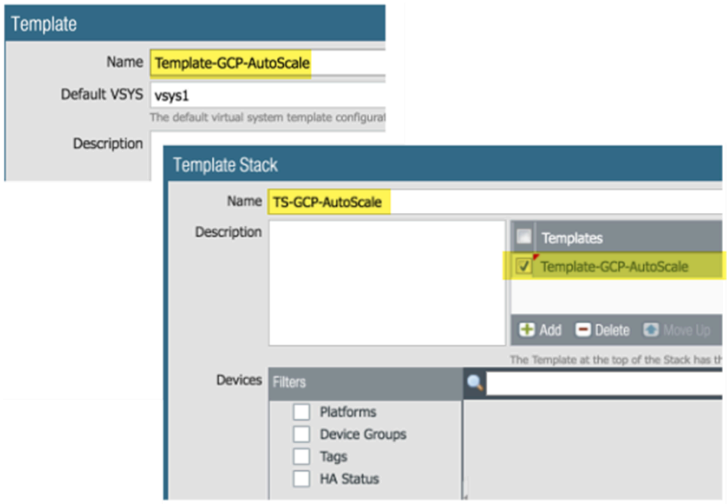
```
request license api-key set key <key>
```

```
La clave de API se ha establecido correctamente
```

Configure el complemento de Panorama para GCP para proteger una implementación de escalado automático

En Panorama, cree activos para admitir la implementación del cortafuegos de escalado automático.

STEP 1 | Cree una plantilla y una pila de plantillas que incluya la plantilla y seleccione **Commit (Confirmar)** los cambios.



 ©2024 Palo Alto Networks, Inc.

STEP 2 | En el contexto de **Network (Red)**, seleccione la plantilla o la pila de plantillas. Seleccione **Virtual Routers (Enrutadores virtuales)** y **Add (Añadir)** para añadir un enrutador virtual.

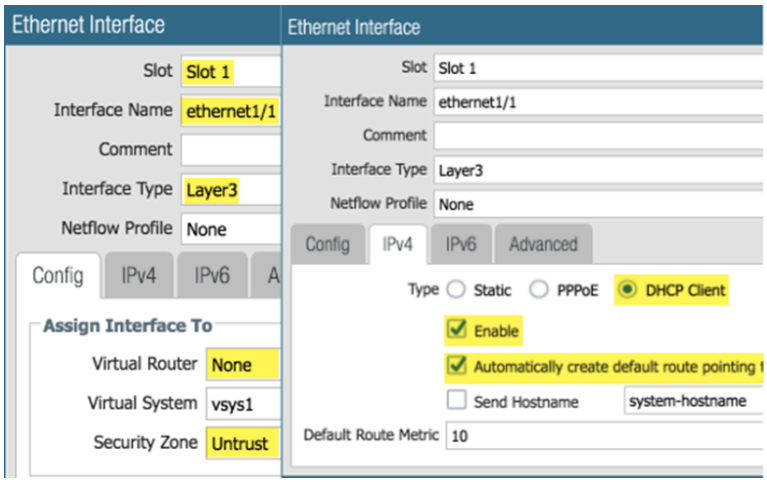
Cuando la plantilla de cortafuegos crea rutas estáticas, estas se añaden a este enrutador virtual.

Defina solo un enrutador para la implementación del escalado automático.



STEP 3 | En el contexto de **Network (Red)**, seleccione la plantilla que creó, seleccione **Interfaces** y **Add Interface (Añadir interfaz)**.

- En la pestaña Configuración, seleccione una ranura, seleccione el **Interface name (Nombre de interfaz)** y seleccione Layer3 **Interface Type (Tipo de interfaz)**. En el menú **Security Zone (Zona de seguridad)**, seleccione **New Zone (Nueva zona)**, asigne el nombre Untrust a la zona y haga clic en **OK (Aceptar)**.
- En la pestaña **IPv4**, habilite **DHCP Client (Cliente DHCP)** y **Automatically create default route pointing to default gateway provided by server (Crear automáticamente una ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor)** (habilitada por defecto) y haga clic en **OK (Aceptar)**.



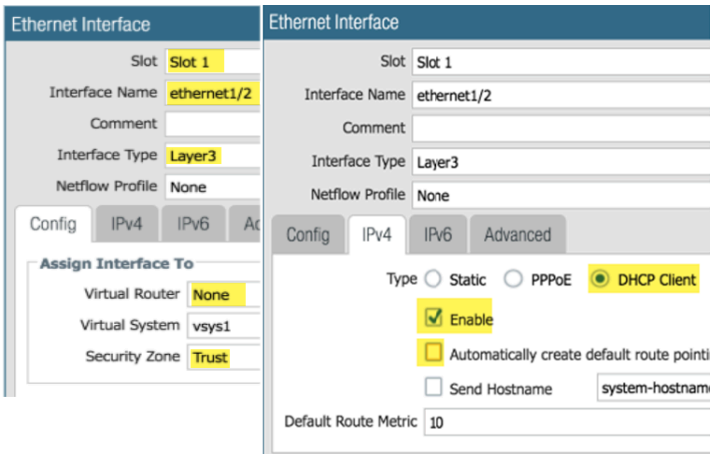
STEP 4 | Añada la interfaz de capa 3 ethernet1/2 (Trust).

- En la pestaña Configuración, elija la misma ranura que en el paso anterior, seleccione el **Interface name (Nombre de la interfaz)** (ethernet1/2) y seleccione Layer3 **Interface Type (Tipo de**

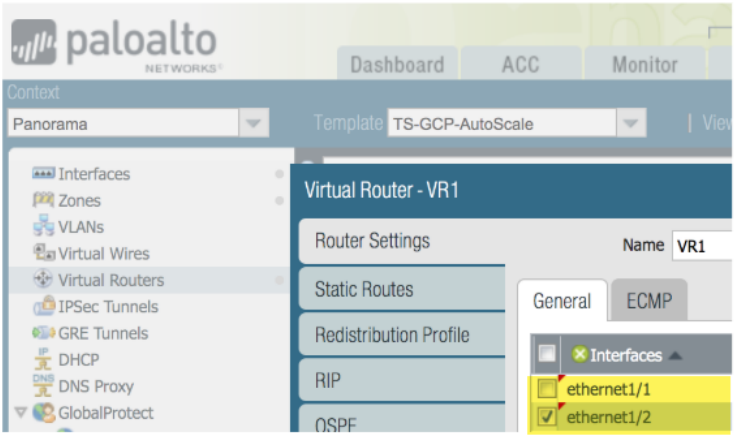
 ©2024 Palo Alto Networks, Inc.

interfaz). En el menú **Security Zone (Zona de seguridad)**, seleccione **New Zone (Nueva zona)**, asigne el nombre Trust a la zona y haga clic en **OK (Aceptar)**.

- En la pestaña **IPv4**, habilite **DHCP Client (Cliente DHCP)**, deshabilite **Automatically create default route pointing to default gateway provided by server (Crear automáticamente ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor)** y haga clic en **OK (Aceptar)**.



STEP 5 | Vuelva a su pila de plantillas y al enrutador virtual que creó anteriormente. Coloque las interfaces untrust y trust (ethernet1 / 1 y ethernet1 / 2) en el enrutador virtual y haga clic en **OK (Aceptar)**.

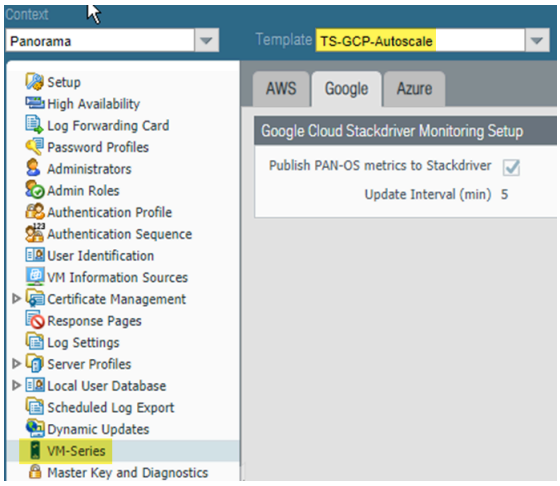


 ©2024 Palo Alto Networks, Inc.

STEP 6 | Configure Stackdriver para su implementación de escalado automático.

Debe tener el Complemento VM-Series en Panorama para configurar Stackdriver.

1. En el contexto **Device (Dispositivo)**, seleccione la pila de plantillas que creó anteriormente en el menú desplegable Plantilla.
2. Seleccione **Device (Dispositivo)** > **VM-Series** > **Google** y haga clic en el engranaje Editar ( ). Consulte **Publish PAN-OS metrics to Stackdriver (Publicación de métricas de PAN-OS en Stackdriver)**.



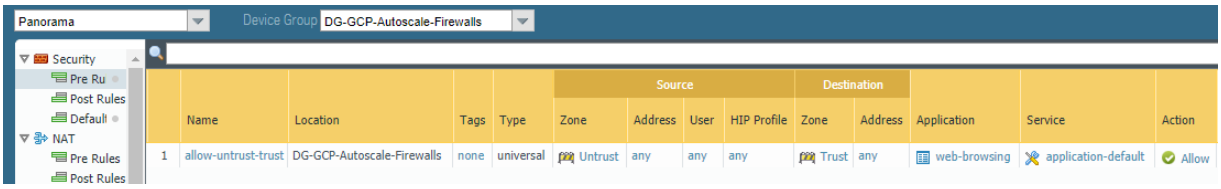
3. Confirme los cambios.

STEP 7 | Cree un Grupo de dispositivos que haga referencia a la plantilla o la pila de plantillas que creó en el Paso 1.

Este Grupo de dispositivos contendrá los cortafuegos VM-Series que cree con la plantilla de cortafuegos.

1. Añada una política de seguridad que permita el tráfico de exploración web de Untrust a Trust.

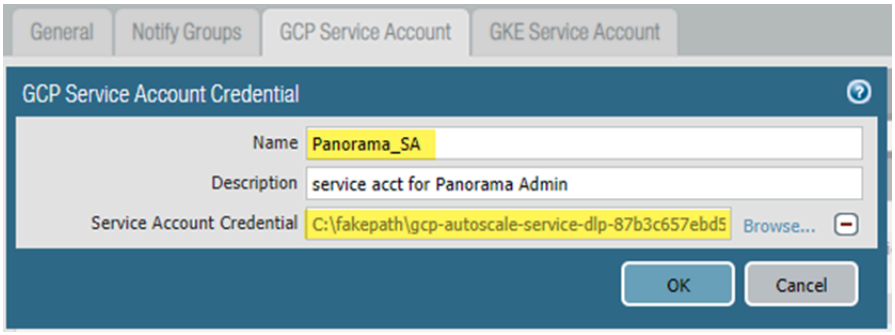
   En el contexto Políticas, seleccione el Grupo de dispositivos que acaba de crear. Seleccione **Security (Seguridad)** > **Pre Rules (Reglas previas)** y **Add (Añadir)** la siguiente política de seguridad.



 ©2024 Palo Alto Networks, Inc.

STEP 8 | Configure la cuenta de servicio de GCP para el proyecto host.

1. En el contexto de Panorama, expanda Google Cloud Platform, seleccione **Setup (Configuración)** y haga clic en **Add (Añadir)**.
2. Proporcione un nombre y una descripción para la cuenta de servicio de host que creó en el Paso 4.
3. Suba el archivo de credenciales JSON que creó en el Paso 4. 4.

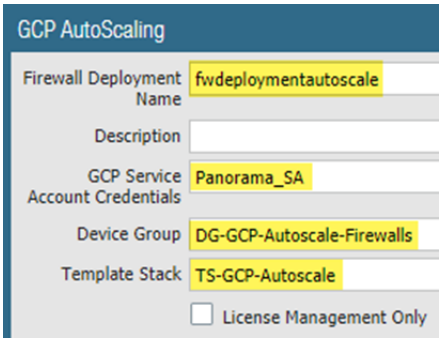


Después de añadir una credencial de cuenta de servicio, puede validar la credencial desde su línea de comando de Panorama (no puede validar desde la interfaz web):

```
request plugins gcp validate-service-account
 gcp_service_account <svc-acct-credential-name>
```

STEP 9 | Configure el escalado automático en el complemento Panorama para GCP.

1. En el contexto de Panorama, expanda Google Cloud Platform, seleccione Escalado automático y haga clic en **Add (Añadir)**.
2. Proporcione el nombre de implementación del cortafuegos y una descripción opcional para la implementación.
3. Para la credencial de la cuenta de servicio de GCP, proporcione el nombre de la cuenta de servicio de GCP del Paso 8.



4. Seleccione el Grupo de dispositivos que creó en el Paso 7 y la pila de plantillas que creó en el Paso 1.
5. Desactive **License Management Only (Solo administración de licencias)** para garantizar que el tráfico esté protegido.

STEP 10 | Confirme los cambios.

 ©2024 Palo Alto Networks, Inc.

Prepare un paquete de arranque de cortafuegos VM-Series para escalado automático

Durante el arranque, la solicitud inicial del cortafuegos proporciona la dirección IP del host y el número de serie, y la clave de autenticación de la máquina virtual para que Panorama pueda validar la clave de autenticación de VM y añadir el cortafuegos como un dispositivo gestionado. A continuación, Panorama puede asignar el cortafuegos al grupo de dispositivos y la plantilla adecuados para que pueda configurar y gestionar de forma centralizada el cortafuegos utilizando Panorama.

En este caso, debe generar una clave de autenticación de máquina virtual en Panorama e incluir la clave en el archivo init-cfg.txt que utiliza para el arranque. La clave de autenticación VM permite a Panorama autenticar el cortafuegos VM-Series que acaba de bootstrap. El paquete de arranque debe incluir.

- En el directorio /config, un archivo init-cfg.txt que incluye la dirección IP de Panorama
- En el directorio /license, la clave de autenticación de VM en un archivo llamado authcodes.

  La vida útil de la tecla puede variar entre 1 hora y 8760 horas (un año). Tras el tiempo especificado, la clave expira y Panorama no registrará los cortafuegos VM-Series sin una tecla de autenticación válida en esta solicitud de conexión.

STEP 1 | Configure un depósito de almacenamiento de Google con las carpetas necesarias para arrancar el cortafuegos VM-Series en Google Cloud Platform. Puede utilizar un paquete de arranque existente o crear un nuevo paquete de arranque para estas carpetas.

STEP 2 | Edite los valores en el archivo `init-cfg.txt` de muestra para personalizar el archivo para su entorno.

Las plantillas de cortafuegos incluyen un archivo `init-cfg.txt` de muestra.

Parámetros	Valor	Comentarios
tipo	dhcp-client	
hostname	<pa-vm>	Nombre opcional que asignó cuando preparó el proyecto host. Solo se requiere si un host específico es necesario y dhcp-send-hostname no lo es.
vm-auth-key	<vmauthkey>	Una clave que Panorama debe validar antes de añadir un cortafuegos como dispositivo gestionado. Consulte Generación de la clave de autenticación de VM en Panorama.
panorama-server	<panorama-ip>	La dirección IP del dispositivo de gestión de Panorama que configuró en Configure el complemento de Panorama para GCP para proteger una

 ©2024 Palo Alto Networks, Inc.

Parámetros	Valor	Comentarios
		implementación de escalado automático
Tplname	<template-stack-name>	La pila de plantillas que creó en Configure el complemento de Panorama para GCP para proteger una implementación de escalado automático.
Dgname	<dg-name>	El nombre del grupo de dispositivos que creó en el complemento de Panorama para GCP.
dns-primary		Su servidor DNS principal.
dns-secondary		Su servidor DNS secundario.
dhcp-send-hostname	sí	Dejar tal y como está.
dhcp-send-client-id	sí	Dejar tal y como está.
dhcp-accept-server-hostname	sí	Dejar tal y como está.
dhcp-accept-server-domain	sí	Dejar tal y como está.

STEP 3 | Suba el archivo `init-cfg.txt` editado a la carpeta `/config` en tu paquete de arranque.

STEP 4 | Si utiliza BYOL, cree un archivo de texto llamado `authcodes` (sin extensión), añada su código de autenticación y cargue el archivo en la carpeta `/license`.

Implementar plantillas de escalado automático de GCP

- Acerca de las plantillas de escalado automático
- Implemente la plantilla del cortafuegos
- Preparación de un proyecto de servicio
- Configuración de la VPC compartida
- Implementación de la plantilla de la aplicación
- Incorporación de una nueva aplicación
- Plantillas de servicio de GKE de muestra

Acerca de las plantillas de escalado automático

Descargue las plantillas de escalado automático de Palo Alto Networks desde https://github.com/PaloAltoNetworks/GCP-AutoScaling. El archivo zip contiene archivos zip independientes para las plantillas del cortafuegos y de la aplicación. Cada archivo zip es un directorio de plantilla que contiene varios archivos, pero solo necesita editar los archivos YAML.

 ©2024 Palo Alto Networks, Inc.

- Plantillas de cortafuegos
- Plantilla de aplicación

Plantillas de cortafuegos

Los archivos del directorio de cortafuegos crean cortafuegos VM-Series y otros recursos de implementación. Crean nuevas redes y las subredes familiares para el cortafuegos VM-series: gestión, untrust y trust. También implementan un servicio de mensajería Cloud Pub/Sub para transmitir información desde GCP al complemento de Panorama para GCP. Con esta infraestructura implementada, el complemento puede aprovechar los grupos de direcciones dinámicas para aplicar la política de seguridad en el tráfico de entrada enrutado a los servicios que se ejecutan en GCP y usar métricas de escalado automático para implementar cortafuegos VM-series para satisfacer la mayor demanda de recursos de carga de trabajo de aplicaciones, o para eliminar cortafuegos. que ya no son necesarios.

Para configurar su balanceador de carga, edite el archivo `.yaml` para un balanceador de carga de aplicación externo (ALB) o balanceador de carga de red (NLB).

- **ALB** (balanceador de carga externo de HTTP)

  Para personalizar un ALB, edite `vm-series-fw-alb.yaml`.

  El balanceador de carga externo de HTTP es un balanceador de carga basado en proxy que realiza SNAT y DNAT en el tráfico de entrada de Internet. El balanceador de carga de HTTP está diseñado para admitir solo los puertos TCP 80 y 8080.

  Para admitir varias aplicaciones que usan el balanceador de carga HTTP en la arquitectura de sándwich del balanceador de carga, podemos usar el balanceador de carga HTTP de GCP *urlMap* y *namedPort* para asignar diferentes URL a diferentes puertos en el balanceador de carga. A su vez, el cortafuegos VM-Series puede trasladar los puertos a diferentes aplicaciones, cada una representada por un balanceador de carga interno por aplicación.
- **NLB** (balanceador de carga TCP)

  Para personalizar un NLB, edite `vm-series-fw-nlb.yaml`.

  El balanceador de carga de TCP es un balanceador de carga no basado en proxy, lo que significa que no realiza NAT en el tráfico de entrada de Internet.

  El balanceador de carga de TCP en GCP permite añadir varias direcciones IP frontend con un puerto arbitrario, lo que hace posible admitir varias aplicaciones.

  Otra ventaja del balanceador de carga de TCP es que conserva la dirección IP original del cliente, lo que es deseable para algunas aplicaciones.

Plantilla de aplicación

El directorio de la aplicación proporciona una aplicación de muestra. Configura e implementa un balanceador de carga interno (ILB) para permitir que sus servidores de aplicaciones se suscriban al servicio Pub/Sub y se comuniquen con sus cortafuegos VM-Series y el complemento de GCP en Panorama.

Para personalizar la plantilla de la aplicación, edite `apps.yaml` como se describe en Implemente la plantilla del cortafuegos y Plantilla de aplicación.

Implemente la plantilla del cortafuegos

Edite el Plantillas de cortafuegos del proyecto host.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Edite las variables de entorno `vm-series-fw-nlb.yaml` o `vm-series-fw-alb.yaml` para reflejar su entorno de nube.

El ejemplo de este flujo de trabajo es para el NLB. Consulte vm-series-fw-nlb.yaml y vm-series-fw-alb.yaml para obtener una explicación más detallada de los parámetros de la plantilla.

```
properties:     region: us-east1     zones:     -us-east1-b     #
 Do not modify the lb-type field.     lb-type: nlb     cloud-nat:
 yes     forwarding-rule-port: 80
```

```
# Only one app is allowed     urlPath-namedPort-maps:     -
 appName: app1
```

```
# ssh key PUBLIC:     - optional
```

La plantilla de cortafuegos de escalado automático requiere que introduzca el valor entre comillas simples y anteponga la clave con **`admin:`** seguido de un espacio. Esta es la misma convención utilizada para la plantilla de Google Marketplace, como se detalla en Par de claves SSH. Por ejemplo:

```
    sshkey: 'admin: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDe0gJHd8okxPGWXsmdTdcZBJNI6ONT/NSz6INs2CNtKW
[redacted]
oTKXL8t0SRnOKaKV73NR5KnfpsNfwGxG8aQtEkeMCZIxX+6WOnRf/N4K3
yourname@[redacted].paloaltonetworks.local'
```

```
    bootstrap-bucket: bootstrap-autoscale
```

```
    image: vmseries-byol-814     machine-type: n1-standard-4
```

Para la cuenta de servicio, proporcione la dirección de correo electrónico de la cuenta de servicio del proyecto host que creó anteriormente (paso 3).

```
     service-account: sa-pan@gcp-autoscale-
kk.iam.gserviceaccount.com
```

El valor fw-instance-tag será el nombre del grupo de instancias gestionadas en la implementación.

```
     fw-instance-tag: vm-series-fw
```

Elija una métrica para el escalado automático. Los valores posibles son: panSessionActive, panSessionUtilization, DataPlaneCPUUtilizationPct, DataPlanePacketBufferUtilization o panSessionUtilization.

```
metric: custom.googleapis.com/VMSeries/panSessionActive
```

 ©2024 Palo Alto Networks, Inc.

```
max-size 2 min-size 1 target-type GAUGE util-target: 100
```

```
# Greenfield deployment 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
```

STEP 2 | Implemente la plantilla del cortafuegos.

```
gcloud deployment-manager deployments create <your-template> --
config apps.yaml --automatic-rollback-on-error
```

Tome nota de los resultados que imprime la CLI después de la implementación: los nombres de subred, el nombre de la implementación y el nombre del tema Pub/Sub de Panorama. Necesita estos valores para configurar la VPC compartida y para la implementación de la plantilla de la aplicación.

El nombre de la implementación del cortafuegos debe configurarse en el complemento de Panorama para la definición de escalado automático de GCP.

Preparación de un proyecto de servicio

Cree un proyecto de servicio independiente o elija un proyecto existente para su aplicación.

Para obtener más información sobre los proyectos de servicio y host en una VPC compartida, consulte la Descripción general de la VPC compartida y revise las funciones de Administradores e IAM. Un administrador de proyecto host debe tener la función adecuada para configurar la VPC compartida y convertir el proyecto de aplicación en un proyecto de servicio para el proyecto host. Consulte las instrucciones en Aprovisionamiento de VPC compartida.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Habilite las API del proyecto de servicio desde la consola de GCP o la CLI.

Las API requeridas son:

- ❑ API de Cloud Deployment Manager
- ❑ API de Cloud Pub/Sub
- ❑ API de Compute Engine

Habilitación de las API desde la consola de GCP

1. Seleccione el proyecto de servicio y, en el menú de navegación, seleccione **APIs & Services (API y servicios)**.
2. Busque y vea cada API solicitada.
3. Debe **ENABLE (HABILITAR)** cualquier API que no muestre el estado "API habilitada".

Habilitación de las API desde la CLI

1. En la CLI, vea su configuración para asegurarse de que está en el proyecto correcto.

```
gcloud config list
```

Si no es así, defina el proyecto de la siguiente manera:

```
gcloud config set project <project-name>
```

2. Emita los siguientes comandos para habilitar las API necesarias.

```
gcloud services enable deploymentmanager.googleapis.com gcloud
 services enable pubsub.googleapis.com gcloud services enable
 compute.googleapis.com
```

3. Compruebe que las API necesarias estén habilitadas.

```
gcloud services list --enabled
```

STEP 2 | Convierta el proyecto de aplicación en un proyecto de servicio para el proyecto host.

Añada la cuenta de servicio del administrador del proyecto de servicio/aplicación como miembro en el proyecto host con las siguientes funciones:

- Usuario de la red de Compute
- Administrador de Pub/Sub

STEP 3 | Elija una configuración de VPC.

- Si el proyecto de servicio va a compartir las redes en el proyecto host, continúe a Configuración de la VPC compartida.
- Si el proyecto de servicio tiene su propia red de VPC para la implementación de la aplicación, vaya a Configuración de una VPC emparejada.

 ©2024 Palo Alto Networks, Inc.

Configuración de la VPC compartida

Una vez implementada la plantilla de cortafuegos en el proyecto host, configure el proyecto de servicio que admita sus aplicaciones. Un administrador con credenciales de VPC compartidas realiza estas tareas desde el proyecto host. Para comprender más sobre el proyecto host y los proyectos de servicio en el contexto de la VPC compartida, consulte la Descripción general de la VPC compartida.

STEP 1 | Cree una VPC compartida utilizando la VPC de Trust creada cuando implementó la plantilla de cortafuegos.

Configure una VPC compartida para el proyecto de host (cortafuegos):

```
gcloud compute shared-vpc enable HOST_PROJECT_ID
```

STEP 2 | Adjunte el proyecto de servicio/aplicación al proyecto host.

```
gcloud compute shared-vpc associated-projects add
[SERVICE_PROJECT_ID]--host-project [HOST_PROJECT_ID]
```

Hay opciones adicionales disponibles para compartir solo subredes específicas, en lugar de todas las subredes en el proyecto host.

STEP 3 | Si desea utilizar la plantilla de aplicación de muestra para implementar una aplicación, continúe con Implementación de la plantilla de la aplicación.

Si ya ha implementado una aplicación y desea protegerla en su implementación de escalado automático, vaya a Incorporar manualmente una aplicación a una implementación de escalado automático existente.

Si ha implementado un servicio en un clúster de GKE, continúe con Incorporación de un clúster de GKE en una VPC compartida.

Configuración de una VPC emparejada

Se debe establecer una conexión de emparejamiento de redes de VPC entre dos VPC. Si las VPC están en dos proyectos diferentes, se debe crear una conexión en **ambos** proyectos.

STEP 1 | En el proyecto host, empareje la red VPC Trust de la implementación del cortafuegos con la VPC de la aplicación.

```
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 | En el proyecto de servicio, empareje la red VPC Trust de la implementación de la aplicación con la red VPC Trust de la implementación del cortafuegos.

```
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]
```

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Si desea utilizar la plantilla de aplicación de muestra para implementar una aplicación, continúe con Implementación de la plantilla de la aplicación.

Si ya ha implementado una aplicación y desea protegerla en su implementación de escalado automático, vaya a Incorporar manualmente una aplicación a una implementación de escalado automático existente.

Si ha implementado un servicio en un clúster de GKE, continúe con Incorporación de un clúster de GKE en una VPC emparejada.

Implementación de la plantilla de la aplicación

El administrador del proyecto de servicio implementa el Plantilla de aplicación del proyecto de servicio.

STEP 1 | Cree un proyecto de aplicación independiente (proyecto de servicio) para implementar la aplicación (consulte Preparación de un proyecto de servicio).

STEP 2 | Prepare el archivo `apps.yaml` como se describe en apps.yaml.

STEP 3 | Implemente una nueva aplicación con la plantilla de aplicación y defina una etiqueta para el puerto designado.

```
gcloud deployment-manager deployments create <your-template> --
config apps.yaml --automatic-rollback-on-error
```

Continúe a Ver la aplicación incorporada en el complemento de Panorama para GCP.

Incorporación de una nueva aplicación

Cuando utilice la Plantilla de aplicación para implementar una aplicación, se encarga de la conexión con el proyecto host. Puede proteger aplicaciones que no ha implementado con la plantilla de aplicación, siempre que se implementen en un proyecto de servicio con las capacidades descritas en Preparación de un proyecto de servicio.

- Incorporar manualmente una aplicación a una implementación de escalado automático existente
- Incorporación de un clúster de GKE

Incorporar manualmente una aplicación a una implementación de escalado automático existente

Para proteger una aplicación que ha implementado con un balanceador de carga externo y una implementación de cortafuegos VM-series con escalado automático, siga estos pasos. Para cada aplicación que incorpore, debe proporcionar el nombre de la aplicación, los puertos con nombre y la ruta.

STEP 1 | Prepárese para agregar un nuevo puerto con nombre y una ruta URL al balanceador de carga externo de HTTP creado cuando implementó la plantilla de cortafuegos .

STEP 2 | Actualice todos los puertos con nombre de los grupos de instancias con un nombre de servicio adicional y valores de puerto. El siguiente ejemplo incorpora las aplicaciones `app2` y `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
 gcloud compute instance-groups set-named-ports fw-
```

 ©2024 Palo Alto Networks, Inc.

```
template2-fw-igm-us-east1-c --zone us-east1-c --named-
ports=app1:80,app2:81,app3:82
```

STEP 3 | Cree una nueva http-health-check.

```
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 | Cree un nuevo servicio de backend con el nombre de puerto creado anteriormente en el balanceador de carga externo de 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
```

Verifique si el nuevo servicio de backend está visible.

```
gcloud compute backend-services list
```

STEP 5 | Edite mapas de URL y añada una nueva regla de ruta. Por ejemplo:

```
- 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 | Para proteger esta aplicación con el cortafuegos VM-series, active manualmente el mensaje pub/sub a través de la CLI de gcloud. Esto envía un mensaje al tema creado en la plantilla de cortafuegos.

```
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 | Ver la aplicación incorporada en el complemento de Panorama para GCP.

STEP 8 | (Opcional) Para actualizar los atributos de la aplicación, como ilb-ip, ilb-port o named-port, emita el comando pubsub:

```
gcloud pubsub topics publish projects/gcp-pavmqa/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-
```

 ©2024 Palo Alto Networks, Inc.

```
cidr=172.22.9.0/24,     fw-deployment-name=hj-asg-891ca3,     host-
project=gcp-pavmqa,     type=UPDATE-APP   --message "UPDATE-APP"
```

STEP 9 | (Opcional) Para dejar de proteger la aplicación, ejecute el siguiente comando:

```
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"
```

Incorporación de un clúster de GKE

Para incorporar un clúster GKE privado, el complemento de GCP para Panorama requiere la siguiente información.

- En GCP, exponga el frontend del ELB para el clúster al servicio de GKE para que el cortafuegos VM-Series pueda obtener la información del puerto con nombre para el servicio.
- La dirección del servidor de la API del clúster.
- La credencial de la cuenta de servicio para el servicio en el que se implementa el clúster, en formato JSON.

El nombre del clúster de GKE no debe superar los 24 caracteres. Esto garantiza que si implementa el escalado automático en una configuración de VPC emparejada, el nombre de la ruta estática no supera los 31 caracteres.

- Incorporación de un clúster de GKE en una VPC compartida
- Incorporación de un clúster de GKE en una VPC emparejada
- Ver la aplicación incorporada en el complemento de Panorama para GCP
- Ver el estado de implementación desde la CLI

Incorporación de un clúster de GKE en una VPC compartida

Para incorporar el clúster de GKE, debe compartir la VPC de red Trust del proyecto de host con el Proyecto de servicio. Consulte Configuración de la VPC compartida.

Por motivos de seguridad, solo se deben usar clústeres privados en una implementación de escalado automático. Consulte Creación de un clúster privado.

STEP 1 | Establezca el ID del proyecto host.

```
Proyecto de conjunto de configuración de gcloud [HOST_PROJECT_ID]
```

 ©2024 Palo Alto Networks, Inc.

STEP 2 | (opcional) Establezca la zona o región de compute para los clústeres.

Si el clúster es zonal, introduzca lo siguiente:

```
gcloud config set compute/zone [COMPUTE_ZONE]
```

Si el clúster es regional, introduzca lo siguiente:

```
gcloud config set compute/region [COMPUTE_REGION]
```

STEP 3 | En el proyecto host, actualice los intervalos secundarios en la subred VPC de Trust.

```
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]
```

Los intervalos de IP de servicio y pods deben estar dentro de: 10.0.0.0/8, 172.16.0.0/12 o 192.168.0.0/16 y no pueden chocar con los intervalos de IP existentes en la subred.

STEP 4 | En el proyecto de servicio, cree un clúster privado en la VPC compartida.

1. Establezca el ID del proyecto de servicio.

   ```
   gcloud config set project [SERVicE_PROJECT_ID]
   ```

2. Cree un clúster privado en la VPC compartida.

   ```
   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 | Verifique el contexto de su clúster actual:

```
kubectl config current-context
```

STEP 6 | Verifique todos los contextos del clúster.

```
kubectl config get-context
```

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Cambie a otro clúster.

```
kubectl config use-context [CONTEXT_NAME]
```

Si ha creado su clúster en la consola de GCP, genere una entrada kubeconfig:

```
gcloud container clusters get-credentials [CLUSTER_NAME]
```

STEP 8 | Cree una función de clúster en un archivo `.yaml`, por ejemplo, `gke_cluster_role.yaml`.

```
apiVersion: rbac.authorization.k8s.io/v1beta1 tipo: ClusterRole
 metadata:   name: gke-plugin-role rules:   - apiGroups:       - ""
     resources:       - services     verbs:       - list
```

STEP 9 | Aplique la función de clúster.

```
kubectl apply -f gke_cluster_role.yaml
```

STEP 10 | Cree un enlace de función de clúster en un archivo `.yaml`, por ejemplo, `gke_cluster_role_binding.yaml`.

```
tipo: 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 | Aplicar el enlace de función de clúster.

```
kubectl apply -f gke_cluster_role_binding.yaml
```

STEP 12 | Cree una cuenta de servicio.

```
kubectl create serviceaccount [SERVICEACCOUNT_NAME]
```

STEP 13 | Exporte el token secreto de la cuenta de servicio en formato 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 | Obtenga la dirección del servidor API.

```
kubectl config view --minify | grep server | cut -f 2- -d ":" | tr
 -d " "
```

 ©2024 Palo Alto Networks, Inc.

STEP 15 | En el complemento de Panorama para GCP, añada la información de la cuenta de servicio.

Seleccione **Panorama** > **Google Cloud Platform** > **Setup (Configuración)**.

Nombre la credencial, introduzca una descripción e introduzca la **API server address (Dirección del servidor API)** del paso 14, y para la **Credencial de cuenta de servicio de GKE**, suba el archivo JSON que exportó en el paso 13.

Después de añadir una credencial de cuenta de servicio, puede validar la credencial desde su línea de comando de Panorama (no puede validar desde la interfaz web):

```
request plugins gcp validate-service-account gke_service_account
 <svc-acct-credential-name>
```

STEP 16 | Configure el escalado automático en el complemento Panorama para GCP.

1. En el contexto de Panorama, expanda Google Cloud Platform, seleccione Escalado automático y haga clic en **Add (Añadir)**.
2. Proporcione el **Firewall Deployment Name (Nombre de la implementación del cortafuegos)** y una descripción opcional para la implementación.
3. Para la **GCP Service Account Credential (Credencial de la cuenta de servicio de GCP)**, proporcione el nombre de la cuenta de servicio de GCP creado enPrepare un proyecto host y las cuentas de servicio necesarias, paso 4.
4. Seleccione el grupo de dispositivos y la pila de plantillas que ha creado cuando configuró el complemento de Panorama.
5. Desactive **License Management Only (Solo administración de licencias)** para garantizar que el tráfico esté protegido.
6. Introduzca el **GKE Cluster Name (Nombre del clúster de GKE)** exacto.
7. (Opcional) Introduzca una **Description (Descripción)** del clúster GKE.
8. Introduzca el **Network CIDR (CIDR de red)** para el clúster de GKE.
9. Seleccione la **GKE Service Account (Cuenta de servicio de GKE)** correspondiente al clúster de GKE.

STEP 17 | Confirme los cambios.

STEP 18 | (Opcional) Cree e implemente una plantilla de servicio de acuerdo con Uso de las plantillas de servicio de GKE de muestra, o implemente un servicio de GKE en la consola de GCP.

Incorporación de un clúster de GKE en una VPC emparejada

Para incorporar el clúster de GKE, debe crear y emparejar la VPC de servicio con la red de confianza Trust del cortafuegos en el proyecto host, como se describe en Configuración de una VPC emparejada.

Por motivos de seguridad, solo se deben usar clústeres privados en una implementación de escalado automático. Consulte Creación de un clúster privado.

STEP 1 | Establezca el ID del proyecto.

```
gcloud config set project [PROJECT_ID]
```

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Establezca la zona o región de compute para los clústeres.

Si el clúster es zonal, introduzca lo siguiente:

```
gcloud config set compute/zone [COMPUTE_ZONE]
```

Si el clúster es regional, introduzca lo siguiente:

```
gcloud config set compute/region [COMPUTE_REGION]
```

STEP 3 | Actualice la red de VPC del proyecto de servicio con los intervalos de IP secundarios para los pods y los servicios.

```
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 | Habilite la nube de NAT.

Cloud NAT es necesaria para implementar un clúster privado.

```
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 | Cree un nuevo clúster privado en la VPC de servicio.

```
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]
```

STEP 6 | Verifique el contexto de su clúster actual:

```
kubectl config current-context
```

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Verifique todos los contextos del clúster.

```
kubectl config get-context
```

STEP 8 | Cambie a otro clúster.

```
kubectl config use-context [CONTEXT_NAME]
```

Si ha creado su clúster en la consola de GCP, genere una entrada kubeconfig:

```
gcloud container clusters get-credentials [CLUSTER_NAME]
```

STEP 9 | Cree una función de clúster en un archivo `.yaml`, por ejemplo, `gke_cluster_role.yaml`.

```
apiVersion: rbac.authorization.k8s.io/v1beta1 tipo: ClusterRole
 metadata:   name: gke-plugin-role rules:   - apiGroups:       - ""
     resources:       - services     verbs:       - list
```

STEP 10 | Aplique la función de clúster.

```
kubectl apply -f gke_cluster_role.yaml
```

STEP 11 | Cree un enlace de función de clúster en un archivo `.yaml`, por ejemplo, `gke_cluster_role_binding.yaml`.

```
tipo: 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 | Aplicar el enlace de función de clúster.

```
kubectl apply -f gke_cluster_role_binding.yaml
```

STEP 13 | Cree una cuenta de servicio.

```
kubectl create serviceaccount [SERVICEACCOUNT_NAME]
```

STEP 14 | Exporte el token secreto de la cuenta de servicio en formato JSON.

```
MY_TOKEN=`kubectl get serviceaccounts [SERVICEACCOUNT_NAME] -o
 jsonpath='{.secrets[0].name}'` kubectl get secret $MY_TOKEN -o
 json >[FILE_NAME].json
```

 ©2024 Palo Alto Networks, Inc.

STEP 15 | Obtenga la dirección del servidor API.

```
kubectl config view --minify | grep server | cut -f 2- -d ":" | tr
 -d " "
```

STEP 16 | En el complemento de Panorama para GCP, añada la información de la cuenta de servicio.

Seleccione **Panorama** > **Google Cloud Platform** > **Setup (Configuración)**.

Nombre la credencial e introduzca la **API server address (Dirección del servidor API)** del Paso 15, y cargue el archivo JSON que exportó en el Paso 14.

Después de añadir una credencial de cuenta de servicio, puede validar la credencial desde su línea de comando de Panorama:

```
request plugins gcp validate-service-account <svc-acct-credential-
name>
```

STEP 17 | Configure el escalado automático en el complemento Panorama para GCP.

1. En el contexto de Panorama, expanda Google Cloud Platform, seleccione Escalado automático y haga clic en **Add (Añadir)**.
2. Proporcione el **Firewall Deployment Name (Nombre de la implementación del cortafuegos)** y una descripción opcional para la implementación.
3. Para la **GCP Service Account Credential (Credencial de la cuenta de servicio de GCP)**, proporcione el nombre de la cuenta de servicio de GCP del Paso 16.
4. Seleccione el grupo de dispositivos y la pila de plantillas que ha creado cuando configuró el complemento de Panorama.
5. Desactive **License Management Only (Solo administración de licencias)** para garantizar que el tráfico esté protegido.
6. Introduzca el **GKE Cluster Name (Nombre del clúster de GKE)** exacto.
7. (Opcional) Introduzca una **Description (Descripción)** del clúster GKE.
8. Introduzca el **Network CIDR (CIDR de red)** para el clúster de GKE.
9. Seleccione la **GKE Service Account (Cuenta de servicio de GKE)** correspondiente al clúster de GKE.

STEP 18 | (Opcional) En su proyecto de servicio, cree e implemente una plantilla de GKE de acuerdo con Uso de las plantillas de servicio de GKE de muestra, o implemente un servicio de GKE con la consola de GCP. Incorporación de un clúster de GKE

Ver la aplicación incorporada en el complemento de Panorama para GCP

Seleccione **Panorama** > **Google Cloud Platform** > **Autoscaling (Escalado automático)** para ver su aplicación incorporada. La columna **Details (Detalles)** solo es visible si tiene una aplicación incorporada.

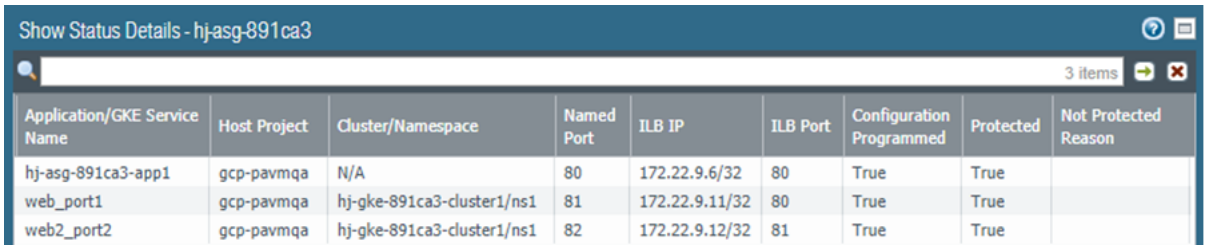
 ©2024 Palo Alto Networks, Inc.

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

Cada vínculo de la columna Detalles desencadena una acción.

©2024 Palo Alto Networks, Inc.

- **Mostrar estado**: Ver los detalles de las aplicaciones incorporadas en una implementación de cortafuegos VM-Series de 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	

Los siguientes campos muestran información obtenida de la implementación seleccionada. Estos valores se especificaron en el mensaje pub/sub o mediante el sondeo del servicio de clúster de GKE.

- **Application/GKE Service Name (Nombre del servicio de aplicación/GKE)**: un nombre de implementación de la aplicación o el nombre de un servicio de GKE.
- **Host Project (Proyecto host)**: el nombre del proyecto host.
- **Cluster/Namespace (Clúster/Espacio de nombres)**: un nombre de clúster de GKE seguido del espacio de nombres, por ejemplo, **`mycluster/namespace9`**.
- **Named Port (Puerto determinado)**: el puerto asignado al puerto determinado para el servicio.
- **ILB IP (IP del ILB)**: la dirección IP del ILB.
- **ILB Port (Puerto del ILB)**: el número de puerto del ILB.

  Para realizar el escalado automático de una aplicación, esta propiedad es **`ilb-port`** en `apps.yaml`.

  Para proteger un clúster de GKE, este valor es el número de puerto del clúster de GKE, como se especifica en el archivo `.yaml` que utilizó para implementar el servicio en su clúster.
- **Configuration Programmed (Configuración programada)**: verdadero si existe una regla NAT, falso si no.
- **Protected (Protegido)**: verdadero cuando una aplicación se ha incorporado correctamente o falso si la incorporación ha fallado. Si es falso, consulte la columna **Not Protected Reason (Motivo para la no protección)** para obtener una explicación.
- **Not Protected Reason (Motivo para la no protección)**: si **Protected (Protegido)** es Falso, muestra el motivo por el que la aplicación no está protegida. Algunos motivos comunes son:
  - **Configuration Programmed (Configuración programada)**: Verdadero si existe una regla NAT, de lo contrario Falso.
  - **Protected (Protegido)**: Verdadero cuando una aplicación se ha incorporado correctamente o Falso si la incorporación ha fallado. Si es falso, consulte la columna **Not Protected Reason (Motivo para la no protección)** para obtener una explicación.
  - **Not Protected Reason (Motivo para la no protección)**: si **Protected (Protegido)** es Falso, muestra el motivo por el que la aplicación no está protegida. Algunos motivos comunes son:
    - Se ha implementado un servicio UDP en el clúster de GKE.
    - Se ha especificado un puerto determinado que ya está en uso. Solo una aplicación puede escuchar en un puerto con nombre específico.

 ©2024 Palo Alto Networks, Inc.

- Se ha seleccionado la opción **License management only (Solo gestión de licencias)**, por lo que no se programa la configuración.
- No se ha encontrado ninguna etiqueta coincidente para los servicios de GKE.

- **Retirar la licencia de VM inactivas**: responda **Yes (Sí)** para activar la función de eliminación de licencias para VM inactivas.
- **Activar sincronización de servicios de GKE**: responda **Yes (Sí)** para sondear los servicios que se ejecutan en los clústeres y programar el NAT, la dirección y los objetos de servicio, y las rutas estáticas si es necesario. De forma predeterminada, Panorama sondea automáticamente 10 minutos después de la finalización del sondeo anterior.

Ver el estado de implementación desde la CLI

Puede utilizar la CLI de Panorama para gestionar las aplicaciones implementadas. Las acciones de la línea de comando están en línea con las descritas en Ver la aplicación incorporada en el complemento de Panorama para GCP. En los siguientes comandos, **`autoscaling_name`** es el nombre de implementación del cortafuegos que se introdujo en la configuración de escalado automático.

- Enumere las aplicaciones incorporadas (protegidas).

```
show plugins gcp show-protected-apps autoscaling_name <fw-deployment-name>
```

- Active la función de eliminación de licencias para cortafuegos en la implementación especificada.

```
request plugins gcp force-delicensing autoscaling_name <fw-deployment-name>
```

- Para una implementación de GKE, obligue al complemento a leer los mensajes pub-sub y sincronice las reglas de NAT que se programan en función de los mensajes pub-sub.

```
request plugins gcp gke-service-discovery autoscaling_name <fw-deployment-name>
```

Parámetros en las plantillas de escalado automático para GCP

Puede descargar el archivo de plantilla `.zip` desde https://github.com/PaloAltoNetworks/GCP-AutoScaling. El archivo `.zip` contiene directorios para admitir plantillas de cortafuegos para el balanceador de carga de red y las configuraciones del balanceador de carga de la aplicación, y la plantilla de la aplicación.

Los archivos YAML de plantilla tienen el siguiente formato general:

```
#Copyright and license information     :     :
 imports:                      <do not change>     :     : resources:
     -name: vm-series-fw       <do not change>     -type:vm-series-
fw.py    <do not change
    -properties:
    :
    :
outputs:                      <do not change>     :     :
```

 ©2024 Palo Alto Networks, Inc.

En todos los archivos `.yaml`, se personaliza las propiedades de `recursos` para su implementación. No cambie nada en las secciones `importaciones` o `salidas`.

- Plantillas de cortafuegos
- Plantilla de aplicación

Plantillas de cortafuegos

Las siguientes secciones detallan los parámetros para los archivos `.yaml` de NLB y ALB.

- vm-series-fw-nlb.yaml
- vm-series-fw-alb.yaml

vm-series-fw-nlb.yaml

En la plantilla `vm-series-fw-nlb.yaml`, edite las `-properties`.

Parámetros	Valor de muestra	Comentarios
región	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <list of zones>	zones- us-central1-a	Si corresponde, enumere varias zonas de la siguiente manera: zones- us-central1-a- us-central1-b- us-central1-c- us-central1-f
lb-type	nlb	No cambiar.
cloud-nat	sí	No cambiar.
forwarding-rule-port	80	80 o 8080
urlPath-namedPort-maps-appname	`urlPath-namedPort-maps -MyApplication`	Introduzca el nombre de su aplicación.
sshkey	'admin:ssh-rsa <PASTE KEY>'	Revisión Par de claves SSH. Entre comillas simples, escriba **`admin:`** seguido de un espacio y pegue su clave. Esta es la misma convención utilizada para la plantilla de Google Marketplace.
bootstrap-bucket	bootstrap-autoscale	El nombre del depósito de GCP que contiene el archivo de arranque.
imagen	vm-series-byol-814	La imagen BYOL actualmente disponible en el marketplace de Google.

 ©2024 Palo Alto Networks, Inc.

Parámetros	Valor de muestra	Comentarios
		Si está utilizando PAYG u otro modelo de licencia, la imagen puede ser diferente.
Tipo de máquina	n1-standard-4	n1-standard-4 es predeterminado para BYOL. Si su licencia lo permite, puede utilizar cualquier tipo de máquina en Requisitos mínimos del sistema para el cortafuegos VM-Series.
service-account		El nombre de cuenta de servicio único para el proyecto host.
fw-instance-tag	vm-series-fw	La etiqueta de instancia que proporcionó en GCP.
métrica	custom.googleapis.com/VMSeries/panSessionActive	La ruta de API personalizada para VM-Series y la métrica de escalado automático elegida. Proporcione solo una de las siguientes métricas. `panSessionActive panSessionUtilization DataPlaneCPUUtilizationPct DataPlanePacketBufferUtilization panSessionUtilization`
max-size	2	
min-size	1	
target-type	GAUGE	Actualmente GAUGE es el único tipo válido.
util-target	100	

Para implementar el cortafuegos VM-Series, necesita una red y subred dedicadas para las interfaces de gestión, untrust y trust del cortafuegos. Complete la información para una implementación greenfield (configure la plantilla para crear nuevas redes) o una implementación brownfield (use redes existentes). Asegúrese de retirar o comentar los parámetros de implementación de red que está utilizando.

Implementación Greenfield: Introduzca los valores para crear redes y subredes de gestión, untrust y trust para el cortafuegos.

 ©2024 Palo Alto Networks, Inc.

Parámetros	Valor de muestra	Comentarios
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`	
Implementación brownfield: Introduzca el nombre de cada red o subred existente		
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

En la plantilla `vm-series-fw-alb.yaml`, edite las `-properties`.

Parámetros	Valor de muestra	Comentarios
región	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <list of zones>	zones- us-central1-a	Si corresponde, enumere varias zonas de la siguiente manera: zones- us-central1-a- us-central1-b- us-central1-c- us-central1-f
lb-type	alb	No cambiar.
cloud-nat	sí	No cambiar.

 ©2024 Palo Alto Networks, Inc.

Parámetros	Valor de muestra	Comentarios
forwarding-rule-port	80	80
connection-draining-timeout	300	El valor de tiempo de espera en segundos.
`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/*'`	Enumera sus aplicaciones y el puerto determinado correspondiente
sshkey	'admin:ssh-rsa <PASTE KEY>'	Revisión Par de claves SSH. Entre comillas simples, escriba **`admin:`** seguido de un espacio y pegue su clave. Esta es la misma convención utilizada para la plantilla de Google Marketplace.
bootstrap-bucket	bootstrap-bucket-name	El nombre del depósito de GCP que contiene el archivo de arranque.
imagen	vm-series-byol-814	La imagen BYOL actualmente disponible en el marketplace de Google. Si está utilizando PAYG u otro modelo de licencia, la imagen puede ser diferente
Tipo de máquina	n1-standard-4	n1-standard-4 es predeterminado para BYOL. Si su licencia lo permite, puede utilizar cualquier tipo de máquina en Requisitos mínimos del sistema para el cortafuegos VM-Series.
service-account	El nombre de cuenta de servicio único para el proyecto de servicio.	
fw-instance-tag	vm-series-fw	La etiqueta de instancia que proporcionó en GCP.

 ©2024 Palo Alto Networks, Inc.

Parámetros	Valor de muestra	Comentarios
métrica	custom.googleapis.com/VMSeries/panSessionActive	La ruta de API personalizada para VM-Series y la métrica de escalado automático elegida. Proporcione solo una de las siguientes métricas. `panSessionActive panSessionUtilization DataPlaneCPUUtilizationPct DataPlanePacketBufferUtilization panSessionUtilization`
max-size	2	
min-size	1	
target-type	GAUGE	Actualmente GAUGE es el único tipo válido.
util-target	100	Introduzca el valor objetivo de utilización del objetivo para el escalado automático.
Implementación Greenfield: Introduzca los valores para crear redes y subredes de gestión, untrust y trust para el cortafuegos.		
mgmt-network-cidr	192.168.12.0/24	
untrust-network-cidr	192.168.11.0/24	
trust-network-cidr	192.168.11.0/24	
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`	
Implementación brownfield: Introduzca el nombre de cada red o subred existente		
mgmt-network	existing-vpc-mgmt	
mgmt-subnet	existing-subnet-mgmt	
trust-network	existing-vpc-trust	

 ©2024 Palo Alto Networks, Inc.

Parámetros	Valor de muestra	Comentarios
trust-subnet	existing-subnet-trust	
untrust-network	existing-vpc-untrust	
untrust-subnet	existing-subnet-untrust	

Plantilla de aplicación
apps.yaml

La plantilla de aplicación crea la conexión entre el proyecto host (que contiene los cortafuegos VM-Series) y el proyecto de servicio, que contiene la aplicación o los servicios que protege la implementación del cortafuegos.

Parámetros	Valor de muestra	Comentarios
host-project	your-host-project-name	El nombre del proyecto que incluye la implementación del cortafuegos VM-Series.
fw-deployment-name	my-vm-series-firewall-name	
región	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <list of zones>	zones- us-central1-a	Si corresponde, enumere varias zonas de la siguiente manera: `zones- us-central1-a - us-central1-b- us-central1-c- us-central1-f`
app-machine-type	n1-standard-2	El tipo de máquina para la máquina virtual que ejecuta su aplicación o servicio. Si su licencia lo permite, puede utilizar cualquier tipo de máquina en Requisitos mínimos del sistema para el cortafuegos VM-Series.
app-instance-tag	web-app-vm	Esta etiqueta (etiqueta) se aplicó en GCP.
sshkey	'admin:ssh-rsa <PASTE KEY>'	Revisión Par de claves SSH. Entre comillas simples, escriba **`admin:`** seguido de un espacio y pegue su clave. Esta es la misma

©2024 Palo Alto Networks, Inc.

Parámetros	Valor de muestra	Comentarios
		convención utilizada para la plantilla de Google Marketplace.
trust-network	<project-name>/<vpc-network-name>	Para una VPC compartida, el <project-name> es el nombre del proyecto host. Para las VPC emparejadas, el <project-name> es el nombre del proyecto de servicio.
trust-subnet	<project-name>/<subnet-name>	Para una VPC compartida, el <project-name> es el nombre del proyecto host. Para las VPC emparejadas, el <project-name> es el nombre del proyecto de servicio.
trust-subnet-cidr	10.2.0.0/24	Para una implementación totalmente nueva (greenfield), el CIDR de subnet Trust del proyecto de host (el parámetro trust-network-cidr en la plantilla de cortafuegos). Para una implementación brownfield, el CIDR para la red Trust.
vm-series-fw-template-topic	<pubsub-topic>	Introduzca el nombre del tema creado por la implementación del cortafuegos. La plantilla de la aplicación envía un mensaje al tema para programar la configuración del cortafuegos para reenviar el tráfico.
ilb-port	80	Introduzca el número de puerto para la salida del puerto del balanceador de carga interno de su aplicación.
urlPath-namedPort	83	Introduzca el número de puerto para la salida urlPath-namedPort.

 ©2024 Palo Alto Networks, Inc.

Plantillas de servicio de GKE de muestra

Estas plantillas de muestra demuestran cómo configurar un servicio de GKE para que el cortafuegos VM-Series lo proteja. Para conocer los conceptos básicos sobre la creación de sus propios servicios de clúster, consulte Creación de un clúster privado.

- Uso de las plantillas de servicio de GKE de muestra
- gke_cluster_role.yaml
- gke_cluster_role_binding.yaml
- web-deployment.yaml
- web-service.yaml
- web-deployment-v2.yaml
- web-service-v2.yaml
- Varios puertos en un servicio

Uso de las plantillas de servicio de GKE de muestra

Puede crear una plantilla de servicio basada en el contenido de muestra en los archivos `.yaml` que siguen. Normalmente se crea un único archivo `.yaml`.

Para estar protegido por el cortafuegos VM-Series, los servicios en el clúster deben etiquetarse como "panw-named-port = <named_port>" como se muestra en web-service.yaml o web-service-v2.yaml.

1. Implemente un archivo `.yaml` de la siguiente forma:

   ```
   kubectl apply -f [FILE_NAME].yaml
   ```

2. Configure la implementación de la VPC.
   - En una implementación de VPC compartida, inicie el clúster de GKE en la VPC compartida como se describe en Configuración de la VPC compartida.
   - En una implementación de VPC emparejada, empareje la VPC del clúster de GKE con la red Trust del proyecto host. Consulte Configuración de una VPC emparejada.

Después de una implementación, puede eliminar todos los servicios implementados en el archivo `.yaml` de la plantilla de servicio de la siguiente manera:

```
kubectl delete -f [FILE_NAME].yaml
```

gke_cluster_role.yaml

```
apiVersion: rbac.authorization.k8s.io/v1beta1 tipo: ClusterRole
 metadata:   name: gke-plugin-role rules:   - apiGroups:       - ""
     resources:       - services     verbs:       - list
```

gke_cluster_role_binding.yaml

```
tipo: ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/
v1beta1 metadata:   name: gke-plugin-role-binding subjects:   - kind:
 ServiceAccount     name: hj-gke-891ca3-cluster1-sa     namespace:
```

 ©2024 Palo Alto Networks, Inc.

```
 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:
   # the port that this service should serve on   - name: port1
     port: 80     protocol: TCP     targetPort: 8080   selector:
     run: web   type: LoadBalancer
```

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
```

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:     # the port that this service
 should serve on     - name: port2       port: 81       protocol:
 TCP       targetPort: 8080     selector:       run: web2     type:
 LoadBalancer
```

Varios puertos en un servicio

Para varios puertos en un servicio, edite las etiquetas y asigne el nombre y el número del puerto de destino en el formato panw-named-port-<*service-spec-port-name*>, como se muestra en el ejemplo a continuación.

```
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:   # the port that this service should serve on   - name:
```

 ©2024 Palo Alto Networks, Inc.

```
carts-http     protocol: TCP     port: 80     targetPort: 80   -
name: carts-https     protocol: TCP     port: 443     targetPort:
443   selector:     name: carts
```

 ©2024 Palo Alto Networks, Inc.

Configurar HA activa/pasiva en Google Cloud Platform

Puede configurar un par de cortafuegos VM-Series alojados en Google Cloud Platform (GCP) en una configuración de alta disponibilidad (HA) activa/pasiva. Para HA en GCP, debe implementar ambos pares de HA de cortafuegos dentro del mismo grupo de recursos y debe instalar la misma versión del Complemento VM-Series en ambos pares de HA.

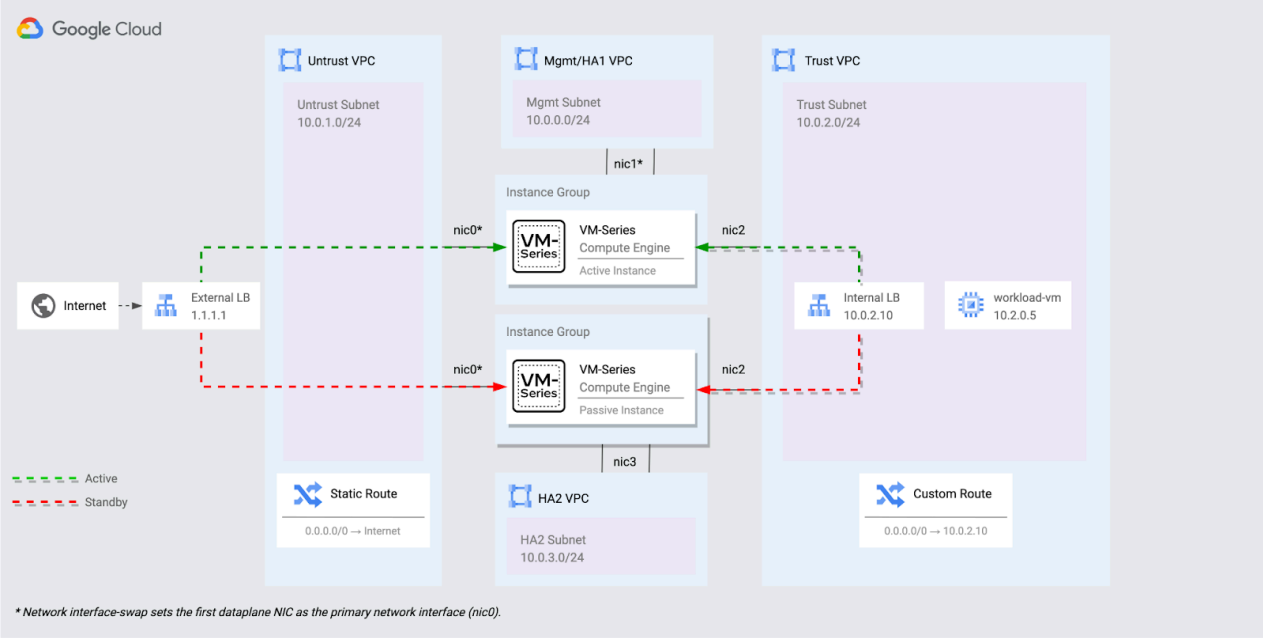
La implementación de un par de cortafuegos VM-Series de alta disponibilidad activo/pasivo alojados en GCP proporciona beneficios como:

- Sincronización en toda la configuración de Palo Alto Networks.
- Sincronización de estado entre instancias para mantener el estado en caso de conmutación por error.
- Conmutación por error de HA controlada en aproximadamente 3 segundos.

Arquitectura de alta disponibilidad activa/pasiva en GCP

La arquitectura es muy similar a la arquitectura tradicional del Balanceador de carga (LB) recomendada para GCP, en la que los puntos del LB externos gestionan el tráfico de no confianza y un LB interno gestiona el tráfico de confianza/salida o de este-oeste.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

Los cortafuegos VM-Series se implementan como un par activo-pasivo y la interfaz HA2 está dedicada a la interfaz HA2 del cortafuegos VM-Series en NIC 3.

La configuración de alta disponibilidad en GCP admite el seguimiento de conexiones, que realiza un seguimiento de la conexión entre un servidor cliente externo a través del LB externo hasta el backend del cortafuegos. Durante una conmutación por error del cortafuegos, los LB transfieren las conexiones al cortafuegos secundario (que ahora se activa) sin interrupciones.

Los LB internos (grupo de backend) se establecen en activo-activo, pero el cortafuegos en espera no procesará ningún tráfico. Los LB realizan una comprobación de estado y, si se dan cuenta de que el cortafuegos activo está inactivo y el cortafuegos en espera está activo, ejecutan una comprobación de estado en el nuevo cortafuegos activo. El tráfico ahora se distribuye a través del cortafuegos que ahora se ha activado.

Nota: GCP HA es compatible con el seguimiento de conexiones de interfaz. Sin embargo, en situaciones más allá de las interfaces (como tener reglas en la infraestructura de Google para detener las verificaciones de estado), las verificaciones de estado del LB no se consideran como parte de la transición de alta disponibilidad.

A continuación, se muestran los casos de uso para implementar HA en GCP:

- Terminación IPSec de las VPN de sitio a sitio.
- Aplicaciones heredadas que necesitan visibilidad de la IP del cliente de origen original (sin solución SNAT) para los flujos de tráfico entrante.
- Requisitos para la conmutación por error de la sesión en caso de error del cortafuegos VM-Series.

Implementar el HA activa/pasiva en GCP

Puede utilizar los siguientes procedimientos para gestionar sus perfiles de implementación existentes.

- Preparación para configurar una HA activa/pasiva en GCP
- Implementación de HA activo/pasivo en GCP
- Prueba de la implementación de HA activo/pasivo en GCP
- Incorporación de aplicaciones de Internet
- Eliminación de los recursos

Preparación para configurar una HA activa/pasiva en GCP

STEP 1 | Habilite las API necesarias, genere una clave SSH y duplique el repositorio Github usando:

```
gcloud services enable compute.googleapis.com ssh-keygen -f
 ~/.ssh/vmseries-tutorial -t rsa git clone https://github.com/
PaloAltoNetworks/google-cloud-vmseries-ha-tutorial cd google-cloud-
vmseries-ha-tutorial
```

STEP 2 | Cree un archivo `terraform.tfvars`.

```
cp terraform.tfvars.example terraform.tfvars
```

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Edite el nuevo archivo `terraform.tfvars` y establezca variables para las siguientes variables:

Variable	Description (Descripción)
project_id	Establezca en su proyecto de implementación de Google Cloud.
public_key_path	Establezca para que coincida con la ruta completa que creó anteriormente.
mgmt_allow_ips	Establezca en una lista de rangos IPv4 que pueden acceder a la interfaz de gestión de la serie VM-Series.
prefijo	(Opcional) Si se establece, esta cadena se antepondrá a los recursos creados.
vmseries_image_name	(Opcional) Define la imagen del VM-Series a implementar. Una lista completa de imágenes se puede encontrar aquí.

STEP 4 | (Opcional) Si está usando la imagen BYOL (es decir, `vmseries-flex-byol-*`), la licencia se puede aplicar durante la implementación añadiendo su código de autenticación VM-Series a los `bootstrap_files/authcodes`

STEP 5 | Guarde su archivo `terraform.tfvars`.

Implementación de HA activo/pasivo en GCP

STEP 1 | Inicialice y aplique el plan Terraform.

```
terraform init terraform apply
```

STEP 2 | Introduzca `sí` para iniciar la implementación. Después de crear todos los recursos, Terraform muestra el siguiente mensaje:

```
Aplicación completada. Salidas:
 EXTERNAL_LB_IP = "ssh paloalto@1.1.1.1 -i ~/.ssh/vmseries-
tutorial" EXTERNAL_LB_URL = "https://1.1.1.1" VMSERIES_ACTIVE =
 "https://2.2.2.2" VMSERIES_PASSIVE = "https://3.3.3.3"
```

Toda la infraestructura debería desplegarse y arrancar y configurarse por sí misma. Visite la `external_nat_ip` usando http://x.x.x.x después de unos minutos después de la implementación para encontrar la página web predeterminada de `workload-vm`.

 ©2024 Palo Alto Networks, Inc.

Prueba de la implementación de HA activo/pasivo en GCP

Ahora puede probar la implementación accediendo a la `workload-vm` que reside en la red VPC de confianza. Todo el tráfico de `workload-vm` se enruta directamente a través del par de HA de VM-Series.

STEP 1 | Utilice la salida `EXTERNAL_LB_URL` para acceder al servicio web en el `workload-vm` a través del cortafuegos VM-Series.

```
gcloud compute ssh workload-vm
```

STEP 2 | Utilice la salida `EXTERNAL_LB_SSH` para abrir una sesión SSH a través del VM-series a la `workload-vm`.

```
ssh paloalto@1.1.1.1 -i ~/.ssh/vmseries-tutorial
```

STEP 3 | Ejecute un script precargado en la máquina virtual de carga de trabajo para probar el mecanismo de conmutación por error en los cortafuegos VM-Series.

```
/network-check.sh
```

Observará una salida similar al bloque de código a continuación, donde `x.x.x.x` en la dirección IP es la dirección `EXTERNAL_LB_IP`.

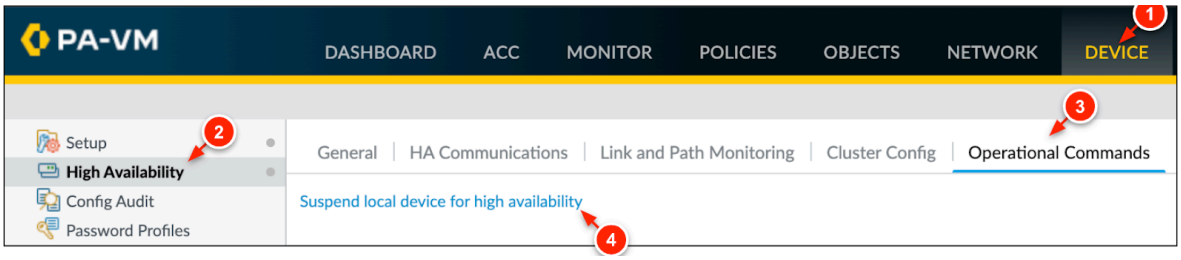
```
Wed Mar 12 16:40:18 UTC 2023 -- Online -- Source IP = x.x.x.x Wed
 Mar 12 16:40:19 UTC 2023 -- Online -- Source IP = x.x.x.x Wed Mar
 12 16:40:20 UTC 2023 -- Online -- Source IP = x.x.x.x Wed Mar 12
 16:40:21 UTC 2023 -- Online -- Source IP = x.x.x.x
```

Inicie sesión en los cortafuegos VM-Series utilizando los valores de salida `VMSERIES_ACTIVE` y `VMSERIES_PASSIVE`. Observe el estado de HA de los cortafuegos en la esquina inferior derecha de la ventana de gestión.

 ©2024 Palo Alto Networks, Inc.

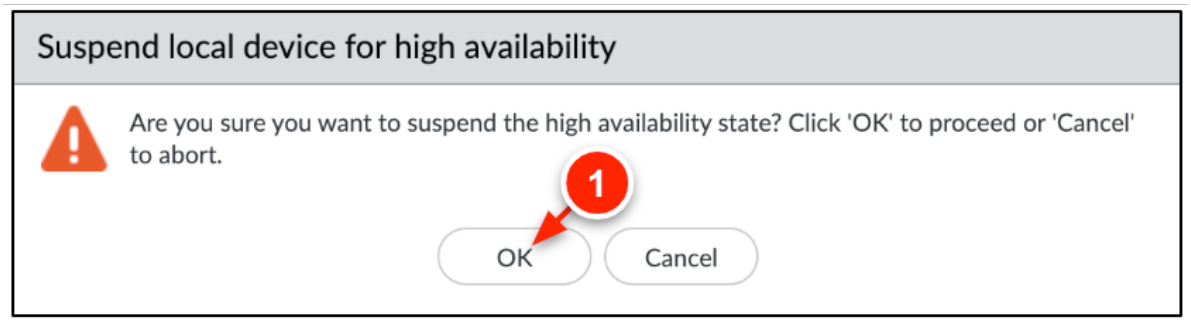
STEP 4 | Realice una conmutación por error iniciada por el usuario.

- En el cortafuegos `Activo`, haga clic en `Dispositivo` > `Alta disponibilidad` > `Comandos operativos`.
- Haga clic en `Suspender dispositivo local para alta disponibilidad.`



- Cuando se le solicite, haga clic en `OK` (Aceptar) para iniciar la conmutación por error.

 ©2024 Palo Alto Networks, Inc.



- Puede notar que la sesión SSH a la `workload-vm` sigue activa. Esto indica que la sesión realizó la conmutación por error correctamente entre los cortafuegos VM-Series. El resultado del script también debe mostrar la misma dirección IP de origen.

```
Wed Mar 12 16:47:18 UTC 2023 -- Online -- Source IP = x.x.x.x Wed
 Mar 12 16:47:19 UTC 2023 -- Online -- Source IP = x.x.x.x Wed
 Mar 12 16:47:21 UTC 2023 -- Offline Wed Mar 12 16:47:22 UTC 2023
 -- Offline Wed Mar 12 16:47:23 UTC 2023 -- Online -- Source IP
 = x.x.x.x Wed Mar 12 16:47:24 UTC 2023 -- Online -- Source IP =
 x.x.x.x
```

Incorporación de aplicaciones de Internet

Puede incorporar y asegurar múltiples aplicaciones orientadas a Internet a través del cortafuegos VM-Series. Esto se hace asignando reglas de reenvío en el balanceador de carga externo a políticas NAT definidas en el cortafuegos VM-Series.

STEP 1 | En Cloud Shell, implemente una máquina virtual en una subred dentro de la red VPC de confianza. La máquina virtual en este ejemplo ejecuta una aplicación de ejemplo para usted.

```
                            gcloud compute instances create my-app2
 \ --network-interface subnet="panw-us-central1-trust",no-address \
 --zone=us-central1-a \ --image-project=panw-gcp-team-testing \ --
image=ubuntu-2004-lts-apache-ac \ --machine-type=f1-micro
```

STEP 2 | Registre la dirección `INTERNAL_IP` de la nueva máquina virtual.

```
                            name: my-app2 ZONE: us-central1-
a MACHINE_TYPE: f1-micro PREEMPTIBLE: INTERNAL_IP: 10.0.2.4
 EXTERNAL_IP: status: RUNNING
```

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Cree una nueva regla de reenvío en el balanceador de carga TCP externo.

```
                        gcloud compute forwarding-rules create
 panw-vmseries-extlb-rule2 \ --load-balancing-scheme=EXTERNAL \ --
region=us-central1 \ --ip-protocol=L3_DEFAULT \ --ports=ALL \ --
backend-service=panw-vmseries-extlb
```

STEP 4 | Recupere y registre la dirección de la nueva regla de reenvío.

```
                        gcloud compute forwarding-rules
 describe panw-vmseries-extlb-rule2 \ --region=us-central1 \ --
format='get(IPAddress)'
```

(resultado)

```
                        34.172.143.223
```

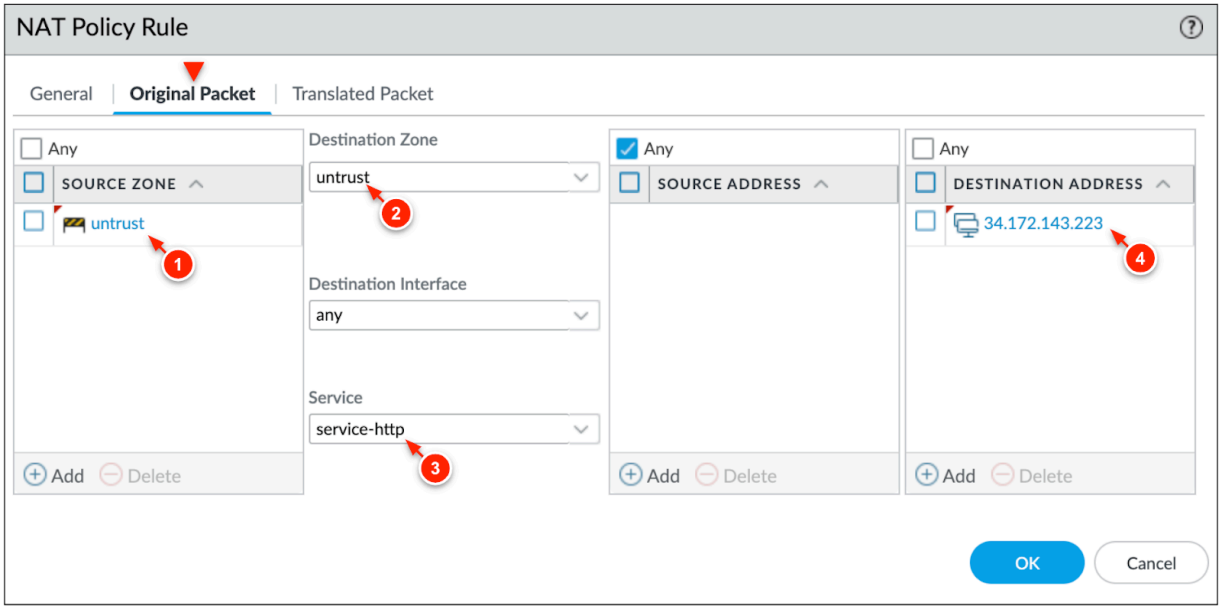
STEP 5 | En el VM-Series activo, haga clic en **Policies (Políticas)** > **NAT** > **Add (Añadir)** e introduzca un nombre para la regla.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Configure el paquete original de la siguiente manera:

- Zona de origen: `untrust`
- Zona de destino: `untrust`
- servicio: `service-http`
- Dirección de destino: Establezca la dirección IP de la regla de reenvío (es decir, 34.172.143.223).

 ©2024 Palo Alto Networks, Inc.

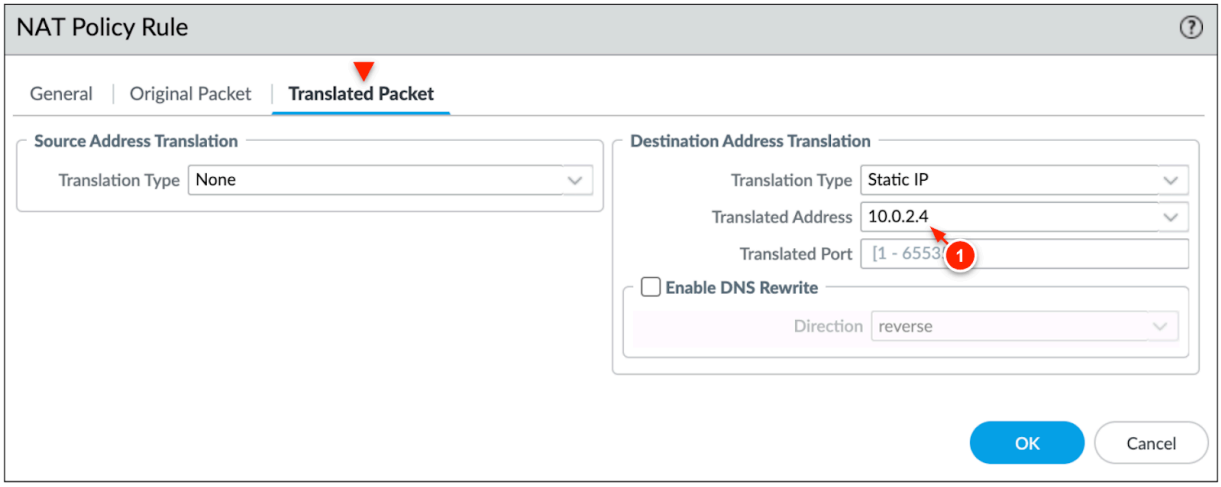


 ©2024 Palo Alto Networks, Inc.

STEP 7 | En la pestaña Paquete traducido, configure la traducción de direcciones de destino de la siguiente manera:

- Tipo traducido: `IP estática`
- Dirección traducida: Establezca en la `IP_INTERNA` de la aplicación de muestra (es decir, 10.0.2.4).

 ©2024 Palo Alto Networks, Inc.

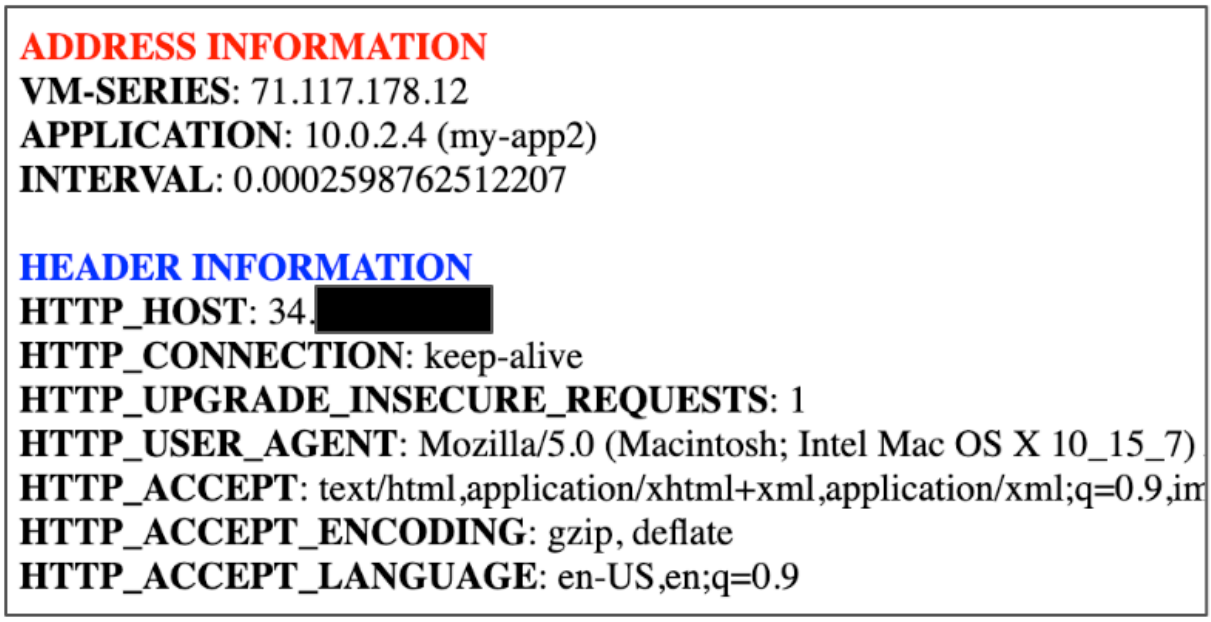


 ©2024 Palo Alto Networks, Inc.

STEP 8 | Haga clic en **OK** (Aceptar) y confirme los cambios.

STEP 9 | Acceda a la aplicación de ejemplo utilizando la dirección de la regla de reenvío.

```
http://34.172.143.223/
```



Eliminación de los recursos

Puede eliminar todos los recursos cuando ya no los necesite.

STEP 1 | (Opcional) Si incorporó una aplicación adicional, elimine la regla de reenvío y la máquina de aplicación de muestra.

```
                          gcloud compute forwarding-rules delete
panw-vmseries-extlb-rule2 \ --region=us-central1 gcloud compute
instances delete my-app2 \ --zone=us-central1-a
```

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Elimine el Terraform usando el comando:

```
terraform destroy
```

STEP 3 | Cuando se le solicite realizar las acciones, introduzca `sí`. Después de eliminar todos los recursos, Terraform muestra el siguiente mensaje:

```
¡Destrucción completa!
```

 ©2024 Palo Alto Networks, Inc.

Configuración de un cortafuegos VM-Series en una red Cisco ENCS

Si ha virtualizado la infraestructura de red basada en dispositivos tradicional en su sucursal u oficina remota con el dispositivo Cisco 5400 Series Enterprise Network Compute System (ENCS), puede utilizar el software de infraestructura Enterprise NFV (NFVIS) para implementar el cortafuegos VM-Series dentro de su red Cisco. El cortafuegos VM-Series sirve como una función de red virtual (VNF) con capacidades de cortafuegos de última generación para habilitar de forma segura todas las aplicaciones y proteger a los usuarios de sucursales u oficinas remotas y a la red de amenazas.

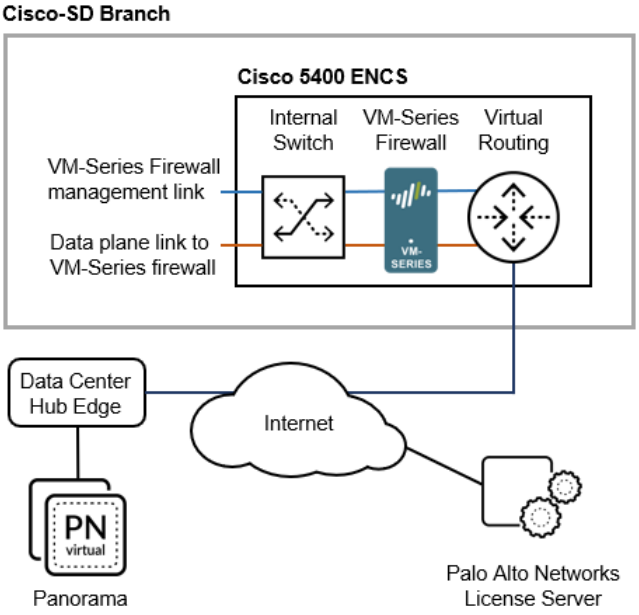
Los dispositivos Cisco Enterprise Network Compute System (ENCS) se combinan con los enrutadores virtuales de servicios integrados de Cisco (ISRV) y el software NFVIS para soportar arquitecturas de red de sucursales (SD-Branch) definidas por software.

- Planificación de su implementación ENCS de Cisco
- Preparación de la imagen del cortafuegos VM-Series para Cisco ENCS
- Implemente el cortafuegos VM-Series en Cisco ENCS

Planificación de su implementación ENCS de Cisco

En su SD-Branch de Cisco, implemente el cortafuegos VM-Series en el dispositivo Cisco ENCS como un VNF que proporciona capacidades de cortafuegos de última generación para proteger sus aplicaciones y usuarios en la sucursal. Puede implementar el cortafuegos en un cable virtual, Capa 2 o Capa 3, y en la configuración de alta disponibilidad.

Para gestionar el cortafuegos VM-Series, el dispositivo Panorama se puede implementar localmente o en la nube. La siguiente topología muestra el cortafuegos VM-Series en el extremos de la sucursal.



Requisitos de Cisco ENCS

Para versiones de NFVIS y plataformas de hardware compatibles, consulte la Matriz de compatibilidad de Palo Alto Networks.

- Configure redes y puentes en NFVIS.
  - Cree NIC virtuales y adjúntelos a un puente virtual para que el dispositivo ENCS pueda dirigir el tráfico a través del cortafuegos VM-Series.

    En el dispositivo Cisco ENCS, el cortafuegos VM-Series admite hasta 8 interfaces de plano de datos.

    Las interfaces de plano de datos del cortafuegos VM-Series en Cisco ENCS solo admiten el modo Virtio; Los modos ENCS SR-IOV y envío PCI no son compatibles.
  - Configure las conexiones de red para el acceso de gestión al cortafuegos VM-Series. Si está utilizando Panorama, asegúrese de que Panorama tenga acceso a la red para gestionar el cortafuegos que implementa.
- Python 2.7. Requerido en su máquina local si está utilizando la línea de comandos para convertir.

Requisitos del cortafuegos VM-Series y Panorama

- Cortafuegos VM-Series: se recomiendan el VM-50 y el VM-100. VM-300, VM-500 y VM-700 también son compatibles, siempre que el hardware ENCS tenga recursos suficientes que se pueden asignar al

 ©2024 Palo Alto Networks, Inc.

cortafuegos VM-Series. Consulte los Requisitos del sistema para VM-Series para asegurarse de que el dispositivo Cisco ENCS tenga los recursos adecuados para soportar el modelo VM-Series que elija.

- Archivo qcow2 (PAN-OS para la imagen base de KVM de VM-Series) para PAN-OS 9.1 o posterior. Consulte Convertir un archivo qcow2 desde la interfaz gráfica de usuario, Paso 2 o Convertir un archivo qcow2 desde la interfaz de línea de comandos, Paso 2.
- La licencia de capacidad del cortafuegos VM-Series y los códigos de autenticación de suscripción que cumplen con sus requisitos. Consulte Tipos de licencia del modelo VM-Series. Introduzca los códigos de autenticación en la interfaz de usuario de NFVIS, o incluya los códigos de autenticación en el archivo de texto **`authcodes`** en la carpeta de conversión como se describe en Convertir un archivo qcow2 desde la interfaz de línea de comandos, Paso 4.
- Con PAN-OS 9.1, el cortafuegos VM-Series en Cisco ENCS es compatible con Virtio con el modo DPDK habilitado de manera predeterminada.

- Dispositivo virtual o hardware de Panorama. Si bien puede implementar un único cortafuegos VM-Series en una red SD-Branch de Cisco, es más común implementar cortafuegos en muchas sucursales y gestionarlas centralmente con Panorama.
  - Panorama versión 9.1 o posterior. La versión debe ser igual o superior a la versión en su cortafuegos VM-Series.
  - Una clave de autenticación VM generado en Panorama. Esta clave permite que el cortafuegos VM-Series se autentique con Panorama.

 ©2024 Palo Alto Networks, Inc.

Preparación de la imagen del cortafuegos VM-Series para Cisco ENCS

Puede convertir un archivo qcow2 de PAN-OS desde la interfaz gráfica de usuario de NFVIS o desde la interfaz de línea de comandos.

- Convertir un archivo qcow2 desde la interfaz gráfica de usuario
- Convertir un archivo qcow2 desde la interfaz de línea de comandos

Convertir un archivo qcow2 desde la interfaz gráfica de usuario

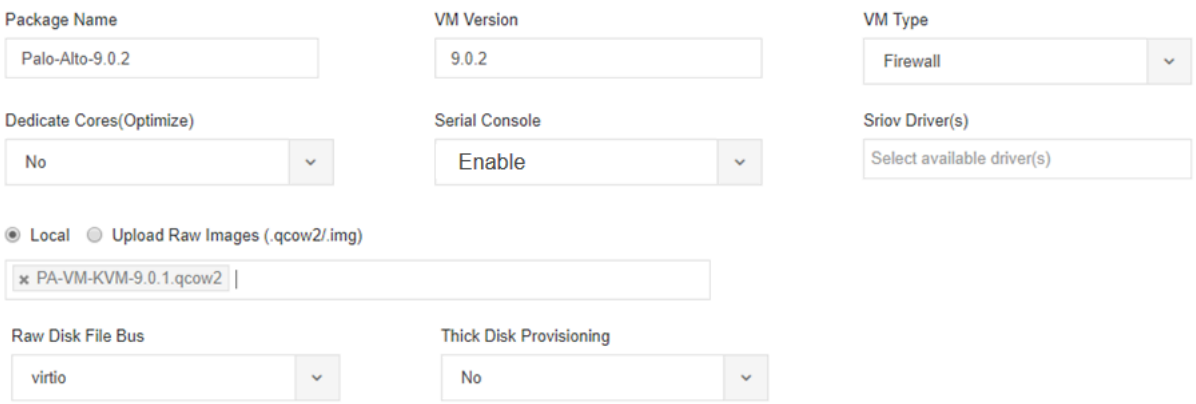
Utilice la interfaz gráfica de usuario de NFVIS para introducir el paquete de imagen y la información de arranque.

STEP 1 | En NFVIS, vaya a **VM Life Cycle (Ciclo de vida de VM)** > **Image Repository (Repositorio de imágenes)** > **Image Packaging (Paquete de imagen)**.

STEP 2 | Complete la información del paquete como se muestra a continuación, proporcionando sus propios valores.

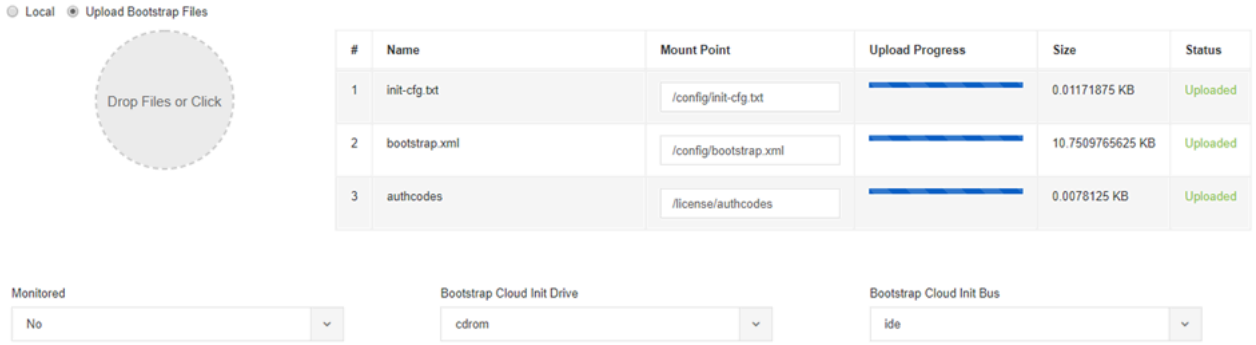
1. Introduzca un **Package Name (Nombre del paquete)** y **VM Version (Versión de VM)**, y para el **VM Type (Tipo de VM)**, seleccione **Firewall (Cortafuegos)**.
2. **Enable (Habilitar)** la **Serial Console (Consola serie)**.
3. Deje el campo **Sriov Driver(s) [Controlador(es) de Sioviov]** en blanco, ya que SR-IOV no es compatible.
4. Seleccione **Local** para elegir un archivo qcow2 que cargó previamente, o haga clic en **Upload Raw Images (Cargar imágenes en bruto)** para cargar un archivo qcow2.
   - Inicie sesión en el Portal de atención al cliente de Palo Alto Networks.

     Si aún no lo ha hecho, cree una cuenta de asistencia técnica y registre el cortafuegos VM-Series.
   - Seleccione **Support (Asistencia técnica)** > **Software Updates (Actualizaciones de software)** y de la lista desplegable **Filter by (Filtrar por)**, seleccione **Pan OS for VM-Series KVM Base Image (Pan OS para imágenes base KVM de VM-Series)**, por ejemplo, la versión 9.1.
   - Descargue la imagen qcow2.

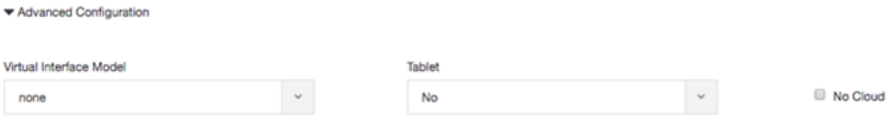


 ©2024 Palo Alto Networks, Inc.

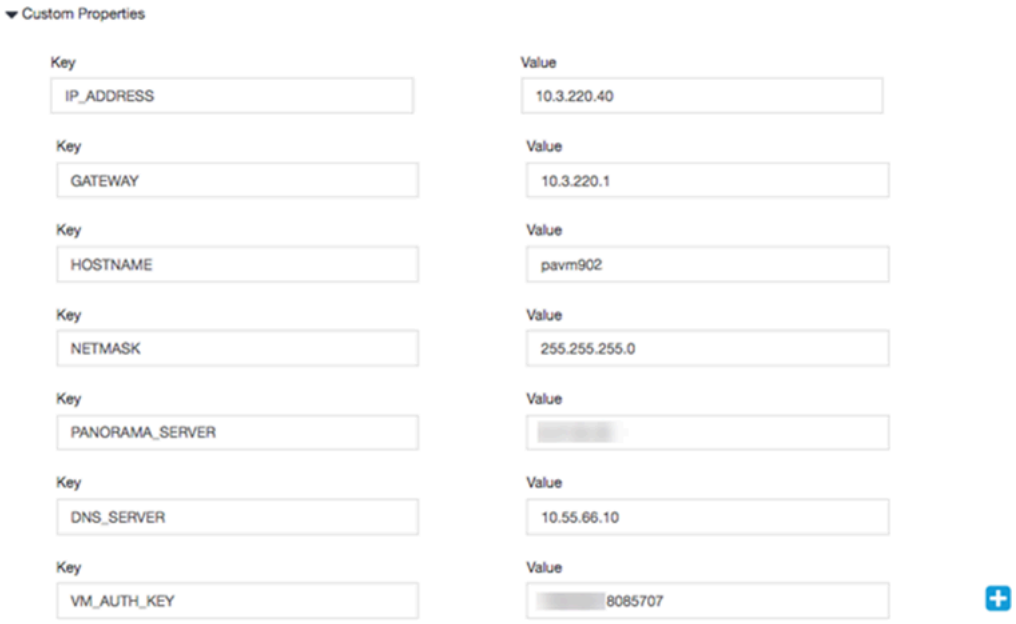
STEP 3 | Cargue los archivos de arranque.



STEP 4 | Seleccione la **Advanced Configuration (Configuración avanzada)**.



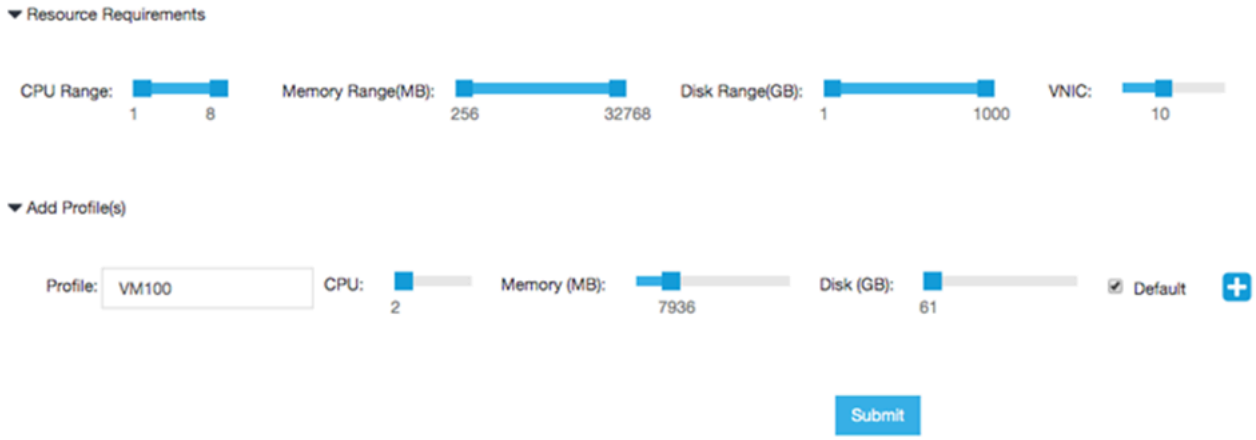
STEP 5 | Introduzca valores para **Custom Properties (Propiedades personalizadas)**.



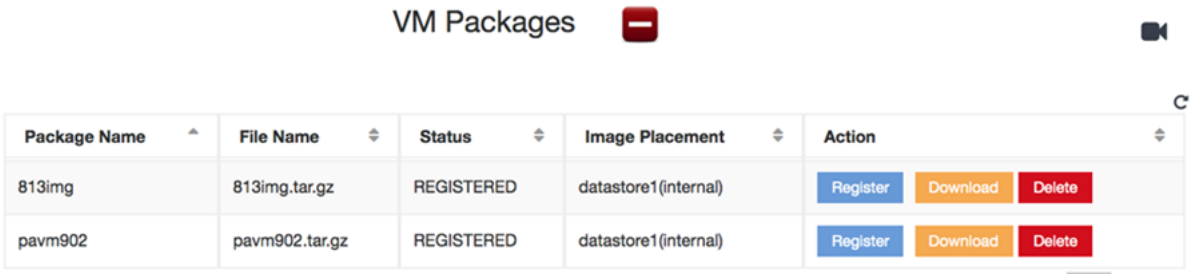
 ©2024 Palo Alto Networks, Inc.

STEP 6 | Establezca valores para sus requisitos de recursos y seleccione el perfil predeterminado, o añada un perfil para la configuración actual.

Haga clic en **Submit (Enviar)** para guardar su paquete.



STEP 7 | Haga clic en **Register (Registrar)** para registrar la nueva imagen.



Convertir un archivo qcow2 desde la interfaz de línea de comandos

Para crear un archivo de arranque desde la interfaz de línea de comandos, cree el archivo `image_properties_template.xml` y a continuación utilice la Utilidad de empaquetado de imágenes VM para crear un archivo `.tar`, que se convierte utilizando el script `nfvpt.py`. El resultado es un archivo `tar.gz` que se puede cargar desde la interfaz de usuario de NFVIS.

STEP 1 | Cree o seleccione una carpeta en su máquina local (la carpeta de conversión) en la que desea descargar y guardar los archivos necesarios para convertir la imagen qcow2 del cortafuegos VM-Series al formato Cisco ENCS.

STEP 2 | Obtenga la imagen qcow2 del cortafuegos VM-Series.

1. Inicie sesión en el Portal de atención al cliente de Palo Alto Networks.

   Si aún no lo ha hecho, cree una cuenta de asistencia técnica y registre el cortafuegos VM-Series.
2. Seleccione **Support (Asistencia técnica)** > **Software Updates (Actualizaciones de software)** y de la lista desplegable **Filter by (Filtrar por)**, seleccione **Pan OS for VM-Series KVM Base Image (Pan OS para imágenes base KVM de VM-Series)**, por ejemplo, la versión 9.1.
3. Descargue la imagen qcow2 a la carpeta de conversión.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Cree el siguiente init-cfg.txt archivo en la carpeta de conversión.

```
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 | Cree un archivo de texto llamado `authcodes` (sin extensión), e introduzca los códigos de autenticación para la capacidad y suscripciones del cortafuegos VM-Series. Guarde el archivo en la carpeta de conversión.

STEP 5 | Cree el siguiente archivo `image_properties_template.xml` en la carpeta de conversión y suministre valores para su implementación:

```
<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>
 <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>
```

 ©2024 Palo Alto Networks, Inc.

```
 <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 | Descargue la Utilidad de empaquetado de imágenes.

1. Inicie sesión en la interfaz de usuario de Enterprise NFVIS y seleccione **VM Life Cycle (Ciclo de vida de VM)** > **Image Repository (Repositorio de imágenes)**.
2. Haga clic en la pestaña **Browse Datastore (Explorar almacén de datos)** y vaya a **data (datos)** > **intdatastore** > **uploads (cargas)** > **vmpackagingutility**.
3. Descargue `nfvisvmpackagingtool.tar` a la carpeta de conversión.
4. Descomprima el archivo:

   ```
   tar -xvf nfvisvmpackagingtool.tar
   ```

STEP 7 | En la carpeta de conversión que contiene el qcow2, el `init-config.txt` y el archivo `authcodes`, ejecute el script `nfvpt.py`. Consulte la documentación de la utilidad de empaquetado de imágenes `nfvpt.py`.

El siguiente ejemplo crea el archivo de imagen Palo-Alto-9.1.0 y un perfil VM-100. Las opciones están separadas por espacios (el ejemplo muestra opciones en líneas separadas solo por claridad) y las opciones personalizadas son pares de clave-valor con un separador de dos puntos.

```
./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 | Cargue la imagen convertida.

1. En la interfaz de usuario de NFVIS, seleccione **VM Life Cycle (Ciclo de vida de VM)** > **Image Repository (Repositorio de imágenes)** y haga clic en el icono azul de Imágenes para mostrar el círculo **Drop Files or Click (Soltar archivos o hacer clic)**.
2. Arrastre el archivo convertido al círculo, o haga clic para explorar y seleccionar su archivo.
3. En la columna Estado, haga clic en **Start (Iniciar)**.

   Cuando se completa la carga, la imagen se registra y el archivo que cargó se muestra en la pestaña **Image Registration (Registro de imagen)** de la lista **Images (Imágenes)**.

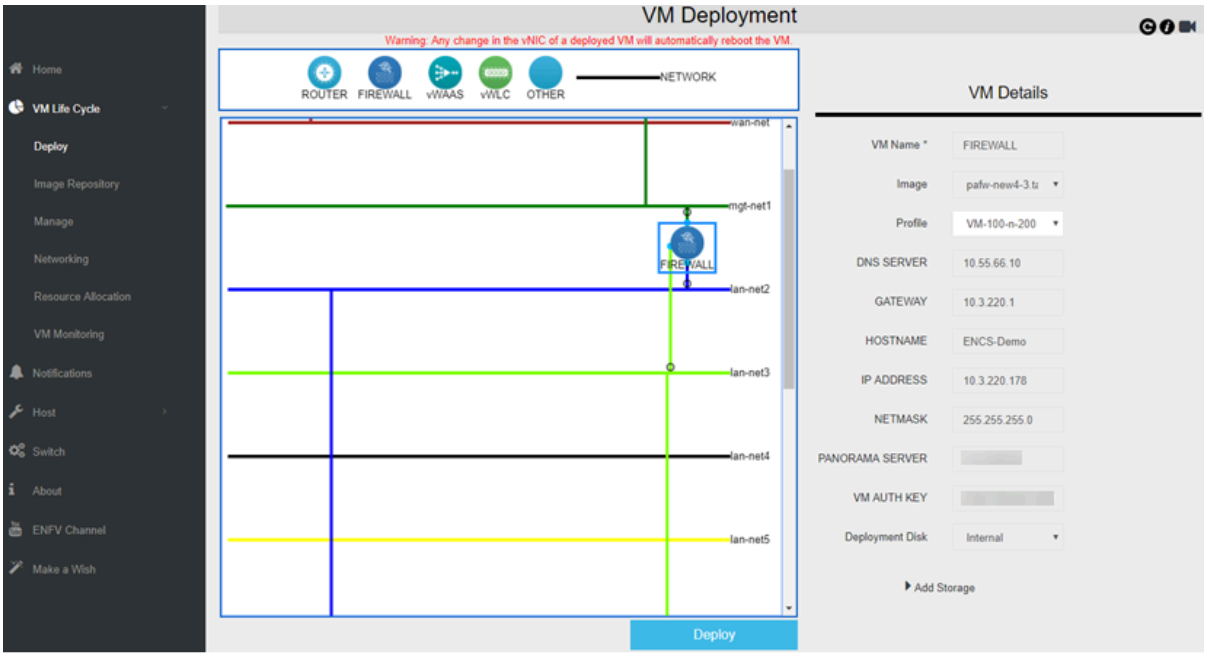
 ©2024 Palo Alto Networks, Inc.

Implemente el cortafuegos VM-Series en Cisco ENCS

Antes de comenzar a implementar el cortafuegos, asegúrese de haber creado conexiones de red para el acceso de gestión al cortafuegos VM-Series. Si está utilizando Panorama, asegúrese de que Panorama tenga conectividad de gestión con el cortafuegos.

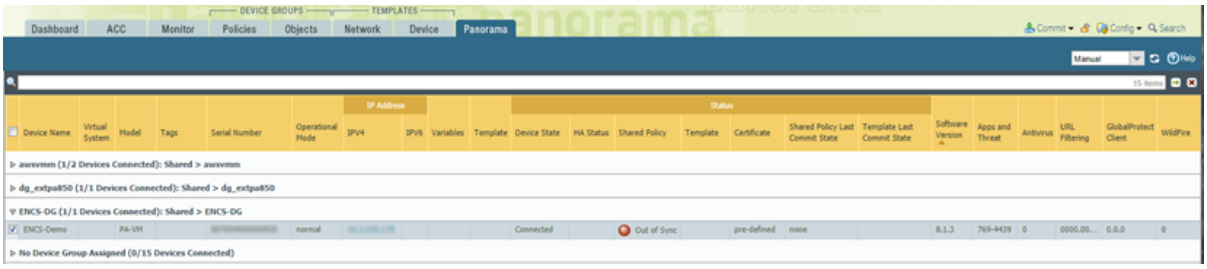
STEP 1 | Implemente el cortafuegos VM-Series.

1. En Enterprise NFVIS, haga clic en **VM Life Cycle (Ciclo de vida de VM)** > **Deploy (Implementar)**.
2. Arrastre el icono del cortafuegos a la red apropiada. En este ejemplo, el cortafuegos se conecta a una red de gestión y una red LAN.



3. Hay que **Deploy (Implementar)** el cortafuegos VM-Series..

   Si está utilizando Panorama para gestionar el cortafuegos, el cortafuegos se muestra como **Connected (Conectado)** en **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**. Si el cortafuegos no está conectado a Panorama, verifique que haya proporcionado la dirección IP de Panorama correcta y que los dispositivos puedan comunicarse a través de la red.

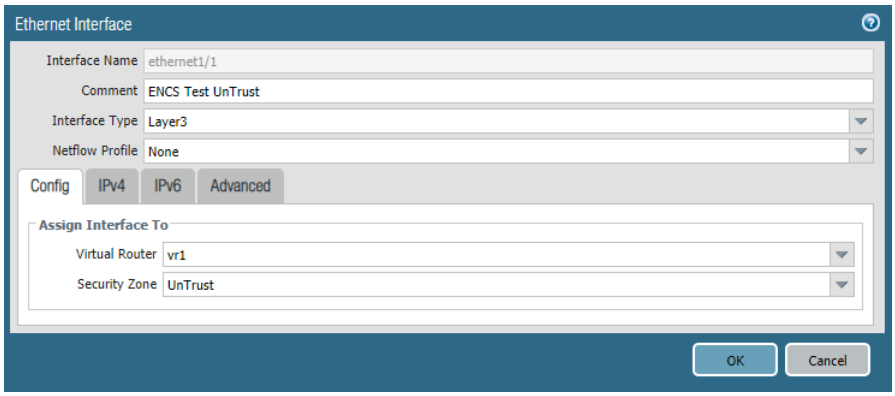


 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configure las interfaces de plano de datos del cortafuegos VM-Series.

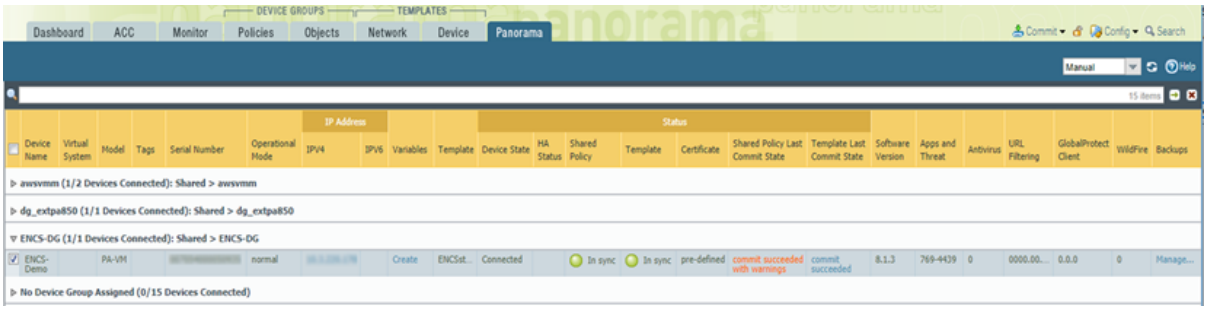
Consulte configurar una interfaz de capa 3, configurar una interfaz de capa 2o configurar cables virtuales. Si usa Panorama, los siguientes pasos le muestran cómo configurar el cortafuegos para una implementación de Capa 3.

1. Añada una plantilla y asigne el cortafuegos a la plantilla.
2. Seleccione la **Network (Red)** y, en la lista desplegable Template (Plantilla) seleccione la plantilla que había creado.
3. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
4. Haga clic en **ethernet 1/1** y configúrelo del siguiente modo:
   - Establezca **Interface Type (Tipo de interfaz)** en **Layer3 (Capa 3)**.
   - En la pestaña **Config (Configurar)**, asigne la interfaz el enrutador predeterminado.
   - También en la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. Defina una zona nueva denominada **`UnTrust`**, por ejemplo, y haga clic en **OK (Aceptar)**.
   - En la pestaña **IPv4**, seleccione **DHCP Client (Cliente DHCP)** o **Static (Estático)**. Si selecciona estático, introduzca la dirección IP.



5. Repita b-e para cada interfaz de red.
6. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** para confirmar todos los cambios de configuración en Panorama y los cortafuegos gestionados.

   Verifique que el estado del enlace para las interfaces del cortafuegos esté activo.

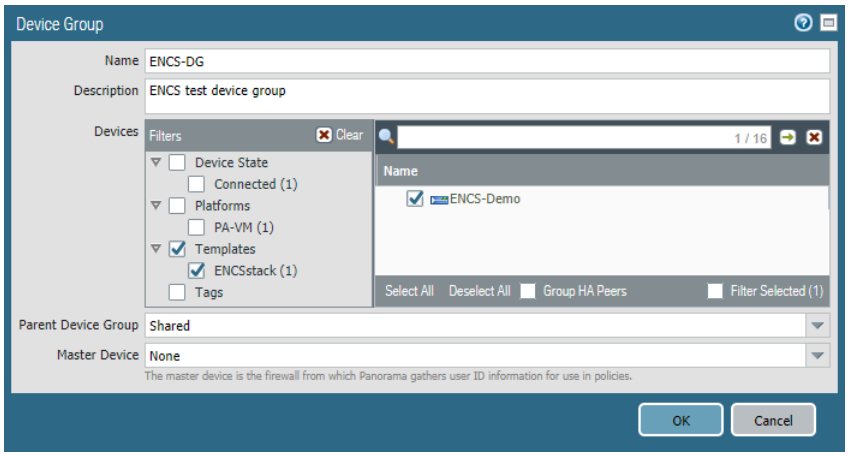


 ©2024 Palo Alto Networks, Inc.

STEP 3 | Configure políticas de seguridad para habilitar de forma segura aplicaciones y usuarios en su red.

Si usa Panorama, los siguientes pasos le muestran cómo usar grupos de dispositivos para gestionar de manera centralizada las reglas de políticas para sus cortafuegos gestionados.

1. Añada un grupo de dispositivos y asigne los cortafuegos gestionados a su grupo de dispositivos.



2. Configure las políticas de seguridad para el grupo de dispositivos.

STEP 4 | Compruebe que el cortafuegos VM-Series está protegiendo el tráfico en su red.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en Oracle Cloud Infrastructure

Implemente el cortafuegos VM-Series en la nube de Oracle Cloud Infrastructure (OCI). Con VM-Series en OCI, puede proteger y segmentar sus cargas de trabajo, prevenir amenazas avanzadas y mejorar la visibilidad de sus aplicaciones a medida que se traslada a la nube.

OCI es un servicio de computación en la nube pública que le permite ejecutar sus aplicaciones en un entorno hospedado de alta disponibilidad ofrecido por Oracle. Puede implementar el cortafuegos VM-Series para asegurar sus aplicaciones y servicios que ejecutan su entorno OCI.

- Tipos de formas OCI
- Implementaciones compatibles con OCI
- Preparación para la configuración del cortafuegos VM-Series en OCI
- Implementación del cortafuegos VM-Series desde Oracle Cloud Marketplace
- Configuración de la HA activa/pasiva en OCI

Tipos de formas OCI

Los cortafuegos VM-Series admiten las siguientes formas de OCI VM. Consulte la documentación de Oracle Cloud Infrastructure para más información sobre formas de VM.

Modelo VM-Series	Forma mínima de OCI
• VM-100 • VM-Series basada en créditos NFGW de software	VM.Standard2.4
• VM-300 • VM-Series basada en créditos NFGW de software	VM.Standard2.4
• VM-500 • VM-Series basada en créditos NFGW de software	VM.Standard2.8
• VM-700 • VM-Series basada en créditos NFGW de software	VM.Standard2.16
• VM-100, VM-300, VM-500 y VM-700 • VM-Series basada en créditos NFGW de software	VM.Optimized3.Flex VM.Standard3.Flex

Puede implementar el cortafuegos VM-Series en una instancia de OCI con más recursos que el mínimo Requisitos del sistema para VM-Series. Si elige un tamaño de forma más grande para el modelo de cortafuegos VM-Series. Aunque el cortafuegos solo usa el máximo de núcleos de vCPU y la memoria que figuran en la página de requisitos del sistema, aprovecha el rendimiento de red más rápido que proporciona la forma más grande.

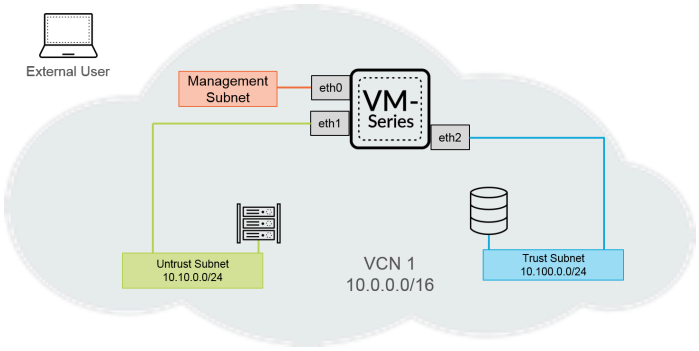
 ©2024 Palo Alto Networks, Inc.

Implementaciones compatibles con OCI

Utilice el cortafuegos VM-Series en OCI para proteger su entorno de nube en las siguientes situaciones:

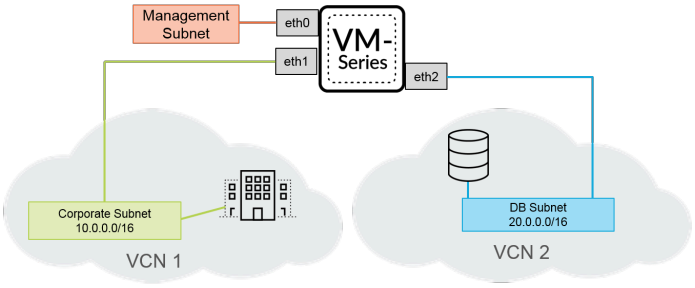
- Tráfico norte-Sur: puede usar el cortafuegos VM-Series para asegurar el tráfico que ingresa a su red en la nube desde una fuente no fiable o que sale de su red en la nube para llegar a una fuente no fiable. Para cualquier tipo de tráfico, debe configurar las reglas de la tabla de rutas en su Red de nube virtual (VCN) y las reglas de política NAT en el cortafuegos.

  En este ejemplo, el tráfico saliente está saliendo de la subred fiable en su VCN. Debe configurar la política de traducción de la dirección de origen en una dirección IP pública y una regla de tabla de ruta que redireccione ese tráfico al cortafuegos. La regla de ruta dirige el tráfico saliente a la interfaz del cortafuegos en la subred fiable de la VCN. Cuando el cortafuegos recibe este tráfico, realiza la traducción de la dirección de origen en el tráfico y aplica cualquier otra política de seguridad que se haya configurado.



- Tráfico Inter-VCN (este-oeste): el cortafuegos VM-Series le permite asegurar el tráfico que se mueve dentro de su entorno de nube entre las Redes de nube virtual (VCN). Cada subred debe pertenecer a una VCN diferente porque, de forma predeterminada, no se utilizan reglas de ruta para habilitar el tráfico dentro de una VCN. En este escenario, configure una interfaz en el cortafuegos conectado a una subred en cada VCN.

  En el ejemplo a continuación, un usuario en la subred Trust desea acceder a los datos en la subred DB. Configure una ruta en OCI que llegue al siguiente salto de DB de CIDR de subred, que apunta a la red de la subred Trust de la interfaz en el cortafuegos VM-Series.



Para obtener más información, consulte Cargas de trabajo seguras con el cortafuegos VM-Series de Palo Alto Networks utilizando una Red flexible.

 ©2024 Palo Alto Networks, Inc.

Preparación para la configuración del cortafuegos VM-Series en OCI

El proceso para implementar el cortafuegos VM-Series en Oracle Cloud Infrastructure requiere la finalización de las tareas de preparación.

- Redes virtuales en la nube
- Claves SSH
- Datos de usuario de la configuración inicial

Redes virtuales en la nube

Una red virtual en la nube (VCN) es una red privada virtual que configura en su entorno OCI. Para implementar el cortafuegos VM-Series en OCI, su VCN debe tener al menos tres tarjetas de interfaz de red virtual (VNIC) para la interfaz de gestión y dos interfaces de datos.

OCI utiliza una serie de tablas de rutas para enviar tráfico desde su VCN y se añade una tabla de rutas a cada subred. Una subred es una división de su VCN. Si no especifica una tabla de ruta, la subred usa la tabla de ruta predeterminada de VCN. Cada regla de tabla de ruta especifica un bloque CIDR de destino y un próximo salto (destino) para cualquier tráfico que coincida con el CIDR. OCI solo usa la tabla de rutas de una subred si la dirección IP de destino está fuera del bloque CIDR especificado por la VCN; las reglas de ruta no son necesarias para habilitar el tráfico dentro de VCN. Y, si el tráfico tiene reglas superpuestas, OCI usa la regla más específica en la tabla de rutas para enrutar el tráfico.

Si no hay una regla de ruta que coincida con el tráfico que está intentando abandonar VCN, el tráfico se descarta.

Cada subred requiere una tabla de rutas y una vez que ha añadido una tabla de rutas a una subred, no puede cambiarla. Sin embargo, puede añadir, eliminar o editar reglas en una tabla de ruta después de que se haya creado.

Claves SSH

Debe crear un par de claves SSH para iniciar sesión en el cortafuegos por primera vez. No puede usar el nombre de usuario y contraseña predeterminados para acceder al cortafuegos por primera vez. Después de que el cortafuegos se inicie por primera vez, debe acceder al cortafuegos a través de la CLI y crear un nuevo nombre de usuario y contraseña.

1. Cree un par de claves SSH y almacene el par de claves SSH en la ubicación predeterminada para su sistema operativo.
   - En Linux o MacOS, utilice `ssh-keygen` para crear el par de claves en su directorio .ssh.
   - En Windows, use PuTTYgen para crear el par de claves.

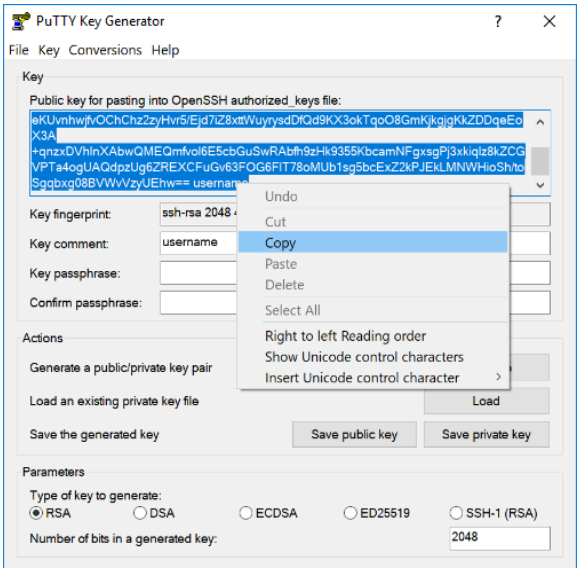
     El contenido en el campo **Key comment (Comentario sobre la clave)** no es relevante para el cortafuegos VM-Series; puede aceptar el valor predeterminado (la fecha de creación de la clave) o introducir un comentario que ayude a recordar el nombre del par de claves. Use el botón **Save private key (Guardar clave privada)** para almacenar la clave privada en su directorio .ssh.

 ©2024 Palo Alto Networks, Inc.

2. Seleccione la clave pública completa.
   - Linux o MacOS

     : abra la clave pública en un editor de texto y copie la clave pública.
   - Windows: Debe usar el generador de claves de PuTTY para ver la clave pública. Inicie PuTTYgen, haga clic en Load (Cargar) y busque la clave privada que guardó en su directorio .ssh.

     En PuTTYgen, desplácese hacia abajo para asegurarse de seleccionar la clave completa, haga clic derecho y seleccione Copy (Copiar).



Datos de usuario de la configuración inicial

Debe proporcionar los siguientes parámetros de arranque al configurar la instancia del cortafuegos VM-Series. OCI utiliza esta información para realizar la configuración inicial del cortafuegos, que proporciona al cortafuegos un nombre de host y una licencia y conecta el cortafuegos a Panorama, si corresponde.

El parámetro ***Códigos de autenticación*** *solo es necesario si el cortafuegos VM-Series puede conectarse a los servidores de licencias de Palo Alto Networks.*

Los campos relacionados con Panorama son obligatorios solo si tiene un dispositivo Panorama y desea usar Panorama para gestionar su cortafuegos VM-Series.

Campo	Description (Descripción)
hostname=	Nombre de host para el cortafuegos.
vm-auth-key=	Clave de autenticación de máquina virtual para registrar el cortafuegos con Panorama.
panorama-server=	Dirección IPv4 o IPv6 del servidor Panorama principal. Este campo no es obligatorio, pero se recomienda para gestionar de forma centralizada sus cortafuegos.

 ©2024 Palo Alto Networks, Inc.

Campo	Description (Descripción)
panorama-server-2=	Dirección IPv4 o IPv6 del servidor Panorama secundario. Este campo no es obligatorio, sino recomendado.
tplname=	Nombre de la pila de plantillas de Panorama. Si añade una dirección IP del servidor de Panorama, se recomienda asignar al cortafuegos a una pila de plantillas en Panorama e introducir el nombre de la pila de plantillas en este campo de modo que pueda gestionar y enviar ajustes de configuración al cortafuegos de forma centralizada.
dgname=	Nombre de grupo de dispositivos de Panorama. Si añade una dirección IP del servidor de Panorama, recomienda crear un grupo de dispositivos en Panorama e introducir el nombre del grupo de dispositivos en este campo para que pueda agrupar los cortafuegos de forma lógica y enviar las reglas de la política al cortafuegos.
authcodes=	Se utiliza para licenciar el cortafuegos VM-Series con el servidor de licencias de Palo Alto Networks.
op-command-modes=jumbo-frame	Se utiliza para habilitar el modo de trama gigante en el cortafuegos VM-Series. Debido a que OCI implementa instancias de VM en modo de trama gigante de manera predeterminada, se recomienda que inicie el cortafuegos VM-Series en modo jumbo para obtener el mejor rendimiento.

Pegue los parámetros de arranque en la consola de OCI con el siguiente formato.

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

 ©2024 Palo Alto Networks, Inc.

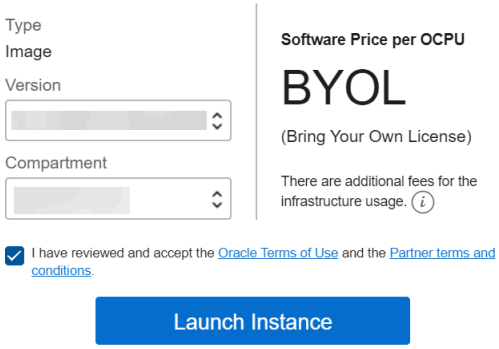
Implementación del cortafuegos VM-Series desde Oracle Cloud Marketplace

Complete el siguiente procedimiento para implementar el cortafuegos VM-Series en OCI desde Oracle Cloud Marketplace.

STEP 1 | Inicie sesión en Oracle Cloud Marketplace.

STEP 2 | Encuentre la aplicación del cortafuegos VM-Series en el Oracle Cloud Marketplace.

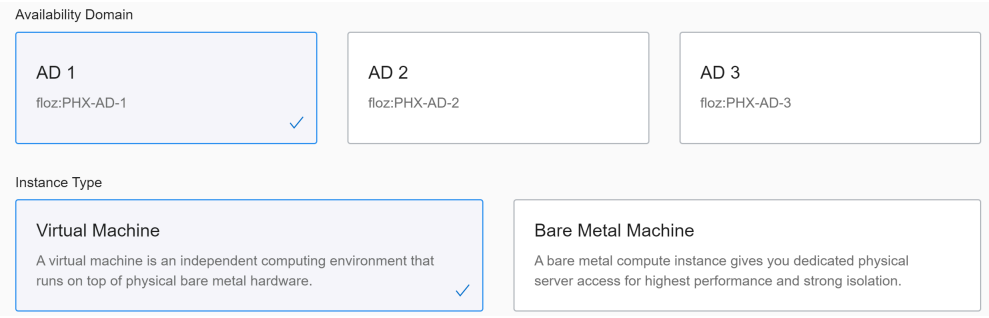
1. Busque Palo Alto Networks y aparecerá una lista de ofertas para el cortafuegos VM-Series.
2. Selecciona una oferta.
3. Haga clic en **Obtener aplicación**.
4. Seleccione su **Región** y haga clic en **Iniciar sesión**.
5. Seleccione la **Versión** y **Compartimento**.
6. Acepte los términos de Oracle and Partner.
7. Haga clic en **Iniciar instancia**.



STEP 3 | Introduzca un **Name (Nombre)** descriptivo para el cortafuegos VM-Series.

STEP 4 | Seleccione un **Availability Domain (Dominio de disponibilidad)**.

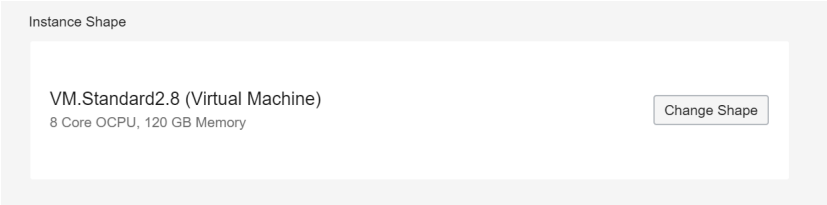
STEP 5 | Seleccione **Virtual Machine (Máquina virtual)** en **Shape Type (Tipo de forma)**.



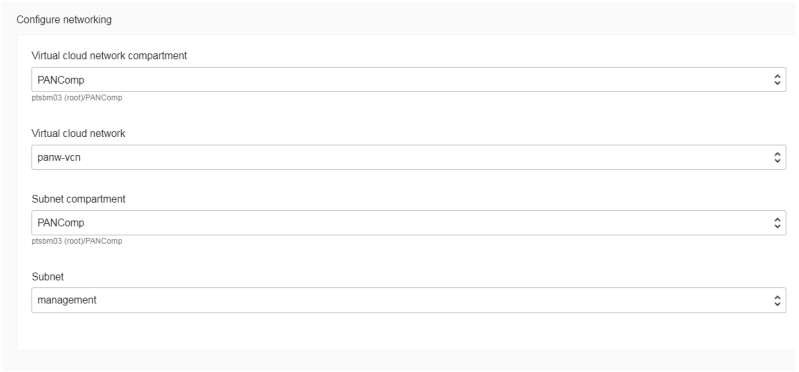
STEP 6 | Seleccione la forma con el número de CPU, la cantidad de RAM y los números de interfaces necesarias para el modelo de cortafuegos VM-Series. Consulte la página Formas de cálculo para la cantidad de recursos proporcionados por las diferentes formas de cálculo. Consulte Requisitos

 ©2024 Palo Alto Networks, Inc.

del sistema para VM-Series para obtener más información sobre los recursos necesarios para cada modelo de los cortafuegos VM-Series.



STEP 7 | En Redes, seleccione su **Virtual cloud network compartment (Compartimiento de red de nube virtual)**, **Virtual cloud network (Red de nube virtual)**, **Subnet compartment (Compartimento de subred)** y **Subnet (Subred)** para su interfaz de gestión. Solo puede añadir una interfaz al crear la instancia de cortafuegos VM-Series. Podrá añadir interfaces adicionales más adelante.

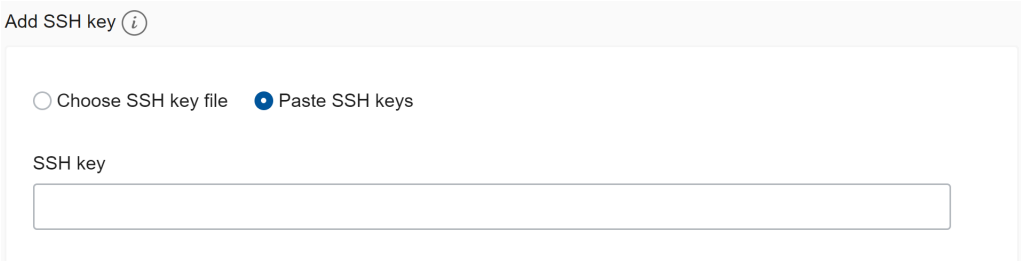


STEP 8 | (Opcional) Establezca el volumen de arranque en un tamaño mayor que el predeterminado. De forma predeterminada, el volumen de arranque está establecido en 60 GB. Complete este procedimiento si necesita un volumen de arranque más grande para que admita funciones como adjuntar logs.

1. Seleccione **Tamaño de volumen de arranque personalizado (en GB)**.
2. Introduzca 60 o más. 60 GB es el tamaño mínimo de disco duro requerido por el cortafuegos VM-Series.

STEP 9 | Añada su clave SSH.

1. En **Añadir clave SSH**, seleccione **Pegar clave SSH**.
2. Pegue su clave SSH en el campo provisto.



 ©2024 Palo Alto Networks, Inc.

STEP 10 | Añada los parámetros de arranque.

1. Haga clic en **Mostrar opciones avanzadas**.
2. En **Datos de usuario**, seleccione **Pegar script de inicio en la nube**.
3. Pegue los parámetros de arranque en el campo provisto.

   hostname=<*fw-hostname*>

   vm-auth-key=<*auth-key*>

   panorama-server=<*panorama-ip*>

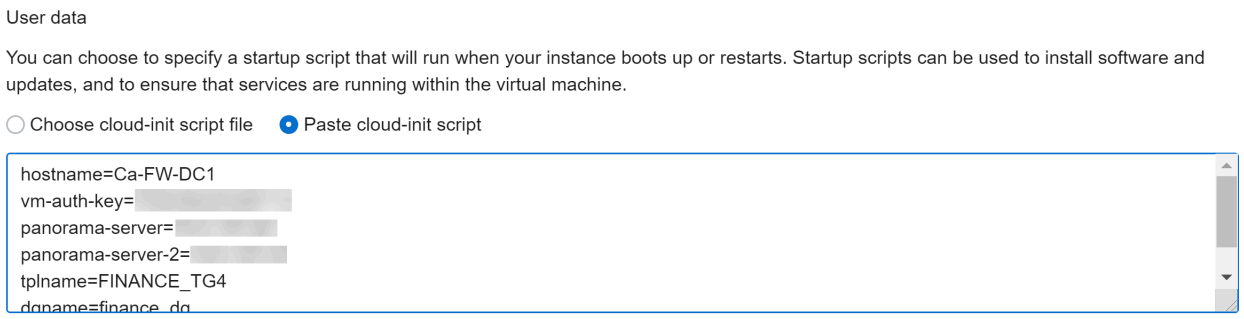
   panorama-server-2=<*panorama2-ip*>

   tplname=<*template-stack-name*>

   dgname=<*device-group-name*>

   authcodes=<*firewall-authcode*>

   op-command-modes=jumbo-frame



STEP 11 | Haga clic en **Create (Crear)**.

Cuando se inicia el cortafuegos VM-Series, OCI crea y conecta una VNIC primaria a la instancia. Esta VNIC reside en la subred que especificó en la configuración de red de la instancia y se conecta a la interfaz de gestión del cortafuegos VM-Series.

STEP 12 | Configure una nueva contraseña de administración para el cortafuegos.

1. Use la dirección IP de gestión para hacer SSH en la interfaz de línea de comando (CLI) del cortafuegos VM-Series.
2. Introduzca el siguiente comando para iniciar sesión en el cortafuegos:

   ssh -i <*private_key.pem*> admin@<*public-ip_address*>
3. Configure una nueva contraseña usando el siguiente comando y siga las indicaciones en pantalla:

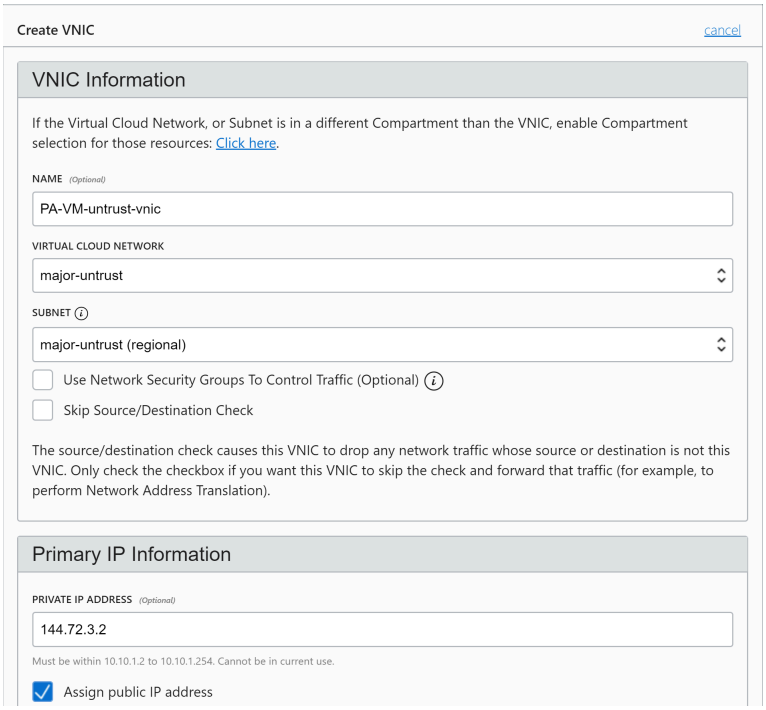
   configure

   set mgt-config users admin password

 ©2024 Palo Alto Networks, Inc.

STEP 13 | Adjunte una vNIC a su instancia de cortafuegos VM-Series para cada interfaz de datos. Debe adjuntar al menos dos interfaces de datos a su instancia de cortafuegos: desconfianza y confianza.

1. Seleccione su instancia de cortafuegos VM-Series recién iniciada y seleccione **Attached VNICs (VNIC adjuntas)** > **Create VNIC (Crear VNIC)**.
2. Introduzca un **Name (Nombre)** descriptivo para su vNIC.
3. Seleccione su VCN en la lista desplegable **Virtual Cloud Network (Red virtual en la nube)**.
4. Seleccione su subred en la lista desplegable **Subnet (Subred)**.
5. Especifique una **Private IP Address (Dirección IP privada)**. Esto solo es necesario si desea elegir una IP particular para el vNIC. Si no especifica una IP, OCI asignará una dirección IP desde el bloque CIDR que asignó a la subred.
6. Seleccione **Assign Public IP Address (Asignar dirección IP pública)** para los vNIC públicos, como su subred untrust.
7. Haga clic en **Create VNIC (Crear VNIC)**.
8. Repita este procedimiento para cada vNIC que requiera su implementación.



 ©2024 Palo Alto Networks, Inc.

STEP 14 | Configure las interfaces de red del plano de datos como interfaces de capa 3 en el cortafuegos.

1. Inicie sesión en el cortafuegos.
2. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
3. Haga clic en el enlace de **ethernet 1/1** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **capa 3**
   - En la pestaña **Config (Configurar)**, asigne la interfaz el enrutador predeterminado.
   - En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. Defina una zona nueva, por ejemplo untrust-zone, y a continuación haga clic en **OK (Aceptar)**.
   - En la pestaña **IPv4**, seleccione **Static (Estática)**.
   - Haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para la interfaz. Asegúrese de que la dirección IP coincide con la dirección IP que ha asignado a la subred correspondiente en VCN. Por ejemplo, si añade esta interfaz a su zona no fiable untrust, asegúrese de asignar la dirección IP de vNIC no fiable configurada en su VCN.
4. Repita este procedimiento para cada vNIC configurada en su VCN, excepto su vNIC de gestión.



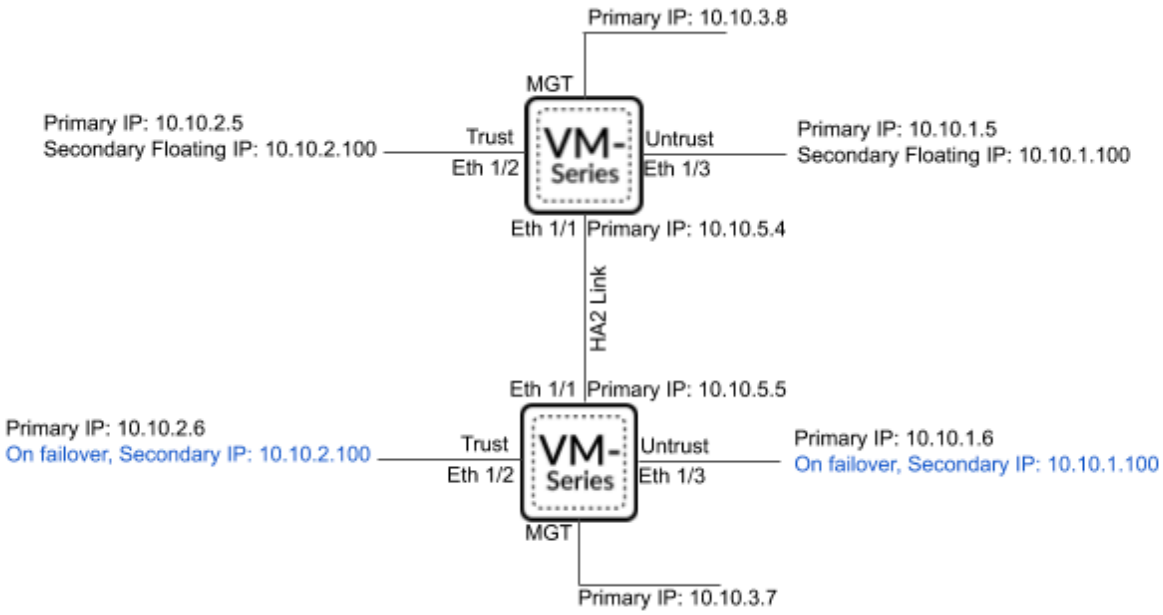
Siempre solo elimine interfaces en la parte inferior de la lista de interfaces. La eliminación de las interfaces del cortafuegos en el orden incorrecto provoca una discrepancia entre la interfaz y la OCI. Por ejemplo, supongamos que tiene cinco interfaces de datos, elimine la interfaz dos en el cortafuegos y añada una nueva interfaz en la parte inferior. Después de reiniciar el cortafuegos, la interfaz recién añadida tomará el lugar de la interfaz dos eliminada en lugar de tomar un lugar en la parte inferior de la lista.

 ©2024 Palo Alto Networks, Inc.

Configuración de la HA activa/pasiva en OCI

Puede configurar un par de cortafuegos VM-Series en OCI en una configuración de alta disponibilidad (HA) activa/pasiva. Para garantizar el tiempo de actividad en una configuración de HA en OCI, debe crear una dirección IP flotante secundaria que pueda moverse rápidamente de un par a otro. Cuando el cortafuegos activo se desactiva, la dirección IP flotante pasa del cortafuegos activo al pasivo, de modo que el cortafuegos pasivo puede proteger el tráfico sin problemas tan pronto como se convierta en el par activo. Además de la dirección IP flotante, los equipos en HA también necesitan Enlaces de HA, un enlace de control (HA1) y un enlace de datos (HA2), para sincronizar los datos y mantener la información de estado.

El cortafuegos VM-Series para OCI en modo FIPS no admite alta disponibilidad.



Para permitir que los cortafuegos muevan la dirección IP flotante tras una conmutación por error, debe colocar las instancias del cortafuegos en un grupo dinámico en OCI. Los grupos dinámicos le permiten agrupar las instancias del cortafuegos como actores principales y crear políticas para permitir que las instancias en el grupo dinámico realicen llamadas API contra los servicios OCI. Utilizará reglas de coincidencia para añadir las instancias de HA del mismo nivel al grupo dinámico y luego creará la política de IP flotante de una VNIC a otra.

Ambos cortafuegos VM-Series en el par de HA deben tener el mismo número de interfaces de red. Cada cortafuegos requiere un mínimo de cuatro interfaces: gestión, untrust, trust y alta disponibilidad (HA). Puede configurar interfaces de datos adicionales según lo requiera su implementación.

- **Interfaz de gestión**: las direcciones IP privada y pública asociadas con la interfaz principal. Puede usar la dirección IP privada en la interfaz de gestión como la dirección IP para la interfaz HA1 entre los pares. Si desea una interfaz de HA dedicada, debe adjuntar una interfaz adicional a cada cortafuegos, para un total de cinco interfaces cada una.

 ©2024 Palo Alto Networks, Inc.

- **Interfaces untrust** y **trust**: cada una de estas interfaces de datos en el par de HA activa requiere una dirección IP primaria y secundaria. Tras una conmutación por error, cuando el par pasivo pasa al estado activo, la dirección IP privada secundaria se separa del par previamente activo y se une al par de HA ahora activo.
- **Interfaz HA2**: esta interfaz tiene una única dirección IP privada en cada par de HA. La interfaz HA2 es el enlace de datos que los pares usan para sincronizar sesiones, reenviar tablas, asociaciones de seguridad IPSec y tablas ARP.

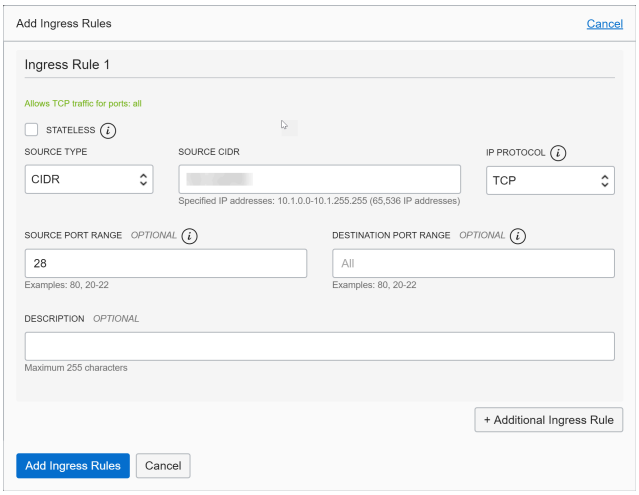
STEP 1 | Implementación del cortafuegos VM-Series desde Oracle Cloud Marketplace y configure las interfaces de red para HA.

1. (Opcional) Configure una interfaz HA1 dedicada en cada par de HA.
   1. Desde la consola OCI, seleccione **Calcular** > **Instancias** y haga clic en el nombre de su instancia de par activa.
   2. Seleccione **VNIC adjuntas** y haga clic en **Crear VNIC**.
   3. Introduzca un nombre descriptivo para su interfaz HA1.
   4. Seleccione el VCN y la subred.
   5. Introduzca una dirección IP privada.
   6. Haga clic en **Create VNIC (Crear VNIC)**.
   7. Repita este proceso en su instancia de par pasiva.
2. Configure una interfaz HA2 en cada par de HA.
   1. Desde la consola OCI, seleccione **Calcular** > **Instancias** y haga clic en el nombre de su instancia de par activa.
   2. Seleccione **VNIC adjuntas** y haga clic en **Crear VNIC**.
   3. Introduzca un nombre descriptivo para su interfaz HA2.
   4. Seleccione el VCN y la subred. La interfaz HA2 debe estar en una subred separada de sus interfaces de datos.
   5. Introduzca una dirección IP privada.
   6. Haga clic en **Create VNIC (Crear VNIC)**.
   7. Repita este proceso en su instancia de par pasiva.
3. Añada una dirección IP secundaria a las interfaces de su plano de datos en el par activo.
   1. Desde la consola OCI, seleccione **Calcular** > **Instancias** y haga clic en el nombre de su instancia de par activa.
   2. Seleccione **VNIC adjuntas** y haga clic en su VNIC de no confianza.
   3. Seleccione **Direcciones IP** y haga clic en **Asignar dirección IP privada**.
   4. Introduzca la dirección IP y haga clic en **Asignar**.
   5. Repita este procedimiento para cada interfaz de plano de datos en su par activo.

 ©2024 Palo Alto Networks, Inc.

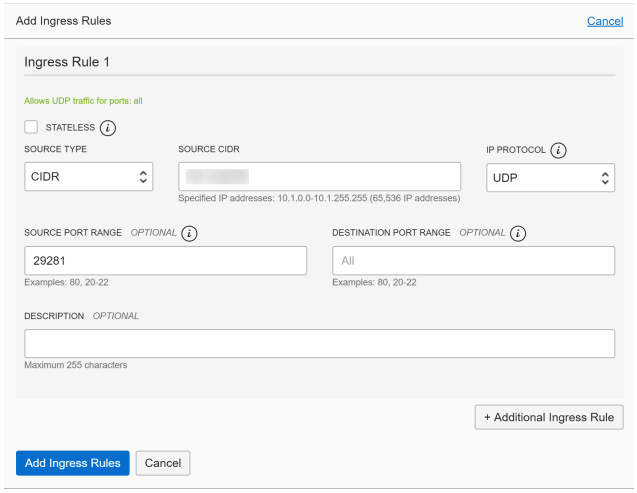
STEP 2 | Cree reglas de seguridad para permitir a los pares de HA sincronizar datos y mantener la información de estado. De manera predeterminada, OCI solo permite el tráfico ICMP. Debe abrir los puertos HA necesarios.

1. Abra los puertos para su interfaz HA1.
   1. Desde la consola OCI, seleccione **Networking (Redes)** > **Virtual Cloud Networks (Redes virtuales en la nube)** y seleccione su VCN.
   2. Seleccione **Subredes** y seleccione la subred que contiene su interfaz HA1.
   3. Seleccione **Listas de seguridad** y haga clic en la lista de seguridad predeterminada para editarla.
   4. Haga clic en **Añadir regla de ingreso**.
   5. Introduzca el **CIDR de fuente** que incluye la dirección IP del puerto del par HA1 de HA.
   6. Seleccione **TCP** del menú desplegable **protocolo IP**.
   7. Haga clic en **+Regla de entrada adicional**. Debe crear dos reglas adicionales para los puertos TCP 28260 y 28769.
   8. Si el cifrado está habilitado en su cortafuegos VM-Series para el enlace HA1, cree reglas adicionales para el puerto 28 de TCP y ICMP.
   9. Haga clic en **Añadir reglas de ingreso**.



2. Abra los puertos para su interfaz HA2.
   1. Desde la consola OCI, seleccione **Networking (Redes)** > **Virtual Cloud Networks (Redes virtuales en la nube)** y seleccione su VCN.
   2. Seleccione **Subredes** y seleccione la subred que contiene su interfaz HA2.
   3. Seleccione **Listas de seguridad** y haga clic en la lista de seguridad predeterminada para editarla.
   4. Haga clic en **Añadir regla de ingreso**.
   5. Introduzca el **CIDR fuente** que incluye la dirección IP del puerto del par HA2 de HA.
   6. Seleccione **UDP** o **IP** del menú desplegable **Protocolo IP**.
   7. Si el modo de transporte es UDP, introduzca **29281** en **Nombre del puerto de origen**. Si el modo de transporte es IP, introduzca **99** en **Nombre del puerto de origen**.
   8. Haga clic en **Añadir reglas de ingreso**.

 ©2024 Palo Alto Networks, Inc.

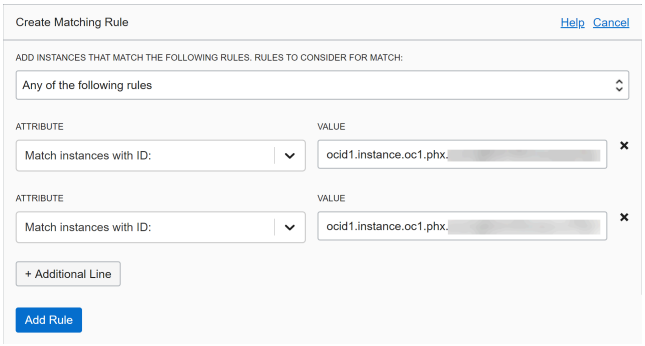


STEP 3 | Añada ambos pares de HA a un grupo dinámico y cree una política que permita a los pares de HA mover la dirección IP flotante. Debe tener el OCID de cada instancia de par de HA para crear las

 ©2024 Palo Alto Networks, Inc.

reglas de coincidencia de grupos dinámicos, por lo que debe tenerlas a mano en el generador de reglas.

1. Crear el grupo dinámico.
    1. Desde la consola OCI, seleccione **Identidad** > **Grupos dinámicos** > **Crear grupo dinámico**.
    2. Introduzca un **Nombre** descriptivo para su grupo dinámico.
    3. Haga clic en **Generador de reglas**.
    4. Seleccione **Cualquiera de las siguientes reglas** del primer menú desplegable.
    5. Seleccione **Hacer coincidir instancias con ID:** del menú desplegable **Atributo)** y pegue uno de los OCID pares en el campo **Valor**.
    6. Haga clic en **+ Línea adicional**.
    7. Seleccione **Hacer coincidir instancias con ID:** del menú desplegable **Atributos** y pegue el otro OCID par en el campo **Valor**.
    8. Haga clic en **Add Rule (Añadir regla)**.

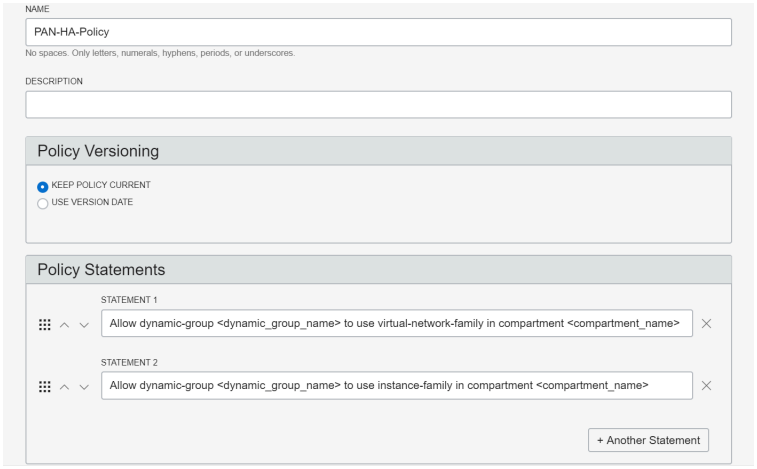


    9. Haga clic en **Crear grupo dinámico**.
2. Crear la regla de política.
    1. Desde la consola OCI, seleccione **Identidad** > **Políticas** > **Crear política**.
    2. Introduzca un **Nombre**descriptivo para su política.
    3. Introduzca la primera declaración de política.

       Permitir que el grupo dinámico <*dynamic_group_name*> utilice la familia de red virtual en el compartimento <*compartment_name*>
    4. Haga clic en **+Otra declaración**.
    5. Introduzca la segunda declaración de política.

       Permitir que el grupo dinámico < *dynamic_group_name*> utilice la familia de instancias en el compartimento < *compartment_name*>
    6. Haga clic en **Create (Crear)**.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

STEP 4 | Configure las interfaces en el cortafuegos. Debe configurar el enlace de datos HA2 y al menos dos interfaces de Capa 3 para sus interfaces trust y untrust. Complete este flujo de trabajo en el primer par de HA y luego repita los pasos en el segundo par de HA.

1. Inicie sesión en la interfaz web del cortafuegos.
2. (Opcional) Si está utilizando la interfaz de gestión como HA1, debe establecer el tipo de IP de la interfaz en estático y configurar un servidor DNS.
   1. Seleccione **Dispositivo** > **Configuración** > **Interfaces** > **Gestión**.
   2. Establezca **Tipo de IP** en **Estática**.
   3. Introduzca la **Dirección IP** privada de la VNIC principal de su instancia de cortafuegos VM-Series.
   4. Haga clic en **OK (Aceptar)**.
   5. Seleccione **Dispositivo** > **Configuración** > **Servicios**.
   6. Haga clic en **Editar**.
   7. Introduzca la dirección IP del **Servidor DNS principal**.
   8. Haga clic en **OK (Aceptar)**.
   9. **Commit (Confirmar)** los cambios.
3. Seleccione **Red** > **Interfaces** > **Ethernet** y haga clic en su interfaz untrust. En este ejemplo, la interfaz HA2 es 1/1, la interfaz trust es ethernet 1/2 y la interfaz untrust es ethernet 1/3.
4. Haga clic en el enlace de **ethernet 1/1** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **HA**
5. Haga clic en el enlace de **ethernet 1/2** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **capa 3**
   - En la pestaña **Config (Configurar)**, asigne la interfaz el enrutador predeterminado.
   - En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. Defina una zona nueva, por ejemplo trust-zone, y a continuación haga clic en **Aceptar**.
   - En la pestaña **IPv4**, seleccione **Static (Estática)**.
   - Haga clic en **Añadir** en la sección IP e introduzca la dirección IP y la máscara de red para la interfaz. Asegúrese de que la dirección IP coincide con la dirección IP que ha asignado a la

 ©2024 Palo Alto Networks, Inc.

subred correspondiente en VCN. Por ejemplo, si añade esta interfaz a su zona trust, asegúrese de asignar la dirección IP de vNIC de trust configurada en su VCN.

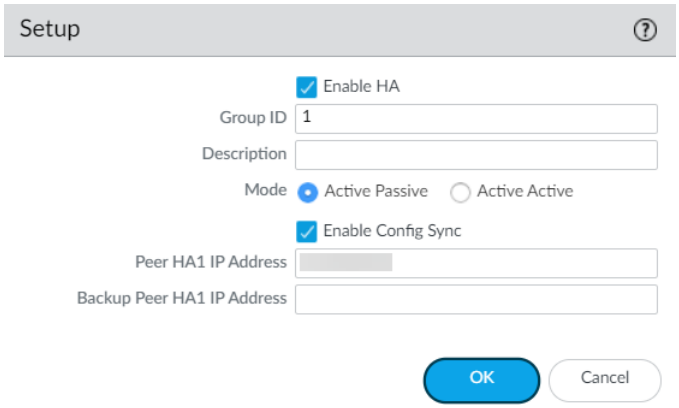
- Haga clic en **Añadir** en la sección IP e introduzca la dirección IP flotante secundaria y la máscara de red.

6. Haga clic en el enlace de **ethernet 1/3** y configúrelo del siguiente modo:
   - **Tipo de interfaz**: **capa 3**
   - En la pestaña **Config (Configurar)**, asigne la interfaz el enrutador predeterminado.
   - En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. Defina una zona nueva, por ejemplo untrust-zone, y a continuación haga clic en **OK (Aceptar)**.
   - En la pestaña **IPv4**, seleccione **Static (Estática)**.
   - Haga clic en **Añadir** en la sección IP e introduzca la dirección IP y la máscara de red para la interfaz. Asegúrese de que la dirección IP coincide con la dirección IP que ha asignado a la subred correspondiente en VCN. Por ejemplo, si añade esta interfaz a su zona no fiable untrust, asegúrese de asignar la dirección IP de vNIC no fiable configurada en su VCN.
   - Haga clic en **Añadir** en la sección IP e introduzca la dirección IP flotante secundaria y la máscara de red.

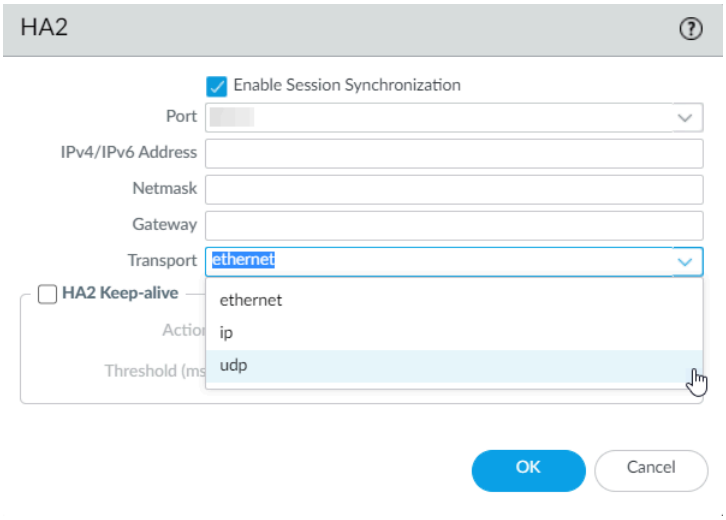
 ©2024 Palo Alto Networks, Inc.

STEP 5 | Habilitar HA.

1. Seleccione **Dispositivo** > **Alta disponibilidad** > **General**.
2. Edite los ajustes de la configuración.
3. Introduzca la dirección IP privada del par pasivo en el **Campo de dirección IP del par HA1**.
4. Haga clic en **OK (Aceptar)**.



5. (Opcional) Edite el enlace de control (HA1). Si no planifica usar la interfaz de gestión para el enlace de control y ha añadido una interfaz adicional (por ejemplo, ethernet 1/4), edite esta sección para seleccionar la interfaz que se usará para la comunicación de HA1.
6. Edite el enlace de datos (HA2) para usar **Puerto** Ethernet 1/1 y añada la dirección IP del par activo y la dirección IP de la **Puerta de enlace** para la subred.
7. Seleccione **IP** o **UDP** del menú desplegable Transporte. Ethernet no es compatible.



8. Haga clic en **OK (Aceptar)**.

STEP 6 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 7 | Repita el paso 4 y el paso 5 en el par HA pasivo.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | Cuando termine de configurar la HA en ambos cortafuegos, verifique que los dispositivos están emparejados en la HA activo/pasivo.

1. Acceda al **Panel** de ambos dispositivos y visualice el widget de Alta disponibilidad.
2. En el par de HA activo, haga clic en **Sincronizar con el par**.
3. Confirme que los cortafuegos estén emparejados y sincronizados.
   - En el cortafuegos pasivo: el estado del cortafuegos local debería mostrar **Pasivo** y la **Config. en ejecución** debería mostrar como sincronizada.
   - En el cortafuegos activo: el estado del cortafuegos local debe mostrar **Activo** y la **Config. en ejecución** debe aparecer como Sincronizada.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en IMB Cloud

Puede utilizar el cortafuegos VM-Series para proteger sus recursos implementados en IBM Cloud.

- Acerca del cortafuegos VM-Series en IBM Cloud
- Prepárese para configurar los cortafuegos VM-Series en IBM Cloud
- Implemente el cortafuegos VM-Series utilizando IBM Cloud Schematics
- Alta resiliencia para el cortafuegos VM-Series en IBM Cloud
- Caso de uso: Implementar un NLB usando el cortafuegos VM-Series

Acerca del cortafuegos VM-Series en IBM Cloud

Los cortafuegos de nueva generación (NGFW) de la serie VM-Series le permiten migrar sus aplicaciones críticas para el negocio a la nube y proteger la mayor huella de nube pública de amenazas, pérdida de datos e interrupción del negocio al:

- Ofrecer una visibilidad inigualable de la aplicación y un control preciso.
- Evitar que las amenazas se muevan lateralmente entre cargas de trabajo y detener la exfiltración de datos.
- Eliminar los cuellos de botella de desarrollo de aplicaciones inducidos por la seguridad con automatización y gestión centralizada.

Consulte los siguientes temas para obtener información acerca de los requisitos del sistema y la información sobre licencias:

- Información sobre licencias
- Requisitos del sistema para el cortafuegos VM-series en IBM Cloud

Información sobre licencias

El cortafuegos VM-Series admite el modelo traiga su propia licencia (BYOL) en IBM Cloud. Para obtener más información, consulte

Traer su propia licencia (BYOL).

Requisitos del sistema para el cortafuegos VM-series en IBM Cloud

Para implementar un cortafuegos VM-Series en una instancia de IBM Cloud, debe elegir un tipo de máquina que admita los requisitos del sistema de VM-Series para su licencia.

Consulte la siguiente tabla para ver los tipos mínimos recomendados de máquinas estándar predefinidas.

Capacidad	tipos mínimos recomendados de máquinas predefinidas
Cortafuegos VM-100	bx2d-2x8
Cortafuegos VM-200	bx2d-2x8
Cortafuegos VM-300	bx2d-4x16
Cortafuegos VM-500	bx2d-4x16
Cortafuegos VM-700	bx2d-16x64

Puede elegir un tipo de máquina con mayor rendimiento o crear su propio tipo personalizado de máquina, si los requisitos del recurso son compatibles con la licencia de su cortafuegos VM-Series. Una sola instancia de IBM Cloud admite hasta cinco interfaces de red. Para obtener más información sobre los tipos de máquina, consulte Perfiles de instancia.

©2024 Palo Alto Networks, Inc.

Prepárese para configurar los cortafuegos VM-Series en IBM Cloud

Implementar el cortafuegos VM-Series desde IBM Cloud Platform requiere tareas de preparación. Si está realizando una implementación utilizando el catálogo de IBM Cloud, debe crear las redes y subredes de su proyecto, y planificar las asignaciones de direcciones IP para las interfaces del cortafuegos VM-Series por adelantado. Durante la implementación, debe seleccionar entre las redes y subredes existentes.

- Requisitos previos
- Dependencias
- Requisitos generales

Requisitos previos

Para configurar el cortafuegos VM-Series en IBM Cloud, necesitará:

- Acceso a la VPC de IBM Cloud Gen 2
- Una VPC con al menos dos subredes y una dirección IP sin asignar en cada subred. Las direcciones IP a la VSI del VM-Series se asignarán desde las subredes proporcionadas por el usuario. Para obtener más información, consulte
- Una de las siguientes regiones para instalar PAN-OS:
  - us-east
  - us-south
  - ca-tor
  - eu-gb
  - eu-de
  - eu-fr2
  - au-syd
  - jp-osa
  - jp-tok

Dependencias

Antes de aplicar la plantilla en IBM Cloud, realice los siguientes pasos:

- Asegúrese de tener los siguientes permisos en Identidad de IBM Cloud y Gestión de accesos:
  - **Manager (Gestor)** Función de acceso a servicios para IBM Cloud Schematics
  - **Operator (Operador)** Función de plataforma para la infraestructura de VPC

©2024 Palo Alto Networks, Inc.

- Asegúrese de que los siguientes recursos existan en su entorno VPC Gen 2:
  - VPC
  - SSH Key - Doc de Clave SSH pública
  - VPC tiene 2 subredes: una para la gestión, la otra para el tráfico del plano de datos
  - Dirección de IP flotante (FIP) para asignar a la interfaz de gestión de instancias del VM-Series después de la implementación. FIP se utiliza para acceder a su instancia de servidor virtual VPC a través de Internet público. Para obtener más información, consulte Creación de una dirección IP flotante.

Requisitos generales

Los componentes de esta lista de comprobación son comunes para implementar un cortafuegos VM-Series que gestiona directamente o con Panorama.

Consulte la Matriz de compatibilidad para la información del complemento Panorama para nubes públicas. Esta versión requiere el siguiente software:

- **Cuenta de IBM Cloud**: debe tener una cuenta de usuario de IBM Cloud con una dirección de correo electrónico enlazada y debe conocer el nombre de usuario y la contraseña de esa dirección de correo electrónico.

  IBM Cloud SDK: si no lo ha hecho, instale el software de IBM Cloud, que incluye las API de IBM Cloud y herramientas de línea de comandos. Puede utilizar la interfaz de línea de comandos para implementar la plantilla de cortafuegos y otras plantillas.
- **PAN-OS en cortafuegos VM-Series en IBM Cloud**: cortafuegos VM-Series que ejecutan una versión de PAN-OS disponible en el catálogo de IBM Cloud.
  - **Cortafuegos VM-Series**: los cortafuegos VM-Series que desea gestionar desde Panorama deben implementarse en la plataforma de IBM Cloud mediante una imagen de Palo Alto Networks del catálogo de IBM Cloud. Los cortafuegos deben cumplir con Requisitos mínimos del sistema para el cortafuegos VM-Series.
  - **Licencias VM-Series**: debe obtener una licencia de un cortafuegos VM-Series para obtener un número de serie. Se requiere un número de serie para añadir un cortafuegos VM-Series como dispositivo gestionado de Panorama. Si está utilizando el complemento de Panorama para IBM Cloud para implementar cortafuegos VM-Series, debe proporcionar un código de autenticación de BYOL. IBM Cloud gestiona la facturación de su servicio, pero los cortafuegos que implemente se conectarán directamente con el servidor de licencias de Palo Alto Networks.
  - **Complemento de VM-Series en el cortafuegos**: los cortafuegos VM-Series que ejecutan PAN-OS 9.0 y versiones posteriores incluyen el Complemento de VM-Series, que gestiona la integración con nubes públicas y privadas. Como se muestra en la Matriz de compatibilidad, el Complemento de VM-Series tiene una versión mínima que corresponde a cada versión de PAN-OS.

    Cuando hay una actualización importante de PAN-OS, la versión del complemento de VM-Series se actualiza automáticamente. Para versiones menores, depende de usted determinar si es necesaria una actualización del complemento de VM-Series y, de ser así, realizar una actualización manual.

 ©2024 Palo Alto Networks, Inc.

- **Panorama ejecutado en modo de gestión** : un dispositivo físico o virtual de Panorama que ejecuta una versión de PAN-OS que es igual o posterior a los cortafuegos gestionados. No es necesario implementar instancias virtuales en IBM Cloud.

  Debe tener:

  - Una versión con licencia de Panorama.
  - Panorama con acceso de red a las VPC en las que están implementadas las máquinas virtuales que desea gestionar.
  - Complemento de VM-Series en Panorama. Consulte Instalación del complemento VM-Series en Panorama.

 ©2024 Palo Alto Networks, Inc.

Implemente el cortafuegos VM-Series utilizando IBM Cloud Schematics

Para implementar el cortafuegos VM-Series con la plantilla de catálogo de IBM, primero debe crear una red de VPC para cada interfaz en el cortafuegos. Para obtener instrucciones sobre cómo crear una red VPC, consulte Introducción a la Red de VPC.

Puede implementar el cortafuegos de nueva generación VM-series (BYOL) a través de IBM Cloud Schematics. La plantilla terraform en IBM Cloud implementa una instancia del cortafuegos VM-Series con un mínimo de una interfaz de gestión y dos interfaces del plano de datos. Puede añadir interfaces del plano de datos adicionales para hasta cinco instancias de IBM Cloud en su nube privada virtual (VPC).

Antes de implementar el cortafuegos VM-Series, debe crear o seleccionar un proyecto en su organización y crear las redes y subredes que se conectarán con el cortafuegos. No puede conectar varias interfaces de red a la misma red de VPC. Cada interfaz que crea debe tener una red dedicada con al menos una subred. Asegúrese de que sus redes incluyan las instancias del plano de datos adicionales que crea.

Todas las interfaces de cortafuegos VM-Series deben tener asignada una dirección IPv4 cuando se implementan en un entorno de nube pública. Las direcciones IPv6 no son compatibles.

STEP 1 | Localice la lista de cortafuegos VM-Series en IBM Cloud Catalog.

1. Inicie sesión en IBM Cloud.
2. Haga clic en **Catálogo**.
3. Busque **Cortafuegos VM-Series de Palo Alto Networks: BYOL** en el cuadro de búsqueda del catálogo de IBM Cloud.
4. Haga clic en el mosaico **Cortafuegos VM-Series de Palo Alto Networks: BYOL**.

STEP 2 | Configure su espacio de trabajo.

1. Introduzca el Nombre de la implementación (este nombre de muestra en el gestor de implementaciones). El nombre debe ser único y no puede entrar en conflicto con ninguna otra implementación del proyecto.
2. Seleccione un grupo de recursos. Para obtener instrucciones para crear un grupo de recursos, consulte Creación de un grupo de recursos.
3. Introduzca las etiquetas relevantes. Las etiquetas le ayudan a identificar su implementación.

STEP 3 | Especifique los valores para los siguientes parámetros:

Parámetros	Description (Descripción)	Valor de muestra
image_name	Imagen VM-Series a instalar.	pa-vm-kvm-9-1-3-1 o pa-vm-kvm-10-0-6
región	Región VPC que desea que se aprovisionen sus servidores virtuales VPC.	us-east

 ©2024 Palo Alto Networks, Inc.

Parámetros	Description (Descripción)	Valor de muestra
ssh_key_name	El nombre de su clave SSH pública para usar para VSI. Para obtener información sobre cómo crear una clave SSH, consulte Clave SSH pública.	vm-series-ssh-key
subnet_id1	El ID de la subred (gestión) que se asociará a la primera interfaz de la instancia VNF. Haga clic en los detalles de la subred en el listado de subredes de VPC para determinar este valor.	0717-xxxxxx-xxxx-xxxxx-8fae-xxxxx
subnet_id2	El ID de la subred (plano de datos) que se asociará con la segunda interfaz de la instancia VNF. Haga clic en los detalles de la subred en el listado de subredes de VPC para determinar este valor.	0717-xxxxxx-xxxx-xxxxx-8fae-xxxxx
vnf_instance_name	Nombre de la instancia VNF a aprovisionar (minúsculas).	vm-series-fw-vsi
vnf_profile	El perfil de CPU de cómputo y recursos de memoria que se utilizarán al aprovisionar la instancia vnf. Para obtener más información, consulte Perfiles de instancia.	bx2-8x32
vnf_security_group	El nombre del grupo de seguridad al que pertenece la primera interfaz (gestión) de la instancia VNF.	vm-series-mgmt-sg

STEP 4 | Instalación de la plantilla terraform.

1. Haga clic en **Install (Instalar)**.
2. Vaya a **IBM Cloud SchematicsWorkspaces (Espacios de trabajo)** y seleccione su espacio de trabajo para ver y editar detalles relacionados con su espacio de trabajo.

STEP 5 | Acceso a la interfaz de gestión del cortafuegos VM Series.

1. Vaya a **IBM cloud** > **VPC Infrastructure (Infraestructura de VPC)** > **Floating IPs (IP flotante)** y copie la IP flotante de su instancia de VPC en la que ha implementado el cortafuegos VM-Series.
2. Abra un navegador e introduzca la dirección IP en la región URL del navegador con el prefijo https (por ejemplo, https://161.xxx.173.xxx). Aparecerá la pantalla de inicio de sesión de la interfaz de gestión del cortafuegos VM-Series. Si está utilizando una conexión VPN, es posible que tenga que terminar la conexión antes de conectarse a la consola VM-Series (URL).
3. Inicie sesión en la interfaz con las siguientes credenciales: Nombre de usuario: admin Contraseña: admin

Se le solicitará que cambie su contraseña en su primer inicio de sesión. Podrá acceder a la interfaz solo después de iniciar sesión con la contraseña cambiada.

 ©2024 Palo Alto Networks, Inc.

Alta resiliencia para el cortafuegos VM-Series en IBM Cloud

Puede implementar los cortafuegos VM-Series en IBM Cloud para garantizar la redundancia en la red utilizando la configuración de alta disponibilidad (HA) activa/activa. La función de modo de ruta del balanceador de carga de red (NLB) se usa para admitir la alta disponibilidad del VM-Series y, actualmente, solo se admite con IP privada y tráfico de datos TCP.

La capacidad de enrutamiento de entrada le permite asociar tablas de ruta con la puerta de enlace de Internet de IBM y añadir reglas de ruta para redirigir el tráfico de la aplicación a través del cortafuegos VM-Series. Esta redirección garantiza que todo el tráfico de Internet pase a través del cortafuegos sin tener que reconfigurar los endpoints de la aplicación.

- Configuración del VM-Series de IBM VPC para alta disponibilidad
- Implementación del cortafuegos VM-Series
- Implemente el NLB.
- Configurar grupos de seguridad
- Configurar rutas personalizadas
- Consideraciones sobre las conmutaciones por error de NLB y las rutas personalizadas

Para obtener más información sobre la oferta de Network Load Balancer para VPC Gen 2, consulte el mosaico

- Catálogo de Balanceador de carga para VPC Gen 2
- Acerca del Balanceador de cargas de IBM Cloud Network para VPC

Configuración del VM-Series de IBM VPC para alta disponibilidad

Para configurar los recursos de VPC para alta disponibilidad, deberá hacer lo siguiente:

- Crear una VPC. Para obtener instrucciones sobre cómo crear una red VPC, consulte Introducción a la Red de VPC.
- Cree una subred para la interfaz de tráfico de gestión del VM-Series. Esto se puede compartir entre varios VM-Series para admitir la agrupación en clústeres.
- Cree una subred que se compartirá entre la interfaz de tráfico de datos del VM-Series y el balanceador de carga de red (NLB).
- Cree las subredes adicionales necesarias para las cargas de trabajo de VSI que se enrutarán a través de NLB o VNF.
- Conceda una autorización de servicio para su cuenta de IBM Cloud para permitir que el NLB modifique las rutas personalizadas si se produce una conmutación por error de NLB.

Implementación del cortafuegos VM-Series

Al implementar el cortafuegos VM-Series en modo de alta disponibilidad, deberá asegurarse de lo siguiente:

- La interfaz de datos del VM-Series se encuentra en la misma subred compartida que el NLB que aprovisionaremos más adelante.

 ©2024 Palo Alto Networks, Inc.

- **`Permitir la suplantación de IP`** está habilitada en la interfaz de datos del VM-Series (subred compartida con NLB) a través de la página Interfaces de red de la interfaz de usuario de VSI de VPC.
- **`Comprobaciones de estado`** para la configuración de VNF está habilitada desde el NLB.

Implemente el NLB.

Puede implementar un NLB mediante la interfaz de usuario, la CLI o la API de REST. Para obtener instrucciones sobre cómo implementar un NLB, consulte Creación de un balanceador de carga de red en modo de ruta para VPC.

Configurar grupos de seguridad

La interfaz de red de datos del VM-Series está conectada a un grupo de seguridad de VPC. Al configurar los grupos de seguridad, asegúrese de que el grupo de seguridad tenga reglas de entrada que permitan el tráfico en la configuración del puerto de estado entre el NLB y el VM-Series. Por ejemplo, si la comprobación de estado está configurada para TCP en el puerto 80 (HTTP), cree una regla de entrada en el mismo grupo de seguridad. Además, asegúrese de que las reglas se crean para permitir o restringir el tráfico de datos.

Configurar rutas personalizadas

Las rutas personalizadas se crean para garantizar que el tráfico de datos de entrada se enruta a través del NLB en su camino al VM-Series y al destino objetivo. En algunos casos, es posible que también se necesiten rutas personalizadas para garantizar que el tráfico de salida se devuelva al origen del cliente original. Para obtener más información, consulte Acerca de las tablas de enrutamiento y las rutas.

Consideraciones sobre las conmutaciones por error de NLB y las rutas personalizadas

- Implemente el NLB como un clúster activo/pasivo. Asegúrese de que cada nodo tenga una IP distinta y que la IP activa se utilice en las rutas personalizadas que se creen. Puede utilizar un **nslookup** en el nombre de host del NLB, para determinar la IP principal que se utilizará en la configuración de ruta.
- Configure el VM-Series para permitir el tráfico de los nodos NLB activos y pasivos. Esto es necesario para la comprobación de estado. Las IP de NLB se pueden recuperar de la **NLB UI (UI de NLB)** > **Overview (Descripción general)** > **Private IPs (IP privadas)**.
- Las rutas personalizadas se actualizan automáticamente para saltar a la nueva IP de NLB, si el NLB conmuta por error al otro nodo.

 ©2024 Palo Alto Networks, Inc.

Caso de uso: Implementar un NLB usando el cortafuegos VM-Series

En este ejemplo, el cliente se encuentra en una zona diferente al resto de los recursos.

PASO 1: La tabla de enrutamiento de entrada dirige el tráfico hacia los LB en dirección de cliente a servidor. En este caso, dado que el cliente se encuentra en una zona diferente, la fuente de tráfico para la tabla de enrutamiento es la Zona VPC.

Paso 2: El balanceador de carga envía los paquetes a uno de los cortafuegos. Dado que las subredes DP del FW y la subred de servidor están en la misma VPC, pueden alcanzarse a través de las puertas de enlace predeterminadas.

No es necesario configurar el enrutamiento personalizado en el cortafuegos si la interfaz DP está configurada como DHCP. Si la IP estática está configurada en la interfaz de DP, entonces la ruta predeterminada debe configurarse en el cortafuegos.

Paso 3: Adjunte el perfil de gestión de interfaz que permite sondas HTTP/HTTPS a la interfaz de DP.

Paso 4: Configure la política de seguridad para permitir el tráfico de entrada.

Paso 5: Para que el tráfico de retorno se mueva en la dirección de servidor a cliente, debe haber una tabla de enrutamiento de salida adjunta a la subred del servidor, que dirige el tráfico (destinado al cliente) al LB. El LB reenvía el paquete al mismo cortafuegos que el tráfico en la otra dirección. El cortafuegos reenviará el paquete a través de su puerta de enlace predeterminada al cliente.

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en Alibaba Cloud

La implementación del cortafuegos VM-Series en Alibaba Cloud protege las redes que crea dentro de Alibaba Cloud. Puede implementar cortafuegos VM-Series para proteger las aplicaciones accesibles desde Internet y las implementaciones de nube híbrida.

- Cortafuegos VM-Series en Alibaba Cloud
- Requisitos mínimos del sistema para el cortafuegos VM-Series en Alibaba Cloud
- Preparación para la implementación del cortafuegos VM-Series en Alibaba Cloud
- Implemente el cortafuegos VM-Series en Alibaba Cloud
- Configuración de la HA activa/pasiva en Alibaba Cloud

Cortafuegos VM-Series en Alibaba Cloud

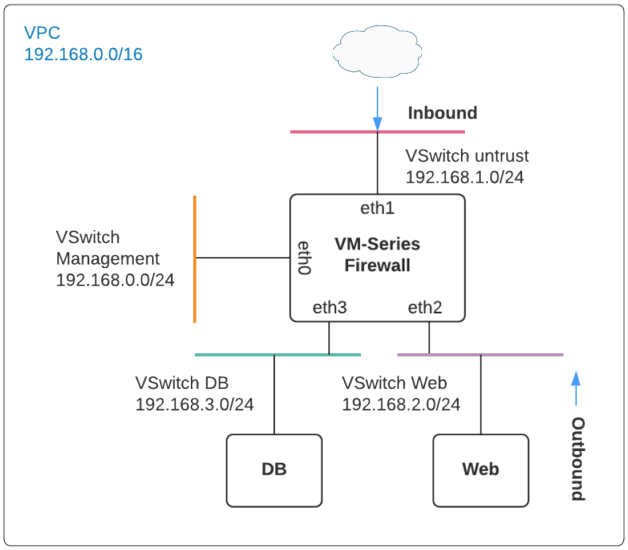
Puede implementar el cortafuegos VM-Series para proteger el tráfico de entrada y saliente de norte a sur en Alibaba Cloud.

Asegurar el tráfico de este a oeste dentro de la misma VPC no es compatible porque Alibaba Cloud no admite el enrutamiento de subred.

El cortafuegos VM-Series en Alibaba Cloud se ejecuta en el hipervisor de KVM y admite hasta 8 interfaces de red cuando selecciona una instancia de Alibaba Cloud con recursos suficientes (consulte Requisitos mínimos del sistema para el cortafuegos VM-Series en Alibaba Cloud).

El cortafuegos VM-Series en Alibaba Cloud es compatible con licencias BYOL y VM-Series ELA en Alibaba Cloud Regiones internacionales y China continental. Actualmente, no se admiten las licencias PAYG.

En Alibaba Cloud, su VPC aísla de forma lógica su red virtual. Después de crear una VPC, puede crear VSwitches para segmentar aún más su red privada virtual, como se muestra en el siguiente diagrama. Para asegurar el tráfico entrante, tanto el DNAT como el SNAT deben configurarse en el cortafuegos.



El tráfico de entrada se origina en un cliente fuera de su VPC que va a la interfaz untrust del cortafuegos VM-Series. El cortafuegos inspecciona el tráfico y lo envía a una aplicación a través de la interfaz trust. El tráfico que vuelve de la aplicación va a través de la interfaz trust del cortafuegos, donde el cortafuegos inspecciona el flujo de tráfico de retorno y lo envía a través de la interfaz untrust.

El tráfico saliente normalmente se origina en una aplicación externa. Normalmente, el tráfico de cara a internet se enruta dentro de una VPC a una puerta de enlace NAT (con un EIP adjunto). Para hacer esto, añada una ruta de puerta de enlace predeterminada en la tabla de enrutamiento de VPC, con la dirección IP del cortafuegos VM-Series de la subred de la aplicación como el siguiente salto. Configure SNAT utilizando la IP de interfaz Untrust para asegurarse de que el tráfico que se origina en internet pase a través del cortafuegos VM-Series.

Consulte Asegurar el tráfico norte-sur en Alibaba Cloud para obtener una configuración de muestra.

©2024 Palo Alto Networks, Inc.

Requisitos mínimos del sistema para el cortafuegos VM-Series en Alibaba Cloud

En Alibaba Cloud, es posible implementar el cortafuegos VM-Series en el hipervisor KVM (consulte Implementaciones de VM-Series).

- Requisitos de software del cortafuegos VM-Series
- Recomendaciones de tipo de instancia de Alibaba Cloud para el cortafuegos VM-Series
- CLI de Alibaba Cloud

Requisitos de software del cortafuegos VM-Series

Asegúrese de tener el software y las licencias necesarias para completar una implementación de VM-Series en Alibaba Cloud.

- Para implementar el cortafuegos VM-Series en Alibaba Cloud, debe utilizar una imagen de VM-Series que obtenga de Alibaba Marketplace. La imagen incorpora PAN-0S versión 10.0.3 y el complemento VM-Series versión 2.0.3.
- Antes de la implementación, seleccione el ELA de VM-Series o la licencia BYOL, una licencia de capacidad y un paquete de suscripción. Consulte Tipos de licencia del modelo VM-Series.
- Debe poder abrir sesión SSH en el cortafuegos VM-Series para completar la implementación. Si su sistema operativo no es compatible con SSH, instale un software de terceros, como Putty.

Recomendaciones de tipo de instancia de Alibaba Cloud para el cortafuegos VM-Series

Antes de crear el cortafuegos VM-Series, debe elegir un tipo de instancia de Elastic Compute Service (ECS) que admite los Requisitos mínimos del sistema para su modelo VM-Series. Revisa la documentación del tipo de instancia para garantizar que el tipo de instancia de ECS tenga los recursos para asegurar su configuración de red.

Modelo VM-Series	Tipo de instancia de servicio de máquina virtual elástica
VM-100 Créditos de NGFW de software	ecs.g5.xlarge ecs.g6.xlarge ecs.g7ne.xlarge ecs.sn2ne.xlarge
VM-300 Créditos de NGFW de software	ecs.g5.xlarge ecs.g6.2xlarge ecs.g7ne.2xlarge ecs.sn2ne.xlarge

©2024 Palo Alto Networks, Inc.

Modelo VM-Series	Tipo de instancia de servicio de máquina virtual elástica
VM-500 Créditos de NGFW de software	ecs.g5.xlarge ecs.g6.2xlarge ecs.g7ne.2xlarge ecs.sn2ne.xlarge
VM-700 Créditos de NGFW de software	ecs.g5.4xlarge ecs.g6.4xlarge ecs.g7ne.4xlarge ecs.sn2ne.4xlarge
Software NGFW Credits	g6 Instance Family g7ne Instance Family

The VM-Series for AliCloud deployed on g5, g6, and g7 instances support Packet MMAP only.

CLI de Alibaba Cloud

Aliyun versión 3.0.4 o superior. Consulte Preparación para el uso de la interfaz de línea de comandos de Aliyun.

©2024 Palo Alto Networks, Inc.

Preparación para la implementación del cortafuegos VM-Series en Alibaba Cloud

Esta tarea utiliza la CLI de Aliyun para crear una VPC y VSwitches para el cortafuegos VM-Series, sin embargo, debe planificar su red antes de comenzar. Evalúe las aplicaciones que desea proteger y determine dónde implementará el cortafuegos VM-Series para inspeccionar y asegurar el tráfico norte-sur.

- Seleccione licencias y planifique las redes
- Preparación para el uso de la interfaz de línea de comandos de Aliyun

Seleccione licencias y planifique las redes

Evalúe las aplicaciones que necesita para proteger y crear redes que permitan al cortafuegos VM-Series inspeccionar el tráfico de aplicaciones entrantes y salientes.

STEP 1 | Planificar y diseñar su VPC.

1. Planifique redes, incluyendo Bloques CIDR para sus VPC y VSwitch.

   Consulte Cree una VPC y configure redes para ver un procedimiento de muestra.
2. Planifique sus direcciones IP. Si necesita direcciones o rangos de direcciones específicos, consulte la Guía del usuario de direcciones IP elásticas.
3. Planifique los grupos de seguridad.

STEP 2 | Evalúe sus aplicaciones y configuraciones de red y calcule la capacidad de cortafuegos que necesita para proteger sus aplicaciones y redes.

STEP 3 | Obtenga licencias de cortafuegos VM-Series.

Aunque no necesita una licencia para instalar el cortafuegos VM-Series (puede activar una licencia después de la instalación), debe elegir un modelo de la VM-series y el tipo de instancia ECS adecuados antes de implementar el cortafuegos.

1. Seleccione un modelo VM-Series.

   El cortafuegos VM-Series admite hasta 8 interfaces, siempre que el modelo de la serie VM-Series y la instancia de Alibaba Cloud tengan suficientes recursos. Puede usar el modelo

   Use el modelo de la VM-series que ha elegido para elegir uno de los Recomendaciones de tipo de instancia de Alibaba Cloud para el cortafuegos VM-Series.
2. Seleccione una licencia de capacidad de VM-Series que satisfaga sus necesidades.
3. Compre un paquete de suscripción BYOL (si aún no tiene uno). Recibirá un código de autenticación para su suscripción de VM-Series y debe proporcionarlo durante la implementación.

STEP 4 | Planifique cómo configurar las cuentas y los permisos de Alibaba para acceder al cortafuegos VM-Series. Para empezar, consulte las Preguntas frecuentes sobre seguridad y obtenga información sobre las Funciones de RAM de instancias.

 ©2024 Palo Alto Networks, Inc.

Preparación para el uso de la interfaz de línea de comandos de Aliyun

Este capítulo se centra en la Consola de ECS; sin embargo, todo lo que hace en la Consola de ECS se puede hacer desde la interfaz de línea de comandos de Aliyun. La CLI es necesaria si desea utilizar el cortafuegos VM-Series para proteger el balanceo de carga en Alibaba Cloud.

Instale y configure una versión reciente de Aliyun, la interfaz de línea de comandos de Alibaba Cloud.

STEP 1 | Cree una AccessKey y guarde el ID y la clave secreta de la clave de acceso en un lugar seguro.

STEP 2 | Descargue una versión compatible de Aliyun desde https://github.com/aliyun/aliyun-cli.

STEP 3 | Instale Aliyun.

STEP 4 | Configure Aliyun.

La configuración le solicita la información de su clave de acceso y otra información.

Si su implementación usa un depósito de almacenamiento, la región debe coincidir con la región de su depósito.

```
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: ...
```


©2024 Palo Alto Networks, Inc.

Implemente el cortafuegos VM-Series en Alibaba Cloud

El cortafuegos VM-Series asume un mínimo de tres interfaces: gestión, no fiable (untrust) y fiable (trust). Cuando crea una VPC de Alibaba Cloud, esta está aislada lógicamente. Para segmentar su red privada virtual en subredes, cree VSwitches, cada uno con su propio bloque CIDR. Debido a que el cortafuegos VM-Series tiene múltiples interfaces, puede inspeccionar el tráfico en todas las subredes.

Por lo general, el tráfico externo entrante se encuentra con la interfaz untrust de cortafuegos VM-Series. El cortafuegos inspecciona el tráfico entrante y lo envía a una aplicación a través de la interfaz trust. El tráfico de retorno de la aplicación va a la interfaz trust del cortafuegos, donde el cortafuegos inspecciona el tráfico de retorno y lo envía a través de la interfaz untrust.

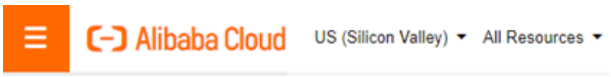
Las siguientes tareas demuestran cómo utilizar la consola para crear la infraestructura de cortafuegos VM-Series.

- Cree una VPC y configure redes
- Creación y configuración del cortafuegos VM-Series
- Asegurar el tráfico norte-sur en Alibaba Cloud
- Configuración del equilibrio de carga en Alibaba Cloud

Cree una VPC y configure redes

Utilice la consola de Alibaba Cloud para crear una VPC, VSwitches, grupos de seguridad y reglas de grupo de seguridad.

STEP 1 | Abra la Consola de VPC y seleccione su región del menú. Tenga en cuenta que la región que seleccione debe proporcionar uno de los tipos de instancia que admite Palo Alto Networks.



STEP 2 | En la página de inicio de Alibaba Cloud Console, seleccione **Products and Services (Productos y servicios)** > **Networking (Redes)** > **Virtual Private Cloud (Nube privada virtual)**.

STEP 3 | **Create a VPC (Crear una VPC)**.

En este paso, creará un VPC y VSwitches de gestión, untrust y trust. La consola de ECS crea un VPC y un conmutador utilizando el mismo formulario.

1. Seleccione **Create VPC (Crear VPC)**.

   Especifique el nombre de la VPC, un bloque CIDR de IPv4 y una descripción. Consulte Create a VPC (Crear una VPC).

Propiedad	Valor
Nombre	Su elección
Bloque CIDR de IPV4	Su elección. Consulte las Preguntas frecuentes sobre el bloque CIDR.

 ©2024 Palo Alto Networks, Inc.

Propiedad	Valor
Grupo de recursos	Su elección.

2. Seleccione **Create VSwitch (Crear VSwitch)**.
   - Nombre el vSwitch **`Management`**.
   - Seleccione la **Zone (Zona)**, especifique un **IPv4 CIDR Block (Bloque CIDR de IPv4)** que sea un subconjunto del bloque que especificó para la VPC y especifique una **Description (Descripción)**.
   - En la parte inferior, haga clic en **Add (Añadir)** para añadir otro vSwitch (no haga clic en **OK [Aceptar]** hasta que haya añadido todos los VSwitches).

   Consulte Create a VSwitch (Crear un vSwitch).
3. **Add (Añadir)** vSwitch Untrust de la misma manera.
4. **Add (Añadir)** el VSwitch Trust.
5. Haga clic en **OK (Aceptar)**.

   Vea los detalles de la VPC y realice cambios antes de hacer clic en **Complete (Completar)**.

STEP 4 | Cree grupos de seguridad y reglas de grupos de seguridad.

- Desde la página de inicio de la consola de Alibaba Cloud, seleccione **Elastic Compute Service** > **Networking & Security (Redes y seguridad)** > **Security Groups (Grupos de seguridad)**.
- En la parte superior derecha, haga clic en **Create Security Group (Crear grupo de seguridad)**.

1. Cree el grupo de seguridad de gestión.

   Consulte Crear un grupo de seguridad para completar los siguientes campos.

Propiedad	Valor
Plantilla	Personalizar
Nombre del grupo de seguridad	Gestión
Tipo de grupo de seguridad	Básico
Tipo de red	VPC
VPC	Seleccione la VPC que creó anteriormente.

 ©2024 Palo Alto Networks, Inc.

Propiedad	Valor
Grupo de recursos	Su elección

- Complete el formulario y haga clic en **OK (Aceptar)**.

  La consola de ECS le solicita que cree reglas para este grupo de seguridad. Esta tarea describe algunas reglas del grupo de seguridad básicas que le permiten abrir el cortafuegos VM-Series. Puede crear más reglas para hacer cumplir los requisitos de seguridad de su red.

2. Seleccione **Create Rules Now (Crear reglas ahora)** y cree reglas para HTTPS y SSH.

   Seleccione la pestaña Entrante y haga clic en **Add Security Group Rule (Añadir regla de grupo de seguridad)**.

   - Cree una regla de entrada para permitir HTTPS en este grupo de seguridad. Por ejemplo:

Propiedad	Valor
Dirección de la regla	Entrante
Acción	Permitir
Tipo de protocolo	HTTPS (443)
Prioridad	100
Tipo de autorización	Consulte Add security group rules (Añadir reglas de grupo de seguridad).
Objeto de autorización	

   - Haga clic en Añadir **Security Group Rule (Regla de grupo de seguridad)** para crear una regla de entrada para permitir SSH en la interfaz de gestión.

Propiedad	Valor
Dirección de la regla	Entrante
Acción	Permitir
Tipo de protocolo	TCP personalizado
Intervalo de puertos	1/65535
Tipo de autorización	Consulte Add security group rules (Añadir reglas de grupo de seguridad).
Objeto de autorización	

   Haga clic en **OK (Aceptar)** y seleccione **Back (Volver)** para volver a la página Grupos de seguridad.

 ©2024 Palo Alto Networks, Inc.

3. Seleccione **Create Security Group (Crear grupo de seguridad)** y cree el grupo de seguridad Untrust.

   Cuando se le solicite, cree una regla para el grupo de seguridad Untrust, no fiable.

Propiedad	Valor
Dirección de la regla	Entrante
Acción	Permitir
Tipo de protocolo	TCP personalizado
Intervalo de puertos	1/65535
Prioridad	100
Tipo de autorización	Consulte Add security group rules (Añadir reglas de grupo de seguridad).
Objeto de autorización	

   Haga clic en **OK (Aceptar)** y seleccione **Back (Volver)** para volver a la página Grupos de seguridad.

4. Crea el grupo de seguridad Trust.

   Cuando se le solicite, haga clic en **Add Security Group Rule (Añadir regla de grupo de seguridad)** y duplique la regla Untrust.

   Continúe a Creación y configuración del cortafuegos VM-Series.

Creación y configuración del cortafuegos VM-Series

Esta tarea usa la consola de ECS para crear una instancia de cortafuegos VM-Series con un mínimo de tres interfaces: administración, untrust y trust. Una instancia de ECS es compatible con una única NIC de forma predeterminada y le adjunta automáticamente una interfaz de red elástica (ENI). Para admitir el cortafuegos VM-Series, debe crear por separado las Interfaces de red elásticas de Untrust y Trust (ENI) y adjuntarlas a su instancia.

STEP 1 | En la página de inicio de la consola de Alibaba Cloud, seleccione **Elastic Compute Service** > **Instances & Images (Instancias e imágenes)** > **Instances (Instancias)** y haga clic en **Create Instance (Crear instancia)** en la parte superior derecha.

STEP 2 | Seleccione **Custom Launch (Inicio personalizado)**.

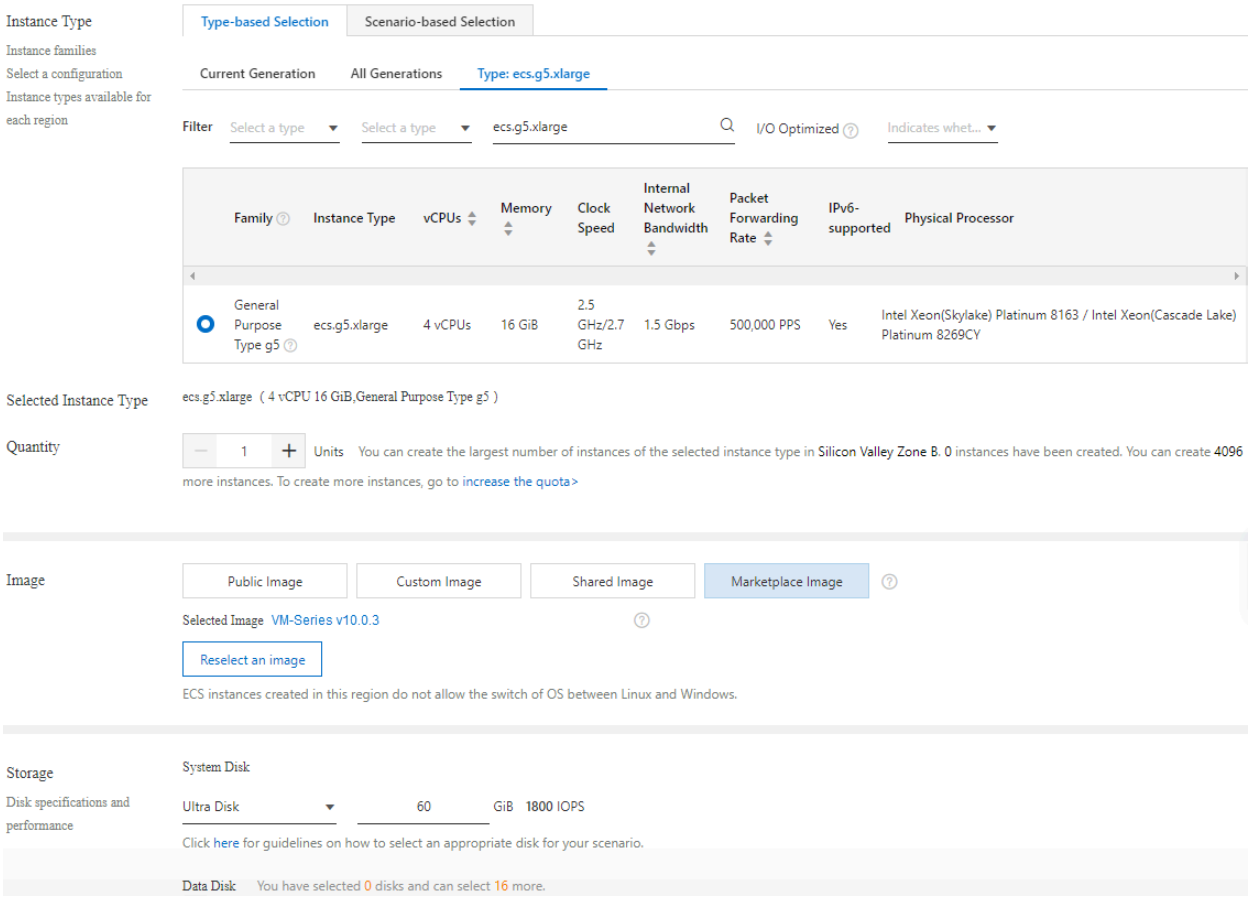
STEP 3 | Configuraciones básicas.

1. Complete los siguientes valores. Por ejemplo:

Propiedad	Valor
Método de facturación	Suscripción.

 ©2024 Palo Alto Networks, Inc.

Propiedad	Valor
Región	Su elección. También puede seleccionar una zona. La región que seleccione debe proporcionar uno de los tipos de instancia obligatorios.
Tipo de instancias	Uno de los tipos en Recomendaciones de tipo de instancia de Alibaba Cloud para el cortafuegos VM-Series. Puede utilizar la selección basada en tipo para buscar el tipo de instancia.
Imagen	Seleccione **Marketplace Image (Imagen de Marketplace)** y busque "VM-Series" en Alibaba Marketplace. La imagen combina el sistema operativo y el cortafuegos VM-Series.
Almacenamiento	Seleccione un tipo de disco y especifique 60 GB.
Instantánea	Su elección.
Duración	Su elección.



2. Seleccione **Siguiente: Redes**.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | En la página de Redes, suministre los siguientes valores.

1. Red (seleccione VPC).
   - Seleccione la VPC que creó en Cree una VPC y configure redes.
   - Seleccione el vSwitch de gestión.
2. Dirección IP pública.

   Si no tiene una dirección IP pública, habilite **Assign Public IP address (Asignar dirección IP pública)** y el sistema asignará una. Si debe utilizar una dirección IP específica o una dirección en un rango específico, puede solicitar una dirección IP personalizada. Consulte la Guía del usuario de direcciones IP elásticas.
3. Grupo de seguridad.

   Seleccione el grupo de seguridad de gestión.
4. Interfaz de red elástica.

   La interfaz de gestión ya está adjunta a eth0.
5. Seleccione **Siguiente: Configuraciones del sistema**.

STEP 5 | En la página Configuraciones del sistema, complete los siguientes valores.

1. Credenciales de inicio de sesión: Seleccione **Key Pair (Par de claves)**.

   No se admite la autenticación de contraseña.
2. Nombre la instancia de cortafuegos VM-Series y proporcione un nombre de host.

   Realice cualquier corrección.

   Seleccione **Preview (Vista previa)** para ver su configuración hasta el momento.
3. Después de **Advanced (based or instance RAM roles or cloud-init) (Avanzado [funciones de RAM basadas o de instancia, o cloud-init])** haga clic en **Show (Mostrar)**.
   - La función de RAM es opcional.
   - En el campo Datos de usuario, introduzca la información de arranque básica como pares clave-valor separados por líneas nuevas. Consulte Introduzca una configuración básica como datos de usuario (AWS, Azure o GCP). Por ejemplo, introduzca lo siguiente en el campo **User Data (Datos de usuario)**.

```
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-
```

 ©2024 Palo Alto Networks, Inc.

```
pin-id=abcdefgh1234**** vm-series-auto-registration-pin-
value=zyxwvut-0987****
```

> ***op-command-modes*** *(mgmt-interface-swap y trama gigante) no son compatibles con Alibaba Cloud.*
>
> ***op-cmd-dpdk-pkt-io = on*** *compatible con DPDK. Si desea especificar PacketMMAP, especifique op-cmd-dpdk-pkt-io=off*

La agrupación es opcional. Seleccione **Preview (Vista previa)** para ver la configuración antes de realizar el pedido.

STEP 6 | Vea los términos de servicio y seleccione **Create Order (Crear pedido)** para crear la instancia de cortafuegos VM-Series.

Vea el pedido de compra y seleccione **Subscribe (Suscribir)**.

STEP 7 | Desde la página de inicio de la consola, seleccione > **Elastic Compute Service** > **Network and Security (Redes y seguridad)** > **ENIs** y seleccione **Create ENI (Crear ENI)** en la esquina superior derecha. Cree interfaces de red elásticas para las interfaces Untrust y Trust.

1. Cree el ENI Untrust.

   En la columna **Actions (Acciones)**, seleccione **Bind to Instance (Vincular a instancia)** y seleccione la instancia que acaba de crear.
2. Cree el ENI Trust y vincúlelo a la instancia.

STEP 8 | Asigne las direcciones IP elásticas (EIP).

Asigne direcciones EIP para la interfaz de gestión del cortafuegos VM-Series y la interfaz de red Untrust. En este ejemplo, la interfaz Trust no está expuesta a Internet, por lo que no necesita una tercera dirección IP.

Si ya tiene dos EIP, vaya al siguiente paso.

1. Asocie una EIP con la interfaz de gestión del cortafuegos VM-Series.
2. Asocie una EIP con la interfaz de red Untrust del cortafuegos VM-Series.

   La segunda interfaz que adjunta se asigna a la interfaz de red 1 en el cortafuegos VM-Series.

STEP 9 | Reinicie su instancia para adjuntar las nuevas interfaces de red.

En la lista de instancias, seleccione su instancia, seleccione **Manage (Gestionar)** y haga clic en **Restart (Reiniciar)** en la parte superior derecha.

STEP 10 | Acceda mediante SSH al cortafuegos VM-Series con la clave de seguridad y establezca la contraseña de administrador:

```
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
```

 ©2024 Palo Alto Networks, Inc.

STEP 11 | Acceda a la interfaz web del cortafuegos VM-Series.

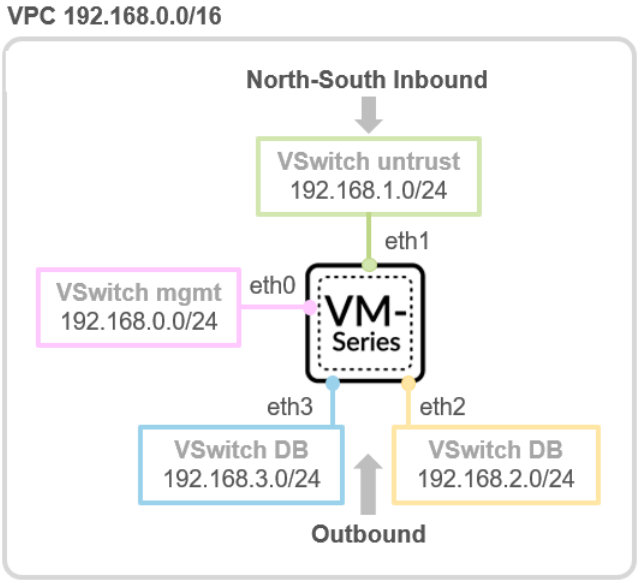
Abra un navegador web e introduzca la EIP para la interfaz de gestión.

Asegurar el tráfico norte-sur en Alibaba Cloud

Después de crear una VPC, puede crear VSwitches para segmentar su red privada virtual en subredes. El ejemplo cuenta con una VPC con CIDR 192.168.0.0/16; puede introducir sus propios valores. Cuatro VSwitches crean cuatro subredes.

Nombre del vSwitch	Interface (Interfaz)	CIDR de muestra
mgmt	eth0	192.168.0.0/24
no fiable	eth1	192.168.1.0/24
web	eth2	192.168.2.0/24
db	eth3	192.168.3.0/24

En el siguiente diagrama, el cortafuegos VM-Series se conecta a dos subredes de confianza, web y bases de datos. El tráfico de entrada se inicia cuando un cliente externo accede a la interfaz Untrust del cortafuegos VM-Series. El cortafuegos inspecciona el tráfico y lo envía a una aplicación. Por ejemplo, el cortafuegos envía el tráfico a un servidor web a través de la interfaz Trust. El tráfico que regresa del servidor web debe llegar a la interfaz Trust del cortafuegos VM-Series. El cortafuegos inspecciona el flujo de tráfico de retorno y lo envía a través de la interfaz Untrust.



Para asegurar el tráfico entrante, tanto el DNAT como el SNAT deben configurarse en el cortafuegos.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Cree reglas de NAT para el tráfico entrante.

Este es un ejemplo de las reglas de NAT para la protección del tráfico entrante.

```
          <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
 name="web_server"> <ip-netmask>192.168.2.203</ip-netmask> </entry>
 </address>
```

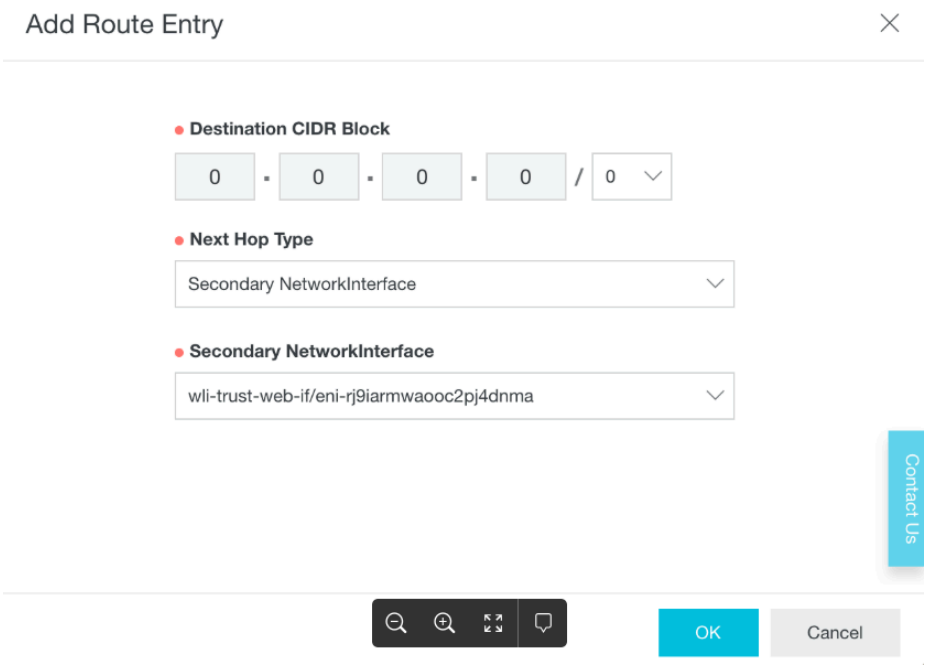
STEP 2 | Asegurar el tráfico saliente.

Tal y como se muestra en el diagrama anterior, una aplicación inicia el tráfico saliente. Por ejemplo, un servidor web debe ejecutar **`yum install`** para actualizar paquetes rpm. Normalmente, el tráfico

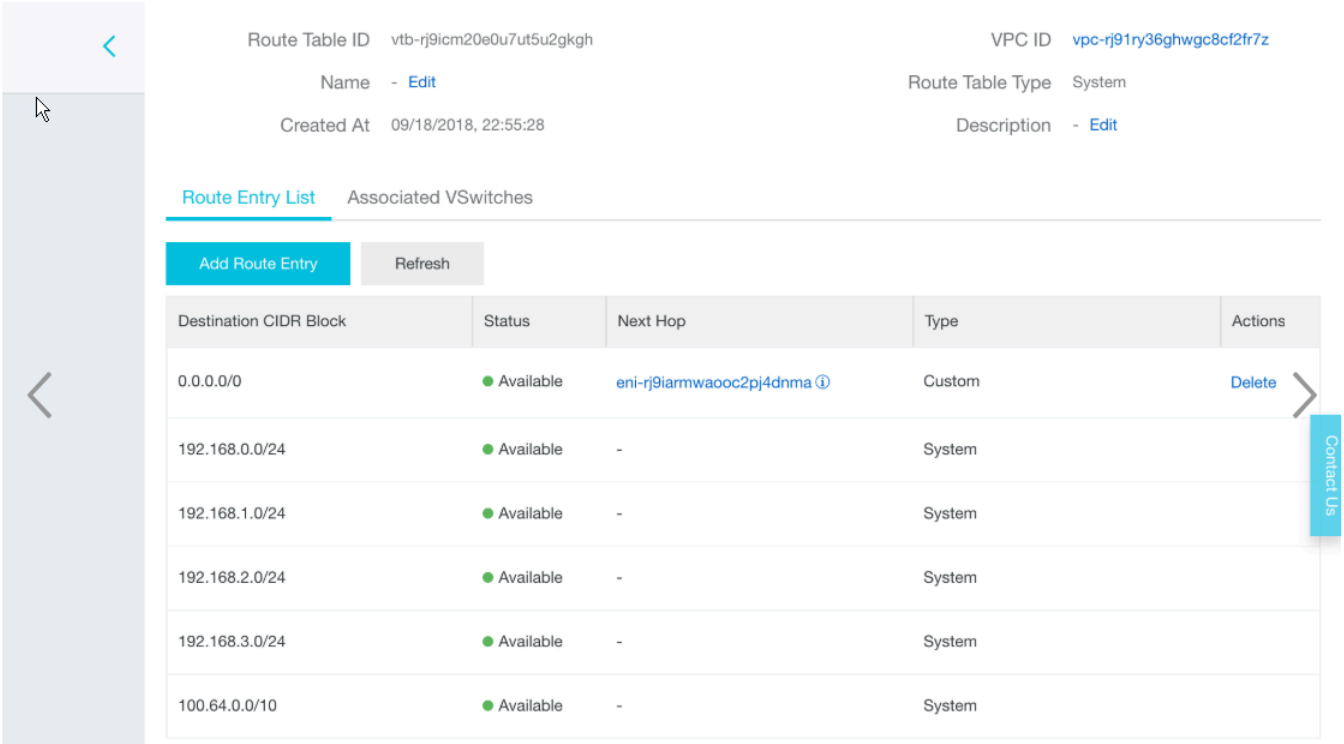
 ©2024 Palo Alto Networks, Inc.

de cara a internet dentro de una VPC se enruta a una puerta de enlace NAT (con un EIP adjunto). Para asegurar el tráfico saliente, debe forzar el tráfico saliente para que pase por el cortafuegos VM-Series.

1. Añada una ruta de puerta de enlace predeterminada en la tabla de enrutamiento de VPC con IP de cortafuegos en la subred del servidor web como el siguiente salto.



2. Vea su entrada en la tabla de rutas.



3. Configure las reglas de SNAT usando la IP de interfaz Untrust para asegurarse de que el tráfico que regresa de internet pase a través del cortafuegos VM-Series.

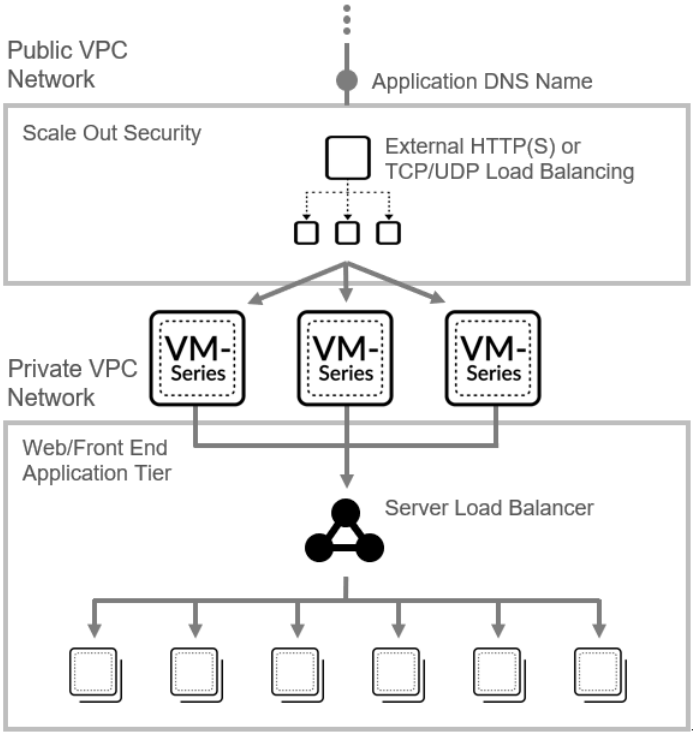
 ©2024 Palo Alto Networks, Inc.

Este es un ejemplo de una configuración de 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>
```

Configuración del equilibrio de carga en Alibaba Cloud

En Alibaba Cloud, puede implementar el cortafuegos VM-Series en una configuración de sándwich de balanceador de carga donde el cortafuegos se implementa entre una red pública y una red privada, como se muestra a continuación.



En Crear una VPC y configurar redes, creó las ENI Untrust y Trust y las adjuntó a la instancia del cortafuegos VM-Series como ENI secundarias.

Cuando utiliza la consola para añadir varios servidores backend en el balanceador de carga del servidor (SLB) de Alibaba, el SLB envía tráfico a la ENI principal de los servidores backend del siguiente salto. Debido a que la ENI principal es la interfaz de gestión, el tráfico debe ir a la interfaz Untrust (una ENI secundaria) para su inspección.

Para asegurarse de que el tráfico de internet vaya a las interfaces del plano de datos en lugar de a la interfaz de gestión, use la CLI de Alibaba para adjuntar las ENIs no fiables untrust del cortafuegos VM-Series a su instancia de SLB.

©2024 Palo Alto Networks, Inc.

Debe instalar la interfaz de línea de comandos de Aliyun *para utilizar los siguientes comandos de la CLI.*

STEP 1 | Cree las VPC públicas y privadas para una configuración de sándwich del balanceador de carga e implemente los cortafuegos VM-Series.

Los pasos restantes son ejemplos de comandos de CLI que puede adaptar a su entorno.

STEP 2 | Crear el balanceador de carga.

```
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 | Añadir servidores backend.

Use la CLI para añadir interfaces una por una. El orden en el que añade las interfaces determina qué NIC recibe la interfaz.

```
aliyun slb AddBackendServers --LoadBalancerId lb-
******************mvz --BackendServers '[ { "ServerId":"eni-
******************bzw", "Type":"eni","Weight":"100" } ]'
```

STEP 4 | Cree una Escucha HTTP que realiza una comprobación de salud.

```
aliyun slb CreateLoadBalancerHTTPListener --LoadBalancerId lb-
******************mvz --ListenerPort 80 --StickySession on --
HealthCheck on --HealthCheckURI '/'
```

 ©2024 Palo Alto Networks, Inc.

Configuración de la HA activa/pasiva en Alibaba Cloud

El cortafuegos VM-Series en Alibaba Cloud ahora es compatible con implementaciones activas/pasivas de HA utilizando una nueva característica de Alibaba Cloud llamada HAVIP.

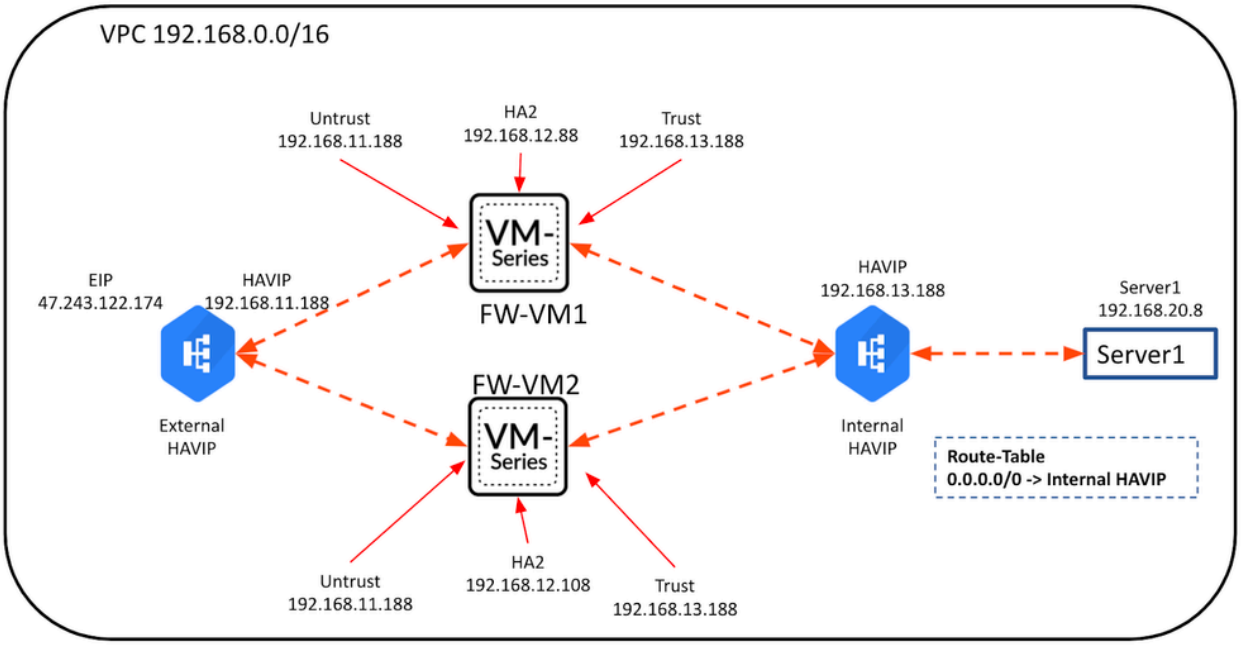
La HAVIP escucha los mensajes ARP/GARP enviados por los cortafuegos VM-Series para determinar qué interfaces de red pertenecen al cortafuegos VM-Series activo y, a continuación, reenvía tráfico a esas interfaces.

Arquitectura

La arquitectura de implementación de HAVIP consta de dos interfaces HAVIP y dos cortafuegos VM-Series que se configuran en modo de alta disponibilidad activo/en espera.

Uno de los HAVIP está configurado con una dirección IP pública (HAVIP externo). La interfaz de no confianza (Untrust) de cada cortafuegos VM-Series está enlazada a este HAVIP externo. El otro HAVIP (HAVIP interno) no tiene una dirección IP pública adjunta. La interfaz de confianza (Trust) de cada cortafuegos VM-Series está vinculada al HAVIP interno.

 ©2024 Palo Alto Networks, Inc.



En este ejemplo, el HAVIP externo se encuentra en la misma subred que las interfaces de no confianza, Untrust, mientras que el HAVIP interno está en la misma subred que las interfaces de confianza, Trust.

 ©2024 Palo Alto Networks, Inc.

- *La dirección HAVIP debe estar en la misma subred que las interfaces de red enlazadas a ella.*
- *Las subredes de Alibaba Cloud no pueden abarcar varias zonas, por lo que esta solución solo funcionará si ambos cortafuegos VM-Series están en la misma zona de disponibilidad.*

Implementar la HA activa/pasiva en Alibaba Cloud

Utilice los siguientes pasos para implementar la alta disponibilidad activa/pasiva en Alibaba Cloud:

- Crear HAVIP
- Enlazar una dirección IP elástica (EIP)
- Enlazar una instancia de ECS
- Configurar tabla de rutas
- Configurar el cortafuegos VM-Series.
- Probar el tráfico
- Pruebas de conmutación por error
- Tipos de instancias de CPU virtual (vCPU)

Crear HAVIP

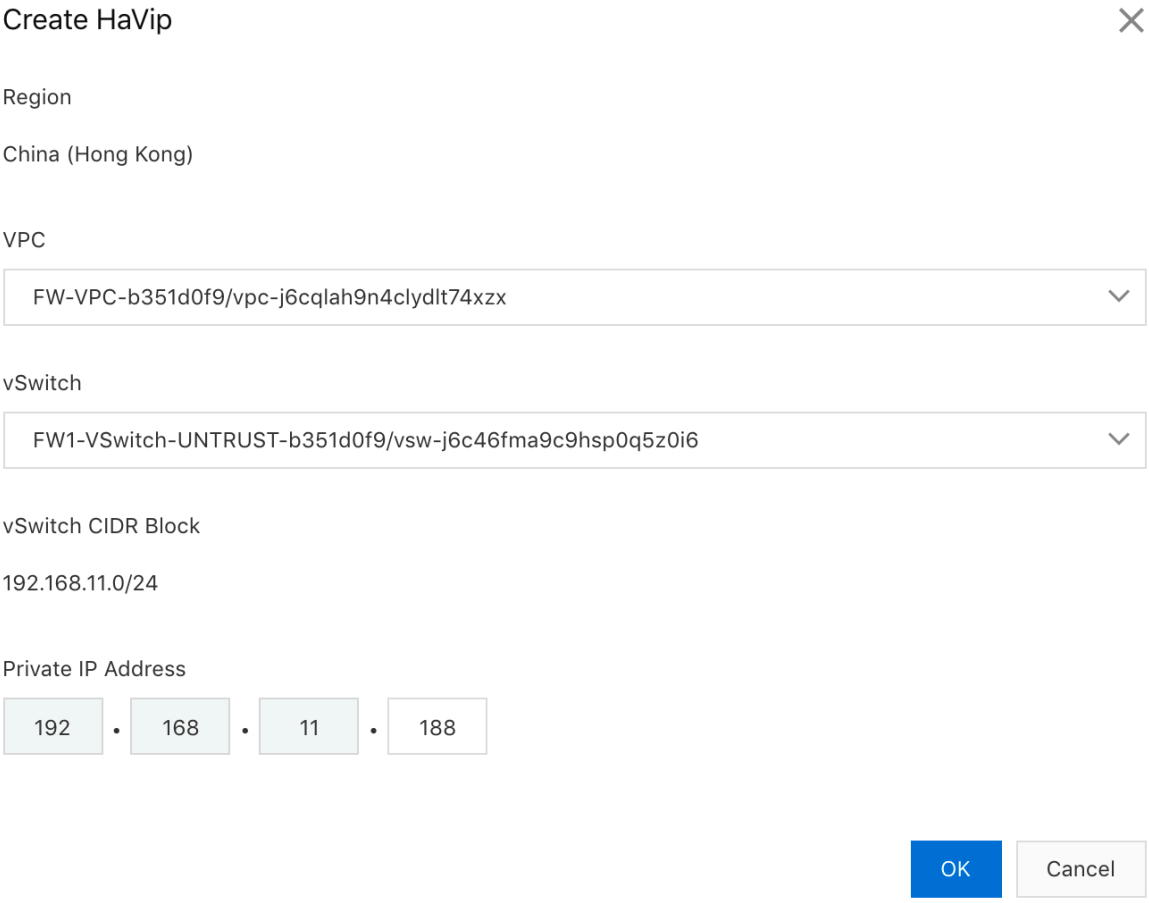
STEP 1 | Haga clic en **VPC** > **HAVIP** > **Create HAVIP (Crear HAVIP)** en su consola de Alibaba Cloud.

STEP 2 | Elija la **VPC** y el **vSwitch**.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Proporcione una dirección IP privada para la HAVIP y haga clic en **OK** (Aceptar).

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

Enlazar una dirección IP elástica (EIP)

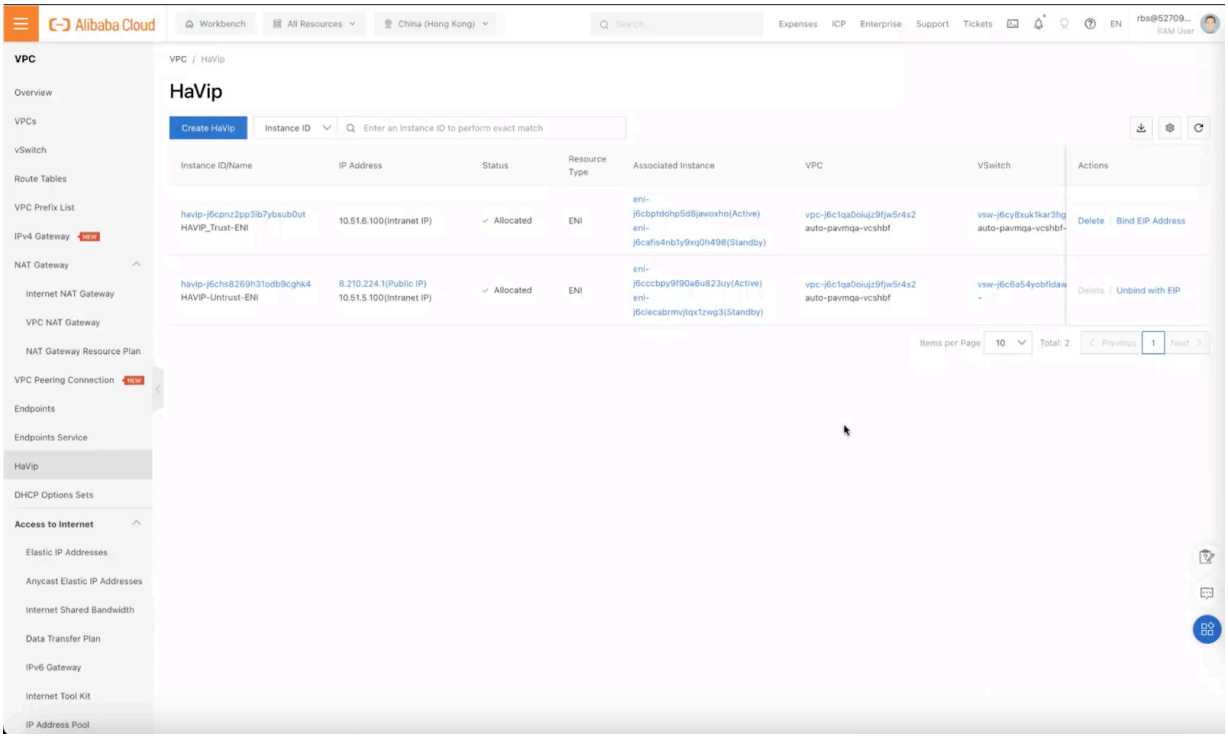
STEP 1 | Haga clic en la HAVIP que ha creado para introducir su configuración.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Cree una dirección IP elástica (EIP) y haga clic en **Enlazar**, para enlazar el EIP a la HAVIP.



 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

Enlazar una instancia de ECS

Para enlazar con una instancia, utilice la interfaz de red principal de la instancia. En el caso de los cortafuegos VM-Series, la interfaz de red principal es la interfaz de gestión.

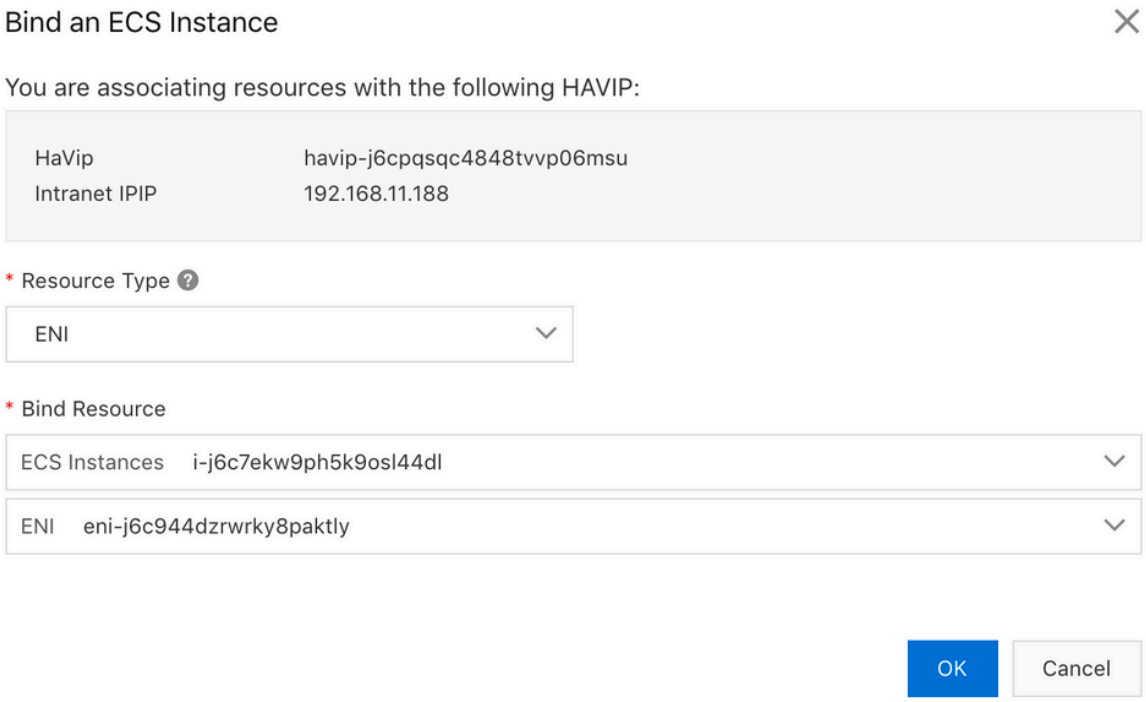
Para enlazar las interfaces de no confianza, Untrust, de los cortafuegos VM-Series a la HAVIP:

STEP 1 | Haga clic en el botón **Enlazar** en instancias de ECS.

STEP 2 | Seleccione **ENI** como tipo de recurso y, a continuación, elija la instancia y la ENI para enlazar a la HAVIP.

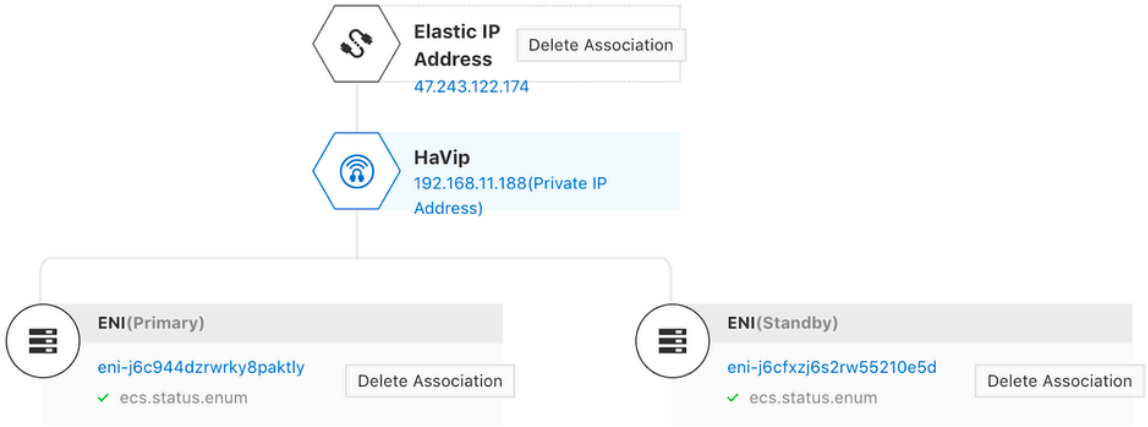
 ©2024 Palo Alto Networks, Inc.

STEP 3 | Repita el mismo procedimiento para la otra interfaz de no confianza, Untrust.



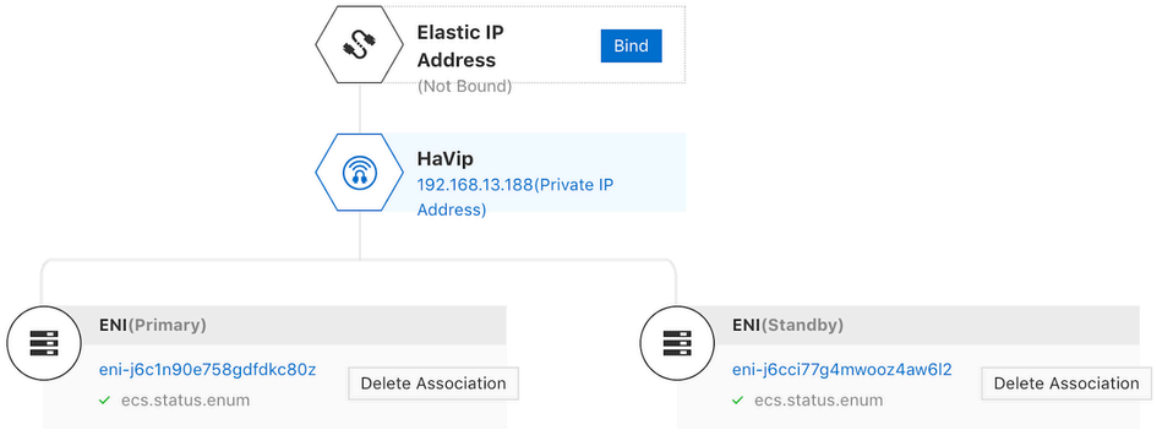
 ©2024 Palo Alto Networks, Inc.

Una vez que el EIP y ambas interfaces Untrust están enlazadas al HAVIP, puede encontrarlas en la página de configuración de HAVIP.



 ©2024 Palo Alto Networks, Inc.

STEP 4 | Repita el mismo procedimiento para crear la HAVIP interna. Para la HAVIP interna, no es necesario vincular ningún EIP a ella. La configuración de la HAVIP interna debe ser similar a la imagen a continuación:



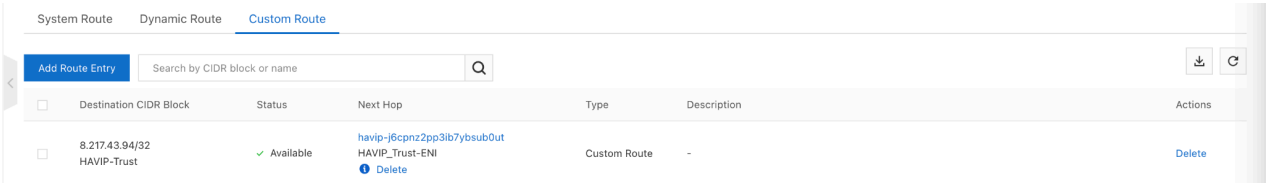
Configurar tabla de rutas

El tráfico de los servidores debe enrutarse a la HAVIP interna. Para lograr esto, se configura una ruta estática en la tabla de rutas asociada con la subred del servidor.

Haga clic en **VPC** > **Route Tables (Tablas de rutas)**.

Después de crear la tabla de rutas, añada una entrada de ruta personalizada para apuntar la ruta predeterminada a la HAVIP interna y asocie esta tabla de rutas con el vSwitch del servidor.

 ©2024 Palo Alto Networks, Inc.



Configurar el cortafuegos VM-Series.

Los cortafuegos VM-Series se configuran en modo de alta disponibilidad activo/pasivo con la sincronización de configuración habilitada.

STEP 1 | Configure las interfaces de no confianza, Untrust, y confianza, Trust, con direcciones IP estáticas. La interfaz de no confianza se configura con la dirección IP privada de la HAVIP externa, mientras que la interfaz de confianza se configura con la dirección IP privada de la HAVIP interna. A medida que se habilita la sincronización de configuración, cuando se produce una conmutación por error, el

 ©2024 Palo Alto Networks, Inc.

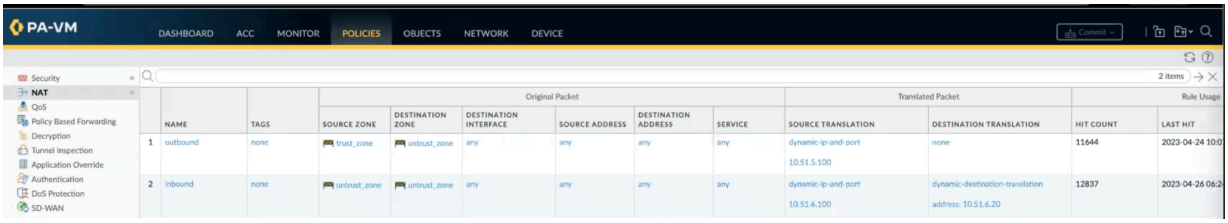
cortafuegos VM-Series recién activo usará el mismo conjunto de direcciones IP para sus interfaces de confianza y no confianza.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS
ethernet1/1	Layer3			192.168.11.188/24
ethernet1/2	HA			none
ethernet1/3	Layer3			192.168.13.188/24

STEP 2 | Asegúrese de que la tabla de rutas del cortafuegos VM-Series incluya la ruta predeterminada a través de la interfaz de no confianza y una ruta a la subred del servidor a través de la interfaz de confianza.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Configure las reglas NAT para el tráfico entrante y saliente.



Para el tráfico entrante, la regla NAT debe tener una coincidencia de dirección de destino en la dirección IP privada de la HAVIP externa. Esta dirección de destino se traducirá a la dirección del servidor web mediante la regla NAT.

Para el tráfico de salida, la regla SNAT coincidirá con las direcciones de origen de los servidores. A continuación, la dirección de origen será SNAT a la dirección IP privada de la HAVIP externa. La HAVIP externa, a su vez, hace SNAT y envía el tráfico a la dirección IP pública de la HAVIP externa.

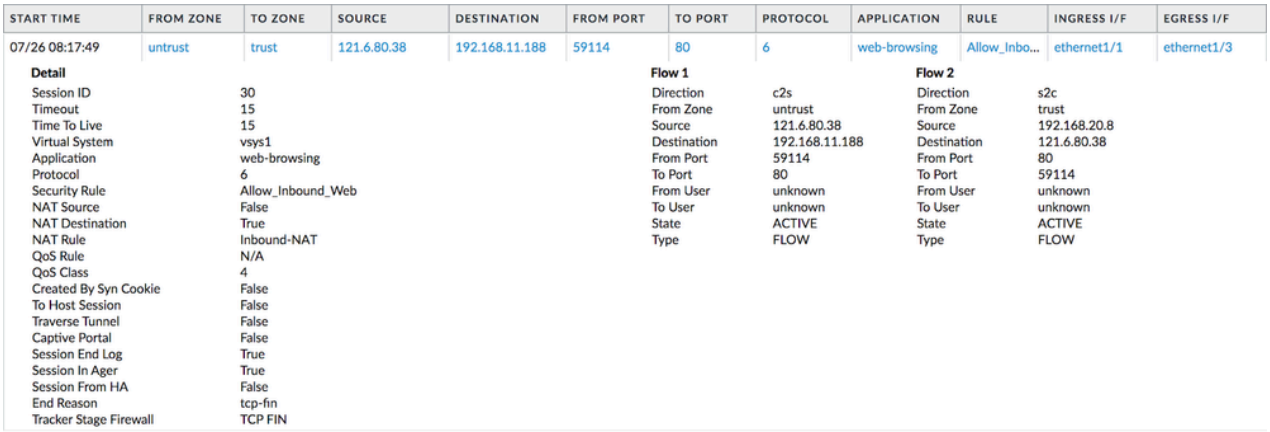
Probar el tráfico

Probando el tráfico entrante

Se puede acceder al servidor web a través de la dirección IP pública de la HAVIP externa. En los siguientes diagramas observe que el cliente pueda acceder con éxito al servidor web, así como a la dirección IP pública del cliente.

 ©2024 Palo Alto Networks, Inc.





START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PROTOCOL	APPLICATION	RULE	INGRESS I/F	EGRESS I/F
07/26 08:17:49	untrust	trust	121.6.80.38	192.168.11.188	59114	80	6	web-browsing	Allow_Inbo...	ethernet1/1	ethernet1/3

Detail	
Session ID	30
Timeout	15
Time To Live	15
Virtual System	vsys1
Application	web-browsing
Protocol	6
Security Rule	Allow_Inbound_Web
NAT Source	False
NAT Destination	True
NAT Rule	Inbound-NAT
QoS Rule	N/A
QoS Class	4
Created By Syn Cookie	False
To Host Session	False
Traverse Tunnel	False
Captive Portal	False
Session End Log	True
Session In Ager	True
Session From HA	False
End Reason	tcp-fin
Tracker Stage Firewall	TCP FIN

Flow 1	
Direction	c2s
From Zone	untrust
Source	121.6.80.38
Destination	192.168.11.188
From Port	59114
To Port	80
From User	unknown
To User	unknown
State	ACTIVE
Type	FLOW

Flow 2	
Direction	s2c
From Zone	trust
Source	192.168.20.8
Destination	121.6.80.38
From Port	80
To Port	59114
From User	unknown
To User	unknown
State	ACTIVE
Type	FLOW

 ©2024 Palo Alto Networks, Inc.

```
root@linux-server1:/var/log/apache2#
root@linux-server1:/var/log/apache2# tail access.log
121.6.80.38 - - [26/Jul/2021:16:17:58 +0800] "GET / HTTP/1.1" 200 3476 "-"
eWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
121.6.80.38 - - [26/Jul/2021:16:17:58 +0800] "GET / HTTP/1.1" 200 3476 "-"
eWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
121.6.80.38 - - [26/Jul/2021:16:17:58 +0800] "GET / HTTP/1.1" 200 3476 "-"
eWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36"
```

Probando el tráfico saliente

Al acceder a Internet desde el servidor, se detecta que la dirección IP de origen utilizada es la de la HAVIP externa.

```
root@linux-server1:~#
root@linux-server1:~# curl ip.42.pl/short
47.243.122.174root@linux-server1:~#
root@linux-server1:~#
```

 ©2024 Palo Alto Networks, Inc.

START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PROTOCOL	APPLICATION	RULE	INGRESS I/F	EGRESS I/F
07/26 08:29:54	trust	untrust	192.168.20.8	79.98.145.42	48632	80	6	web-browsing	Allow-Outbound	ethernet1/3	ethernet1/1

Detail	
Session ID	39
Timeout	15
Time To Live	3
Virtual System	vsys1
Application	web-browsing
Protocol	6
Security Rule	Allow-Outbound
NAT Source	True
NAT Destination	False
NAT Rule	Outbound-SNAT
QoS Rule	N/A
QoS Class	4
Created By Syn Cookie	False
To Host Session	False
Traverse Tunnel	False
Captive Portal	False
Session End Log	True
Session In Ager	True
Session From HA	False
End Reason	tcp-fin
Tracker Stage Firewall	TCP FIN

Flow 1	
Direction	c2s
From Zone	trust
Source	192.168.20.8
Destination	79.98.145.42
From Port	48632
To Port	80
From User	unknown
To User	unknown
State	ACTIVE
Type	FLOW

Flow 2	
Direction	s2c
From Zone	untrust
Source	79.98.145.42
Destination	192.168.11.188
From Port	80
To Port	10742
From User	unknown
To User	unknown
State	ACTIVE
Type	FLOW

Pruebas de conmutación por error

Inicie una prueba de ping en el servidor. El cortafuegos activo VM-Series se suspende y el cortafuegos pasivo VM-Series se activa. A partir de la prueba de ping, podría haber alrededor de 11 caídas de ping antes de que se reanude el tráfico. Por lo tanto, el tiempo de conmutación por error es de alrededor de 11 segundos.

©2024 Palo Alto Networks, Inc.



Se pueden implementar dos cortafuegos VM-Series en Alibaba Cloud en modo HA activo/pasivo con HAVIP de Alibaba Cloud para proporcionar alta disponibilidad. Esto proporciona sincronización de sesión y configuración entre los dos cortafuegos VM-Series. Sin embargo, esto solo funciona en una única zona de disponibilidad.

Si se requiere un aumento de la capacidad, es necesario ampliar los cortafuegos VM-Series, por ejemplo, VM300 # VM500.

 ©2024 Palo Alto Networks, Inc.

Tipos de instancias de CPU virtual (vCPU)

Los cortafuegos VM-Series utilizados en las pruebas tienen cuatro interfaces de red: Gestión, Untrust, trust y HA2. En la mayoría de los Tipos de instancias de Alibaba Cloud, los 4 tipos de instancia de vCPU proporcionan tres interfaces de red. Los 8 tipos de instancia de vCPU y superiores proporcionan cuatro o más interfaces de red.

Instance type	vCPUs	Memory (GiB)	Bandwidth (Gbit/s)	Packet forwarding rate (pps)	NIC queues	ENIs	Private IP addresses per ENI
ecs.g5.large	2	8	1	300,000	2	2	6
ecs.g5.xlarge	4	16	1.5	500,000	2	3	10
ecs.g5.2xlarge	8	32	2.5	800,000	2	4	10

Si es necesario utilizar 4 tipos de instancias de vCPU, los cortafuegos VM-Series deben implementarse en modo de un brazo, ya que solo puede haber 3 interfaces de red conectadas a cada cortafuegos. El tráfico entrante y saliente atravesará la misma interfaz de datos.

©2024 Palo Alto Networks, Inc.

Configuración de un cortafuegos en Cisco ACI

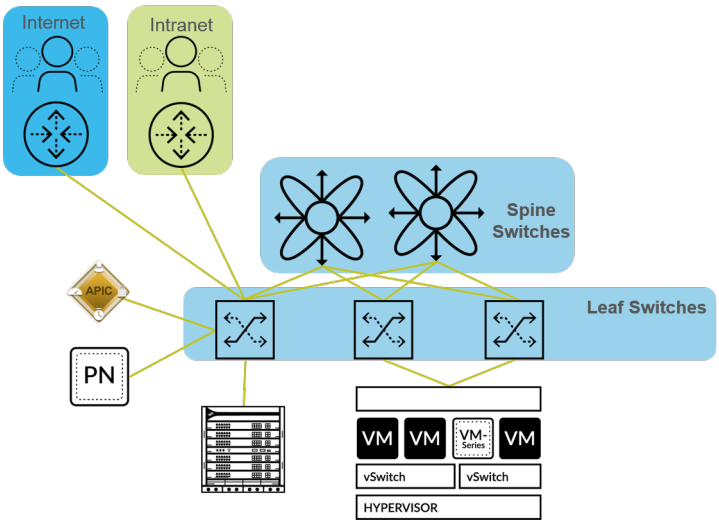
Palo Alto Networks se integra como un servicio con la Infraestructura centrada en aplicaciones (ACI) de Cisco. ACI es una solución de red definida por software (software-defined networking, SDN) para implementar fácilmente nuevas cargas de trabajo y servicios de red. Cuando usa un controlador SDN llamado Controlador de infraestructura de políticas de aplicaciones de Cisco (APIC), usted implementa el servicio de cortafuegos entre los grupos de endpoints (EPG). Los EPG actúan como un contenedor para aplicaciones o niveles de aplicación. Cuando coloca un cortafuegos entre los EPG, la política de seguridad configurada en el cortafuegos asegura el tráfico entre los EPG. El APIC proporciona un único panel de cristal para gestionar la topología de red, las políticas de red y la conectividad para todo el centro de datos y admite la inserción de dispositivos L4 - L7, como un cortafuegos VM-Series o basado en hardware. Panorama es necesario para la gestión de seguridad centralizada.

- Integración del cortafuegos de Palo Alto Networks con Cisco ACI
- Preparación de su entorno ACI para la integración
- Integre el cortafuegos con Cisco ACI en modo de política de red
- Supervisión de los endpoints en Cisco ACI

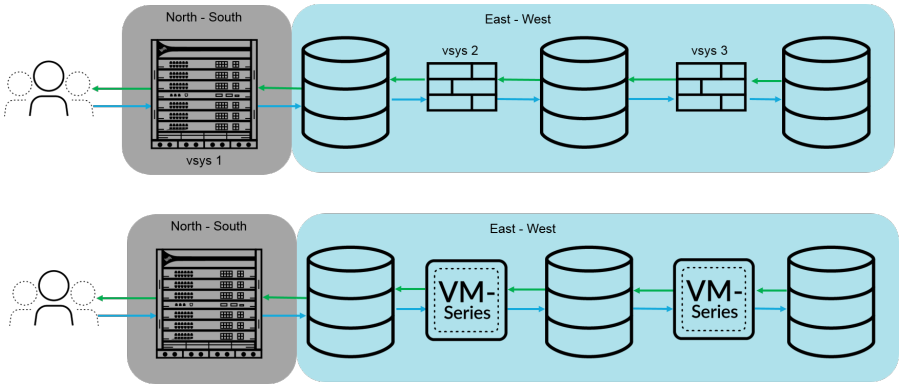
Integración del cortafuegos de Palo Alto Networks con Cisco ACI

La integración de Palo Alto Networks con Cisco ACI le permite insertar un cortafuegos entre los EPG como un servicio de Capa 4 a Capa 7. El cortafuegos luego asegura el tráfico horizontal entre los niveles de aplicación dentro de esos EPG o el tráfico vertical entre los usuarios y las aplicaciones.

La figura siguiente muestra un ejemplo de una implementación física de ACI que incluye cortafuegos integrados de Palo Alto Networks. Todas las entidades en la estructura ACI están conectadas a conmutadores Leaf y estos están conectados a conmutadores Spine más grandes. A medida que los usuarios acceden a la aplicación, la ACI fabric mueve el tráfico al destino correcto. Para asegurar el tráfico entre los niveles de aplicación, el administrador de red inserta los cortafuegos de Palo Alto Networks como servicios L4 a L7 entre cada EPG y crea un gráfico de servicio para definir qué servicios proporciona el dispositivo L4 a L7.



Una vez implementados los servicios de cortafuegos, el tráfico fluye de forma lógica tal y como se muestra a continuación. Tráfico desde y hacia los usuarios finales y cada nivel en la aplicación, independientemente de dónde o cómo cada entidad esté físicamente conectada a la red.



Cuando el cortafuegos está integrado con Cisco ACI, el tráfico se envía al cortafuegos con un redireccionamiento basado en políticas (PBR). Además, la configuración del cortafuegos y la configuración del APIC son completamente independientes. El modo de política de red no depende de

 ©2024 Palo Alto Networks, Inc.

ninguna otra integración de configuración entre el cortafuegos y el APIC, por lo que proporciona una mayor flexibilidad de configuración e implementación del cortafuegos.

Para el tráfico este-oeste, defina un dominio de puente y una subred en la estructura ACI para el cortafuegos. Configure los contratos entre los EPG que envían tráfico al cortafuegos utilizando un PBR. El PBR reenvía el tráfico al cortafuegos según la política que contiene la dirección IP y MAC del cortafuegos. Las interfaces del cortafuegos están siempre en modo Capa 3 y el tráfico se recibe y se enruta de nuevo a la estructura ACI. Puede configurar interfaces separadas para las conexiones de consumidores y proveedores o una interfaz única para el tráfico de ingreso y egreso. El procedimiento en este documento utiliza una sola interfaz porque simplifica la integración; no es necesario configurar tantas interfaces, direcciones IP o VLAN. Sin embargo, cuando usa una sola interfaz, no puede usar la información de la zona para definir la política de seguridad y debe modificar la política de intrazona predeterminada en el cortafuegos para rechazar el tráfico.

Para el tráfico norte-sur, debe utilizar una política dedicada llamada L3Out. Una L3Out contiene la información necesaria para que el inquilino se conecte a dispositivos de enrutamiento externos y acceda a redes externas. Las conexiones L3Out contienen una red externa EPG que representa las redes accesibles a través de la política L3Out. Al igual que L3Out puede agrupar todas las redes externas en un solo EPG, usted puede usar un objeto vzAny de ACI para representar todas los EPG en un VRF. El uso de un objeto vzAny implica la aplicación del contrato de tráfico saliente porque cada vez que se añade un nuevo EPG al VRF, el contrato se aplica automáticamente. En este escenario, la red externa proporciona el contrato y el objeto vzAny (todos los EPG internos) lo consume.

La siguiente sección proporciona detalles adicionales sobre los componentes y conceptos que conforman la integración entre el cortafuegos de nueva generación y Cisco ACI.

- Plantillas de gráficos de servicio
- Implementaciones de contexto múltiple

Plantillas de gráficos de servicio

Los cortafuegos se implementan en Cisco ACI a través de gráficos de servicio. Un gráfico de servicio le permite integrar los dispositivos de Capa 4 - Capa 7, como un cortafuegos, en el flujo de tráfico sin la necesidad de que el dispositivo L4-L7 sea la puerta de enlace predeterminada para los servidores en la estructura ACI.

Los cortafuegos están representados en la estructura ACI como un dispositivo L4-L7 que se configura en el APIC como un grupo de dispositivos. Un solo cortafuegos o dos cortafuegos implementados como un par de alta disponibilidad (HA) se configuran como un clúster de dispositivos. Cada clúster de dispositivos tiene una o más interfaces lógicas que describen la información de la interfaz del clúster de dispositivos y asignan la ruta del cortafuegos miembro con una VLAN del dominio físico o del monitor de máquina virtual (VMM).

Las plantillas de gráficos de servicio definen el clúster de dispositivos del cortafuegos que inserte en el flujo de tráfico entre los EPG. Además, la plantilla de gráficos de servicio define la forma en que se integra el cortafuegos y las interfaces lógicas que se asignan a los EPG del consumidor y proveedor. Después de crear su plantilla de gráficos de servicio, esta se asigna a los EPG y contratos. Debido a que la plantilla del gráficos de servicio no está vinculada a un EPG o contrato específicos, puede reutilizarla entre varios EPG. El APIC luego implementa la plantilla de gráficos de servicio conectándola al dominio de puente entre los EPG.

 ©2024 Palo Alto Networks, Inc.

Implementaciones de contexto múltiple

La integración de Cisco ACI admite cortafuegos físicos divididos en contextos administrados por ACI como cortafuegos individuales. En el cortafuegos, estos contextos son los sistemas virtuales (vsys) en los cortafuegos y cada cortafuegos tiene licencia para admitir un cierto número de instancias vsys. Al implementar un cortafuegos multi-vsys en ACI, debe configurar un administrador de chasis en el inquilino y asignarlo al servicio de cortafuegos.

©2024 Palo Alto Networks, Inc.

Preparación de su entorno ACI para la integración

Antes de que pueda integrar el cortafuegos con un paquete de dispositivos, debe completar los siguientes pasos para preparar su entorno Cisco ACI.

STEP 1 | Implemente Panorama.

STEP 2 | Implemente el cortafuegos.

- Cortafuegos físico: Conecte el puerto de gestión fuera de banda del cortafuegos al puerto de un conmutador leaf y conecte al conmutador al menos una interfaz de datos de cortafuegos. Las interfaces de cortafuegos en un cortafuegos físico se configuran con VLAN para garantizar la conectividad a las redes correctas. Implemente el cortafuegos de acuerdo con la guía de instalación específica de la plataforma.
- Cortafuegos VM-Series: Al configurar el hardware virtual para el cortafuegos VM-Series, establezca el grupo de puertos para la interfaz de gestión. Cada cortafuegos VM-Series conectado a la red requiere su propia NIC virtual. Implemente el cortafuegos VM-Series basado en su hipervisor.

STEP 3 | Configure la dirección IP de gestión en cada cortafuegos y Panorama.

Realice la configuración inicial en:

- Cortafuegos basado en hardware
- Cortafuegos VM-Series
- Panorama

STEP 4 | Añada los cortafuegos a Panorama como dispositivo gestionado.

STEP 5 | Instale licencias de funciones en su(s) cortafuegos.

- Registre y active licencias en su cortafuegos físico.
- Regístrese y Activar licencias del modelo VM-Series en su cortafuegos VM-Series.
- Gestione licencias de cortafuegos usando Panorama.

STEP 6 | Establezca ACI fabric de Cisco y la gestión de la conectividad.

Como parte de esta configuración, cree un dominio físico y un espacio de nombres VLAN. Asegúrese de que las interfaces de datos de cualquier cortafuegos físico sean parte del dominio físico.

STEP 7 | Cree un perfil de dominio VMM de la ACI de Cisco.

Si está utilizando máquinas virtuales o el cortafuegos VM-Series, cree un perfil de dominio de monitor de máquina virtual (VMM) para el entorno de VMware vSphere. El dominio VMM especifica la política de conectividad entre vSphere y ACI fabric.

 ©2024 Palo Alto Networks, Inc.

Integre el cortafuegos con Cisco ACI en modo de política de red

En el modo de política de red, integre un par de cortafuegos en alta disponibilidad (HA) en el tráfico este-oeste o norte-sur mediante el uso de un redireccionamiento basado en políticas a una única interfaz lógica de HA. El cortafuegos y la estructura ACI se configuran por separado y los objetos de dirección en el cortafuegos se asignan a los EPG en la estructura ACI.

Puede usar el modo de política de red para implementar un cortafuegos de Palo Alto Networks para proteger el tráfico este-oeste o norte-sur.

- Implementación del cortafuegos para asegurar el tráfico este-oeste en el modo de política de red
- Implementación del cortafuegos para asegurar el tráfico norte-sur en el modo de política de red

Implementación del cortafuegos para asegurar el tráfico este-oeste en el modo de política de red

El siguiente procedimiento describe cómo implementar un cortafuegos de Palo Alto Networks para proteger el tráfico este-oeste en su entorno de Cisco ACI usando un modo no gestionado con redireccionamiento basado en políticas. Este procedimiento asume que ha completado lo siguiente:

- Los cortafuegos están operativos y conectados a un conmutador leaf en su entorno Cisco ACI. Además, la APIC debe poder acceder a la interfaz de gestión de cada cortafuegos.
- Los cortafuegos se implementan en modo HA activo/pasivo. Este procedimiento no cubre la configuración de la red de alta disponibilidad y asume que lo ha completado de antemano.

Para proteger el tráfico este-oeste, defina un dominio de puente y una subred en la estructura ACI para el cortafuegos. Configure los contratos entre los EPG que envían tráfico al cortafuegos utilizando un PBR. El PBR reenvía el tráfico al cortafuegos según la política que contiene la dirección IP y MAC del cortafuegos. Las interfaces del cortafuegos están siempre en modo Capa 3 y el tráfico se recibe y se enruta de nuevo a la estructura ACI. Puede configurar interfaces separadas para las conexiones de consumidores y proveedores o una interfaz única para el tráfico de ingreso y egreso. El procedimiento en este documento utiliza una sola interfaz porque simplifica la integración; no es necesario configurar tantas interfaces, direcciones IP o VLAN. Sin embargo, cuando usa una sola interfaz, no puede usar la información de la zona para definir la política de seguridad y debe modificar la política de intrazona predeterminada en el cortafuegos para rechazar el tráfico.

Este procedimiento implementa el cortafuegos en modo de un solo brazo. En el modo de un solo brazo, el tráfico entra y sale del cortafuegos a través de una única interfaz. Esta interfaz de cortafuegos común se usa para las interfaces de consumidor y proveedor en la plantilla de gráfico de servicio. El uso de una sola interfaz simplifica la integración con el cortafuegos al reducir el número de direcciones IP, VLAN e interfaces que debe configurar. Sin embargo, un modelo de implementación de un solo brazo es intrazona, por lo que no puede usar la información de zona para definir la política de seguridad.

En el cortafuegos:

- Creación de un enrutador virtual y zona de seguridad
- Configuración de las interfaces de red
- Configure una ruta estática predeterminada

 ©2024 Palo Alto Networks, Inc.

- Creación de objetos de dirección para los EPG
- Creación de reglas de política de seguridad

En el APIC de Cisco:

- Cree un conjunto y dominio de VLAN
- Configure una política de interfaz para LLDP y LACP para el tráfico este-oeste
- Establecimiento de la conexión entre el cortafuegos y la estructura ACI
- Creación de un VRF y dominio de puente
- Cree un dispositivo L4-L7
- Creación de un redireccionamiento basado en política
- Cree e implemente una plantilla de gráfico de servicio

Creación de un enrutador virtual y zona de seguridad

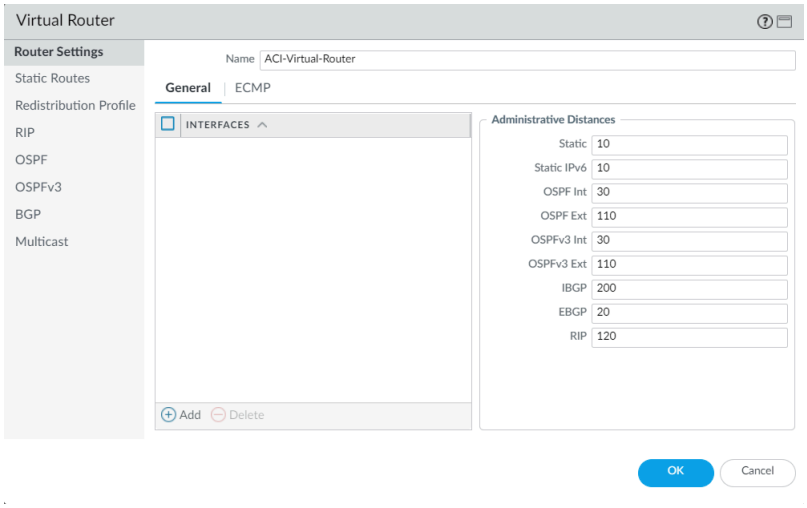
Configure un enrutador virtual y una zona en el cortafuegos para cada VRF en el inquilino.

STEP 1 | Inicie sesión en el cortafuegos.

STEP 2 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y haga clic en **Add (Añadir)**.

STEP 3 | Dé al enrutador virtual un **Name (Nombre)** descriptivo.

STEP 4 | Haga clic en **OK (Aceptar)**.



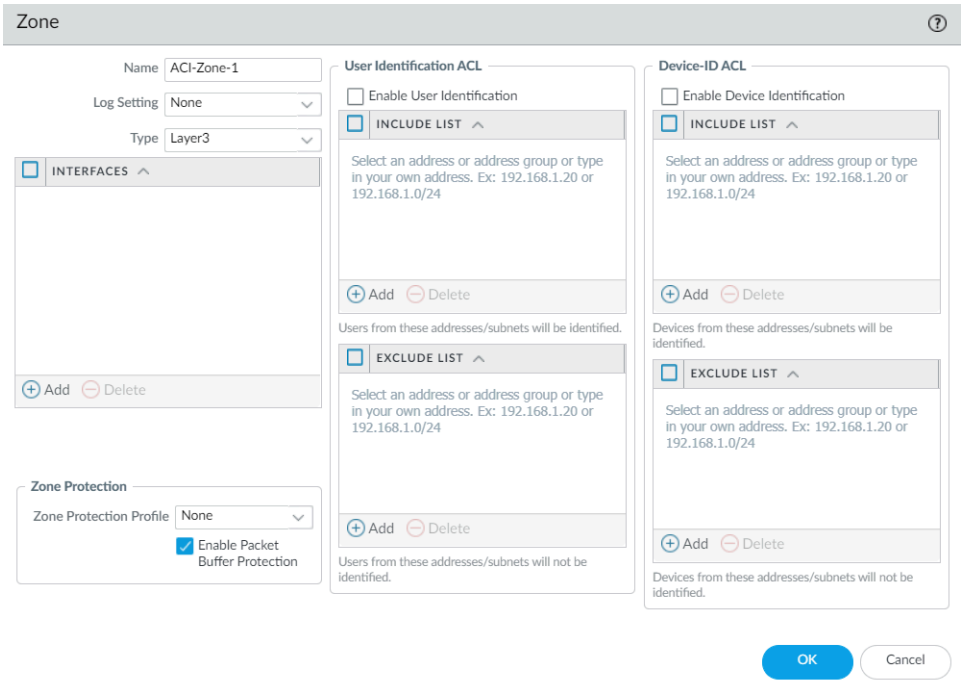
STEP 5 | Seleccione **Network (Red)** > **Zones (Zonas)** y haga clic en **Add (Añadir)**.

STEP 6 | Dé a la zona un **Name (Nombre)** descriptivo.

STEP 7 | Seleccione Capa 3 de la lista desplegable **Type (Tipo)**.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | Haga clic en **OK (Aceptar)**.



STEP 9 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

Configuración de las interfaces de red

Configure las interfaces Ethernet que conectan el cortafuegos a los conmutadores Leaf de ACI. El número de ID de VLAN utilizado en esta configuración debe ser un miembro del conjunto de VLAN asignado a los cortafuegos en ACI.

El cortafuegos VM-Series no es compatible con los grupos Ethernet de agregación.

STEP 1 | Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y haga clic en **Add Aggregate Group (Añadir grupo de agregación)**.

STEP 2 | Introduzca un número para el grupo de agregación en el segundo campo **Interface Name (Nombre de la interfaz)**.

STEP 3 | Seleccione Layer 3 (Capa 3) del menú desplegable **Interface Type (Tipo de interfaz)**.

STEP 4 | Seleccione la pestaña **LACP** y haga clic en **Enable LACP (Habilitar LACP)**.

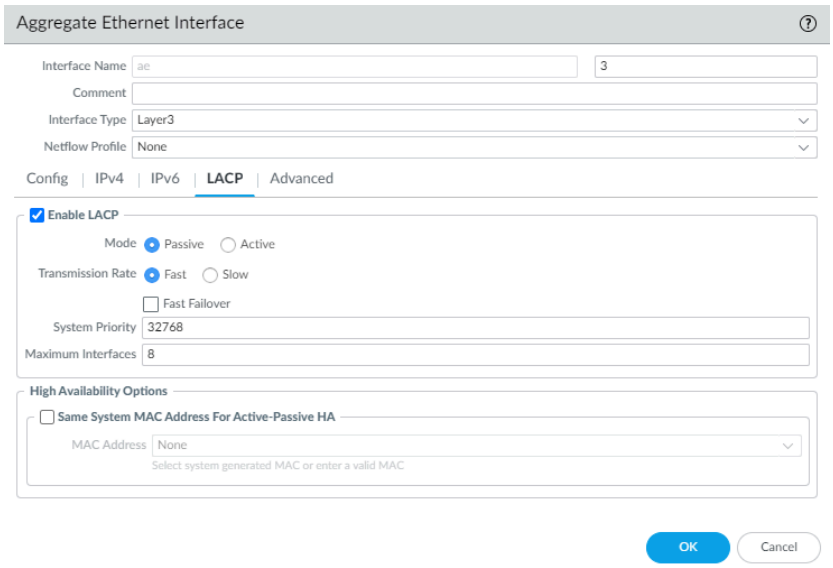
STEP 5 | Seleccione **Fast (Rápido)** como la **Transmission Rate (Velocidad de transmisión**.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | En Opciones de alta disponibilidad, seleccione **Enable in HA Passive State (Habilitar en estado pasivo HA)**.

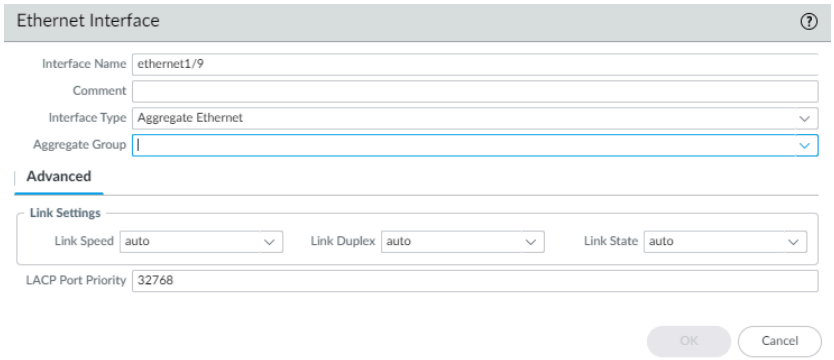
*No seleccione **Same System MAC Address for Active-Passive HA (Misma dirección MAC del sistema para modo activo-pasivo de HA)**. Esta opción hace que el par de cortafuegos aparezca como un solo dispositivo para el conmutador, por lo que el tráfico fluirá hacia ambos cortafuegos en lugar de solo el cortafuegos activo.*

STEP 7 | Haga clic en **OK (Aceptar)**.



STEP 8 | Haga clic en el nombre de una interfaz Ethernet para configurarla y añadirla al grupo de agregación.

1. Seleccione **Aggregate Ethernet (Ethernet de agregación)** en el menú desplegable Tipo de interfaz.
2. Seleccione la interfaz que definió en la configuración del grupo de Ethernet de agregación.
3. Haga clic en **OK (Aceptar)**.
4. Repita este paso para cada uno de los otros miembros de la interfaz del grupo de Ethernet de agregación.



 ©2024 Palo Alto Networks, Inc.

STEP 9 | Agregue una subinterfaz en la interfaz de Ethernet de agregación para el arrendatario y el VRF.

1. Seleccione la fila de su grupo de Ethernet de agregación y haga clic en **Add Subinterface (Añadir subinterfaz)**.
2. En el segundo campo de **Interface Name (Nombre de la interfaz)**, introduzca un sufijo numérico para identificar la subinterfaz.
3. En el campo **Tag (Etiqueta)**, introduzca la etiqueta VLAN de la subinterfaz.
4. Seleccione el enrutador virtual que configuró anteriormente desde el menú desplegable **Virtual Router (Enrutador virtual)**.
5. Seleccione la zona que configuró previamente del menú desplegable **Zone (Zona)**.
6. Seleccione la pestaña **IPv4**.
7. Seleccione el tipo **Static (Estático)**.
8. Haga clic en **Add (Añadir)** e introduzca la dirección IP de subinterfaz y la máscara de red en notación CIDR.
9. Haga clic en **OK (Aceptar)**.

Configure una ruta estática predeterminada

Configure una ruta estática predeterminada para dirigir el tráfico desde las subinterfaces Ethernet al enrutador de subred.

STEP 1 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y haga clic en el enrutador virtual que creó anteriormente en este procedimiento.

STEP 2 | Seleccione **Static Routes (Rutas estáticas)** > **IPv4** y haga clic en **Add (Añadir)**.

STEP 3 | Introduzca un **Name (Nombre)** descriptivo.

STEP 4 | Introduzca 0.0.0.0/0 en el campo **Destination (Destino)**.

STEP 5 | Desde la lista desplegable **Interface (Interfaz)**, seleccione el grupo de Ethernet de agregación que creó anteriormente en este procedimiento.

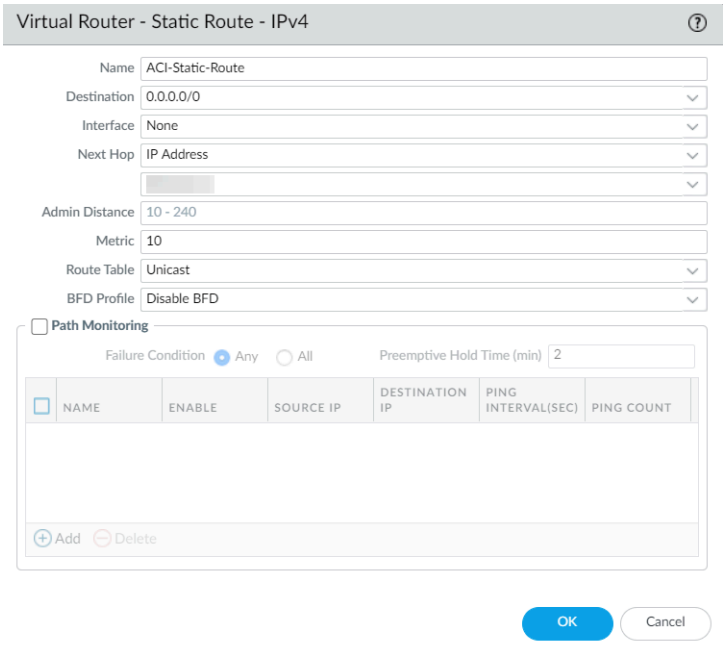
STEP 6 | Seleccione la dirección IP de la lista desplegable **Next Hop (Siguiente salto)** e introduzca la dirección IP del siguiente enrutador de salto.

STEP 7 | Haga clic en **OK (Aceptar)**.

STEP 8 | Haga clic en **OK (Aceptar)** nuevamente.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Haga clic en **Commit (Confirmar)** para compilar los cambios.



Creación de objetos de dirección para los EPG

Debe definir los objetos de dirección y asignarlos a grupos de endpoint (EPG) que se utilizarán en la política de seguridad. Los grupos de direcciones son la mejor manera de asignar grupos de seguridad a un grupo de servidores utilizando un rango de direcciones IP de endpoint. Cree un objeto de dirección para cada uno de sus EPG.

STEP 1 | Seleccione **Objects (Objetos)** > **Address (Dirección)** y haga clic en **Add (Añadir)**.

STEP 2 | Introduzca un nombre descriptivo para su objeto de dirección.

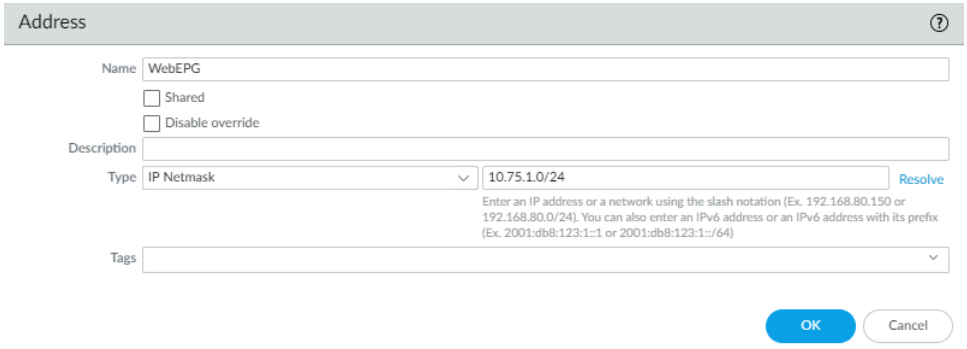
STEP 3 | Seleccione máscara de red IP de la lista desplegable **Type (Tipo)**.

STEP 4 | Introduzca la máscara de red IP.

STEP 5 | Haga clic en **OK (Aceptar)**.

STEP 6 | Repita este proceso para cada EPG.

STEP 7 | Haga clic en **Commit (Confirmar)** para compilar los cambios.



 ©2024 Palo Alto Networks, Inc.

Creación de reglas de política de seguridad

Cree reglas de política de seguridad para controlar el tráfico entre sus EPG. De manera predeterminada, el cortafuegos permite todo el tráfico de intrazona. Por lo tanto, debido a que los EPG están en la misma zona, todo entre esas EPG está permitido. Antes de crear nuevas reglas, cambiará la regla de intrazona predeterminada de "permitir" a "denegar".

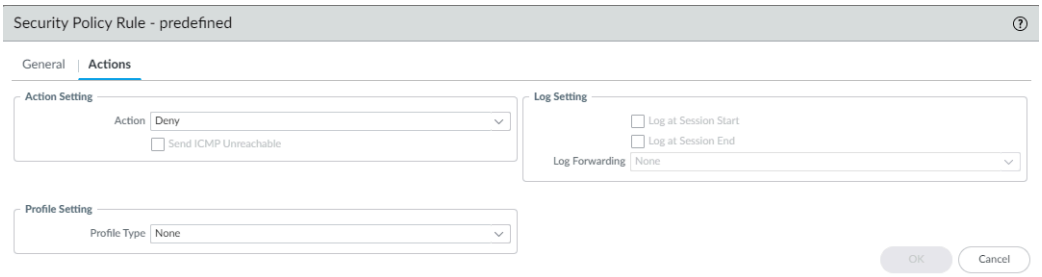
STEP 1 | Seleccione **Policies (Políticas)** > **Security (Seguridad)**.

STEP 2 | Haga clic en predeterminada intrazonal para resaltar la fila y haga clic en **Override (Anular)**.

STEP 3 | Seleccione la pestaña **Action (Acción)**.

STEP 4 | Seleccione "Denegar" en el menú desplegable **Action (Acción)**.

STEP 5 | Haga clic en **OK (Aceptar)**.



STEP 6 | Configure reglas de política de seguridad adicionales según sus necesidades, utilice los objetos de dirección y la zona que creó para su EPG.

Cree un conjunto y dominio de VLAN

Configure el grupo de VLAN que se utilizará para asignar las VLAN al cortafuegos cuando conecte interfaces a la infraestructura ACI para EPG. El grupo de VLAN del cortafuegos debe tener un rango de VLAN estático.

Configure una dominio dedicado para el cortafuegos. Se requiere un dominio para el cortafuegos para asignar las VLAN a los EPG. Cree un dominio físico para un cortafuegos físico y cree un dominio VMM para un cortafuegos VM-Series.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Cree un grupo de VLAN.

1. Inicie sesión en su APIC.
2. Seleccione **Fabric (Estructura)** > **Access Policies (Políticas de acceso)** > **Pools (Grupos)** > **VLAN**.
3. Haga clic con el botón derecho en **VLAN** y seleccione **Create VLAN Pool (Crear grupo de VLAN)**.
4. Introduzca un **Name (Nombre)** descriptivo para su grupo de VLAN.
5. Seleccione **Dynamic Allocation (Asignación dinámica)** para el modo de asignación.
6. Haga clic en el botón más (+) a la derecha de **Encap Blocks (Bloques endcap)**.
7. Introduzca su intervalo de VLAN en el campo **VLAN Range (Rango de VLAN)**.
8. Seleccione **Static Allocation (Asignación estática)** del menú desplegable Modo de asignación.
9. Haga clic en **OK (Aceptar)**.
10. Haga clic en **Submit (Enviar)** para enviar.

STEP 2 | (Solo cortafuegos físico) Crear un dominio físico.

1. Seleccione **Fabric (Estructura)** > **Access Policies (Políticas de acceso)** > **Physical and External Domains (Dominios físicos y externos)** > **Physical Domains (Dominios físicos)**.
2. Haga clic con el botón derecho en **Physical Domain (Dominio físico)** y seleccione **Create Bridge Domain (Crear dominio de puente)**.
3. Introduzca un **Name (Nombre)** descriptivo para su dominio físico.
4. Seleccione el grupo de VLAN que creó en el procedimiento anterior de la lista de grupos de VLAN.
5. Haga clic en **Submit (Enviar)** para enviar.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | (Solo cortafuegos VM-Series) Crear un dominio VMM.

1. Seleccione **Virtual Networking (Redes virtuales)** > **VMM Domains (Dominios VMM)** > **VMware**.
2. Haga clic con el botón derecho en **VMware** y seleccione **Create vCenter Domain (Crear dominio vCenter)**.
3. Introduzca un **Name (Nombre)** descriptivo para su dominio VMM.
4. Seleccione **VMware vSphere Distributed Switch Conmutador distribuido vSphere de VMware)** desde la lista desplegable **Virtual Switch (Conmutador virtual)**.
5. Seleccione **VLAN** de la lista desplegable **Encapsulation (Encapsulación)**.
6. Seleccione su grupo de VLAN de la lista desplegable **VLAN Pool (Grupo de VLAN)**.
7. Haga clic en el botón más (+) a la derecha de **vCenter Credentials (Credenciales de vCenter)**.
8. Introduzca un **Profile Name (Nombre de perfil)** descriptivo y la información de inicio de sesión de vCenter.
9. Haga clic en el botón más (+) a la derecha de **vCenter**.
10. Introduzca un **Name (Nombre)** descriptivo.
11. Seleccione vCenter de la lista desplegable Type (Tipo).
12. Introduzca su dirección IP de vCenter en **IP/Hostname (IP/nombre de host)**.
13. Seleccione el perfil de credenciales de vCenter que acaba de crear en la lista desplegable **Associated Credential (Credencial asociada)**.
14. Haga clic en **Submit (Enviar)** para enviar.

Configure una política de interfaz para LLDP y LACP para el tráfico este-oeste

Cree una política que habilite LLDP y LACP en las interfaces de ACI que se conectan a su cortafuegos.

LLDP es necesario para que el reenvío funcione correctamente en el entorno ACI; ACI no implementa una interfaz de enrutador de subred en un conmutador Leaf a menos que detecte un endpoint en el conmutador que lo requiera. LLDP ayuda a determinar si una interfaz de enrutador de subred es necesaria.

LACP proporciona mayor resistencia y velocidad de recuperación en un fallo de enlace.

STEP 1 | Crear una política de interfaz LLDP.

1. Seleccione **Fabric (Tejido)** > **Access Policies (Políticas de acceso)** > **Interface Policies (Políticas de interfaz)** > **Policies (Políticas)** > **LLDP Interface (Interfaz LLDP)**.
2. Haga clic con el botón derecho en **LLDP Interface (Interfaz LLDP)** y seleccione **Create LLDP Interface Policy (Crear política de interfaz LLDP)**.
3. Introduzca un **Name (Nombre)** descriptivo para su política de interfaz LLDP.
4. Seleccione **Enabled (Habilitado)** para **Receive State (Estado de recepción)**.
5. Seleccione **Enabled (Habilitado)** para **Transmit State (Estado de transmisión)**.
6. Haga clic en **Submit (Enviar)** para enviar.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Cree una política de canal de puerto para habilitar LACP.

1. Seleccione **Fabric (tejido)** > **Access Policies (Políticas de acceso)** > **Interface Policies (Políticas de interfaz)** > **Policies (Políticas)** > **Port Channel (Canal de puerto)**.
2. Haga clic con el botón derecho en **Port Channel (Canal de puerto)** y seleccione **Create Port Channel Policy (Crear política de canal de puerto)**.
3. Introduzca un **Name (Nombre)** descriptivo para su política de canal de puerto.
4. Seleccione **LACP Active (LACP activo)** de la lista desplegable **Mode (Modo)**.
5. Haga clic en **Submit (Enviar)** para enviar.

Establecimiento de la conexión entre el cortafuegos y la estructura ACI

Conecte su cortafuegos al conmutador leaf a través de una conexión VPC utilizando la interfaz Ethernet (o el grupo de Ethernet de agregación) que configuró en su cortafuegos previamente en este procedimiento. Conecte la interfaz o interfaces a los mismos puertos en los conmutadores leaf.

STEP 1 | Seleccione **Fabric (Tejido)** > **Access Policies (Políticas de acceso)** > **Quick Start (Inicio rápido)**.

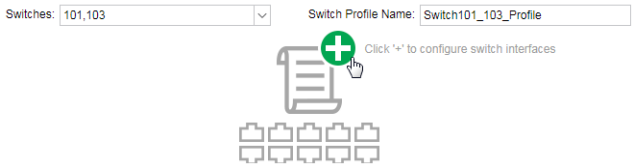
STEP 2 | Haga clic en **Configure an interface, PC, and VPC (Configurar una interfaz, PC y VPC)**.

STEP 3 | Haga clic en el signo más verde y blanco (+).



STEP 4 | Seleccione el interruptor leaf o los interruptores a los que está conectado su cortafuegos en la lista desplegable **Switches (Interruptores)**.

STEP 5 | Haga clic en el signo más verde y blanco (+).



STEP 6 | Seleccione VPC como el **Interface Type (Tipo de interfaz)**.

STEP 7 | En el campo **Interfaces**, introduzca el número de la interfaz que utiliza su cortafuegos para conectarse al interruptor leaf.

STEP 8 | Introduzca un nombre descriptivo en el campo **Interface Selector Name (Nombre del selector de interfaz)**.

STEP 9 | Seleccione **LLDP-Enabled (Habilitado para LLDP)** de la lista desplegable **LLDP Policy (Política de LLDP)**.

STEP 10 | Seleccione **LACP Active (LACP activo)** de la lista desplegable **Port Channel Policy (Política de canal de puerto)**.

 ©2024 Palo Alto Networks, Inc.

STEP 11 | Seleccione **Bare Metal (Sin sistema operativo)** para un cortafuegos físico o **ESX Hosts (Hosts ESX)** para la VM-Series de la lista desplegable **Attached Device Type (Tipo de dispositivo adjunto)**.

STEP 12 | Seleccione **Choose One (Seleccionar uno)** para **Domain (Dominio)**.

STEP 13 | Seleccione el dominio físico o el dominio VMM que creó anteriormente en este procedimiento de la lista desplegable **Domain (Dominio)**.

STEP 14 | Haga clic en **Save (Guardar)**.

STEP 15 | Haga clic en **Save (Guardar)** y luego en **Send (Enviar)**.

STEP 16 | Repita este procedimiento para el segundo cortafuegos en su equipo de HA.

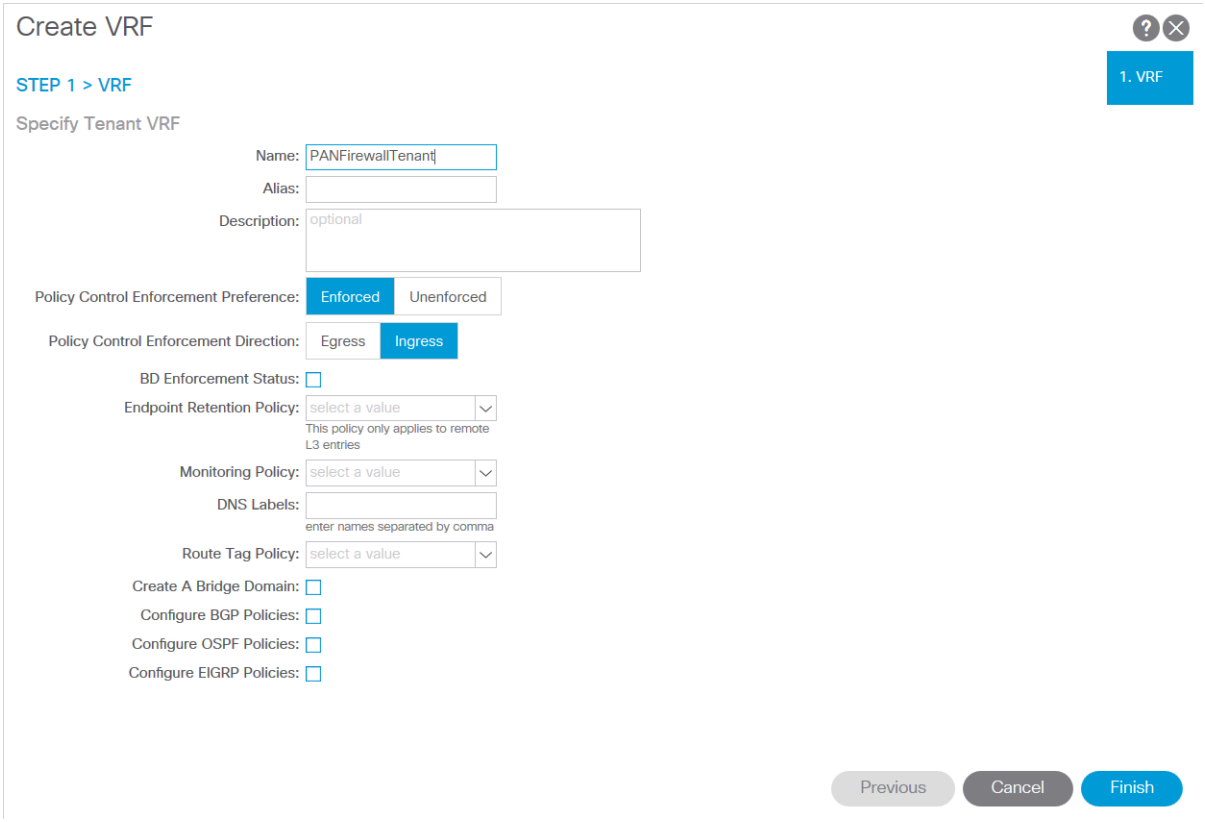
Creación de un VRF y dominio de puente

Un inquilino requiere un VRF para todos los dominios de puente y subredes. En este ejemplo, creará un VRF común y único para el cortafuegos y los endpoints. Luego, configure un dominio de puente dedicado para su cortafuegos y desactive el aprendizaje del plano de datos. Es necesario deshabilitar el aprendizaje del plano de datos para utilizar el redireccionamiento basado en políticas en un dominio puente.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Crear un VRF.

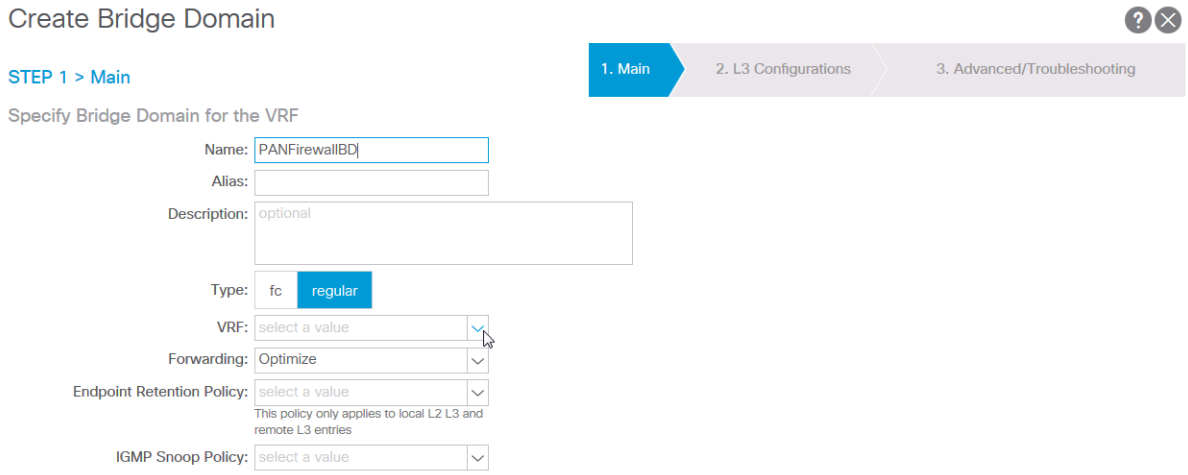
1. En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino.
2. Seleccione **Network (Red)** > **VRF**.
3. Haga clic con el botón derecho en **VRF** y seleccione **Create VRF (Crear VRF)**.
4. Introduzca un **Name (Nombre)** descriptivo para su VRF.
5. Quite la marca de la casilla de verificación **Create A Bridge Domain (Crear un dominio de puente)**.
6. Haga clic en **Finish (Finalizar)**.



 ©2024 Palo Alto Networks, Inc.

STEP 2 | Cree una dominio de puente para el cortafuegos.

1. En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino.
2. Seleccione **Networking (redes)** > **Bridge Domains (Dominio de puente)**.
3. Haga clic con el botón derecho en **Bridge Domains (Dominios de puente)** y seleccione **Create Bridge Domain (Crear dominio de puente)**.
4. Introduzca un **Name (Nombre)** descriptivo para su dominio de puente.
5. Seleccione el VRF que creó en el procedimiento anterior de la lista desplegable **VRF**.
6. Haga clic en **Next (Siguiente)**.



Cree un dispositivo L4-L7

Debe definir el cortafuegos como un dispositivo L4-L7 en el APIC para que ACI pueda insertarlo en el flujo de tráfico. Los dispositivos L4-L7 se configuran en el APIC como un clúster de dispositivos, que es una construcción que representa un solo cortafuegos o un par de HA de cortafuegos que actúa como un solo dispositivo. Los clústeres de dispositivos tienen una o más interfaces lógicas, que definen la ruta de los cortafuegos miembros con una VLAN de dominio físico.

STEP 1 | En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino.

STEP 2 | Seleccione **Services (Servicios)** > **L4-L7** > **Devices (Dispositivos)**.

STEP 3 | Haga clic con el botón derecho en **Devices (Dispositivos)** y seleccione **Create L4-L7 Device (Crear dispositivo L4-L7)**.

STEP 4 | Quite la marca de la casilla de verificación **Managed (Gestionado)**.

STEP 5 | Introduzca un **Name (Nombre)** descriptivo para su dispositivo L4-L7.

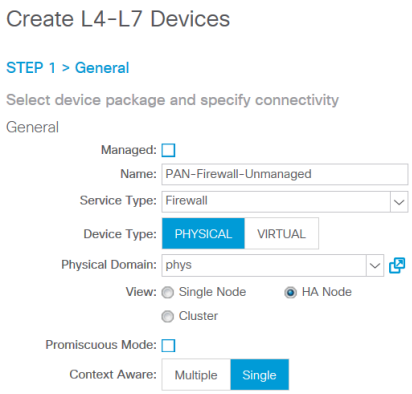
STEP 6 | Seleccione **Firewall (Cortafuegos)** en el menú desplegable **Service Type (Tipo de servicio)**.

STEP 7 | Seleccione **Physical (Físico)** para un cortafuegos físico o **Virtual** para un cortafuegos VM-Series de la lista desplegable **Device Type (Tipo de dispositivo)**.

STEP 8 | Seleccione el dominio físico o VMM que creó anteriormente desde la lista desplegable **Domain (Dominio)**.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Seleccione Nodo HA para **View (Ver)**.



STEP 10 | En **Device 1 (Dispositivo 1)**, haga clic en el icono más (+) a la derecha de **Device Interfaces (Interfaces de dispositivos)**.

STEP 11 | Introduzca un **Name (Nombre)** descriptivo para la interfaz.

STEP 12 | En **Path (Ruta)**, seleccione la ruta al cortafuegos principal en su par de HA.

STEP 13 | Haga clic en **Update (Actualizar)**.

STEP 14 | En **Device 2 (Dispositivo 2)**, haga clic en el icono más (+) a la derecha de **Device Interfaces (Interfaces de dispositivos)**.

STEP 15 | Introduzca un **Name (Nombre)** descriptivo para la interfaz.

STEP 16 | En **Path (Ruta)**, seleccione la ruta al cortafuegos secundario en su par de HA.

STEP 17 | Haga clic en **Update (Actualizar)**.

STEP 18 | En **Cluster (Clúster)**, haga clic en el icono más (+) a la derecha de **Cluster Interfaces (Interfaces de clúster)**.

STEP 19 | Introduzca un **Name (Nombre)** descriptivo para el clúster.

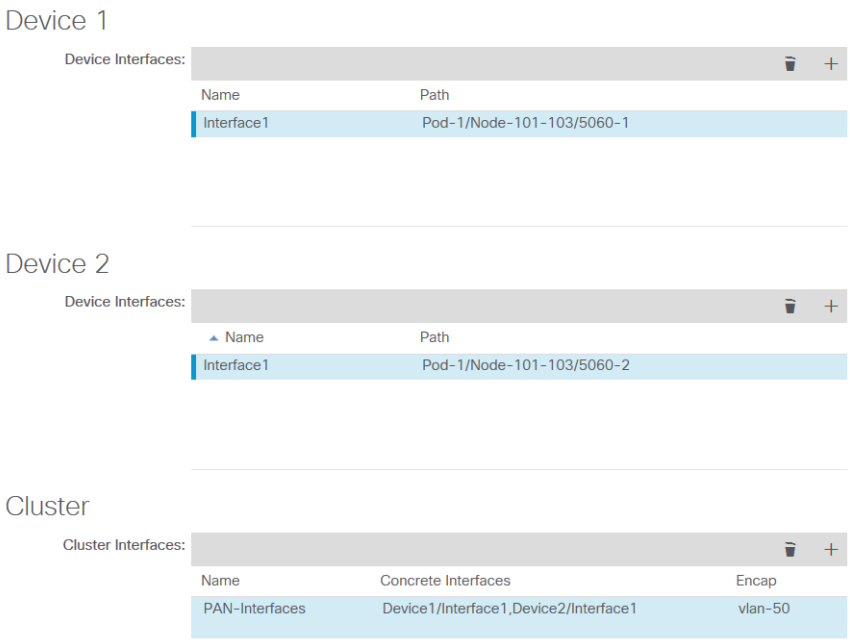
STEP 20 | Seleccione las dos interfaces que configuró arriba de la lista en **Concrete Interfaces (Interfaces concretas)**. El APIC requiere que configure dos interfaces. Sin embargo, debido a que solo hay una conexión entre el cortafuegos y la estructura ACI, solo se usa una de las interfaces.

STEP 21 | En **Encap**, introduzca una VLAN desde el conjunto de VLAN estática que creó anteriormente. El tráfico se redireccionará al cortafuegos en la VLAN asignada aquí.

STEP 22 | Haga clic en **Update (Actualizar)**.

 ©2024 Palo Alto Networks, Inc.

STEP 23 | Haga clic en **Finish (Finalizar)**.



Creación de un redireccionamiento basado en política

Configure el redireccionamiento basado en políticas que envía el tráfico entre sus EPG al cortafuegos. El redireccionamiento basado en políticas aprovecha la dirección MAC de la interfaz en el cortafuegos. Antes de configurar la configuración de PBR en el APIC, debe obtener la dirección MAC del cortafuegos.

STEP 1 | Obtenga la dirección MAC del cortafuegos.

1. Inicie sesión en la CLI del cortafuegos.
2. Utilice el comando **`show interface all`** para visualizar las direcciones MAC de sus interfaces configuradas.
3. Copie la dirección MAC de la interfaz que recibirá el tráfico redireccionado.

STEP 2 | Cree el redireccionamiento basado en políticas L4-L7.

1. Inicie sesión en el APIC.
2. En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino.
3. Seleccione **Policies (Políticas)** > **Protocol (Protocolo)** > **L4-L7 Policy Based Redirect (Redireccionamiento basado en políticas L4-L7)**.
4. Haga clic con el botón derecho en **L4-L7 Policy Based Redirect (Redireccionamiento basado en políticas L4-L7)** y seleccione **Create L4-L7 Policy Based Redirect (Crear redireccionamiento basado en políticas L4-L7)**.
5. Introduzca un **Name (Nombre)** descriptivo para su Redireccionamiento basado en políticas.
6. Haga clic en el icono más (+) a la derecha de **Destinations (Destinos)**.
7. En el campo **IP**, introduzca la dirección IP de la interfaz que recibirá el tráfico redireccionado.
8. En el campo **MAC**, introduzca la dirección MAC que copió de la CLI del cortafuegos.
9. Haga clic en **OK (Aceptar)**.
10. Haga clic en **Submit (Enviar)** para enviar.

 ©2024 Palo Alto Networks, Inc.

Cree e implemente una plantilla de gráfico de servicio

Cree una plantilla de gráfico de servicio que utilice el clúster de dispositivos que representa el cortafuegos en una integración de redireccionamiento basada en políticas. Después de crear el gráfico de servicio, debe aplicarlo a los EPG para proteger el tráfico. Un contrato y las reglas de filtro de contrato definen el tráfico que se puede reenviar al cortafuegos.

STEP 1 | Cree una plantilla de gráfico de servicio.

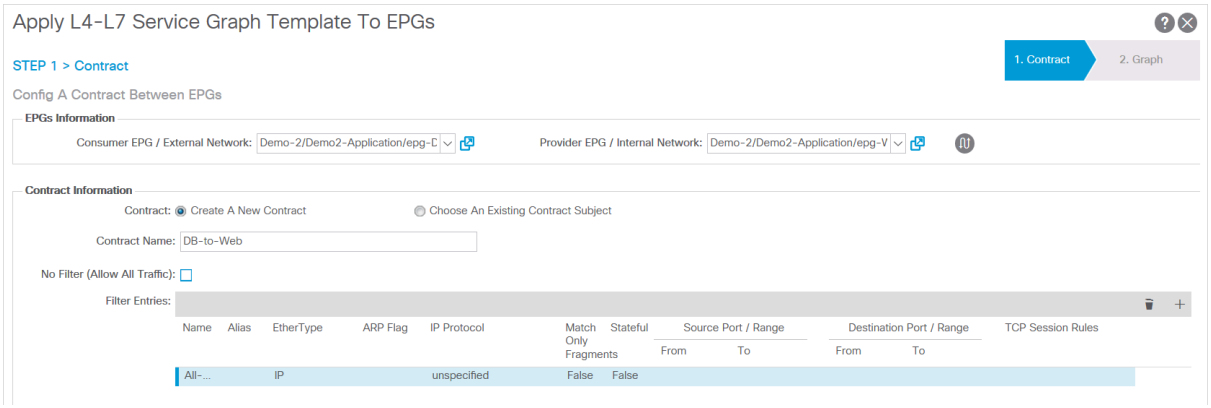
1. En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino.
2. Seleccione **Services (Servicios)** > **L4-L7** > **L4-L7 Service Graph Templates (Plantillas de gráficos de servicio L4-L7)**.
3. Haga clic con el botón derecho del ratón en **L4-L7 Service Graph Templates (Plantillas de gráficos de servicio L4-L7)** y seleccione **Create L4-L7 Service Graph Template (Crear plantilla de gráfico de servicio L4-L7)**.
4. Introduzca un **Graph Name (Nombre del gráfico)** descriptivo para su plantilla gráfica de servicio.
5. Seleccione **Create a New One (Crear uno nuevo)** para **Graph Type (Tipo de gráfico)**.
6. Haga clic y arrastre el dispositivo L4-L7 que creó en el procedimiento anterior entre los EPG del consumidor y del proveedor.
7. Seleccione **Routed (Enrutado)** para **Firewall (Cortafuegos)**.
8. Seleccione **Routed Redirect (Redireccionamiento enrutado)**.
9. Haga clic en **Submit (Enviar)** para enviar.



 ©2024 Palo Alto Networks, Inc.

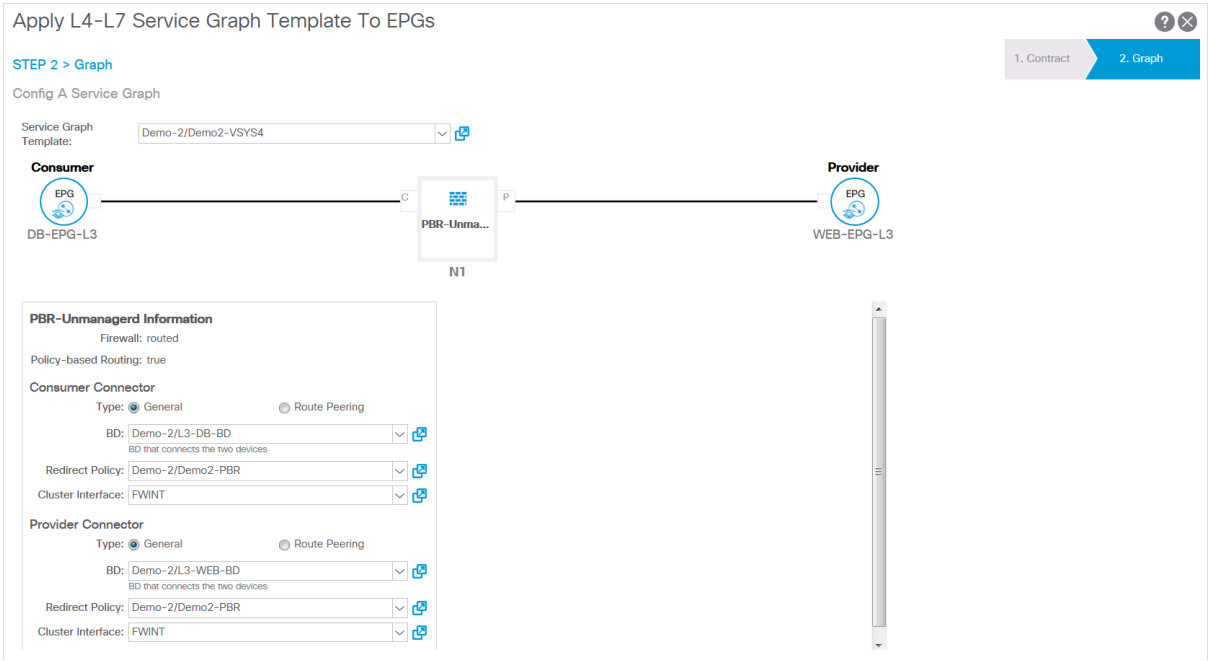
STEP 2 | Aplique la plantilla de gráfico de servicio.

1. En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino.
2. Seleccione **Services (Servicios)** > **L4-L7**.
3. En el panel **EPGs Information (Información de EPG)**, seleccione sus EPG de consumidor y proveedor en las listas desplegables **Consumer EPG (EPG del consumidor)** y **Provider EPG (EPG del proveedor)**.
4. Seleccione **Create a New Contract (Crear un nuevo contrato)**.
5. Introduzca un **Contract Name (Nombre de contrato)** descriptivo.
6. Borrar sin filtro **(Allow all Traffic) [(Permitir todo el tráfico)]**. No se recomienda utilizar esta opción. Para permitir que todo el tráfico entre los EPG se redireccione al cortafuegos, se recomienda crear un filtro para hacer esto.
7. Haga clic en el icono más (+) a la derecha de **Filter Entries (Entradas de filtro)**.
8. Cree una regla (o reglas) para definir qué tráfico puede pasar entre los EPG y ser redireccionado al cortafuegos.
9. Haga clic en **Next (Siguiente)**.



10. Seleccione la plantilla de gráfico de servicio que creó en el procedimiento anterior de la lista desplegable **Service Graph Template (Plantilla de gráfico de servicio)**.
11. En el panel de consumidores y proveedores, seleccione el dominio de puente que contiene su cortafuegos en la lista desplegable **BD**.
12. Seleccione el redireccionamiento basado en políticas que creó anteriormente en la lista desplegable **Redirect Policy (Política de redireccionamiento)**.
13. Seleccione la interfaz de clúster que creó con su dispositivo L4-L7 en la lista desplegable **Cluster Interface (Interfaz de clúster)**.

 ©2024 Palo Alto Networks, Inc.



Implementación del cortafuegos para asegurar el tráfico norte-sur en el modo de política de red

Use el modo de política de red para proteger el tráfico norte-sur que entra y sale de su centro de datos utilizando el modo no gestionado con redireccionamiento basado en políticas. Este procedimiento asume que ha completado lo siguiente:

- Los cortafuegos están operativos y conectados a un conmutador leaf en su entorno Cisco ACI. Además, la APIC debe poder acceder a la interfaz de gestión de cada cortafuegos.
- Los cortafuegos se implementan en modo HA activo/pasivo. Este procedimiento no cubre la configuración de la red de alta disponibilidad y asume que lo ha completado de antemano.

Para establecer conectividad externa a redes fuera de su estructura ACI, debe configurar un L3Out. Y L3Out es una política dedicada que contiene los parámetros necesarios para conectar dispositivos de enrutamiento externos a un inquilino. Además, una L3Out contiene un EPG externo (denominado red externa en la interfaz de usuario APIC) que representa redes accesibles a través de L3Out. El EPG externo no se rellena dinámicamente y sigue un modelo de fiabilidad cero, por lo que debe definir las redes en el EPG. Para facilitar la configuración, puede configurar una red de 0.0.0.0/0 para asignar todas las redes al EPG externo.

Para asegurar el tráfico entrante, conecte su o sus cortafuegos en un par de HA a sus conmutadores leaf de extremo. Los conmutadores leaf de extremo son conmutadores leaf que proporcionan conexiones de Capa 3 a enrutadores externos. Los cortafuegos se combinan con los conmutadores leaf de extremo que usan el protocolo de ruta más corta abierta primero (OSPF) que se configura en cada conmutador leaf en el par de vPC y se comunica con los cortafuegos mediante una interfaz virtual de conmutador (SVI). En el cortafuegos, configure un enrutador virtual dedicado a las interfaces que se conectan a su centro de datos. Este procedimiento también incluye

Para el tráfico saliente, el cortafuegos anuncia las redes externas a los conmutadores leaf de extremo que usan OSPF. Además, el EPG de la red externa está configurado para admitir todas las redes anunciadas por el cortafuegos en ese EPG. Usted crea un contrato entre un objeto gestionado vzAny y sus redes EPG

 ©2024 Palo Alto Networks, Inc.

externas para permitir que el tráfico de cualquier EPG dentro del VRF alcance las redes externas a través del cortafuegos. El objeto gestionado vzAny le permite consolidar todos los EPG en un VRF en uno o más contratos en lugar de crear contratos separados para cada EPG. Los EPG recopilados en el objeto gestionado vzAny consumen el contacto proporcionado por el EPG externo.

A diferencia del modo de administrador de servicios, la administración de la infraestructura ACI y los cortafuegos se completa por separado.

En el APIC—

- Creación de un conjunto de VLAN y un dominio enrutado externo
- Configure una política de interfaz para LLDP y LACP para tráfico Norte-Sur
- Creación de una red enrutada externa
- Configuración de las subredes para anunciarse al cortafuegos externo
- Creación de un contrato de salida
- Cree un contrato web de entrada
- Aplique contratos de salida y entrada a los EPG

En el cortafuegos—

- Creación de un enrutador virtual y una zona de seguridad para el tráfico norte-sur
- Configuración de las interfaces de red
- Configuración de la redistribución de ruta y OSPF
- Configuración de NAT para conexiones externas

Creación de un conjunto de VLAN y un dominio enrutado externo

Cree un conjunto de VLAN para asignar VLAN al cortafuegos cuando conecte las interfaces a la infraestructura para admitir los EPG en su estructura ACI. Debería usar un rango de VLAN estático para el cortafuegos.

Además, debe crear un dominio físico para asignar las VLAN a los EPG. El siguiente procedimiento crea un dominio físico dedicado al cortafuegos.

STEP 1 | Cree un grupo de VLAN.

1. Inicie sesión en su APIC.
2. Seleccione **Fabric (Estructura)** > **Access Policies (Políticas de acceso)** > **Pools (Grupos)** > **VLAN**.
3. Haga clic con el botón derecho en **VLAN** y seleccione **Create VLAN Pool (Crear grupo de VLAN)**.
4. Introduzca un **Name (Nombre)** descriptivo para su grupo de VLAN.
5. Seleccione **Dynamic Allocation (Asignación dinámica)** para el modo de asignación.
6. Haga clic en el botón más (+) a la derecha de **Encap Blocks (Bloques endcap)**.
7. Introduzca su intervalo de VLAN en el campo **VLAN Range (Rango de VLAN)**.
8. Seleccione **Static Allocation (Asignación estática)** del menú desplegable Modo de asignación.
9. Haga clic en **OK (Aceptar)**.
10. Haga clic en **Submit (Enviar)** para enviar.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Crear un dominio enrutado externo.

1. Seleccione **Fabric (Estructura)** > **Access Policies (Políticas de acceso)** > **Physical and External Domains (Dominios físicos y externos)** > **External Domains (Dominios externos)**.
2. Haga clic con el botón derecho en **External Routed Domain Dominio enrutado externo)** y seleccione **Create Layer 3 Domain (Crear dominio de capa 3)**.
3. Introduzca un **Name (Nombre)** descriptivo para su dominio físico.
4. Seleccione el grupo de VLAN que creó en el procedimiento anterior de la lista de grupos de VLAN.
5. Haga clic en **Submit (Enviar)** para enviar.

Configure una política de interfaz para LLDP y LACP para tráfico Norte-Sur

Cree una política que habilite LLDP y LACP en las interfaces de ACI que se conectan a su cortafuegos.

LLDP es necesario para que el reenvío funcione correctamente en el entorno ACI; ACI no implementa una interfaz de enrutador de subred en un conmutador Leaf a menos que detecte un endpoint en el conmutador que lo requiera. LLDP ayuda a determinar si una interfaz de enrutador de subred es necesaria.

LACP proporciona mayor resistencia y velocidad de recuperación en un fallo de enlace.

STEP 1 | Crear una política de interfaz LLDP.

1. Seleccione **Fabric (Tejido)** > **Access Policies (Políticas de acceso)** > **Interface Policies (Políticas de interfaz)** > **Policies (Políticas)** > **LLDP Interface (Interfaz LLDP)**.
2. Haga clic con el botón derecho en **LLDP Interface (Interfaz LLDP)** y seleccione **Create LLDP Interface Policy (Crear política de interfaz LLDP)**.
3. Introduzca un **Name (Nombre)** descriptivo para su política de interfaz LLDP.
4. Seleccione **Enabled (Habilitado)** para **Receive State (Estado de recepción)**.
5. Seleccione **Enabled (Habilitado)** para **Transmit State (Estado de transmisión)**.
6. Haga clic en **Submit (Enviar)** para enviar.

STEP 2 | Cree una política de canal de puerto para habilitar LACP.

1. Seleccione **Fabric (tejido)** > **Access Policies (Políticas de acceso)** > **Interface Policies (Políticas de interfaz)** > **Policies (Políticas)** > **Port Channel (Canal de puerto)**.
2. Haga clic con el botón derecho en **Port Channel (Canal de puerto)** y seleccione **Create Port Channel Policy (Crear política de canal de puerto)**.
3. Introduzca un **Name (Nombre)** descriptivo para su política de canal de puerto.
4. Seleccione **LACP Active (LACP activo)** de la lista desplegable **Mode (Modo)**.
5. Haga clic en **Submit (Enviar)** para enviar.

Creación de una red enrutada externa

Los cortafuegos pasan información de enrutamiento de IP al ACI sobre una red OSPF de Capa 3. ACI utiliza una interfaz virtual de conmutador (SVI) en los conmutadores leaf con una dirección IP en cada conmutador para la resistencia de la conexión. Cree una red enrutada de capa 3 para emparejarse con el cortafuegos utilizando OSPF.

STEP 1 | En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Seleccione **Networking (Redes)** > **External Routed Networks (Redes enrutadas externas)**.

STEP 3 | Haga clic con el botón derecho del ratón en **External Routed Networks (Redes enrutadas externas)** y seleccione **Create Routed Outside (Crear enrutado fuera)**.

STEP 4 | Introduzca un **Name (Nombre)** descriptivo para su **External Routed Network (Redes enrutadas externas)**.

STEP 5 | Seleccione su VRF con conectividad externa desde el menú desplegable **VRF**.

STEP 6 | Seleccione el dominio enrutado externo que creó anteriormente desde el menú desplegable **External Routed Domain (Dominio enrutado externo)**.

STEP 7 | Seleccione **OSPF**.

STEP 8 | Introduzca un **OSPF Area ID (ID de área OSPF)**. El ID de área se puede expresar en número decimal o en notación decimal con puntos. Por ejemplo, Área 1 es el mismo que el Área 0.0.0.1 o el Área 271 es el mismo que el Área 0.0.1.15. El rango de ID de área es 0 (0.0.0.0) a 4294967295 (255.255.255.255).

STEP 9 | Seleccione **Regular Area (Área regular)** para el **OSPF Area Type (Tipo de área OSPF)**.

STEP 10 | Haga clic en el botón más (+) a la derecha de **Nodes and Interface Profiles (Nodos y perfiles de interfaz)** para crear un perfil de nodo con un nodo que para los conmutadores leaf de borde que se conectan al cortafuegos.

STEP 11 | Introduzca un **Name (Nombre)** descriptivo para su **Node Profile (Perfil de nodo)**.

STEP 12 | Adjunte nodos a su Perfil de nodo.

1. Haga clic en el botón más (+) a la derecha de **Nodes (Nodos)**. Esto abre la ventana **Select Node (Seleccione Nodo)**.
2. Seleccione el nodo al que está conectado su cortafuegos desde el menú desplegable **Node ID (ID de nodo)**.
3. Introduzca la dirección IP del enrutador conectado al conmutador leaf en **Router ID (ID de enrutador)**.
4. Haga clic en **OK (Aceptar)**.
5. Haga clic en el botón más (+) a la derecha de **Nodes and Interface Profiles (Nodos y perfiles de interfaz)**.
6. Introduzca un **Name (Nombre)** descriptivo para su **Node Profile (Perfil de nodo)**.
7. Haga clic en el botón más (+) a la derecha de **Nodes (Nodos)**. Esto abre la ventana **Select Node (Seleccione Nodo)**.
8. Seleccione el nodo al que está conectado su cortafuegos HA secundario desde el menú desplegable **Node ID (ID de nodo)**.
9. Introduzca la dirección IP del enrutador conectado al conmutador leaf secundario en **Router ID (ID de enrutador)**.
10. Haga clic en **OK (Aceptar)**.

 ©2024 Palo Alto Networks, Inc.

STEP 13 | Adjunte un perfil de interfaz OSPF para su perfil de nodo.

1. Introduzca un **Name (Nombre)** descriptivo para su perfil de interfaz OSPF.
2. Haga clic en **Next (Siguiente)**.
3. Seleccione **Create OSPF Interface Policy (Crear política de interfaz OSPF)** desde el menú desplegable de políticas OSPF.
4. Introduzca un **Name (Nombre)** descriptivo para su política de interfaz OSPF.
5. Seleccione **MTU Ignore**.
6. Haga clic en **Submit (Enviar)** para enviar.
7. Haga clic en **Next (Siguiente)**.
8. Haga clic en **SVI**.
9. Haga clic en el botón más (+) a la derecha de **SVI Interfaces (Interfaces SVI)**. Esto abre la ventana **Select SVI (Seleccione SVI)**.
10. Haga clic en **Virtual Port Channel (Canal de puerto virtual)**.
11. Seleccione la ruta al puerto y a la interfaz del canal de puerto donde el cortafuegos se conecta al interruptor leaf.
12. En **Encap**, introduzca la encapsulación VLAN utilizada para su capa 3 fuera del perfil.
13. Seleccione **Trunk (Enlace)** para Modo.
14. En el campo **Side A IPv4 Primary Address (Dirección IPv4 primaria de lado A)**, introduzca la dirección IP principal de la ruta adjunta al perfil exterior de la capa 3.
15. En el campo **Side B IPv4 Primary Address (Dirección IPv4 primaria de lado B)**, introduzca la dirección IP secundaria de la ruta adjunta al perfil exterior de la capa 3.
16. Haga clic en **OK (Aceptar)**.

STEP 14 | Haga clic en **OK (Aceptar)** para cerrar la ventana Crear perfil de interfaz.

STEP 15 | Haga clic en **OK (Aceptar)** para cerrar la ventana Crear perfil de nodo.

STEP 16 | Haga clic en **Next (Siguiente)**.

STEP 17 | Haga clic en el botón más (+) a la derecha de **External EPG Networks (Redes EPG externas)**. Esto abre la ventana **Create Routed Outside (Crear enrutado fuera)**.

STEP 18 | Introduzca un **Name (Nombre)** descriptivo para su red externa.

STEP 19 | Añada una subred a su red externa.

1. Haga clic en el botón más (+) a la derecha de **Subnets (Subredes)**.
2. Introduzca la dirección IP y la máscara de la puerta de enlace predeterminada de la subred.
3. Seleccione **Export Route Control Subnet (Exportar subred de control de ruta)**.
4. Seleccione **External Subnets for External EPG (Subredes externas para EPG externo)**.
5. Haga clic en **OK (Aceptar)**.

STEP 20 | Haga clic en **Finish (Finalizar)**.

 ©2024 Palo Alto Networks, Inc.

Configuración de las subredes para anunciarse al cortafuegos externo

Por defecto, las subredes en el tejido ACI no se anuncian a redes externas. Debe configurar las subredes para ser anunciadas externamente.

STEP 1 | En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino.

STEP 2 | Seleccione **Networking (redes)** > **Bridge Domains (Dominio de puente)** > **<your bridge domain>**.

STEP 3 | Haga clic en **L3 Configurations (Configuraciones L3)**.

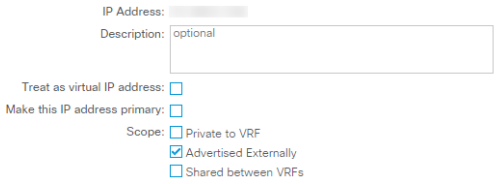
STEP 4 | Haga clic en el botón más (+) a la derecha de **Associated L3 Outs (Salidas de L3 asociadas)**.

STEP 5 | Seleccione la conexión de red enrutada externa de Capa 3 que creó en el procedimiento anterior de la lista desplegable **L3 Out (Salida de L3)**.

STEP 6 | Haga clic en **Update (Actualizar)**.

STEP 7 | Seleccione **Networking (Redes)** > **Bridge Domains (Dominio de puente)** > **<your bridge domain>** > **Subnets (Subredes)** > **<externally advertised subnet>**.

STEP 8 | Establezca el alcance en **Advertised Externally (Anunciado Externamente)**.



STEP 9 | Haga clic en **Submit (Enviar)** para enviar.

Creación de un contrato de salida

Cree un contrato con un filtro que permita el tráfico de DNS, NTP, HTTP y HTTPS. Utilizará este contrato para permitir que todos los endpoints del VRF lleguen a las redes externas, pero limita el tráfico enviado al cortafuegos.

STEP 1 | En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino.

STEP 2 | Seleccione **Contracts (Contratos)** > **Filters (Filtros)**

STEP 3 | Haga clic con el botón derecho en **Filters (Filtros)** y seleccione **Create Filter (Crear filtro)**.

STEP 4 | Introduzca un **Name (Nombre)** descriptivo para el filtro.

STEP 5 | Crear una entrada de filtro para el tráfico UDP.

1. Haga clic en el botón más (+) a la derecha de **Entries (Entradas)**.
2. Introduzca un **Name (Nombre)** descriptivo para el filtro **UDP**.
3. Seleccione **IP** de la lista desplegable **Ether Type (Tipo de ether)**.
4. Seleccione **udp** de la lista desplegable **IP Protocol (Protocolo IP)**.
5. Seleccione **dns** desde la lista desplegable **Destination Port From (Puerto de destino desde)**.
6. Haga clic en **Update (Actualizar)**.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Crear una entrada de filtro para el tráfico TCP.

1. Haga clic en el botón más (+) a la derecha de **Entries (Entradas)**.
2. Introduzca un **Name (Nombre)** descriptivo para el filtro **TCP**.
3. Seleccione **IP** de la lista desplegable **Ether Type (Tipo de ether)**.
4. Seleccione **tcp** de la lista desplegable **IP Protocol (protocolo IP)**.
5. Seleccione **dns** desde la lista desplegable **Destination Port From (Puerto de destino desde)**.
6. Haga clic en **Update (Actualizar)**.

STEP 7 | Crear una entrada de filtro para el tráfico NTP.

1. Haga clic en el botón más (+) a la derecha de **Entries (Entradas)**.
2. Introduzca un **Name (Nombre)** descriptivo para el filtro **NTP**.
3. Seleccione **IP** de la lista desplegable **Ether Type (Tipo de ether)**.
4. Seleccione **udp** de la lista desplegable **IP Protocol (Protocolo IP)**.
5. En el campo **Destination Port From (Puerto de destino desde)**, escriba 123.
6. Haga clic en **Update (Actualizar)**.

STEP 8 | Crear una entrada de filtro para el tráfico HTTP.

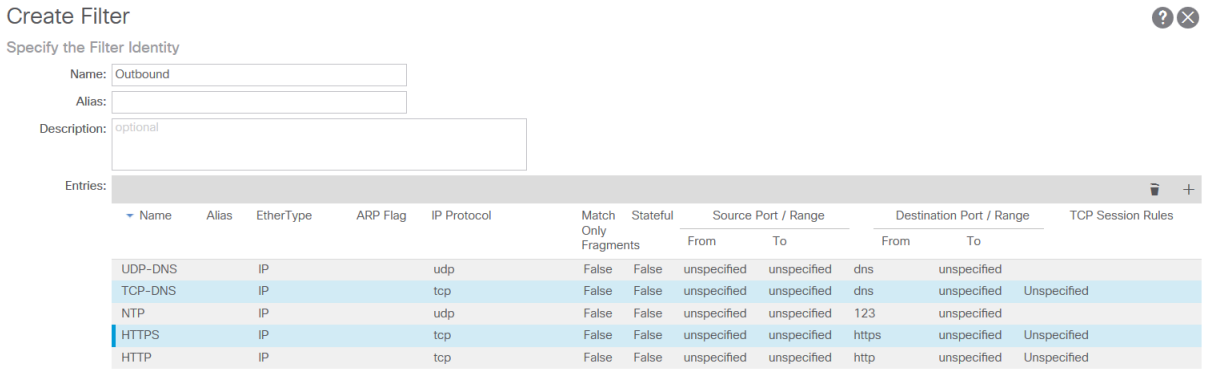
1. Haga clic en el botón más (+) a la derecha de **Entries (Entradas)**.
2. Introduzca un **Name (Nombre)** descriptivo para el filtro **HTTP**.
3. Seleccione **IP** de la lista desplegable **Ether Type (Tipo de ether)**.
4. Seleccione **tcp** de la lista desplegable **IP Protocol (protocolo IP)**.
5. Seleccione **http** de la lista desplegable **Destination Port From (Puerto de destino desde)**.
6. Haga clic en **Update (Actualizar)**.

STEP 9 | Crear una entrada de filtro para el tráfico HTTPS.

1. Haga clic en el botón más (+) a la derecha de **Entries (Entradas)**.
2. Introduzca un **Name (Nombre)** descriptivo para el filtro **HTTP**.
3. Seleccione **IP** de la lista desplegable **Ether Type (Tipo de ether)**.
4. Seleccione **tcp** de la lista desplegable **IP Protocol (protocolo IP)**.
5. Seleccione **https** de la lista desplegable **Destination Port From (Puerto de destino desde)**.
6. Haga clic en **Update (Actualizar)**.

 ©2024 Palo Alto Networks, Inc.

STEP 10 | Haga clic en **Submit (Enviar)** para enviar.



STEP 11 | Crear un contrato para el tráfico saliente.

1. En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino y seleccione **Contracts (Contratos)**.
2. Haga clic con el botón derecho en **Contracts (Contratos)** y seleccione **Create Contract (Crear Contrato)**.
3. Introduzca un **Name (Nombre)** descriptivo para su **Contract (Contrato)**.
4. Haga clic en el botón más (+) a la derecha de **Subjects (Sujetos)**.
5. Introduzca un **Name (Nombre)** descriptivo para su **Subject (Sujeto)**.
6. En Cadena de filtros, haga clic en el botón más (+) a la derecha de **Filters (Filtros)**.
7. Seleccione el filtro que configuró previamente del menú desplegable.
8. Haga clic en **OK (Aceptar)**.

STEP 12 | Haga clic en **Submit (Enviar)** para enviar.

Cree un contrato web de entrada

También debe crear un contrato y filtros para permitir que el tráfico entrante llegue a los servidores detrás del cortafuegos. El siguiente procedimiento describe el proceso de creación de un contrato y filtros que permiten que el tráfico web HTTP y HTTPS acceda a los recursos detrás del cortafuegos.

STEP 1 | En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino.

STEP 2 | Seleccione **Contracts (Contratos)** > **Filters (Filtros)**

STEP 3 | Haga clic con el botón derecho en **Filters (Filtros)** y seleccione **Create Filter (Crear filtro)**.

STEP 4 | Introduzca un **Name (Nombre)** descriptivo para el filtro.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Crear una entrada de filtro para el tráfico HTTP.

1. Haga clic en el botón más (+) a la derecha de **Entries (Entradas)**.
2. Introduzca un **Name (Nombre)** descriptivo para el filtro **HTTP**.
3. Seleccione **IP** de la lista desplegable **Ether Type (Tipo de ether)**.
4. Seleccione **tcp** de la lista desplegable **IP Protocol (protocolo IP)**.
5. Seleccione **http** de la lista desplegable **Destination Port From (Puerto de destino desde)**.
6. Haga clic en **Update (Actualizar)**.

STEP 6 | Crear una entrada de filtro para el tráfico HTTPS.

1. Haga clic en el botón más (+) a la derecha de **Entries (Entradas)**.
2. Introduzca un **Name (Nombre)** descriptivo para el filtro **TCP**.
3. Seleccione **IP** de la lista desplegable **Ether Type (Tipo de ether)**.
4. Seleccione **tcp** de la lista desplegable **IP Protocol (protocolo IP)**.
5. Seleccione **https** de la lista desplegable **Destination Port From (Puerto de destino desde)**.
6. Haga clic en **Update (Actualizar)**.

STEP 7 | Haga clic en **Submit (Enviar)** para enviar.

STEP 8 | Crear un contrato para el tráfico web entrante.

1. En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino y seleccione **Contracts (Contratos)**.
2. Haga clic con el botón derecho en **Contracts (Contratos)** y seleccione **Create Contract (Crear Contrato)**.
3. Introduzca un **Name (Nombre)** descriptivo para su **Contract (Contrato)**.
4. Haga clic en el botón más (+) a la derecha de **Subjects (Sujetos)**.
5. Introduzca un **Name (Nombre)** descriptivo para su **Subject (Sujeto)**.
6. En Cadena de filtros, haga clic en el botón más (+) a la derecha de **Filters (Filtros)**.
7. Seleccione el filtro que configuró previamente del menú desplegable.
8. Haga clic en **OK (Aceptar)**.

STEP 9 | Haga clic en **Submit (Enviar)** para enviar.

Aplique contratos de salida y entrada a los EPG

Ahora debe aplicar los contratos de entrada y salida a los EPG correspondientes.

Para que todos los EPG (colección de EPG) dentro de un VRF envíen tráfico a un destino externo, cada EPG interno debe tener un contrato con el EPG externo. Normalmente, deberá crear un contrato separado entre cada EPG interno y EPG externo. Sin embargo, si utiliza un objeto vzAny puede aplicar el mismo contrato a todos los EPG de forma dinámica. La colección de EPG hace uso del contrato y el EPG externo proporciona el contrato. Puede configurar perfiles de tráfico específicos en el contrato o enviar todo el tráfico al cortafuegos y permitirle controlar el tráfico que sale del centro de datos. Además, cualquier EPG nuevo que se una al VRF tendrá automáticamente el contrato aplicado.

 ©2024 Palo Alto Networks, Inc.

Aplique el contrato de entrada para que el EPG interno sea el proveedor y el EPG externo sea el consumidor. El tráfico que fluye al EPG interno se verifica por primera vez en el contrato y cualquier tráfico permitido son asegura más a través del cortafuegos, según sea necesario.

STEP 1 | Aplique el contrato de salida a todos los EPG en el VRF.

1. En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino.
2. Seleccione **Networking (Redes)** > **VRFs (VRF)** > **<you VRF>** > **EPG Collection for VRFm(Colección EPG para VRF)**.
3. Haga clic en el botón más (+) a la derecha de **Consumed Contracts (Contratos consumidos)**.
4. Seleccione su contrato saliente de la lista desplegable **Name (Nombre)**.
5. Haga clic en **Update (Actualizar)**.
6. Seleccione **Networking (redes)** > **External Routed Networks (Redes externas enrutadas)** > **<your external routed network>** > **Networks (Redes)** > **External (Externas)**.
7. Haga clic en el botón más (+) a la derecha de **Provided Contracts (Contratos proporcionados)**.
8. Seleccione su contrato saliente de la lista desplegable **Name (Nombre)**.
9. Haga clic en **Update (Actualizar)**.

STEP 2 | Aplique el contrato de entrada para que un EPG interno le proporcione al EPG externo.

1. En la pestaña **Tenants (Inquilinos)**, haga doble clic en el nombre de su inquilino.
2. Seleccione **Application Profiles (Perfiles de aplicación)** > **<your application profile>** > **Application EPGs (EPGs de aplicación)** > **<your application EPG>** > **Contracts (Contratos)**.
3. Haga clic con el botón derecho en **Contracts (Contratos)** y seleccione **Add Provided Contract (Añadir contrato provisto)**.
4. Seleccione su contrato de entrada de la lista desplegable **Contract (Contrato)**.
5. Haga clic en **Submit (Enviar)** para enviar.
6. En el mismo inquilino, seleccione **Networking (Redes)** > **External Routed Networks (Redes enrutadas externas)** > **<your external routed network>** > **Networks (Redes)** > **External (Externas)**.
7. En la pestaña Contratos, haga clic en el botón más (+) a la derecha de **Consumed Contracts (Contratos consumidos)**.
8. Seleccione su contrato de entrada de la lista desplegable **Name (Nombre)**.
9. Haga clic en **Update (Actualizar)**.

Creación de un enrutador virtual y una zona de seguridad para el tráfico norte-sur

Cree un enrutador virtual y una zona de seguridad en el cortafuegos para que coincida con el inquilino y el VRF en ACI.

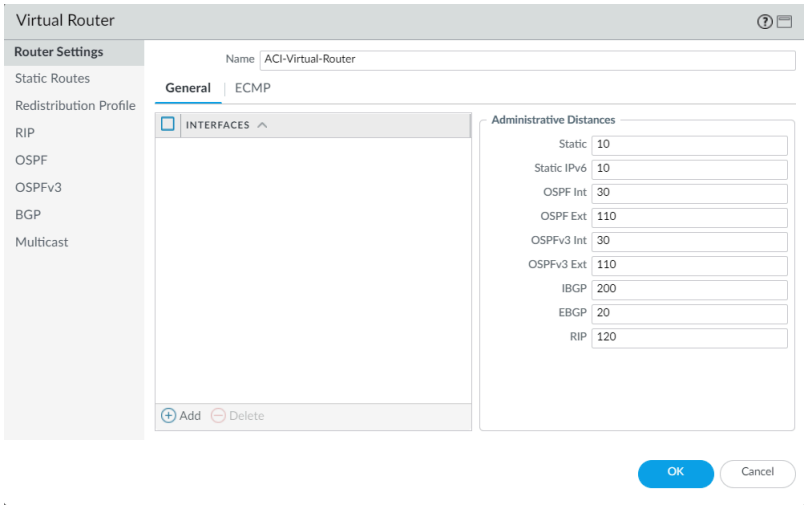
STEP 1 | Inicie sesión en el cortafuegos.

STEP 2 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y haga clic en **Add (Añadir)**.

STEP 3 | Dé al enrutador virtual un **Name (Nombre)** descriptivo.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Haga clic en **OK (Aceptar)**.

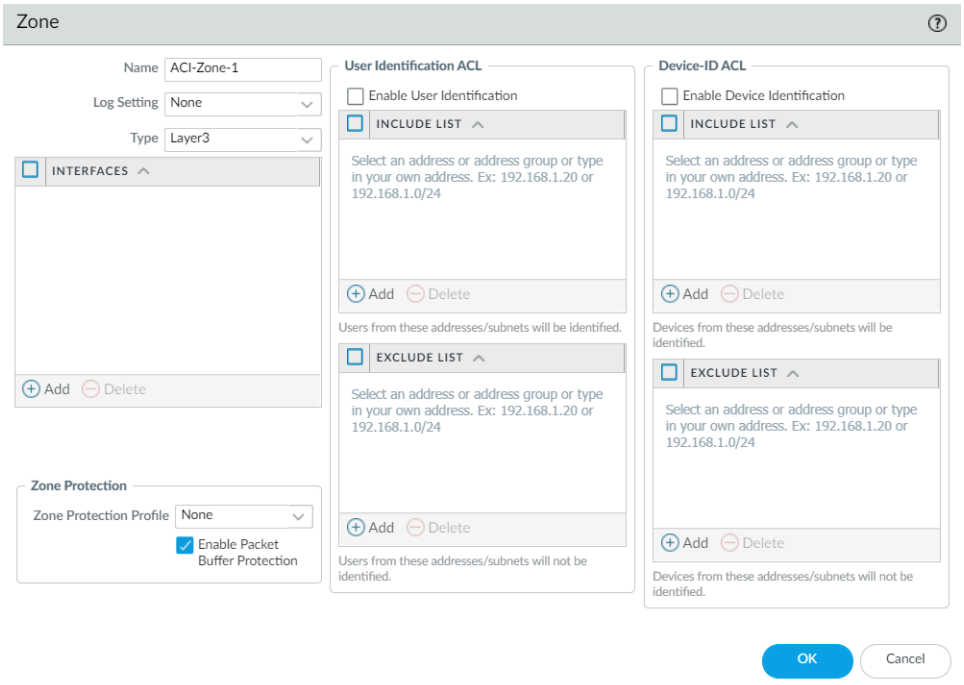


STEP 5 | Seleccione **Network (Red)** > **Zones (Zonas)** y haga clic en **Add (Añadir)**.

STEP 6 | Dé a la zona un **Name (Nombre)** descriptivo.

STEP 7 | Seleccione Capa 3 de la lista desplegable **Type (Tipo)**.

STEP 8 | Haga clic en **OK (Aceptar)**.



STEP 9 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

 ©2024 Palo Alto Networks, Inc.

Configuración de las interfaces de red

Configure una interfaz de Ethernet de agregación, interfaces miembro y subinterfaz que su cortafuegos usa para conectarse a los conmutadores leaf de ACI. Si está utilizando un cortafuegos VM-Series, utilice interfaces discretas en lugar de interfaces agregadas.

El cortafuegos VM-Series no es compatible con los grupos Ethernet de agregación.

STEP 1 | Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y haga clic en **Add Aggregate Group (Añadir grupo de agregación)**.

STEP 2 | Introduzca un número para el grupo de agregación en el segundo campo **Interface Name (Nombre de la interfaz)**.

STEP 3 | Seleccione Layer 3 (Capa 3) del menú desplegable **Interface Type (Tipo de interfaz)**.

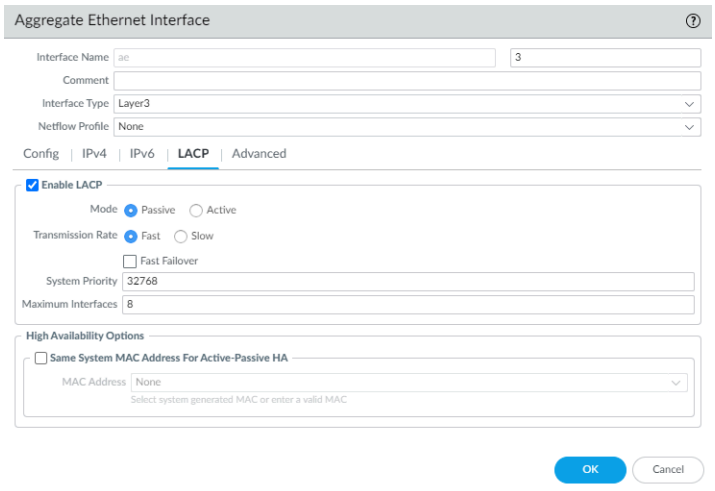
STEP 4 | Seleccione la pestaña **LACP** y haga clic en **Enable LACP (Habilitar LACP)**.

STEP 5 | Seleccione **Fast (Rápido)** como la **Transmission Rate (Velocidad de transmisión**.

STEP 6 | En Opciones de alta disponibilidad, seleccione **Enable in HA Passive State (Habilitar en estado pasivo HA)**.

*No seleccione **Same System MAC Address for Active-Passive HA (Misma dirección MAC del sistema para modo activo-pasivo de HA)**. Esta opción hace que el par de cortafuegos aparezca como un solo dispositivo para el conmutador, por lo que el tráfico fluirá hacia ambos cortafuegos en lugar de solo el cortafuegos activo.*

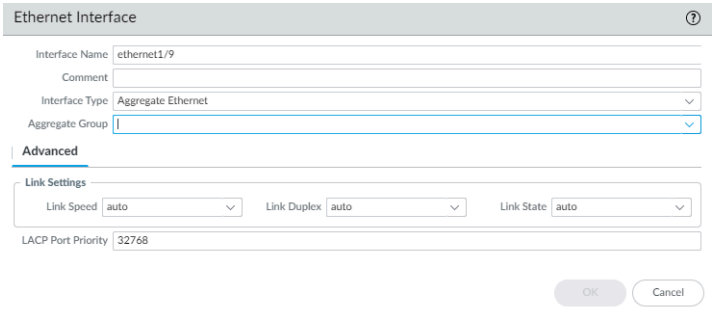
STEP 7 | Haga clic en **OK (Aceptar)**.



 ©2024 Palo Alto Networks, Inc.

STEP 8 | Haga clic en el nombre de una interfaz Ethernet para configurarla y añadirla al grupo de agregación.

1. Seleccione **Aggregate Ethernet (Ethernet de agregación)** en el menú desplegable Tipo de interfaz.
2. Seleccione la interfaz que definió en la configuración del grupo de Ethernet de agregación.
3. Haga clic en **OK (Aceptar)**.
4. Repita este paso para cada uno de los otros miembros de la interfaz del grupo de Ethernet de agregación.



STEP 9 | Agregue una subinterfaz en la interfaz de Ethernet de agregación para el arrendatario y el VRF.

1. Seleccione la fila de su grupo de Ethernet de agregación y haga clic en **Add Subinterface (Añadir subinterfaz)**.
2. En el segundo campo de **Interface Name (Nombre de la interfaz)**, introduzca un sufijo numérico para identificar la subinterfaz.
3. En el campo **Tag (Etiqueta)**, introduzca la etiqueta VLAN de la subinterfaz.
4. Seleccione el enrutador virtual que configuró anteriormente desde el menú desplegable **Virtual Router (Enrutador virtual)**.
5. Seleccione la zona que configuró previamente del menú desplegable **Zone (Zona)**.
6. Seleccione la pestaña **IPv4**.
7. Seleccione el tipo **Static (Estático)**.
8. Haga clic en **Add (Añadir)** e introduzca la dirección IP de subinterfaz y la máscara de red en notación CIDR.
9. Haga clic en **OK (Aceptar)**.

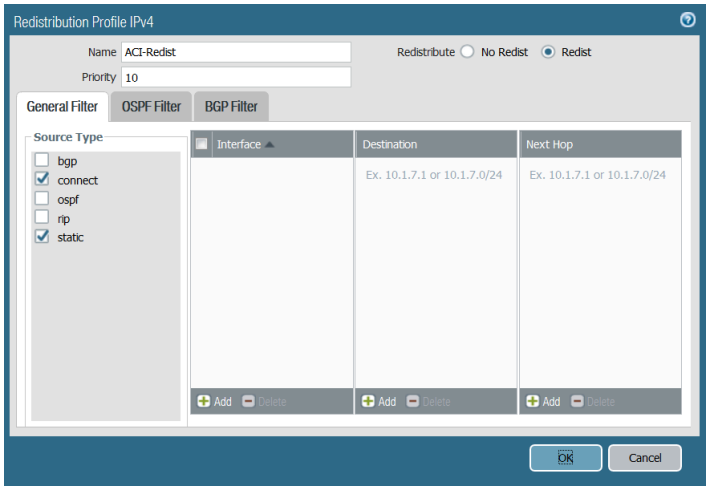
Configuración de la redistribución de ruta y OSPF

Configure la redistribución de rutas para que la información de enrutamiento del cortafuegos esté disponible para los enrutadores externos conectados a los conmutadores Leaf. Luego, configure OSPF en el cortafuegos y asigne un ID de enrutador, un número de área y una interfaz para formar adyacencias.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Configuración de la redistribución de rutas.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y haga clic en el enrutador virtual que creó anteriormente.
2. Seleccione **Redistribution Profile (Perfil de redistribución)** > **IPv4** > **Add (Añadir)**.
3. Introduzca un **Name (Nombre)** descriptivo para su perfil de redistribución.
4. Introduzca una prioridad.
5. Para **Redistribute (Redistribuir)**, seleccione **Redist (Redistr.)**.
6. Marque **connect (conectar)** y **static (estático)** en **General Filters (Filtros generales)**.
7. Haga clic en **OK (Aceptar)**.



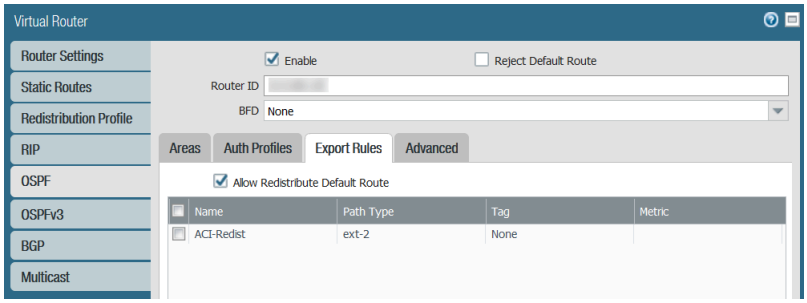
STEP 2 | Configure OSPF.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y haga clic en el enrutador virtual que creó anteriormente.
2. Seleccione **Router Settings (Configuración de enrutador)** > **ECMP** y seleccione **Enable (Habilitar)**.
3. Seleccione **OSPF** y seleccione **Enable (Habilitar)**.
4. Introduzca el **Router ID (Identificador de enrutador)** OSPF.
5. En **Area (Zona)**, haga clic en **Add (Añadir)**.
6. Introduzca el **Area ID (ID de área)**. Este valor debe coincidir con el valor que asignó cuando creó la red enrutada externa en el APIC. En el cortafuegos, esto se debe introducir en notación

 ©2024 Palo Alto Networks, Inc.

decimal con puntos. Por ejemplo, si introdujo un ID de área de 10 en el APIC, el equivalente en el cortafuegos es 0.0.0.10.

7. Seleccione **Interface (Interfaz)** > **Add (Añadir)**.
8. Introduzca la interfaz que se conecta a su red EPG externa y haga clic en **OK (Aceptar)**.
9. Seleccione **Export Rules (Reglas de exportación)** > **Add (Añadir)**.
10. Seleccione el perfil de redistribución que creó anteriormente del menú desplegable **Name (Nombre)** y haga clic en **OK (Aceptar)**.
11. Seleccione **Allow Redistribute Default Route (Permitir redistribución de ruta predeterminada)**.
12. Haga clic en **OK (Aceptar)**.



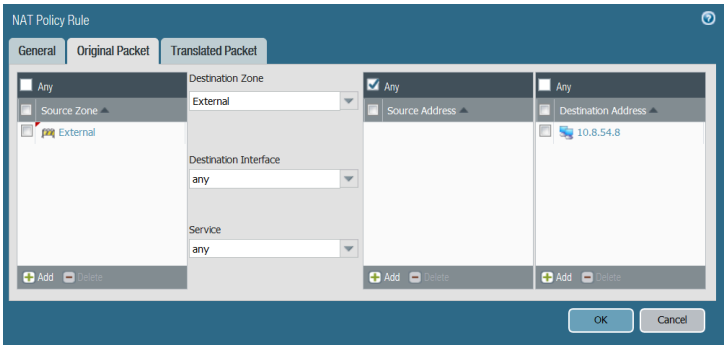
Configuración de NAT para conexiones externas

Solo necesita configurar NAT si el cortafuegos tiene una interfaz externa utilizada para conectarse a redes fuera de su centro de datos. Si bien NAT no es necesario, puede usar este procedimiento para traducir el direccionamiento IP privado en su centro de datos a direccionamiento IP público externo. Inicie la configuración de NAT configurando la traducción de direcciones para el tráfico que entra al servidor dentro de un EPG en su centro de datos. A continuación, configure una política de NAT que traduzca la dirección de origen del tráfico saliente de cualquier EPG a la dirección IP de la interfaz externa.

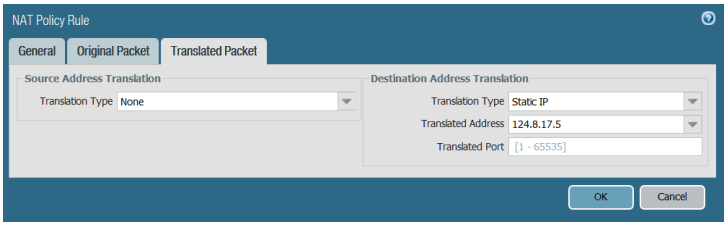
 ©2024 Palo Alto Networks, Inc.

STEP 1 | Configure la traducción de direcciones para el tráfico que entra a un EPG en su centro de datos.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** descriptivo para su regla de política de NAT.
3. Seleccione **Original Packet (Paquete original)** y haga clic en **Add (Añadir)** en **Source Zone (Zona de origen)**.
4. Seleccione la zona de origen del menú desplegable.
5. Seleccione la zona de destino del menú desplegable **Destination Zone (Zona de destino)**.
6. Seleccione **Any (Cualquiera)** para la **Source Address (Dirección de origen)**.
7. Haga clic en **Add (Añadir)** en **Destination Address (Dirección de destino)** e introduzca la dirección IP externa.



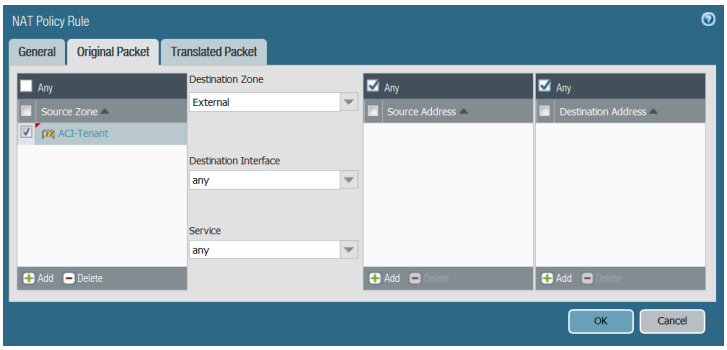
8. En la pestaña **Translated Packet (Paquete traducido)**, seleccione el **Translation Type (Tipo de traducción)** en **Destination Address Translation (Traducción de dirección de destino)**.
9. Seleccione una dirección del menú desplegable **Translated Address (Dirección traducida)**.
10. Haga clic en **OK (Aceptar)**.



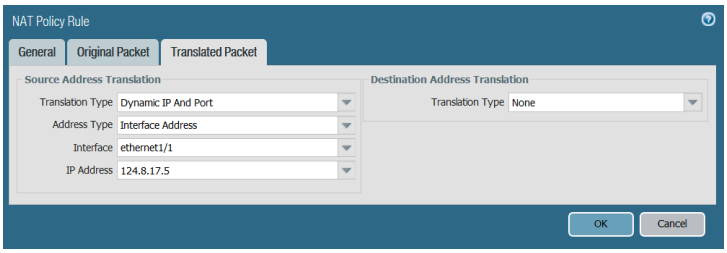
 ©2024 Palo Alto Networks, Inc.

STEP 2 | Configuración de la traducción de direcciones para el tráfico saliente.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** descriptivo para su política de salida de NAT.
3. Seleccione **Original Packet (Paquete original)** y haga clic en **Add (Añadir)** en **Source Zone (Zona de origen)**.
4. Seleccione la zona que coincida con su inquilino ACI y VRF.
5. Seleccione la zona externa en el menú desplegable **Destination Zone (Zona de destino)**.



6. En la pestaña **Translated Packet (Paquete traducido)**, seleccione el **Translation Type (Tipo de traducción)** en **Source Address Translation (Traducción de la dirección de origen)**.
7. Introduzca la información de dirección adicional requerida.
8. Haga clic en **OK (Aceptar)**.



STEP 3 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

 ©2024 Palo Alto Networks, Inc.

Supervisión de los endpoints en Cisco ACI

El plugin de Cisco ACI para Panorama le permite crear una política de seguridad para su estructura Cisco ACI usando Grupos de direcciones dinámicas. El plugin supervisa los cambios en la estructura de un Controlador de infraestructura de políticas de aplicación (APIC) en su entorno de Cisco ACI y comparte esa información con Panorama. Cada Panorama con el plugin Cisco ACI instalado puede admitir hasta 16 clústeres de APIC. Y cada definición de monitorización tiene un clúster y un grupo de notificación.

El número de endpoints que el plugin Cisco ACI puede supervisar depende de la cantidad de memoria asignada a Panorama. Si tiene un dispositivo virtual de Panorama, asegúrese de asignar la cantidad necesaria de memoria para los endpoints en su entorno. Consulte la Guía de administración de Panorama para más información sobre la preparación de su Panorama virtual.

Memoria de Panorama	Endpoints
8GB	10.000
16GB	20.000

El plugin Cisco ACI procesa la información del endpoint y la convierte en un conjunto de etiquetas que se pueden usar como criterios de coincidencia para colocar direcciones IP en grupos de direcciones dinámicas. Las etiquetas se construyen en el siguiente formato:

cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.{epg_<EPG> | uepg_<micro-EPG>}

- **cisco.cl_<cluster>**: esta etiqueta agrupa las direcciones IP en un grupo de direcciones dinámicas basado en el clúster de Cisco ACI y muestra el nombre de su clúster.
- **cisco.cl_<cluster>.tn_<tenant><tenant>**: esta etiqueta agrupa las direcciones IP en un grupo de direcciones dinámicas en función del inquilino y muestra el nombre de su clúster e inquilino.
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>**: esta etiqueta agrupa las direcciones IP en un grupo de direcciones dinámicas basado en el perfil de la aplicación y muestra el nombre de su clúster, inquilino y perfil de la aplicación.
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.epg_<EPG>**: esta etiqueta agrupa las direcciones IP en un grupo de direcciones dinámicas basado en EPG y muestra el nombre de su clúster, inquilino, perfil de aplicación y EPG.
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.uepg_<micro-EPG>**: esta etiqueta agrupa las direcciones IP en un grupo de direcciones dinámicas basado en micro-EPG y muestra el nombre de su clúster, inquilino, perfil de aplicación y micro-EPG.
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.esg_<ESG>**: esta etiqueta agrupa las direcciones IP en un grupo de direcciones dinámicas basado en Endpoint Security Group (ESG) y muestra el nombre de su clúster, inquilino, perfil de aplicación y ESG.
- **cisco.cl_<cluster>.tn_<tenant>.l2out_<L2-external-endpoint>**: esta etiqueta agrupa las direcciones IP en grupos de direcciones dinámicas basadas en el endpoint externo L2 y muestra el nombre de su clúster, inquilino y endpoint externo L2.
- **cisco.cl_<cluster>.tn_<tenant>.bd_<bridge-domain>.subnet_<subnet>**: esta etiqueta agrupa la dirección IP en un grupo de direcciones dinámicas basado en la subred y muestra el nombre de su clúster, inquilino, dominio de puente y subred.

 ©2024 Palo Alto Networks, Inc.

Para recuperar la información de asignación de la dirección IP a la etiqueta del endpoint, debe configurar una definición de monitorización para cada estructura APIC en su entorno Cisco ACI. La definición de monitorización especifica el nombre de usuario y la contraseña que permite a Panorama conectarse a los APIC. También especifica los grupos de dispositivos y los grupos de notificación correspondientes que contienen los cortafuegos a los que Panorama envía las etiquetas. Después de configurar la definición de monitorización y de que el complemento de Cisco ACI recupera las etiquetas, puede crear grupos de direcciones dinámicas y añadir las etiquetas como criterios de coincidencia.

El plugin Cisco ACI utiliza dos intervalos para recuperar información del APIC. El primero es el intervalo de supervisión.

- Intervalo de supervisión: El intervalo de supervisión es la cantidad de tiempo que el plugin espera antes de consultar los cambios en la estructura. Si no se producen cambios, se restablece el intervalo de supervisión. Si se detectan cambios, el plugin procesa los cambios antes de restablecer el intervalo de supervisión. El intervalo de supervisión predeterminado es 60 segundos. Puede configurar el intervalo de supervisión de 60 segundos a un día (86.400 segundos).
- Intervalo de sincronización completa: El intervalo de sincronización completa es la cantidad de tiempo que el plugin espera antes de actualizar los objetos dinámicos de todas las estructuras, independientemente de los cambios ocurridos. Esto garantiza que el plugin se sincronice con la estructura incluso si el intervalo de supervisión no detecta un evento de cambio. El intervalo de sincronización completa predeterminado es 10 minutos. Puede configurar el intervalo de sincronización completa de 600 segundos (10 minutos) a 86.400 segundos (un día).

  Debe configurar el intervalo de sincronización completa a través de la CLI de Panorama.

Si configura un valor para el intervalo de supervisión mayor que el del intervalo de sincronización completa, el intervalo de sincronización completa se ignora y se realiza una sincronización completa en cada intervalo de supervisión.

Si Panorama pierde su conexión con el APIC, Panorama intentará volver a conectarse cinco veces. Después de cinco intentos fallidos, Panorama deja de supervisar los cambios en sus grupos y muestra los intentos de reconexión en el registro del sistema. Para recuperar y volver a supervisar sus clústeres nuevamente, debe realizar una confirmación en Panorama.

- Instalación del complemento de Panorama para Cisco ACI
- Configure el plugin Cisco ACI
- Complemento de Panorama para el panel de Cisco ACI

Instalación del complemento de Panorama para Cisco ACI

Para comenzar con la supervisión de endpoints en Cisco ACI, descargue e instale el complemento Cisco ACI en Panorama.

Si tiene una configuración de HA en Panorama, repita el proceso de instalación en cada peer Panorama. Al instalar el complemento en Panorama en un par de HA, instale el complemento en el par pasivo antes de hacerlo en el par activo. Después de instalar el complemento en el peer pasivo, pasará a un estado no funcional. La instalación del plugin en el peer activo devuelve el peer pasivo a un estado funcional.

Si tiene un Panorama independiente o dos dispositivos Panorama instalados en un par de alta disponibilidad con varios complementos instalados, es posible que los complementos no reciban información actualizada sobre la etiqueta IP si uno o más de los complementos no están configurados. Esto ocurre porque Panorama no reenviará la información de la etiqueta IP a los complementos no configurados.

 ©2024 Palo Alto Networks, Inc.

Además, este problema puede ocurrir si uno o más de los complementos de Panorama no están en el estado Registrado o Correcto (el estado positivo varía según cada complemento). Asegúrese de que sus complementos estén en el estado positivo antes de continuar o ejecutar los comandos que se describen a continuación.

Si encuentra este problema, hay dos soluciones:

- Desinstale el complemento o complementos no configurados. Se recomienda que no instale un complemento que no planifique configurar de inmediato
- Puede utilizar los siguientes comandos para solventar este problema. Ejecute el siguiente comando para cada complemento no configurado en cada instancia de Panorama, para evitar que Panorama espere para enviar actualizaciones. Si no lo hace, sus cortafuegos pueden perder cierta información de la etiqueta IP.

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

  Puede cancelar este comando ejecutando:

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

Los comandos descritos no son persistentes en los reinicios y deben usarse de nuevo para cualquier reinicio posterior. Para Panorama en el par de HA, los comandos deben ejecutarse en cada Panorama.

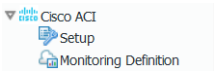
STEP 1 | Verifique que su Panorama virtual tenga suficiente memoria para admitir los endpoints numéricos en su entorno ACI.

STEP 2 | Seleccione **Panorama** > **Plugins (Complementos)**.

STEP 3 | Seleccione **Check Now (Comprobar ahora)** para recuperar una lista de actualizaciones disponibles.

STEP 4 | Seleccione **Download (Descargar)** en la columna Action (Acción) para descargar el plugin.

STEP 5 | Seleccione la versión del complemento y haga clic en **Install (Instalar)** en la columna Action (Acción) para instalar el complemento. Panorama le alertará cuando se complete la instalación.



Configure el plugin Cisco ACI

Después de instalar el plugin, debe establecer el intervalo de supervisión, configurar un grupo de notificación y establecer una conexión entre Panorama y la estructura APIC.

STEP 1 | (Opcional) Configure el intervalo de sincronización completa.

1. Inicie sesión en la CLI de Panorama.
2. Entre en el modo de configuración.

   `admin@Panorama> configure`
3. Use el siguiente comando para establecer el intervalo de sincronización completa. El intervalo predeterminado es 600 segundos (10 minutos). El intervalo es de 600 segundos a 86.400 segundos (un día).

   admin@Panorama# **`set plugins cisco full-sync-interval <interval-in-seconds>`**

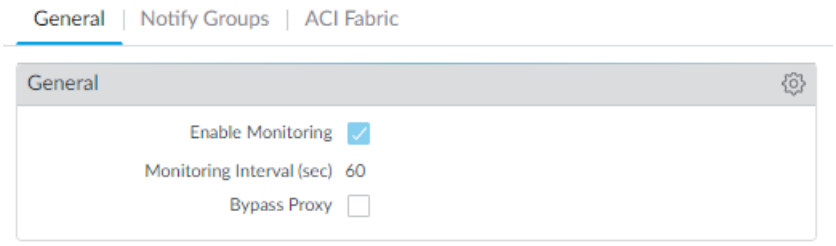
 ©2024 Palo Alto Networks, Inc.

STEP 2 | Inicie sesión en la interfaz web de Panorama.

STEP 3 | Debe añadir los cortafuegos como dispositivos gestionados en Panorama y crear grupos de dispositivos, de modo que pueda configurar Panorama para notificar a estos grupos con la información de la VM que recupera. Los grupos de dispositivos pueden incluir cortafuegos serie VM o sistemas virtuales en los cortafuegos del hardware.

STEP 4 | Habilite la supervisión, establezca el intervalo de supervisión y habilite la omisión del proxy.

1. Seleccione **Panorama** > **Cisco ACI** > **Setup (Configuración)** > **General**.
2. Seleccione **Enable Monitoring (Habilitar supervisión)**. Esto permite la supervisión de todos los clústeres en su implementación.
3. Establezca el **Monitoring Interval (Intervalo de supervisión)** en segundos. El intervalo de supervisión es la frecuencia con la que Panorama recupera la información de red actualizada del APIC. El valor predeterminado es 60 segundos con un intervalo de 60 segundos a 86.400 segundos (un día).
4. (Opcional) Seleccione Omitir proxy para omitir la configuración del servidor proxy, configurado en Panorama en **Panorama** > **Configuración** > **Servicios** > **Servidor proxy**, para la comunicación entre Panorama y el APIC. Esto permite que Panorama se comunique directamente con el APIC mientras mantiene la comunicación proxy para otros servicios.



STEP 5 | Cree un grupo de notificación.

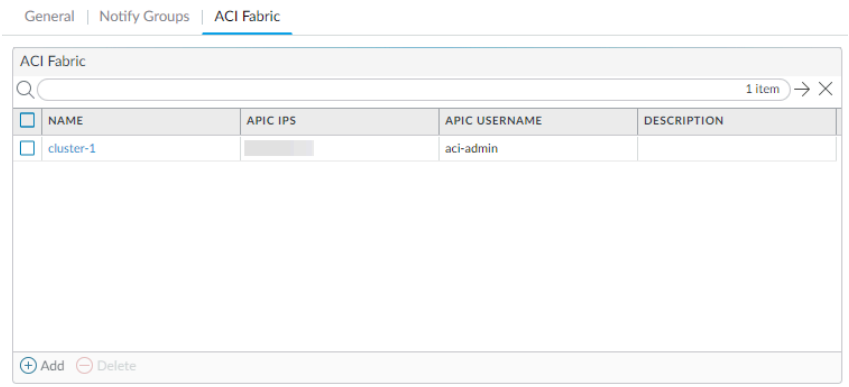
1. Seleccione **Panorama** > **Cisco ACI** > **Setup (Configuración)** > **Notify Groups (Grupos de notificación)**.
2. Haga clic en **Add (Añadir)**.
3. Introduzca un **Name (Nombre)** descriptivo para el grupo de notificación.
4. Seleccione los grupos de dispositivos en su implementación de ACI.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Añada información de la estructura de ACI.

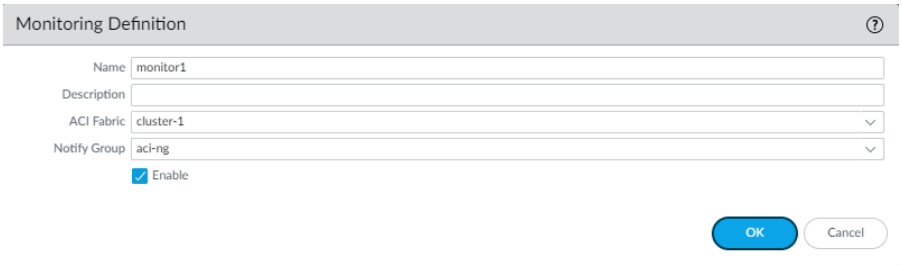
1. Seleccionar **Panorama** > **Cisco ACI** > **Setup (Configuración)** > **ACI Fabric (Estructura ACI)**.
2. Introduzca un **Name (Nombre)** descriptivo para su clúster.
3. Introduzca la dirección IP o FQDN para cada APIC en el clúster como una lista separada por comas.

   Cuando utilice FQDN, no incluya https: // en la URL.
4. Introduzca su nombre de usuario de APIC.
5. Introduzca y confirme su contraseña de APIC.
6. Haga clic en **OK (Aceptar)**.



STEP 7 | Configure la definición de monitorización.

1. Seleccione **Panorama** > **Cisco ACI** > **Monitoring Definition (Definición de monitorización)** y haga clic **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** descriptivo y, opcionalmente, una descripción para identificar el clúster de Cisco ACI para el que usa esta definición.
3. Seleccione la **Cluster Info (Información del clúster)** y el **Notify Group (Grupo de notificación)**.
4. Haga clic en **OK (Aceptar)**.



STEP 8 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Compruebe que puede ver la información de EPG en Panorama y defina los criterios de coincidencia para los grupos de direcciones dinámicas.

Algunas extensiones del navegador pueden bloquear las llamadas a la API entre Panorama y el APIC, lo que evita que Panorama reciba criterios de coincidencia. Si Panorama no muestra ningún criterio de coincidencia y usted está usando extensiones de navegador, deshabilite las extensiones y Sincronizar objetos dinámicos para completar las etiquetas disponibles para Panorama.

Panorama no procesa de inmediato las nuevas definiciones de supervisión y llena los criterios de coincidencia disponibles para la dirección dinámica. Debe esperar el tiempo que dure su intervalo de supervisión configurado antes de verificar esa información de EPG.

STEP 10 | Verifique que las direcciones en sus EPG se añadan a los grupos de direcciones dinámicas.

1. Seleccione **Panorama** > **Objects (Objetos)** > **Address Groups (Grupos de direcciones)**.
2. Haga clic en **Más** en la columna Direcciones de un grupo de direcciones dinámicas.

   Panorama muestra una lista de direcciones IP añadidas a ese grupo de direcciones dinámicas según los criterios de coincidencia que especificó.

STEP 11 | Usar grupos de direcciones dinámicas en la política.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Haga clic en **Add (Añadir)** y escriba un **Name (Nombre)** y una **Description (Descripción)** para la política.
3. Añada la **Source Zone (Zona de origen)** para especificar la zona desde la que se origina el tráfico.
4. Añada la **Destination Zone (Zona de destino)** donde finaliza el tráfico.
5. Para la **Destination Address (Dirección de destino)**, seleccione el grupo de direcciones dinámicas que ha creado anteriormente.
6. Especifique la acción (**Permitir** o **Denegar**) para el tráfico y, de manera opcional, incluya los perfiles de políticas de seguridad en la regla.
7. Repita los pasos del 1 al 6 para crear otra regla de política.
8. Haga clic en **Commit (Confirmar)**.

   Consulte Usar grupos de direcciones dinámicas en la política para obtener más información.

STEP 12 | Puede actualizar los objetos dinámicos desde el APIC en cualquier momento mediante la sincronización de objetos dinámicos. La sincronización de objetos dinámicos le permite mantener el contexto en los cambios del entorno virtual y activar aplicaciones, ya que actualiza de forma automática los grupos de direcciones dinámicas en las reglas de la política.

1. Seleccione **Panorama** > **Cisco ACI** > **Monitoring Definition (Definición de monitorización)**.

 ©2024 Palo Alto Networks, Inc.

2. Haga clic en **Synchronize Dynamic Objects (Sincronizar objetos dinámicos)**.

Durante una conmutación por error de HA, la instancia de Panorama activada recientemente intenta reconectarse al APIC y recuperar las etiquetas de todas las definiciones de supervisión. Si se produce un error durante la reconexión en una definición de monitorización, Panorama genera un mensaje en el log del sistema

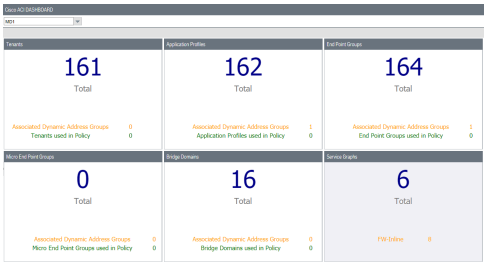
```
No es posible procesar las suscripciones después
 del cambio de alta disponibilidad; se requiere la
 intervención del usuario.
```

Si se produce este error, debe iniciar sesión en Panorama y corregir el problema (por ejemplo, eliminar una IP de APIC no válida o proporcionar credenciales válidas) y confirmar los cambios para permitir que Panorama se vuelva a conectar y recuperar las etiquetas de todas las definiciones de supervisión. Incluso cuando Panorama esté desconectado del APIC, los cortafuegos tienen la lista de todas las etiquetas que se recuperaron antes de la conmutación por error y pueden continuar aplicando la política en esa lista de direcciones IP. Si realiza una confirmación antes de resolver el error de conmutación por error, el nuevo Panorama activo no enviará ninguna información de asignación de IP a etiqueta y borrará la información de asignación de los cortafuegos. Se recomienda que para supervisar este problema, configure el reenvío de logs a un destino HTTPS orientado a la acción desde Panorama, de modo que pueda actuar de inmediato.

Complemento de Panorama para el panel de Cisco ACI

El complemento de Panorama para el panel de Cisco ACI proporciona una vista panorámica de la infraestructura ACI supervisada por el complemento. El panel consta de dos páginas: la primera página proporciona una descripción general de varios objetos supervisados por el complemento en un conjunto de mosaicos en los que se puede hacer clic; hacer clic en un mosaico le lleva a la segunda página que proporciona más información sobre el objeto presentado en el mosaico.

Después de instalar el complemento, puede acceder al panel seleccionando **Panorama** > **Cisco ACI** > **Dashboard (Tablero)**.



El tablero solo consulta y cuenta las políticas de seguridad previas a las reglas configuradas en Panorama; no incluye reglas posteriores, reglas predeterminadas ni reglas NAT.

 ©2024 Palo Alto Networks, Inc.

Mosaicos del panel	Description (Descripción)
Tenant Tags (Etiquetas de inquilino) *Si la puntuación del estado de un inquilino es cero (0) en el APIC, Panorama no recupera información sobre ese inquilino. Por lo tanto, el recuento de inquilinos en Panorama no coincidirá con el total en el APIC.*	Muestra el número total de inquilinos que Panorama ha recuperado del APIC. Además, muestra el número de grupos de direcciones dinámicas asociados con los inquilinos y el número de inquilinos utilizados en la política. Haga clic en el mosaico para profundizar y ver las siguientes columnas. • **Tenant Name (Nombre del inquilino)**: enumera todos los inquilinos recuperados por Panorama. • **Tenant Tag (Etiqueta de inquilino)**: la etiqueta de Panorama asociada con cada inquilino. • **Dynamic Address Group (Grupo de direcciones dinámicas)**: muestra los grupos de direcciones dinámicas asociados con la etiqueta de la lista. • **In Policy (En Política)**: muestra si el grupo de direcciones dinámicas enumeradas se usa en la política.
Application Profiles (Perfiles de aplicación)	Muestra el número total de perfiles de aplicación que Panorama ha recuperado del APIC. Además, muestra el número de grupos de direcciones dinámicas asociados con los perfiles de aplicación y el número de perfiles de aplicación utilizados en la política. Haga clic en el mosaico para profundizar y ver las siguientes columnas. • **Application Profile Name (Nombre de perfil de aplicación)**: enumera todos los perfiles de aplicación recuperados por Panorama. • **Tenant Name (Nombre del inquilino)**: muestra el inquilino asociado con el perfil de aplicación enumerado.

 ©2024 Palo Alto Networks, Inc.

Mosaicos del panel	Description (Descripción)
	• **Application Profile Tag (Etiqueta de perfil de aplicación)**: la etiqueta de Panorama asociada con cada perfil de aplicación. • **Dynamic Address Group (Grupo de direcciones dinámicas)**: muestra los grupos de direcciones dinámicas asociados con la etiqueta de la lista. • **In Policy (En Política)**: muestra si el grupo de direcciones dinámicas enumeradas se usa en la política.
End Point Groups (Grupos de endpoints)	Muestra el número total de grupos de endpoints (EPG) que Panorama recuperado del APIC. Además, muestra el número de grupos de direcciones dinámicas asociados con los EPG y el número de los EPG utilizados en la política. Haga clic en el mosaico para profundizar y ver las siguientes columnas. • **EPG Name (Nombre de EPG)**: enumera todos los EPG recuperados por Panorama. • **Application Profile Name (Nombre del perfil de la aplicación)**: enumera los perfiles de aplicación asociados a la EPG. • **Tenant Name (Nombre del inquilino)**: muestra el inquilino asociado con el perfil de aplicación enumerado. • **EPG Tag (Etiqueta EPG)**: la etiqueta Panorama asociada con cada EPG. • **Dynamic Address Group (Grupo de direcciones dinámicas)**: muestra los grupos de direcciones dinámicas asociados con la etiqueta de la lista. • **In Policy (En Política)**: muestra si el grupo de direcciones dinámicas enumeradas se usa en la política.
Micro End Point Groups (Grupos de microendpoints)	Muestra el número total de grupos de microendpoints (EPG) que Panorama ha recuperado del APIC. Además, muestra el número de grupos de direcciones dinámicas asociados con micro EPG y el número de micro EPG utilizadas en la política. Haga clic en el mosaico para profundizar y ver las siguientes columnas. • **Micro EPG Name (Nombre de micro EPG)**: enumera todas los EPG recuperados por Panorama. • **Application Profile Name (Nombre de perfil de aplicación)**: enumera el perfil de aplicación asociado de los Micro EPG. • **Tenant Tag (Etiqueta de inquilino)**: muestra el inquilino asociado con el perfil de aplicación enumerado. • **Micro EPG Tag (Etiqueta de Micro EPG)**: la etiqueta de Panorama asociada con cada Micro EPG. • **Dynamic Address Group (Grupo de direcciones dinámicas)**: muestra los grupos de direcciones dinámicas asociados con la etiqueta de la lista. • **In Policy (En Política)**: muestra si el grupo de direcciones dinámicas enumeradas se usa en la política.

 ©2024 Palo Alto Networks, Inc.

Mosaicos del panel	Description (Descripción)
Bridge Domains (Dominios de puente)	Muestra el número total de dominios de puente que Panorama ha recuperado del APIC. Además, muestra el número de grupos de direcciones dinámicas asociados con dominios de puente y el número de dominios de puente utilizados en la política. Haga clic en el mosaico para profundizar y ver las siguientes columnas. • **Bridge Domain Name (Nombre de dominio de puente)**: enumera todos los dominios de puente recuperados por Panorama. • **Tenant Name (Nombre del inquilino)**: muestra el inquilino asociado con el dominio de puente enumerado. • **Bridge Domain Tag (Etiqueta de dominio de puente)**: la etiqueta de Panorama asociada con cada dominio de puente. • **Dynamic Address Group (Grupo de direcciones dinámicas)**: muestra los grupos de direcciones dinámicas asociados con la etiqueta de la lista. • **In Policy (En Política)**: muestra si el grupo de direcciones dinámicas enumeradas se usa en la política.
Service Graphs (Gráficos de servicio)	Muestra el número total de gráficos de servicio supervisados por el complemento, así como el número de cortafuegos en línea con los gráficos de servicio supervisados. Haga clic en el mosaico para profundizar y ver las siguientes columnas. • **Service Graph Name (Nombre del gráfico de servicio)**: enumera todos los gráficos de servicio recuperados por Panorama. • **Producer EPG (EPG de productor)** : muestra el EPG del productor asociado con el gráfico de servicio. • **FW InLine (Reenvío en línea)**: muestra el cortafuegos asociado con el gráfico de servicio.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en Cisco CSP

Puede implementar el cortafuegos VM-Series como un servicio virtual de red en la plataforma de seguridad en la nube de Cisco (CSP). Debido a que Cisco CSP es una plataforma KVM de RHEL, el cortafuegos VM-Series se implementa utilizando el cortafuegos VM-Series para la imagen base de KVM.

Con el cortafuegos VM-Series en Cisco CSP, puede proteger sus cargas de trabajo, evitar amenazas avanzadas y mejorar la visibilidad de las aplicaciones en su red virtual.

- Requisitos del sistema para VM-Series en Cisco CSP
- Implemente el cortafuegos VM-Series en Cisco CSP

Requisitos del sistema para VM-Series en Cisco CSP

Puede crear e implementar una o varias instancias, independientes o como parte de un par de HA, del cortafuegos VM-Series en su Cisco CSP.

El cortafuegos VM-Series tiene los siguientes requisitos:

- Consulte la Matriz de compatibilidadpara versiones compatibles de CSP y PAN-OS.
- Paquete de arranque convertido a un archivo ISO
- Consulte Requisitos del sistema para VM-Series para los requisitos mínimos de hardware para su modelo VM-Series.
- Mínimo de dos interfaces de red (vNIC). Una es una vNIC dedicada para la interfaz de gestión y la otra para la interfaz de datos. A continuación, podrá añadir hasta ocho vNIC más para el tráfico de datos.
- El cortafuegos VM-Series en Cisco CSP es compatible con todos los modelos VM-Series, excepto el VM-50.
- SR-IOV y modo de paquete MMAP solo; DPDK no es compatible.

 ©2024 Palo Alto Networks, Inc.

Implemente el cortafuegos VM-Series en Cisco CSP

Complete el siguiente procedimiento para implementar el cortafuegos VM-Series en Cisco CSP.

STEP 1 | Descargue el archivo de imagen base qcow2 de VM-Series desde el Portal de atención al cliente.

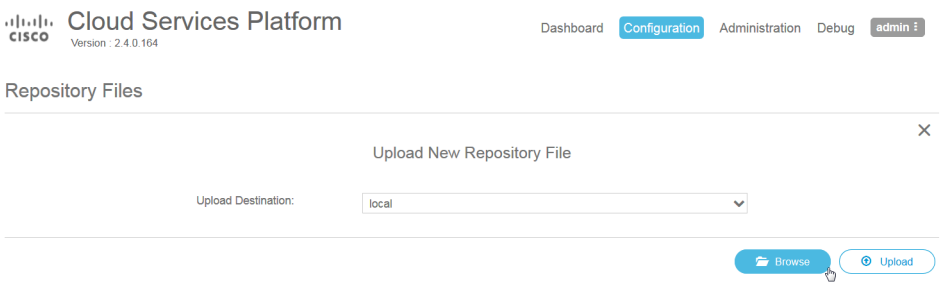
STEP 2 | Cree un archivo ISO de arranque para el cortafuegos VM-Series.

1. Cree un Paquete de arranque para su cortafuegos VM-Series.
2. Cree un archivo ISO que contenga el paquete bootstrap usando su herramienta preferida.

STEP 3 | Inicie sesión en la interfaz web de Cisco CSP.

STEP 4 | Cargue la imagen qcow2 del cortafuegos VM-Series y el archivo ISO.

1. Seleccione **Configuration (Configuración)** > **Repository (Repositorio)**.
2. Haga clic en el icono más (+).
3. Haga clic en **Browse (Examinar)** y vaya a su archivo qcow2.
4. Haga clic en **Upload (Cargar)**.
5. Haga clic en **Browse (Examinar)** y vaya a su archivo ISO.
6. Haga clic en **Upload (Cargar)**.



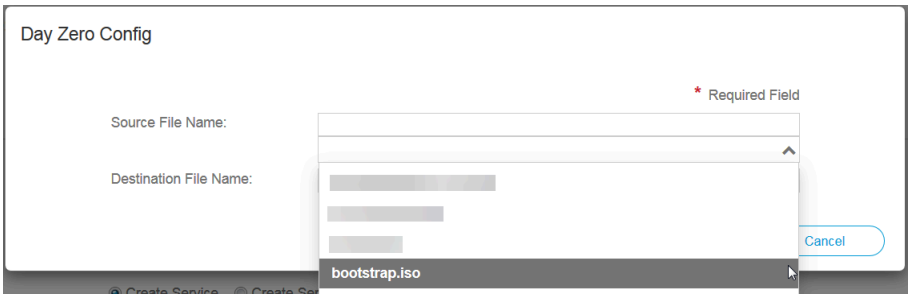
 ©2024 Palo Alto Networks, Inc.

STEP 5 | Cree el servicios del cortafuegos VM-Series.

1. Añada un **Name (Nombre)** descriptivo para el cortafuegos VM-Series.
2. Seleccione el **Target Host Name (Nombre de host de destino)** del menú desplegable.
3. Seleccione el archivo qcow2 que cargó de la lista desplegable**Image Name (Nombre de la imagen)**.



4. Seleccione la configuración de día cero.
   1. Haga clic en el icono más (+) de **Day Zero Config (Día Cero Config)**.
   2. Seleccione el archivo ISO de arranque de la lista desplegable **Source File Name (Nombre del archivo origen)**.
   3. Haga clic en **Submit (Enviar)** para enviar.



5. Asigne el número de núcleos y memoria necesarios para su Modelo de cortafuegos VM-Series.
6. Añada suficientes vNIC para admitir el número de interfaces VM-Series configuradas en su archivo ISO de arranque.

Consulte la Documentación de Cisco Cloud Service Platform para obtener más información sobre cómo crear e implementar una instancia de servicio.

STEP 6 | Una vez finalizado el proceso de arranque, inicie sesión en su cortafuegos VM-Series utilizando la dirección IP de administración que especificó en el archivo ISO de arranque.

El cortafuegos debería estar activo y configurado de acuerdo con los parámetros que definió en el paquete de arranque.

 ©2024 Palo Alto Networks, Inc.

Configuración del cortafuegos VM-Series en Nutanix AHV

El cortafuegos VM-Series para Nutanix AHV le permite implementar el cortafuegos VM-Series en dispositivos capaces de ejecutar el hipervisor Nutanix Acropolis. Si está utilizando Panorama para gestionar sus cortafuegos VM-Series en Nutanix AHV, puede usar el complemento de Panorama para Nutanix para realizar la supervisión de máquinas virtuales. Esto le permite informar dinámicamente al cortafuegos de los cambios en su entorno Nutanix y garantizar que la política se aplique a las máquinas virtuales a medida que se unen a su red.

- Implementación del cortafuegos VM-Series en NSX-T
- Supervisión de máquinas virtuales en Nutanix

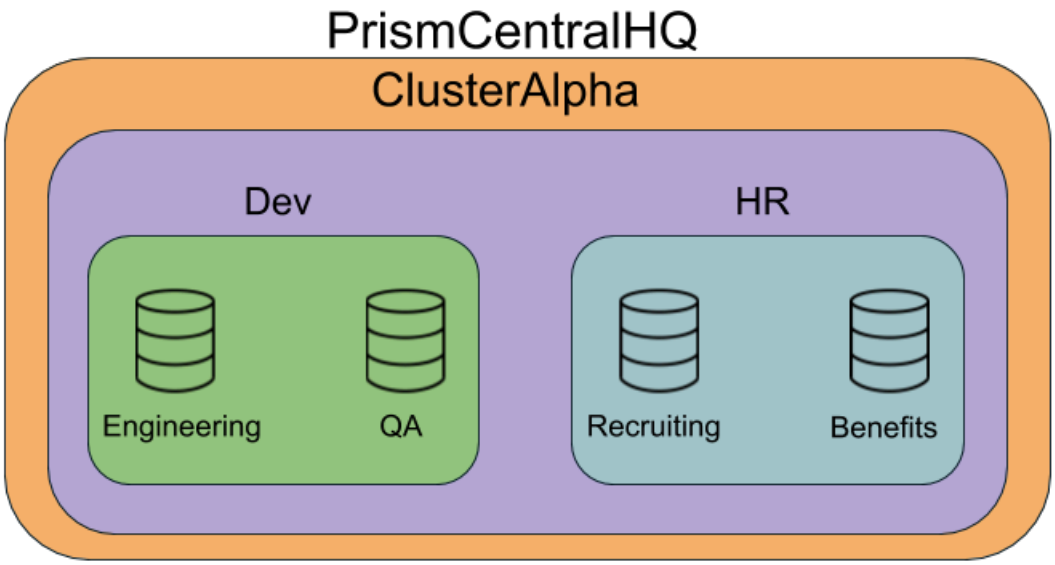
Supervisión de máquinas virtuales en Nutanix

Instale y configure el complemento Panorama para Nutanix para supervisar los cambios en su entorno Nutanix y crear políticas utilizando grupos de direcciones dinámicas.

- Acerca de la supervisión de máquinas virtuales en Nutanix
- Instalación del complemento de Panorama para Nutanix
- Configuración del complemento de Panorama para Nutanix

Acerca de la supervisión de máquinas virtuales en Nutanix

El complemento Panorama para Nutanix facilita el uso de grupos de direcciones dinámicas al supervisar máquinas virtuales en su entorno Nutanix. Prism Central agrupa entidades en sus entornos Nutanix por categorías y las filtra aún más por valor. Panorama crea etiquetas basadas en categorías y valores que usted define en Prism Central. Cuando una máquina virtual se coloca en una categoría y se le asigna un valor, Panorama aplica la etiqueta correspondiente a la dirección IP de la máquina virtual. Luego puede crear una política de seguridad utilizando las etiquetas como criterios de coincidencia para los grupos de direcciones dinámicas en Panorama.



En el ejemplo anterior, tenemos dos categorías: Dev y HR, con dos valores dentro de cada una de ellas. Y estas categorías están dentro del clúster, que está dentro de Prism Central. Después de comenzar a supervisar su entorno Nutanix, Panorama usa valor, categoría, clúster y Prism Central para formar etiquetas. Cuando visualiza los criterios de coincidencia para grupos de direcciones dinámicas, las etiquetas se enumeran en el siguiente formato.

ntnx.PC-<prism-central-name>.CL-<cluster-name>.<category>.<value>

Con la información del ejemplo anterior, Panorama crea las siguientes etiquetas.

`ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.Dev.Engineering`

`ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.Dev.QA`

 ©2024 Palo Alto Networks, Inc.

`ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.HR.Recruiting`

`ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.HR.Benefits`

Para proteger estas cargas de trabajo en estas categorías, utilice etiquetas como estas como criterios de coincidencia en los grupos de direcciones dinámicas. Luego puede usar los grupos de direcciones dinámicas como grupos de direcciones de origen y destino en sus reglas de política de seguridad. Cuando una máquina virtual se une a un grupo de direcciones dinámicas, la política que ha creado se aplica automáticamente.

Instalación del complemento de Panorama para Nutanix

Para comenzar con la supervisión de endpoints en Nutanix, descargue e instale el complemento de Panorama para Nutanix.

Si tiene una configuración de HA en Panorama, repita el proceso de instalación en cada peer Panorama. Al instalar el complemento en Panorama en un par de HA, instale el complemento en el par pasivo antes de hacerlo en el par activo. Después de instalar el complemento en el peer pasivo, pasará a un estado no funcional. La instalación del plugin en el peer activo devuelve el peer pasivo a un estado funcional.

Si tiene un Panorama independiente o dos dispositivos Panorama instalados en un par de alta disponibilidad con varios complementos instalados, es posible que los complementos no reciban información actualizada sobre la etiqueta IP si uno o más de los complementos no están configurados. Esto ocurre porque Panorama no reenviará la información de la etiqueta IP a los complementos no configurados. Además, este problema puede ocurrir si uno o más de los complementos de Panorama no están en el estado Registrado o Correcto (el estado positivo varía según cada complemento). Asegúrese de que sus complementos estén en el estado positivo antes de continuar o ejecutar los comandos que se describen a continuación.

Si encuentra este problema, hay dos soluciones:

- Desinstale el complemento o complementos no configurados. Se recomienda que no instale un complemento que no planifique configurar de inmediato
- Puede utilizar los siguientes comandos para solventar este problema. Ejecute el siguiente comando para cada complemento no configurado en cada instancia de Panorama, para evitar que Panorama espere para enviar actualizaciones. Si no lo hace, sus cortafuegos pueden perder cierta información de la etiqueta IP.

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

  Puede cancelar este comando ejecutando:

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

Los comandos descritos no son persistentes en los reinicios y deben usarse de nuevo para cualquier reinicio posterior. Para Panorama en el par de HA, los comandos deben ejecutarse en cada Panorama.

STEP 1 | Inicie sesión en la interfaz de usuario de Panorama.

STEP 2 | Seleccione **Panorama** > **Plugins (Complementos)**.

STEP 3 | Seleccione **Check Now (Comprobar ahora)** para recuperar una lista de actualizaciones disponibles.

STEP 4 | Seleccione **Download (Descargar)** en la columna Action (Acción) para descargar el plugin.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Seleccione la versión del complemento y haga clic en **Install (Instalar)** en la columna Action (Acción) para instalar el complemento. Panorama le alertará cuando se complete la instalación.

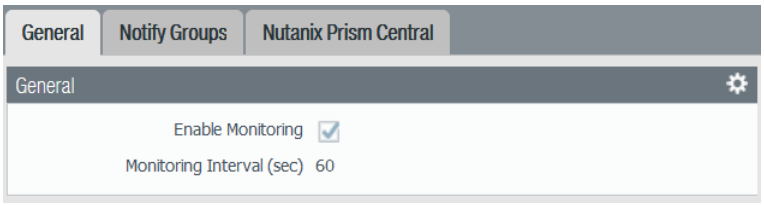
Configuración del complemento de Panorama para Nutanix

Después de instalar el complemento, complete el siguiente procedimiento para establecer una conexión entre Panorama y Prism Central.

STEP 1 | Inicie sesión en la interfaz web de Panorama.

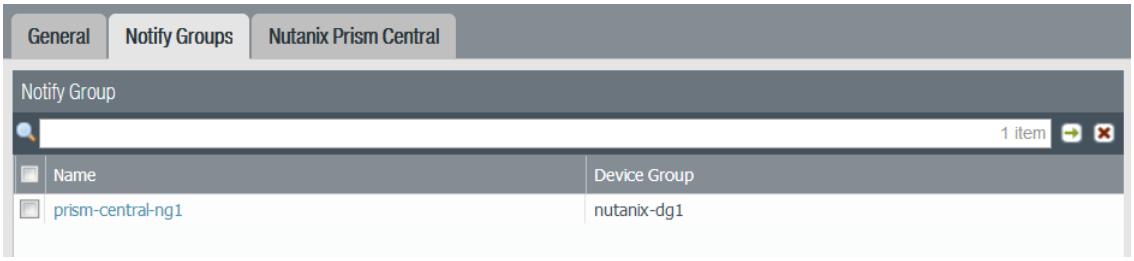
STEP 2 | Habilite la supervisión y establezca el intervalo de supervisión.

1. Seleccione **Panorama** > **Nutanix** > **Configuración** > **General** .
2. Seleccione **Enable Monitoring (Habilitar supervisión)**.
3. Establezca el **Monitoring Interval (Intervalo de supervisión)** en segundos. El intervalo de supervisión es la frecuencia con la que Panorama recupera la información de red actualizada de Prism Central.



STEP 3 | Cree un grupo de notificación.

1. Seleccione **Panorama** > **Nutanix** > **Configuración** > **Grupos de notificación**.
2. Haga clic en **Add (Añadir)**.
3. Introduzca un **Name (Nombre)** descriptivo para el grupo de notificación.
4. Seleccione los grupos de dispositivos en su implementación de Nutanix.



 ©2024 Palo Alto Networks, Inc.

STEP 4 | Añada información de Prism Central.

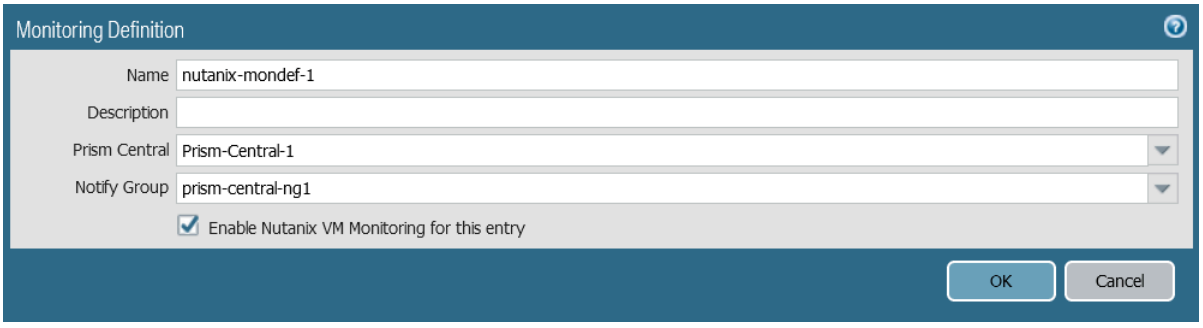
1. Seleccione **Panorama** > **Nutanix** > **Configuración** > **Nutanix Prism Central**.
2. Haga clic en **Add (Añadir)**.
3. Introduzca un **Nombre** descriptivo para su Prism Central.
4. Introduzca la dirección IP o FQDN para Prism Central.
5. Introduzca su nombre de usuario de Prism Central.
6. Introduzca y confirme su contraseña de Prism Central.
7. Haga clic en **Validar** para confirmar que ha introducido las credenciales de Prism Central correctamente.

   Si vuelve a la ventana de información de Nutanix Prism Central después de hacer clic en Aceptar, al hacer clic en el botón Validar, se devuelve un mensaje de error de validación de credencial. Este es el comportamiento previsto. Aunque Panorama muestra puntos en el campo de contraseña, el campo está vacío; esto hace que la validación falle a pesar de que Panorama se conectó con éxito a Prism Central.
8. Haga clic en **OK (Aceptar)**.



STEP 5 | Configure la definición de monitorización.

1. Seleccione **Panorama** > **Nutanix** > **Definición de supervisión** y haga clic en **Añadir**.
2. Introduzca un **Nombre** descriptivo y, opcionalmente, una descripción para identificar el Prism Central para el que utiliza esta definición.
3. Seleccione **Prism Central** y **Grupo de notificación**.
4. Haga clic en **OK (Aceptar)**.

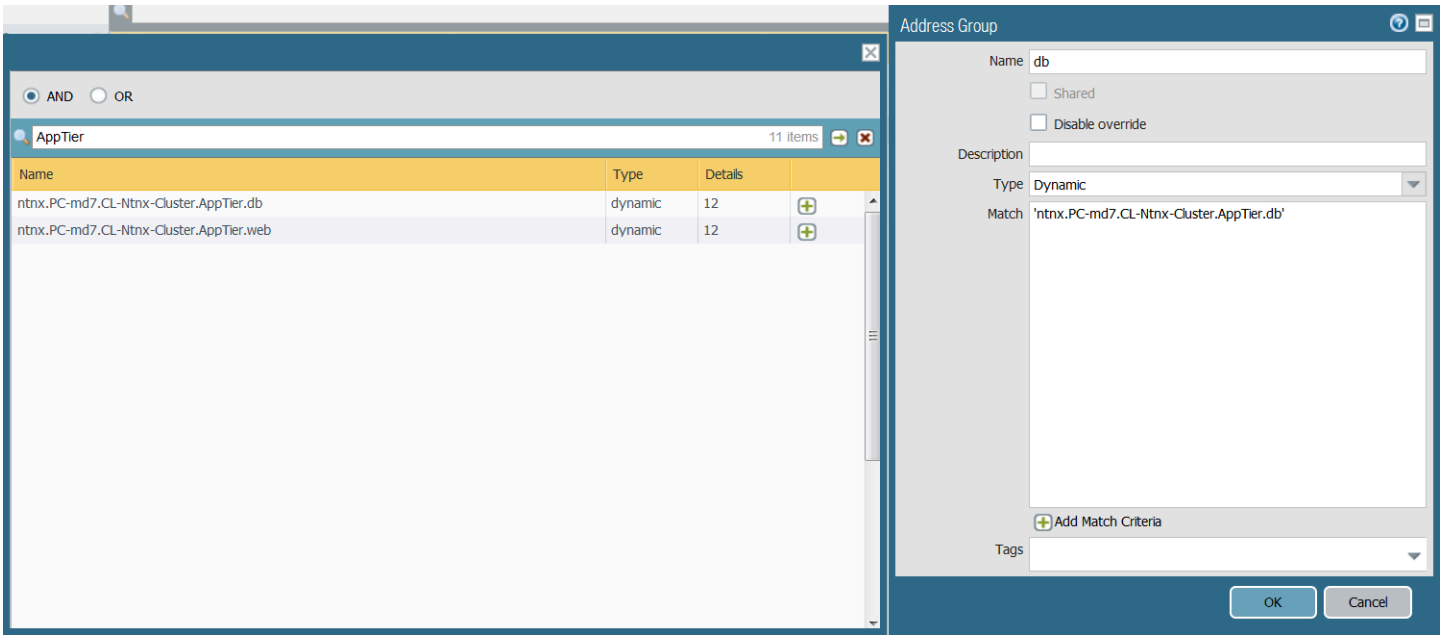


STEP 6 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Compruebe que puede ver la información de la VM en Panorama y defina los criterios de coincidencia para los grupos de direcciones dinámicas.

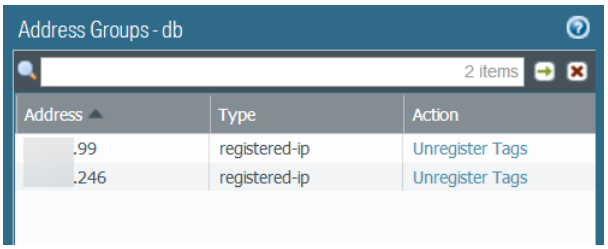
1. Seleccione **Panorama** > **Objetos** > **Grupos de direcciones** y haga clic en **Añadir**.
2. Introduzca un **Nombre** descriptivo para sus grupos de direcciones dinámicas.
3. Seleccione **Dinámico** del menú desplegable Tipo.
4. Haga clic en **Añadir criterios de coincidencia**. Puede seleccionar etiquetas dinámicas como los criterios de coincidencia para añadir miembros del grupo. Seleccione el operador **And** o **Or** y seleccione los atributos por los que desea filtrar o comparar, a continuación haga clic en **Aceptar**.
5. Haga clic en **Commit (Confirmar)** para compilar los cambios.



STEP 8 | Verifique que las direcciones en sus máquinas virtuales se añadan a grupos de direcciones dinámicas.

1. Seleccione **Panorama** > **Objects (Objetos)** > **Address Groups (Grupos de direcciones)**.
2. Haga clic en **Más** en la columna Direcciones de un grupo de direcciones dinámicas.

   Panorama muestra una lista de direcciones IP añadidas a ese grupo de direcciones dinámicas según los criterios de coincidencia que especificó.



 ©2024 Palo Alto Networks, Inc.

STEP 9 | Usar grupos de direcciones dinámicas en la política.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Haga clic en **Add (Añadir)** y escriba un **Name (Nombre)** y una **Description (Descripción)** para la política.
3. Añada la **Source Zone (Zona de origen)** para especificar la zona desde la que se origina el tráfico.
4. Añada la **Destination Zone (Zona de destino)** donde finaliza el tráfico.
5. Para la **Destination Address (Dirección de destino)**, seleccione el grupo de direcciones dinámicas que ha creado anteriormente.
6. Especifique la acción (**Permitir** o **Denegar**) para el tráfico y, de manera opcional, incluya los perfiles de políticas de seguridad en la regla.
7. Repite los pasos del 1 al 6 para crear otra regla de política.
8. Haga clic en **Commit (Confirmar)**.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

Arranque del cortafuegos VM-Series

El arranque le permite crear un proceso repetible y sencillo de implementación de los nuevos cortafuegos VM-Series en su red porque le permite crear un paquete con la configuración del modelo para su red y, posteriormente, utilizar el paquete para implementar los cortafuegos VM-Series en cualquier lugar.

Puede arrancar el cortafuegos con la configuración **completa** para que el cortafuegos esté completamente configurado cuando se inicie, o puede empezar con una configuración **básica**, una configuración inicial mínima que le permite iniciar el cortafuegos y luego regístrese con Panorama para completar la configuración.

Si elige la configuración **básica** y va a implementar en AWS, Azure o GCP, puede usar el paquete de arranque y un archivo `init-cfg.txt`. De forma alternativa, puede arrancar con **datos de usuario**. En lugar de proporcionar parámetros de configuración de arranque en archivos, los introduce como pares clave-valor directamente en la interfaz de usuario de AWS o GCP cuando inicia un cortafuegos VM-Series. Azure tiene un proceso similar con el que proporciona los parámetros de arranque en una plantilla u otro archivo de texto al que se accede desde la CLI de Azure.

Si crea el paquete de arranque, lo entrega desde un dispositivo externo [como un disco virtual, un CD-ROM virtual o un dispositivo de almacenamiento en la nube (como un depósito)].

- Seleccione un método de arranque
- Flujo de trabajo de arranque del cortafuegos VM-Series
- Paquete de arranque
- Archivos de configuración de arranque
- Generación de la clave de autenticación de VM en Panorama
- Creación del archivo init-cfg.txt
- Creación del archivo bootstrap.xml
- Preparación de las licencias para el arranque
- Preparación del paquete de arranque
- Arranque del cortafuegos VM-Series en AWS
- Arranque del cortafuegos VM-Series en Azure
- Arranque del cortafuegos VM-Series en Azure Stack HCI
- Arranque del cortafuegos VM-Series en ESXi
- Arranque del cortafuegos VM-Series en Google Cloud Platform
- Arranque del cortafuegos VM-Series en Hyper-V
- Arranque del cortafuegos VM-Series en KVM
- Verificación de la realización del bootstrap
- Errores de arranque

Seleccione un método de arranque

Puede iniciar el cortafuegos VM-Series con una **configuración básica** o una **configuración completa**.

Una configuración **completa** utiliza el paquete de arranque e incluye todo lo que necesita para configurar por completo el cortafuegos en el arranque. Esto incluye parámetros de configuración (en init-cfg.txt), actualizaciones de contenido y versiones de software. Una configuración completa puede incluir archivos init-cfg.txt y archivos bootstrap.xml.

Método de configuración	Ubicación de la configuración	Comentarios
Especifique la información de configuración completa en /config/bootstrap.xml en el paquete de arranque.	**Almacenamiento en la nube pública** Depósito de AWS S3, cuenta de almacenamiento de Azure o depósito de almacenamiento de Google.	• Paquete de arranque completo en el depósito de almacenamiento. • Requiere almacenamiento en la nube y una función de IAM para acceder a él.

Una configuración **básica** es una configuración mínima que le permite iniciar, licenciar y registrar el cortafuegos VM-Series. La configuración básica no admite complementos, contenido, imágenes de software o bootstrap.xml.

Después de iniciar el cortafuegos, puede conectarse con Panorama para completar la configuración o iniciar sesión en el cortafuegos para actualizar el contenido y el software manualmente. La siguiente tabla contrasta brevemente tres formas en las que puede almacenar y acceder a una configuración básica:

Método de configuración	Ubicación de la configuración	Comentarios
init-cfg.txt Almacene los parámetros de configuración básicos como pares clave-valor en config/init-cfg.txt en el paquete de arranque.	**Almacenamiento en la nube pública** • Depósito de AWS S3 • Cuenta de almacenamiento de Azure • Depósito de almacenamiento de GCP	• Requiere almacenamiento en la nube y una función de IAM para acceder a él. El administrador de Panorama también debe tener acceso al depósito.
Datos de usuario Introduzca los parámetros de configuración en la interfaz de usuario de la nube pública como pares clave-valor.	**Instancia de VM** • AWS: Datos de usuario • Azure: Datos personalizados • GCP: Metadatos de GCP	• Los parámetros de configuración inicial se almacenan con la máquina virtual. • No es necesario un almacenamiento independiente y la función de IAM asociada.
AWS Secret Manager	Cifrado en AWS Secret Manager.	• Necesita una función de IAM para crear un secreto. A otros se

 ©2024 Palo Alto Networks, Inc.

Método de configuración	Ubicación de la configuración	Comentarios
Introduzca los parámetros de configuración en AWS secret manager como pares clave-valor.		les puede otorgar permiso para obtener el secreto. • Para obtener el secreto, pase el nombre secreto utilizando los datos del usuario.

Consulte el flujo de trabajo de arranque del cortafuegos VM-Series para comparar el flujo de trabajo de las configuraciones básica y completa.

- Configuración básica
- Configuración completa

Configuración básica

Una configuración básica incluye la configuración inicial y las licencias. Puede utilizar el paquete de arranque para pasar los pares clave-valor para la configuración inicial, o puede introducir los pares clave-valor de los parámetros bootstrap como datos de usuario.

Si no utiliza Panorama, puede usar la configuración inicial para arrancar el cortafuegos, luego iniciar sesión y completar la configuración manualmente. Si utiliza Panorama, su configuración inicial debe incluir parámetros de arranque para las direcciones IP de sus servidores de Panorama y la clave de autenticación de VM para que el cortafuegos arrancado se pueda registrar con Panorama y completar la configuración completa.

- Añadir una configuración básica al paquete de arranque
- Introduzca una configuración básica como datos de usuario (AWS, Azure o GCP)
- Guardar una configuración básica en AWS Secrets Manager

Añadir una configuración básica al paquete de arranque

La configuración inicial es una configuración mínima que le permite iniciar, licenciar y registrar el cortafuegos VM-Series, y conectarse con Panorama, si corresponde. La configuración se entrega en (init-cfg.txt) en el paquete de arranque.

Introduzca una configuración básica como datos de usuario (AWS, Azure o GCP)

Cuando incluye parámetros de conectividad de Panorama en su init-cfg.txt, Panorama intenta enviar la configuración al cortafuegos VM-Series tras la primera conexión. La conexión a Panorama falla si faltan valores de nombre de host, pila de plantillas o grupo de dispositivos en el archivo init-cfg.txt.

Cuando implementa el cortafuegos VM-Series desde la interfaz de usuario de AWS, Azure o GCP, puede introducir los parámetros de configuración como datos de usuario durante el proceso de lanzamiento/implementación. Si tiene permisos suficientes para implementar un cortafuegos desde su cuenta en la nube y acceder a Panorama (si lo está usando), puede omitir la creación de un paquete de arranque, la creación de archivos de configuración y otras tareas de arranque relacionadas con el almacenamiento en la nube (un depósito de almacenamiento, Funciones de IAM o cuentas de servicio que otorgan acceso externo al almacenamiento).

 ©2024 Palo Alto Networks, Inc.

Los parámetros de configuración incluyen los valores en Componentes de archivo de init-cfg.txt, y los siguientes valores adicionales solo están disponibles como datos de usuario:

- **`authcodes`**: el código de autenticación que se utiliza para registrar el cortafuegos VM-Series. Por ejemplo, **`authcodes = I7115398`**.
- **`mgmt-interface-swap`**: se usa para intercambiar la interfaz de administración cuando el cortafuegos VM-Series está detrás de un balanceador de carga en una implementación de AWS o GCP. Por ejemplo, **`mgmt-interface-swap=enable`**.

Puede introducir parámetros de configuración como pares clave-valor directamente en la interfaz de usuario de AWS o GCP. También puede definir la configuración desde un archivo de texto o una plantilla nativa de la nube, como una plantilla AWS Cloud Formation, una plantilla Azure ARM, un archivo YAML de GCP o una plantilla Terraform.

Cada nube tiene un término diferente para los datos del usuario y utiliza diferentes separadores entre los parámetros de arranque.

- **Datos de usuario de AWS**: use un punto y coma o nueva línea (\n). Si un parámetro tiene más de una opción, separe las opciones con una coma. Por ejemplo:

  Si elige guardar su configuración básica en AWS Secrets Manager, introduzca el nombre secreto como un par clave-valor en el campo de datos del usuario. Por ejemplo:

```
  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>
```

- **Datos personalizados de Azure**:use un punto y coma. Si un parámetro tiene más de una opción, separe las opciones con una coma. Por ejemplo:

```
type=dhcp-client; op-command-modes=jumbo-frame; vm-series-auto-
registration-pin-id=abcdefgh1234****; vm-series-auto-registration-
pin-value=zyxwvut-0987****
```

- **Metadatos personalizados de GCP**: en un archivo, como un archivo YAML o una plantilla de Terraform, use una línea nueva (\n) para cada parámetro y, si un parámetro tiene varias opciones, use comas para separarlas. Por ejemplo:

```
type=dhcp-client op-command-modes=mgmt-interface-swap,jumbo-frame
 vm-series-auto-registration-pin-id=abcdefgh1234**** vm-series-
auto-registration-pin-value=zyxwvut-0987****
```

 ©2024 Palo Alto Networks, Inc.

Guardar una configuración básica en AWS Secrets Manager

Puede utilizar AWS Secrets Manager para almacenar la configuración básica como un secreto y luego usar los datos de usuario para arrancar una máquina virtual con los parámetros almacenados en el secreto. Para realizar esta tarea, necesita permiso para utilizar Secrets Manager.

- El creador del secreto debe tener permisos de administrador completos de Secrets Manager. Un administrador de Secrets Manager puede permitir que otros usen el secreto, como se describe en Autenticación y control de acceso para AWS Secrets Manager.

  Por ejemplo, la siguiente declaración de política le permite obtener el valor secreto:

  ```
  { "Version": "2012-10-17", { "Effect": "Allow",
   "Action": "secretsmanager:GetSecretValue", "Resource":
   "arn:aws:secretsmanager:us-east-1:688382******:secret:My_bts-
  ******" } }
  ```

  Consulte Acciones, recursos y claves de contexto que puede utilizar en una política de IAM o una política secreta para AWS Secrets Manager para ver las acciones que requieren permiso, como enumerar, obtener y girar secreto.
- (Opcional) Para cifrar el secreto, puede utilizar DefaultEncryptionKey de AWS Secrets Manager.

STEP 1 | Inicie sesión en la consola de AWS y en seguridad, identidad y cumplimiento, seleccione **Secrets Manager** y seleccione **Store a new secret (Almacenar un nuevo secreto)**.

STEP 2 | Seleccione **other type of secrets (otro tipo de secretos)**.

1. Introduzca los pares clave-valor para definir la configuración básica.

   mgmt-interface-swap *no funciona como un par clave-valor en un secreto de AWS. Se debe introducir como:* ***op-command-modes=mgmt-interface-swap***

2. Seleccione DefaultEncryptionKey y haga clic en **Next (Siguiente)**.

STEP 3 | Proporcione el nombre secreto y la descripción.

1. Edite los permisos de recursos para acceder de forma segura a secretos en todas las cuentas de AWS. Por ejemplo:

   ```
   { "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" } ] }
   ```

 ©2024 Palo Alto Networks, Inc.

2. (Opcional) Puede examinar el secreto desde la línea de comando (si tiene permiso). Por ejemplo:

```
# 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-
santosh\",\"license-authcode\":\"AAAA\"}", "VersionStages":
 [ "AWSCURRENT" ], "CreatedDate": 1581018411.847 }
```

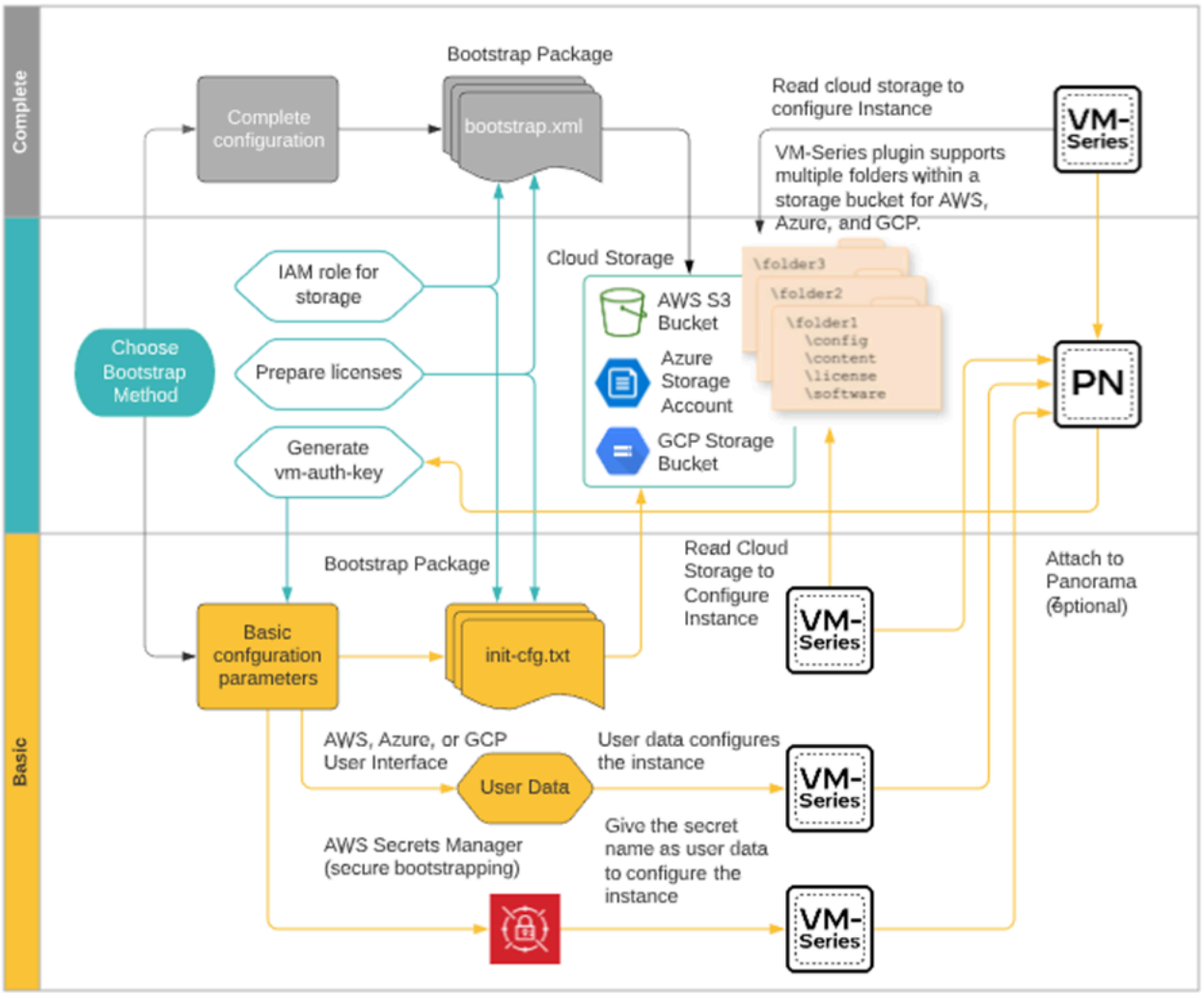
Configuración completa

Una configuración completa garantiza que el cortafuegos esté completamente configurado al arrancar. El archivo bootstrap.xml incluye la configuración inicial, licencias, software, contenido y una versión del complemento VM-Series. Puede crear `bootstrap.xml` manualmente o puede exportar una configuración existente, como se describe en Crear el archivo bootstrap.xml .

 ©2024 Palo Alto Networks, Inc.

Flujo de trabajo de arranque del cortafuegos VM-Series

Utilice el siguiente flujo de trabajo para arrancar su cortafuegos VM-Series. Consulte la siguiente figura para obtener una descripción general de los procedimientos de arranque básicos y completos.



STEP 1 | (Opcional) Por razones de seguridad, solo se puede arrancar un cortafuegos cuando se encuentra en su estado de fábrica. Si desea utilizar el paquete de arranque para arrancar un cortafuegos VM-Series que se haya configurado previamente, realice un restablecimiento del cortafuegos a los ajustes predeterminados de fábrica.

STEP 2 | Seleccione un método de arranque.

Después de familiarizarse con el paquete de arranque, evalúe si desea utilizar una configuración completa, o una configuración básica y, opcionalmente, utilizar Panorama para gestionar el cortafuegos activo.

Si elige una configuración básica, decida si usar el paquete de arranque o introducir los parámetros de configuración como pares clave-valor en los datos de usuario.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | (Opcional) Si desea utilizar Panorama para gestionar los cortafuegos VM-Series que se están iniciando, genere la clave de autenticación de VM en Panorama. Debe incluir esta clave en el archivo `init-cfg.txt` (**`vm-auth-key`**) o introducir el par clave-valor como datos de usuario.

STEP 4 | Preparación de las licencias para el arranque.

El mecanismo de recuperación de licencias solo funciona con la interfaz de gestión de VM-Series. Las rutas de servicio no son compatibles porque ocurren después de recuperar la licencia.

STEP 5 | Si selecciona la configuración básica y planea arrancar con datos del usuario, vaya al Paso 7.

Si considera utilizar la configuración básica y el paquete de arranque, cree el archivo init-cfg.txt y prepare el paquete de arranque.

Si elige la configuración completa, cree el archivo bootstrap.xml y prepare el paquete de arranque completo.

STEP 6 | Prepare el paquete de arranque y guárdelo en el formato de entrega adecuado para su hipervisor.

STEP 7 | Arranque del cortafuegos VM-Series.

- Arranque del cortafuegos VM-Series en AWS
- Arranque del cortafuegos VM-Series en Azure
- Arranque del cortafuegos VM-Series en ESXi
- Arranque del cortafuegos VM-Series en Google Cloud Platform
- Arranque del cortafuegos VM-Series en Hyper-V
- Arranque del cortafuegos VM-Series en KVM

STEP 8 | Verificación de la realización del arranque.

 ©2024 Palo Alto Networks, Inc.

Paquete de arranque

El proceso de bootstrap se inicia solamente con el primer inicio cuando el cortafuegos está en estado por defecto de fábrica.

- Estructura del paquete de arranque
- Entrega del paquete de arranque

Estructura del paquete de arranque

El paquete de arranque debe incluir las carpetas `/config`, `/license`, `/software` y `/content`, incluso si están vacías. La carpeta `/plugins` es opcional. Para ver un ejemplo, consulte Preparación del paquete de arranque.

- **/carpeta config**: Contiene los archivos de configuración. La carpeta puede tener dos archivos: `init-cfg.txt` y `bootstrap.xml`. Para obtener detalles, consulte Archivos de la configuración de arranque.

  Si desea pre-registrar cortafuegos VM-Series en Panorama con bootstrapping, debe generar una clave de autenticación de VM en Panorama e incluir la tecla generada en el archivo `init-cfg`. Consulte Generación de la clave de autenticación de VM en Panorama.

- **/carpeta licencia**: Contiene las teclas de licencia o códigos de autenticación para las licencias y suscripciones que tiene previsto activar en los cortafuegos. Si el cortafuegos no tiene conectividad de Internet, deberá obtener manualmente las claves de licencia del portal de Asistencia de Palo Alto Networks o utilizar la API de licencias para obtener las claves y guardar cada clave en la carpeta. Para más detalles, consulte Preparación de las licencias de arranque.

  Debe incluir un lote de códigos de autenticación en vez de códigos de autenticación individuales, de modo que el cortafuegos o el servicio de orquestación pueda recoger al mismo tiempo todas las teclas asociadas con un cortafuegos. Si utiliza códigos de autenticación individuales, en vez de un lote, el cortafuegos recuperará solamente la clave de licencia para el primer código de autenticación del archivo.

- **/carpeta software**: Contiene las imágenes de software necesarias para actualizar un cortafuegos recién abastecido a la versión PAN-OS deseada para su red. Debe incluir todas las versiones de software intermedias entre la versión actual y la versión de software final de PAN-OS a la que desea actualizar el cortafuegos VM-Series. Consulte Soporte del hipervisor de cortafuegos VM-Series en la Matriz de compatibilidad.
- **/carpeta contenido**: Contiene las actualizaciones de la aplicación y de amenazas, actualizaciones de WildFire y la base de datos de filtración de URL de BrightCloud para las suscripciones válidas en el cortafuegos VM-Series. Debe incluir las versiones de contenido mínimas requeridas para la versión de PAN-OS deseada. Si no tiene la versión de contenido mínima requerida asociada con la versión de PAN-OS, el cortafuegos VM-Series no puede completar la actualización del software.
- **/ carpeta de complementos**: Opcional la carpeta contiene una única imagen del Plugin VM-Series.
- **/carpeta ace**: Opcional la carpeta contiene un paquete de contenido de App-ID Cloud Engine (ACE). VM-Series instala la versión del catálogo Cloud App-ID incluida en el paquete de contenido en el

 ©2024 Palo Alto Networks, Inc.

primer arranque. Debe descargar el paquete de contenido del Portal de atención al cliente y añadirlo a la carpeta **ace** . Para descargar el paquete de contenido, complete los siguientes pasos.

1. Inicie sesión en el Portal de atención al cliente.
2. Seleccione **Updates (Actualizaciones)** > **Dynamic Updates (Actualizaciones dinámicas)**.
3. Seleccione **Bootstrap files for VM Flex with SaaS Subscription (Archivos de arranque para la suscripción VM Flex with SaaS)** en el menú desplegable Tipo de contenido.
4. Seleccione un paquete de contenido y haga clic en **Download (Descargar)**.

Entrega del paquete de arranque

El tipo de archivo utilizado para enviar el paquete de arranque al cortafuegos VM-Series varía según su supervisor. Utilice la tabla a continuación para determinar el tipo de archivo que admite su hipervisor o proveedor de nube.

Dispositivo externo para bootstrapping (formato de paquete de arranque)	AWS	Azure	ESXi	Google	Hyper-V	KVM
CD-ROM (imagen ISO)	—	—	Sí	—	Sí	Sí
Dispositivo de almacenamiento en bloque	—	—	Sí	—	Sí	Sí
Cuenta de almacenamiento	—	Sí	—	—	—	—
Paquete de almacenamiento	Sí	—	—	Sí	—	—

Cuando se adjunta el dispositivo de almacenamiento al cortafuegos, el cortafuegos busca un paquete de arranque y, si existe, el cortafuegos utiliza los ajustes definidos en el paquete de arranque.

Si ha incluido una dirección IP de servidor Panorama en el archivo, el cortafuegos se conecta con Panorama. Si el cortafuegos tiene conectividad con Internet, se pone en contacto con el servidor de licencias para actualizar la UUID y obtener las claves de licencia y suscripciones. A continuación, el cortafuegos se añade como activo en el portal de Asistencia de Palo Alto Networks. Si el cortafuegos no tiene conectividad de Internet, utiliza las teclas de licencia que ha incluido en el paquete de arranque, o se conecta con Panorama para recuperar las licencias apropiadas y las implementa para los cortafuegos gestionados.

 ©2024 Palo Alto Networks, Inc.

Archivos de configuración de arranque

El paquete de arranque debe incluir la configuración básica en `config / init-cfg.txt`. La configuración completa (en el archivo `/config/bootstrap.xml`) es opcional.

Cuando incluye los archivos `init-cfg.txt` y `bootstrap.xml` en el paquete de arranque, el cortafuegos fusiona las configuraciones de esos archivos y, si alguna configuración se superpone, el cortafuegos utiliza los valores definidos en el archivo `init-cfg.txt`.

- init-cfg.txt
- bootstrap.xml

init-cfg.txt

Incluye información básica para la configuración de la interfaz de gestión del cortafuegos, como el tipo de dirección IP (estática o DHCP), dirección IP (IPv4 solo o ambos IPv4 e IPv6), máscara de red y puerta de enlace por defecto. La dirección IP del servidor DNS, la dirección IP de Panorama y los parámetros del grupo de dispositivos y plantillas son opcionales.

Puede utilizar el nombre genérico `init-cfg.txt`, o para ser más específico, puede anteponer el UUID o número de serie de cada cortafuegos al nombre de archivo (por ejemplo: `0008C100105-init-cfg.txt`).

Cuando se inicia el cortafuegos, busca un archivo de texto que coincide con su UUID o número de serie y, si no se encuentra ninguno, busca utilizando el nombre de archivo genérico `init-cfg.txt`. Para un archivo de muestra, consulte Creación del archivo init-cfg.txt.

Si usa Panorama para administrar sus cortafuegos VM-Series iniciados:

- *Debe generar una clave de autenticación de máquina virtual en Panorama e incluir la clave en el archivo `init-cfg.txt`. Para obtener más información, consulte* Generación de la clave de autenticación de VM en Panorama.
- *El dispositivo Panorama que administra los cortafuegos debe estar en el modo de Panorama. Si usa un dispositivo Panorama en el modo Management-Only (Solo gestión), se descartan los logs del cortafuegos porque Panorama en el modo de solo gestión no tiene un grupo de recopiladores de logs que pueda almacenar logs del cortafuegos.*
- *Cuando incluye parámetros de conectividad de Panorama en su init-cfg.txt, Panorama intenta enviar la configuración al cortafuegos VM-Series tras la primera conexión. La conexión a Panorama falla si faltan valores de nombre de host, pila de plantillas o grupo de dispositivos en el archivo init-cfg.txt.*

bootstrap.xml

El archivo opcional `bootstrap.xml` contiene una configuración completa para el cortafuegos. Si no usa Panorama para administrar sus cortafuegos de forma centralizada, el archivo `bootstrap.xml` proporciona una forma de automatizar el proceso de implementación de cortafuegos que se configuran en el inicio.

 ©2024 Palo Alto Networks, Inc.

Puede definir la configuración manualmente o exportar la configuración en ejecución (`running-config.xml`) desde un cortafuegos existente y guardar el archivo como `bootstrap.xml`. Si exporta el archivo `bootstrap.xml`, asegúrese de exportar el archivo XML desde un cortafuegos implementado en la misma plataforma o hipervisor que su implementación. Consulte Creación del archivo bootstrap.xml.



Para garantizar un arranque correcto para el enrutamiento avanzado utilizando los archivos init-cfg.txt y bootstrap.xml, habilite el enrutamiento avanzado tanto en* init-cfg.txt* como en bootstrap.xml. Si no se habilita el Enrutamiento avanzado en ambos archivos, se podría generar un entorno inestable; por ejemplo, si utiliza* ***show advanced routing route,*** *el resultado indica que el enrutamiento avanzado está habilitado; sin embargo, el comando* ***show deviceconfig setting*** *indica que enrutamiento avanzado no está habilitado. Además, el enrutamiento avanzado no funcionará al 100% y puede terminar en un error de confirmación. Si la configuración se encuentra en el estado anterior, para habilitar el enrutamiento avanzado, reinicie el cortafuegos VM-Series después de configurar* ***set deviceconfig setting advanced-routing yes***

.

 ©2024 Palo Alto Networks, Inc.

Generación de la clave de autenticación de VM en Panorama

Si desea utilizar Panorama para gestionar los cortafuegos VM-Serie que está bootstrapping, debe generar una clave de autenticación de VM en Panorama e incluir la clave de la configuración básica (init-cfg.txt). La clave de autenticación VM permite a Panorama autenticar el cortafuegos VM-Series que acaba de bootstrap. Por tanto, para gestionar el cortafuegos con Panorama, debe incluir la dirección IP para Panorama y la clave de autenticación de VM del archivo de configuración básica, además de los códigos de autenticación de la licencia en la carpeta /license del paquete de arranque. El cortafuegos puede proporcionar la dirección IP, el número de serie y la tecla de autenticación de VM en su solicitud de conexión inicial a Panorama, de modo que Panorama pueda verificar la validez de la clave de autenticación de VM y añadir el cortafuegos como dispositivo gestionado. Si facilita un grupo de dispositivos y una plantilla en el archivo de configuración básica, Panorama asignará el cortafuegos al grupo de dispositivos y la plantilla apropiados, de modo que pueda configurar centralmente y administrar el cortafuegos con Panorama.

La vida útil de la tecla puede variar entre 1 hora y 8760 horas (un año). Tras el tiempo especificado, la clave expira y Panorama no registrará los cortafuegos VM-Series sin una tecla de autenticación válida en esta solicitud de conexión.

STEP 1 | Inicie sesión en el CLI de Panorama o acceda a la API:

- En la CLI, use el siguiente comando de operación:

  ```
  request bootstrap vm-auth-key generate lifetime <1-8760>
  ```

  Por ejemplo, para generar una tecla con validez de 24 horas, introduzca lo siguiente:

  ```
  request bootstrap vm-auth-key generate lifetime 24
  VM auth key 755036225328715 generated. Expires at: 2015/12/29
   12:03:52
  ```

- En la API, utilice la siguiente URL:

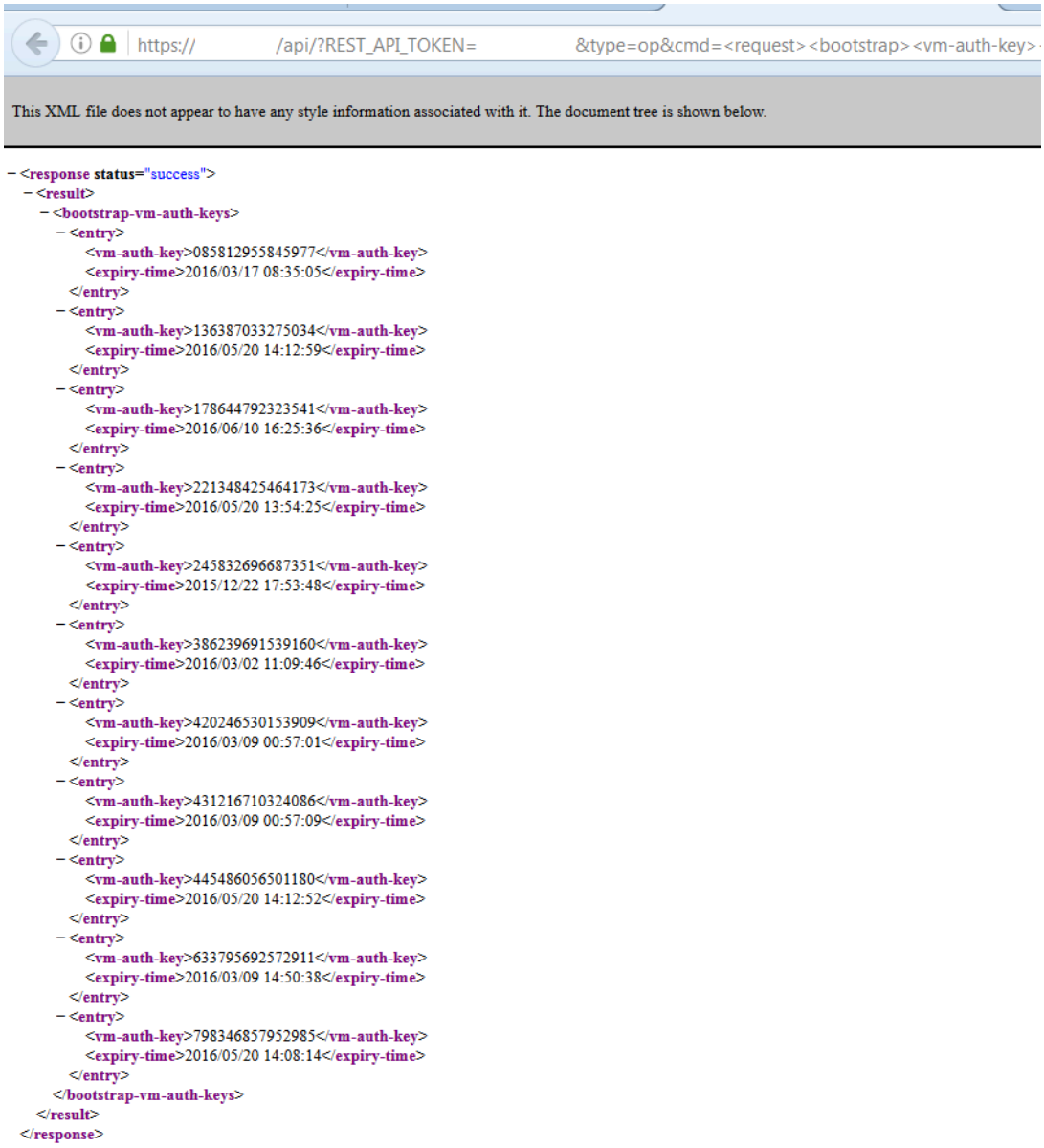
  ```
  https://<Panorama_IP_address>/api/?
  type=op&cmd=<request><bootstrap><vm-auth-
  key><generate><lifetime><number-of-hours></lifetime></generate></
  vm-auth-key></bootstrap></request>
  ```

  donde la vida útil es el número de horas para las que tiene validez la clave de autenticación de VM.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Verifique la duración de validez de la clave o claves de autenticación de VM generadas en Panorama. Asegúrese de que la duración permita el tiempo suficiente para el registro del o de los cortafuegos en Panorama.

```
https://<Panorama_IP_address>/api/?
type=op&cmd=<request><bootstrap><vm-auth-key><show></show></vm-
auth-key></bootstrap></request>
```



STEP 3 | Añada la clave de autenticación de VM generada al archivo de configuración básica (init-cfg.txt). Consulte Creación del archivo init-cfg.txt.

STEP 4 | Compruebe que la clave de autenticación de registro de dispositivo que ha generado se ha creado correctamente.

```
request bootstrap vm-auth-key show
```

 ©2024 Palo Alto Networks, Inc.

Creación del archivo init-cfg.txt

El archivo `init-cfg.txt` es necesario para arrancar el cortafuegos VM-Series. Este proporciona la información básica que el cortafuegos necesita para conectarse a su red.

- Componentes de archivo de init-cfg.txt
- Archivo de muestra de init-cfg.txt

Complete el siguiente procedimiento para crear el archivo `init-cfg.txt`.

STEP 1 | Cree un nuevo archivo de texto.

Utilice un editor de texto, como Notepad, EditPad u otros editores de texto para crear un archivo de texto.

STEP 2 | Añada la configuración de red básica para la interfaz de gestión del cortafuegos.



Si falta en el archivo alguno de los parámetros necesarios, el cortafuegos sale del proceso de bootstrap y se inicia utilizando la dirección IP por defecto 192.168.1.1. Puede visualizar el log del sistema en el cortafuegos para detectar la razón del fallo del bootstrap. Para errores, consulte API de licencias.



No hay espacios entre la clave y el valor de cada campo. No añada espacios porque pueden causar fallos durante el análisis en el lado mgmtsrvr.

- Para configurar la interfaz de gestión con una dirección IP estática, debe especificar la dirección IP, el tipo de dirección, la puerta de enlace por defecto y la máscara de red. Se requiere una dirección IPv4, la dirección IPv6 es opcional. Para la sintaxis, consulte Archivo init-cfg.txt de muestra.
- Para configurar la interfaz de gestión como cliente DHCP, debe especificar solamente el tipo de dirección. Si habilita el cliente DHCP en la interfaz de gestión, el cortafuegos ignora los valores de dirección IP, puerta de enlace por defecto, máscara de red, dirección IPv6 y de puerta de enlace IPv6 por defecto definidos en el archivo. Para la sintaxis, consulte Archivo init-cfg.txt de muestra.

Cuando habilite DHCP en la interfaz de gestión, el cortafuegos toma la dirección IP asignada a DHCP y se puede acceder en la red. Puede visualizar la dirección IP asignada en DHCP en el widget de información general del panel o con el comando CLI **`show system info`**. Sin embargo, la dirección IP de gestión estática por defecto 192.168.1.1 se conserva en la configuración en ejecución (**`show config running`**) del cortafuegos. Esta dirección IP estática garantiza que siempre pueda recuperar la conectividad con el cortafuegos, si pierde el acceso DHCP al cortafuegos.

STEP 3 | Añada la clave de autenticación de VM para registrar un cortafuegos VM-Series con Panorama.

Para añadir un cortafuegos VM-Series en Panorama, debe añadir la clave de autenticación de VM que ha generado en Panorama al archivo de configuración básica (`init-cfg.txt`). Para obtener más información sobre cómo generar una clave, consulte Generación de la clave de autenticación de VM en Panorama.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Añada detalles para el acceso a Panorama.

- Añada las direcciones IP para los servidores Panorama principal y secundario.
- Un nombre de host de cortafuegos.
- Especifique la plantilla y el grupo de dispositivos a los que desea asignar el cortafuegos.
- Para especificar el Strata Cloud Manager para su host Panorama, use `set panorama-server=cloud` para iniciar una conexión TLS con el borde del servicio de gestión en la nube.

> *Cuando incluye parámetros de conectividad de Panorama en su init-cfg.txt, Panorama intenta enviar la configuración al cortafuegos VM-Series tras la primera conexión. La conexión a Panorama falla si faltan valores de nombre de host, pila de plantillas o grupo de dispositivos en el archivo init-cfg.txt.*

STEP 5 | (Recomendado) Añada el pin de registro de VM-Series y el valor para instalar el certificado del dispositivo.

Si desea instalar el certificado del dispositivo en el cortafuegos VM-Series en el momento del inicio, debe generar el ID y el valor del pin del registro de VM-Series en el CSP e incluirlo en el archivo `init-cfg. txt`. Este pin y valor también se aplica a cualquier licencia de sitio que use la licencia PAYG.

STEP 6 | Opcional Incluya los parámetros adicionales para el cortafuegos.

- Añada la dirección IP para los servidores DNS principal y secundario.
- Añada el nombre de host para el cortafuegos.
- Habilite tramas gigantes o sistemas virtuales múltiples (o ambos)
- Habilite el intercambio de interfaz de gestión (mgmt) y la interfaz del plano de datos (ethernet 1/1) para el cortafuegos VM-Series en AWS o GCP. Para obtener más información sobre cómo cambiar la interfaz de gestión, consulte Asignación de interfaz de gestión para su uso con el servicio Amazon ELB o Intercambio de interfaces de gestión para el equilibrio de carga de Google Cloud Platform.
- Habilitar o deshabilitar DPDK.

Componentes de archivo de init-cfg.txt

La siguiente tabla describe los parámetros de arranque en el archivo `init-cfg.txt`.

Campo	Description (Descripción)
type=	Tipo de dirección IP de gestión: estática o cliente dhcp. Este campo es obligatorio.
ip-address=	Dirección IPv4. Este campo se ignora si el tipo es cliente dhcp. Si el tipo es estático, se requiere una dirección IPv4; el campo dirección ipv6 es opcional y se puede incluir. No puede especificar la dirección IP de gestión y la configuración de máscara de red para el cortafuegos VM-Series en AWS y Azure. Si se ha definido, el cortafuegos ignora los valores especificados por usted.

 ©2024 Palo Alto Networks, Inc.

Campo	Description (Descripción)
default-gateway=	Puerta de enlace por defecto IPv4 para la interfaz de gestión. Este campo se ignora si el tipo es cliente dhcp. Si el tipo es estático, y se utiliza una dirección ip, este campo es obligatorio.
netmask=	Máscara de red IPv4. Este campo se ignora si el tipo es cliente dhcp. Si el tipo es estático, y se utiliza una dirección ip, este campo es obligatorio.
ipv6-address=	Dirección IPv6 y longitud del prefijo /de la interfaz de gestión. Este campo se ignora si el tipo es cliente dhcp. Si el tipo es estático, este campo se puede especificar junto con el campo dirección ip necesario.
ipv6-default-gateway=	Puerta de enlace por defecto IPv6 para la interfaz de gestión. Este campo se ignora si el tipo es cliente dhcp. Si el tipo es estático, y se utiliza una dirección ipv6, este campo es obligatorio.
hostname=	Nombre de host para el cortafuegos. Este campo es obligatorio cuando se añaden parámetros de configuración de Panorama.
panorama-server=	Dirección IPv4 o IPv6 del servidor Panorama principal. Este campo no es obligatorio, pero se recomienda para gestionar de forma centralizada sus cortafuegos. Al crear un paquete de arranque, establezca **panorama-server=cloud**. El parámetro cloud se debe utilizar al conectar el cortafuegos a Strata Cloud Manager. *Cuando proporciona una dirección IP de Panorama en su archivo init-cfg.txt, Panorama envía la configuración al cortafuegos automáticamente en la primera conexión.*
panorama-server-2=	Dirección IPv4 o IPv6 del servidor Panorama secundario. Este campo no es obligatorio, sino recomendado. Un valor definido para **panorama-server-2** se ignora cuando se utiliza **panorama-server=cloud**.
tplname=	Nombre de la pila de plantillas de Panorama. Si añade una dirección IP del servidor Panorama, debe incluir un nombre de pila de plantilla en este campo para que pueda gestionar y enviar los ajustes de configuración de forma centralizada al cortafuegos. Si no incluye un nombre de pila de plantillas, se produce un error en la conexión de los cortafuegos a Panorama.
dgname=	Nombre del grupo de dispositivos de Panorama. Si añade una dirección IP del servidor Panorama, debe incluir un nombre de grupo de dispositivos en este campo para que pueda agrupar los cortafuegos de forma lógica y enviar reglas de políticas al cortafuegos. Si no incluye un nombre de grupo

 ©2024 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	de dispositivos, se produce un error en la conexión de los cortafuegos a Panorama.
cgname=	Nombre del grupo del recopilador Panorama. Si desea arrancar el cortafuegos para enviar logs a un grupo de recopiladores de Panorama, primero debe configurar un grupo de recopiladores en Panorama y, a continuación, configurar el cortafuegos para reenviar logs a Panorama. Los dispositivos M-Series tienen predefinido un grupo de recopiladores predeterminado que ya incluye como miembro al recopilador de logs local. En el dispositivo virtual Panorama, debe añadir el grupo de recopiladores y añadir el recopilador de logs local como miembro.
dns-primary=	Dirección IPv4 o IPv6 del servidor DNS principal.
dns-secondary=	Dirección IPv4 o IPv6 del servidor DNS secundario.
vm-auth-key=	Clave de autenticación de máquina virtual para Panorama (consulte Generación de la clave de autenticación de VM en Panorama). Este campo se ignora cuando se hace el bootstrapping de cortafuegos de hardware.

op-command-modes=	Se permiten los siguientes valores: multi-vsys, jumbo-frame, mgmt-interface-swap. Si introduce valores múltiples, utilice un espacio o una coma para separar las entradas.
	• **multi-vsys**: Solo para cortafuegos basados en hardware, habilita múltiples sistemas virtuales.
	• **Tramas gigantes**: habilita el tamaño predeterminado de MTU para todas las interfaces de Capa 3 que se establece en 9192 bytes.
	• **mgmt-interface-swap**: Solo para cortafuegos VM-Series en AWS, Google, ESXi y KVM, permite intercambiar la interfaz de gestión (management, MGT) con la interfaz del plano de datos (ethernet 1/1) cuando se implementa el cortafuegos. Para obtener más detalles, consulte
	  • Asignación de interfaz de gestión para su uso con Amazon ELB
	  • Intercambio de interfaces de gestión para el equilibrio de carga de Google Cloud Platform
	  • Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión en ESXi
	  • Uso de la CLI del cortafuegos VM-Series para intercambiar la interfaz de gestión en KVM

op-cmd-dpdk-pkt-io=	El valor **activado** o desactivado le permite habilitar o deshabilitar el Kit de desarrollo de plano de datos (Data Plane Development Kit, DPDK) en entornos donde el **cortafuegos es compatible con DPDK**. DPDK permite que el host procese los paquetes más rápido eludiendo

 ©2024 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	el kernel de Linux; las interacciones con el NIC se realizan utilizando controladores y las bibliotecas DPDK.
plugin-op-commands=	Especifique los comandos de operación del complemento de VM-Series. *Se deben introducir varios comandos en una sola lista separada por comas y sin espacios.* • **`sriov-access-mode-on`**: este comando solo es válido para el cortafuegos VM-Series en los hipervisores ESXi y KVM. Solo para KVM, si habilita **`sriov-acceso-mode-on`**, no habilite **`op-command-modes = jumbo-frame`**. • **`aws-gwlb-inspect:enable`**: habilita Integración de VM-Series con un balanceador de carga Gateway de AWS. • **`aws-gwlb-associate-vpce:<vpce-id>@ethernet<subinterface>`**: Le permite Asociar un endpoint VPC con una interfaz de VM-Series o subinterfaz en el cortafuegos. La interfaz especificada se asigna a una zona de seguridad. • **`aws-gwlb-overlay-routing:enable`**: utilice este comando para Habilitar el enrutamiento de superposición para la VM-Series en AWS cuando está integrado con un AWS GWLB. • **`set-dp-cores:<#-cores>`**: personalice el número de vCPU de plano de datos para un cortafuegos VM-Series que ejecute PAN-OS 11.0 o posterior implementado con una licencia software NGFW. Esta opción no es compatible con NSX-T. Para obtener más información, consulte Personalizar núcleos de plano de datos. • **`numa-perf-optimize:enable`**: permite la optimización del rendimiento de NUMA en el cortafuegos VM-Series con el complemento VM-Series 2.1.2 o posterior instalado. Para obtener más información, consulte Habilitar la optimización del rendimiento de NUMA en el VM-Series. • **`enrutamiento avanzado:activar`**: activa el Enrutamiento avanzado. Para garantizar un arranque correcto para el enrutamiento avanzado utilizando archivos init-cfg.txt* y bootstrap.xml, habilite el Enrutamiento avanzado tanto en * init-cfg.txt* como en bootstrap.xml. Si no se habilita el Enrutamiento avanzado en ambos archivos, se podría generar un entorno inestable; por ejemplo, si utiliza **show advanced routing route,** el resultado indica que el enrutamiento avanzado está habilitado; sin embargo, el comando **show deviceconfig setting** indica que enrutamiento avanzado no está habilitado. Además, el enrutamiento avanzado no funcionará al 100% y puede terminar en un error de confirmación. Si la configuración se encuentra en el estado anterior, para habilitar el enrutamiento avanzado, reinicie el cortafuegos VM-Series después de configurar **set deviceconfig setting advanced-routing yes**

 ©2024 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	• **`setsess-ress:True`**: habilita la resiliencia de sesión en el cortafuegos VM-Series para AWS y GCP.
dhcp-send-hostname=	El valor de sí o no llega del servidor DHCP. En caso afirmativo, el cortafuegos enviará su nombre de host al servidor DHCP. Este campo es relevante solo si el tipo es cliente dhcp.
dhcp-send-client-id=	El valor de sí o no llega del servidor DHCP. En caso afirmativo, el cortafuegos enviará su ID de cliente al servidor DHCP. Este campo es relevante solo si el tipo es cliente dhcp.
dhcp-accept-server-hostname=	El valor de sí o no llega del servidor DHCP. En caso afirmativo, el cortafuegos enviará su nombre de host desde el servidor DHCP. Este campo es relevante solo si el tipo es cliente dhcp.
dhcp-accept-server-domain=	El valor de sí o no llega del servidor DHCP. En caso afirmativo, el cortafuegos aceptará su servidor DNS desde el servidor DHCP. Este campo es relevante solo si el tipo es cliente dhcp.
vm-series-auto-registration-pin-id y vm-series-auto-registration-pin-value	El ID del PIN de registro de VM-Series y el valor para instalar el certificado del dispositivo en el cortafuegos VM-Series. El ID del PIN y el valor también le permiten activar automáticamente las licencias del sitio para AutoFocus y Cortex Data Lake en instancias PAYG del cortafuegos. Debe generar esto en el ID y valor de PIN de registro en el CSP de Palo Alto Networks. Consulte Instalación de un certificado de dispositivo en el cortafuegos VM-Series para obtener información sobre cómo generar ID y valor del PIN.
redis-endpoint=	Proporcione la dirección IP o FQDN y el puerto de su endpoint de Redis. Para usar con resiliencia de sesión en el VM-Series para AWS y GCP.
redis-auth=	Opcional El código de autenticación que usa el cortafuegos VM-Series para conectarse con el endpoint de Redis. Para usar con resiliencia de sesión en el VM-Series para AWS y GCP.
redis-certificate=	Opcional La cadena de certificado de CA raíz utilizada para conectarse al punto de conexión de Redis. El certificado debe ser una cadena codificada en base64 con codificación utf-8. Para su uso con resiliencia de sesión en el VM-Series para GCP; no es necesario para la resiliencia de sesión en AWS.

Archivo de muestra de init-cfg.txt

Los siguientes archivos de configuración básica de muestra muestran todos los parámetros compatibles en el archivo; los parámetros necesarios se muestran en **negrita**.

 ©2024 Palo Alto Networks, Inc.

Archivo init-cfg.txt de muestra (dirección IP estática)	Archivo init-cfg.txt de muestra (cliente DHCP)
type=static	**type=dhcp-client**
ip-address=10.x.x.19	ip-address=
default-gateway=10.x.x.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.x.x.20*	panorama-server=10.x.x.20*
panorama-server-2=10.x.x.21*	panorama-server-2=10.x.x.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*****

 ©2024 Palo Alto Networks, Inc.

No puede especificar la dirección IP de gestión y la configuración de máscara de red para el cortafuegos VM-Series en AWS. Si así se define, el cortafuegos ignora los valores especificados porque AWS utiliza un archivo de metadatos back-end para asignar la dirección IP de gestión y la máscara de red.

**Si añade una dirección IP del servidor Panorama, debe incluir un nombre de host de cortafuegos (`nombre de host=`), nombre de la pila de plantillas (`tplname=`) y el nombre del grupo de dispositivos (`dgname=`).*

***Se requiere la puerta de enlace predeterminada de IPv6 si incluye una dirección IPv6.*

****El comando de operación `mgmt-interface-swap` pertenece solamente a un cortafuegos VM-Series en AWS o GCP.*

*****`op-cmd-dpdk-pkt-io=off` es para deshabilitar DPDK en el cortafuegos VM-Series en ESXi, KVM y GCP (DPDK está habilitado de manera predeterminada).*

****** `vm-series-auto-registration-pin-id` y `vm-series-auto-registration-pin-value` se requieren para dos casos de uso:*

- *Activación de licencias de sitio, AutoFocus o Cortex Data Lake, con opciones de licencia Pay-As-You-Go (PAYG) del cortafuegos VM-Series.*
- *Recuperación e instalación de un certificado de dispositivo en el cortafuegos VM-Series.*

Ejemplo de archivo init-cfg-txt utilizado para un paquete de arranque cuando se utiliza Strata Cloud Manager

Ejemplo de archivo init-cfg.txt utilizado para un paquete de arranque cuando se utiliza Strata Cloud Manager

Al crear un archivo init-cfg.txt para el paquete de arranque, asegúrese de que incluya como mínimo parámetros para:

- tipo
- panorama-server
- vm-series-auto-registration-pin-id
- vm-series-auto-registration-pin-value

Por ejemplo:

```
type=static ip-address=1.1.1.1 netmask=111.111.11.1 default-
gateway=1.1.1.1 hostname=host_1 panorama-server=cloud plugin-
op-commands-advance-routing=enable dgname=host_1_directory dns-
```

 ©2024 Palo Alto Networks, Inc.

```
primary=1.1.1.1 vm-series-auto-registration-pin-id=VALUE vm-series-
auto-registration-pin-value=VALUE
```

 ©2024 Palo Alto Networks, Inc.

Creación del archivo bootstrap.xml

Utilice estas instrucciones para exportar la configuración de un cortafuegos que se ejecuta en la misma plataforma o hipervisor que su implementación de destino.

STEP 1 | Exporte una configuración desde el cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Seleccione el archivo de configuración que desea exportar.
   - Para exportar la configuración en ejecución, en la sección de Gestión de configuración, **Export named configuration snapshot (Exportar instantáneas de configuración con nombre)** y seleccione **running config.xml (config.xml en ejecución)**del menú desplegable.
   - Para exportar una versión anterior de una configuración de cortafuegos, en la sección Gestión de configuración, **Export configuration version (Exportar la versión de configuración)** y seleccione la versión de configuración apropiada en el menú desplegable.

STEP 2 | Cambie el nombre del archivo de configuración y guárdelo.

1. Cambie el nombre del archivo a `bootstrap.xml`.

   Para que el proceso de bootstrap tenga éxito, el nombre del archivo debe coincidir exactamente (con distinción entre mayúsculas y minúsculas).
2. Guarde el archivo `bootstrap.xml` en la misma ubicación que el archivo `init-cfg.txt`.

 ©2024 Palo Alto Networks, Inc.

Preparación de las licencias para el arranque

Para licenciar el cortafuegos durante el proceso de bootstrapping, debe adquirir los códigos de autenticación y registrar las licencias y suscripciones en el portal de asistencia de Palo Alto Networks antes de comenzar el bootstrapping.

Para cortafuegos VM-Series con BYOL (no aplicable para licencias basadas en uso, PAYG), debe tener un lote de códigos de autenticación que incluya el código de autenticación de capacidad, suscripción de asistencia, y cualquier otra suscripción necesaria. El proceso de preparación de las licencias para bootstrapping depende de si el cortafuegos tiene acceso a Internet durante el arranque:

- Acceso directo a Internet: El cortafuegos está conectado directamente a Internet.
- Acceso indirecto a Internet: El cortafuegos es gestionado por Panorama, que tiene acceso directo a Internet y la capacidad de recibir las claves de licencia en nombre del cortafuegos.
- Sin acceso a Internet: El cortafuegos utiliza un servicio de orquestación o un script personalizado para recoger las claves de licencia en nombre del cortafuegos.

- Para cortafuegos VM-Series con acceso a Internet.

  Introduzca el código de autenticación en la carpeta `/license` cuando Preparación del paquete de arranque.

- Para cortafuegos VM-Series con acceso indirecto a Internet.

  1. Registre el código de autenticación en el portal de asistencia de Palo Alto Networks.

     1. Vaya al Portal de asistencia técnica, inicie sesión y seleccione **Products (Productos)** > **VM-Series Auth-Codes (Códigos de autenticación de VM-Series)** > **Add VM-Series Auth-Code (Añadir código de autenticación de VM-Series)**.
     2. Siga los pasos para Registro del cortafuegos VM-Series.
     3. Haga clic en **Submit (Enviar)** para enviar.

  2. Active los códigos de autenticación en el portal de asistencia de Palo Alto Networks para generar claves de licencia.

     1. Vaya al Support Portal (Portal de atención al cliente), inicie sesión y seleccione la pestaña **Assets (Activos)**.
     2. Para cada número de serie, haga clic en el enlace **Action (Acción)**.
     3. Seleccione el botón **Activate Auth-Code (Activar código de autenticación)**.
     4. Introduzca el **Authorization code (Código de autorización)**, y haga clic en **Agree (Aceptar)** y **Submit (Enviar)**.
     5. Descargue las claves de licencia y guárdelas en una carpeta local.
     6. Continúe a Preparación del paquete de arranque; debe añadir las claves de licencia que ha descargado en la carpeta `\license` del paquete de arranque.

- Para un script personalizado o un servicio de orquestación que puede acceder a lnternet en nombre de los cortafuegos.

  El script o servicio debe recoger la ID de CPU y la UUID del hipervisor en el que se implementa el cortafuegos y acceder al portal de asistencia de Palo Alto Networks con la ID de CPU, UUID, la clave

 ©2024 Palo Alto Networks, Inc.

API y el código de autenticación para obtener las claves necesarias. Consulte API de licencias basada en modelos.

 ©2024 Palo Alto Networks, Inc.

Preparación del paquete de arranque

En AWS, Azure o GCP, puede crear el paquete bootstrap en su almacenamiento en la nube pública.

- El complemento de VM-Series versión 1.0.13 y anteriores, y las versiones 2.0.0 y 2.0.1 son compatibles con un paquete de arranque por depósito de almacenamiento.
- Las versiones 2.0.2 y posteriores del complemento de VM-Series también son compatibles con subcarpetas dentro de su depósito de almacenamiento en la nube pública. Dentro de un depósito, puede crear varias carpetas y subcarpetas, cada una de las cuales contiene un paquete de arranque. Normalmente, una carpeta representa la configuración de un grupo de máquinas virtuales, como un grupo de dispositivos de Panorama.

  Para acceder al paquete de arranque, especifique la ruta completa a la carpeta de arranque. Por ejemplo: `my-storage/my-firewalls/bootstrap-2020-10-15`

Utilice el siguiente procedimiento para preparar el paquete de arranque.

STEP 1 | Cree la estructura del directorio de nivel superior parea el paquete de arranque.

En su cliente o portátil local, o en un depósito de almacenamiento en la nube pública, cree las siguientes carpetas:

```
/config
/content
/software
/license
/plugins
```

Puede dejar una carpeta vacía, pero debe tener las carpetas. **`/config`**, **`/license`**, **`/software`** y **`/content`**. La carpeta **`/ plugins`** es opcional y solo es necesaria si está actualizando el Complemento VM-Series independientemente de una versión PAN-OS.

No coloque ningún otro archivo o carpeta en la estructura de arranque. La adición de otros archivos o carpetas resultará en un error de arranque.

```
/my-storage                          /my-firewalls
       /internal     /external             /config        /config
         /content       /content           /license       /license
         /plugins       /plugins           /software      /software
```

STEP 2 | Añada contenido en cada carpeta.

Para obtener una perspectiva general del proceso, consulte Paquete de arranque. Para obtener información sobre los archivos de la carpeta **`/config`** consulte Archivos de configuración de arranque.

```
/config
  0008C100105-init-cfg.txt
  0008C100107-init-cfg.txt
  bootstrap.xml
/content
```

 ©2024 Palo Alto Networks, Inc.

```
  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 guarda las claves en la carpeta `license`, puede usar una convención de nomenclatura de archivos que le venga bien, pero mantenga la extensión `.key` en el nombre del archivo. Para los códigos de autenticación, cree un archivo de texto llamado `authcodes` (sin una extensión de archivo), añada sus códigos de autenticación a ese archivo y guárdelo en la carpeta `license`.*
- *Utilice un lote de códigos de autenticación en vez de códigos de autenticación individuales, de modo que el cortafuegos o el servicio de orquestación pueda recoger al mismo tiempo todas las claves asociadas con un cortafuegos. Si utiliza códigos de autenticación individuales, en vez de un lote, el cortafuegos recuperará solamente la clave de licencia para el primer código de autenticación del archivo.*
- *En la carpeta `/plugins`, suministre solo un binario del plugin VM-Series. No suministre múltiples versiones del plugin.*

STEP 3 | Cree el paquete de arranque.

Para cortafuegos VM-Series, cree la imagen en el forma apropiado para su hipervisor. Consulte Entrega del paquete de arranque.

 ©2024 Palo Alto Networks, Inc.

Arranque del cortafuegos VM-Series en AWS

STEP 1 | Seleccione un método de arranque.

- Para añadir una configuración básica al paquete de arranque, continúe al Paso 2.
- Para introducir una configuración básica como datos de usuario o usar datos de usuario para obtener la configuración básica de un secreto de AWS, continúe al Paso 3.

STEP 2 | Prepare un depósito S3 y una función de IAM para habilitar el acceso de lectura.

Para realizar el bootstrapping utilizando un archivo, debe familiarizarse con AWS S3 y los permisos IAM necesarios para completar este proceso. Para instrucciones detalladas sobre la creación de políticas, consulte la documentación de AWS en Creación de políticas gestionadas del cliente.

La interfaz de gestión del cortafuegos VM-Series debe poder acceder al depósito S3 para completar el arranque. Puede asignar una dirección IP pública o una dirección IP elástica a la interfaz de gestión para que se pueda acceder al depósito S3 a través de internet. O bien, cree un endpoint AWS VPC en la misma región que el depósito S3, si prefiere crear una conexión privada entre su VPC y el depósito S3 y no desea habilitar el acceso a Internet en la interfaz de gestión del cortafuegos. Para obtener más información, consulte la documentación de AWS sobre la configuración Endpoints de VPC.

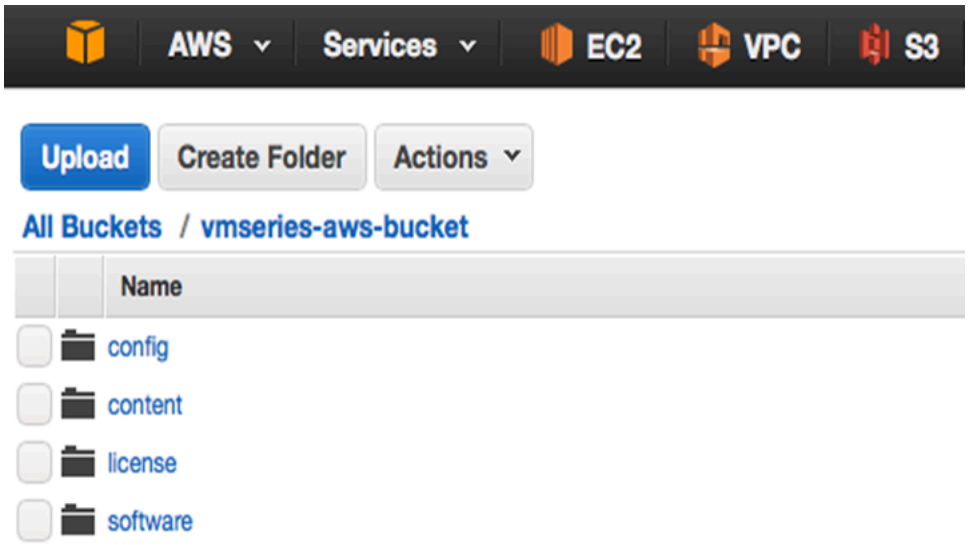
1. Cree una función IAM con la política en línea para habilitar el acceso de lectura al depósito S3 [ListBucket, GetObject]. Para obtener instrucciones detalladas sobre cómo crear una función de IAM, cómo definir qué cuentas o servicios de AWS pueden asumir la función, cómo definir qué acciones y recursos de API puede usar la aplicación luego de asumir la función, consulte la documentación de AWS sobre Funciones de IAM para Amazon EC2. Cuando inicie el cortafuegos VM-Series, debe adjuntar este papel para habilitar el acceso al depósito S3 y los objetos incluidos en el depósito para el arranque con éxito.
2. En la consola de AWS, cree un depósito de Amazon Simple Storage Service (S3) o cree un subdirectorio en un depósito S3 existente.

   El depósito S3 en el siguiente ejemplo, vmseries-aws-bucket, se encuentra en el nivel de la carpeta raíz de Todos los depósitos.

```
{    "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>/*"]       }    ] }
```

 ©2024 Palo Alto Networks, Inc.

3. Cree las carpetas dentro del depósito S3 como se describe en Preparación del paquete de arranque.
   - Cree la estructura directamente en su depósito S3.



   - (Opcional) Añada contenido en cada carpeta. Puede dejar una carpeta vacía, pero debe tener todas las carpetas \config, \content, \license y \software. La carpeta \plugins es opcional.

> *Si ha habilitado el inicio de sesión en Amazon S3, se crea automáticamente una carpeta de logs creada en el depósito S3. La carpeta de logs ayuda a solucionar problemas con acceso al depósito S3.*

STEP 3 | Inicio del cortafuegos VM-Series en AWS. Elija una de las siguientes opciones.

- **`init-cfg.txt`**: si utiliza un archivo para configurar el cortafuegos, adjunte la función de IAM que creó en el Paso 2.1, expanda la sección **Advanced Details (Detalles avanzados)** y, en el campo **User Data (Datos de usuario)**, especifique la ruta a un depósito S3, directorio o subdirectorio. Por ejemplo,

```
vmseries-bootstrap-aws-s3bucket=<bucketname>
```

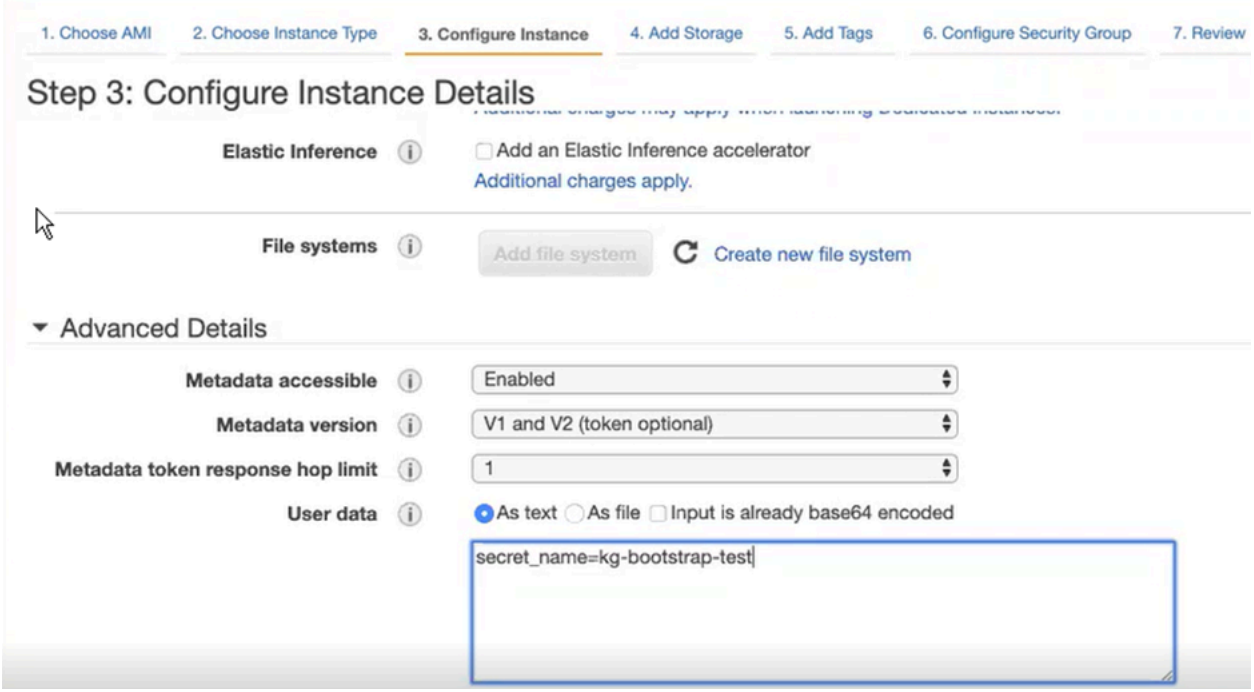
  O

```
vmseries-bootstrap-aws-s3bucket=<bucketname/directoryname>
```

- **Datos del usuario**: si está utilizando datos del usuario para configurar el cortafuegos, expanda la sección **Advanced Details (Detalles avanzados)** y en el campo **User Data (Datos del usuario)** introduzca los parámetros de arranque iniciales como se describe en Introduzca una configuración básica como datos de usuario (AWS, Azure o GCP).
- **AWS Secrets Manager**: si almacenó su configuración básica como se describe en Guardar una configuración básica en AWS Secrets Manager, amplíe la sección **Advanced Details (Detalles**

 ©2024 Palo Alto Networks, Inc.

avanzados) y en el campo **User Data (Datos de usuario)** seleccione **As text (Como texto)** e introduzca el nombre secreto como un par clave-valor. Por ejemplo:

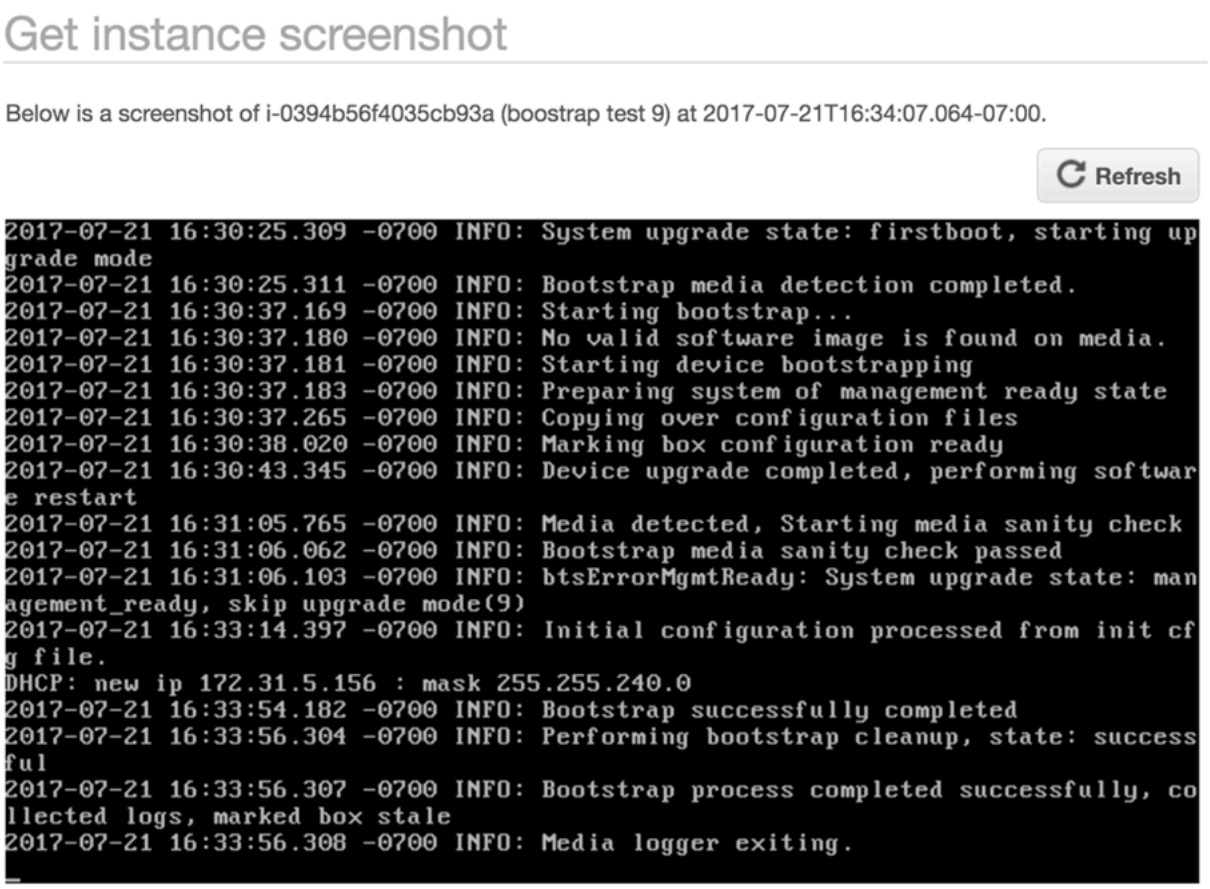


Seleccione **Review and Launch (Revisar e iniciar)**. Para más detalles, consulte Inicio del cortafuegos VM-Series en AWS.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Verificación de la realización del arranque. Seleccione la instancia de cortafuegos en la consola de administración de AWS y elija **Actions (Acciones)** > **Instance Settings (Configuraciones de instancias)** > **Get Instance Screenshot (Obtener captura de pantalla de instancia)**.

- La captura de pantalla muestra el arranque en curso. A continuación se muestra un arranque realizado correctamente:



- Si está utilizando un depósito S3 y dicho depósito S3 no tiene los permisos correctos, o no tiene las cuatro carpetas en el depósito S3, verá el siguiente mensaje de error:



 ©2024 Palo Alto Networks, Inc.

Arranque del cortafuegos VM-Series en Azure

El cortafuegos VM-Series en Azure admite el servicio de *archivos de Azure* para el arranque.

STEP 1 | Seleccione un método de arranque.

- Para añadir una configuración básica al paquete de arranque, continúe al Paso 2.

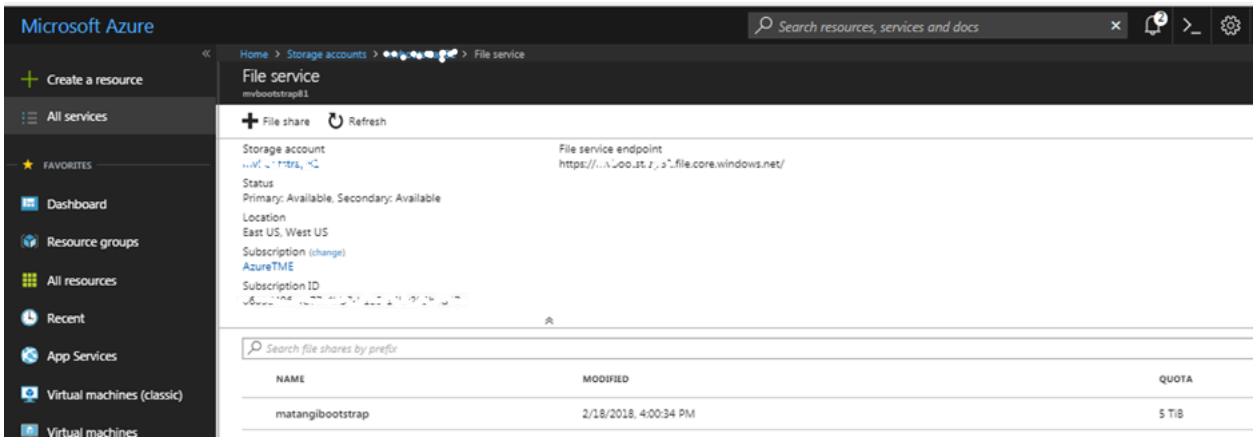
  Para gestionar el paquete de arranque para el cortafuegos VM-Series en Azure, debe estar familiarizado con las cuentas de almacenamiento en Azure y conocer cómo crear un recurso compartido de archivos y objetos de directorio que contengan la estructura de carpeta requerida para el paquete de arranque. Puede compartir un recurso compartido de archivos de Azure en varias máquinas virtuales de modo que todos los cortafuegos implementados en la misma región como la cuenta de almacenamiento que aloja el recurso compartido de archivos puedan acceder a los archivos al mismo tiempo.

  La interfaz de gestión del cortafuegos VM-Series debe poder acceder al recurso compartido de archivos que contiene el paquete de arranque de modo que pueda completar el arranque.

- Para Introduzca una configuración básica como datos de usuario (AWS, Azure o GCP), Continúe al paso 3.2.

STEP 2 | Configure el paquete de arranque dentro del servicio de archivos de Azure.

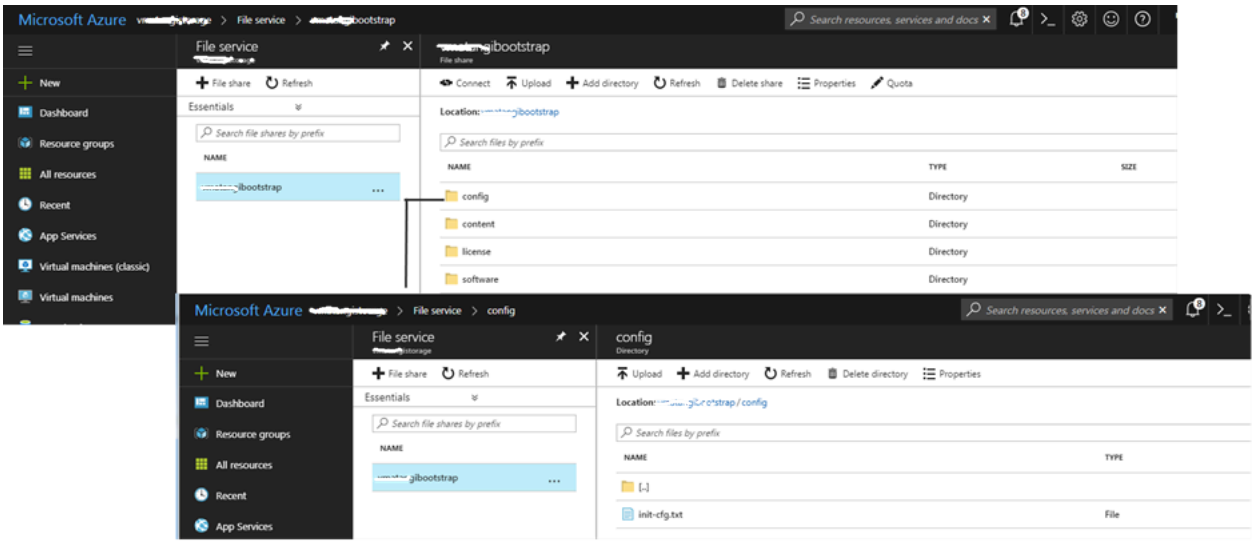
1. En el portal de Azure, seleccione o cree una cuenta de almacenamiento.
2. Cree un recurso compartido de archivos dentro del servicio de archivos de Azure.



3. Cree las carpetas dentro de la cuenta de almacenamiento.
   - Cree la estructura de directorio de nivel superior para el paquete de arranque directamente en la carpeta raíz y cree una subcarpeta para cada configuración de arranque.
   - Añada carpetas de contenido dentro de cada carpeta. Puede dejar una carpeta vacía, pero debe tener las cuatro carpetas (configuración, licencia, software y contenido) en la carpeta

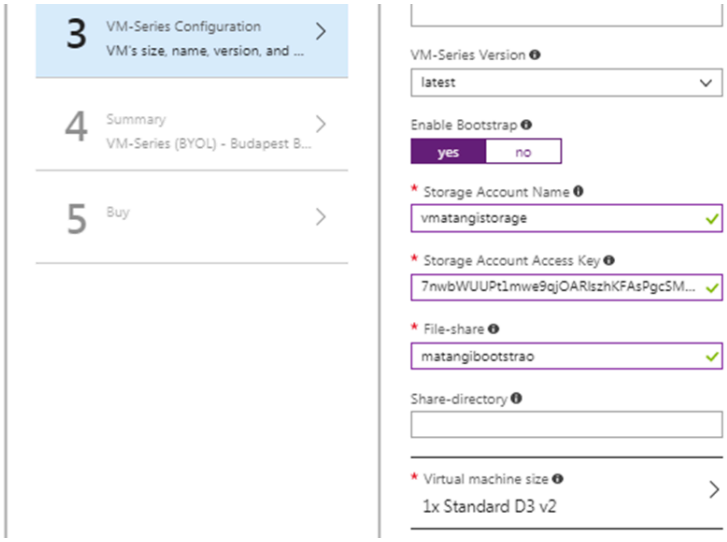
 ©2024 Palo Alto Networks, Inc.

principal. En la siguiente captura de pantalla, puede ver que la carpeta `config` tiene el archivo `init-cfg.txt` cargado en ella.



STEP 3 | Implemente el cortafuegos VM-Series desde Azure Marketplace (plantilla de soluciones).

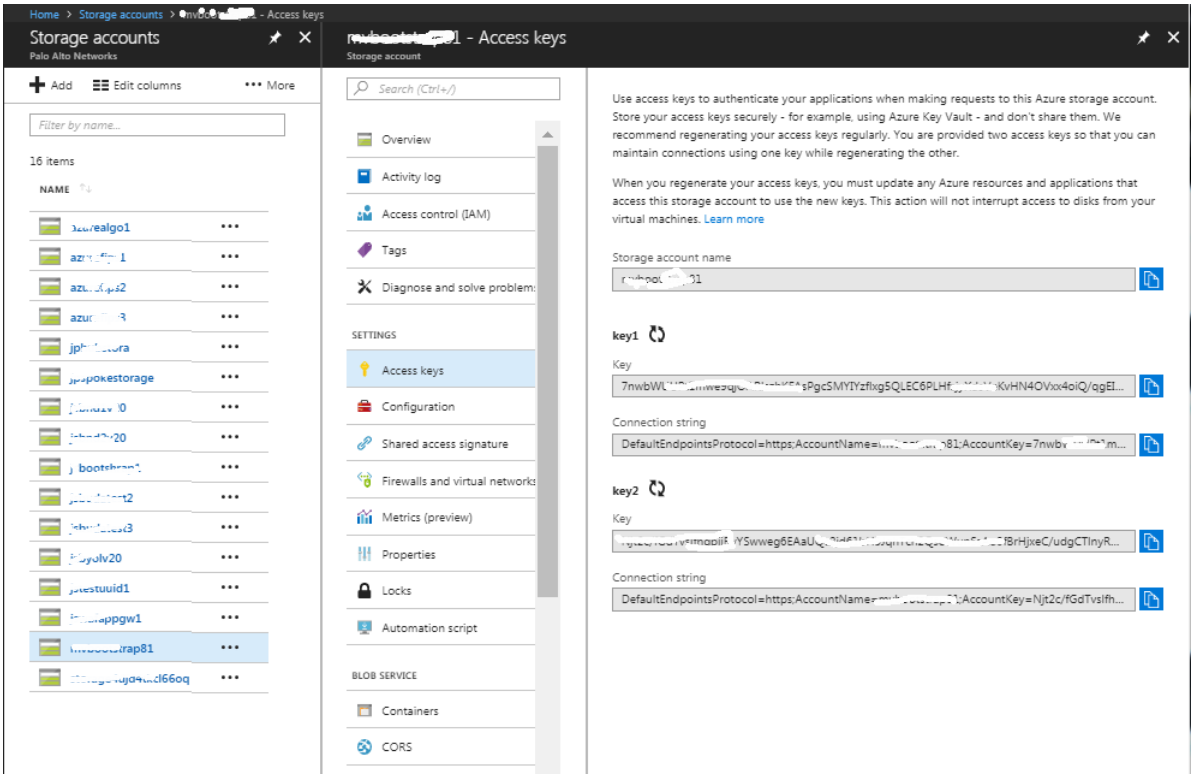
- Si está utilizando un archivo para configurar el cortafuegos, continúe con el Paso 3.1
- Si está utilizando datos personalizados para configurar el cortafuegos, continúe con el Paso 3.2.



1. Si elige utilizar el paquete de arranque, seleccione **Habilitar Bootstrap: Sí** y proporcione la información necesaria para acceder al recurso compartido de archivos que contiene los archivos de arranque.
    1. **Storage Account Name (Nombre de la cuenta de almacenamiento)**: esta es la cuenta de almacenamiento de Azure en la que creó el recurso compartido de archivo para las carpetas de arranque.
    2. **Storage Account Access Key (Clave de acceso de la cuenta de almacenamiento)**: el cortafuegos necesita esta clave de acceso para autenticarse en la cuenta de almacenamiento y acceder a los archivos almacenados dentro de ella. Para copiar esta clave de acceso,

 ©2024 Palo Alto Networks, Inc.

seleccione el nombre de la cuenta de almacenamiento y, luego, seleccione **Settings (Configuración)** > **Access Keys (Claves de acceso)**.



3. **File-share**: el nombre del recurso compartido de archivo que contiene el paquete de arranque.
4. (Opcional) **Share-directory** : la ruta a una subcarpeta dentro del recurso compartido de archivo. Si tiene un recurso compartido de archivos en común que sirva como repositorio para las configuraciones de arranque para diferentes ajustes, puede usar un directorio de recurso compartido para crear una jerarquía de carpetas y acceder a un conjunto específico de subcarpetas dentro del recurso compartido de archivos en común.

2. Introduzca los parámetros de configuración como datos personalizados. Para los pares clave-valor, consulte Introduzca una configuración básica como datos de usuario (AWS, Azure o GCP). Separe cada par clave-valor con un punto y coma. Por ejemplo:

```
type=dhcp-client; op-command-modes=jumbo-frame; vm-series-
auto-registration-pin-id=abcdefgh1234****; vm-series-auto-
registration-pin-value=zyxwvut-0987****
```

Proporcione datos personalizados mediante uno de los métodos de Datos personalizados y Cloud-Init en Azure Virtual Machines.

STEP 4 | Verificación de la realización del arranque.

 ©2024 Palo Alto Networks, Inc.

Arranque del cortafuegos VM-Series en Azure Stack HCI

El cortafuegos VM-Series en Azure Stack HCI admite el arranque mediante una imagen ISO. El arranque le permite crear un proceso repetible y sencillo de implementación de los nuevos cortafuegos VM-Series en su red porque le permite crear un paquete con la configuración del modelo para su red y, posteriormente, utilizar el paquete para implementar los cortafuegos VM-Series en cualquier lugar. Para obtener más información, consulte Bootstrap the VM-Series Firewall (Arranque del cortafuegos VM-Series)y los parámetros de arranque para configurarlo en el cortafuegos VM-Series.

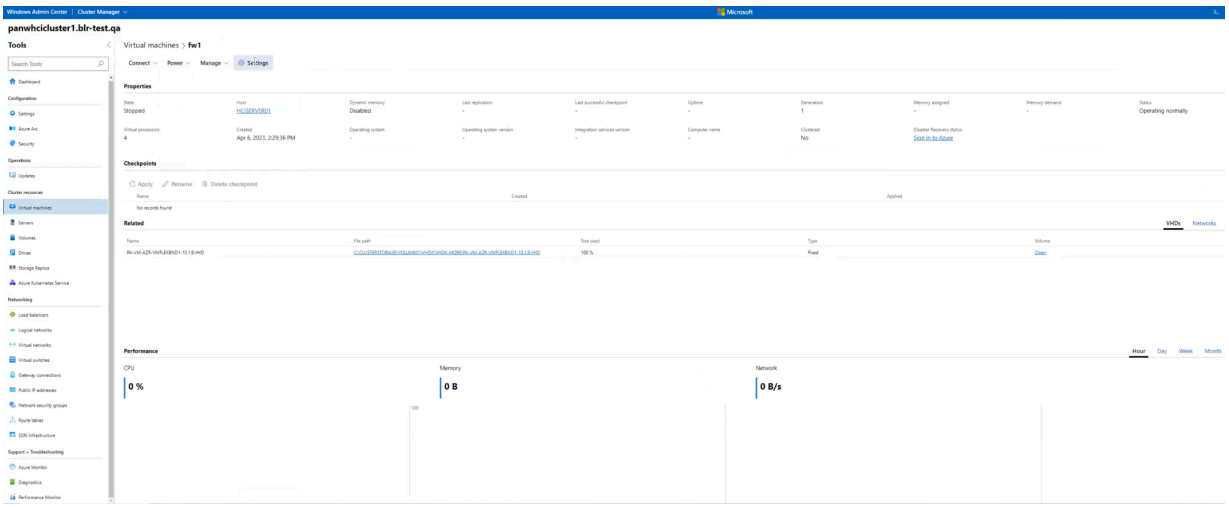
Realice los siguientes pasos para arrancar el cortafuegos VM-Series en Azure Stack HCI mediante una imagen ISO:

STEP 1 | Inicie sesión en **Windows Admin Center**.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Seleccione **Clúster HCI** y vaya a **Máquina virtual** > **Configuración**.

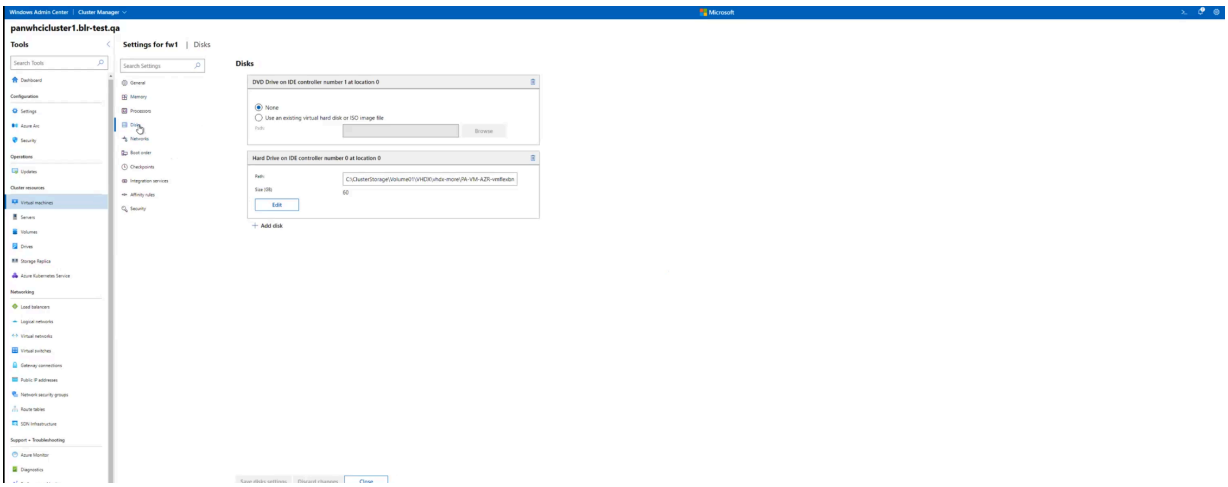
 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

STEP 3 | Vaya a **Discos.**

 ©2024 Palo Alto Networks, Inc.



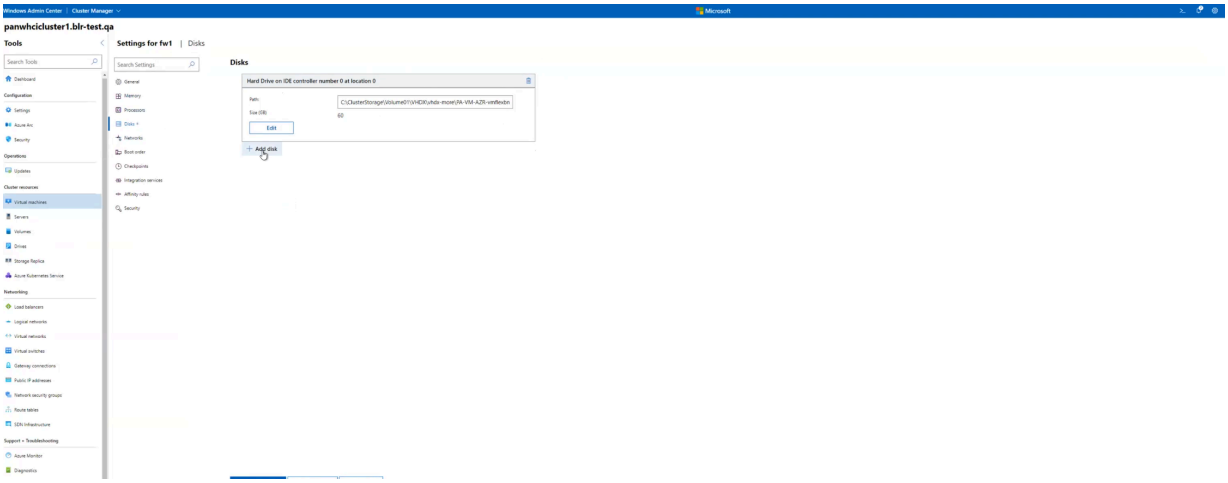
 ©2024 Palo Alto Networks, Inc.

STEP 4 | Elimine **Unidad DVD del controlador IDE número 1 en la ubicación 0**.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Haga clic en **Añadir disco**.

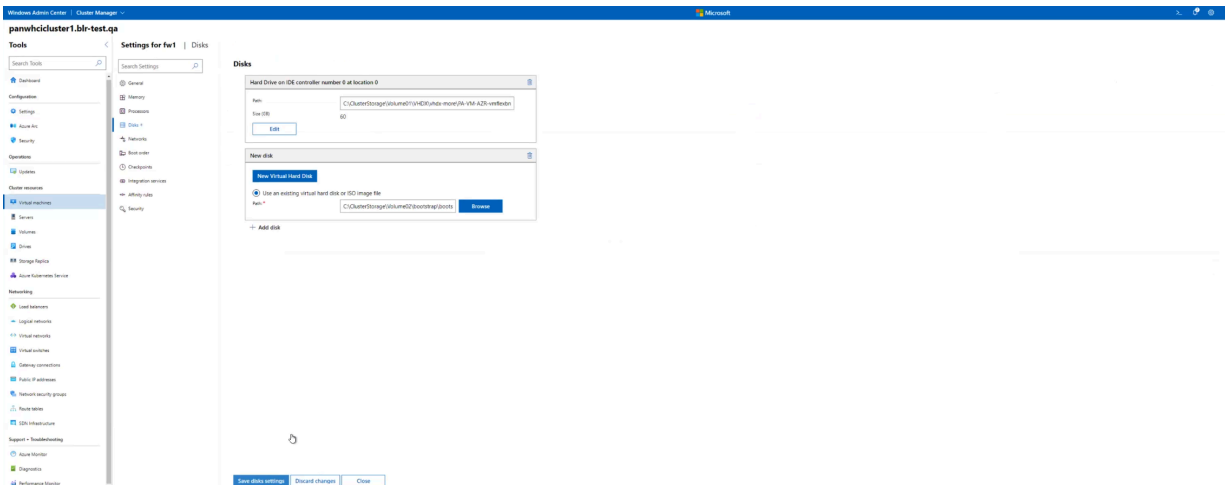
 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

Puede utilizar un disco duro virtual existente o un archivo de imagen ISO.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

Para obtener más información sobre los pasos para arrancar el cortafuegos VM-Series en Azure Stack HCI, consulte Arranque del cortafuegos VM-Series en Hyper-V con una ISO.

STEP 6 | Haga clic en **Guardar configuración de disco**.

Si el controlador IDE 0 está en la ubicación 0, la ISO de arranque debe estar bajo el controlador IDE 0 en la ubicación 1

 ©2024 Palo Alto Networks, Inc.

Arranque del cortafuegos VM-Series en ESXi

Puede arrancar el cortafuegos serie VM utilizando una imagen ISO o un disco duro virtual.

- Arranque del cortafuegos VM-Series en ESXi con una ISO
- Arranque del cortafuegos VM-Series en ESXi con un dispositivo de almacenamiento en bloque

Arranque del cortafuegos VM-Series en ESXi con una ISO

Siga estas instrucciones para iniciar el cortafuegos VM-Series en un servidor ESXi con una ISO.

STEP 1 | Cree una imagen ISO y cárguela en un almacén de datos del sistema de archivos de máquina virtual (VMFS) o un volumen del sistema de archivos de red (NFS).

1. Preparación del paquete de arranque.
2. Cree una imagen ISO. La herramienta utilizada para crear la imagen varía según el sistema operativo de su cliente.
3. Cargue la imagen ISO en un almacén de datos VMFS o en un volumen NFS accesibles al host ESX/ESXI.

STEP 2 | Implemente el cortafuegos.

1. Aprovisionamiento del cortafuegos VM-Series en un servidor ESXi.

   Por defecto, el cortafuegos se implementa con dos interfaces de red, una para tráfico de gestión y la otra para tráfico de datos. Asegúrese de que la primera interfaz ethernet del cortafuegos, es decir, la interfaz de gestión, está conectada al grupo de puertos de conmutador virtual asignado para la gestión de dispositivos.
2. No inicie el cortafuegos.

STEP 3 | Adjunte la imagen de bootstrap al cortafuegos.

1. Seleccione el cortafuegos VM-Series de la lista **Inventory (Inventario)**.
2. Haga clic en **Edit Settings (Editar ajustes)** y seleccione **Virtual Hardware (Hardware virtual)**.
3. Seleccione **Datastore iso file (Archivo iso de centro de datos)** en el menú desplegable de la **CD DVD drive (unidad CD DVD)**, y **browse (examinar)** a la imagen ISO.
4. Inicie el cortafuegos. El cortafuegos se iniciará con el proceso de bootstrapping, para el que se necesitarán varios minutos. Se mostrarán en la consola los mensajes de estado sobre el éxito o fallo del proceso.
5. Verificación de la realización del bootstrap.

Arranque del cortafuegos VM-Series en ESXi con un dispositivo de almacenamiento en bloque

Siga estas instrucciones para iniciar el cortafuegos VM-Series en un servidor ESXi con un dispositivo de almacenamiento en bloque.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Cree el paquete de arranque y el disco duro virtual.

1. Cree el paquete de arranque.
2. Implemente una máquina virtual Linux.
3. En la máquina Linux, Preparación del paquete de arranque. Puede dejar la carpeta vacía pero debe tener las cuatro carpetas.
4. Adjunte un nuevo disco de datos inferior a 39 GB a la máquina virtual Linux.
5. Haga la partición del disco y formatee el sistema de archivos ext3.
6. Cree un directorio para el nuevo sistema de archivos y monte el disco para la máquina virtual Linux.
7. Copie el contenido del paquete de arranque al disco.
8. Desmonte el disco.
9. Retire el disco de la máquina virtual Linux. Tome nota del archivo de disco que describe el disco de arranque que creó; este muestra el nombre del almacén de datos y la ruta al disco. Además, no marque la casilla de verificación Delete Files From Datastore (Eliminar archivos del almacén de datos); si lo hace, eliminará el disco.

STEP 2 | Implemente el cortafuegos.

1. Aprovisionamiento del cortafuegos VM-Series en un servidor ESXi.
2. No inicie el cortafuegos.

STEP 3 | Adjunte el paquete de arranque al cortafuegos.

1. Seleccione el cortafuegos VM-Series de la lista Inventario.
2. Haga clic en **Edit Settings (Editar ajustes)** y seleccione **Virtual Hardware (Hardware virtual)**.
3. En el menú desplegable Nuevo dispositivo, seleccione **Existing Hard Disk (Disco duro existente)**. Seleccione el disco de arranque según el almacén de datos y la ruta anotados anteriormente.
4. Inicie el cortafuegos. El cortafuegos se iniciará con el proceso de bootstrapping, para el que se necesitarán varios minutos. Se mostrarán en la consola los mensajes de estado sobre el éxito o fallo del proceso.
5. Verificación de la realización del bootstrap.

 ©2024 Palo Alto Networks, Inc.

Arranque del cortafuegos VM-Series en Google Cloud Platform

STEP 1 | Seleccione un método de arranque.

STEP 2 | Inicie sesión en Google Cloud Console.

- Para añadir una configuración básica al paquete de arranque, cree archivos de arranque como se describe en Preparación del paquete de arranque y continúe al Paso 3.
- Para introducir una configuración básica como metadatos personalizados, salte al Paso 4.

 ©2024 Palo Alto Networks, Inc.

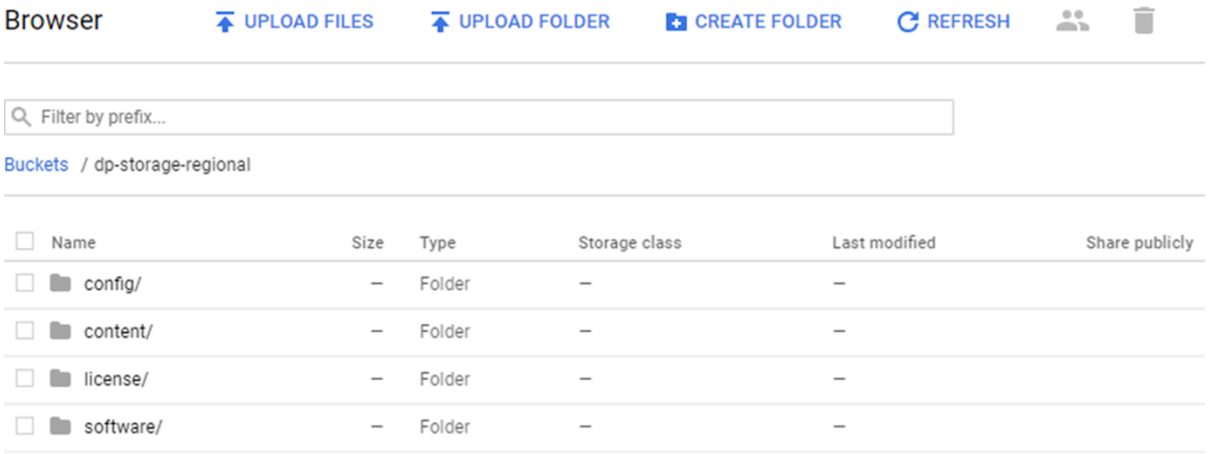
STEP 3 | Seleccione **Storage (Almacenamiento)** > **Browser (Explorar)** y haga clic en **Create Bucket (Crear depósito)**.

Puede utilizar este depósito para arrancar el cortafuegos cuando Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace.

Si planea realizar el arranque mediante un depósito de almacenamiento de Google en el mismo proyecto, debe contar con los privilegios de IAM devstorage.read_only.

Puede crear y rellenar el depósito en el nivel superior, o puede crear un depósito con subcarpetas dentro de él para que muchos paquetes de arranque puedan compartir el mismo depósito.

1. Introduzca el nombre del depósito, elija la clase de almacenamiento predeterminada y seleccione una ubicación. Tenga en cuenta que la ubicación del depósito de almacenamiento debe ser compatible con la zona que especifica para la instancia de Compute Engine.
2. Haga clic en **Create (Crear)**.
3. En Storage Browser (Explorador de almacenamiento), haga clic en el nombre del depósito para abrirlo.
4. Haga clic en **Create Folder (Crear carpeta)** y nombre la carpeta `config`. Haga clic en **Create (Crear)**.
5. Repita los pasos y cree carpetas para `content`, `license` y `software`, como se muestra a continuación. Todas las carpetas deben estar presentes, incluso si están vacías.



6. (Opcional) Si creó un archivo **`init-cfg.txt`**, abra la carpeta `config`. Haga clic en **Upload Files (Cargar archivos)**, busque y seleccione su archivo **`init-cfg.txt`** y haga clic en **Open (Abrir)**.
7. Abra la carpeta `license` y cargue el archivo **`authcodes`**.
8. Continúe hasta que haya cargado todos los archivos de arranque.

STEP 4 | Añada los parámetros de configuración inicial como metadatos. Seleccione **Add (Añadir)** cada par clave-valor como se describe en Introduzca una configuración básica como datos de usuario (AWS, Azure o GCP).

STEP 5 | Consulte Implementación del cortafuegos VM-Series desde Google Cloud Platform Marketplace para obtener información detallada sobre la implementación.

 ©2024 Palo Alto Networks, Inc.

Arranque del cortafuegos VM-Series en Hyper-V

Puede arrancar el cortafuegos serie VM utilizando una imagen ISO o un disco duro virtual.

- Arranque del cortafuegos VM-Series en Hyper-V con una ISO
- Arranque del cortafuegos VM-Series en Hyper-V con un dispositivo de almacenamiento en bloque

Arranque del cortafuegos VM-Series en Hyper-V con una ISO

Siga estas instrucciones para arrancar el cortafuegos VM-Series en un servidor Hyper-V con una ISO.

STEP 1 | Cree una imagen ISO.

1. Preparación del paquete de arranque.
2. Cree una imagen ISO. La herramienta utilizada para crear la imagen varía según el sistema operativo de su cliente.
3. Cargue la imagen ISO en una ubicación accesible al host Hyper-V.

STEP 2 | Implemente el cortafuegos.

1. Provisión de cortafuegos VM-Series en un host Hyper-V con gestor de Hyper-V.

   Por defecto, el cortafuegos se implementa con dos interfaces de red, una para tráfico de gestión y la otra para tráfico de datos. Asegúrese de que la primera interfaz ethernet del cortafuegos, es decir, la interfaz de gestión, está conectada a vSwitch asignado para la gestión de dispositivos.
2. No inicie el cortafuegos.

STEP 3 | Adjunte la imagen de bootstrap al cortafuegos.

1. En el gestor de Hyper-V, seleccione el cortafuegos VM-Series de la lista de **Virtual Machines (Máquinas virtuales)**.
2. Haga clic en **Settings (Configuración)** > **Hardware** > **IDE Controller (Controlador IDE)** > **DVD Drive (Unidad DVD)**.

   Si tiene más de una unidad de DVD, la imagen ISO debe aplicarse a la primera unidad.
3. Bajo Medios, haga clic en el botón de opción **Image file (Archivo de imagen)**.
4. Haga clic en **Browse (Examinar)** y seleccione la imagen ISO cargada.
5. Haga clic en **Aplicar (Aplicar)** y **OK (Aceptar)** para salir de los ajustes de máquina virtual.
6. Inicie el cortafuegos. El cortafuegos se iniciará con el proceso de bootstrapping, para el que se necesitarán varios minutos. Se mostrarán en la consola los mensajes de estado sobre el éxito o fallo del proceso.
7. Verificación de la realización del bootstrap.

Arranque del cortafuegos VM-Series en Hyper-V con un dispositivo de almacenamiento en bloque

Siga estas instrucciones para arrancar el cortafuegos VM-Series en un servidor Hyper-V con un dispositivo de almacenamiento en bloque.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Cree el paquete de arranque y el disco duro virtual.

1. Implemente una máquina virtual Linux.
2. En la máquina Linux, Preparación del paquete de arranque. Puede dejar la carpeta vacía pero debe tener las cuatro carpetas.
3. Adjunte un nuevo disco de datos inferior a 39 GB a la máquina virtual Linux.
    1. Apague la máquina virtual Linux.
    2. En Hyper-V, seleccione la máquina virtual de Linux de la lista de Máquinas virtuales.
    3. Seleccione **Settings (Configuración)** > **Hardware** > **IDE Controller (Controlador IDE)**.
    4. Seleccione **Hard Drive (Disco duro)** y haga clic en **Add (Añadir)**.
    5. Seleccione **Virtual Hard Disk (Disco duro virtual)** y haga clic en **New (Nuevo)**.
    6. Siga las instrucciones en pantalla para crear un nuevo VHD. Tenga en cuenta el nombre y la ruta del nuevo VHD.
    7. Haga clic en **Apply (Aplicar)** y **OK (Aceptar)** para salir de la configuración de la máquina virtual.
    8. Encienda la máquina virtual Linux.
4. Conéctese a la CLI de la máquina virtual Linux.
5. Haga la partición del disco y formatee el sistema de archivos ext3.
6. Cree un directorio para el nuevo sistema de archivos y monte el disco para la máquina virtual Linux.
7. Copie el contenido del paquete de arranque al disco.
8. Desmonte el disco.
9. Retire el disco de la máquina virtual Linux.
    1. Apague la máquina virtual Linux.
    2. Seleccione la máquina virtual Linux de la lista de máquinas virtuales.
    3. Seleccione **Settings (Configuración)** > **Hardware** > **IDE Controller (Controlador IDE)**.
    4. Seleccione el VHD que creó.
    5. Haga clic en **Remove (Retirar)**. Esto desconecta el VHD pero no lo elimina.

STEP 2 | Implemente el cortafuegos.

1. Provisión de cortafuegos VM-Series en un host Hyper-V con gestor de Hyper-V.
2. No inicie el cortafuegos.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Adjunte la imagen de disco de arranque al cortafuegos.

1. Seleccione el cortafuegos de la lista de máquinas virtuales.
2. Seleccione **Settings (Configuración)** > **Hardware** > **IDE Controller (Controlador IDE)**.
3. Seleccione **Hard Drive (Disco duro)** y haga clic en **Add (Añadir)**.
4. Seleccione **Virtual Hard Disk (Disco duro virtual)** y haga clic en **Browse (Examinar)**.
5. Busque el VHD de arranque que creó, selecciónelo y haga clic en **Open (Abrir)**.
6. Haga clic en **Apply (Aplicar)** y **OK (Aceptar)** para salir de la configuración de máquina virtual.
7. Inicie el cortafuegos. El cortafuegos se iniciará con el proceso de bootstrapping, para el que se necesitarán varios minutos. Se mostrarán en la consola los mensajes de estado sobre el éxito o fallo del proceso.
8. Verificación de la realización del bootstrap.

 ©2024 Palo Alto Networks, Inc.

Arranque del cortafuegos VM-Series en KVM

Puede arrancar el cortafuegos VM-Series en KVM utilizando una imagen ISO o un disco duro virtual.

- Arranque del cortafuegos VM-Series en KVM con una ISO
- Arranque del cortafuegos VM-Series en KVM con un dispositivo de almacenamiento en bloque

Arranque del cortafuegos VM-Series en KVM con una ISO

Siga estas instrucciones para iniciar el cortafuegos VM-Series en un servidor KVM con una ISO.

STEP 1 | Cree una imagen ISO.

1. Preparación del paquete de arranque.
2. Cree una imagen ISO. La herramienta utilizada para crear la imagen varía según el sistema operativo de su cliente.
3. Cargue la imagen ISO en una ubicación accesible al host KVM.

STEP 2 | Implemente el cortafuegos.

1. Instalación del cortafuegos VM-Series en KVM.

   Por defecto, el cortafuegos se implementa con dos interfaces de red, una para tráfico de gestión y la otra para tráfico de datos. Asegúrese de que la primera interfaz ethernet del cortafuegos, es decir, la interfaz de gestión, está conectada al grupo de puertos de conmutador virtual asignado para la gestión de dispositivos.
2. No inicie el cortafuegos.

STEP 3 | Adjunte la imagen de bootstrap al cortafuegos.

1. En el gestor virtual, haga doble clic en el cortafuegos VM-Series para abrir la consola.
2. Para ver los detalles de hardware de VM vaya a **View (Ver)** > **Details (Detalles)**.
3. Abra el menú Añadir nuevo hardware virtual haciendo clic en **Añadir hardware**.
4. Cambie el tipo de dispositivo a IDE CDROM.
5. Haga clic en el botón de opción **Select managed or other existing storage (Seleccionar gestionados u otros almacenajes existentes)** y haga clic en **Browse (Examinar)**. Localice la imagen ISO que ha creado y haga clic en **Elegir volumen**.
6. Haga clic en **Finalizar** para salir del menú Añadir nuevo hardware virtual.
7. Para iniciar el cortafuegos vaya a **Virtual Machine (Máquina virtual)** > **Run (Ejecutar)**. El cortafuegos se iniciará con el proceso de bootstrapping, para el que se necesitarán varios minutos. Se mostrarán en la consola los mensajes de estado sobre el éxito o fallo del proceso.
8. Verificación de la realización del arranque.

Arranque del cortafuegos VM-Series en KVM con un dispositivo de almacenamiento en bloque

Siga estas instrucciones para arrancar el cortafuegos VM-Series en un servidor KVM con un dispositivo de almacenamiento en bloque.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Cree el paquete de arranque y el disco duro virtual.

1. Cree el paquete de arranque.
2. Cree una nueva imagen de disco de menos de 39 GB de tamaño, y particione el disco y formatee el sistema de archivos como ext3. Las herramientas utilizadas para completar este proceso varían según el sistema operativo de su cliente.
3. Monte el archivo de imagen de disco y copie el paquete de arranque preparado en los archivos de imagen del disco.
4. Copie el contenido del paquete de arranque al disco.
5. Desmonte la imagen de disco.
6. Cargue el archivo de imagen de disco a una ubicación a la que pueda acceder el host KVM.

STEP 2 | Implemente el cortafuegos.

1. Instalación del cortafuegos VM-Series en KVM.
2. No inicie el cortafuegos.

STEP 3 | Adjunte la imagen de disco de arranque al cortafuegos.

1. En virt-manager, haga doble clic en el cortafuegos VM-Series para abrir la consola.
2. Para ver los detalles de hardware de VM seleccione **View (Ver)** > **Details (Detalles)**.
3. Abra el menú Añadir nuevo hardware virtual haciendo clic en **Añadir hardware**.
4. Seleccione **Storage (Almacenamiento)** y luego seleccione **Select or create custom storage (Seleccione o cree un almacenamiento personalizado)**.
5. Haga clic en el botón **Manage (Gestionar)** para abrir el cuadro de diálogo **Choose Storage Volume (Elija el Volumen de almacenamiento)** y seleccione el archivo de imagen de disco que creó previamente.
6. Haga clic en Choose Volume (Elegir volumen).
7. Asegúrese de que el tipo de dispositivo sea Disk Device (Dispositivo de disco) y no cambie Bus Type (Tipo de bus).
8. Haga clic en Finish (Finalizar).
9. Inicie el cortafuegos. El cortafuegos se iniciará con el proceso de bootstrapping, para el que se necesitarán varios minutos. Se mostrarán en la consola los mensajes de estado sobre el éxito o fallo del proceso.
10. Verificación de la realización del arranque.

 ©2024 Palo Alto Networks, Inc.

Verificación de la realización del bootstrap

Puede ver logs de estado básicos en la consola durante el arranque y puede verificar que el proceso se haya completado.

STEP 1 | Si ha incluido **`panorama-server`**, **`tplname`**, y **`dgname`** en su archivo `init-cfg.txt`, compruebe los dispositivos gestionados por Panorama, el grupo de dispositivos y el nombre de la plantilla.

STEP 2 | Verifique los ajustes generales del sistema y la configuración. Acceda a la interfaz web y seleccione **Dashboard (Panel)** > **Widgets** > **System (Sistema)** o utilice los comandos de operación de la CLI **`show system info`** y **`showconfig running`**.

STEP 3 | Verifique la instalación de la licencia. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)**o use el comando de operación de la CLI **`request license info (solicitar información de licencia)`**.

STEP 4 | Si tiene Panorama configurado, gestione las versiones de contenido y las versiones del software desde Panorama. Si no tiene Panorama configurado, utilice la interfaz web para gestionar versiones de contenido y versiones de software.

 ©2024 Palo Alto Networks, Inc.

Errores de arranque

Si recibe un mensaje de error durante el proceso de bootstrapping, consulte los detalles en la tabla siguiente.

Mensaje de error (gravedad)	Motivos
Error de imagen de inicio (alta)	• No se ha detectado ningún dispositivo externo con el paquete bootstrap. O • Se ha producido un error crítico al arrancar desde la imagen en el dispositivo externo. Se ha interrumpido el proceso de bootstrap.
No hay un archivo config de bootstrap en el dispositivo externo (alta)	El dispositivo externo no tiene el archivo de configuración de bootstrap.
Sin parámetros o parámetros erróneos para información obligatoria de red en el archivo config de bootstrap (alta)	Faltan los parámetros de red para bootstrapping o no son correctos. El mensaje de error indica el valor: dirección IP, máscara de red, puerta de enlace por defecto, que ha causado el fallo del bootstrap.
Fallo al instalar la clave de licencia para el archivo <license-key-filename> (alto)	No se ha podido aplicar la clave de licencia. Este error indica que la clave de licencia utilizada no es válida. La salida incluye el nombre de la clave de licencia que no se ha podido aplicar.
Fallo al instalar la clave de licencia con authcode <authcode> (alto)	No se ha podido aplicar el código de autenticación de licencia. Este error indica que el código de autenticación de licencia no es válido. La salida incluye el nombre del código de autenticación de licencia que no se ha podido aplicar.
Fallo de confirmación de actualización de contenidos (alta)	No se han aplicado con éxito las actualizaciones de contenidos.
Medio USB preparado con éxito usando el conjunto dado (informativa)	La imagen de bootstrap se ha compilado con éxito en el dispositivo flash USB. <username>: El USB se ha preparado correctamente usando el paquete <bundlename>
Bootstrap con éxito (informativa)	El cortafuegos se ha aprovisionado con éxito con el archivo de configuración de bootstrap. La salida incluye las claves de licencia instaladas y el nombre de archivo de la configuración de bootstrap.

 ©2024 Palo Alto Networks, Inc.

Mensaje de error (gravedad)	Motivos
	Solamente en los cortafuegos VM-Series, también se muestran la versión de PAN-OS y la versión de actualización de contenidos.

Lea acerca del Paquete de arranque y cómo Preparación del paquete de arranque.

©2024 Palo Alto Networks, Inc.