paloalto TECHDOCS

Guía del administrador de SD-WAN

3.2

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

May 20, 2024

Table of Contents

Descripción general de SD-WAN

Obtenga información sobre SD-WAN y planifique su configuración para garantizar una implementación correcta.

Acerca de SD-WAN

La WAN definida por software (SD-WAN) es una tecnología que le permite utilizar varios servicios privados y de Internet para crear una WAN inteligente y dinámica, lo que ayuda a reducir los costes y a maximizar la calidad de la aplicación y el uso. A partir de PAN-OS® 9.1, Palo Alto Networks® ofrece una seguridad sólida con una superposición de SD-WAN en un solo sistema de gestión. SD-WAN en un cortafuegos de Palo Alto Networks le permite usar servicios de Internet más económicos y un número inferior de piezas de equipo en lugar de utilizar MPLS costosos y que precisan mucho tiempo con componentes como enrutadores, cortafuegos, controladores de ruta WAN y optimizadores WAN para conectar su red WAN a Internet. No es necesario que compre y mantenga otros componentes de WAN.

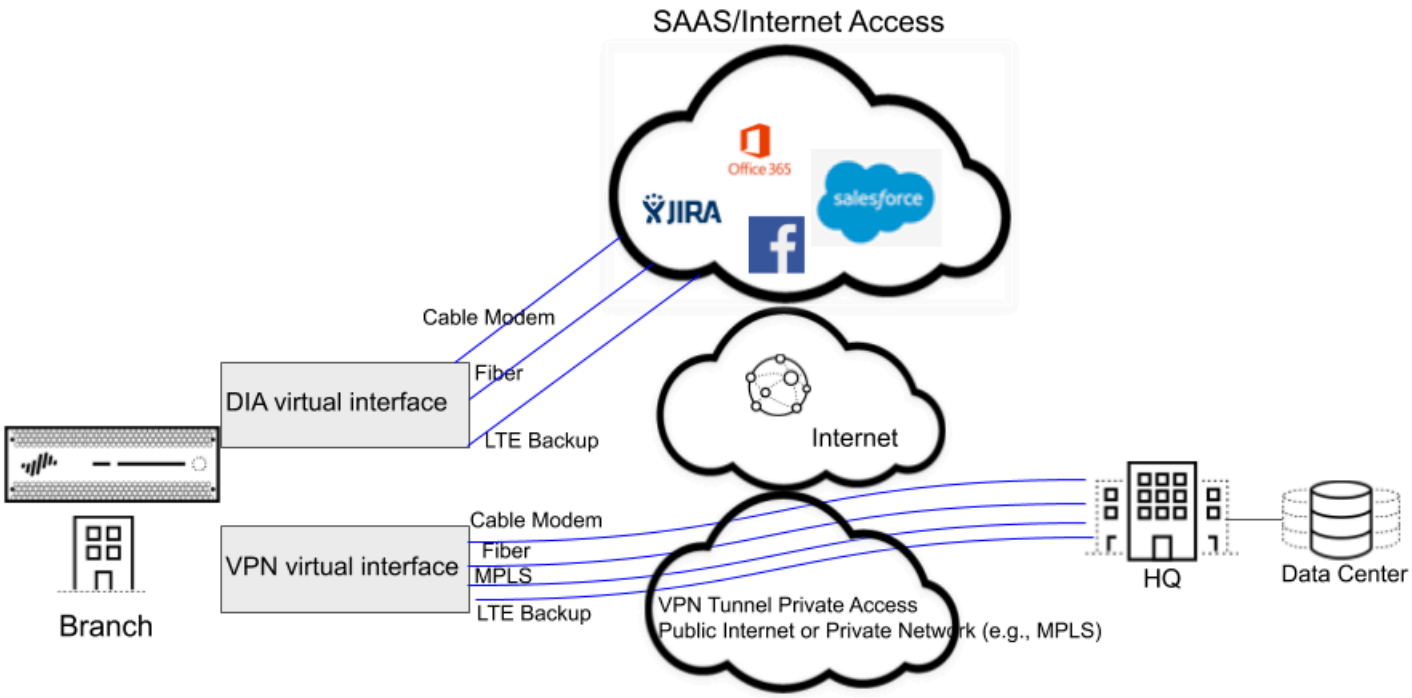
- Seguridad de PAN-OS con funcionalidad SD-WAN
- Compatibilidad del enlace de SD-WAN y el cortafuegos
- Compatibilidad con el hub de Prisma Access
- Gestión centralizada

Seguridad de PAN-OS con funcionalidad SD-WAN

El complemento de SD-WAN está integrado con PAN-OS, para que obtenga las características de seguridad de un cortafuegos PAN-OS y la funcionalidad de SD-WAN de un solo proveedor. La superposición de SD-WAN admite una selección de ruta dinámica e inteligente basada en aplicaciones y servicios y las condiciones de los enlaces que cada aplicación o servicio pueden usar. La supervisión del estado de la ruta para cada enlace incluye latencia, jitter y pérdida de paquetes. Los controles granulares de aplicaciones y servicios le permiten dar prioridad a las aplicaciones en función de si la aplicación es de misión crítica, sensible a la latencia o, por ejemplo, cumple ciertos criterios de estado. La selección de ruta dinámica permite evitar problemas de fallo de nodo y caída de voltaje porque las sesiones se conmutan por error a una ruta de mejor rendimiento en menos de un segundo.

La superposición de SD-WAN funciona con todas las funciones de seguridad de PAN-OS, como User-ID™ y App-ID™, para proporcionar un control de seguridad completo a las sucursales. El conjunto completo de capacidades de App-ID (descodificador de App-ID, caché de App-ID y listas dinámicas externas de direcciones IP de lista de origen/destino [EDL]) identifica las aplicaciones para el control del tráfico de SD-WAN basado en aplicaciones. Puede implementar el cortafuegos con la segmentación de tráfico de Zero Trust. Puede configurar y gestionar SD-WAN centralmente desde la interfaz web de Panorama o la API de REST de Panorama.

Es posible que tenga servicios basados en la nube y, en lugar de hacer que su tráfico de Internet fluya desde las sucursales al hub hasta nube, desee que el tráfico de Internet fluya directamente desde las sucursales a la nube mediante un ISP conectado directamente. Dicho acceso desde una sucursal a Internet es el Acceso directo a Internet (DIA). No tiene por qué gastar el ancho de banda y el dinero de su hub en el tráfico de Internet. El cortafuegos de sucursal ya se encarga de la seguridad, por lo que no necesita el cortafuegos del hub para que se cumpla la seguridad en el tráfico de Internet. Utilice DIA en sucursales para SaaS, exploración web o aplicaciones de gran ancho de banda que no deberían devolverse a un hub. En la siguiente figura se muestra una interfaz virtual de DIA que consta de tres enlaces desde la sucursal a la nube. La figura también muestra una interfaz virtual de túnel VPN que consta de cuatro enlaces que conectan la sucursal a la sede.



Compatibilidad del enlace de SD-WAN y el cortafuegos

La agrupación de enlaces le permite agrupar varios enlaces físicos (que los distintos ISP usan para comunicarse con el mismo destino) en una interfaz de SD-WAN virtual. Sobre la base de las aplicaciones y servicios, el cortafuegos elige entre los enlaces (selección de ruta) para compartir la carga de la sesión y proporcionar protección contra fallos en caso de una caída de tensión o un apagón. Por lo tanto, está proporcionando a la aplicación el mejor rendimiento de calidad. El cortafuegos realiza automáticamente el intercambio de carga de la sesión a través de los enlaces en una interfaz de SD-WAN virtual para utilizar el ancho de banda disponible de manera que resulte ventajosa. Una interfaz de SD-WAN debe tener el mismo tipo de conexión (DIA o VPN). Los enlaces de la VPN son compatibles con la topología de red radial.

SD-WAN admite los siguientes tipos de conexiones WAN: ADSL/DSL, cable módem, Ethernet, fibra, LTE/3G/4G/5G, MPLS, microondas/radio, satélite, WiFi y cualquiera que finalice como Ethernet en la interfaz del cortafuegos. La decisión de la estrategia adecuada sobre cómo usar los enlaces es suya. Puede usar conexiones de banda ancha de bajo coste en lugar de las costosas conexiones MPLS o LTE. También puede usar túneles VPN específicos para llegar a los hubs específicos en una región.

Consulte los requisitos del sistema para SD-WAN para obtener una lista completa de los modelos de cortafuegos que admiten las capacidades del software SD-WAN.

Si es un cliente nuevo que adquiere un cortafuegos de nueva generación de Palo Alto Networks, utilizará el enrutador virtual predeterminado para SD-WAN. Si es un cliente existente, puede optar por dejar que PAN-OS sobrescriba los enrutadores virtuales existentes o usar un nuevo

enrutador virtual y nuevas zonas para SD-WAN para mantener el contenido de SD-WAN separado de su configuración preexistente.

A partir de PAN-OS 11.0, el complemento 3.1 de SD-WAN admite un motor de enrutamiento avanzado que utiliza una metodología de configuración estándar del sector para facilitar las tareas del administrador. Aunque conceptualmente equivalente, el motor de enrutamiento avanzado utiliza enrutadores lógicos en lugar de enrutadores virtuales para crear instancias de dominios de enrutamiento. Cuando habilita el enrutamiento avanzado, se crean enrutadores lógicos y se utiliza el motor de enrutamiento avanzado para el enrutamiento. Cuando deshabilita el enrutamiento avanzado, se crean enrutadores virtuales y se utiliza un motor heredado para el enrutamiento.

Compatibilidad con el hub de Prisma Access

Con el complemento SD-WAN 2.2 y versiones posteriores, PAN-OS Secure SD-WAN ofrece compatibilidad con el hub de Prisma Access para brindarle un control total acerca de cómo y dónde se protegen las aplicaciones. La compatibilidad con el hub de Prisma Access permite que los cortafuegos PAN-OS se conecten a los nodos de cómputo (CN) de Prisma Access para lograr seguridad basada en la nube en una topología de hub-and-spoke de SD-WAN. Esta compatibilidad permite una conmutación por error de enlace sin interrupciones desde la seguridad local a Prisma Access y la capacidad de combinar ambos para satisfacer sus necesidades de seguridad.

En una topología mixta con cortafuegos SD-WAN y hubs de Prisma Access, los hubs SD-WAN son CN (nodos de terminación IPSec) de Prisma Access y las sucursales SD-WAN son cortafuegos PAN-OS. SD-WAN crea automáticamente túneles IKE e IPSec que conectan la sucursal al hub. Con los perfiles de distribución de tráfico, puede crear políticas SD-WAN para que coincidan con aplicaciones de Internet específicas y redirigirlas a un cortafuegos PAN-OS o a una implementación de Prisma Access de su elección. Con la compatibilidad con el hub de Prisma Access, las plataformas de seguridad locales y en la nube trabajan juntas para brindar una solución completa con políticas de seguridad coherentes gestionadas por Panorama.

Consulte los requisitos del sistema para SD-WAN para conocer las versiones mínimas de complementos de PAN-OS y SD-WAN requeridas para la compatibilidad con el hub de Prisma Access.

La compatibilidad con el hub de Prisma Access tiene las siguientes limitaciones:

- No se admite la importación y la exportación de una configuración SD-WAN relacionada con Prisma Access.
- La carga, la carga parcial, la reversión y la reversión parcial para la configuración de Prisma Access no son compatibles.
- No se admite la incorporación a un nodo de procesamiento de seguridad de red remoto de Prisma Access (RN-SPN). Para una sucursal existente que está conectada a Prisma Access, debe eliminar la sucursal y luego incorporarla nuevamente.
- No hay comandos de la CLI de SD-WAN disponibles en los cortafuegos de Prisma Access.
- En un CN, no hay selección de ruta para el tráfico que se origina en el CN.
- Las estadísticas de Prisma Access no se proporcionan en los informes y estadísticas de SD-WAN.

Gestión centralizada

Panorama™ proporciona los medios para configurar y gestionar SD-WAN, lo que hace que la configuración de varias opciones en muchos cortafuegos dispersos geográficamente sea mucho más rápida y fácil que la configuración individual de cortafuegos. Puede cambiar las configuraciones de red desde una única ubicación en lugar de configurar cada cortafuegos individualmente. La configuración de VPN automática permite que Panorama configure sucursales y hubs con conexiones IKE/IPSec seguras. Un clúster de VPN define los hubs y las sucursales que se comunican entre sí en una región geográfica. El cortafuegos utiliza túneles VPN para la supervisión del estado de la ruta entre una sucursal y un hub para proporcionar una detección subsecundaria de las condiciones de caída de tensión.

El panel de Panorama ofrece visibilidad de los enlaces y el rendimiento de su SD-WAN para que pueda ajustar los umbrales de calidad de ruta y otros aspectos de SD-WAN para mejorar su rendimiento. Las estadísticas y los informes centralizados incluyen estadísticas de rendimiento de aplicaciones y enlaces, mediciones de estado de ruta y análisis de tendencias, y vistas enfocadas de problemas de aplicaciones y enlaces.

Comience por comprender su caso de uso de SD-WAN, luego revise los elementos de configuración de SD-WAN y los métodos de distribución de tráfico y, después, planifique su configuración de SD-WAN. Para acelerar en gran medida la configuración, la práctica recomendada es exportar un CSV de dispositivo de SD-WAN vacío e introducir información como la dirección IP de la sucursal, el enrutador virtual que se utilizará, el nombre del sitio del cortafuegos, las zonas a las que pertenece el cortafuegos e información sobre la ruta de BGP. Panorama utiliza el archivo CSV para configurar los hubs y las sucursales de SD-WAN y para aprovisionar automáticamente túneles VPN entre los hubs y sucursales. SD-WAN admite el enrutamiento dinámico a través de eBGP y se configura mediante el complemento de SD-WAN de Panorama para permitir que todas las sucursales se comuniquen solo con el hub, o con el hub y otras sucursales.

Si Panorama administra un cortafuegos de sistemas virtuales múltiples, todas las interfaces y configuraciones habilitadas para SD-WAN deben configurarse en vsys1.

SD-WAN no admite una configuración SD-WAN en varios sistemas virtuales de un cortafuegos de sistemas virtuales múltiples.

Las interfaces SD-WAN deben configurarse en el mismo enrutador virtual; no se pueden dividir entre enrutadores virtuales.

Requisitos del sistema para SD-WAN

Revise las versiones mínimas de software, las versiones del complemento y los requisitos de recursos para el complemento Panorama™ para SD-WAN.

A partir de PAN-OS 11.0, puede configurar el enrutamiento avanzado para SD-WAN con la versión 3.1 del complemento.

La siguiente tabla proporciona las versiones de complementos que son compatibles entre sí. Le sugerimos que utilice la versión del complemento de configuración en la nube de Prisma Access con la versión del complemento SD-WAN compatible correspondiente que figura en la tabla, ya que las versiones compatibles contienen nuevas funciones, correcciones de errores o mejoras.

Zero Trust	PAN-OS	Requisitos del sistema	Complemento de configuración de la nube de Prisma Access	Complemento SD-WAN
Panorama	11.2.3	• (Dispositivo virtual Panorama) **Disco del sistema:**disco del sistema de 224 GB • **CPU:**16 CPU • **Memoria:**memoria de 64 GB • **Modo de sistema:**modo panorámico y modo de solo administración • (Aplicación M-Series únicamente en modo de solo administración) Un par de discos de creación de logs RAID de 8 TB habilitado	—	3.3.1
	11.2.0		5.0.0-h22	3.3.0
	11.1.5		—	3.2.2
	11.1.3		5.0.0-h31	3.2.1
	11.1.0		4.0.0 y 5.0.0	3.2.0
	11.0.4		5.0.0-h21	3.1.3
	11.0.3		4.0.0 y 5.0.0	3.1.2
	11.0.2		4.0.0	3.1.2
	11.0.2		4.0.0	3.1.1
	11.0.1		3.2.1.h21	3.0.1-h6

Zero Trust	PAN-OS	Requisitos del sistema	Complemento de configuración de la nube de Prisma Access	Complemento SD-WAN
	11.0.1 es la versión 11.0.x recomendada.	*La información anterior se aplica a un máximo de 500 dispositivos gestionados. Para obtener información sobre el uso de un máximo de 1000 dispositivos gestionados, consulte* Requisitos del sistema para el dispositivo virtual Panorama		
	11.0.0		3.2.1-h3	3.1.0-h6
	10.2.8		4.0.0-h80, 4.1.0-h49 y 5.0.0-h9	3.0.7
	10.2.7		4.0.0 y 5.0.0	3.0.6
	10.2.6		4.0.0	3.0.6
	10.2.5		4.0.0	3.0.5
	10.2.4 *10.2.4 es la versión 10.2.x recomendada.*		3.2.1-h21	3.0.4
	10.2.3		3.2.1-h5	3.0.4
	10.2.1		No se admite en esta versión; se espera que se admita en una versión futura. No actualice a PAN-OS 11.1 si está utilizando SD-WAN	3.0.1
	10.2.0			3.0.0

Zero Trust	PAN-OS	Requisitos del sistema	Complemento de configuración de la nube de Prisma Access	Complemento SD-WAN
			con el complemento de configuración de la nube de Prisma Access.	
	10.1.11		4.0.0 y 5.0.0	2.2.6
	10.1.11		4.0.0	2.2.5
	10.1.10  *10.1.10 es la versión 10.1.x recomendada.*		4.0.0	2.2.4
	10.1.9  *10.1.9 es la versión 10.1.x recomendada.*		3.2.1-h5	2.2.4
	10.1.8		3.2.1-h5	2.2.2
	10.1.5-h1		2.1	2.2.1
	10.1.0		2.1	2.2
Cortafuegos de nueva generación	• **PAN-OS 11.1**: 11.1.0 • **PAN-OS 11.0**: 11.0.0 • **PAN-OS 10.2**: 10.2.0	n/c		

Zero Trust	PAN-OS	Requisitos del sistema	Complemento de configuración de la nube de Prisma Access	Complemento SD-WAN
	• **PAN-OS 10.1**: 10.1.4 • **PAN-OS 10.0**: 10.0.8			
Nodo de cómputo de Prisma Access	10.0.7*	* Nodo de cómputo de Prisma Access (nodos de terminación de IPSec) debe ejecutar PAN-OS 10.0.7 o una versión posterior a 10.0. Si es necesario, trabaje con su equipo de ventas para solicitar una actualización antes de intentar incorporar una sucursal a la central de Prisma Access.		

Los siguientes modelos de cortafuegos admiten las capacidades del software de SD-WAN:

- PA-220 y PA-220R
- PA-400 Series
- PA-820 y PA-850
- PA-1400 Series
- Serie PA-3200
- Serie PA-3400
- PA-5200 Series
- Serie PA-5400
- PA-7000 Series
- Cortafuegos VM-Series.

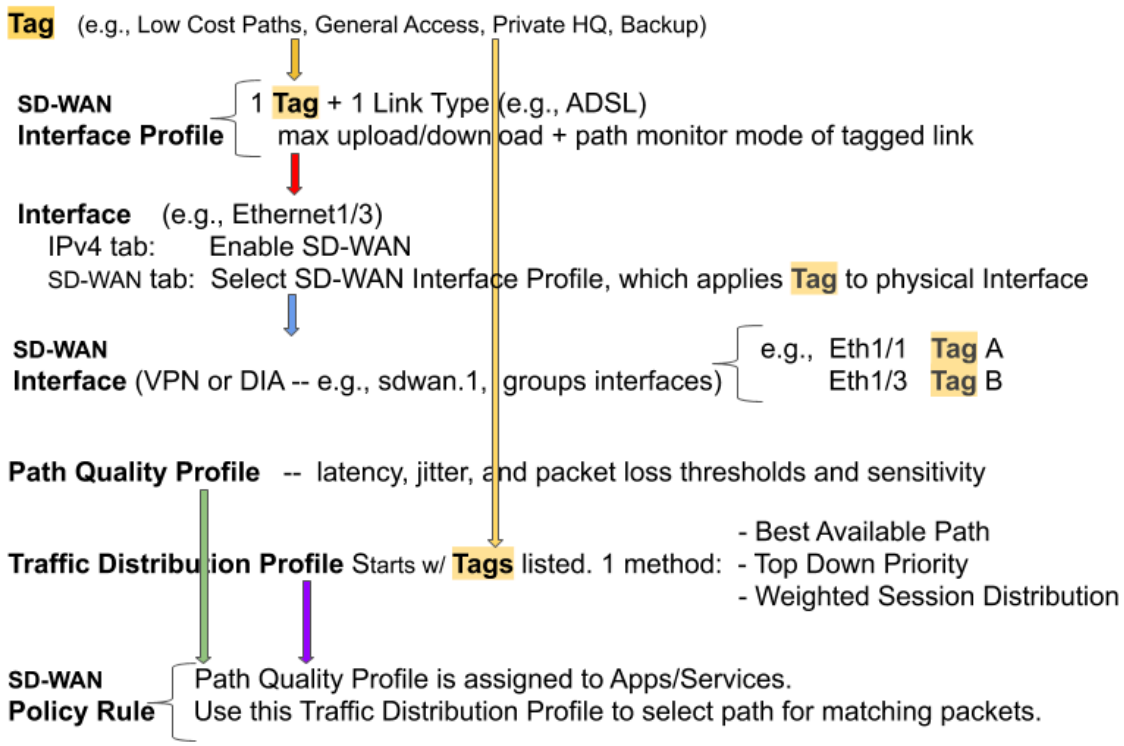
Para obtener más información sobre la disponibilidad de hardware específico, consulte la matriz de compatibilidad.

Elementos de configuración de SD-WAN

Los elementos de una configuración de SD-WAN funcionan juntos, lo que le permite:

- Agrupar las interfaces físicas de Ethernet que comparten un destino común en una interfaz de SD-WAN lógica.
- Especificar velocidades de enlace.
- Establecer los umbrales en los que una ruta deteriorada (caída de tensión o apagón) a una SD-WAN garantiza la selección de una nueva mejor ruta.
- Especificar el método de selección de esa nueva mejor ruta.

Esta vista indica las relaciones entre elementos de un vistazo.



El objetivo de una configuración de SD-WAN es controlar qué enlaces toma el tráfico al especificar los túneles VPN o el acceso directo a Internet (DIA) que ciertas aplicaciones o servicios llevan de una sucursal a una central o de una sucursal a Internet. Agrupe las rutas de modo que si una ruta se deteriora, el cortafuegos seleccione una nueva mejor ruta.

- El nombre de **etiqueta** que elija identificará a un enlace; aplique la etiqueta al enlace (interfaz) mediante un perfil de interfaz a la interfaz, como indica la flecha roja. Un enlace solo puede tener una etiqueta. Las dos flechas amarillas indican que se hace referencia a una etiqueta en el perfil de interfaz y el perfil de distribución de tráfico. Las etiquetas le permiten controlar el orden en que se utilizan las interfaces para la distribución del tráfico. Las etiquetas permiten que Panorama configure sistemáticamente muchas interfaces de cortafuegos con la funcionalidad de SD-WAN.

- Un **perfil de interfaz SD-WAN** especifica la etiqueta que aplica a la interfaz física y también el tipo de enlace que es esa interfaz (ADSL/DSL, cable módem, Ethernet, fibra, LTE/3G/4G/5G, MPLS, microondas/radio, satélite, WiFi u otro). El perfil de interfaz también es donde se especifican las velocidades máximas de carga y descarga (en Mbps) de la conexión del ISP. También puede cambiar si el cortafuegos supervisa la ruta con frecuencia o no; el cortafuegos supervisa los tipos de enlace adecuadamente de forma predeterminada.
- Una **interfaz** Ethernet de capa 3 con una dirección IPv4 o IPv6 puede admitir las funcionalidades de SD-WAN. Aplique un perfil de interfaz de SD-WAN a esta interfaz (flecha roja) para indicar las características de la interfaz. La flecha azul indica que las interfaces físicas están referenciadas y agrupadas en una interfaz de SD-WAN virtual.
- Una **interfaz de SD-WAN virtual** es un túnel VPN o grupo DIA de una o más interfaces que constituyen una interfaz de SD-WAN virtual numerada a la que puede enrutar el tráfico. Todas las rutas que pertenecen a una interfaz de SD-WAN van a la misma WAN de destino y son todas del mismo tipo (DIA o túnel VPN). La etiqueta A y la etiqueta B indican que las interfaces físicas para la interfaz virtual pueden tener etiquetas diferentes.
- Un **perfil de calidad de ruta** especifica los umbrales máximos de latencia, vibración y pérdida de paquetes. La superación de un umbral indica que la ruta se ha deteriorado y el cortafuegos debe seleccionar una nueva ruta hacia el destino. Una configuración de sensibilidad alta, media o baja le permite indicar al cortafuegos qué parámetro de supervisión de ruta es más importante para las aplicaciones a las que se aplica el perfil. La flecha verde indica que hace referencia a un perfil de calidad de ruta en una o más reglas de políticas de SD-WAN; por lo tanto, puede especificar diferentes umbrales para las reglas aplicadas a los paquetes que tienen diferentes aplicaciones, servicios, orígenes, destinos, zonas y usuarios.
- Un **perfil de distribución de tráfico** especifica cómo el cortafuegos determina una nueva mejor ruta si la ruta preferida actual supera un umbral de calidad de ruta. Especifique las etiquetas que usará el método de distribución para limitar su selección de una nueva ruta; por lo tanto, la flecha amarilla debe apuntar desde las etiquetas hasta el perfil de distribución de tráfico. Un perfil de distribución de tráfico especifica el método de distribución para la regla.
- Los elementos anteriores se recopilan en **Reglas de políticas de SD-WAN**. La flecha morada indica que hace referencia a un perfil de elegibilidad de ruta y un perfil de distribución de tráfico en una regla, junto con aplicaciones/servicios de paquetes, fuentes, destinos y usuarios para indicar específicamente cuándo y cómo el cortafuegos realiza la selección de ruta de SD-WAN basada en aplicaciones para un paquete que no pertenece a una sesión. (También puede hacer referencia a un **perfil de calidad de SaaS** y un **perfil de corrección de errores** en una regla de políticas SD-WAN).

Ahora que comprende la relación entre los elementos, revise los métodos de distribución del tráfico y, a continuación, Planificación de la configuración de SD-WAN.

Planificación de la configuración de SD-WAN

Planifique la topología completa de las interfaces de cortafuegos de su sucursal y central habilitadas para SD-WAN para poder crear plantillas de Panorama™ con archivos CSV y luego enviar las configuraciones a los cortafuegos.

STEP 1 | Planifique las ubicaciones de sucursales y centrales, los requisitos de enlace y las direcciones IP. Desde Panorama, deberá exportar un CSV de dispositivo de SD-WAN vacío y completarlo con información de la sucursal y la central.

1. Decida la función de cada cortafuegos (sucursal o central).
2. Determine qué sucursales se comunicarán con qué centrales; cada grupo funcional de cortafuegos de sucursal y central que se comunican entre sí es un clúster de VPN. Por ejemplo, sus clústeres de VPN pueden estar organizados geográficamente o por función.
3. Determine los tipos de enlace de ISP que admite cada sucursal y central: ADSL/DSL, cable módem, Ethernet, fibra, LTE/3G/4G/5G, MPLS, microondas/radio, satélite y WiFi.
4. Determine el ancho de banda máximo de carga y descarga (Mbps) que admiten los tipos de enlace y cómo desea aplicar estos controles de velocidad a los enlaces, como se describe en el paso 2. Registre el ancho de banda máximo de carga y descarga del enlace ISP (Mbps). Esta información servirá como máximos de salida de referencia si necesita configurar QoS para controlar el ancho de banda de la aplicación.
5. Reúna las direcciones IP públicas de los cortafuegos de las sucursales, ya sean estáticas o asignadas dinámicamente. El cortafuegos debe tener una dirección IP pública enrutable a Internet para poder iniciar y finalizar túneles IPSec y enrutar el tráfico de aplicaciones hacia o hasta Internet.

   El equipo de las instalaciones del cliente del ISP debe estar conectado directamente a la interfaz Ethernet en el cortafuegos.

   Si tiene un dispositivo que realiza NAT ubicado entre el cortafuegos de la sucursal y la central, el dispositivo NAT puede evitar que el cortafuegos muestre los túneles IPSec y la creación de peers de IKE. Si el túnel falla, trabaje con el administrador del dispositivo NAT remoto para resolver el problema.
6. Reúna los prefijos de red privada y los números de serie de los cortafuegos de sucursales y centrales.
7. Decida el tipo de enlace de cada interfaz de cortafuegos.

   Asigne los mismos tipos de enlace en las mismas interfaces Ethernet a través de los cortafuegos de la sucursal para facilitar la configuración. Por ejemplo, Ethernet1/1 es siempre cable módem.
8. Decida las convenciones de nomenclatura para sus sitios y dispositivos de SD-WAN.

   No utilice los nombres de host simples "central" o "sucursal" porque la configuración de VPN automática utiliza estas palabras clave para generar varios elementos de configuración.
9. Si ya tiene zonas en su lugar antes de configurar SD-WAN, decida cómo asignar esas zonas a las zonas predefinidas que SD-WAN usa para la selección de ruta. Asignará

zonas existentes a las zonas predefinidas llamadas Zona a interno, zona a central, zona a sucursal y zona a Internet.

La información que especificará en un CSV (para poder añadir varios dispositivos de SD-WAN a la vez) incluye: número de serie, tipo de dispositivo (sucursal o central), nombres de zonas para asignar a zonas predefinidas (clientes preexistentes), dirección de bucle invertido, prefijos para redistribuir, número AS, ID del enrutador y nombre del enrutador virtual.

STEP 2 | Planifique paquetes de enlaces y seguridad VPN para enlaces privados.

Un paquete de enlaces le permite combinar varios enlaces físicos en una interfaz SD-WAN virtual con fines de selección de ruta y protección contra conmutación por error. Si tiene un paquete de más de un enlace físico, se maximiza la calidad de la aplicación en caso de que se deteriore un enlace físico. Para crear un paquete, aplique la misma etiqueta de enlace a varios enlaces (a través de un perfil de interfaz de SD-WAN). La etiqueta de enlace identifica un conjunto de enlaces que tienen un tipo similar de acceso y gestión de políticas de SD-WAN. Por ejemplo, puede crear una etiqueta de enlace denominada **`banda ancha de bajo coste`** e incluir los servicios de módem de cable y banda ancha de fibra.

STEP 3 | Identifique las aplicaciones que utilizarán la optimización de SD-WAN y QoS.

1. Identifique las aplicaciones comerciales críticas y sensibles a la latencia para las que proporcionará control y políticas de SD-WAN. Estas son aplicaciones que requieren una buena experiencia de usuario y susceptibles a fallar en condiciones de enlace deficientes.

   Comience con las aplicaciones más críticas y sensibles a la latencia; puede añadir aplicaciones después de que SD-WAN funcione sin problemas.

2. Identifique las aplicaciones que requieran políticas de QoS para dar prioridad al ancho de banda. Estas deberían ser las mismas aplicaciones que identificó como críticas o sensibles a la latencia.

   Comience con las aplicaciones más críticas y sensibles a la latencia; puede añadir aplicaciones después de que SD-WAN funcione sin problemas.

STEP 4 | Determine cuándo y cómo desea que los enlaces se conmuten por error a un enlace diferente en caso de que el enlace original se degrade o falle.

1. Decida el modo de supervisión de ruta para un enlace, aunque se recomienda mantener la configuración predeterminada para el tipo de enlace:

   - **Agresivo**: el cortafuegos envía paquetes de sondeo al extremo opuesto del enlace de SD-WAN a una frecuencia constante (cinco sondas por segundo de manera predeterminada). El modo agresivo es apropiado para enlaces donde la calidad de la ruta de supervisión es crítica; donde necesita detección rápida y conmutación por error para condiciones de caída de tensión y apagón. El modo agresivo proporciona detección por debajo de un segundo y conmutación por error.
   - **Relajado**: el cortafuegos observa un tiempo inactivo configurable entre el envío de paquetes de sondeo durante siete segundos (a la frecuencia de sondeo que configure), lo que hace que la supervisión de la ruta sea menos frecuente que el modo agresivo. El modo relajado es adecuado para enlaces que tienen un ancho de banda muy bajo, enlaces con un coste de funcionamiento alto, como satélite o LTE, o

cuando la detección rápida no es tan importante como conservar el coste y el ancho de banda.

2. Priorice el orden en que el cortafuegos selecciona el primer enlace para una nueva sesión y el orden en que los enlaces deben ser candidatos para reemplazar un enlace que está fallando, en el caso de que haya más de un candidato.

   Por ejemplo, si desea que un enlace LTE de respaldo costoso sea el último enlace utilizado (solo cuando haya una suscripción excesiva de los enlaces de banda ancha de bajo coste o estén completamente inactivos), utilice el método de distribución de tráfico prioritario de arriba hacia abajo y coloque la etiqueta que está en el enlace LTE en el último lugar de la lista de etiquetas para el perfil de distribución de tráfico.

3. Para las aplicaciones y los servicios, determine los umbrales de estado de la ruta en los que considere que una ruta se ha degradado lo suficiente como para que el cortafuegos seleccione una nueva ruta (conmutación por error). Las características de calidad son latencia (intervalo de 10 a 2000 ms), fluctuación (intervalo de 10 a 1000 ms) y porcentaje de pérdida de paquetes.

   Estos umbrales constituyen un perfil de calidad de ruta, al que hace referencia en una regla de políticas de SD-WAN. Cuando se supera cualquier umbral único (para pérdida de paquetes, vibración o latencia) (y se cumplen los criterios de regla restantes), el cortafuegos elige una nueva ruta preferida para el tráfico correspondiente. Por ejemplo, puede crear el perfil AAA de calidad de ruta con umbrales de latencia/vibración/pérdida de paquetes de 1000/800/10 que usar en la regla 1 con paquetes provenientes de la zona de origen XYZ, y crear el perfil BBB de calidad de ruta (con umbrales de 50/200/5) para usarlo en la regla 2 con paquetes FTP provenientes de la dirección IP de origen 10.1.2.3. Se recomienda comenzar con umbrales altos y probar cómo los tolera la aplicación. Si establece valores demasiado bajos, la aplicación puede cambiar las rutas con demasiada frecuencia.

   Considere si las aplicaciones y servicios que está utilizando son especialmente sensibles a la latencia, la vibración o la pérdida de paquetes. Por ejemplo, una aplicación de vídeo puede tener un buen almacenamiento en búfer que reduzca la latencia y la vibración de fase, pero sería sensible a la pérdida de paquetes, lo que afectaría la experiencia del usuario. Puede establecer la sensibilidad de los parámetros de calidad de ruta en el perfil en alta, media o baja. Si la configuración de sensibilidad para la latencia, vibración y pérdida de paquetes es la misma, el cortafuegos examina los parámetros en el orden de pérdida de paquetes, latencia y vibración.

4. Decida si hay enlaces entre los que cargar nuevas sesiones compartidas para una aplicación o servicio.

STEP 5 | Planifique las configuraciones de BGP que Panorama enviará a las sucursales y centrales para enrutar dinámicamente el tráfico entre ellas.

1. Planifique la información de ruta de BGP, incluido un número de sistema autónomo (ASN) de cuatro bytes. Cada sitio de cortafuegos está en un AS separado y, por lo tanto, debe tener un ASN único. Los cortafuegos también deben tener un ID de enrutador único.
2. Antes de implementar SD-WAN con enrutamiento BGP en un entorno donde BGP ya está en uso, asegúrese de que la configuración BGP generada por el complemento SD-WAN no entre en conflicto con su configuración BGP existente. Por ejemplo, debe

utilizar el número BGP AS existente y los valores de ID del enrutador para los valores de dispositivo SD-WAN correspondientes.

3. Si no desea utilizar el enrutamiento dinámico de BGP, planifique utilizar las funciones de configuración de red de Panorama para eliminar otras configuraciones de enrutamiento. Puede configurar un enrutamiento estático entre la sucursal y las centrales. Simplemente omita toda la información de BGP en el complemento de Panorama y use rutas estáticas de enrutador virtual normales para realizar el enrutamiento estático.

STEP 6 | Tenga en cuenta las capacidades de los modelos de cortafuegos para las interfaces de SD-WAN, reglas de políticas de SD-WAN, tamaño de log, túneles IPSec (incluidos los ID de proxy), peers de IKE, tablas de rutas estáticas y BGP, peers de enrutamiento de BGP y rendimiento para su modo de cortafuegos (App-ID™, amenaza, IPSec y descifrado). Asegúrese de que los modelos de cortafuegos de sucursal y central que desee utilizar admitan las capacidades que necesita.

Configuración de SD-WAN

Después de Planificación de la configuración de SD-WAN, instale el complemento de SD-WAN y configure el servidor de gestión Panorama™ para administrar de manera centralizada la configuración de SD-WAN de los cortafuegos de su central y sucursal. Al aprovechar Panorama, reduce los requisitos de gestión y la sobrecarga operativa para administrar su implementación de SD-WAN. Además, podrá supervisar más fácilmente el estado de su enlace y solucionar problemas en caso de que surjan.

Si Panorama administra un cortafuegos de sistemas virtuales múltiples, todas las interfaces y configuraciones habilitadas para SD-WAN deben configurarse en vsys1.

SD-WAN no admite una configuración SD-WAN en varios sistemas virtuales de un cortafuegos de sistemas virtuales múltiples.

- Instalación del complemento de SD-WAN
- Configuración de Panorama y cortafuegos para SD-WAN
- Creación de una etiqueta de enlace
- Configuración de un perfil de la interfaz de SD-WAN
- Configuración de una interfaz Ethernet física para SD-WAN
- (Opcional) Configuración de una interfaz Ethernet de agregación subinterfaces para SD-WAN
- (Opcional) Configuración de subinterfaces de capa 3 para SD-WAN
- Configuración de una interfaz de SD-WAN virtual
- Creación de una ruta predeterminada a la interfaz de SD-WAN
- Configuración de los perfiles de gestión de enlaces SD-WAN
- Configuración de una regla de políticas de SD-WAN
- Permiso para realizar la conmutación por error del tráfico de acceso a Internet directo en el enlace de MPLS
- Configuración de AnyPath de DIA
- Distribución de sesiones no coincidentes
- Adición de dispositivos de SD-WAN a Panorama
- (Opcional) Configurar varios enrutadores virtuales en el hub de SD-WAN
- (Opcional) Configurar varios enrutadores virtuales en la sucursal SD-WAN
- (Opcional) Configuración de dispositivos de HA para SD-WAN
- Creación de un clúster de VPN
- Creación de un clúster de VPN de malla completa con servicio DDNS
- (Opcional) Creación de una ruta estática para SD-WAN
- (Opcional) Configure el enrutamiento avanzado para SD-WAN

Instalación del complemento de SD-WAN

Se requiere un servidor de gestión Panorama™ con un complemento de SD-WAN para configurar y gestionar una implementación de SD-WAN. Si Panorama está conectado a Internet, descargue el complemento de SD-WAN directamente desde Panorama e instálelo en el servidor de gestión Panorama. Si Panorama no está conectado a Internet, descargue el complemento de SD-WAN del Portal de atención al cliente de Palo Alto Networks® e instálelo en el servidor de gestión Panorama.

- Instalación del complemento de SD-WAN con Panorama conectado a Internet
- Instalación del complemento de SD-WAN sin Panorama conectado a Internet

Instalación del complemento de SD-WAN con Panorama conectado a Internet

Se requiere un servidor de gestión Panorama™ con un complemento de SD-WAN instalado para configurar y gestionar una implementación de SD-WAN. Cuando Panorama esté conectado a Internet, debe descargar e instalar el complemento de SD-WAN directamente desde la interfaz web de Panorama. El complemento debe instalarse solo en la solución de Panorama que gestione sus cortafuegos de SD-WAN, y no en los cortafuegos de la central y de la sucursal individuales.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **Complementos**, busque el complemento **`sd_wan`** y elija **Comprobar ahora** para obtener la versión más reciente del complemento.

STEP 3 | Seleccione **Descargar** e **Instalar** el complemento de SD-WAN.

STEP 4 | Después de instalar correctamente el complemento de SD-WAN, seleccione **Confirmar** y **Confirmar en Panorama**.

Este paso es necesario para poder confirmar cualquier cambio de configuración en Panorama.

STEP 5 | (Únicamente modo de solo gestión) Habilite los discos de creación de logs necesarios para almacenar datos de supervisión de SD-WAN.

- **Dispositivos M-Series**: todos los dispositivos de M-Series vienen con dos pares de discos de creación de logs de 8 TB en RAID 1 de manera predeterminada. Al gestionar cortafuegos que aprovechan SD-WAN de Panorama en modo de solo gestión, debe habilitar el primer par de los pares de discos de creación de logs para almacenar datos de supervisión de SD-WAN.

  1. Inicio de sesión en la CLI de Panorama.
  2. Habilite el primer par de los pares de discos de creación de logs incluidos de forma predeterminada con su dispositivo M-Series.

     ```
     > request system raid add A1
     ```


3. Verifique que la creación de logs del `par de discos de creación de logs A` esté `disponible`:

```
> show system raid detail
```

Cuando la configuración de RAID finalice, aparece la siguiente respuesta:

```
Disk Pair A       Available Status         clean Disk id A1
     Present model : ST91000640NS size : 953869 MB status :
 active sync
```

4. Haga que los pares de discos de creación de logs estén disponibles para la creación de logs.
   1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
   2. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir cada matriz.
   3. Haga clic en **OK (Aceptar)** para guardar los cambios.
   4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** para confirmar los cambios.
   5. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)**, seleccione el grupo de recopiladores y haga clic en **Push (Enviar)** para enviar los cambios.

- **Dispositivos virtuales de Panorama**: si implementó el dispositivo virtual de Panorama en modo de solo administración, debe aumentar el disco del sistema a 224 GB para almacenar datos de supervisión de SD-WAN.

STEP 6 | Continúe con Configuración de Panorama y cortafuegos para SD-WAN para comenzar a configurar la implementación de SD-WAN.

Instalación del complemento de SD-WAN sin Panorama conectado a Internet

Se requiere un servidor de gestión Panorama™ con un complemento de SD-WAN para configurar y gestionar una implementación de SD-WAN. Si Panorama no está conectado a Internet, debe descargar el complemento de SD-WAN del Portal de atención al cliente de Palo Alto Networks y cargar el complemento en Panorama. El complemento debe instalarse solo en la solución de Panorama que gestione sus cortafuegos de SD-WAN, y no en los cortafuegos de la central y de la sucursal individuales.

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

STEP 2 | Seleccione **Actualizaciones** > **Actualizaciones de software** y, en el menú desplegable Filtrar por, seleccione **Complemento de integración de Panorama**.

STEP 3 | Localice y descargue el **complemento de SD-WAN**.

STEP 4 | Inicio de sesión en la interfaz web de Panorama.

STEP 5 | Seleccione **Panorama** > **Complementos** y **cargue** el complemento de SD-WAN.

STEP 6 | **Examine** y busque el complemento de SD-WAN que descargó del Portal de atención al cliente y haga clic en **Aceptar**.

STEP 7 | **Instale** el complemento de SD-WAN.

STEP 8 | Después de instalar correctamente el complemento de SD-WAN, seleccione **Confirmar** y **Confirmar en Panorama**.

Este paso es necesario para poder confirmar cualquier cambio de configuración en Panorama.

STEP 9 | (Únicamente modo de solo gestión) Habilite los discos de creación de logs necesarios para almacenar datos de supervisión de SD-WAN.

- **Dispositivos M-Series**: todos los dispositivos de M-Series vienen con dos pares de discos de creación de logs de 8 TB en RAID 1 de manera predeterminada. Al gestionar cortafuegos que aprovechan SD-WAN de Panorama en modo de solo gestión, debe habilitar el primer par de los pares de discos de creación de logs para almacenar datos de supervisión de SD-WAN.

  1. Inicio de sesión en la CLI de Panorama.
  2. Habilite el primer par de los pares de discos de creación de logs incluidos de forma predeterminada con su dispositivo M-Series.

     ```
     > request system raid add A1
     ```

  3. Verifique que la creación de logs del `par de discos de creación de logs A` esté `disponible`:

     ```
     > show system raid detail
     ```

     Cuando la configuración de RAID finalice, aparece la siguiente respuesta:

     ```
     Disk Pair A       Available Status         clean Disk id A1
          Present model : ST91000640NS size : 953869 MB status :
      active sync
     ```

  4. Haga que los pares de discos de creación de logs estén disponibles para la creación de logs.

     1. Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** y edite el recopilador de logs.
     2. Seleccione **Disks (Discos)** y haga clic en **Add (Añadir)** para añadir cada matriz.
     3. Haga clic en **OK (Aceptar)** para guardar los cambios.
     4. Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y seleccione **Commit (Confirmar)** para confirmar los cambios.
     5. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)**, seleccione el grupo de recopiladores y haga clic en **Push (Enviar)** para enviar los cambios.

- **Dispositivos virtuales de Panorama**: si implementó el dispositivo virtual de Panorama en modo de solo administración, debe aumentar el disco del sistema a 224 GB para almacenar datos de supervisión de SD-WAN.

STEP 10 | Continúe con Configuración de Panorama y cortafuegos para SD-WAN para comenzar a configurar la implementación de SD-WAN.

Configuración de Panorama y cortafuegos para SD-WAN

Para poder comenzar a configurar la implementación de SD-WAN, debe añadir sus cortafuegos de la central y sucursal como dispositivos gestionados, y crear las plantillas necesarias y las configuraciones de grupo de dispositivos para enviar con éxito su configuración de SD-WAN a los cortafuegos de SD-WAN.

- Adición de tus cortafuegos SD-WAN como dispositivos gestionados
- Creación de una plantilla de red de SD-WAN
- Creación de zonas predefinidas en Panorama
- Creación de grupos de dispositivos de SD-WAN

Adición de tus cortafuegos SD-WAN como dispositivos gestionados

Para empezar a configurar la implementación de SD-WAN, primero debe Instalación del complemento de SD-WAN y añadir sus cortafuegos del hub y sucursal como dispositivos gestionados al servidor de gestión Panorama™. Como parte de la adición de su cortafuegos de SD-WAN como dispositivo gestionado en el servidor de gestión Panorama™, debe activar la licencia de SD-WAN para habilitar la funcionalidad de SD-WAN para el cortafuegos.

Además, como parte de la adición de sus cortafuegos de SD-WAN como dispositivos gestionados, debe configurar sus cortafuegos gestionados para reenviar logs a Panorama. Panorama recopila información de varios orígenes, como logs de configuración, logs de tráfico y mediciones de características de enlace para generar la visibilidad de la aplicación de SD-WAN y la información de estado del enlace.

No permita que su conexión de servidor de gestión de Panorama dependa solo de la superposición SD-WAN. Para mantener una conexión fiable, donde Panorama siempre es accesible para los cortafuegos PAN-OS, le recomendamos crear un túnel IPSec dedicado desde los cortafuegos PAN-OS para llegar a Panorama (que está fuera de la superposición SD-WAN entre el hub / sucursales donde se encuentra Panorama). Con este enfoque, puede garantizar que el servidor de gestión de Panorama siempre sea accesible, incluso si hay algún impacto en la superposición SD-WAN.

STEP 1 | Inicie la interfaz web del cortafuegos.

STEP 2 | Active su licencia de SD-WAN para habilitar la funcionalidad de SD-WAN en el cortafuegos.

Los cortafuegos que intente utilizar en su implementación de SD-WAN requieren un código de autenticación único para activar la licencia. Por ejemplo, si tiene 100 cortafuegos, debe adquirir

100 licencias de SD-WAN y activar cada licencia de SD-WAN en cada cortafuegos mediante uno de los 100 códigos de autenticación únicos.

Para los cortafuegos de VM-Series, debe aplicar el código de autenticación de SD-WAN en el cortafuegos específico de VM-Series. Si desactiva el cortafuegos de VM-Series, el código de autenticación de SD-WAN puede activarse en un cortafuegos de VM-Series diferente del mismo modelo.

Asegúrese de que su licencia de SD-WAN siga siendo válida para continuar aprovechando SD-WAN. Si la licencia de SD-WAN caduca, se produce lo siguiente:

- *Aparece una advertencia cuando **confirma** cualquier cambio de configuración, pero no se produce ningún fallo de confirmación.*
- *Su configuración de SD-WAN deja de funcionar, pero no se elimina.*
- *Los cortafuegos ya no supervisan ni recopilan métricas de estado del enlace y dejan de enviar sondas de supervisión.*
- *Los cortafuegos dejan de enviar aplicaciones y vinculan métricas de estado a Panorama.*
- *La lógica de selección de ruta de SD-WAN se deshabilita.*
- *Las nuevas sesiones funcionan por turnos en la interfaz virtual de SD-WAN.*
- *Las sesiones existentes permanecen en el enlace específico en el que estaban cuando caducó la licencia.*
- *Si se produce una interrupción del servicio de Internet, el tráfico sigue utilizando el enrutamiento estándar y ECMP si están configurados.*

STEP 3 | Añada la dirección IP de Panorama al cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de Panorama.
2. Introduzca la dirección IP de Panorama en el primer campo.

   El FQDN de Panorama no es compatible con SD-WAN.

3. (Opcional) Si configura un par de alta disponibilidad (high availability, HA) en Panorama, introduzca la dirección IP de la instancia secundaria de Panorama en el segundo campo.
4. Compruebe que tiene la opción **Habilitar la inserción de datos de supervisión del dispositivo en Panorama** activada.
5. Haga clic en **OK (Aceptar)**.
6. **Commit (Confirmar)** los cambios.

STEP 4 | Configure el reenvío de logs a Panorama.

Es necesario reenviar logs desde los cortafuegos de SD-WAN a Panorama para mostrar los datos de Supervisión y creación de informes.

De forma predeterminada, la inspección HTTP/2 se habilita automáticamente si se activa el descifrado para el tráfico de aplicaciones. Las sesiones principales que utilizan una conexión HTTP/2 no generan ningún log de tráfico porque no incluyen tráfico de aplicaciones. Sin embargo, las sesiones secundarias generadas por las transmisiones dentro de la sesión principal HTTP/2 siguen generando logs de tráfico. Para obtener más información sobre cómo visualizar los logs para conexiones HTTP/2, consulte la base de conocimientos de Palo Alto Networks.

STEP 5 | Añada un cortafuegos o varios a Panorama.

Para obtener más detalles sobre cómo añadir cortafuegos a Panorama, consulte Adición de un cortafuegos como dispositivo gestionado.

1. Inicio de sesión en la interfaz web de Panorama.
2. Seleccione **Panorama** > **Dispositivos gestionados** > **Resumen** y **añada** los cortafuegos.
3. Especifique los números de serie de los cortafuegos.
4. Si va a añadir cortafuegos cuando los grupos de dispositivos y plantillas requeridos ya están creados, habilite (marque) **Asociar dispositivos** para asignar nuevos cortafuegos a los grupos de dispositivos y a la pila de plantillas adecuados.
5. Para añadir varios cortafuegos mediante un CSV, haga clic en **Importar** y **Descargar CSV de ejemplo** para completar la información del cortafuegos y, a continuación, **búsquelos** para importarlos.
6. Haga clic en **OK (Aceptar)**.

STEP 6 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esas acciones en su configuración.

STEP 7 | Repita los pasos del 2 al 5 en cada cortafuegos que pienses usar en la implementación de SD-WAN.

Creación de una plantilla de red de SD-WAN

Cree una plantilla que contenga todos los objetos de configuración de red para sus centrales y sucursales de SD-WAN. Debe crear una plantilla y una pila de plantillas independientes para los cortafuegos de su central y una plantilla y una pila de plantillas independientes para los cortafuegos de su sucursal. Se recomienda limitar la cantidad de plantillas y pilas de plantillas utilizadas para gestionar la configuración de su dispositivo de SD-WAN. La limitación de la cantidad de plantillas y pilas de plantillas utilizadas en todas las centrales y sucursales permite reducir en gran medida la sobrecarga operativa de la gestión de las configuraciones de varias centrales y sucursales de SD-WAN . Utilice la plantilla o las variables de pila de plantillas para ayudar a reducir la cantidad de plantillas utilizadas.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Cree la plantilla de red de la central de SD-WAN.

1. Seleccione **Panorama** > **Plantillas** y **añada** una nueva plantilla.
2. Introduzca un **Nombre** descriptivo para la plantilla.
3. (Opcional) Introduzca una **Description (Descripción)** para la plantilla.
4. Haga clic en **Aceptar** para guardar los cambios.

STEP 3 | Cree una pila de plantillas de la central.

1. Seleccione **Panorama** > **Plantillas** y haga clic en **Añadir pila** para agregar una nueva pila de plantillas.
2. Introduzca un **Nombre** descriptivo para la pila de plantillas.
3. (Opcional) Introduzca una **Description (Descripción)** para la plantilla.
4. **Añada** la plantilla de la red de SD-WAN que creó en el paso 2.
5. En la sección **Dispositivos**, active las casillas de todos los cortafuegos de la central de SD-WAN.
6. Haga clic en **Aceptar** para guardar los cambios.

STEP 4 | Cree la plantilla de red de la sucursal de SD-WAN.

1. **Añada** una nueva plantilla.
2. Introduzca un **Nombre** descriptivo para la plantilla.
3. (Opcional) Introduzca una **Description (Descripción)** para la plantilla.
4. Haga clic en **Aceptar** para guardar los cambios.

STEP 5 | Cree una pila de plantillas de la sucursal.

1. Haga clic en **Añadir pila** para agregar una nueva pila de plantillas.
2. Introduzca un **Nombre** descriptivo para la pila de plantillas.
3. (Opcional) Introduzca una **Description (Descripción)** para la plantilla.
4. **Añada** la plantilla de la red de SD-WAN que creó en el paso 4.
5. En la sección **Dispositivos**, active las casillas de todos los cortafuegos de la sucursal de SD-WAN.
6. Haga clic en **Aceptar** para guardar los cambios.

STEP 6 | Haga clic en **Commit (Confirmar)** para aceptar los cambios en la configuración.

Creación de zonas predefinidas en Panorama

Las reglas de políticas de SD-WAN usan zonas predefinidas para la selección de rutas internas y para files de reenvío de tráfico. Hay dos casos de uso; su caso de uso depende de si habilita SD-WAN en sus cortafuegos actuales de PAN-OS® con reglas de la política de seguridad existentes o si inicia una nueva implementación de PAN-OS sin reglas de la política de seguridad previas. Si sus cortafuegos actuales tienen reglas de la política de seguridad, puede asignar sus zonas existentes a las zonas predefinidas que usan las políticas de SD-WAN.

El motor de SD-WAN utiliza las zonas predefinidas para reenviar el tráfico. Además, la creación de zonas predefinidas en las plantillas de Panorama™ proporciona una visibilidad constante entre los cortafuegos gestionados y Panorama:

- **Zona a Internet**: para el tráfico que va y viene de Internet que no es fiable.
- **Zona a hub**: para el tráfico que sale de los cortafuegos de la sucursal a los del hub y para el tráfico entre cortafuegos del hub.
- **Zona a sucursal**: para el tráfico que sale de los cortafuegos del hub a los de la sucursal y para el tráfico entre cortafuegos de la sucursal.
- **Zona a interno**: para el tráfico interno en una ubicación específica.
- **Zona a PA Hub**: para que el tráfico interno llegue al hub de Prisma Access.

Si no crea las zonas predefinidas, el complemento de SD-WAN creará automáticamente las zonas predefinidas en la sucursal y el cortafuegos del hub, pero no las verá en Panorama.

Existen dos casos de uso principales para zonas predefinidas:

- **Zonas existentes**: ya tiene zonas preexistentes que creó para usar en User-ID™ o varias políticas (reglas de la política de seguridad, reglas de la política de QoS, protección de zona y protección de búfer de paquetes). Debe asignar las zonas preexistentes a las zonas predefinidas que SD-WAN usa para que el cortafuegos pueda reenviar el tráfico correctamente. Debe continuar usando las zonas preexistentes en todas sus políticas porque las nuevas zonas predefinidas se usan solo para el reenvío de SD-WAN. Se asignarán las zonas cuando vaya a Adición de dispositivos de SD-WAN a Panorama mediante la creación de su archivo CSV. (Si no está utilizando un archivo CSV, asignará zonas cuando configure **Panorama** > **SD-WAN** > **Devices [Dispositivos]** y añada las zonas existentes en **Zone Internet [Zona a Internet]**, **Zone to Hub [Zona a hub]**, **Zone to Branch [Zona a sucursal]** y **Zone Internal [Zona a interno]**.)

  El resultado de la asignación es que un cortafuegos de sucursal o hub puede realizar una búsqueda de reenvío para determinar la interfaz de salida de SD-WAN y, por lo tanto, la zona de salida. Si no asigna zonas preexistentes a zonas predefinidas, una sesión permitida no utilizará SD-WAN. La asignación es necesaria porque los clientes existentes tienen diferentes nombres de zona en su lugar, y el cortafuegos debe limitar todos esos nombres de zona a las zonas predefinidas. No tiene que asignar necesariamente zonas a todas las zonas predefinidas, pero debe asignar zonas existentes al menos a las zonas **`Zona a hub`** y **`Zona a sucursal`**.
- **Sin zonas existentes**: tiene una nueva implementación de cortafuegos de Palo Alto Networks® y SD-WAN. En este caso, no tiene zonas para asignar; le recomendamos que utilice las zonas predefinidas en sus políticas de PAN-OS y User-ID para simplificar la implementación.

Antes de comenzar a configurar la implementación de SD-WAN, para ambos casos de uso, creará las zonas predefinidas necesarias en Panorama denominadas **`zone-internet`**, **`zone-internal`**, **`zone-to-hub`**, **`zone-to-branch`** y **`zone-to-pa-hub`**. Cuando incorpore los cortafuegos de su sucursal y hub, Adición de dispositivos de SD-WAN a Panorama. Para clientes preexistentes, el complemento de SD-WAN asignará internamente zonas preexistentes a estas zonas predefinidas al ejecutar reglas de políticas de SD-WAN, reglas de políticas de QoS, protección de zona, User-ID y protección de búfer de paquetes, y utilizará las zonas predefinidas para la creación de logs de zonas y la visibilidad en Panorama. Los nuevos clientes estarán configurados correctamente mediante las zonas predefinidas.

Las zonas predefinidas también son necesarias para configurar automáticamente túneles VPN entre sus hubs y sucursales de SD-WAN cuando transfiera la configuración de Panorama a sus dispositivos de SD-WAN gestionados.

Los nombres de zona distinguen entre mayúsculas y minúsculas y deben coincidir con los nombres proporcionados en este procedimiento. Se produce un error en la confirmación en el cortafuegos si los nombres de zona no coinciden con los descritos en este procedimiento.

En este ejemplo, estamos creando la zona denominada **`Zona a Internet`** .

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

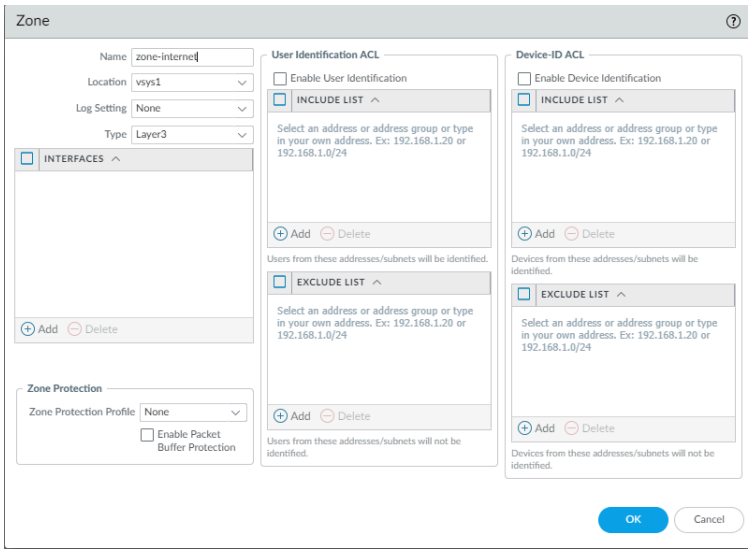
STEP 2 | Seleccione **Red** > **Zonas** y el cuadro desplegable contextual **Plantilla**, elija la plantilla de red creada anteriormente.

STEP 3 | **Añada** una nueva zona.

STEP 4 | Especifique **`Zona a Internet`**, por ejemplo, como el **nombre** de la zona.

STEP 5 | Para el **Type (Tipo)** de zona, seleccione **Layer3 (Capa3)**.

STEP 6 | Haga clic en **OK (Aceptar)**.



STEP 7 | Repita los pasos anteriores para crear las zonas restantes. En total, debe crear las siguientes zonas:

- **`Zona a sucursal`**
- **`Zona a hub`**
- **`Zona a interno`**
- **`Zona a Internet`**
- **`Zona a pa hub`**

STEP 8 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

STEP 9 | **Commit (Confirmar)** los cambios.

Creación de grupos de dispositivos de SD-WAN

Cree grupos de dispositivos, uno para sus centrales y otro para sus sucursales, que contenga todas las reglas de políticas y objetos de configuración para sus centrales y sucursales de SD-WAN. Después de crear los grupos de dispositivos para sus centrales y sucursales, debe crear una regla de la política de seguridad en cada grupo de dispositivos que permita el tráfico entre las zonas de la sucursal y de la central. La creación de estas reglas de la política de seguridad garantiza que se permita el tráfico entre las zonas de dispositivos de SD-WAN cuando el complemento de SD-WAN cree los túneles VPN después de crear un clúster de VPN.

Establezca configuraciones idénticas en los cortafuegos de la central y de la central. Esto reducirá en gran medida la sobrecarga operativa que supone tener que gestionar las configuraciones de varias centrales y sucursales de SD-WAN, y le permitirá solucionar problemas, aislar y actualizar problemas de configuración mucho más rápidamente.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Creación de zonas predefinidas en Panorama.

STEP 3 | Cree el grupo de dispositivos de la central de SD-WAN.

1. Seleccione **Panorama** > **Grupos de dispositivos** y **añada** un grupo de dispositivos.
2. Especifique **`SD-WAN_Hub`** como **nombre** en el grupo de dispositivos.
3. (Opcional) Introduzca una **Description (Descripción)** para la plantilla.
4. En la sección **Dispositivos**, active las casillas de verificación para asignar las centrales de SD-WAN al grupo.
5. Para el **grupo de dispositivos principal**, seleccione **Compartido**.
6. Haga clic en **OK (Aceptar)**.

STEP 4 | Cree el grupo de dispositivos de la sucursal de SD-WAN.

1. Seleccione **Panorama** > **Grupos de dispositivos** y **añada** un grupo de dispositivos.
2. Especifique **`SD-WAN_Branch`** como **nombre** en el grupo de dispositivos.
3. (Opcional) Introduzca una **Description (Descripción)** para la plantilla.
4. En la sección **Dispositivos**, active las casillas de verificación para asignar las sucursales de SD-WAN al grupo.
5. Para el **grupo de dispositivos principal**, seleccione **Compartido**.
6. Haga clic en **OK (Aceptar)**.

STEP 5 | Cree una regla de la política de seguridad para controlar los flujos de tráfico de las sucursales a la zona interna de la central y de la zona interna de la central a las sucursales.

1. Seleccione **Políticas** > **Seguridad** y en el menú desplegable contextual **Grupo de dispositivos**, seleccione el grupo de dispositivos **SD-WAN_Hub**.
2. **Añada** una nueva regla de políticas.
3. Especifique un **nombre** para la regla de políticas, como **`SD-WAN access--hub DG`**.
4. Seleccione **Origen** > **Zona de origen** y **añada** la **Zona a interno** y la **Zona a sucursal**.
5. Seleccione **Destino** > **Zona de destino** y **añada** la **Zona a interno** y la **Zona a sucursal**.
6. Seleccione **Aplicación** y **añada** aplicaciones que permitir.

   Debe permitir BGP si utiliza el enrutamiento de BGP.
7. Seleccione **Acciones** y **Permitir** para permitir las aplicaciones que seleccionó.
8. Seleccione **Objetivo** y especifique los dispositivos de destino a los que Panorama™ debe enviar esta regla.

STEP 6 | Cree una regla de la política de seguridad para controlar el tráfico que se origina desde la zona interna de las sucursales hacia la central y desde la central hasta la zona interna de las sucursales.

1. Seleccione **Políticas** > **Seguridad** y en el menú desplegable contextual **Grupo de dispositivos**, seleccione el grupo de dispositivos **SD-WAN_Branch**.
2. **Añada** una nueva regla de políticas.
3. Especifique un **nombre** para la regla de políticas, como **`SD-WAN access--branch DG`**.
4. Seleccione **Origen** > **Zona de origen** y **añada** la **Zona a interno** y la **Zona a central**.
5. Seleccione **Destino** > **Zona de destino** y **añada** la **Zona a interno** y la **Zona a central**.
6. Seleccione **Aplicación** y **añada** aplicaciones que permitir.

   Debe permitir BGP si utiliza el enrutamiento de BGP.
7. Seleccione **Acciones** y **Permitir** para permitir las aplicaciones que seleccionó.
8. Seleccione **Objetivo** y especifique los dispositivos de destino a los que Panorama debe enviar esta regla.

STEP 7 | Confirme y envíe su configuración.

1. Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.
2. En la sección Ámbito de envío, haga clic en **Editar selecciones**.
3. Habilite (active) **Incluir plantillas de dispositivo y red** y haga clic en **Aceptar**.
4. **Confirme y envíe** sus cambios de configuración.

   *Existen dos operaciones de confirmación que se realizan automáticamente cuando confirma y envía el grupo de dispositivos y la configuración de la plantilla. Compruebe las **tareas** para verificar que la segunda confirmación sea correcta. De estas dos operaciones de confirmación, la primera siempre falla.*

Creación de una etiqueta de enlace

Cree una etiqueta de enlace para identificar uno o más enlaces físicos que desee que las aplicaciones y servicios utilicen en un orden específico durante la distribución del tráfico de SD-WAN y la protección contra conmutación por error. La agrupación de varios enlaces físicos le permite maximizar la calidad de la aplicación y el servicio si el estado del enlace físico se deteriora.

Cuando planifique cómo agrupar sus enlaces, considere el uso o el fin de los enlaces y agrúpelos en consecuencia. Por ejemplo, si está configurando enlaces destinados a tráfico de bajo coste o no crítico para la empresa, cree una etiqueta de enlace y agrupe estas interfaces para garantizar que el tráfico previsto fluya principalmente en esos enlaces y no en enlaces más caros que puedan impactar en aplicaciones o servicios críticos para la empresa.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Objetos** > **Etiquetas** y seleccione el grupo de dispositivos del menú desplegable contextual **Grupo de dispositivos**.

STEP 3 | **Añada** una nueva etiqueta.

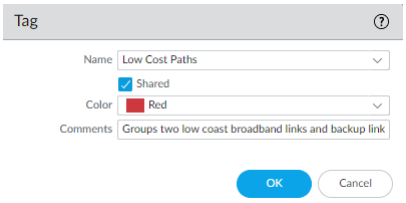
STEP 4 | Introduzca un nombre descriptivo en **Nombre** para la etiqueta. Por ejemplo; Rutas de bajo coste, Rutas costosas, Acceso general, Sede privada o Respaldo.

STEP 5 | Habilite (marque) **Shared (Compartido)** para que la etiqueta de vínculo esté disponible para todos los grupos de dispositivos en el servidor de gestión Panorama™ y para los sistemas virtuales múltiples predeterminados en una sola central o sucursal de los sistemas virtuales múltiples, o para vsys1 en cualquier central o sucursal de varios sistemas virtuales múltiples al cual se realizan envíos.

Al configurar una etiqueta de enlace compartida, Panorama puede hacer referencia a las etiquetas de enlace en la validación de la configuración del cortafuegos y confirmar y enviar con éxito la configuración a sucursales y centrales. La confirmación falla si Panorama no puede hacer referencia a una etiqueta de enlace.

STEP 6 | (Opcional) Seleccione un **color** para la etiqueta.

STEP 7 | Especifique **comentarios** útiles sobre la etiqueta. Por ejemplo, **`Agrupar dos enlaces de banda ancha de bajo coste y un enlace de respaldo para el acceso general a Internet.`**



STEP 8 | Haga clic en **Aceptar** para guardar los cambios.

STEP 9 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

STEP 10 | Configuración de un perfil de la interfaz de SD-WAN.

Configuración de un perfil de la interfaz de SD-WAN

Cree un perfil de interfaz de SD-WAN para definir las características de las conexiones ISP y para especificar la velocidad de los enlaces y con qué frecuencia el cortafuegos supervisa el enlace, y especifique una etiqueta de enlace para el enlace. Cuando especifique la misma etiqueta de enlace en varios enlaces, agrupa (empaqueta) esos enlaces físicos en un paquete de enlaces o una tubería gruesa. Debe configurar un perfil de interfaz de SD-WAN y especificarlo para una interfaz Ethernet compatible con SD-WAN para poder guardar la interfaz Ethernet.

Agrupe los enlaces según un criterio común. Por ejemplo, agrupe enlaces por preferencia de ruta de más preferido a menos preferido, o agrupe enlaces por coste.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Red** > **Perfiles de red** > **Perfil de la interfaz de SD-WAN** y seleccione la plantilla adecuada en el menú desplegable contextual **Plantilla**.

STEP 3 | **Añada** un perfil de la interfaz de SD-WAN.

STEP 4 | Introduzca un **nombre** sencillo para el perfil de interfaz de SD-WAN, que será el que verá en los informes, la solución de problemas y la estadísticas.

STEP 5 | Seleccione la **ubicación** del sistema virtual si tiene un servidor de gestión Panorama ™ de sistemas virtuales múltiples. De forma predeterminada, se selecciona vsys1.

STEP 6 | Seleccione la **etiqueta de enlace** que este perfil asignará a la interfaz.

STEP 7 | Añada una **descripción** para el perfil.

STEP 8 | Seleccione el **Link Type (Tipo de enlace)** físico de la lista predefinida (**ADSL/DSL**, **Cable modem (Cable módem)**, **Ethernet**, **Fiber (Fibra)**, **LTE/3G/4G/5G**, **MPLS**, **Microwave/Radio (Microondas/Radio)**, **Satellite (Satélite)**, **WiFi**, **Private Link1 (Enlace privado1)**, **Private Link2 (Enlace privado2)**, **Private Link3 (Enlace privado3)**, **Private Link4 (Enlace privado4)**, u **Other (Otros)**). Con PAN-OS 11.1.3, el complemento SD-WAN 3.2.1 y las versiones posteriores admiten los tipos adicionales de enlaces privados punto a punto como **Private Link1 (Enlace privado1)**, **Private Link2 (Enlace privado2)**, **Private Link3 (Enlace privado3)y** Private Link4 (Enlace privado4)**.** No admitimos tráfico de texto sin formato desde el cortafuegos de sucursal SD-WAN al cortafuegos de hub SD-WAN para los tipos de enlaces **Private Link1 (Enlace privado1)**, **Private Link2 (Enlace privado2)**, **Private Link3 (Enlace privado3)** y **Private Link4 (Enlace privado4)**. Cuando configure cualquiera de los nuevos tipos de enlaces privados, asegúrese de tener una regla de políticas SD-WAN en el hub que esté configurado solo con el tipo de enlace público. Porque cuando el tráfico que va a Internet retrocede o falla al hub desde la sucursal, debe coincidir con esta regla de políticas SD-WAN. De lo contrario, el tráfico se pierde ya que estos enlaces privados (**Private Link1 [Enlace privado1]**,

Private Link2 [Enlace privado2], **Private Link3 [Enlace privado3]** y **Private Link4 [Enlace privado4]**) forman parte de la interfaz SD-WAN de acceso directo a Internet (DIA).

(Para PAN-OS 11.1.3 y versiones posteriores, complemento SD-WAN 3.2.1 y versiones posteriores) Para habilitar los tipos de enlaces privados punto a punto adicionales, debe asegurarse de lo siguiente:

- *El Servidor de gestión de Panorama debería ejecutarse en PAN-OS 11.1.3*
- *Los dispositivos gestionados por Panorama deben ejecutarse en PAN-OS 11.1.3*
- *La versión del complemento SD-WAN debe ser 3.2.1*

(Para PAN-OS 11.2.0 y versiones posteriores, complemento SD-WAN 3.3.0 y versiones posteriores) Para habilitar los tipos de enlaces privados punto a punto adicionales, debe asegurarse de lo siguiente:

- *El servidor de gestión de Panorama debería ejecutarse en PAN-OS 11.2.0*
- *Los dispositivos gestionados por Panorama deben ejecutarse en PAN-OS 11.2.0*
- *La versión del complemento SD-WAN debe ser 3.3.0*

El cortafuegos puede admitir cualquier dispositivo CPE que finalice y se transfiera como una conexión Ethernet al cortafuegos; por ejemplo, los puntos de acceso WiFi, los módems LTE y el CPE láser/microondas pueden terminar con una transferencia de Ethernet.

Los siguientes tipos de enlaces formarán túneles con solo el mismo tipo de enlace:

- *Tipos de enlaces públicos (u **Ohter (Otros)**): **Ethernet**, **ASDL/DSL**, **Cable modem (Cable módem)**, **Fiber (Fibra)**, **LTE/3G/4G/5G**, **WiFi** y **Other (Otros)**.*

  Cualquier tipo de enlace público a cualquier otro tipo de enlace público creará un túnel de forma correcta. Por ejemplo, los tipos de enlace Ethernet-to-Other y Other-to-Other crearán los túneles correctamente.
- *Tipos de enlaces privados y punto a punto: **MPLS**, **Satellite (Satélite)**, **Private Link1 (Enlace privado1)**, **Private Link2 (Enlace privado2)**, **Private Link3 (Enlace privado3)**, **Private Link4 (Enlace privado4)** y **Microwave/Radio (Microondas/Radio)**.*

  Un tipo de enlace privado puede crear el túnel solo con el mismo tipo de enlace privado. Por ejemplo, los tipos de enlace MPLS a MPLS y satélite a satélite son válidos y, por lo tanto, los túneles se crearán correctamente, pero MPLS a satélite no creará el túnel.

Para las implementaciones de PAN-OS existentes que tienen zonas definidas en las interfaces que se utilizarán para admitir SD-WAN, Panorama puede configurar automáticamente el nombre de la zona de la interfaz en una de las zonas SD-WAN predefinidas bajo las siguientes condiciones:

1. *La interfaz SD-WAN se configura como un tipo de vínculo privado punto a punto (**MPLS**, **Satellite [Satélite]**, **Private Link1 [Enlace privado1]**, **Private Link2 [Enlace privado2]**, **Private Link3 [Enlace privado3]**, **Private Link4 [Enlace privado4]**, o **Microwave [Microondas]**) en su perfil de interfaz.*
2. *La casilla de verificación **VPN Data Tunnel Support (Compatibilidad con túnel de datos VPN)** está deshabilitada (sin marcar) en el perfil de interfaz SD-WAN. Esto le indica a PAN-OS que reenvíe el tráfico en texto no cifrado fuera del túnel SD-WAN VPN. Como los tipos de enlaces **Private Link1 (Enlace privado1)**, **Private Link2 (Enlace privado2)**, **Private Link3 (Enlace privado3)** y **Private Link4 (Enlace privado4)** no admiten tráfico de texto sin formato desde el cortafuegos de sucursal SD-WAN al cortafuegos de hub de SD-WAN, debe dejar habilitada la opción **VPN Data Tunnel Support (Compatibilidad de túnel de datos de VPN)** cuando configure estos tipos de enlaces privados.*

En el cortafuegos de hub, el nombre de la zona se configura como `zone-to-branch (zona a sucursal)` cuando se cumple la condición “a)”. En el cortafuegos de la sucursal, el nombre de la zona se configura como `zone-to-hub` cuando se cumplen las condiciones “a)” y “b)”. Panorama automatiza este paso para simplificar la configuración y garantizar una comunicación adecuada entre los cortafuegos de hub y sucursal. Si tiene políticas de cortafuegos preexistentes que hacen referencia al nombre de zona anterior, debe actualizar las políticas para que reflejen el nuevo nombre de zona SD-WAN predefinido.

STEP 9 | Especifique la velocidad de **descarga máxima (Mbps)** del ISP en megabits por segundo (el intervalo es de 0 a 100 000; no hay ningún valor predeterminado). Puede especificar un intervalo con hasta tres decimales, por ejemplo, 10,456. Solicítele a su ISP la velocidad del enlace o pruebe las velocidades máximas del enlace con una herramienta como speedtest.net y haga una media de los tiempos máximos durante un buen periodo.

STEP 10 | Especifique la velocidad de **carga máxima (Mbps)** en el ISP en megabits por segundo (el intervalo es de 0 a 100 000; no hay ningún valor predeterminado). Puede especificar un intervalo con hasta tres decimales, por ejemplo, 10,456. Solicítele a su ISP la velocidad del enlace o pruebe las velocidades máximas del enlace con una herramienta como speedtest.net y haga una media de los tiempos máximos durante un buen periodo.

STEP 11 | Seleccione **Eligible for Error Correction Profile interface selection (Elegible para la selección de la interfaz del perfil de corrección de errores)** para habilitar la corrección de errores de reenvío (FEC, Forward Error Correction) o la duplicación de paquetes para las interfaces. Debe habilitar esta opción en los cortafuegos de codificación y decodificación; también

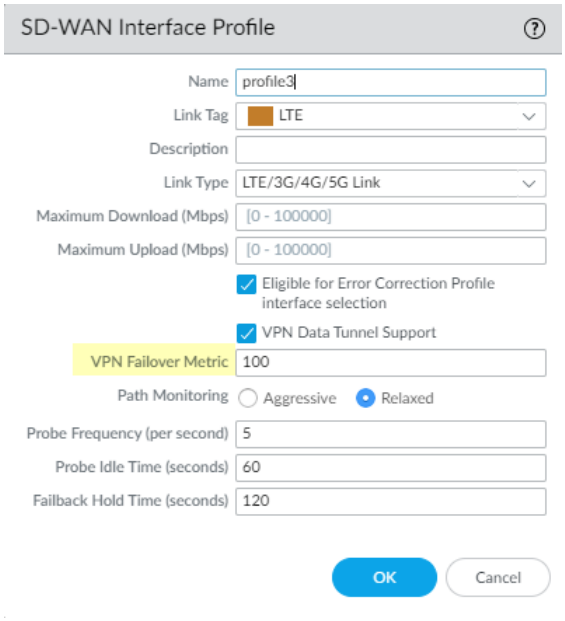
debe crear un perfil de corrección de errores que aplicar a la regla de políticas SD-WAN para aplicaciones específicas.

STEP 12 | La **compatibilidad del túnel de datos VPN** determina si el tráfico de la sucursal al hub y el tráfico de retorno fluyen a través de un túnel VPN para mayor seguridad (el método predeterminado) o fluye fuera del túnel VPN para evitar la sobrecarga de cifrado.

- Deje la opción **Compatibilidad del túnel de datos VPN** habilitada para los tipos de enlaces públicos que tienen conexiones directas a Internet o capacidad de conexión a Internet, como módem de cable, ADSL y otras conexiones a Internet.
- Puede desactivar **VPN Data Tunnel Support (Compatibilidad de túnel de datos de VPN)** para tipos de enlaces privados como MPLS, satélite o microondas que no tienen capacidad de conexión a Internet excepto los tipos de enlaces **Private Link1 (Enlace privado1)**, **Private Link2 (Enlace privado2)**, **Private Link3 (Enlace privado3)** y **Private Link4 (Enlace privado4)**. Sin embargo, primero debe asegurarse de que el tráfico no pueda interceptarse, porque se enviará fuera del túnel VPN.
- (Complemento SD-WAN 3.2.1 y versiones posteriores) dado que los tipos de enlace **Private Link1 (Enlace privado1)**, **Private Link2 (Enlace privado2)**, **Private Link3 (Enlace privado3)** y **Private Link4 (Enlace privado4)** no admiten el tráfico de texto sin formato desde el cortafuegos de sucursales de SD-WAN al cortafuegos del concentrador de SD-WAN, debe dejar **VPN Data Tunnel Support (Compatibilidad de túnel de datos de VPN)** habilitado al configurar estos tipos de vínculos privados.
- La sucursal puede tener tráfico de DIA que precise la conmutación por error en el enlace MPLS privado que se conecta al hub y que tenga que llegar a Internet desde el hub. La configuración **Compatibilidad del túnel de datos VPN** determina si los datos privados fluyen a través del túnel VPN o si fluyen fuera del túnel, y el tráfico fallido usa la otra conexión (que el flujo de datos privados no usa). El cortafuegos usa zonas para segmentar el tráfico de conmutación por error de DIA del tráfico privado de MPLS.

STEP 13 | Si Configuración de AnyPath de DIA, una interfaz virtual principal puede disponer de distintas interfaces virtuales del hub, por lo que debe priorizar el orden de selección del hub para la conmutación por error. Configure la **métrica de conmutación por error de la VPN** para los túneles VPN incluidos en la interfaz virtual del hub donde se aplique este perfil para especificar la prioridad. Cuanto menor sea la métrica, mayor será la prioridad de la interfaz

que se seleccionará durante la conmutación por error. Si hay varias interfaces virtuales del hub que tienen la misma métrica, SD-WAN envía tráfico de sesión nuevo a ellas por turnos.



STEP 14 | (Opcional) Seleccione el modo **Supervisión de rutas** en el que el cortafuegos supervisa las interfaces donde aplica ese perfil de interfaz de SD-WAN.

*El cortafuegos selecciona el que considera el mejor método de supervisión basado en **Tipo de enlace**. Conserve la configuración predeterminada para el tipo de enlace a no ser que una interfaz (donde aplique este perfil) tenga problemas que requieran una supervisión de rutas más agresiva o más relajada.*

- **Agresiva**: (valor predeterminado para todos los tipos de enlace excepto LTE y satélite) El cortafuegos envía paquetes de sonda al extremo opuesto del enlace de SD-WAN a una frecuencia constante. Utilice este modo si necesita una detección rápida y una conmutación por error para condiciones de caída de tensión y apagón.
- **Relajada**: (valor predeterminado para los tipos de enlace LTE y satélite) El cortafuegos espera varios segundos (el **tiempo de inactividad de la sonda**) entre los conjuntos de envío de los paquetes de sonda, lo que hace que la supervisión de la ruta sea menos frecuente. Cuando se agota el tiempo de inactividad de la sonda, el cortafuegos envía sondas durante siete segundos a la **frecuencia de la sonda** configurada. Utilice este modo cuando tenga enlaces de ancho de banda bajo, enlaces de pago por uso (como LTE) o cuando la detección rápida no sea tan importante como conservar el coste y el ancho de banda.

STEP 15 | Configure la **frecuencia de sonda (por segundo)**, que es la cantidad de veces por segundo que el cortafuegos envía un paquete de sonda al extremo opuesto del enlace de SD-WAN (el intervalo es de 1 a 5; el valor predeterminado es 5). La configuración predeterminada proporciona detección subsecundaria de caídas de tensión y apagones.

*Si cambia la frecuencia de la sonda para una plantilla de Panorama, también debe ajustar el umbral de porcentaje de **Pérdida de paquetes** en un perfil de Calidad de ruta para un grupo de dispositivos de Panorama.*

STEP 16 | Si selecciona la supervisión de ruta **Relajada**, puedes establecer el **tiempo de inactividad de la sonda (segundos)** que el cortafuegos espera entre conjuntos de paquetes de sonda (el rango es de 1 a 60; el valor predeterminado es 60).

STEP 17 | Introduzca el **tiempo de retención de recuperación de fallos (segundos)** que el cortafuegos espera a que un enlace recuperado siga siendo apto antes de que el cortafuegos restablezca ese enlace como el enlace preferido después de que se haya realizado la conmutación por error (el intervalo es de 20 a 120; el valor predeterminado es 120).

STEP 18 | Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 19 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

STEP 20 | Supervise las métricas de estado de la ruta de la aplicación y el enlace, y genere informes de su aplicación y el rendimiento del estado del enlace. Para obtener más información, consulte Supervisión y creación de informes.

Configuración de una interfaz Ethernet física para SD-WAN

En Panorama™, configure una interfaz Ethernet de Capa 3 física y habilite la funcionalidad de SD-WAN. Para configurar una interfaz física, debe asignarle una dirección IPv4 o IPv6, o ambas. También debe asignar a la interfaz una puerta de enlace de siguiente salto completamente cualificada y asignar un perfil de interfaz SD-WAN a la interfaz. (SD-WAN solo admite un tipo de interfaz de Capa 3; no admite redes de Capa 2, como VPLS).

Después de usar Panorama para crear un clúster de VPN y exportar la información de su hub y sucursal en el CSV, una configuración de VPN automática en el complemento de SD-WAN utiliza esa información para generar una configuración para las sucursales y hubs asociadas que incluye las zonas de SD-WAN predefinidas y crea túneles VPN seguros entre las sucursales y hubs de SD-WAN. La configuración de VPN automática también genera la configuración de BGP si especifica la información de BGP en el CSV o en Panorama cuando añada una sucursal o hub de SD-WAN.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Network (Red)** > **Interfaces** > **Ethernet**, seleccione la plantilla adecuada en el menú desplegable de contexto **Template (Plantilla)**, seleccione un número de ranura, como Ranura1, y seleccione una interfaz (como por ejemplo, ethernet1/1).

STEP 3 | Seleccione **Tipo de interfaz** como **Capa 3** .

STEP 4 | En la pestaña **Config (Configuración)**, para un motor de enrutamiento heredado, seleccione un **Virtual router (Enrutador virtual)** o cree un nuevo enrutador virtual. Para el motor de enrutamiento avanzado, seleccione un **enrutador lógico** o cree un nuevo.

STEP 5 | Asigne la **zona de seguridad** adecuada para la interfaz que está configurando.

Por ejemplo, si crea un enlace de subida en un ISP, debe saber que la interfaz Ethernet que elija se va a dirigir a una zona no fiable.

STEP 6 | Para habilitar SD-WAN en una interfaz IPv4, seleccione la pestaña **IPv4** y **Enable SD-WAN (Habilitar SD-WAN)**.

Con el complemento SD-WAN 3.2.0 y versiones posteriores, puede configurar hasta cuatro direcciones IP para una interfaz habilitada para SD-WAN. El complemento SD-WAN utiliza solo la primera dirección IP de la lista de direcciones IP configurada para crear el túnel SD-WAN.

La SD-WAN considera solo la primera dirección **IP** para la **Next Hop Gateway (Puerta de enlace de siguiente salto)** e ignora las direcciones **IP** restantes de la lista.

(Solo implementaciones HA) Si desea cambiar de la versión 3.2.0 del complemento SD-WAN a la 3.1.0 o anterior, elimine las configuraciones activas/pasivas de HA en ambos cortafuegos antes de intentar un procedimiento de actualización, como la actualización de las versiones del complemento PAN-OS y SD-WAN.

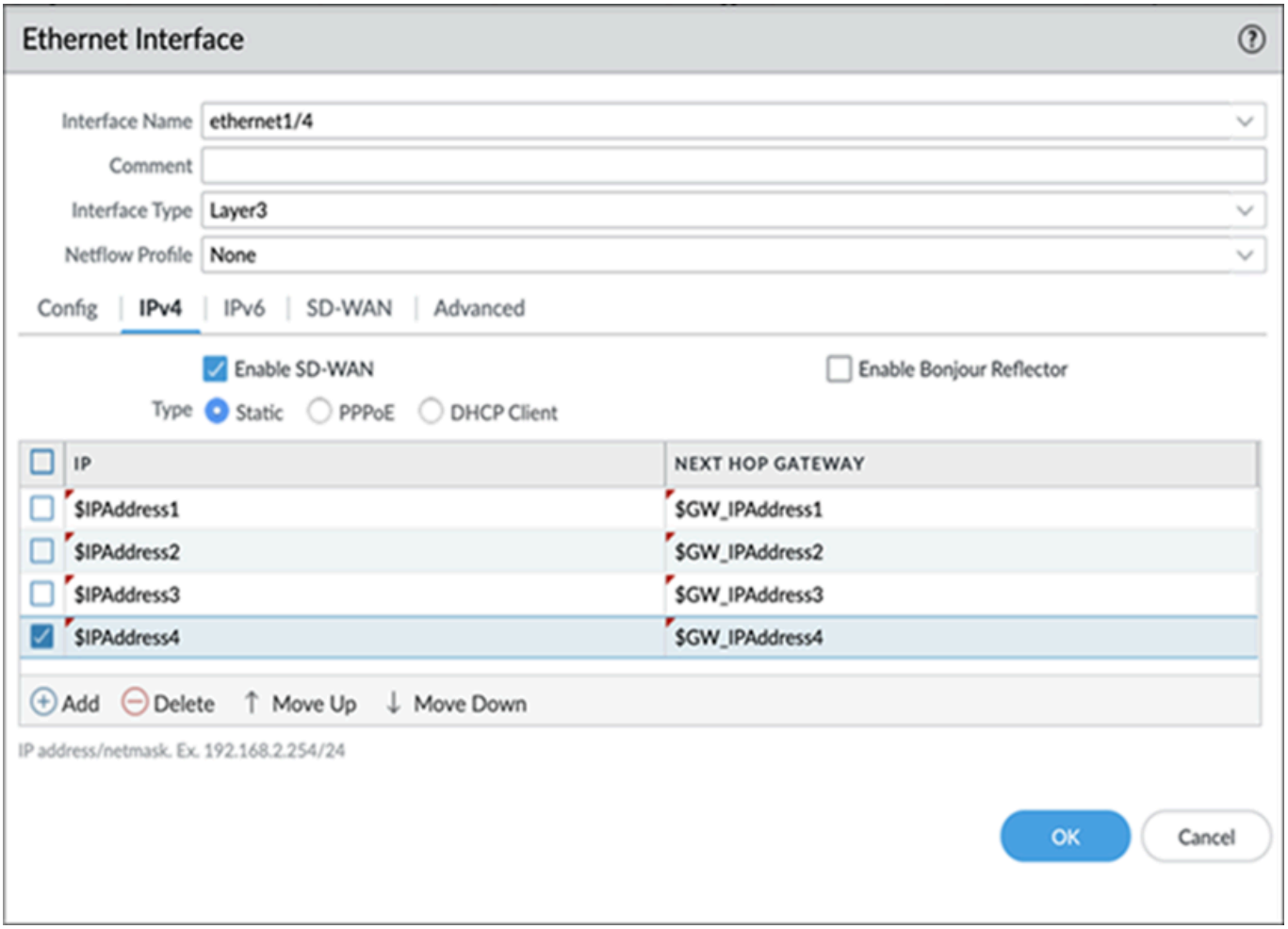
STEP 7 | Para una interfaz IPv4, seleccione **Type (Tipo)** de dirección:

- **Estática**: en el campo **IP**, **añada** una dirección IPv4 y una longitud de prefijo para la interfaz. Puede usar una variable definida, como $uplink, con un intervalo de direcciones. Especifique la dirección IPv4 completamente calificada de **Puerta de enlace de siguiente salto** (el siguiente salto de la dirección IPv4 que acaba de ingresar). La puerta de enlace de siguiente salto debe estar en la misma subred que la dirección IPv4. La puerta de enlace de siguiente salto es la dirección IP del enrutador predeterminado del ISP que este le proporcionó cuando adquirió el servicio. Es la dirección IP del siguiente salto a la que el cortafuegos envía tráfico para llegar a la red del ISP y, en última instancia, a Internet y al hub.
- **PPPoE**: **habilite la** autenticación PPPoE para enlaces DSL, especifique el **nombre de usuario** y la **contraseña** y **confirme la contraseña**.
- **DHCP Client (Cliente DHCP)**: es fundamental que DHCP asigna una puerta de enlace predeterminada, a la que también se le conoce como "puerta de enlace" de siguiente salto

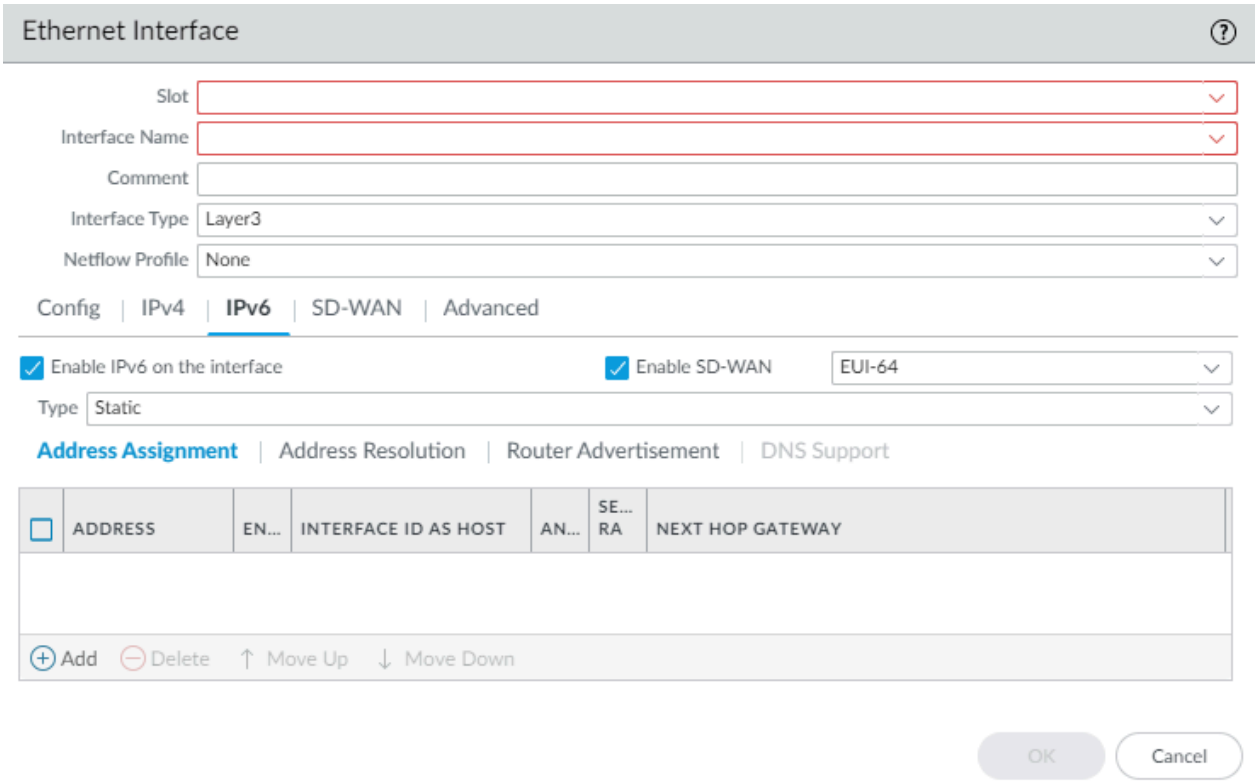
para la conexión de ISP. El ISP proporcionará toda la información de conectividad necesaria, como la dirección IP dinámica, los servidores DNS y la puerta de enlace predeterminada.

*Aunque el cliente DHCP es compatible con una interfaz de hub o sucursal, en una interfaz de hub es preferible que asigne una dirección **Static (Estática)** en lugar de un cliente DHCP. El uso de DHCP en un hub requiere el servicio DDNS de Palo Alto Networks. El uso de una dirección estática en el sitio del hub crea un entorno más estable, porque DDNS no se involucra cuando se resuelve los cambios de dirección IP de DHCP y porque el servicio DDNS puede tardar unos minutos en registrar la nueva dirección IP cuando cambia. Si tiene varios sitios de sucursales conectados a un sitio de hub, tener estabilidad es fundamental para mantener la red en funcionamiento.*

*Si selecciona Cliente DHCP, asegúrese de que deshabilita la opción **Crear automáticamente ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor**, que se habilita de forma predeterminada.*



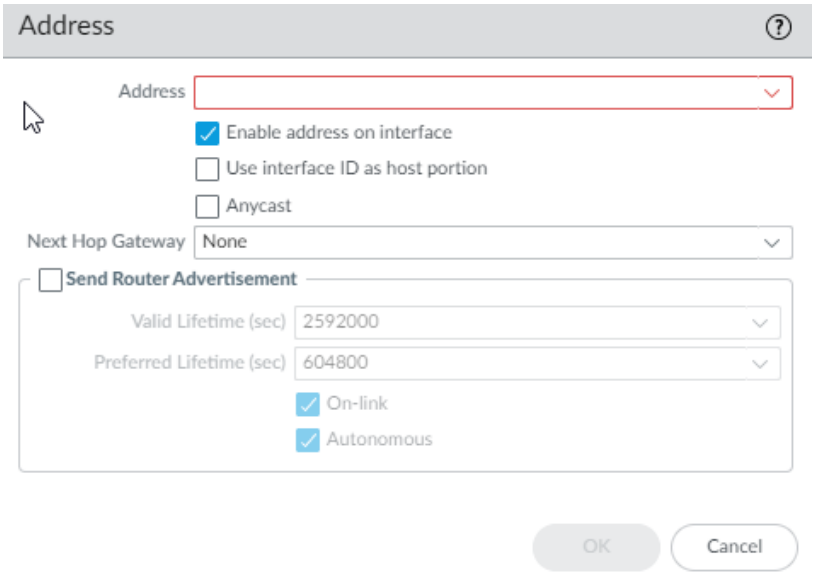
STEP 8 | Para habilitar SD-WAN en una interfaz IPv6, seleccione la pestaña **IPv6**, **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)** y **Enable SD-WAN (Habilitar SD-WAN)**.



STEP 9 | En el campo **EUI-64 (default 64-bit Extended Unique Identifier) [EUI-64 (Identificador único ampliado de 64 bits predeterminado)]**, introduzca el EUI de 64 bits en formato hexadecimal. Si deja este campo en blanco, el cortafuegos utilizará el EUI-64 generado desde la dirección MAC de la interfaz física. Si activa la opción **Use interface ID as host portion (Usar la ID de interfaz como parte de host)** cuando se añade una dirección, el cortafuegos utiliza el ID de interfaz como la parte de host de esa dirección.

STEP 10 | Para una interfaz IPv6, seleccione el **Type (Tipo)** de dirección como **Static (Estática)**. Seleccione la pestaña **Address Assignment (Asignación de direcciones)**.

1. Debe **Add (Añadir)** una **dirección** IPv6 para la interfaz o seleccionar **New Variable (Nueva variable)** para crear la variable. SD-WAN es compatible con una dirección IPv6 por interfaz física.
2. **Enable address on interface (Habilitar dirección en la interfaz)**.



3. **Use interface ID as host portion (Usar el ID de interfaz como parte del host)**: consulte el paso anterior para una explicación.
4. **Anycast (Difusión por proximidad)**: seleccione esta opción para convertir la dirección IPv6 (ruta) en una dirección Anycast (ruta), lo que significa que varias ubicaciones pueden anunciar el mismo prefijo, e IPv6 envía el tráfico anycast al nodo que considere más cercano, en función de los costes del protocolo de enrutamiento y otros factores.
5. **Next Hop Gateway (Puerta de enlace de siguiente salto)**: introduzca la dirección IPv6 de la puerta de enlace de siguiente salto (el siguiente salto desde la dirección IPv6 que introdujo). La puerta de enlace de siguiente salto debe estar en la misma subred que la dirección IPv6. La puerta de enlace de siguiente salto es la dirección IP del enrutador predeterminado del ISP que este le proporcionó cuando adquirió el servicio. Es la dirección IP de siguiente salto a la que el cortafuegos envía tráfico para llegar a la red del ISP, y en última instancia, a internet y al hub.
6. **Send Router Advertisement (Enviar anuncio de enrutador)**: seleccione para habilitar el cortafuegos para que envíe esta dirección en los anuncios del enrutador (RA), en cuyo caso también debe habilitar la opción global **Enable Router Advertisement (Habilitar anuncio de enrutador)** para la interfaz (en la pestaña **Router Advertisement (Anuncio de enrutador)**.
7. **Valid Lifetime (sec) [Duración válida (seg.)]**: Introduzca la duración válida (en segundos) que el cortafuegos considera que la dirección es válida. La duración válida debe ser igual o superar la **Preferred Lifetime (sec) [Duración preferida (seg.)]** (el valor predeterminado es 2 592 000).
8. **Preferred Lifetime (sec) [Duración preferida (en segundos)]**: introduzca el periodo de tiempo preferido (en segundos) durante el cual se prefiere la dirección válida, lo que

significa que el cortafuegos puede usarlo para enviar y recibir tráfico. Cuando caduca la duración preferida, el cortafuegos deja de poder utilizar la dirección para establecer nuevas conexiones, pero cualquier conexión existente es válida hasta que caduque la duración válida (el valor predeterminado es 604 800).

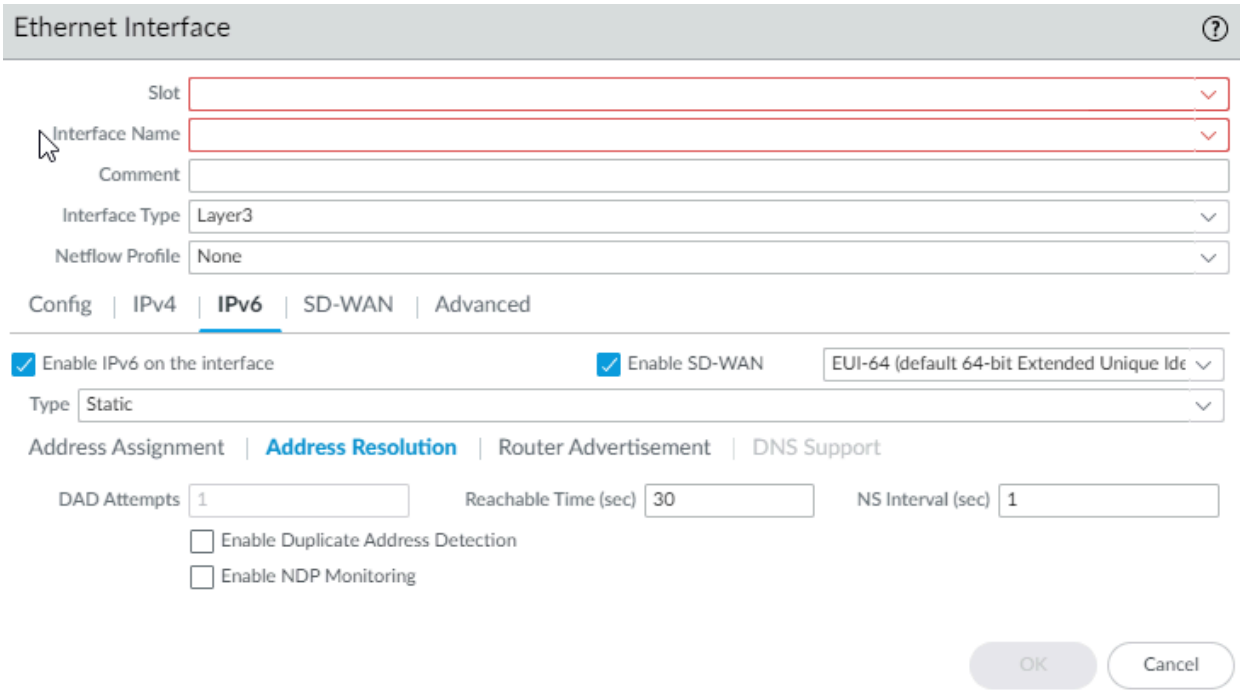
9. **On-link (Enlace activo)**: seleccione esta opción si se puede establecer comunicación con los sistemas con direcciones en el prefijo sin necesidad de un enrutador.
10. **Autonomous (Autónomo)**: seleccione esta opción si los sistemas pueden crear una dirección IP de forma independiente combinando el prefijo publicado con un ID de interfaz.
11. Haga clic en **OK (Aceptar)**.

STEP 11 | Para una interfaz IPv6 estática, configure la resolución de direcciones.

1. Seleccione **Address Resolution (Resolución de dirección)**.
2. Habilite **Duplicate Address Detection (Detección de direcciones duplicadas)** (DAD) si desea que se verifique la unicidad de una posible dirección IPv6 antes de que se asigne a la interfaz (habilitado de forma predeterminada).
3. Si seleccionó **Enable Duplicate Address Detection (Habilitar detección de direcciones duplicadas)**, especifique la cantidad de **DAD Attempts (Intentos de DAD)** dentro del intervalo de solicitud de vecinos (NS) antes de que falle el intento de identificar a los vecinos; el intervalo es de 1 a 10; el valor predeterminado es 1.
4. Ingrese el **Reachable Time (sec) (Tiempo alcanzable [s])**, la cantidad de tiempo que el cliente asume que un vecino es alcanzable después de recibir un mensaje de confirmación de accesibilidad; el intervalo es de 10 a 36 000; el valor predeterminado es 30.
5. Introduzca el **NS Interval (sec) [Intervalo NS (seg.)]** (intervalo de solicitud de vecino), el período de tiempo entre las solicitudes de vecinos; el rango es de 1 a 3600; el valor predeterminado es 1.
6. **Habilite la supervisión NDP** para habilitar la supervisión del protocolo de detección de vecinos. Cuando está habilitado, puede seleccionar el icono NDP en la columna Features [Funciones] y acceder a información como la dirección IPv6 de un vecino que

ha descubierto el cortafuegos, la dirección MAC correspondiente y el User-ID (en el mejor de los casos).

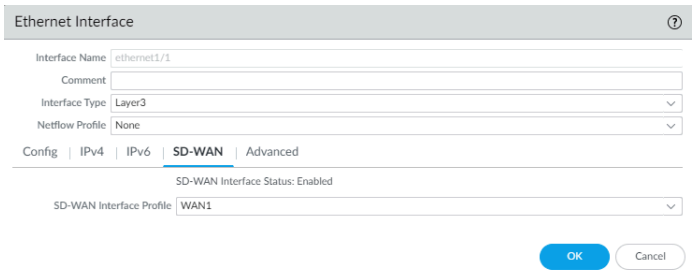
7. Haga clic en **OK (Aceptar)**.



STEP 12 | Si desea habilitar la interfaz para enviar anuncios de enrutador (RA) IPv6 y, opcionalmente, ajustar los parámetros de RA, configure el anuncio de enrutador como se documenta en la Guía del administrador de redes de PAN-OS, Configurar interfaces de Capa 3.

STEP 13 | En la pestaña **SD-WAN**, seleccione un **perfil de la interfaz de SD-WAN** que ya haya creado (o cree un nuevo perfil de la interfaz de SD-WAN) que aplicar a esta interfaz. El perfil de la interfaz de SD-WAN dispone de una etiqueta de enlace asociada, por lo que las interfaces en las que se aplica este perfil tendrán la etiqueta de enlace asociada. Una interfaz solo puede tener una etiqueta de enlace.

STEP 14 | Haga clic en **OK (Aceptar)** para guardar la interfaz de Ethernet.

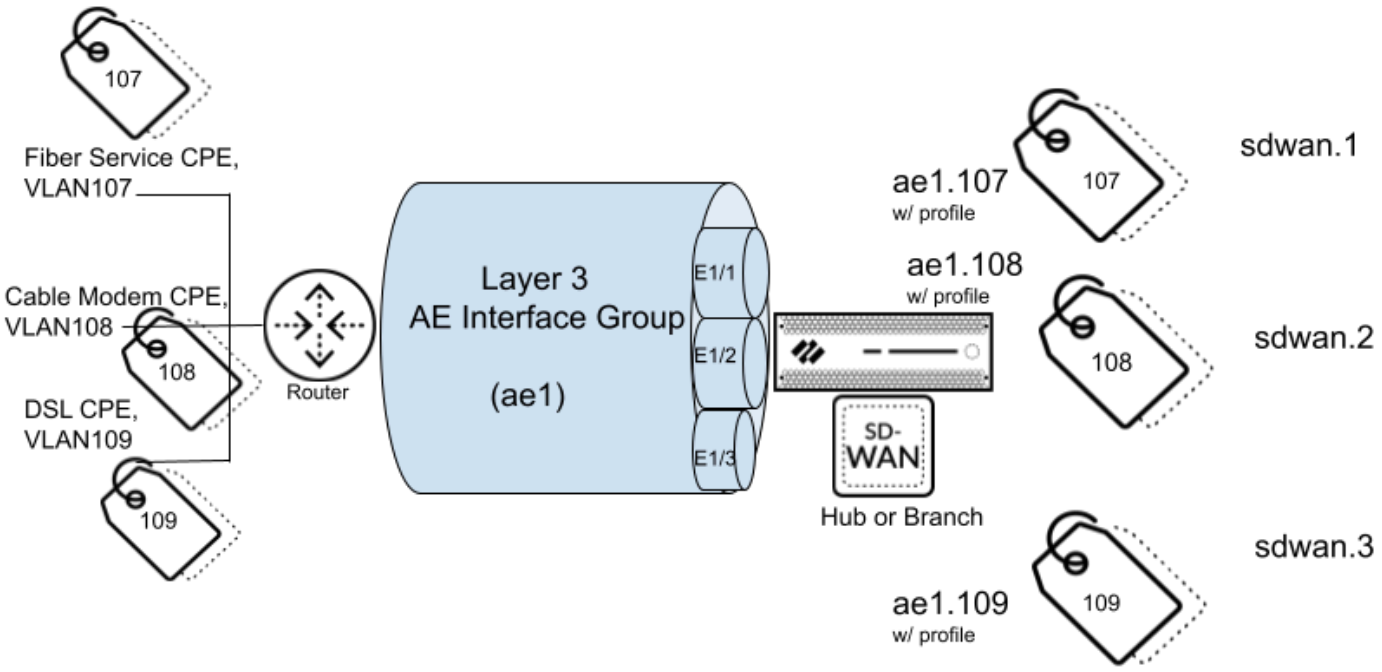


STEP 15 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

STEP 16 | (Solo configuración manual de SD-WAN) Configuración de una interfaz de SD-WAN virtual. La configuración de VPN automática realizará esta tarea si utiliza la VPN automática.

Configuración de una interfaz Ethernet de agregación subinterfaces para SD-WAN

Los cortafuegos físicos que ejecutan PAN-OS 11.0 y el complemento SD-WAN 2.1.0 admiten SD-WAN en interfaces de Ethernet de agregación (AE) para que un cortafuegos SD-WAN en un centro de datos, por ejemplo, pueda tener un grupo de interfaces de agregación (paquete) de interfaces de Ethernet físicas que proporcionan redundancia de enlace. SD-WAN admite interfaces AE con o sin subinterfaces. Puede crear una interfaz AE con subinterfaces que puede etiquetar para diferentes servicios ISP con el fin de proporcionar segmentación de tráfico de un extremo a otro. Por lo tanto, los servicios de su ISP pueden llegar a varios laboratorios o edificios sin necesidad de contar con un par de fibras dedicadas para cada conexión. Un grupo de interfaz AE de capa 3 se conecta a un enrutador, como se muestra en la siguiente figura:



Los cortafuegos VM-Series no admiten interfaces AE. Un cortafuegos de hub o sucursal de SD-WAN que tiene una interfaz AE no debe pertenecer al mismo clúster VPN que un cortafuegos de hub o de sucursal SD-WAN VM-Series porque las interfaces AE no son compatibles con los cortafuegos VM-Series.

No se admite PPPoE en subinterfaces.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Configuración de un perfil de la interfaz de SD-WAN para cada conexión ISP (subinterfaz) en el grupo de interfaces AE para definir sus atributos de enlace.

STEP 3 | Cree un grupo de interfaz AE.

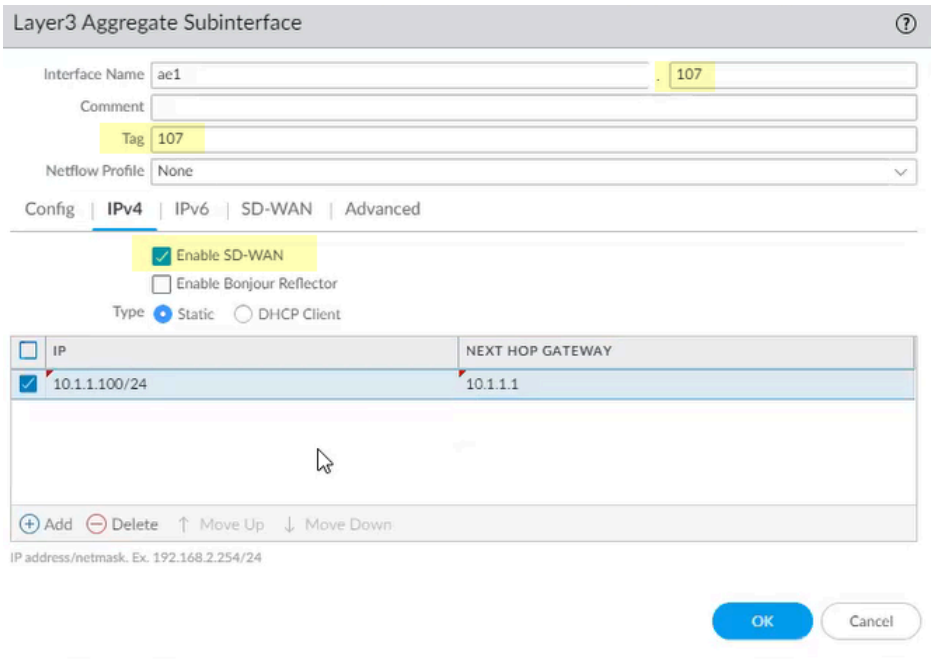
1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)**, seleccione una **plantilla** de Panorama y **agregue un grupo de agregación**.
2. En **Interface Name (Nombre de la interfaz)**, ingrese el número para identificar el grupo de agregación; el rango es de 1 a 16.
3. En **NAT Type (Tipo de NAT)**, seleccione **Layer3**.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | Asignar interfaces físicas al grupo de agregación.

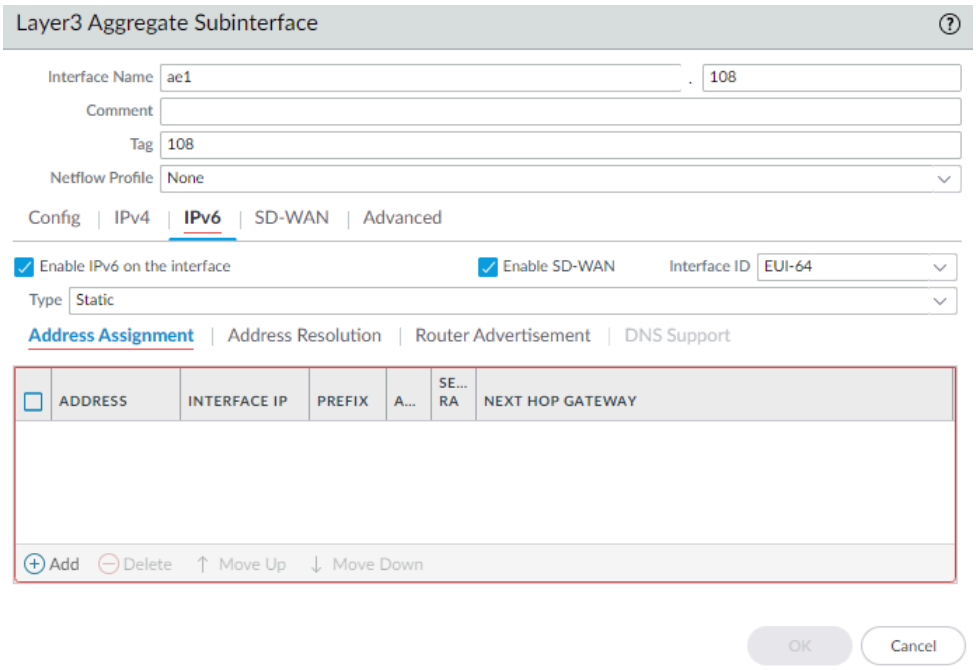
1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** y seleccione la interfaz que desea asignar al grupo de agregación.
2. Seleccione el **tipo de interfaz** como **Ethernet de agregación**.
3. Seleccione el **grupo de agregación** que creó, por ejemplo, ae1.
4. En la pestaña **Advanced (Avanzado)**, seleccione **Link Speed (Velocidad de enlace)**, **Link Duplex (Enlace dúplex)** y **Link State (Estado de enlace)**.
5. Haga clic en **OK (Aceptar)**.
6. Repita este paso para cada interfaz que desee asignar al grupo de agregación.

STEP 5 | Para el grupo de agregación, cree una subinterfaz que use una dirección IP estática.

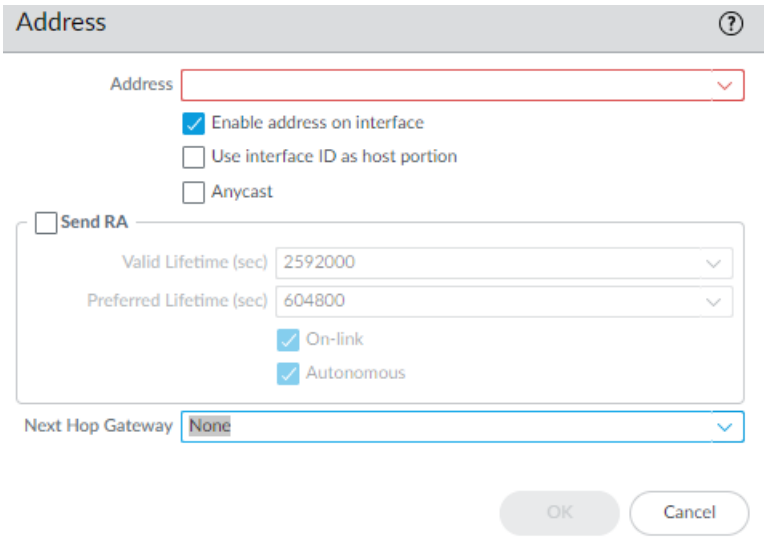
1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)**, resalte la interfaz de agregación, como ae1, y haga clic en **Add Subinterface (Agregar subinterfaz)** en la parte inferior de la pantalla.
2. En **Interface Name (Nombre de la interfaz)**, ingrese un número después del punto, como 107.
3. Ingrese la **etiqueta** VLAN para diferenciar entre las subinterfaces. Por comodidad, el número de la etiqueta debe ser el mismo que el ID de la subinterfaz.
4. Para configurar una dirección IPv4 estática para la subinterfaz, seleccione la pestaña **IPv4** y **Enable SD-WAN (Habilitar SD-WAN)**.



5. Seleccione el **tipo** de dirección: **Estática**.
6. **Agregue** la dirección **IP** (y la máscara de subred) de la subinterfaz.
7. Introduzca la dirección IP de la **puerta de enlace de salto siguiente**.
8. Para configurar una dirección IPv6 estática para la subinterfaz, seleccione la pestaña **IPv6**, **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)** y **Enable SD-WAN (Habilitar SD-WAN)**.



9. En el campo **EUI-64 (default 64-bit Extended Unique Identifier) [EUI-64 (Identificador único ampliado de 64 bits predeterminado)]**, introduzca el EUI de 64 bits en formato hexadecimal. Si deja este campo en blanco, el cortafuegos utilizará el EUI-64 generado desde la dirección MAC de la interfaz física. Si activa la opción **Use interface ID as host portion (Usar la ID de interfaz como parte de host)** cuando se añade una dirección, el cortafuegos utiliza el ID de interfaz como la parte de host de esa dirección.
10. Seleccione**Address Assignment (Asignación de direcciones)** y **Add (Añadir)** una **Address (Dirección)** IPv6 para la interfaz o seleccione **New Variable (Nueva variable)** para crear la variable.



11. **Use interface ID as host portion (Usar el ID de interfaz como parte del host)**; Consulte el paso secundario anterior para **EUI-64**.
12. Seleccione **Anycast (Difusión por proximidad)** para hacer que la dirección IPv6 (ruta) sea una dirección Anycast (ruta), lo que significa que varias ubicaciones pueden anunciar el

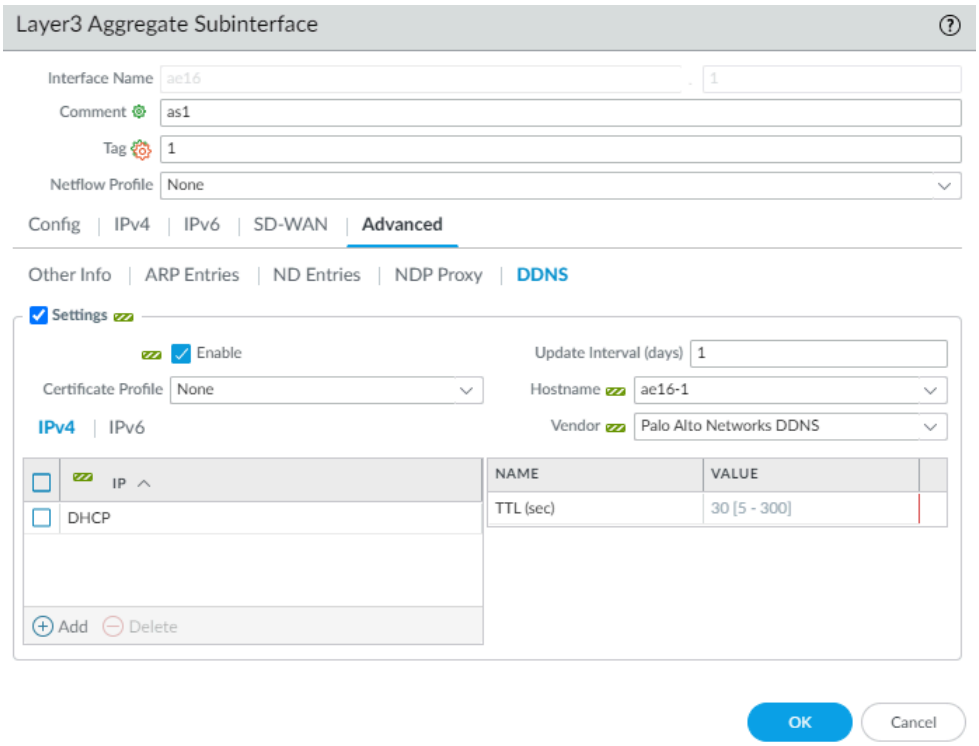
mismo prefijo, e IPv6 envía el tráfico Anycast al nodo que considere más cercano, en función de los costes del protocolo de enrutamiento y otros factores.

13. Introduzca la dirección IPv6 de la **Next Hop Gateway (Puerta de enlace de siguiente salto)** (el siguiente salto desde la dirección IPv6 que introdujo). La puerta de enlace de siguiente salto debe estar en la misma subred que la dirección IPv6. La puerta de enlace de siguiente salto es la dirección IP del enrutador predeterminado del ISP que este le proporcionó cuando adquirió el servicio. Es la dirección IP del siguiente salto a la que el cortafuegos envía tráfico para llegar a la red del ISP y, en última instancia, a Internet y al hub, o central.
14. Seleccione **Send Router Advertisement (Enviar anuncio de enrutador)** para habilitar el cortafuegos para que envíe esta dirección en los anuncios del enrutador (RA), en cuyo caso también debe habilitar la opción global **Enable Router Advertisement (Habilitar anuncio de enrutador)** para la interfaz (en la pestaña Anuncio de enrutador).
15. Introduzca el archivo **Valid Lifetime (sec) [Duración válida (seg.)]** en segundos que el cortafuegos considera que la dirección es válida. La duración válida debe ser igual o superar la **Preferred Lifetime (sec) [Duración preferida (seg.)]** (el valor predeterminado es 2 592 000).
16. Introduzca la **Preferred Lifetime (sec) [Duración preferida (seg.)]** (en segundos) durante el cual se prefiere la dirección válida, lo que significa que el cortafuegos la puede utilizar para enviar y recibir tráfico. Cuando caduca la duración preferida, el cortafuegos deja de poder utilizar la dirección para establecer nuevas conexiones, pero cualquier conexión existente es válida hasta que caduque la duración válida (el valor predeterminado es 604 800).
17. Seleccione **On-link (Enlace activo)**si se puede establecer comunicación con los sistemas con direcciones en el prefijo sin necesidad de un enrutador.
18. Seleccione **Autonomous (Autónomo)** si los sistemas pueden crear de forma independiente una dirección IP combinando el prefijo anunciado con el ID de interfaz.
19. Haga clic en **OK (Aceptar)**.

STEP 6 | Como alternativa a una dirección estática, para el grupo agregado, cree una subinterfaz que utilice DHCP para obtener su dirección.

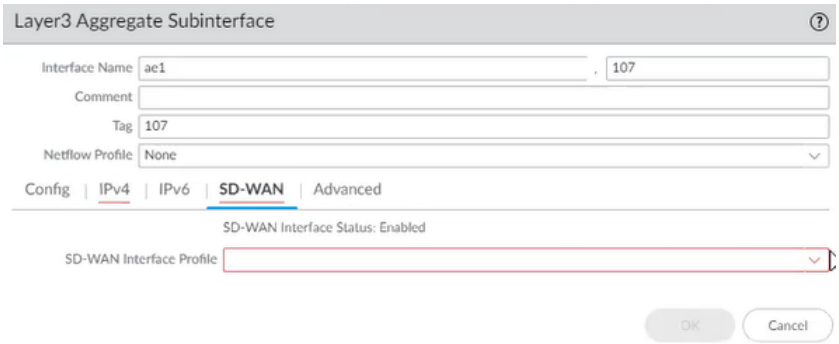
1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y, en el campo **Template (Plantilla)**, seleccione una pila de plantillas.
2. Resalte la interfaz de agregación, como ae1, y haga clic en **Add Subinterface (Agregar subinterfaz)** en la parte inferior de la pantalla.
3. Resalte la subinterfaz y haga clic en **Override (Cancelar)** en la parte inferior de la pantalla.
4. Resalte la subinterfaz y, para **Interface Name (Nombre de la interfaz)**, ingrese un número después del punto, como 1.
5. Ingrese la **etiqueta** VLAN para diferenciar entre las subinterfaces. Por comodidad, el número de la etiqueta debe ser el mismo que el ID de la subinterfaz.
6. Seleccione la pestaña **IPv4** y **habilite SD-WAN**.

   Una subinterfaz en un grupo de interfaces agregadas solo admite una dirección IPv4 como un cliente DHCP, no una dirección IPv6.
7. Seleccione el **tipo** de dirección: **Cliente DHCP**.
8. Seleccione **Enabled (Habilitado)**.
9. Anule la selección de **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)**.
10. Seleccione la pestaña **Advanced (Avanzado)** y la pestaña **DDNS**.
11. Seleccione **Settings (Configuración)** y **Enable (Habilitar)**. El complemento Panorama SD-WAN genera de forma automática el **nombre de host**.
12. Seleccione el **Vendor (proveedor)** como **Palo Alto Networks DDNS (DDNS de Palo Alto Networks)**.
13. Haga clic en **OK (Aceptar)**.



STEP 7 | Aplique un perfil de interfaz SD-WAN a la subinterfaz.

1. Resalte la subinterfaz que creó y seleccione la pestaña **SD-WAN**.
2. Seleccione el **perfil de interfaz SD-WAN** que creó para este enlace o cree un nuevo perfil.



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

STEP 8 | Repita los pasos anteriores para crear subinterfaces de capa 3 adicionales para el grupo de interfaces de agregación y aplique un perfil de interfaz SD-WAN a cada subinterfaz.

STEP 9 | Seleccione **Confirmar**.

Configuración de subinterfaces de capa 3 para SD-WAN

Los cortafuegos que ejecutan PAN-OS 11.0 y el complemento SD-WAN 2.1.0 admiten SD-WAN en subinterfaces de capa 3 para que el cortafuegos pueda segmentar el tráfico mediante etiquetas VLAN. En la siguiente tarea, se muestra cómo crear una subinterface de capa 3 en la que se utiliza una dirección IP estática y cómo crear una en la que se utiliza DHCP para obtener su dirección. Se muestra cómo asignar una etiqueta VLAN a la subinterfaz y habilitar SD-WAN en la subinterfaz. Cree un perfil de interfaz SD-WAN para definir cada conexión ISP y asigne el perfil a la subinterfaz correspondiente (una interfaz SD-WAN virtual).

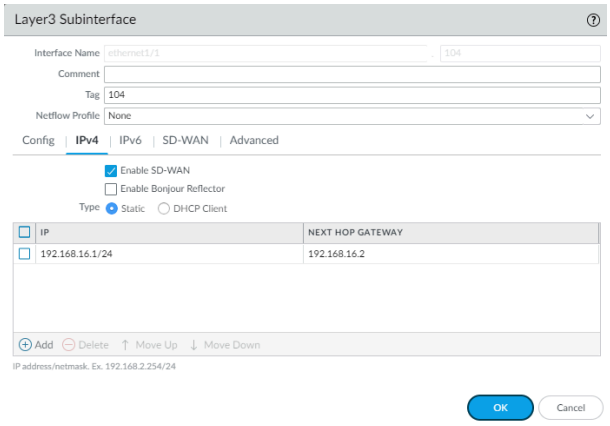
Si configura subinterfaces SD-WAN de capa 3 en cortafuegos VM-Series, la configuración de VMware debe tener grupos de puertos respectivos conectados a esas interfaces que permitan todas las VLAN.

No se admite PPPoE en subinterfaces.

STEP 1 | Configuración de un perfil de la interfaz de SD-WAN para cada conexión ISP (subinterface) para definir sus atributos de enlace.

STEP 2 | Cree una subinterfaz de Capa 3 en la que se utilice una dirección IPv4 estática.

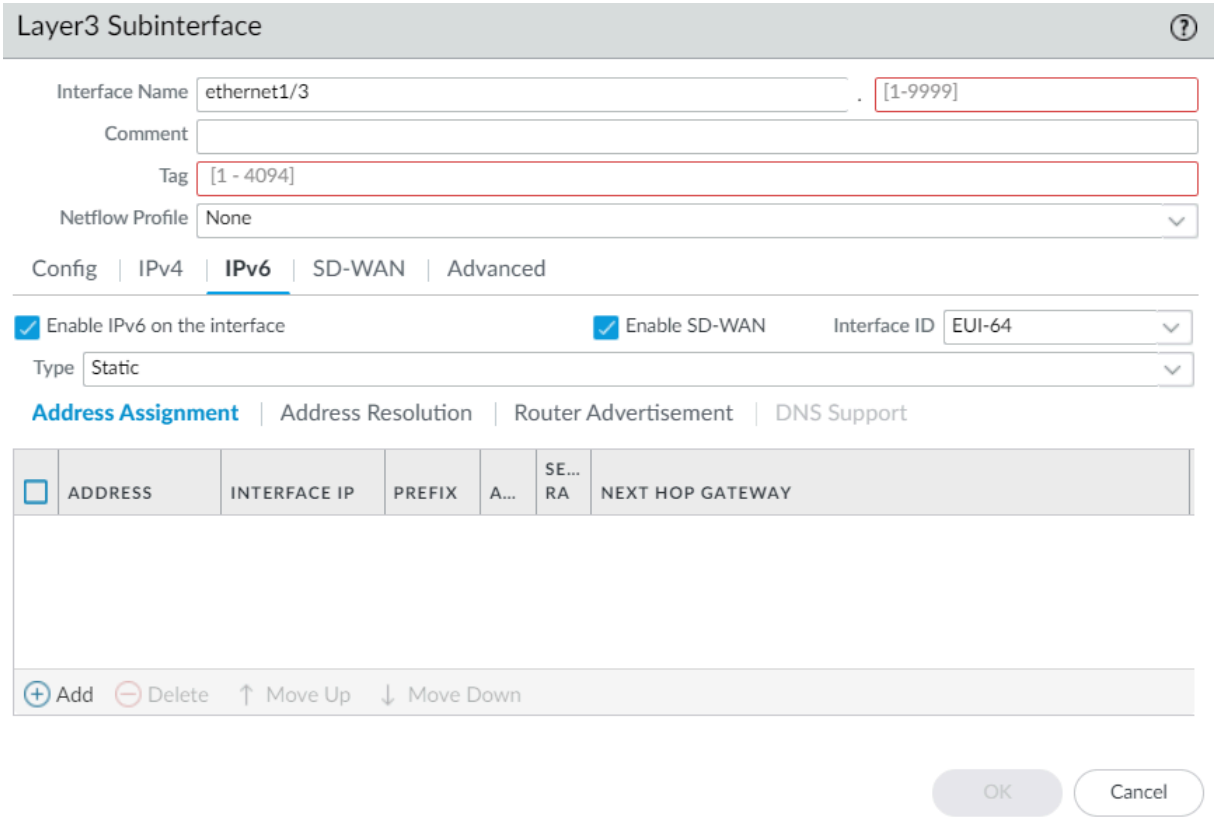
1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y, en el campo **Template (Plantilla)**, seleccione una plantilla.
2. Seleccione una interfaz.
3. En **Interface Type (Tipo de interfaz)**, seleccione **Layer 3 (Capa 3)** y haga clic en **OK (Aceptar)**.
4. Resalte la interfaz y haga clic en **Add Subinterface (Agregar subinterface)** en la parte inferior de la pantalla.
5. Después de **Interface Name (Nombre de la interfaz)** y el punto, introduzca el número de subinterfaz.
6. Introduzca una **etiqueta** para la subinterfaz (el rango es de 1 a 4.094). Por comodidad, el número de la etiqueta debe ser el mismo que el ID de la subinterfaz.
7. En la pestaña **IPv4**, seleccione la opción **Habilitar SD-WAN** .
8. Seleccione el **tipo** de dirección: **Estática**.
9. **Agregue** la dirección **IP** y la máscara de subred.
10. Introduzca la dirección IP de la **puerta de enlace de salto siguiente**.
11. Haga clic en **OK (Aceptar)**.



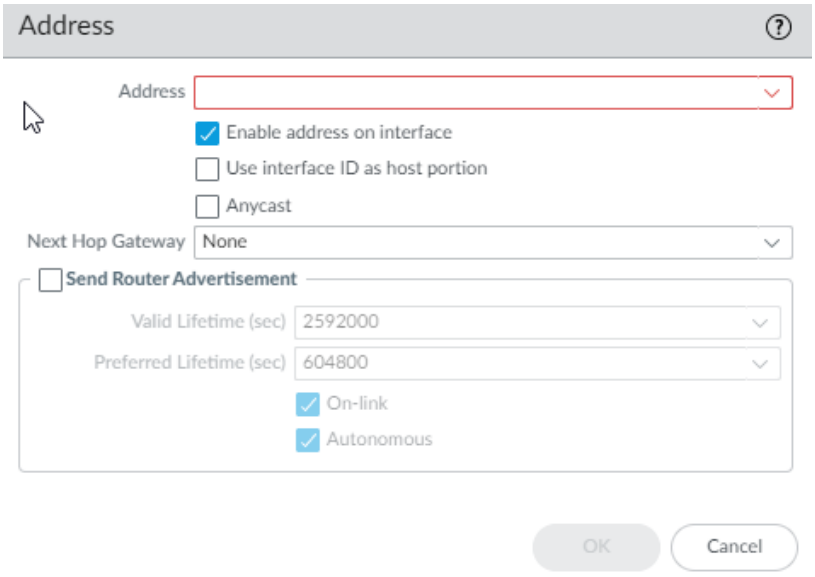
STEP 3 | Cree una subinterfaz de Capa 3 en la que se utilice una dirección IPv6 estática.

1. Realice los primeros seis pasos secundarios del paso para crear una subinterfaz de Capa 3 que utilice una dirección IPv4 estática, ya que son los mismos para una dirección IPv6.
2. En la pestaña **IPv6**, marque **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)** y **Enable SD-WAN (Habilitar SD-WAN)**.
3. En el campo **EUI-64 (default 64-bit Extended Unique Identifier) [EUI-64 (Identificador único ampliado de 64 bits predeterminado)]**, introduzca el EUI de 64 bits en formato hexadecimal. Si deja este campo en blanco, el cortafuegos utilizará el EUI-64 generado desde la dirección MAC de la interfaz física. Si activa la opción **Use interface ID as host portion (Usar la ID de interfaz como parte de host)** cuando se añade una dirección, el cortafuegos utiliza el ID de interfaz como la parte de host de esa dirección.
4. Seleccione el **tipo** de dirección: **Estática**.

5. Seleccione **Address Assignment (Asignación de direcciones)**.



6. Debe **Add (Añadir)** una **dirección** IPv6 para la interfaz o seleccionar **New Variable (Nueva variable)** para crear la variable. SD-WAN es compatible con una dirección IPv6 por interfaz física.
7. **Enable address on interface (Habilitar dirección en la interfaz)**.

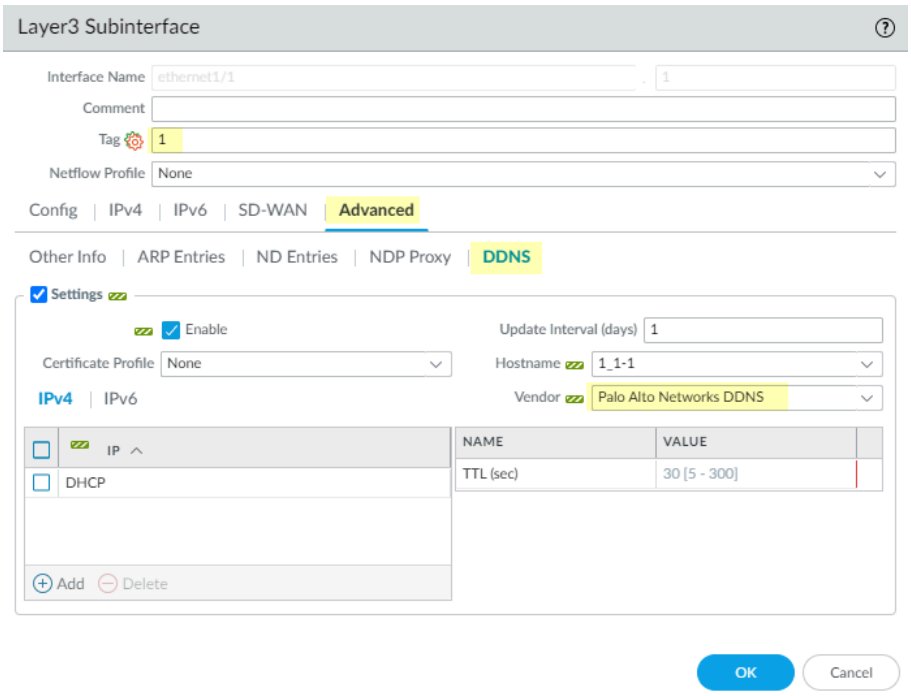


8. **Use interface ID as host portion (Usar ID de la interfaz como parte del host)**: consulte el tercer paso secundario arriba para obtener una explicación.

9. **Anycast (Difusión por proximidad)**: seleccione esta opción para convertir la dirección IPv6 (ruta) en una dirección Anycast (ruta), lo que significa que varias ubicaciones pueden anunciar el mismo prefijo, e IPv6 envía el tráfico anycast al nodo que considere más cercano, en función de los costes del protocolo de enrutamiento y otros factores.
10. **Next Hop Gateway (Puerta de enlace de siguiente salto)**: introduzca la dirección IPv6 de la puerta de enlace de siguiente salto (el siguiente salto desde la dirección IPv6 que introdujo). La puerta de enlace de siguiente salto debe estar en la misma subred que la dirección IPv6. La puerta de enlace de siguiente salto es la dirección IP del enrutador predeterminado del ISP que este le proporcionó cuando adquirió el servicio. Es la dirección IP de siguiente salto a la que el cortafuegos envía tráfico para llegar a la red del ISP, y en última instancia, a internet y al hub.
11. **Send Router Advertisement (Enviar anuncio de enrutador)**: seleccione para habilitar el cortafuegos para que envíe esta dirección en los anuncios del enrutador (RA), en cuyo caso también debe habilitar la opción global **Enable Router Advertisement (Habilitar anuncio de enrutador)** para la interfaz (en la pestaña **Router Advertisement (Anuncio de enrutador)**.
12. **Valid Lifetime (sec) [Duración válida (seg.)]**: Introduzca la duración válida (en segundos) que el cortafuegos considera que la dirección es válida. La duración válida debe ser igual o superar la **Preferred Lifetime (sec) [Duración preferida (seg.)]** (el valor predeterminado es 2 592 000).
13. **Preferred Lifetime (sec) [Duración preferida (en segundos)]**: introduzca el periodo de tiempo preferido (en segundos) durante el cual se prefiere la dirección válida, lo que significa que el cortafuegos puede usarlo para enviar y recibir tráfico. Cuando caduca la duración preferida, el cortafuegos deja de poder utilizar la dirección para establecer nuevas conexiones, pero cualquier conexión existente es válida hasta que caduque la duración válida (el valor predeterminado es 604 800).
14. **On-link (Enlace activo)**: seleccione esta opción si se puede establecer comunicación con los sistemas con direcciones en el prefijo sin necesidad de un enrutador.
15. **Autonomous (Autónomo)**: seleccione esta opción si los sistemas pueden crear una dirección IP de forma independiente combinando el prefijo publicado con un ID de interfaz.
16. Haga clic en **OK (Aceptar)**.

STEP 4 | Como alternativa a una dirección estática, cree una subinterfaz de Capa 3 que utilice DHCP para obtener su dirección IPv4.

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y, en el campo **Template (Plantilla)**, seleccione una pila de plantillas (no una plantilla).
2. Seleccione una interfaz.
3. En **Interface Type (Tipo de interfaz)**, seleccione **Layer 3 (Capa 3)** y haga clic en **OK (Aceptar)**.
4. Resalte la interfaz y haga clic en **Add Subinterfaces (Agregar subinterfaces)** en la parte inferior de la pantalla.
5. Resalte la subinterfaz y haga clic en **Override (Cancelar)**.
6. Resalte la subinterfaz y, después de **Interface Name (Nombre de la interfaz)** y el punto, ingrese el número de la subinterfaz.
7. Introduzca una **etiqueta** para la subinterfaz (el rango es de 1 a 4.094). Por comodidad, el número de la etiqueta debe ser el mismo que el ID de la subinterfaz.
8. En la pestaña **IPv4**, seleccione la opción **Habilitar SD-WAN** .
9. Seleccione el tipo de dirección en **Tipo** : **Cliente DHCP** y **Habilitar**.
10. Anule la selección de **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)**.
11. Seleccione la pestaña **Advanced (Avanzado)** y, a continuación, la pestaña **DDNS (DDNS).**
12. Seleccione **Settings (Configuración)** y **Enable (Habilitar)**. El complemento Panorama SD-WAN genera de forma automática el **nombre de host**.
13. Seleccione el **Vendor (proveedor)** como **Palo Alto Networks DDNS (DDNS de Palo Alto Networks)**.
14. Haga clic en **OK (Aceptar)**.



STEP 5 | Aplique un perfil de interfaz SD-WAN a la subinterfaz.

1. Resalte la subinterfaz que creó y seleccione la pestaña **SD-WAN**.
2. Seleccione el **perfil de interfaz SD-WAN** que creó para este enlace o cree un nuevo perfil.
3. Haga clic en **OK (Aceptar)**.

STEP 6 | Repita los pasos anteriores para agregar más subinterfaces a la interfaz.

STEP 7 | Seleccione **Confirmar**.

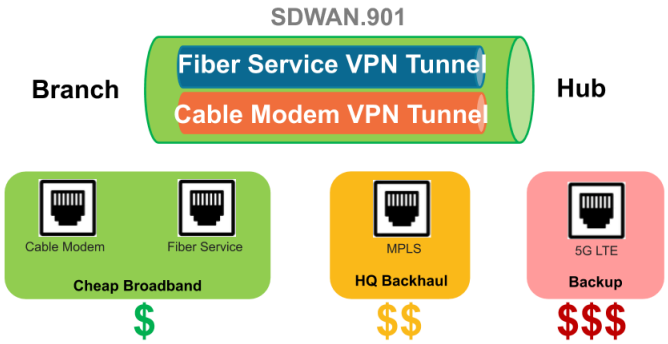
Configuración de una interfaz de SD-WAN virtual

Si utiliza la configuración de VPN automática a través de Panorama, esta crea las interfaces de SD-WAN por usted, por lo que no tiene que crear una interfaz SD-WAN virtual.

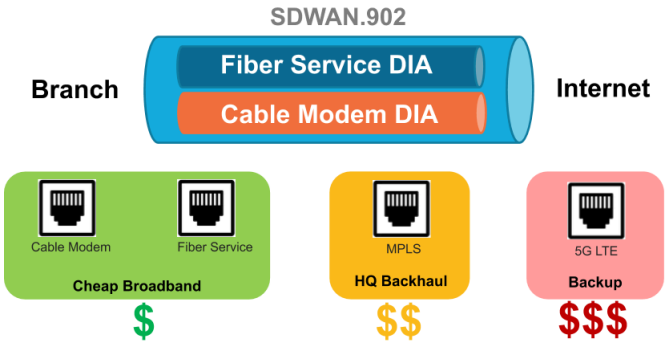
Si no utiliza la configuración de VPN automática con Panorama, cree y configure una interfaz de SD-WAN virtual para especificar una o más interfaces Ethernet físicas compatibles con SD-WAN que van al mismo destino, como a un hub específico o a Internet. De hecho, todos los enlaces de una interfaz de SD-WAN virtual deben ser del mismo tipo: todos los enlaces de túnel VPN o todos los enlaces de acceso directo a Internet (DIA).

La primera figura muestra un ejemplo de una interfaz de SD-WAN denominada SDWAN.901 que agrupa dos interfaces físicas, que utilizan diferentes operadores: Ethernet1/1 (el enlace de módem de cable) y Ethernet1/2 (el enlace de servicio de fibra). Ambos enlaces son un túnel VPN desde la sucursal hasta el hub.

En esta figura, ambos enlaces de la interfaz SD-WAN utilizan la misma etiqueta de enlace (banda ancha barata), pero los enlaces en una interfaz de SD-WAN pueden tener etiquetas de enlace diferentes.



En la siguiente figura, SDWAN.902 agrupa enlaces Ethernet1/1 y Ethernet1/2, que son ambos enlaces de DIA desde la sucursal a Internet:



STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Network (Red)** > **Interfaces** > **SD-WAN** y seleccione la plantilla adecuada en el menú desplegable contextual **Plantilla**.

STEP 3 | **Añada** una interfaz lógica de SD-WAN. Para ello, especifique un número (con un intervalo de 1 a 9,999) después del prefijo **sdwan**.

La configuración de VPN automática crea interfaces SD-WAN numeradas .901, .902, etc., etc. Por lo tanto, si desea crear las interfaces SD-WAN manualmente, no utilice el formato sdwan.90x para un nombre de interfaz SD-WAN. Del mismo modo, la configuración de VPN automática crea una interfaz SD-WAN numerada .9016 para una interfaz IPv6, así que no use sdwan.9016 para un nombre de interfaz SD-WAN.

STEP 4 | Escriba un **comentario** descriptivo.

Añada un comentario útil, como ***`De sucursal a Internet`*** *o* ***`(De sucursal a hub del Este de Estados Unidos`*** *si está en la plantilla Sucursal. Sus comentarios permitirán que la solución de problemas sea más sencilla y no tendrá que intentar descifrar los nombres generados automáticamente en logs e informes.*

STEP 5 | Seleccione el **Protocol (Protocolo)** para indicar el tipo de interfaz SD-WAN virtual:

- **ipv4** indica una interfaz virtual IPv4 DIA.
- **ipv6** indica una interfaz virtual IPv6 DIA.
- **none (ninguna)** indica una interfaz virtual de túnel VPN.

STEP 6 | En la pestaña **Configuración**, asigne la interfaz de SD-WAN a un enrutador en **Enrutador virtual**.

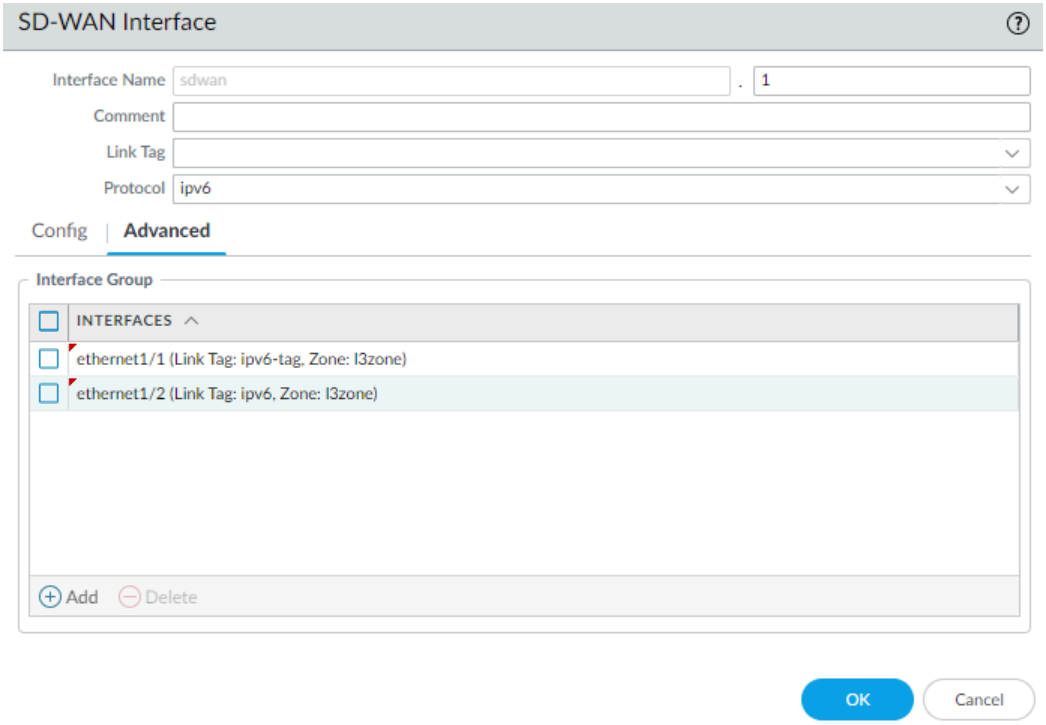
STEP 7 | Asigne la interfaz de SD-WAN a una zona segura en **Zona de seguridad**.

La interfaz virtual de SD-WAN y todos sus miembros de interfaz deben estar en la misma zona de seguridad. De esa forma, se asegura de se apliquen las mismas reglas de la política de seguridad a todas las rutas desde la sucursal hasta el mismo destino.

STEP 8 | Para ello, en la pestaña **Avanzado**, **Añadir Interfaces**, que son miembros que van al mismo destino, seleccione una o más interfaces Ethernet de capa 3 (para DIA) o una interfaz de túnel VPN virtual más (para hub). Si especifica más de una interfaz, todas deben ser del mismo tipo (túnel VPN o DIA).

El enrutador virtual del cortafuegos utiliza esta interfaz de SD-WAN virtual para enrutar el tráfico de SD-WAN a una ubicación del hub o DIA. Durante el enrutamiento, la tabla de rutas determina qué interfaz de SD-WAN virtual (interfaz de salida) del paquete saldrá en función de la dirección IP de destino del paquete. A continuación, el estado de la ruta de SD-WAN y los perfiles de distribución de tráfico en la regla de políticas de SD-WAN que coincide con el paquete determinan qué ruta usar (y el orden en el que considerar las nuevas rutas si una se deteriora).

STEP 9 | Haga clic en **Aceptar** para guardar el cambio de configuración.



STEP 10 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

Creación de una ruta predeterminada a la interfaz de SD-WAN

Si está utilizando una ruta de servicio a fin de acceder a Panorama™, para abrir el cortafuegos debe crear una ruta predeterminada que apunte a una interfaz SD-WAN que haya creado.

La VPN automática crea una interfaz de SD-WAN virtual denominada sdwan.901 para IPv4 DIA y otra denominada sdwan.9016 para IPv6 DIA. Crea una interfaz virtual SD-WAN llamada sdwan.902 para túneles VPN. La VPN automática también crea su propia ruta predeterminada que usa la interfaz sdwan.901 (IPv4) y sdwan.9016 (IPv6) como interfaz de salida y utiliza una métrica baja, por lo que la interfaz sdwan.901 (IPv4) y la interfaz sdwan.9016 (IPv6) son preferibles a la ruta predeterminada que creó.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione la **plantilla** en la que está trabajando.

STEP 3 | Seleccione **Red** > **Enrutadores virtuales** y seleccione un enrutador virtual, como **sd-wan**.

STEP 4 | Seleccione **Static Routes (Rutas estáticas)**.

STEP 5 | Seleccione **IPv4** o **IPv6** y **Add (Añadir)** una ruta estática por **Name (Nombre)**.

STEP 6 | Para un **Destination (Destino)** IPv4, introduzca 0.0.0.0/0. Para un **Destination (Destino)** IPv6, introduzca ::/0.

STEP 7 | En la **Interface (Interfaz)** de salida, seleccione una de las interfaces lógicas de SD-WAN que creó para abrir el cortafuegos.

La interfaz de salida que seleccione puede ser cualquier interfaz de SD-WAN lógica, excepto sdwan.901, sdwan.902 o sdwan.9016.

STEP 8 | Para **Siguiente salto**, seleccione **Ninguno**.

STEP 9 | En **Métrica**, especifique un valor superior a 50, de modo que esta ruta predeterminada no sea la preferida sobre la ruta predeterminada que la VPN automática crea con una métrica baja.

STEP 10 | Haga clic en **OK (Aceptar)**.

STEP 11 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

STEP 12 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 13 | Repita esta tarea para otras plantillas que estén en cortafuegos en los que se use una ruta de servicio para acceder a Panorama™.

Configuración de los perfiles de gestión de enlaces SD-WAN

Cree y configure un perfil de calidad de ruta, calidad de SaaS, distribución de tráfico y corrección de errores para gestionar las conmutaciones por error de enlaces de SD-WAN.

- Creación de un perfil de calidad de ruta
- Configuración de la supervisión de SaaS
- Perfiles de distribución del tráfico de SD-WAN
- Creación de un perfil de distribución de tráfico
- Creación de un perfil de corrección de errores

Creación de un perfil de calidad de ruta

Cree un perfil de calidad de ruta para cada conjunto de aplicaciones críticas para la empresa y sensibles a la latencia, filtros de aplicaciones, grupos de aplicaciones, servicios, objetos de servicio y objetos de grupo de servicios que tengan requisitos únicos de calidad de red (estado) basados en latencia, vibración y porcentaje de pérdida de paquetes. Las aplicaciones y los servicios pueden compartir un perfil de calidad de ruta. Especifique el umbral máximo para cada parámetro por encima del que el cortafuegos considera que la ruta se ha deteriorado lo suficiente como para seleccionar una ruta mejor.

Como alternativa a la creación de un perfil de calidad de ruta, puede usar cualquiera de los perfiles de calidad de ruta predefinidos, como **empresa general**, **vídeo voip**, **uso compartido de archivos**, **transmisión de audio**, **foto-vídeo**, **acceso remoto**, etc. Los perfiles predefinidos se configuran para optimizar los umbrales de latencia, vibración y pérdida de paquetes para el tipo de aplicaciones y servicios sugeridos por el nombre del perfil.

*Los perfiles de calidad de ruta predefinidos para un grupo de dispositivos de Panorama se basan en la configuración predeterminada de **Frecuencia de sonda** en el perfil de la interfaz de SD-WAN para una plantilla de Panorama. Si cambia la configuración predeterminada de la frecuencia de la sonda, debe ajustar el umbral de porcentaje de **Pérdida de paquetes** en el perfil de calidad de ruta para los cortafuegos en un grupo de dispositivos afectados por la plantilla de Panorama donde cambió el perfil de la interfaz.*

El cortafuegos trata los umbrales de latencia, vibración y pérdida de paquetes como condiciones OR, lo que significa que si se supera alguno de los umbrales, el cortafuegos selecciona la nueva ruta mejor (preferida). Cualquier ruta que tenga una latencia, vibración y pérdida de paquetes menor o igual a los tres umbrales se considerará apta y el cortafuegos seleccionará la ruta en función del perfil de distribución de tráfico asociado.

De forma predeterminada, el cortafuegos mide la **latencia** y la **vibración** cada 200 ms y hace una media de las últimas tres mediciones para medir la calidad de la ruta en una ventana deslizante. Puede modificar este comportamiento seleccionando la supervisión de rutas agresiva o relajada cuando Configuración de un perfil de la interfaz de SD-WAN.

Si una ruta falla porque superó el umbral de **pérdida de paquetes** configurado, el cortafuegos sigue enviando paquetes de prueba en la ruta fallida y calcula su porcentaje de pérdida de

paquetes a medida que la ruta se recupera. Puede que tengan que transcurrir aproximadamente tres minutos para que el porcentaje de pérdida de paquetes en una ruta recuperada sea inferior al umbral de pérdida de paquetes configurado en el perfil de calidad de ruta. Por ejemplo, suponga que una regla de políticas de SD-WAN para una aplicación tiene un perfil de calidad de ruta que especifica un umbral de pérdida de paquetes del 1 % y un perfil de distribución de tráfico que especifica la distribución de arriba hacia abajo con la etiqueta 1 (aplicada a tunnel.1) primero en el lista y etiqueta 2 (aplicada a tunnel.2) siguiente en la lista. Cuando tunnel.1 supera el 1 % de pérdida de paquetes, los paquetes de datos realizan una conmutación por error en tunnel.2. Después de que tunnel.1 se recupere al 0 % de pérdida de paquetes (según los paquetes de sondeo), la tasa de pérdida de paquetes supervisada para tunnel.1 puede tardar hasta tres minutos en ser inferior al 1 %. En ese momento, el cortafuegos selecciona tunnel.1 como la mejor ruta de nuevo.

La configuración de sensibilidad indica qué parámetro (latencia, vibración o pérdida de paquetes) es más importante (preferido) para las aplicaciones a las que se aplica el perfil. Cuando el cortafuegos evalúa la calidad del enlace, primero considera un parámetro con una configuración **alta**. Por ejemplo, cuando el cortafuegos compara dos enlaces, suponga que un enlace tiene una latencia de 100 ms y una vibración de 20 ms; el otro enlace tiene una latencia de 300 ms y una vibración de 10 ms. Si la sensibilidad para la latencia es alta, el cortafuegos elige el primer enlace. Si la sensibilidad para la vibración es alta, el cortafuegos elige el segundo enlace. Si los parámetros tienen la misma sensibilidad (de forma predeterminada, los parámetros se establecen en **medio**), el cortafuegos evalúa primero la pérdida de paquetes, luego la latencia y, por último, la vibración.

Como afirma el concepto Perfiles de distribución del tráfico de SD-WAN, la nueva selección de ruta se produce en menos de un segundo si deja lasupervisión de rutas y la frecuencia de sondeo con la configuración predeterminada; de lo contrario, la nueva selección de ruta podría llevar más de un segundo. Para lograr una conmutación por error de subsegundos basada en la pérdida de paquetes, debe establecer la sensibilidad de latencia en **high (alta)** y el umbral de latencia en no más de 250 ms.

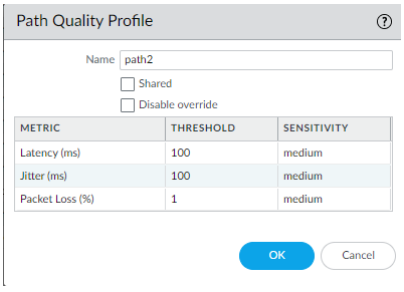
Consulte el perfil de calidad de ruta en una regla de políticas de SD-WAN para controlar el umbral en el que el cortafuegos reemplaza una ruta deteriorada por una nueva ruta para hacer coincidir los paquetes de aplicaciones.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione un **grupo de dispositivos**.

STEP 3 | Seleccione **Objetos** > **Gestión de enlaces de SD-WAN** > **Perfil de calidad de ruta**.

STEP 4 | **Añada** un perfil de calidad de ruta por **nombre** con un máximo de 31 caracteres alfanuméricos.



STEP 5 | Para **Latencia** , haga doble clic en el valor **Umbral** e introduzca la cantidad de milisegundos permitidos para que un paquete salga del cortafuegos, llegue al extremo opuesto del túnel de SD-WAN y el paquete de respuesta regrese al cortafuegos antes de que se supere el umbral (el intervalo es de 10 a 2000; el valor predeterminado es 100).

STEP 6 | Para **Latencia**, seleccione **Sensibilidad** (**baja**, **media** o **alta**). El valor predeterminado es **medio**.

Haga clic en la flecha al final de la columna del umbral para ordenar umbrales en orden numérico ascendente o descendente.

STEP 7 | Para **Jitter (Vibración)**, haga doble clic en el valor **Umbral** y especifique el número de milisegundos (el intervalo es de 10 a 1,000; el valor predeterminado es 100).

STEP 8 | Para **Jitter (Vibración)**, seleccione **Sensibilidad** (**baja**, **media** o **alta**). El valor predeterminado es **medio**.

STEP 9 | Para **Pérdida de paquete**, haga doble clic en el valor **Umbral** y especifique el porcentaje de paquetes perdidos en el enlace antes de que se supere el umbral (el intervalo es de 1 a 100.0; el valor predeterminado es 1).

*El establecimiento de la **sensibilidad** para la **pérdida de paquetes** no tiene ningún efecto, así que deje la configuración predeterminada.*

*Si cambia la **frecuencia de sonda** en un perfil de la interfaz de SD-WAN para una plantilla de Panorama, también debe ajustar el umbral de Pérdida de paquete para un grupo de dispositivos de Panorama.*

STEP 10 | Haga clic en **OK (Aceptar)**.

STEP 11 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

STEP 12 | **Commit (Confirmar)** los cambios.

STEP 13 | Repita esta tarea para cada grupo de dispositivos.

Configuración de la supervisión de SaaS

Configure un perfil de calidad de SaaS para supervisar los enlaces de acceso directo a Internet (DIA, Direct Internet Access) entre una aplicación SaaS y el cortafuegos de su sucursal.

La supervisión de rutas de la aplicación SaaS solo es compatible con los cortafuegos PAN-OS habilitados para SD-WAN. La supervisión de rutas de la aplicación SaaS no es compatible con las centrales de Prisma Access.

- Creación de un perfil de calidad de SaaS
- Caso de uso: Configuración de la supervisión de SaaS para un cortafuegos de sucursal
- Caso de uso: Configuración de una conmutación por error del cortafuegos de central para la supervisión de SaaS desde un cortafuegos de sucursal para el mismo destino de la aplicación SaaS

- Caso de uso: Configuración de una conmutación por error del cortafuegos de central para la supervisión de SaaS desde un cortafuegos de sucursal para un destino distinto de la aplicación SaaS

Creación de un perfil de calidad de SaaS

Si el cortafuegos de su sucursal tiene un enlace de acceso directo a Internet (DIA, Direct Internet Access) a una aplicación de software como servicio (SaaS, Software-as-a-Service), cree un perfil de calidad de SaaS para especificar cómo se deben supervisar una o más aplicaciones SaaS. Los perfiles de calidad SaaS están asociados con una regla de políticas SD-WAN para determinar cómo el cortafuegos de sucursal establece los umbrales de calidad de la ruta para la latencia, la fluctuación y la pérdida de paquetes, y selecciona la ruta preferida para un paquete saliente.

El perfil de calidad de SaaS admite hasta cuatro direcciones IP estáticas o un nombre de dominio completo (FQDN, Fully Qualified Domain Name) o URL por perfil de calidad de SaaS. Cuando se configuran varias direcciones IP estáticas, el cortafuegos de sucursal supervisa una dirección IP a la vez en orden en cascada según cómo se ordenen las direcciones IP en el perfil de calidad de SaaS. Por ejemplo, si añade IP1, IP2, IP3 e IP4, el cortafuegos de sucursal supervisa IP1 para determinar si se han superado los umbrales de calidad de la ruta. Después pasa a IP2, y así sucesivamente.

Los datos de supervisión e informes de SD-WAN muestran la aplicación SaaS y la IP, FQDN o URL de la aplicación SaaS tal como están configuradas actualmente en el perfil de calidad de SaaS asociado con una regla de políticas SD-WAN independientemente del filtro de tiempo aplicado al ver sus datos de supervisión SD-WAN.

Por ejemplo, hace tres días, configuró inicialmente la dirección IP de su aplicación SaaS como ***192.168.10.50*** *en un perfil de calidad de SaaS y el tráfico coincidió con la regla de políticas SD-WAN a la que está asociado el perfil de calidad de SaaS. Hoy ha reconfigurado este perfil de calidad de SaaS existente y ha cambiado la dirección IP de la aplicación SaaS a* ***192.168.10.20****. Cuando revisa los datos de supervisión de SD-WAN, todos los datos de supervisión existentes para esta aplicación SaaS muestran la dirección IP* ***192.168.10.20****.*

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Objects (Objetos)** > **SD-WAN Link Management (Gestión de enlaces SD-WAN)** > **SaaS Quality Profile (Perfil de calidad de SaaS)** y especifique el **grupo de dispositivos** que contiene su configuración SD-WAN.

STEP 3 | **Añada** un nuevo perfil de calidad de SaaS.

STEP 4 | Introduzca un **nombre** descriptivo para el perfil de calidad de SaaS.

STEP 5 | (Opcional) Habilite (marque) **Shared (Compartido)** para que el perfil de calidad de SaaS se comparta en todos los grupos de dispositivos.

STEP 6 | (Opcional) Habilite (marque) **Disable override (Deshabilitar anulación)** para deshabilitar la anulación de la configuración del perfil de calidad de SaaS en el cortafuegos local.

> ***Disable override (Deshabilitar anulación)*** *solo se puede habilitar si* ***Shared (Compartido)*** *está deshabilitado en el paso anterior.*

STEP 7 | Configure el modo de supervisión de SaaS.

- Supervise automáticamente el estado de la ruta de la aplicación SaaS.

  La supervisión **adaptativa**, que se habilita de forma predeterminada, permite que el cortafuegos de sucursal supervise pasivamente la sesión de la aplicación SaaS para la actividad de envío y recepción para determinar si se han superado los umbrales de

calidad de la ruta. La calidad del estado de la ruta de la aplicación SaaS se determina automáticamente sin ningún control de estado adicional en la interfaz SD-WAN.

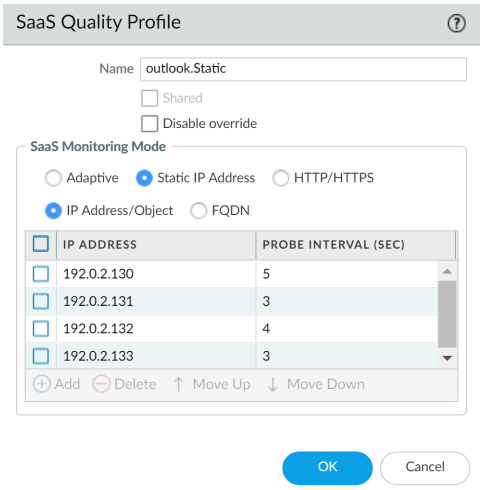
La supervisión adaptativa de SaaS solo es compatible con las aplicaciones SaaS TCP.

- Configure la dirección IP estática para la aplicación SaaS.

  Cree un perfil de calidad de SaaS por aplicación SaaS crítica que necesite supervisar. Si una aplicación SaaS tiene varias direcciones IP, configure un perfil de calidad de SaaS con varias direcciones IP estáticas para esa aplicación SaaS.

  La supervisión de SaaS consume muchos recursos y puede afectar el rendimiento del cortafuegos si se supervisa una gran cantidad de aplicaciones SaaS. Es una práctica recomendada supervisar solo aquellas aplicaciones SaaS críticas para el negocio que necesiten un buen uso.

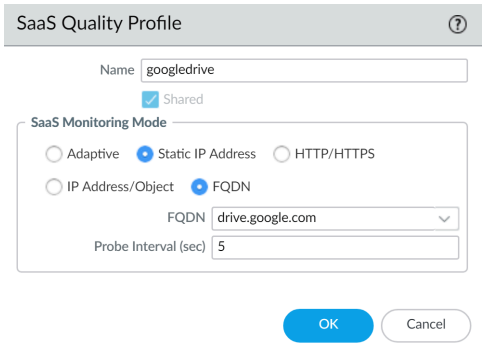
  1. Seleccione **IP Address/Object (Dirección IP/Objeto)** > **Static IP Address (Dirección IP estática)** y **añada** una dirección IP.
  2. Especifique la dirección IP de la aplicación SaaS o seleccione un objeto de dirección configurado.
  3. Especifique el **intervalo de sondeo** mediante el que el cortafuegos de sucursal prueba la ruta de la aplicación SaaS para obtener información del estado.
  4. Haga clic en **Aceptar** para guardar los cambios.



- Configure el nombre de dominio completo (FQDN, Fully Qualified Domain Name) para la aplicación SaaS.

  1. Configure un objeto de dirección FQDN para la aplicación SaaS.
  2. Seleccione **IP Address/Object (Dirección IP/Objeto)** > **FQDN** y **añada** el FQDN.
  3. Seleccione el objeto de dirección **FQDN** para la aplicación SaaS.
  4. Especifique el **intervalo de sondeo** mediante el que el cortafuegos de sucursal prueba la ruta de la aplicación SaaS para obtener información del estado.

5. Haga clic en **Aceptar** para guardar los cambios.

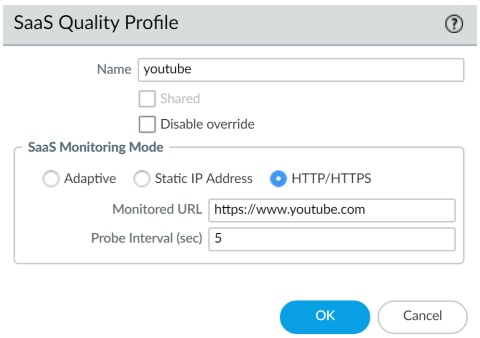


- Configure la URL para la aplicación SaaS.

  La supervisión de URL solo es compatible con el tráfico a través de los puertos 80, 443, 8080, 8081 y 143.

  1. Seleccione **HTTP/HTTPS**.
  2. Especifique la **URL supervisada** de la aplicación SaaS.
  3. Especifique el **intervalo de sondeo** mediante el que el cortafuegos de sucursal prueba la ruta de la aplicación SaaS para obtener información del estado.

     El intervalo de sondeo mínimo admitido para una aplicación SaaS HTTP/HTTPS es de 3 segundos.
  4. Haga clic en **Aceptar** para guardar los cambios.



STEP 8 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

Caso de uso: Configuración de la supervisión de SaaS para un cortafuegos de sucursal

Si su organización aprovecha una aplicación SaaS crítica para la empresa en una ubicación de cortafuegos de sucursal, puede configurar un perfil de calidad de SaaS y asociarlo con una regla de políticas SD-WAN para supervisar las métricas de estado de latencia, vibración y pérdida de paquetes de la aplicación SaaS crítica e intercambiar enlaces desde un cortafuegos de sucursal SD-WAN a una aplicación SaaS en un enlace de acceso directo a Internet (DIA, Direct Internet Access) para garantizar el uso de la aplicación.

Si se superan los umbrales de métrica de estado del enlace DIA de la aplicación SaaS crítica para la empresa, el enlace se intercambia al siguiente enlace DIA configurado en el perfil de distribución de tráfico para todas las sesiones nuevas. La sesión existente en el enlace DIA degradado no se transfiere al siguiente enlace DIA.

STEP 1 | Configure su implementación de SD-WAN.

1. Instalación del complemento de SD-WAN.
2. Configuración de Panorama y cortafuegos para SD-WAN.
3. Adición de dispositivos de SD-WAN a Panorama.
4. (Solo configuraciones de alta disponibilidad) Configuración de dispositivos de HA para SD-WAN.
5. Creación de un clúster de VPN.

STEP 2 | Creación de una etiqueta de enlace para agrupar los enlaces DIA de la aplicación SaaS.

Cree varias etiquetas de enlace para sus enlaces DIA para aplicar diferentes configuraciones de supervisión de SD-WAN para cada enlace DIA de la aplicación SaaS según el tipo de enlace.

Además, puede crear una sola etiqueta de enlace para varios enlaces DIA con el fin de agrupar los enlaces en un solo paquete de enlaces. La creación de una sola etiqueta de enlace para varios enlaces DIA le permite añadir ancho de banda entre enlaces agrupados y permitir que el cortafuegos distribuya sesiones entre varios enlaces.

STEP 3 | Configure un perfil de interfaz SD-WAN para definir las características de la conexión de su ISP y especificar la velocidad del enlace DIA, la frecuencia con la que el cortafuegos de sucursal supervisa el enlace, y seleccione la etiqueta de enlace para especificar a qué enlace aplicar el perfil de interfaz SD-WAN.

Si ha creado varias etiquetas de enlace, debe configurar un perfil de interfaz SD-WAN para cada una.

Si ha creado un paquete de enlaces asignando varios enlaces DIA a una sola etiqueta de enlace, cuando especifique esa etiqueta de enlace se aplicará la configuración del perfil de la interfaz SD-WAN a todos los enlaces DIA del paquete.

STEP 4 | Configure una interfaz Ethernet física para cada enlace DIA de la aplicación SaaS.

Todas las interfaces Ethernet físicas para enlaces DIA deben ser de capa 3.

STEP 5 | Configuración de una interfaz de SD-WAN virtual que agrupa todas las interfaces Ethernet físicas para los enlaces DIA de la aplicación SaaS en un solo grupo de interfaces.

El enrutador virtual del cortafuegos utiliza esta interfaz de SD-WAN virtual para enrutar el tráfico de SD-WAN a una ubicación de DIA. El estado de la ruta de SD-WAN y los perfiles de distribución de tráfico en la regla de políticas de SD-WAN determinan qué ruta usar y el orden en el que considerar las nuevas rutas si se deteriora el estado de una.

STEP 6 | Cree un perfil de calidad de ruta para configurar la latencia, la vibración y los umbrales de pérdida de paquetes y la sensibilidad con el fin de especificar el momento en el que el cortafuegos de sucursal debe cambiar al siguiente enlace DIA.

STEP 7 | Cree un perfil de calidad de SaaS para especificar su aplicación SaaS y la frecuencia con la que se supervisa el enlace DIA.

STEP 8 | Cree un perfil de distribución de tráfico para especificar el orden en que el cortafuegos de sucursal cambia a los enlaces DIA en caso de degradación del estado del enlace.

STEP 9 | Configure una regla de políticas SD-WAN para especificar la aplicación SaaS y las métricas de estado del enlace, y determine cómo el cortafuegos selecciona el enlace preferido para el tráfico crítico de la aplicación SaaS.

*En la pestaña **Application (Aplicación)**, añada la aplicación SaaS que está supervisando a la regla de políticas SD-WAN para asegurarse de que la configuración de supervisión SaaS se aplique solo a la aplicación SaaS deseada.*

Caso de uso: Configuración de una conmutación por error del cortafuegos de central para la supervisión de SaaS desde un cortafuegos de sucursal para el mismo destino de la aplicación SaaS

Si su empresa está aprovechando una aplicación SaaS en una ubicación de cortafuegos de sucursal, pero ese cortafuegos no tiene enlaces DIA en buen estado para intercambiar, puede configurar el cortafuegos de central como una alternativa de conmutación por error para mantener una conexión correcta con su aplicación SaaS.

Si se superan los umbrales de la métrica de estado del enlace DIA de la aplicación SaaS y el cortafuegos de sucursal no tiene enlaces DIA en buen estado disponibles, el enlace se cambia al siguiente cortafuegos de central para todas las sesiones nuevas. La sesión existente en el enlace DIA degradado no se transfiere al cortafuegos de central.

Por ejemplo, supongamos que los cortafuegos de sucursal y central están ubicados en la misma región y acceden a una aplicación SaaS mediante la misma IP de destino. Puede configurar el cortafuegos de central para que actúe como una conmutación por error en caso de que no haya enlaces DIA en buen estado desde el cortafuegos de sucursal a la aplicación SaaS mediante el establecimiento de un perfil de calidad de SaaS con el mismo nombre en los cortafuegos de sucursal y de central para realizar una conmutación por error automáticamente en el cortafuegos de central si no hay enlaces DIA en buen estado disponibles desde el cortafuegos de sucursal. Esto le permite mantener una ruta de estado para su aplicación SaaS y conservar datos precisos de supervisión de aplicaciones SaaS de extremo a extremo sin congestionar el ancho de banda de su red.

STEP 1 | Configure su implementación de SD-WAN.

1. Instalación del complemento de SD-WAN.
2. Configuración de Panorama y cortafuegos para SD-WAN.
3. Adición de dispositivos de SD-WAN a Panorama.
4. (Solo configuraciones de alta disponibilidad) Configuración de dispositivos de HA para SD-WAN.
5. Creación de un clúster de VPN.

STEP 2 | Creación de una etiqueta de enlace para agrupar los enlaces DIA de la aplicación SaaS.

Cree varias etiquetas de enlace para sus enlaces DIA para aplicar diferentes configuraciones de supervisión de SD-WAN para cada enlace DIA de la aplicación SaaS según el tipo de enlace.

Además, puede crear una sola etiqueta de enlace para varios enlaces DIA con el fin de agrupar los enlaces en un solo paquete de enlaces.

STEP 3 | Configure un perfil de interfaz SD-WAN para definir las características de la conexión de su ISP y especificar la velocidad del enlace DIA, la frecuencia con la que el cortafuegos de sucursal supervisa el enlace, y seleccione la etiqueta de enlace para especificar a qué enlace aplicar el perfil de interfaz SD-WAN.

Si ha creado varias etiquetas de enlace, debe configurar un perfil de interfaz SD-WAN para cada una.

Si ha creado un paquete de enlaces asignando varios enlaces DIA a una sola etiqueta de enlace, cuando especifique esa etiqueta de enlace se aplicará la configuración del perfil de la interfaz SD-WAN a todos los enlaces DIA del paquete.

STEP 4 | Configure una interfaz Ethernet física para cada enlace DIA de la aplicación SaaS.

Todas las interfaces Ethernet físicas para enlaces DIA deben ser de capa 3.

STEP 5 | Configuración de una interfaz de SD-WAN virtual que agrupa todas las interfaces Ethernet físicas para los enlaces DIA de la aplicación SaaS en un solo grupo de interfaces.

El enrutador virtual del cortafuegos utiliza esta interfaz de SD-WAN virtual para enrutar el tráfico de SD-WAN a una ubicación de DIA. El estado de la ruta de SD-WAN y los perfiles de distribución de tráfico en la regla de políticas de SD-WAN determinan qué ruta usar y el orden en el que considerar las nuevas rutas si se deteriora el estado de una.

STEP 6 | Cree perfiles de calidad SaaS con el mismo nombre para los cortafuegos de central y de sucursal.

Se deben configurar dos perfiles de calidad SaaS con el mismo nombre en los cortafuegos de central y sucursal para aprovechar correctamente el cortafuegos de central como una conmutación por error alternativa. La forma más sencilla de lograr esto es crear un único perfil de calidad de SaaS en el grupo de dispositivos compartidos. También puede crear dos perfiles de calidad SaaS con nombres idénticos en diferentes grupos de dispositivos y enviarlos a sus cortafuegos de central y sucursal.

1. Seleccione **Objects (Objetos)** > **SD-WAN Link Management (Gestión de enlaces SD-WAN)** > **SaaS Quality Profile (Perfil de calidad de SaaS)** y, en la lista desplegable Device Group (Grupo de dispositivos), seleccione **Shared (Compartido)**.
2. **Añada** un nuevo perfil de calidad de SaaS.
3. Introduzca un **nombre** descriptivo para el perfil de calidad de SaaS.
4. Habilite (marque) **Shared (Compartido)** para que el perfil de calidad de SaaS se comparta en todos los grupos de dispositivos.

   Esto es necesario para que el perfil de calidad de SaaS esté disponible para todos los grupos de dispositivos a los que pertenecen sus cortafuegos de sucursal y central.

5. Habilite (marque) **Disable override (Deshabilitar anulación)** para deshabilitar la anulación de la configuración del perfil de calidad de SaaS en el cortafuegos local.
6. Configure el modo de supervisión de SaaS mediante uno de los siguientes métodos.
   - Configure la dirección IP estática para la aplicación SaaS.

     Cree un perfil de calidad de SaaS por aplicación SaaS. Si una aplicación SaaS tiene varias direcciones IP, configure un perfil de calidad de SaaS con varias direcciones IP estáticas para esa aplicación SaaS.

     1. Seleccione **IP Address/Object (Dirección IP/Objeto)** > **Static IP Address (Dirección IP estática)** y **añada** una dirección IP.
     2. Especifique la dirección IP de la aplicación SaaS o seleccione un objeto de dirección configurado.
     3. Especifique el **intervalo de sondeo** mediante el que el cortafuegos de sucursal prueba la ruta de la aplicación SaaS para obtener información del estado.
     4. Haga clic en **Aceptar** para guardar los cambios.
   - Configure el nombre de dominio completo (FQDN, Fully Qualified Domain Name) para la aplicación SaaS.
     1. Configure un objeto de dirección FQDN para la aplicación SaaS.
     2. Seleccione **IP Address/Object (Dirección IP/Objeto)** > **FQDN** y **añada** el FQDN.
     3. Seleccione el objeto de dirección **FQDN** para la aplicación SaaS.
     4. Especifique el **intervalo de sondeo** mediante el que el cortafuegos de sucursal prueba la ruta de la aplicación SaaS para obtener información del estado.
     5. Haga clic en **Aceptar** para guardar los cambios.
   - Configure la URL para la aplicación SaaS.

     La supervisión de URL solo es compatible con el tráfico a través de los puertos 80, 443, 8080, 8081 y 143.

     1. Seleccione **HTTP/HTTPS**.
     2. Especifique la **URL supervisada** de la aplicación SaaS.
     3. Especifique el **intervalo de sondeo** mediante el que el cortafuegos de sucursal prueba la ruta de la aplicación SaaS para obtener información del estado.
     4. Haga clic en **Aceptar** para guardar los cambios.

STEP 7 | Cree un perfil de distribución de tráfico para especificar el orden en que el cortafuegos de sucursal cambia de los enlaces DIA a los enlaces VPN al cortafuegos de central en caso de degradación del estado del enlace.

STEP 8 | Configure una regla de políticas SD-WAN para especificar la aplicación SaaS y las métricas de estado del enlace, y determine cómo el cortafuegos selecciona el enlace preferido para el tráfico crítico de la aplicación SaaS.

*En la pestaña **Application (Aplicación)**, añada la aplicación SaaS que está supervisando a la regla de políticas SD-WAN para asegurarse de que la configuración de supervisión SaaS se aplique solo a la aplicación SaaS deseada.*

Caso de uso: Configuración de una conmutación por error del cortafuegos de central para la supervisión de SaaS desde un cortafuegos de sucursal para un destino distinto de la aplicación SaaS

Si su empresa está aprovechando una aplicación SaaS en una ubicación de cortafuegos de sucursal, pero ese cortafuegos no tiene enlaces DIA en buen estado para intercambiar, puede configurar el cortafuegos de central como una alternativa de conmutación por error para mantener una conexión correcta con su aplicación SaaS mediante un perfil de calidad de SaaS dirigido a un destino de la aplicación SaaS diferente.

Si se superan los umbrales de la métrica de estado del enlace DIA de la aplicación SaaS y el cortafuegos de sucursal no tiene enlaces DIA en buen estado disponibles, el enlace se cambia al siguiente cortafuegos de central para todas las sesiones nuevas. La sesión existente en el enlace DIA degradado no se transfiere al cortafuegos de central.

Por ejemplo, supongamos que los cortafuegos de central y sucursal están ubicados en lados opuestos del país y acceden a una aplicación en la nube SaaS implementada en un proveedor de la nube como GCP. Puede configurar el cortafuegos de central para que actúe como una conmutación por error en caso de que no haya enlaces DIA en buen estado desde el cortafuegos de central a la aplicación SaaS. Para lograr esto, configure un perfil de calidad de SaaS con el mismo nombre en los cortafuegos de sucursal y central para realizar una conmutación por error automáticamente al cortafuegos de central si no hay enlaces DIA en buen estado disponibles desde el cortafuegos de sucursal. El perfil de calidad de SaaS configurado en el cortafuegos de central para indicar la ubicación de la rampa de acceso más cercana a la central para aprovechar los recursos locales más próximos a ella. Esto le proporciona flexibilidad para especificar rutas de conmutación por error en buen estado y la capacidad de mantener datos precisos de supervisión de aplicaciones SaaS de extremo a extremo sin congestionar el ancho de banda de su red.

STEP 1 | Configure su implementación de SD-WAN.

1. Instalación del complemento de SD-WAN.
2. Configuración de Panorama y cortafuegos para SD-WAN.
3. Adición de dispositivos de SD-WAN a Panorama.
4. (Solo configuraciones de alta disponibilidad) Configuración de dispositivos de HA para SD-WAN.
5. Creación de un clúster de VPN.

STEP 2 | Creación de una etiqueta de enlace para agrupar los enlaces DIA de la aplicación SaaS.

Cree varias etiquetas de enlace para sus enlaces DIA para aplicar diferentes configuraciones de supervisión de SD-WAN para cada enlace DIA de la aplicación SaaS según el tipo de enlace.

Además, puede crear una sola etiqueta de enlace para varios enlaces DIA con el fin de agrupar los enlaces en un solo paquete de enlaces.

STEP 3 | Configure un perfil de interfaz SD-WAN para definir las características de la conexión de su ISP y especificar la velocidad del enlace DIA, la frecuencia con la que el cortafuegos de sucursal supervisa el enlace, y seleccione la etiqueta de enlace para especificar a qué enlace aplicar el perfil de interfaz SD-WAN.

Si ha creado varias etiquetas de enlace, debe configurar un perfil de interfaz SD-WAN para cada una.

Si ha creado un paquete de enlaces asignando varios enlaces DIA a una sola etiqueta de enlace, cuando especifique esa etiqueta de enlace se aplicará la configuración del perfil de la interfaz SD-WAN a todos los enlaces DIA del paquete.

STEP 4 | Configure una interfaz Ethernet física para cada enlace DIA de la aplicación SaaS.

Todas las interfaces Ethernet físicas para enlaces DIA deben ser de capa 3.

STEP 5 | Configuración de una interfaz de SD-WAN virtual que agrupa todas las interfaces Ethernet físicas para los enlaces DIA de la aplicación SaaS en un solo grupo de interfaces.

El enrutador virtual del cortafuegos utiliza esta interfaz de SD-WAN virtual para enrutar el tráfico de SD-WAN a una ubicación de DIA. El estado de la ruta de SD-WAN y los perfiles de distribución de tráfico en la regla de políticas de SD-WAN determinan qué ruta usar y el orden en el que considerar las nuevas rutas si se deteriora el estado de una.

STEP 6 | Cree perfiles de calidad SaaS con el mismo nombre para los cortafuegos de central y de sucursal.

Se deben configurar dos perfiles de calidad SaaS con el mismo nombre en los cortafuegos de central y sucursal para aprovechar correctamente el cortafuegos de central como una conmutación por error alternativa. Cree dos perfiles de calidad SaaS con nombres idénticos, cada uno dirigido a un destino de aplicación de SaaS diferente en diferentes grupos de dispositivos y envíelos a sus cortafuegos de central y sucursal.

1. Seleccione **Objects (Objetos)** > **SD-WAN Link Management (Gestión de enlaces SD-WAN)** > **SaaS Quality Profile (Perfil de calidad de SaaS)** y seleccione el grupo de dispositivos de destino que contiene el cortafuegos de sucursal del menú desplegable Device Group (Grupo de dispositivos).
2. **Añada** un nuevo perfil de calidad de SaaS.
3. Introduzca un **nombre** descriptivo para el perfil de calidad de SaaS.
4. Habilite (marque) **Disable override (Deshabilitar anulación)** para deshabilitar la anulación de la configuración del perfil de calidad de SaaS en el cortafuegos local.

5. Configure el modo de supervisión de SaaS mediante uno de los siguientes métodos.
   - Configure la dirección IP estática para la aplicación SaaS.

     Cree un perfil de calidad de SaaS por aplicación SaaS. Si una aplicación SaaS tiene varias direcciones IP, configure un perfil de calidad de SaaS con varias direcciones IP estáticas para esa aplicación SaaS.

     1. Seleccione **IP Address/Object (Dirección IP/Objeto)** > **Static IP Address (Dirección IP estática)** y **añada** una dirección IP.
     2. Especifique la dirección IP de la aplicación SaaS o seleccione un objeto de dirección configurado.
     3. Especifique el **intervalo de sondeo** mediante el que el cortafuegos de sucursal prueba la ruta de la aplicación SaaS para obtener información del estado.
     4. Haga clic en **Aceptar** para guardar los cambios.
   - Configure el nombre de dominio completo (FQDN, Fully Qualified Domain Name) para la aplicación SaaS.
     1. Configure un objeto de dirección FQDN para la aplicación SaaS.
     2. Seleccione **IP Address/Object (Dirección IP/Objeto)** > **FQDN** y **añada** el FQDN.
     3. Seleccione el objeto de dirección **FQDN** para la aplicación SaaS.
     4. Especifique el **intervalo de sondeo** mediante el que el cortafuegos de sucursal prueba la ruta de la aplicación SaaS para obtener información del estado.
     5. Haga clic en **Aceptar** para guardar los cambios.
   - Configure la URL para la aplicación SaaS.

     La supervisión de URL solo es compatible con el tráfico a través de los puertos 80, 443, 8080, 8081 y 143.

     1. Seleccione **HTTP/HTTPS**.
     2. Especifique la **URL supervisada** de la aplicación SaaS.
     3. Especifique el **intervalo de sondeo** mediante el que el cortafuegos de sucursal prueba la ruta de la aplicación SaaS para obtener información del estado.
     4. Haga clic en **Aceptar** para guardar los cambios.
6. Seleccione **Objects (Objetos)** > **SD-WAN Link Management (Gestión de enlaces SD-WAN)** > **SaaS Quality Profile (Perfil de calidad de SaaS)** y seleccione el grupo de dispositivos de destino que contiene el cortafuegos de central del menú desplegable Device Group (Grupo de dispositivos).
7. Repita los pasos del 6.2 al 6.5 para crear un perfil de calidad de SaaS con el mismo nombre para una aplicación SaaS en un destino diferente.

   Este paso es necesario para crear un perfil de calidad de SaaS con el mismo nombre en el grupo de dispositivos al que pertenece el cortafuegos de central.

STEP 7 | Cree un perfil de distribución de tráfico para especificar el orden en que el cortafuegos de sucursal cambia de los enlaces DIA a los enlaces VPN al cortafuegos de central en caso de degradación del estado del enlace.

STEP 8 | Configure una regla de políticas SD-WAN para especificar la aplicación SaaS y las métricas de estado del enlace, y determine cómo el cortafuegos selecciona el enlace preferido para el tráfico crítico de la aplicación SaaS.

*En la pestaña **Application (Aplicación)**, añada la aplicación SaaS que está supervisando a la regla de políticas SD-WAN para asegurarse de que la configuración de supervisión SaaS se aplique solo a la aplicación SaaS deseada.*

Perfiles de distribución del tráfico de SD-WAN

En una topología de SD-WAN, el cortafuegos detecta una caída de tensión, un apagón y un deterioro de la ruta *por aplicación* y selecciona una nueva ruta para garantizar que experimente el mejor rendimiento para sus aplicaciones empresariales críticas. Disponer de varios enlaces de ISP le permite escalar su capacidad de tráfico y reducir costes. La nueva selección de ruta se produce en menos de un segundo si deja Supervisión de rutas y frecuencia de sondeo con la configuración predeterminada; de lo contrario, la nueva selección de ruta podría llevar más de un segundo.

Para implementar dicha selección de ruta, el cortafuegos utiliza reglas de políticas de SD-WAN, que hacen referencia a un perfil de distribución de tráfico que especifica cómo seleccionar rutas para la distribución de carga de sesión y para la conmutación por error a una ruta mejor cuando la calidad de ruta para una aplicación se deteriora.

Decida qué método de distribución de tráfico debe usar una aplicación o servicio (que coincida con una regla de políticas de SD-WAN):

- **Mejor ruta disponible**: seleccione este método si el coste no es un factor; permitirá que las aplicaciones usen cualquier ruta fuera de la sucursal. El cortafuegos utiliza métricas de calidad de ruta para distribuir el tráfico y conmutar por error a uno de los enlaces que pertenecen a una etiqueta de enlace en la lista, lo que proporciona la mejor experiencia de aplicación a los usuarios.
- **Prioridad de arriba hacia abajo**: si tiene enlaces caros o de baja capacidad que desee usar solo como último recurso o como enlace de respaldo, utilice el método de prioridad de arriba hacia abajo y coloque las etiquetas que incluyen esos los últimos enlaces en la lista de etiquetas de enlaces en el perfil. El cortafuegos utiliza primero la etiqueta de enlace superior en la lista para determinar los enlaces en los que se debe cargar el tráfico de sesión y en el que se puede conmutar por error. Si ninguno de los enlaces en la etiqueta de enlace superior es apto en función del perfil de calidad de ruta, el cortafuegos selecciona un enlace de la segunda etiqueta de enlace en la lista. Si ninguno de los enlaces en la segunda etiqueta de enlace es apto, el proceso continúa según sea necesario hasta que el cortafuegos encuentre un enlace apto en la última etiqueta de enlace. Si todos los enlaces asociados están sobrecargados y ningún enlace cumple con los umbrales de calidad, el cortafuegos utiliza el método Mejor ruta disponible para seleccionar un enlace en el que reenviar el tráfico. Al comienzo de un evento de conmutación por error, el cortafuegos empieza por la parte superior de la lista Prioridad de arriba hacia abajo de etiquetas de enlace para encontrar un enlace en el que realizar la conmutación por error.
- **Distribución de sesión ponderada**: seleccione este método si desea cargar manualmente el tráfico (que coincide con la regla) en los enlaces de su ISP y WAN, y no necesita conmutación por error durante las condiciones de caída de tensión. Especifique manualmente la carga del enlace cuando aplique un porcentaje estático de nuevas sesiones que obtendrán las interfaces agrupadas con una sola etiqueta de enlace. El cortafuegos distribuye nuevas sesiones por turnos entre los enlaces que tienen las etiquetas de enlace especificadas hasta que el enlace asignado al porcentaje más bajo alcanza ese porcentaje de sesiones. El cortafuegos usa después

los enlaces restantes de la misma manera. Puede seleccionar este método para aplicaciones que no son sensibles a la latencia y que requieren una gran capacidad de ancho de banda de enlace, como copias de seguridad de sucursales grandes y transferencias de archivos grandes.

Si el enlace experimenta una caída de tensión, el cortafuegos no redirige el tráfico coincidente a un enlace diferente.

En el caso de una condición de ruta defectuosa, el método de distribución de tráfico que elija para las aplicaciones en una regla de políticas de SD-WAN, junto con las etiquetas de enlace en grupos de enlaces, determina si el cortafuegos selecciona una nueva ruta (realiza una conmutación por error del enlace) de la siguiente manera:

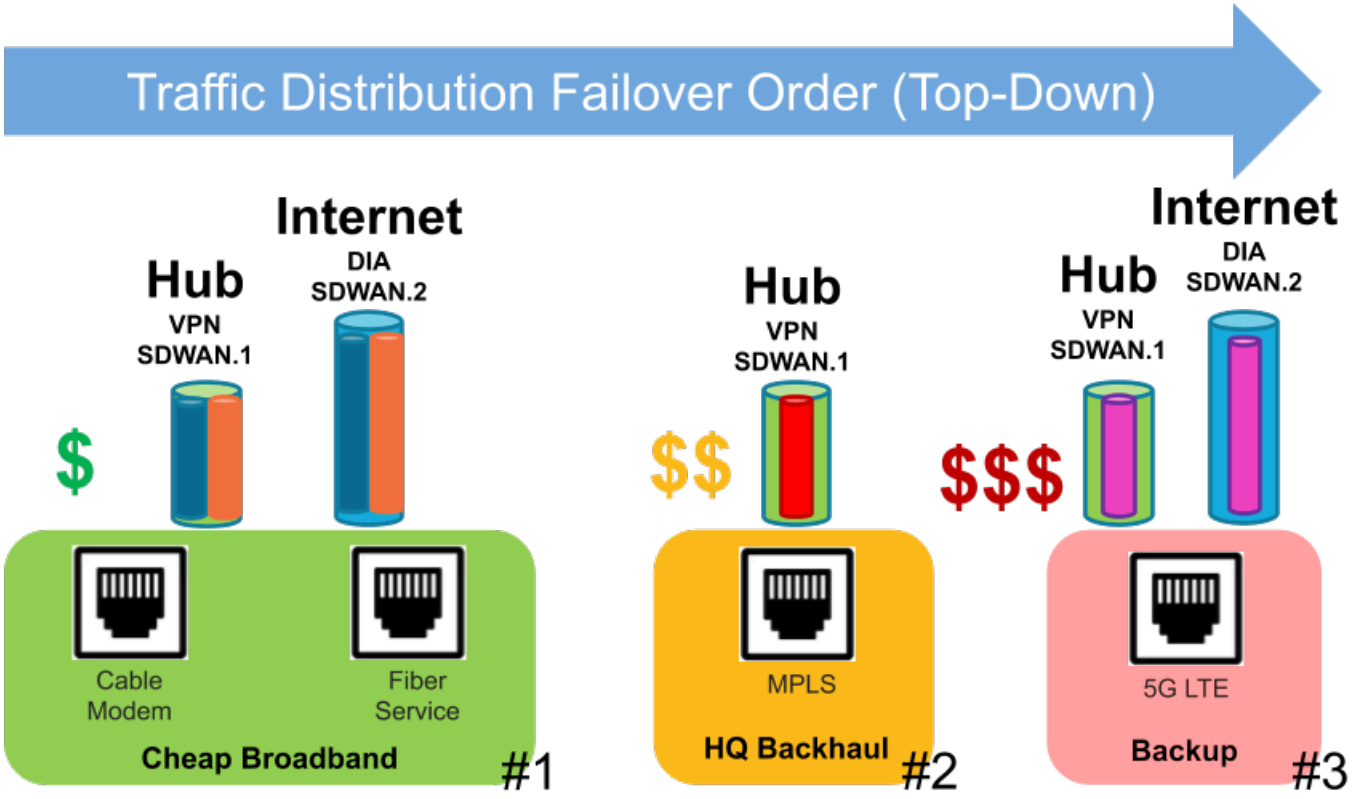
Condición de ruta	Prioridad de arriba hacia abajo	Mejor ruta disponible	Distribución de sesión ponderada
Se produce un error en la sesión de la ruta existente en un umbral de estado de ruta (caída de tensión).	Se realiza una conmutación por error de una sesión afectada a una mejor ruta (si está disponible).	Se realiza una conmutación por error de una sesión afectada a una mejor ruta (si está disponible).	No se realiza la conmutación por error de las sesiones afectadas.
La ruta de arriba hacia abajo o mejor ruta disponible se recupera: la ruta existente es apta aún (buen estado).	La sesión afectada retrocede a la ruta anterior.	La sesión afectada permanece en la ruta existente y no retrocede.	No se realiza la conmutación por error de las sesiones afectadas.
De arriba hacia abajo o la mejor ruta disponible recuperada: se produce un error en la comprobación de estado de la ruta existente.	Todas las sesiones retroceden a la ruta anterior.	Las sesiones selectivas retroceden a la ruta anterior hasta que la ruta existente afectada se recupere.	No se realiza la conmutación por error de las sesiones afectadas.
La ruta existente está inactiva (apagón).	Se produce la conmutación por error de todas las sesiones en la siguiente ruta de la lista.	Se produce la conmutación por error de todas las sesiones en la siguiente mejor ruta.	Se produce la conmutación por error de todas las sesiones para las demás etiquetas según la configuración de ponderación.

Condición de ruta	Prioridad de arriba hacia abajo	Mejor ruta disponible	Distribución de sesión ponderada
La caída de tensión no tiene una ruta apta (mejor).	Elija la mejor ruta disponible.	Elija la mejor ruta disponible.	Elija la mejor ruta disponible.

Además, el cortafuegos realiza automáticamente el intercambio de carga de sesión entre los miembros de la interfaz de una sola etiqueta de enlace. Después de que esas interfaces se aproximen a los Mbps máximos, las nuevas sesiones fluirán a interfaces que tengan una etiqueta de enlace diferente (según el método de distribución de tráfico) si esas interfaces tienen mejores métricas de estado.

Condición de ruta	Prioridad de arriba hacia abajo	Mejor ruta disponible	Distribución de sesión ponderada
Varios enlaces con la misma etiqueta de SD-WAN.	Comparta la carga de sesión por igual entre los enlaces dentro de la etiqueta de SD-WAN.	Comparta la carga de la sesión en función de la mejor ruta dentro de la etiqueta de SD-WAN.	Comparta la carga de la sesión en función de la ponderación (porcentaje) asignada a la etiqueta de SD-WAN.
Varios enlaces con diferentes etiquetas de SD-WAN.	Comparta la carga de la sesión según la prioridad de la lista; cargue primero los enlaces en la primera etiqueta de SD-WAN.	Comparta la carga de la sesión en función de la mejor ruta desde todas las etiquetas de SD-WAN.	Comparta la carga de la sesión en función de la ponderación (porcentaje) asignada a las etiquetas de SD-WAN.

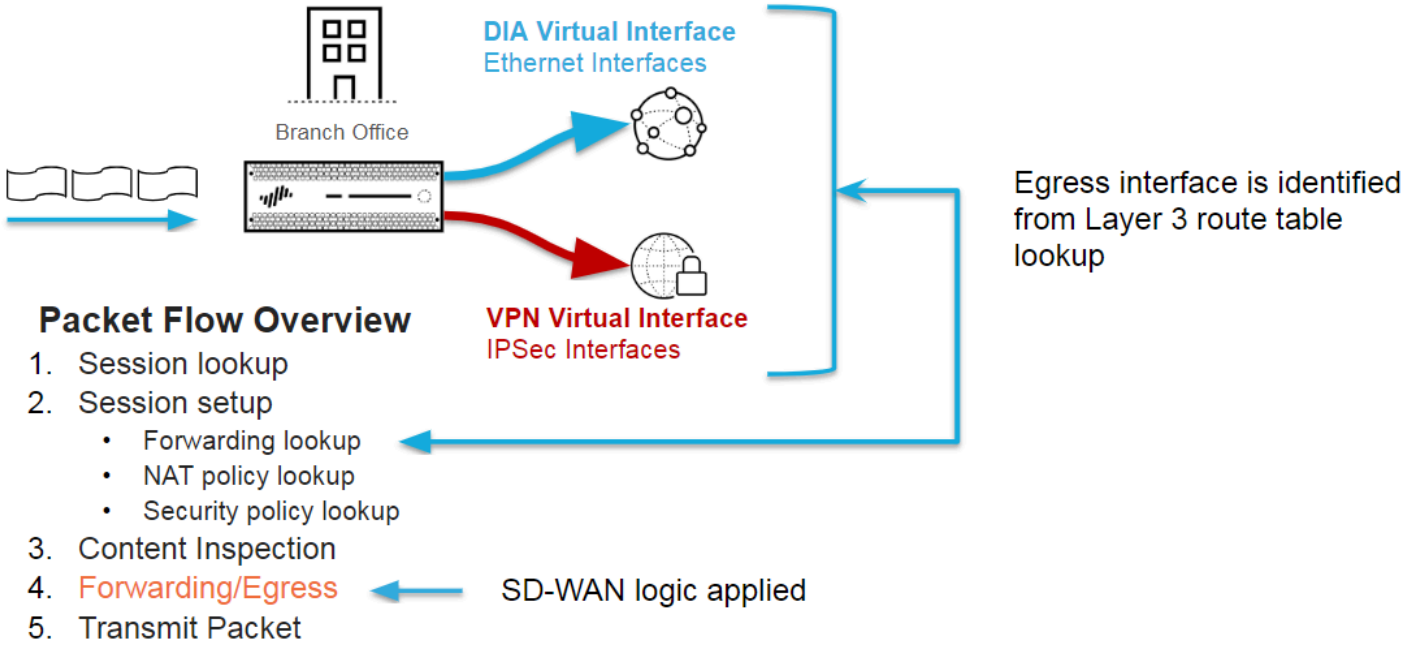
La siguiente figura muestra un ejemplo de un perfil de distribución de tráfico que utiliza el método Prioridad de arriba hacia abajo. Los n.° 1, n.° 2 y n.° 3 son el orden de las etiquetas de enlace de los enlaces que el cortafuegos examina, si es necesario, para detectar una ruta con buen estado para completar una conmutación por error en la sesión de la aplicación. Para cada evento de conmutación por error independiente que surja, el cortafuegos comenzará al principio de la lista de etiquetas de enlace de arriba hacia abajo.



1. En este ejemplo de prioridad de arriba hacia abajo, los paquetes de una sucursal con una aplicación específica (por ejemplo, office365-enterprise-access) llegan al cortafuegos. El cortafuegos utiliza la tabla de rutas para determinar el próximo salto al destino y la interfaz de salida, que es el túnel de la interfaz de SD-WAN virtual denominado sdwan.901. La regla de la política de seguridad permite los paquetes. Después, los paquetes coinciden con una regla de políticas de SD-WAN (denominada Office365 para Hub1) que especifica la zona de destino para la central. El cortafuegos utiliza el perfil de calidad de ruta de la regla de políticas de SD-WAN, el perfil de distribución de tráfico y las etiquetas de enlace de ese perfil para determinar qué miembro de la interfaz (enlace) de sdwan.901 utilizar. El perfil de distribución de tráfico enumera tres etiquetas de enlace en este orden: banda ancha barata n.° 1, sede de red de retorno n.° 2 y copia de seguridad n.° 3 (que es el orden de etiquetas de enlace en el que el cortafuegos examina los enlaces para buscar uno al que aplicar la conmutación por error).
2. Suponiendo que todas las rutas sean aptas (por el perfil de calidad de ruta), el cortafuegos distribuye los paquetes a uno de los enlaces físicos etiquetados con la primera etiqueta de enlace en la lista de perfiles de distribución de tráfico: Banda ancha barata. El túnel sdwan.901 tiene dos interfaces miembro (dos operadores): el túnel VPN del módem de cable y el túnel VPN del servicio de fibra. El cortafuegos primero examina un enlace por turnos y elige el primer enlace que encuentre que sea apto, por ejemplo, el enlace del módem de cable.
3. Si el primer enlace de banda ancha barata (cable módem) no es un enlace apto, el cortafuegos selecciona el segundo enlace de banda ancha barata (servicio de fibra).
4. Si el segundo enlace de banda ancha barata (servicio de fibra) no es un enlace apto, el cortafuegos selecciona el enlace etiquetado con la etiqueta de enlace de sede de red de retorno n.° 2, que es un enlace de MPLS de mayor coste a la misma central.

5. Si el enlace de MPLS no es un enlace apto, el cortafuegos selecciona el enlace etiquetado con la copia de seguridad de la etiqueta de enlace n.º 3, que es un enlace 5G LTE con un coste aún mayor a la misma central.
6. Si el cortafuegos no encuentra un enlace apto al que aplicar la conmutar por error, utiliza el método de mejor disponible para seleccionar un enlace.
7. Al comienzo de un nuevo evento de conmutación por error, el cortafuegos comienza por la parte superior de la lista de arriba hacia abajo de etiquetas de enlace para encontrar un enlace en el que realizar la conmutación por error.

Tenga en cuenta que la distribución del tráfico de SD-WAN es uno de los pasos posteriores en la lógica del flujo de paquetes. Alejémonos para ver una vista más amplia del flujo de paquetes.

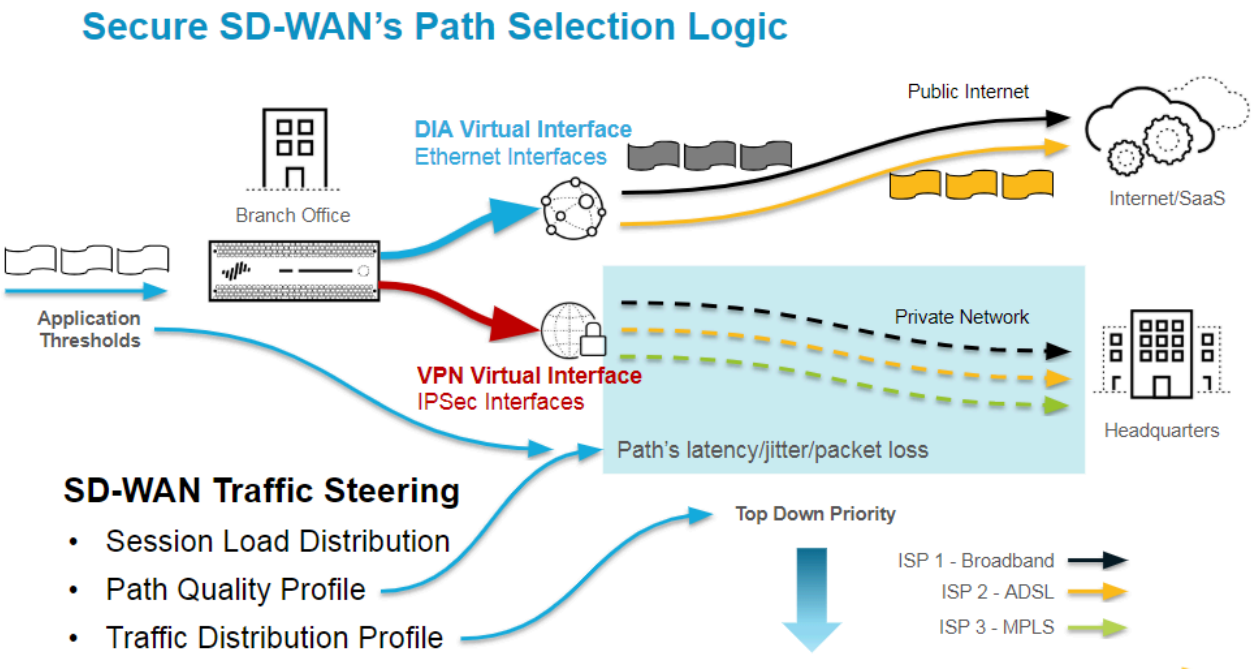


Los detalles del flujo de paquetes para la figura son los siguientes:

1. Cuando una sesión para una aplicación llega al cortafuegos, este realiza una búsqueda de sesión para determinar si la sesión es una sesión existente o una nueva sesión.
2. Una nueva sesión pasa por la configuración de la sesión:
    1. Búsqueda de reenvío: el cortafuegos obtiene la zona de salida, la interfaz de salida y el sistema virtual de la tabla de ruta de capa 3, la búsqueda de la base de datos de reenvío de capa 2, etc. Para las aplicaciones que coinciden con una regla de políticas de SD-WAN, el cortafuegos utiliza la interfaz virtual de SD-WAN como interfaz de salida.
    2. Búsqueda de política de NAT: si la sesión coincide con una regla de NAT, el cortafuegos realiza otra búsqueda de reenvío para determinar la interfaz y zona de salida final (traducida).
    3. Búsqueda de política de seguridad: si una regla de la política de seguridad permite la sesión, esta se crea e instala en la tabla de sesión. El cortafuegos luego realiza una clasificación adicional mediante App-ID™ y User-ID™.

3. Inspección de contenido: el cortafuegos realiza una inspección de amenazas (antispyware para IPS [Protección de vulnerabilidad], antivirus, filtrado de URL, WildFire®, etc.) en la carga útil y los encabezados según sea necesario.
4. La etapa de reenvío/salida realiza la selección de ruta y reenvía los paquetes. Esta etapa es donde se produce la selección de ruta de SD-WAN.
    1. Proceso de reenvío de paquetes: el cortafuegos utiliza la interfaz de ingreso para determinar el dominio de reenvío; realiza el enrutamiento, la conmutación o el reenvío virtual de cables.
    2. La selección de ruta de SD-WAN se produce cuando la aplicación coincide con una regla de políticas de SD-WAN; el perfil de calidad de ruta determina la elegibilidad de ruta; el perfil de distribución de tráfico determina el método de selección de ruta y el orden en que se consideran las rutas durante la selección.
    3. El cifrado de túnel VPN de IPSec/SSL se produce si es necesario.
    4. Proceso de salida de paquetes: se aplica la configuración de QoS, la reescritura de DSCP y la fragmentación de IP (si es necesario).
5. Paquete de transmisión: el cortafuegos reenvía el paquete a través de la interfaz de salida seleccionada.

Ahora volvemos a acercarnos para examinar la lógica de selección de ruta de SD-WAN con más detalle.



1. El cortafuegos consulta la tabla de rutas durante la búsqueda de reenvío; en función de la dirección IP de destino que coincide con un prefijo de capa 3, el cortafuegos determina la interfaz virtual de salida de SD-WAN. El paquete se dirige directamente a Internet público o regresa a la central a través de un enlace de VPN seguro.
2. El cortafuegos supervisa cada ruta realizando comprobaciones de estado que se ejecutan en un túnel VPN. Cada circuito DIA tiene un túnel VPN que supervisa la información de estado.

3. La aplicación en la regla de políticas de SD-WAN está asociada a un perfil de calidad de ruta, y el cortafuegos compara los valores de latencia, vibración y pérdida de paquetes medios reales de la ruta con los valores de umbral.
4. No se selecciona ninguna ruta que tenga un valor de latencia, vibración o pérdida de paquetes mayor que el umbral.
5. Todas las rutas aptas en la interfaz de SD-WAN virtual están sujetas al método del perfil de distribución de tráfico y a la lógica de prioridad de ruta (ordenación). Las etiquetas de enlace de SD-WAN agrupan los servicios de ISP, y el orden de esas etiquetas en el perfil de distribución de tráfico prioriza las rutas durante la selección de ruta.
6. Por lo tanto, el perfil de calidad de ruta y el perfil de distribución de tráfico determinan la siguiente mejor ruta que usar y el cortafuegos reenvía el tráfico fuera de ese enlace.

Creación de un perfil de distribución de tráfico

En función de su plan de configuración SD-WAN, cree el Perfiles de distribución del tráfico de SD-WAN que necesite en función de cómo desee que las aplicaciones en sus reglas de políticas de SD-WAN se carguen en la sesión y se conmuten por error.

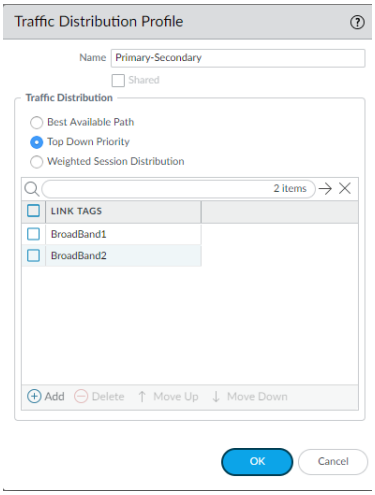
STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Asegúrese de haber configurado las etiquetas de enlace en un perfil de interfaz de SD-WAN y haberlas confirmado y enviado. Las etiquetas de enlace deben enviarse a sus centrales y sucursales para que Panorama™ asocie correctamente las etiquetas de enlace que especifique en este perfil de distribución de tráfico a un perfil de interfaz de SD-WAN.

STEP 3 | Seleccione un **grupo de dispositivos**.

STEP 4 | Cree un perfil de distribución de tráfico.

1. Seleccione **Objetos** > **Gestión de enlaces de SD-WAN** > **Perfil de distribución de tráfico**.
2. **Añada** un perfil de distribución de tráfico por **nombre** con un máximo de 31 caracteres alfanuméricos.



3. Seleccione **Compartido** solo si desea utilizar este perfil de distribución de tráfico en todos los grupos de dispositivos (tanto centrales como sucursales).
4. Seleccione un método de distribución de tráfico y añada un máximo de cuatro etiquetas de enlace que usen este método para este perfil.

   - **Mejor ruta disponible**: **añada** una o más **etiquetas de enlace**. Durante los intercambios iniciales de paquetes, antes de que App-ID clasifique la aplicación en el paquete, el cortafuegos usará la ruta en la etiqueta que tenga las mejores métricas de estado (según el orden de las etiquetas). Después de que el cortafuegos identifique la aplicación, compara el estado (calidad de ruta) de la ruta que estaba usando con el estado de la primera ruta (interfaz) en la primera etiqueta de enlace. Si el estado de la ruta original es mejor, seguirá siendo la ruta seleccionada; de lo contrario, el cortafuegos reemplazará a la ruta original. El cortafuegos repite este proceso hasta que se evalúen todas las rutas en la etiqueta de enlace. La ruta final es la ruta que selecciona el cortafuegos cuando llega un paquete que cumple con los criterios de coincidencia.

     *Cuando un enlace deja de ser apto y debe conmutar por error a la siguiente mejor ruta, el cortafuegos puede migrar un máximo de 1000 sesiones por minuto desde el enlace no apto a la siguiente mejor ruta. Por ejemplo, supongamos que tunnel.901 tiene 3000 sesiones; 2000 de esas sesiones coinciden con la regla de políticas de SD-WAN A y 1000 con la regla de políticas de SD-WAN B (ambas reglas tienen una política de distribución de tráfico configurada con **Mejor ruta disponible**). Si tunnel.901 no es apto, tarda tres minutos en migrar las 3000 sesiones desde el enlace no apto a la siguiente mejor ruta.*

   - **Prioridad de arriba hacia abajo**: **añada** una o más **etiquetas de enlace**. El cortafuegos distribuye nuevas sesiones (que cumplen con los criterios de coincidencia) a los enlaces mediante el orden de arriba a abajo de las **etiquetas de enlace** que añadió. El cortafuegos examina la primera etiqueta configurada para este perfil y las rutas que

usan esa etiqueta. Para ello, selecciona la primera ruta apta que encuentra (por debajo del umbral de calidad de ruta para esa regla). Si no se encuentra una ruta apta en esa etiqueta de enlace, el cortafuegos examina las rutas que usan la siguiente etiqueta de enlace. Si el cortafuegos no encuentra ninguna ruta después de examinar todas las rutas en todas las etiquetas de enlace, utiliza el método **Mejor ruta disponible**. La primera ruta seleccionada es la ruta preferida hasta que se supera uno de los umbrales de calidad de la ruta para esa ruta, momento en el que el cortafuegos comienza nuevamente en la parte superior de la lista de etiquetas de enlace para encontrar la nueva ruta preferida.

*Si solo tiene un enlace en la central, ese enlace es compatible con todas las interfaces virtuales y el tráfico DIA. Si desea utilizar los tipos de enlaces en un orden específico, debe aplicar un perfil de distribución de tráfico a la central que especifique la **prioridad de arriba hacia abajo** y, luego, ordenar las etiquetas de enlace para especificar el orden preferido. Si aplica un perfil de distribución de tráfico que, en su lugar, especifica la **mejor ruta de acceso disponible**, el cortafuegos utilizará el vínculo independientemente del costo para elegir la ruta de acceso de mejor rendimiento a la sucursal. En resumen, las etiquetas de enlace en un perfil de distribución de tráfico, la etiqueta de enlace aplicada a una* interfaz virtual de central *y una **métrica de conmutación por error de VPN** en un perfil de interfaz de SD-WAN funcionan solo cuando el perfil de distribución de tráfico especifica la **prioridad de arriba hacia abajo**.*

- **Distribución de sesión ponderada**: **añada** una o más **etiquetas de enlace** y, a continuación, especifique el porcentaje de **ponderación** de cada **etiqueta de enlace** para que el total de la ponderación sea del 100 %. El cortafuegos realiza la distribución de carga de sesión entre las etiquetas de enlace hasta que se alcanzan sus porcentajes máximos. Si hay más de una ruta en la etiqueta de enlace, el cortafuegos se distribuye equitativamente mediante la distribución por turnos hasta que se

alcanzan las métricas de estado de la ruta y, a continuación, distribuye sesiones a los otros miembros que no están en el límite.

Si varias interfaces físicas tienen la misma etiqueta, el cortafuegos distribuye las sesiones coincidentes de manera uniforme entre ellas. Si todas las rutas fallan con un umbral de estado (caída de tensión), el cortafuegos selecciona la ruta que tiene las mejores estadísticas de estado. Si no hay enlaces de SD-WAN disponibles (quizás debido a un apagón), el cortafuegos usa un enrutamiento estático o dinámico para enrutar los paquetes coincidentes.

Si un paquete se enruta a una interfaz de SD-WAN virtual, pero el cortafuegos no puede encontrar una ruta preferida para la sesión basada en el perfil de distribución de tráfico de la política de SD-WAN, el cortafuegos utiliza implícitamente el método Mejor ruta disponible para encontrar la ruta preferida. El cortafuegos distribuye cualquier sesión de aplicación que no coincida con una regla de políticas de SD-WAN basada en la regla final implícita del cortafuegos, que distribuye las sesiones por turnos entre todos los enlaces disponibles, independientemente del perfil de distribución de tráfico.

Si prefiere controlar cómo el cortafuegos distribuye sesiones no coincidentes, cree una regla final general para Distribución de sesiones no coincidentes a enlaces específicos en el orden que especifique.

5. (Opcional) Después de añadir etiquetas de enlace, use las flechas **Mover arriba** o **Mover abajo** para cambiar el orden de las etiquetas en la lista para que reflejen el orden en el que desea que el cortafuegos use enlaces para este perfil y para las aplicaciones seleccionadas en la regla de políticas de SD-WAN.
6. Haga clic en **OK (Aceptar)**.

STEP 5 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

STEP 6 | **Commit (Confirmar)** los cambios.

Creación de un perfil de corrección de errores

La corrección de errores de reenvío (FEC, Forward Error Correction) es un método que permite corregir ciertos errores de transmisión de datos que se producen en líneas de comunicación ruidosas, por lo que se mejora así la fiabilidad de los datos sin que sea necesaria la retransmisión. La FEC es útil para aplicaciones sensibles a la pérdida o daños de paquetes, como audio, VoIP y videoconferencias. Con FEC, el cortafuegos receptor puede recuperar paquetes perdidos o dañados mediante bits de paridad que el codificador de envío incrusta en un flujo de aplicación. La reparación del flujo evita la necesidad de que los datos de SD-WAN realicen la conmutación por error a otra ruta o de que TCP reenvíe los paquetes. FEC también puede ayudar con las aplicaciones UDP mediante la recuperación de los paquetes perdidos o dañados, ya que UDP no retransmite los paquetes.

La FEC de SD-WAN admite cortafuegos de sucursales y centrales que actúan como codificadores y descodificadores. El mecanismo de FEC permite que el codificador añada bits redundantes a un flujo de bits. Además, el descodificador usa esa información para corregir los datos recibidos, si es necesario, antes de enviarlos al destino.

SD-WAN también admite la duplicación de paquetes como método alternativo de corrección de errores. En la duplicación de paquetes se realiza una duplicación completa de una sesión de aplicación de un túnel a un segundo túnel. La duplicación de paquetes requiere más recursos que FEC y debe usarse solo para aplicaciones críticas que tengan baja tolerancia a los paquetes descartados.

Las aplicaciones modernas que disponen de sus propios mecanismos de recuperación integrados pueden no necesitar FEC o duplicación de paquetes. Aplique la FEC o la duplicación de paquetes solo en aplicaciones que realmente puedan beneficiarse de dicho mecanismo; de lo contrario, se añadirá mucho ancho de banda adicional y se sobrecargará la CPU sin que se produzca ningún beneficio. Ni la FEC ni la duplicación de paquetes son útiles si su problema de SD-WAN es la congestión.

Las funcionalidades de FEC y de duplicación de paquetes requieren que Panorama ejecute PAN-OS 10.0.2 o una versión posterior y el complemento SD-WAN 2.0 o una versión posterior compatible con la versión PAN-OS. El codificador y el descodificador deben utilizar PAN-OS 10.0.2 o una versión posterior. Si una sucursal o central utiliza una versión de software más antigua que la requerida, se descarta el tráfico con un encabezado de duplicación de paquetes o FEC en ese cortafuegos.

A partir de PAN-OS 10.0.3, FEC y la duplicación de paquetes se admiten en una topología de malla completa, además de la topología de central ya admitida.

No se debe utilizar FEC ni la duplicación de paquetes en enlaces DIA; solo están destinados a enlaces de túnel VPN entre una sucursal y una central.

FEC y la duplicación de paquetes solo es compatible con cortafuegos PAN-OS habilitados para SD-WAN. FEC y la duplicación de paquetes no es compatible con las centrales de Prisma Access.

Para configurar FEC o la duplicación de paquetes en el codificador (el lado que inicia FEC o la duplicación de paquetes), use Panorama para:

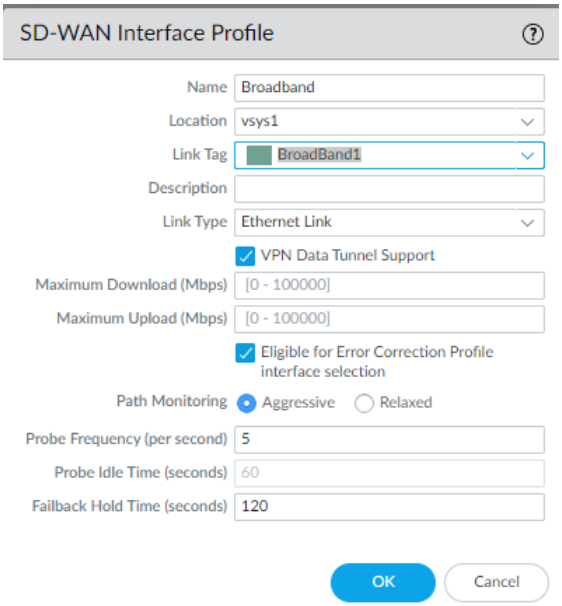
- Crear un perfil de interfaz SD-WAN que especifique **Eligible for Error Correction Profile interface selection (Elegible para la selección de la interfaz del perfil de corrección de errores)** y aplique el perfil a una o más interfaces.
- Crear un perfil de corrección de errores para implementar FEC o la duplicación de paquetes.
- Aplique el perfil de corrección de errores a una regla de políticas SD-WAN y especifique una única aplicación específica a la que aplica la regla.
- Enviar la configuración a los codificadores. (El descodificador [el lado receptor] no requiere una configuración específica para FEC o duplicación de paquetes; los mecanismos están habilitados de forma predeterminada en el descodificador siempre que el codificador inicie la corrección de errores).

FEC y la duplicación de paquetes admiten una MTU de 1340 bytes. Si el paquete es superior a esa cantidad, no pasará por el proceso de duplicación de paquetes o FEC.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Configuración de un perfil de la interfaz de SD-WAN, donde selecciona **Eligible for Error Correction Profile interface selection (Elegible para la selección de la interfaz del perfil de corrección de errores)** para indicar que el cortafuegos puede usar automáticamente las interfaces (donde se aplica el perfil de interfaz SD-WAN) para la corrección de errores. Si esta opción está seleccionada de forma predeterminada o no, depende del **tipo de enlace** que seleccione para el perfil.

*Puede desmarcar **Eligible for Error Correction Profile interface selection (Elegible para la selección de la interfaz del perfil de corrección de errores)** en un perfil y aplicar el perfil a un enlace 5G LTE costoso, por ejemplo, para que nunca se realice una costosa corrección de errores en ese enlace.*



STEP 3 | Configuración de una interfaz Ethernet física para SD-WAN y aplique el perfil de interfaz SD-WAN que creó a una interfaz Ethernet.

STEP 4 | Crear un perfil de corrección de errores para FEC o la duplicación de paquetes.

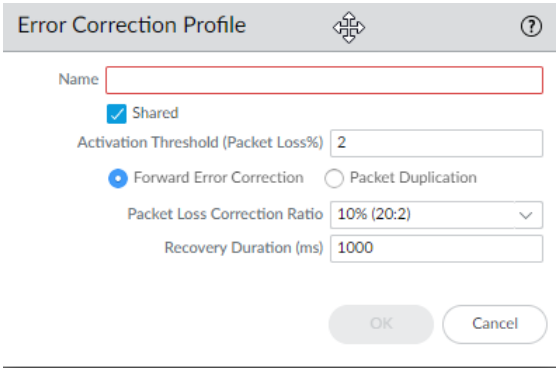
1. Seleccione **Objects (Objetos)** > **SD-WAN Link Management (Gestión de enlaces SD-WAN)** > **Error Correction Profile (Perfil de corrección de errores)**.
2. **Añada** un perfil de corrección de errores y especifique un **nombre** de hasta 31 caracteres alfanuméricos; por ejemplo, EC_VOIP.
3. Seleccione **Shared (Compartido)** para que el perfil de corrección de errores esté disponible para todos los grupos de dispositivos en Panorama y para los sistemas virtuales múltiples predeterminados en una central o sucursal de un solo sistema virtual múltiple, o para el vsys1 en una central o sucursal de varios sistemas virtuales múltiples al que envíe esta configuración.
4. Especifique la configuración **Activar cuando la pérdida de paquetes exceda (%)**: cuando la pérdida de paquetes excede este porcentaje, FEC o duplicación de paquetes se activa

para las aplicaciones configuradas en la regla de política SD-WAN donde se aplica este perfil de corrección de errores. El intervalo es de 1 a 99; el valor predeterminado es 2.

5. Seleccione **Forward Error Correction (Corrección de errores de reenvío)** o **Packet Duplication (Duplicación de paquetes)** para indicar qué método de corrección de errores utiliza el cortafuegos cuando una regla de políticas SD-WAN hace referencia a este perfil de interfaz SD-WAN; el valor predeterminado es Forward Error Correction (Corrección de errores de reenvío). Si selecciona la duplicación de paquetes, SD-WAN selecciona una interfaz a través de que enviar paquetes duplicados. (SD-WAN selecciona una de las interfaces que configuró con **Eligible for Error Correction Profile interface selection [Elegible para la selección de la interfaz del perfil de corrección de errores]** en el paso anterior).
6. (Solo en corrección de errores de reenvío) Seleccione la **proporción de corrección de pérdida de paquetes**: **10 % (20:2)**, **20 % (20:4)**, **30 % (20:6)**, **40 % (20:8)** o **50 % (20:10)**: proporción entre los bits de paridad para paquetes de datos; el valor predeterminado es 10 % (20:2). Cuanto mayor sea la relación entre los bits de paridad y los paquetes de datos que envía el cortafuegos (codificador) emisor, mayor será la probabilidad de que el cortafuegos receptor (descodificador) pueda reparar la pérdida de paquetes. Sin embargo, una relación más alta requiere más redundancia y, por lo tanto, más sobrecarga de ancho de banda, que es una compensación para lograr la corrección de errores. La relación de paridad se aplica al tráfico saliente del cortafuegos de codificación. Por ejemplo, si el índice de paridad del cortafuegos del central es del 50 % y el índice de paridad del cortafuegos de sucursal es del 20 %, el cortafuegos del central recibirá el 20 % y el cortafuegos de sucursal recibirá el 50 %.
7. Especifique la **duración de recuperación (ms)**: número máximo de milisegundos que el cortafuegos receptor (descodificador) puede dedicar a realizar la recuperación de paquetes en paquetes de datos perdidos mediante los paquetes de paridad que recibió; el intervalo es de 1 a 5000; el valor predeterminado es 1000. El cortafuegos envía inmediatamente los paquetes de datos que recibe al destino. Durante la Duración de la recuperación, el descodificador realiza la recuperación de paquetes para cualquier paquete de datos perdido. Cuando la duración de la recuperación expira, se liberan todos los paquetes de paridad. La duración de la recuperación se configura en el perfil de corrección de errores del codificador, que envía el valor de duración de la recuperación

al descodificador. Un ajuste de duración de recuperación en el descodificador no tiene ningún impacto.

Utilice primero la configuración predeterminada de duración de recuperación y ajústela si es necesario, según sus pruebas con caídas de tensión normales e intermitentes.



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

STEP 5 | Configuración de una regla de políticas de SD-WAN, haga referencia al **perfil de corrección de errores** que creó en la regla y especifique una aplicación crítica a la que aplica la regla.

Especifique solo una aplicación en la regla de políticas SD-WAN cuando configure FEC o la duplicación de paquetes. No debe combinar varias aplicaciones en una sola regla de políticas para FEC o la duplicación de paquetes.

STEP 6 | **Commit (Confirmar)**y **Commit and Push (Confirmar y enviar)** los cambios de configuración a los cortafuegos de codificación (sucursales y centrales).

Configuración de una regla de políticas de SD-WAN

Una regla de políticas de SD-WAN especifica las aplicaciones o servicios y un perfil de distribución de tráfico para determinar cómo el cortafuegos selecciona la ruta preferida para un paquete entrante que no pertenece a una sesión existente y que coincide con todos los demás criterios, como las zonas de origen y destino, las direcciones IP de origen y destino y el usuario de origen. La regla de políticas de SD-WAN también especifica un perfil de calidad de ruta de umbrales para latencia, fluctuación de fase y pérdida de paquetes. Cuando se excede uno de los umbrales, el cortafuegos selecciona una nueva ruta para las aplicaciones o servicios.

Cuando supervise el tráfico de SD-WAN, el tráfico que se origina en un origen detrás del dispositivo de la central se evalúa con respecto a las políticas de SD-WAN enviadas al dispositivo de la central cuando entra en el dispositivo de la sucursal, y puesto que la decisión de selección de ruta ya se ha tomado, el dispositivo de la sucursal no evalúa el tráfico con respecto a sus políticas de SD-WAN a medida que pasa a través del dispositivo de la sucursal al dispositivo de destino final. Por el contrario, el tráfico que se origina en un origen detrás del dispositivo de sucursal se evalúa según las políticas de SD-WAN enviadas al dispositivo de la sucursal y no el dispositivo de la central. El servidor de gestión Panorama™ añade los logs tanto de la central como de la sucursal y, para el mismo tráfico, se muestran dos entradas de sesión, pero solo el dispositivo de SD-WAN que evaluó originalmente el tráfico contendrá los detalles de SD-WAN.

En una regla de políticas SD-WAN, puede hacer referencia a un perfil de corrección de errores para poder aplicar la corrección de errores de reenvío (FEC, Forward Error Correction) o la duplicación de paquetes para aplicaciones críticas específicas que tengan una baja tolerancia para paquetes descartados o dañados.

En una regla de políticas de SD-WAN, especifique también los dispositivos a los que desee que Panorama envíe la regla.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Policies (Políticas)** > **SD-WAN** y seleccione el grupo de dispositivos del menú desplegable contextual **Device Group (Grupo de dispositivos)**.

STEP 3 | **Añada** una regla de políticas de SD-WAN.

STEP 4 | En la pestaña **General**, introduzca un nombre descriptivo para la regla en **Nombre**.

STEP 5 | En la pestaña **Origen**, configure los parámetros de origen de la regla de políticas.

1. Añada la **zona de origen** o seleccione **cualquier** zona de origen.
2. **Añada** una o más direcciones de origen, establezca una lista dinámica externa (EDL) o seleccione **cualquier** dirección de origen.
3. **Añada** uno o más usuarios de origen o seleccione **cualquier** usuario de origen.

STEP 6 | En la pestaña **Destino**, configure los parámetros de destino de la regla de políticas.

1. **Añada** la **zona de destino** o seleccione **cualquier** zona de destino.
2. **Añada** una o más direcciones de destino, establezca un EDL o seleccione **cualquier** dirección de destino.

STEP 7 | En la pestaña **Application/Service (Aplicación/Servicio)**, adjunte sus perfiles de gestión de enlaces SD-WAN y especifique sus aplicaciones y servicios.

PAN-OS 10.0.2 admite la asociación de solo un perfil de calidad de SaaS o una corrección de errores, pero no ambos. Si asocia uno de estos perfiles con una regla de políticas SD-WAN, no puede asociar el otro.

Por ejemplo, si asocia un perfil de calidad de SaaS con una regla de políticas SD-WAN, no podrá asociar un perfil de corrección de errores con la misma regla de políticas SD-WAN.

1. Seleccione la **calidad de la ruta** o Creación de un perfil de calidad de ruta.
2. Seleccione el **perfil de calidad de SaaS** o Creación de un perfil de calidad de SaaS si el cortafuegos de sucursal tiene un enlace de acceso directo a Internet (DIA, Direct Internet Access) a una aplicación SaaS. El valor predeterminado es **None (disabled) [Ninguno (deshabilitado)]**.
3. Seleccione el **perfil de conexión de errores** o Creación de un perfil de corrección de errores para aplicar la corrección de errores de reenvío (FEC, Forward Error Correction) o la duplicación de paquetes a las aplicaciones que coincidan con la regla de políticas SD-WAN. El valor predeterminado es **None (disabled) [Ninguno (deshabilitado)]**.
4. **Añada aplicaciones** y seleccione una o más aplicaciones de la lista, o seleccione **cualquier** aplicación. Todas las aplicaciones que seleccione están sujetas a los umbrales de estado especificados en el perfil de Calidad de ruta seleccionado. Si un paquete coincide con una de estas aplicaciones y esa aplicación supera uno de los umbrales de estado en el perfil de Calidad de ruta (y el paquete coincide con los criterios de la regla restante), el cortafuegos selecciona una nueva ruta preferida.

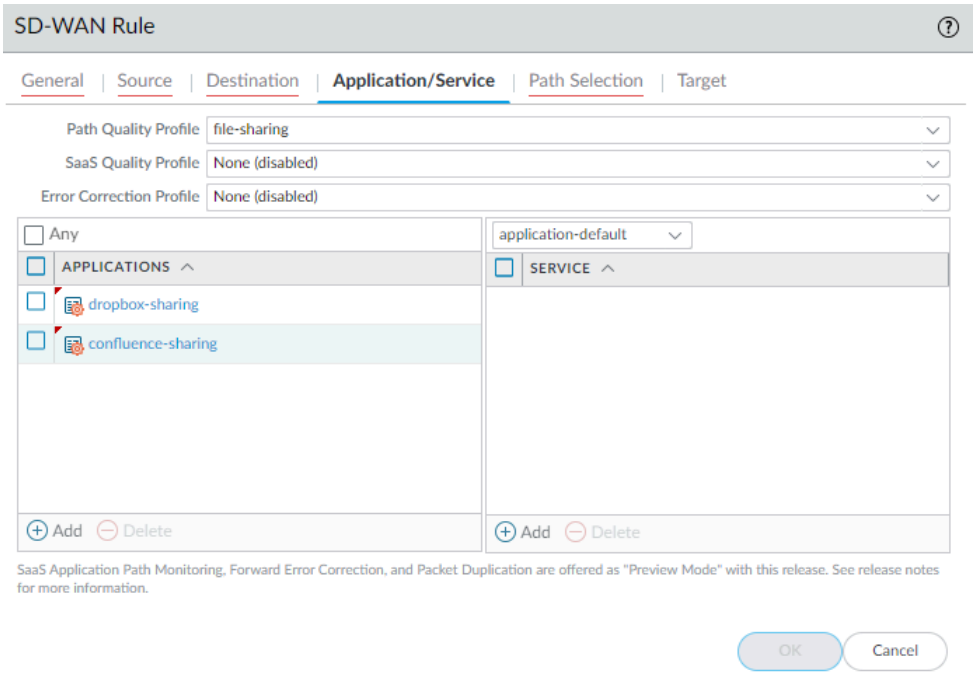
   Añada solo aplicaciones críticas para el negocio y aplicaciones que sean sensibles a las condiciones de ruta para su capacidad de uso.

   *Si asocia un perfil de calidad de SaaS en el modo **adaptativo** con la política SD-WAN, añada las aplicaciones SaaS específicas que desee supervisar. El uso de la supervisión adaptativa para todas las aplicaciones que coinciden con la regla de políticas SD-WAN puede afectar el rendimiento del cortafuegos SD-WAN.*

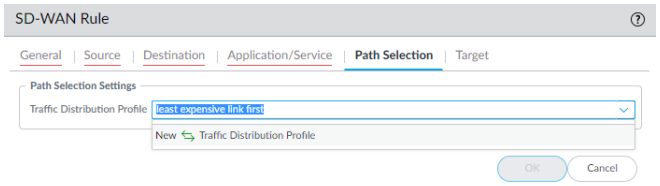
   Si asocia un perfil de calidad de SaaS con una aplicación SaaS específica, añada la aplicación SaaS a la regla SD-WAN para asegurarse de que la configuración de supervisión de SaaS se aplique solo a la aplicación SaaS deseada.
5. **Añada servicios** y seleccione uno o más servicios de la lista o seleccione **cualquier** servicio. Todos los servicios que seleccione están sujetas a los umbrales de estado especificados en el perfil de Calidad de ruta seleccionado. Si un paquete coincide con uno de estos servicios y ese servicio supera uno de los umbrales de estado en el

perfil de Calidad de ruta (y el paquete coincide con los criterios de la regla restante), el cortafuegos selecciona una nueva ruta preferida.

Añada solo servicios críticos para el negocio y servicios que sean sensibles a las condiciones de ruta para su capacidad de uso.

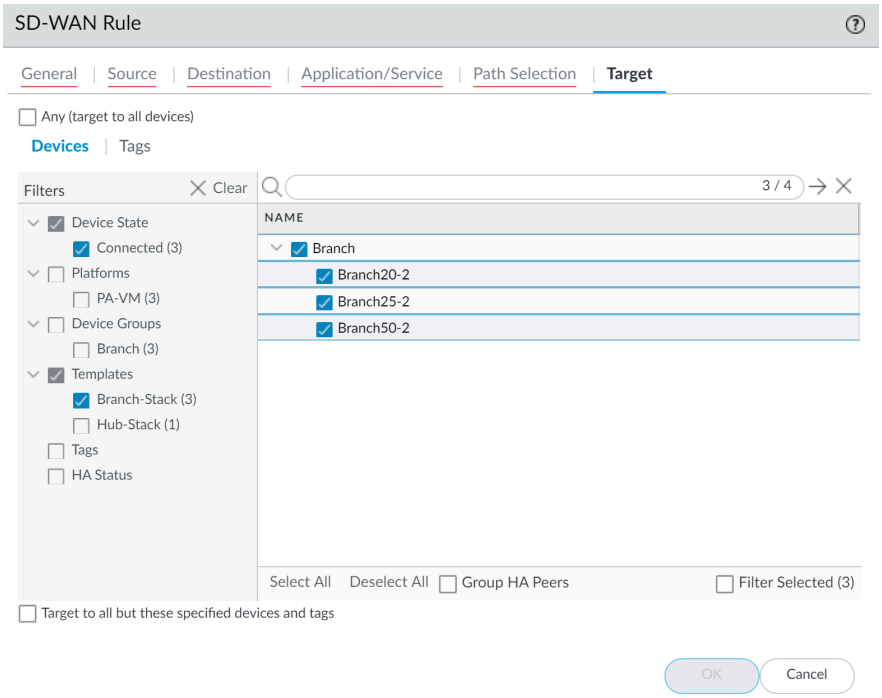


STEP 8 | En la pestaña **Path Selection (Selección de ruta)**, elija el perfil **Traffic Distribution (Distribución de tráfico)** o Creación de un perfil de distribución de tráfico. Cuando un paquete entrante (no asociado a una sesión) coincide con todos los criterios de coincidencia de la regla, el cortafuegos usa este perfil de Traffic Distribution (Distribución de tráfico) para seleccionar una nueva ruta preferida.

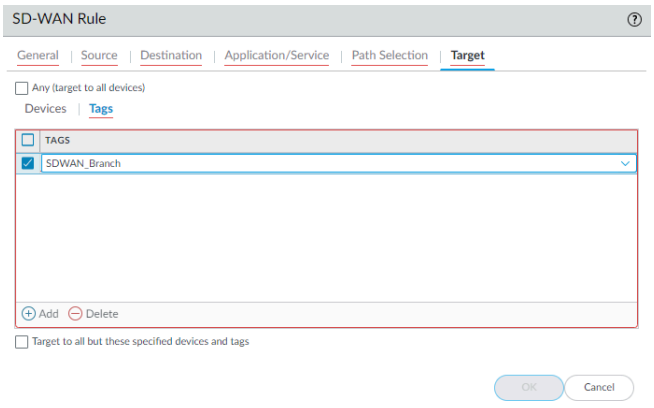


STEP 9 | En la pestaña **Destino**, use uno de los siguientes métodos para especificar los cortafuegos de destino en el grupo de dispositivos al que Panorama aplica la regla de políticas de SD-WAN:

- Seleccione **Cualquiera (destino para todos los dispositivos)** (valor predeterminado) para enviar la regla a todos los dispositivos. También puede seleccionar **Dispositivos** o **Etiquetas** para especificar los dispositivos a los que Panorama aplica la regla de políticas de SD-WAN.
- En la pestaña **Devices (Dispositivos)**, seleccione uno o más filtros para restringir las selecciones que aparecen en el campo Name (Nombre), luego seleccione uno o más dispositivos en los que Panorama aplique la regla, como en este ejemplo:



- En la pestaña **Tags (Etiquetas)**, **añada** una o más **etiquetas** y seleccione las etiquetas para especificar que Panorama aplica la regla a los dispositivos que están etiquetados con las etiquetas seleccionadas, como en este ejemplo:



- Si especificó Dispositivos o Etiquetas, puede seleccionar **Destino para todos menos estos dispositivos y etiquetas especificados** para que Panorama envíe la regla de políticas de SD-WAN a todos los dispositivos excepto los dispositivos especificados o etiquetados.

STEP 10 | Haga clic en **OK (Aceptar)**.

STEP 11 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

STEP 12 | (Práctica recomendada) Cree una regla de políticas general de SD-WAN Distribución de sesiones no coincidentes para controlar qué enlaces usan las sesiones no coincidentes y ver sesiones no coincidentes en el log y los informes en el complemento de SD-WAN.

Si no crea una regla general para distribuir sesiones no coincidentes, el cortafuegos las distribuye por turnos entre todos los enlaces disponibles porque no hay ningún perfil de distribución de tráfico para sesiones no coincidentes. La distribución por turnos de sesiones no coincidentes puede aumentar sus costes inesperadamente y provocar la pérdida de visibilidad de la aplicación.

STEP 13 | Después de configurar las reglas de políticas de SD-WAN, cree una regla de la política de seguridad para permitir el tráfico (por ejemplo, **bgp** como **aplicación**) desde sucursales a Internet, desde sucursales a centrales o desde centrales a sucursales.

STEP 14 | (Opcional) Configure QoS para las aplicaciones críticas.

Si las aplicaciones de SD-WAN precisan capacidades de ancho de banda garantizadas o si no desea que otras aplicaciones tomen ancho de banda de aplicaciones empresariales críticas, cree reglas de QoS para controlar el ancho de banda correctamente.

STEP 15 | Para configurar automáticamente el enrutamiento de BGP entre los miembros del clúster de la VPN, en el complemento de SD-WAN, configure el enrutamiento de BGP entre sucursales y centrales para enrutar dinámicamente el tráfico que estará sujeto a la conmutación por error de SD-WAN y la carga compartida.

También, si desea configurar manualmente el enrutamiento de BGP en cada cortafuegos o usar una plantilla de Panorama independiente para configurar el enrutamiento de BGP para contar con un mayor control, deje en blanco la información de BGP en el complemento. En su lugar, configure el enrutamiento de BGP.

STEP 16 | Configure NAT para interfaces de SD-WAN virtuales orientadas al público.

Permiso para realizar la conmutación por error del tráfico de acceso a Internet directo en el enlace de MPLS

En una sucursal de SD-WAN, el cortafuegos realiza un túnel dividido para que cualquier aplicación que tenga una dirección IP pública seleccionen la interfaz de acceso directo a Internet (DIA) a Internet, y para que las aplicaciones que tengan direcciones IP privadas que pertenezcan a la central seleccionen la interfaz de la VPN . El cortafuegos realiza una conmutación por error automáticamente de las aplicaciones de DIA en la conexión privada de MPLS a la central cuando es necesario, por lo que el tráfico destinado a Internet toma una ruta alternativa a través de la central para llegar a Internet. Para permitir que esto funcione, debe realizar el siguiente procedimiento:

STEP 1 | Cree un enlace de MPLS entre su sucursal y la central. Cuando crea el perfil de la interfaz de SD-WAN, el tipo de enlace debe ser **MPLS** tanto para la central como para la sucursal.

STEP 2 | Si desea que el tráfico privado atraviese el túnel VPN, habilite **Compatibilidad del túnel de datos VPN** en el perfil de la interfaz de SD-WAN. Si deshabilita **Compatibilidad del túnel de datos VPN**, los datos privados saldrán del túnel VPN.

STEP 3 | Configuración de una regla de políticas de SD-WAN para aplicaciones específicas, Creación de un perfil de calidad de ruta y Creación de un perfil de distribución de tráfico que especifica el método**Prioridad de arriba hacia abajo**. El perfil Distribución de tráfico también debe especificar un enlace de **MPLS** como una de las opciones de conmutación por error (identificado por una etiqueta). Compruebe que las aplicaciones de la regla de políticas de SD-WAN hagan referencia a los perfiles correctos de Calidad de ruta y Distribución de tráfico, y que el perfil de Distribución de tráfico especifica Prioridad de arriba hacia abajo.

Después de habilitar Compatibilidad del túnel de datos VPN, tanto en la central como en la sucursal, y de que el enlace de MPLS esté operativo, el cortafuegos usará automáticamente la conexión de MPLS para realizar la conmutación por error del tráfico de DIA cuando sea necesario.

STEP 4 | En la configuración de la central, asegúrese de que esta tenga una ruta a Internet y que el enrutamiento esté configurado correctamente para que el tráfico de la central llegue a Internet.

El cortafuegos utiliza la interfaz virtual de DIA y la interfaz virtual de la VPN para garantizar que el tráfico público de Internet se mantenga separado del tráfico privado en la misma ruta; es decir, el tráfico de Internet y el tráfico privado no pasan por el mismo túnel VPN. La segmentación completa con una zonificación adecuada surte efecto al completo.

Configuración de AnyPath de DIA

Cuando se produce un apagón o una caída de tensión en los enlaces de acceso directo a Internet (DIA, Direct Internet Access) SD-WAN de un ISP, es necesario que esos enlaces realicen la conmutación por error en otro enlace para garantizar la continuidad de la empresa. Los enlaces DIA pueden realizar la conmutación por error en un enlace MPLS, pero es posible que no disponga de un enlace MPLS. Los enlaces DIA deben poder realizar la conmutación por error en otro enlace que tenga una ruta directa o una ruta indirecta (a través de un central o sucursal) a Internet; el tráfico DIA puede seleccionar *cualquier ruta* disponible para acceder a Internet sin que haya restricciones para DIA. AnyPath de DIA admite un enlace DIA que realiza la conmutación por error en un túnel VPN privado que va a un cortafuegos de central para acceder luego a Internet. Además, si su topología es de malla completa (sucursal a sucursal) y no hay una central, el tráfico DIA puede realizar la conmutación por error en un cortafuegos de sucursal para acceder a Internet.

AnyPath de DIA requiere PAN-OS 10.0.3 o una versión posterior de PAN-OS y la versión del complemento SD-WAN compatible, que se muestra en la tabla SD-WAN en la sección de complementos de Panorama de la Matriz de compatibilidad.

Existen varios casos de uso en los que se puede querer que un enlace de Internet realice la conmutación por error en un túnel VPN (AnyPath de DIA):

- Desea pasar de un enlace MPLS costoso a una o más conexiones públicas de Internet, generalmente de diferentes proveedores.
- Tiene varias centrales en un clúster de VPN para permitir una conmutación por error de tipo cascada desde el central principal a una sucesión de centrales de reserva.
- En un escenario de túnel dividido, solo desea que una aplicación determinada de uso intensivo de ancho de banda acceda directamente a Internet a través del enlace DIA de la sucursal en lugar de volver a la central del centro de datos a través del túnel VPN, lo que ahorra costes de ancho de banda WAN. En caso de un apagón o caída de tensión de DIA, el tráfico de esta aplicación conmuta por error en la central del centro de datos para acceder a Internet; si es necesario, puede realizar una conmutación por error en una segunda central para acceder a Internet.
- En un escenario diferente de túnel dividido, desea que la mayor parte de su tráfico de Internet salga del enlace DIA en lugar de devolver el tráfico al centro de datos para la caída de tensión de Internet. Sin embargo, desea que las aplicaciones específicas (que pueden necesitar un escaneo adicional o un registro de otro dispositivo de seguridad) regresen al centro de datos. Crea una regla de políticas SD-WAN para dirigir esas aplicaciones a una ruta principal a la central en lugar del enlace DIA normal según lo que determina la ruta predeterminada en la tabla de rutas del cortafuegos. En caso de una caída de tensión o un apagón, esas aplicaciones realizan una conmutación por error para seleccionar la interfaz DIA de la sucursal.

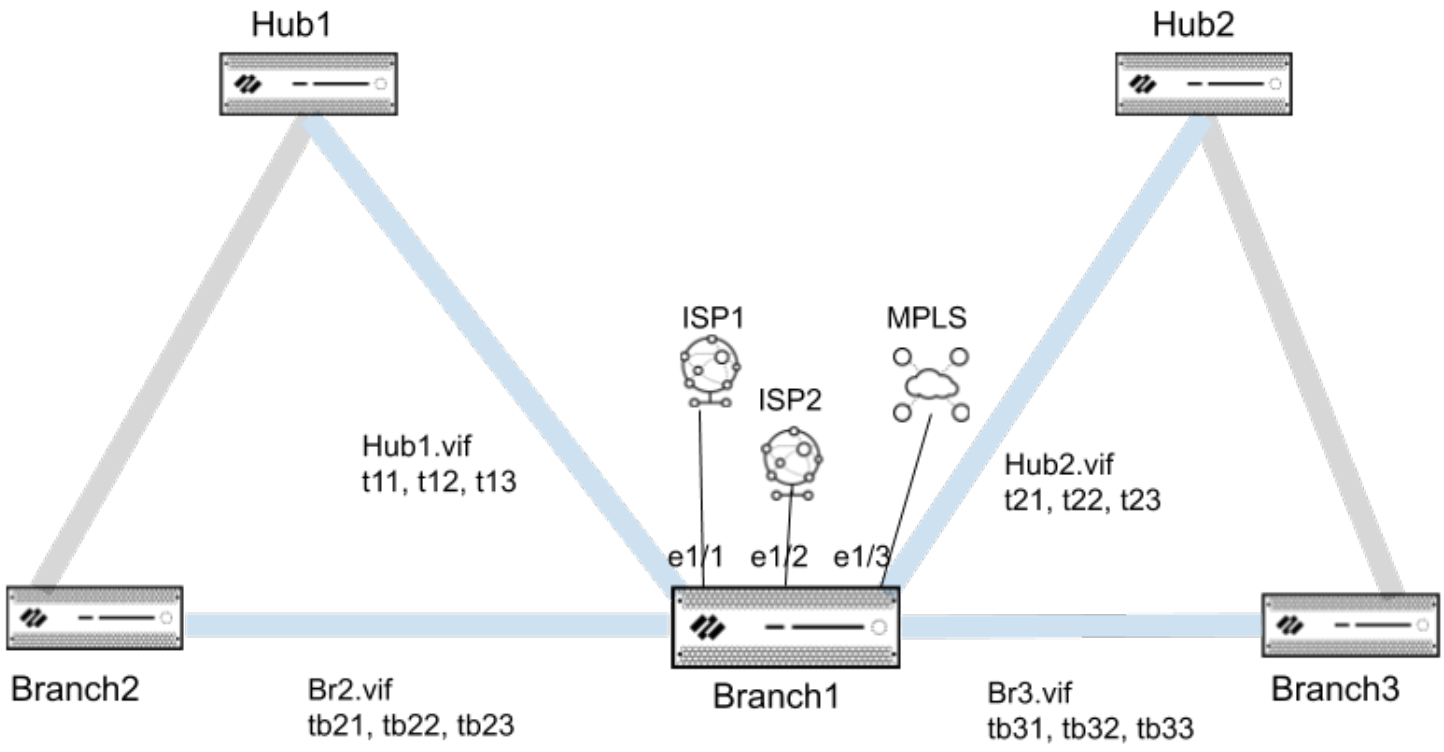
AnyPath de DIA introduce el concepto de una *interfaz virtual principal*, que puede incluir enlaces DIA e *interfaces virtuales de central* anidadas e *interfaces virtuales de sucursal* (túneles VPN) que incluyen sus propios enlaces. La interfaz virtual principal puede tener un máximo de nueve interfaces DIA (Ethernet) e interfaces virtuales de central y de sucursal. Asigna una etiqueta de enlace a una central cuando añade el dispositivo central a Panorama. Suponiendo que usa el complemento SD-WAN, la VPN automática asigna esa etiqueta de enlace a la interfaz virtual

de la central, lo que le permite especificar la etiqueta en un perfil de distribución de tráfico para controlar el orden de conmutación por error entre las interfaces virtuales.

A la interfaz virtual principal se le conoce como DIA-VIF en los comandos de la CLI.

Una interfaz virtual principal puede tener miembros de interfaz que pertenezcan a diferentes zonas de seguridad. Sin embargo, la práctica recomendada es que todas las interfaces miembro de la interfaz virtual principal pertenezcan a la misma zona de seguridad. Otra práctica recomendada es tener, al menos, una interfaz miembro en la interfaz virtual principal del tipo de enlace Ethernet, modo cable, ADSL, fibra, LTE o WiFi.

El siguiente ejemplo de topología muestra Branch1 (Sucursal1) con dos conexiones ISP y un enlace MPLS. Branch1 (Sucursal1) también tiene una interfaz virtual Hub1 (Central1) con tres túneles VPN que se conectan a Hub1 (Central1) y una interfaz virtual Hub2 (Central2) de tres túneles VPN que se conectan a Hub2 (Central2). Branch1 (Sucursal1) también tiene una interfaz virtual branch2 (sucursal2) con tres túneles VPN que se conectan a Branch2 (Sucursal2) y una interfaz virtual branch3 (sucursal3) con tres túneles VPN que se conectan a Branch3 (Sucursal 3). El objetivo de AnyPath de DIA es configurar el orden en el que DIA puede realizar la conmutación por error en los túneles VPN para acceder a Internet directa o indirectamente y así mantener la continuidad de la empresa.



Cuando configura una interfaz virtual principal, esta se convierte automáticamente en la ruta predeterminada para que el tráfico de Internet se enrute correctamente a cualquiera de los

miembros de la interfaz virtual principal (tanto enlaces DIA como túneles VPN). La selección de la ruta se basa en los perfiles de calidad de la ruta SD-WAN y los perfiles de distribución del tráfico, los que tendría que configurar para usar el método de distribución de prioridad de arriba hacia abajo para controlar el orden de la conmutación por error. En la topología de ejemplo, un perfil de distribución de tráfico puede mostrar primero la etiqueta de la interfaz virtual principal, después la etiqueta de la interfaz virtual Hub1 (Central1) y, finalmente, la etiqueta de la interfaz virtual Hub2 (Central2).

Si nos aproximamos a un nivel más profundo de prioridad de conmutación por error, una interfaz virtual de central dispone de varios miembros de túnel, por lo que necesita una forma de priorizar el orden de conmutación por error de los miembros, como la priorización de uso de un túnel VPN de banda ancha antes que un túnel VPN LTE. La prioridad se especifica mediante la **métrica de conmutación por error de VPN** en el perfil de interfaz SD-WAN que se aplica a la interfaz Ethernet. Cuanto menor sea el valor de la métrica, mayor será la prioridad para que el túnel se seleccione en caso de conmutación por error. En el ejemplo de topología, en la interfaz virtual de Hub1 (Central1), una métrica de conmutación por error de VPN más baja para t11 que para t12 hará que el tráfico de Internet realice la conmutación por error en t11 antes que en t12. Si hay varios túneles en una interfaz virtual que tienen la misma métrica, SD-WAN envía tráfico de sesión nuevo a los túneles por turnos.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Especifique la prioridad de la conmutación por error para un túnel VPN incluido en una interfaz virtual de central o de sucursal.

1. Seleccione o Configuración de un perfil de la interfaz de SD-WAN.

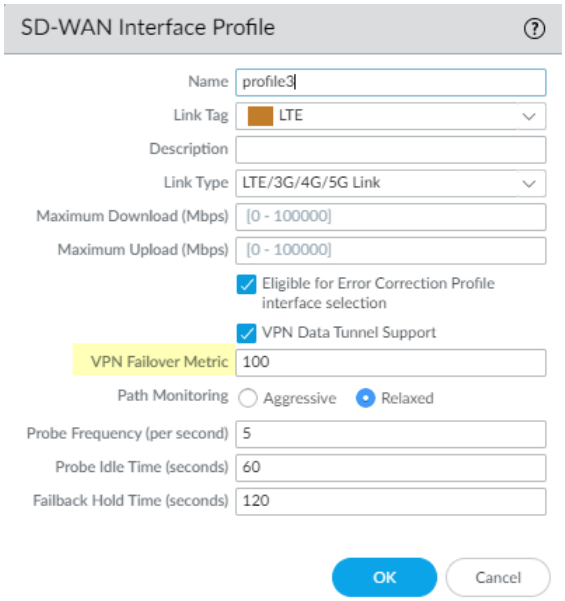
   La práctica recomendada es configurar, al menos, una interfaz con el tipo de enlace de Ethernet, módem por cable, ADSL, fibra, LTE o WiFi.

2. Debe habilitar **VPN Data Tunnel Support (Compatibilidad de túnel de datos de VPN)**.
3. Especifique la **métrica de conmutación por error de VPN** para el túnel VPN; el intervalo es de 1 a 65 535; el valor predeterminado es 10. Cuanto menor sea el valor de la métrica, mayor será la prioridad del túnel VPN (enlace) en la que aplica este perfil.

   Por ejemplo, establezca la métrica en un valor bajo y aplique el perfil a una interfaz de banda ancha; a continuación, cree un perfil diferente que establezca una métrica alta para

aplicar a una interfaz LTE costosa para garantizar que se use solo después de que la banda ancha haya fallado.

Si solo tiene un enlace en la central, ese enlace admite todas las interfaces virtuales y el tráfico de DIA. Si desea utilizar los tipos de enlaces en un orden específico, debe aplicar un perfil de distribución de tráfico a la central que especifique la ***prioridad de arriba hacia abajo*** *y, luego, ordenar las etiquetas de enlace para especificar el orden preferido. Si aplica un perfil de distribución de tráfico que, en su lugar, especifica la* ***mejor ruta de acceso disponible****, el cortafuegos utilizará el vínculo independientemente del costo para elegir la ruta de acceso de mejor rendimiento a la sucursal. En resumen, vincule etiquetas en un perfil de distribución de tráfico. La etiqueta de vínculo aplicada a una interfaz virtual de central (paso 6 de esta tarea) y una* ***métrica de conmutación por error de VPN*** *solo funcionan cuando el perfil de distribución de tráfico especifica la* ***prioridad de arriba hacia abajo.***



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

STEP 3 | Configuración de una interfaz Ethernet física para SD-WAN y en la pestaña SD-WAN, aplique el perfil de la interfaz SD-WAN que creó en el paso anterior.

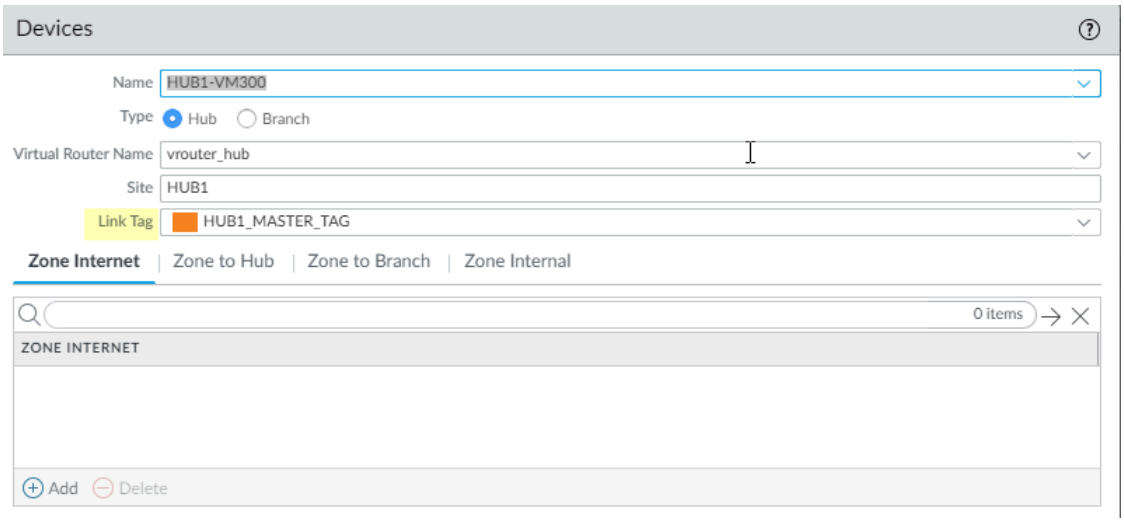
La práctica recomendada es que todas las interfaces de la interfaz virtual principal pertenezcan a la misma zona de seguridad.

STEP 4 | Repita los pasos 2 y 3 para configurar perfiles de la interfaz SD-WAN adicionales con una métrica de conmutación por error de VPN diferente y aplique los perfiles a diferentes interfaces Ethernet para determinar el orden en el que se produce la conmutación por error en los enlaces.

STEP 5 | Creación de una etiqueta de enlace para una interfaz virtual de central.

STEP 6 | Añada la etiqueta de enlace a un centro que desee que participe en AnyPath de DIA.

1. En **Panorama** > **SD-WAN** > **Devices (Dispositivos)**, Adición de un dispositivo de SD-WAN para añadir una central que gestione Panorama.
2. Seleccione la central.
3. Seleccione la **etiqueta de enlace** que creó en el paso anterior, que la VPN automática aplica a toda la interfaz virtual de la central, no a un enlace individual. Por lo tanto, puede hacer referencia a esta etiqueta de enlace en el perfil de distribución de tráfico para indicar la interfaz virtual de la central para la orden de conmutación por error para AnyPath de DIA. En el dispositivo de sucursal, Auto VPN (VPN automática) usa esa etiqueta para completar el campo Link Tag (Etiqueta de enlace) en la interfaz virtual SD-WAN que termina en el dispositivo de la central.



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

STEP 7 | Repita los pasos 5 y 6 para crear una etiqueta de enlace para cada interfaz virtual de central y añada la etiqueta a las centrales que participarán en AnyPath de DIA. Realice el mismo procedimiento con cualquier interfaz virtual de sucursal.

STEP 8 | Cree un perfil de distribución de tráfico para implementar AnyPath de DIA.

1. Creación de un perfil de distribución de tráfico.
2. Seleccione **Top Down Priority (Prioridad de arriba hacia abajo)**.
3. Añada las etiquetas de enlace para que aparezcan en el orden en que desee que se usen sus enlaces asociados para la conmutación por error.

   Por ejemplo, si en su caso de uso quiere que ciertas aplicaciones usen DIA primero, enumere primero la etiqueta DIA, después una etiqueta de interfaz virtual de central y, posteriormente, una segunda etiqueta de interfaz virtual de central. Si en su caso de uso quiere que ciertas aplicaciones vayan primero a la central y después a Internet, enumere primero una interfaz virtual de central y, después, quizás, una segunda. Finalmente, enumere una etiqueta DIA. Si tiene una malla completa sin central, use la etiqueta DIA y las etiquetas de la interfaz virtual de sucursal en el orden que desee.

STEP 9 | Cree perfiles de calidad SaaS con el mismo nombre para los cortafuegos de central y de sucursal.

Se deben configurar dos perfiles de calidad SaaS con el mismo nombre en los cortafuegos de central y sucursal para aprovechar correctamente el cortafuegos de central como una conmutación por error alternativa.

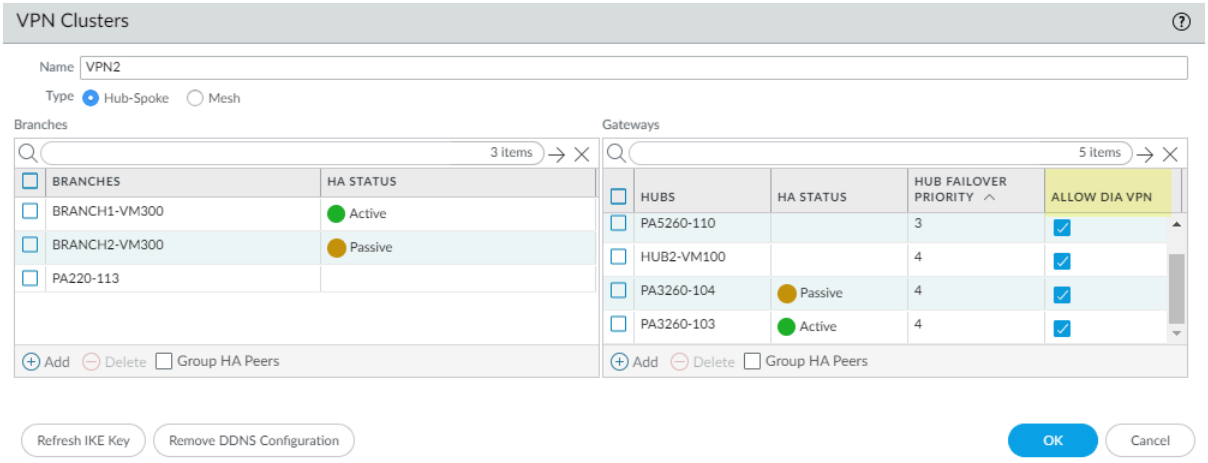
La forma más sencilla de configurar la conmutación por error en un cortafuegos de central con el mismo destino de la aplicación SaaS es crear un único perfil de calidad de SaaS en el grupo de dispositivos compartidos. También puede crear dos perfiles de calidad SaaS con nombres idénticos en diferentes grupos de dispositivos y enviarlos a sus cortafuegos de central y sucursal.

Para la conmutación por error a un cortafuegos de central con diferentes destinos de aplicaciones de SaaS, cree dos perfiles de calidad SaaS con nombres idénticos, cada uno dirigido a un destino de aplicación de SaaS diferente en diferentes grupos de dispositivos y envíelos a sus cortafuegos de central y sucursal.

También debe crear una regla de políticas SD-WAN que haga referencia a este perfil de calidad de SaaS para permitir que la central publique estadísticas de calidad de enlace para el perfil de calidad de SaaS en la sucursal. Si lo hace, proporcionará una supervisión de SaaS de un extremo a otro a través de la central. Sin esta regla de políticas SD-WAN, solo tendría las medidas de enlace de la sucursal a la central, pero no de la central a la aplicación SaaS.

STEP 10 | Permita que las centrales participen en AnyPath de DIA.

1. Creación de un clúster de VPN y seleccione una central.
2. Seleccione **Allow DIA VPN (Permitir VPN de DIA)** para la central. Se admite un máximo de cuatro centrales (cualquier combinación de centrales de PAN-OS que participen en las centrales de AnyPath de DIA y de Prisma Access). Si son centrales de HA, se admiten un total de ocho centrales. Si **permite la VPN de DIA** para un peer de HA en un par, también debe habilitarla para el otro peer de HA.



STEP 11 | Cree una regla de políticas SD-WAN para aplicaciones específicas para usar AnyPath de DIA.

1. Configuración de una regla de políticas de SD-WAN.
2. En la pestaña **Application/Service (Aplicación/Servicio)**, especifique las aplicaciones y servicios para los que desee implementar AnyPath de DIA.
3. Asocie el **perfil de calidad de SaaS** que creó en el paso anterior.

   Si está configurando un perfil de calidad de SaaS con un destino de aplicación SaaS diferente, debe asociar el perfil de calidad de SaaS con la regla de políticas SD-WAN en cada grupo de dispositivos de central y sucursal.
4. En la pestaña **Selección de ruta**, seleccione el **perfil de distribución de tráfico** que ha creado para las aplicaciones.

STEP 12 | Enrute sesiones nuevas que no coincidan con ninguna regla de políticas de SD-WAN y sesiones que lleguen durante un cambio de configuración de cortafuegos o Panorama.

1. Cree un perfil de calidad de ruta y un perfil de distribución de tráfico adecuados para gestionar estas sesiones.
2. Configuración de una regla de políticas de SD-WAN que sea una regla general para esas sesiones.
3. Coloque la regla en el último lugar de la lista.

STEP 13 | Seleccione **Commit (Confirmar)** y **Push to Devices (Enviar a dispositivos)**.

STEP 14 | Cree una regla de la política de seguridad para permitir el tráfico de DIA en las **zonas de destino** denominadas `zone-internet (zona a Internet)` y `zone-to-hub (Zona a central)` y especifique el asunto **Applications (Aplicaciones)** en la regla. Confirme y realice el envío a las sucursales.

STEP 15 | Utilice los siguientes comandos de la CLI para supervisar la información de DIA:

1. **`show sdwan connection <dia-vif-name>`**
2. **`show sdwan path-monitor stats dia-vif all`**
3. **`show sdwan path-monitor dia-anypath`**
4. **`show sdwan path-monitor dia-anypath packet-buffer all`**
5. **`show sdwan path-monitor stats conn-idx <IDX>`**

Distribución de sesiones no coincidentes

El cortafuegos intenta hacer coincidir las sesiones que llegan a una interfaz virtual de SD-WAN con una regla de políticas de SD-WAN; el cortafuegos examina las reglas de políticas de SD-WAN en orden de arriba hacia abajo, tal como lo hace para las reglas de la política de seguridad.

- Si hay una coincidencia de la regla de SD-WAN, el cortafuegos ejecuta la supervisión de la ruta y la distribución del tráfico para esa regla de políticas de SD-WAN.
- Si no hay una coincidencia con ninguna regla de políticas de SD-WAN en la lista, la sesión coincide con una regla de políticas de SD-WAN implícita al final de la lista que usa el método por turnos para distribuir sesiones no coincidentes entre todos los enlaces en una interfaz de SD- WAN, que se basa en la búsqueda de ruta.

Además, si no existe una regla de políticas de SD-WAN para una aplicación específica, el cortafuegos no rastrea el rendimiento de esa aplicación en las herramientas de visibilidad específicas de SD-WAN, como la creación de logs e informes en el complemento de SD-WAN.

Para ilustrar la regla de políticas implícita, tenga en cuenta lo siguiente:

- Supongamos que el cortafuegos tiene tres reglas de política de SD-WAN: una regla especifica cinco aplicaciones de voz, una regla especifica seis aplicaciones de videoconferencia y una regla especifica diez aplicaciones SaaS.
- Una sesión, por ejemplo, una sesión de aplicación de vídeo, llega al cortafuegos y no coincide con ninguna de las reglas de políticas de SD-WAN. Debido a que la sesión no coincidía con una regla, el cortafuegos no tiene un perfil de calidad de ruta o un perfil de distribución de tráfico que aplicar a la sesión.
- Por lo tanto, el cortafuegos compara la aplicación de vídeo con la regla implícita y distribuye cada sesión de vídeo entre todas las etiquetas de enlace de SD-WAN disponibles y sus enlaces asociados en el cortafuegos, que podrían ser dos enlaces de banda ancha, un enlace MPLS y un enlace LTE. La sesión 1 se dirige a un miembro de la interfaz de banda ancha, la sesión 2 va a otro miembro de la interfaz de banda ancha, la sesión 3 se dirige a MPLS, la sesión 4 va a LTE, la sesión 5 se dirige al primer miembro de la interfaz de banda ancha, la sesión 6 va al segundo miembro de la interfaz de banda ancha, y la distribución por turnos continúa.

Es posible que no desee permitir que sus sesiones no coincidentes recurran a la regla de SD-WAN implícita porque no tenga control sobre la distribución de esa sesión. En su lugar, le recomendamos que cree una regla general de políticas de SD-WAN y la coloque en último lugar en la lista de reglas de política de SD-WAN. Una regla general de políticas de SD-WAN le permite realizar las siguientes acciones:

- Controlar qué enlaces usan las sesiones no coincidentes.
- Ver todas las aplicaciones en el cortafuegos (incluidas las sesiones de aplicaciones no coincidentes) en la creación de logs e informes en el complemento de SD-WAN.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Creación de un perfil de calidad de ruta que establece umbrales de latencia, fluctuación de fase y pérdida de paquetes muy altos que nunca se superarán. Por ejemplo, latencia de 2000 ms, vibración de 1000 ms y pérdida de paquetes del 99 %.

STEP 3 | Creación de un perfil de distribución de tráfico que especifica las etiquetas de enlace de SD-WAN que desea usar, en el orden en que desea que las sesiones no coincidentes usen los enlaces asociados con esas etiquetas de enlace.

> *Si no desea que las aplicaciones no coincidentes usen una ruta específica (interfaz física), omita la etiqueta que incluye ese enlace de la lista de etiquetas de enlace en el perfil de distribución de tráfico. Por ejemplo, si no desea que una aplicación no coincidente, como la transmisión de películas, utilice el costoso enlace LTE, omita la etiqueta de enlace para el enlace LTE de la lista de etiquetas de enlace en el perfil de distribución de tráfico.*

STEP 4 | **Añada** una regla de políticas de SD-WAN general y, en la pestaña **Aplicación/Servicio**, especifique el **perfil de calidad de la ruta** que ha creado.

STEP 5 | Seleccione **Cualquiera** para las **aplicaciones** y el **servicio**.

STEP 6 | En la pestaña **Selección de ruta**, seleccione el **perfil de distribución de tráfico** que ha creado.

STEP 7 | **Mueva** la regla hacia abajo a la última posición en la lista de reglas de políticas de SD-WAN.

STEP 8 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

STEP 9 | **Commit (Confirmar)** los cambios.

Adición de dispositivos de SD-WAN a Panorama

Añada un único cortafuegos de sucursal o hub de SD-WAN o use un CSV para importar de forma masiva varios cortafuegos de hub y sucursal de SD-WAN con clave precompartida o tipo de autenticación de certificado.

- Configurar la autenticación basada en certificados para dispositivos SD-WAN
- Adición de un dispositivo de SD-WAN
- Importación masiva de varios dispositivos de SD-WAN
- Incorporación de cortafuegos PAN-OS a Prisma Access

Configurar la autenticación basada en certificados para dispositivos SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

Puede autenticar un dispositivo SD-WAN utilizando cualquiera de los dos tipos de autenticación siguientes:

- Clave precompartida (tipo de autenticación predeterminado)
- Certificado (complemento SD-WAN 3.2.0 y versiones posteriores)

Cuando crea un nuevo clúster SD-WAN o actualiza la clave con una versión de complemento SD-WAN anterior a 3.2.0, el complemento SD-WAN genera la clave precompartida automáticamente. Además del tipo de autenticación de clave precompartida, proporcionamos autenticación basada en certificados con el complemento SD-WAN 3.2.0 y versiones posteriores para que los cortafuegos de nueva generación satisfagan sus necesidades de seguridad. Lleve su seguridad al siguiente nivel con una autenticación y validación más sólidas para todos los sitios SD-WAN con autenticación basada en certificados.

La autenticación basada en certificados es compatible con todos los dispositivos de software y hardware que ejecutan motores de enrutamiento heredados o avanzados compatibles con SD-WAN.

Siga los pasos mencionados en las Consideraciones sobre el cambio a versiones anteriores/posteriores antes de actualizar o cambiar a una versión anterior de su complemento SD-WAN actual.

Utilice el siguiente flujo de trabajo para configurar la autenticación basada en certificados para su dispositivo SD-WAN:

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Generar un certificado para dispositivos SD-WAN en Panorama.

1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)**.
2. Cree un certificado de CA raíz autofirmado o importe un certificado de su empresa CA. Basado en la CA raíz, genere el certificado de dispositivos para un dispositivo SD-WAN. No admitimos certificados generados por SCEP.

   El certificado generado debe ser único para cada dispositivo SD-WAN. Es decir, no puede generar un certificado y compartirlo entre varios dispositivos SD-WAN.

   Tenga en cuenta lo siguiente al generar los certificados de cortafuegos de sucursal y hub que se utilizan para la autenticación de túnel SD-WAN:

   - Dos dispositivos de hub diferentes pueden usar el mismo certificado de hub.
   - Dos dispositivos de sucursal diferentes pueden utilizar los mismos certificados de sucursal si se cumplen las siguientes condiciones:
     - Los dispositivos de sucursales no son parte del mismo clúster VPN
     - No hay un dispositivo hub común entre los clústeres de VPN del que estos dispositivos de sucursal formarían parte.

     .
   - (Solo implementaciones de HA) Dos dispositivos de sucursal diferentes también pueden tener los mismos certificados de sucursal si están configurados como miembros de HA.
   - Si el dispositivo de hub es común entre clústeres VPN, los certificados para dispositivos de sucursal que forman parte de estos clústeres VPN deben tener certificados únicos con todos los atributos que tienen valores únicos. Si no garantiza la exclusividad del certificado y sus valores, la confirmación fallará en el dispositivo de hub (sin fallo de confirmación en Panorama).

   Asegúrese también de que los certificados específicos (certificados de cortafuegos de sucursal y de hub) utilizados para la autenticación de túnel SD-WAN se generan cumpliendo los siguientes criterios:

   - *El uso de claves debe tener firmas digitales*
   - *Todos los certificados deben estar firmados por la misma CA raíz*
   - *El certificado del dispositivo debe estar firmado directamente por la CA raíz.*
   - *El formato del certificado deberá ser PKCS12*

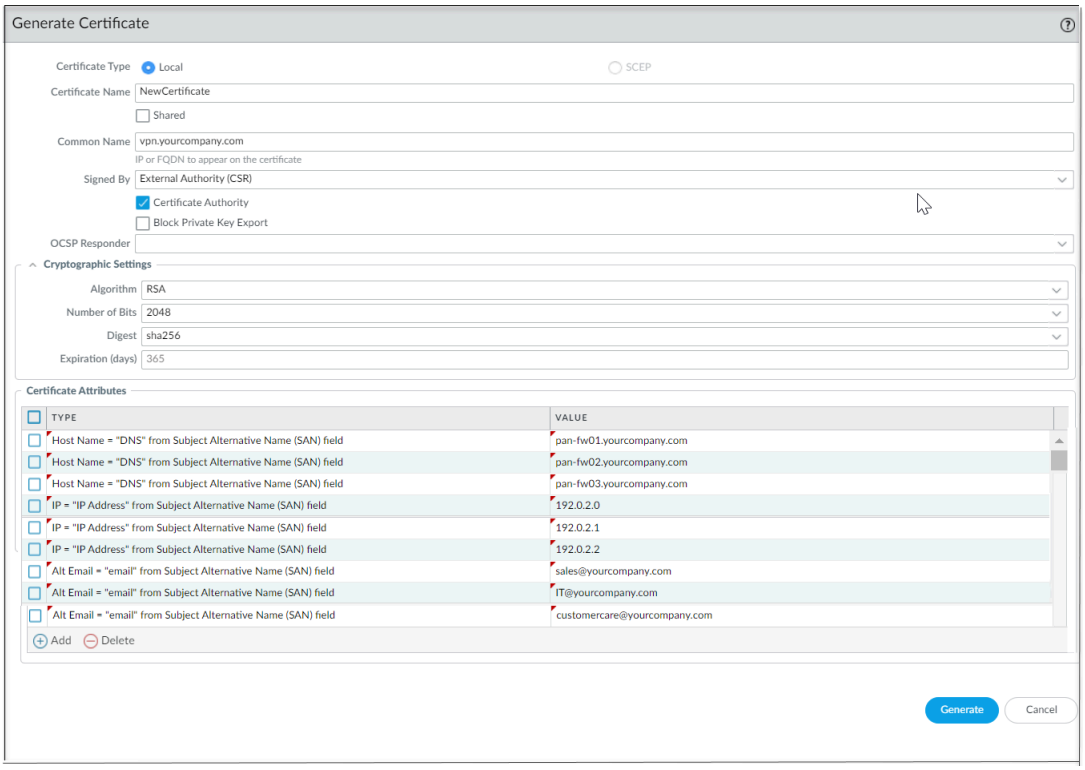
   Los atributos del certificado se utilizan para determinar el ID local y el ID de peer para puertas de enlace IKE. Por lo tanto, los certificados específicos, es decir, los certificados de cortafuegos de sucursal y hub que se utilizan para la autenticación de túnel SD-WAN, deben generarse con los siguientes tres atributos de certificado y a cada atributo de

certificado se le deben asignar tres valores de atributo únicos. De lo contrario, se lanzará un error de confirmación.

- FQDN (**Host Name [Nombre de host]**)
- Dirección IP (**IP**)
- Usuario FQDN (**Alt Email (Correo electrónico Alt**)

*Es obligatorio tener atributos de certificado de **Host Name (Nombre de host)**, **IP** y **Alt Email (Correo electrónico Alt)** exclusivos entre todos los certificados. Es decir, ninguno de los certificados debe tener estos valores de atributo en común.*

En el ejemplo a continuación, NewCertificate se genera con el total de nueve atributos de certificado obligatorios. El atributo de certificado **Host Name (Nombre de host)** está configurado con tres valores de atributo únicos: pan-fw01.yourcompany.com, pan-fw02.yourcompany.com y pan-fw03.yourcompany.com. El atributo del certificado **IP** está configurado con tres valores de atributo únicos: 192.0.2.0, 192.0.2.1 y 192.0.2.2. El certificado de **Alt Email (Correo electrónico Alt)** está configurado con tres valores de atributo únicos: sales@yourcompany.com, IT@yourcompany.com y customercare@yourcompany.com.



STEP 3 | (Opcional) Configure un perfil de certificado que incluya la CA raíz y la CA intermedia para la comunicación de servidor segura.

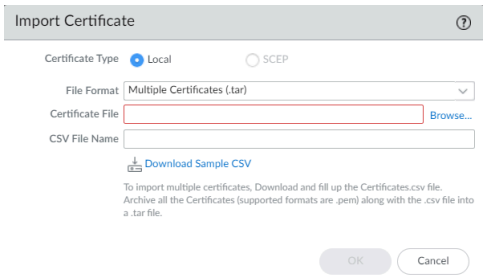
1. Seleccione **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificados)**.
2. Configuración de un perfil de certificado.

   Si configura una CA intermedia como parte de un perfil de certificado, también debe incluir la CA raíz.

   Este perfil de certificado define cómo los hubs de SD-WAN y las sucursales se autentican mutuamente.

STEP 4 | Importe los certificados CA para validar la identidad de los dispositivos SD-WAN.

1. **Panorama** > **Gestión de certificados** > **certificates**
2. Importar el certificado CA y el par de claves en Panorama para cada dispositivo SD-WAN en un clúster o importar varios certificados con **Multiple Certificates (.tar) [Múltiples certificados (.tar)]**. Utilice CSV para importar en bloque los certificados al servidor de gestión de Panorama. El CSV le permite importar varios certificados a la vez, en lugar de añadir cada certificado manualmente.



3. **Commit (Confirmar)** los cambios. Es importante confirmar después de importar los certificados para que los certificados importados estén disponibles para su configuración posterior.

STEP 5 | Configure un tipo de autenticación basado en certificados mientras añade un cortafuegos de hub o sucursal de SD-WAN que gestionará el servidor de gestión de Panorama. Al añadir sus dispositivos, especifique qué tipo de dispositivo es (sucursal o hub), un tipo de autenticación para el dispositivo y asigne a cada dispositivo su nombre para poder identificarlo fácilmente.

1. Seleccione **Devices (Dispositivos)** > **Panorama** > **SD-WAN** para añadir un dispositivo SD-WAN (cortafuegos de hub o sucursal de SD-WAN) que gestionará el servidor de gestión de Panorama.
2. Seleccione la pestaña **VPN tunnel (Túnel VPN)** y configure el tipo de **authentication (autenticación)**. Para la autenticación basada en certificados, seleccione **Certificate (Certificado)** y configure los campos relacionados con certificados. Es obligatorio seleccionar un tipo de autenticación al añadir un dispositivo SD-WAN.

STEP 6 | Configure la autenticación basada en certificados al incorporar cortafuegos PAN-OS a Prisma Access.

1. Seleccione **Devices (Dispositivos)** > **Panorama** > **SD-WAN** para seleccionar el cortafuegos de sucursal SD-WAN para conectarse al hub de Prisma Access y configurar la conexión.
2. Seleccione **Prisma Access Onboarding (Incorporación de Prisma Access)** y luego **Add (Añadir)** para añadir un nodo de cómputo a una **Region (Región)**. En el **VPN Tunnel (Túnel VPN)**, es obligatorio seleccionar el tipo de autenticación para autenticar el CN (hub de Prisma Access). Para la autenticación basada en certificados, seleccione **Certificate (Certificado)** como el tipo de **Authentication (Autenticación)** y configure los campos relacionados del certificado. Es obligatorio seleccionar un tipo de autenticación mientras se incorporan cortafuegos PAN-OS a Prisma Access.

   Asegúrese de seleccionar el mismo tipo de autenticación para todos los dispositivos de sucursal y el hub de Prisma Access que se añade. Si intenta utilizar diferentes tipos de autenticación para la sucursal y el hub de Prisma, se produce un error de confirmación en Panorama.

STEP 7 | Configure la autenticación basada en certificados mientras crea un clúster VPN.

1. Seleccione **Panorama** > **SD-WAN** > **VPN Clusters (Clústeres de VPN)**.
2. Seleccione el **tipo** de clúster de VPN.
3. Seleccione el **Authentication Type (Tipo de autenticación)** como **Certificate (Certificado)**. Es obligatorio especificar el tipo de autenticación para añadir un dispositivo en un clúster de VPN. Un clúster VPN deberá tener el mismo tipo de autenticación seleccionado para todos sus dispositivos. No puede cambiar el tipo de autenticación de un dispositivo SD-WAN que ya se ha añadido a un clúster VPN. Si desea cambiar, elimine el clúster VPN y sus dispositivos SD-WAN y configúrelo nuevamente con el tipo de autenticación de su elección. De forma predeterminada, el tipo de autenticación de clave precompartida es compatible con los dispositivos de un clúster VPN (si no ha seleccionado el tipo de certificado manualmente).

STEP 8 | Haga clic en **Commit (Confirmar)** para aceptar los cambios en la configuración.

STEP 9 | Seleccione **Enviar a dispositivos** para enviar sus cambios de configuración a sus cortafuegos gestionados.

Adición de un dispositivo de SD-WAN

Añada un cortafuegos de sucursal o hub de SD-WAN para que el servidor de gestión Panorama™ lo gestione. Al añadir sus dispositivos, especifique qué tipo de dispositivo es (sucursal o hub) y asigne a cada dispositivo su nombre para poder identificarlo fácilmente. Antes de añadir sus dispositivos, planifique su configuración de SD-WAN para asegurarse de que tiene todas las direcciones IP necesarias y que la topología de SD-WAN se entiende bien. Esto ayuda a reducir los errores de configuración.

Si desea que la HA activa/pasiva se ejecute en dos cortafuegos de sucursal o en dos cortafuegos de hub, no añada esos cortafuegos como dispositivos de SD-WAN en este momento. Tendrá que añadirlos como peers de HA por separado cuando Configuración de dispositivos de HA para SD-WAN.

Si utiliza el enrutamiento de BGP, debe añadir una Regla de política de seguridad para permitir BGP desde la zona interna a la zona del hub y desde la zona del hub a la zona interna. Si desea utilizar ASN de 4 bytes, primero debe habilitar los ASN de 4 bytes para el enrutador virtual.

Cuando se visualizan dispositivos SD-WAN, si no hay datos presentes o la pantalla indica que SD-WAN no está definida, compruebe en la Matriz de compatibilidad que la versión de Panorama que está utilizando sea compatible con la versión del complemento SD-WAN que está intentando utilizar.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Devices (Dispositivos)** y luego **Add (Añadir)** para añadir un nuevo cortafuegos SD-WAN.

STEP 3 | Seleccione el **nombre** del cortafuegos gestionado que añadir como dispositivo de SD-WAN. Debe añadir sus cortafuegos de SD-WAN como dispositivos gestionados para poder añadirlos como un dispositivo de SD-WAN.

STEP 4 | Seleccione el **tipo** de dispositivo de SD-WAN.

- **Hub**: un cortafuegos centralizado implementado en una oficina o ubicación principales a la que todos los dispositivos de sucursal se conectan mediante una conexión VPN. El tráfico entre sucursales pasa a través de el hub antes de continuar hacia la sucursal objetivo y conecta las sucursales con los recursos centralizados en la ubicación del hub. El dispositivo del hub procesa el tráfico, aplica las reglas de políticas y gestiona el intercambio de enlaces en la oficina o ubicación principales.
- **Sucursal**: un cortafuegos implementado en una ubicación de sucursal física que conecta el hub mediante una conexión VPN y proporciona seguridad a nivel de sucursal. El dispositivo de la sucursal procesa el tráfico, aplica las reglas de políticas y gestiona el intercambio de enlaces en la ubicación de la sucursal.

STEP 5 | (Opcional) (PAN-OS 11.1.3 y versiones posteriores, y complemento SD-WAN 3.2.1 y versiones posteriores) Configure varios enrutadores virtuales en el hub de SD-WAN.

Seleccione **Enable Multi-VR Support (Habilitar compatibilidad con varios VR)** para configurar varios enrutadores virtuales en el hub de SD-WAN.

Hemos introducido compatibilidad para varios enrutadores virtuales en el hub de SD-WAN que le permiten tener direcciones de subred IP superpuestas en dispositivos de sucursal que se conectan al mismo hub de SD-WAN. Cuando seleccione el **Type (Tipo)** de SD-WAN como Hub, podrá configurar varios enrutadores virtuales seleccionando la opción **Enable Multi-VR Support (Habilitar compatibilidad con varios VR)**.

STEP 6 | Seleccione el **Router Name (Nombre del enrutador)** para usar para el enrutamiento entre el hub y las sucursales de SD-WAN. De forma predeterminada, se crea un enrutador virtual

`sdwan-default` y permite a Panorama impulsar automáticamente las configuraciones del enrutador.

(**Enrutamiento avanzado** habilitado) Si configuró el enrutamiento avanzado y los enrutadores lógicos se crearon correctamente, el**nombre del enrutador** muestra los nombres de los enrutadores virtuales y lógicos:

- Si los nombres del enrutador virtual y del enrutador lógico son los mismos, entonces el **Router Name (Nombre del enrutador)** muestra el mismo nombre porque el enrutador avanzado crea un enrutador lógico con el mismo nombre que el enrutador virtual, de forma predeterminada. Es importante que el nombre del enrutador lógico y el nombre del enrutador virtual sean los mismos para la misma plantilla cuando se utiliza el motor de enrutamiento avanzado.
- Si los nombres del enrutador virtual y del enrutador lógico son diferentes (ocurre solo cuando actualiza el nombre del enrutador lógico manualmente), entonces el nombre del enrutador muestra tanto el nombre del enrutador virtual como el del enrutador lógico. Puede seleccionar un enrutador virtual (para un motor heredado) o un enrutador lógico (para un motor de enrutamiento avanzado) según sus necesidades. Si no habilitó el **Advanced Routing (Enrutamiento avanzado)**, solo tendrá enrutadores virtuales para seleccionar desde el **Router Name (Nombre del enrutador)** (para el motor heredado).

(PAN-OS 11.1.3 y versiones posteriores, y complemento SD-WAN 3.2.1 y versiones posteriores) Cuando esté habilitada la opción para varios enrutadores virtuales (**Enable Multi-VR Support [Habilitar la compatibilidad con varios VR]**), seleccione enrutador virtual DIA para el **Virtual Router Name (Nombre del enrutador virtual)**.

STEP 7 | Especifique el nombre del **sitio** de SD-WAN para identificar la ubicación geográfica o el fin del dispositivo.

*El nombre del sitio de SD-WAN admite todos los caracteres alfanuméricos y especiales en mayúsculas y minúsculas. No se admiten espacios en el nombre del sitio y provocan que no se muestre la supervisión de datos (**Panorama** > **Monitoring (Supervisión)**) para ese sitio.*

Todos los dispositivos SD-WAN, incluidos los dispositivos SD-WAN en una configuración de alta disponibilidad (HA), deben tener un nombre de sitio único.

STEP 8 | Seleccione la **etiqueta de enlace** que creó para la interfaz virtual del hub (o la interfaz virtual de la sucursal), que la VPN automática asignará a la interfaz virtual. Utilizará esta etiqueta de enlace en un perfil de distribución de tráfico para permitir que el hub (o la sucursal) participe en AnyPath de DIA.

STEP 9 | Si añade un Hub detrás de un dispositivo que realiza NAT para el hub, debe especificar la dirección IP o el FQDN de la interfaz pública en ese dispositivo de rendimiento NAT de subida, de modo que la configuración de VPN automática pueda usar esa dirección como el endpoint del túnel del hub. Se trata de la dirección IP a la que los flujos IKE e IPSec de la sucursal deben poder acceder. (Debe tener ya configurada una interfaz Ethernet física para SD-WAN).

1. En la pestaña **NAT de subida**, habilite **NAT de subida**.
2. **Añada** una **interfaz de SD-WAN**; seleccione una interfaz que ya haya configurado para SD-WAN.

3. Seleccione **Dirección IP** o **FQDN** y especifique la dirección IPv4 sin una máscara de subred (por ejemplo, 192.168.3.4) o el FQDN del dispositivo de subida, respectivamente.
4. Haga clic en **OK (Aceptar)**.

También, en el dispositivo de subida encargado de NAT, debe configurar el NAT de destino entrante con una política de NAT personalizada, y no debe configurar la traducción del puerto a los flujos de tráfico IKE o IPSec.

Si cambia la dirección IP en el dispositivo de subida, debe configurar la nueva dirección IP y enviarla al clúster de la VPN. Debe usar los comandos de la CLI ***clear vpn ipsec-sa***, ***clear vpn ike-sa*** *y* ***clear session all*** *tanto en la sucursal como en el hub. También debe* ***borrar la sesión de todo*** *en el enrutador virtual donde configuró la política de NAT para las direcciones IP.*

La NAT ascendente no es compatible con las interfaces de Capa 2.

STEP 10 | (Solo implementaciones de malla completa) Si está añadiendo una sucursal que está detrás de un dispositivo que realiza NAT para la sucursal, debe especificar la dirección IP o el FQDN de la interfaz pública en ese dispositivo que efectúa la NAT ascendente, o seleccionar DDNS para indicar que la dirección IP para la interfaz en el dispositivo NAT se obtiene del servicio DDNS de Palo Alto Networks. Por lo tanto, la configuración de VPN automática usa esa dirección IP pública como el endpoint del túnel para la sucursal. Se trata de la dirección IP a la que los flujos IKE e IPSec de la sucursal deben poder acceder. (Debe tener ya configurada una interfaz Ethernet física para SD-WAN).

1. En la pestaña **NAT de subida**, habilite **NAT de subida**.
2. **Añada** una **interfaz de SD-WAN**; seleccione una interfaz que ya haya configurado para SD-WAN.
3. Si selecciona **NAT IP Address Type (Tipo de dirección IP de NAT)** para que sea **Static IP (IP estática)**, seleccione **IP Address (Dirección IP)** o **FQDN** y especifique la dirección IPv4 sin máscara de subred (por ejemplo, 192.168.3.4) o el FQDN del dispositivo de subida respectivamente.
4. También puede seleccionar **NAT IP Address Type (Tipo de dirección IP de NAT)** para que sea **DDNS**.

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

También, en el dispositivo de subida encargado de NAT, debe configurar el NAT de destino entrante con una política de NAT personalizada, y no debe configurar la traducción del puerto a los flujos de tráfico IKE o IPSec.

Si cambia la dirección IP en el dispositivo de subida, debe configurar la nueva dirección IP y enviarla al clúster de la VPN. Debe usar los comandos de la CLI ***`clear ipsec`****,* ***`clear ike-sa`*** *y* ***`clear session all`*** *tanto en la sucursal como en el hub. También debe* ***`borrar la sesión de todo`*** *en el enrutador virtual donde configuró la política de NAT para las direcciones IP.*

Hay una segunda ubicación en la interfaz web donde puede configurar la NAT de subida para una sucursal, pero la siguiente ubicación no es la preferida y no debe configurarla para una sucursal en ambos lugares. La ubicación secundaria no preferida para configurar la NAT de subida está en Panorama en ***Network (Red)*** *>* ***Interfaces (Interfaces)*** *>* ***Ethernet****. Seleccione una plantilla en el campo* ***Template (Plantilla)****, elija una interfaz Ethernet y seleccione la pestaña* ***SD-WAN****. En este momento, puede* ***habilitar*** *la NAT ascendente y seleccionar un* ***tipo de dirección IP de NAT****. El segundo método tiene prioridad. Si la NAT de subida se configura primero para la interfaz Ethernet en Panorama a través de la pila de plantillas, el complemento SD-WAN no cambiará la configuración, independientemente de si usa ajustes diferentes en la página de configuración del dispositivo de complemento. La configuración del complemento para la NAT de subida se aplica solo si no hay una NAT ascendente configurada en Panorama a través de la pila de plantillas.*

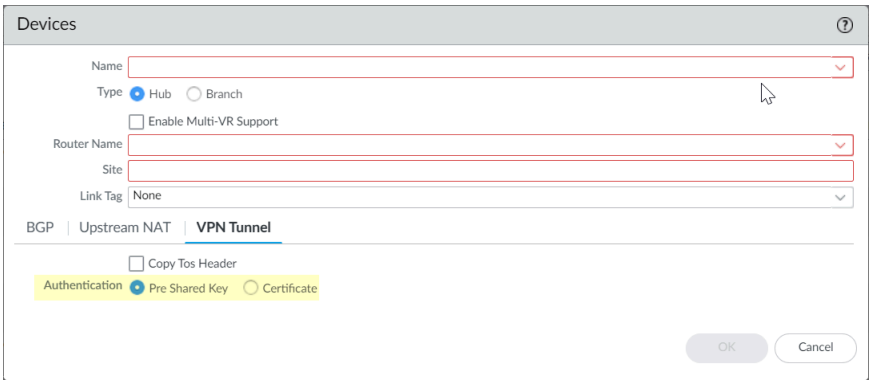
La NAT ascendente no es compatible con las interfaces de capa 2.

STEP 11 | Si el tráfico de su aplicación está etiquetado con bits de tipo de servicio (ToS) o marcas de punto de código de servicios diferenciados (DSCP), copie el campo ToS desde el encabezado interno hasta el encabezado VPN externo de los paquetes encapsulados que pasan por el túnel VPN para preservar la información de QoS.

1. Seleccione la pestaña **VPN Tunnel (Túnel VPN)** .
2. Seleccione **Copy ToS Header (Copiar encabezado de ToS)**.
3. Haga clic en **OK (Aceptar)**.

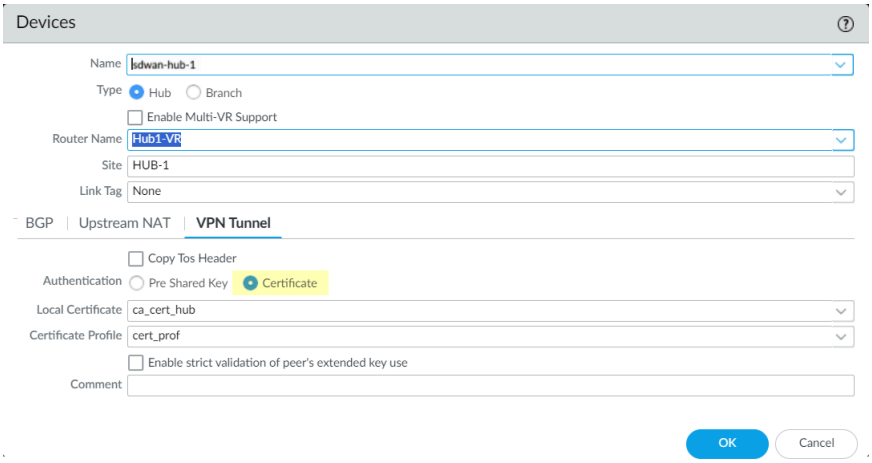
STEP 12 | (Obligatorio) (Complemento SD-WAN 3.2.0 y versiones posteriores) Especifique cómo autenticar el peer.

Seleccione el tipo de **Authentication (Autenticación)**. **Pre-Shared Key (Clave precompartida)** o **Certificate (Certificado)**. Si elige una clave precompartida, la clave precompartida se generará automáticamente.



- *Debe utilizar un certificado único para cada dispositivo del clúster SD-WAN.*
- *No es posible cambiar el tipo de autenticación después de añadir un dispositivo SD-WAN al clúster VPN.*
- *(Solo implementaciones HA) Si ha configurado un par de alta disponibilidad (HA) en Panorama, tanto el cortafuegos activo como el pasivo deben usar el mismo certificado. Durante el proceso RMA, debe configurar el cortafuegos de reemplazo con el mismo certificado que el cortafuegos activo. Si se revoca el certificado de un cortafuegos activo y se envía un nuevo certificado, el cortafuegos pasivo también debe actualizarse con el nuevo certificado. Es decir, los cortafuegos activos y pasivos deben tener el mismo certificado configurado en una implementación de alta disponibilidad.*

STEP 13 | (Solo si habilita el tipo de autenticación de certificado) Configure la autenticación basada en certificados.



1. Seleccione un **Local Certificate (Certificado local)**: un certificado que ya se encuentre en Panorama, haga clic en **Import (Importar)** un certificado o bien en **Generate (Generar)** para crear un certificado.

   - Para implementar la función **Import (Importar)** de un certificado, realice la Importación de un certificado para la autenticación de la puerta de enlace IKEv2 y regrese a esta tarea. Los certificados generados por SCEP no son compatibles.
   - Si desea **Generate (Generar)** un nuevo certificado, entonces primero genere un certificado en el Panorama y luego vuelva a esta tarea. El certificado generado debe ser único para cada dispositivo SD-WAN. Es decir, no se puede generar un certificado y compartirlo entre varios dispositivos SD-WAN.

     Tenga en cuenta lo siguiente al generar los certificados de cortafuegos de sucursal y hub que se utilizan para la autenticación de túnel SD-WAN:

     - Dos dispositivos de hub diferentes pueden usar el mismo certificado de hub.
     - Dos dispositivos de sucursal diferentes pueden utilizar el mismo certificado de sucursal si se cumplen las siguientes condiciones:
       - Los dispositivos de sucursal no forman parte del mismo clúster VPN.
       - No hay un dispositivo hub común entre los clústeres VPN del que formarían parte estos dispositivos de sucursal.
     - (Solo implementaciones de HA) Dos dispositivos de sucursal diferentes también pueden tener los mismos certificados de sucursal si están configurados como miembros de HA.
     - Si el dispositivo de hub es común entre clústeres VPN, los certificados para dispositivos de sucursal que forman parte de estos clústeres VPN deben tener certificados únicos con todos los atributos que tienen valores únicos. Si no

garantiza la exclusividad del certificado y sus valores, la confirmación fallará en el dispositivo de hub (sin fallo de confirmación en Panorama).

Asegúrese también de que los certificados específicos (certificados de cortafuegos de sucursal y de hub) utilizados para la autenticación de túnel SD-WAN se generan cumpliendo los siguientes criterios:

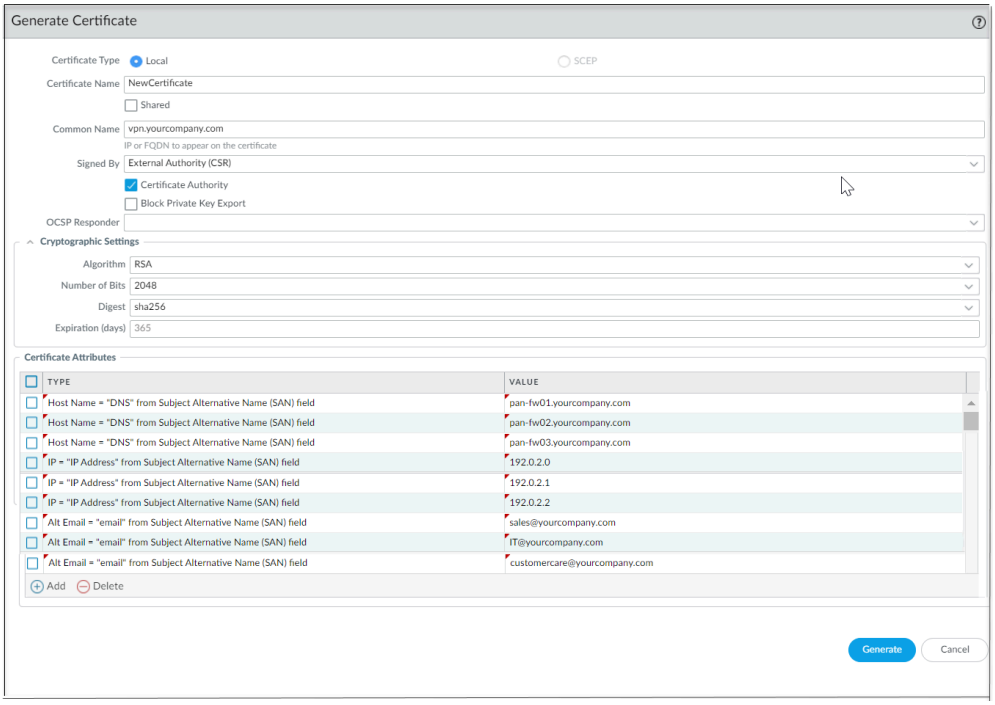
- *El uso de claves deberá tener firmas digitales.*
- *Todos los certificados deben estar firmados por la misma CA raíz.*
- *La CA raíz debe firmar directamente el certificado de dispositivo.*
- *El formato del certificado deberá ser PKCS12.*

- Los atributos del certificado se utilizan para determinar el ID local y el ID de peer para puertas de enlace IKE. Por lo tanto, los certificados específicos, es decir, los certificados de cortafuegos de sucursal y de hub que se utilizan para la autenticación de túnel SD-WAN, deben generarse con los siguientes tres atributos de certificado y a cada atributo de certificado se le deben asignar tres valores de atributo únicos. De lo contrario, se lanzará un error de confirmación.
  - FQDN (**Host Name [Nombre de host]**)
  - IP address [Dirección IP] (**IP**)
  - User FQDN [Usuario FQDN] (**Alt Email [correo electrónico Alt]**)

  *Es obligatorio tener atributos únicos de certificado **Host Name (Nombre de host)**, **IP** y **Alt Email (Correo electrónico Alt)** entre todos los certificados. Es decir, ninguno de los certificados debe tener estos valores de atributo en común.*

  En el ejemplo siguiente, NewCertificate se genera con el total de nueve atributos de certificado obligatorios. El atributo de certificado **Host Name (Nombre de host)** está configurado con tres valores de atributo únicos: pan-fw01.yourcompany.com, pan-fw02.yourcompany.com y pan-fw03.yourcompany.com. El certificado **IP** atribuido se configura con tres valores de atributo únicos: 192.0.2.0, 192.0.2.1 y 192.0.2.2. El certificado de **Alt Email (Correo electrónico Alt)** está configurado con

tres valores de atributo únicos: sales@yourcompany.com, IT@yourcompany.com y customercare@yourcompany.com.



2. (Opcional) Seleccione un **Certificate Profile (Perfil de certificado)**. Un perfil del certificado contiene información sobre el modo de autenticar la puerta de enlace del peer.
3. (Opcional) Seleccione **Enable strict validation of peer's extended key use (Habilitar validación estricta de uso de clave extendida de peer)** para controlar de forma estricta cómo se puede utilizar la clave.

STEP 14 | (Opcional) Configure el enrutamiento de BGP.

Para configurar automáticamente el enrutamiento de BGP entre los miembros del clúster de la VPN, especifique la información de BGP siguiente. Si desea configurar manualmente el enrutamiento de BGP en cada cortafuegos o usar una plantilla de Panorama independiente

para configurar el enrutamiento de BGP para contar con un mayor control, deje en blanco la información de BGP siguiente.

Antes de implementar SD-WAN con enrutamiento BGP en un entorno donde BGP ya está en uso, asegúrese de que la configuración BGP generada por el complemento SD-WAN no entre en conflicto con su configuración BGP ya existente. Por ejemplo, debe utilizar el número BGP AS existente y los valores de ID del enrutador para los valores de dispositivo SD-WAN correspondientes. Si la configuración de BGP generada por el complemento entra en conflicto con la configuración de BGP preexistente, la configuración de BGP preexistente tiene prioridad. Si desea que la configuración enviada tenga prioridad, debe habilitar forzar valor de plantilla al realizar una transferencia panorámica.

1. Seleccione la pestaña **BGP** y habilite **BGP** para configurar el enrutamiento de BGP para el tráfico de SD-WAN.
2. Introduzca el **ID del enrutador** de BGP, que debe ser único entre todos los enrutadores.
3. Introduzca el **número de sistema autónomo**. El número de sistema autónomo (número AS) especifica una política de enrutamiento comúnmente definida para Internet. El número AS debe ser único para cada ubicación del hub y la sucursal.

STEP 15 | Para configurar BGP para usar IPv4, seleccione **IPv4 BGP**. Ya sea que su entorno BGP sea solo IPv4 o una pila dual (IPv4 e IPv6), debe habilitar IPv4 BGP.

1. **Habilite la compatibilidad con IPv4 BGP**.

   *Para una configuración actualizada (una configuración IPv4 SD-WAN ya existente), se selecciona **Enable IPv4 BGP support (Habilitar la compatibilidad con IPv4 BGP)** de forma predeterminada. De lo contrario, debe **Enable IPv4 BGP support (Habilitar la compatibilidad con IPv4 BGP)** explícitamente.*

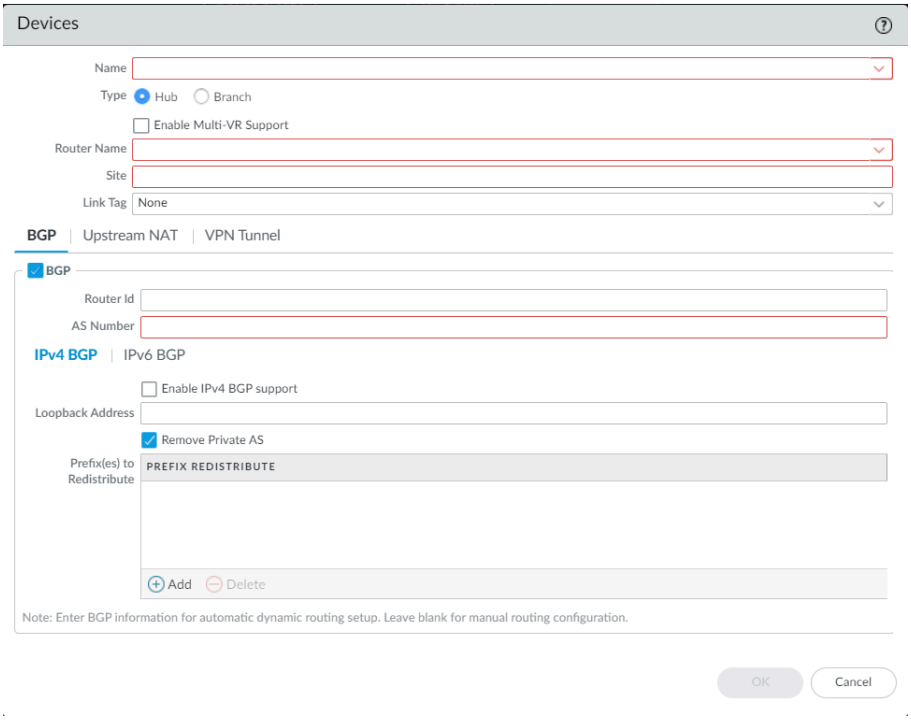
2. Especifique una **dirección de bucle invertido** IPv4 estática para el establecimiento de peers de BGP. La configuración de VPN automática crea una interfaz de bucle invertido de forma automática con la misma dirección IPv4 que especifique. Si especifica una dirección de bucle invertido existente, la confirmación fallará, por lo que deberá especificar una dirección IPv4 que no sea ya una dirección de bucle invertido.
3. Inhabilite la opción **Quitar AS privada** (por configuración predeterminada, está habilitado) si tiene endpoints que necesitan intercambiar rutas con un cortafuegos de hub o sucursal en una topología BGP SD-WAN y, por lo tanto, no desea quitar los números AS privados (64512 a 65534) del atributo AS_PATH en Actualizaciones BGP.

En este caso, debe permitir que los números AS privados salgan del AS privado SD-WAN en las actualizaciones de BGP.

*La configuración **Quitar AS privada** aplica a todos los grupos de par BGP en el cortafuegos de sucursal o hub. Si necesita que esta configuración difiera entre los grupos de pares BGP o pares, debe establecer la configuración por fuera del complemento SD-WAN.*

*Si cambia el ajuste **Remove Private AS (Eliminar AS privado)**, debe compilar todos los nodos del clúster SD-WAN y, posteriormente, cambiar a una versión inferior del complemento SD-WAN anterior a la 2.0.2. Por ende, toda la configuración relacionada con **Remove Private AS (Eliminar AS privado)** debe aplicarse por fuera del complemento SD-WAN o directamente en los cortafuegos.*

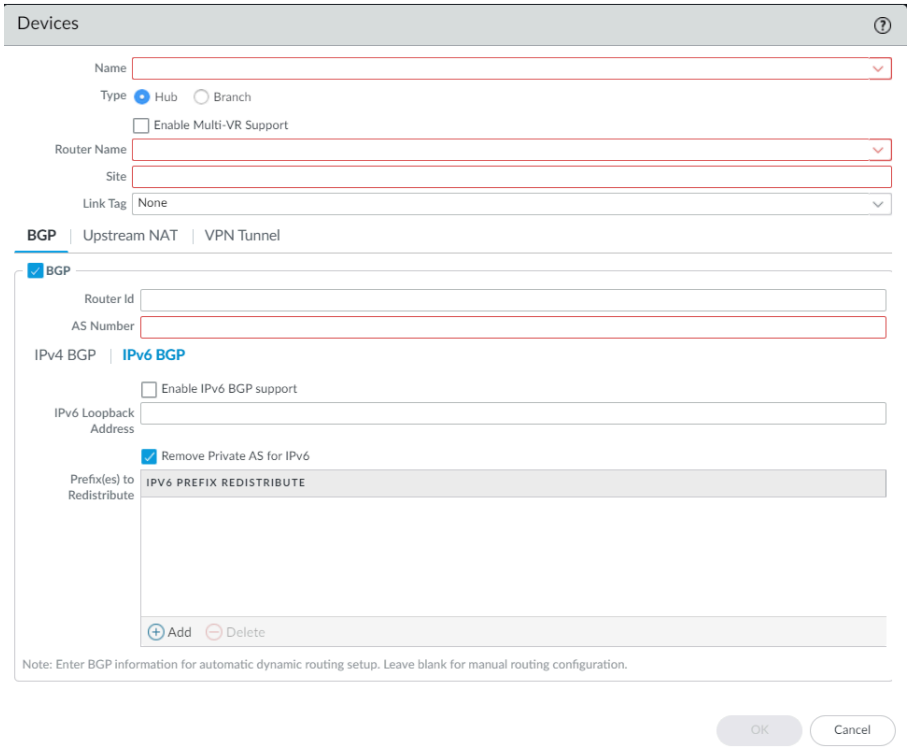
4. **Ad (Añadir)** el **Prefix(es) to Redistribute (Prefijo(s) a redistribuir)**. En un dispositivo de hub, debe introducir al menos un prefijo para redistribuir en el túnel SD-WAN. Los dispositivos de sucursal no tienen este requisito de configuración obligatorio porque las subredes conectadas a ubicaciones de sucursal se redistribuyen de forma predeterminada.



STEP 16 | Para configurar BGP para usar IPv6, seleccione **IPv6 BGP**.

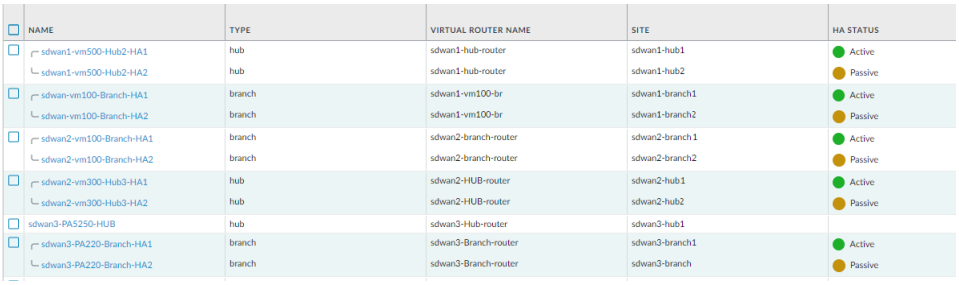
1. **Habilite la compatibilidad con IPv6 BGP**.
2. Especifique una **dirección de bucle invertido IPv6** estática para el establecimiento de peers de BGP. La configuración de VPN automática crea una interfaz de bucle invertido de forma automática con la misma dirección IPv6 que especifique. Si especifica una dirección de bucle invertido existente, la confirmación fallará, por lo que debe especificar una dirección IPv6 que no sea ya una dirección de bucle invertido.

3. **Add (Añadir)** los **Prefix(es) to Redistribute (Prefijo(s) a redistribuir)** en el túnel SD-WAN. En un dispositivo de hub, debe introducir al menos un prefijo para redistribuir en el túnel SD-WAN. Los dispositivos de sucursal no tienen este requisito de configuración obligatorio porque las subredes conectadas a ubicaciones de sucursal se redistribuyen de forma predeterminada.



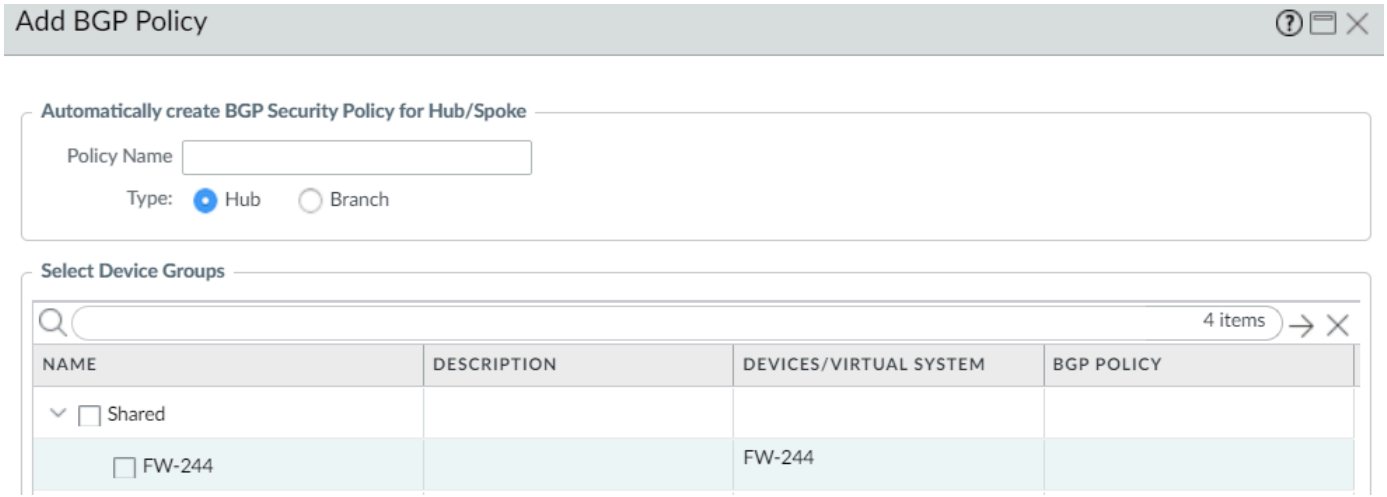
STEP 17 | Haga clic en **OK (Aceptar)**.

STEP 18 | Seleccione **Group HA Peers (Agrupar peers de HA)** en la parte inferior de la pantalla para mostrar las sucursales (o hubs) que son peers de HA juntas.



STEP 19 | Haga que Panorama cree y envíe a los cortafuegos una regla de la política de seguridad que permita que BGP se ejecute entre sucursales y hubs.

1. En la parte inferior de la pantalla, seleccione **IPv4 BGP Policy (Política de IPv4 BGP)** o **IPv6 BGP Policy (Política de IPv6 BGP)** y seleccione **Add (Añadir)** una regla de política.
2. Especifique un **nombre de política** para la regla de la política de seguridad que creará Panorama automáticamente.
3. Seleccione **Type (Tipo)** como **Hub (Hub)** o **Branch (Sucursal)**.
4. Elija **Seleccionar grupo de dispositivos** para especificar los grupos de dispositivos a los que Panorama envía la regla de la política de seguridad.
5. Haga clic en **OK (Aceptar)**.



STEP 20 | Seleccione **Enviar a dispositivos** para enviar sus cambios de configuración a sus cortafuegos gestionados.

Importación masiva de varios dispositivos de SD-WAN

Añada varios dispositivos de SD-WAN para incorporar rápidamente cortafuegos de sucursal y hub en lugar de añadir manualmente cada dispositivo de uno en uno. Al añadir sus dispositivos, especifique qué tipo de dispositivo es (sucursal o hub) y asigne a cada dispositivo su nombre para poder identificarlo fácilmente. Antes de agregar sus dispositivos, planifique su configuración SD-WAN para asegurarse de tener todas las direcciones IP requeridas y de que comprende la topología SD-WAN. Esto ayuda a reducir los errores de configuración.

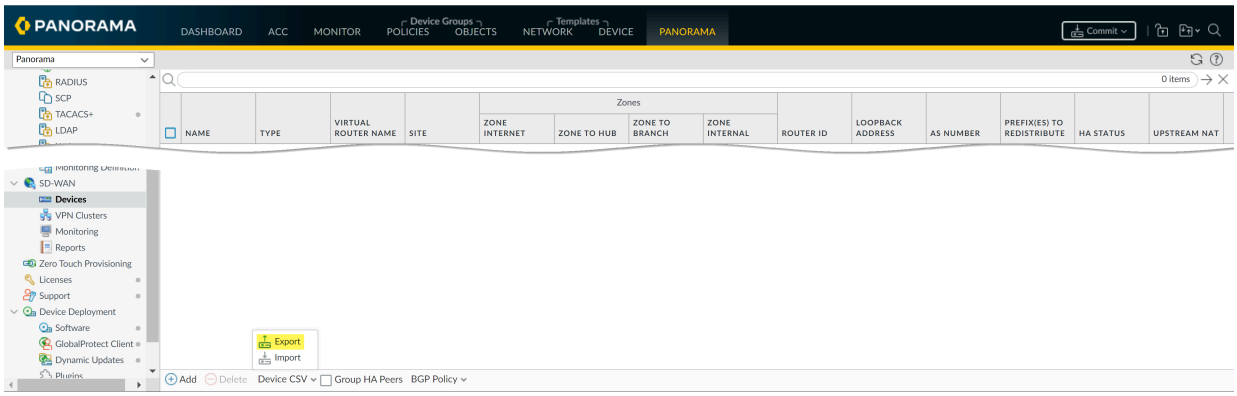
Si desea que la HA activa/pasiva se ejecute en dos cortafuegos de sucursal o en dos cortafuegos de hub, no añada esos cortafuegos como dispositivos de SD-WAN en su archivo CSV. Tendrá que añadirlos como peers de HA por separado cuando Configuración de dispositivos de HA para SD-WAN.

Si utiliza el enrutamiento de BGP, debe añadir una Regla de política de seguridad para permitir BGP desde la zona interna a la zona del hub y desde la zona del hub a la zona interna. Si desea utilizar números del sistema autónomo (ASN) de 4 bytes, primero debe habilitar los ASN de 4 bytes para el enrutador virtual.

Si dispone de zonas preexistentes para sus cortafuegos de Palo Alto Networks, tendrá que asignarlas a las zonas predefinidas utilizadas en SD-WAN.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Dispositivos** > **CSV para dispositivo** y **exporte** un CSV de dispositivo de SD-WAN. El CSV le permite importar varios dispositivos de sucursal y hub a la vez en lugar de añadir cada dispositivo manualmente.



STEP 3 | Complete el CSV de dispositivo de SD-WAN con la información de la sucursal y el hub y guarde el CSV. Todos los campos son obligatorios a no ser que se especifique lo contrario. Introduzca lo siguiente para cada hub y sucursal:

- **device-serial**: el número de serie del cortafuegos de la sucursal o el hub.
- **type**: especifique si un dispositivo es una **`sucursal`** o un **hub**.
- **site**: especifique el nombre del sitio de SD-WAN para que le ayude a identificar la ubicación geográfica o el fin del dispositivo.

  *El nombre del sitio de SD-WAN admite todos los caracteres alfanuméricos y especiales en mayúsculas y minúsculas. Los espacios no son compatibles en el nombre del sitio y es supone que no se muestre la supervisión de datos (**Panorama** > **SD-WAN** > **Monitoring [Supervisión]**) para ese sitio.*

  Todos los dispositivos SD-WAN, incluidos los dispositivos SD-WAN en una configuración de alta disponibilidad (HA), deben tener un nombre de sitio único.
- **router-name**: especifique el nombre del enrutador virtual que usar para el enrutamiento entre el hub y las sucursales de SD-WAN. De forma predeterminada, Panorama crea un

enrutador virtual `sdwan-default` y permite que Panorama impulse automáticamente las configuraciones del enrutador.

- **vif-link-tag**: especifique una etiqueta de enlace para identificar el hub cuando las aplicaciones y servicios utilicen este enlace durante la distribución del tráfico SD-WAN y la conmutación por error.
- (Opcional) **router-id**: especifique el ID de enrutador de BGP, que debe ser único entre todos los enrutadores virtuales o virtuales.

  Especifique la dirección de bucle invertido como ID de enrutador.

  Antes de implementar SD-WAN con enrutamiento BGP en un entorno donde BGP ya está en uso, asegúrese de que la configuración BGP generada por el complemento SD-WAN no entre en conflicto con su configuración BGP existente. Por ejemplo, debe utilizar el número BGP AS existente y los valores de ID del enrutador para los valores de dispositivo SD-WAN correspondientes.
- (Opcional) **as-number** : especifique el ASN del AS privado al que pertenece el enrutador virtual del hub o la sucursal. El complemento de SD-WAN admite solo sistemas autónomos privados. El ASN debe ser único para cada hub y sucursal. El intervalo de ASN de 4 bytes es de 4 200 000 000 a 4 294 967 294 o de 64 512,64512 a 65 535,65534. El intervalo de ASN de 2 bytes es de 64 512 a 65 534.

  Utilice un ASN privado de 4 bytes.

  Antes de implementar SD-WAN con enrutamiento BGP en un entorno donde BGP ya está en uso, asegúrese de que la configuración BGP generada por el complemento SD-WAN no entre en conflicto con su configuración BGP existente. Por ejemplo, debe utilizar el número BGP AS existente y los valores de ID del enrutador para los valores de dispositivo SD-WAN correspondientes.
- (Opcional) **ipv4-bgp-enable**: especifique sí o no para habilitar o deshabilitar BGP para direcciones IPv4.
- (Opcional) **loopback-address**: especifique una dirección IPv4 estática de bucle invertido para el emparejamiento BGP. El complemento SD-WAN 3.1.1 y las versiones posteriores a 3.1 son compatibles con una dirección de bucle invertido IPv6 para el emparejamiento BGP.
- (Opcional) **remove-private-as**: indique que no se deshabilite la opción Quitar AS privada (la opción predeterminada es habilitada) si tiene endpoints que necesitan intercambiar rutas con un cortafuegos de hub o sucursal en una topología BGP SD-WAN y, por lo tanto, no desea quitar los números AS privados (64512 a 65534) del atributo AS_PATH en Actualizaciones BGP.

  Este ajuste se aplica a todos los grupos de pares BGP en el cortafuegos de sucursal o hub. Si necesita que esta configuración difiera entre los grupos de pares BGP o pares, debe establecer la configuración por fuera del complemento SD-WAN.
- (Opcional) **prefix-redistribute**: especifique los prefijos de IP que según la sucursal puede alcanzar un hub. Para añadir más de un prefijo, sepárelos con un espacio, un signo de ampersand (&) y un espacio; por ejemplo, 192.2.10.0/24 & 192.168.40.0/24. De forma

predeterminada, el cortafuegos de la sucursal informa de todos los prefijos de Internet conectados localmente al hub.

Palo Alto Networks no redistribuye la o las rutas predeterminadas de la sucursal obtenidas del ISP.

- (Opcional) **ipv6-bgp-enable**: especifique sí/no para habilitar/deshabilitar BGP para direcciones IPv6.
- (Opcional) **ipv6-loopback-address**: especifique una dirección IPv6 estática de bucle invertido para el emparejamiento BGP.
- (Opcional) **ipv6-prefix-redistribute:**introduzca los prefijos IPv6 para redistribuirlos al enrutador hub desde la sucursal. De forma predeterminada, todos los prefijos de IPv6 de internet conectados localmente se anuncian en la ubicación del hub.
- (Opcional) **copy-tos-header**: especifique sí/no para habilitar/deshabilitar esta opción para copiar el encabezado de Tipo de servicio (TOS) del encabezado IP interno al encabezado IP externo de los paquetes encapsulados para preservar la información del TOS original.
- **authentication-type**: especifique el tipo de autenticación que admite el dispositivo (hub o sucursal): clave precompartida o autenticación de certificado.
- (Solo para el tipo de autenticación de **Certificate [Certificado]**) **certificate-name**: introduzca un nombre de certificado. El nombre distingue entre mayúsculas y minúsculas y puede tener hasta 63 caracteres en el cortafuegos o hasta 31 caracteres en Panorama. Debe ser exclusivo y utilizar únicamente letras, números, guiones y guiones bajos.

  Para el tipo de autenticación de clave precompartida, este campo debe dejarse vacío.

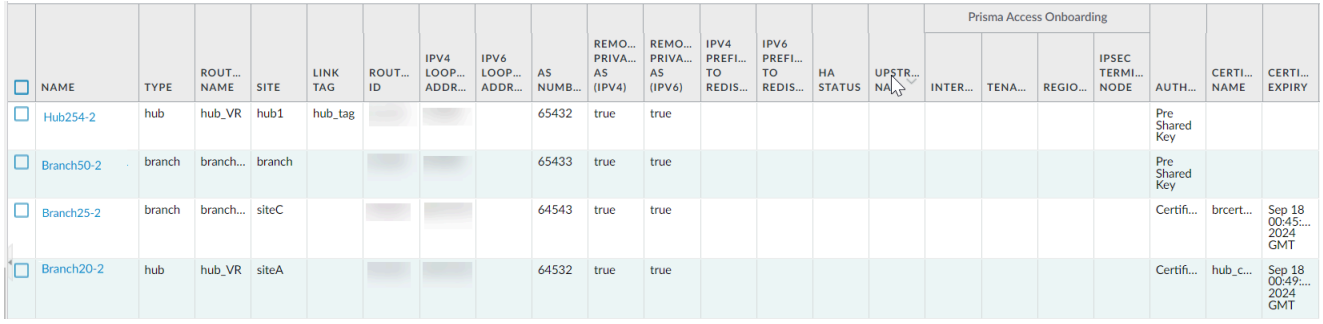
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	device-serial	type	site	router-name	vif-link-tag	router-id	as-number	ipv4-bgp-enable	loopback-addres	remove-private-a	prefix-redistribut	ipv6-bgp-enable	ipv6-loopback-a	ipv6-prefix-redis	copy-tos-he	authentication-ty	certificate-name
2		hub	hub1	hub_VR			65520			yes						pre-shared-key	
3		branch	branch	branch_VR			65501			yes						pre-shared-key	
4		branch	siteC	branch_VR			65502			yes						certificate	brcert1_cacert
5		hub	siteA	hub_VR			65525			yes						certificate	hub_cacert
6																	

STEP 4 | Importe el CSV de dispositivo de SD-WAN en Panorama.

Compruebe que no haya confirmaciones pendientes en Panorama. De lo contrario, se producirá un error en la importación.

1. En Panorama, seleccione **Panorama** > **SD-WAN** > **Dispositivos** > **CSV para dispositivo** e **importe** el CSV que editó en el paso anterior.
2. **Examine** y seleccione el CSV de dispositivo de SD-WAN.
3. Haga clic en **Aceptar** para importar los dispositivos de SD-WAN.

STEP 5 | Compruebe que sus dispositivos de SD-WAN se hayan añadido correctamente.



NAME	TYPE	ROUT... NAME	SITE	LINK TAG	ROUT... ID	IPV4 LOOP... ADDR...	IPV6 LOOP... ADDR...	AS NUMB...	REMO... PRIVA... AS (IPV4)	REMO... PRIVA... AS (IPV6)	IPV4 PREFI... TO REDIS...	IPV6 PREFI... TO REDIS...	HA STATUS	UPSTR... NA...	Prisma Access Onboarding: INTER...	TENA...	REGIO...	IPSEC TERMI... NODE	AUTH...	CERTI... NAME	CERTI... EXPIRY
Hub254-2	hub	hub_VR	hub1	hub_tag				65432	true	true									Pre Shared Key		
Branch50-2	branch	branch...	branch					65433	true	true									Pre Shared Key		
Branch25-2	branch	branch...	siteC					64543	true	true									Certifi...	brcert...	Sep 18 00:45:... 2024 GMT
Branch20-2	hub	hub_VR	siteA					64532	true	true									Certifi...	hub_c...	Sep 18 00:49:... 2024 GMT

STEP 6 | Haga clic en **Commit (Confirmar)** para aceptar los cambios en la configuración.

STEP 7 | Seleccione **Enviar a dispositivos** para enviar sus cambios de configuración a sus cortafuegos gestionados.

Incorporación de cortafuegos PAN-OS a Prisma Access

El complemento SD-WAN 2.2 proporciona compatibilidad con el hub de Prisma Access, en la que los cortafuegos PAN-OS que se conectan a los nodos de cómputo (CN) de Prisma Access logran seguridad basada en la nube en una topología hub-and-spoke de SD-WAN. En esta topología, los hubs de SD-WAN son CN (nodos de terminación IPSec) de Prisma Access y las sucursales de SD-WAN son cortafuegos PAN-OS. Se admite un máximo de cuatro hubs (cualquier combinación de hubs de PAN-OS que participen en los hubs de AnyPath de DIA y de Prisma Access). SD-WAN crea automáticamente túneles IKE e IPSec que conectan la sucursal al hub. Revise los requisitos del sistema para SD-WAN y Prisma Access.

Es importante configurar Prisma Access primero y luego configurar SD-WAN.

- *Si está iniciando una nueva configuración de Prisma Access, lea la Guía del administrador de Prisma Access y complete los pasos de configuración de la fase 1 y luego los de la fase 2.*
- *Si ya tiene Prisma Access ejecutándose, asegúrese de que la fase 1 esté completa y luego complete la fase 2.*

El siguiente diagrama de flujo muestra el orden de las dos fases de configuración y los pasos básicos dentro de cada fase. Los requisitos previos completos de Prisma Access con enlaces y los pasos de configuración para SD-WAN siguen el diagrama de flujo.

FASE 1: ACCESO A PRISMA (COMPLETAR FASE 1 PRIMERO)	FASE 2: SD-WAN (COMENZAR SOLO DESPUÉS DE COMPLETAR LA FASE 1)
1. Configure la subred de infraestructura, la infraestructura AS de BGP, la pila de plantillas y el grupo de dispositivos para un inquilino. 2. Configure las pilas de plantillas, las plantillas, los grupos de dispositivos, las	1. Configure un cortafuegos de sucursal con una interfaz que tenga SD-WAN habilitado. 2. Inicio de sesión en la interfaz web de Panorama.

FASE 1: ACCESO A PRISMA (COMPLETAR FASE 1 PRIMERO)	FASE 2: SD-WAN (COMENZAR SOLO DESPUÉS DE COMPLETAR LA FASE 1)
zonas fiables y no fiables y la asignación de ancho de banda para regiones específicas. 3. Asegúrese de que la implementación de Prisma Access tenga licencia para redes remotas. 4. Asegúrese de que la implementación asigne ancho de banda por ubicación de cómputo, en lugar de por ubicación. 5. Asegúrese de haber asignado ancho de banda a la ubicación de cómputo que corresponde a la ubicación a la que desea incorporarse. 6. Realice una confirmación local y haga el envío a la nube de Prisma Access.	3. Especifique el grupo de direcciones locales de BGP para las direcciones de bucle invertido. 4. Seleccione el cortafuegos de sucursal SD-WAN para conectarse al hub de Prisma Access y configure la conexión. 5. Confirme y envíe la configuración a la nube. 6. Verifique que la incorporación esté completa. 7. Sincronice el cortafuegos de sucursal con Prisma Access. 8. Confirmar en Panorama. 9. Envíe a dispositivos. 10. Observe la nueva interfaz que se creó. 11. Verifique que el túnel IPSec esté activo. 12. Verifique que la puerta de enlace IKE esté activa. 13. Cree una regla de políticas SD-WAN para generar datos de supervisión. 14. Confirme y luego confirme y envíe a los cortafuegos de sucursal. 15. Supervise el rendimiento de la aplicación y del enlace del hub de Prisma Access.

Antes de conectar SD-WAN a Prisma Access, debe tener un cortafuegos de sucursal con una interfaz que tenga SD-WAN habilitado. Además, asegúrese de haber realizado los siguientes requisitos previos de Prisma Access para uno o más inquilinos; estos son los pasos de la fase 1:

1. Para **la configuración** > **servicios en la nube** > **Panorama**, configure la subred de infraestructura, la infraestructura AS de BGP, la pila de plantillas y el grupo de dispositivos para un inquilino en la página **Service Setup (Configuración del servicio)** .
2. En la página **Remote Networks (Redes remotas)**, configure pilas de plantillas, plantillas, grupos de dispositivos, zonas fiables y no fiables y la asignación de ancho de banda para regiones específicas.

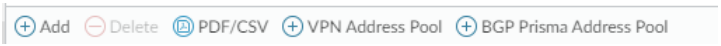
3. Asegúrese de que su implementación de Prisma Access cuente con Licencia para redes remotas seleccionando **Panorama** > **Licenses (Licencias)** y verificando la información de su licencia.
   - Las licencias disponibles después del 17 de noviembre de 2020 muestran el volumen de ancho de banda con licencia que tiene para redes remotas en la zona de **Net Capacity (Capacidad neta)**.
   - Las licencias disponibles antes del 17 de noviembre de 2020 muestran el ancho de banda de red remota disponible en el área **GlobalProtect Cloud Service for Remote Networks (Servicio en la nube de GlobalProtect para redes remotas)** en **Total Mbps (Mbps totales)**.
4. Asegúrese de que la implementación asigne ancho de banda por ubicación de cómputo, en lugar de por ubicación.
5. Asegúrese de haber asignado ancho de banda a la ubicación de cómputo que corresponde a la ubicación a la que desea incorporarse. Prisma Access asigna un nodo de terminación IPSec por cada 500 Mbps de ancho de banda que se asigne a una región.
6. Realice una confirmación local y haga el envío a la nube de Prisma Access.

Después de haber realizado los pasos anteriores para la fase 1 con Prisma Access, realice los siguientes pasos de la fase 2 para SD-WAN.

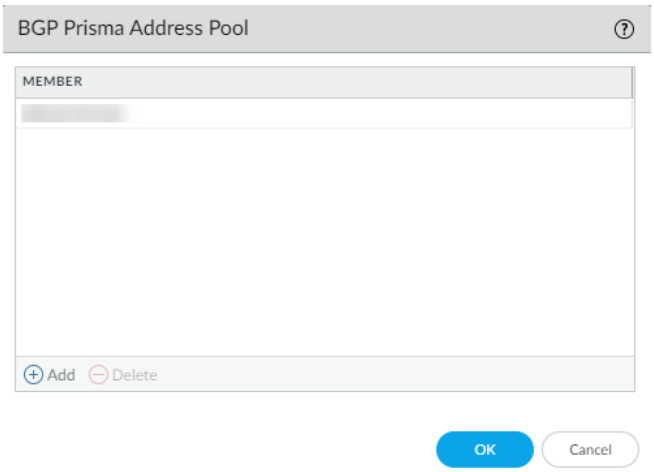
STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Especifique el grupo de direcciones locales de BGP para las direcciones de bucle invertido.

1. Seleccione **Panorama** > **SD-WAN** > **Clústeres de VPN**.
2. En la parte inferior de la pantalla, seleccione **BGP Prisma Address Pool (Grupo de direcciones BGP de Prisma)**.



3. **Agregue** una subred privada no utilizada (prefijo y máscara de red) para las direcciones BGP locales para Prisma Access.



4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Confirmar**.

No realice un simple cambio de un grupo de direcciones existente si Prisma Access ya está incorporado. Si necesita cambiar un grupo de direcciones, realice los siguientes pasos durante un periodo de mantenimiento para actualizar la sucursal SD-WAN y el CN de Prisma Access con los cambios de su grupo de direcciones:

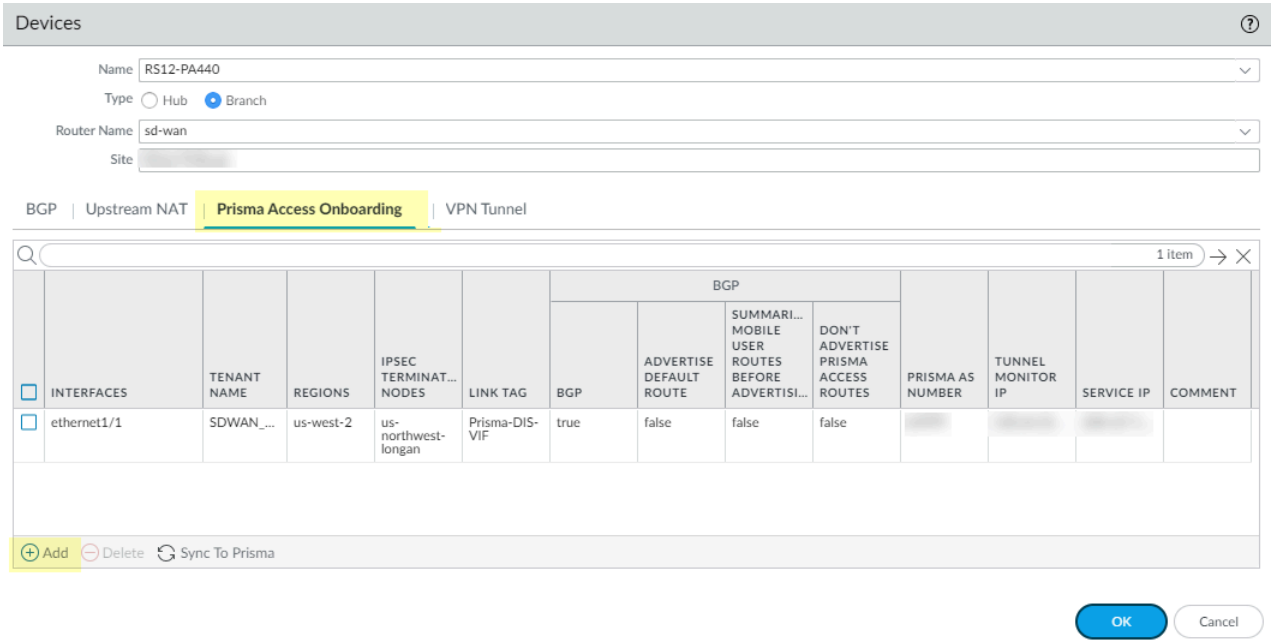
1. *Use Panorama para acceder a una sucursal SD-WAN y elimine la incorporación existente que afectará el cambio del grupo de direcciones; luego haga una confirmación local.*
2. *Actualice el grupo de direcciones VPN y luego realice una confirmación local.*
3. *Realice nuevamente la incorporación de Prisma Access y luego haga una confirmación local y el envío.*

STEP 3 | Seleccione el cortafuegos de sucursal SD-WAN para conectarse al hub de Prisma Access y configure la conexión.

1. Seleccione **Panorama** > **SD-WAN** > **Devices (Dispositivos)**.
2. Seleccione el cortafuegos de sucursal en el que habilitó SD-WAN, cuyo nombre completa el campo **Name (Nombre)** .
3. Seleccione el **tipo** de dispositivo como **sucursal**.
4. Seleccione el **nombre del enrutador**.
5. Ingrese al **sitio**.

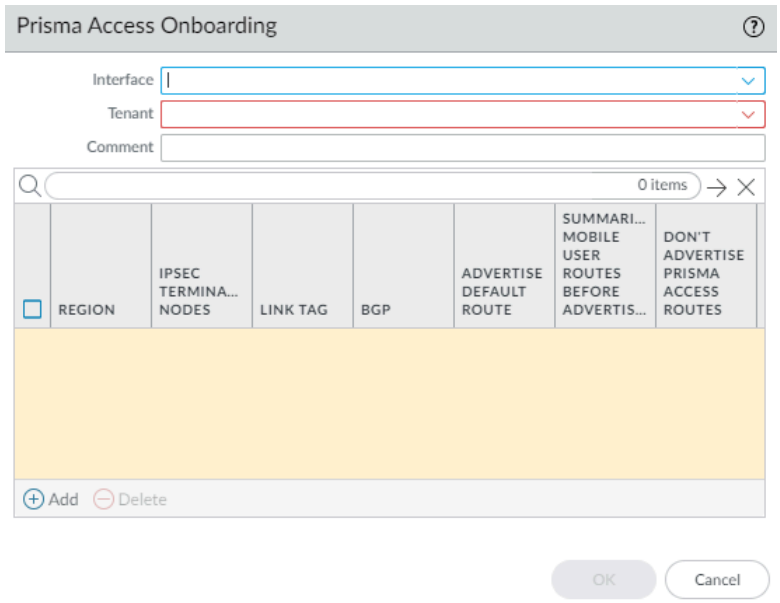
   Todos los dispositivos SD-WAN deben tener un nombre de sitio único.

6. Seleccione **Prisma Access Onboarding (Incorporación de Prisma Access)** y **Add (Agregar)**.



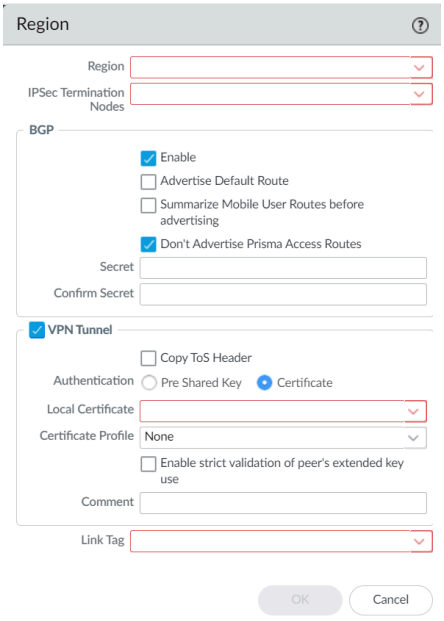
7. Seleccione una **interfaz** local habilitada para SD-WAN en el cortafuegos para conectarse al hub de Prisma Access.
8. Seleccione un **inquilino** de Prisma Access (seleccione el **valor predeterminado** para un entorno de inquilino único).

   Todas las interfaces SD-WAN en un cortafuegos de sucursal deben usar el mismo inquilino de Prisma Access.
9. Introduzca un **comentario**útil.



10. **Agregue** un nodo de cómputo a una **región** seleccionando la región donde se encuentra el CN (hub de Prisma Access).

    Puede haber varias regiones por interfaz.



11. Seleccione un **nodo de terminación IPSec** (puerta de enlace GP) de la lista de nodos; la lista se basa en los nodos que Prisma Access activó anteriormente para la región. Está

eligiendo el hub al que se conecta esta sucursal. La configuración de VPN automática de SD-WAN crea túneles y relaciones IKE e IPSec con este nodo.

12. **Habilite** BGP para la comunicación entre la sucursal y el hub (Viene habilitada de forma predeterminada).
13. **Anuncie la ruta predeterminada** para permitir que la ruta predeterminada del hub de Prisma Access se anuncie en el cortafuegos de sucursal.
14. **Resuma rutas de usuarios móviles antes de anunciar** para que el hub de Prisma Access anuncie rutas de subred de IP de usuarios móviles resumidas, reduciendo así la cantidad de anuncios en las sucursales.
15. **No anuncie la rutas de Prisma Access** para evitar que el hub/nodo de terminación de IPSec anuncie las rutas de Prisma Access en las sucursales de SD-WAN.
16. Ingrese el **secreto** para la autenticación de las comunicaciones BGP y **confirme el secreto**.
17. (Complemento SD-WAN 3.2.0 y versiones posteriores) Configure los parámetros del túnel VPN y el tipo de autenticación para autenticar el cortafuegos PAN-OS y el hub de Prisma Access.
    1. (Opcional) Si desea conservar la información de tipo de servicio (ToS) en los paquetes encapsulados, seleccione **Copy TOS Header (Copiar encabezado de TOS)**.

       Si hay varias sesiones dentro del túnel (cada una con un valor diferente de ToS), copiar el archivo ToS puede hacer que los paquetes IPSec lleguen desordenados.
    2. Seleccione la **Authentication (Autenticación)**: **Pre-Shared Key (Clave precompartida)** o **Certificate (Certificado)**.

       Asegúrese de seleccionar el mismo tipo de autenticación para todos los dispositivos de sucursal y el dispositivo Prisma Access que se añade.

       La clave precompartida se genera de forma automática si se selecciona como tipo de autenticación para una región.
18. Seleccione **Certificate (Certificado)** para configurar la autenticación basada en certificados.
19. (Solo si se habilita el tipo de autenticación por **Certificate (Certificado)**) El certificado debe estar presente en el Panorama antes de realizar la incorporación de Prisma Access del cortafuegos de sucursal SD-WAN. El certificado generado por SCEP no es

compatible. Seleccionar un **Local Certificate (Certificado local)**: uno que ya está en el Panorama.

Asegúrese de lo siguiente para el certificado que tiene en el Panorama para que el proceso de incorporación de Prisma Access se realice correctamente:

- El certificado debe ser único para cada dispositivo SD-WAN. Es decir, no es posible compartir el certificado entre varios dispositivos SD-WAN.

  Tenga en cuenta lo siguiente al generar los certificados de cortafuegos de sucursales y hubs que se utilizan para la autenticación de túnel SD-WAN:

  - Dos dispositivos hubs diferentes pueden usar el mismo certificado de hubs.
  - Dos dispositivos de sucursales diferentes pueden utilizar certificados de la misma sucursal si se cumplen las siguientes condiciones:
    - Los dispositivos de sucursal no forman parte del mismo clúster de VPN
    - No hay ningún dispositivo hub común entre los clústeres de VPN de los que formarían parte estos dispositivos de sucursal
  - (Solo implementaciones de alta disponibilidad) Dos dispositivos de derivación diferentes también pueden tener los certificados de la misma sucursal si están configurados como miembros de alta disponibilidad.
  - Si el dispositivo de hub es común entre clústeres VPN, los certificados para dispositivos de sucursal que forman parte de estos clústeres VPN deben tener certificados únicos con todos los atributos que tienen valores únicos. Si no garantiza la exclusividad del certificado y sus valores, la confirmación fallará en el dispositivo de hub (sin fallo de confirmación en Panorama).

  > *Asegúrese también de que los certificados específicos (certificados de cortafuegos de sucursales y hubs) utilizados para la autenticación de túnel SD-WAN se generen cumpliendo los siguientes criterios:*
  >
  > - *El uso de claves debe tener firmas digitales*
  > - *Todos los certificados deben estar firmados por la misma CA raíz*
  > - *El certificado del dispositivo debe estar firmado directamente por la CA raíz*
  > - *El formato del certificado debe ser PKCS12*

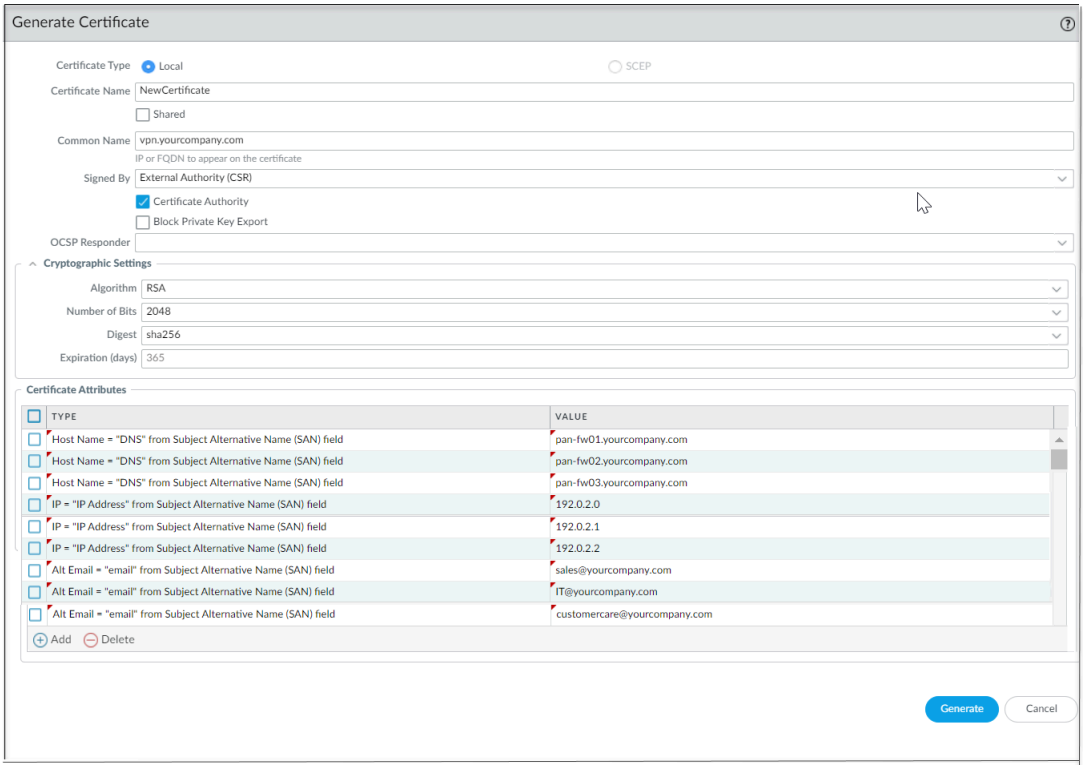
- Los atributos de certificado se utilizan para determinar el ID local y el ID de peer para las puertas de enlace IKE. Por lo tanto, los certificados específicos, es decir, los certificados de cortafuegos de sucursal y hub que se utilizan para la autenticación de túnel SD-WAN, deben generarse con los siguientes tres atributos de certificado y a cada atributo de certificado se le deben asignar tres valores de atributo únicos. De lo contrario, se lanzará un error de confirmación.
  - FQDN (**Host Name [Nombre de host]**)
  - IP Address [Dirección IP] (**IP**)

- User FQDN (FQDN de usuario) (**Alt Email [Correo electrónico Alt.]**)

> *Es obligatorio tener atributos de certificado exclusivos de **Host Name (Nombre de host)**, **IP**y **Alt Email (Correo electrónico Alt.)** entre todos los certificados. Es decir, ninguno de los certificados debe tener estos valores de atributo en común.*

En el ejemplo siguiente, NewCertificate se genera con el total de nueve atributos de certificado obligatorios. El atributo de certificado **Host Name (Nombre de host)** está configurado con tres valores de atributo únicos: pan-fw01.yourcompany.com, pan-fw02.yourcompany.com y pan-fw03.yourcompany.com. El atributo del certificado **IP** está configurado con tres valores de atributo únicos: 192.0.2.0, 192.0.2.1 y 192.0.2.2. El atributo de certificado **Alt Email (Correo electrónico Alt.)** se configura con tres

valores de atributo exclusivos: sales@yourcompany.com, IT@yourcompany.com y customercare@yourcompany.com.

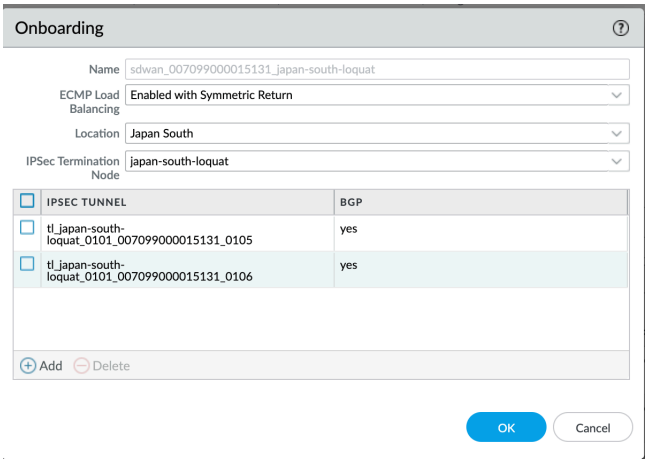


20. (Opcional) (Solo si se habilita el tipo de autenticación **Certificate [Certificado]**) Seleccione un **Certificate Profile (Perfil de certificado)**. Un Perfil de certificado contiene información sobre el modo de autenticar la puerta de enlace del peer.
21. (Opcional) Seleccione **Enable strict validation of peer's extended key use (Habilitar validación estricta de uso de clave extendida de peer)** para controlar de forma estricta cómo se puede utilizar la clave.
22. Seleccione una **etiqueta de enlace** para el hub.

    Cuando desee habilitar ECMP para un hub de Prisma Access, incorpore más de una interfaz de sucursal al mismo nodo de cómputo (CN) y use la misma etiqueta de enlace en esas interfaces de sucursal.
23. Haga clic en **OK (Aceptar)**. La pantalla incluirá un número AS de peer y la dirección IP de supervisión de túnel proporcionada por Prisma Access.

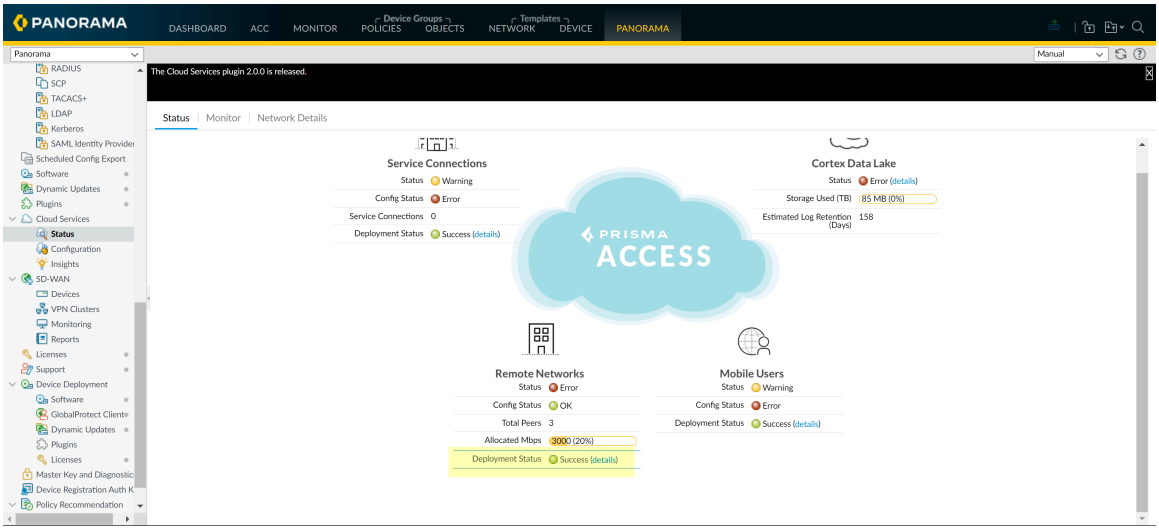
STEP 4 | **Confirmar y enviar** la configuración a la nube, donde Prisma Access activa la cantidad correcta de nodos de terminación IPSec en función del ancho de banda solicitado.

Cuando más de un túnel IPSec va al mismo CN, la configuración de Prisma Access tiene ECMP habilitado con retorno simétrico, como se muestra en este ejemplo de Prisma Access:

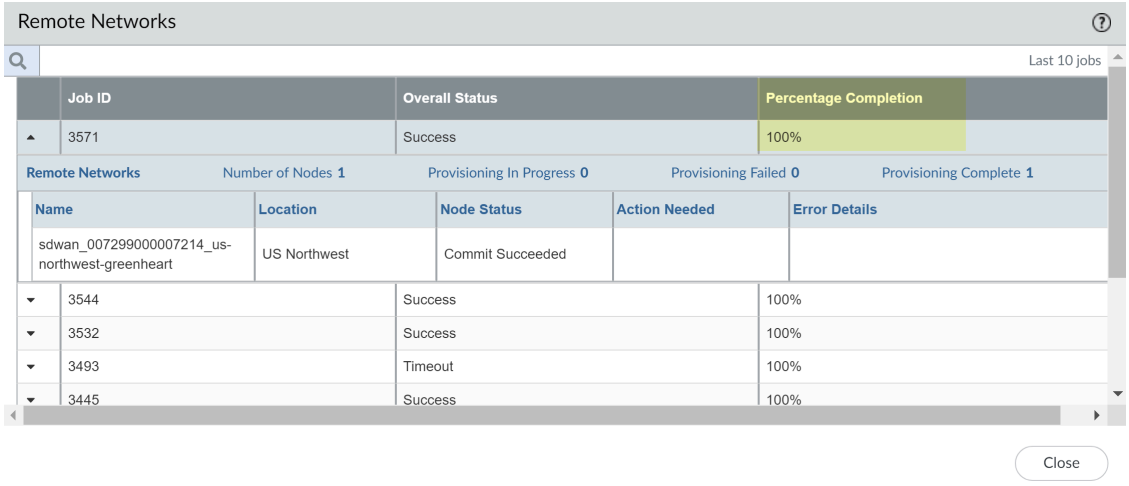


STEP 5 | Verifique que la incorporación esté completa.

1. Seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** y verifique que Remote Networks Deployment Status (Estado de implementación de redes remotas) muestre `success (correcto)`.



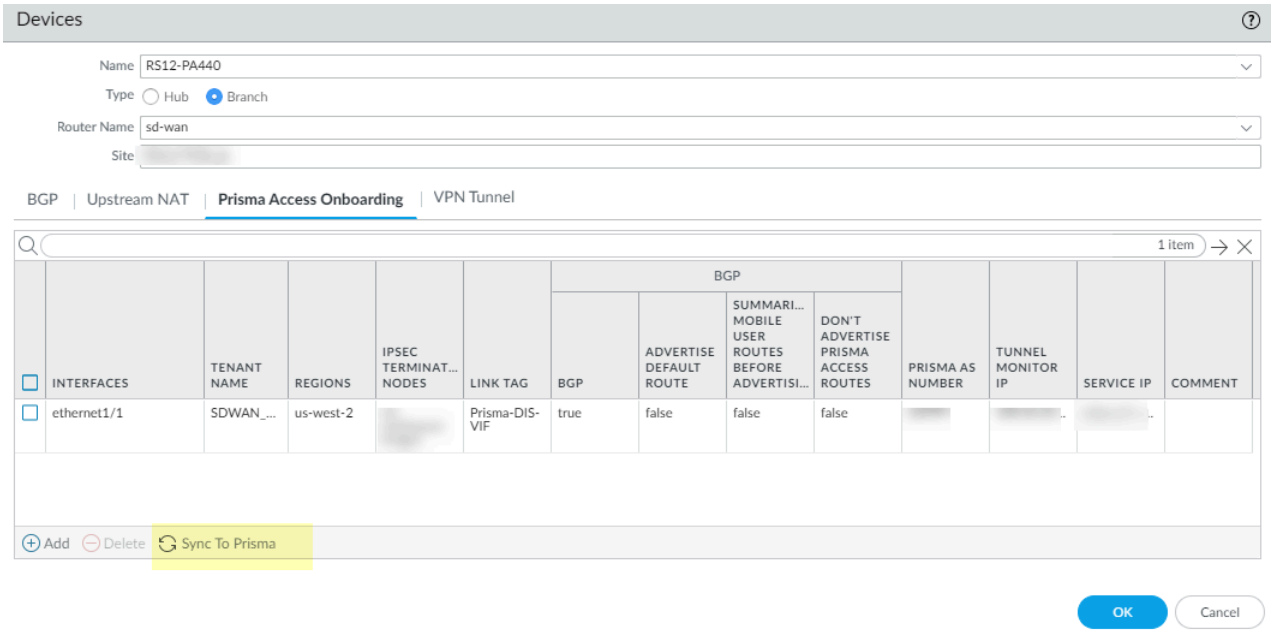
2. Seleccione los **detalles**del estado de implementación de redes remotas.
3. Confirme que la finalización del nodo de Prisma Access muestre 100 %.



STEP 6 | Sincronice el cortafuegos de sucursal con Prisma Access para recuperar las direcciones IP de servicio de los CN.

1. Seleccione **Panorama** > **SD-WAN** > **Devices (Dispositivos)**.
2. Seleccione el dispositivo de sucursal SD-WAN.
3. Seleccione **Prisma Access Onboarding (Incorporación de Prisma Access)** y **Sync To Prisma (Sincronizar con Prisma)** (y responda al mensaje para continuar). Repita para cada dispositivo de sucursal.

> *Después de que se realice una correcta sincronización con Prisma, verá los parámetros de configuración de Prisma Access en el cortafuegos de sucursal SD-WAN. De lo contrario, espere aproximadamente 15 minutos y repita la sincronización con Prisma. Si es necesario, vaya al complemento Prisma Access y verifique que la incorporación del CN haya finalizado (puede ver el CN con el ancho de banda y las direcciones IP asignadas). Después de esa verificación, vuelva a intentar sincronizar con Prisma.*



STEP 7 | **Commit (Confirmar)** en Panorama.

STEP 8 | **Realice el envío a dispositivos** para enviar al cortafuegos de sucursal local. **Edite las selecciones** para establecer la selección del ámbito de envío. Seleccione la **plantilla** y **el grupo de dispositivos**correctos.

STEP 9 | En el cortafuegos de sucursal, seleccione **Network (Red)** > **Interfaces** > **SD-WAN** y observe la nueva interfaz que se creó con la etiqueta de enlace que se creó, asignada a la zona de seguridad denominada **zone-to-pa-hub**, y con el túnel IPSec que se conecta al CN.

STEP 10 | Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)** y verifique que el túnel IPSec esté activo.

STEP 11 | Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace IKE)** y verifique que la puerta de enlace IKE esté activa.

STEP 12 | Cree una regla de políticas SD-WAN para generar datos de supervisión.

Este paso es necesario para establecer los valores de referencia de los datos de latencia, fluctuación y pérdida de paquetes del hub de Prisma Access para una distribución precisa del tráfico. Los datos de supervisión de SD-WAN se generan a partir del tráfico que coincide con las reglas de políticas de su SD-WAN.

1. Creación de un perfil de distribución de tráfico.
2. Creación de un perfil de calidad de ruta con umbrales altos de latencia, fluctuación y pérdida de paquetes.

   Se requiere un perfil de calidad de ruta para crear una regla de políticas de SD-WAN. La creación de un perfil de calidad de ruta con umbrales altos le permite establecer la latencia, la fluctuación y la pérdida de paquetes de referencia para el hub de Prisma Access sin que la aplicación cambie a un enlace diferente.
3. Configuración de una regla de políticas de SD-WAN.

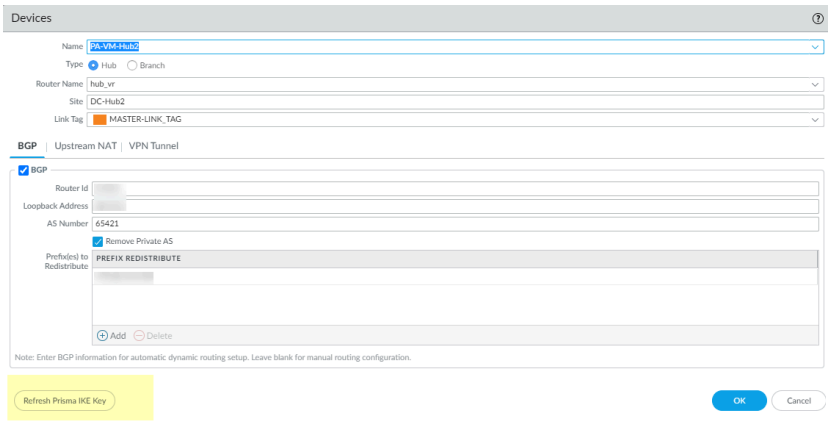
STEP 13 | **Confirme** y luego **confirme y envíe** al cortafuegos de sucursal.

STEP 14 | (Solo si se habilita el tipo de autenticación **Pre Shared Key [Clave precompartida]**) Actualice la clave precompartida de Prisma IKE.

Si necesita cambiar la clave IKE de Prisma actual que se usa para asegurar la conexión IPSec entre la sucursal y el hub de Prisma, realice este paso para generar aleatoriamente una nueva clave para el túnel y actualizar ambos lados del túnel. Realice este paso cuando el hub y la sucursal no estén ocupadas.

No cree una puerta de enlace IKE manualmente con un nombre que comience con "gw_" porque dichos nombres están reservados para la creación de IKE de Prisma durante la incorporación. Este paso para actualizar la clave precompartida IKE de Prisma actualiza todas las puertas de enlace IKE con nombre, si hubiera otras además de las creadas por Prisma Access.

1. Seleccione **Panorama** > **SD-WAN** > **Devices (Dispositivos)** y seleccione un dispositivo.
2. En el margen inferior de la pantalla, seleccione **Refresh Prisma IKE Key (Actualizar la clave IKE de Prisma)**.



3. Aparece un mensaje que le notifica que la `actualización de la clave IKE actualizará todos los túneles SD-WAN entre la sucursal y el hub de Prisma Access y requerirá el envío de una configuración simultánea a todos los dispositivos de sucursal y del hub de Prisma Access. La práctica recomendada es realizar la actualización durante una periodo de mantenimiento, ya que el tráfico puede verse afectado. ¿Desea continuar?` Seleccione `Yes (Sí)` si desea continuar.

STEP 15 | **Confirme** y luego **confirme y envíe** al cortafuegos de sucursal.

STEP 16 | Supervisión del rendimiento del enlace y de la aplicación de la central de Prisma Access para comprender la latencia de referencia, la fluctuación y la pérdida de paquetes de los enlaces para Prisma Access.

Este paso es necesario para recopilar datos precisos de latencia, fluctuación y pérdida de paquetes para configurar con precisión los perfiles de calidad de rutadel hub de Prisma Access.

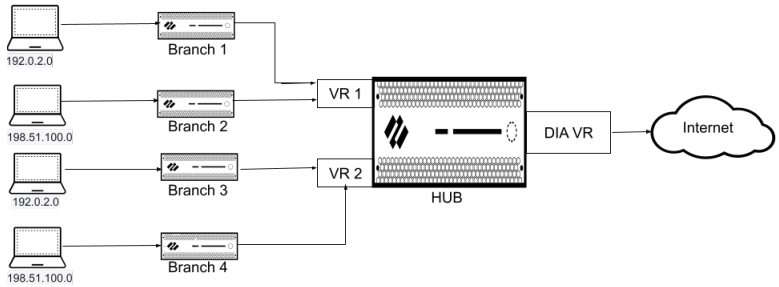
Configurar varios enrutadores virtuales en el hub de SD-WAN

¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

(PAN-OS 11.1.3 y versiones posteriores, y SD-WAN Plugin 3.2.1 y versiones posteriores) Hemos introducido compatibilidad con varios enrutadores virtuales en el hub de SD-WAN que le permiten tener direcciones de subred IP superpuestas en dispositivos de sucursal que se conectan al mismo hub de SD-WAN. Con esta característica puede tener varios dominios de enrutamiento lógico con subredes superpuestas. Cuando habilita esta función, el hub de SD-WAN admite subredes superpuestas solo si las subredes superpuestas se encuentran en enrutadores virtuales diferentes.

De forma predeterminada, la opción de varios enrutadores virtuales en un hub de SD-WAN está deshabilitada.

La siguiente figura ilustra un hub de SD-WAN con dos enrutadores virtuales. Al habilitar la **compatibilidad con varios enrutadores virtuales** en el hub de SD-WAN, las cuatro sucursales que se conectan al mismo hub SD-WAN pueden tener subredes IP superpuestas o pertenecer a diferentes entidades y funcionar de forma independiente porque su tráfico va a diferentes enrutadores virtuales.



La función de varios enrutadores virtuales es compatible tanto con el cortafuegos de hub de SD-WAN como con el hub de Prisma Access. Puede incorporar Prisma Access como hub desde la sucursal, cuando la sucursal está conectada a un hub local donde está habilitada la función de enrutador virtual múltiple.

Configure varios enrutadores virtuales mientras añade un cortafuegos de hub de SD-WAN (**Panorama** > **SD-WAN** > **Devices (Dispositivos)**).

La importación de varias configuraciones relacionadas con enrutadores virtuales mediante un archivo CSV mientras se importa el dispositivo SD-WAN no es compatible.

Apoyamos el enrutamiento avanzado cuando los múltiples enrutadores virtuales en el hub SD-WAN están habilitados.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Devices (Dispositivos)** y luego **Add (Añadir)** para añadir un nuevo cortafuegos SD-WAN.

Mientras crea una plantilla de hub, añada todos los enrutadores virtuales que participan en el hub de SD-WAN donde se habilitará el enrutador virtual múltiple. Debe hacer esto antes de añadir el dispositivo SD-WAN utilizando el complemento SD-WAN. Mientras crea la plantilla de hub, asegúrese de que el nombre del enrutador virtual en la sucursal coincida con uno de los enrutadores virtuales en el hub.

STEP 3 | Para configurar varios enrutadores virtuales en el hub de SD-WAN:

- Seleccione el **Type (Tipo)** de dispositivo SD-WAN como **Hub**.
- Seleccione **Enable Multi-VR Support (Habilitar compatibilidad con varias VR)**.

El enrutador virtual seleccionado para el **Virtual Router Name (Nombre del enrutador virtual)** se utiliza como enrutador virtual de acceso directo a internet (DIA) del hub y se considera el enrutador virtual predeterminado. La configuración especificada en la pestaña **BGP** debe ser específica del enrutador virtual DIA.

- *No admitimos FEC ni duplicación de paquetes cuando la función de varios enrutadores virtuales está habilitada en el hub de SD-WAN.*
- *La característica de varios enrutadores virtuales en el hub de SD-WAN es compatible solo en una topología hub-spoke (y no se admite en una topología de malla completa).*
- *Para procesar el tráfico de Internet en el hub de SD-WAN, la política de SD-WAN debe garantizar que la etiqueta MPLS se seleccione solo cuando el enlace MPLS tenga acceso a Internet y NAT.*
- *PAN-OS no admite el reenvío de tráfico en texto no cifrado (cuando la **VPN Data Tunnel Support (Compatibilidad de túnel de datos de VPN)** está deshabilitada en el **SD-WAN Interface Profile (Perfil de interfaz SD-WAN)** fuera del túnel VPN SD-WAN cuando se habilitan varios enrutadores virtuales compatibles con la función de hub de SD-WAN.*

El número de enrutadores virtuales compatibles con los cortafuegos de Palo Alto Networks es el siguiente:

Cortafuegos de Palo Alto Networks	Número máximo de enrutadores virtuales admitidos	Número máximo de enrutadores virtuales de hub de SD-WAN admitidos
PA-3400	11	10
PA-5220 y PA-5410	20	20

Cortafuegos de Palo Alto Networks	Número máximo de enrutadores virtuales admitidos	Número máximo de enrutadores virtuales de hub de SD-WAN admitidos
PA-5250 y PA-5430	125	50
PA-5420	50	20
PA-5260, PA-5280, PA-5400, PA-5440, PA-5445, y PA-7000.	225	50

STEP 4 | (Opcional) Configurar enrutadores virtuales.

1. Seleccione la pestaña **Virtual Routers (Enrutadores virtuales)** para configurar varios enrutadores virtuales para el hub de SD-WAN.
2. El enrutamiento BGP utiliza IPv4 de forma predeterminada y, por lo tanto, **Enable IPv4 BGP Support (Habilitar la compatibilidad con IPv4 BGP)** está habilitado y no puede cambiar esta configuración.
3. Introduzca el nombre del **Virtual Router (Enrutador virtual)**.
4. Seleccione una **Zone (Zona)** ya creada en la plantilla de del hub (**Network [Red]** > **Zones [Zonas]**) que sea apropiada para el enrutador virtual que está configurando.

   *Si configura la misma zona para dos o más enrutadores virtuales en la **Multi-VR Configuration (Configuración de varios VR)**, asegúrese de que los enrutadores virtuales no estén configurados con las subredes superpuestas.*
5. (Opcional) Introduzca el **Router ID (ID del enrutador)** virtual, que debe ser único entre todos los enrutadores.
6. Especifique una **dirección de bucle invertido** IPv4 estática para el establecimiento de peers de BGP. La configuración de VPN automática crea una interfaz de bucle invertido de forma automática con la misma dirección IPv4 que especifique. Si especifica una dirección de bucle invertido existente, la confirmación fallará, por lo que debe especificar una dirección IPv4 que no sea ya una dirección de bucle invertido.
7. Introduzca el **número de sistema autónomo**. El número de sistema autónomo (número AS) especifica una política de enrutamiento comúnmente definida para Internet. El número AS debe ser único para cada ubicación del hub y la sucursal.
8. Inhabilite la opción **Quitar AS privada** (por configuración predeterminada, está habilitado) si tiene endpoints que necesitan intercambiar rutas con un cortafuegos de hub o sucursal en una topología BGP SD-WAN y, por lo tanto, no desea quitar los números AS privados (64512 a 65534) del atributo AS_PATH en Actualizaciones BGP.

En este caso, debe permitir que los números AS privados salgan del AS privado SD-WAN en las actualizaciones de BGP.

*La configuración **Quitar AS privada** aplica a todos los grupos de par BGP en el cortafuegos de sucursal o hub. Si necesita que esta configuración difiera entre los grupos de pares BGP o pares, debe establecer la configuración por fuera del complemento SD-WAN.*

*Si cambia la configuración **Remove Private AS (Eliminar AS privado)**, debe compilar todos los nodos del clúster SD-WAN y, posteriormente, cambiar a una versión inferior del complemento SD-WAN anterior a la 2.0.2. Por ende, toda la configuración relacionada con **Remove Private AS (Eliminar AS privado)** debe aplicarse por fuera del complemento SD-WAN o directamente en los cortafuegos.*

9. Especifique **Prefijo(s) que redistribuir**. En un dispositivo de hub, debe introducir al menos un prefijo que redistribuir.
10. Haga clic en **OK (Aceptar)**.
11. Haga clic en **Add (Añadir)** en la parte inferior de la pestaña **Virtual Routers (Enrutadores virtuales)** para añadir más enrutadores virtuales.

Configurar varios enrutadores virtuales en la sucursal SD-WAN

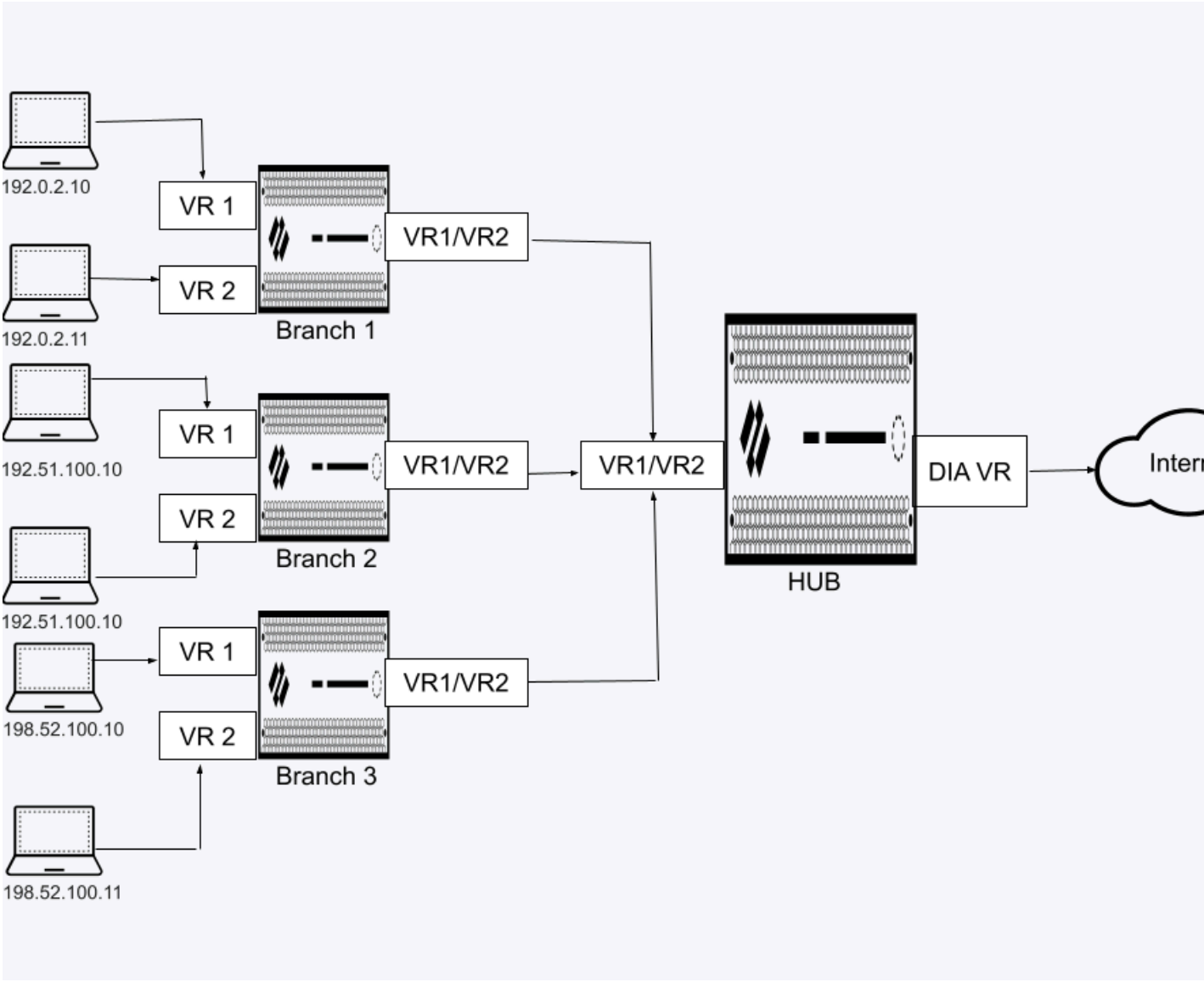
¿Dónde puedo usar esto?	¿Qué necesito?
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

(PAN-OS 11.2.3 y versiones posteriores a 11.2, y complemento SD-WAN 3.3.1 y versiones posteriores a 3.3) Hemos introducido compatibilidad para varios enrutadores virtuales en las sucursales de SD-WAN para tener direcciones de subred IP superpuestas tanto en dispositivos de hub como de sucursal. Con esta función puede tener varios dominios de enrutamiento lógico con subredes superpuestas.

Asegúrese de lo siguiente antes de habilitar los varios enrutadores virtuales en los dispositivos de sucursal SD-WAN:

- El dispositivo de hub, al que están conectadas las sucursales debe ser compatible para varios enrutadores virtuales.
- Los dispositivos de hub a los que se conectan las sucursales deben tener todos los enrutadores virtuales presentes en los dispositivos de las sucursales.
- En un clúster VPN, para que las sucursales tengan la compatibilidad con varios enrutadores virtuales, primero debe habilitar la compatibilidad con varios enrutadores virtuales en todos los hubs.

La siguiente figura ilustra tres sucursales SD-WAN con cada una configurada con uno o más enrutadores virtuales. Al permitir la **compatibilidad con varios enrutadores virtuales** en las sucursales SD-WAN, las tres sucursales que se conectan al mismo hub de SD-WAN pueden tener subredes IP superpuestas o pertenecer a diferentes entidades y funcionar de forma independiente porque su tráfico va a diferentes enrutadores virtuales.



STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Devices (Dispositivos)** y luego **Add (Añadir)** para añadir un nuevo cortafuegos SD-WAN.

STEP 3 | Para configurar varios enrutadores virtuales en el dispositivo de sucursal SD-WAN:

- Seleccione el **Type (Tipo)** de dispositivo SD-WAN como **Branch (Sucursal)**.
- Seleccione **Enable Multi-VR Support (Habilitar compatibilidad con varias VR)**.

El enrutador virtual seleccionado para el **Virtual Router Name (Nombre del enrutador virtual)** se utiliza como enrutador virtual de acceso directo a internet (DIA) de la sucursal y se

considera el enrutador virtual predeterminado. La configuración especificada en la pestaña **BGP** debe ser específica del enrutador virtual DIA.

- *No admitimos FEC ni duplicación de paquetes cuando la función de varios enrutadores virtuales está habilitada en la sucursal de SD-WAN.*
- *La característica de varios enrutadores virtuales en la sucursal de SD-WAN es compatible solo en una topología hub-spoke (y no se admite en una topología de malla completa).*
- *Para procesar el tráfico de Internet en la sucursal de SD-WAN, la política de SD-WAN debe garantizar que la etiqueta MPLS se seleccione solo cuando el enlace MPLS tenga acceso a Internet y NAT.*
- *PAN-OS no admite el reenvío de tráfico en texto no cifrado (cuando la **VPN Data Tunnel Support (Compatibilidad de túnel de datos de VPN)** está deshabilitada en el **SD-WAN Interface Profile (Perfil de interfaz SD-WAN)** fuera del túnel VPN SD-WAN cuando se habilitan varios enrutadores virtuales compatibles con la función de sucursal de SD-WAN.*

Un máximo de 20 enrutadores virtuales son compatibles con el dispositivo de sucursal SD-WAN. Sin embargo, el número de enrutadores virtuales compatibles con la sucursal SD-WAN varía según la plataforma:

Cortafuegos Palo Alto Networks	Enrutadores virtuales máximos compatibles	Número máximo de enrutadores virtuales de sucursal SD-WAN compatibles
PA-460	5	5
PA-450	5	5
PA-445	3	3
PA-440	3	3
PA-415	3	3
PA-1420	10	10
PA-1410	10	10
PA-850	5	5
PA-820	5	5

Cortafuegos Palo Alto Networks	Enrutadores virtuales máximos compatibles	Número máximo de enrutadores virtuales de sucursal SD-WAN compatibles
PA-3200	10	10

STEP 4 | (Opcional) Configurar enrutadores virtuales.

1. Seleccione la pestaña **Virtual Routers (Enrutadores virtuales)** para configurar varios enrutadores virtuales para la sucursal de SD-WAN.
2. El enrutamiento BGP utiliza IPv4 de forma predeterminada y, por lo tanto, **Enable IPv4 BGP Support (Habilitar la compatibilidad con IPv4 BGP)** está habilitado y no puede cambiar esta configuración.
3. Introduzca el nombre del **Virtual Router (Enrutador virtual)**.
4. Seleccione una zona única para el enrutador virtual.

   En un clúster VPN con configuración de enrutador virtual múltiple, cada dispositivo (sucursal o hub) con enrutador virtual que participa en la configuración de enrutador virtual múltiple debe tener una zona única.
5. (Opcional) Introduzca el **Router ID (ID del enrutador)** virtual, que debe ser único entre todos los enrutadores.
6. Especifique una **dirección de bucle invertido** IPv4 estática para el establecimiento de peers de BGP. La configuración de VPN automática crea una interfaz de bucle invertido de forma automática con la misma dirección IPv4 que especifique. Si especifica una dirección de bucle invertido existente, la confirmación fallará, por lo que debe especificar una dirección IPv4 que no sea ya una dirección de bucle invertido.
7. Introduzca el **número de sistema autónomo**. El número de sistema autónomo (número AS) especifica una política de enrutamiento comúnmente definida para Internet. El número AS debe ser único para cada ubicación del hub y la sucursal.
8. Inhabilite la opción **Quitar AS privada** (por configuración predeterminada, está habilitado) si tiene endpoints que necesitan intercambiar rutas con un cortafuegos de hub o sucursal en una topología BGP SD-WAN y, por lo tanto, no desea quitar los números AS privados (64512 a 65534) del atributo AS_PATH en Actualizaciones BGP.

En este caso, debe permitir que los números AS privados salgan del AS privado SD-WAN en las actualizaciones de BGP.

*La configuración **Quitar AS privada** aplica a todos los grupos de par BGP en el cortafuegos de sucursal o hub. Si necesita que esta configuración difiera entre los grupos de pares BGP o pares, debe establecer la configuración por fuera del complemento SD-WAN.*

*Si cambia la configuración **Remove Private AS (Eliminar AS privado)**, debe compilar todos los nodos del clúster SD-WAN y, posteriormente, cambiar a una versión inferior del complemento SD-WAN anterior a la 2.0.2. Por ende, toda la configuración relacionada con **Remove Private AS (Eliminar AS privado)** debe aplicarse por fuera del complemento SD-WAN o directamente en los cortafuegos.*

9. Especifique **Prefijo(s) que redistribuir**. En un dispositivo de hub, debe introducir al menos un prefijo que redistribuir.
10. Haga clic en **OK (Aceptar)**.
11. Haga clic en **Add (Añadir)** en la parte inferior de la pestaña **Virtual Routers (Enrutadores virtuales)** para añadir más enrutadores virtuales.

Configuración de dispositivos de HA para SD-WAN

Puede configurar dos cortafuegos como una sucursal en modo HA activo/pasivo (o dos cortafuegos como una central en modo HA activo/pasivo) para que formen parte del entorno SD-WAN. En este caso, Panorama™ necesita enviar la misma configuración al peer activo y pasivo en lugar de tratar los dos cortafuegos individualmente. Para que esto suceda, debe configurar la HA activa/pasiva antes de añadir los dispositivos para SD-WAN de modo que Panorama sepa que los dispositivos son peers de HA y les envíe la misma configuración. (Solo se admite el modo HA activo/pasivo).

Lea el siguiente procedimiento antes de comenzar para no confirmar después de añadir sus peers de HA como dispositivos de SD-WAN.

En HA, el cortafuegos no sincroniza las estadísticas de distribución de sesiones SD-WAN. Después de una conmutación por error de HA, las estadísticas de distribución de la sesión muestran solo las estadísticas de las nuevas sesiones; las estadísticas de las sesiones existentes se pierden.

STEP 1 | Antes de habilitar SD-WAN en sus peers de HA, configure la HA activa/pasiva en dos modelos de cortafuegos compatibles con SD-WAN.

STEP 2 | Añada los peers de HA como dispositivos de SD-WAN, **pero no realice el último paso para confirmar**.

STEP 3 | En Panorama, seleccione **Panorama** > **Dispositivos gestionados** > **Resumen**.

STEP 4 | En la parte inferior de la pantalla, seleccione **Agrupar peers de HA**. Confirme que debajo de la pantalla Estado, la columna Estado de HA incluya los dos cortafuegos, uno activo y uno pasivo. Panorama conoce el estado de la HA y enviará la misma configuración de SD-WAN a los dos peers de HA cuando confirme.

STEP 5 | Seleccione las opciones **Confirmar** y **Confirmar y enviar**.

Creación de un clúster de VPN

En su configuración de SD-WAN, debe configurar uno o más grupos de VPN para determinar qué sucursales se comunican con qué hubs y crean una conexión segura entre la sucursal y los dispositivos del hub. Los clústeres de VPN son agrupaciones lógicas de dispositivos, así que tenga en cuenta elementos como la ubicación geográfica o la función al agrupar lógicamente sus dispositivos.

PAN-OS® admite topologías de VPN SD-WAN de hub y de malla completa. En una topología hub-spoke, un hub de cortafuegos centralizado en una oficina o ubicación principal actúa como la puerta de enlace entre dispositivos de la sucursal. La conexión de hub a sucursal es un túnel VPN. En esta configuración, el tráfico entre sucursales debe pasar por el hub.

La primera vez que Configuración de una interfaz de SD-WAN virtual con enlaces de acceso de Internet directo (DIA) para un cortafuegos de hub o sucursal, se crea automáticamente un clúster de VPN denominado `autogen_hubs_cluster` y el cortafuegos de SD-WAN se añade automáticamente al clúster de VPN. Esto permite que el servidor de gestión Panorama™ Supervisión del rendimiento del enlace y de la aplicación de SD-WAN para dispositivos protegidos por el cortafuegos de SD-WAN y que pueda acceder a recursos fuera de su red empresarial. Además, cualquier cortafuegos de SD-WAN con enlaces de DIA que configure en el futuro se añadirán automáticamente al clúster de VPN `autogen_hubs_cluster` que contiene todas los hubs y sucursales con enlaces de DIA para permitir que Panorama supervise el rendimiento de las aplicaciones y enlaces. `autogen_hubs_cluster` es solo para supervisar la aplicación y el estado del enlace, no para crear túneles VPN entre los hubs y las sucursales con enlaces de DIA. Si necesita conectar hubs y sucursales con túneles VPN, debe crear un nuevo clúster de VPN y añadir todas los hubs y sucursales necesarios a ese clúster.

Cuando selecciona **Pre-shared key (Clave precompartida)** como un **Authentication Type (Tipo de autenticación)**, se crea una clave compartida previa de IKE segura y aleatoria para todos los hubs y sucursales del clúster de VPN, con el fin de proteger los túneles de VPN, y cada cortafuegos tiene una clave maestra que cifra la clave precompartida. El sistema protege la clave previamente compartida, incluso del administrador. Puede actualizar la clave previamente compartida IKE que Panorama envía a todos los miembros del clúster.

Actualice la clave precompartida cuando los miembros del clúster no estén ocupados.

Cuando selecciona **Certificate (Certificado)** como el **Authentication Type (Tipo de autenticación)**, entonces los hubs y las sucursales del clúster de VPN de SD-WAN se basan en la Autenticación basada en certificados.

Después de actualizar el complemento SD-WAN a 2.1.0, los cortafuegos de hub y sucursal en un único clúster VPN deben ejecutar PAN-OS 10.0.4 (o una versión posterior a 10.0) o 10.1.0, no una combinación de las dos versiones.

Cuando visualiza clústeres de VPN, si no hay datos presentes o la pantalla indica que SD-WAN no está definida, compruebe en la Matriz de compatibilidad que la versión Panorama que está utilizando sea compatible con la versión del complemento SD-WAN que está intentando usar.

El hecho de que se forme un túnel IPSec IPv4 o IPv6 entre dos puertos Ethernet (o subinterfaz o interfaz AE) (enlace DIA) depende de si la interfaz Ethernet (o subinterfaz o interfaz AE) tiene una dirección IPv4 o IPv6. Si ambas interfaces tienen una dirección IPv4, se activa un túnel IPv4. Si ambas interfaces tienen una dirección IPv6, se activa un túnel IPv6. En el caso de la doble pila, se activa un túnel IPv4.

La dirección IP de la interfaz de túnel proviene del grupo de VPN. Puede crear un grupo de direcciones IPv6 independiente de un grupo de direcciones IPv4. Si se configuran direcciones IPv4 e IPv6, a la interfaz de túnel solo se le asigna una dirección IPv4, como se muestra en la tabla a continuación. Si se agota el grupo de direcciones VPN IPv4 y existe un grupo de direcciones IPv6, se asigna una dirección IPv6 a la interfaz de túnel. Si solo se configura IPv4, el túnel utilizará una dirección IPv4. Si solo se configura IPv6, el túnel utilizará una dirección IPv6.

Grupo de VPN	Configurado		
IPv4	Sí	yes (sí)	No
IPv6	Sí	No	Sí
IP de la interfaz de túnel	Solo IPv4	Solo IPv4	Solo IPv6

STEP 1 | Planifique la topología de VPN del hub y la sucursal para determinar qué sucursales se comunican con cada una de sus hubs. Para obtener más información, consulte Planificación de la configuración de SD-WAN.

STEP 2 | Inicio de sesión en la interfaz web de Panorama.

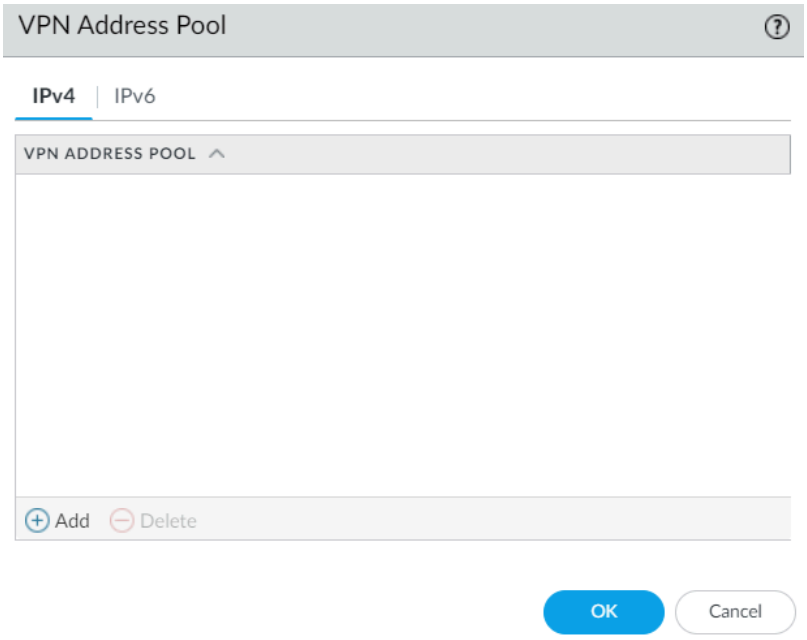
STEP 3 | Especifique los intervalos de direcciones IP para los túneles VPN IPSec que crea la configuración de VPN automática.

La configuración de VPN automática crea un túnel VPN entre un hub y sucursales y asigna direcciones IP a los endpoints del túnel. Introduzca los intervalos de subred que desea que la VPN automática utilice como direcciones de túnel VPN. Puede introducir hasta 20 intervalos de prefijo IP/máscara de red. La VPN automática extrae de ese grupo para las direcciones de túnel VPN, extrayendo primero del rango más grande (para la familia de direcciones) y, a continuación, extrayendo del siguiente rango más grande cuando sea necesario. Debe configurar al menos un intervalo para el grupo. Si no realiza este paso antes de enviar la configuración a un hub o sucursal, la confirmación y el envío fallarán.

*Si actualiza desde una versión anterior del complemento de SD-WAN, debe comprobar que sus intervalos sigan siendo correctos. Si no es así, introduzca nuevos intervalos. Después de la **confirmación**, todos los túneles se descartan y se usan túneles nuevos. Por lo tanto, realice esta acción en un momento en el que el tráfico sea reducido.*

1. Seleccione **Panorama** > **SD-WAN** > **VPN Clusters (Clústeres de VPN)**.
2. En la parte inferior de la pantalla, seleccione **Grupo de direcciones de VPN**.

3. Seleccione **IPv4** o **IPv6** y **Add (Añadir)** un grupo de direcciones con uno o más (hasta 20) intervalos de direcciones IP y máscaras de red de **Member (Miembro)**, por ejemplo, 192.168.0.0/16 o 2001::/16, respectivamente.
4. Haga clic en **OK (Aceptar)**.



No realice un simple cambio de un grupo de direcciones existente si Prisma Access está incorporado. Si necesita cambiar un grupo de direcciones, realice los siguientes pasos durante un periodo de mantenimiento para actualizar la sucursal y el CN de Prisma Access con los cambios de su grupo de direcciones:

1. *Use Panorama para acceder a una sucursal SD-WAN y elimine la incorporación existente que afectará el cambio del grupo de direcciones; luego haga una confirmación local.*
2. *Actualice el grupo de direcciones VPN y luego realice una confirmación local.*
3. *Vuelva a realizar la incorporación de Prisma Access y luego haga una confirmación local y haga el envío.*

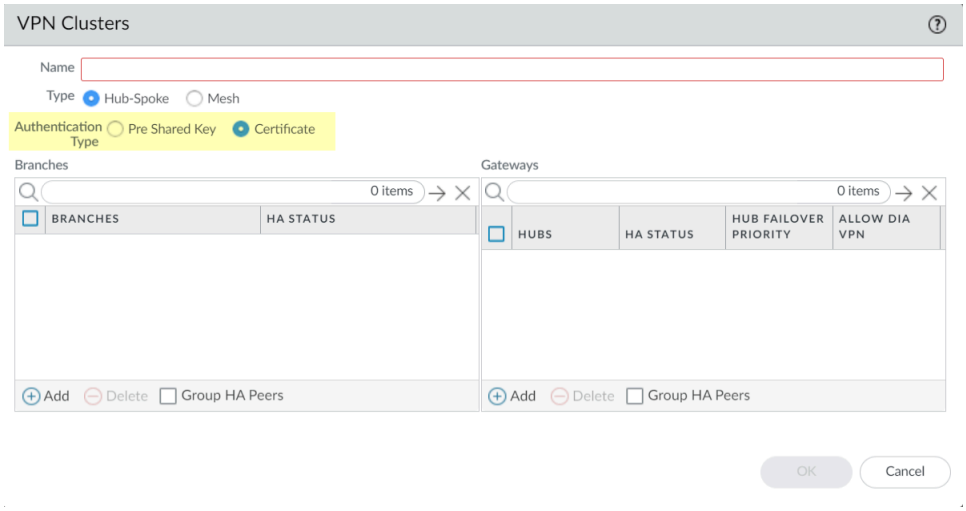
STEP 4 | Configure el clúster de VPN. Repita este paso para crear clústeres de VPN según sea necesario.

1. Seleccione **Panorama** > **SD-WAN** > **VPN Clusters (Clústeres de VPN)** y luego **Add (Añadir)** para añadir un clúster de VPN.
2. Introduzca un nombre descriptivo para el clúster de VPN.

   *Los guiones bajos y los espacios no son compatibles en el nombre del clúster de VPN y provoca que no se muestre la supervisión de datos (**Panorama** > **SD-WAN** > **Monitoring (Supervisión)**) para ese clúster. Elija cuidadosamente el nombre del clúster de VPN para que no tenga que cambiarlo en el futuro. Los datos de supervisión de SD-WAN se generan en función del nombre del clúster anterior y no se pueden conciliar con un nuevo nombre de clúster, por lo que provocarán problemas con la cantidad de clústeres informados cuando se supervisen los clústeres de VPN o se generen informes.*
3. Seleccione el **tipo** de clúster de VPN.

   *Solo el tipo de clúster de VPN de **Hub-Spoke** es compatible con PAN-OS 10.0.2 y versiones anteriores a 11.0. A partir de PAN-OS 10.0.3, puede Creación de un clúster de VPN de malla completa con servicio DDNS.*
4. (Complemento SD-WAN 3.2.0 y versiones posteriores) Seleccione la opción **Tipo de autenticación: Clave precompartida** o **Certificate (Certificado)**. Es obligatorio especificar

el tipo de autenticación para añadir un dispositivo en un clúster de VPN. Un clúster VPN deberá tener el mismo tipo de autenticación seleccionado para todos sus dispositivos.



Al seleccionar el tipo de autenticación para un clúster de VPN, solo las sucursales y los hubs que están configurados con el mismo tipo de autenticación (que el clúster de VPN) se pueden añadir al clúster de VPN. Por ejemplo, al seleccionar certificado como tipo de autenticación para un clúster de VPN, todos los hubs y sucursales que se añaden al clúster deben configurarse con certificado como tipo de autenticación.

No es posible modificar el tipo de autenticación ni el nombre del clúster de VPN de un clúster de VPN que ya se ha configurado. Para realizar un cambio, elimine el clúster de VPN y sus dispositivos SD-WAN, y configúrelo de nuevo con el nuevo tipo de autenticación o el nombre del clúster de VPN. De forma predeterminada, se admite

el tipo de autenticación precompartida para los dispositivos de un clúster VPN (si el método de certificado no se selecciona manualmente).

- *Una vez que haya configurado el clúster de VPN, no puede cambiar el nombre del clúster ni su tipo de autenticación (tanto a nivel de clúster como de dispositivo).*
- *No puede tener diferentes tipos de autenticación dentro de un solo clúster de VPN. Es decir, un tipo de autenticación de clúster VPN debe coincidir con todos los dispositivos SD-WAN en el clúster VPN. Cualquier diferencia daría lugar a un error de confirmación.*
- *Puede tener diferentes clústeres de VPN con diferentes tipos de autenticación configurados.*
- *En un clúster de VPN, no puede tener dispositivos SD-WAN con diferentes tipos de autenticación seleccionados. Si un hub de SD-WAN forma parte de dos clústeres de VPN, los dos clústeres deben configurarse con el mismo tipo de autenticación.*

Si desea cambiar el tipo de autenticación a **Certificate (Certificado)** en el caso de un clúster de VPN existente, elimine el clúster de VPN y vuelva a crearlo con el tipo de autenticación que prefiera.

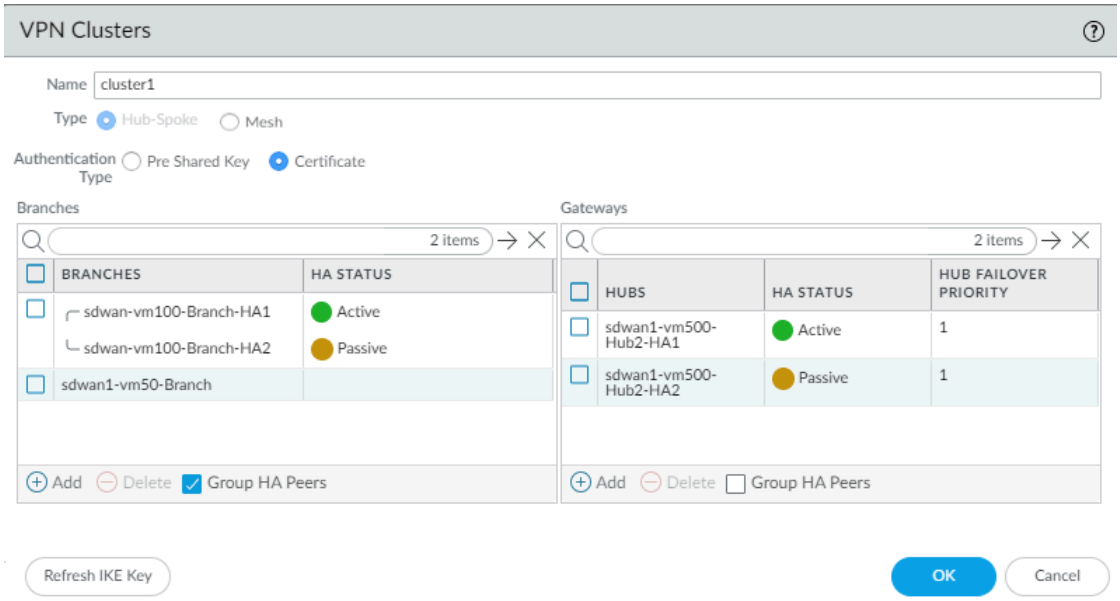
Después de crear un clúster de VPN con el tipo de autenticación de certificado, si desea cambiar a una versión del complemento PAN-OS o SD-WAN que no admita el tipo de autenticación de certificado, siga estos pasos:

- Eliminar el clúster de VPN existente. La autenticación de dispositivos SD-WAN cambiará automáticamente a una clave precompartida al cambiar a una versión anterior.
- Cambie a la versión del complemento PAN-OS o SD-WAN de su preferencia. Consulte los requisitos del sistema para SD-WAN para las versiones de los

complementos PAN-OS y SD-WAN mínimas necesarias para configurar el tipo de autenticación de certificado.

Siga los pasos mencionados en las Consideraciones sobre el cambio a versiones anteriores/posteriores antes de actualizar o cambiar a una versión anterior de su complemento SD-WAN actual.

5. **Añada** uno o más dispositivos de sucursal que determine que necesitan comunicarse entre sí.
   - Seleccione **Group HA Peers (Agrupar peers de HA)** para mostrar los dispositivos de sucursal que son peers de HA juntos.



   - Seleccione los dispositivos de la sucursal que añadir al clúster.
   - Haga clic en **OK (Aceptar)**.
6. **Add (Añadir)** uno o más dispositivos del hub que determine que necesitan comunicarse con los dispositivos de la sucursal.

   Los hubs de SD-WAN en una configuración de HA se consideran un solo cortafuegos de hub de SD-WAN.

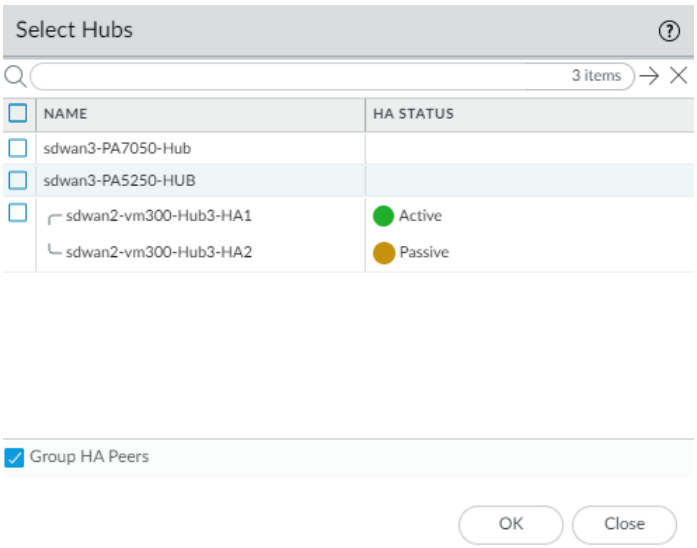
   MPLS y los tipos de enlace de satélite formarán túneles con solo el mismo tipo de enlace; por ejemplo, MPLS a MPLS y satélite a satélite. No se crearán túneles entre un enlace MPLS y un enlace Ethernet, por ejemplo.

   Para las versiones de SD-WAN anteriores a la 3.1.3, puede añadir hasta cuatro cortafuegos de hub de SD-WAN a un clúster de VPN.

   (Complemento SD-WAN 3.2.1 y versiones posteriores) Puede añadir hasta 16 cortafuegos de hub de SD-WAN a un clúster de VPN. Solo cuatro de los 16 hubs pueden tener la misma prioridad de hubs dentro de un clúster VPN debido a ECMP. Cualquier

intento de configurar la misma prioridad para más de cuatro hubs de SD-WAN daría como resultado un error de confirmación.

- Seleccione **Group HA Peers (Agrupar peers de HA)** para mostrar los dispositivos del hub que son peers de HA juntos.
- Seleccione los hubs que añadir al clúster y haga clic en **OK (Aceptar)**.



- Para cualquier clúster VPN nuevo o existente anteriormente que tenga más de un hub, debe priorizar los hubs para determinar a) que el tráfico se envíe a un hub en particular y b) el orden de conmutación por error del hub posterior. El intervalo de prioridad de conmutación por error del hub es de 1 a 4. Si actualiza, la prioridad predeterminada se establece en 4. El complemento traduce internamente la prioridad de conmutación por error del hub a un número de preferencia local BGP como se muestra en la siguiente tabla. Cuanto menor sea el valor de prioridad, mayor será la prioridad y la preferencia local. Un clúster admite un máximo de cuatro hubs para las versiones de SD-WAN anteriores a la 3.1.3. Con el complemento SD-WAN 3.2.1 y versiones posteriores, puede agregar hasta 16 cortafuegos de hub de SD-WAN a un clúster de VPN. Un peer de HA activo/pasivo cuenta como un hub. Varios hubs pueden tener la misma prioridad; un par de HA debe tener la misma prioridad. Panorama utiliza la plantilla BGP de la sucursal para enviar la preferencia local de los hubs a las sucursales del clúster.

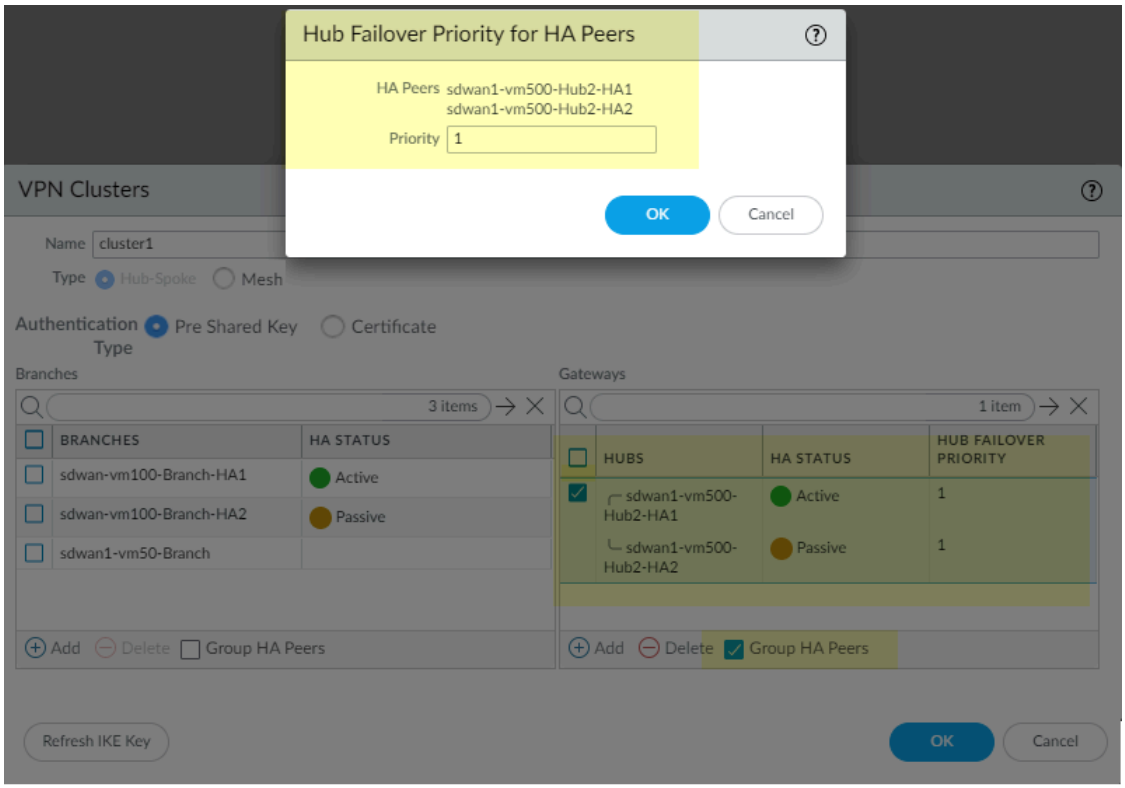
Prioridad de conmutación por error	Preferencia local
1	250
2	200
3	150

Prioridad de conmutación por error	Preferencia local
4	100

*Si varios hubs tienen la misma prioridad, Panorama habilita ECMP en dos lugares en cada cortafuegos de sucursal para determinar cómo las sucursales seleccionan la ruta. ECMP está habilitado para el enrutador virtual (**Network [Red]** > **Virtual Routers [Enrutadores virtuales]** > **ECMP**) y **ECMP Multiple AS Support (Soporte de AS de múltiple ECMP)** está habilitado para BGP (**Network [Red]** > **Virtual Routers [Enrutadores virtuales]** > **BGP** > **Advanced [Avanzado]**). Si todos los hubs del clúster tienen una prioridad única, ECMP se deshabilita en las sucursales. Si cambia una configuración de prioridad del hub, Panorama reevalúa si habilitar o deshabilitar ECMP.*

- Si ha seleccionado **Group HA Peers (Peers de HA de grupo)**, seleccione el par y haga clic en el campo **Hub Failover Priority (Prioridad de conmutación por error**

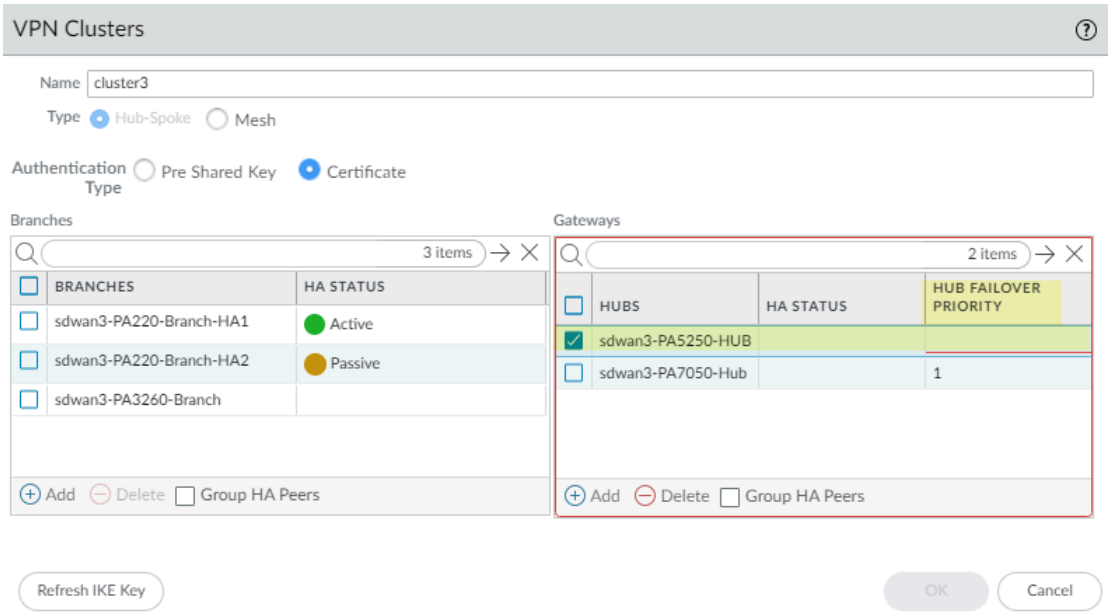
del hub); especifique una única **Priority (Prioridad)** (el intervalo es de 1 a 4), que se aplica a ambos hubs en el par de HA, y haga clic en **OK (Aceptar)**.



La ventana Failover Priority for HA Peers (Prioridad de conmutación por error para peers de HA) aparece solo para los pares de HA configurados. Si agrega un nuevo par de HA, debe configurar la prioridad de la conmutación por error del hub para cada uno de los dos peers nuevos de forma independiente.

*Recibirá un mensaje de error si asigna prioridades diferentes a los hubs que son peers de HA desagrupados y luego selecciona **Group HA Peers (Agrupar peers de HA)** y **Submit (Enviar)**.*

- Para los hubs que no son pares de HA, seleccione un hub y haga clic en el campo **Hub Failover Priority (Prioridad de conmutación por error del hub)**; especifique una prioridad (el intervalo es de 1 a 4).



7. Haga clic en **OK (Aceptar)** para guardar el clúster de la VPN.

STEP 5 | Anuncie prefijos adicionales en la sucursal para el hub.

*El cortafuegos redistribuye automáticamente (anuncia) todas las rutas conectadas no públicas desde la sucursal hasta el hub. También puede redistribuir cualquier prefijo adicional desde la sucursal al hub. El campo **Prefix(es) Prefijos que redistribuir** acepta una lista de prefijos en lugar de un solo prefijo.*

1. Seleccione **Panorama** > **SD-WAN** > **Devices (Dispositivos)** y seleccione un cortafuegos de sucursal.
2. Seleccione **BGP** y **añada** una o más direcciones IP con la máscara de red a **Prefix(es) Prefijos que redistribuir**.
3. Haga clic en **OK (Aceptar)**.

STEP 6 | Seleccione **Confirmar** y en **Confirmar en Panorama**.

STEP 7 | (Complemento SD-WAN 2.0.1 y versiones posteriores a la 2.0) Si los cortafuegos de su hub en un clúster VPN hub-spoke tienen interfaces DHCP o PPPoE, debe usar DDNS. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y, en el campo **Template (Plantilla)**, seleccione Template-stack for a hub (Pila de plantillas para un hub).

STEP 8 | (Complemento SD-WAN 2.0.1 y versiones posteriores a la 2.0) Seleccione las interfaces cuya dirección IP indique `Dynamic-DHCP Client (Cliente DHCP dinámico)` o PPPOE, haga clic en **Override (Cancelar)** en la parte inferior de la pantalla y haga clic en **OK (Aceptar)** para cerrar.

STEP 9 | (Complemento SD-WAN 2.0.1 y versiones posteriores a la 2.0) Verifique en Panorama que se hayan configurado los ajustes de DDNS.

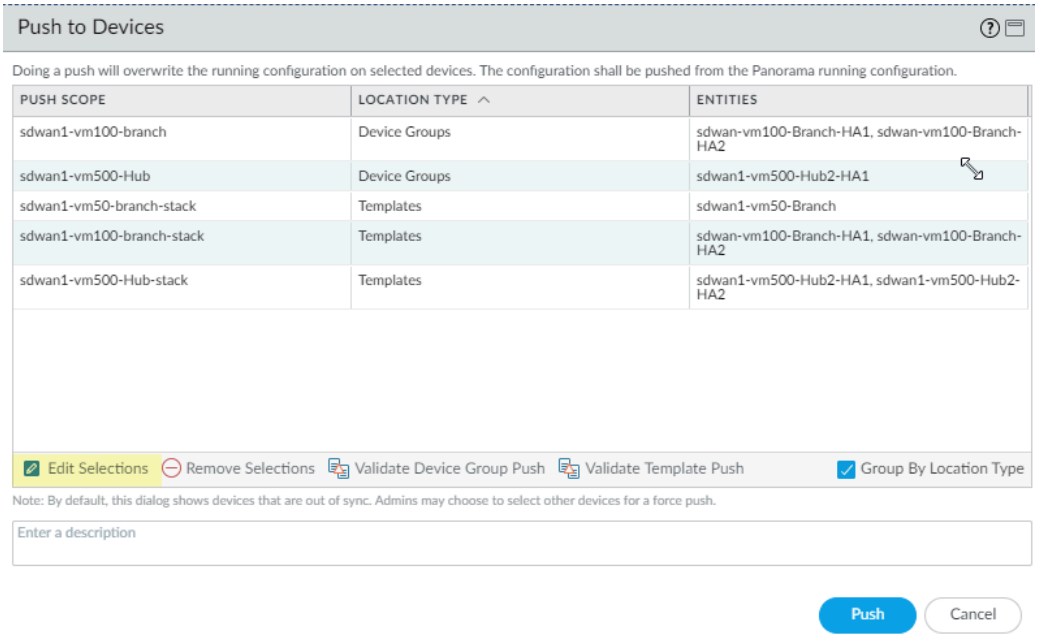
1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y vuelva a seleccionar la misma interfaz.
2. Seleccione **Advanced (Avanzado)** > **DDNS**.
3. Compruebe que la configuración de DDNS se haya configurado automáticamente con un **nombre de host** y que el **proveedor** esté establecido en `Palo Alto Networks DDNS (DDNS de Palo Alto Networks)`.
4. Haga clic en **OK (Aceptar)**.

STEP 10 | (Complemento SD-WAN 2.0.1 y versiones posteriores a la 2.0) **Confirme** y **confirme en Panorama**.

STEP 11 | Envíe la configuración a los hubs.

Cuando Panorama crea interfaces virtuales de SD-WAN para hubs, no necesariamente crea las interfaces mediante números de interfaz contiguos. Puede omitir aleatoriamente un número de interfaz, por ejemplo, sdwan.921, sdwan.922, sdwan.924 y sdwan.925. A pesar de la numeración no contigua, Panorama crea el número correcto de interfaces de SD-WAN. Utilice el comando operativo de la CLI ***`show interface sdwan?`*** *para ver las interfaces de SD-WAN.*

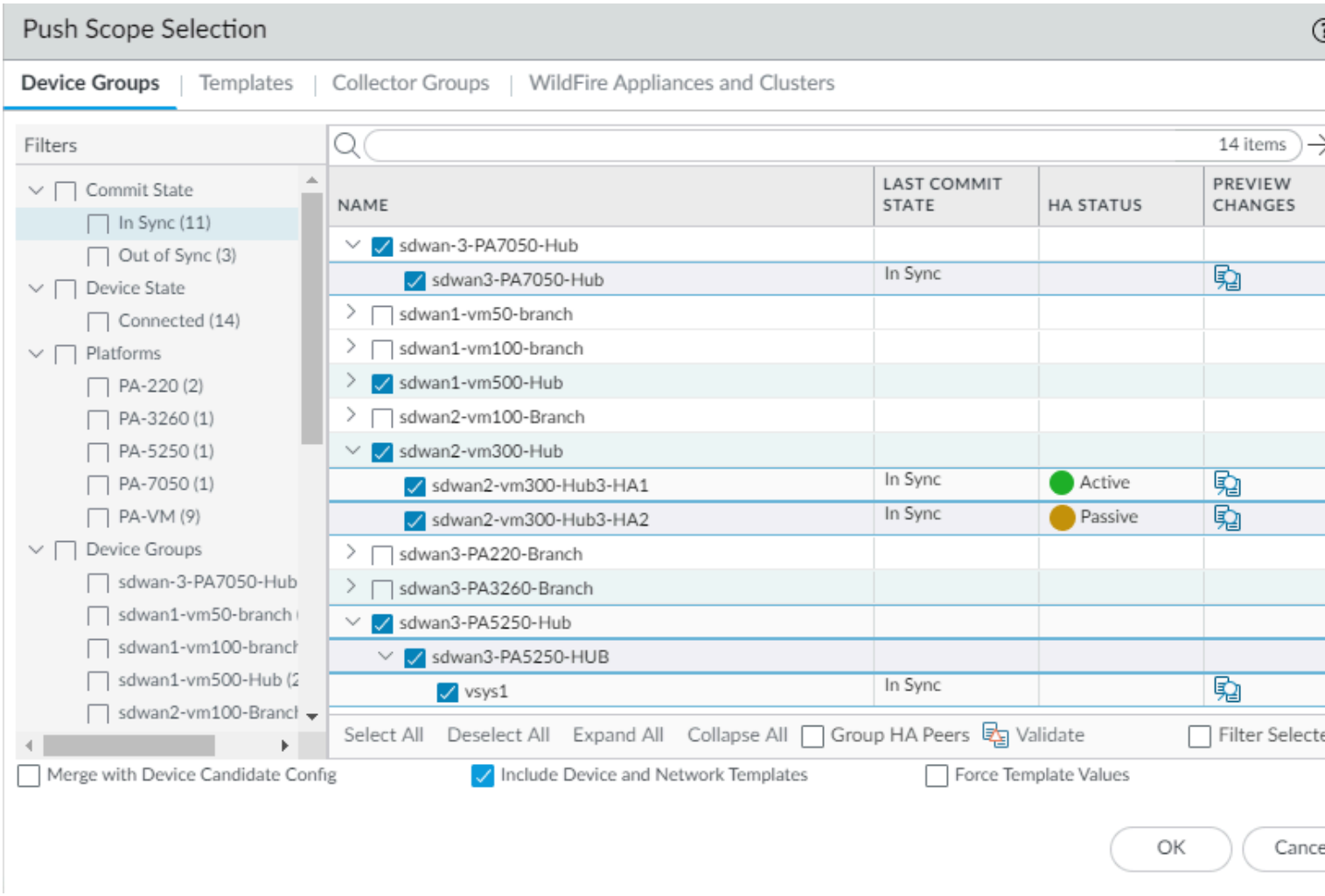
1. Seleccione **Confirmar** y **Enviar a dispositivos**.
2. **Edite selecciones** en la parte inferior izquierda de la pantalla.



3. Anule la sección de la opción **Filtro seleccionado**.
4. Haga clic en **Anular selección de todo**.
5. Seleccione su grupo de dispositivos del hub. Seleccione **Incluir plantillas de dispositivo y red** en la parte inferior de la pantalla. Debe enviarlos a los hubs antes de hacerlo a las sucursales.

   La mayoría de las sucursales tienen direcciones IP dinámicas a través de sus proveedores de servicios, por lo que deben iniciar la conexión IKE/IPSec, ya que el hub no tiene la dirección IP de las sucursales. Para asegurarse de que el hub esté lista para recibir las conexiones IKE/IPSec, la configuración debe confirmarse y enviarse antes de la

configuración de la sucursal. Por lo tanto, cuando se envíen las configuraciones de la sucursal y las sucursales inicien la conexión al hub, el hub estará listo.



6. Seleccione la pestaña **Plantillas** y **Anular selección de todo**.
7. El **ámbito de envío** será el grupo de dispositivos. **Envíe** la configuración a los hubs.

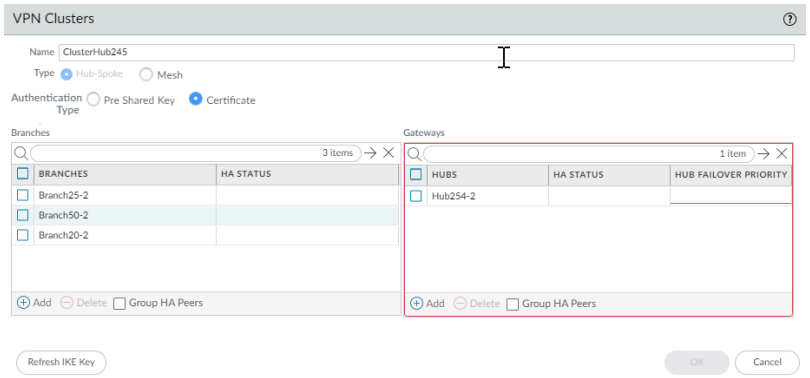
STEP 12 | Envíe la configuración a las sucursales. Para ello, repita el paso anterior, pero seleccionando su el grupo de dispositivos de la sucursal.

STEP 13 | Actualice la clave compartida previamente de IKE.

Si necesita cambiar la clave IKE actual que se usa para garantizar las conexiones IPSec entre dispositivos de clúster de VPN, realice este paso para generar aleatoriamente una nueva clave para el clúster.

Realice este paso cuando los miembros del clúster no estén ocupados.

1. Seleccione **Panorama** > **SD-WAN** > **VPN Clusters (Clústeres de VPN)** y seleccione un clúster.
2. En la parte inferior de la pantalla, seleccione **Actualizar clave IKE**.



3. Aparecerá un mensaje de notificación acerca de que `la actualización de la clave IKE generará una nueva asociación de seguridad (SA) para cada cortafuegos SD-WAN en el clúster VPN. Esto puede causar una interrupción del servicio. ¿Desea continuar? Sí | No` Seleccione `Sí` si desea continuar.
4. Seleccione **Confirmar**.

   *Después de **actualizar la clave IKE**,debe compilar todo el clúster; una compilación parcial desactivará los túneles.*
5. Seleccione **Enviar a dispositivos**.

Creación de un clúster de VPN de malla completa con servicio DDNS

A partir de PAN-OS 10.0.3, SD-WAN admite una topología de malla completa, además de la topología hub-spoke. La malla puede constar de sucursales con o sin hubs. Utilice la malla completa cuando las sucursales necesiten comunicarse entre sí directamente. Entre los ejemplos de casos de uso para la malla completa se incluyen minoristas que tienen sucursales y hubs, y empresas que operan con o sin hubs.

Algunas interfaces de cortafuegos usan DHCP para obtener su dirección IP. Las sucursales suelen utilizan un servicio de Internet de nivel de consumidor y reciben una dirección IP dinámica, que por supuesto puede cambiar. Por ese motivo, los cortafuegos requieren un DNS dinámico (DDNS) para que un servicio DDNS pueda detectar la dirección IP pública de la interfaz de cortafuegos que ejecuta SD-WAN. Cuando envía la configuración DDNS a todos los cortafuegos, se notifica a cada cortafuegos que registre su dirección IP de interfaz externa con el servicio en la nube DDNS de Palo Alto Networks para que la dirección IP se convierta en un FQDN.

DDNS también es obligatorio, ya que el dispositivo CPE del ISP puede estar realizando una NAT de origen. (La NAT de origen puede traducir o no la dirección IP dinámica). El servicio DDNS permite que el cortafuegos registre la dirección IP pública con el servidor DDNS. Cuando cuenta con dispositivos que se conectan para la malla de sucursal a sucursal, la VPN automática se comunica con el servicio DDNS de esos cortafuegos para extraer sus direcciones IP públicas que están registradas en la nube DDNS y usa esas direcciones IP públicas para crear el emparejamiento IKE y los túneles VPN. Si el dispositivo CPE está realizando la NAT de origen, cuando añade un dispositivo de sucursal de SD-WAN para que lo gestione Panorama, habilitará **Upstream NAT (NAT de subida)** y el tipo de dirección IP de NAT será **DDNS**.

Para el dispositivo CPE o el dispositivo de enrutamiento de subida que usa NAT de origen, usted será el responsable de crear la regla de NAT de destino una a una (sin traducción de puerto) en ese dispositivo para traducir la dirección IP externa a la dirección IP privada asignada a la interfaz del cortafuegos. Esta traducción permite que los protocolos IKE e IPSec vuelvan al cortafuegos. (Palo Alto Networks no tiene derechos de acceso al CPE de subida o al enrutador de subida que realiza NAT de origen).

La malla completa de SD-WAN con servicio DDNS requiere lo siguiente:

- PAN-OS 10.0.3 o una versión posterior a la 11.1
- Complemento SD-WAN 2.0.1 o una versión posterior a la 2.0
- Complemento ZTP 1.0.1 o una versión posterior a la 1.0 que se descargue, instale y configure para aprovechar el DDNS asociado con ZTP. Panorama debe estar registrado en ZTP y comunicarse con el servicio ZTP.
- Aplicaciones y amenazas Versión de contenido 8354 o una versión posterior
- Todos los cortafuegos que participan en DDNS de malla completa deben registrarse en la misma cuenta del portal de atención al cliente (CSP, Customer Support Portal).
- Todos los cortafuegos que participan en DDNS de malla completa deben tener instalado el certificado de dispositivo más reciente. La autenticación adecuada de los cortafuegos,

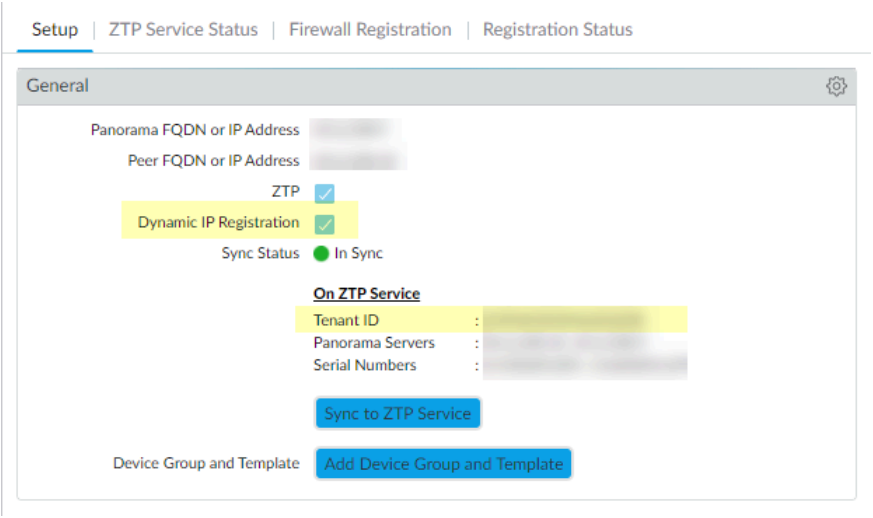
Panorama y los servicios en la nube son procedimientos de seguridad importantes que requieren el certificado del dispositivo y los servicios CSP y ZTP.

- Si tiene un cortafuegos u otro dispositivo de red que controla el tráfico saliente ubicado frente al cortafuegos de Palo Alto Networks, debe cambiar la configuración en ese dispositivo para permitir el tráfico desde las interfaces habilitadas para DDNS a los siguientes FQDN:
  - https://myip .ngfw-ztp.paloaltonetworks.com/ (para acceder al servicio de whatsmyIP)
  - https://ngfw-ztp.paloaltonetworks.com/ (para acceder al servicio de registro de DDNS)

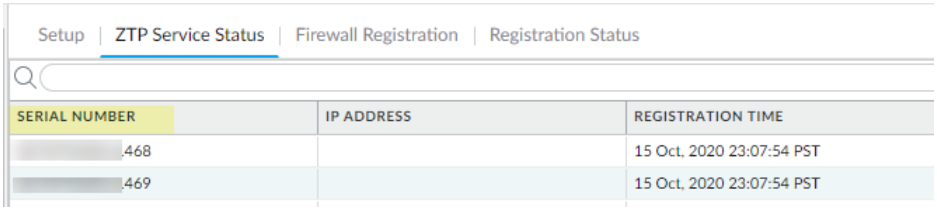
STEP 1 | Instale el certificado de dispositivo más reciente para Panorama y para todos los cortafuegos gestionados que sean hubs o sucursales.

STEP 2 | Instale el complemento ZTP 1.0.1 para configurar Zero Touch Provisioning (aprovisionamiento táctil cero).

1. En la Guía del administrador de Panorama, lea la descripción general de ZTP.
2. Instale el complemento de ZTP.
3. Configure la cuenta de administrador del instalador de ZTP.
4. Seleccione **Panorama** > **Zero Touch Provisioning** > **Setup (Configuración)** y edite la configuración general para habilitar el **registro de IP dinámica**.
5. Haga clic en **OK (Aceptar)**. La configuración general indica On ZTP Service (En servicio ZTP) con un número de ID de inquilino.



6. Seleccione **ZTP Service Status (Estado del servicio ZTP)** y confirme que aparece el número de serie del cortafuegos.



STEP 3 | Si aún no lo ha hecho, instale el complemento SD-WAN 2.0.1 o una versión posterior a la 2.0.

STEP 4 | **Confirme** en Panorama.

STEP 5 | Inicio de sesión en la interfaz web de Panorama.

STEP 6 | Cree el grupo de direcciones VPN como se muestra en Creación de un clúster de VPN.

STEP 7 | Cree el clúster de VPN de malla completa.

1. Seleccione **Panorama** > **SD-WAN** > **Clústeres de VPN**.
2. Seleccione el **tipo** para que sea **Mesh (Malla)**.
3. **Añada** las **sucursales** que tienen que comunicarse entre ellas.
4. (Opcional) puede **Add (Añadir)** una o más **Hubs** si también desea un hub en la malla.
5. Haga clic en **OK (Aceptar)**.

STEP 8 | Seleccione **Confirmar** y en **Confirmar en Panorama**. Si sus cortafuegos tienen direcciones IP estáticas, el procedimiento está completado. Si los cortafuegos de su sucursal o hub en una malla VPN tienen interfaces DHCP o PPPoE, debe usar DDNS, así que continúe con este procedimiento de la siguiente manera.

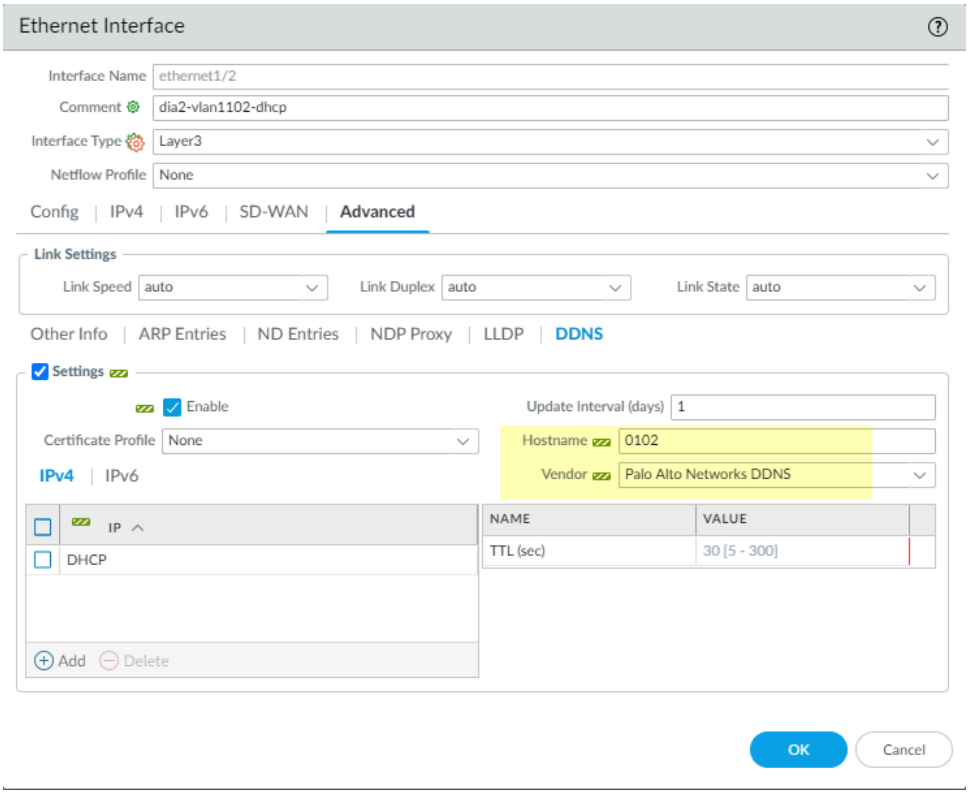
STEP 9 | Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y, en el campo **Template (Plantilla)**, seleccione Template-stack for a hub (Pila de plantillas para un hub) para una sucursal determinada.

STEP 10 | Seleccione las interfaces cuya dirección IP indique `Dynamic-DHCP Client (Cliente DHCP dinámico)` o PPPOE, haga clic en **Override (Cancelar)** en la parte inferior de la pantalla y haga clic en **OK (Aceptar)** para cerrar.

STEP 11 | Verifique en Panorama que se hayan configurado los ajustes de DDNS.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione de nuevo la misma interfaz.
2. Seleccione **Advanced (Avanzado)** > **DDNS**.
3. Compruebe que la configuración de DDNS se haya configurado automáticamente con un **nombre de host** basado en el nombre de la interfaz y que el **proveedor** esté establecido

en `Palo Alto Networks DDNS (DDNS de Palo Alto Networks)`. Por ejemplo, en la interfaz Ethernet1/2, el nombre de host resultante es 0102.



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

STEP 12 | Si el clúster de VPN incluye hubs que tienen una interfaz DHCP o PPPoE, repita los pasos del 9 al 11, pero en el campo **Template (Plantilla)**, seleccione la pila de plantillas para un hub determinado.

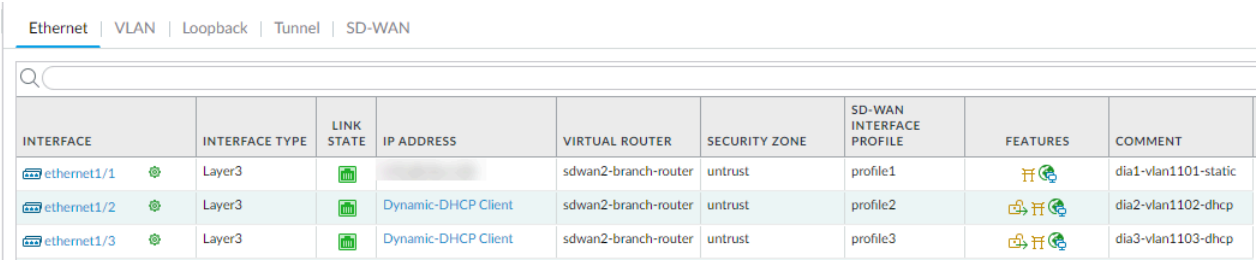
Incluso si su hub no está en un clúster de malla completa, pero está en un clúster de hub-spoke, si el hub usa DHCP o PPPOE para obtener su dirección IP para una interfaz SD-WAN, debe realizar los pasos de cancelación para habilitar DDNS.

STEP 13 | **Confirme** en Panorama y **envíe a los dispositivos**.

STEP 14 | Verifique en el cortafuegos de sucursal que la sucursal esté configurada con DDNS.

1. Inicie sesión en el cortafuegos de sucursal.
2. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y para la interfaz Ethernet que ha configurado, desplácese sobre el icono de información de DDNS en la

columna Features (Funciones) para ver el proveedor, el nombre de host, la dirección IP y otra información de DDNS.



STEP 15 | En otra sucursal del clúster, observe que la dirección de peers de la interfaz es un FQDN generado por el sistema para el registro de DDNS.

1. Inicie sesión en otra sucursal y seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace de IKE)**.
2. Compruebe que la dirección del par sea un nombre seguro, no es sea fácil de referenciar y no muestre información de la empresa; por ejemplo 0101.8ced8460fcc5177cd3665ce41b6345323a15a612b8e52ec1d9ec057a582cb4.t13855f6c9a92c

STEP 16 | Compruebe los FQDN de sucursales y hubs y actualice la información DDNS.

1. Acceso a la CLI.
2. Consulte el FQDN (generados por DDNS) para otras sucursales y hubs: **`show dns-proxy fqdn all`**.
3. Actualice las direcciones DDNS: **`request system fqdn refresh`**.

Creación de una ruta estática para SD-WAN

Además del enrutamiento de BGP (o como alternativa a él), puede crear rutas estáticas para enrutar el tráfico de SD-WAN.

Puede configurar rutas estáticas mediante Panorama™ o directamente en el hub o sucursal del cortafuegos. Si va a utilizar Panorama, debe estar familiarizado con el proceso para configurar una variable en una plantilla o pila de plantillas. Tendrá que crear una variable que usar como destino en su ruta estática, como se muestra en el siguiente procedimiento. (También puede crear una variable para el siguiente salto). Tendrá que enviar una ruta estática (que se dirige al hub) a la sucursal. Tendrá que enviar una ruta estática (que se dirige a la sucursal) al hub.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Configure una variable en una plantilla o una pila de plantillas y especifique la variable **Nombre** con el siguiente formato: $*peerhostname_clustername.customname*. Por ejemplo, $branchsanjose_clusterca.10 o $DIA_cluster2.location3. Después del signo de dólar ($), los elementos en la variable son los siguientes:

- *peerhostname*: nombre de host del hub o sucursal de destino al que va la ruta estática. Para una ruta estática a Internet, el nombre de host del peer debe ser **DIA**. Una alternativa al nombre de host del peer es usar el número de serie del peer. Si el peer es parte de un par de HA, puede usar el nombre de host o el número de serie de uno de los dos cortafuegos de HA.
- *clustername*: nombre del clúster de VPN al que pertenece el hub o sucursal de destino.
- *customname*: cadena de texto de su elección; no puede usar un punto (.) en el nombre personalizado.

Puede tener más de una ruta estática que vaya al mismo peer, lo que implicará que las variables tendrán el mismo nombre de host y nombre de clúster; diferencie las variables mediante un nombre personalizado diferente.

STEP 3 | Seleccione la variable **Type (Tipo)** para que sea **IP Netmask (Máscara de red IP)** y especifique la dirección IP de destino con una barra y una longitud de máscara de red, como 192.168.2.1/24. Para IPv6, introduzca la dirección IPv6 con una barra y longitud de prefijo, como 2001:DB8::/32.

STEP 4 | Haga clic en **Aceptar** para guardar la variable.

STEP 5 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.

STEP 6 | Seleccione **Static Routes (Rutas estáticas)**.

STEP 7 | Seleccione **IPv4** o **IPv6** y luego **Add (Añadir)** para añadir un **Name (Nombre)** para la ruta estática.

STEP 8 | Para **Destino**, seleccione la variable que creó.

STEP 9 | En **Interface (Interfaz)**, realice la selección a partir de la lista desplegable, que incluye solo interfaces de la plantilla; por ejemplo, Ethernet1/1, Tunnel.x o sdwan.xx.

STEP 10 | Para el **Next Hop (Siguiente salto)**, seleccione **IP Address (Dirección IP)** o **IPv6 Address (Dirección IPv6)** e introduzca la dirección IP o variable del siguiente salto para la ruta estática (el hub o sucursal a la que se dirige la ruta estática).

STEP 11 | Haga clic en **OK (Aceptar)**.

STEP 12 | **Confirme** y **envíe** sus cambios.

La configuración de VPN automática reemplaza a la palabra clave **sdwan** en el campo Interfaz de la ruta estática con la interfaz de SD-WAN virtual de salida que determina según la variable Destino. Por lo tanto, la ruta estática en la tabla de enrutamiento indica que el tráfico que se dirige al host del peer en el clúster de VPN identificado saldrá de la interfaz de SD-WAN virtual para alcanzar el siguiente salto especificado.

STEP 13 | Configure una ruta estática para el tráfico de retorno.

Configuración de enrutamiento avanzado para SD-WAN

El motor de enrutamiento avanzado permite que el cortafuegos escale y proporcione funciones de enrutamiento estables, de alto rendimiento y de alta disponibilidad a grandes centros de datos, proveedores de servicios de Internet (ISP), empresas y usuarios de la nube. El motor de enrutamiento avanzado se basa en la metodología de configuración estándar del sector, lo que facilita las tareas del administrador. Permite la creación de perfiles que se usan para diferentes funciones (como filtrado, redistribución y cambios de métricas), todos los cuales se pueden usar en enrutadores lógicos. Estos perfiles proporcionan una granularidad más detallada para filtrar rutas para cada protocolo de enrutamiento dinámico y mejorar la redistribución de rutas a través de varios protocolos.

Aunque conceptualmente equivalente, el motor de enrutamiento avanzado utiliza enrutadores lógicos en lugar de enrutadores virtuales para crear instancias de dominios de enrutamiento.

A diferencia de los enrutadores virtuales, los enrutadores lógicos no se crean de forma predeterminada; debe crear uno antes de configurar las funciones de enrutamiento.

Puede usar un motor de enrutamiento avanzado o un motor heredado según los requisitos de su red:

- Cuando habilita el enrutamiento avanzado, se crean enrutadores lógicos y se utiliza el motor de enrutamiento avanzado para el enrutamiento.
- Cuando deshabilita el **enrutamiento avanzado**, se crean enrutadores virtuales y se utiliza un motor heredado para el enrutamiento.

El motor de enrutamiento avanzado admite varios enrutadores lógicos (conocidos como “enrutadores virtuales” en el motor de enrutamiento heredado). El motor de enrutamiento avanzado tiene opciones de menú más convenientes y hay más configuraciones BGP que se pueden ajustar fácilmente en un perfil (autenticación, temporizadores, familia de direcciones o perfil de redistribución) que se aplica a un peer o grupo de peers de BGP, por ejemplo.

El motor de enrutamiento avanzado admite rutas estáticas, MP-BGP, OSPFv2, OSPFv3, RIPv2, modo disperso de multidifusión independiente del protocolo (PIM-SM), multidifusión de origen específico (SSM) de PIM, BFD, redistribución, filtrado de rutas en RIB, listas de acceso , listas de prefijos y mapas de rutas.

Para configurar el motor de enrutamiento avanzado en SD-WAN necesitará lo siguiente:

Zero Trust	Cortafuegos que ejecuten la versión PAN-OS	Complemento SD-WAN
Panorama™	11.1 y posteriores	3.1.0 y posteriores

El complemento SD-WAN crea un enrutador lógico o un enrutador virtual según el valor de la opción de enrutamiento avanzado. Cuando se habilita el enrutamiento avanzado, se crea un enrutador lógico; de lo contrario, se crea un enrutador virtual.

Cuando habilita el enrutamiento avanzado en la pila de plantillas y realiza una confirmación de Panorama y un envío al cortafuegos, el complemento SD-WAN ejecuta el script de migración

para crear los objetos relacionados de SD-WAN (ruta estática, interfaces, perfil de redistribución, BGP) en el enrutador lógico. El script de migración crea el nombre del enrutador lógico igual que el nombre del enrutador virtual para la misma plantilla. Por lo tanto, los hubs y las sucursales siempre tienen el mismo nombre de enrutador.

Después de la migración, Panorama no le permite eliminar los enrutadores virtuales migrados.

El complemento Panorama SD-WAN 3.1.0 puede administrar simultáneamente cortafuegos mediante el motor de enrutamiento avanzado y los cortafuegos a través del motor de enrutamiento heredado. El beneficio es que puede migrar cortafuegos gestionados seleccionados al nuevo motor de enrutamiento avanzado y al mismo tiempo mantener la configuración actual del motor de enrutamiento heredado en otros.

Si bien el complemento SD-WAN 3.1.0 gestiona un cortafuegos independientemente del motor de enrutamiento, solo una configuración de motor de enrutamiento puede estar en vigencia por vez en un cortafuegos gestionado. Puede utilizar la opción de **enrutamiento avanzado** para habilitar o deshabilitar el motor de enrutamiento avanzado. Cada vez que cambia el motor que usa el cortafuegos (se puede habilitar o deshabilitar el enrutamiento avanzado para acceder al motor avanzado o al motor heredado, respectivamente), debe confirmar la configuración y reiniciar el cortafuegos para que los cambios surtan efecto.

Antes de cambiar al motor de enrutamiento avanzado, realice una copia de seguridad de la configuración actual. De modo similar, si configura Panorama con una pila de plantillas que habilita o deshabilita el enrutamiento avanzado, después de confirmar y enviar la pila de plantillas a los dispositivos, debe reiniciar los dispositivos de la pila de plantillas para que el cambio surta efecto.

Al configurar Panorama, cree grupos de dispositivos y pila de plantillas para dispositivos que usen la misma configuración de enrutamiento avanzado (deben estar todos habilitados o todos deshabilitados). Panorama no envía configuraciones con el enrutamiento avanzado habilitado a cortafuegos más pequeños que no admiten el enrutamiento avanzado. Para estos cortafuegos, Panorama envía una configuración heredada si existe una.

Asegúrese de cambiar a una versión adecuada de complemento SD-WAN y de PAN-OS y deshabilite **el enrutamiento avanzado** si planea usar un enrutador virtual. Use una plantilla separada donde el **enrutamiento avanzado** esté deshabilitado (en este caso, se crean enrutadores virtuales) al degradar el complemento SD-WAN.

Si configuró **el enrutamiento avanzado** y desea cambiar a un enrutador virtual, deshabilite el enrutamiento avanzado para volver a la configuración previamente guardada del enrutador virtual. Confirme y envíe cualquier cambio realizado en el cortafuegos después de deshabilitar el enrutamiento avanzado antes de intentar un procedimiento de degradación, como degradar las versiones de los complementos PAN-OS y SD-WAN.

Si habilita el enrutamiento avanzado, las interfaces SD-WAN deben configurarse en el mismo enrutador lógico; no se pueden dividir entre enrutadores lógicos.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Actualice Panorama a 11.1 e instale el complemento SD-WAN 3.1.0.

STEP 3 | Agregue los cortafuegos de hub y sucursal como dispositivos gestionados al servidor de gestión de Panorama™ .

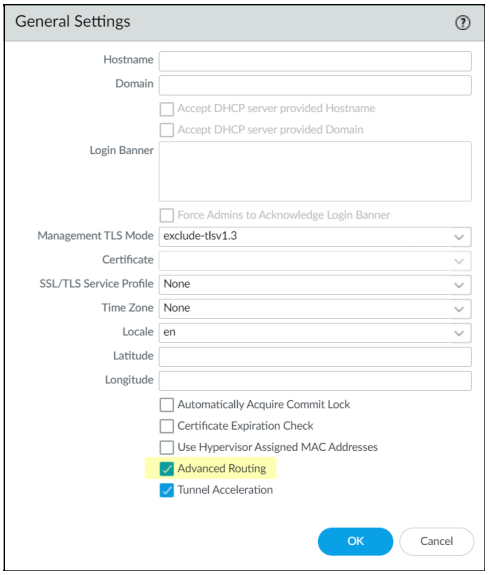
STEP 4 | Realice una copia de seguridad de su configuración actual antes de habilitar el enrutamiento avanzado.

STEP 5 | En la sección **Device (Dispositivo)**, seleccione la pila de plantillas correspondiente en el menú desplegable de contexto **Template (Plantilla)** .

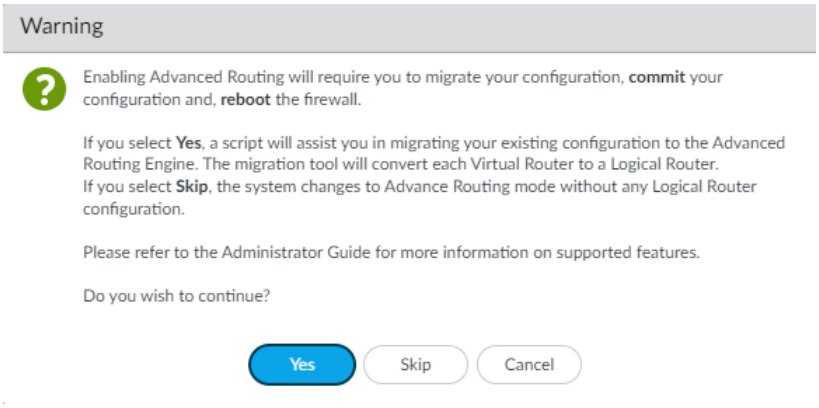
STEP 6 | Habilitar el motor de enrutamiento avanzado.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite {0>General Settings (Configuración general)<0}.
2. Habilite **Advanced Routing (Enrutamiento avanzado)**. El complemento SD-WAN creará un enrutador lógico o un enrutador virtual según el valor de la opción de enrutamiento

avanzado. Cuando el enrutamiento avanzado está habilitado, se crea un enrutador lógico. De lo contrario, se crea un enrutador virtual.

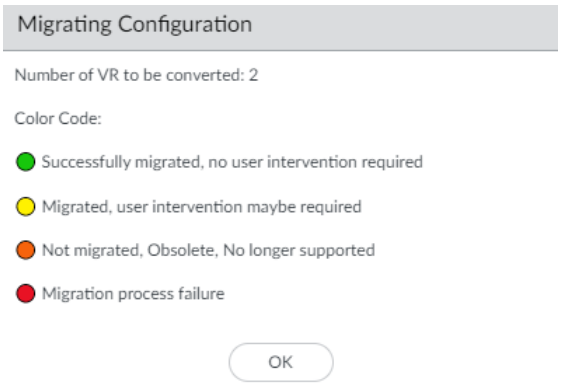


3. Haga clic en **OK (Aceptar)**.
4. Aparece un mensaje de advertencia sobre la migración; haga clic en **Yes (Sí)** para continuar.

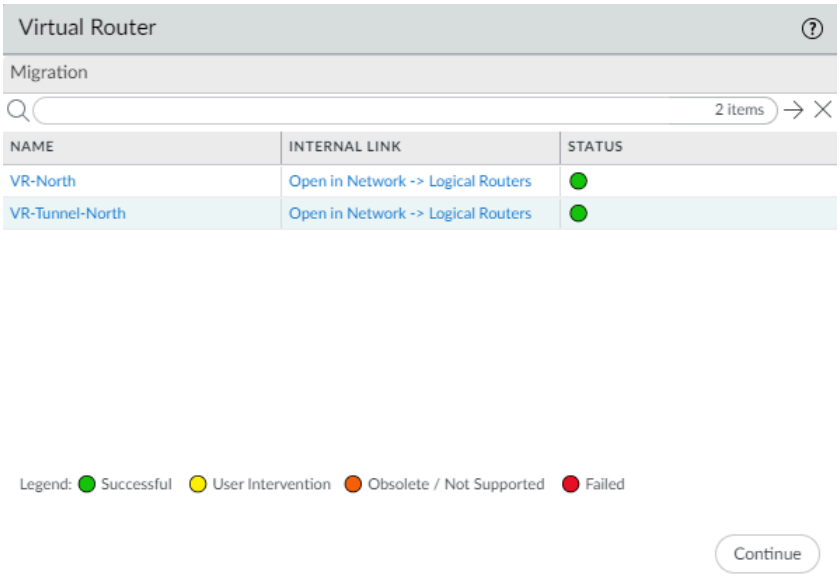


Al hacer clic en **Yes (Sí)**, un script de migración incorporado migrará la configuración existente al motor de enrutamiento avanzado. Si selecciona **Skip (Omitir)**, se crea una configuración vacía para el motor de enrutamiento avanzado.

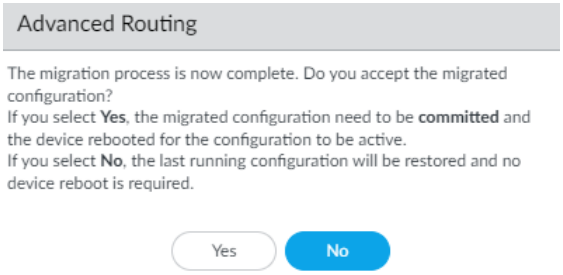
La **configuración de migración** muestra los códigos de color que indican el estado de la migración.



En el **enrutador virtual**, revise el **ESTADO** de las plantillas en las pilas de plantillas. El **ESTADO** debe ser verde para una migración exitosa. De lo contrario, tome las medidas necesarias para las plantillas con migración fallida.



La migración exitosa convierte automáticamente cada enrutador virtual en un correspondiente enrutador lógico. Es obligatorio confirmar la configuración y reiniciar el cortafuegos para que los cambios surtan efecto.



5. Seleccione **Confirmar**.
6. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y **Reboot Device (Reiniciar dispositivo)**.

STEP 7 | Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** y **confirme** los cambios

STEP 8 | Confirme y envíe los cambios de configuración a los cortafuegos gestionados. Realice el **envío a los dispositivos** para ver los enrutadores lógicos agregados en los cortafuegos SD-WAN seleccionados.

1. Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y **Edit Selections (Editar selecciones)**.
2. Seleccione **Templates (Plantillas)** y elija la pila de plantillas y la plantilla de la lista.
3. Habilite **Force Template Values (Forzar valores de plantilla)** para sobrescribir la configuración local con los valores de plantilla actualizados. Antes de usar esta opción, verifique los valores anulados en los cortafuegos para asegurarse de que la compilación no derive en interrupciones imprevistas de la red o en problemas causados por el reemplazo de los valores anulados.
4. Haga clic en **OK (Aceptar)** y **Push (Enviar)** a dispositivos.

STEP 9 | Vuelva a iniciar sesión en el cortafuegos.

STEP 10 | Seleccione **Network (Red)**.

Observe los elementos de menú, que se acercan más a los estándares de la industria y son más detallados que el elemento único (enrutadores virtuales) del menú heredado. El **enrutamiento** incluye **enrutadores lógicos** y **perfiles de enrutamiento**, que, a su vez, incluyen **BGP**, **BFD**, **OSPF**, **OSPFv3**, **RIPv2**, **filtros**, y **multidifusión**.

STEP 11 | Debe habilitar el **enrutamiento avanzado** para cada pila de plantillas individualmente cuando tenga más de una pila de plantillas en su configuración. Repita los pasos 5 a 10 para otras pilas de plantillas en los cortafuegos que desee actualizar para el enrutamiento avanzado.

De acuerdo con nuestro requisito de diseño, el nombre del enrutador lógico debe ser el mismo que el nombre del enrutador virtual para la misma plantilla cuando se usa el motor de enrutamiento avanzado. Esto significa que los hubs y las sucursales siempre tienen el mismo nombre de enrutador. Al crear manualmente enrutadores lógicos en lugar de usar un script de migración, debe asegurarse de que el nombre del enrutador lógico y del enrutador virtual sean iguales.

STEP 12 | Seleccione un enrutador virtual o un enrutador lógico en la implementación de SD-WAN.

Seleccione **Panorama** > **SD-WAN** > **Devices (Dispositivos)**para agregar un dispositivo SD-WAN (cortafuegos de hub o de sucursal de SD-WAN) para que lo gestione el servidor de gestión Panorama.

Además de las opciones de configuración existentes para agregar un dispositivo SD-WAN, ahora puede seleccionar un enrutador lógico (para un motor de enrutamiento avanzado) o un enrutador virtual (para un motor heredado) para un **nombre de enrutador**. Es importante que el

nombre del enrutador lógico y el nombre del enrutador virtual sean los mismos para la misma plantilla cuando se utiliza el motor de enrutamiento avanzado.

Seleccione el **Router Name (Nombre del enrutador)** (enrutador lógico o virtual) que usar para el enrutamiento entre el hub y las sucursales de SD-WAN:

- Si los nombres del enrutador virtual y el enrutador lógico son los mismos, entonces el **nombre del enrutador** muestra un nombre.
- Si los nombres del enrutador virtual y del enrutador lógico son diferentes, entonces el **nombre del enrutador** muestra tanto el nombre del enrutador virtual como el del enrutador lógico. Puede seleccionar un enrutador virtual (para un motor heredado) o un enrutador lógico (para un motor de enrutamiento avanzado) según sus necesidades.

Supervisión y creación de informes

Supervise y genere informes sobre el estado de la aplicación y el enlace en sus clústeres de VPN para identificar y resolver problemas. Para que el servidor de gestión Panorama™ muestre la aplicación de SD-WAN y vincule la información de estado, debe habilitar los cortafuegos de SD-WAN para enviar los datos de supervisión del dispositivo a Panorama y configurar el reenvío de logs a Panorama cuando Adición de tus cortafuegos SD-WAN como dispositivos gestionados. Si no ha configurado sus cortafuegos de SD-WAN para reenviar logs a Panorama, la **supervisión** de SD-WAN no mostrará información sobre el estado de la aplicación o del enlace.

Para que Panorama recopile datos de supervisión de SD-WAN, debe enviar la configuración de SD-WAN de Panorama a sus cortafuegos de SD-WAN. Si no se muestran datos de supervisión de SD-WAN, verifique que haya introducido correctamente la configuración de SD-WAN.

- Supervisión de tareas de SD-WAN
- Supervisión del rendimiento del enlace y de la aplicación de SD-WAN
- Supervisión de hubs de Prisma Access
- Generación de un informe de SD-WAN

Supervisión de tareas de SD-WAN

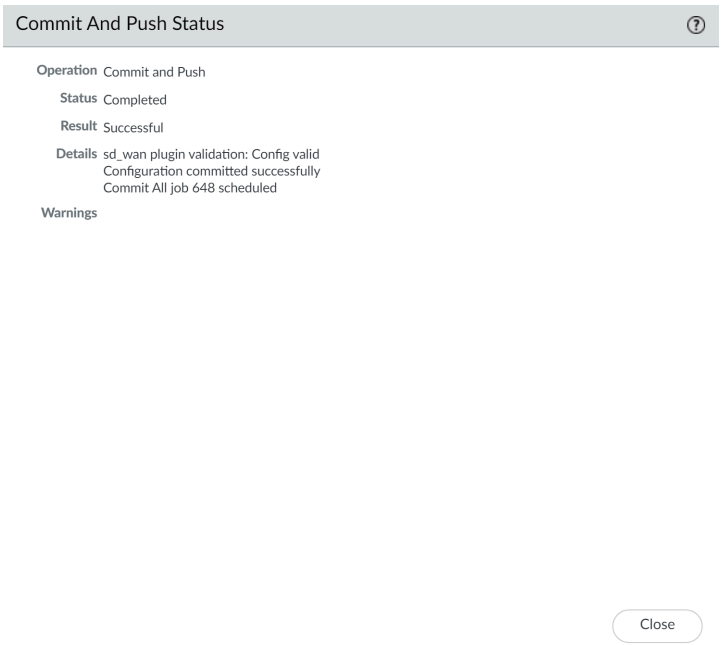
Supervise las confirmaciones, los envíos y otras tareas de SD-WAN que se ejecuten desde el servidor de gestión Panorama™ para obtener información detallada sobre la tarea específica.

Si una tarea se completa con advertencias o errores, puede ver las advertencias detalladas y una descripción para comprender mejor cómo resolver la configuración incorrecta. Además, puede ver los últimos detalles del estado de envío para revisar información detallada sobre lo que provocó las advertencias o los errores de la tarea.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

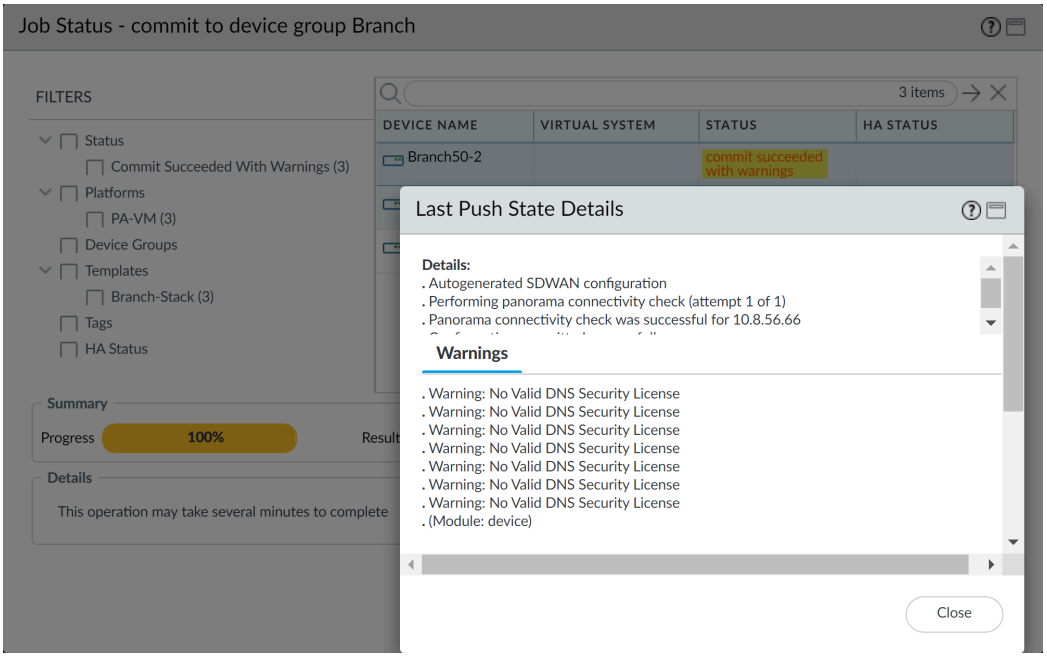
STEP 2 | Después de editar la configuración de SD-WAN, **confirme** sus cambios para ver el estado del trabajo.

La ventana de estado del trabajo muestra la operación realizada, el resultado y todos los detalles y advertencias relacionados con el estado del trabajo.



STEP 3 | Vea los últimos detalles de envío para trabajos completados con advertencias o errores.

1. Haga clic en **Tareas** (Tasks) en la parte inferior de la interfaz web para abrir el Administrador de tareas.
2. Haga clic en el **tipo** de trabajo para la tarea de SD-WAN.
3. Haga clic en el **estado** del trabajo para ver los últimos detalles del estado de envío para la tarea.
4. Revise los últimos detalles del estado de envío para identificar y resolver los problemas de configuración.



Supervisión del rendimiento del enlace y de la aplicación de SD-WAN

Para supervisar el rendimiento de la aplicación y el enlace en sus clústeres de VPN para solucionar problemas, consulte la información de resumen de todos los clústeres de VPN y, a continuación, realice un desglose sucesivamente para aislar los problemas de los sitios, aplicaciones y enlaces afectados. La visibilidad del tráfico SD-WAN se muestra en el cortafuegos SD-WAN que recibe el tráfico. Por ejemplo, para el tráfico del cortafuegos del hub al cortafuegos de sucursal, los datos de supervisión de SD-WAN se reflejan en el cortafuegos de sucursal. El panel de inicio muestra lo siguiente:

- Rendimiento de la aplicación
  - **Impactado**: una o más aplicaciones del clúster de VPN para las que ninguna de las rutas tiene vibración, latencia o rendimiento de pérdida de paquetes que cumplen con los umbrales especificados en el perfil de calidad de ruta en la lista de rutas a partir de las que el cortafuegos puede elegir.
  - **Correcto**: número de clústeres, hubs y sucursales VPN que no experimentan problemas de rendimiento de vibración, latencia o pérdida de paquetes.
- Enlace de rendimiento
  - **Error**: uno o más sitios en el clúster de VPN tienen problemas de conectividad, como cuando un túnel o una interfaz virtual (VIF) están inactivos.
  - **Advertencia**: número de clústeres, hubs y sucursales VPN que tienen enlaces con mediciones de rendimiento de fluctuación, latencia o pérdida de paquetes que superan el valor promedio móvil de siete días de la métrica deancho de banda (compatible con PAN-OS 11.2.0 con el complemento SD-WAN 3.3.0 y versiones posteriores)ancho de banda (compatible con PAN-OS 11.1.5 y versiones posteriores con el complemento SD-WAN 3.2.2 y versiones posteriores) .
  - **OK**: número de clústeres, hubs y sucursales de VPN que no experimentan ninguna fluctuación, latencia o problemas de rendimiento de pérdida de paquetes de ancho de banda (compatible con PAN-OS 11.2.0 con el complemento SD-WAN 3.3.0 y versiones posteriores), ancho de banda (compatible con PAN-OS 11.1.5 y versiones posteriores con el complemento SD-WAN 3.2.2 y versiones posteriores).

  A partir de PAN-OS 11.2.0, el complemento SD-WAN 3.3.0 y versiones posteriores son compatibles con el 'ancho de banda' que es la medida principal del rendimiento del enlace.A partir de PAN-OS 11.1.5, el complemento SD-WAN 3.2.2 y las versiones posteriores son compatibles con el 'ancho de banda', que es la medida principal del rendimiento del enlace.

Si un servidor de seguridad del hub o sucursal tiene una regla de políticas SD-WAN configurada con la corrección de errores de reenvío, se muestra un mensaje `Error Correction Initiated (Corrección de errores iniciada)` para notificarle que el cortafuegos de hub o sucursal detectó y corrigió errores en los datos transmitidos para una aplicación.

Los hubs de SD-WAN muestran `Error Correction Initiated (Corrección de errores iniciada)` solo si el tráfico se originó desde el hub de SD-WAN a la sucursal SD-WAN y coincidió con una regla de políticas SD-WAN con un perfil de corrección de errores adjunto.

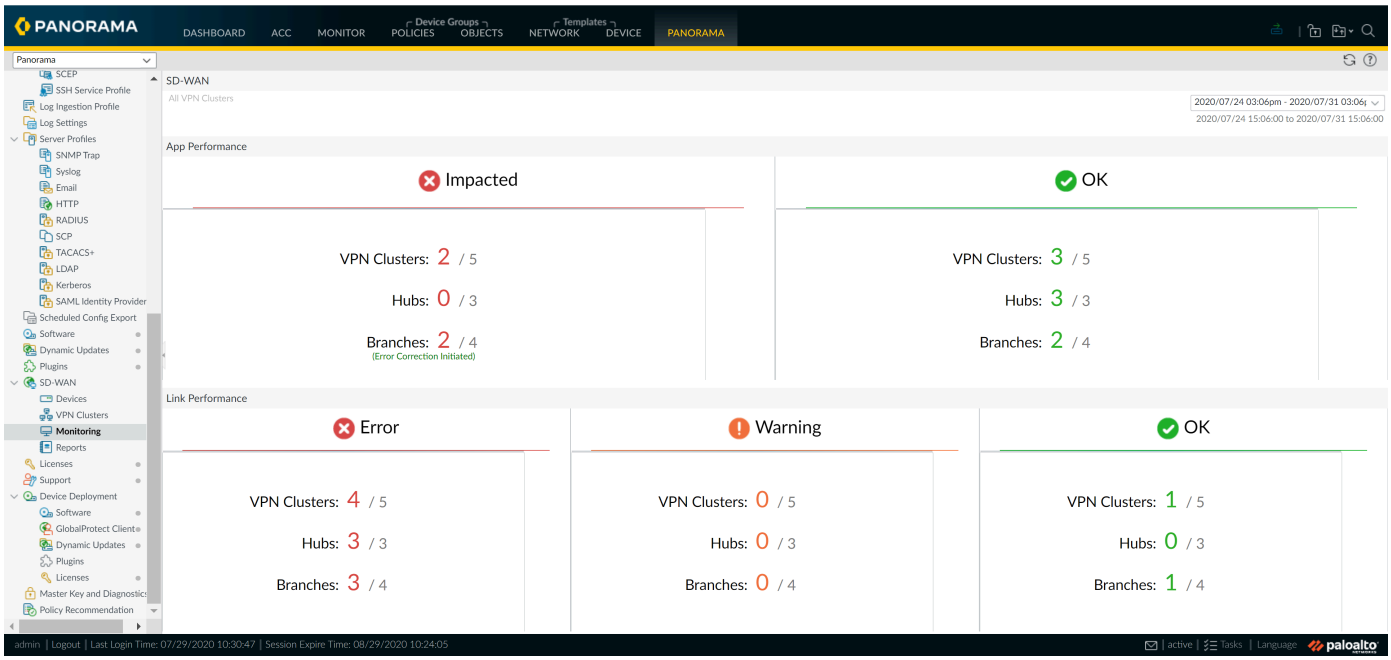
Desde el panel de inicio, reduzca la vista a aplicaciones o enlaces afectados que tengan el estado de Error o Advertencia. A continuación, seleccione un sitio afectado para ver los detalles a nivel de sitio. Desde el sitio, vea los detalles a nivel de aplicación o de enlace.

Consulte Supervisión del rendimiento del enlace y de la aplicación de la central de Prisma Accesspara supervisar el rendimiento de la aplicación y el enlace para los hubs de Prisma Access.

Si no hay datos presentes o la pantalla indica que SD-WAN no está definida, compruebe en la Matriz de compatibilidad que la versión de Panorama que está utilizando sea compatible con la versión del complemento de SD-WAN que está intentando utilizar.

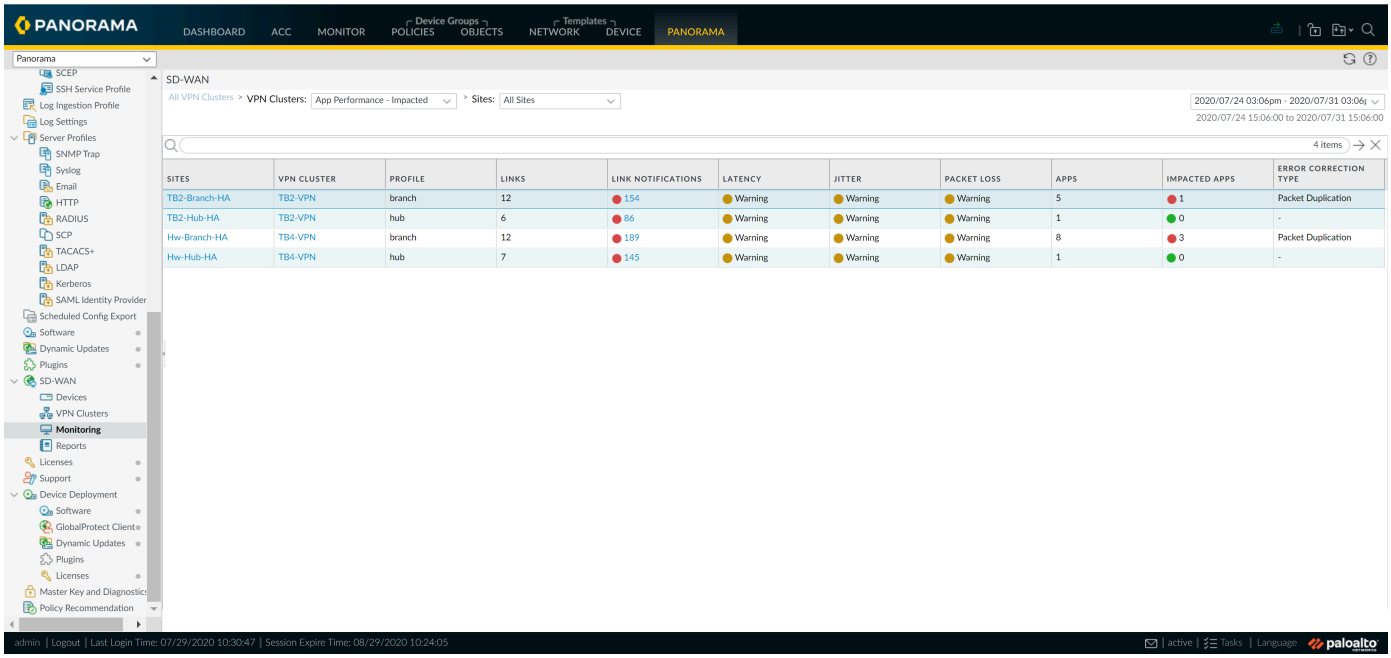
STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Supervisión** para ver resúmenes de estado de sus clústeres de VPN, hubs y sucursales.



STEP 3 | Haga clic en un resumen del rendimiento de la aplicación o del rendimiento del enlace que indique los recuentos de impacto, error o advertencias para ver una lista detallada de sitios y su estado según la latencia, la fluctuación y la pérdida de paquetes ancho de banda (compatible con PAN-OS 11.2.0 con el complemento SD-WAN 3.3.0 y versiones posteriores

para el rendimiento del enlace), ancho de banda (compatible con PAN-OS 11.1.5 y versiones posteriores con el complemento SD-WAN 3.2.2 y versiones posteriores).



STEP 4 | Haga clic en un sitio que muestre Advertencia o Error para ver un clúster de VPN. Los datos del sitio muestran el rendimiento de la aplicación y el rendimiento del enlace, incluidas las aplicaciones impactadas. Además, use el filtro Sitios para ver los clústeres de VPN basados en notificaciones de enlaces, desviaciones de latencia, desviaciones de vibración, desviaciones de pérdida de paquetes o aplicaciones impactadas.

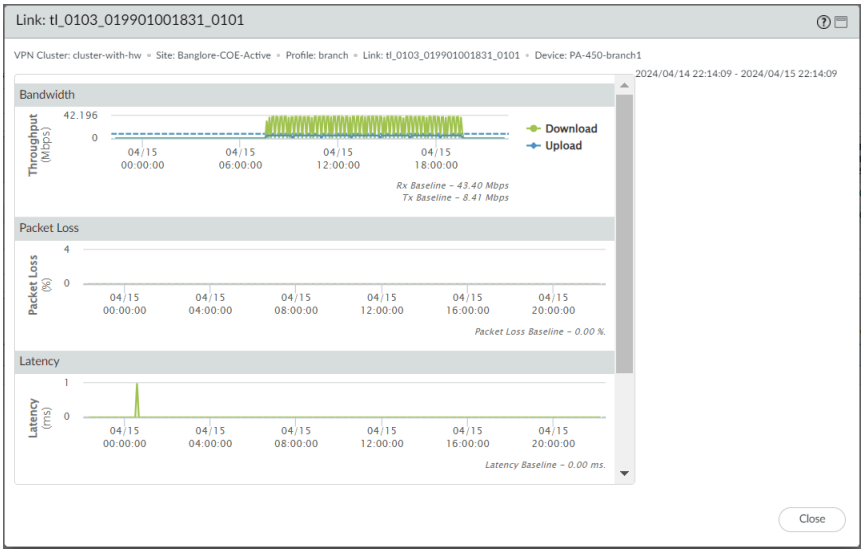
(PAN-OS 11.2.0 con complemento SD-WAN 3.3.0 y versiones posteriores) (PAN-OS 11.1.5 y versiones posteriores con complemento SD-WAN 3.2.2 y versiones posteriores) Ahora puede ver el nuevo parámetro de rendimiento del enlace, **maximum upload/download speed (velocidad máxima de carga/descarga)** para el sitio seleccionado en un clúster VPN.

Haga clic en cada **Link (Enlace)** para ver la fluctuación, la pérdida de paquetes y la latencia de referencia medida para el túnel ancho de banda (compatible con PAN-OS 11.2.0 con el complemento SD-WAN 3.3.0 y versiones posteriores) ancho de banda (compatible con PAN-OS 11.1.5 y versiones posteriores con complemento SD-WAN 3.2.2 y versiones posteriores).

(PAN-OS 11.2.0 con complemento SD-WAN 3.3.0 y versiones posteriores) (PAN-OS 11.1.5 y versiones posteriores con complemento SD-WAN 3.2.2 y versiones posteriores) El gráfico de **Bandwidth (Ancho de banda)** muestra las velocidades máximas de carga y descarga de los enlaces físicos y de túnel.

- Para el enlace físico, el gráfico muestra la configuración del perfil de interfaz SD-WAN (si está configurada) como el valor máximo. De lo contrario, el gráfico muestra el valor máximo de Tx y Rx que el enlace físico ha visto hasta ahora como el valor máximo.

- Para los enlaces de túnel, el gráfico muestra el valor máximo de Tx y Rx que el túnel ha visto hasta ahora como el valor máximo.



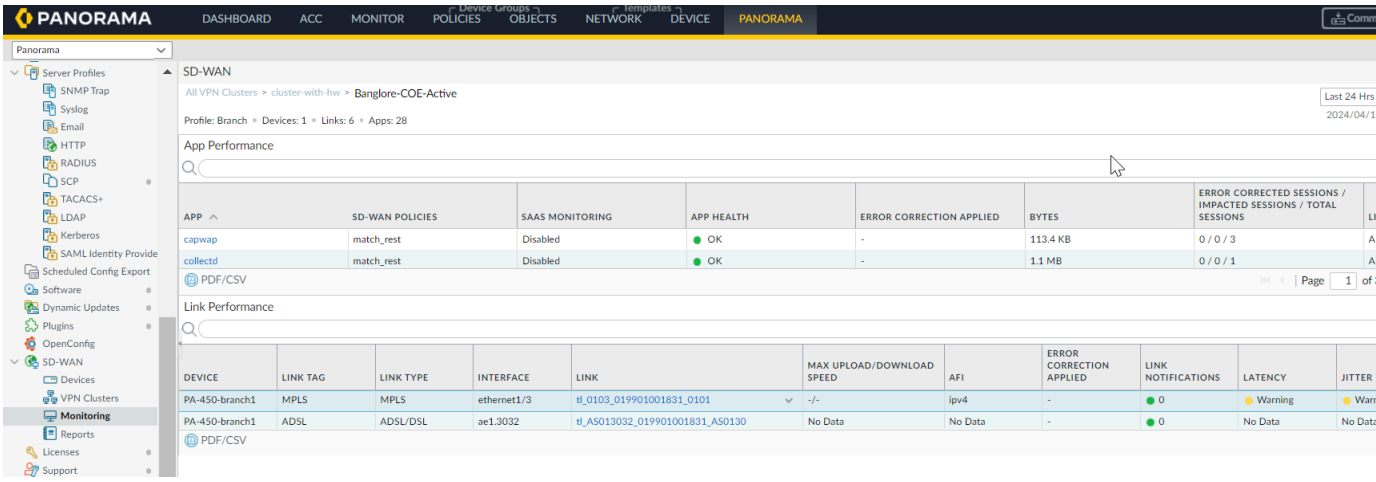
Para las aplicaciones SaaS a través de un enlace de acceso directo a Internet (DIA, Direct Internet Access), la columna **SaaS Monitoring (Supervisión SaaS)** indica si la aplicación se crea en un perfil de SaaS Quality (Calidad SaaS) y está asociada con uno o más reglas de políticas SD-WAN.

- `Disabled (Deshabilitado)`: la aplicación no es una aplicación SaaS configurada en un perfil de calidad de SaaS.
- `Enabled (Habilitado)`: la aplicación es una aplicación SaaS configurada en un perfil de calidad de SaaS y está asociada con una o más políticas de SD-WAN.

Si asoció un perfil de corrección de errores con una regla de políticas SD-WAN para una aplicación, las columnas **Error Correction Applied (Corrección de errores aplicada)** muestran si se aplicó y el tipo de corrección de errores. Además, puede ver las **sesiones corregidas de errores/sesiones afectadas/sesiones totales** para conocer el número de sesiones para las que

el cortafuegos de hub o sucursal corrigió errores en relación con la cantidad total de sesiones para el período especificado.

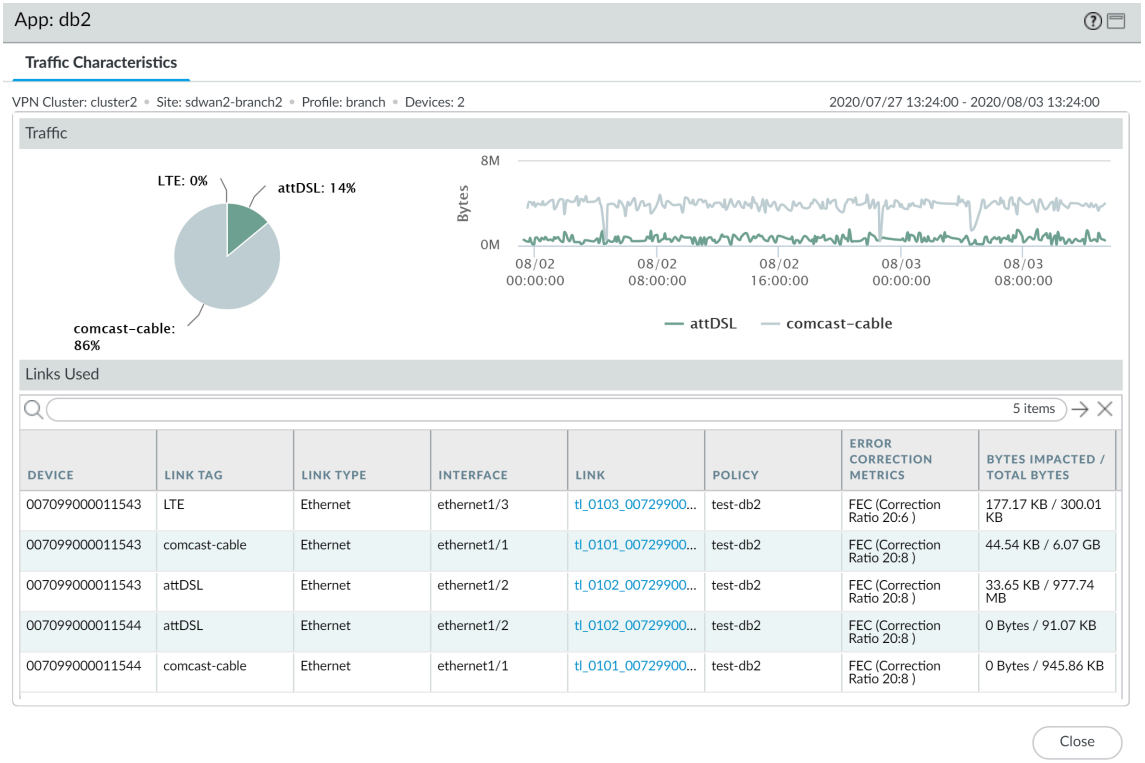
Haga clic en **PDF/CSV** para exportar la información de estado detallada para las aplicaciones y enlaces en el sitio en formato PDF o CSV.

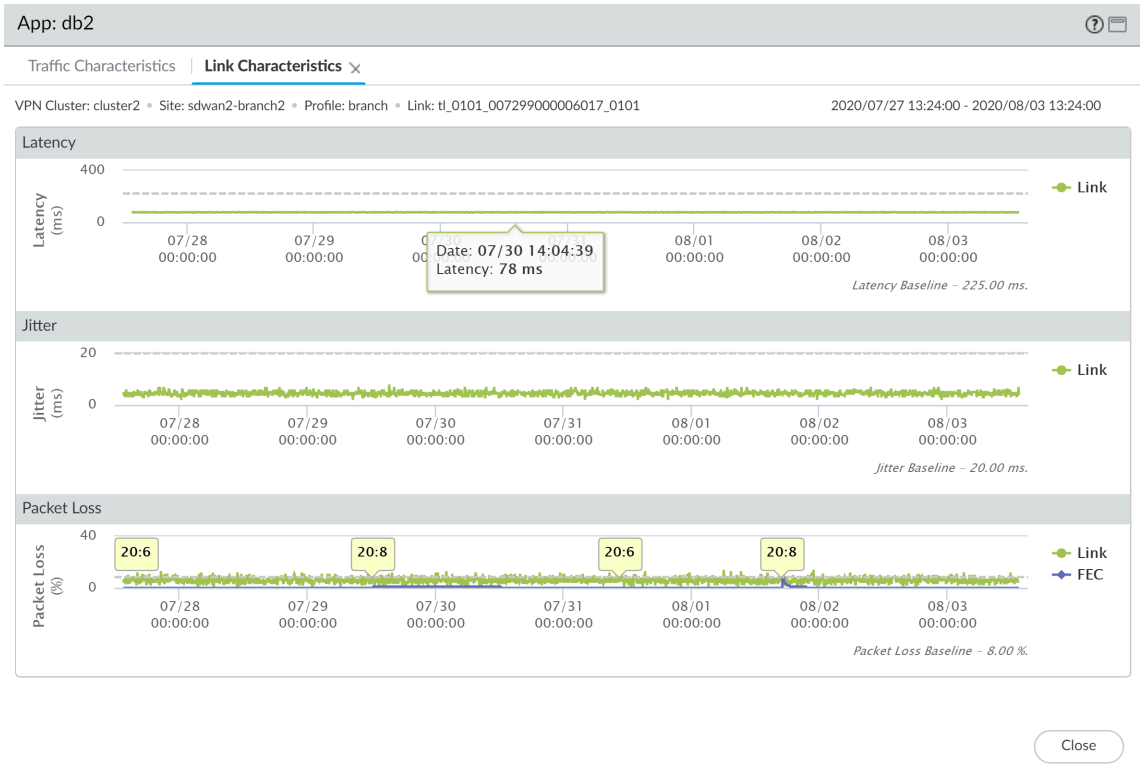


STEP 5 | Haga clic en la sucursal o hub que tengan una aplicación que precise atención.

STEP 6 | Haga clic en una aplicación impactada para ver los detalles a nivel de aplicación o de enlace.

Por ejemplo, observe las características del enlace de una aplicación para comprender la latencia, la fluctuación y la pérdida de paquetes de la aplicación a través del enlace especificado. Además, puede ver cuándo se aplicó la corrección de errores para el enlace.





Supervisión de hubs de Prisma Access

Establezca los valores de referencia y supervise el rendimiento del enlace y de la aplicación de la central de Prisma Access para comprender cómo configurar y modificar sus perfiles de gestión de enlaces de SD-WAN.

- Valores de referencia del rendimiento del enlace y de la aplicación de central de Prisma Access
- Supervisión del rendimiento del enlace y de la aplicación de la central de Prisma Access

Valores de referencia del rendimiento del enlace y de la aplicación de central de Prisma Access

Antes de Configuración de los perfiles de gestión de enlaces SD-WAN, Palo Alto Networks recomienda que establezca los valores de referencia del rendimiento del enlace y de la aplicación de central de Prisma Access para comprender mejor la actividad de carga útil normal de la central de Prisma Access para evitar el innecesario intercambio de enlaces para aplicaciones y tráfico que no lo requieran.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Incorporación de cortafuegos PAN-OS a Prisma Access.

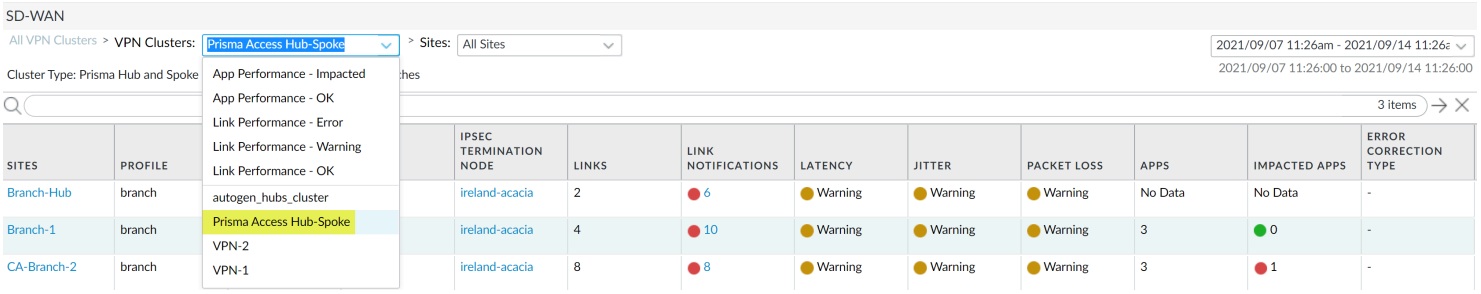
STEP 3 | Seleccione **Panorama** > **SD-WAN** > **Monitoreo (Supervisión)** y modifique el rango de tiempo de supervisión SD-WAN.

Cuanto más extenso sea el marco de tiempo que utilice para establecer los valores de referencia del rendimiento del enlace y de la aplicación de central de Prisma Access, más precisa será la referencia. Como mínimo, evalúe el rendimiento de tres días de la aplicación y del enlace para establecer los valores de referencia para los datos de latencia, fluctuación y pérdida de paquetes que utiliza para crear sus perfiles de gestión de enlaces SD-WAN.

Palo Alto Networks recomienda evaluar siete días de datos de rendimiento de aplicaciones y enlaces para establecer los valores de referencia de la latencia, fluctuación y pérdida de paquetes para la central de Prisma Access.

STEP 4 | Filtre la supervisión SD-WAN para mostrar solo los clústeres VPN de central y radio de Prisma Access.

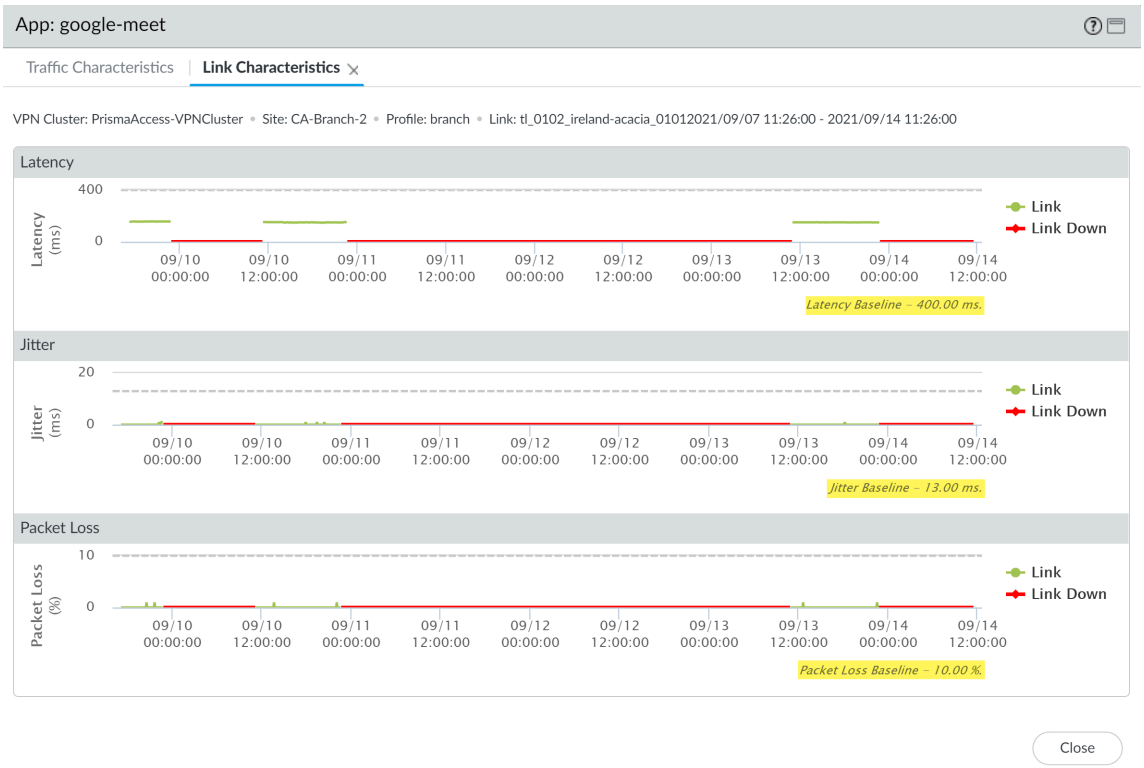
1. Haga clic en el resumen de rendimiento de la aplicación o rendimiento del enlace que indica los recuentos de Impactado, Error o Advertencia para ver una lista detallada de los sitios y su estado en función de la latencia, la vibración y la pérdida de paquetes.
2. En el filtro del clúster VPN, seleccione **Prisma Access Hub-Spoke (Central y radio de Prisma Access)**.
3. Haga clic en un sitio para ver detalles del estado en profundidad para la central de Prisma Access.



STEP 5 | Revise las características del enlace para una aplicación de central de Prisma Access.

1. Haga clic en una aplicación en la sección App Performance (Rendimiento de la aplicación) para ver las características de tráfico y los vínculos utilizados para el tráfico de aplicaciones.
2. Haga clic en cada enlace para ver los valores de referencia de la latencia, la fluctuación y la pérdida de paquetes medidos para la aplicación a través del enlace.

   Repita esto para todos los enlaces hasta que reúna suficientes datos de referencia para modificar el perfil de calidad de ruta de la central de Prisma Access.



STEP 6 | Modifique el perfil de calidad de ruta de la central de Prisma Access en función de los valores de referencia de latencia, fluctuación y pérdida de paquetes que recopiló.

STEP 7 | A continuación,configure SD-WAN según sea necesario.

STEP 8 | Supervisión del rendimiento del enlace y de la aplicación de la central de Prisma Access para configurar con precisión los perfiles de gestión de enlaces SD-WAN.

Supervisión del rendimiento del enlace y de la aplicación de la central de Prisma Access

Supervise el rendimiento de la aplicación y el enlace de la central de Prisma Access para solucionar problemas mediante la consulta de información de resumen de todos los clústeres de VPN y luego realice un desglose sucesivo para aislar los problemas de los sitios, aplicaciones y enlaces afectados. La visibilidad del tráfico de SD-WAN se muestra en la implementación de Prisma Access o en el cortafuegos SD-WAN que recibe el tráfico. Por ejemplo, para el tráfico del

cortafuegos del hub al cortafuegos de sucursal, los datos de supervisión de SD-WAN se reflejan en el cortafuegos de sucursal. El panel de inicio muestra lo siguiente:

- Rendimiento de la aplicación
  - **Impactado**: una o más aplicaciones del clúster de VPN para las que ninguna de las rutas tiene vibración, latencia o rendimiento de pérdida de paquetes que cumplen con los umbrales especificados en el perfil de calidad de ruta en la lista de rutas a partir de las que el cortafuegos puede elegir.
  - **Correcto**: número de clústeres, hubs y sucursales VPN que no experimentan problemas de rendimiento de vibración, latencia o pérdida de paquetes.
- Enlace de rendimiento
  - **Error**: uno o más sitios en el clúster de VPN tienen problemas de conectividad, como cuando un túnel o una interfaz virtual (VIF) están inactivos.
  - **Advertencia**: número de clústeres de VPN, centrales y sucursales que tienen enlaces con mediciones de rendimiento de pérdida de paquetes, vibración o latencia que superan el valor medio móvil de siete días de la métrica.
  - **Correcto**: número de clústeres, hubs y sucursales VPN que no experimentan problemas de rendimiento de vibración, latencia o pérdida de paquetes.

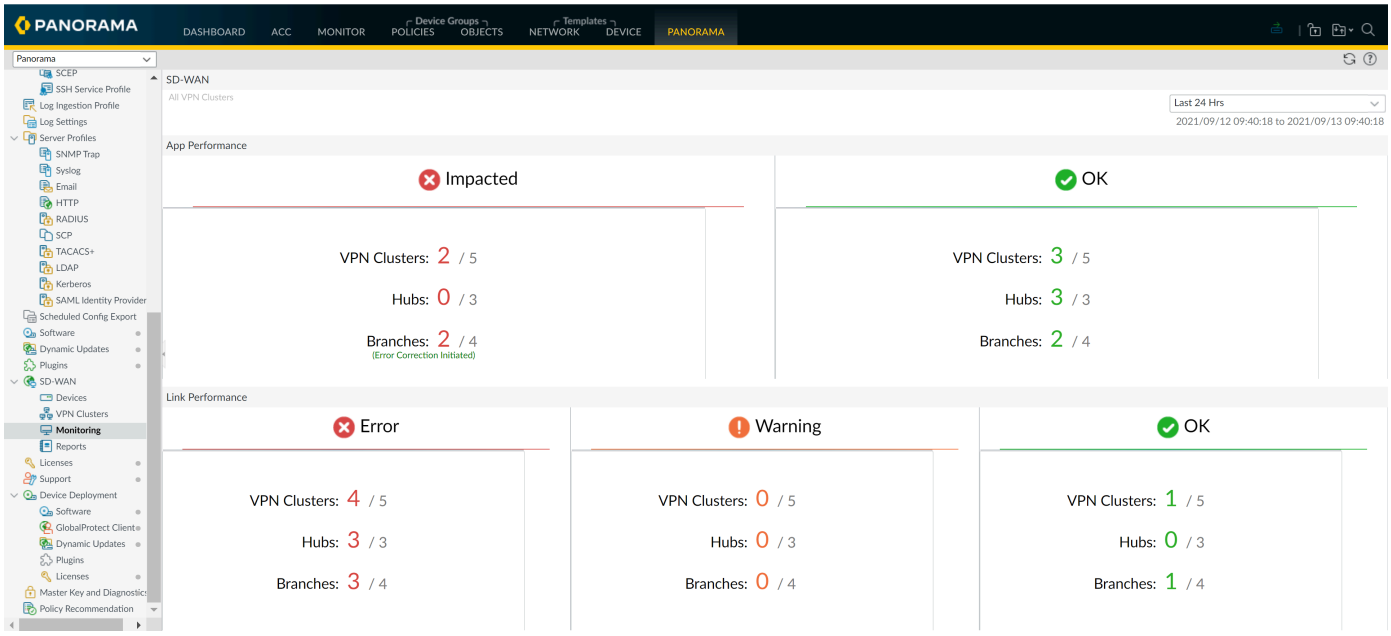
Desde el panel de inicio, reduzca la vista a aplicaciones o enlaces afectados que tengan el estado de Error o Advertencia. A continuación, seleccione un sitio afectado para ver los detalles a nivel de sitio. Desde el sitio, vea los detalles a nivel de aplicación o de enlace.

Consulte Supervisión del rendimiento del enlace y de la aplicación de SD-WAN para supervisar el rendimiento de la aplicación y del enlace en todos los sitios SD-WAN.

Si no hay datos presentes o la pantalla indica que SD-WAN no está definida, compruebe en la Matriz de compatibilidad que la versión de Panorama que está utilizando sea compatible con la versión del complemento de SD-WAN que está intentando utilizar.

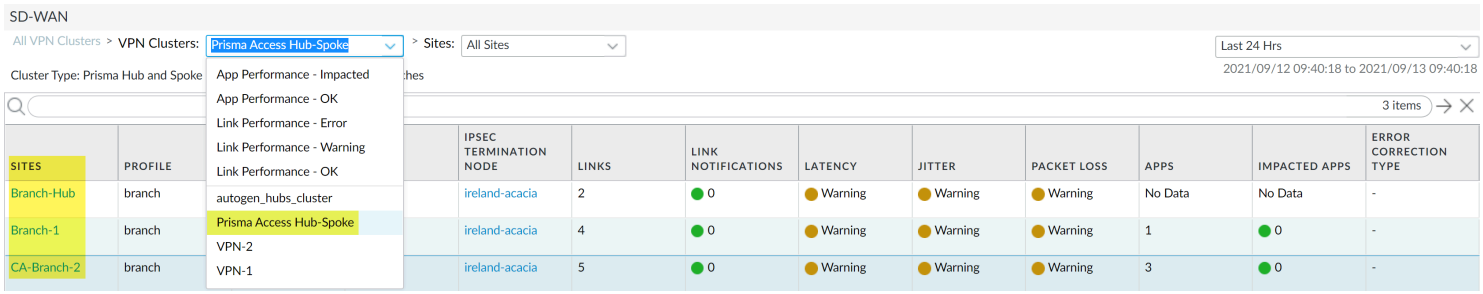
STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Supervisión** para ver resúmenes de estado de sus clústeres de VPN, hubs y sucursales.



STEP 3 | Filtre la supervisión SD-WAN para mostrar solo los clústeres VPN de central y radio de Prisma Access.

1. Haga clic en el resumen de rendimiento de la aplicación o rendimiento del enlace que indica los recuentos de Impactado, Error o Advertencia para ver una lista detallada de los sitios y su estado en función de la latencia, la vibración y la pérdida de paquetes.
2. En el filtro del clúster VPN, seleccione **Prisma Access Hub-Spoke (Central y radio de Prisma Access)**.
3. Haga clic en un sitio para ver detalles del estado en profundidad para la central de Prisma Access.



STEP 4 | Revise los detalles del estado en profundidad de la central de Prisma Access.

Los datos del sitio muestran los detalles de incorporación de Prisma Access, así como el rendimiento de la aplicación y del enlace, incluidas las aplicaciones afectadas.

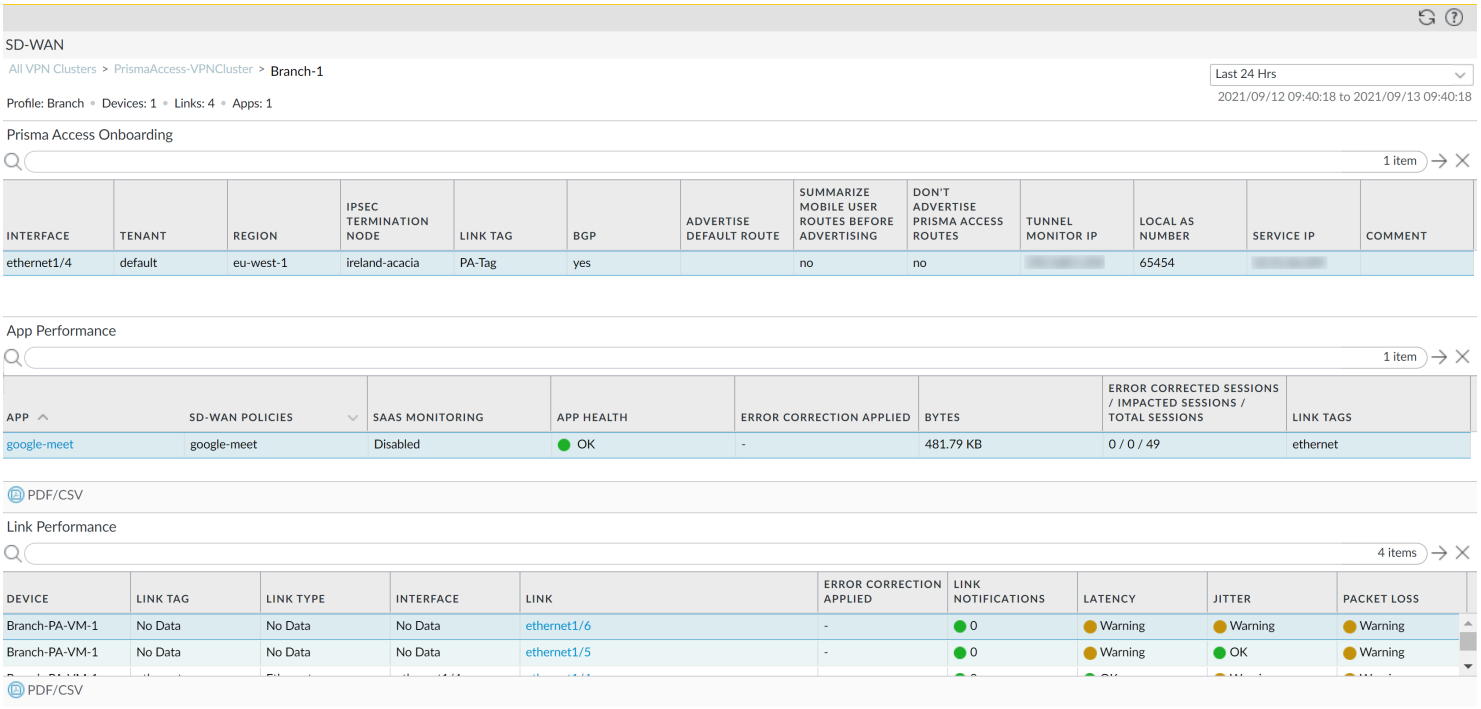
Para las aplicaciones SaaS a través de un enlace de acceso directo a Internet (DIA, Direct Internet Access), la columna **SaaS Monitoring (Supervisión SaaS)** indica si la aplicación se crea

en un perfil de SaaS Quality (Calidad SaaS) y está asociada con uno o más reglas de políticas SD-WAN.

- `Disabled (Deshabilitado)`: la aplicación no es una aplicación SaaS configurada en un perfil de calidad de SaaS.
- `Enabled (Habilitado)`: la aplicación es una aplicación SaaS configurada en un perfil de calidad de SaaS y está asociada con una o más políticas de SD-WAN.

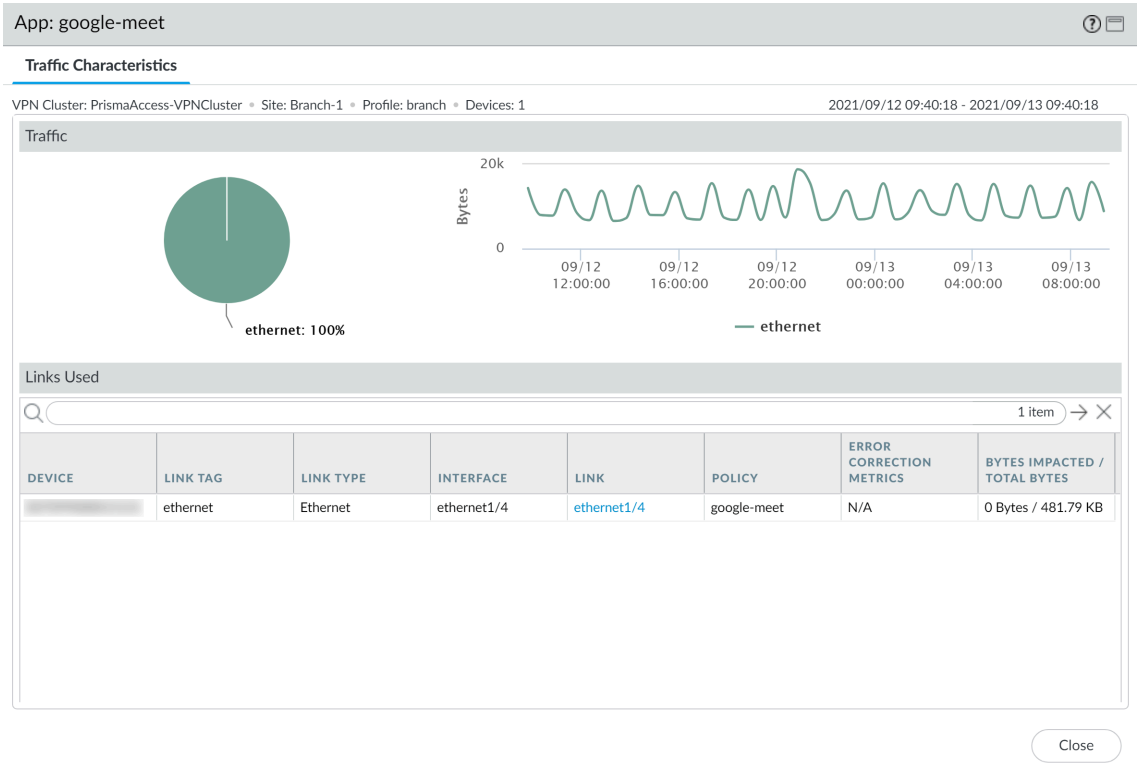
Si asoció un perfil de corrección de errores con una regla de políticas SD-WAN para una aplicación, las columnas **Error Correction Applied (Corrección de errores aplicada)** muestran si se aplicó y el tipo de corrección de errores. Además, puede ver las **sesiones corregidas de errores/sesiones afectadas/sesiones totales** para conocer el número de sesiones para las que el cortafuegos de hub o sucursal corrigió errores en relación con la cantidad total de sesiones para el período especificado.

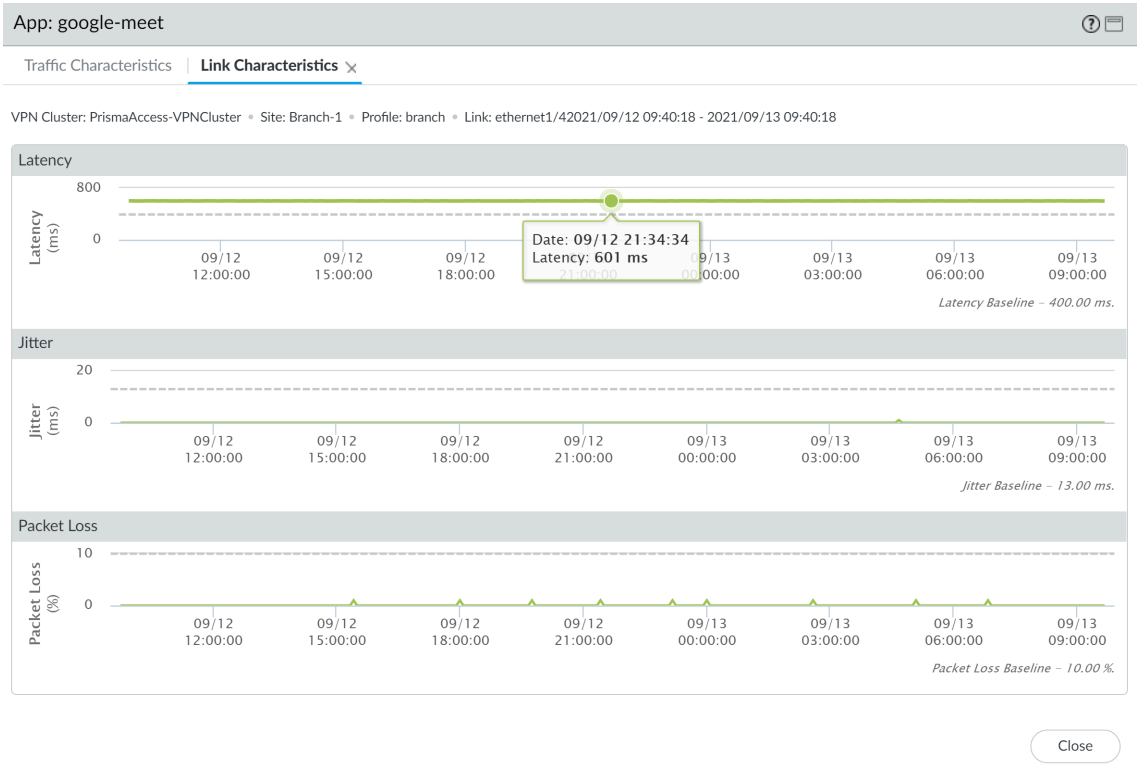
Haga clic en **PDF/CSV** para exportar la información de estado detallada para las aplicaciones y enlaces en el sitio en formato PDF o CSV.



STEP 5 | Haga clic en una aplicación impactada para ver los detalles a nivel de aplicación o de enlace.

Por ejemplo, observe las características del enlace de una aplicación para comprender la latencia, la fluctuación y la pérdida de paquetes de la aplicación a través del enlace especificado. Además, puede ver cuándo se aplicó la corrección de errores para el enlace.





Generación de un informe de SD-WAN

Configure y genere un informe de SD-WAN que detalle las principales aplicaciones o enlaces con la mayor frecuencia de degradación de la calidad de la ruta. La solicitud de pedido o los enlaces que aparecen en un informe se basan en la cantidad de datos afectados; cuantos más datos se vean afectados, mayor será la aplicación o el enlace que aparecerá en el informe. Los informes de SD-WAN se generan según sea necesario y no se pueden programar. Utilice los informes de SD-WAN para comprobar el rendimiento correcto de la aplicación o el enlace, o asegúrese de que los usuarios no noten el impacto de ellos. Por ejemplo, si su ISP garantizó un cierto rendimiento en un enlace, genere un informe de rendimiento de enlace para ese enlace para comprobar que se respete el ancho de banda garantizado.

Desde el servidor de gestión Panorama™, solo puede generar informes para aplicaciones o enlaces en todos los cortafuegos habilitados para SD-WAN. Para generar un informe para aplicaciones o enlaces procesados por un cortafuegos individual, debe crear y generar el informe localmente en el cortafuegos.

Si no hay datos presentes o la pantalla indica que SD-WAN no está definida, compruebe en la Matriz de compatibilidad que la versión de Panorama que está utilizando sea compatible con la versión del complemento de SD-WAN que está intentando utilizar.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Informes** y **añada** un nuevo informe.

STEP 3 | Configure los parámetros del informe de SD-WAN.

1. Introduzca un nombre descriptivo en **Nombre** para el informe.
2. Elija el **tipo de informe** que generar:
   - Seleccione **Rendimiento de la aplicación** para generar un informe que detalle solo el rendimiento del estado de la aplicación.
   - Seleccione **Rendimiento del enlace** para generar un informe que detalle solo el rendimiento del estado del enlace.
3. Seleccione el **clúster** de la VPN para el que desee generar un informe. De forma predeterminada, se selecciona **todos**.
4. Seleccione un **sitio** dentro del clúster de VPN seleccionado para el que generar el informe. De forma predeterminada, se selecciona **todos**.

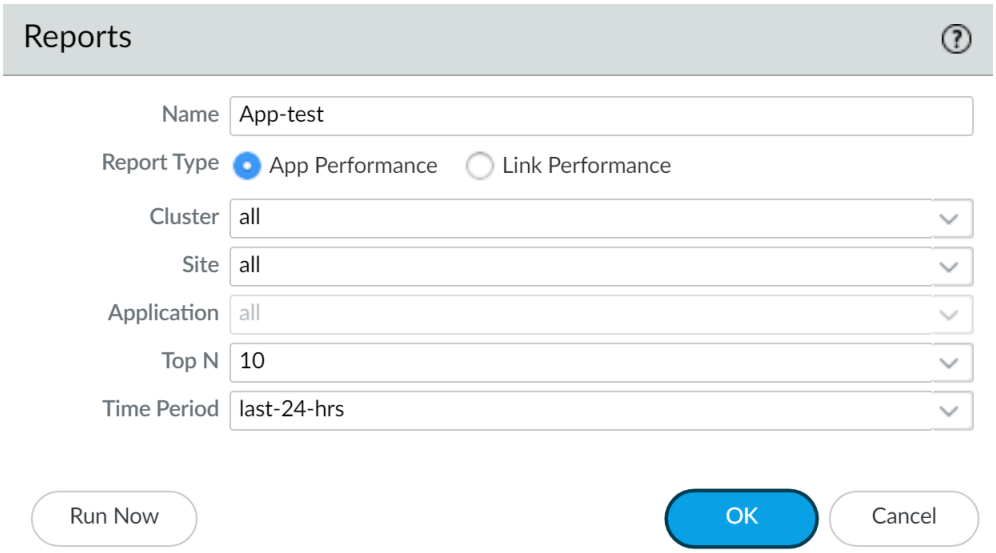
   Si seleccionó **todos** los clústeres, este campo estará atenuado y no se podrá seleccionar un sitio.
5. (Solo rendimiento de la aplicación) Seleccione la **aplicación** para la que generar el informe.

   Si seleccionó **todos** los clústeres y sitios, este campo estará atenuado y no se podrá seleccionar una aplicación individual.
6. (Solo rendimiento del enlace) Seleccione la **etiqueta de enlace** para la que generar el informe. Cuando seleccione una etiqueta de enlace, se generará un informe para

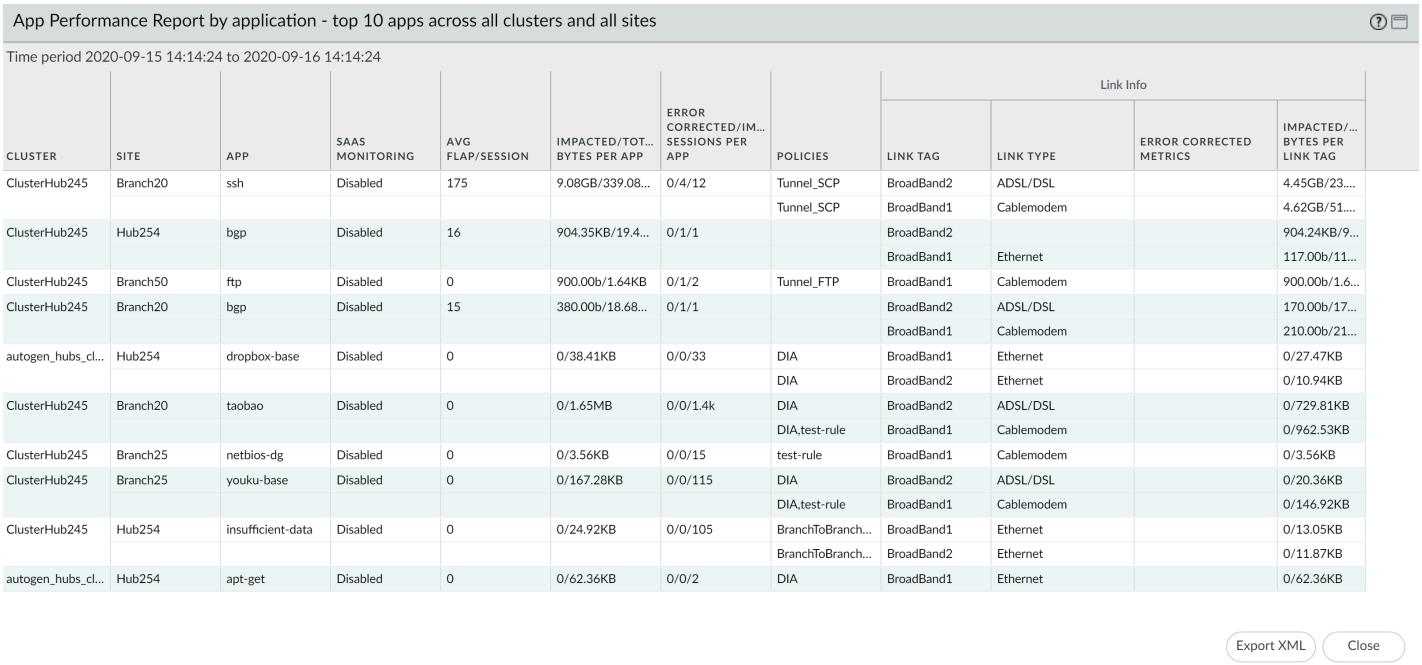
todos los enlaces agrupados mediante la etiqueta en el clúster o sitio. De forma predeterminada, se selecciona **todos**.

7. (Solo rendimiento del enlace) Seleccione el **tipo de enlace** para la que generar el informe. Cuando seleccione un tipo de enlace, se generará un informe para todos los enlaces del tipo especificado en el clúster o sitio. De forma predeterminada, se selecciona **todos**.
8. Seleccione las aplicaciones o enlaces **Top N** que incluir en el informe. Esta configuración determina la cantidad de aplicaciones o enlaces que experimentan una degradación del estado que incluir en el informe. De forma predeterminada, el informe incluye las **5** principales aplicaciones o enlaces que experimentan una degradación del estado.
9. Especifique el **periodo** en el que generar el informe. De manera predeterminada, se selecciona **Ninguno** y se consulta el historial completo del estado de las aplicaciones o enlaces.

STEP 4 | Haga clic en **Ejecutar ahora** para generar el informe.



STEP 5 | Vea el informe generado y seleccione **Exportar XML** para exportar el informe en formato XML en su dispositivo local. Cuando esté listo, haga clic en **Cerrar**.



App Performance Report by application - top 10 apps across all clusters and all sites

Time period 2020-09-15 14:14:24 to 2020-09-16 14:14:24

CLUSTER	SITE	APP	SAAS MONITORING	AVG FLAP/SESSION	IMPACTED/TOT... BYTES PER APP	ERROR CORRECTED/IM... SESSIONS PER APP	POLICIES	Link Info			
								LINK TAG	LINK TYPE	ERROR CORRECTED METRICS	IMPACTED/... BYTES PER LINK TAG
ClusterHub245	Branch20	ssh	Disabled	175	9.08GB/339.08...	0/4/12	Tunnel_SCP	BroadBand2	ADSL/DSL		4.45GB/23....
							Tunnel_SCP	BroadBand1	Cablemodem		4.62GB/51....
ClusterHub245	Hub254	bgp	Disabled	16	904.35KB/19.4...	0/1/1		BroadBand2			904.24KB/9...
								BroadBand1	Ethernet		117.00b/11...
ClusterHub245	Branch50	ftp	Disabled	0	900.00b/1.64KB	0/1/2	Tunnel_FTP	BroadBand1	Cablemodem		900.00b/1.6...
ClusterHub245	Branch20	bgp	Disabled	15	380.00b/18.68...	0/1/1		BroadBand2	ADSL/DSL		170.00b/17...
								BroadBand1	Cablemodem		210.00b/21...
autogen_hubs_cl...	Hub254	dropbox-base	Disabled	0	0/38.41KB	0/0/33	DIA	BroadBand1	Ethernet		0/27.47KB
							DIA	BroadBand2	Ethernet		0/10.94KB
ClusterHub245	Branch20	taobao	Disabled	0	0/1.65MB	0/0/1.4k	DIA	BroadBand2	ADSL/DSL		0/729.81KB
							DIA,test-rule	BroadBand1	Cablemodem		0/962.53KB
ClusterHub245	Branch25	netbios-dg	Disabled	0	0/3.56KB	0/0/15	test-rule	BroadBand1	Cablemodem		0/3.56KB
ClusterHub245	Branch25	youku-base	Disabled	0	0/167.28KB	0/0/115	DIA	BroadBand2	ADSL/DSL		0/20.36KB
							DIA,test-rule	BroadBand1	Cablemodem		0/146.92KB
ClusterHub245	Hub254	insufficient-data	Disabled	0	0/24.92KB	0/0/105	BranchToBranch...	BroadBand1	Ethernet		0/13.05KB
							BranchToBranch...	BroadBand2	Ethernet		0/11.87KB
autogen_hubs_cl...	Hub254	apt-get	Disabled	0	0/62.36KB	0/0/2	DIA	BroadBand1	Ethernet		0/62.36KB

Export XML Close

STEP 6 | En la ventana emergente Informes, haga clic en **Aceptar** para guardar su informe configurado.

STEP 7 | Seleccione **Confirmar** > **Confirmar en Panorama** y haga clic en **Confirmar** para confirmar los cambios.

Solución de problemas

Utilice la Interfaz de línea de comandos (CLI) del servidor de gestión Panorama™ para ver información de SD-WAN y realizar operaciones.

- Uso de comandos de la CLI para tareas de SD-WAN
- Sustituir un dispositivo SD-WAN
- Solución de problemas del rendimiento de la aplicación
- Solución de problemas del rendimiento del enlace
- Actualización de cortafuegos de SD-WAN
- Instalar el complemento de SD-WAN.
- Desinstalación del complemento de SD-WAN

Uso de comandos de la CLI para tareas de SD-WAN

Utilice los siguientes comandos de la CLI para ver y borrar la información de SD-WAN y ver los contadores globales de SD-WAN.. También puede ver la información del túnel VPN, la información de BGP y la información de la interfaz de SD-WAN.

Si quiere...	Use...
Visualización o eliminación de la información de SD-WAN	
• Consulte los nombres de ruta e ID para una interfaz de SD-WAN, su estado, direcciones IP locales y de peers, y el número de interfaz de túnel.	`> show sdwan connection all | <sdwan-interface>`
• Consulte el número y el porcentaje de sesiones distribuidas en cada miembro del túnel de una interfaz de SD-WAN virtual.	`> show sdwan session distribution policy-name <sdwan-policy-name>`
• Consulte los nombres de las reglas de políticas de SD-WAN que envían tráfico a la interfaz de SD-WAN virtual especificada, junto con el método de distribución de tráfico, latencia configurada, vibración y umbrales de pérdida de paquetes, etiquetas de enlace identificadas para la regla e interfaces de túnel miembro.	`> show sdwan rule vif sdwan.x`
• Consulte los eventos de SD-WAN, como la selección de ruta y las mediciones de calidad de ruta. *Para PAN-OS 10.0.0 y 10.0.1, cuando realiza un cambio de configuración de SD-WAN (como un cambio de perfil de calidad de ruta) que provoca la selección de una ruta SD-WAN diferente, el log de tráfico no cuenta ni registra el cambio de ruta.*	`> show sdwan event`
• Elimine los eventos de SD-WAN.	`> clear sdwan event`

Si quiere...	Use...

• Consulte la latencia, la vibración y la pérdida de paquetes en una interfaz de SD-WAN virtual (especifique el número o el nombre de la interfaz).
 	
Las mediciones de latencia, vibración y pérdida de paquetes se toman y promedian en tres periodos. Cada periodo tiene una versión de estado, que se incrementa cuando cambia un valor de parámetro de estado (que supera el umbral). Además de la medición en tiempo real, existe una medición de uso actual, que muestra el valor del parámetro la última vez que el cambio de valor en tiempo real superó el umbral.
	`> show sdwan path-monitor stats vif <sdwan.x>`
	
	`> show sdwan path-monitor stats vif <sdwan-interface-name>`

• Consulte el nombre de la regla de políticas de SD-WAN que coincide con la sesión especificada, las interfaces de túnel de origen y destino, la latencia configurada, la vibración y el porcentaje de pérdida de paquetes para la regla y el método de distribución del tráfico. *Para PAN-OS 10.0.0 y 10.0.1, cuando realiza un cambio de configuración de SD-WAN (como un cambio de perfil de calidad de ruta) que provoca la selección de una ruta SD-WAN diferente, el log de tráfico no cuenta ni registra el cambio de ruta.*	`> show sdwan session path-select session-id <session-id>`
• Consulte el modo de supervisión para el enlace de SD-WAN virtual (agresivo o relajado) e intervalos de actualización.	`> show sdwan path-monitor parameter path-name <sdwan-path-name>`
• Consulte el modo de supervisión para la interfaz de SD-WAN virtual (agresiva o relajada), intervalos de actualización y estadística de sondeo.	`> show sdwan path-monitor parameter vif <sdwan.x>`
Visualización de los contadores globales para solucionar problemas de SD-WAN	

Si quiere...	Use...

• En una sucursal, compruebe que el número de paquetes de solicitud de sondeo de SD-WAN transmitidos sea igual al número de paquetes de respuesta de sondeo recibidos.
 	
En un cortafuegos de sucursal, la mayoría de los túneles de SD-WAN son el iniciador, lo que significa que el túnel tendrá habilitado el sondeo de supervisión de la ruta de SD-WAN.
	`> show counter global filter delta yes`
	
	`flow_sdwan_prob_req_tx`
	
	`flow_sdwan_prob_reply_rx`

• En una central, compruebe que el número de paquetes de solicitud de sondeo de SD-WAN recibidos sea igual al número de paquetes de respuesta de sondeo transmitidos.
 	
En un cortafuegos de central, la mayoría de los túneles de SD-WAN son el respondedor, lo que significa que el túnel tendrá deshabilitado el sondeo de supervisión de la ruta de SD-WAN.
	`> show counter global filter delta yes`
	
	`flow_sdwan_prob_req_rx`
	
	`flow_sdwan_prob_reply_tx`

Visualización de la información del túnel VPN	
• Consulte todos los túneles creados en el cortafuegos.	`> show vpn flow`
• Consulte los detalles de túneles individuales identificados por nombre.	`> show vpn flow name <name>`
• Consulte los detalles de túneles individuales identificados por ID.	`> show vpn flow tunnel-id <tunnel-id>`
• Consulte los detalles de la fase 1 y la fase 2 del intercambio de claves de Internet (IKE) para todos los túneles.	`> show vpn ike-sa`
• Consulte las asociaciones de seguridad (SA) IKEv2 y las SA secundarias de IPSec IKEv2 de una puerta de enlace específica.	`> show vpn ike-sa gateway <gateway>`

Si quiere...	Use...
• Consulte los detalles del túnel.	`> show vpn tunnel`
Visualización de la información de BGP	
• Consulte el resumen de BGP para un enrutador virtual.	`> show routing protocol bgp summary virtual-router <virtual-router>`
• Consulte el resumen del peer de BGP.	`> show routing protocol bgp peer peer-name <peer-name> virtual-router <virtual-router>`
• Consulte el resumen de la base de información de enrutamiento local (RIB).	`> show routing protocol bgp loc-rib`
Visualización de la información de la interfaz de SD-WAN entre RIB y FIB	
• Consulte la nueva interfaz de salida de SD-WAN.	`> show routing route`
• Consulte las interfaces de SD-WAN en la base de información de reenvío (FIB).	`> show routing fib`

Sustituir un dispositivo SD-WAN

El proceso de autorización de devolución de mercancía (RMA) le permite reemplazar los dispositivos SD-WAN que hayan fallado o no funcionen bien con dispositivos SD-WAN funcionales nuevos o usados en una sucursal o en un centro de datos. Un dispositivo SD-WAN puede fallar o no funcionar bien por varias razones, como una fallo en el chip del dispositivo, una configuración incorrecta del dispositivo o por el desgaste. Si el dispositivo SD-WAN no se puede utilizar debido a un mal funcionamiento o a un fallo general, utilice el proceso de RMA para reemplazar el dispositivo que ha fallado o no funciona bien.

Se produce un fallo de confirmación en Panorama™ y los dispositivos gestionados si intenta reemplazar un cortafuegos SD-WAN de una implementación existente sin seguir un proceso RMA adecuado.

Antes de comenzar el proceso de RMA:

- Revise la sección Antes de iniciar una sustitución de un cortafuegos con RMA.
- La SD-WAN genera configuraciones, como puertas de enlace IPSec y keyIDs, basadas en el número de serie del dispositivo. Por lo tanto, debe actualizar el número de serie del cortafuegos de sustitución para SD-WAN, para reconocer el nuevo cortafuegos y evitar errores de confirmación. Descubra si su configuración SD-WAN tiene referencias de objetos IPSec o VPN al cortafuegos antiguo:
  - Para sustituir un cortafuegos de sucursal en una implementación de alta disponibilidad (HA), inicie sesión en el cortafuegos de hub y seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace IKE)**. Busque el número de serie (sin espacios en blanco) del cortafuegos antiguo. Si obtiene uno o más resultados de búsqueda, esto indica que la SD-WAN hace referencia al antiguo número de serie del cortafuegos en la configuración de puerta de enlace. En este caso, le recomendamos que desconecte el cortafuegos de sucursal antiguo de la implementación de Panorama y HA.
  - Para reemplazar un cortafuegos en una implementación de malla completa sin hubs, busque los números de serie del cortafuegos antiguo en cualquiera de los cortafuegos de sucursal. Si obtiene uno o más resultados de búsqueda, esto indica que la SD-WAN hace referencia al antiguo número de serie del cortafuegos en la configuración de puerta de enlace. En este caso, le recomendamos que desconecte el cortafuegos de sucursal antiguo de la implementación de Panorama y malla.
  - Para reemplazar un cortafuegos independiente, no es necesario buscar el número de serie.

Utilice el siguiente flujo de trabajo para restablecer la configuración en un cortafuegos gestionado cuando hay un RMA.

STEP 1 | Seleccione **Panorama** > **SD-WAN** > **VPN Clusters (Clústeres VPN)** y elimine el cortafuegos anterior.

STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Devices (Dispositivos)** y elimine el cortafuegos anterior.

STEP 3 | Compile los cambios realizados en Panorama.

STEP 4 | (Solo implementaciones HA) Envíe los cambios a todos los hubs y a los demás peers de HA (excepto al cortafuegos antiguo que debe reemplazarse). Antes de continuar, asegúrese de que la confirmación se realiza correctamente tanto en hubs como en cortafuegos

independientes. Si la búsqueda del antiguo número de serie del cortafuegos no devuelve ninguna configuración de puerta de enlace, puede omitir este paso.

STEP 5 | Configurar un cortafuegos de reemplazo de RMA.

STEP 6 | (Solo implementaciones HA) Establezca una conexión HA entre el cortafuegos de reemplazo y el cortafuegos independiente. Se designa como activo el cortafuegos que tiene el valor numérico más bajo y, por lo tanto, la prioridad más alta. Para evitar que su cortafuegos de reemplazo asuma la función de un par de HA activo, asegúrese de que no se le asigne una prioridad de dispositivo más alta.

STEP 7 | Seleccione **Panorama** > **SD-WAN** > **Devices (Dispositivos)** y añada el nuevo cortafuegos de sucursal.

STEP 8 | Seleccione **Panorama** > **SD-WAN** > **VPN Clusters (Clústeres VPN)** y añada el nuevo cortafuegos de sucursal.

STEP 9 | Compile los cambios realizados en Panorama.

STEP 10 | Seleccione **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)** y envíe toda la configuración gestionada de Panorama a los hubs y a ambos pares de HA en la sucursal.

*Al **Push to Devices (Enviar a dispositivos)**, Panorama intenta empujar los cambios a todos los dispositivos del clúster tanto para implementaciones de HA como de hub-and-spoke. Para evitar enviar los cambios a todos los dispositivos, seleccione **Edit Selections (Editar selecciones)** en el Ámbito de envío y deshabilite todos los demás dispositivos en dispositivos **Device Groups (Grupos de dispositivos)** y **Templates (Plantillas)**.*

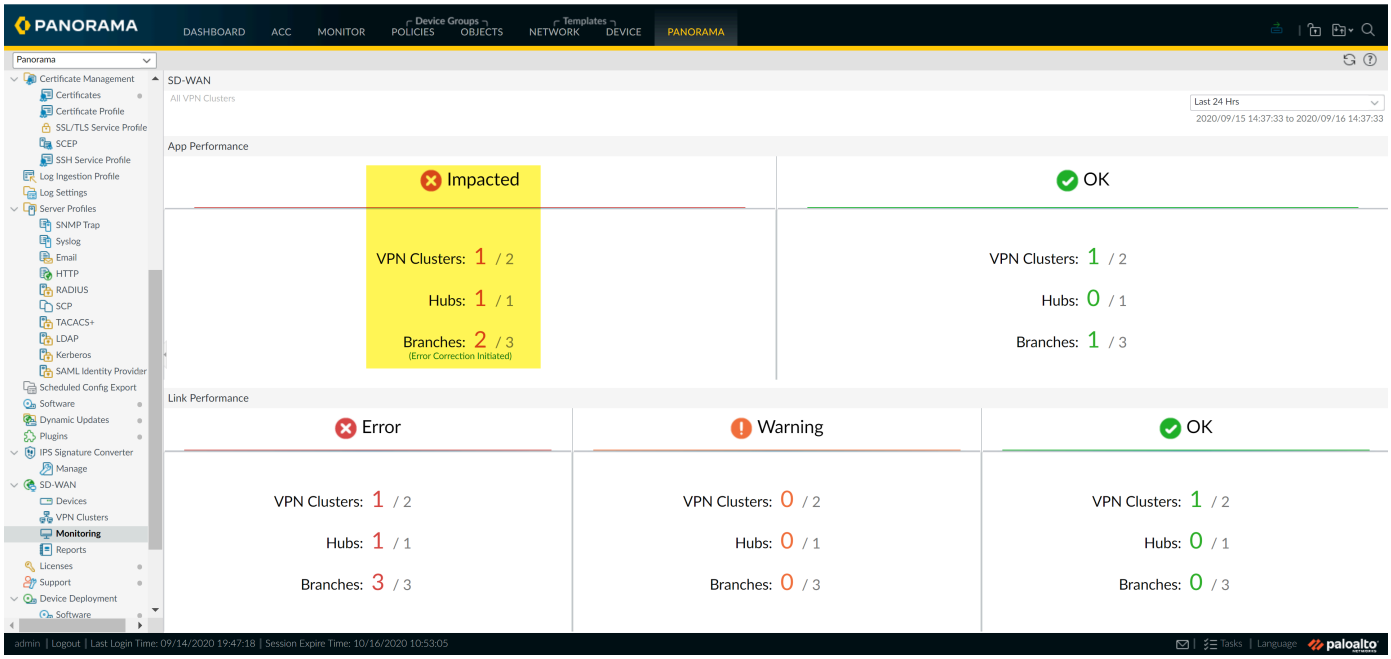
- *En implementaciones hub-and-spoke, seleccione los cortafuegos de hub y la pila de plantillas HA del sistema de sucursales al que desea enviar la configuración. Como resultado, los sitios que no se seleccionan podrían no estar sincronizados.*
- *En implementaciones de malla completa, es obligatorio enviar los cambios a todos los dispositivos del clúster.*

Solución de problemas del rendimiento de la aplicación

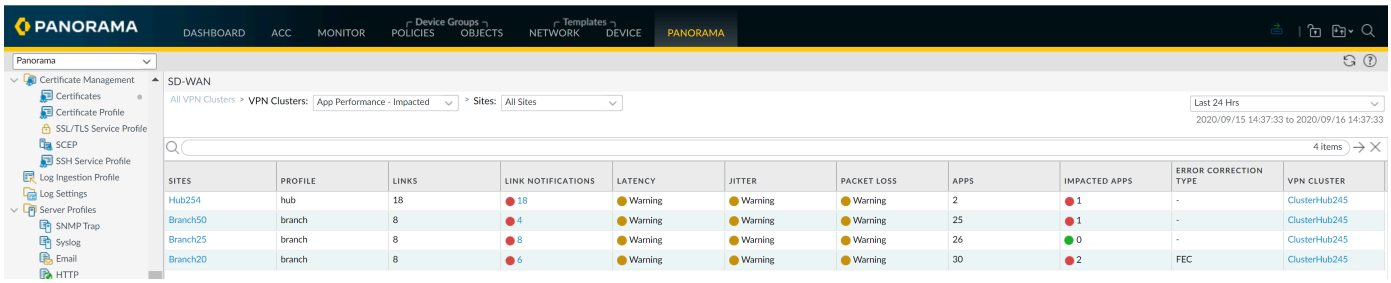
Comprender qué está provocando un rendimiento degradado para sus aplicaciones y servicios es esencial para garantizar que la experiencia del usuario no se vea afectada. Entender por qué sus clústeres de VPN se ven afectados y el motivo por el que se produjo un error en el tráfico de la aplicación en diferentes enlaces ayuda a ajustar su configuración de SD-WAN.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

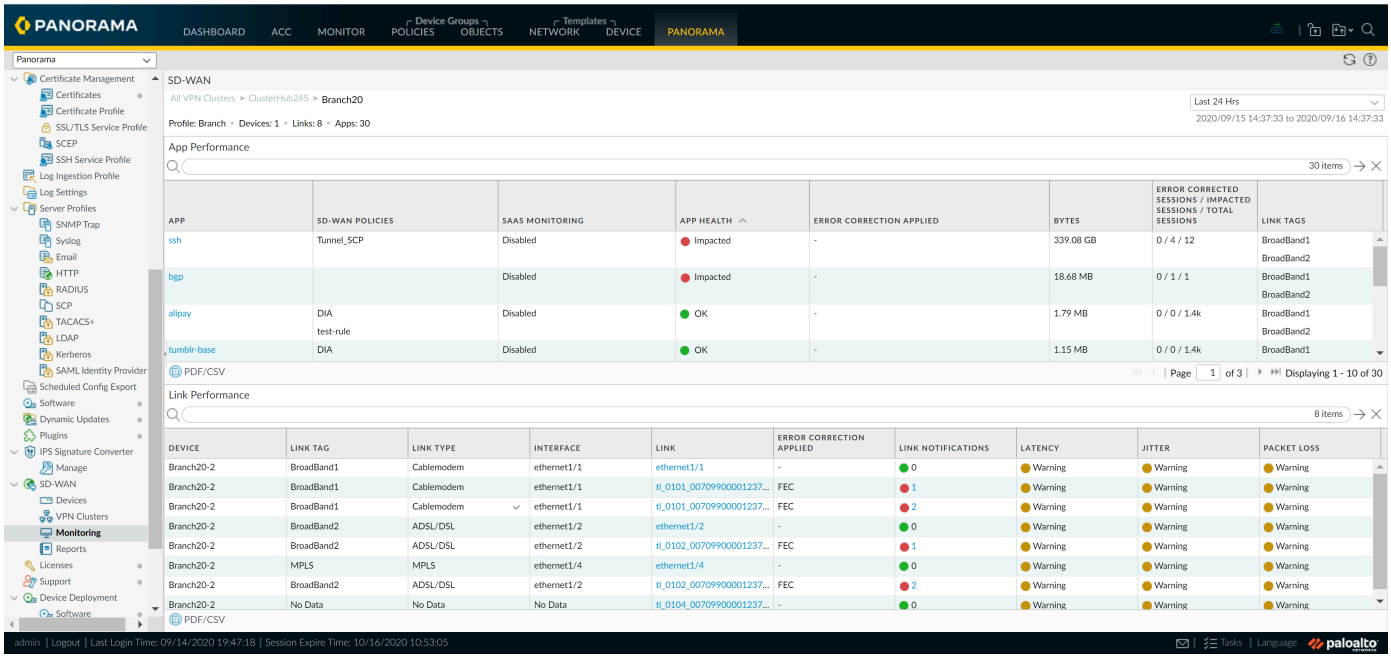
STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Supervisión** y vea los clústeres de VPN **impactados**.



STEP 3 | Filtre los clústeres de VPN según su métrica preferida en menú desplegable **Sitio** y seleccione el periodo. En este ejemplo, estamos viendo **todos los sitios** que contienen clústeres de VPN afectados en las últimas 12 horas.

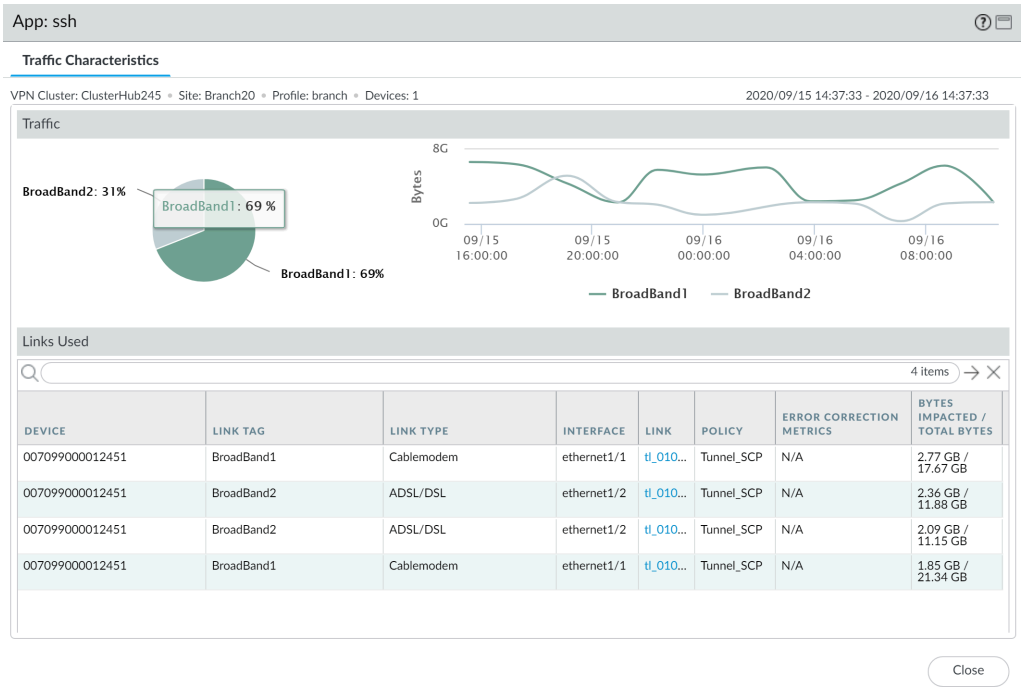


STEP 4 | En la columna Sitios, seleccione el cortafuegos de la central o la sucursal impactados para ver las aplicaciones afectadas y el rendimiento del enlace correspondiente.



STEP 5 | En la sección Rendimiento de la aplicación, haga clic en una aplicación para ver información detallada sobre las características del tráfico sobre el tráfico de la aplicación, como los servicios de Internet y los enlaces utilizados:

- Revise el gráfico circular para comprender el desglose del tráfico de aplicaciones en sus servicios de Internet.
- Revise el gráfico de líneas para comprender cuántos bytes de datos se transfirieron a través de cada servicio de Internet a lo largo del tiempo.
- Revise la sección Enlaces utilizados para comprender qué enlaces usó el tráfico de la aplicación y cuántos bytes se vieron afectados del total de bytes en el periodo seleccionado.

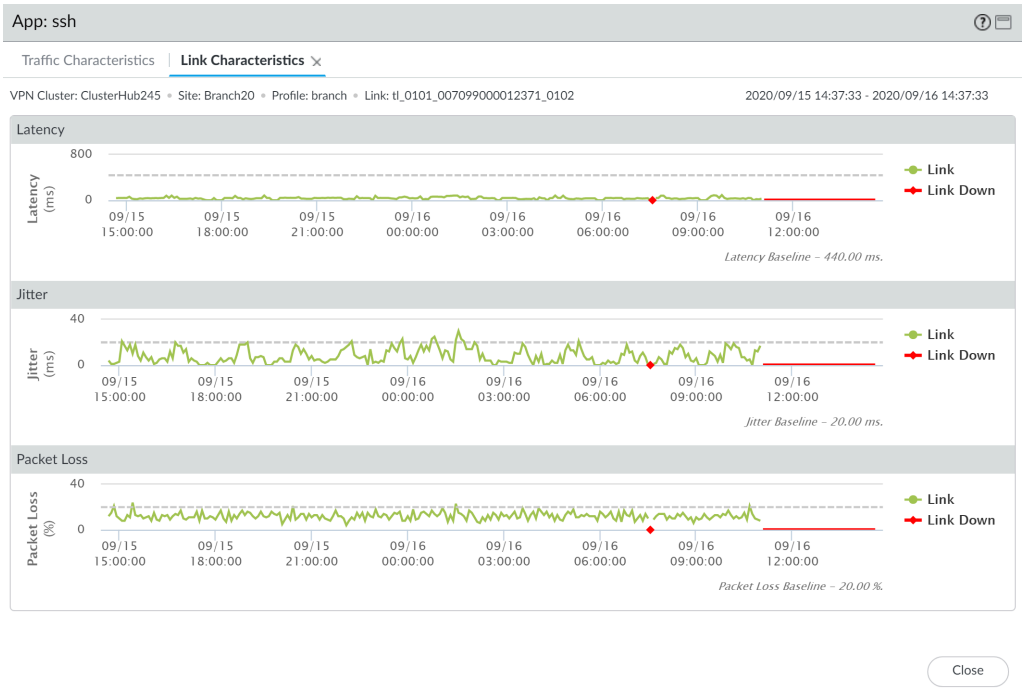


STEP 6 | Investigue qué métrica de estado provocó que la aplicación intercambiara enlaces.

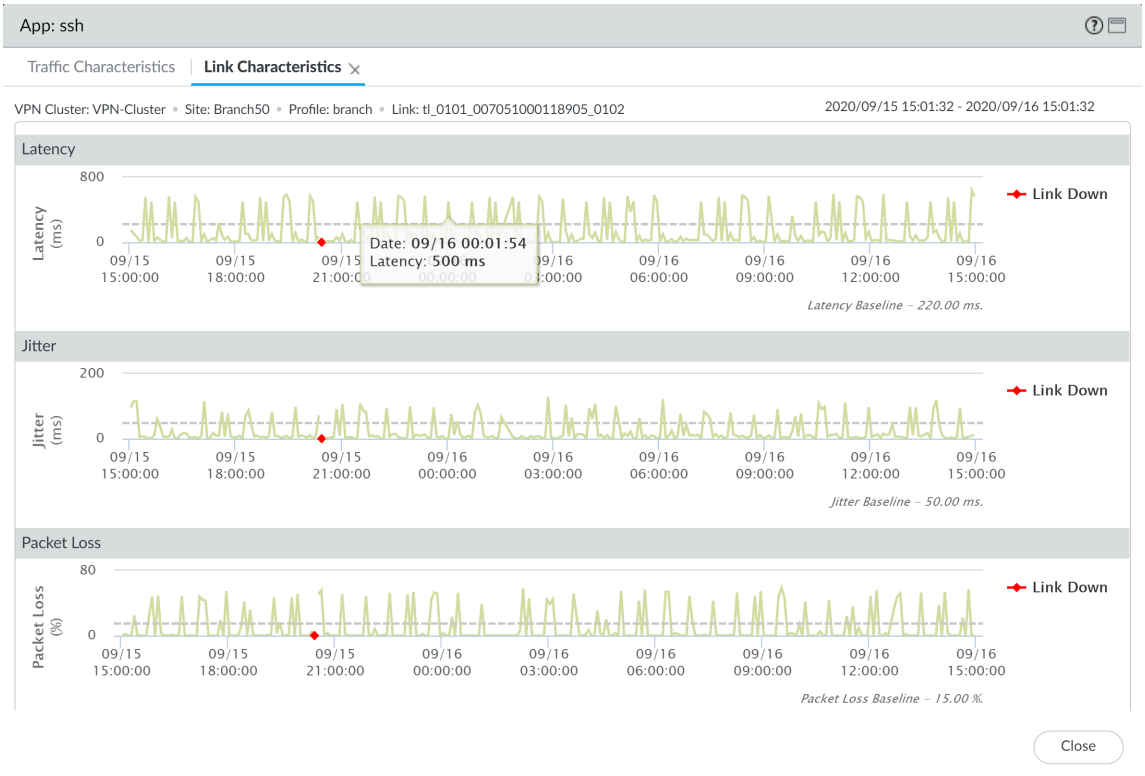
La línea de puntos indica la media de siete días para la métrica de estado.

1. En la sección Enlaces utilizados de la pestaña Características del tráfico, haga clic en un enlace de Ethernet para ver las características detalladas del enlace (latencia, vibración

y pérdida de paquetes) durante el periodo especificado en el paso 2 para investigar qué métrica de estado provocó que la aplicación intercambiara enlaces.



2. En la pestaña **Traffic Characteristics (Características del tráfico)**, seleccione otro enlace para ver las características del enlace de la aplicación secundaria para comprender mejor el motivo del impacto del clúster de la VPN.



STEP 7 | Después de identificar el motivo por el que se ve afectado el tráfico de la aplicación, tenga en cuenta lo siguiente para resolver el problema:

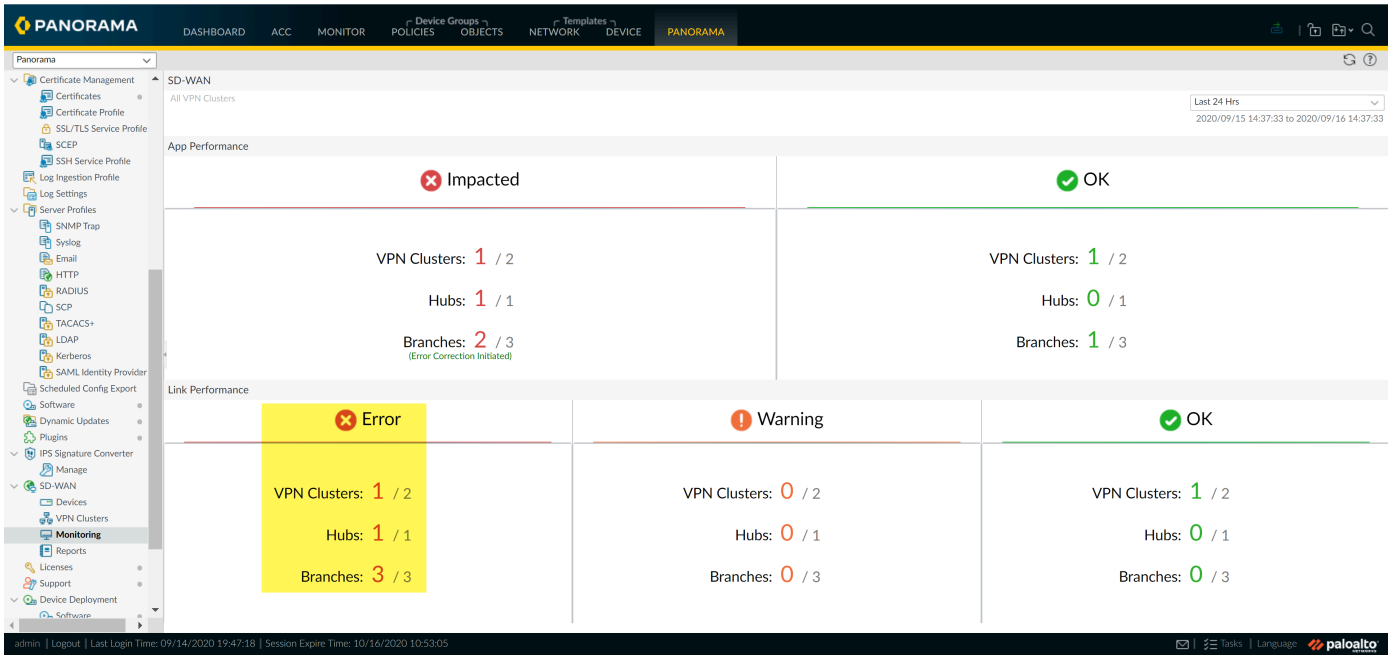
- Considere añadir enlaces adicionales al perfil de distribución de tráfico. Cuando se añaden enlaces adicionales para que se realice la conmutación por error del tráfico de la aplicación, ayuda a garantizar que el tráfico de la aplicación y la experiencia del usuario no se vean afectados por enlaces con un estado degradado.
- Vuelva a configurar los umbrales de estado en su perfil de calidad de ruta. Puede que los umbrales de estado sean demasiado estrictos, lo que provocará una conmutación por error innecesaria del enlace. Por ejemplo, si tiene una aplicación que puede experimentar una pérdida de paquetes de hasta el 18 % antes de que la experiencia del usuario se vea afectada, contar con un umbral de pérdida de paquetes del 10 % generaría una conmutación por error de la aplicación a un enlace diferente sin que sea necesario.
- Consulte con su proveedor de servicios de Internet (ISP) para determinar si hay impactos en su red fuera de su control que puedan resolver.

Solución de problemas del rendimiento del enlace

Comprender lo que está causando un rendimiento del enlace degradado es fundamental para garantizar que la experiencia de usuario al usar aplicaciones y servicios no se vea afectada. Comprender por qué sus clústeres de VPN tienen enlaces afectados ayuda a ajustar su configuración de SD-WAN para garantizar que las experiencias del usuario al usar aplicaciones y servicios no se vean afectadas por enlaces con problemas de estado.

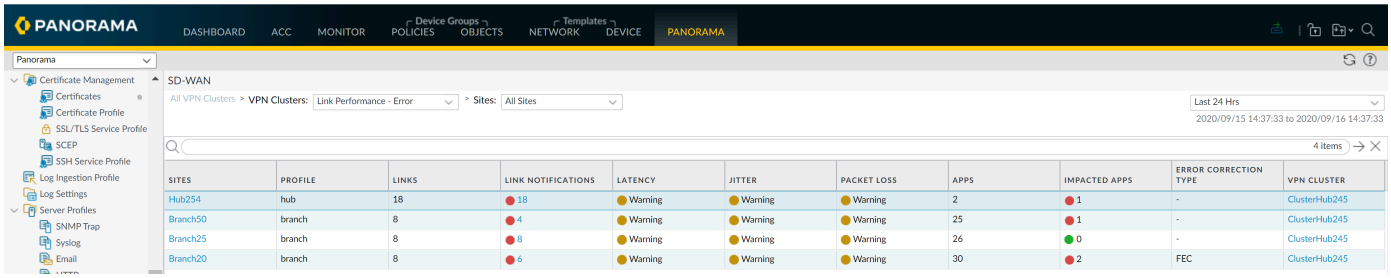
STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Supervisión** y vea los clústeres de VPN **impactados**.

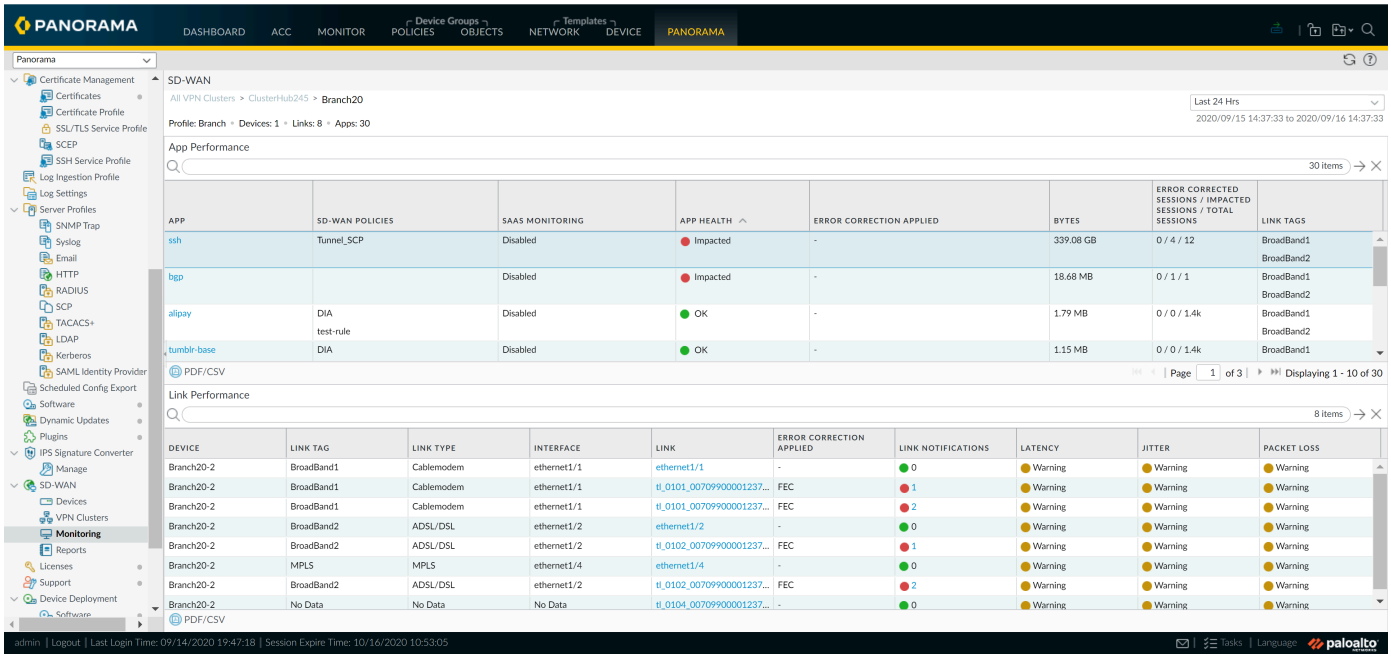


STEP 3 | Filtre los clústeres de VPN según su métrica preferida en menú desplegable **Sitio** y seleccione el periodo. En la columna Sitios, seleccione el cortafuegos de la central o la sucursal impactados para ver las aplicaciones afectadas y el rendimiento del enlace correspondiente.

En este ejemplo, estamos viendo **todos los sitios** que contienen clústeres de VPN afectados en las últimas 24 horas.

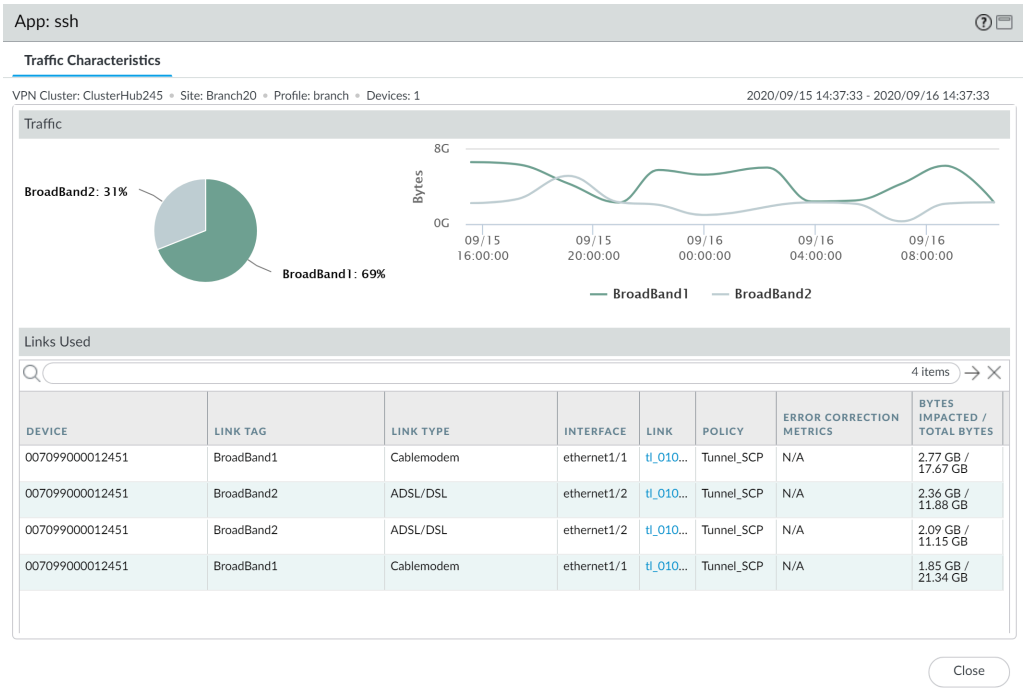


STEP 4 | En la columna Sitios, seleccione el cortafuegos de la central o la sucursal impactados para ver las aplicaciones afectadas y el rendimiento del enlace correspondiente.



STEP 5 | En la sección Rendimiento de la aplicación, haga clic en una aplicación para ver información detallada sobre las características del tráfico sobre el tráfico de la aplicación, como los servicios de Internet y los enlaces utilizados:

- Revise el gráfico circular para comprender el desglose del tráfico de aplicaciones en sus servicios de Internet.
- Revise el gráfico de líneas para comprender cuántos bytes de datos se transfirieron a través de cada servicio de Internet a lo largo del tiempo.
- Revise la sección Enlaces utilizados para comprender qué enlaces usó el tráfico de la aplicación y cuántos bytes se vieron afectados del total de bytes en el periodo seleccionado.

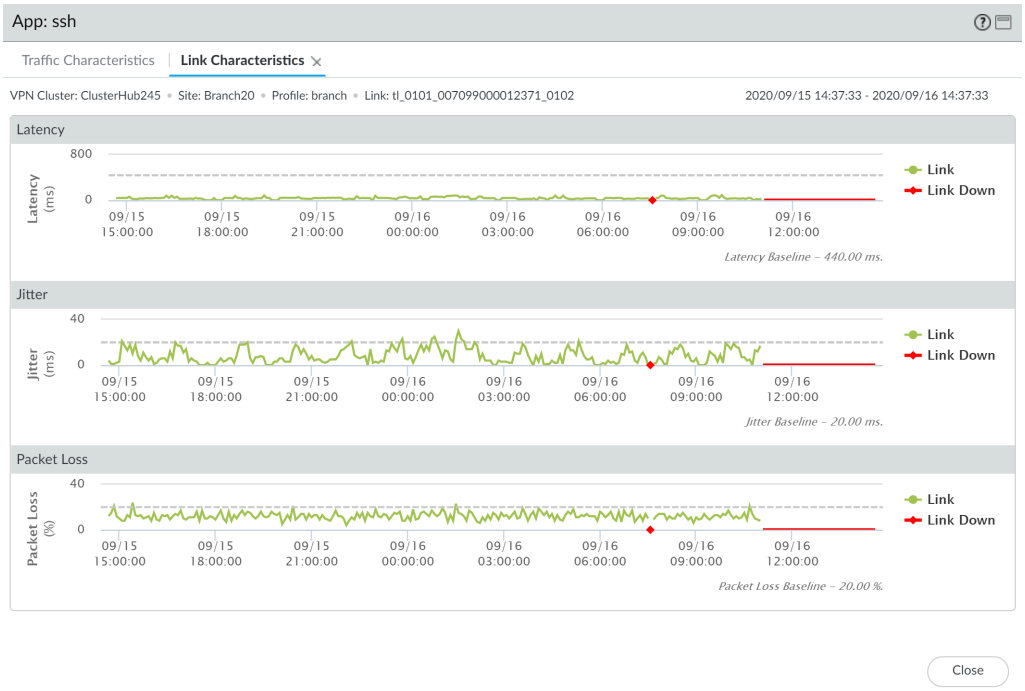


STEP 6 | Investigue qué métrica de estado provocó que la aplicación intercambiara enlaces.

La línea punteada indica el umbral que configura cuando Creación de un perfil de calidad de ruta.

1. En la sección Enlaces utilizados de la pestaña Características del tráfico, haga clic en un enlace de Ethernet para ver las características detalladas del enlace (latencia, vibración y pérdida de paquetes) durante el periodo especificado en el paso 2 para investigar qué métrica de estado provocó que la aplicación intercambiara enlaces. En este ejemplo utilizamos ethernet 1/1 y podemos observar que el porcentaje de paquetes perdidos regularmente superó el umbral configurado en el perfil de calidad de la ruta para la

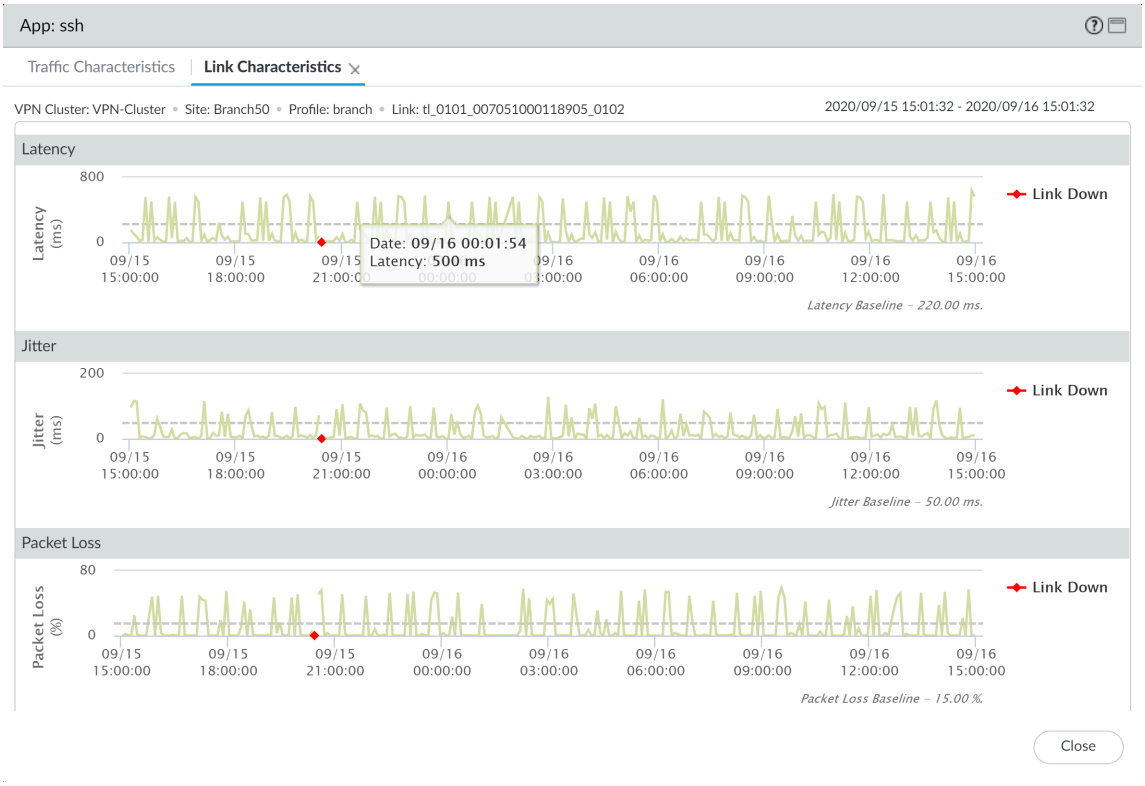
aplicación. Podemos concluir que esa es la razón por la que se produjo la conmutación por error del tráfico de la aplicación al siguiente mejor enlace.



2. En la pestaña **Características del tráfico**, seleccione otro enlace para ver las características del enlace. En este ejemplo, utilizamos ethernet 1/4 y podemos observar que después de que se produjera la conmutación por error del tráfico de la aplicación, ethernet 1/4 experimentó una vibración para la aplicación que superó el umbral

configurado. Esto obligó al tráfico de la aplicación a realizar una conmutación por error a ethernet 1/1.

Puesto que ambos enlaces tenían métricas de estado que se superaron, el tráfico de la aplicación no tenía un enlace con un buen estado para realizar una conmutación por error, lo que provocó que el clúster de la VPN se viera afectado.



STEP 7 | Después de identificar el motivo por el que se ve afectado el tráfico de la aplicación, tenga en cuenta lo siguiente para resolver el problema:

- Considere añadir enlaces adicionales al perfil de distribución de tráfico. Cuando se añaden enlaces adicionales para que se realice la conmutación por error del tráfico de la aplicación, ayuda a garantizar que el tráfico de la aplicación y la experiencia del usuario no se vean afectados por enlaces con un estado degradado.
- Vuelva a configurar los umbrales de estado en su perfil de calidad de ruta. Puede que los umbrales de estado sean demasiado estrictos, lo que provocará una conmutación por error innecesaria del enlace. Por ejemplo, si tiene una aplicación que puede experimentar una pérdida de paquetes de hasta el 18 % antes de que la experiencia del usuario se vea afectada, contar con un umbral de pérdida de paquetes del 10 % generaría una conmutación por error de la aplicación a un enlace diferente sin que sea necesario.
- Consulte con su proveedor de servicios de Internet (ISP) para determinar si hay impactos en su red fuera de su control que puedan resolver.

Actualización de cortafuegos de SD-WAN

Revise las notas de la versión del complemento de Panorama para SD-WAN 2.1 y, a continuación, utilice el siguiente procedimiento para actualizar su Panorama y los cortafuegos SD-WAN gestionados.

STEP 1 | Instale las actualizaciones de contenido y software de Panorama.

STEP 2 | Actualice sus recopiladores de logs gestionados.

- Actualización de recopiladores de logs cuando Panorama está conectado a Internet.
- Actualización de recopiladores de logs cuando Panorama no está conectado a Internet.

STEP 3 | Actualice los cortafuegos de central de SD-WAN.

*Debe actualizar sus cortafuegos de central de PAN-OS 10.0.0 a PAN-OS 10.0.1 o a una versión posterior antes de actualizar sus cortafuegos de sucursales. La actualización de los cortafuegos de sucursales antes que los cortafuegos de central puede provocar datos de supervisión incorrectos (**Panorama** > **SD-WAN** > **Monitoring** **[Supervisión]**) y los enlaces de SD-WAN se muestran erróneamente como down (inactivo).*

- Actualización de los cortafuegos cuando Panorama está conectado a Internet.
- Actualización de los cortafuegos cuando Panorama no está conectado a Internet.

STEP 4 | Actualice los cortafuegos de sucursal de SD-WAN.

- Actualización de los cortafuegos cuando Panorama está conectado a Internet.
- Actualización de los cortafuegos cuando Panorama no está conectado a Internet.

Instalar el complemento de SD-WAN.

Instalar la versión del complemento de SD-WAN en su servidor de gestión Panorama™ y cortafuegos con SD-WAN.

Consulte la Matriz de compatibilidad de complementos de Panorama de Palo Alto Networks y revise la versión mínima requerida de PAN-OS para la versión del complemento SD-WAN de destino. Consulte actualizar el complemento SD-WAN con la versión PAN-OS compatible para actualizar el servidor de gestión de Panorama y los cortafuegos de Palo Alto Networks que son compatibles con la versión del complemento SD-WAN.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Instalar la versión del complemento SD-WAN en Panorama.

Si Panorama tiene una configuración de alta disponibilidad (HA, High Availability), repita este pasos en el peer de HA de Panorama.

1. Seleccione **Panorama** > **Plugins (Complementos)** y **Check Now (Comprobar ahora)** para buscar la versión del complemento **`sd_wan`** más reciente.
2. **Descargue** e **instale** la última versión del complemento de SD-WAN.
3. Después de instalar correctamente el complemento de SD-WAN, seleccione **Confirmar** y **Confirmar en Panorama**.

   Este paso es necesario para poder confirmar cualquier cambio de configuración en Panorama.

STEP 3 | Después de que la nueva versión del complemento se instale correctamente, vea el **Dashboard (Panel)** de Panorama y en el widget de Información general verifique que el `complemento SD-WAN` muestre la versión del complemento SD-WAN que ha instalado.

Desinstalación del complemento de SD-WAN

Para desinstalar el complemento de SD-WAN del servidor de gestión Panorama correctamente, debe eliminar la configuración del complemento de SD-WAN de Panorama.

STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Elimine cualquier regla de la política de seguridad que permita que BGP se ejecute entre sus centrales y sucursales de SD-WAN.

1. Seleccione **Panorama** > **SD-WAN** > **Dispositivos** > **Política de BGP** y **elimine** las reglas de la política de seguridad.
2. Haga clic en **Aceptar** para guardar los cambios.

STEP 3 | Seleccione **Panorama** > **Complementos** y seleccione **Eliminar configuración** para el complemento de SD-WAN.

STEP 4 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** a sus cortafuegos de gestión.

STEP 5 | **Desinstale** el complemento de SD-WAN.

Haga clic en **Aceptar** cuando se le solicite continuar con la desinstalación del complemento de SD-WAN.

