Guía del administrador de SD-WAN

1.0

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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

July 2, 2020

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
- Elementos de configuración de SD-WAN
- Planificación de la configuración de SD-WAN

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.

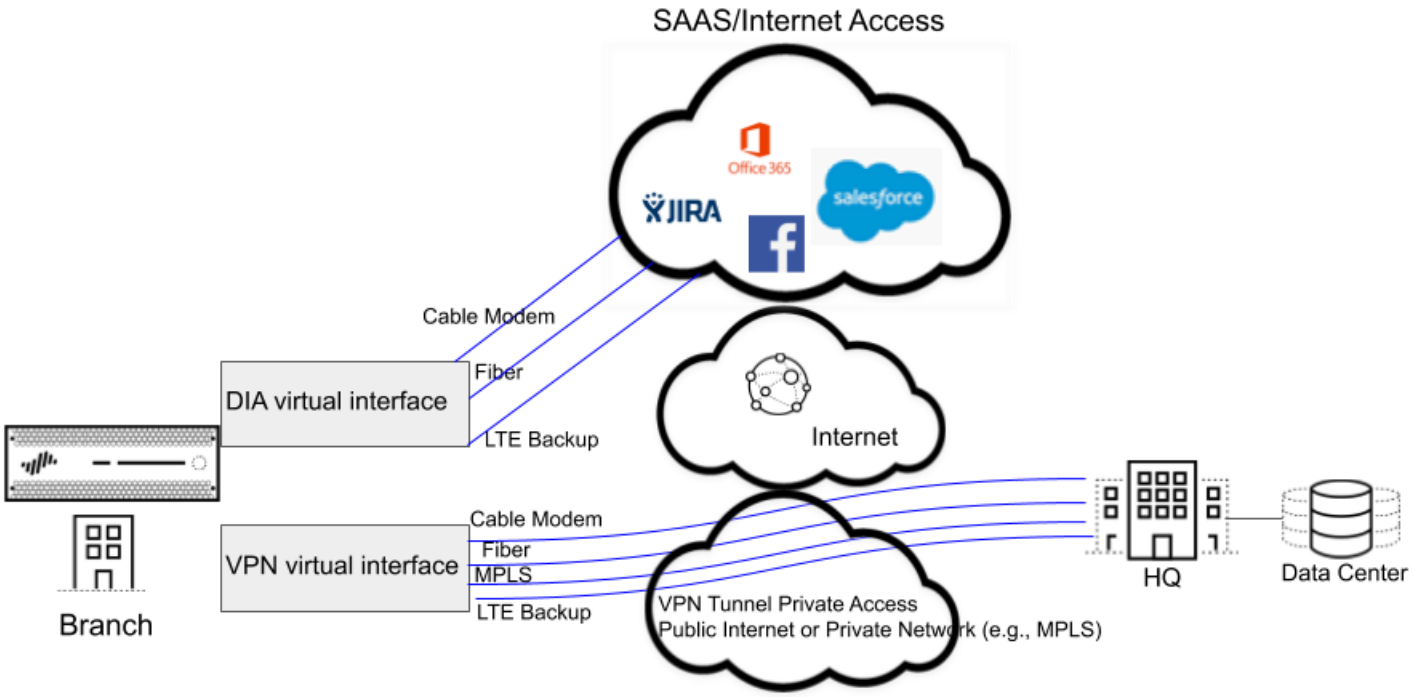
- Seguridad de PAN-OS con funcionalidad SD-WAN
- Compatibilidad del enlace de SD-WAN y el cortafuegos
- Gestión centralizada

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 (decodificador 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 a la central 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 central en el tráfico de Internet. El cortafuegos de la sucursal ya se encarga de la seguridad, por lo que no necesita el cortafuegos de la central 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 una central. 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 centrales específicas en una región.

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

- PA-220
- PA-220R
- PA-820
- PA-850
- Serie PA-3200
- Serie PA-5200
- VM-300

- VM-500
- VM-700

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.

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 automática de VPN permite que Panorama configure sucursales y centrales con conexiones IKE/IPSec seguras. Un clúster de VPN define las centrales 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 una central 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.

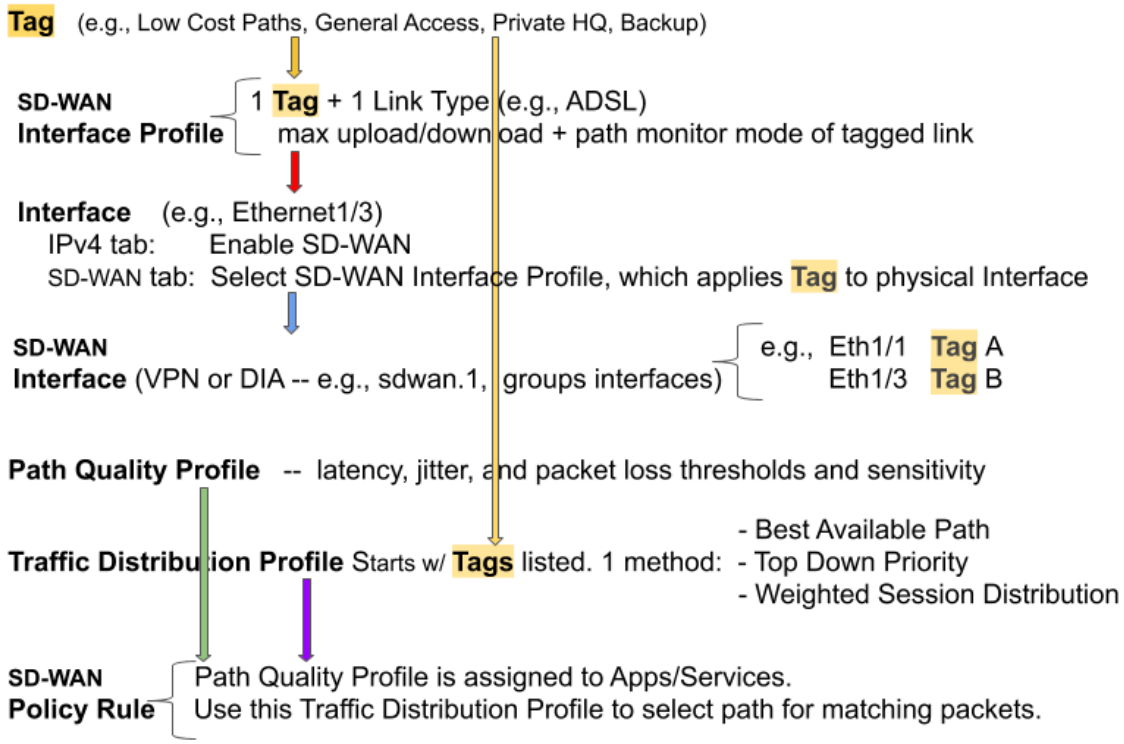
Comience por comprender su caso de uso de SD-WAN, luego revise los elementos de configuración de SD-WAN y los métodos de distribución de tráfico y, después, planifique su configuración de SD-WAN. Para acelerar en gran medida la configuración, la práctica recomendada es exportar un CSV de dispositivo 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 las centrales y sucursales de SD-WAN y para aprovisionar automáticamente túneles VPN entre las centrales 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 la central o con la central y otras sucursales.

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 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.

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. 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.

- 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
- Configuración de una interfaz de SD-WAN virtual
- Creación de una ruta predeterminada a la interfaz de SD-WAN
- Creación de un perfil de calidad de ruta
- Perfiles de distribución del tráfico de SD-WAN
- Creación de un perfil de distribución de tráfico
- Configuración de una regla de políticas de SD-WAN
- (PAN-OS 9.1.2 y versiones 9.1 posteriores)Permiso para realizar la conmutación por error del tráfico de acceso a Internet directo en el enlace de MPLS
- Distribución de sesiones no coincidentes
- Adición de dispositivos de SD-WAN a Panorama
- (Opcional) Configuración de dispositivos de HA para SD-WAN
- Creación de un clúster de VPN
- (Opcional) Creación de una ruta estática 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 | Continúe con Configuración de Panorama y cortafuegos para SD-WAN para comenzar a configurar su 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 | Continúe con Configuración de Panorama y cortafuegos para SD-WAN para comenzar a configurar su 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 de la central 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.

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 disposnibilidad (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.

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 central**: para el tráfico que sale de los cortafuegos de la sucursal a los de la central y para el tráfico entre cortafuegos de la central.
- **Zona a sucursal**: para el tráfico que sale de los cortafuegos de la central 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.

Si no crea las zonas predefinidas, el complemento de SD-WAN creará automáticamente las zonas predefinidas en la sucursal y el cortafuegos de la central, 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** > **Dispositivos** y añada zonas existentes a **Zona a Internet**, **Zona a central** , **Zona a sucursal** y **Zona a interno**).

  El resultado de la asignación es que un cortafuegos de sucursal o central 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 central`** 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 su implementación de SD-WAN, para ambos casos de uso, tendrá que crear las zonas predefinidas necesarias en Panorama denominadas **`Zona a Internet`**, **`Zona a interno`**, **`Zona a central`** y **`Zona a sucursal`**. Cuando incorpore los cortafuegos de su sucursal y central, 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 centrales 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.

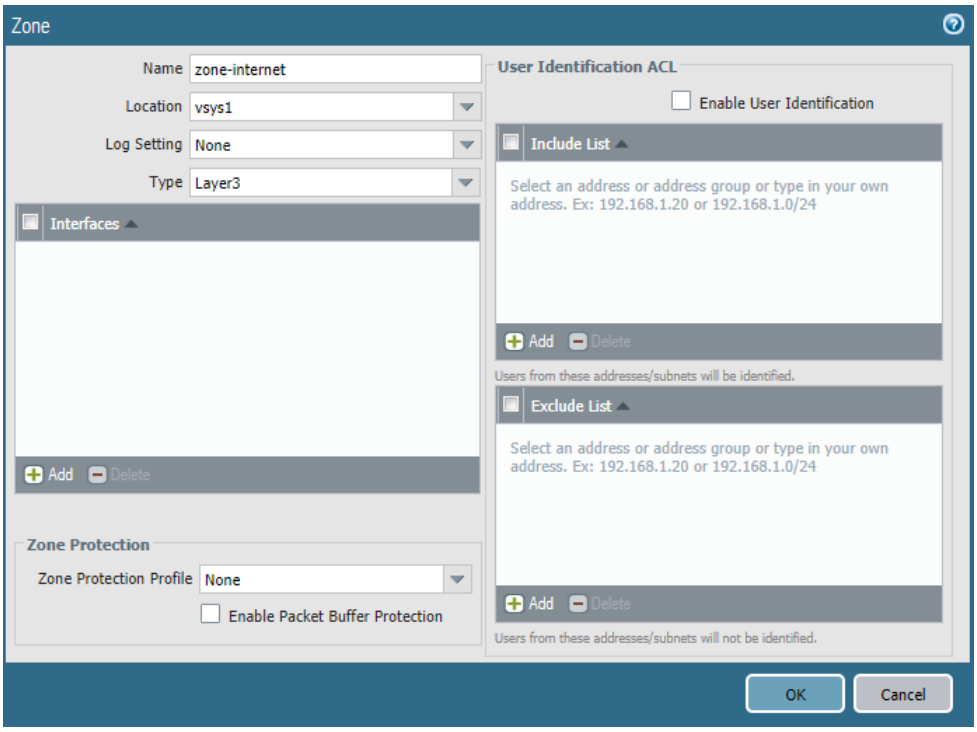
STEP 2 | Seleccione **Red** > **Zonas** y el cuadro desplegable contextual **Plantilla**, elija la plantilla de red creada anteriormente.

STEP 3 | **Añada** una nueva zona.

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

STEP 5 | Para el **tipo de zona**, seleccione **Capa 3**.

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 central`**
- **`Zona a interno`**
- **`Zona a Internet`**

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.

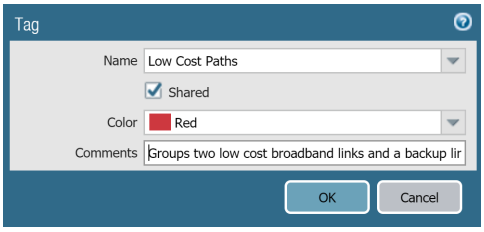
STEP 4 | Introduzca un nombre descriptivo en **Nombre** para la etiqueta. Por ejemplo; Rutas de bajo coste, Rutas costosas, Acceso general, Sede privada o Respaldo.

STEP 5 | Marque **Compartido** para que la etiqueta de enlace esté disponible para todos los grupos de dispositivos en el servidor de gestión Panorama ™ y para todos los sistemas virtuales (vsys) en cualquier central o sucursal servicios virtuales múltiples a los que realice 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 **tipo de enlace** físico de la lista predefinida (**ADSL/DSL**, **Cable modem** , **Ethernet**, **Fibra**, **LTE/3G/4G/5G**, **MPLS**, **Microwave/Radio (Microondas/radio)**, **Satélite**, **WiFi** u **Otros**). 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 tipos de enlaces privados de punto a punto (MPLS, satélite, microondas y otros) 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.

STEP 9 | (PAN-OS 9.1.2 y versiones 9.1 posteriores) **Compatibilidad del túnel de datos VPN** determina si el tráfico de la sucursal a la central 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 deshabilitar **Compatibilidad del túnel de datos VPN** para tipos de enlaces privados como MPLS, satélite o microondas que no tienen capacidad de conexión a Internet. Sin embargo, primero debe asegurarse de que el tráfico no pueda interceptarse, porque se enviará fuera del túnel VPN.
- La sucursal puede tener tráfico de DIA que precise la conmutación por error en el enlace MPLS privado que se conecta a la central y que tenga que llegar a Internet desde la central. 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 10 | 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). 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 | 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). 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 12 | (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.

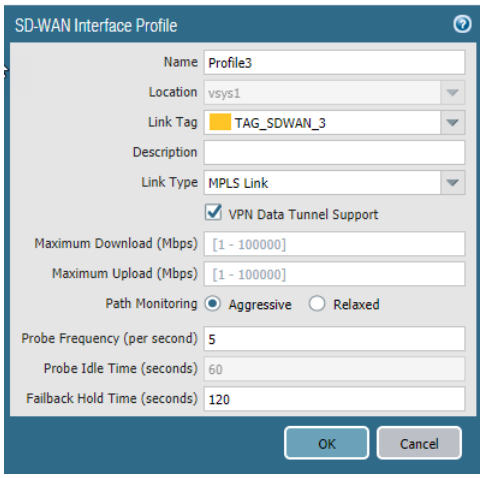
STEP 13 | Configure la **frecuencia de sonda (por segundo)** , que es la cantidad de veces por segundo que el cortafuegos envía un paquete de sonda al extremo opuesto del enlace de SD-WAN (el intervalo es de 1 a 5; el valor predeterminado es 5). La configuración predeterminada proporciona detección subsecundaria 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 14 | 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 15 | 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 16 | Haga clic en **OK (Aceptar)** para guardar el perfil.



STEP 17 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

STEP 18 | 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 y la puerta de enlace de siguiente salto y, a continuación, asignar un perfil de la interfaz de SD-WAN a la interfaz.

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

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

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

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

STEP 4 | Seleccione un **enrutador virtual** o cree uno nuevo.

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

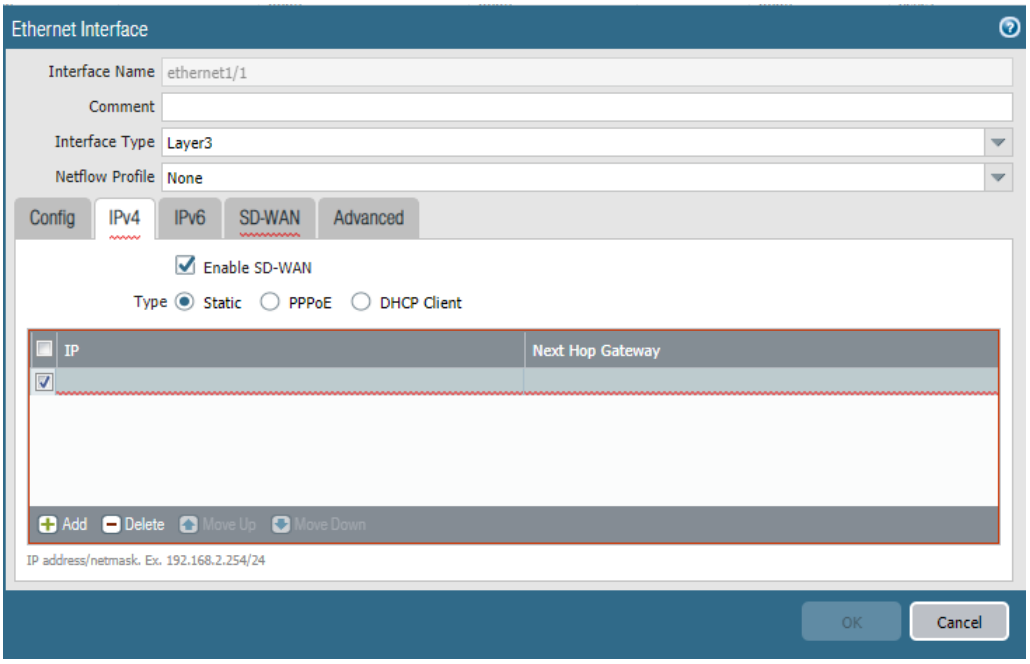
Por ejemplo, si crea un enlace de subida en un ISP, debe saber que la interfaz Ethernet que elija se va a dirigir a una zona no fiable.

STEP 6 | En la pestaña **IPv4**, seleccione la opción **Habilitar SD-WAN** .

STEP 7 | Seleccione el tipo de dirección en **Tipo** :

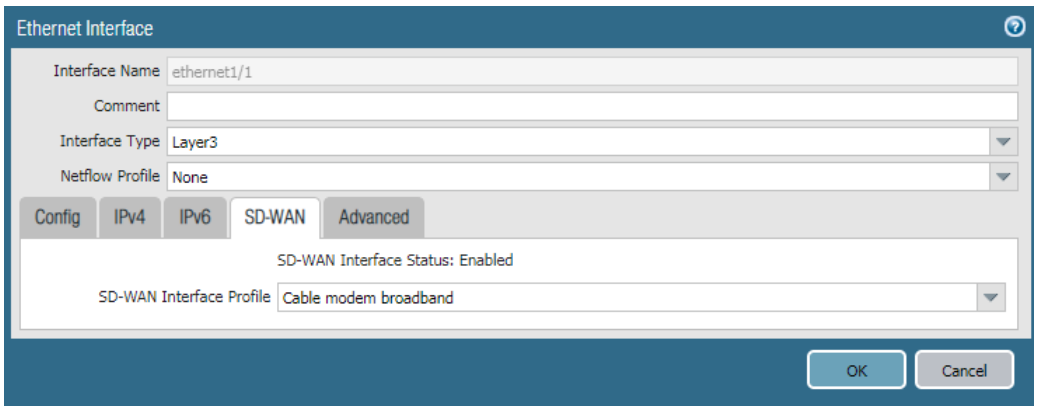
- **Estática**: en el campo **IP**, **añada** una dirección IPv4 y una longitud de prefijo para la interfaz. Puede usar una variable definida, como $uplink, con un intervalo de direcciones. Especifique la dirección IPv4 de **Puerta de enlace de siguiente salto** (el siguiente salto de la dirección IPv4 que acaba de especificar). 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 a la central.
- (PAN-OS 9.1.2 y versiones 9.1 posteriores, y complemento de SD-WAN 1.0.2 y versiones 1.0 posteriores) **PPPoE**:**habilite** la autenticación de PPPoE para los enlaces DSL, especifique el **nombre de usuario** y la **contraseña** y **confírmela**.
- **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.

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 | 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 9 | Haga clic en **OK (Aceptar)** para guardar la interfaz de Ethernet.



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

STEP 11 | (Solo configuración manual de SD-WAN) Configuración de una interfaz de SD-WAN virtual. La configuración automática de la VPN realizará esta tarea si utiliza la VPN automática.

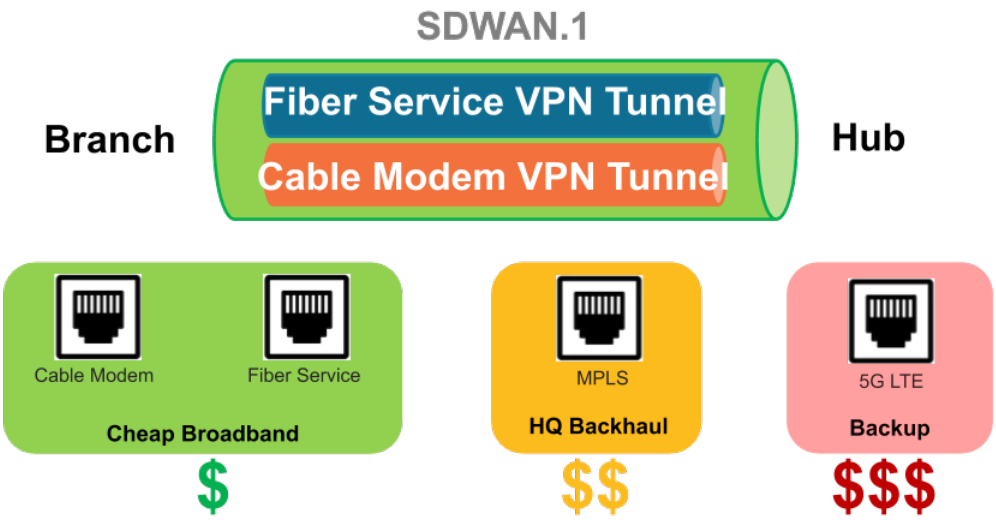
Configuración de una interfaz de SD-WAN virtual

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.

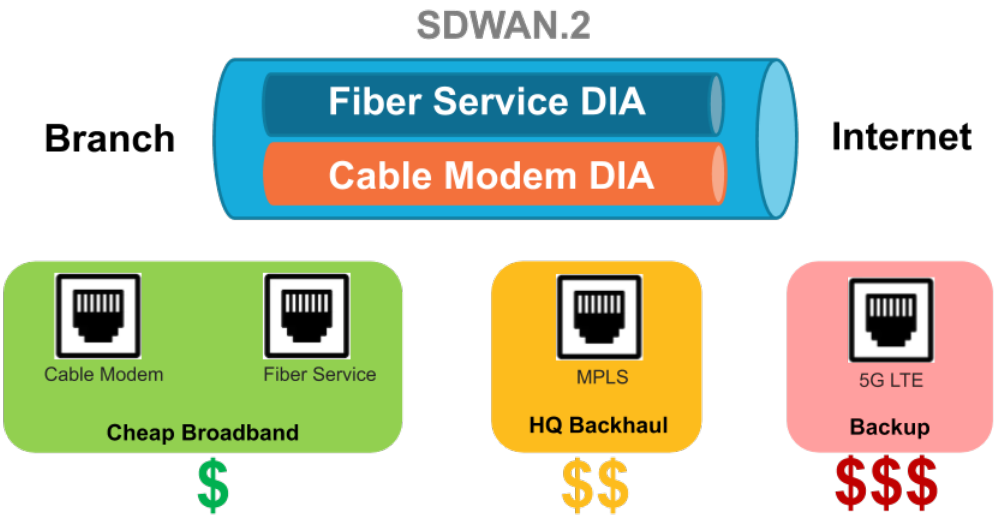
Si no utiliza la configuración de VPN automática a través de Panorama, cree y configure una interfaz de SD-WAN virtual para especificar una o más interfaces Ethernet físicas compatibles con SD-WAN que van al mismo destino, como a una central específica o a Internet. De hecho, todos los enlaces de una 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.1 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 la central.

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.2 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 **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 automática de la VPN crea interfaces de SD-WAN numeradas .901, .902, etc., así que no use esos números.

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

Añada un comentario útil, como ***`De sucursal a Internet`*** *o* ***`(De sucursal a central 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 | En la pestaña **Configuración**, asigne la interfaz de SD-WAN a un enrutador en **Enrutador virtual**.

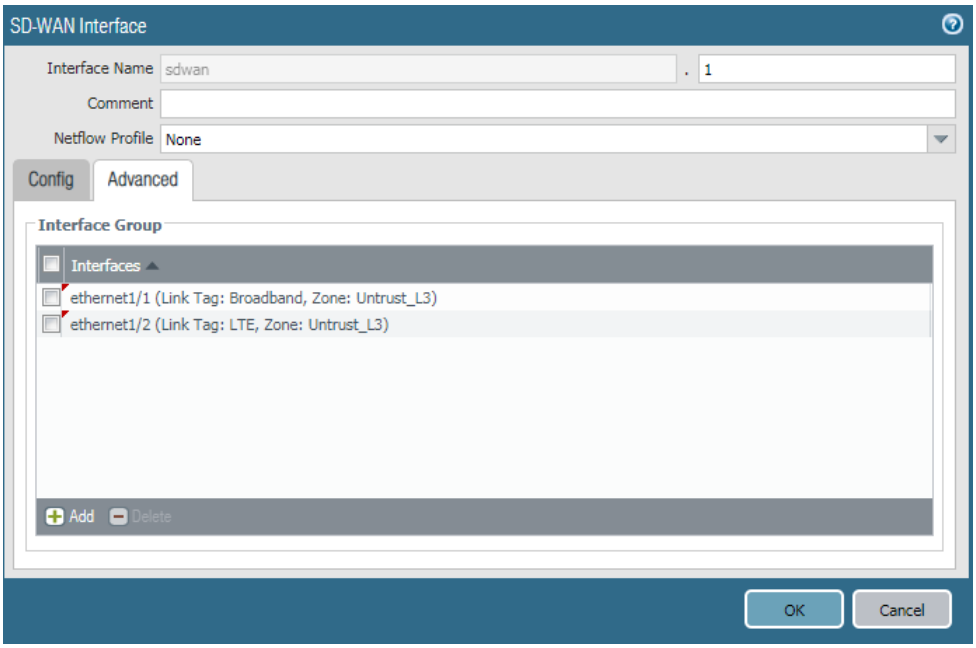
STEP 6 | Asigne la interfaz de SD-WAN a una zona segura en **Zona de seguridad**.

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 7 | 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 la central). 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 de la central 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 8 | Haga clic en **Aceptar** para guardar el cambio de configuración.



STEP 9 | 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 para acceder a Panorama, para abrir el cortafuegos debe crear una ruta predeterminada que apunte a una interfaz de SD-WAN que haya creado.

La VPN automática crea una interfaz de SD-WAN virtual denominada sdwan.901 para DIA y otra denominada sdwan.902 para túneles VPN. La VPN automática también crea su propia ruta predeterminada que usa la interfaz sdwan.901 como interfaz de salida y utiliza una métrica baja, por lo que la interfaz sdwan.901 es preferible 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 **Rutas estáticas** y **Añadir** para añadir una ruta estática por **nombre**.

STEP 5 | En **Destino**, especifique 0.0.0.0/0.

STEP 6 | En la **interfaz** de salida, seleccione una de las interfaces lógicas de SD-WAN que creó para abrir el cortafuegos, como sdwan.1.

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

STEP 7 | Para **Siguiente salto**, seleccione **Ninguno**.

STEP 8 | 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 9 | Haga clic en **OK (Aceptar)**.

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

STEP 11 | **Commit (Confirmar)** los cambios.

STEP 12 | Repita esta tarea para otras plantillas en cortafuegos que usen una ruta de servicio para acceder a Panorama™.

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 ruta 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.

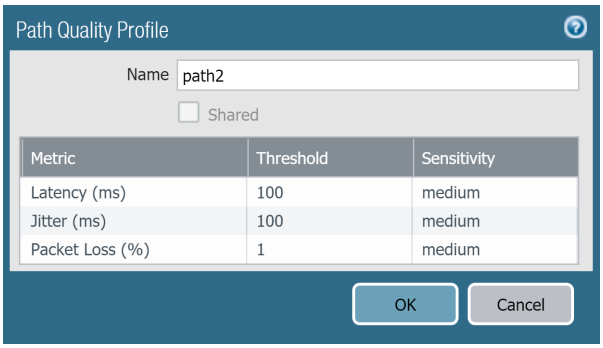
Consulte el perfil de calidad de ruta en una regla de políticas de SD-WAN para controlar el umbral en el que el cortafuegos reemplaza una ruta deteriorada por una nueva ruta para hacer coincidir los paquetes de aplicaciones.

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).

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 | Para **Pérdida de paquete**, seleccione **Sensibilidad** (**baja**, **media** o **alta**). El valor predeterminado es **medio**.

STEP 11 | Haga clic en **OK (Aceptar)**.

STEP 12 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

STEP 13 | **Commit (Confirmar)** los cambios.

STEP 14 | Repita esta tarea para cada grupo de dispositivos.

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 sean sensibles a la latencia y que requieran una gran parte de la capacidad de ancho de banda del enlace, como copias de seguridad de grandes sucursales y grandes transferencias de archivos.

Si el enlace experimenta una caída de tensión, el cortafuegos no redirige el tráfico correspondiente 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:

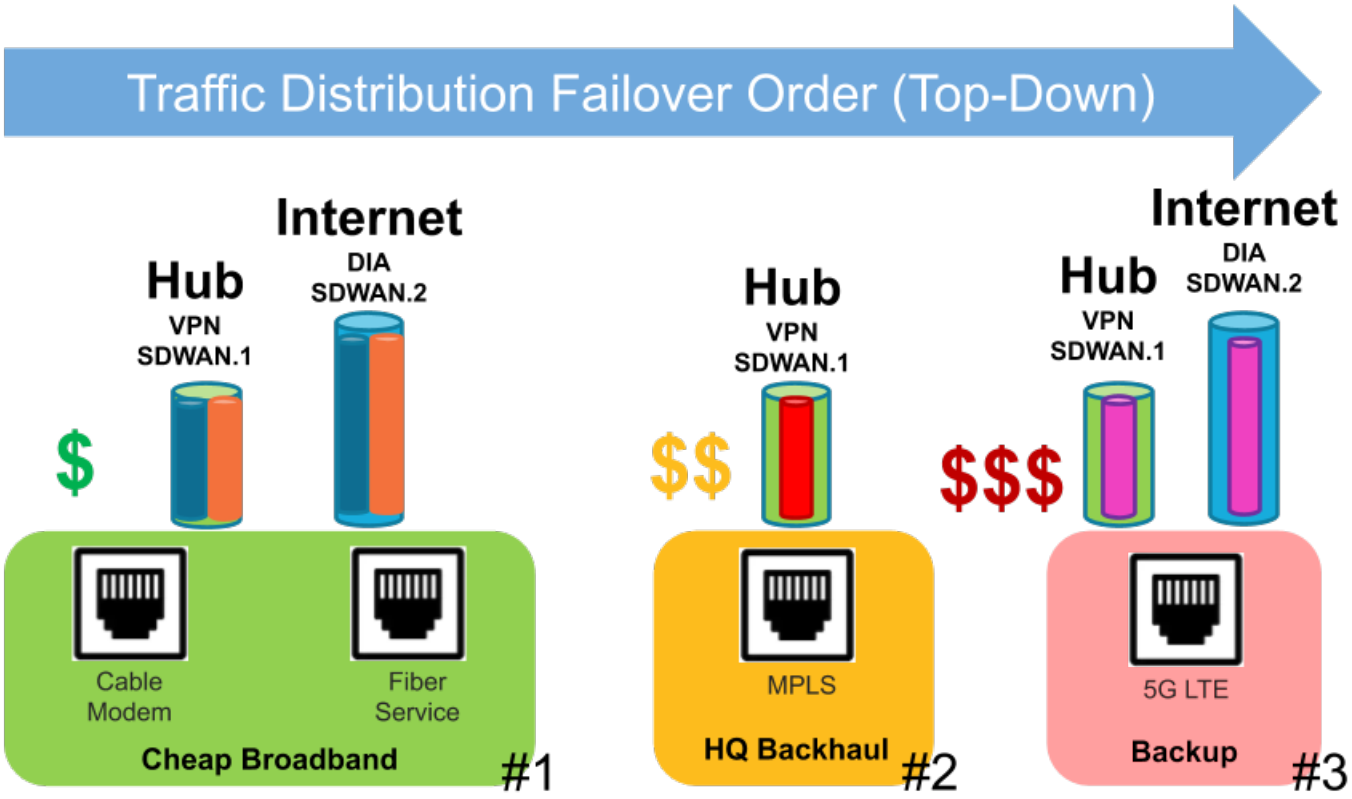
Condición de ruta	Prioridad de arriba hacia abajo	Mejor ruta disponible	Distribución de sesión ponderada
Se produce un error en la sesión de la ruta existente en un umbral de estado de ruta (caída de tensión).	Se realiza una conmutación por error de una sesión afectada a una mejor ruta (si está disponible).	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.
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;	Comparta la carga de la sesión en función de la mejor ruta desde todas	Comparta la carga de la sesión en función de la ponderación

Condición de ruta	Prioridad de arriba hacia abajo	Mejor ruta disponible	Distribución de sesión ponderada
	cargue primero los enlaces en la primera etiqueta de SD-WAN.	las etiquetas de SD-WAN.	(porcentaje) asignada a las etiquetas de SD-WAN.

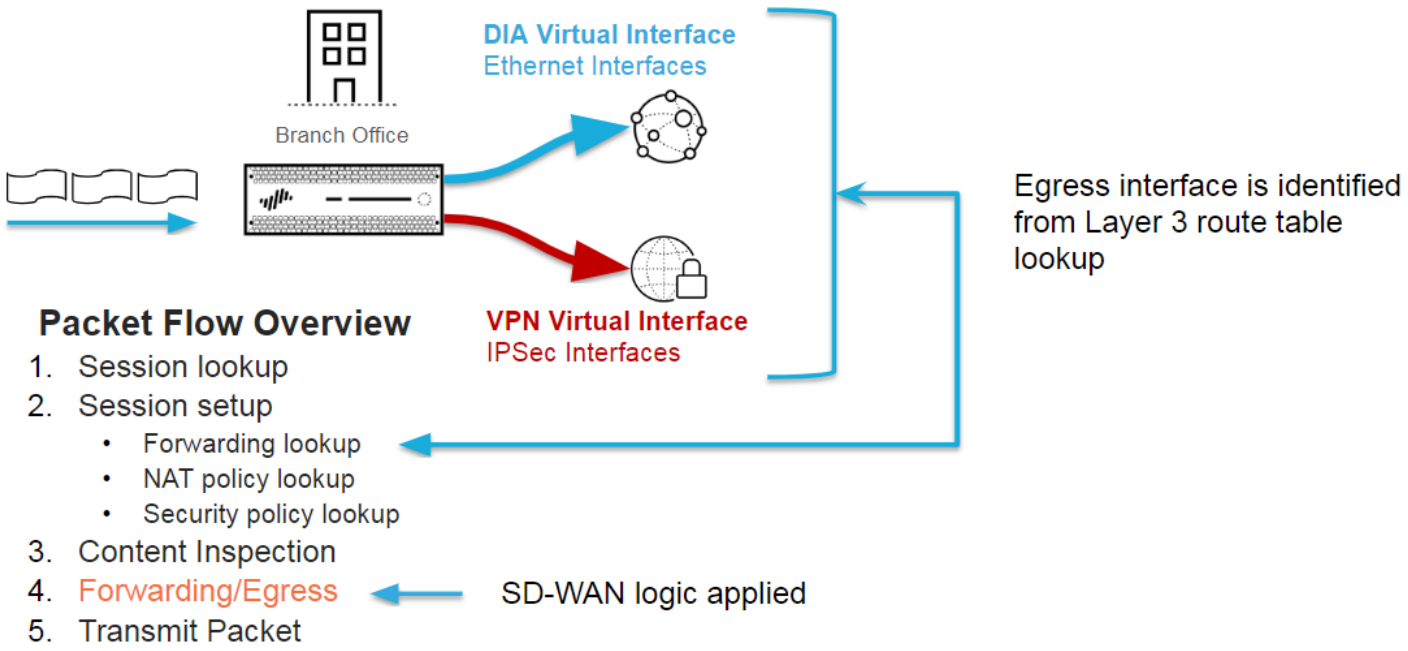
La siguiente figura muestra un ejemplo de un perfil de distribución de tráfico que utiliza el método Prioridad de arriba hacia abajo. Los n.° 1, n.° 2 y n.° 3 son el orden de las etiquetas de enlace de los enlaces que el cortafuegos examina, si es necesario, para detectar una ruta con buen estado para 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.1. 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.1 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.1 tiene dos interfaces miembro (dos portadores): 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.° 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.



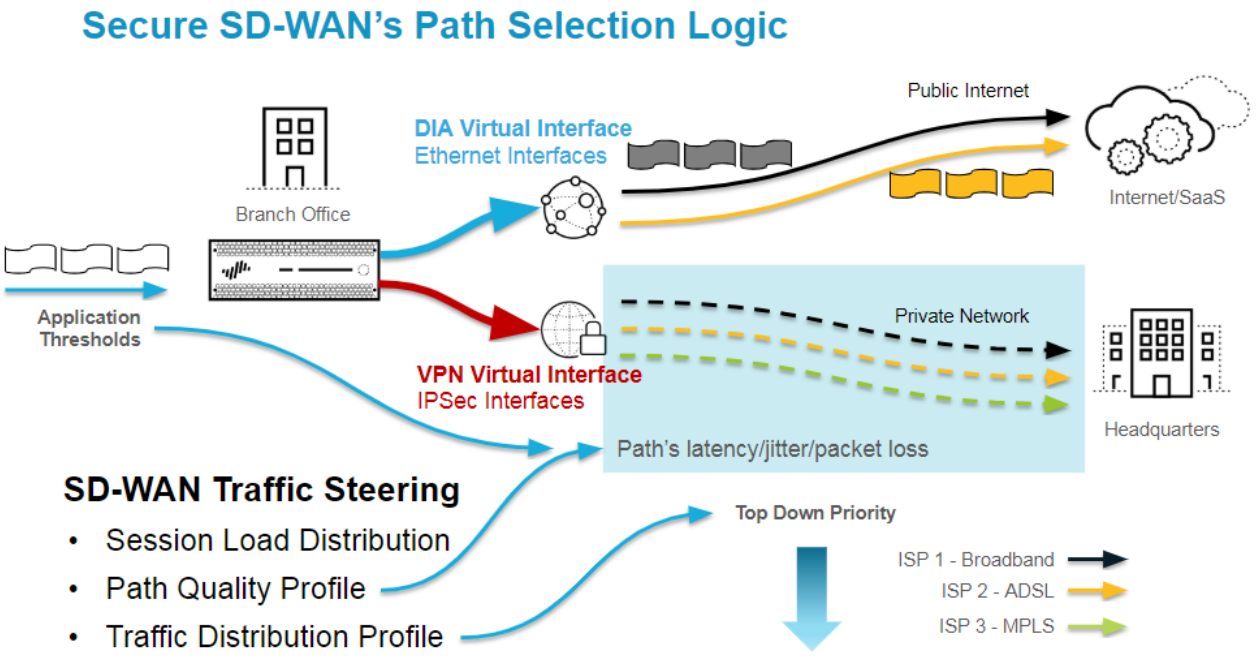
Los detalles del flujo de paquetes para la figura son los siguientes:

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.

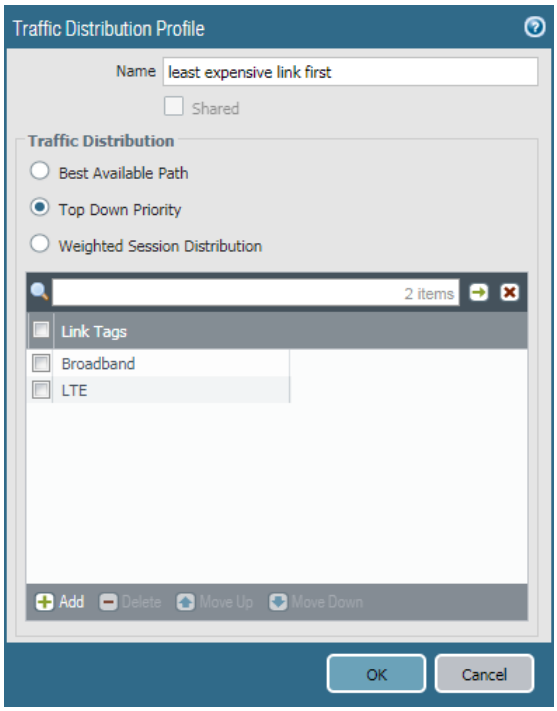
STEP 1 | Inicio de sesión en la interfaz web de Panorama.

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 se debe realizar una conmutación 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 exceda uno de los umbrales de calidad de ruta para esa ruta. En ese momento, el cortafuegos se inicia de nuevo en la parte superior de la lista Etiqueta de enlace para encontrar la nueva ruta preferida.
- **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.

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 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 **Aplicación/servicio**, seleccione un perfil de **Calidad de ruta** o Creación de un perfil de calidad de ruta.

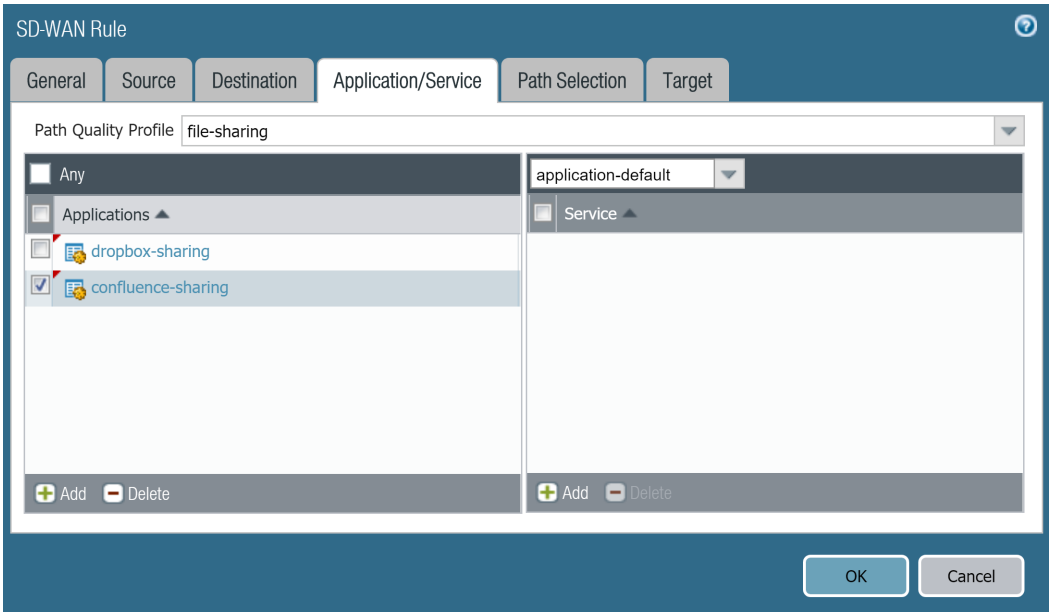
STEP 8 | **Añada aplicaciones** y seleccione una o más aplicaciones de la lista, o seleccione **cualquier** aplicación. Todas las aplicaciones que seleccione están sujetas a los umbrales de estado especificados en el perfil de Calidad de ruta seleccionado. Si un paquete coincide con una de

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.

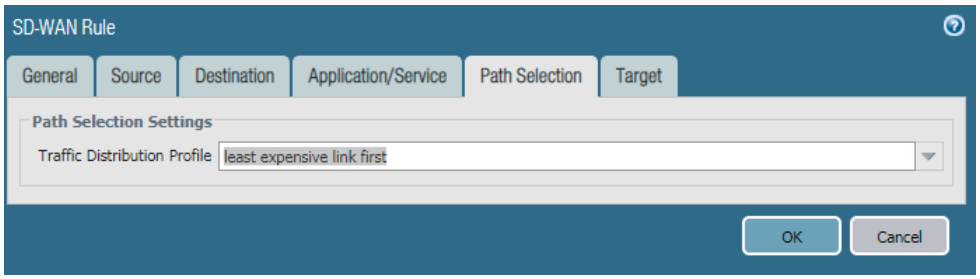
Añada solo aplicaciones críticas para el negocio y aplicaciones que sean sensibles a las condiciones de ruta para su capacidad de uso.

STEP 9 | **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.

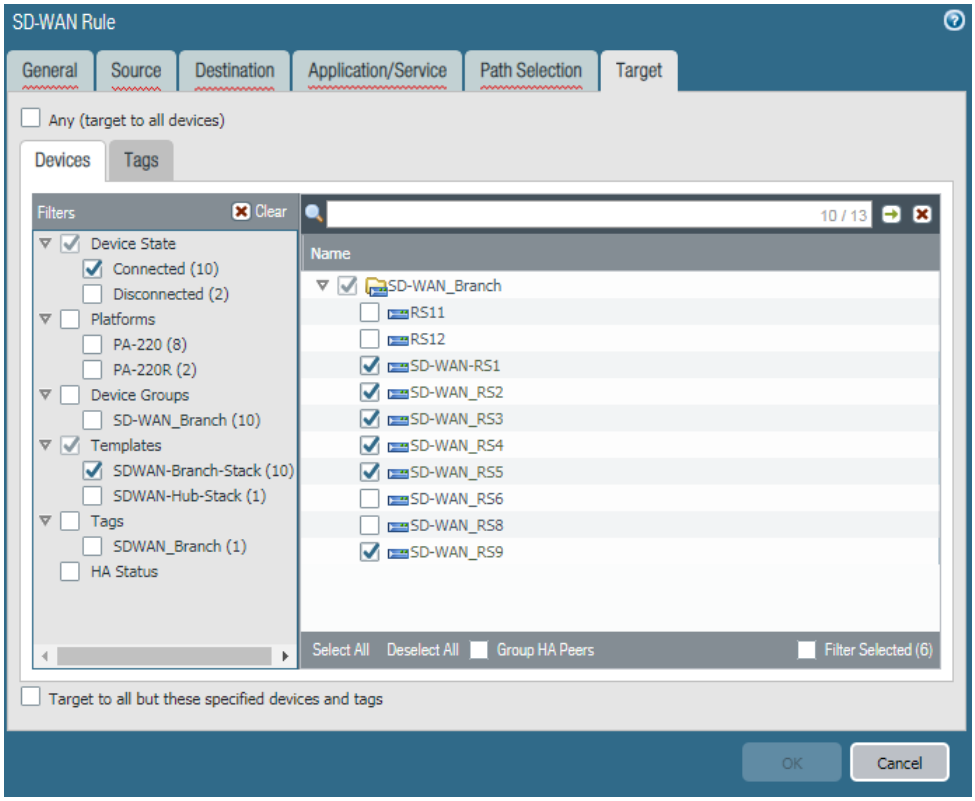


STEP 10 | En la pestaña **Selección de ruta**, elija el perfil **Distribución de tráfico** o Creación de un perfil de distribución de tráfico. Cuando un paquete entrante (no asociado a una sesión) coincide con todos los criterios de coincidencia de la regla, el cortafuegos usa este perfil de Traffic Distribution (Distribución de tráfico) para seleccionar una nueva ruta preferida.

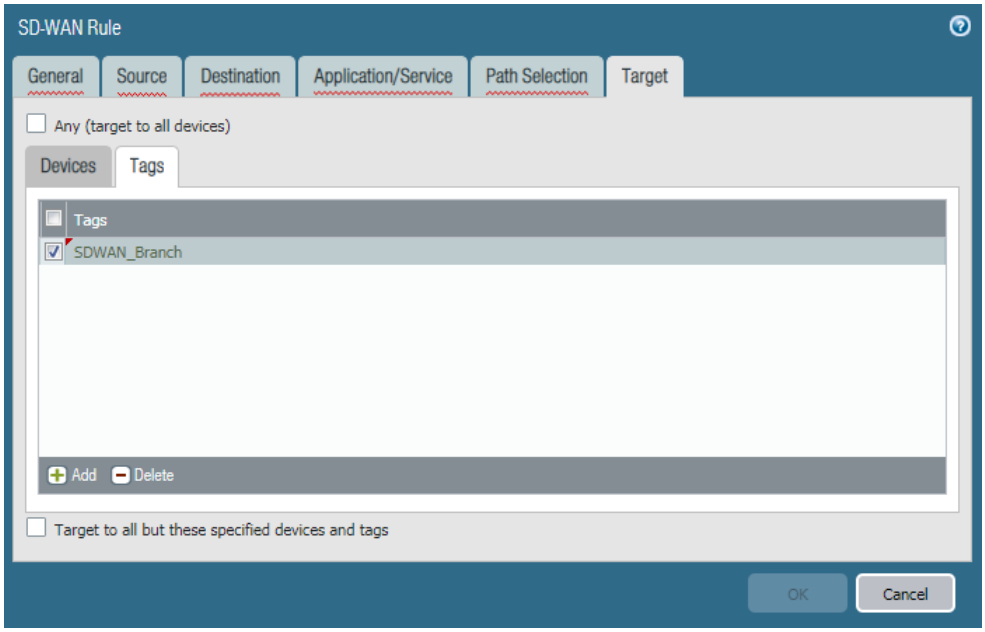


STEP 11 | En la pestaña **Destino**, use uno de los siguientes métodos para especificar los cortafuegos de destino en el grupo de dispositivos al que Panorama aplica la regla de políticas de SD-WAN:

- 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 **Dispositivos**, seleccione uno o más filtros para restringir las selecciones que aparecen en el campo Nombre; luego seleccione uno o más dispositivos en los que Panorama aplique la regla, como en este ejemplo:



- En la pestaña **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 12 | Haga clic en **OK (Aceptar)**.

STEP 13 | Seleccione las opciones**Confirmar** y **Confirmar y enviar** para aplicar esos cambios en su configuración.

STEP 14 | (Práctica recomendada) Cree una regla de políticas general de SD-WAN para 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 15 | 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 16 | (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 17 | 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 18 | 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 . A partir de PAN-OS 9.1.2, 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 | (PAN-OS 9.1.2 y versiones 9.1 posteriores) 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.

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 la central o sucursal de SD-WAN o utilice un CSV para realizar una importación masiva de varios cortafuegos de la central y sucursal de SD-WAN.

- Adición de un dispositivo de SD-WAN
- Importación masiva de varios dispositivos de SD-WAN

Adición de un dispositivo de SD-WAN

Agregue un cortafuegos de la central o sucursal de SD-WAN para que el servidor de gestión Panorama™ lo administre. Al añadir sus dispositivos, especifique qué tipo de dispositivo es (sucursal o central) 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 dispone de zonas preexistentes para sus cortafuegos de Palo Alto Networks®, tendrá que asignarlas a las zonas predefinidas utilizadas en SD-WAN.

Si desea que la HA activa/pasiva se ejecute en dos cortafuegos de sucursal o en dos cortafuegos de la central, 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 la política de seguridad para permitir BGP desde la zona interna a la zona central y desde la zona central a la zona interna. Si desea utilizar ASN de 4 bytes, primero debe habilitar los ASN de 4 bytes para el enrutador virtual.

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

STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Dispositivos** y **añada** un nuevo cortafuegos de 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.

- **Central**: 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 la central antes de continuar hacia la sucursal objetivo y conecta las sucursales con los recursos centralizados en la ubicación de la central. El dispositivo de la central 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 la central 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 | Seleccione el **nombre del enrutador virtual** para usar para el enrutamiento entre la central 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.

STEP 6 | 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. Los espacios no son compatibles en el nombre del sitio y provoca que no se muestre la supervisión de datos (Panorama > SD-WAN > Supervisión) para ese sitio.

STEP 7 | (PAN-OS 9.1.3 y versiones 9.1 posteriores y complemento de SD-WAN 1.0.3 y versiones 1.0 posteriores) Si añade una central detrás de un dispositivo que realiza NAT para la central, debe especifique la dirección IP o el FQDN de la interfaz pública en ese dispositivo de rendimiento NAT de subida, de modo que la configuración automática de VPN pueda usar esa dirección como el endpoint del túnel de la central. 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 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 volver a configurar la nueva dirección IP y enviarla a los miembros del 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 la central. También debe **`borrar la sesión de todo`** en el enrutador virtual donde configuró la política de NAT para las direcciones IP.*

STEP 8 | (Obligatorio para clientes preexistentes) Asigne sus zonas preexistentes a zonas predefinidas utilizadas para SD-WAN.

Cuando asigne sus zonas existentes a una zona de SD-WAN, debe modificar sus reglas de la política de seguridad y añadir las zonas de SD-WAN a las zonas de origen y destino correctas.

1. Seleccione **De Zona a Internet** y **añada** las zonas preexistentes que generarán el tráfico de salida de SD-WAN a Internet.
2. Seleccione **De Zona a central** y **añada** las zonas preexistentes que generarán el tráfico de salida de SD-WAN a la central.
3. Seleccione **De Zona a sucursal** y **añada** las zonas preexistentes que generarán el tráfico de salida de SD-WAN a la sucursal.
4. Seleccione **De Zona a interno** y **añada** las zonas preexistentes que generarán el tráfico de salida de SD-WAN a una zona interna.

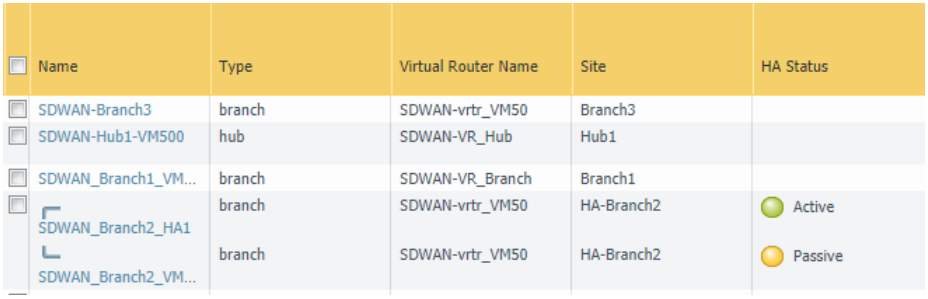
STEP 9 | (Opcional) Configure el enrutamiento del protocolo de puerta de enlace de borde (BGP).

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.

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. Especifique una **dirección de bucle invertido** IPv4 estática para el establecimiento de peers de BGP. La configuración automática de la VPN 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.
4. 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 de la central y la sucursal.
5. Especifique **Prefijo(s) que redistribuir**. En un dispositivo de central, debe introducir al menos un prefijo que redistribuir. Los dispositivos de sucursal no tienen esa opción. Las subredes conectadas a ubicaciones de sucursales se redistribuyen de manera predeterminada.

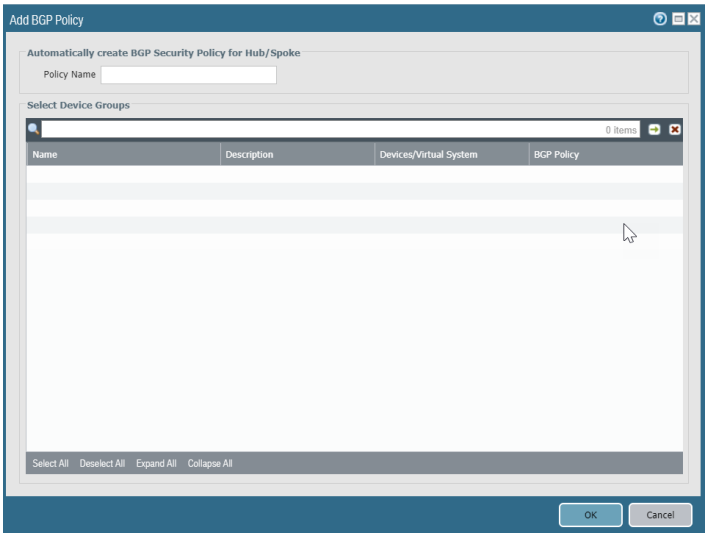
STEP 10 | Haga clic en **OK (Aceptar)**.

STEP 11 | (Complemento de SD-WAN 1.0.1 y versiones posteriores) Seleccione **Agrupar peers de HA** en la parte inferior de la pantalla para ver las sucursales (o centrales) que son peers de HA juntas.



STEP 12 | (PAN-OS 9.1.2 y versiones 9.1 posteriores y complemento de SD-WAN 1.0.2 y versiones 1.0 posteriores) 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 centrales.

1. Seleccione **Política de BGP** en la parte inferior de la pantalla y elija **Añadir** .
2. Especifique un **nombre de política** para la regla de la política de seguridad que creará Panorama automáticamente.
3. Elija **Seleccionar grupo de dispositivos** para especificar los grupos de dispositivos a los que Panorama envía la regla de la política de seguridad.
4. Haga clic en **OK (Aceptar)**.



STEP 13 | 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 central en lugar de agregar manualmente cada dispositivo de uno en uno. Al añadir sus dispositivos, especifique qué tipo de dispositivo es (sucursal o central) 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 la central, 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 la política de seguridad para permitir BGP desde la zona interna a la zona central y desde la zona central 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 central 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 la central y guarde el CSV. Todos los campos son obligatorios a no ser que se especifique lo contrario. Debe introducir lo siguiente para cada central y sucursal:

- **device-serial**: el número de serie del cortafuegos de la sucursal o la central.
- **type**: especifique si un dispositivo es una **`sucursal`** o una **`central`**.
- **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 provoca que no se muestre la supervisión de datos (Panorama > SD-WAN > Supervisión) para ese sitio.
- (Obligatorio para clientes preexistentes) Asigne sus zonas preexistentes a zonas predefinidas utilizadas para SD-WAN.

  Cuando asigne sus zonas existentes a una zona de SD-WAN, debe modificar sus reglas de la política de seguridad y añadir las zonas de SD-WAN a las zonas de origen y destino correctas.

  - **Zona a Internet**: especifique los nombres de las zonas preexistentes del tráfico de salida de SD-WAN para llegar a Internet.
  - **Zona a sucursal** : especifique los nombres de las zonas preexistentes del tráfico de salida de SD-WAN para llegar a una sucursal.
  - **Zona a central**: especifique los nombres de las zonas preexistentes del tráfico de salida de SD-WAN para llegar a una central.
  - **Zona a interno**: especifique los nombres de las zonas preexistentes del tráfico de salida de SD-WAN para llegar a una zona interna.
- (Opcional) **loopback-address**: especifique una dirección IPv4 de bucle invertido estático para la creación de peers del protocolo de puerta de enlace de borde (BGP).
- (Opcional) **prefix-redistribute**: especifique los prefijos de IP que según la sucursal puede alcanzar una central. 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 a la central.

  Palo Alto Networks no redistribuirá las rutas predeterminadas de la sucursal que aprenda del ISP.
- (Opcional) **as-number** : especifique el ASN del AS privado al que pertenece el enrutador virtual de la central o la sucursal. El complemento de SD-WAN admite solo sistemas autónomos privados. El ASN debe ser único para cada central 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.

- (Opcional) **router-id**: especifique el ID del enrutador de BGP, que debe ser único entre todos los enrutadores virtuales.

Especifique la dirección de bucle invertido como ID de enrutador.

- **Nombre de VR**: especifique el nombre del enrutador virtual que usar para el enrutamiento entre la central y las sucursales de SD-WAN. De forma predeterminada, Panorama crea un enrutador virtual `sdwan-default` y permite impulsar automáticamente las configuraciones del enrutador.

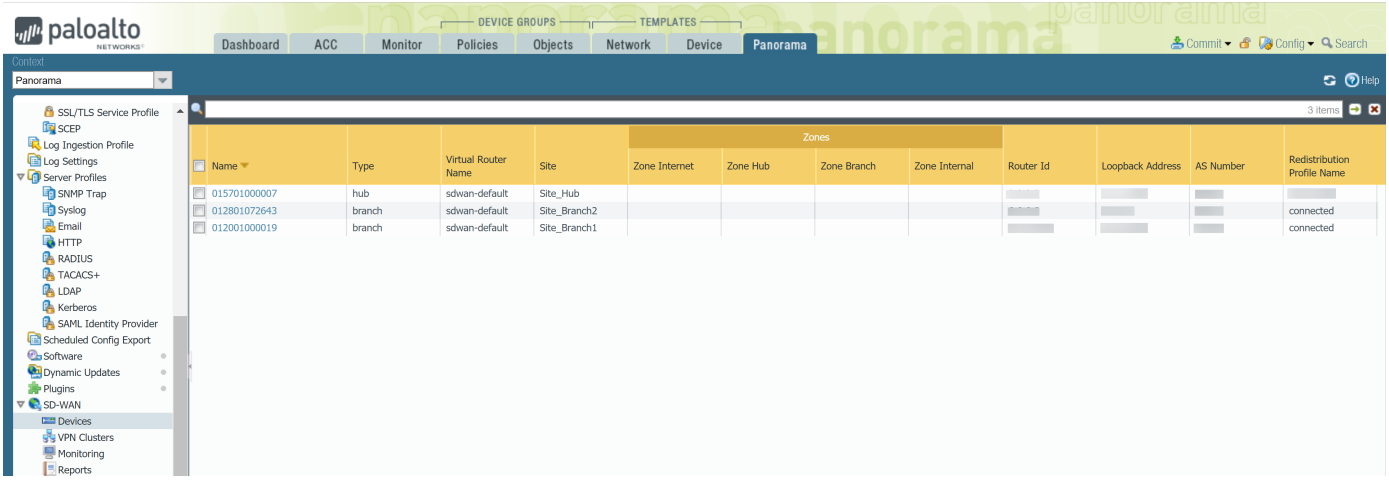
	A	B	C	D	E	F	G	H	I	J	K
1	device-serial	type	site	zone-internet	zone-branch	zone-hub	zone-internal	loopback-address	prefixes redist	as-number	router-id
2	12001000019	branch	Site_Branch1					2.2.2.2/32		65420	5.5.5.5/32
3	12801072643	branch	Site_Branch2					3.3.3.3		65413	6.6.6.6
4	15710000007	hub	Site_Hub					1.1.1.1/32	10.0.0.0/8	65432	1.1.1.1

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.



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.

Configuración de dispositivos de HA para SD-WAN

Puede configurar dos sucursales o dos centrales en el modo de HA activa/pasiva para que forme parte de su entorno de 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.

Lea el siguiente procedimiento antes de comenzar para no confirmar después de añadir sus peers de HA como dispositivos de SD-WAN.

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 centrales y crean una conexión segura entre la sucursal y los dispositivos de la central. 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® 9.1.0 solo es compatible con la topología de la VPN de SD-WAN de concentrador y radio. En una topología de concentrador y radio, una central de cortafuegos centralizado en una oficina o ubicación principal actúa como la puerta de enlace entre dispositivos de la sucursal. La conexión de la central a la sucursal es un túnel VPN. En esta configuración, el tráfico entre sucursales debe pasar por la central.

La topología de la VPN de SD-WAN de malla completa no es compatible con PAN-OS 9.1.0.

La primera vez que Configuración de una interfaz de SD-WAN virtual con enlaces de acceso de Internet directo (DIA) para un cortafuegos de la central 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 las centrales 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 las centrales y las sucursales con enlaces de DIA. Si necesita conectar centrales y sucursales con túneles VPN, debe crear un nuevo clúster de VPN y añadir todas las centrales y sucursales necesarias a ese clúster.

Se crea una clave precompartida IKE segura y aleatoria para todos las centrales y sucursales en el clúster de VPN para garantizar que los túneles VPN y los cortafuegos disponen de una clave maestra que cifra la clave precompartida. El sistema protege la clave previamente compartida, incluso del administrador. A partir de PAN-OS 9.1.2, puede actualizar la clave previamente compartida IKE que Panorama envía a todos los miembros del clúster.

Actualice la clave previamente compartida cuando los miembros del clúster no estén ocupados.

STEP 1 | Planifique la topología de VPN de la central y la sucursal para determinar qué sucursales se comunican con cada una de sus centrales. 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 | (PAN-OS 9.1.2 y versiones 9.1 posteriores, y complemento de SD-WAN 1.0.2 y versiones 1.0 posteriores) Especifique los intervalos de direcciones IP para los túneles VPN IPSec que crea la configuración de VPN automática.

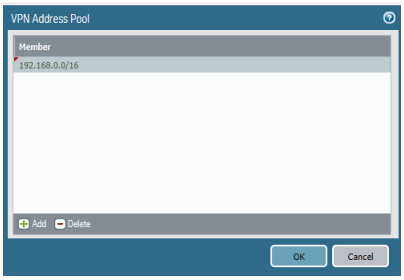
La configuración automática de VPN crea un túnel VPN entre una central y sucursales y asigna direcciones IP a los endpoints del túnel. Especifique los intervalos de subred que desee que la VPN automática use como direcciones de túnel VPN. Puede especificar hasta 20 intervalos de máscara de red/prefijo de IP. La VPN automática se basa en ese

grupo para las direcciones del túnel VPN, y realiza la selección primero del intervalo mayor (y la selección del siguiente intervalo mayor cuando sea necesario). Debe configurar al menos un intervalo para el grupo. Si no realiza este paso antes de enviar la configuración a una central 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. De lo contrario, inserte 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** > **Clústeres de VPN**.
2. En la parte inferior de la pantalla, seleccione **Grupo de direcciones de VPN**.

3. **Añada** uno o más (hasta 20) intervalos de máscara de red y de direcciones IP **miembro**, por ejemplo. 192.168.0.0/16.
4. Haga clic en **OK (Aceptar)**.



STEP 4 | Configure el clúster de VPN. Repita este paso para crear clústeres de VPN según sea necesario.

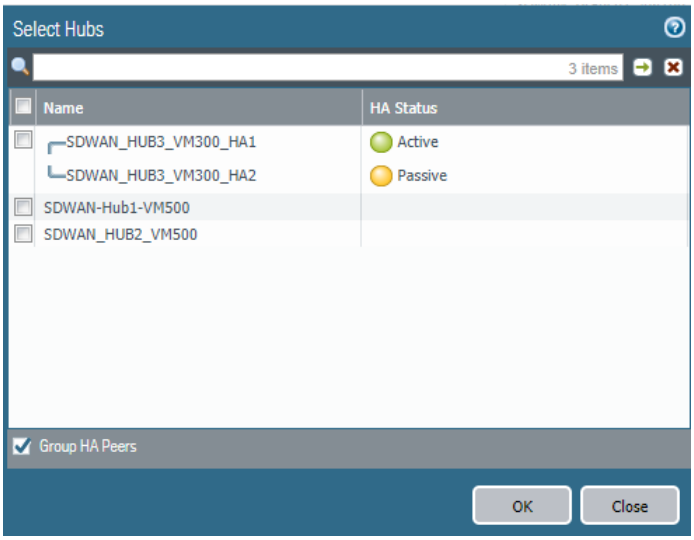
1. Seleccione **Panorama** > **SD-WAN** > **Clústeres de VPN** y **añada** un clúster de VPN.
2. Introduzca un nombre descriptivo para el clúster de VPN.

   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 > 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.

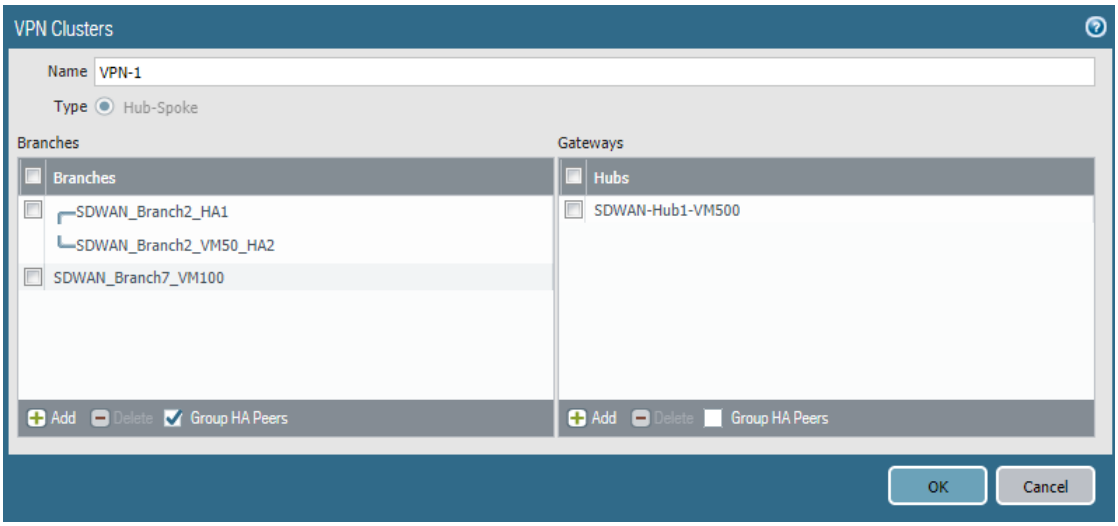
   Solo el tipo de clúster de VPN de concentrador y radio es compatible en PAN-OS 9.1.0.
4. **Añada** uno o más dispositivos de sucursal que determine que necesitan comunicarse entre sí.
   - (Complemento de SD-WAN 1.0.1 y versiones 1.0 posteriores) Seleccione **(Agrupar peers de HA** para ver los peers juntos.
   - Seleccione los dispositivos de la sucursal que añadir al clúster.
   - Haga clic en **OK (Aceptar)**.
5. **Añada** uno o más dispositivos de la central que determine que necesitan comunicarse con los dispositivos de la sucursal. Si se añade más de un dispositivo de la central, debe usar métricas de ruta para controlar qué central es la principal y cuál es la secundaria.

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.

- (Complemento de SD-WAN 1.0.1 y versiones 1.0 posteriores) Seleccione **(Agrupar peers de HA** para ver los peers juntos.
- Seleccione las centrales que añadir al clúster.
- Haga clic en **OK (Aceptar)**.



6. (Complemento de SD-WAN 1.0.1 y versiones 1.0 posteriores) Seleccione **Agrupar peers de HA** en las áreas Branches o Puertas de enlace para mostrar los peers de HA juntos.



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

STEP 5 | (PAN-OS 9.1.2 y versiones 9.1 posteriores, y complemento de SD-WAN 1.0.2 y versiones 1.0 posteriores) Anuncie prefijos adicionales en la sucursal a la central.

En PAN-OS 9.1.0, el cortafuegos redistribuye automáticamente (anuncia) todas las rutas conectadas no públicas desde la sucursal hasta la central. A partir de PAN-OS 9.1.2, también puede redistribuir cualquier prefijo adicional desde la sucursal a la central. El

campo Prefix(es) Prefijos que redistribuir acepta una lista de prefijos en lugar de un solo prefijo.

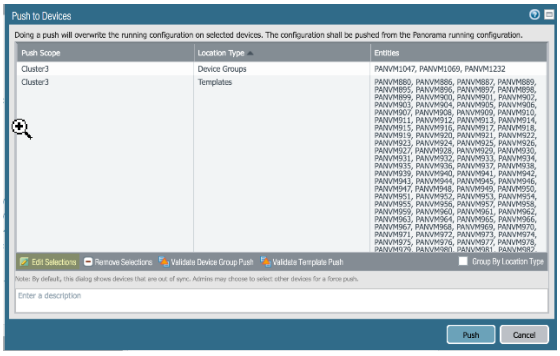
1. Seleccione **Panorama** > **SD-WAN** > **Dispositivos** y seleccione un cortafuegos de la sucursal.
2. Seleccione **BGP** y **añada** una o más direcciones IP con la máscara de red a **Prefix(es) Prefijos que redistribuir**.
3. Haga clic en **OK (Aceptar)**.

STEP 6 | Seleccione **Confirmar** y en **Confirmar en Panorama**.

STEP 7 | Envíe la configuración a las centrales.

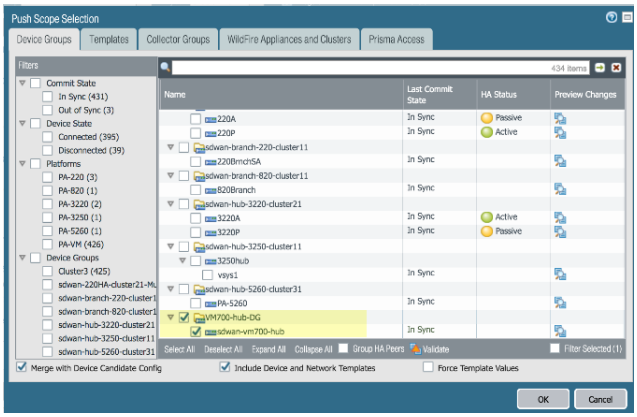
Cuando Panorama crea interfaces virtuales de SD-WAN para centrales, no necesariamente crea las interfaces mediante números de interfaz contiguos. Puede omitir aleatoriamente un número de interfaz, por ejemplo, sdwan.921, sdwan.922, sdwan.924 y sdwan.925. A pesar de la numeración no contigua, Panorama 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 de la central. Seleccione **Incluir plantillas de dispositivo y red** en la parte inferior de la pantalla. Debe enviarlas a las centrales 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 la central no tiene la dirección IP de las sucursales. Para asegurarse de que la central 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 a la central, la central estará lista.



6. Seleccione la pestaña **Plantillas** y **Anular selección de todo**.
7. El **ámbito de envío** será el grupo de dispositivos. **Envíe** la configuración a las centrales.

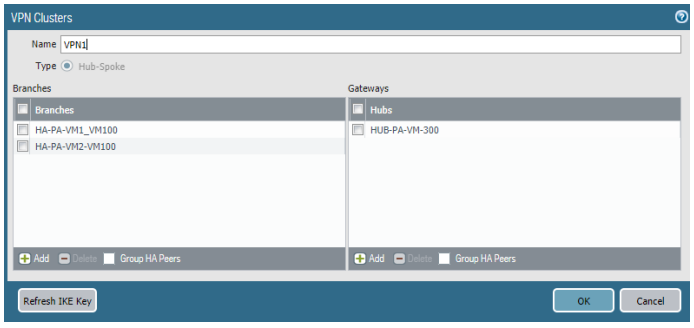
STEP 8 | Envíe la configuración a las sucursales. Para ello, repita el paso anterior, pero seleccionando su el grupo de dispositivos de la sucursal.

STEP 9 | (PAN-OS 9.1.2 y versiones 9.1 posteriores, y complemento de SD-WAN 1.0.2 y versiones 1.0 posteriores) Actualice la clave previamente compartida 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** > **Clústeres de VPN** y seleccione un clúster.
2. En la parte inferior de la pantalla, seleccione **Actualizar clave IKE**.



3. Seleccione **Confirmar**.
4. Seleccione **Enviar a dispositivos**.

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 la central 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. Tendrá que enviar una ruta estática (que se dirige a la central) a la sucursal. Tendrá que enviar una ruta estática (que se dirige a la sucursal) a la central.

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 de la central 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 la central 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 **Tipo** para que se establezca en **Interfaz**.

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 **Rutas estáticas** > **IPv4** y **Añadir** para añadir un nombre en el campo **Nombre** para la ruta estática.

STEP 7 | Para **Destino**, seleccione la variable que creó.

STEP 8 | Para **Interfaz**, seleccione **sd_wan**.

STEP 9 | Para **Siguiente salto**, seleccione **Dirección IP** y especifique la dirección IP del siguiente salto para la ruta estática (la central o sucursal a la que se dirige la ruta estática).

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

STEP 11 | **Confirme** y **envíe** sus cambios.

La configuración automática de VPN reemplaza a la palabra clave **sd_wan** 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 12 | Configure una ruta estática para el tráfico de retorno.

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 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.

- Supervisión de tareas de SD-WAN
- Supervisión del rendimiento del enlace y de la aplicación de SD-WAN
- Solución de problemas del rendimiento de la aplicación
- Solución de problemas del rendimiento del enlace
- Generación de un informe de SD-WAN

Supervisión de tareas de SD-WAN

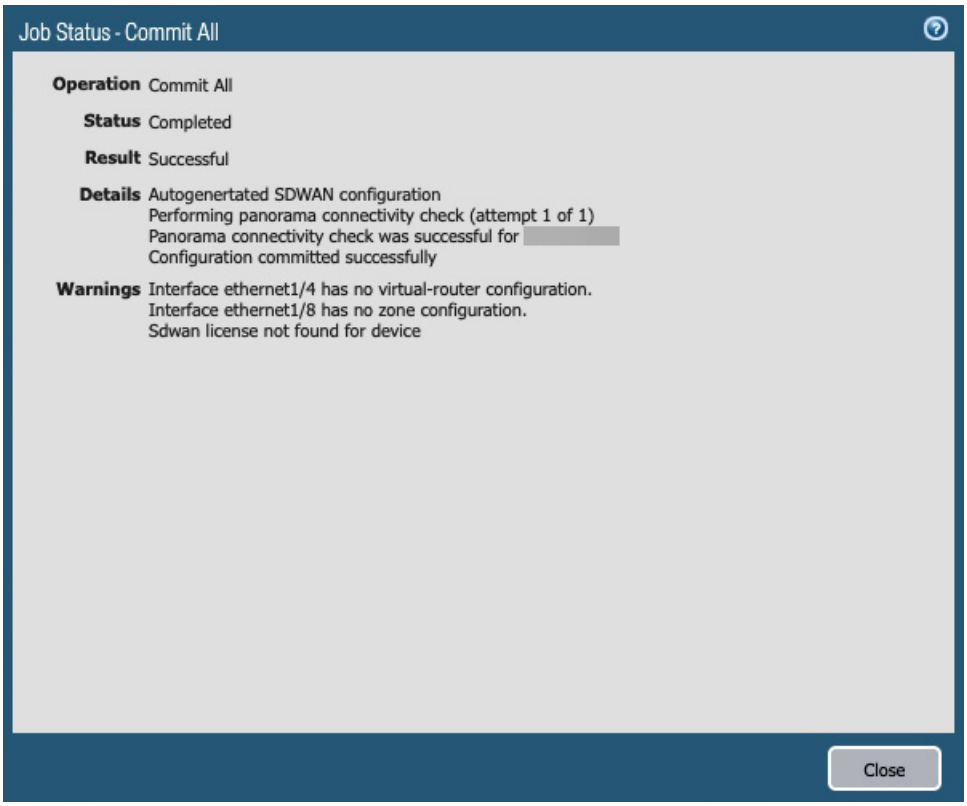
Supervise las confirmaciones, los envíos y otras tareas de SD-WAN que se ejecuten desde el servidor de gestión Panorama™ para obtener información detallada sobre la tarea específica.

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 | Inicie sesión en la interfaz web de Panorama.

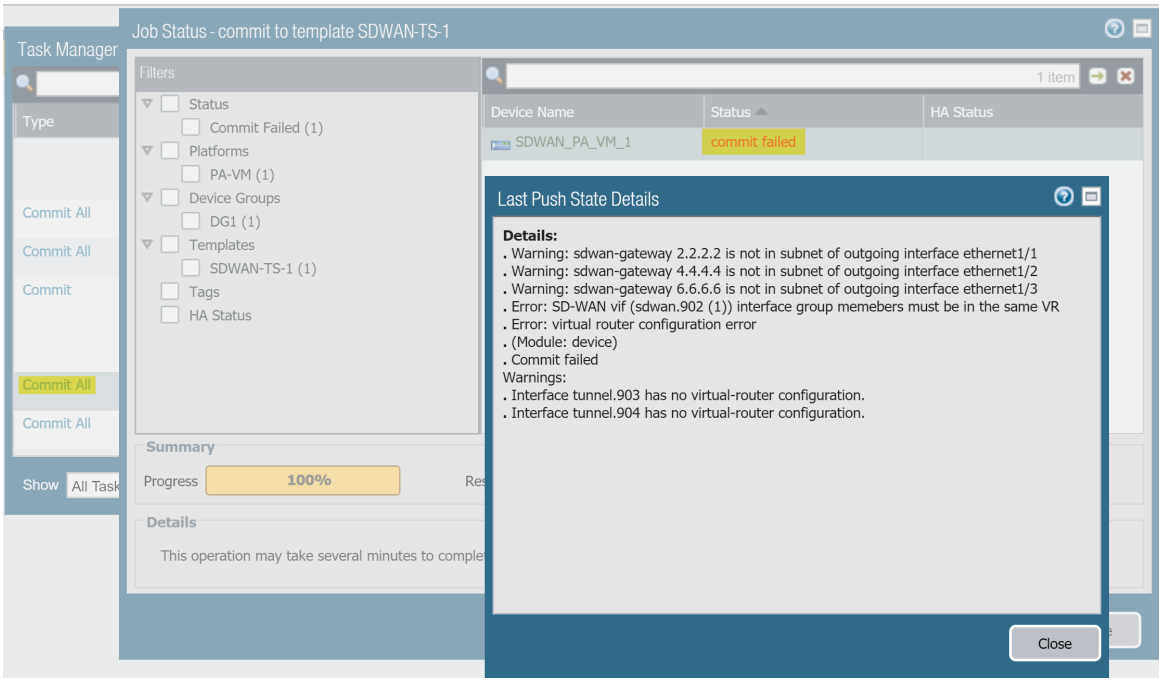
STEP 2 | Después de editar la configuración de SD-WAN, **confirme** sus cambios para ver el estado del trabajo.

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

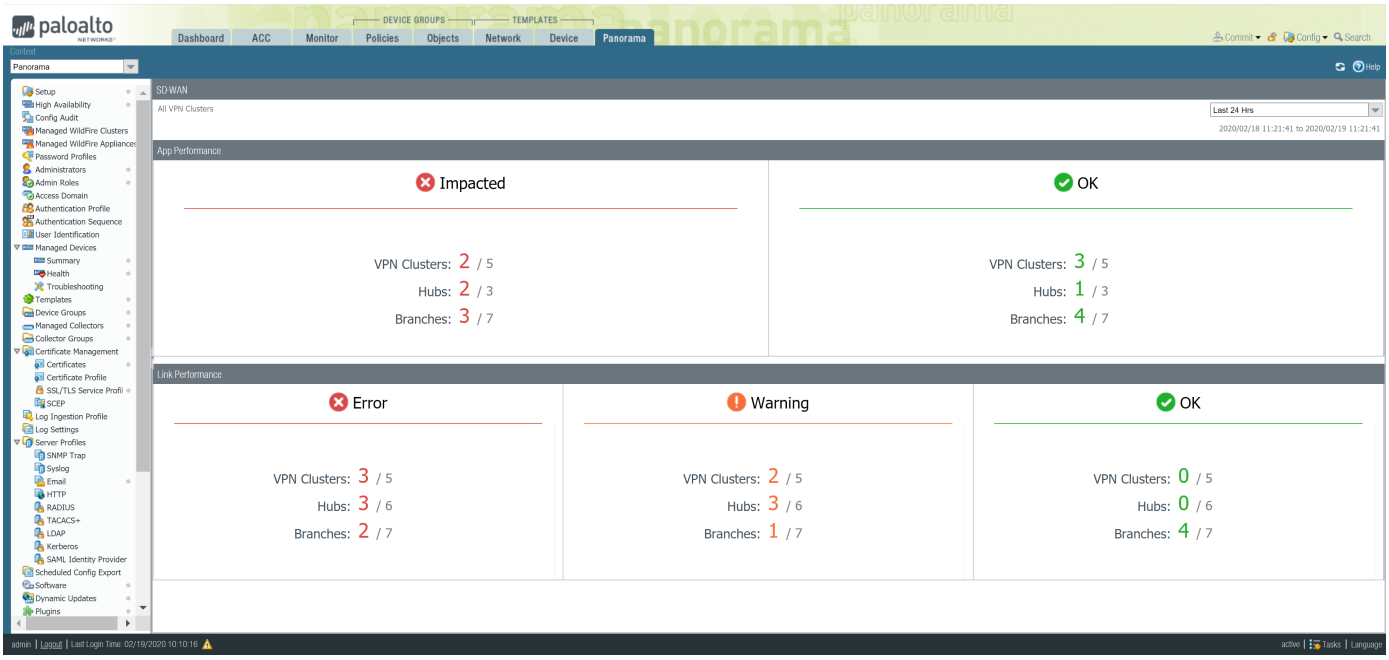
Para supervisar el rendimiento de la aplicación y el enlace en sus clústeres de VPN para solucionar problemas, consulte la información de resumen de todos los clústeres de VPN y, a continuación, realice un desglose sucesivamente para aislar los problemas de los sitios, aplicaciones y enlaces afectados. 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, centrales 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, centrales y sucursales VPN que no experimentan problemas de rendimiento de vibración, latencia o pérdida de paquetes.

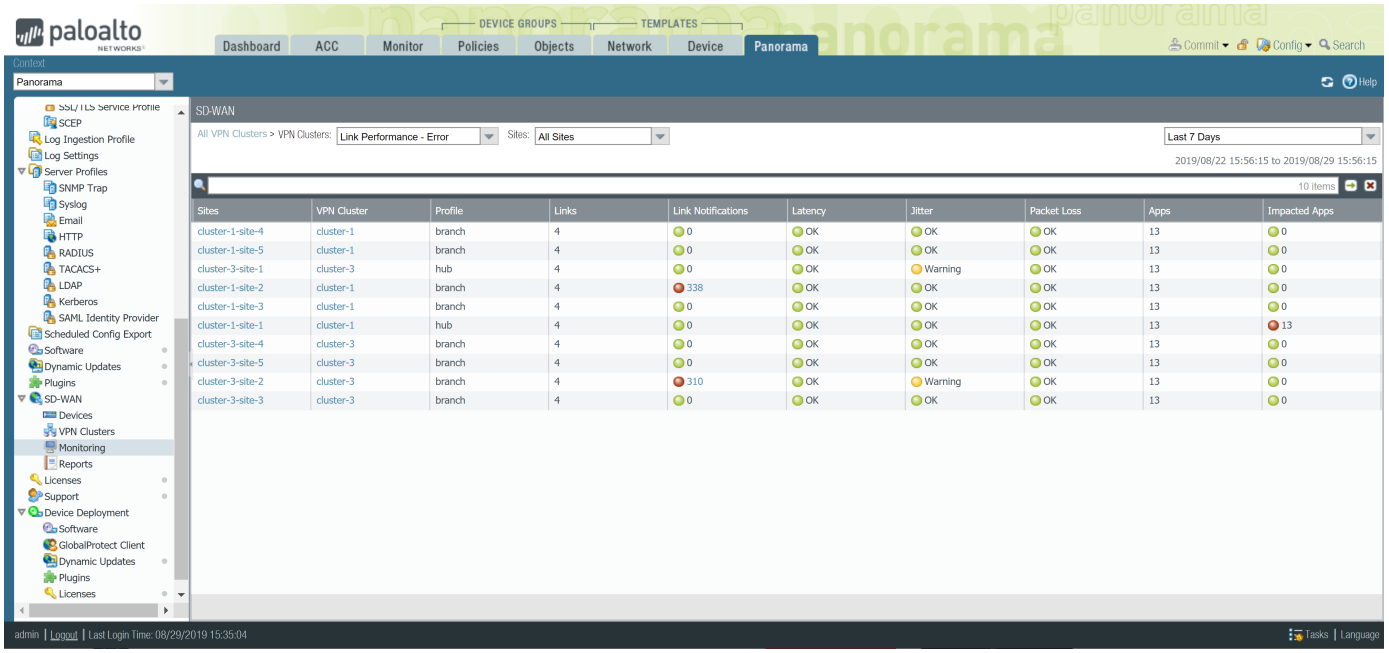
Desde el panel de inicio, reduzca la vista a aplicaciones o enlaces afectados que tengan el estado de Error o Advertencia. A continuación, seleccione un sitio afectado para ver los detalles a nivel de sitio. Desde el sitio, vea los detalles a nivel de aplicación o de enlace.

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, centrales y sucursales.



STEP 3 | 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.



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.

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 central que tengan una aplicación que precise atención.

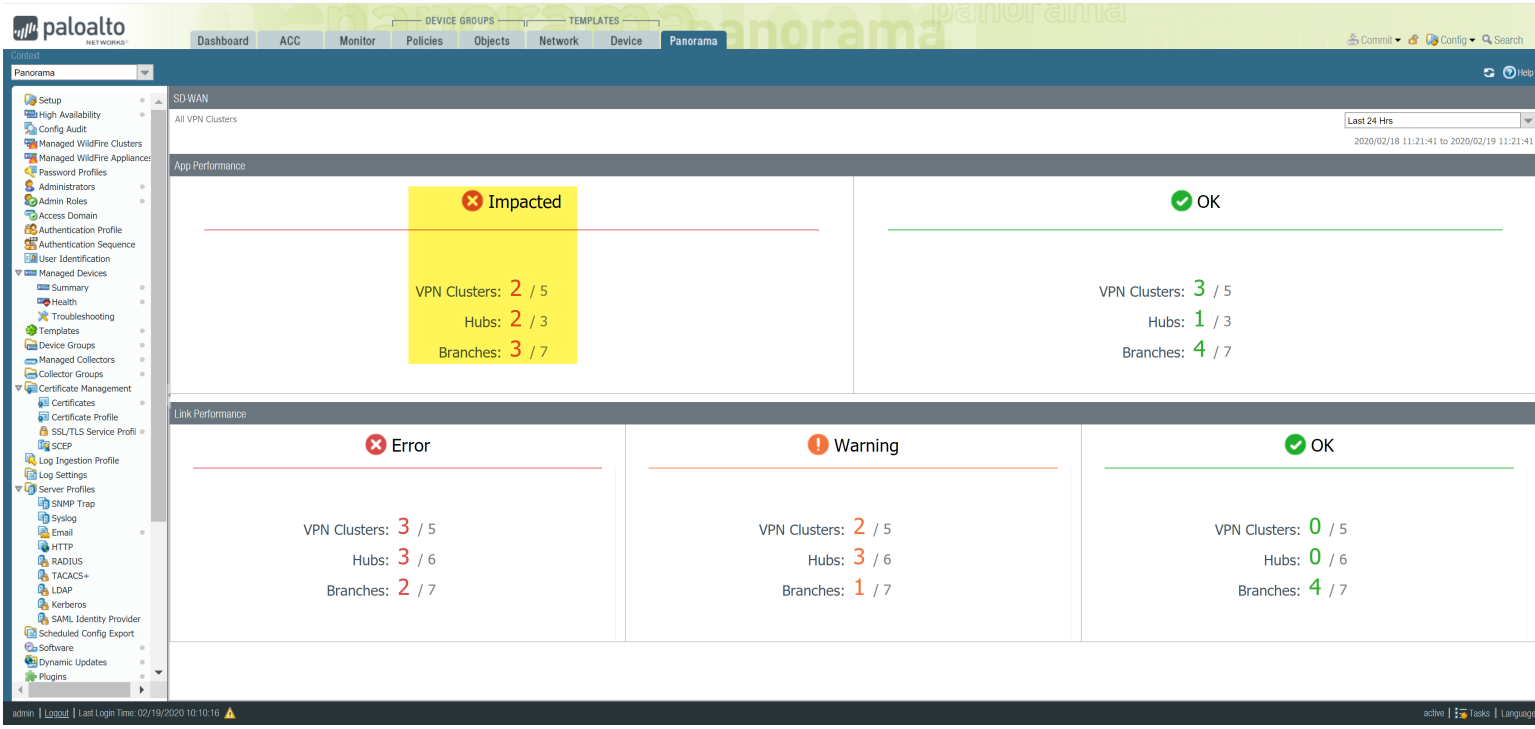
STEP 6 | Haga clic en una aplicación impactada para ver los detalles a nivel de aplicación o de enlace.

Solución de problemas del rendimiento de la aplicación

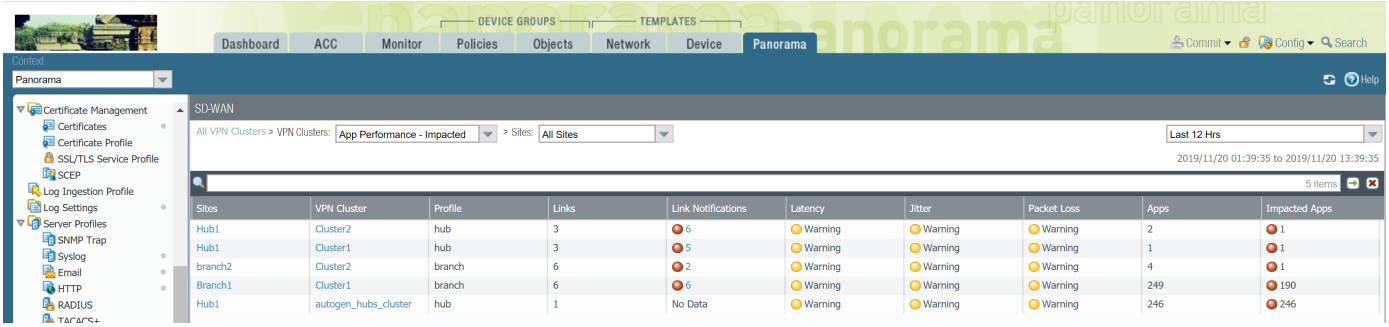
Comprender qué está provocando un rendimiento degradado para sus aplicaciones y servicios es esencial para garantizar que la experiencia del usuario no se vea afectada. Entender por qué sus clústeres de VPN se ven afectados y el motivo por el que se produjo un error en el tráfico de la aplicación en diferentes enlaces ayuda a ajustar su configuración de SD-WAN.

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

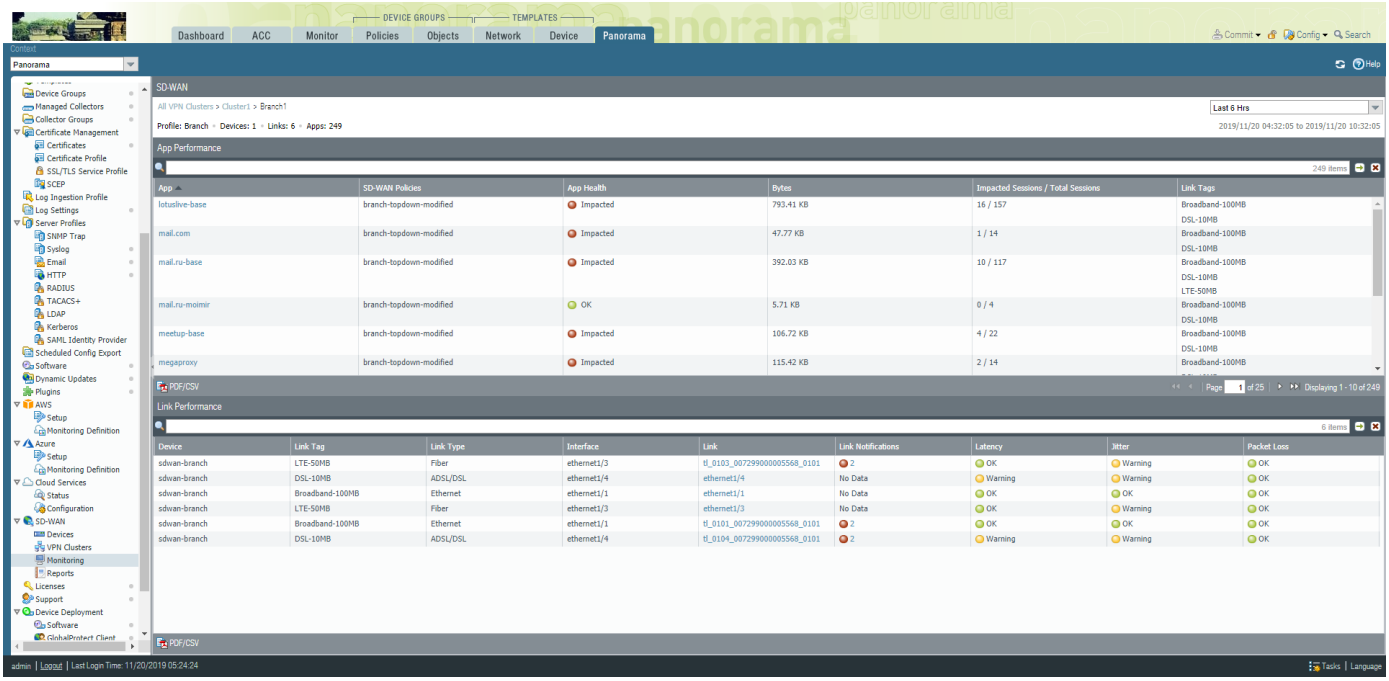
STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Supervisión** y vea los clústeres de VPN **impactados**.



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.

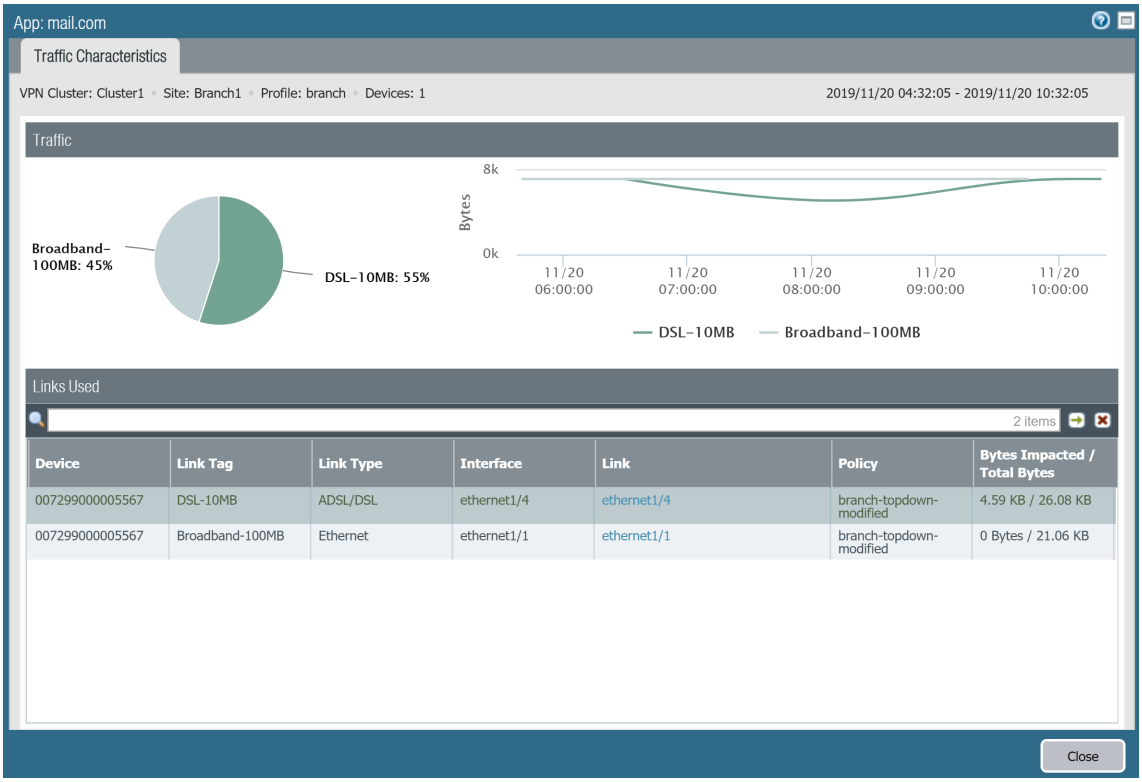


STEP 4 | En la columna Sitios, seleccione el cortafuegos de la central o la sucursal impactados para ver las aplicaciones afectadas y el rendimiento del enlace correspondiente.



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:

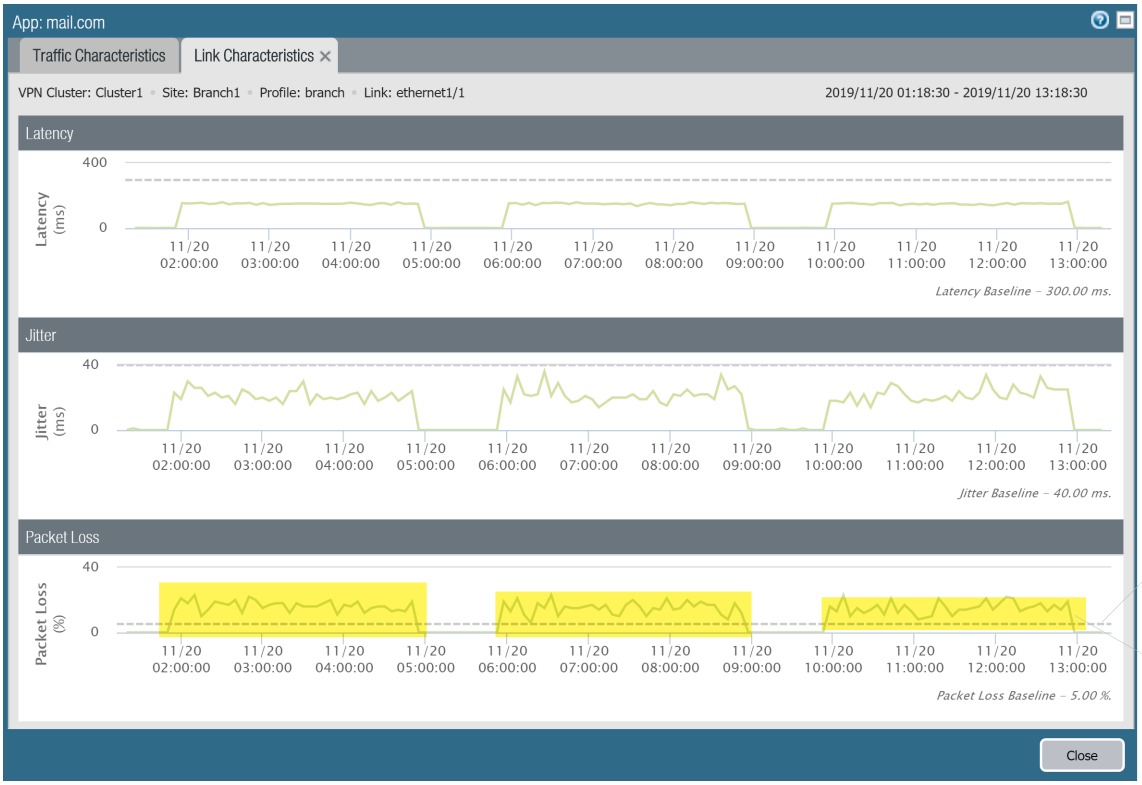
- Revise el gráfico circular para comprender el desglose del tráfico de aplicaciones en sus servicios de Internet.
- Revise el gráfico de líneas para comprender cuántos bytes de datos se transfirieron a través de cada servicio de Internet a lo largo del tiempo.
- Revise la sección Enlaces utilizados 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.

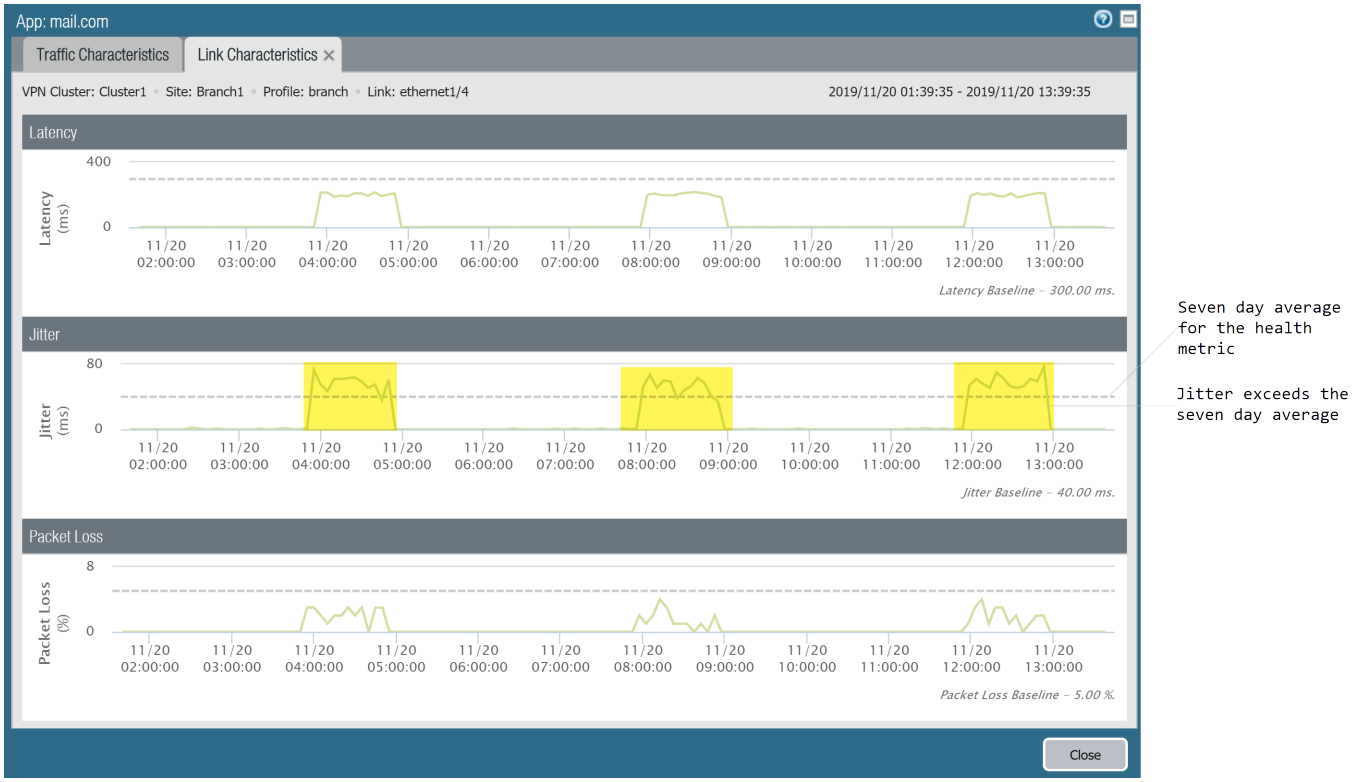
La línea de puntos indica la media de siete días para la métrica de estado.

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. En este ejemplo utilizamos ethernet 1/1 y podemos observar que el porcentaje de paquetes perdidos regularmente superó el umbral medio de siete días 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. En él podemos observar que después de que se produjera el fallo en el tráfico de la aplicación, ethernet 1/4 experimentó una vibración para el enlace que superó el umbral medio de siete días. 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:

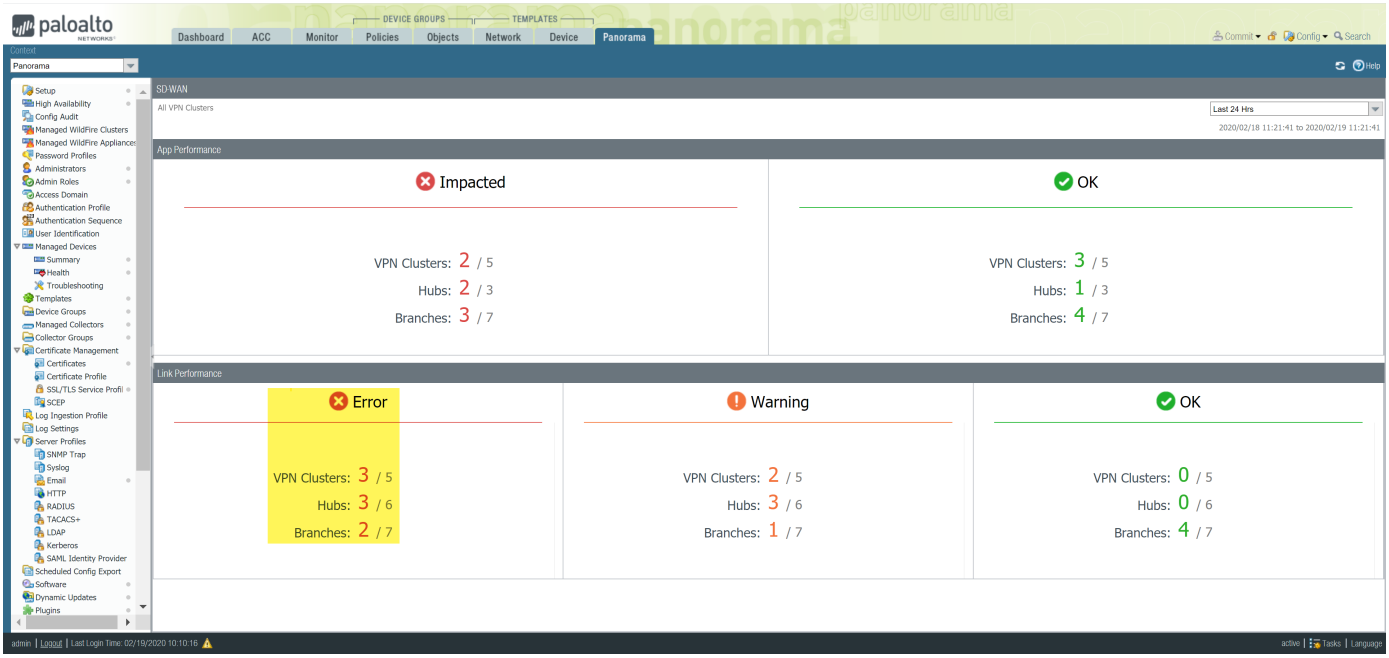
- Considere añadir enlaces adicionales al perfil de distribución de tráfico. Cuando se añaden enlaces adicionales para que se realice la conmutación por error del tráfico de la aplicación, ayuda a garantizar que el tráfico de la aplicación y la experiencia del usuario no se vean afectados por enlaces 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.

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.

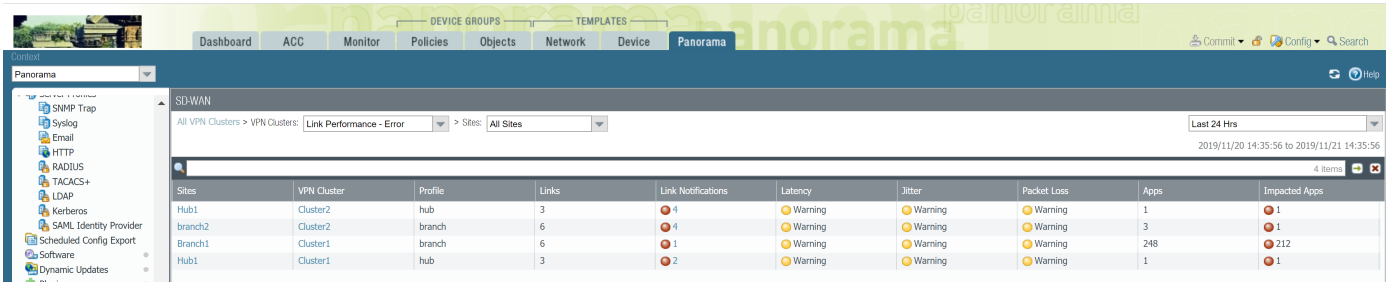
STEP 1 | Inicio de sesión en la interfaz web de Panorama.

STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Supervisión** y vea los clústeres de VPN **impactados**.

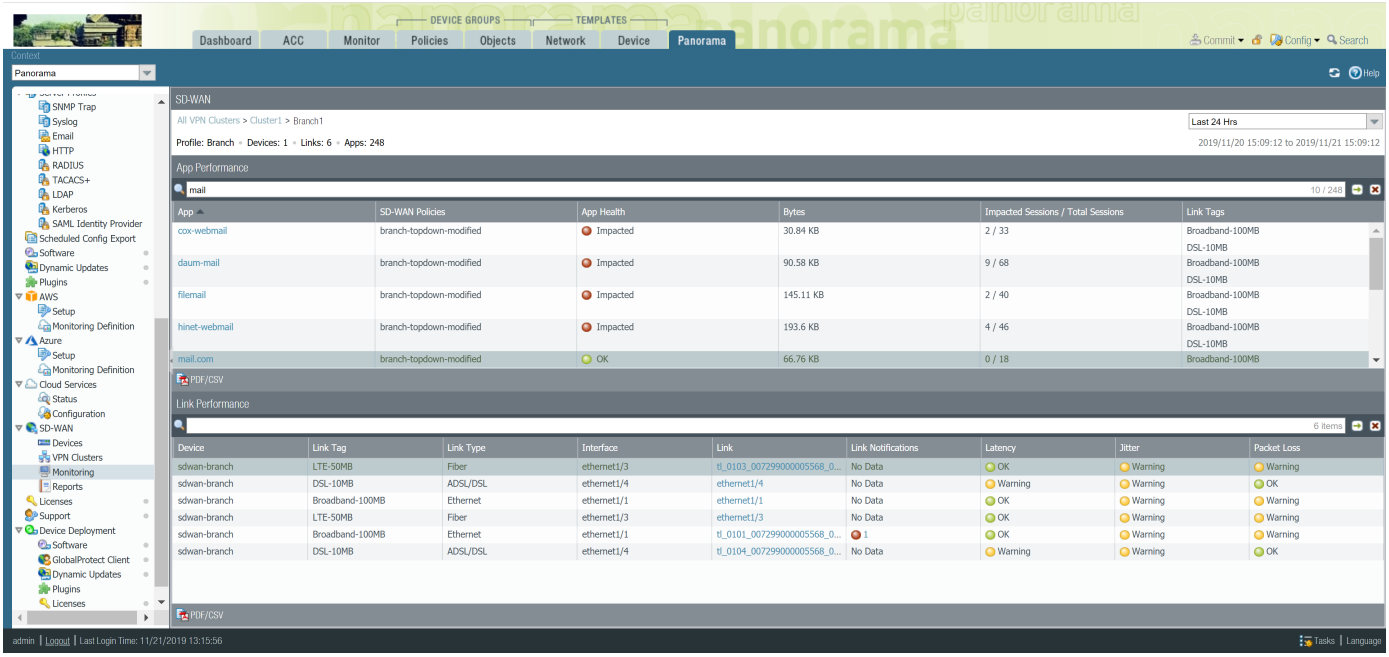


STEP 3 | Filtre los clústeres de VPN según su métrica preferida en menú desplegable **Sitio** y seleccione el periodo. En la columna Sitios, seleccione el cortafuegos de la central o la sucursal impactados para ver las aplicaciones afectadas y el rendimiento del enlace correspondiente.

En este ejemplo, estamos viendo **todos los sitios** que contienen clústeres de VPN afectados en las últimas 24 horas.

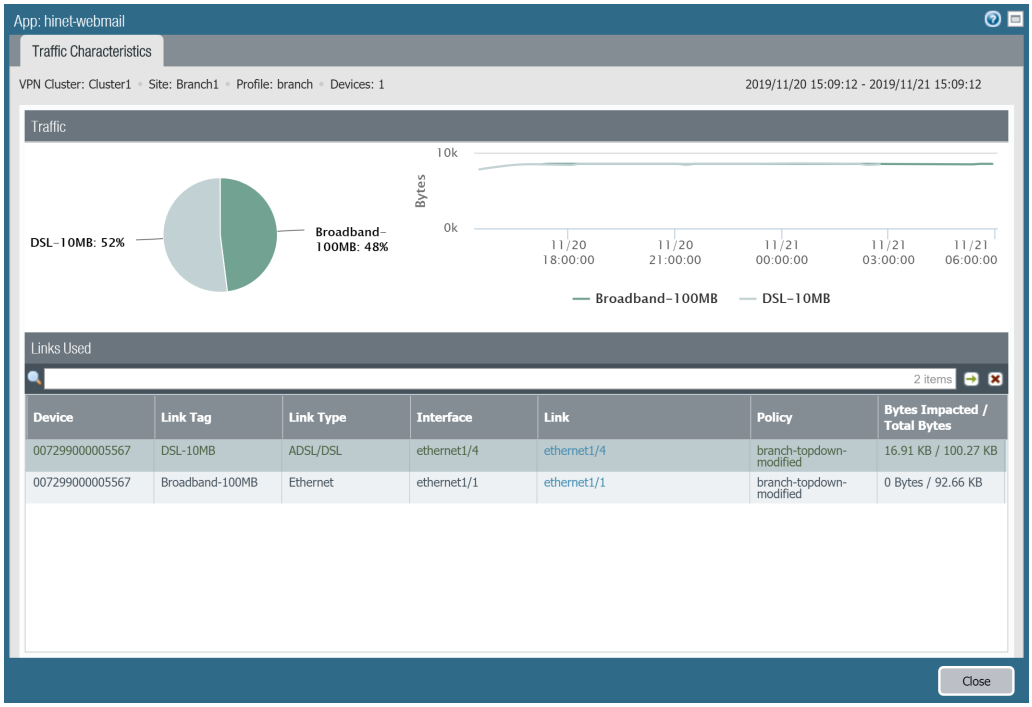


STEP 4 | En la columna Sitios, seleccione el cortafuegos de la central o la sucursal impactados para ver las aplicaciones afectadas y el rendimiento del enlace correspondiente.



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:

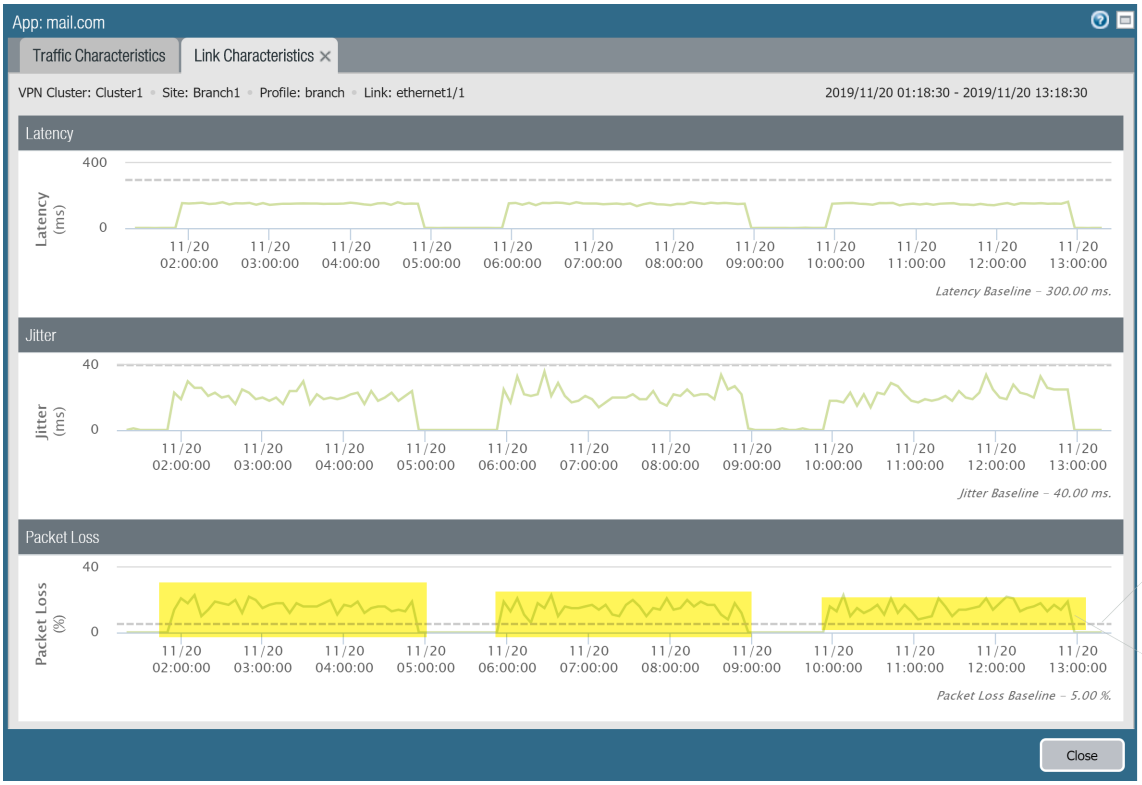
- Revise el gráfico circular para comprender el desglose del tráfico de aplicaciones en sus servicios de Internet.
- Revise el gráfico de líneas para comprender cuántos bytes de datos se transfirieron a través de cada servicio de Internet a lo largo del tiempo.
- Revise la sección Enlaces utilizados 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.

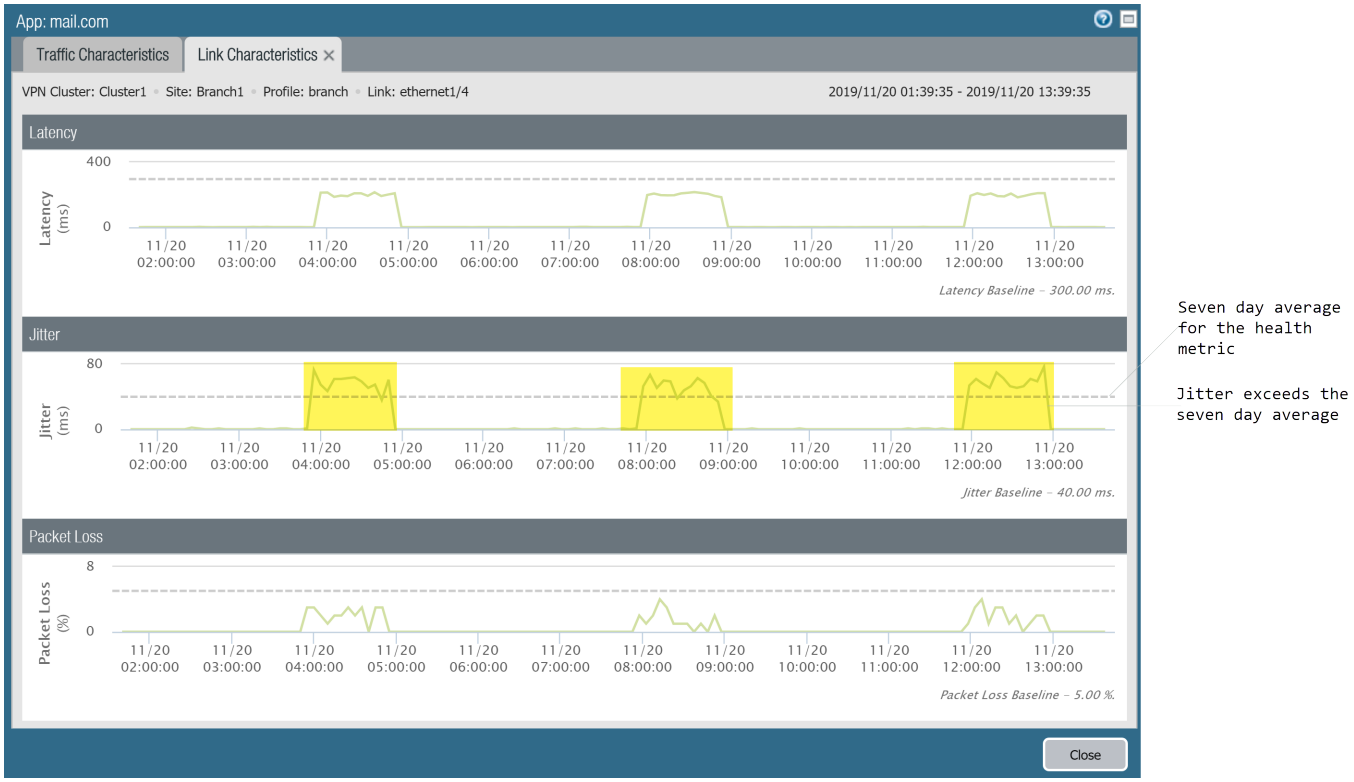
La línea con puntas indica el umbral que configura cuando Creación de un perfil de calidad de ruta.

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.

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.

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

STEP 2 | Seleccione **Panorama** > **SD-WAN** > **Informes** y **añada** un nuevo informe.

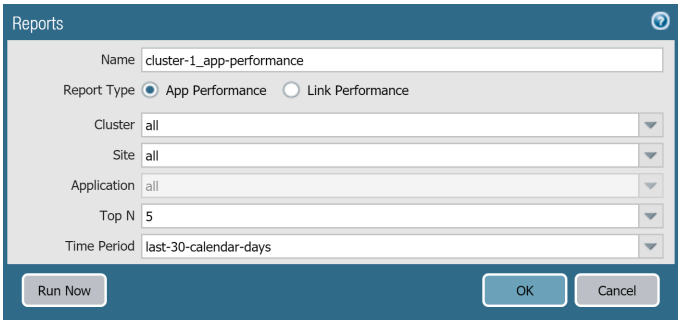
STEP 3 | Configure los parámetros del informe de SD-WAN.

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**.

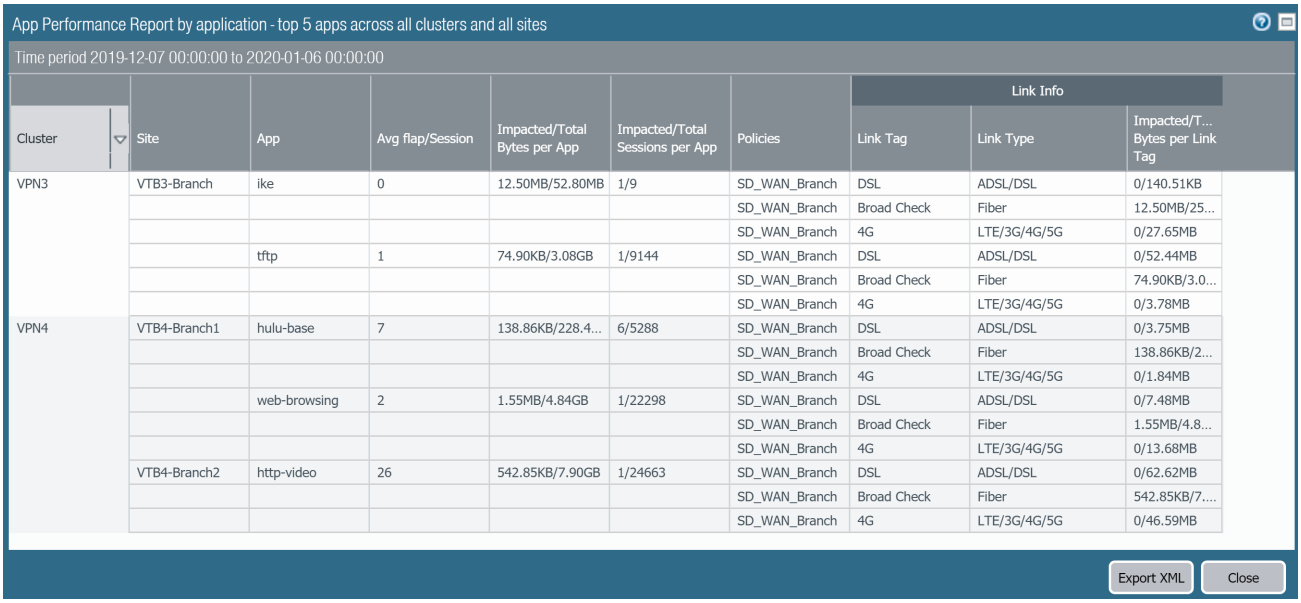
   Si seleccionó **todos** los clústeres, este campo estará atenuado y no se podrá seleccionar un sitio.
5. (Solo rendimiento de la aplicación) Seleccione la **aplicación** para la que generar el informe.

   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**.



Cluster	Site	App	Avg flap/Session	Impacted/Total Bytes per App	Impacted/Total Sessions per App	Policies	Link Info		
							Link Tag	Link Type	Impacted/T... Bytes per Link Tag
VPN3	VTB3-Branch	ike	0	12.50MB/52.80MB	1/9	SD_WAN_Branch	DSL	ADSL/DSL	0/140.51KB
						SD_WAN_Branch	Broad Check	Fiber	12.50MB/25...
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/27.65MB
		tftp	1	74.90KB/3.08GB	1/9144	SD_WAN_Branch	DSL	ADSL/DSL	0/52.44MB
						SD_WAN_Branch	Broad Check	Fiber	74.90KB/3.0...
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/3.78MB
VPN4	VTB4-Branch1	hulu-base	7	138.86KB/228.4...	6/5288	SD_WAN_Branch	DSL	ADSL/DSL	0/3.75MB
						SD_WAN_Branch	Broad Check	Fiber	138.86KB/2...
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/1.84MB
		web-browsing	2	1.55MB/4.84GB	1/22298	SD_WAN_Branch	DSL	ADSL/DSL	0/7.48MB
						SD_WAN_Branch	Broad Check	Fiber	1.55MB/4.8...
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/13.68MB
	VTB4-Branch2	http-video	26	542.85KB/7.90GB	1/24663	SD_WAN_Branch	DSL	ADSL/DSL	0/62.62MB
						SD_WAN_Branch	Broad Check	Fiber	542.85KB/7....
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/46.59MB

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
> 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.	`> show sdwan event`
• Elimine los eventos de SD-WAN.	`> clear sdwan event`
• 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	`> show sdwan path-monitor stats vif <sdwan.x>` `> show sdwan path-monitor stats vif <sdwan-interface-name>`

Si quiere...	Use...
muestra el valor del parámetro la última vez que el cambio de valor en tiempo real superó el umbral.	
• 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.	`> 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	

• 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 la 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 la 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`

Si quiere...	Use...
• 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>`
• 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`

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 | Inicie sesión en la interfaz web de Panorama.

STEP 2 | (Solo complemento de SD-WAN 1.0.2 y versiones posteriores) 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.