Citrix SD-WAN 11.5

Machine translated content

Disclaimer

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Cloud Software Group solo tiene traducción automática. Cloud Software Group no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Cloud Software Group se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Cloud Software Group, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Cloud Software Group no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

Contents

Notas de la versión de Citrix SD-WAN 11.5

November 16, 2022

Este documento de notas de la versión describe las mejoras y los cambios, los problemas resueltos y conocidos que existen para Citrix SD-WAN 11.5.

Notas

Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

Novedades

Las mejoras y los cambios que están disponibles en la versión 11.5 de SD-WAN.

Otros

Especificaciones de la versión 11.5 de Citrix SD-WAN

- Citrix SD-WAN 11.5.0 es una versión de disponibilidad limitada, recomendada y admitida solo para implementaciones de producción/clientes específicos.
- La versión 11.5.0 de SD-WAN no admite implementaciones de Advanced Edition (AE), Premium Edition (PE) ni de optimización de WAN.
- SD-WAN 11.5.0 solo admite las plataformas mencionadas en los modelos de plataforma y paquetes de software de SD-WAN.
- SD-WAN 11.5.0 no admite Citrix SD-WAN Center ni Citrix SD-WAN Orchestrator para entornos locales.
- El firmware de SD-WAN 11.5.0 no está disponible en la página de descargas de Citrix.
- La versión SD-WAN 11.5.0 solo está disponible a través de Citrix SD-WAN Orchestrator Service y solo en los POP geográficos seleccionados.
- Asegúrese de obtener las aprobaciones y la orientación necesarias de Citrix Product Management/Citrix Support antes de implementar 11.5.0 en cualquier red de producción.

[NSSDW-38486]

El**servicio Citrix SD-WAN Orchestrator reemplaza al Editor de configuración de SD-WAN**:

A partir de la versión 11.5 de Citrix SD-WAN, el Editor de configuración de SD-WAN y el Centro de SD-WAN se sustituyen por Citrix SD-WAN Orchestrator Service. El servicio Citrix SD-WAN Orchestrator admite todas las configuraciones que se realizan actualmente a través del Editor de configuración de SD-WAN. Para obtener más información sobre Citrix SD-WAN Orchestrator Service, consulte Servicio Citrix SD-WAN Orchestrator.

[NSSDW-33528]

Compatibilidad con IPv6:

A partir de la versión 11.5.0 de Citrix SD-WAN, las siguientes funciones del plano de datos de los dispositivos Citrix SD-WAN admiten direcciones IPv6:

- Rutas de aplicación
- Optimización del servicio Citrix Cloud y Gateway
- Clasificación de aplicaciones basada en nombres de dominio
- Personalización dinámica de archivos PAC
- Redirección dinámica
- Valores predeterminados del firewall
- Multidifusión
- Optimización de Office 365
- PPPoE
- Informes del sitio: protocolos de redirección
- VRRP

Después de configurar las funciones enumeradas anteriormente, si deshabilita el protocolo IPv4 o IPv6, las funciones no funcionarán como se esperaba.

[SDW-23397, NSSDW-29150, NSSDW-29152, NSSDW-29154, NSSDW-29155, NSSDW-29156, NSSDW-29468, NSSDW-1940, NSSDW-1995]

Mejoras de monitoreo:

Los siguientes paneles de control se han mejorado y están disponibles en la nueva interfaz de usuario del dispositivo:

- Reenviador transparente DNS
- Conexiones de firewall, filtro de firewall, NAT de firewall
- IGMP, proxy IGMP, estadísticas IGMP
- IKE, IPsec

- Grupo multicast, origen del grupo multicast, destino del grupo multicast
- Sesiones PPPoE
- VRRP

[NSSDW-33763]

Plataforma y sistemas

Material de referencia: biblioteca de firmas de aplicaciones

Se ha actualizado la biblioteca de firmas de aplicaciones de PPP.

[NSSDW-38209]

Problemas resueltos

Los problemas que se abordan en la versión 11.5 de SD-WAN.

Otros

El estado de la interfaz de administración de algunos dispositivos SD-WAN se mostraba como Inactivo en la página **Configuración de interfaz Ethernet** de la interfaz de usuario. Este problema se producía cuando algunos dispositivos que admitían la administración dentro de banda, estaba disponible la opción de usar fuera de banda. Por lo tanto, los dispositivos utilizaron una interfaz de administración fuera de banda para acceder al servicio SD-WAN Orchestrator.

[NSSDW-37028]

Problemas conocidos

Los problemas que existen en la versión 11.5 de SD-WAN.

En caso de implementación escalada al cambiar la configuración en cualquier sitio o enlace WAN, el reinicio del motor de redirección provoca que las sesiones de BGP se inactiven.

[SDWANHELP-2594]

Un dispositivo SD-WAN se bloqueó inesperadamente. Este problema se producía cuando:

- El tráfico de multidifusión IPv6 fluía durante una actualización de software.
- El tráfico de multidifusión IPv6 se originó mediante un túnel GRE de Intranet y se replicó en varias sucursales a través de la ruta virtual mediante la configuración de proxy MLDv2.

Solución alternativa: deshabilite el tráfico de multidifusión IPv6 durante la actualización del software y actívelo cuando la actualización se realice correctamente

[NSSDW-38495]

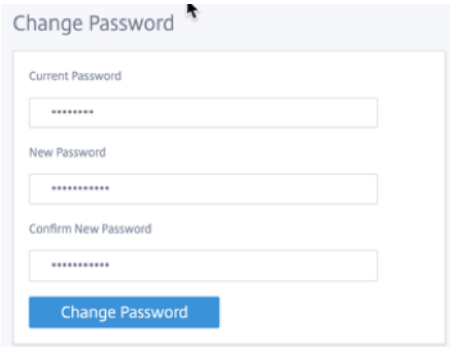
Nueva interfaz de usuario para dispositivos SD-WAN

September 1, 2022

Se introduce una nueva interfaz de usuario (UI) para los dispositivos SD-WAN. La nueva interfaz de usuario se crea mediante las últimas tecnologías de interfaz de usuario. El nuevo diseño de interfaz de usuario mejora la seguridad, tiene un aspecto mejorado, es más eficiente, seguro y sensible. Pero la nueva interfaz de usuario ha conservado el flujo y el diseño de página de cada entidad de la interfaz de usuario heredada.

A partir de la versión 11.4 de Citrix SD-WAN, la nueva interfaz de usuario está habilitada de forma predeterminada en todos los dispositivos Citrix SD-WAN configurados como clientes.

> **Nota**
>
> - El aprovisionamiento de los dispositivos Citrix SD-WAN como MCN lo redirige a la interfaz de usuario heredada.
> - Todos los usuarios locales con un rol de administrador y los usuarios administradores remotos pueden acceder a la nueva interfaz de usuario. Las cuentas de usuario remoto se autentican a través de servidores de autenticación RADIUS o TACACS+. Es obligatorio cambiar la contraseña predeterminada de la cuenta de usuario administrador al Provisioning el dispositivo SD-WAN. La contraseña predeterminada es el número de serie del dispositivo SD-WAN y tiene la obligación de cambiar la primera vez después de iniciar sesión en el dispositivo.



La interfaz de usuario heredada se mantiene para la compatibilidad con versiones anteriores y está obsoleta. Se puede acceder a la interfaz de usuario heredada mediante la URL **https: ///cgi-bin/login.cgi.**< ip-address > El nombre de usuario y la contraseña del **administrador** de usuario

siguen siendo los mismos en ambas interfaces de usuario (nuevas/heredadas), y los procedimientos de inicio de sesión por primera vez se pueden realizar utilizando cualquiera de las interfaces. Se admitirán usuarios adicionales en futuras versiones de la nueva interfaz de usuario.

Citrix SD-WAN nueva interfaz de usuario

Se puede acceder a la nueva interfaz de usuario mediante los exploradores Google Chrome (versión 81), Mozilla Firefox, Microsoft Edge (versión 81+) y Legacy Microsoft Edge (versión 44+).

> **NOTA**
>
> Microsoft Internet Explorer, Apple Safari y otros exploradores no son compatibles.

Para acceder a la nueva página de interfaz de usuario, realice lo siguiente:

1. Abra una nueva ficha del explorador y vaya a **https: // < management-ip >** para acceder a la nueva interfaz de usuario en el dispositivo SD-WAN. Si está accediendo a una dirección IPv6, escriba `https://<[IPv6 address]>`.

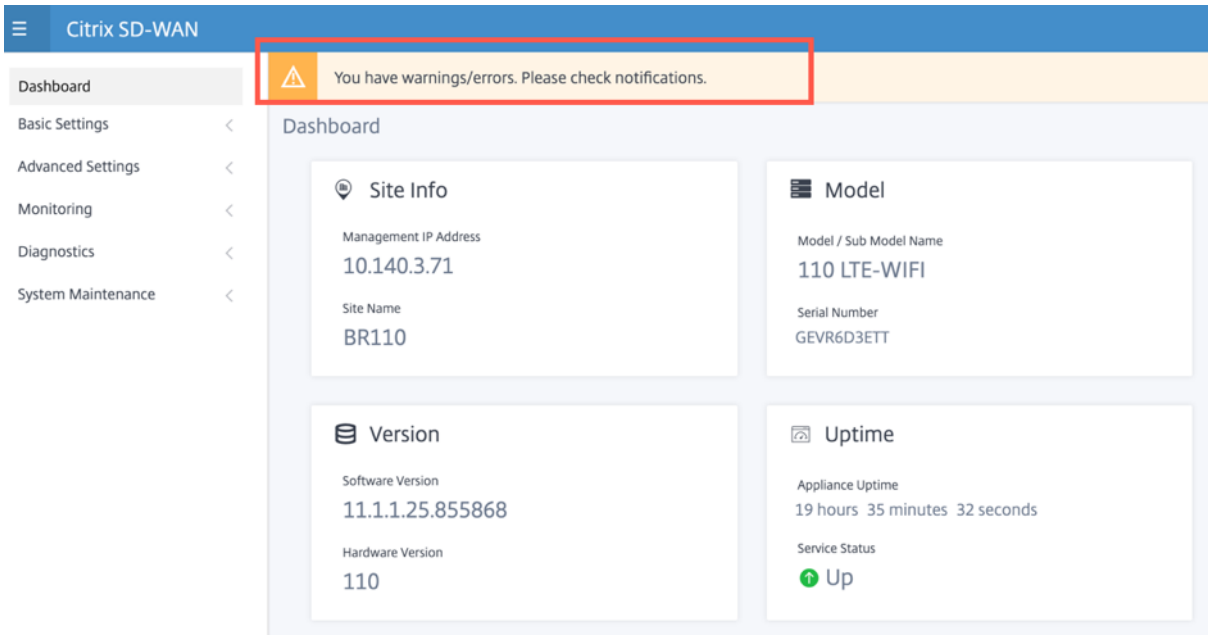
   Ejemplo:`https://[fd73:xxxx:yyyy:26::9]`

> **Nota**
>
> En el caso en el que está habilitada la administración en banda, se puede proporcionar la dirección IP de la interfaz **<management-ip>** para acceder a la nueva interfaz de usuario. La administración en banda se puede habilitar en varias interfaces de confianza que están habilitadas para ser utilizadas para servicios IP. Puede acceder a la interfaz de usuario mediante la IP de administración y las IP virtuales en banda.

1. Proporcione el nombre de usuario y la contraseña. Haga clic en **Sign In**.

Aparece la página de interfaz de usuario de Citrix SD-WAN.

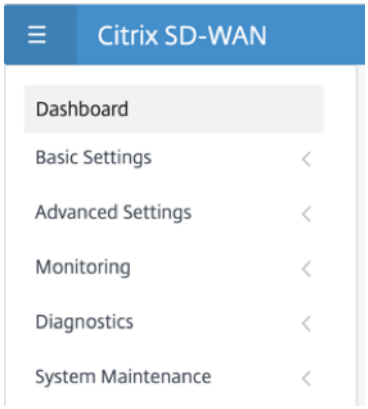
Una vez que hayas iniciado sesión correctamente, podrás ver que el panel de navegación está en el lado izquierdo. Además, puede ver un banner de notificaciones en el panel si hay advertencias o errores.



Navegación

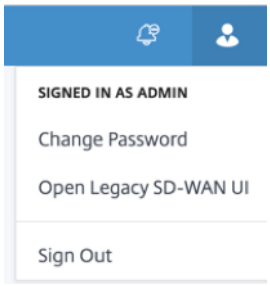
La barra lateral izquierda de navegación se puede ocultar o hacer visible al hacer clic en el icono de la hamburguesa. El icono de hamburguesa en la esquina superior izquierda proporciona

enlaces al tablero, configuración **básica/avanzada**, supervisión y opciones relacionadas con la administración.



Barra de menús

El menú de usuario de la esquina superior derecha muestra los detalles del usuario que ha iniciado sesión. Puede abrir la interfaz de usuario heredada en una nueva ficha del explorador haciendo clic en la opción **Abrir interfaz de usuario SD-WAN heredada**. Haga clic en el icono de campana para ver cualquier notificación.

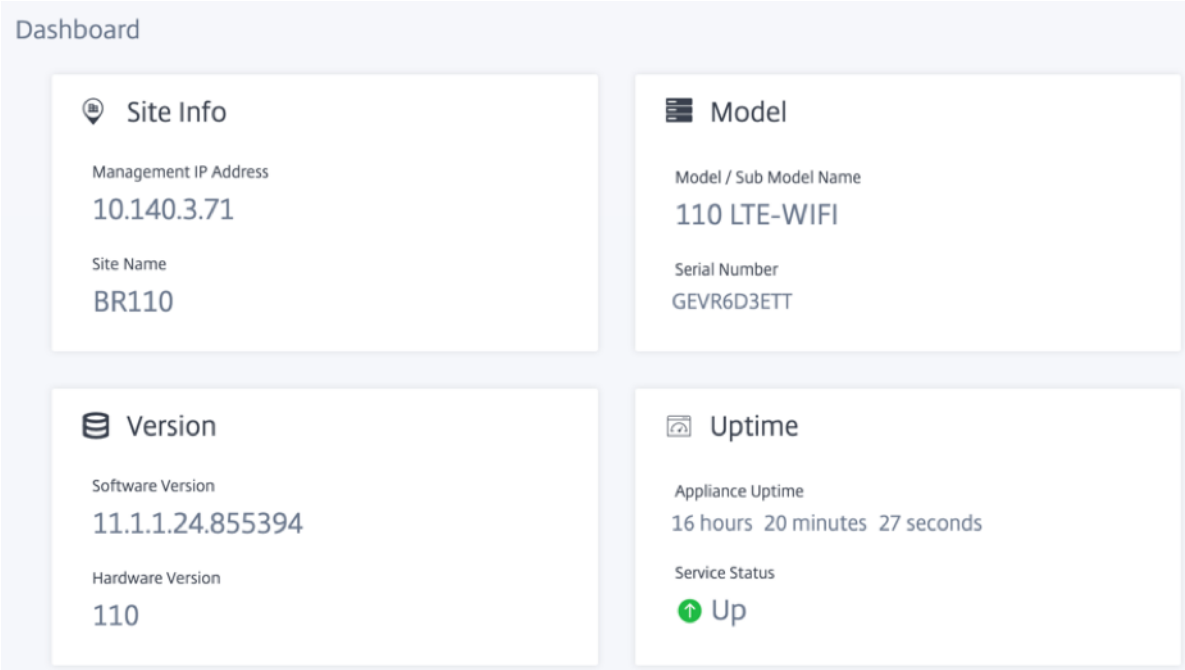


Panel de mandos

La página **Panel** muestra la siguiente información básica del dispositivo SD-WAN como una vista de teselas:

- **Sitio**: Muestra la información del sitio con la **dirección IP de administración** y el **nombre del sitio**
- **Modelo**: Muestra el **nombre del modelo/submodelo y elnúmero de serie**
- **Versión**: Muestra la versión de **software** y **hardware**
- Tiempo de**actividad: muestra el tiempo** de **actividad del dispositivo**, el estado del **servicio Citrix Virtual WAN y el estado** de **conectividad de Orchestrator**.

- **Alta disponibilidad**: Muestra el estado de HA del dispositivo local y del mismo nivel y la hora de recepción de la última actualización de alta disponibilidad.
- **Vínculos medidos**: Muestra los detalles de uso y facturación de los vínculos en los que está habilitada la medición.
- **Conectividad de Orchestrator**: Muestra el estado de conectividad del dispositivo con Citrix SD-WAN Orchestrator Service. Se muestra la siguiente información de estado:
  - **Estado en línea**: Indica el estado de la conexión entre el dispositivo y Citrix SD-WAN Orchestrator Service. El dispositivo envía señales de latido periódicas al servicio Citrix SD-WAN Orchestrator para identificar el estado de la conexión como Bueno o Malo.
  - **Estado del servicio**: Indica la accesibilidad https del dispositivo a todos los servicios de SD-WAN Orchestrator requeridos, como descarga, inicio, registro y estadísticas. Si el estado del servicio es malo, significa que la conexión está establecida, pero no se puede acceder a todos o a algunos de los servicios. Se muestra el nombre del servicio inalcanzable.
  - **Estado de DNS**: Indica el estado de resolución de DNS de FQDN. Si el estado del DNS es incorrecto, significa que la resolución de DNS de uno de los FQDN está fallando. Se muestra el nombre del FQDN sin resolver.
  - **Estado de la puerta de enlace local**: Indica el estado de la puerta de enlace predeterminada. Para una conexión fuera de banda, el estado de la puerta de enlace se determina haciendo ping a la puerta de enlace predeterminada. Para una conexión en banda, el estado de la puerta de enlace se determina haciendo ping a la dirección IP de la interfaz Ethernet en banda.
  - **Conectado a través**: Indica cómo el dispositivo llega al servicio Citrix SD-WAN Orchestrator. Ya sea a través de fuera de banda, que es la configuración predeterminada, o a través de dentro de banda, si la administración en banda está configurada.
  - **Motivo del error**: Motivo del error al conectarse al servicio SD-WAN Orchestrator.



Parámetros básicos

La **configuración básica** del dispositivo SD-WAN incluye la siguiente configuración de entidades. La nueva interfaz de usuario proporciona una página independiente para configurar cada entidad individualmente.

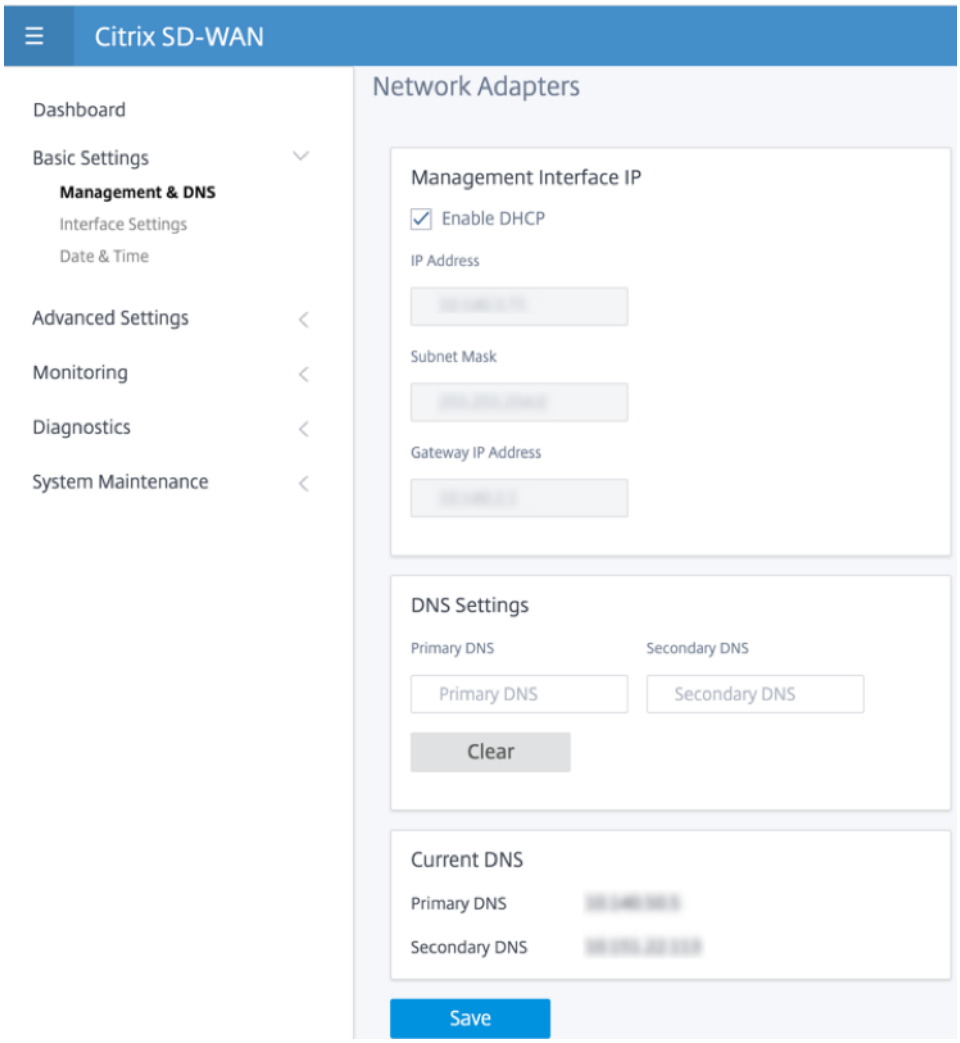
- Administración y DNS
- Configuración de la interfaz
- Grupo LAG LACP
- Fecha y hora
- Servidor RADIUS
- Servidor TACACS+

Administración y DNS

Desde la página **Administración y DNS**, puede configurar la dirección IP de la interfaz de administración y la configuración DNS. Para obtener más información, consulte Configurar la dirección IP de administración.

La lista de permisos de la interfaz de administración es una lista aprobada de direcciones IP o dominios IP que tienen permiso para acceder a la interfaz de administración. Una lista vacía permite acceder a la interfaz de administración desde todas las redes. Puede agregar direcciones IP para asegurarse de que las redes de confianza solo pueden acceder a la dirección IP de administración.

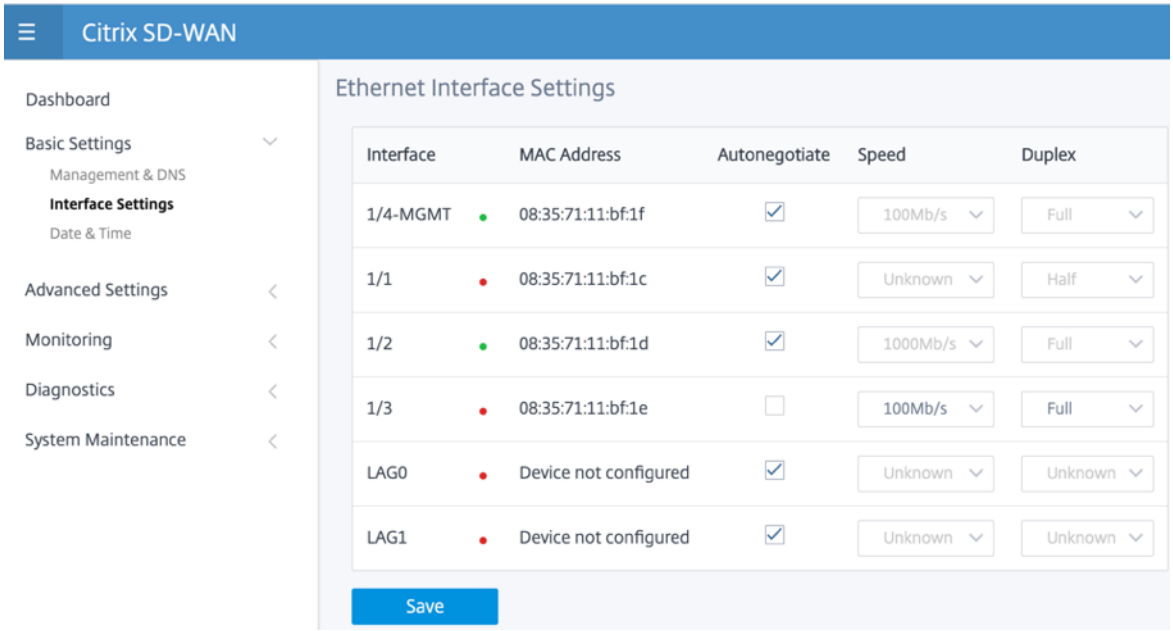
Para agregar o quitar una dirección IPv4 a la lista permitida, debe acceder a la interfaz de administración del dispositivo SD-WAN utilizando únicamente una dirección IPv4. Del mismo modo, para agregar o quitar una dirección IPv6 a la lista permitida, debe acceder a la interfaz de administración del dispositivo SD-WAN utilizando solo una dirección IPv6



Introduzca la **dirección IP, la máscara de subred** y la **dirección IP de la puerta** de enlace del dispositivo que quiere configurar. En la sección **Configuración de DNS**, proporcione los detalles del servidor DNS principal y secundario y haga clic en **Guardar**.

Configuración de la interfaz

La página **Configuración de interfaz** muestra los datos de configuración del puerto Ethernet. Los puertos que están inactivos se indican como un punto rojo contra la dirección MAC.



Grupo LAG LACP

La funcionalidad de grupos de agregación de vínculos (LAG) permite agrupar dos o más puertos en el dispositivo SD-WAN para que funcionen juntos como un solo puerto. Esto garantiza una mayor disponibilidad, redundancia de enlaces y performance mejorado.

Anteriormente, solo el modo Active-Backup era compatible en LAG. A partir de la versión 11.3 de Citrix SD-WAN, se admiten las negociaciones basadas en el protocolo 802.3AD Link Aggregation Control Protocol (LACP). El LACP es un protocolo estándar y proporciona más funcionalidad para LAG.

En el modo Active-Backup, en cualquier momento solo hay un puerto activo y los otros puertos están en modo de copia de seguridad. Los soportes activos y de copia de seguridad se basan en el paquete Kit de desarrollo de planos de datos (DPDK) para la funcionalidad de LAG.

Con el LACP, puede enviar el tráfico a través de todos los puertos simultáneamente. Como ventaja, obtiene más ancho de banda junto con el mecanismo de redundancia de enlaces. La implementación de LACP admite el modo Activo-Activo. Ahora con el modo Active-Backup, también puede seleccionar el modo Activo-Activo LACP completo desde la interfaz de usuario de SD-WAN.

La funcionalidad LAG solo está disponible en las siguientes plataformas compatibles con DPDK:

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 2100 SE/PE
- Citrix SD-WAN 4100 y 5100 SE

- Citrix SD-WAN 6100 SE

> **Nota**
>
> La funcionalidad LAG no es compatible con las plataformas VPX/VPXL.

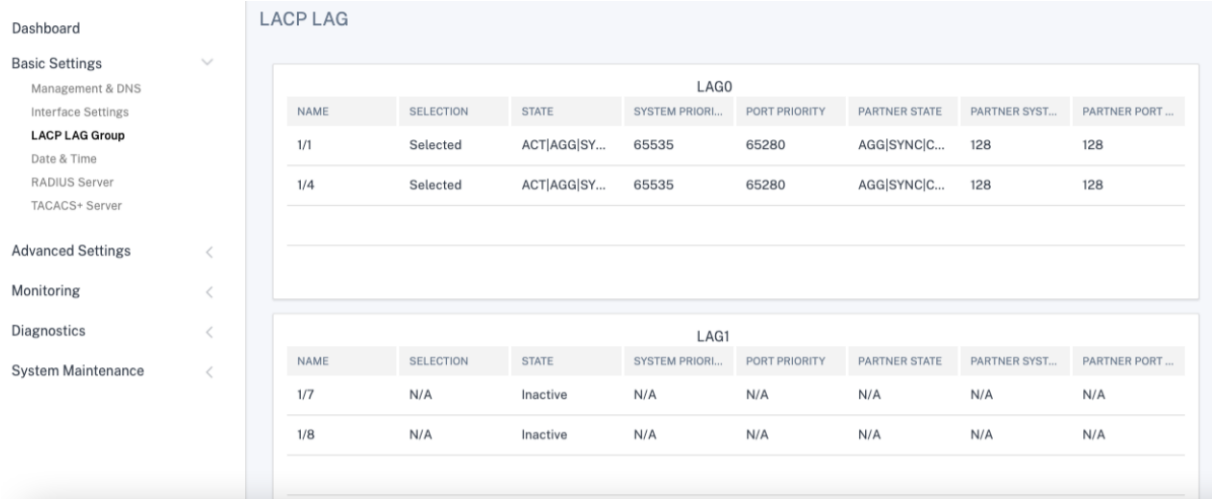
Puede crear un máximo de 4 LAG con un máximo de 4 puertos agrupados en cada LAG en los dispositivos Citrix SD-WAN.

Para los dispositivos Citrix SD-WAN 210 y 410, se puede crear un máximo de 3 LAG y para el dispositivo Citrix SD-WAN 110, se pueden crear un máximo de 2 LAG.

Puede crear LAG únicamente con la interfaz de usuario heredada o SD-WAN Orchestrator. En la nueva interfaz de usuario, solo puede ver los detalles del LAG creado.

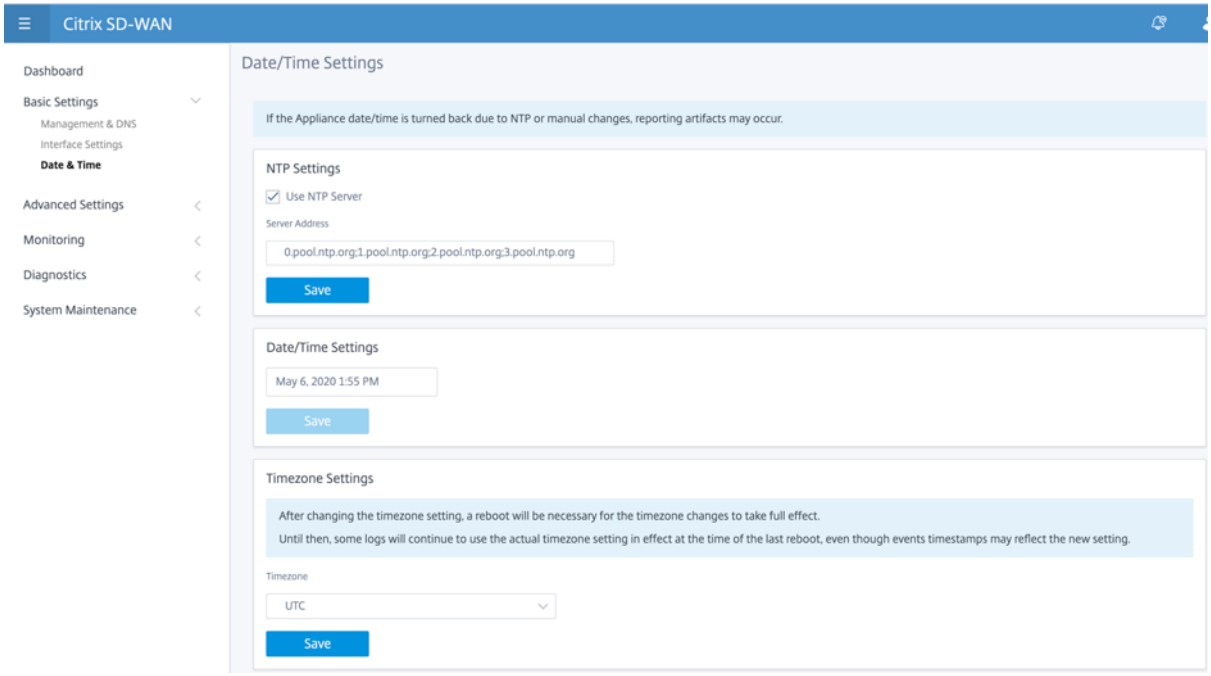
Para ver los detalles del LAG, vaya a **Configuración básica** > **Grupo LAG LACP**.

Puede ver los detalles del LAG de LACP, como el estado actual, el sistema y los detalles de prioridad de puerto de los puertos activos y asociados.



Fecha y hora

En la página Configuración de **fecha y hora**, debe establecer la fecha y la hora en el dispositivo. Para obtener más información, consulte Establecer fecha y hora.



Servidor RADIUS

Puede configurar un dispositivo SD-WAN para autenticar el acceso de usuarios con uno o varios servidores RADIUS.

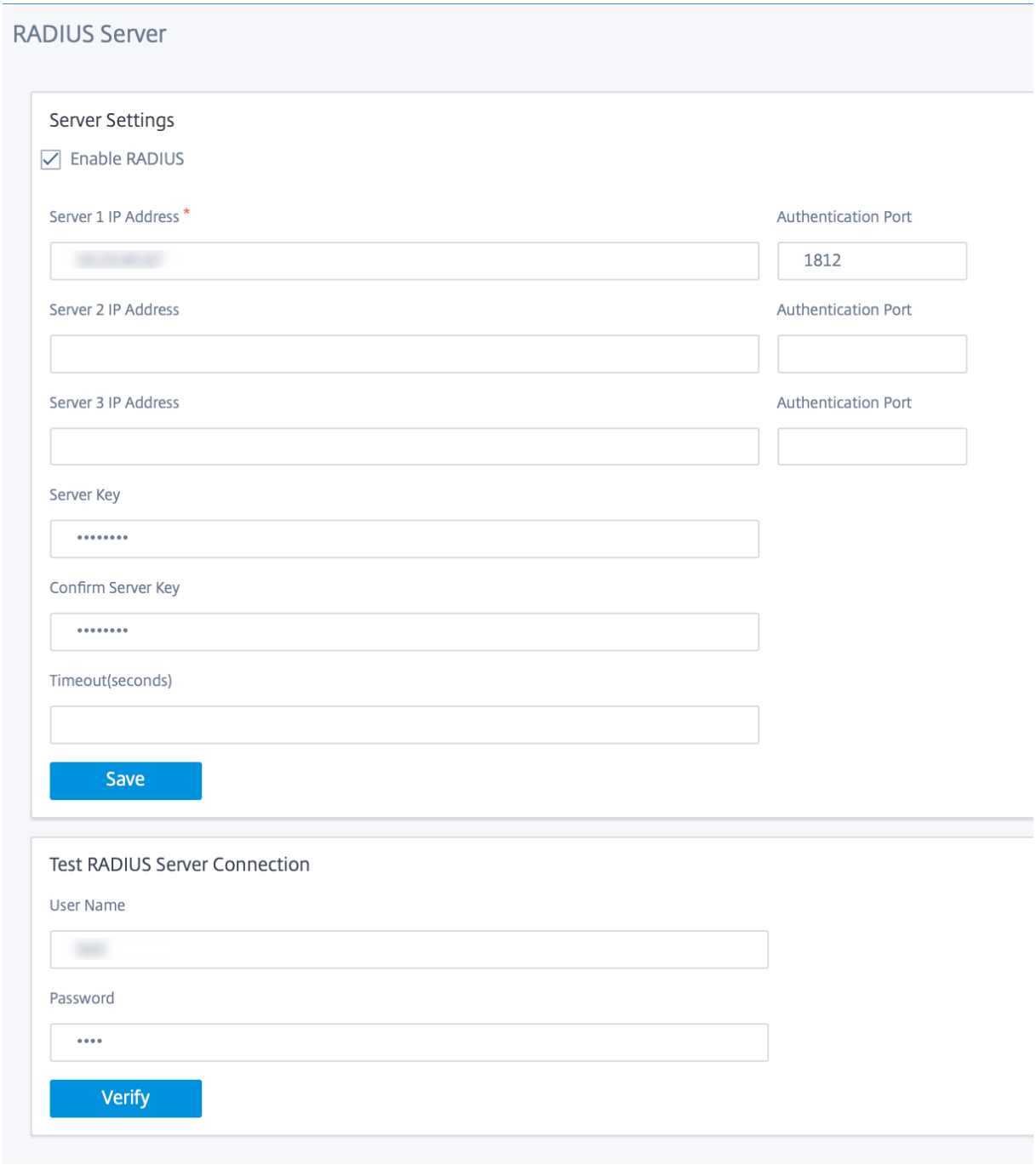
Para configurar el servidor RADIUS:

1. Marque la casilla **Habilitar RADIUS**.
2. Introduzca la **dirección IP del servidor** y el **puerto de autenticación**. Se puede configurar un máximo de tres direcciones IP de servidor.

   > **NOTA**
   >
   > Para configurar una dirección IPv6, asegúrese de que el servidor RADIUS también está configurado con una dirección IPv6.

3. Introduzca la **clave del servidor** y confirme.
4. Introduzca el valor de **Tiempo de espera** en segundos.
5. Haga clic en **Guardar**.

También puede probar la conexión del servidor RADIUS. Introduzca el **nombre de usuario** y la **contraseña**. Haga clic en **Verificar**.



Servidor TACACS+

Puede configurar un servidor TACACS+ para la autenticación. De forma similar a la autenticación RADIUS, TACACS+ utiliza una clave secreta, una dirección IP y el número de puerto. El número de puerto predeterminado es 49.

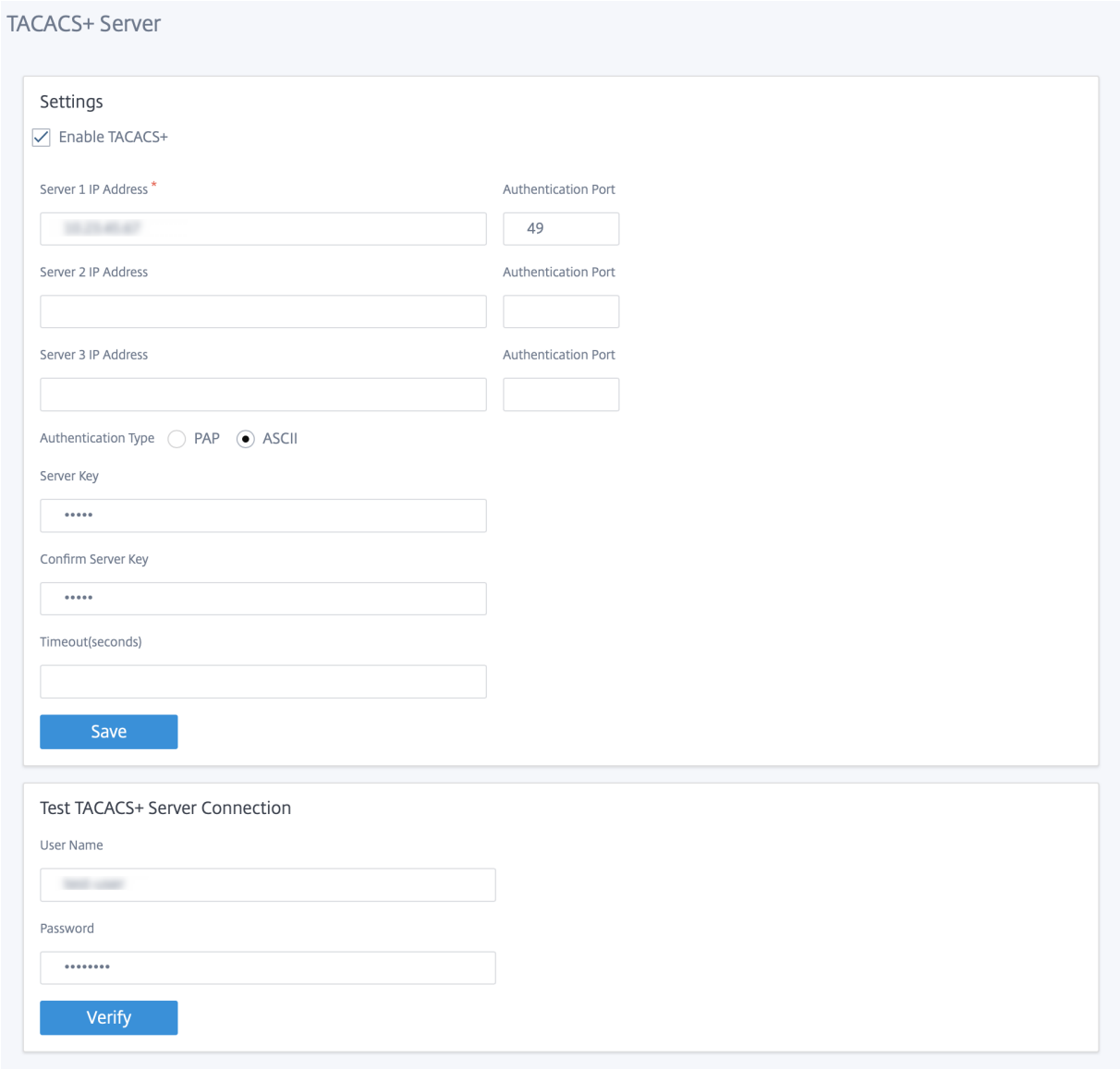
Para configurar el servidor TACACS+:

1. Seleccione la casilla **Habilitar TACACS+**.
2. Introduzca la **dirección IP del servidor** y el **puerto de autenticación**. Se puede configurar un máximo de tres direcciones IP de servidor.

   > **NOTA**
   >
   > Para configurar una dirección IPv6, asegúrese de que el servidor TACACS+ también está configurado con una dirección IPv6.

3. Seleccione **PAP** o **ASCII** como Tipo de autenticación.
   - PAP: Utiliza el Protocolo de autenticación de contraseñas (PAP) para reforzar la autenticación de usuarios mediante la asignación de un secreto compartido seguro al servidor TACACS+.
   - ASCII: utiliza el juego de caracteres ASCII para reforzar la autenticación del usuario mediante la asignación de un secreto compartido seguro al servidor TACACS+.
4. Introduzca la **clave del servidor** y confirme.
5. Introduzca el valor de **Tiempo de espera** en segundos.
6. Haga clic en **Guardar**.

También puede probar la conexión del servidor TACACS+. Introduzca el **nombre de usuario** y la **contraseña**. Haga clic en **Verificar**.



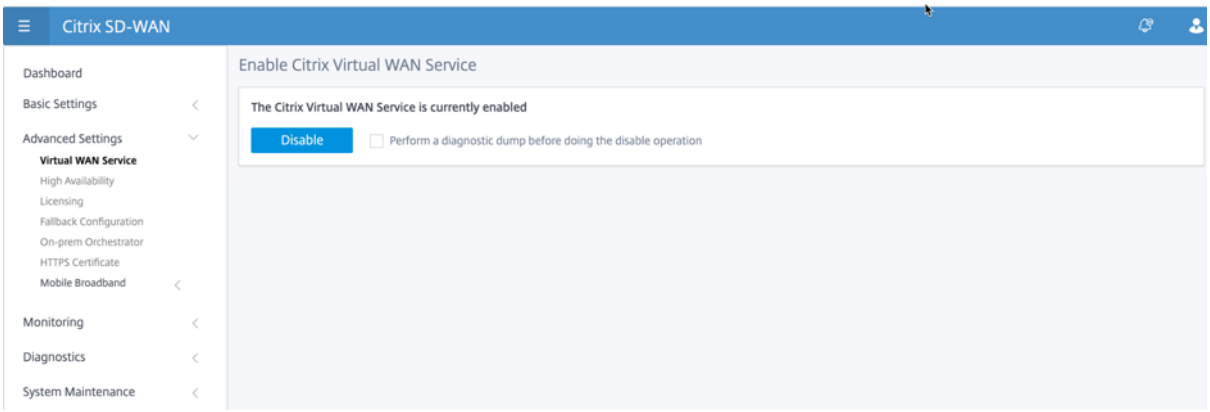
Parámetros avanzados

La **configuración avanzada** del dispositivo SD-WAN incluye la siguiente configuración de entidades.

- Servicio de Citrix Virtual WAN
- Alta disponibilidad
- Banda ancha móvil
- Licencias
- Configuración de reserva
- Certificado HTTPS
- Orchestrator en las instalaciones

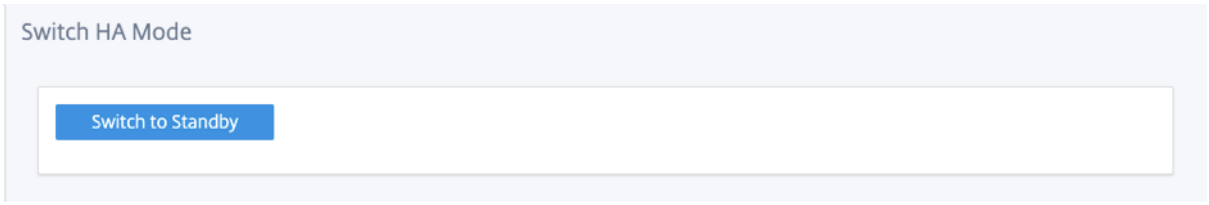
Servicio de Citrix Virtual WAN

La página **Citrix Virtual WAN Service** le permite habilitar/inhabilitar el servicio Citrix Virtual WAN Service. Para obtener más información, consulte Configurar el servicio WAN virtual.



Alta disponibilidad

Desde la página **Alta Disponibilidad**, puede alternar entre el estado activo y el estado en espera para una configuración de alta disponibilidad (HA) de SD-WAN. El estado de alta disponibilidad está disponible en el panel (si la alta disponibilidad está configurada). Para obtener más información, consulte Modo de alta disponibilidad.



Banda ancha móvil

Los dispositivos Citrix SD-WAN, como los dispositivos Citrix SD-WAN 210 SE LTE y 110 LTE Wi-Fi, tienen un módem LTE interno incorporado. También puede conectar un módem USB 3G/4G externo en los siguientes dispositivos Citrix SD-WAN.

- Citrix SD-WAN 210 SE
- Citrix SD-WAN 210 SE LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 LTE Wifi SE

CDC Ethernet, MBIM y NCM son los tres tipos de módems USB externos soportados.

Para obtener más información acerca de la configuración de LTE mediante la GUI heredada, consulte el tema siguiente:

- Configurar la funcionalidad LTE en el dispositivo 210 SE LTE
- Configurar la funcionalidad LTE en el dispositivo 110-LTE-WiFi
- Configurar módem USB LTE externo

Para un módem LTE interno, inserte la tarjeta SIM en la ranura para tarjeta SIM del dispositivo Citrix SD-WAN. Fije las antenas al dispositivo Citrix SD-WAN. Para obtener más información, consulte Instalación de antenas LTE y encender el dispositivo.

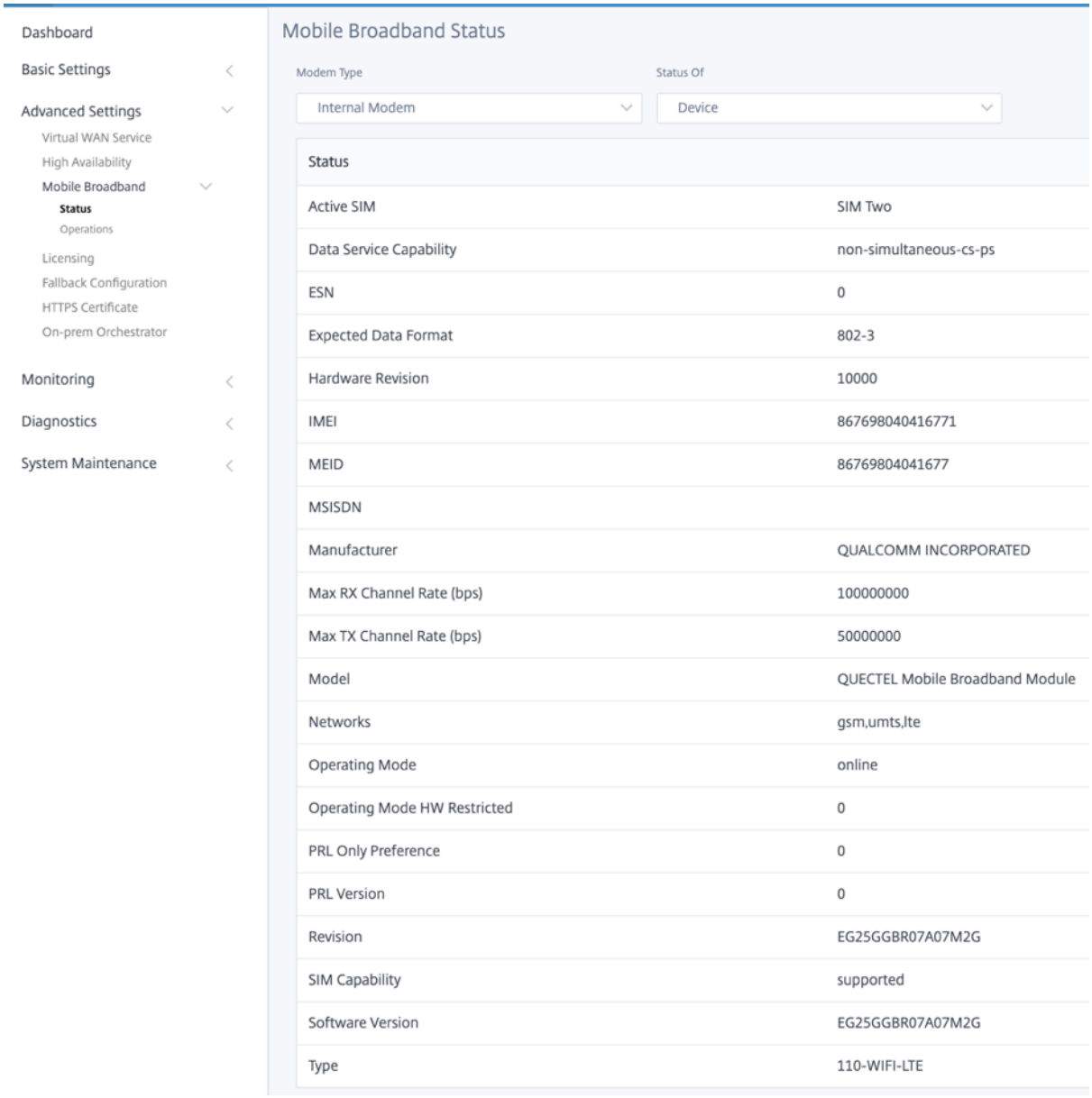
> **Nota El**
>
> dispositivo Citrix SD-WAN 110-LTE-WiFi tiene dos ranuras SIM estándar (2FF). Para utilizar SIM de tamaño Micro (3FF) y Nano (4FF), utilice un adaptador SIM. Conecte la SIM más pequeña en el adaptador. Puede obtener el adaptador de Citrix como una unidad reemplazable en campo (FRU) o del proveedor de SIM. El intercambio en caliente de SIM para el módem LTE interno solo se admite en el dispositivo Citrix SD-WAN 110-LTE-WiFi.

Requisitos previos para módem LTE externo:

- Utilice los dongles USB LTE compatibles. Los modelos de hardware de dongle compatibles son Verizon USB730L y AT&T USB800.
- Asegúrese de que se inserta una tarjeta SIM en el dongle USB LTE. Los dongles CDC Ethernet LTE están preconfigurados con una dirección IP estática, esto interfiere con la configuración y causa un fallo de conexión o una conexión intermitente, si no se inserta la tarjeta SIM.
- Antes de insertar un dongle CDC Ethernet LTE en el dispositivo SD-WAN, conecte la memoria USB externa a una máquina Windows/Linux y asegúrese de que Internet funciona correctamente con la configuración adecuada de APN y Mobile Data Roaming. Asegúrese de que el **modo de conexión** del dongle USB cambia del valor predeterminado **Manual** a **Auto**.

> **Nota**
>
> - Los dispositivos Citrix SD-WAN solo admiten un dongle USB LTE a la vez. Si hay más de un dongle USB enchufado, desconecte todos los dongles y conecte solo un dongle.
> - Los dispositivos Citrix SD-WAN no admiten el nombre de usuario y la contraseña para módems USB. Asegúrese de que la función de nombre de usuario y contraseña estén inhabilitadas en el módem durante la instalación.
> - Desconectar o reiniciar un dongle MBIM externo afecta a la sesión de datos del módem LTE interna. Este es un comportamiento esperado.
> - Cuando se conecta un módem LTE externo, el dispositivo SD-WAN tarda unos 3 minutos en reconocerlo.

Para ver el estado de la banda ancha móvil, seleccione el tipo de módem.

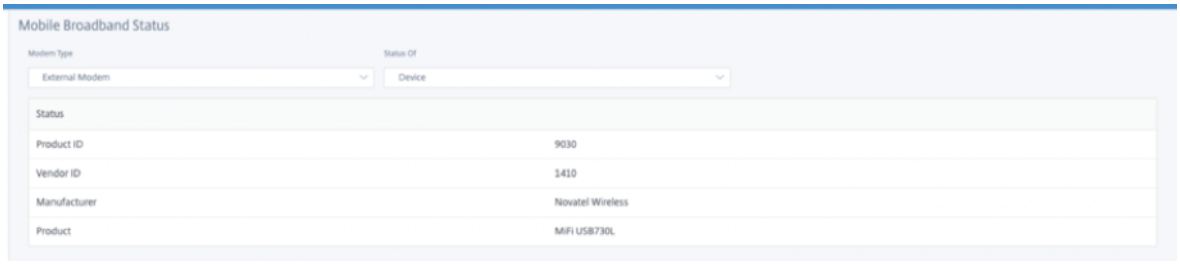


A continuación se muestra información de estado útil:

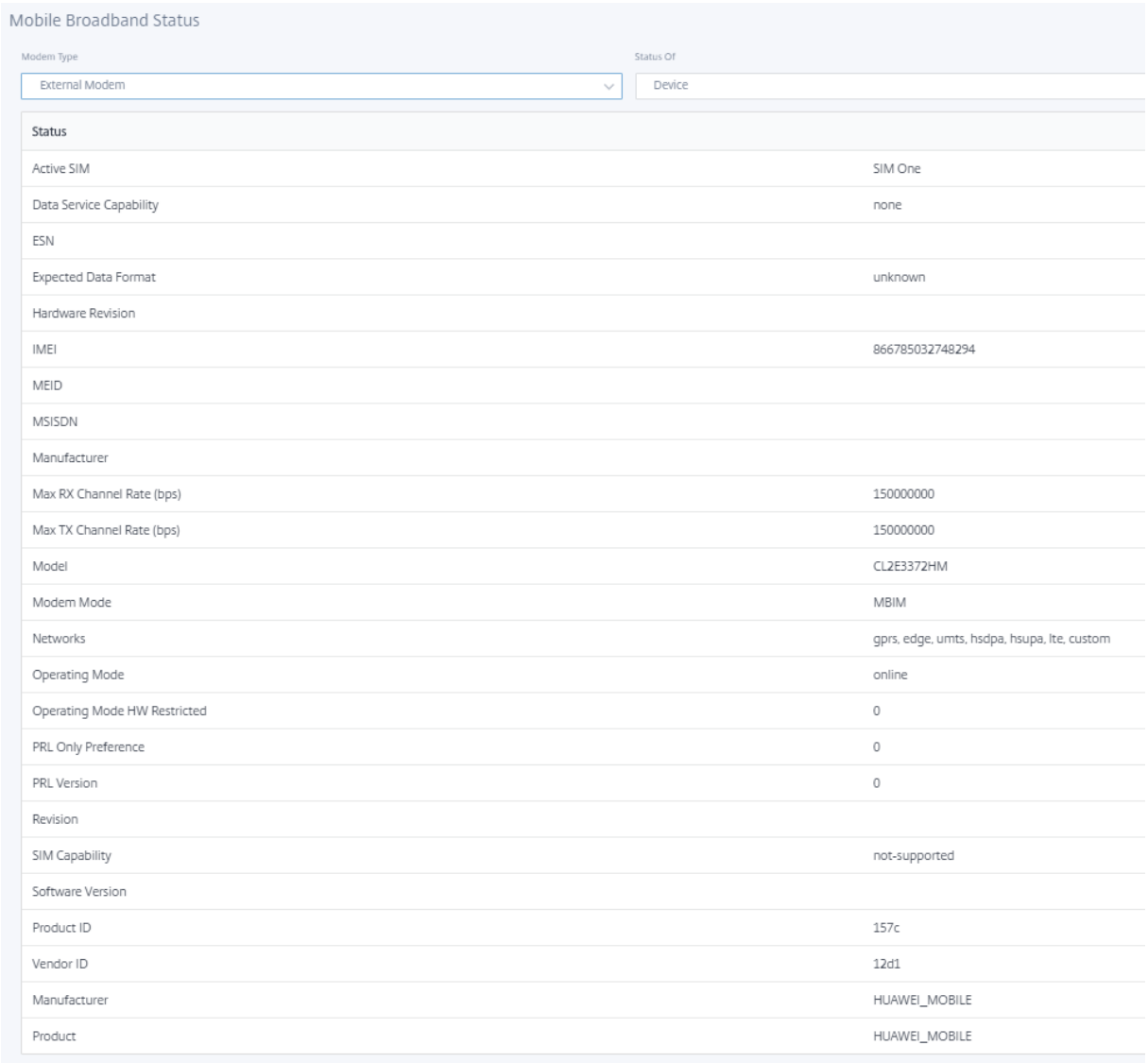
- **Tipo de módem**: Seleccione el tipo de módem como Externo o Interno. El módem interno muestra el estado en la página **Banda ancha móvil > Estado**. Todas las demás secciones, como la preferencia de SIM, la configuración de APN, Habilitar/Inhabilitar el módem, Reiniciar módem y Actualizar SIM, están disponibles en la página **Banda ancha móvil > Operaciones**.
- **SIM activa**: En cualquier momento, solo puede estar activa una SIM. Muestra la SIM que está activa actualmente.
- **Modo de funcionamiento**: muestra el estado del módem.
- **Capacidades de SIM**: Muestra si la SIM es compatible o no.
- **Modelo**: Muestra el nombre del módulo de banda ancha móvil.

Si selecciona el módem **externo**, se muestra el estado del módem externo. Pero si el módem externo no está configurado, muestra un mensaje de advertencia como el **módem seleccionado no está configurado en este dispositivo**.

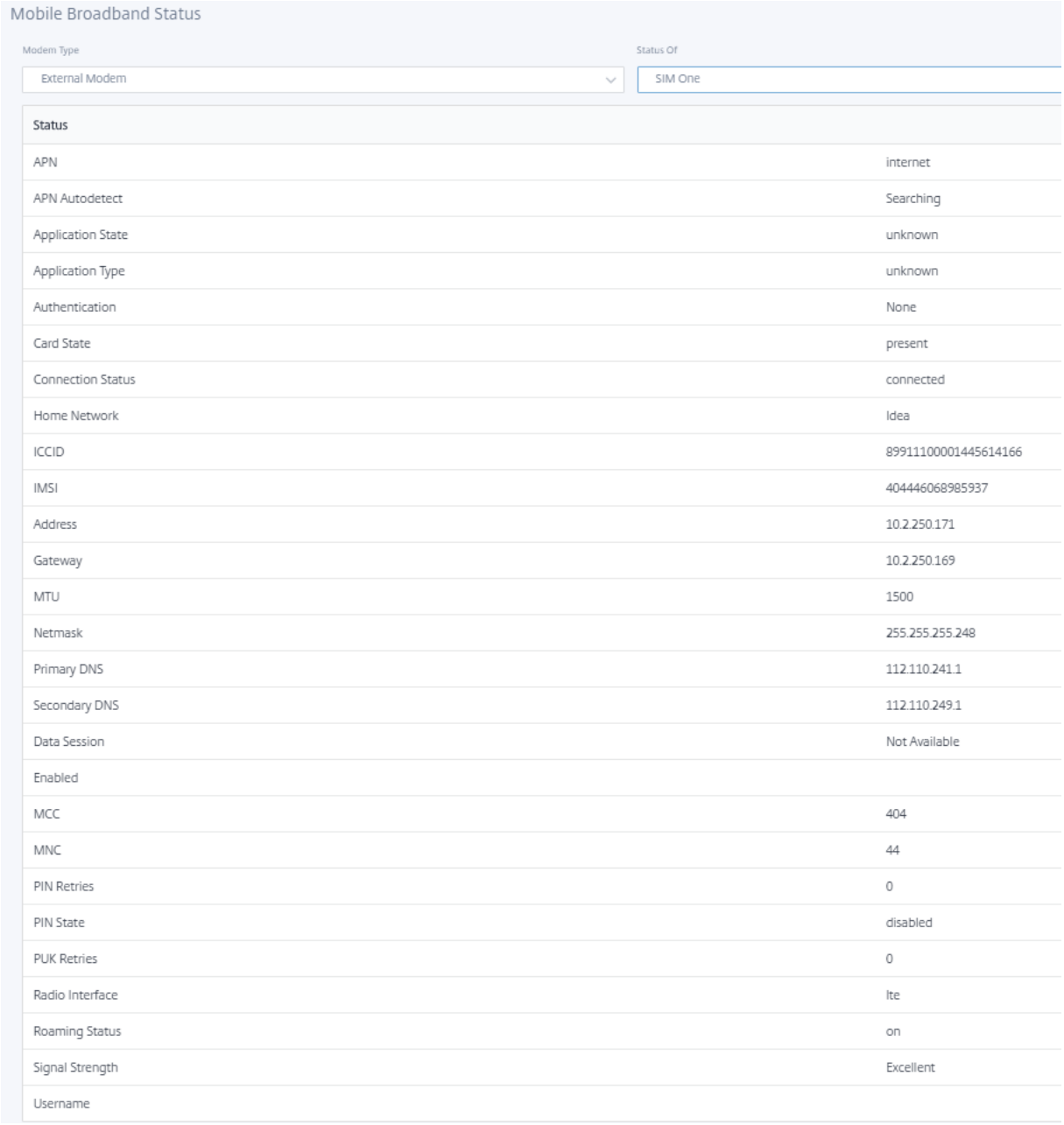
Detalles del dispositivo para el módem externo CDC Ethernet.



Detalles del dispositivo para módems externos MBIM y NCM. El campo **Modo módem** muestra el tipo de dongle externo.



Los detalles de SIM solo se muestran para módems externos MBIM y NCM.



Operaciones de banda ancha móvil Operaciones compatibles con módems internos y externos:

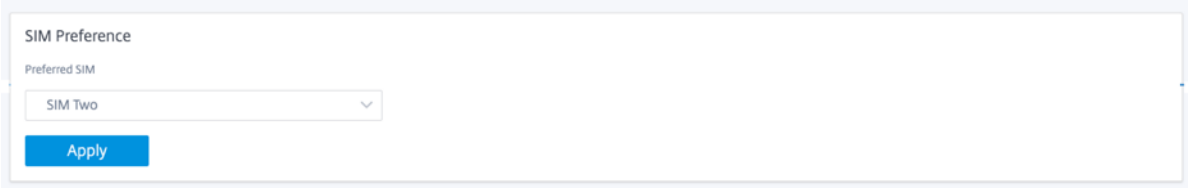
Operaciones	Módem interno	Módem externo - CDC Ethernet	Módem externo - MBIM y NCM
Preferencia de SIM	Sí - Para dispositivos que admiten doble SIM	No	No

Operaciones	Módem interno	Módem externo - CDC Ethernet	Módem externo - MBIM y NCM
PIN de la SIM	Sí	No	No
Configuración de APN	Sí	No	Sí
Configuración de la red	Sí	No	No
Itinerancia	Sí	No	No
Administrar firmware	Sí	No	No
Activar/desactivar módem	Sí	No	Sí
Reiniciar el módem	Sí	No	No
Actualizar SIM	Sí	No	No

Preferencia de SIM Puede insertar dos SIM en un dispositivo Citrix SD-WAN 110-LTE-WiFi. En un momento dado, solo hay una SIM activa. Seleccione la **preferencia de SIM**:

- **SIM One preferida**: Si se insertan dos SIM, al arrancar, el módem LTE usa SIM One, si está disponible. Cuando el módem LTE está activo y en funcionamiento, utiliza la SIM (SIM uno o SIM dos) que se pueda utilizar en ese momento y continuará utilizándola hasta que la SIM esté activa.
- **SIM Dos preferidos**: si se insertan dos SIM, al arrancar el módem LTE utiliza SIM Two, si está disponible. Cuando el módem LTE está activo y en funcionamiento, utiliza la SIM (SIM uno o SIM dos) que se pueda utilizar en ese momento y continuará utilizándola hasta que la SIM esté activa.
- **SIM One**: Solo se utiliza SIM One, independientemente del estado de la SIM en ambas ranuras SIM. SIM One siempre está activo.
- **SIM Dos**: Solo se utiliza SIM Two, independientemente del estado de la SIM en ambas ranuras SIM. SIM dos siempre está activo.

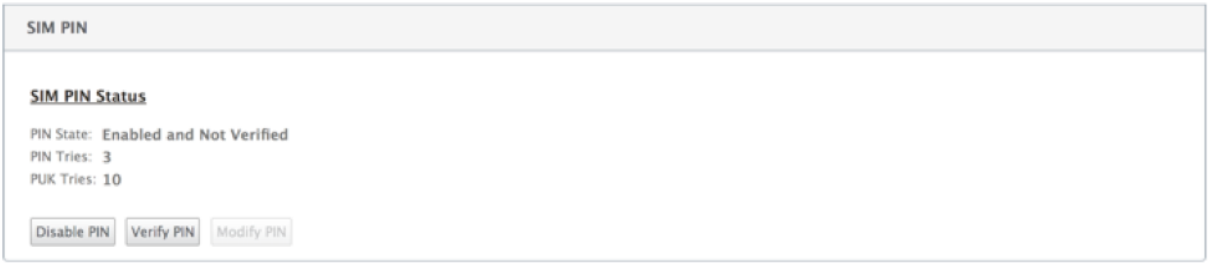
> **Nota**
>
> La opción Preferencia de SIM no está disponible para el dispositivo Wi-Fi Citrix SD-WAN 210-SE LTE, ya que solo tiene una ranura para tarjeta SIM.



PIN de la SIM

Si ha insertado una tarjeta SIM bloqueada con un PIN, el estado de la SIM está en estado **Habilitado y No verificado**. No puede usar la tarjeta SIM hasta que se verifique con el PIN de la SIM. Puede obtener el PIN de la tarjeta SIM del operador.

Para realizar operaciones PIN de la SIM, vaya a **Configuración avanzada > Banda ancha móvil > Operaciones > Estado del PIN de la SIM**.



Puede realizar las siguientes operaciones:

- **Verificar el PIN de la SIM**: haga clic en **Verificar**. Introduzca el PIN de la SIM proporcionado por el operador y haga clic en **Verificar**. El estado cambia a **Habilitado y Verificado**.
- **Habilitar el PIN de la SIM**: puede habilitar el PIN de la SIM para una SIM que tenga el PIN de la SIM inhabilitado. Haga clic en **Activar**. Introduzca el PIN de la tarjeta SIM proporcionado por el operador y haga clic en **Habilitar**. Si el estado del PIN de la SIM cambia a **Habilitado y No Verificado**, significa que el PIN no está verificado y que no puede realizar ninguna operación relacionada con LTE hasta que se verifique el PIN. Haga clic en **Verificar**. Introduzca el PIN de la SIM proporcionado por el operador y haga clic en **Verificar**.
- **Inhabilitar el PIN de la SIM**: puede optar por desactivar la funcionalidad de PIN de la SIM para una SIM para la que el PIN de la SIM está habilitado y verificado. Haga clic en **Inhabilitar**. Introduzca el PIN de la SIM y haga clic en **Inhabilitar**.
- **Modificar el PIN de la SIM**: una vez que el PIN esté en estado Habilitado y Verificado, puede elegir cambiar el PIN. Haga clic en **Modificar**. Introduzca el PIN de la tarjeta SIM proporcionado por el operador. Introduzca el nuevo PIN de la SIM y confírmelo. Haga clic en **Modificar**.
- **Desbloquear SIM**: Si olvida el PIN de la SIM, puede restablecer el PIN de la SIM utilizando el PUK de la SIM obtenido del operador. Para desbloquear una SIM, haga clic en **Desbloquear**. Introduzca el PIN de la SIM y el PUK de la SIM obtenidos del operador y haga clic en **Desbloquear**.

  > **Nota**
  >
  > La tarjeta SIM se bloquea permanentemente con 10 intentos fallidos de PUK, mientras desbloquea la SIM. Póngase en contacto con el proveedor de servicios del operador para obtener una nueva tarjeta SIM.

Configuración de APN

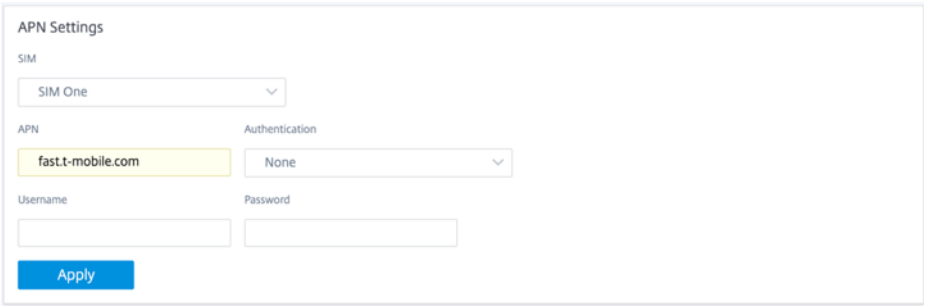
1. Para configurar los ajustes de APN, vaya a **Configuración avanzada > Banda ancha móvil > Operaciones** y vaya a la sección **Configuración de APN**.

   > **Nota**
   >
   > Obtenga la información de APN del transportista.

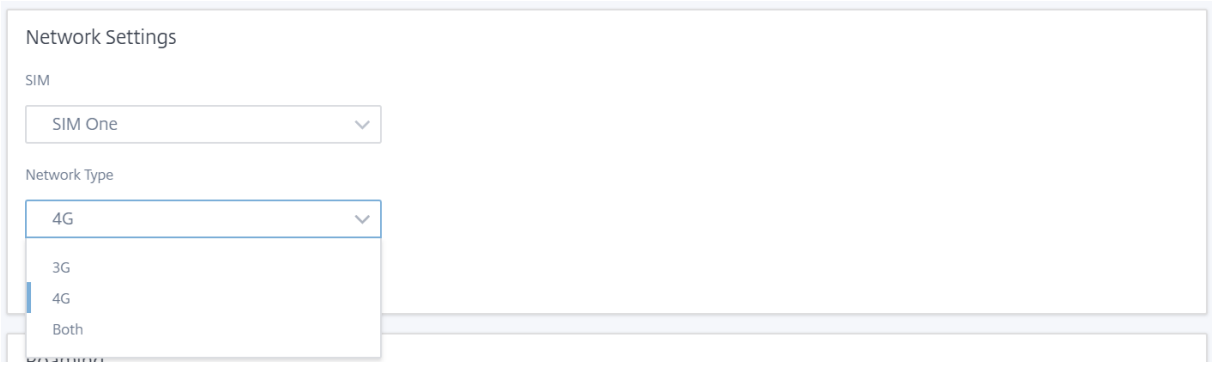
2. Seleccione la tarjeta SIM, introduzca el **APN, el nombre de usuario, la contraseña** y la **autenticación** proporcionados por el operador. Puede elegir entre los protocolos de autenticación PAP, CHAP y PAPCHAP. Si el transportista no ha proporcionado ningún tipo de autenticación, establezca en **Ninguno**.

   > **Nota**
   >
   > Todos estos campos son opcionales.

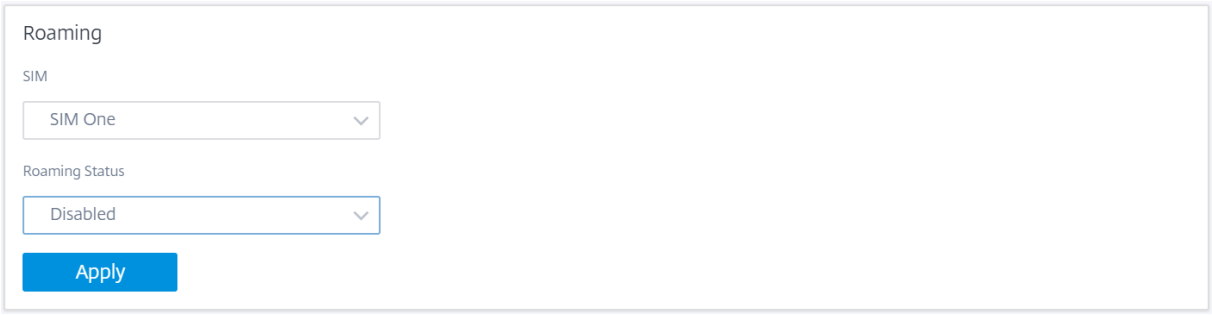
3. Haga clic en **Aplicar**.



Configuración de la red Puede seleccionar la red móvil en los dispositivos Citrix SD-WAN que admitan el módem LTE interno. Las redes admitidas son 3G, 4G o ambas.



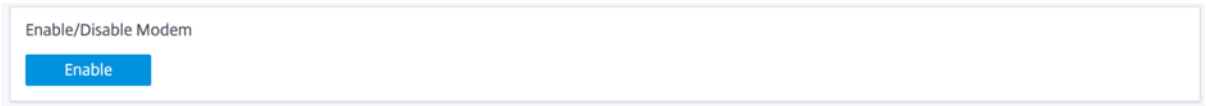
Itinerancia La opción de itinerancia está habilitada de forma predeterminada en sus dispositivos LTE, puede optar por inhabilitarla.



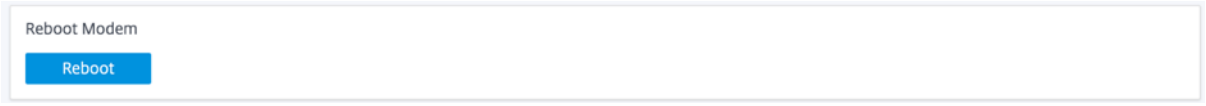
Administrar firmware

Todos los dispositivos habilitados para LTE tienen un conjunto de firmware disponible. Puede seleccionar de la lista existente de firmware o cargar un firmware y aplicarlo. Si no está seguro de qué firmware usar, seleccione la opción **AUTO-SIM**. La opción AUTO-SIM permite al módem LTE elegir el firmware más coincidente basado en la tarjeta SIM insertada.

Activar/desactivar módem Habilitar/inhabilitar el módem según su intención de utilizar la funcionalidad LTE. De forma predeterminada, el módem LTE está habilitado.

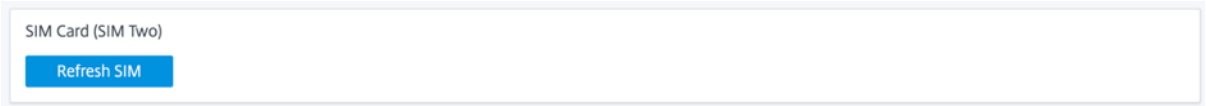


Reiniciar el módem Reinicia el módem. La operación de reinicio puede tardar hasta 7 minutos en completarse.



Actualizar SIM Utilice la opción **Actualizar SIM** cuando el módem LTE-WiFi no detecte correctamente la tarjeta SIM.

> **Nota**
>
> La operación Actualizar SIM solo se aplica a la SIM activa.



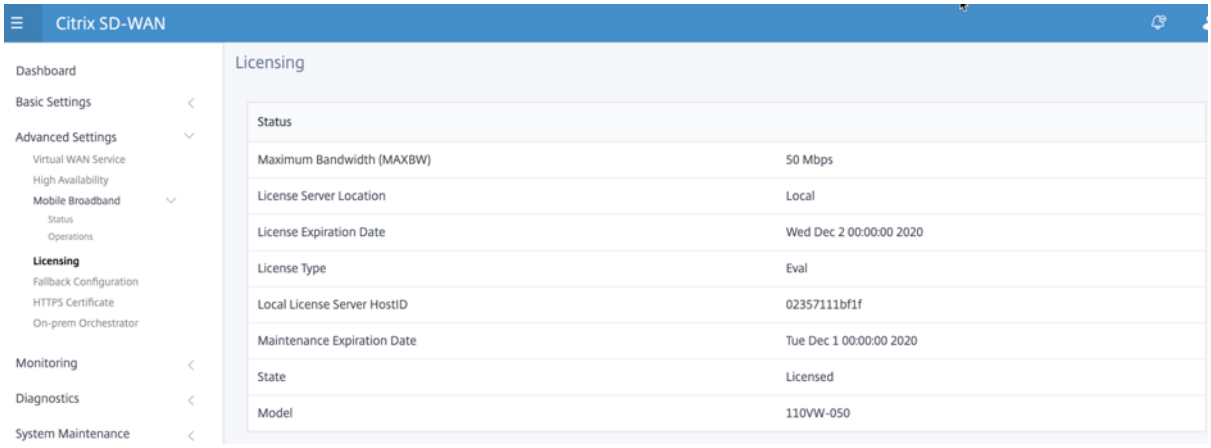
Puede ver y administrar de forma remota todos los sitios LTE de la red mediante el Citrix SD-WAN Center. Para obtener más información, consulte Administración remota de sitios LTE.

Para obtener más información sobre la configuración LTE, consulte Configurar la funcionalidad LTE en el dispositivo 110-LTE-WiFi y Configurar la funcionalidad LTE en el dispositivo 210 SE LTE.

Para obtener información sobre cómo configurar un módem LTE externo, consulte Configurar un módem LTE USB externo.

Licencias

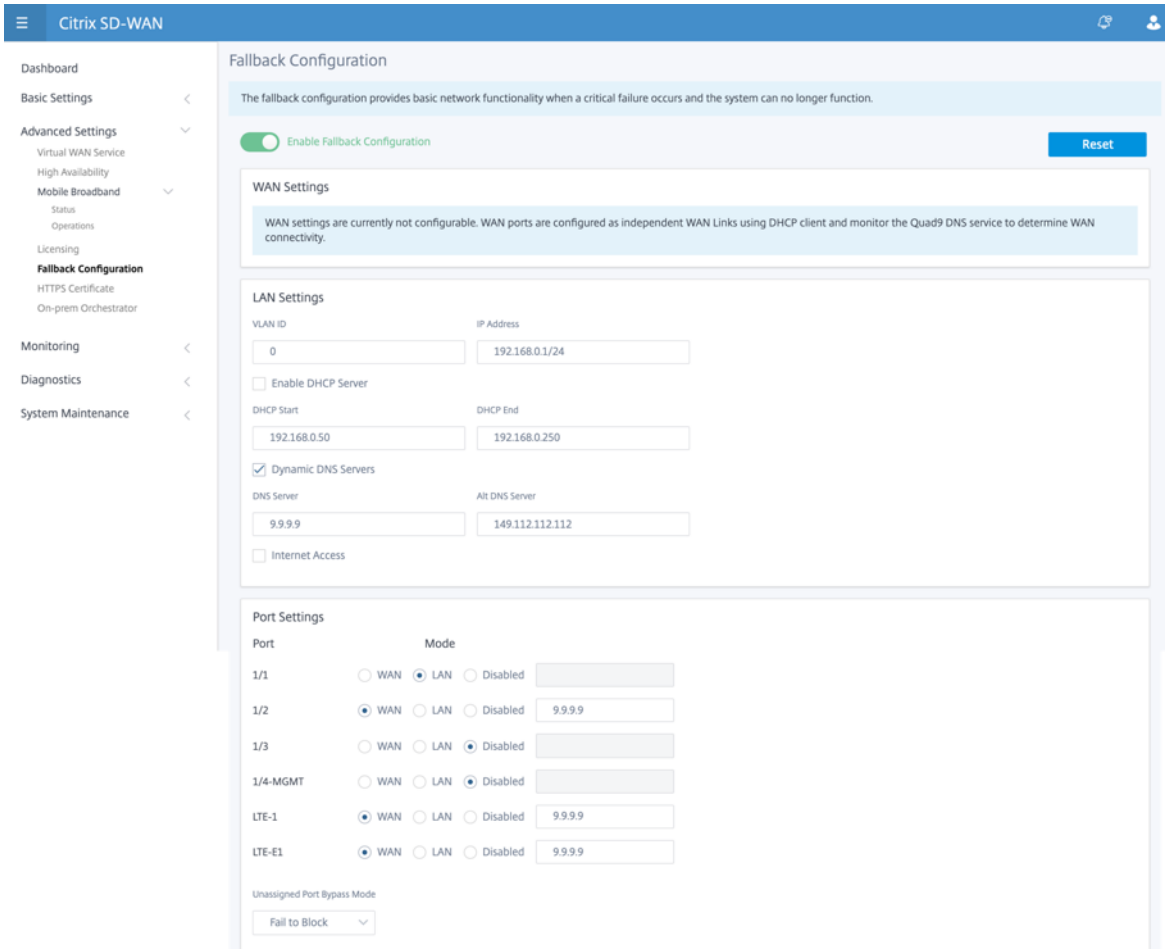
La página **Licencias** muestra los detalles de la licencia, como la ubicación del servidor, el modelo, el tipo de licencia, etc.



> **Nota**
>
> Al instalar y aplicar una licencia desde el Centro de SD-WAN, asegúrese de que el dispositivo específico admite la modificación del dispositivo SD-WAN que quiere habilitar y de que dispone de la versión de software correcta disponible.

Configuración predeterminada/reserva

La página **Configuración Predeterminada/Fallback** muestra los datos de configuración de reserva almacenados. Si la configuración de reserva está inhabilitada, puede activarla activando el conmutador **Activar configuración de reserva**.

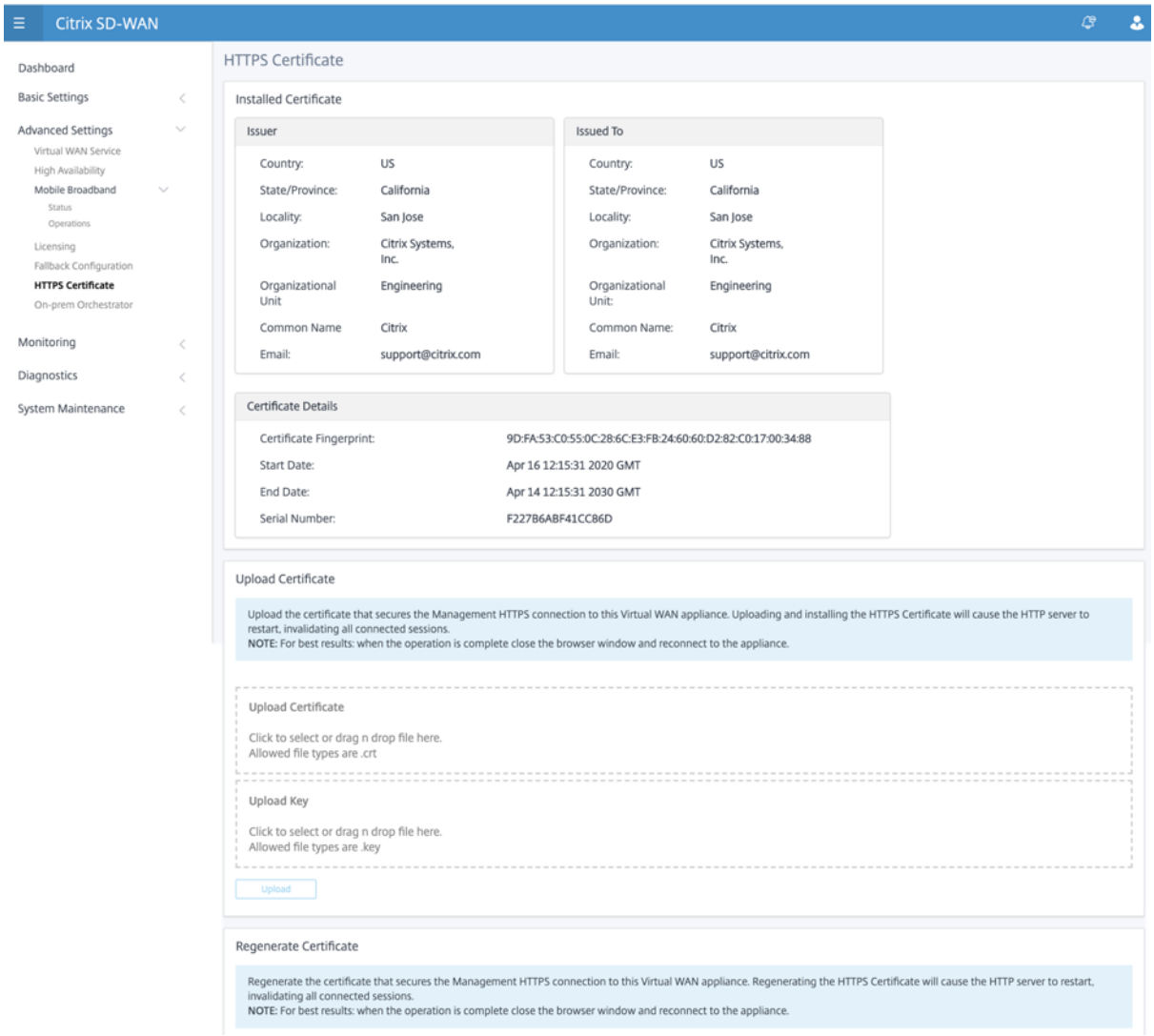


> **Nota**
>
> Las interfaces LTE no se pueden configurar con dirección IP estática.

Para obtener más información, consulte Configuración de default/Fallback.

Certificado HTTPS

Se requiere un certificado HTTPS para establecer una conexión segura. La página **Certificado HTTPS** muestra los detalles del certificado HTTPS que ya está instalado. Para obtener más información, consulte Certificados HTTPS.



Orchestrator en las instalaciones

Orchestrator local de Citrix SD-WAN es la versión de software local de Citrix SD-WAN Orchestrator Service. Orchestrator local de Citrix SD-WAN proporciona una plataforma de administración de vidrio de un solo panel para que los socios de Citrix administren varios clientes de forma centralizada, con controles de acceso adecuados basados en roles.

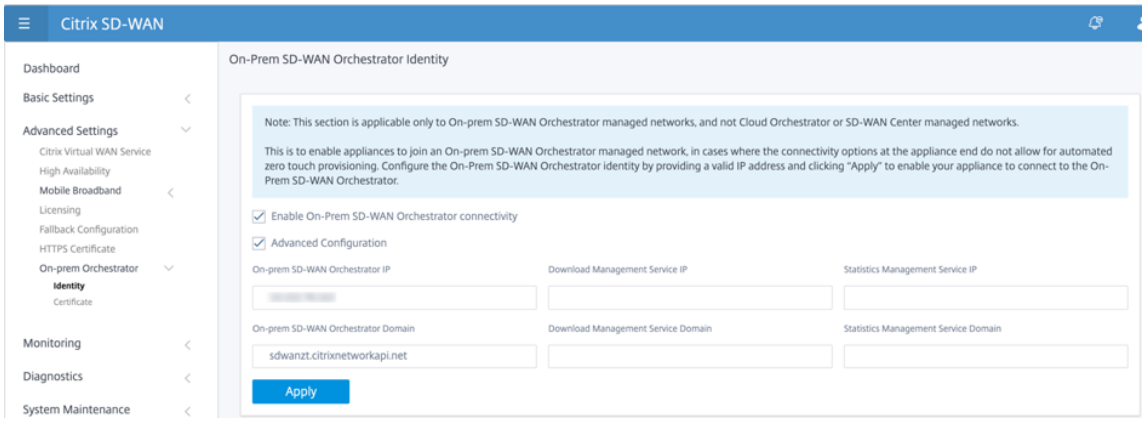
Puede establecer una conexión entre el dispositivo Citrix SD-WAN y Orchestrator local de Citrix SD-WAN habilitando la conectividad de Orchestrator y especificando la identidad Orchestrator local de SD-WAN.

> **Nota**
>
> - La función de **configuración de Orchestrator local de SD-WAN en el dispositivo SD-WAN**

> es un habilitador para Orchestrator local de Citrix SD-WAN. La función de configuración de Orchestrator local de Citrix SD-WAN en el dispositivo SD-WAN no está disponible actualmente. Está destinado a un lanzamiento futuro.
> - La implementación sin táctiles no funcionará si la **configuración de SD-WAN Orchestrator en la función SD-WAN del dispositivo SD-WAN** está configurada en los dispositivos SD-WAN.

Para habilitar la conectividad de Orchestrator:

1. En la GUI del dispositivo, vaya a **Configuración avanzada > Orchestrator local > Identidad**.
2. Marque la casilla**Habilitar conectividad de SD-WAN Orchestrator** en las instalaciones.



3. Introduzca la dirección IP SD-WAN Orchestrator local o el dominio o ambos (dirección IP y dominio) para la configuración.

   Si el cliente configura solo Dominio, debe asegurarse de agregar registro DNS en su servidor DNS local y debe configurar la dirección IP del servidor DNS en dispositivos SD-WAN. Para configurar, vaya a **Configuración > Adaptadores de red > Dirección IP**.

   Por ejemplo, si el dominio SD-WAN Orchestrator local está configurado como citrix.com. debe crear un registro DNS en el servidor DNS para la siguiente dirección IP de FQDN y SD-WAN Orchestrator:

   - download.citrix.com
   - sdwanzt.citrix.com
   - sdwan-home.citrix.com

   En caso de configuración avanzada:

   Por ejemplo: si el dominio Orchestrator local está configurado como **citrix.com**, el dominio del servicio de administración de descargas se configura como **download.citrix**.com y el dominio del servicio de administración de estadísticas se configura como **statistics.citrix.com**. A continuación, debe crear un registro DNS en el servidor DNS para el siguiente FQDN y la dirección IP correspondiente:

- download.citrix.com
- sdwanzt.citrix.com
- statistics.citrix.com

Orchestrator local puede admitir servicios en ejecución como descarga, estadísticas en instancia de servidor independiente, para permitir una mejor escalabilidad para redes grandes. Puede seleccionar la **Configuración avanzada** y configurar el Servicio de **administración de descargas y el servicio de administración de estadísticas**.

Marque la casilla**Configuración avanzada** y proporcione los siguientes detalles:

- **Servicio de administración de descargas IP/Dominio**: Proporcione la dirección IP /dominio que ayuda a descargar los aspectos de descarga de software SD-WAN y configuración, a una instancia de servidor independiente, para permitir una mejor escalabilidad para redes grandes.
- **Servicio de administración de estadísticas IP/dominio**: Proporcione la dirección IP/dominio que ayuda a descargar la recopilación y administración de estadísticas de SD-WAN desde dispositivos, a una instancia de servidor independiente, para permitir una mejor escalabilidad para redes grandes.

4. Haga clic en **Aplicar**.

   Para regenerar, descargar y cargar el dispositivo SD-WAN o el certificado SD-WAN Orchestrator en las instalaciones, vaya a **Configuración avanzada > Orchestrator local > Certificado**.

   Si el **tipo de autenticación** local de Orchestrator está inhabilitado, el dispositivo puede conectarse al Orchestrator local mediante el **modo**Sin autenticación**, Autenticación**unidireccional o Autenticación**bidireccional**.

   Si el **tipo de autenticación** de Orchestrator On-prem está habilitado, el dispositivo solo puede conectarse al Orchestrator local mediante **autenticación bidireccional**.

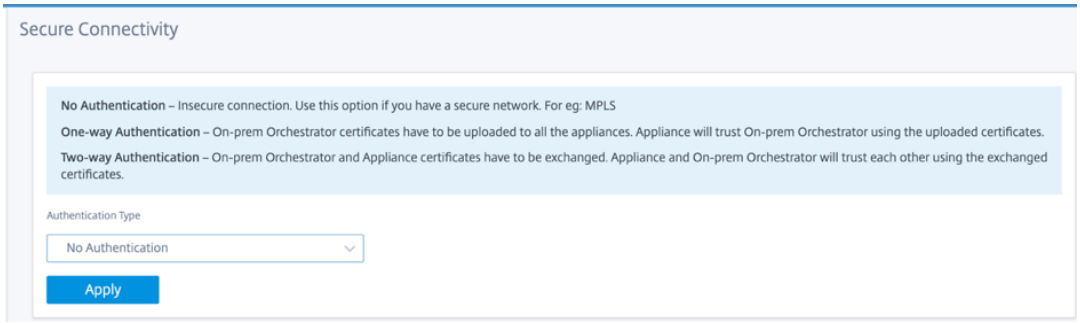
   Al inhabilitar el **tipo de autenticación** en Orchestrator local del estado de habilitación, los dispositivos existentes en el modo Autenticación unidireccional pasan al estado desconectado. Los clientes deben cambiar el Tipo de autenticación del dispositivo a Autenticación bidireccional y cargar el certificado del dispositivo SD-WAN en Orchestrator local para conectarlo.

   > **Nota**
   >
   > - Los certificados generados son certificados autofirmados X509.
   > - El cliente debe volver a generar los certificados si el certificado ha caducado o está comprometido.
   > - La validez del certificado es de 10 años.
   > - Puede ver los detalles del certificado como, huella digital, fecha de inicio y fecha de finalización

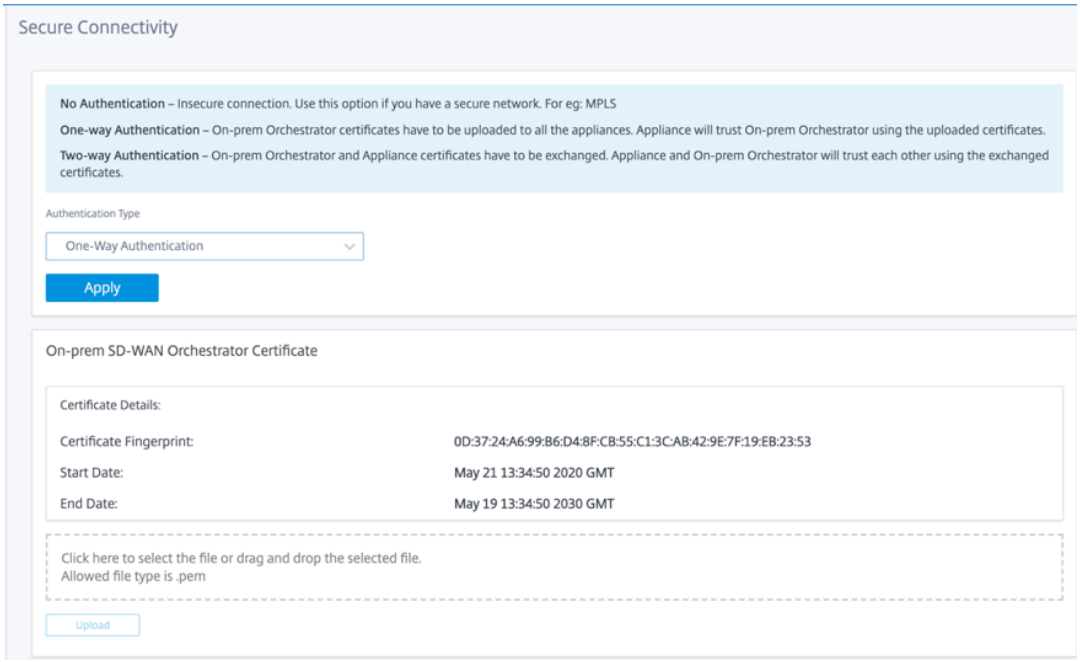
> - El cliente debe asegurarse de que los certificados se regeneran e intercambian entre Orchestrator local y el dispositivo SD-WAN para evitar la pérdida de conectividad del dispositivo con el orquestador local.

5. Seleccione el **tipo de autenticación**. A continuación se indican los tipos de autenticación que se admiten entre el dispositivo SD-WAN y la conectividad Orchestrator local de SD-WAN:

   - **Sin autenticación**: No hay autenticación entre el Orchestrator local de SD-WAN y el dispositivo SD-WAN, y no es necesario utilizar el dispositivo SD-WAN ni el certificado de Orchestrator local de SD-WAN. Pero puede usar esta opción si tiene una red segura como MPLS.

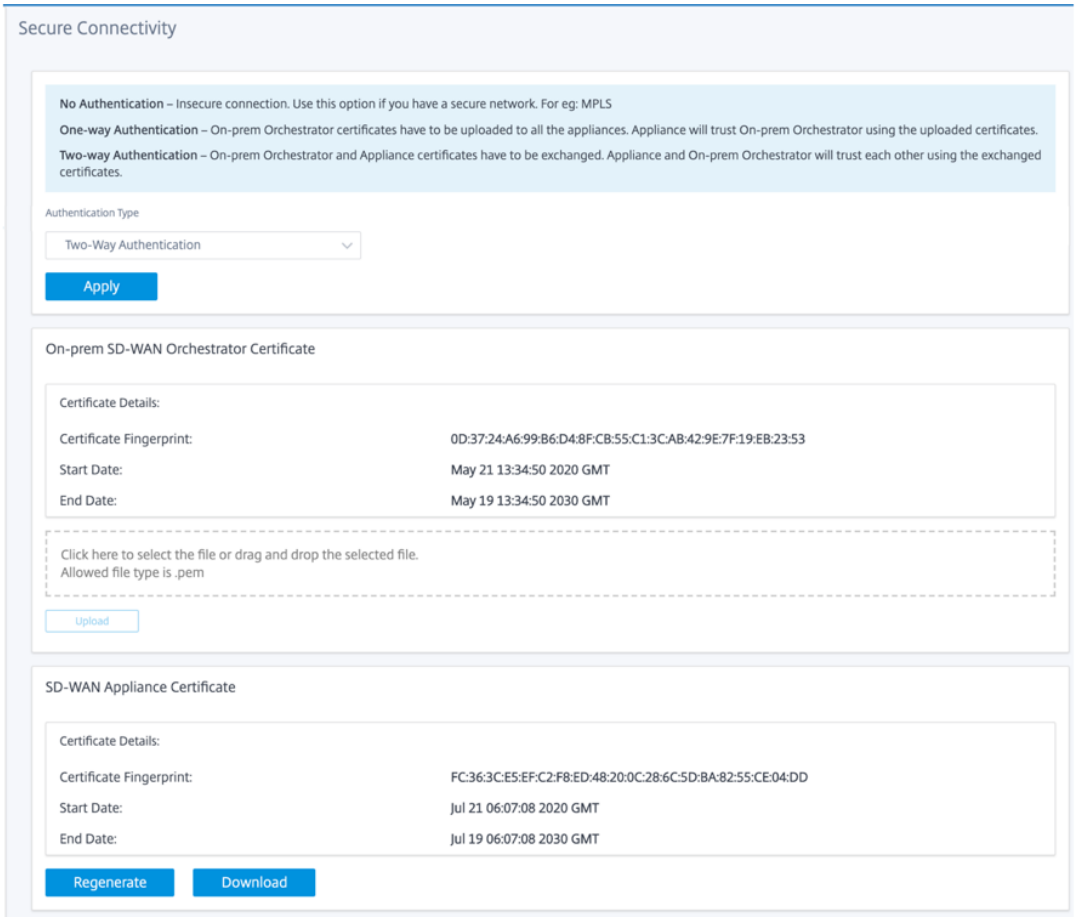


   - **Autenticación unidireccional**: Al seleccionar el tipo de autenticación unidireccional, debe cargar el certificado Orchestrator local. Descargue Orchestrator local desde Orchestrator local y haga clic en Cargar. El dispositivo SD-WAN confía en Orchestrator local mediante los certificados cargados.



   - **Autenticación bidireccional**: Los certificados Orchestrator local y Appliance deben intercambiarse entre sí. Para la **autenticación bidireccional**, debe regenerar, descargar y car-

gar el certificado del dispositivo SD-WAN en el Orchestrator local. El dispositivo SD-WAN y Orchestrator local confían entre sí mediante los certificados intercambiados.



> **Nota**
>
> Se recomienda utilizar solo Autenticación unidireccional o Autenticación bidireccional. Si no hubo Autenticación, debe elegir el servidor DNS seguro.

Para inhabilitar la conectividad local de SD-WAN Orchestrator, desactive **Habilitar conectividad de SD-WAN Orchestrator local** y haga clic en **Aplicar**. Para convertir la red administrada Orchestrator local a Cloud Orchestrator o MCN Managed Network, debe inhabilitar la conectividad Orchestrator local de SD-WAN y debe realizar el restablecimiento de la configuración. Para restablecer la configuración, vaya a **Configuración > Mantenimiento del sistema > Restablecimiento de configuración**.

Actualizar y degradar

- Después de actualizar el dispositivo SD-WAN de la versión de software 11.1.1/11.2.0/10.2.7 a 11.2.1, debe intercambiar los certificados de dispositivo y Orchestrator local.

- Después de degradar la versión de software del dispositivo SD-WAN de 11.2.1 a 11.1.1/11.2.0/10.2.7, debe volver a aplicar la configuración de identidad en la interfaz de usuario del dispositivo Citrix SD-WAN. Si hay algún problema relacionado con la configuración local de SD-WAN Orchestrator o la conectividad del dispositivo SD-WAN, desactive la conectividad SD-WAN Orchestrator local y, a continuación, vuelva a habilitar la conectividad Orchestrator local de SD-WAN.

El tipo de autenticación de SD-WAN Orchestrator en las instalaciones debe estar inhabilitado para administrar los dispositivos SD-WAN que ejecutan la versión de software 10.2.7/11.1.1/11.2.0.

Supervisión

En la sección Supervisión, puede ver las estadísticas de **Protocolo de resolución de direcciones (ARP), Ruta, Ethernet, Ethernet MAC** junto con **enlaces WAN de cliente DHCP, vínculos WAN SLAAC, Servidor/retransmisión DHCP, Conexiones de firewall, Flujos** y **estadísticas DNS**.

- **Estadísticas MAC de ARP, Route, Ethernet y Ethernet**: Puede ver la información estadística de ARP, Route, Ethernet y Ethernet MAC. Mediante la información estadística, puede verificar cualquier error de tráfico o interfaz. Para obtener más información, consulte Visualización de información estadística.
- **Vínculos WAN de cliente DHCP**: La página Enlaces WAN del Cliente DHCP proporciona el estado de las IP aprendidas. Puede solicitar la renovación de la IP, que actualiza el tiempo de concesión. También puede elegir **Liberar Renovación**, que emite una nueva dirección IP con una nueva concesión. Para obtener más información, consulte Supervisión de vínculos WAN de clientes DHCP.
- **Vínculos WAN**de SLAAC: la página de vínculos WAN de SLAAC proporciona detalles sobre las direcciones IPv6 que SLAAC asigna a las interfaces virtuales. También puede seleccionar **Release Renew** para permitir que SLAAC asigne una nueva dirección IP o la misma dirección IP con una nueva concesión al cliente IPv6.
- **Servidor/retransmisión DHCP**: puede utilizar el dispositivo SD-WAN como servidores DHCP o agentes de retransmisión DHCP.
  - La función de servidor DHCP permite a los dispositivos de la misma red que la interfaz LAN/WAN del dispositivo SD-WAN obtener su configuración IP del dispositivo SD-WAN.
  - La función de retransmisión DHCP permite a los dispositivos SD-WAN reenviar paquetes DHCP entre el cliente DHCP y el servidor.

  Para obtener más información, consulte Servidor DHCP y retransmisión DHCP.
- **Conexiones de firewall**: La página **Conexiones de firewall** proporciona las estadísticas de conexión. Puede ver cómo actúan las directivas de firewall sobre el tráfico de cada aplicación.

Para obtener más información, consulte Visualización de estadísticas de firewall.

- **Flujos**: La sección **Flujos** proporciona instrucciones básicas para ver información de flujo WAN virtual. Para obtener más información, consulte Visualización de información de flujo.
- **Estadísticas de proxy DNS**: esta página proporciona detalles sobre los proxies DNS configurados. Haga clic en **Actualizar** para obtener los datos actuales. Para obtener más información, consulte Sistema de nombres de dominio.

Diagnóstico

La sección **Diagnósticos** proporciona las opciones para probar e investigar problemas de conectividad. Para obtener más información, consulte Diagnóstico.

> **Nota**
>
> Para el dispositivo Citrix SD-WAN 110, solo puede estar presente un paquete de diagnóstico a la vez. Para el dispositivo Citrix SD-WAN 210, se permite un máximo de cinco paquetes de diagnóstico.

Mantenimiento del sistema

Utilice la sección **Mantenimiento del sistema** para realizar actividades de mantenimiento. La página **Mantenimiento del sistema** contiene las siguientes opciones:

- **Eliminar archivos**: puede eliminar archivos de registro, archivos de copia de seguridad y bases de datos archivadas. Seleccione el archivo que quiere eliminar en el menú desplegable y haga clic en el botón Eliminar.
- **Reiniciar el sistema**: puede reiniciar el servicio WAN virtual o reiniciar el sistema.
- **Administración de cambios locales: el proceso de administración de cambios locales** permite cargar un nuevo paquete de dispositivo en este dispositivo individual.
- **Restablecimiento de configuración**: puede restablecer la configuración. Esta opción borra los datos de usuario, los registros, el historial y los datos de configuración local de este dispositivo.
- Restablecimiento de**fábrica**: utilice la opción de **restablecimiento de fábrica** para restablecer el dispositivo SD-WAN a la versión enviada.

> **Nota**
>
> Todas estas funciones ya se explican en detalle en la documentación existente de SD-WAN.

Plataformas no compatibles

La nueva interfaz de usuario no admite los siguientes dispositivos SD-WAN:

- Citrix SD-WAN 1000 SE/PE unidad de red
- Citrix SD-WAN 2000 SE / PE
- Citrix SD-WAN 4000 SE

Impacto de la actualización de Citrix SD-WAN 11.5

August 26, 2022

- Citrix SD-WAN 11.5.0 es una versión de disponibilidad limitada, recomendada y admitida solo para implementaciones de producción/clientes específicos.
- La versión 11.5.0 de SD-WAN no admite implementaciones de Advanced Edition (AE), Premium Edition (PE) ni de optimización de WAN.
- SD-WAN 11.5.0 solo admite las plataformas mencionadas en los modelos de plataforma y paquetes de software de SD-WAN.
- SD-WAN 11.5.0 no admite Citrix SD-WAN Center ni Citrix SD-WAN Orchestrator para entornos locales.
- El firmware de SD-WAN 11.5.0 no está disponible en la página de descargas de Citrix.
- La versión SD-WAN 11.5.0 solo está disponible a través de Citrix SD-WAN Orchestrator Service y solo en los POP geográficos seleccionados.
- Asegúrese de obtener las aprobaciones y la orientación necesarias de Citrix Product Management/Citrix Support antes de implementar 11.5.0 en cualquier red de producción.

Requisitos del sistema

August 26, 2022

Requisitos de hardware

Las instrucciones para instalar dispositivos SD-WAN se proporcionan en Configuración de los dispositivos SD-WAN.

Requisitos de firmware

Todos los modelos de dispositivos Citrix SD-WAN en un entorno de WAN virtual deben ejecutar la misma versión de firmware de Citrix SD-WAN.

> **Nota**
>
> Los dispositivos que ejecutan versiones anteriores de software no pueden establecer una conexión Virtual Path con el dispositivo que ejecuta la versión 11.4 de SD-WAN. Para obtener más información, póngase en contacto con el equipo de soporte técnico de Citrix.

Requisitos de software

A partir de la versión 11.5 de SD-WAN, las licencias de los dispositivos SD-WAN se administran a través de Citrix SD-WAN Orchestrator Service. Para obtener más información sobre los requisitos de licencia, consulte Licencias.

Requisitos del explorador

Los exploradores deben tener habilitadas las cookies y JavaScript instalado y habilitado.

La interfaz web de administración de SD-WAN es compatible con los siguientes exploradores:

- Mozilla Firefox 49+
- Google Chrome 51+
- Microsoft Edge 13+

Los exploradores compatibles deben tener las cookies habilitadas y JavaScript instalado y habilitado.

Hipervisor

Citrix SD-WAN SE/PE VPX se puede configurar en los siguientes hipervisores:

- Servidor VMware ESXi, versión 5.5.0 o posterior.
- Citrix Hypervisor 6.5 o posterior.
- Microsoft Hyper-V 2012 R2 o posterior.
- Linux KVM

Plataforma en la nube

Citrix SD-WAN SE/PE VPX se puede configurar en las siguientes plataformas en la nube:

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

Modelos de plataforma SD-WAN

September 26, 2023

Los siguientes son los modelos de dispositivos de hardware de modificación estándar de SD-WAN compatibles:

MODELO DE PLATAFORMA SD-WAN SE	ROL
110-SE/110-LTE-WiFi/110-WiFi-SE	Dispositivo de sucursal pequeña
210-SE/210-SE LTE	Dispositivo de sucursal pequeña
1100-SE	Dispositivo de sucursal grande
2100-SE	Dispositivo de sucursal grande
4100-SE	Centro de datos: dispositivo de nodo de control maestro (MCN)
5100-SE	Centro de datos: dispositivo de nodo de control maestro (MCN)
6100-SE	Centro de datos: dispositivo de nodo de control maestro (MCN)

Dispositivos virtuales SD-WAN VPX (SD-WAN VPX-SE)

Los siguientes son los modelos de dispositivo virtual VPX de SD-WAN (VPX-SE) compatibles:

MODELOS DE PLATAFORMA SD-WAN VPX-SE	ROL
VPX 20-SE	MCN o dispositivo cliente, sucursal pequeña
VPX 50-SE	MCN o dispositivo cliente, sucursal pequeña
VPX 100-SE	MCN o dispositivo cliente, sucursal pequeña
VPX 200-SE	MCN o dispositivo cliente, sucursal pequeña
VPX 500-SE	MCN o dispositivo cliente, sucursal pequeña
VPX 1000-SE	MCN o dispositivo cliente, sucursal pequeña

Para obtener más información, consulte los requisitos previos de Citrix SD-WAN Virtual VPX Standard Edition.

Rutas de actualización

August 26, 2022

En la tabla siguiente se proporcionan detalles de todas las versiones de software de Citrix SD-WAN a las que se puede actualizar desde las versiones anteriores.

SD-WAN	11.1	11.0	10.2	10.1	10	9.3.5	9.3.4	9.3	9.2
SD-WAN 11.0	✓								
SD-WAN 10.2	✓	✓							
SD-WAN 10.1	✓	✓	✓						
SD-WAN 10	✓	✓	✓	✓					
SD-WAN 9.3.5	✓	✓	✓	✓	✓				
SD-WAN 9.3.4	—	—	—	—	—	✓			
SD-WAN 9.3	—	—	—	—	—	✓	✓		
SD-WAN 9.2	—	—	—	—	—	✓	✓	✓	
SD-WAN 9.1	—	—	—	—	—	✓	✓	✓	✓

La información sobre las rutas de actualización también está disponible en la Guía de actualización de Citrix.

> **Nota**
>
> - Se recomienda a los clientes que actualicen desde la versión 9.3.x de Citrix SD-WAN que actualicen a la versión 10.2.8 antes de actualizar a cualquier versión principal.
> - Al realizar la actualización del software, asegúrese de que se ha completado la puesta en escena en todos los sitios conectados antes de activarla. Si la activación se realiza antes de que finalice el ensayo mediante la activación de Ignorar incompleto, es posible que la ruta virtual no presente MCN para los sitios en los que el ensayo aún estaba en curso. Para recuperar la red, es necesario realizar manualmente la administración de cambios locales para esos sitios.
> - A partir de la versión 11.0.0 de Citrix SD-WAN, el núcleo operativo subyacente para el software SD-WAN se actualiza a una versión más reciente. Requiere un reinicio automático para que se realice durante el proceso de actualización. Como resultado, el tiempo esperado para actualizar cada dispositivo aumenta en aproximadamente 100 segundos. Además, al

> incluir el nuevo sistema operativo, el tamaño del paquete de actualización transferido a cada dispositivo de sucursal aumenta en aproximadamente 90 MB.

Configuración

September 26, 2023

Después de instalar el software y las licencias de SD-WAN, puede configurar la configuración del dispositivo SD-WAN para empezar a administrar la red y la implementación.

Configuración inicial

Estos procedimientos deben completarse para cada dispositivo que quiera agregar a su SD-WAN. En consecuencia, este proceso requerirá cierta coordinación con los administradores del sitio en toda la red para garantizar que los dispositivos estén preparados y listos para implementarse en el momento adecuado. Sin embargo, una vez configurado e implementado el nodo de control maestro (MCN), puede agregar dispositivos cliente (nodos cliente) a su SD-WAN en cualquier momento.

Para cada dispositivo que quiera agregar a su WAN virtual, deberá hacer lo siguiente.

1. Configure el hardware del dispositivo SD-WAN y cualquier dispositivo virtual VPX SD-WAN (SD-WAN VPX-VW) que vaya a implementar.
2. Establezca la dirección IP de administración para el dispositivo y verifique la conexión.
3. Establezca la fecha y la hora del dispositivo.
4. Establezca el umbral de **tiempo de espera** de la sesión de consola en un valor máximo o alto.

   > **Advertencia**
   >
   > Si se cierra el tiempo de espera de la sesión de consola o se cierra la sesión de la interfaz web de administración antes de guardar la configuración, se perderán los cambios de configuración que no se hayan guardado. A continuación, debe volver a iniciar sesión en el sistema y repetir el procedimiento de configuración desde el principio. Por este motivo, se recomienda encarecidamente establecer el intervalo de tiempo de **espera** de la sesión de consola en un valor alto al crear o modificar un paquete de configuración o realizar otras tareas complejas.

5. Cargue e instale el archivo de licencia de software en el dispositivo.

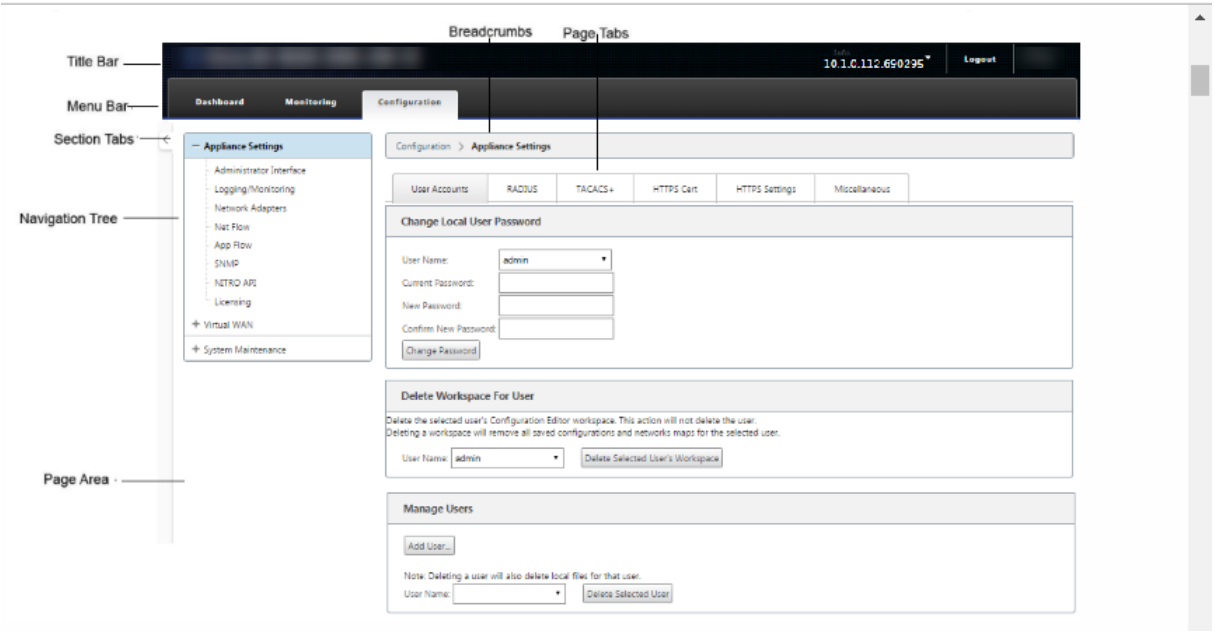
Para obtener instrucciones sobre la instalación de un dispositivo virtual SD-WAN (SD-WAN VPX), consulte las secciones siguientes:

- Acerca de SD-WAN VPX.
- Instalación e implementación de un VPX-SE de SD-WAN en ESXi.

Introducción al diseño de la Interfaz Web (UI)

En esta sección se proporcionan instrucciones básicas de navegación y una hoja de ruta de navegación de la jerarquía de páginas de la interfaz de administración web de SD-WAN.

Navegación básica En la ilustración siguiente se describen los elementos básicos de navegación de la interfaz de administración web y la terminología utilizada para identificarlos.



Los elementos básicos de navegación son los siguientes:

- **Barra de título**: Muestra el número de modelo del dispositivo, la dirección IP del host del dispositivo, la versión del paquete de software que se ejecuta actualmente en el dispositivo y el nombre de usuario de la sesión de inicio de sesión actual. La barra de título también contiene el botón **Cerrar** sesión para finalizar la sesión.
- **Barra de menús principal**: Es la barra que se muestra debajo de la barra de título en todas las pantallas de la interfaz web de administración. Contiene las fichas de sección para mostrar el árbol de navegación y las páginas de una sección seleccionada.
- **Fichas** de sección: las fichas de sección se encuentran en la barra de menú principal en la parte superior de la página. Estas son las categorías de nivel superior de las páginas y formularios de la Interfaz de administración web. Cada sección tiene su propio árbol de navegación para nave-

gar por la jerarquía de páginas de esa sección. Haga clic en una ficha de **sección** para mostrar el árbol de navegación de esa sección.

- **Árbol de navegación**: El árbol de navegación se encuentra en el panel izquierdo, debajo de la barra de menús principal. Muestra el árbol de navegación de una sección. Haga clic en una ficha de sección para mostrar el árbol de navegación de esa sección. El árbol de navegación ofrece las siguientes opciones de visualización y navegación:
  - Haga clic en una ficha de sección para mostrar el árbol de navegación y la jerarquía de páginas de esa sección.
  - Haga clic en + (signo más) junto a una rama del árbol para mostrar las páginas disponibles para ese tema de la rama.
  - Haga clic en el nombre de una página para mostrarla en el área de página.
  - Haga clic en —(signo menos) junto a un elemento de rama para cerrar la rama.
- **Breadcrumbs**: Muestra la ruta de navegación a la página actual. Las migas de pan se encuentran en la parte superior del área de la página, justo debajo de la barra del menú principal. Los enlaces de navegación activa se muestran en color azul. El nombre de la página actual aparece en negrita negra.
- **Área de página**: Es la visualización de la página y el área de trabajo de la página seleccionada. Seleccione un elemento del árbol de navegación para mostrar la página predeterminada de ese elemento.
- **Fichas de página**: Algunas páginas contienen fichas para mostrar más páginas secundarias para ese tema o formulario de configuración. Estos se encuentran en la parte superior del área de la página, justo debajo de la pantalla de migas de pan. A veces (al igual que en el Asistente para **administración de cambios**), las fichas se encuentran en el panel izquierdo del área de página, entre el árbol de navegación y el área de trabajo de la página.
- Cambio de**tamaño del área de página:** en algunas páginas, puede aumentar o reducir el ancho del área de página (o de sus secciones) para mostrar más campos en una tabla o formulario. En este caso, hay una barra de redimensionamiento vertical gris en el borde derecho de un panel, formulario o tabla del área de página. Pase el cursor sobre la barra de cambio de tamaño hasta que el cursor cambie a una flecha bidireccional. A continuación, haga clic y arrastre la barra hacia la derecha o hacia la izquierda para aumentar o reducir el ancho del área.

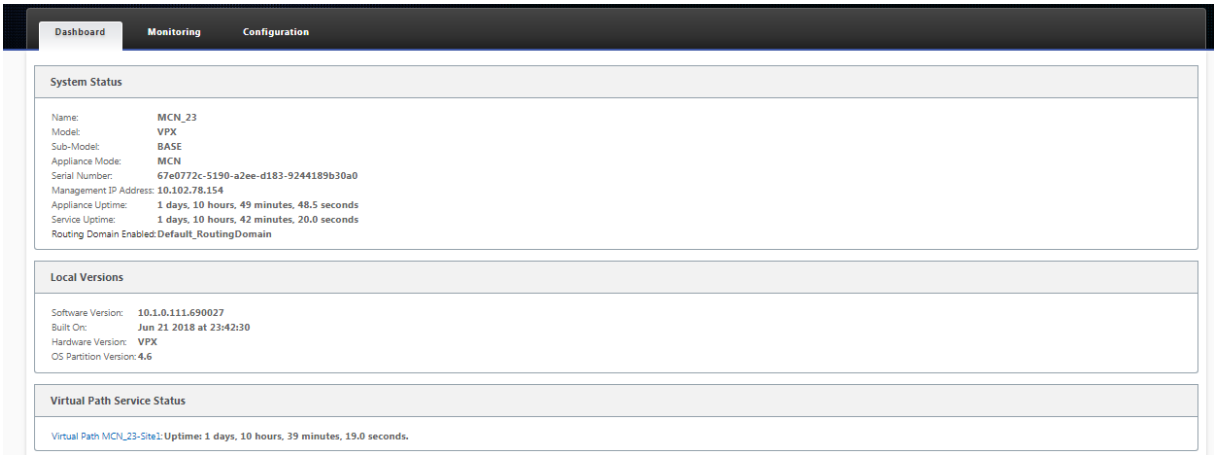
  Si la barra de cambio de tamaño no está disponible para una página, puede hacer clic y arrastrar el borde derecho del explorador para mostrar la página completa.

Panel de interfaz de administración web Haga clic en la ficha de la sección **Panel** de control para mostrar la información básica del dispositivo local.

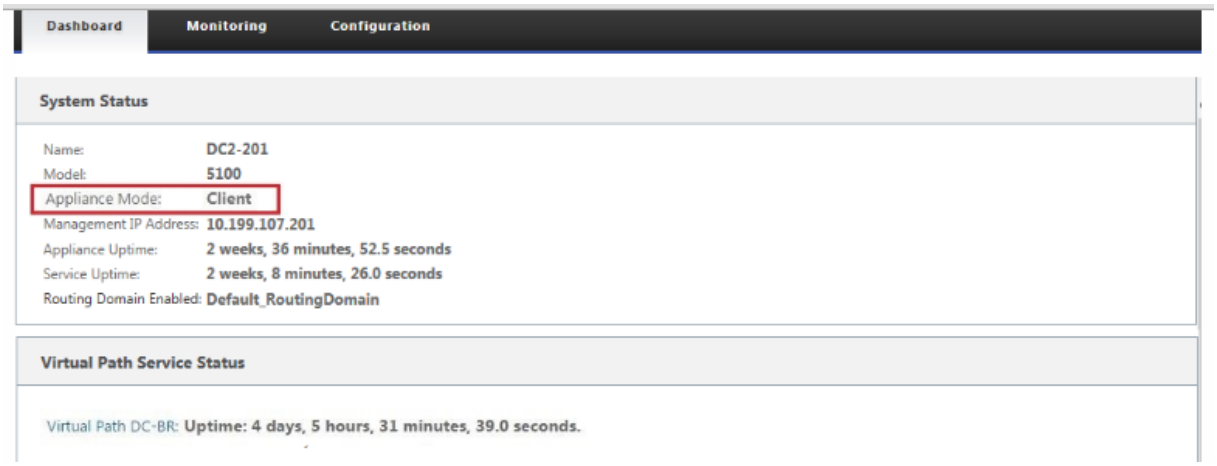
La página **Panel** de control muestra la siguiente información básica del dispositivo:

- Estado del sistema
- Estado del servicio Virtual Path
- Información de versión del paquete de software del dispositivo local

En la siguiente ilustración se muestra un ejemplo de la pantalla del **panel** de control del dispositivo del nodo de control maestro (MCN).



En la siguiente ilustración se muestra un ejemplo de visualización del panel de control del dispositivo cliente.



Configuración del hardware del dispositivo

Para configurar el hardware del dispositivo Citrix SD-WAN (dispositivo físico), haga lo siguiente:

1. Configura el chasis.

   Los dispositivos Citrix SD-WAN se pueden instalar en un rack estándar. Para la instalación de escritorio, coloque el chasis sobre una superficie plana. Asegúrese de que haya un espacio libre

mínimo de 2 pulgadas en los laterales y en la parte trasera del dispositivo para una ventilación adecuada.

2. Conecte la alimentación.

   a) Asegúrese de que el interruptor de alimentación está desactivado.
   b) Enchufe el cable de alimentación en el dispositivo y en un tomacorriente de CA.
   c) Presione el botón de encendido en la parte frontal del dispositivo.

3. Conecte la alimentación.

   a) Asegúrese de que el interruptor de alimentación está desactivado.
   b) Enchufe el cable de alimentación en el dispositivo y en un tomacorriente de CA.
   c) Presione el botón de encendido en la parte frontal del dispositivo.

4. Conecte el puerto de administración del dispositivo a un equipo personal.

   Debe conectar el dispositivo a un PC como preparación para completar el siguiente procedimiento, establecer la dirección IP de administración del dispositivo.

   > **Nota**
   >
   > Antes de conectar el equipo, asegúrese de que el puerto Ethernet está habilitado en el PC. Utilice un cable Ethernet para conectar el puerto de administración de dispositivos SD-WAN al puerto Ethernet predeterminado de un equipo personal.

Puerto de administración VPX-SE de SD-WAN El dispositivo virtual VPX-SE SD-WAN es una máquina virtual, por lo que no hay un puerto de administración físico. Sin embargo, si no configuró la dirección IP de administración para SD-WAN VPX-SE cuando creó la máquina virtual VPX, deberá hacerlo ahora, como se describe en la sección Configuración de la dirección IP de administración para SD-WAN VPX-SE.

El dispositivo virtual VPX-SE SD-WAN es una máquina virtual, por lo que no hay un puerto de administración físico. Sin embargo, si no configuró la dirección IP de administración para SD-WAN VPX-SE cuando creó la máquina virtual VPX, deberá hacerlo ahora, como se describe en la sección Configuración de la dirección IP de administración para SD-WAN VPX-SE.

Configurar dirección IP de administración

Para habilitar el acceso remoto a un dispositivo SD-WAN, debe especificar una dirección IP de administración única para el dispositivo. Para ello, primero debe conectar el dispositivo a un PC. A continuación, puede abrir un explorador en el PC y conectarse directamente a la Interfaz Web de administración del dispositivo, donde puede establecer la dirección IP de administración de ese dispositivo. La dirección IP de administración debe ser única para cada dispositivo.

Los dispositivos Citrix SD-WAN admiten protocolos IPv4 e IPv6. Puede configurar IPv4, IPv6 o ambos (doble pila). Cuando se configuran los protocolos IPv4 e IPv6, el protocolo IPv4 tiene prioridad sobre el protocolo IPv6.

> **NOTA**
>
> - Para configurar una dirección IPv4 o IPv6 en configuraciones específicas de función, asegúrese de que el mismo protocolo está habilitado y configurado como el protocolo de interfaz de administración. Por ejemplo, si quiere configurar una dirección IPv6 para un servidor SMTP, asegúrese de que una dirección IPv6 está configurada como dirección de interfaz de administración.
> - No se permiten direcciones locales de enlace (direcciones IPv6 que empiezan por "fe80").
> - Para configurar una dirección IPv6, debe tener un enrutador en la red que anuncie la dirección IPv6.

Los procedimientos son diferentes para configurar la dirección IP de administración para un dispositivo SD-WAN de hardware y un dispositivo virtual VPX (Citrix SD-WAN VPX-SE). Para obtener instrucciones sobre cómo configurar la dirección para cada tipo de dispositivo, consulte lo siguiente:

- **Dispositivo virtual VPX de SD-WAN:** consulte las secciones [Configuración de la dirección IP de administración para SD-WAN VPX-SE y Diferencias entre una instalación VPX-SE de SD-WAN y SD-WAN WANOP VPX.

Para configurar la dirección IP de administración para un dispositivo SD-WAN de hardware, haga lo siguiente:

> **Nota**
>
> Debe repetir el siguiente proceso para cada dispositivo de hardware que quiera agregar a la red.

1. Si va a configurar un dispositivo SD-WAN de hardware, conecte físicamente el dispositivo a un PC.
    - Si aún no lo ha hecho, conecte un extremo de un cable Ethernet al puerto de administración del equipo y el otro extremo al puerto Ethernet predeterminado del PC.

    > **Nota**
    >
    > Asegúrese de que el puerto Ethernet esté habilitado en el PC que utiliza para conectarse al dispositivo.

2. Registre la configuración actual del puerto Ethernet para el equipo que está utilizando para establecer la dirección IP de administración del dispositivo.

Debe cambiar la configuración del **puerto Ethernet** en el equipo para poder configurar la dirección IP de administración del dispositivo. Asegúrese de registrar la configuración original para poder restaurarla después de configurar la dirección IP de administración.

3. Cambia la dirección IP del PC.

   En el PC, abre la configuración de la interfaz de red y cambia la dirección IP de su PC a la siguiente:

   - 192.168.100.50

4. Cambie la configuración **Máscara de subred** de su PC a la siguiente:

   - 255.255.0.0

5. En el PC, abra un explorador e introduzca la dirección IP predeterminada del dispositivo. Introduzca la siguiente dirección IP en la línea de dirección del explorador:

   - 192.168.100.1

   > **Nota**
   >
   > Se recomienda utilizar el explorador Google Chrome cuando se conecte a un dispositivo SD-WAN.
   >
   > Omitir las advertencias de certificados del explorador para la interfaz web de administración.

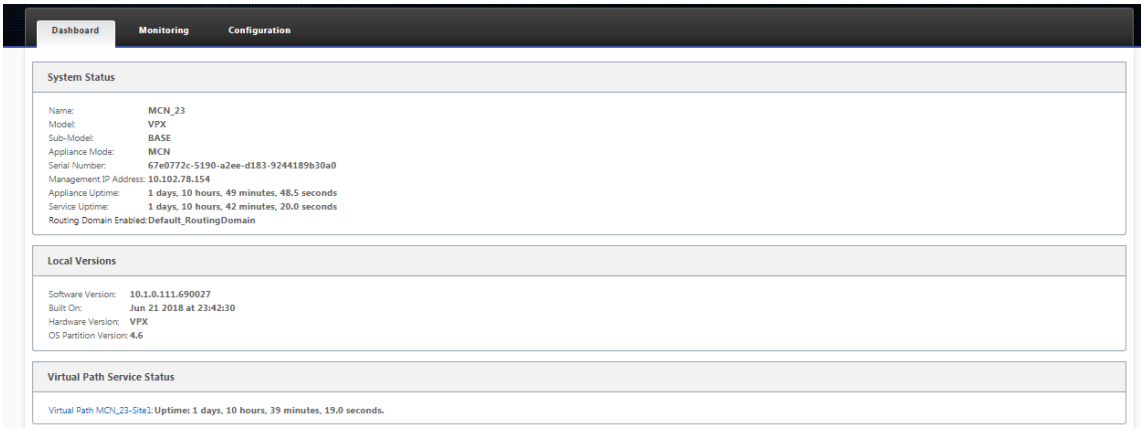
   Se abre la pantalla de inicio de sesión de la interfaz web de administración de SD-WAN en el dispositivo conectado.

6. Introduzca el nombre de usuario y la contraseña del administrador y haga clic en **Iniciar sesión**.

   - Nombre de usuario de administrador predeterminado: *admin*
   - Contraseña de administrador predeterminada: *contraseña*

   > **Nota**
   >
   > Se recomienda cambiar la contraseña predeterminada. Asegúrese de registrar la contraseña en una ubicación segura, ya que la recuperación de la contraseña puede requerir un restablecimiento de la configuración.

   Después de haber iniciado sesión en la interfaz web de administración, aparece la página **Panel**, como se muestra a continuación.



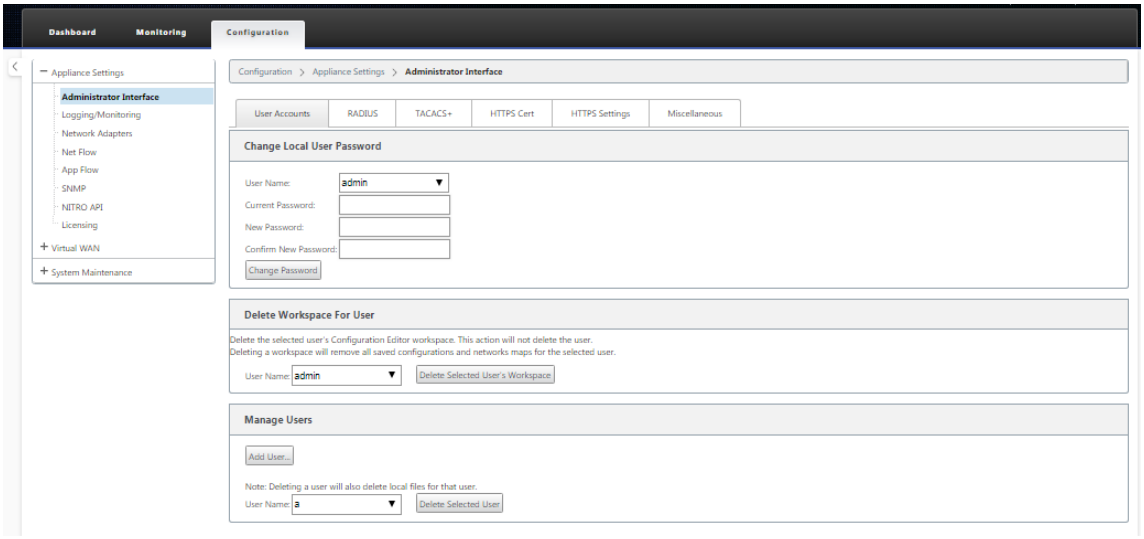
La primera vez que inicie sesión en la interfaz web de administración de un dispositivo, el **panel** muestra un icono de alerta (delta de vara dorada) y un mensaje de alerta que indica que el servicio SD-WAN está inhabilitado y que la licencia no se ha instalado. Por ahora, puede ignorar esta alerta. La alerta se resolverá una vez que haya instalado la licencia y haya completado el proceso de configuración e implementación del dispositivo.

7. En la barra de menús principal, selecciona la ficha de la sección **Configuración**.

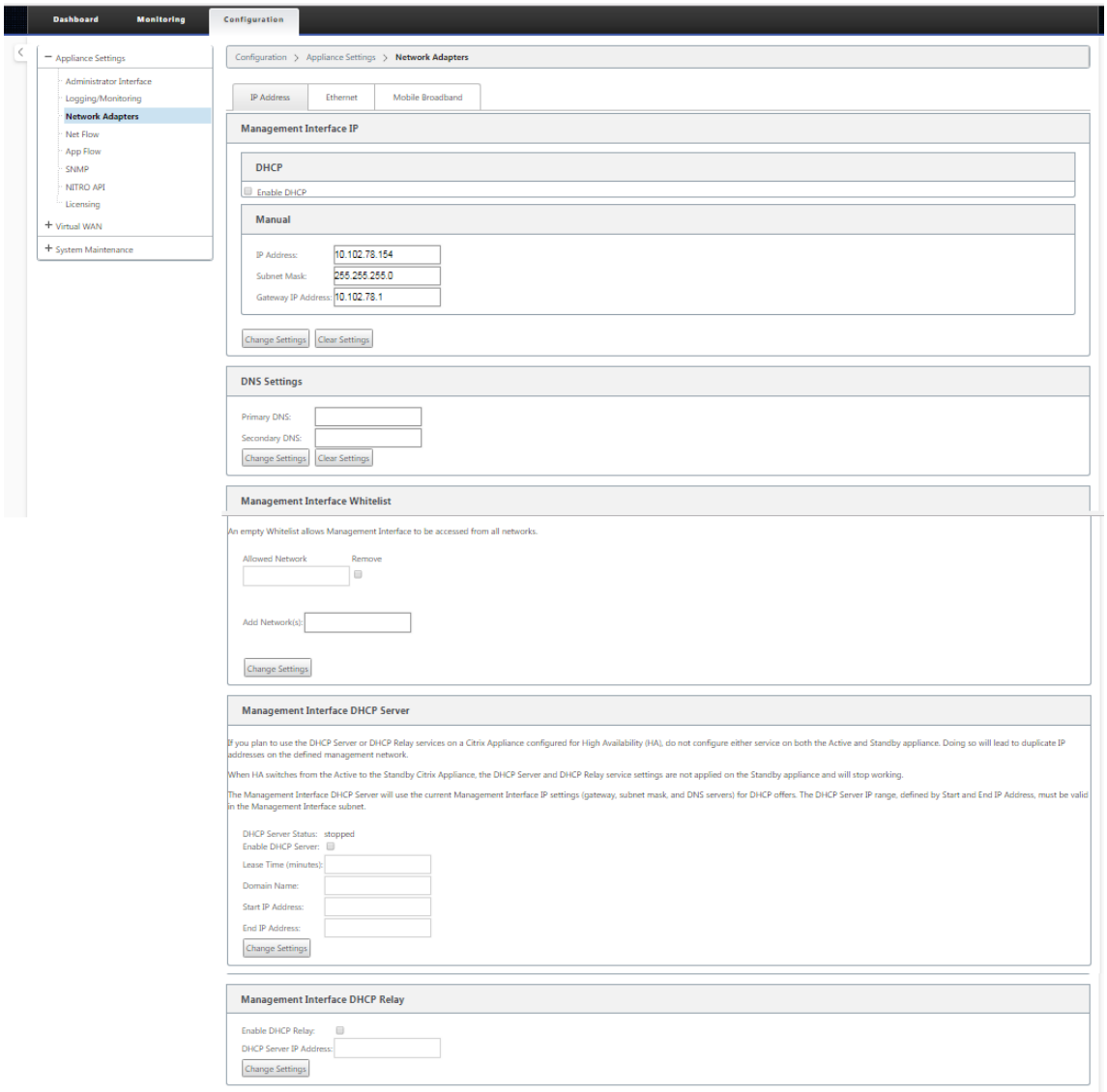
   Muestra el árbol **de navegación Configuración** en el panel izquierdo de la pantalla. El árbol **de navegación de Configuración** contiene las tres ramas principales siguientes:

   - Configuración del dispositivo
   - WAN virtual
   - Mantenimiento del sistema

   Al seleccionar la ficha **Configuración**, se abre automáticamente la sucursal **Configuración del dispositivo**, con la página **Interfaz de administrador** preseleccionada de forma predeterminada, como se muestra en la ilustración siguiente.



8. En la rama **Configuración del dispositivo** del árbol de navegación, seleccione **Adaptadores de red**. Esto muestra la página de configuración de **Adaptadores de red** con la ficha **Dirección IP** preseleccionada de forma predeterminada, como se muestra en la ilustración siguiente.



9. En la ficha Dirección IP, habilite una de las siguientes opciones:

   - **Protocolo IPv4**: Para habilitar la dirección IPv4, marque la casilla **Habilitar IPv4**. Dynamic Host Control Protocol (DHCP) asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo de la red. Seleccione **Habilitar DHCP** para asignar direcciones IP dinámicamente. Para configurar manualmente la dirección IP, proporcione los siguientes detalles:

     - Dirección IP
     - Máscara de subred
     - Dirección IP de la puerta de enlace

- **Protocolo IPv6**: Para habilitar la dirección IPv6, marque la casilla **Habilitar IPv6**. Puede configurar la dirección IPv6 manualmente o habilitar DHCP o SLAAC para asignar direcciones IP automáticamente.

  Para configurar manualmente, proporcione los siguientes detalles:

  - Dirección IP
  - Prefijo

  Para configurar SLAAC, marque la casilla **SLAAC**. SLAAC asigna automáticamente una dirección IPv6 a cada dispositivo de la red. SLAAC permite a un cliente IPv6 generar sus propias direcciones utilizando una combinación de información disponible localmente e información anunciada por los enrutadores a través del Protocolo de detección de vecinos (NDP).

  Para configurar DHCP, marque la casilla **DHCP**. Para habilitar DHCP sin estado, active las casillas de verificación **SLAAC** y **DHCP**.

- **Protocolos IPv4 e IPv6**: Active las casillas de verificación **Habilitar IPv6y Habilitar IPv4** para habilitar los protocolos IPv4 e IPv6. En tales casos, el dispositivo SD-WAN tiene una dirección IP de administración IPv4 y una dirección de administración IPv6.

> **NOTA**
>
> - La dirección IP de administración debe ser única para cada dispositivo.
> - Las secciones **Servidor DHCP de la interfaz de administración** y **retransmisión DHCP** de la ficha Dirección IP solo son aplicables si el protocolo IPv4 está habilitado en la interfaz de administración.
> - Cuando la interfaz de administración actúa como cliente DHCP, el nombre de host se utiliza en los mensajes del cliente DHCP como opción 12. A partir de la versión 11.2.3 de Citrix SD-WAN y hasta la versión 11.4.1, el nombre de host se estableció como **sdwan**. A partir de la versión 11.4.1 de Citrix SD-WAN, el nombre de host es el mismo que el nombre del sitio.
>
> Si se cambia o configura el nombre del sitio por primera vez, hasta que se complete la actualización de la configuración y el servicio WAN virtual esté activo, se utilizará el nombre del sitio antiguo o **sdwan** como nombre de host en los mensajes del cliente DHCP. Una vez finalizada la actualización de la configuración y el servicio WAN virtual esté activo, los mensajes del cliente DHCP posteriores utilizan el nuevo nombre del sitio.

10. Haga clic en **Change Settings**. Aparece un cuadro de diálogo de confirmación en el que se le pide que compruebe si quiere cambiar esta configuración.
11. Haga clic en **Aceptar**.
12. Vuelva a cambiar la configuración de la interfaz de red de su PC a la configuración original.

> **Nota**
>
> Al cambiar la dirección IP de su PC, se cierra automáticamente la conexión con el dispositivo y se termina la sesión de inicio de sesión en la interfaz web de administración.

13. Desconecte el equipo del PC y conéctelo al router o conmutador de red. Desconecte el cable Ethernet del PC, pero no lo desconecte del dispositivo. Conecte el extremo libre del cable al router o conmutador de red.

    El dispositivo SD-WAN ya está conectado a la red y está disponible en ella.

14. Pruebe la conexión. En un equipo conectado a la red, abra un explorador e introduzca la dirección IP de administración que configuró para el dispositivo en el siguiente formato:

    Para la dirección IPv4: `https://<IPv4 address>`

    Ejemplo:`https://10.10.2.3`

    Para la dirección IPv6: `https://<[IPv6 address]>`

    Ejemplo:`https://[fd73:xxxx:yyyy:26::9]`

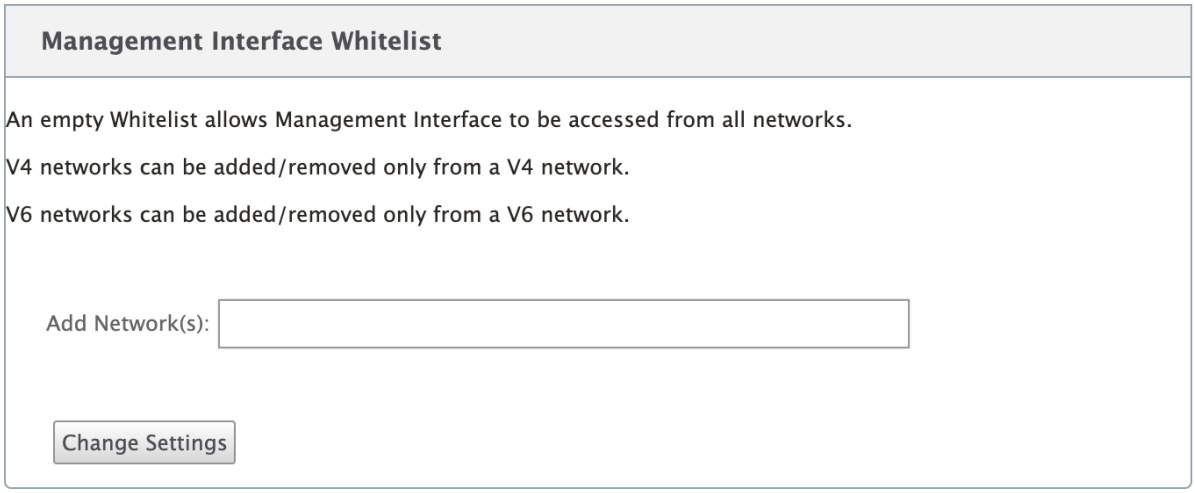
    Si la conexión se realiza correctamente, se muestra la pantalla **Inicio de sesión** de la interfaz web de administración de SD-WAN en el dispositivo que ha configurado.

    > **Sugerencia**
    >
    > Después de verificar la conexión, no cierre la sesión de la interfaz web de administración. Lo utilizará para completar las tareas restantes descritas en las secciones siguientes.

    Ahora ha establecido la dirección IP de administración del dispositivo SD-WAN y puede conectarse al dispositivo desde cualquier ubicación de la red.

Lista de permitir la interfaz de administración Lista permitida es una lista aprobada de direcciones IP o dominios IP que tienen permiso para acceder a la interfaz de administración. Una lista vacía permite acceder a la interfaz de administración desde todas las redes. Puede agregar direcciones IP para asegurarse de que las redes de confianza solo pueden acceder a la dirección IP de administración.

Para agregar o quitar una dirección IPv4 a la lista permitida, debe acceder a la interfaz de administración del dispositivo SD-WAN utilizando únicamente una dirección IPv4. Del mismo modo, para agregar o quitar una dirección IPv6 a la lista de permitidos, debe acceder a la interfaz de administración del dispositivo SD-WAN utilizando únicamente una dirección IPv6.



Establecer fecha y hora

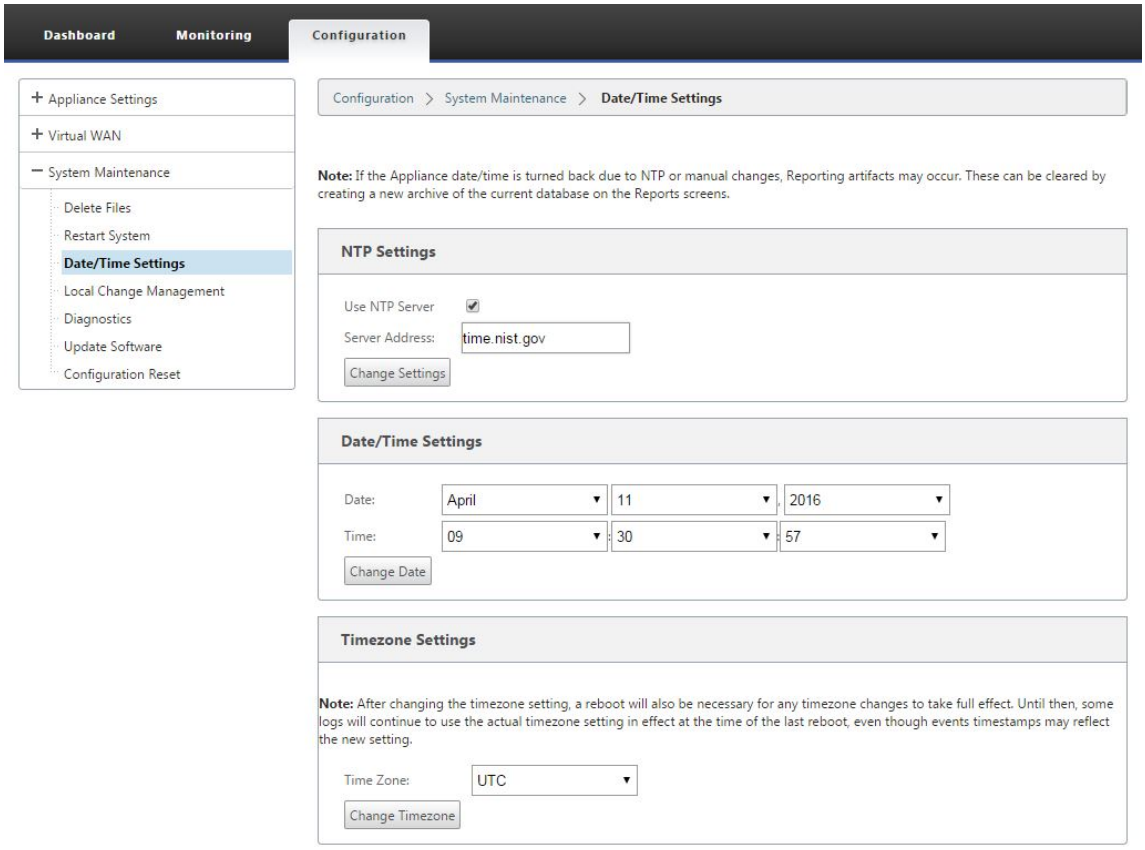
Antes de instalar la licencia de software SD-WAN en un dispositivo, debe establecer la fecha y la hora del dispositivo.

> **Nota**
>
> - Debe repetir este proceso para cada dispositivo que quiera agregar a la red.
> - Si la hora actual se cambia manualmente o a través del servidor NTP, y el tiempo recién establecido es superior al temporizador de tiempo de espera de sesión, la sesión de la interfaz de usuario se cerrará.

Para establecer la fecha y la hora, haga lo siguiente:

1. Inicie sesión en la interfaz web de administración del dispositivo que va a configurar.
2. En la barra de menús principal, selecciona la **ficha Configuración.**

   Muestra el árbol **de navegación Configuración** en el panel izquierdo de la pantalla.
3. Abra la **rama Mantenimiento del sistema** en el árbol de navegación.
4. En la **rama Mantenimiento del sistema, selecciona Configuración de fecha y hora**. Muestra la página **Configuración de fecha/hora**, como se indica a continuación.



5. Seleccione la zona horaria en el menú implementable del campo **Zona horaria** en la parte inferior de la página.

> **Nota**
>
> Si tiene que cambiar la configuración de la zona horaria, debe hacerlo antes de establecer la fecha y la hora, o la configuración no se conservará tal y como se introdujo.

6. Haga clic en **Cambiar zona horaria**. Esto actualiza la zona horaria y vuelve a calcular la configuración actual de fecha y hora según corresponda. Si configura la fecha y la hora correctas antes de este paso, la configuración ya no será correcta. Cuando finaliza la actualización de la zona horaria, aparece un icono de alerta correcta (marca de verificación verde) y un mensaje de estado en la sección superior de la página.
7. (Opcional) Habilite el servicio Servidor NTP.
   a) Seleccione **Usar servidor NTP**.
   b) Introduzca la dirección del servidor en el campo **Dirección del servidor**.
   c) Haga clic en **Change Settings**.
   Aparece un icono de alerta de éxito (marca de verificación verde) y un mensaje de estado cuando finaliza la actualización.
8. Seleccione el mes, el día y el año en los menús desplegables del campo **Fecha**.

9. Seleccione la hora, los minutos y los segundos en los menús desplegables del campo **Hora**.
10. Haga clic en **Cambiar fecha**.

> **Nota:**
>
> Esto actualiza la configuración de fecha y hora, pero no muestra un icono de alerta ni un mensaje de estado correctos.

El siguiente paso consiste en establecer el umbral de tiempo de **espera** de la sesión de consola en el valor máximo. Este paso es opcional, pero recomendado. Esto evita que la sesión termine prematuramente mientras trabaja en la configuración, lo que puede resultar en una pérdida de trabajo. Las instrucciones para configurar el valor de Tiempo de **espera de** la sesión de consola se proporcionan en la siguiente sección. Si no quiere restablecer el umbral de tiempo de espera, puede ir directamente a la sección Carga e instalación del archivo de licencia de software de SD-WAN.

> **Advertencia**
>
> Si el tiempo de espera de la sesión de consola o cierra sesión en Management Web Interface antes de guardar la configuración, se perderán los cambios de configuración no guardados. Vuelva a iniciar sesión en el sistema y repita el procedimiento de configuración desde el principio.

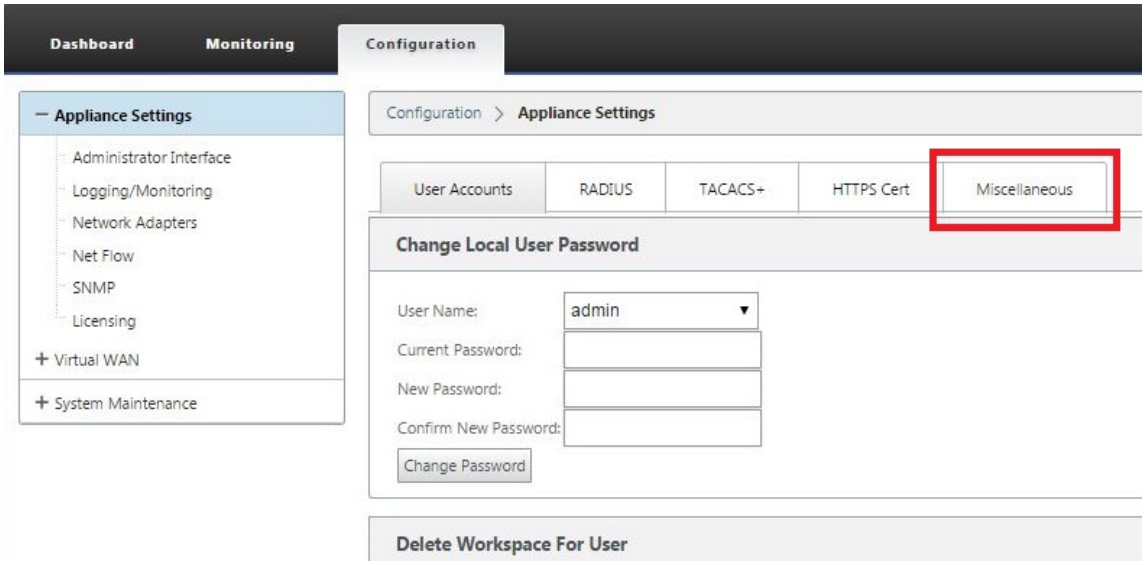
Tiempo de espera de la sesión

Si el tiempo de espera de la sesión de consola o cierra sesión en Management Web Interface antes de guardar la configuración, se perderán los cambios de configuración no guardados. A continuación, debe volver a iniciar sesión en el sistema y repetir el procedimiento de configuración desde el principio. Por ese motivo, se recomienda establecer el intervalo de **tiempo de espera** de la sesión de consola en un valor alto al crear o modificar un paquete de configuración, o al realizar otras tareas complejas. El valor predeterminado es 60 minutos. El máximo es de 9.999 minutos. Por razones de seguridad, debe restablecerlo a un umbral inferior después de completar esas tareas.

Para restablecer el intervalo de tiempo de **espera** de la sesión de consola, haga lo siguiente:

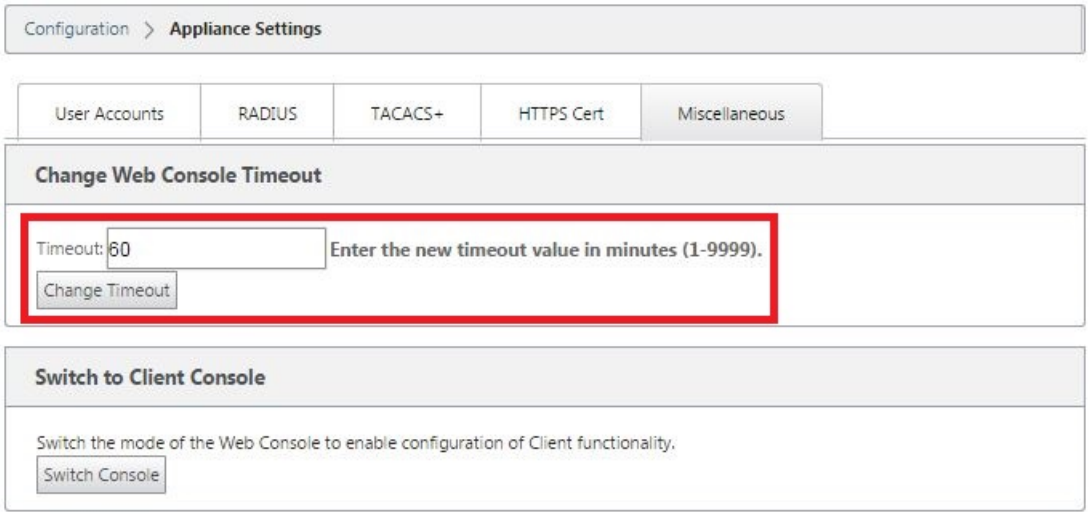
1. Seleccione la ficha **Configuración** y, a continuación, seleccione la rama **Configuración del dispositivo** en el árbol de navegación.

   Aparece la página Configuración del dispositivo, con la ficha **Cuentas de usuario** preseleccionada de forma predeterminada.



2. Selecciona la ficha **Miscelánea** (esquina derecha).

   Muestra la página de la ficha **Varios**.



3. Introduzca el valor de tiempo de **espera de la** consola.

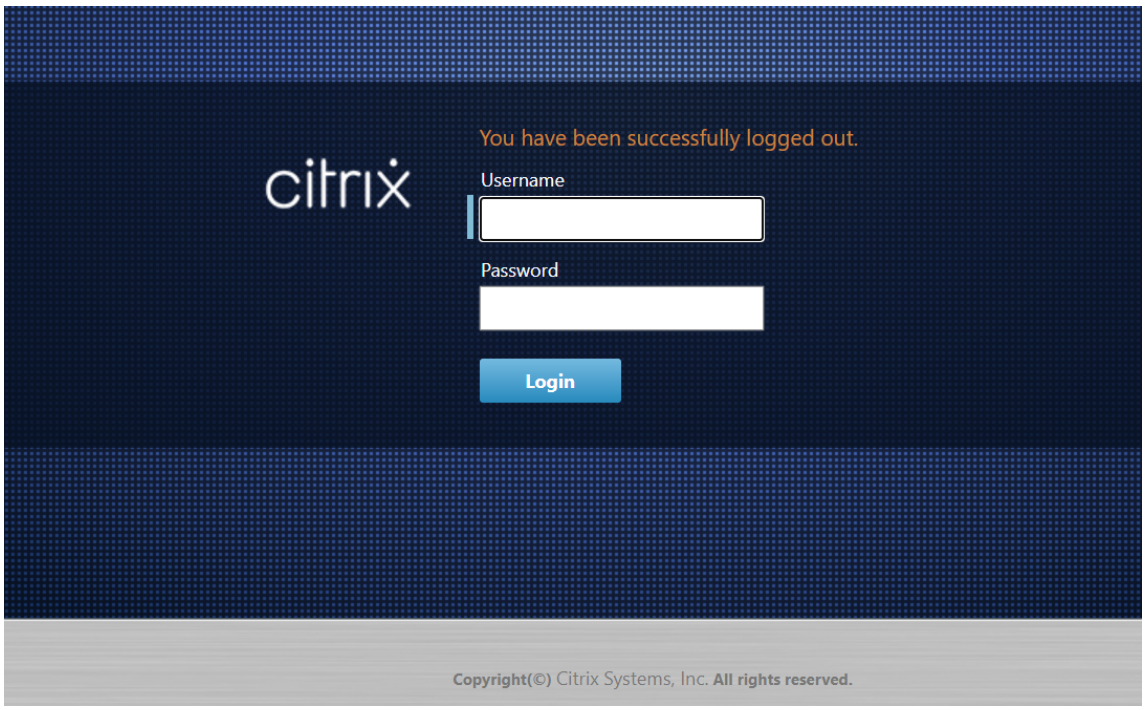
   En el campo Tiempo de **espera** de la sección **Cambiar tiempo de espera de la consola web**, introduzca un valor superior (en minutos) hasta el valor máximo de 9999. El valor predeterminado es 60, lo que es demasiado breve para una sesión de configuración inicial.

   > **Nota**
   >
   > Por motivos de seguridad, asegúrese de restablecer este valor a un intervalo inferior después de completar la configuración y la implementación.

4. Haga clic en **Cambiar tiempo de espera**.

Esto restablece el intervalo de **tiempo de espera** de la sesión y muestra un mensaje de éxito cuando finaliza la operación.

Tras un breve intervalo (unos segundos), la sesión finaliza y se cierra automáticamente la sesión de la interfaz web de administración. Aparecerá la página de inicio de sesión.



5. Introduzca el nombre de usuario del administrador (*admin*) y la contraseña (*contraseña*) y haga clic en **Iniciar sesión**.

   El siguiente paso es cargar e instalar el archivo de licencia de software SD-WAN en el dispositivo.

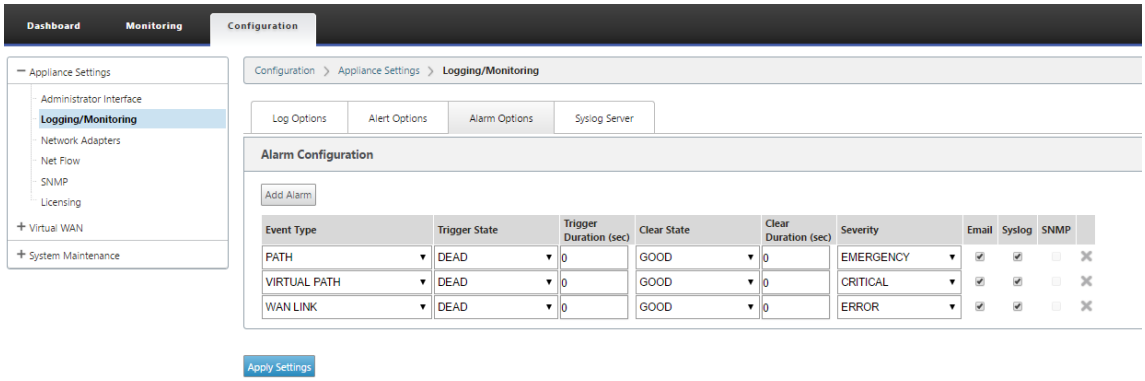
Configurar alarmas

Ahora puede configurar su dispositivo SD-WAN para identificar las condiciones de alarma en función de su red y sus prioridades, generar alertas y recibir notificaciones por correo electrónico, syslog o captura SNMP.

Una alarma es una alerta configurada que consta de un tipo de evento, un estado de activación, un estado claro y una gravedad.

Para configurar los ajustes de alarma:

1. En la interfaz de administración web de SD-WAN, vaya a **Configuración > Configuracióndel equipo**>**Registrar/Supervisión**y haga clic en**Opciones de alarma**.
2. Haga clic en **Agregar alarma para** agregar una nueva alarma.



3. Seleccione o introduzca valores para los campos siguientes:

   - **Tipo de evento**: El dispositivo SD-WAN puede activar alarmas para subsistemas u objetos concretos de la red, denominados tipos de eventos. Los tipos de eventos disponibles son SERVICE, VIRTUAL_PATH, WANLINK, PATH, DYNAMIC_VIRTUAL_PATH, WAN_LINK_CONGESTION, USAGE_CONGESTION, FAN, POWER_SUPPLY, PROXY_ARP, ETHERNET, DISCOVERED_MTU, GRE_TUNNEL y IPSEC_TUNNEL.
   - **Estado de activación:** el estado del evento que activa una alarma para un tipo de evento. Las opciones de estado del desencadenador disponibles dependen del tipo de evento elegido.
   - **Duración del disparador**: La duración en segundos, determina la rapidez con la que el dispositivo activa una alarma. Introduzca"0"para recibir alertas inmediatas o introduzca un valor entre 15-7200 segundos. Las alarmas no se activan si se producen más eventos en el mismo objeto durante el período de duración del desencadenador. Solo se activan más alarmas si un evento persiste durante más tiempo que el período de duración del desencadenador.
   - **Borrar estado**: Estado de evento que borra una alarma para un tipo de evento después de que se activa la alarma. Las opciones de Borrar estado disponibles dependen del estado del desencadenador elegido.
   - **Duración de borrado:** la duración en segundos, determina cuánto tiempo se debe esperar antes de borrar una alarma. Introduzca "0"para borrar inmediatamente la alarma o introduzca un valor entre 15 y 7200 segundos. La alarma no se borra si se produce otro evento de estado claro en el mismo objeto dentro del tiempo especificado.

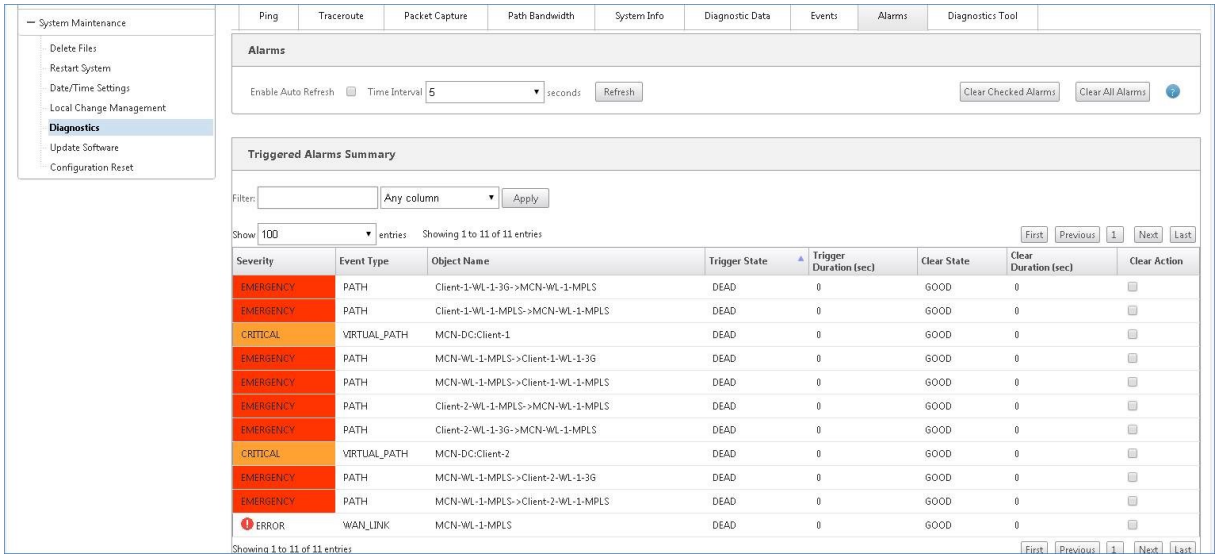
- **Gravedad**: campo definido por el usuario que determina la urgencia de una alarma. La gravedad se muestra en las alertas enviadas cuando se activa o borra la alarma y en el resumen de la alarma activada.
- **Correo electrónico**: Las alertas de activación de alarma y borrado para el tipo de evento se envían por correo electrónico.
- **Syslog**: Las alertas de activación y borrado de alarmas para el tipo de evento se envían a través de Syslog.
- **SNMP**: El disparador de alarma y las alertas claras para el tipo de evento se envían a través de la captura SNMP.

4. Continúe agregando alarmas según sea necesario.
5. Haga clic en **Aplicar configuración**.

Visualización de alarmas activadas **Para ver un resumen de todas las alarmas activadas:**

En la interfaz de administración web de SD-WAN, vaya a **Configuración** > **Mantenimiento del sistema > Diagnóstico** > **Alarmas**.

Se muestra una lista de todas las alarmas activadas.



Borrado de alarmas activadas **Para borrar manualmente las alarmas activadas:**

1. En la interfaz de administración web de SD-WAN, vaya a **Configuración** > **Mantenimiento del sistema > Diagnóstico** > **Alarmas**.
2. En la columna **Acción de borrado**, seleccione las alarmas que quiera borrar.
3. Haga clic en **Borrar alarmas comprobadas**. Alternativamente, haga clic en **Borrar todas las alarmas** para borrar todas las alarmas.

Configuración del nodo de control maestro

El **nodo de control maestro (MCN) de SD-WAN** es el dispositivo principal de la WAN virtual. Por lo general, se trata de un dispositivo WAN virtual implementado en el centro de datos. El MCN sirve como punto de distribución para la configuración inicial del sistema y cualquier cambio de configuración posterior. Además, la mayoría de los procedimientos de actualización se llevan a cabo a través de la interfaz web de administración del MCN. Solo puede haber un MCN activo en una WAN virtual.

De forma predeterminada, los dispositivos tienen la función de cliente asignada previamente. Para establecer un dispositivo como MCN, primero debe agregar y configurar el sitio de MCN y, a continuación, preparar y activar la configuración y el paquete de software adecuado en el dispositivo MCN designado.

A partir de la versión 11.5 de Citrix SD-WAN, puede configurar una MCN a través de Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Implementación y Configuración del sitio.

Conexión de los dispositivos cliente a la red

Para una implementación inicial o si va a agregar nodos cliente a una SD-WAN existente, el siguiente paso consiste en que los administradores del sitio de sucursal conecten los dispositivos cliente a la red en sus sucursales respectivas. Esto se prepara para cargar y activar los paquetes de dispositivos SD-WAN adecuados para los clientes. Conecte a cada administrador del sitio de sucursal para iniciar y coordinar estos procedimientos.

Para conectar los dispositivos del sitio a la SD-WAN, los administradores del sitio deben hacer lo siguiente:

1. Si aún no lo ha hecho, configure los dispositivos cliente.

   Para cada dispositivo que quiera agregar a la SD-WAN, haga lo siguiente:

   a) Configure el hardware del dispositivo SD-WAN y cualquier dispositivo virtual VPX SD-WAN (SD-WAN VPX-SE) que esté implementando.
   b) Establezca la dirección IP de administración para el dispositivo y verifique la conexión.
   c) Establezca la fecha y la hora del dispositivo. Establezca el umbral de tiempo de espera de la sesión de consola en un valor máximo o alto.
   d) Cargue e instale el archivo de licencia de software en el dispositivo.

2. Conecte el dispositivo a la LAN de la sucursal. Conecte un extremo de un cable Ethernet a un puerto configurado para LAN del dispositivo SD-WAN. A continuación, conecte el otro extremo del cable al conmutador LAN.

3. Conecte el dispositivo a la WAN. Conecte un extremo de un cable Ethernet a un puerto configurado para WAN en el dispositivo SD-WAN. Luego conecte el otro extremo del cable al enrutador WAN.

El siguiente paso es que los administradores del sitio de sucursal instalen y activen el paquete de dispositivos SD-WAN adecuado en sus respectivos clientes.

Acceso al comando shell

A partir de la versión 11.4.1 de SD-WAN, los usuarios de cuentas de administrador pueden ejecutar el comando shell desde la consola CLI de SD-WAN directamente, sin que se les soliciten las credenciales de inicio de sesión de la cuenta estática CBVWSSH. Esta función mejora la seguridad de sus dispositivos SD-WAN, ya que elimina la contraseña codificada de forma rígida de la cuenta CBVWSSH y la reemplaza mediante un método más seguro. Para ejecutar el comando shell, inicie sesión en la consola CLI de SD-WAN y escriba `shell`.

> **Nota**
>
> - Esta funcionalidad solo es compatible con los usuarios de cuentas de administrador. No es compatible con administradores de red, administradores de seguridad ni usuarios de cuentas Viewer.
> - Esta funcionalidad está pensada únicamente para solucionar problemas. Citrix supervisa cualquier cambio específico del sistema que se realice mediante el comando `shell`.

Actualización de versión Al actualizar el dispositivo SD-WAN a la versión 11.4.1, la contraseña de la cuenta de administrador predeterminada se sincroniza con la cuenta CBVWSSH. Esta sincronización entre la cuenta CBVWSSH y la cuenta de administrador predeterminada se produce cada vez que modifica/actualiza la cuenta de administrador.

Degradar Al bajar de categoría su dispositivo SD-WAN de la versión 11.4.1 a una versión anterior, tiene la opción de restablecer la contraseña de la cuenta de administrador predeterminada y restablecerla. Sin embargo, la nueva contraseña no se sincroniza con la cuenta CBVWSSH. Por lo tanto, para poder acceder al comando `shell` incluso después de revertir una versión, es obligatorio recordar la contraseña actual antes de revertir la versión del dispositivo.

Implemente Citrix SD-WAN Standard Edition en OpenStack con CloudInit

Ahora puede implementar Citrix SD-WAN Standard Edition (SE) en un entorno OpenStack. Para ello, la imagen de Citrix SD-WAN debe admitir la funcionalidad de unidad de configuración.

> **NOTA**
>
> Cree una imagen de Citrix para admitir la funcionalidad de la unidad de configuración.

La funcionalidad Config-drive admite la siguiente configuración de parámetros para establecer comunicación con Citrix Orchestrator a través de la red de administración:

- Adgmt. dirección ipv4
- Gmt. Gateway
- Name-server1
- Name-server2
- Número de serie: se utiliza para la autenticación y debe reutilizarse para la nueva instancia. El número de serie pasado en la nube debe sobrescribir el número de prueba generado automáticamente en la instancia VPX.

> **Nota**
>
> - Para reutilizar el número de serie, se incorpora un script de inicio en SD-WAN que se ejecuta en un OpenStack y cambia el número de serie en /etc/default/family.
> - Orchestrator debe tener un número de serie único con dispositivos SD-WAN para que funcione.

El script Cloudinit admite la contextualización para la implementación de SD-WAN en OpenStack con config-drive.

En el proceso de contextualización, la infraestructura pone el contexto a disposición de la máquina virtual y la máquina virtual interpreta el contexto. En contextualización, la máquina virtual puede iniciar determinados servicios, crear usuarios o establecer parámetros de red y configuración.

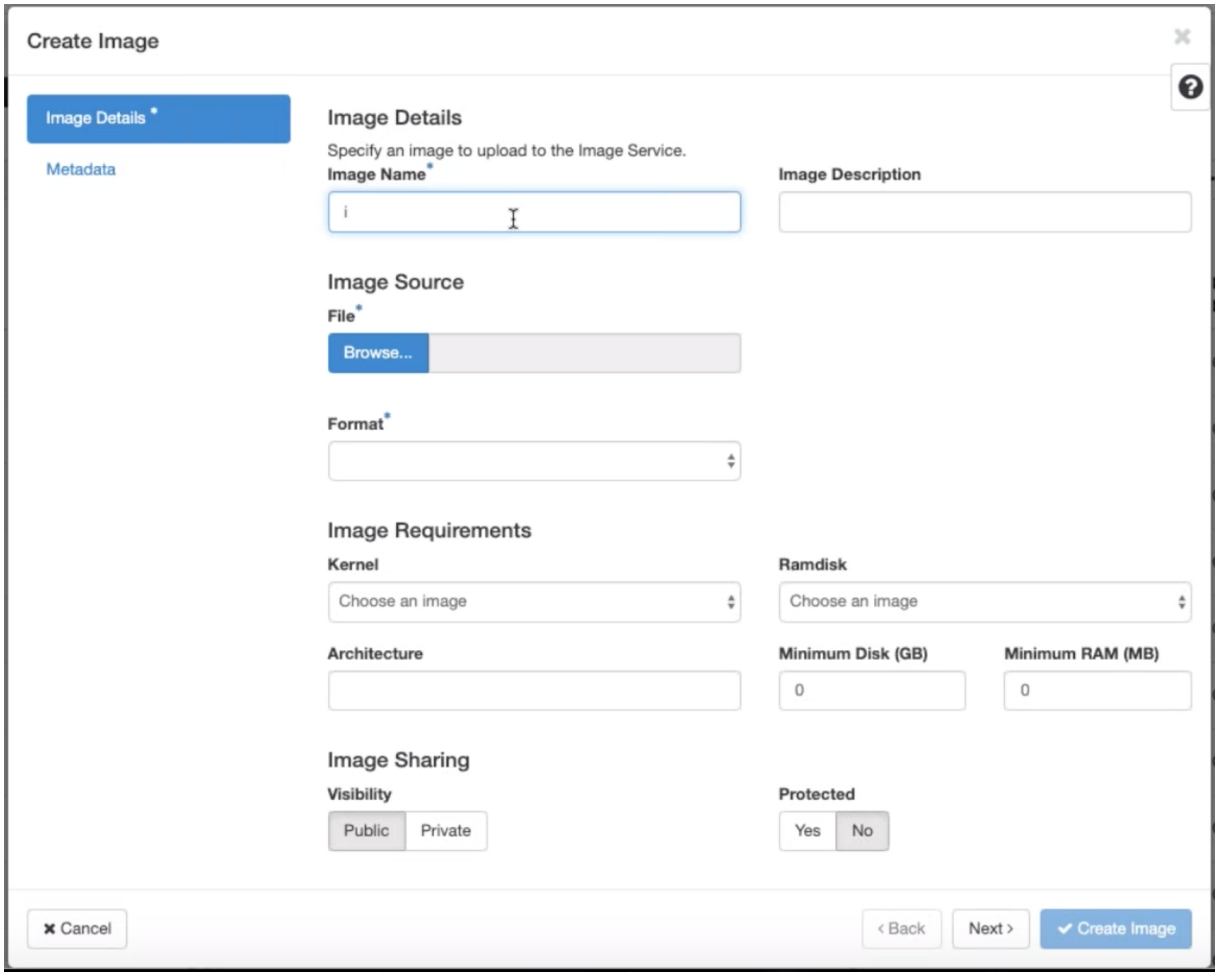
Para una instancia de SD-WAN en OpenStack, las entradas necesarias para IP de administración, DNS y número de serie de los usuarios. El script de Cloudinit analiza estas entradas y aprovisiona la instancia con la información dada.

Al iniciar instancias en un entorno de nube OpenStack, el dispositivo Citrix SD-WAN necesita admitir dos tecnologías que son User Data y CloudInit para admitir la configuración automatizada de instancias en el momento del arranque.

Realice los siguientes pasos para Provisioning SD-WAN SE en un entorno OpenStack:

Requisitos previos

Vaya a **Imágenes** y haga clic en **Crear imagen**.

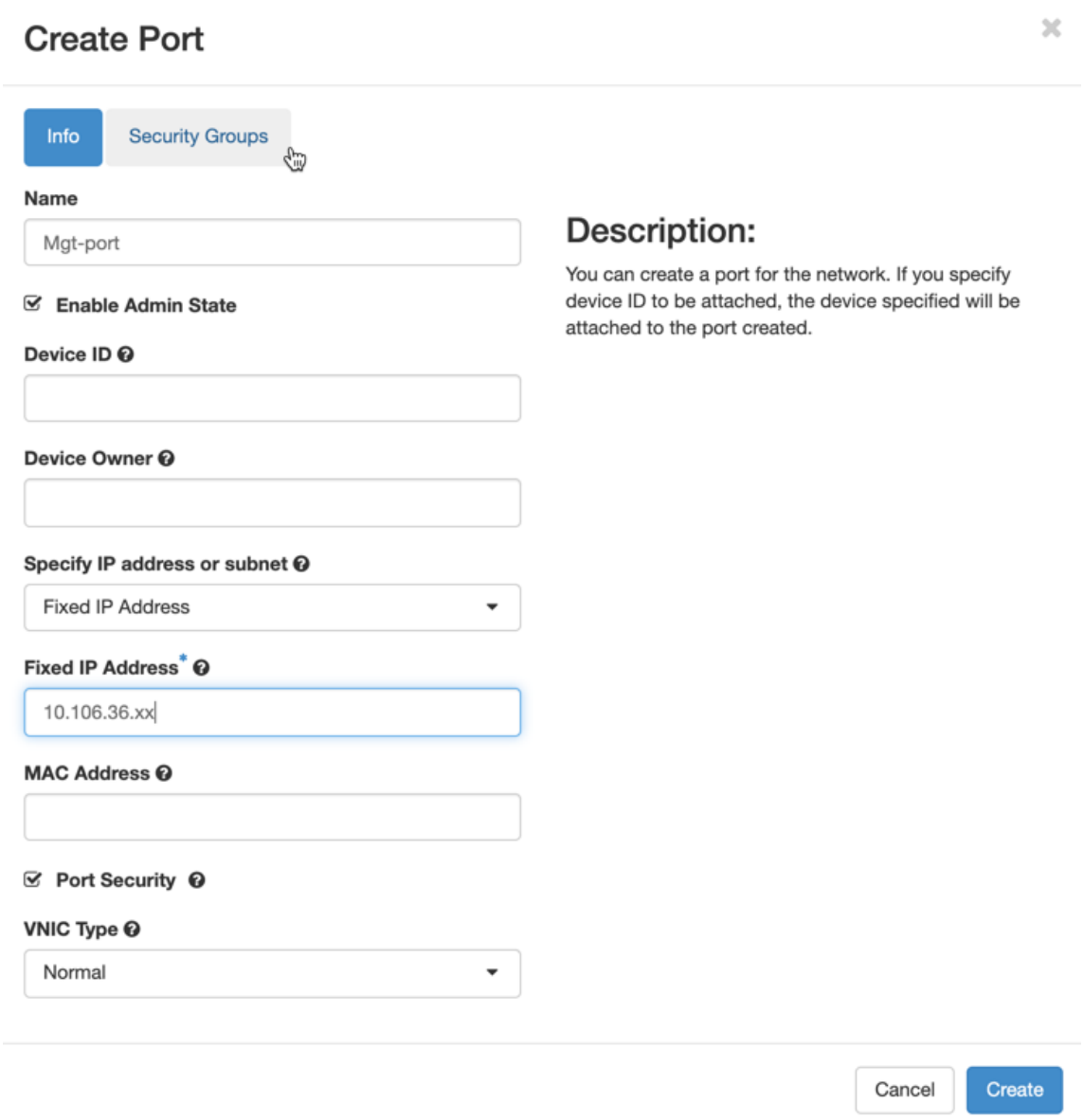


- **Nombre de imagen**: Proporcione el nombre de la imagen.
- **Descripción de la imagen**: Agregue una descripción de imagen.
- **Archivo** - Busque el archivo de imagen kvm.qcow2 desde su unidad local y selecciónelo.
- **Formato**: Seleccione el formato de disco Emulador QCOW2 —QEMU de la lista desplegable.

Haga clic en **Crear imagen**.

Tanto la red como el puerto de red deben crearse inicialmente y predefinidos. Para crear un puerto de red:

1. Seleccione **Redes** en **Red** y vaya a la ficha **Puerto**.
2. Haga clic en **Crear puerto**, proporcione los detalles necesarios y haga clic en Crear.

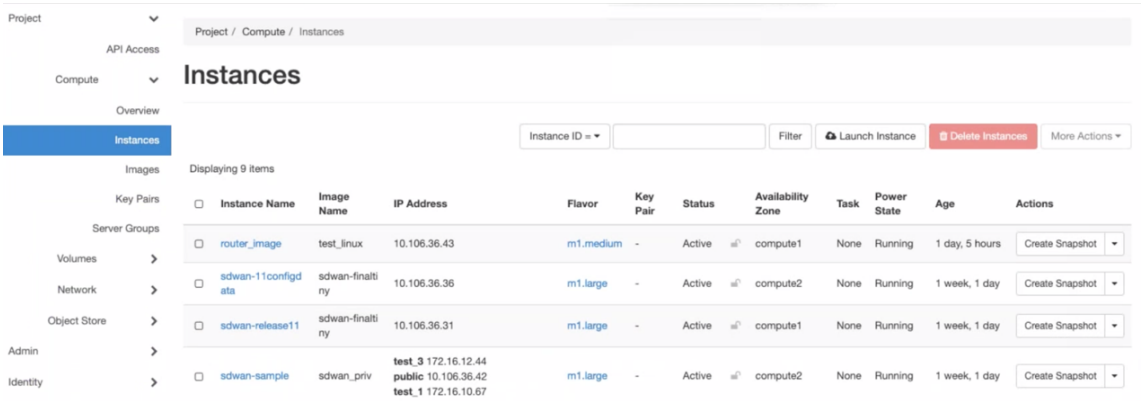


Si selecciona **Dirección IP fija**, debe proporcionar la dirección IP de subred para el nuevo puerto.

Se crea el puerto y, como no está conectado a ningún dispositivo, el estado actual muestra Separada.

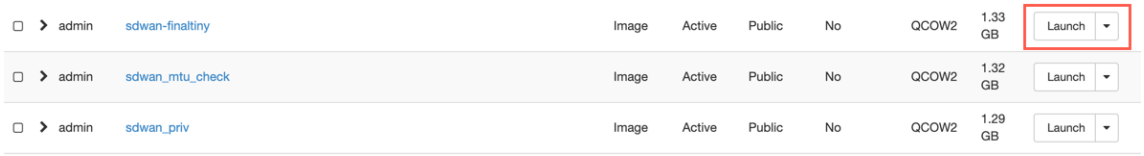
Crear instancia de OpenStack para habilitar config-drive y pasar los user_data.

3. Inicie sesión en OpenStack y configure Instancias.



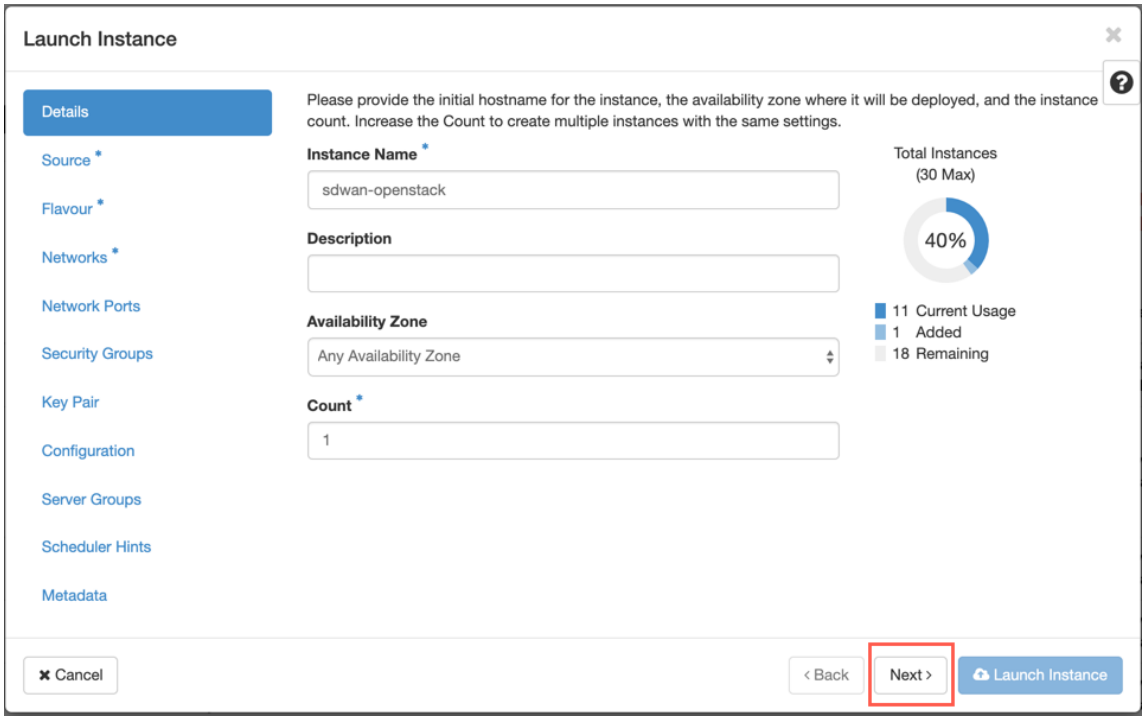
4. Descargue el archivo **kvm.qcow2.gz** y destártelo.
5. Vaya a **Instancias** y haga clic en **Iniciar instancia**.

> **NOTA**
>
> Puede volver a **Instancias** y hacer clic en **Iniciar instancia**o, desde la pantalla Imágenes, hacer clic en **Iniciar** una vez creada la imagen.

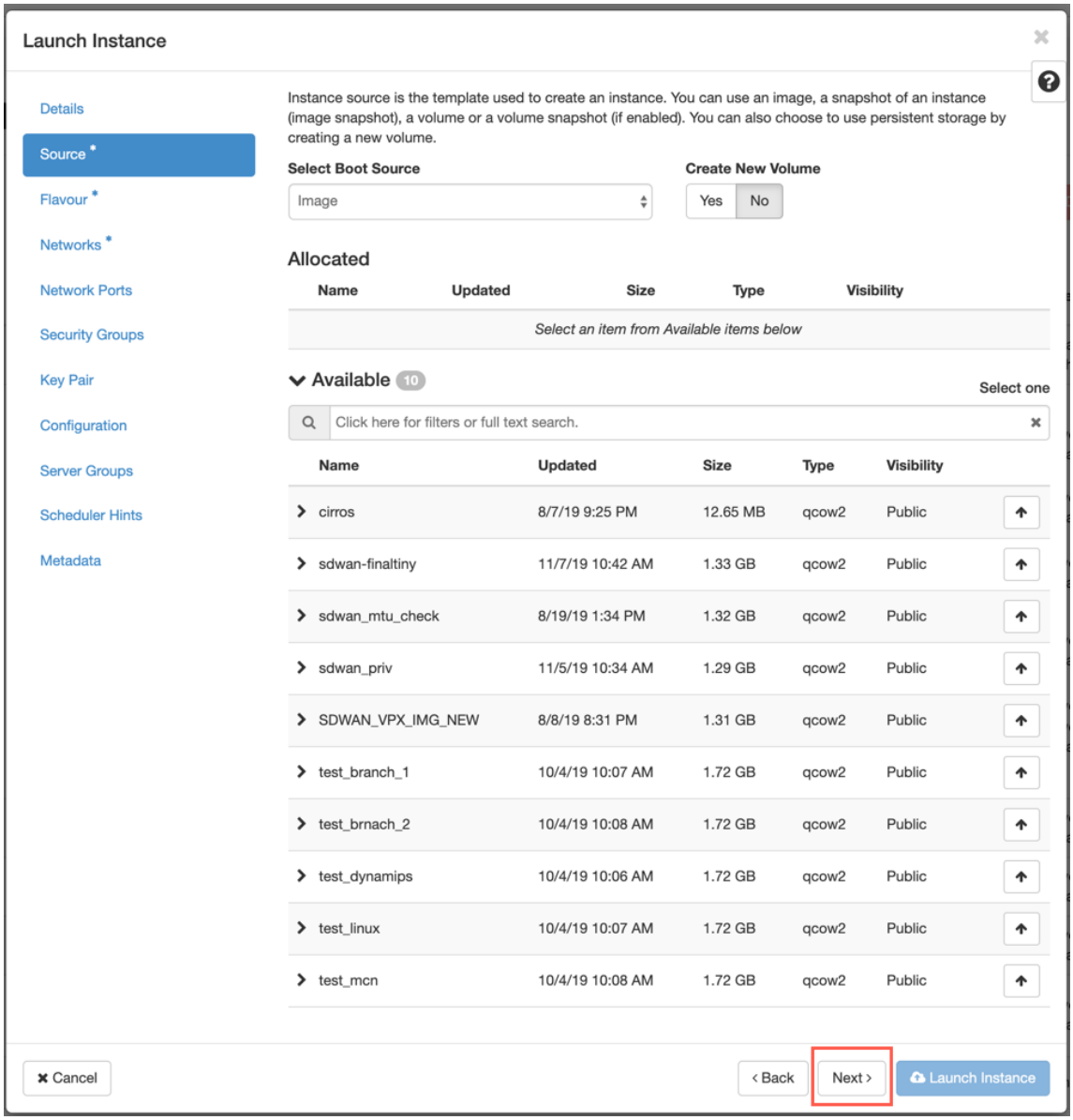


6. En la ficha **Detalles**, proporcione la siguiente información:

   - **Nombre de instancia**: Proporcione el nombre de host de la instancia.
   - **Descripción**: Agregue una descripción para la instancia.
   - **Zona de disponibilidad**: Seleccione la zona de disponibilidad en la lista desplegable donde quiere implementar la instancia.
   - **Recuento**: Introduzca el recuento de instancias. Puede aumentar el recuento para crear varias instancias con la misma configuración. Haga clic en **Siguiente**.



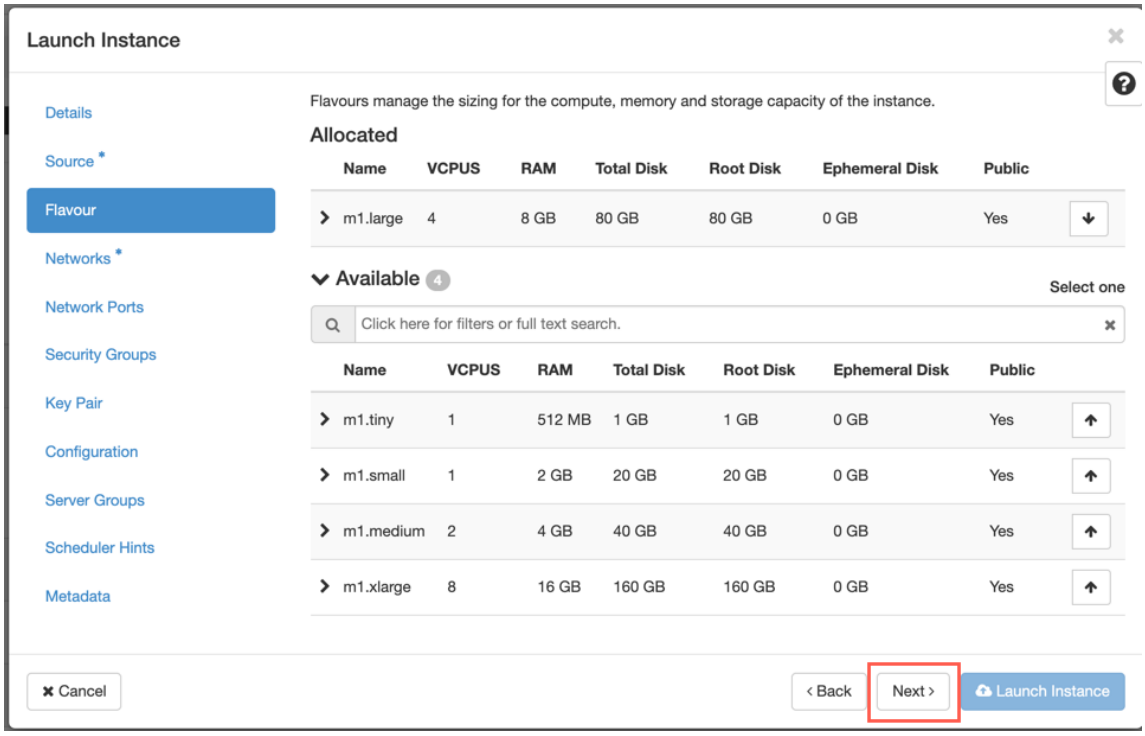
7. En la ficha **Origen**, seleccione **No** en **Crear nuevo volumen** y haga clic en**Siguiente**. El origen de instancia es la plantilla utilizada para crear una instancia.



8. Seleccione **Sabor** para la instancia y haga clic en Siguiente. El tipo que seleccione para una instancia administra la cantidad de capacidad informática, almacenamiento y memoria de la instancia.

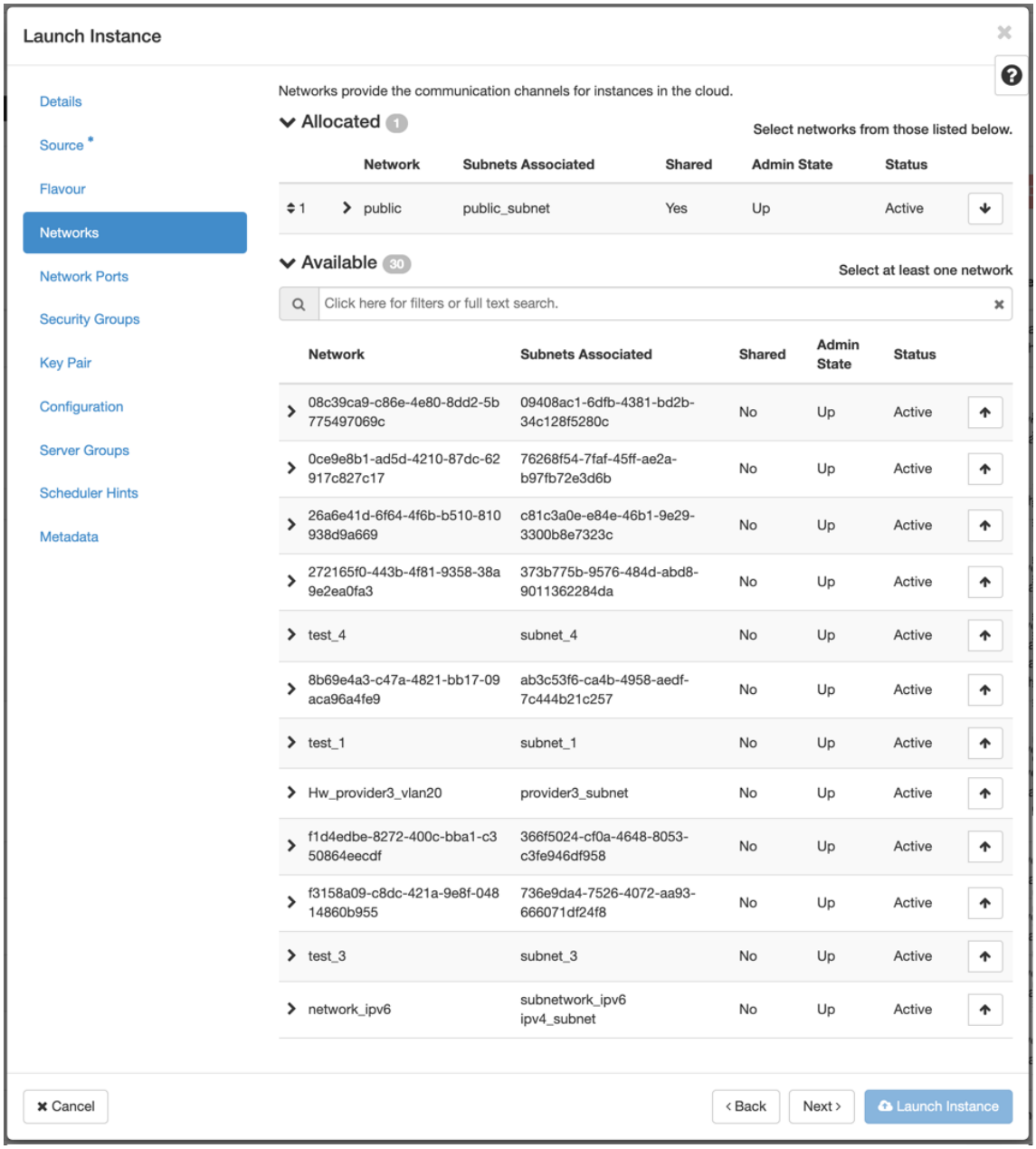
   > **NOTA**
   >
   > El tipo que seleccione debe tener suficientes recursos asignados para admitir el tipo de instancia que está intentando crear. Los tipos que no proporcionan recursos suficientes para su instancia se identifican en la tabla disponible con un icono de advertencia amarillo.

   Los administradores son responsables de crear y administrar tipos. Haga clic en la flecha (en el lado derecho) para asignar.



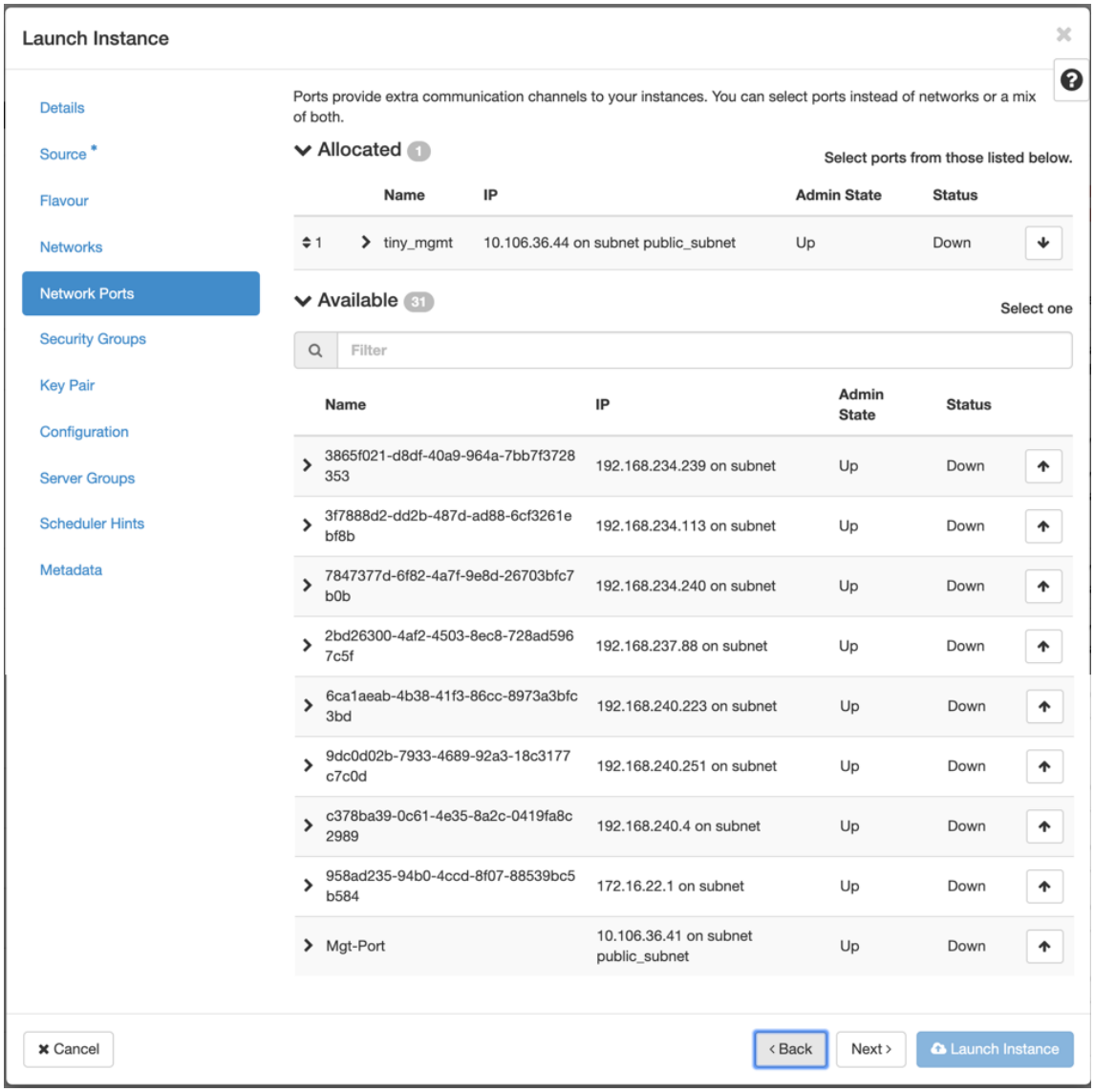
9. Seleccione la red y haga clic en **Siguiente**. Las redes proporcionan los canales de comunicación para las instancias.

> **NOTA**
>
> Se crea un administrador las redes de proveedores y estas redes se asignan a una red física existente en el centro de datos. Del mismo modo, los usuarios crean redes de proyectos y estas redes están completamente aisladas y son específicas del proyecto.

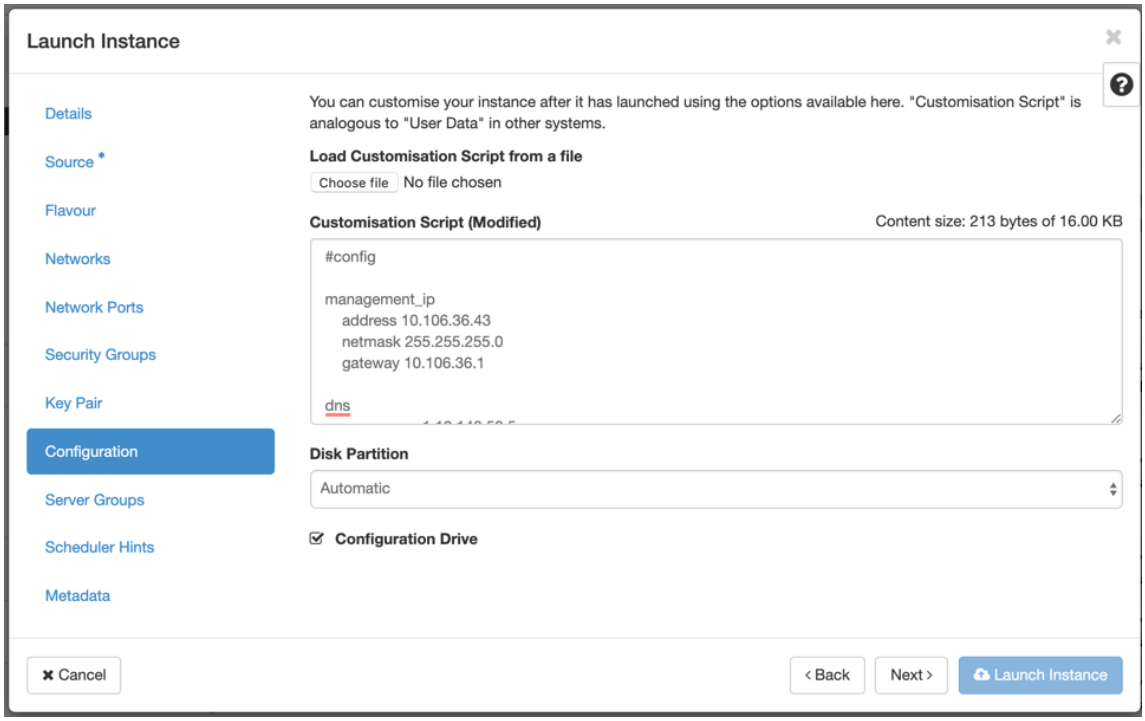


10. Seleccione un puerto de red para la instancia y haga clic en **Siguiente**. Los puertos de red proporcionan canales de comunicación adicionales a las instancias.

> **NOTA**
>
> Puede seleccionar puertos en lugar de redes o una combinación de ambos.



11. Vaya a **Configuración** y haga clic en **Elegir archivo**. Seleccione el archivo user_data. Puede ver la información **de IP de administración**, **DNS**y **número de serie** en el archivo user_data.
12. Marque la casilla **Unidad de configuración**. Al habilitar la unidad de configuración, puede colocar los metadatos del usuario dentro de la imagen.



13. Haga clic en **Iniciar instancia**.

Configurar la funcionalidad LTE en el dispositivo 210 SE LTE

August 26, 2022

Puede conectar un dispositivo Citrix SD-WAN 210-SE LTE a su red mediante una conexión LTE. En este tema se proporcionan detalles sobre la configuración de la banda ancha móvil, la configuración de los dispositivos de centro de datos y sucursales para LTE, etc. Para obtener más información sobre la plataforma de hardware Citrix SD-WAN 210-SE LTE, consulte Dispositivos Citrix SD-WAN 210 Standard Edition.

> **Nota**
>
> La conectividad LTE depende del operador de la SIM o de la red del proveedor de servicios. Para obtener información sobre cómo configurar y administrar los sitios LTE en su red, consulte Actualización de firmware LTE.

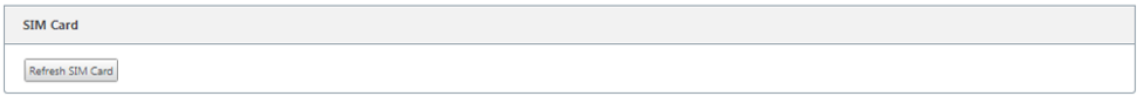
Introducción a Citrix SD-WAN 210-SE LTE

1. Inserte la tarjeta SIM en la ranura para tarjeta SIM del Citrix SD-WAN 210-SE LTE.

> **Nota:**
> Solo se admite una tarjeta SIM estándar o 2FF (15x25 mm).

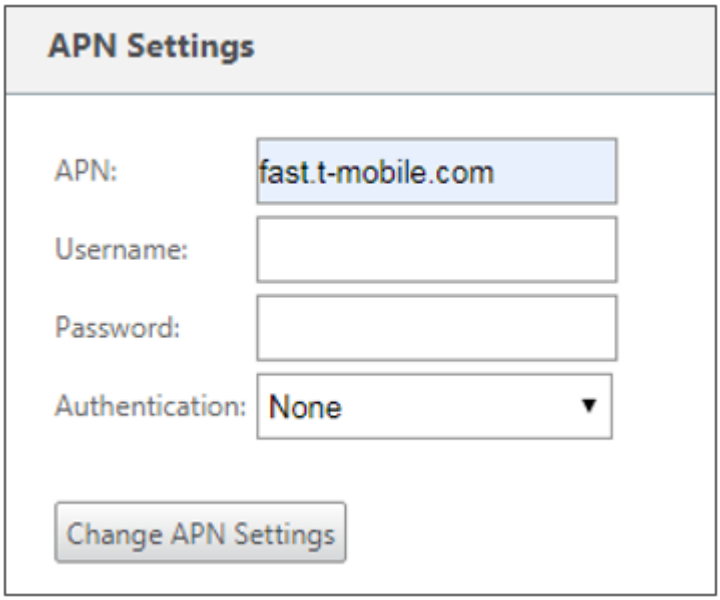
2. Corrija las antenas al dispositivo Citrix SD-WAN 210-SE LTE. Para obtener más información, consulte Instalación de antenas LTE.
3. Encienda el dispositivo.

> **Nota**
>
> Si ha insertado la SIM en un dispositivo que ya está encendido y arrancado, vaya a **Configuración > Configuración del dispositivo > Adaptadores de red > Banda ancha móvil > Tarjeta SIM** y haga clic en **Actualizar tarjeta SIM**.



4. Configure la configuración de APN. En la GUI de SD-WAN, vaya a **Configuración > Configuración del dispositivo > Adaptadores de red > Banda ancha móvil > Configuración de APN**.

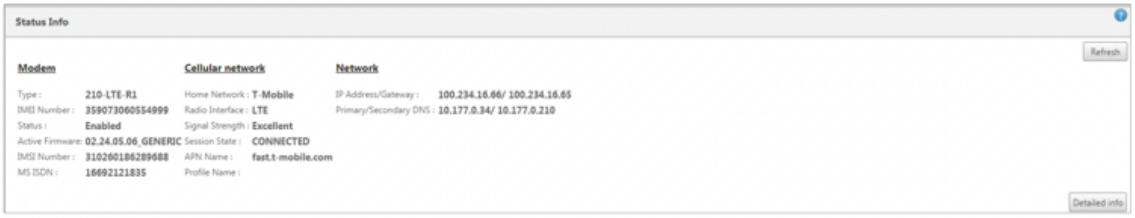
> **Nota:**
> Obtenga la información de APN del transportista.



5. Introduzca el **APN**, el nombre de **usuario**, **la contraseña** y la **autenticación** proporcionados por el operador. Puede elegir entre los protocolos de autenticación PAP, CHAP y PAPCHAP. Si el transportista no ha proporcionado ningún tipo de autenticación, establezca en **Ninguno**.
6. Haga clic en **Cambiar configuración de APN**.

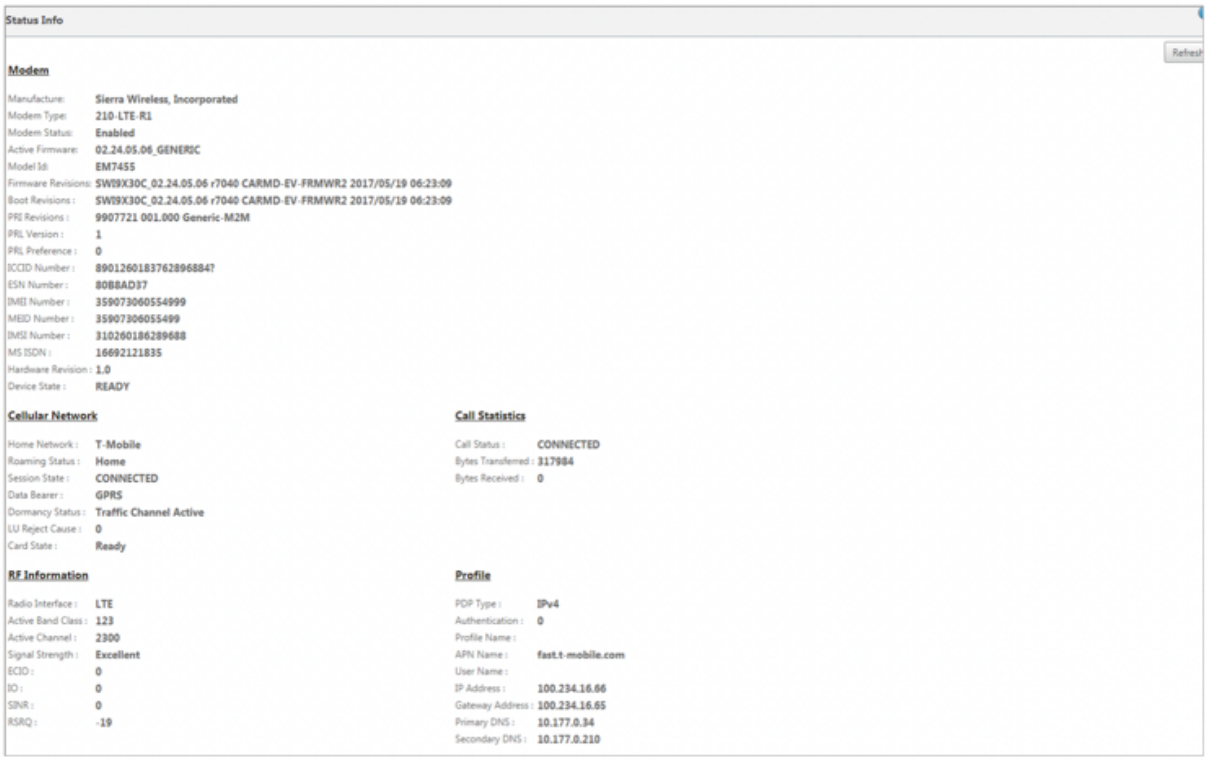
7. En la GUI del dispositivo SD-WAN, vaya a **Configuración > Configuración del dispositivo > Adaptadores de red > Banda ancha móvil**.

   Puede ver la información de estado de la configuración de banda ancha móvil.



A continuación se muestra información de estado útil:

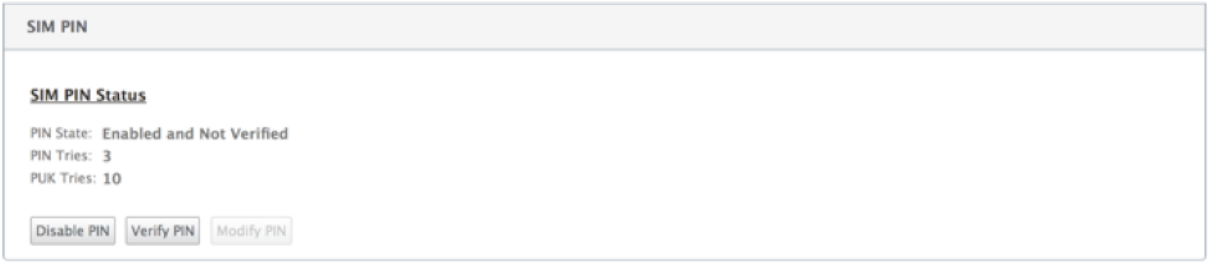
- **Modo de funcionamiento**: muestra el estado del módem.
- **SIM activa**: En cualquier momento, solo puede estar activa una SIM. Se muestra la SIM que está activa actualmente.
- **Estado de la tarjeta**: Presente indica que la SIM está correctamente insertada.
- **Fuerza de la señal**: Calidad de la intensidad de la señal: Excelente, buena, justa, pobre o sin señal.
- **Red doméstica**: portadora de la SIM insertada.
- **Nombre de APN: nombre**del punto de acceso utilizado por el módem LTE.
- **Estado de sesión**: Conectado indica que el dispositivo se ha unido a la red. Si el estado de la sesión está desconectado, compruebe con el operador si la cuenta se ha activado si el plan de datos está habilitado.



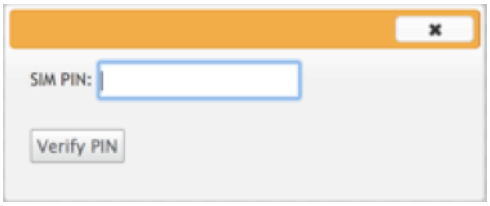
PIN de la SIM

Si ha insertado una tarjeta SIM que está bloqueada con un PIN, el estado de la SIM es Habilitado y** Estado No verificado. No puede usar la tarjeta SIM hasta que se verifique con el PIN de la SIM. Puede obtener el PIN de la tarjeta SIM del operador.

Para realizar operaciones de PIN de la SIM, vaya a **Configuración > Ajustes del dispositivo > Adaptadores de red > Banda ancha móvil > PIN de la SIM**.



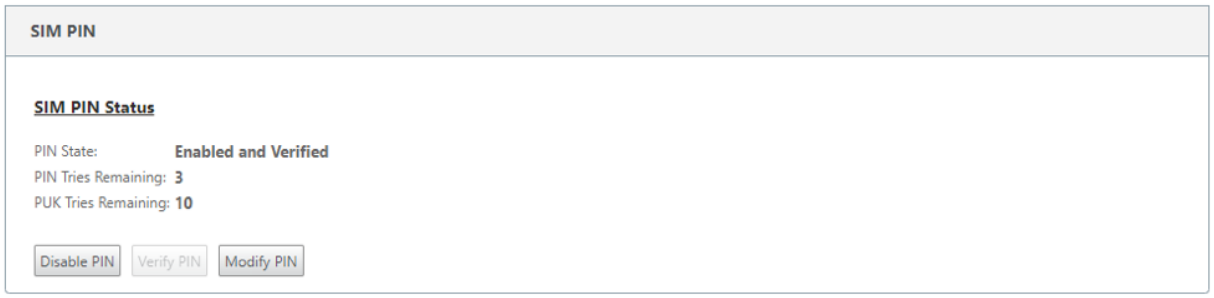
Haga clic en **Verificar PIN**. Introduzca el PIN de la SIM proporcionado por el operador y haga clic en **Verificar PIN**.

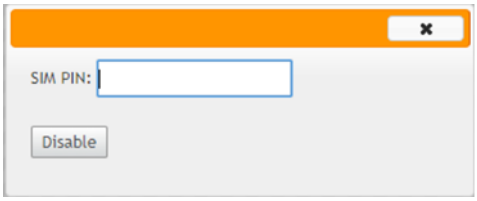


El estado cambia a **Habilitado y Verificado**.

Inhabilitar PIN de la SIM

Puede optar por inhabilitar la funcionalidad PIN de la SIM para una SIM para la que el PIN de la SIM esté habilitado y verificado.

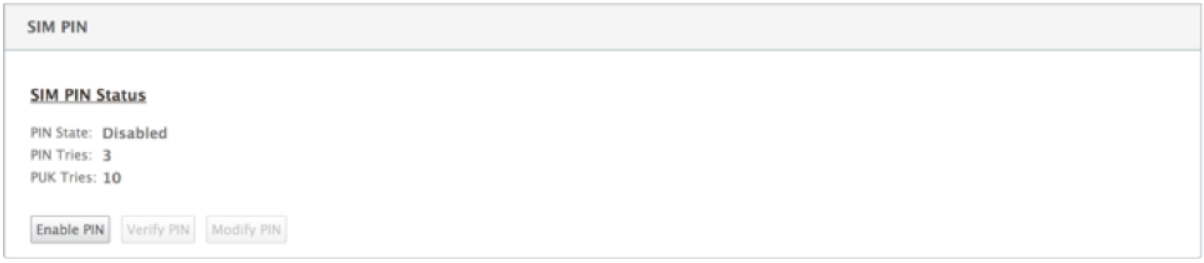




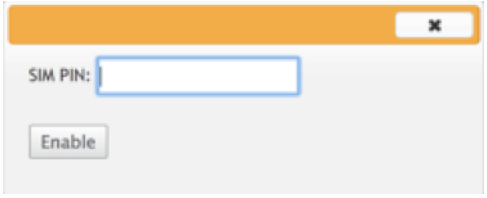
Haga clic en **Inhabilitar PIN**. Introduzca el **PIN de la SIM** y haga clic en **Inhabilitar**.

Habilitar PIN de la SIM

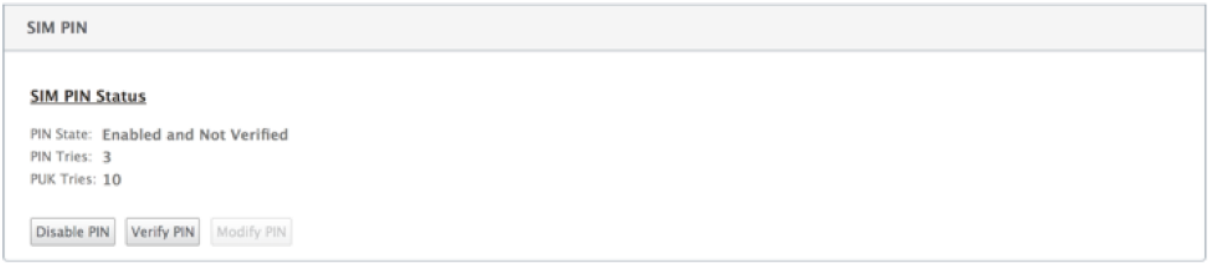
El PIN de la SIM se puede habilitar para la SIM para la que está inhabilitada.



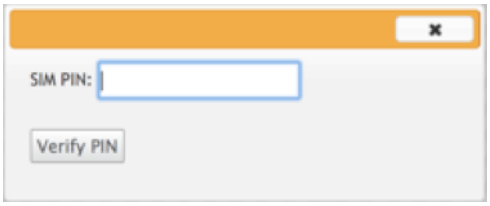
Haga clic en **Habilitar PIN**. Introduzca el PIN de la tarjeta SIM proporcionado por el operador y haga clic en **Habilitar**.



Si el estado del PIN de la SIM cambia a **Habilitado y No Verificado**, significa que el PIN no está verificado y que no puede realizar ninguna operación relacionada con LTE hasta que se verifique el PIN.

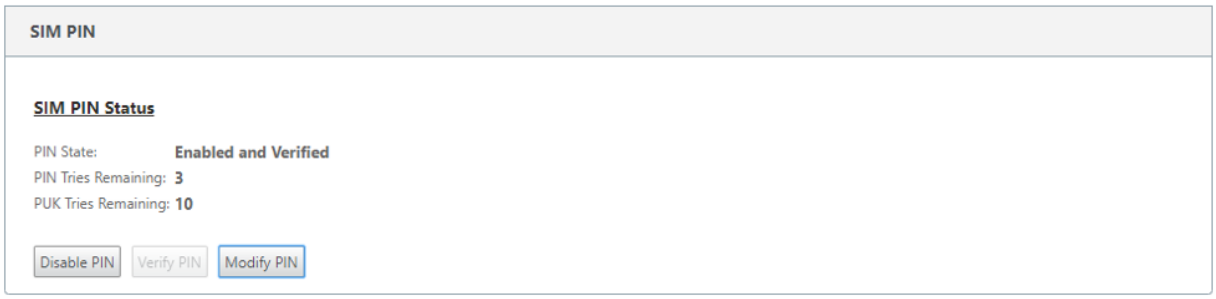


Haga clic en **Verificar PIN**. Introduce el PIN de la SIM proporcionado por el operador y haga clic en **Verificar PIN**.

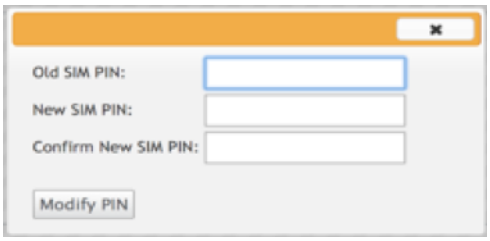


Modificar PIN de la SIM

Una vez que el PIN esté en estado **Habilitado y Verificado**, puede elegir cambiar el PIN.



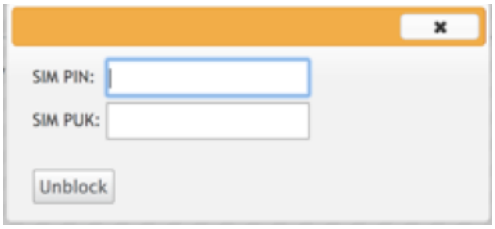
Haga clic en **Modificar PIN**. Introduzca el PIN de la tarjeta SIM proporcionado por el operador. Introduzca el nuevo PIN de la SIM y confírmelo. Haga clic en **Modificar PIN**.



Desbloquear SIM

Si olvida el PIN de la SIM, puede restablecer el PIN de la SIM mediante el PUK de la SIM obtenido del operador.

Para desbloquear una SIM, haga clic en **Desbloquear**. Introduzca el **PIN de la SIM y el PUK** de la SIM obtenidos del operador y haga clic en **Desbloquear**.



> **Nota:**
> La tarjeta SIM se bloquea permanentemente con 10 intentos fallidos de PUK, mientras se desbloquea la SIM. Póngase en contacto con el proveedor de servicios del operador para obtener una nueva tarjeta SIM.

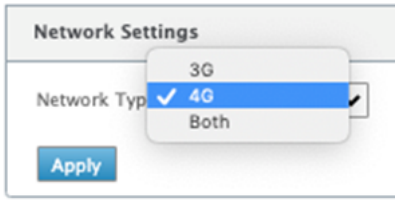
Administrar firmware

Cada equipo que tenga habilitado LTE dispondrá de un conjunto de firmware disponible. Puede seleccionar de la lista existente de firmware o cargar un firmware y aplicarlo.

Si no está seguro de qué firmware utilizar, seleccione la opción AUTO-SIM para permitir que el módem LTE elija el firmware más adecuado según la tarjeta SIM insertada.

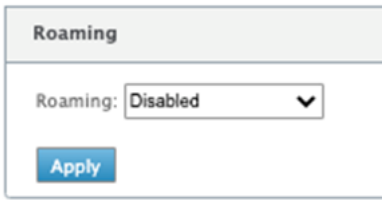
Configuración de red

Puede seleccionar la red móvil en los dispositivos Citrix SD-WAN que admiten módems LTE internos. Las redes admitidas son 3G, 4G o ambas.



Itinerancia

La opción de itinerancia está habilitada de forma predeterminada en sus dispositivos LTE, puede optar por inhabilitarla.



Activar/desactivar módem

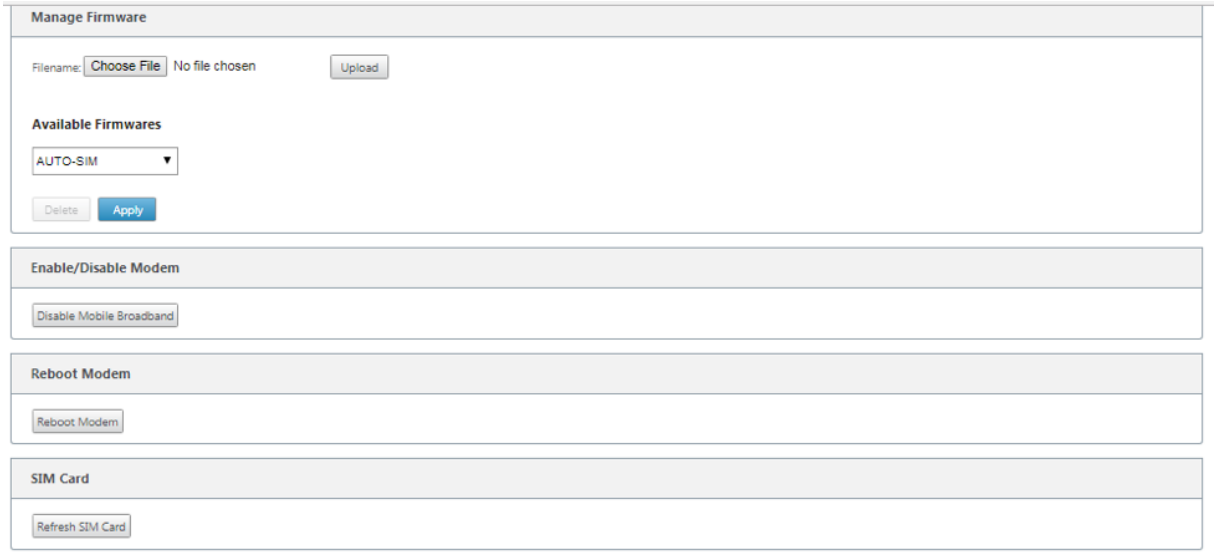
Habilitar/inhabilitar el módem en función de su intención de utilizar la funcionalidad LTE. De forma predeterminada, el módem LTE está habilitado.

Reiniciar el módem

Reinicia el módem. La operación de reinicio puede tardar entre 3 y 5 minutos en completarse.

Actualizar SIM

Utilice esta opción cuando cambie en caliente la tarjeta SIM para detectar la nueva tarjeta SIM mediante el módem 210-SE LTE.



Configurar la funcionalidad LTE mediante CLI

Para configurar el módem 210-SE LTE mediante la CLI.

1. Inicie sesión en la consola del dispositivo Citrix SD-WAN.
2. Cuando se le solicite, escriba el nombre de usuario y la contraseña para obtener acceso a la interfaz CLI.
3. En el símbolo del sistema, escriba el comando **lte**. Escriba **>help**. Muestra la lista de comandos LTE disponibles para la configuración.

```
site210>lte
lte>help
status                                  # Show status
show                                    # Show settings
disable                                 # Disable LTE modem
enable                                  # Enable LTE modem
apn <apn> [<user name> [<password> [<PAP|CHAP|PAPCHAP>]]]   # Set APN
sim-power <off|on|reset>                # Off, on, reset SIM card power
sim-pin <show>                          # SIM card pin status
sim-pin <verify|disable|enable> <sim pin> # Verify/Disable/Enable SIM card PIN
sim-pin <modify> <old pin> <new pin>    # Modify SIM card PIN
sim-pin <unblock> <sim puk> <sim pin>   # Unblock SIM card PIN
reboot                                  # Reboot modem
ping                                    # Check if modem manager ready
list-fw                                 # List available firmware
apply-fw <fw>                           # Apply the specified firmware
```

En la siguiente tabla se enumeran las descripciones de los comandos **LTE**.

Comando	Descripción
Help {lte>help}	Enumera los comandos y parámetros de LTE disponibles
Status {lte>status}	Muestra el estado de conectividad LTE
Show {lte>show}	Muestra la configuración de LTE
Disable {lte>disable}	Inhabilita el módem LTE
Enable {lte>enable}	Habilita el módem LTE
Apn {lte>apn}	Configura la información de configuración de APN
Sim-power off, on, reset>{lte>sim-power off,on,reset}	Apaga la tarjeta SIM, enciende la tarjeta SIM, actualiza la tarjeta SIM
SIM PIN {lte>sim-pin}	Apaga la tarjeta SIM, enciende la tarjeta SIM, actualiza la tarjeta SIM
Reboot {lte>reboot}	Reinicia el módem LTE
Ping {lte>ping}	Módem Pings LTE
List-fw {lte>list-fw}	Enumera el firmware disponible en los módems R1 o R2 LTE
Apply-fw {lte>apply-fw}	Aplica firmware específico a un operador

Implementación sin contacto a través de LTE

Requisitos previos para habilitar el servicio de implementación sin intervención a través de LTE

1. Instale la antena y la tarjeta SIM del equipo 210-SE LTE.
2. Asegúrese de que la tarjeta SIM tiene un plan de datos activado.
3. Asegúrese de que el puerto de administración no está conectado.
    - Si el puerto de administración está conectado, desconecte el puerto de administración y, a continuación, reinicie el dispositivo.
    - Si se configura una dirección IP estática en la interfaz de administración, debe configurar la interfaz de administración con DHCP, aplicar la configuración y, a continuación, desconectar el puerto de administración y reiniciar el dispositivo.
4. Asegúrese de que la configuración del dispositivo 210-SE tenga definido el servicio de Internet para la interfaz LTE.

Cuando el dispositivo está encendido, el servicio de implementación sin intervención utiliza el puerto LTE para obtener el software SD-WAN y la configuración de SD-WAN más recientes solo cuando el

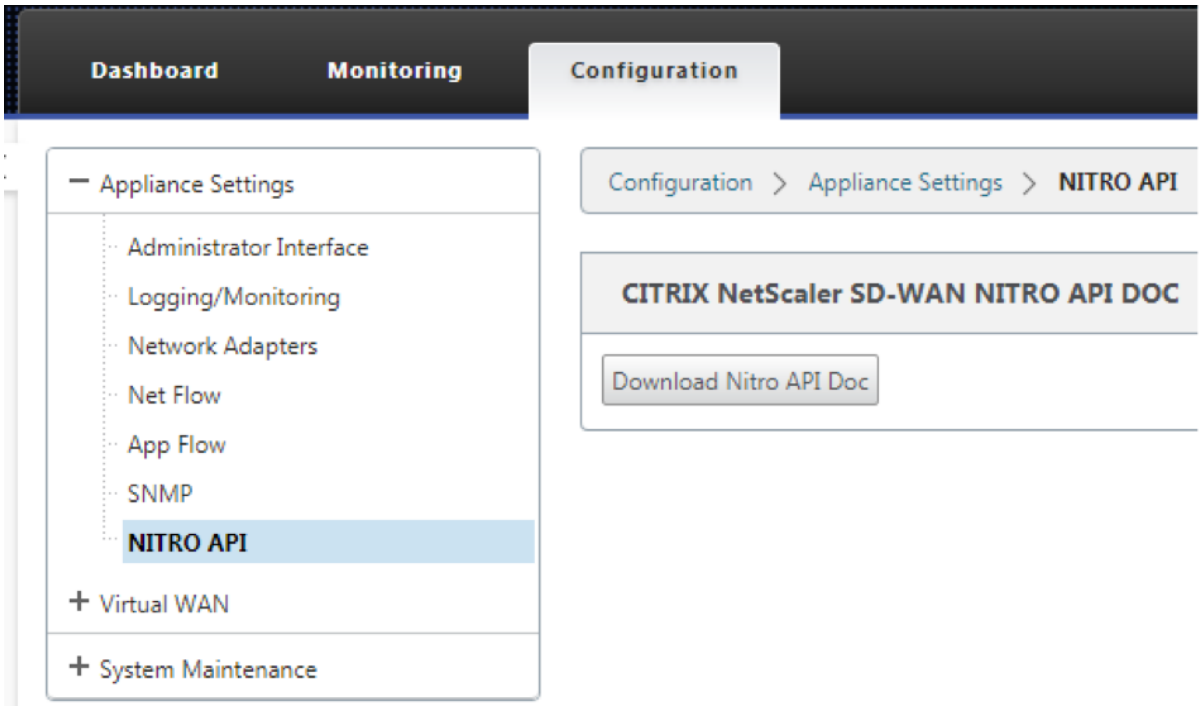
puerto de administración no se ha conectado.

Implementación sin contacto Servicio a través de interfaz de administración para el dispositivo LTE 210-SE

Conecte el puerto de administración y utilice el procedimiento de implementación sin intervención estándar compatible con todas las demás plataformas que no sean LTE.

LTE REST API

Para obtener información sobre la API de REST de LTE, vaya a la GUI de SD-WAN y vaya a **Configuración > Configuración del dispositivo > API NITRO**. Haga clic en **Descargar Nitro API** Doc. La API de REST para la funcionalidad PIN de la SIM se introduce en Citrix SD-WAN 11.0.



Comandos AT

Los comandos AT ayudan a supervisar y solucionar problemas de configuración y estado del módem LTE. AT es la abreviatura de **Attension**. Como todas las líneas de comandos empiezan **por at**, se denominan comandos AT. Los modelos de plataforma Citrix SD-WAN compatibles con LTE admiten la ejecución de comandos AT. Los comandos AT son específicos del módem y, por lo tanto, la lista de comandos AT varía según la plataforma.

Para ejecutar comandos AT, lleve a cabo los siguientes pasos:

1. Inicie sesión en la consola del dispositivo Citrix SD-WAN.
2. Cuando se le solicite, escriba el nombre de usuario y la contraseña para obtener acceso a la interfaz CLI.
3. En la solicitud, escriba **lte**.
4. Escriba **at** y, a continuación, el comando AT.

A continuación, se muestra un ejemplo:

- **at at+cpin**: Proporciona información sobre el estado de la SIM.

```
lte> at at+cpin?
Running at+cpin? command
AT command state: success
  +CPIN: READY
  OK
success
```

- **at! gstatus**: Proporciona información sobre el estado del módem LTE.

```
lte> at at!gstatus?
Running at!gstatus? command
AT command state: success
  !GSTATUS:
  Current Time:  1279298                Temperature: 62
  Reset Counter: 1              Mode:         ONLINE
  System mode:   LTE            PS state:     Attached
  LTE band:      B5                     LTE bw:       10 MHz
  LTE Rx chan:   2559           LTE Tx chan: 20559
  LTE CA state:  NOT ASSIGNED
  EMM state:     Registered             Normal Service
  RRC state:     RRC Connected
  IMS reg state: Full Srv               IMS mode:     Normal
  PCC RxM RSSI:  -73            RSRP (dBm):  -112
  PCC RxD RSSI:  -73            RSRP (dBm):  -107
  Tx Power:      --             TAC:          1F00 (7936)
  RSRQ (dB):     -17.3          Cell ID:      00798912 (7964946)
  SINR (dB):      0.2
  OK
Success
```

- **at! impref?** - Proporciona información sobre el firmware del módem y el operador de red.


```
lte> at at!impref?
Running at!impref? command
AT command state: success
  !IMPREF:
   preferred fw version:    00.00.00.00
   preferred carrier name:  AUTO-SIM
   preferred config name:   AUTO-SIM_000.000_000
   preferred subpri index:  000
   current fw version:      02.33.03.00
   current carrier name:    VERIZON
   current config name:     VERIZON_002.079_001
   current subpri index:    000
  OK
success
```

Configurar la funcionalidad LTE en el dispositivo 110-LTE-WiFi

August 26, 2022

Puede conectar un dispositivo Citrix SD-WAN 110-LTE-WiFi a la red mediante una conexión LTE. En este tema se proporcionan detalles sobre la configuración de la banda ancha móvil, la configuración de los dispositivos de centro de datos y sucursales para LTE, etc. Para obtener más información sobre la plataforma de hardware Citrix 110-LTE-WiFi, consulte Dispositivos Citrix SD-WAN 110 Standard Edition.

> **Nota**
>
> - La conectividad LTE depende del operador de la SIM o de la red del proveedor de servicios.
> - Para obtener información sobre cómo configurar y administrar todos los sitios LTE de su red, consulte Plantilla de firmware LTE.

Introducción a Citrix SD-WAN 110-LTE-WiFi

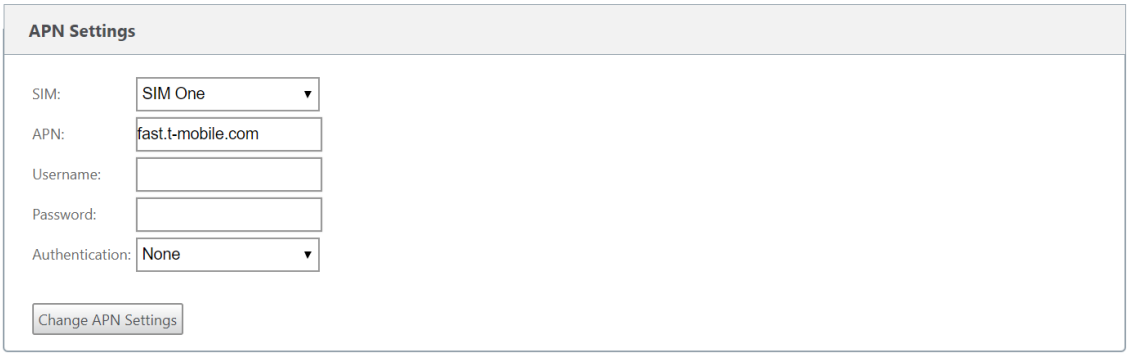
1. Encienda el dispositivo e inserte la tarjeta SIM en la ranura para tarjeta SIM del dispositivo Citrix SD-WAN 110-LTE-WiFi.

   > **Nota**
   >
   > El dispositivo Citrix SD-WAN 110-LTE-WiFi tiene dos ranuras SIM estándar (2FF). Para utilizar SIM de tamaño Micro (3FF) y Nano (4FF), utilice un adaptador SIM. Conecte la SIM más pequeña en el adaptador. Puede obtener el adaptador de Citrix como una unidad reem-

> plazable en campo (FRU) o del proveedor de SIM.

2. Fije las antenas al dispositivo Citrix SD-WAN 110-LTE-WiFi. Para obtener más información, consulte Instalación de antenas LTE.
3. Encienda el dispositivo.
4. Configure la configuración de APN. En la GUI de SD-WAN, vaya a **Configuración > Configuración del dispositivo > Adaptadores de red > Banda ancha móvil > Configuración de APN**.

   > **Nota**
   >
   > Obtenga la información de APN del transportista.

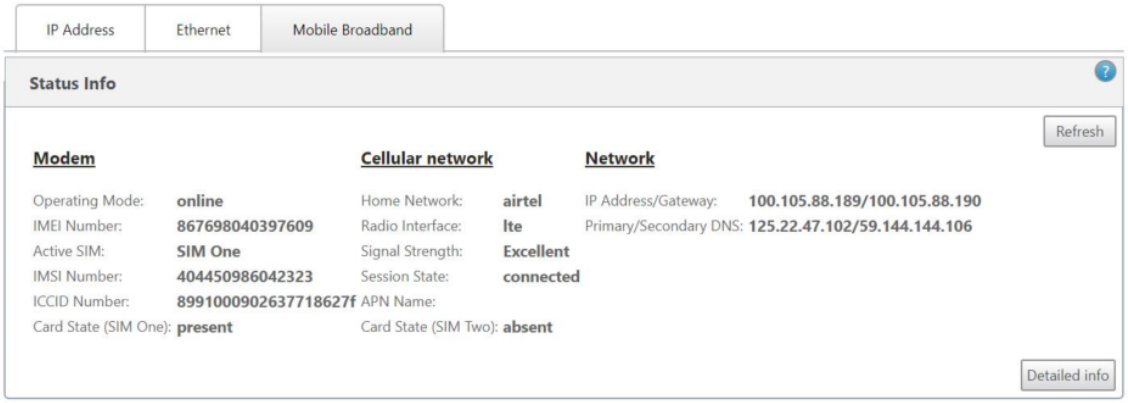
   

5. Seleccione la tarjeta SIM, introduce el **APN**, el **nombre de usuario**, la **contraseña** y la **autenticación** proporcionados por el operador. Puede elegir entre los protocolos de autenticación PAP, CHAP y PAPCHAP. Si el transportista no ha proporcionado ningún tipo de autenticación, establezca en **Ninguno**.

   > **Nota**
   >
   > Todos estos campos son opcionales.

6. Haga clic en **Cambiar configuración de APN**.
7. En la GUI del dispositivo SD-WAN, vaya a **Configuración > Configuración** > **Configuración del dispositivo** > **Adaptadores de red** > **Banda ancha móvil**.

   Puede ver la información de estado de la configuración de banda ancha móvil.



A continuación se muestra información de estado útil:

- **Modo de funcionamiento**: muestra el estado del módem.
- **SIM activa**: En cualquier momento, solo puede estar activa una SIM. Se muestra la SIM que está activa actualmente.
- **Estado de la tarjeta**: Presente indica que la SIM está correctamente insertada.
- **Fuerza de la señal**: Calidad de la intensidad de la señal: Excelente, buena, justa, pobre o sin señal.
- **Red doméstica**: portadora de la SIM insertada.
- **Nombre de APN: nombre**del punto de acceso utilizado por el módem LTE.
- **Estado de sesión**: Conectado indica que el dispositivo se ha unido a la red. Si el estado de la sesión está desconectado, compruebe con el operador si la cuenta está activada y el plan de datos está habilitado.

Preferencia de SIM

Puede insertar dos SIMs en un dispositivo Citrix SD-WAN 110-LTE-WiFi. En un momento dado, solo hay una SIM activa. Seleccione la **preferencia de SIM**:

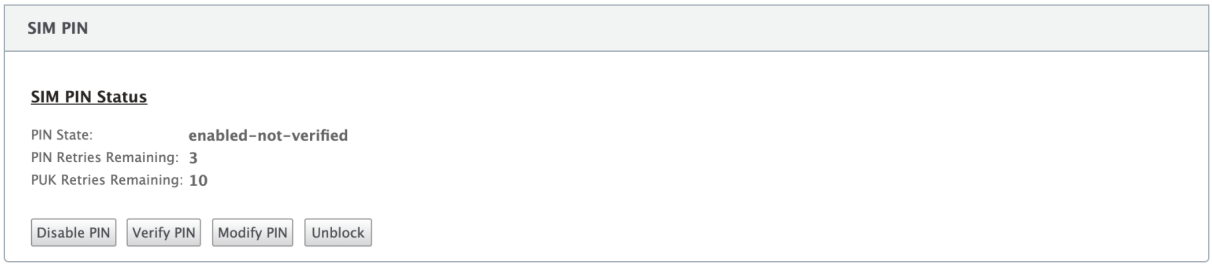
- **Se prefiere SIM One**: Si se insertan dos SIM, al arrancar el módem LTE utilizará SIM One, si está disponible. Cuando el módem LTE está activo y en funcionamiento, utiliza la SIM (SIM uno o SIM dos) que se pueda utilizar en ese momento. Continúa utilizándolo hasta que la SIM esté activa.
- **SIM Dos preferidos**: si se insertan dos SIM, al arrancar el módem LTE utiliza SIM Two, si está disponible. Cuando el módem LTE está activo y en funcionamiento, utiliza la SIM (SIM uno o SIM dos) que se pueda utilizar en ese momento. Continúa utilizándolo hasta que la SIM esté activa.
- **SIM One**: Solo se utiliza SIM One, independientemente del estado de la SIM en ambas ranuras SIM. SIM One siempre está activo.
- **SIM Dos**: Solo se utiliza SIM Two, independientemente del estado de la SIM en ambas ranuras SIM. SIM dos siempre está activo.

PIN de la SIM

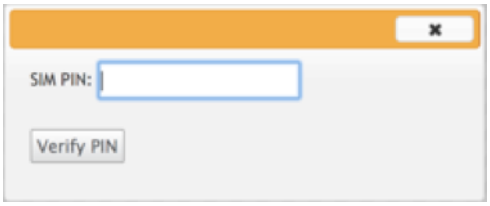
Si ha insertado una tarjeta SIM que está bloqueada con un PIN, el estado de la **SIM es activado, no verificado**. No puede usar la tarjeta SIM hasta que se verifique con el PIN de la SIM. Puede obtener el PIN de la tarjeta SIM del operador.

> **Nota**
>
> Las operaciones del PIN de la SIM son aplicables únicamente a la SIM activa.

Para realizar operaciones de PIN de la SIM, vaya a **Configuración > Ajustes del dispositivo > Adaptadores de red > Banda ancha móvil > PIN de la SIM**.



Haga clic en **Verificar PIN**. Introduce el PIN de la SIM proporcionado por el operador y haga clic en **Verificar PIN**.

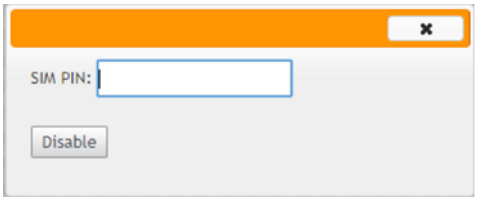


El estado cambia a **habilitado-verificado**.

Inhabilitar PIN de la SIM

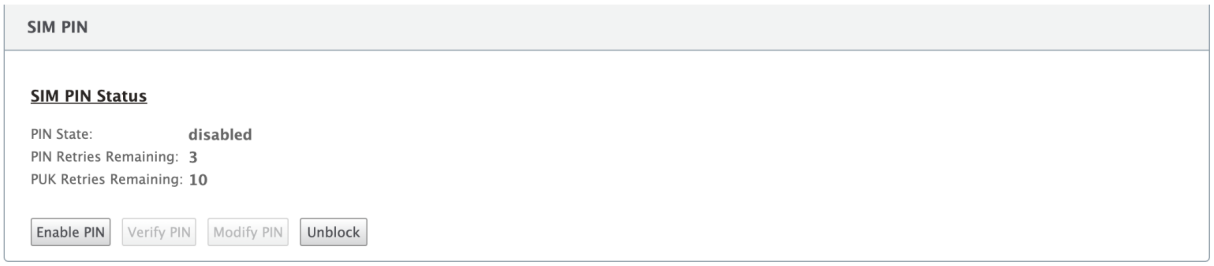
Puede optar por inhabilitar la funcionalidad PIN de la SIM para una SIM para la que el PIN de la SIM esté habilitado y verificado.

Haga clic en **Inhabilitar PIN**. Introduzca el **PIN de la SIM** y haga clic en **Inhabilitar**.

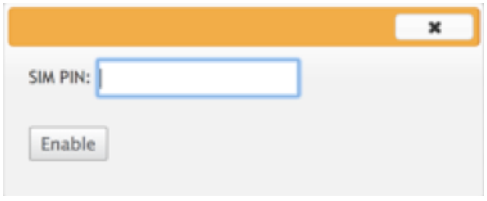


Habilitar PIN de la SIM

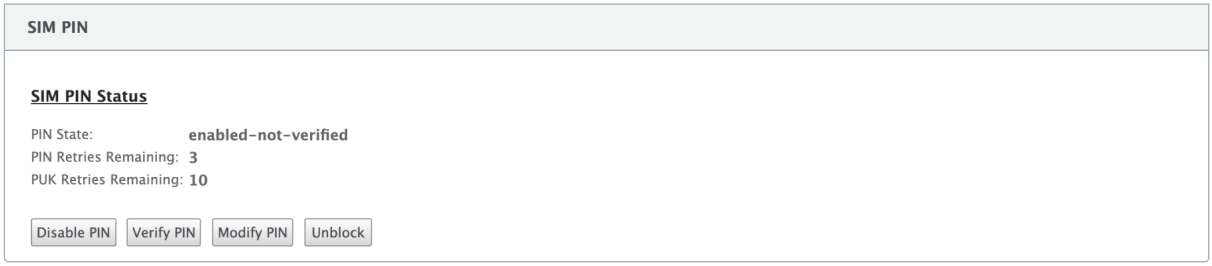
El PIN de la SIM se puede habilitar para la SIM para la que está inhabilitada.



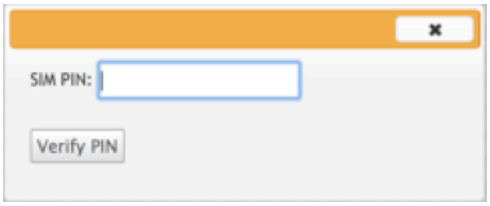
Haga clic en **Habilitar PIN**. Introduzca el PIN de la tarjeta SIM proporcionado por el operador y haga clic en **Habilitar**.



Si el estado del PIN de la SIM cambia a **habilitado-no-verificado**, significa que el PIN no está verificado y no podrá realizar ninguna operación relacionada con LTE hasta que se verifique el PIN.



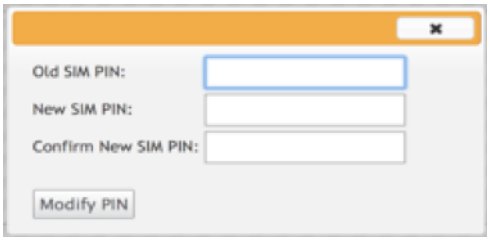
Haga clic en **Verificar PIN**. Introduce el PIN de la SIM proporcionado por el operador y haga clic en **Verificar PIN**.



Modificar PIN de la SIM

Una vez que el PIN esté en estado **verificado habilitado**, puede optar por cambiar el PIN.

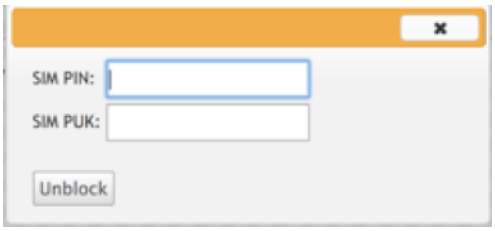
Haga clic en **Modificar PIN**. Introduzca el PIN de la tarjeta SIM proporcionado por el operador. Introduzca el nuevo PIN de la SIM y confírmelo. Haga clic en **Modificar PIN**.



Desbloquear SIM

Si olvida el PIN de la SIM, puede restablecer el PIN de la SIM mediante el PUK de la SIM obtenido del operador.

Para desbloquear una SIM, haga clic en **Desbloquear**. Introduzca el **PIN de la SIM** que quiera. Introduzca el **PUK de la SIM** obtenido del operador y haga clic en **Desbloquear**.



> **Nota:**
> La tarjeta SIM se bloquea permanentemente con 10 intentos fallidos de PUK, mientras se desbloquea la SIM. Debes ponerse en contacto con el proveedor de servicios del operador para obtener una nueva tarjeta SIM.

Configuración de red

Puede seleccionar la red móvil en los dispositivos Citrix SD-WAN que admiten módems LTE internos. Las redes admitidas son 3G, 4G o ambas.

Itinerancia

La opción de itinerancia está habilitada de forma predeterminada en sus dispositivos LTE, puede optar por inhabilitarla.

Activar/desactivar módem

Habilitar/inhabilitar el módem según su intención de utilizar la funcionalidad LTE. De forma predeterminada, el módem LTE está habilitado.

Reiniciar el módem

Reinicia el módem. La operación de reinicio puede tardar hasta 7 minutos en completarse.

Actualizar SIM

Utilice esta opción cuando la tarjeta SIM no sea detectada correctamente por el módem 110-LTE-WiFi.

> **Nota**
>
> La operación Actualizar SIM solo se aplica a la SIM activa.

Configurar la funcionalidad LTE mediante CLI

Para configurar el módem 110-LTE-WiFi mediante CLI.

1. Inicie sesión en la consola del dispositivo Citrix SD-WAN.
2. Cuando se le solicite, escriba el nombre de usuario y la contraseña para obtener acceso a la interfaz CLI.
3. En el símbolo del sistema, escriba el comando **lte**. Escriba **>help**. Muestra la lista de comandos LTE disponibles para la configuración.

```
lte> help
Usage
    ?|help                                      # Print this message
    status [default|verbose]                    # Show status
    show                                        # Show configuration
    select [1|2] [1|2]                          # Show or choose modem and/or sim to work
    enable                                      # Enable the selected modem
    disable                                     # Disable the selected modem
    apn <apn> [<username> [<password> [<NONE|PAP|CHAP|PAPCHAP>]]]   # Set APN
    sim-prefer <prefer|use> <1|2>               # Prefer to use or use SIM one or two
    sim-power <show|off|on|reset>               # Show, off, on, reset SIM card power
    sim-pin <show>                              # SIM card pin status
    sim-pin <verify|disable|enable> <sim pin> # Verify/Disable/Enable SIM card PIN
    sim-pin <modify> <old pin> <new pin>        # Modify SIM card PIN
    sim-pin <unblock> <sim puk> <sim pin>       # Unblock SIM card PIN
    reboot                                      # Reboot modem
    list-fw                                     # List available firmware
    upload-fw <fw file>                         # Upload firmware file
    apply-fw <fw> [keep-AUTO-SIM]               # Apply firmware
    delete-fw <fw>                              # Delete firmware
    session <show|stop|start>                   # Show/stop/start data session
    exit|quit                                   # Exit LTE CLI
```

En la siguiente tabla se enumeran las descripciones de los comandos **LTE**.

Comando	Descripción
Help {lte>help}	Enumera los comandos y parámetros de LTE disponibles
Status {lte>status}	Muestra el estado de conectividad LTE
Show {lte>show}	Muestra la configuración de LTE
Disable {lte>disable}	Inhabilita el módem LTE
Enable {lte>enable}	Habilita el módem LTE
Apn {lte>apn}	Configura la información de configuración de APN
Sim-power off, on, reset>{lte>sim-power off,on,reset}	Se apaga la tarjeta SIM, se enciende la tarjeta SIM, se actualiza la tarjeta SIM
Seleccione [1l2] [1l2] {lte>select [1l2] [1l2]}	Seleccione la SIM para el módem LTE.
SIM-prefer {lte>sim-prefer}	Seleccione la SIM preferida o que se va a utilizar.
SIM PIN {lte>sim-pin}	Operaciones relacionadas con PIN de la SIM

Comando	Descripción
Reboot {lte>reboot}	Reinicia el módem LTE

> **Nota**
>
> Las operaciones relacionadas con el firmware no son compatibles con el dispositivo 110-LTE-WiFi.

Implementación sin contacto a través de LTE

El dispositivo SD-WAN 110 SE admite el Provisioning día-0 y la administración día-n de los dispositivos SD-WAN a través de los puertos de administración y datos

Requisitos previos para habilitar el servicio de implementación sin contacto a través de LTE:

1. Instale la antena, encienda el dispositivo e inserte la tarjeta SIM.
2. Asegúrese de que la tarjeta SIM tiene un plan de datos activado.
3. Asegúrese de que el puerto de administración/datos no está conectado.
    - Si el puerto de administración/datos está conectado, desconecte el puerto de administración/datos.
    - Si se configura una dirección IP estática en la interfaz de administración/datos, debe configurar la interfaz de administración/datos con DHCP, aplicar la configuración y, a continuación, desconectar el puerto de administración/datos.
4. Asegúrese de que la configuración del dispositivo 110-LTE-WiFi tenga el servicio de Internet definido para la interfaz LTE.

Cuando el dispositivo está encendido, el servicio de implementación sin contacto utiliza el puerto LTE para obtener el software SD-WAN más reciente y la configuración SD-WAN.

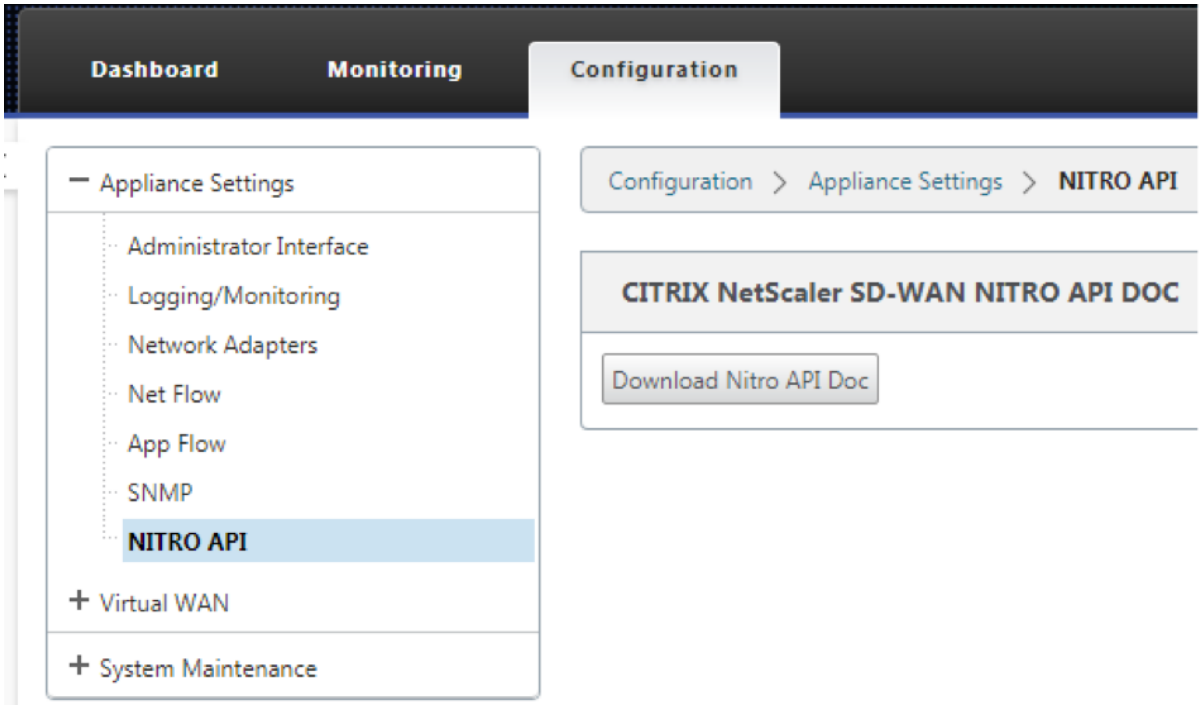
Implementación sin contacto Servicio a través de la interfaz de administración/datos para el dispositivo LTE 110-SE

Conecte el puerto de administración/datos a Internet y utilice el procedimiento de implementación sin intervención estándar que se admite en todas las demás plataformas que no sean LTE.

LTE REST API

Para obtener información sobre la API de REST de LTE, vaya a la GUI de SD-WAN y vaya a **Configuración > Configuración del dispositivo > API NITRO**. Haga clic en **Descargar Nitro API** Doc. La API de REST

para la funcionalidad PIN de la SIM se introduce en Citrix SD-WAN 11.0.



Comandos AT

Los comandos AT ayudan a supervisar y solucionar problemas de configuración y estado del módem LTE. AT es la abreviatura de **Attension**. Como todas las líneas de comandos empiezan **por at**, se denominan comandos AT. Los modelos de plataforma Citrix SD-WAN compatibles con LTE admiten la ejecución de comandos AT. Los comandos AT son específicos del módem y, por lo tanto, la lista de comandos AT varía según la plataforma.

Para ejecutar comandos AT, lleve a cabo los siguientes pasos:

1. Inicie sesión en la consola del dispositivo Citrix SD-WAN.
2. Cuando se le solicite, escriba el nombre de usuario y la contraseña para obtener acceso a la interfaz CLI.
3. En la solicitud, escriba **lte**.
4. Escriba **at** y, a continuación, el comando AT.

A continuación, se muestra un ejemplo:

- **at at+cpin**: Proporciona información sobre el estado de la SIM.


```
lte> at at+cpin?
Running at+cpin? command
AT command state: success
  +CPIN: READY
  OK
success
```

Configurar módem USB LTE externo

August 26, 2022

Puede conectar un módem USB 3G/4G externo en determinados dispositivos Citrix SD-WAN. Los dispositivos utilizan la red 3G/4G junto con otras conexiones para formar una red virtual que agrega ancho de banda y proporciona resistencia. Si hay un error de conectividad en las otras interfaces, el tráfico se redirige automáticamente a través del módem USB LTE. Los siguientes dispositivos admiten un módem USB externo:

- Citrix SD-WAN 210 SE
- Citrix SD-WAN 210 SE LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 Wifi SE
- Citrix SD-WAN 110 LTE Wifi SE
- Citrix SD-WAN 1100 SE
- Citrix SD-WAN 2100 SE

Los dispositivos Citrix SD-WAN 210 SE LTE y Citrix SD-WAN 110 LTE Wi-Fi SE tienen un módem LTE integrado. Estos dispositivos admiten LTE dual activo.

CDC Ethernet, MBIM y NCM son los tres tipos de módems USB externos soportados. Puede configurar los ajustes de **APN** y Activar/Inhabilitar módem en los módems USB MBIM y NCM. Las operaciones de banda ancha móvil no son compatibles con los módems USB CDC Ethernet.

> **Nota**
>
> Las dongles LTE externas con el tipo de módem como MBIM no funcionan en la plataforma Citrix SD-WAN 2100.

Conexión del módem USB

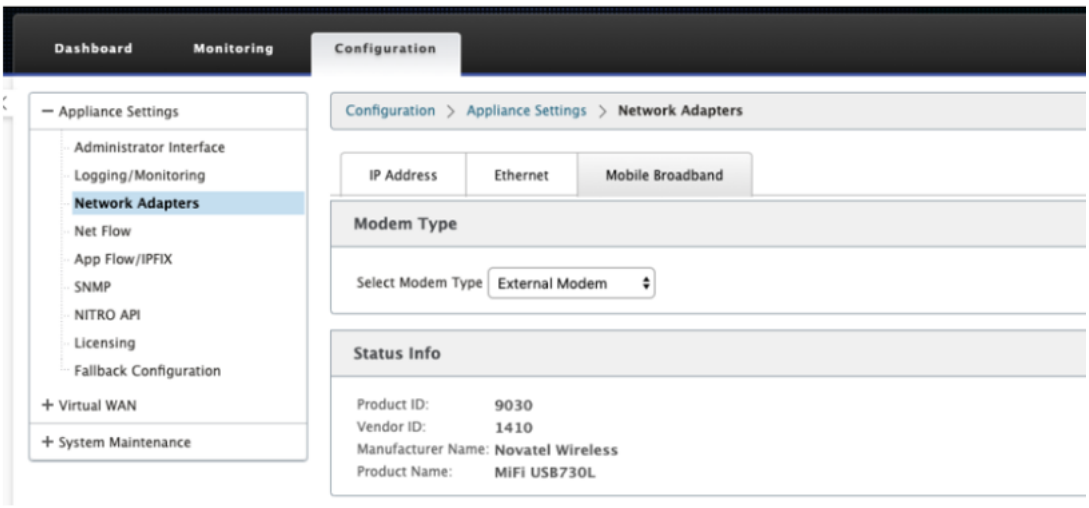
Habilite y pruebe el módem USB de acuerdo con las directrices proporcionadas por su operador de telefonía móvil.

Requisitos previos para módem LTE externo:

- Utilice los dongles USB LTE compatibles. Los modelos de hardware de dongle compatibles son Verizon USB730L y AT&T USB800.
- Asegúrese de que se inserta una tarjeta SIM en el dongle USB LTE. Los dongles CDC Ethernet LTE están preconfigurados con una dirección IP estática, esto interfiere con la configuración y causa un fallo de conexión o una conexión intermitente, si no se inserta la tarjeta SIM.
- Antes de insertar un dongle CDC Ethernet LTE en el dispositivo SD-WAN, conecte la memoria USB externa a una máquina Windows/Linux y asegúrese de que Internet funciona correctamente con la configuración adecuada de APN y Mobile Data Roaming. Asegúrese de que el **modo de conexión** del dongle USB cambia del valor predeterminado **Manual** a **Auto**.

> **Nota**
>
> - Los dispositivos Citrix SD-WAN solo admiten un dongle USB LTE a la vez. Si hay más de un dongle USB enchufado, desconecte todos los dongles y conecte solo un dongle.
> - Los dispositivos Citrix SD-WAN no admiten el nombre de usuario y la contraseña para módems USB. Asegúrese de que la función de nombre de usuario y contraseña estén inhabilitadas en el módem durante la instalación.
> - Desconectar o reiniciar un dongle MBIM externo afecta a la sesión de datos del módem LTE interna. Este es un comportamiento esperado.
> - Cuando se conecta un módem LTE externo, el dispositivo SD-WAN tarda unos 3 minutos en reconocerlo.

Para ver los detalles del módem externo, en la interfaz de usuario del dispositivo vaya a **Configuración** > **Configuración del dispositivo** > **Adaptadores de red** > **Banda ancha móvil**. Seleccione **Módem externo** como tipo de módem.



> **Nota**
>
> El número de modelo de la llave de hardware USB LTE no se muestra en la sección **Información de estado**.

Operaciones de banda ancha móvil

Operaciones compatibles con módems externos CDC Ethernet y MBIM/NCM:

Operaciones	Módem externo - CDC Ethernet	Módem externo - MBIM y NCM
Preferencia de SIM	No	No
PIN de la SIM	No	No
Configuración de APN	No	Sí
Configuración de la red	No	No
Itinerancia	No	No
Administrar firmware	No	No
Activar/desactivar módem	No	Sí
Reiniciar el módem	No	No
Actualizar SIM	No	No

Configurar el módem USB externo

Puede configurar un sitio LTE mediante un módem USB externo a través de Citrix SD-WAN Orchestrator Service. Para obtener más información, consulta Actualización de firmware LTE.

Implementación sin contacto a través de LTE

Requisitos previos para habilitar el servicio de implementación sin contacto a través del módem USB LTE:

- Inserte el módem USB en el dispositivo Citrix SD-WAN. Para obtener más información, consulte Conexión del módem USB.
- Asegúrese de que la tarjeta SIM del módem USB tenga un plan de datos activado.
- Asegúrese de que el puerto de administración/datos no está conectado. Si el puerto de administración/datos está conectado, desconéctelo.
- Asegúrese de que la configuración del dispositivo tenga el servicio de Internet definido para la interfaz LTE.

Cuando el dispositivo está encendido, el servicio de implementación sin contacto utiliza el puerto LTE-E1 para obtener la configuración y el software SD-WAN más recientes.

Para obtener información sobre la implementación sin intervención a través de SD-WAN Orchestrator Service, consulte Implementación sin intervención.

Módems USB compatibles

Los siguientes módems son compatibles con los dispositivos Citrix SD-WAN.

> **Nota**
>
> Citrix no controla las actualizaciones del firmware del operador inalámbrico. Por lo tanto, no se garantiza la compatibilidad del nuevo firmware del módem con el software Citrix SD-WAN. El cliente controla la actualización del firmware del módem. Citrix recomienda probar una actualización de firmware en un solo sitio antes de insertarla en toda la red.

Región	Portadora inalámbrica/Fabricante	Módem USB	Tipo de módem admitido	Interfaces
ESTADOS UNIDOS	Verizon	Módem global USB730L	cdc_ether	Solo 4G
ESTADOS UNIDOS	AT&T	Módem global AT&T USB800	cdc_ether	Solo 4G

Comandos AT

Los comandos AT ayudan a supervisar y solucionar problemas de configuración y estado del módem LTE. AT es la abreviatura de **Attension**. Como todas las líneas de comandos empiezan **por at**, se denominan comandos AT. Los modelos de plataforma Citrix SD-WAN compatibles con LTE admiten la

ejecución de comandos AT. Los comandos AT son específicos del módem y, por lo tanto, la lista de comandos AT varía según la plataforma.

Para ejecutar comandos AT, lleve a cabo los siguientes pasos:

1. Inicie sesión en la consola del dispositivo Citrix SD-WAN.
2. Cuando se le solicite, escriba el nombre de usuario y la contraseña para obtener acceso a la interfaz CLI.
3. En la solicitud, escriba **lte**.
4. Escriba **at** y, a continuación, el comando AT.

A continuación, se muestra un ejemplo:

at at+cpin: Proporciona información sobre el estado de la SIM.

```
lte> at at+cpin?
Running at+cpin? command
AT command state: success
  +CPIN: READY
  OK
success
```

Implementaciones

August 26, 2022

A continuación se presentan algunos de los casos de uso implementados mediante los dispositivos Citrix SD-WAN:

- Implementación de SD-WAN en modo de puerta de enlace
- Modo en línea
- Implementación de SD-WAN en modo PBR (modo virtual en línea)
- Rutas dinámicas para la comunicación de sucursal a sucursal
- Reenvío de WAN a WAN
- Creación de una red SD-WAN
- Redirección para segmentación LAN
- Implementación de Zero Touch

- Implementación de región única
- Implementación multiregión
- Alta disponibilidad

Lista de comprobación y cómo llevas a cabo implementaciones

August 26, 2022

Se recomienda encarecidamente que, antes de comenzar la instalación, lea primero la Guía de planificación de la implementación de Citrix Virtual WAN. En este artículo se describen los conceptos y funciones esenciales de la WAN virtual y se proporcionan pautas para planificar la implementación.

Prepararse para la implementación

La siguiente lista describe los pasos y procedimientos necesarios para implementar las ediciones estándar de SD-WAN.

Para ver algunos de los casos de uso de implementación, consulte Implementaciones.

1. Recopile la información de implementación de Citrix SD-WAN.
2. Configure los dispositivos Citrix SD-WAN.
    - Para cada dispositivo de hardware que quiera agregar a la implementación de SD-WAN, debe realizar las siguientes tareas:
        - Configure el hardware del dispositivo.
        - Establezca la dirección IP de administración para el dispositivo y verifique la conexión.
        - Establezca la fecha y la hora del dispositivo.
        - (Opcional) Establezca el intervalo de **tiempo de espera** de la sesión de consola en un valor alto o máximo.
3. Cargue e instale el archivo de licencia de software en el dispositivo.

Lista de verificación de la Instalación y la configuración

Recopile la siguiente información para cada sitio de SD-WAN que quiera implementar:

- La información de licencia de su producto

- Direcciones IP de red necesarias para cada dispositivo que se va a implementar:
  - Dirección IP de administración
  - Direcciones IP virtuales
  - Nombre del sitio
  - Nombre del dispositivo (uno por sitio)
  - Modelo de dispositivo SD-WAN (para cada dispositivo que se va a implementar)
  - Modo de implementación (MCN o cliente)
  - Topología
  - MPLS de puerta de enlace
  - Información sobre el túnel GRE
  - Rutas
  - VLAN
  - Ancho de banda en cada sitio para cada circuito

Prácticas recomendadas

August 26, 2022

En este artículo se describen las prácticas recomendadas de implementación para la solución Citrix SD-WAN. Proporciona orientación general, ventajas y casos de uso para el siguiente modo de implementación de Citrix SD-WAN.

Modo de borde/puerta de enlace

Recomendaciones

Las siguientes son las recomendaciones para la implementación del modo de **puerta** de enlace:

1. El modo de puerta de enlace se utiliza mejor para sucursales SD-WAN donde se realiza la consolidación de enrutadores y los clientes están listos para permitir que SD-WAN sea el dispositivo perimetral que termina las conexiones.
2. Una gran arquitectura de red se puede renderizar con un diseño escrupuloso cuando un proyecto se construye desde cero.

> **Nota**
>
> El modo Gateway se puede utilizar en el lado del centro de datos para los proyectos existentes con alguna interrupción de la infraestructura.

Ventajas/Casos de uso

Los siguientes son las ventajas/casos de uso para la implementación del modo de puerta de enlace:

1. El mejor caso de uso para la consolidación de elementos de enrutador, firewall y red en la sucursal del cliente.
2. Administración de host LAN sencilla y sencilla a través de DHCP.
    - Permite que SD-WAN se convierta en el salto siguiente y ofrezca direccionamiento IP basado en DHCP a todos los hosts LAN para puertos de datos.
3. Todas las conexiones terminan en el borde o puerta de enlace SD-WAN y la administración se hace fácil.
4. SD-WAN es el punto focal de la redirección perimetral y se dirige a todo el tráfico. Las decisiones se toman en el perímetro de ruptura, backhaul o superposición, incluida la contabilidad de ancho de banda y capacidad.
5. Todos los hosts de subredes LAN como hosts LAN pueden tener SD-WAN LAN VIP como salto siguiente. Si la LAN SD-WAN se conecta a un conmutador central, puede ejecutar la redirección dinámica para obtener visibilidad de todas las subredes LAN.
6. Gran flexibilidad para alta disponibilidad (HA): recomendación estricta para el modo de Gateway para que el sitio funcione con un modo activo/en espera. Además, ayuda a prevenir el agujero negro del tráfico si el dispositivo SD-WAN se apaga.
    - Conmutadores disponibles en la sucursal: la alta disponibilidad paralela puede funcionar en modo de Gateway.
    - Conmutadores no disponibles en la sucursal: SD-WAN también puede operar en el modo de alta disponibilidad de borde SD-WAN (modo de alta disponibilidad de error a cable) donde las dos cajas SD-WAN están conectadas en cadena para hacer uso de puertos de error a cable para actuar como un par convergente de alta disponibilidad.
7. Permita que Internet se defina como interfaces **NO CONFIABLES** que crean automáticamente un NAT dinámico para la ruptura y origen de NAT la conexión para que la respuesta vuelva a SD-WAN.
8. Las consideraciones de seguridad para las interfaces **NO CONFIABLES** están implícitas de forma natural, ya que solo se permiten los paquetes de control ICMP/ARP/UDP en 4980.

Precauciones

La siguiente es la información que debe tener cuidado en el modo de puerta de enlace:

- **Diseño cuidadoso y arquitectura de red**: El modo de puerta de enlace puede necesitar consideraciones de diseño y redes cuidadosas, ya que toda la red de rama o perímetro está en SD-WAN. Qué bloquear, qué redirigir, cómo red LAN, cómo terminar WAN, etc.
- **Fallo del dispositivo: el** modo Edge no puede tener la capacidad de error a cable. Toda la rama se desactiva cuando el dispositivo está apagado.
- **Postura de seguridad**: A medida que la redirección se gestiona en el perímetro, las posturas de seguridad como el firewall, las consideraciones de ruptura/backhaul son cruciales y deben ser concebidas con el cliente.
- **Alta disponibilidad**: La alta disponibilidad de fallos a cables debe tener algunas consideraciones sobre la disponibilidad de puertos y, dependiendo de las implementaciones, puede resultar complicado diseñar.
  - SD-WAN 110 NO es una opción, ya que no tiene puertos de error al cable.

Por ejemplo, si necesita 2 enlaces WAN para operar, necesita 5 puertos, incluido un puerto dedicado para la interfaz de alta disponibilidad, incluida la interfaz LAN.

Modo en línea: Fail-to-cable/Fail-to-block

Recomendaciones

Las siguientes son las recomendaciones para la implementación en modo en **línea** :

1. El modo en línea es el mejor para las sucursales donde no se debe cambiar la infraestructura existente y SD-WAN se encuentra de forma transparente en línea con el segmento LAN.
2. Los centros de datos también pueden emplear fallas en línea o alta disponibilidad paralela en línea, ya que es inmensamente importante asegurarse de que las cargas de trabajo del centro de datos no estén encerradas debido a la caída o caída del dispositivo.

Ventajas y casos de uso

Los siguientes son las ventajas/casos de uso para la implementación en modo en línea:

1. Mantener el router MPLS, por lo tanto, fallar al cable es una función encantadora. Los dispositivos con capacidad de error a cable permiten la conmutación por error sin problemas para la infraestructura subyacente si la caja se apagó.

- Si sus dispositivos admiten fallas a través del cable (SD-WAN 210 y superior), esto permite colocar una sola SD-WAN en línea para evitar el tráfico de LAN al enrutador perimetral del cliente cuando el SD-WAN se bloquea o se desactiva.
- Si los vínculos MPLS están presentes que producen una extensión natural a la LAN/Intranet del cliente, el puerto de par de puente de error a cable es la mejor opción (pares con capacidad de error a cable) de tal manera que, cuando el dispositivo se bloquea o baja, el tráfico LAN se omite el hardware al enrutador perimetral del cliente (se mantiene el siguiente salto).

2. La creación de redes es simple.
3. SD-WAN ve todo el tráfico a través del modo en línea, por lo que es el mejor caso para la contabilidad adecuada del ancho de banda y la capacidad.
4. Pocos requisitos de integración ya que solo necesita una IP del segmento L2. Los segmentos de LAN son bien conocidos por tener un brazo a la interfaz LAN. Si se conecta a un conmutador central, también puede ejecutar la redirección dinámica para obtener visibilidad de todas las subredes LAN.
5. Las expectativas del cliente son que SD-WAN debe integrarse en la infraestructura existente como un nuevo nodo de red (nada más cambia).
6. **ARP proxy**: En modo en línea, es una bendición para SD-WAN proxy solicitudes ARP a la LAN siguiente salto si la puerta de enlace se ha caído o la interfaz SD-WAN hacia el salto siguiente se ha caído.
   - Generalmente, en el modo en línea con el par de puente (error a bloqueo o error a cable) con múltiples conexiones WAN (MPLS/Internet), se recomienda habilitar el ARP de proxy para la interfaz de par de puente que conecta los hosts LAN a su Gateway de salto siguiente.
   - Por cualquier motivo, cuando el salto siguiente está inactivo o la interfaz SD-WAN al salto siguiente está inactiva haciendo que la Gateway sea inaccesible, SD-WAN actúa como un proxy para las solicitudes ARP permitiendo a los hosts LAN enviar paquetes sin problemas y utilizar las conexiones WAN restantes que mantienen el path virtual activo.
7. **Alta disponibilidad**: Si no es una opción, los dispositivos se pueden colocar en dispositivos paralelos de alta disponibilidad (interfaces LAN y WAN comunes para los activos/en espera) para lograr redundancia.
   - Si sus dispositivos no son compatibles con fallas al cable, como el SD-WAN 110, debe utilizar una alta disponibilidad paralela en línea que permita que un dispositivo de espera se conecte si el primario se apagó.

Precauciones

La siguiente es la información que debe tener cuidado en el modo **Inline** :

- La red de fontanería con dos brazos a la SD-WAN (LAN y WAN lado), necesita algo de tiempo de inactividad ya que la red debe ser plomada en dos brazos.
- Debe asegurarse de que si se utiliza un error a cable, está detrás de un enrutador/firewall perimetral del cliente en una zona de **CONFIANZA** para que la seguridad no se vea comprometida.
- MPLS QoS cambia un poco en esto ya que las directivas de QoS anteriores podrían haber dependido de las direcciones IP de origen o basadas en DSCP que ahora se enmascararán debido a una superposición.
- Se debe tener cuidado de reutilizar el enrutador MPLS con un ancho de banda reservado específico SD-WAN bien diseñado con una etiqueta DSCP específica, de modo que la QoS de SD-WAN se encargue de priorizar el tráfico y envíe aplicaciones de alta prioridad inmediatamente seguidas de otras clases (pero puede tener en cuenta el ancho de banda reservado para SD-WAN en el router MPLS). Las colas MPLS son una alternativa o MPLS con un único DSCP establecido en el grupo de rutas automáticas que puede encargarse de esto.
- Si las interfaces de Internet son de **CONFIANZA** ya que los vínculos terminan en el enrutador perimetral del cliente, para utilizar el servicio Internet, debe escribir una regla NAT dinámica exclusiva para habilitar la interrupción de Internet desde el dispositivo.
- Si los vínculos de Internet son las únicas conexiones WAN y aún terminan en el enrutador perimetral del cliente, sigue siendo correcto omitir las conexiones si el enrutador perimetral del cliente toma precauciones para dirigir los paquetes a través de su infraestructura de calco subyacente existente.
  - Se debe tener cuidado para tener en cuenta el flujo de omitir el tráfico LAN a través del par de puentes con una conexión a Internet y cuando el dispositivo está inactivo. Dado que se trata de un tráfico de Intranet empresarial sensible, en vísperas de un fallo, el cliente debe saber cómo manejarlo.

Modo en línea/un brazo virtual

Recomendaciones

Las siguientes son las recomendaciones para la implementación del modo **virtual en línea** :

1. El modo virtual en línea es mejor para redes de centros de datos, ya que la plomería de red SD-WAN se puede trabajar en paralelo mientras el centro de datos atiende a sus cargas de trabajo existentes con la infraestructura existente.

2. SD-WAN se encuentra en una interfaz de un solo brazo que se administra con un seguimiento de SLA en VIP. Si el seguimiento se desactiva, el tráfico reanuda la redirección a través de la infraestructura de calco subyacente existente.
3. Las sucursales también se pueden implementar en modo virtual en línea, sin embargo, son más predominantes con las implementaciones en línea/puerta de enlace.

Ventajas y casos de uso

Las siguientes son las ventajas/casos de uso para la implementación del modo **virtual en línea** :

1. La forma más sencilla y recomendada de conectar SD-WAN en el centro de datos.
    - El modo virtual en línea permite la fontanería de red paralela de SD-WAN con el enrutador de núcleo de cabecera.
    - El modo virtual en línea nos permite definir fácilmente los PBRs para desviar el tráfico LAN debe pasar por SD-WAN y obtener beneficios de superposición.
2. Failover sin problemas a la infraestructura subyacente para que SD-WAN falle y reenvío sin problemas a SD-WAN para obtener beneficios de superposición en condiciones normales.
3. Requisitos sencillos de **redes** e **integración**. La interfaz de un solo brazo desde el enrutador de cabecera a SD-WAN en línea virtual.
4. Redirección dinámica fácil de implementar en el **modo Solo importación** (no exporte nada) para obtener visibilidad de las subredes LAN para que puedan enviarse a dispositivos remotos de pares SD-WAN.
5. Fácil de definir PBR en los routers (1 por WAN VIP) para indicar cómo elegir el físico.

Precauciones

La siguiente es la información sobre la que debe tener cuidado en el modo **Virtual Inline** :

- Se debe tener el cuidado adecuado para asignar claramente el VIP lógico SD-WAN de un enlace WAN definido a la interfaz física correcta (de lo contrario, esto podría causar problemas indeseables en la evaluación de la métrica WAN y en la elección de rutas de WAN).
- Se deben hacer consideraciones de diseño adecuadas para saber si todo el tráfico se desvía a través de SD-WAN o solo tráfico específico.
- Esto significa que SD-WAN debe dedicarse una parte de ancho de banda exclusivamente para sí mismo que debe establecerse en las interfaces de tal manera que la capacidad de SD-WAN no sea utilizada por otro tráfico que no sea SD-WAN, causando resultados indeseables.

  - Pueden producirse problemas de contabilidad de ancho de banda y problemas de congestión si la capacidad de los enlaces WAN de SD-WAN se define incorrectamente.

- La redirección dinámica puede causar algunos problemas si se diseña incorrectamente, donde si los VIPs de centro de datos y sucursales de SD-WAN se exportan a la cabecera y si la redirección se ve influenciada hacia SD-WAN, los paquetes de superposición comienzan a bucle y provocan resultados no deseados.
- La redirección dinámica debe administrarse adecuadamente teniendo en cuenta todos los factores potenciales de qué aprender/qué anunciar.
- La interfaz física de un solo brazo puede convertirse en un cuello de botella a veces. Necesita algunas consideraciones de diseño en esas líneas, ya que atiende tanto a la carga como a la descarga y también actúa como tráfico de LAN a LAN y LAN a WAN/WAN a LAN desde SD-WAN.
- El tráfico excesivo de LAN a LAN puede ser un punto a tener en cuenta durante el diseño.
- Si no se utiliza la redirección dinámica, debe haber cuidado adecuadamente al administrar todas las subredes LAN, lo que de no ser así, podría causar problemas de redirección no deseados.
- Existen posibles problemas de bucle de redirección si define alguna ruta predeterminada (0.0.0.0/0) en el SD-WAN en la línea virtual para volver al enrutador de cabecera. En tales situaciones, si la ruta virtual se apagó, cualquier tráfico procedente de la LAN del centro de datos (como el tráfico de supervisión) se vuelve a la cabecera y de vuelta a SD-WAN causando problemas de redirección no deseados (Si la ruta virtual está inactiva, las subredes de sucursales remotas se vuelven accesibles **NO** causando el ruta predeterminada para ser HIT, que causa problemas de bucle).

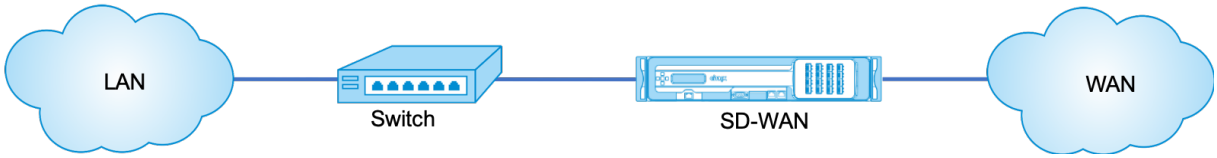
Modo de puerta de enlace

August 26, 2022

El modo de Gateway coloca físicamente el dispositivo SD-WAN en la ruta (implementación de dos brazos) y requiere cambios en la infraestructura de red existente para que el dispositivo SD-WAN sea la puerta de enlace predeterminada para toda la red LAN de ese sitio. Modo de puerta de enlace utilizado para nuevas redes y reemplazo de enrutadores. El modo de puerta de enlace permite dispositivos SD-WAN:

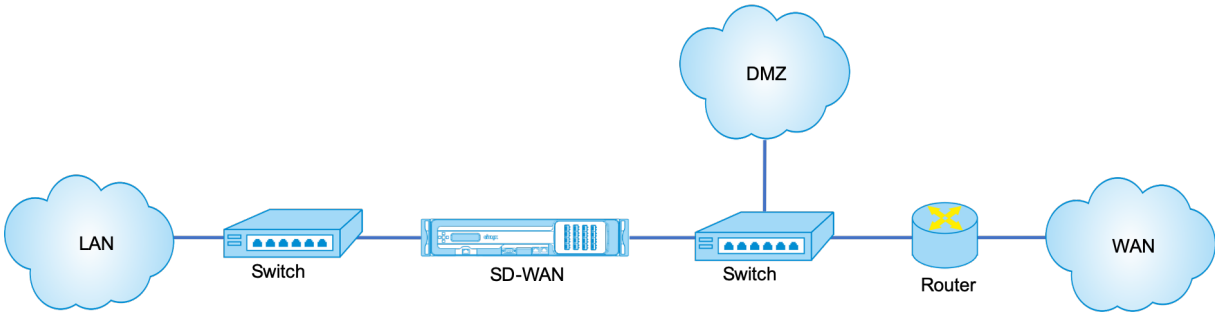
- Para ver todo el tráfico hacia y desde la WAN
- Para realizar la redirección local

El modo de implementación de puerta de enlace se admite en Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Interfaces.



> **Nota**
>
> Una SD-WAN implementada en modo de puerta de enlace actúa como un dispositivo de capa 3 y no puede realizar fallas en cables. Todas las interfaces involucradas se configurarán para **Fail-to-Block**.En caso de fallo del dispositivo, también se producirá un error en la puerta de enlace predeterminada del sitio, lo que provocará una interrupción hasta que se restaure el dispositivo y la puerta de enlace predeterminada.

En el modo **Inline**, el dispositivo SD-WAN parece ser un puente Ethernet. La mayoría de los modelos de dispositivos SD-WAN incluyen una función de error a cable (derivación Ethernet) para el modo en línea. Si falla la alimentación, un relé se cierra y los puertos de entrada y salida se conectan eléctricamente, lo que permite que la señal Ethernet pase de un puerto a otro. En el modo de error al cable, el dispositivo SD-WAN parece un cable cruzado que conecta los dos puertos. Modo en línea utilizado para integrarse en redes ya bien definidas.

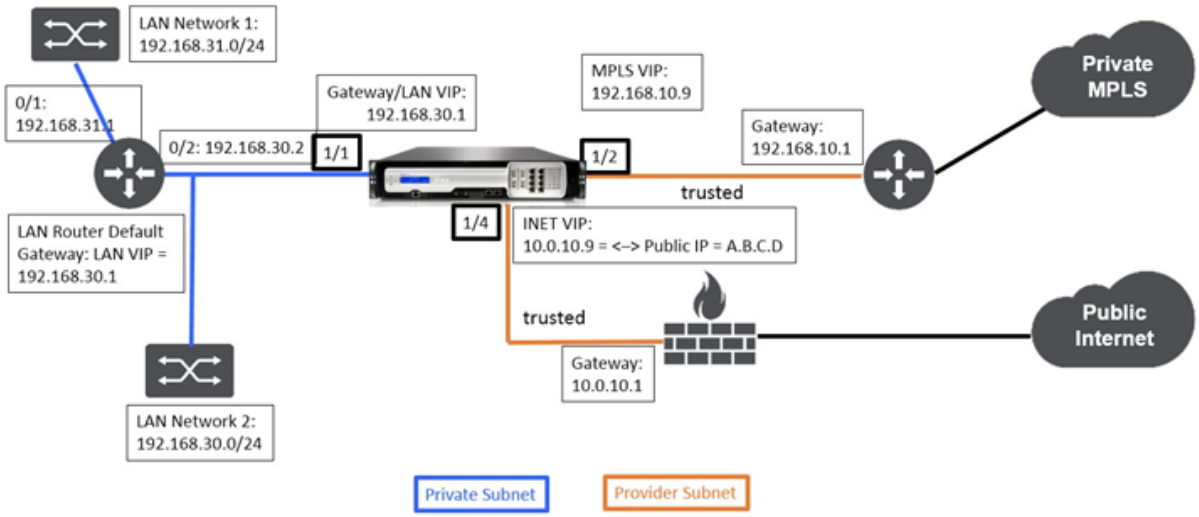


En este artículo se proporciona un procedimiento paso a paso para configurar un dispositivo SD-WAN en modo de puerta de enlace en una configuración de red de ejemplo. La implementación en línea también se describe para que el lado de la sucursal complete la configuración. Una red puede seguir funcionando si se quita un dispositivo en línea, pero pierde todo el acceso si se quita el dispositivo de puerta de enlace.

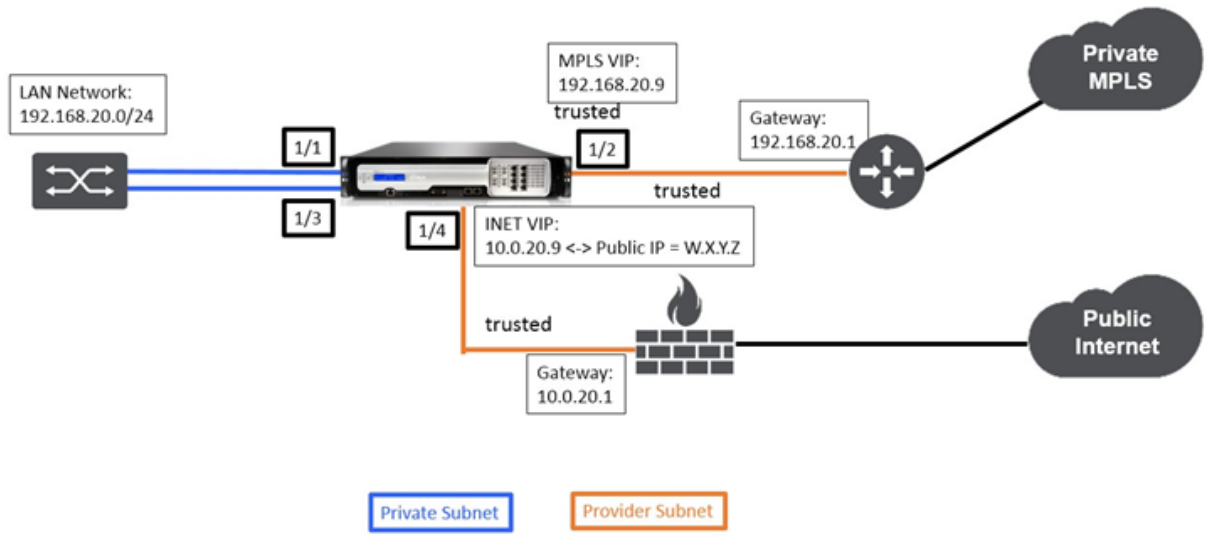
Topología

En las siguientes ilustraciones se describen las topologías admitidas en una red SD-WAN.

Centro de datos en implementación de Gateway



Sucursal en implementación en línea



Configuración del modo de Gateway del sitio de

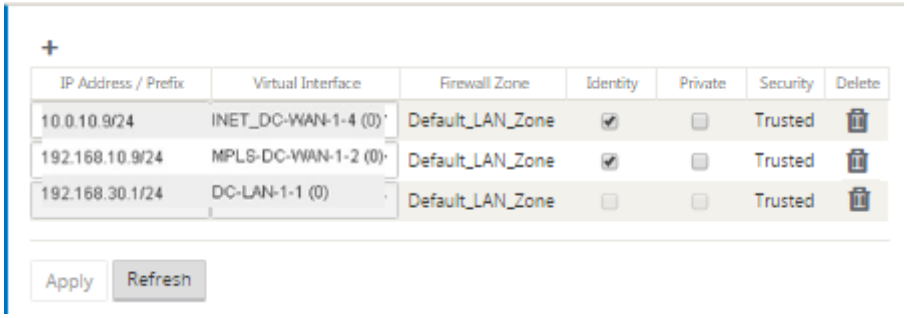
Los siguientes son los pasos de configuración de alto nivel para configurar la implementación de la puerta de enlace del sitio del centro

1. Cree un sitio de DC.
2. Rellene grupos de interfaces basados en interfaces Ethernet conectadas.
3. Cree una dirección IP virtual para cada interfaz virtual.

4. Rellene los enlaces WAN en función de la velocidad física y no de las velocidades de ráfaga mediante Internet y MPLS Links.
5. Rellene rutas si hay más subredes en la infraestructura LAN.

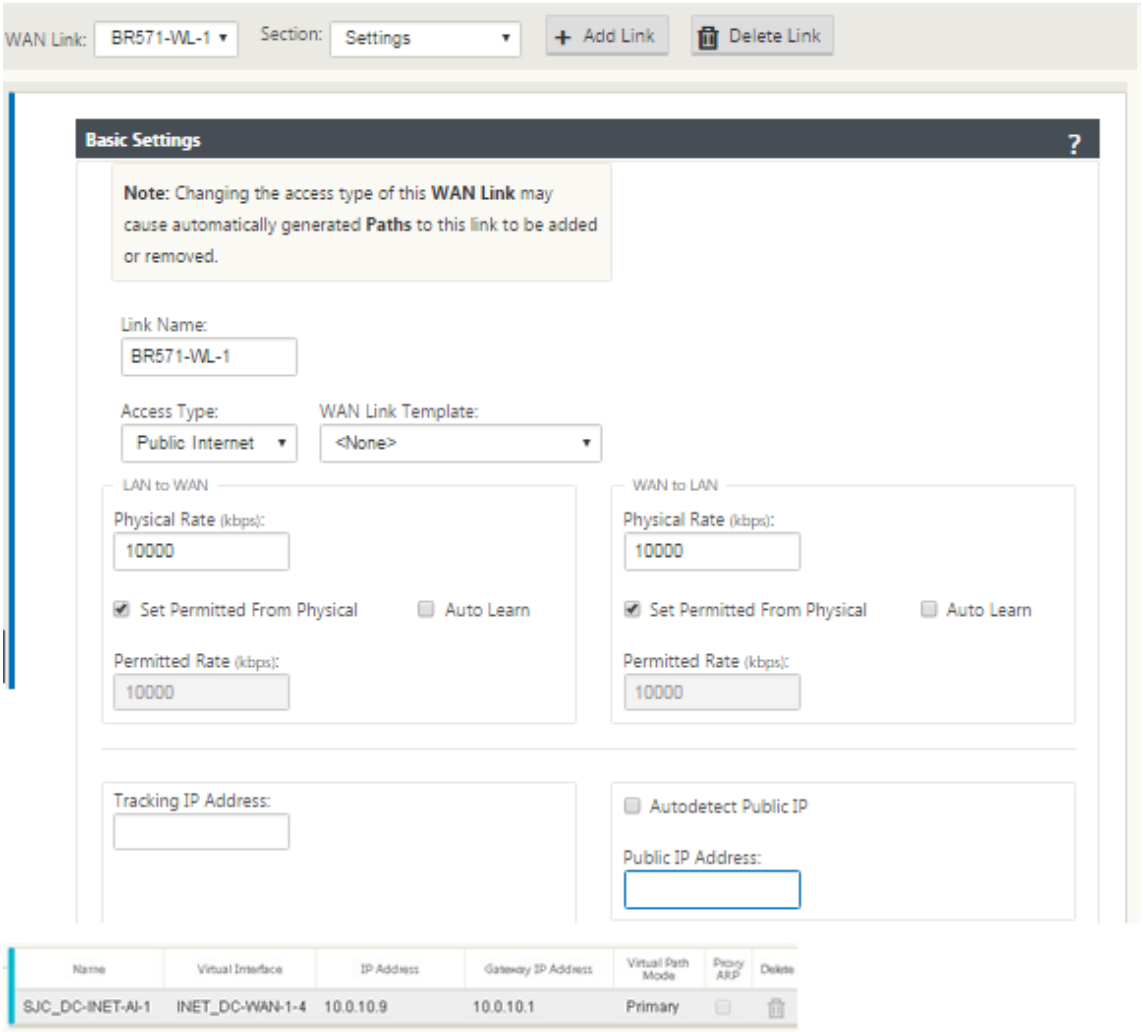
Para crear una dirección IP virtual (VIP) para cada interfaz virtual

1. Cree un VIP en la subred adecuada para cada enlace WAN. Los VIP se utilizan para la comunicación entre dos dispositivos SD-WAN en el entorno WAN virtual.
2. Cree una dirección IP virtual que se utilizará como dirección de puerta de enlace para la red LAN.



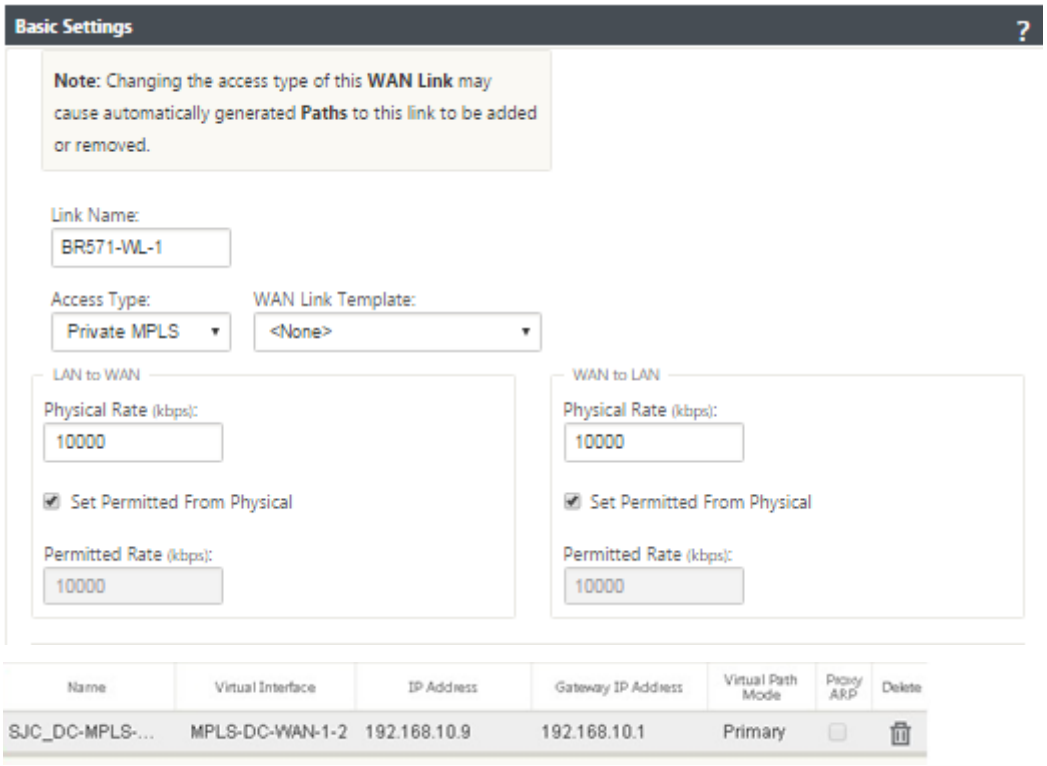
Para rellenar los vínculos WAN en función de la velocidad física y no de las velocidades de ráfaga mediante el enlace de Internet:

1. Vaya a **Vínculos WAN**, haga clic en el botón **+ Agregar vínculo** para agregar un vínculo WAN para el vínculo de Internet.
2. Rellene los detalles del enlace a Internet, incluida la dirección IP pública suministrada como se muestra a continuación. No se puede seleccionar AutoDetect **Public IP** para el dispositivo SD-WAN configurado como MCN.
3. Desplácese hasta **Interfaces de acceso**, en el menú desplegable de la sección, y haga clic en el botón **+ Agregar** para agregar detalles de interfaz específicos para el vínculo de Internet.
4. Rellene la interfaz de acceso para direcciones IP y Gateway como se muestra a continuación.



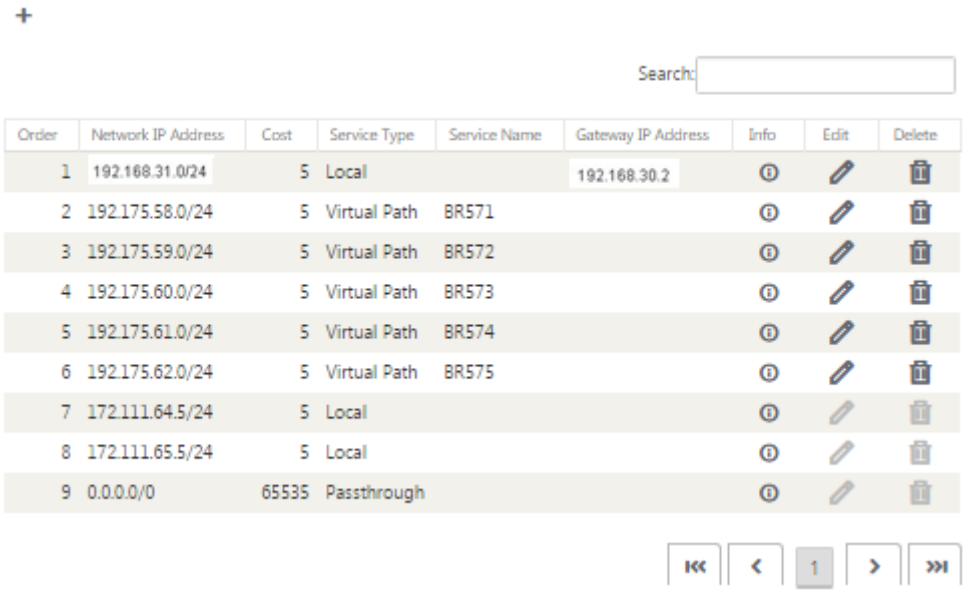
Para crear un vínculo MPLS

1. Vaya a **Enlaces WAN**, haga clic en el botón **+** para agregar un enlace WAN para el enlace MPLS.
2. Rellene los detalles del enlace MPLS como se muestra a continuación.
3. Vaya a **Interfaces de acceso**, haga clic en el botón **+** para agregar detalles de interfaz específicos para el enlace MPLS.
4. Rellene la interfaz de acceso para direcciones IP y Gateway como se muestra a continuación.



Para rellenar rutas

Las rutas se crean automáticamente según la configuración anterior. La topología de ejemplo de DC LAN mostrada anteriormente tiene una subred LAN adicional que es **192.168.31.0/24**. Es necesario crear una ruta para esta subred. La dirección IP de la puerta de enlace debe estar en la misma subred que el VIP de la LAN de CC como se muestra a continuación.



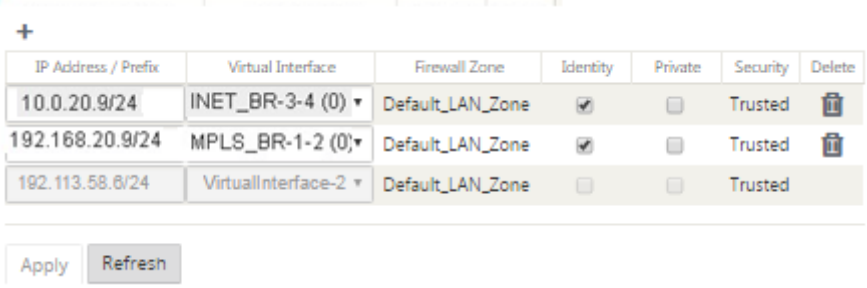
Configuración de implementación en línea del sitio de sucursal

A continuación se indican los pasos de configuración de alto nivel para configurar el sitio de sucursal para la implementación en línea:

1. Cree un sitio de sucursal.
2. Rellene grupos de interfaces basados en interfaces Ethernet conectadas.
3. Cree una dirección IP virtual para cada interfaz virtual.
4. Rellene los enlaces WAN en función de la velocidad física y no de las velocidades de ráfaga mediante Internet y MPLS Links.
5. Rellene rutas si hay más subredes en la infraestructura LAN.

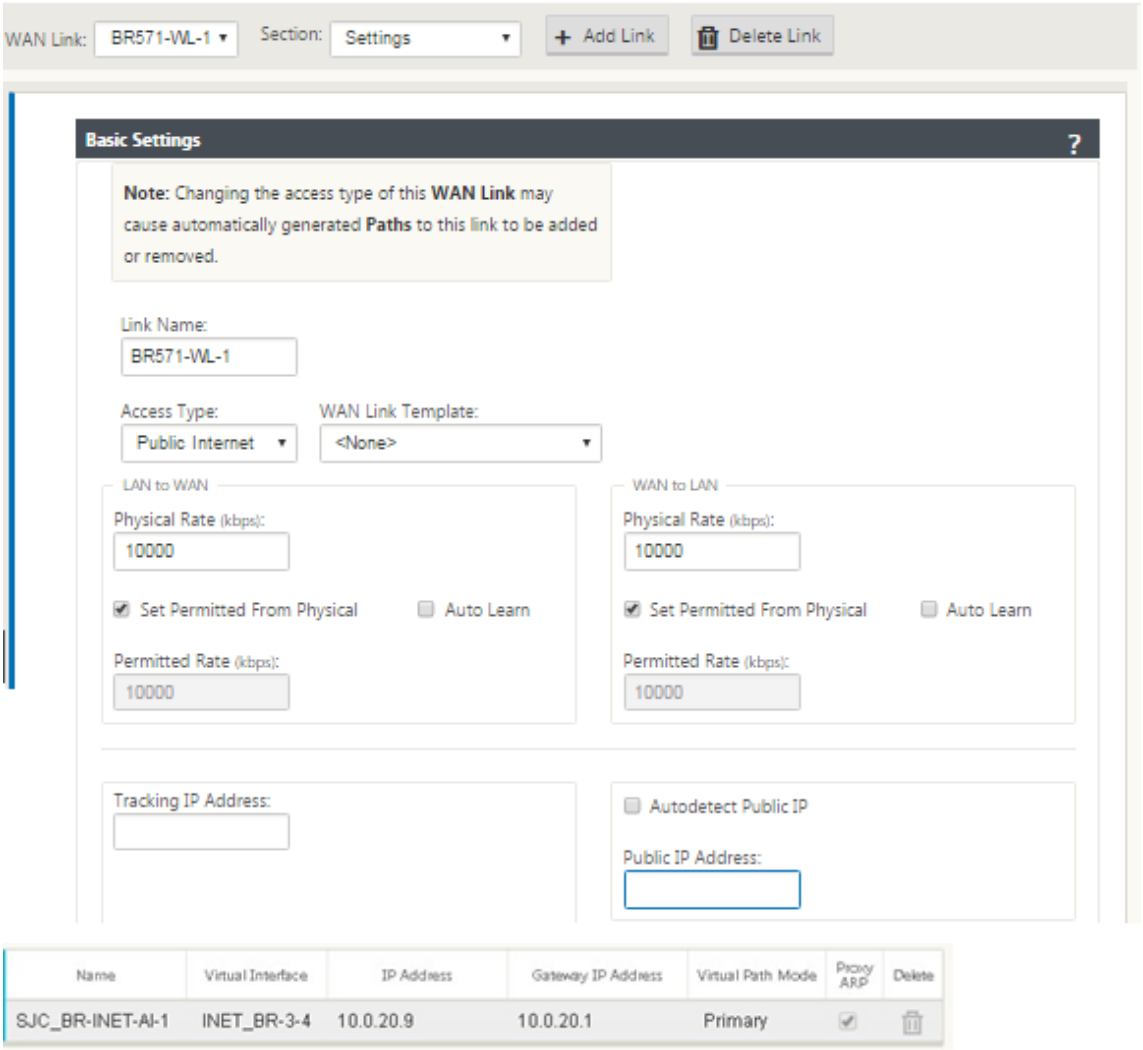
Para crear una dirección IP virtual (VIP) para cada interfaz virtual

1. Cree una dirección IP virtual en la subred adecuada para cada enlace WAN. Los VIP se utilizan para la comunicación entre dos dispositivos SD-WAN en el entorno WAN virtual.



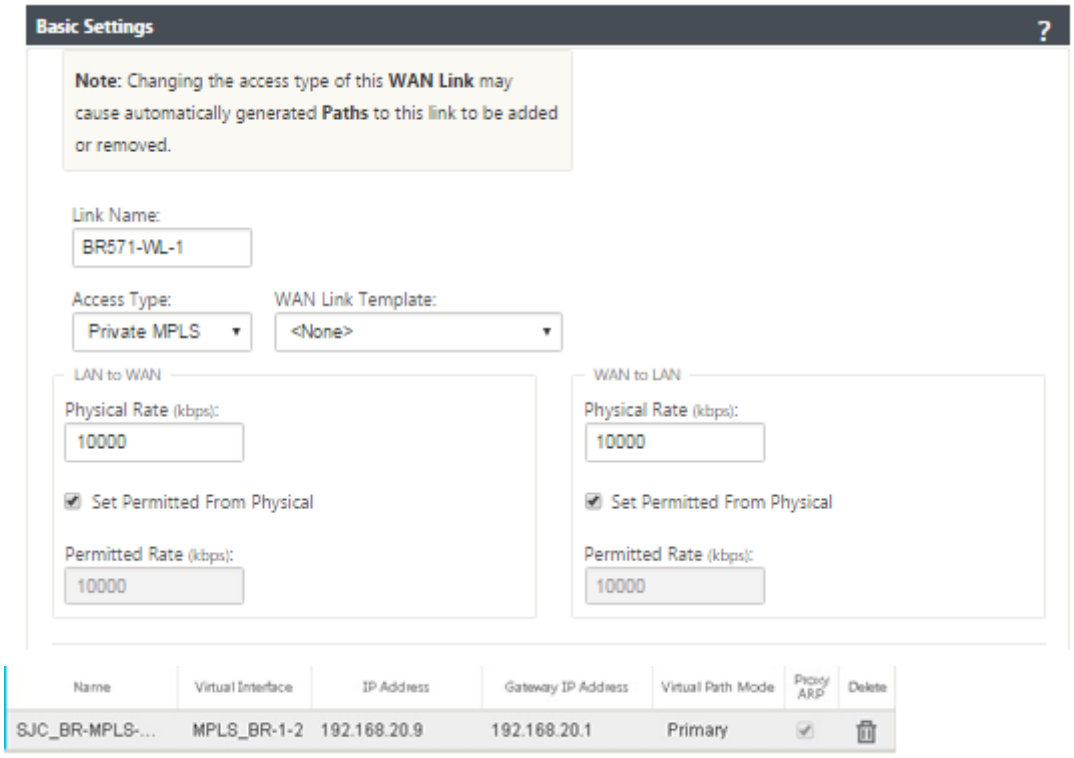
Para rellenar los vínculos WAN en función de la velocidad física y no de las velocidades de ráfaga mediante el enlace de Internet:

1. Vaya a **Enlaces WAN**, haga clic en el botón **+**para agregar un Enlace WAN para el vínculo de Internet.
2. Rellene los detalles del vínculo de Internet, incluida la dirección IP pública de detección automática como se muestra a continuación.
3. Vaya a **Interfaces de acceso**, haga clic en el botón **+**para agregar detalles de interfaz específicos para el vínculo de Internet.
4. Rellene la interfaz de acceso para la dirección IP y la Gateway como se muestra a continuación.



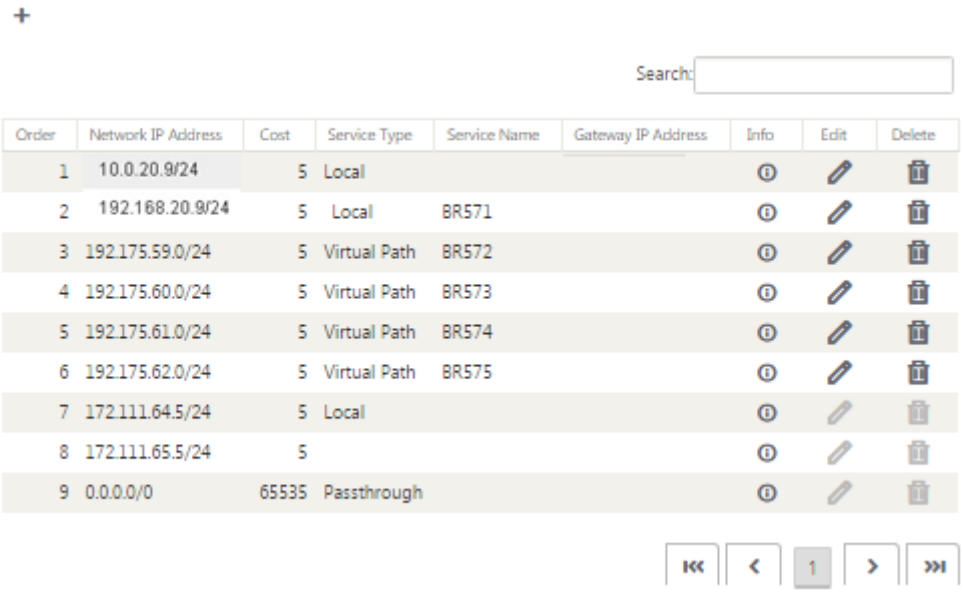
Para crear un vínculo MPLS

1. Vaya a Enlaces WAN, haga clic en el botón **+** para agregar un enlace WAN para el enlace MPLS.
2. Rellene los detalles del enlace MPLS como se muestra a continuación.
3. Vaya a Interfaces de acceso, haga clic en el botón **+** para agregar detalles de interfaz específicos para el enlace MPLS.
4. Rellene la interfaz de acceso para la dirección IP y la Gateway como se muestra a continuación.



Para rellenar rutas

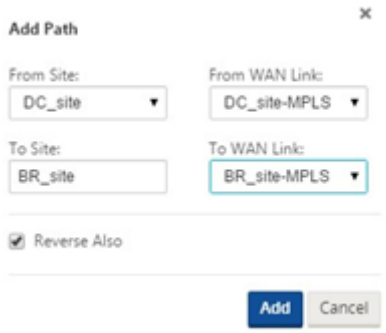
Las rutas se crean automáticamente en función de la configuración anterior. En caso de que haya más subredes específicas para esta sucursal remota, se deben agregar rutas específicas que identifiquen qué Gateway dirigir el tráfico para llegar a esas subredes back-end.



Resolver errores de auditoría

Después de completar la configuración para los sitios de DC y Branch, se le avisará de que resuelva el error de auditoría en los sitios de DC y BR.

De forma predeterminada, el sistema genera rutas de acceso para los vínculos WAN definidos como tipo de acceso Internet público. Deberá utilizar la función de grupo de ruta automática o habilitar rutas de acceso manualmente para Enlaces WAN con un tipo de acceso de Internet privado. Las rutas de los vínculos MPLS se pueden habilitar haciendo clic en Agregar operador (en el rectángulo verde).



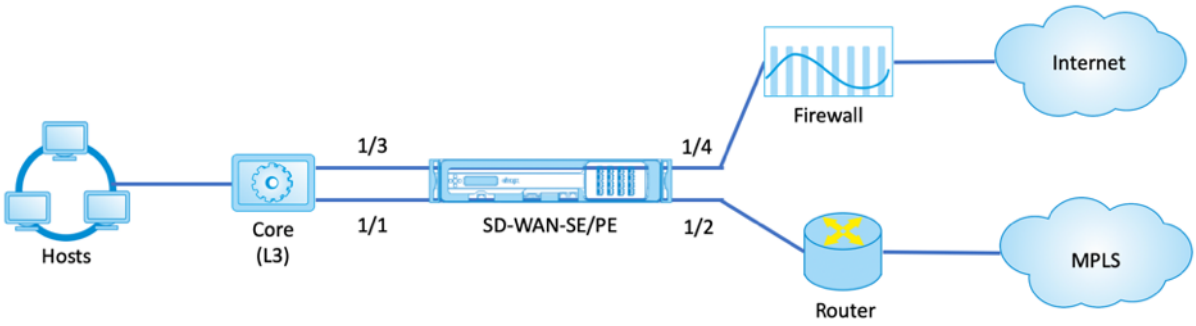
Después de completar todos los pasos anteriores, continúe con Preparación de los paquetes de dispositivos SD-WAN. —>

Modo en línea

August 26, 2022

En este artículo se proporciona información detallada sobre la configuración de una rama con el modo **de implementación en línea**. En este modo, el dispositivo SD-WAN parece ser un puente Ethernet. La mayoría de los modelos de dispositivos SD-WAN incluyen una función **de error a cable** (derivación Ethernet) para el modo en línea. Si falla la alimentación, un relé se cierra y los puertos de entrada y salida se conectan eléctricamente, lo que permite que la señal Ethernet pase de un puerto a otro. En el modo de error al cable, el dispositivo SD-WAN parece un cable cruzado que conecta los dos puertos.

En el siguiente diagrama, las interfaces 1/1 y 1/2 son pares de derivación de hardware y fallarán al conectar el núcleo al enrutador MPLS de borde. Las interfaces 1/3 y 1/4 también son pares de omisión de hardware y fallarán al conectar el Core al firewall perimetral. Para obtener más información sobre la implementación en modo en línea basada en SD-WAN Orchestrator Service, consulte Interfaces.



Modo virtual en línea

August 26, 2022

En el modo virtual en línea, el enrutador utiliza el protocolo de redirección como PBR, OSPF o BGP para redirigir el tráfico WAN entrante y saliente al dispositivo, y el dispositivo reenvía los paquetes procesados al enrutador.

El siguiente artículo describe el procedimiento paso a paso para configurar dos dispositivos SD-WAN (SD-WAN SE):

- Dispositivo del centro de datos en modo virtual en línea
- Dispositivo de sucursal en modo Inline
- El protocolo de redirección debe configurarse ya sea en el conmutador principal o más arriba en el enrutador. El enrutador debe supervisar el estado del dispositivo SD-WAN para que se pueda omitir el dispositivo si falla.
- El modo virtual en línea coloca el dispositivo SD-WAN físicamente fuera de ruta (implementación de un brazo), es decir, solo se utilizará una única interfaz Ethernet (Ejemplo: Interfaz 1/5) con el modo de derivación configurado en error de bloqueo (FTB).
  El dispositivo Citrix SD-WAN debe configurarse para pasar el tráfico a la Gateway adecuada. El tráfico destinado a la ruta virtual se dirige hacia el dispositivo SD-WAN y, a continuación, se encapsula y se dirige al enlace WAN apropiado.

Recopilar información

Recopile la siguiente información necesaria para configurar el modo virtual en línea:

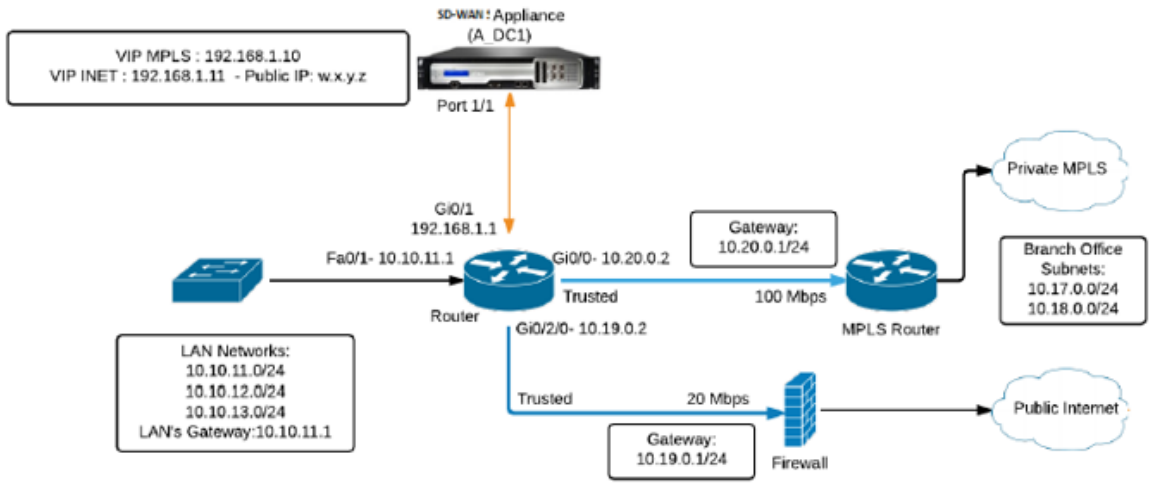
- Diagrama de red preciso de sus sitios locales y remotos, que incluye:
  - Enlaces WAN locales y remotos y sus anchos de banda en ambas direcciones, sus subredes, direcciones IP virtuales y puertas de enlace desde cada enlace, rutas y VLAN.

- Tabla de implementación

Para obtener información sobre la implementación del modo Virtual Inline basada en el servicio de SD-WAN Orchestrator, consulte Interfaces.

A continuación se muestra un diagrama de red y una tabla de implementación de ejemplo:

Topología del centro de datos: Modo en línea virtual



Resolución de errores de auditoría

Después de completar la configuración de los centros de datos y las sucursales, se le avisará para que resuelva los errores de auditoría en los sitios DC y BR. Resuelva los errores de auditoría (si los hubiera).

Crear una red SD-WAN

August 26, 2022

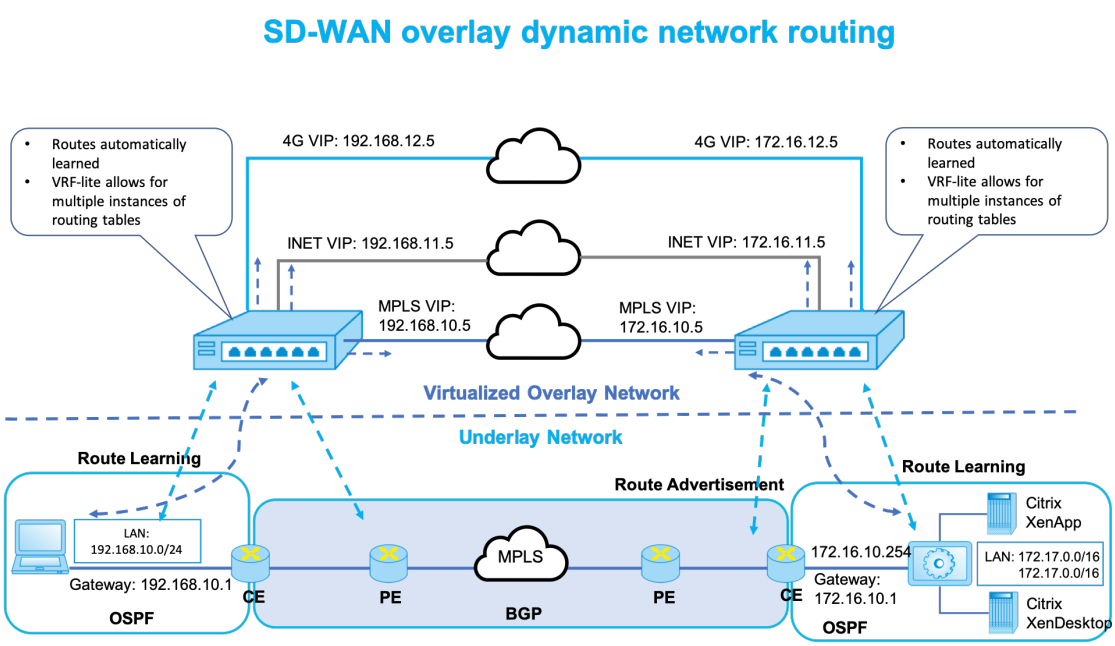
Para crear una red de superposición SD-WAN sin necesidad de crear tablas de rutas de superposición SD-WAN:

1. Cree un túnel de ruta WAN a través de cada enlace WAN entre dos dispositivos SD-WAN.

2. Configure la IP virtual para que represente el punto final de cada enlace WAN. Puede establecer rutas WAN cifradas a través de la red L3 actual.
3. Agregue 2, 3 y 4 rutas WAN (enlaces físicos) en una única ruta virtual que permita que los paquetes atraviesen la WAN utilizando la red superpuesta SD-WAN en lugar de la capa subyacente existente, que es menos inteligente e ineficiente en términos de costes.

Componentes de redirección SD-WAN y topología de red

- Local: la subred reside en este sitio (anunciada en el entorno SD-WAN)
- Ruta virtual: se envía a través de la ruta virtualizada al dispositivo de sitio seleccionado
- Intranet: sitios sin dispositivo SD-WAN
- Internet: tráfico vinculado a internet
- Paso a través: tráfico intacto, en una interfaz de puente hacia la otra
- Ruta predeterminada (0.0.0.0/0) definida: Se utiliza para el tráfico de paso a través no capturado por la tabla de rutas de superposición SD-WAN o utilizado en el MCN para indicar a los sitios de los clientes que reenvíen todo el tráfico al nodo MCN para el backhaul del tráfico de Internet.



Alta disponibilidad

August 26, 2022

Este tema cubre las implementaciones y configuraciones de alta disponibilidad (alta disponibilidad) compatibles con los dispositivos SD-WAN (Standard Edition).

Los dispositivos Citrix SD-WAN se pueden implementar en configuración de alta disponibilidad como un par de dispositivos en roles Activo/En espera. Existen tres modos de implementación de alta disponibilidad:

- Alta disponibilidad en línea paralela
- Alta disponibilidad por error de cableado
- Alta disponibilidad con un brazo

Estos modos de implementación de alta disponibilidad son similares al Protocolo de redundancia de enrutador virtual (VRRP) y utilizan un protocolo SD-WAN propietario. Tanto los nodos de cliente (clientes) como los nodos de control maestro (MCNs) dentro de una red SD-WAN se pueden implementar en una configuración de alta disponibilidad. El dispositivo primario y secundario deben ser los mismos modelos de plataforma.

En la configuración de alta disponibilidad, un dispositivo SD-WAN en el sitio se designa como dispositivo activo. El dispositivo en espera supervisa el dispositivo activo. La configuración se refleja en ambos dispositivos. Si el dispositivo en espera pierde la conectividad con el dispositivo activo durante un período definido, el dispositivo en espera asume la identidad del dispositivo activo y se hace cargo de la carga de tráfico. Según el modo de implementación, este failover rápido tiene un impacto mínimo en el tráfico de aplicaciones que pasa por la red.

Modos de implementación de alta disponibilidad

Modo de un brazo:

En el modo de un brazo, el par de dispositivos de alta disponibilidad está fuera de la ruta de datos. El tráfico de aplicaciones se redirige al par del dispositivo con la redirección basada en directivas (PBR). El modo de un brazo se implementa cuando un único punto de inserción en la red no es factible o para contrarrestar los desafíos de la falla al cable. El dispositivo en espera se puede agregar a la misma VLAN o subred que el dispositivo activo y el enrutador.

En el modo de brazo único, se recomienda que los dispositivos SD-WAN no residan en las subredes de la red de datos. El tráfico de ruta virtual no tiene que atravesar el PBR y evita los bucles de ruta. El dispositivo SD-WAN y el enrutador deben estar conectados directamente, ya sea a través de un puerto Ethernet o en la misma VLAN.

- **Supervisión de SLA IP para respaldo**:

  El tráfico activo fluye incluso si la ruta virtual está inactiva, siempre y cuando uno de los dispositivos SD-WAN esté activo. El dispositivo SD-WAN redirige el tráfico de vuelta al enrutador

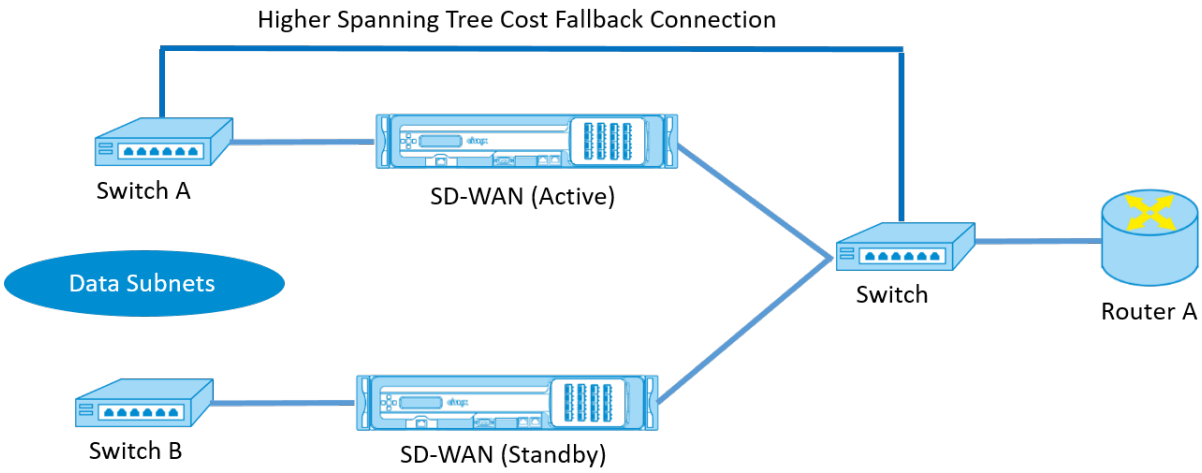
como tráfico de Intranet. Sin embargo, si ambos dispositivos SD-WAN activos/en espera se vuelven inactivos, el router intenta redirigir el tráfico a los dispositivos. La supervisión de SLA de IP se puede configurar en el router para inhabilitar PBR, si no se puede acceder al siguiente dispositivo. Permite al router retroceder para realizar una búsqueda de rutas y reenviar paquetes apropiadamente.

Modo paralelo de alta disponibilidad en línea:

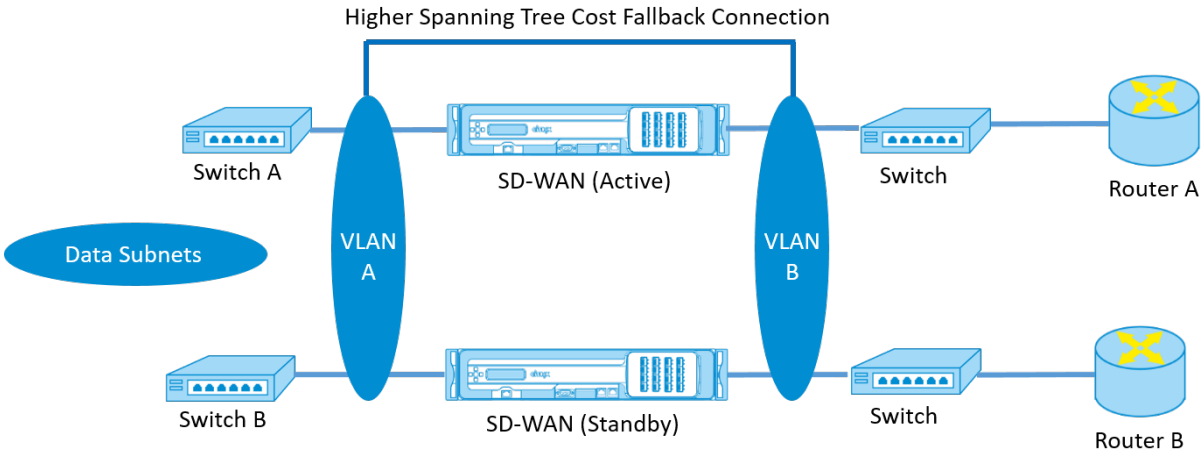
En el modo de alta disponibilidad en línea paralela, los dispositivos SD-WAN se implementan uno junto al otro, en línea con la ruta de datos. Solo se utiliza una ruta a través del dispositivo activo. Es importante tener en cuenta que los grupos de interfaz de omisión están configurados para que no se bloqueen para evitar bucles de puente durante una conmutación por error.

El estado de alta disponibilidad se puede supervisar a través de los grupos de interfaces en línea o a través de una conexión directa entre los dispositivos. El seguimiento externo se puede utilizar para supervisar la accesibilidad de la infraestructura de red ascendente o descendente. Por ejemplo, falla en el puerto del conmutador para dirigir el cambio de estado de alta disponibilidad, si es necesario.

Si los dispositivos SD-WAN activos y en espera están inhabilitados o fallan, se puede utilizar una ruta terciaria directamente entre el switch y el router. Esta ruta debe tener un coste de árbol de expansión mayor que las rutas de SD-WAN para que no se utilice en condiciones normales. La conmutación por error en modo de alta disponibilidad en línea paralela depende del tiempo de conmutación por error configurado; el tiempo de conmutación por error predeterminado es de 1000 ms. Sin embargo, una conmutación por error tiene un impacto en el tráfico de 3 a 5 segundos. El retroceso a la ruta terciaria afecta al tráfico mientras dure la reconvergencia del árbol de expansión. Si hay conexiones fuera de ruta a otros enlaces WAN, ambos dispositivos deben estar conectados a ellos.



En casos más complejos, en los que varios enrutadores podrían estar mediante VRRP, se recomienda VLAN no enrutables para garantizar que el conmutador y los enrutadores del lado LAN sean accesibles en la capa 2.



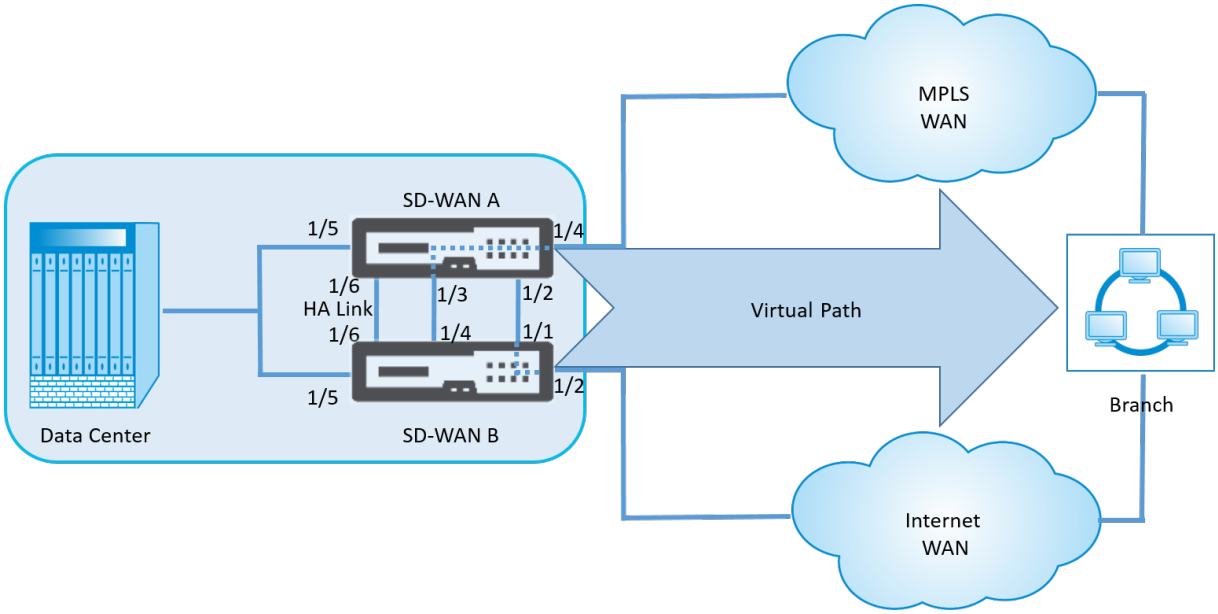
Modo de conmutación por error:

En el modo de conmutación por error, los dispositivos SD-WAN están en línea en la misma ruta de datos. Los grupos de interfaz de omisión deben estar en el modo de error al cable con el dispositivo en espera en un estado de paso o omisión. Se debe configurar y utilizar una conexión directa entre los dos dispositivos en un puerto independiente para el grupo de interfaces de alta disponibilidad.

> **Nota**
>
> - La conmutación de alta disponibilidad en modo de error a cable tarda aproximadamente 10 a 12 segundos debido al retraso en la recuperación de los puertos del modo Fail-to-Wire.
> - Si falla la conexión de alta disponibilidad entre los dispositivos, ambos equipos pasan al estado Activo y provocan una interrupción del servicio. Para mitigar la interrupción del servicio, asigne varias conexiones de alta disponibilidad para que no haya un único punto de falla.
> - Es imperativo que en el modo Fail-to-Wire de alta disponibilidad, se utilice un puerto separado en los pares de dispositivos de hardware para el mecanismo de intercambio de control de alta disponibilidad para ayudar con la convergencia de estado.

Debido a un cambio de estado físico cuando los dispositivos SD-WAN cambian de Activo a En espera, la conmutación por error puede causar una pérdida parcial de conectividad en función del tiempo que tarda la negociación automática en los puertos Ethernet.

En la siguiente ilustración se muestra un ejemplo de la implementación Fail-to-Wire.



La configuración de alta disponibilidad en un brazo o la configuración de alta disponibilidad en línea paralela se recomienda para centros de datos o sitios que reenvíen un gran volumen de tráfico para minimizar la interrupción durante la conmutación por error.

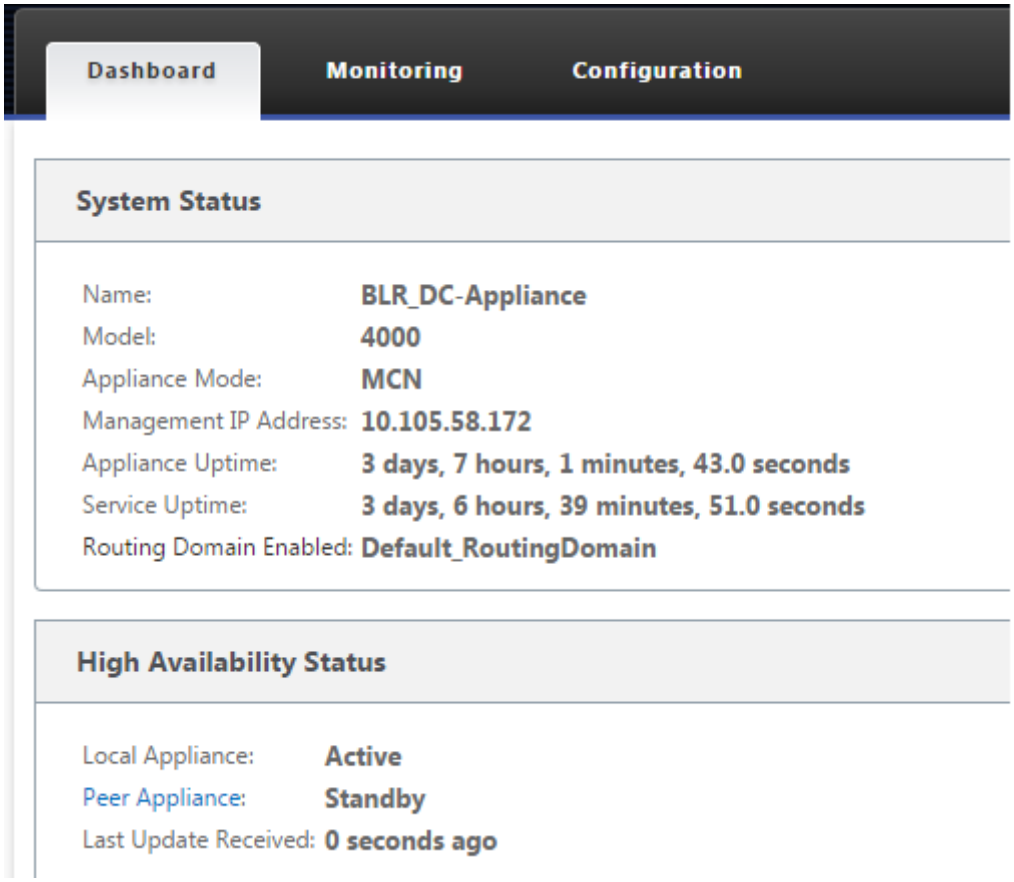
Si se acepta una pérdida mínima de servicio durante una conmutación por error, el modo de alta disponibilidad Fail-to-Wire es una mejor solución. El modo de alta disponibilidad Fail-to-Wire protege contra fallos del dispositivo y la alta disponibilidad en línea paralela protege contra todos los fallos. En todos los casos, la alta disponibilidad es valiosa para preservar la continuidad de la red SD-WAN durante un fallo del sistema.

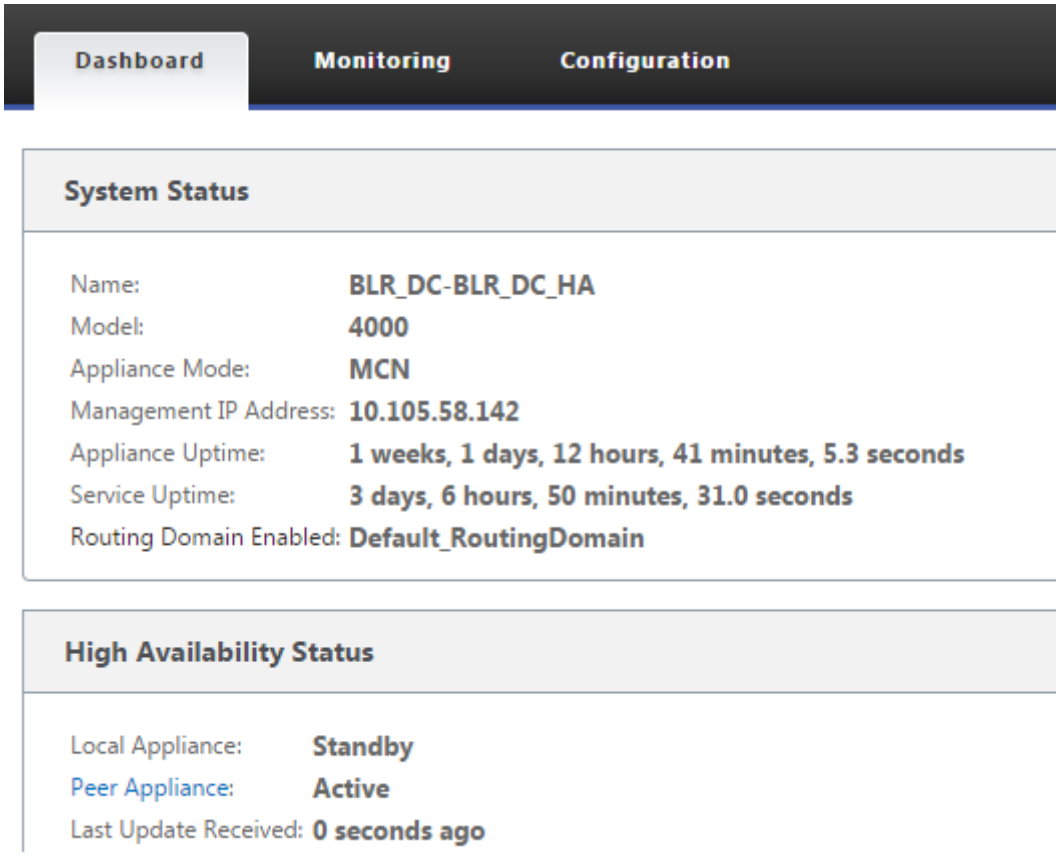
Para obtener más información sobre la implementación de alta disponibilidad basada en SD-WAN Orchestrator Service, consulte Detalles del dispositivo.

Supervisión

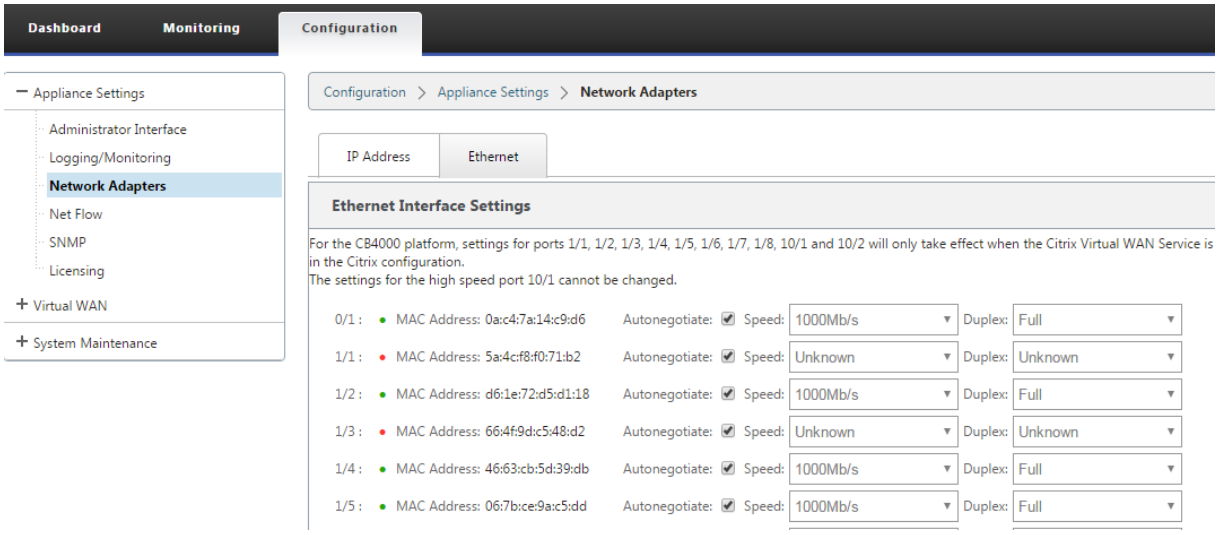
Para supervisar la configuración de alta disponibilidad:

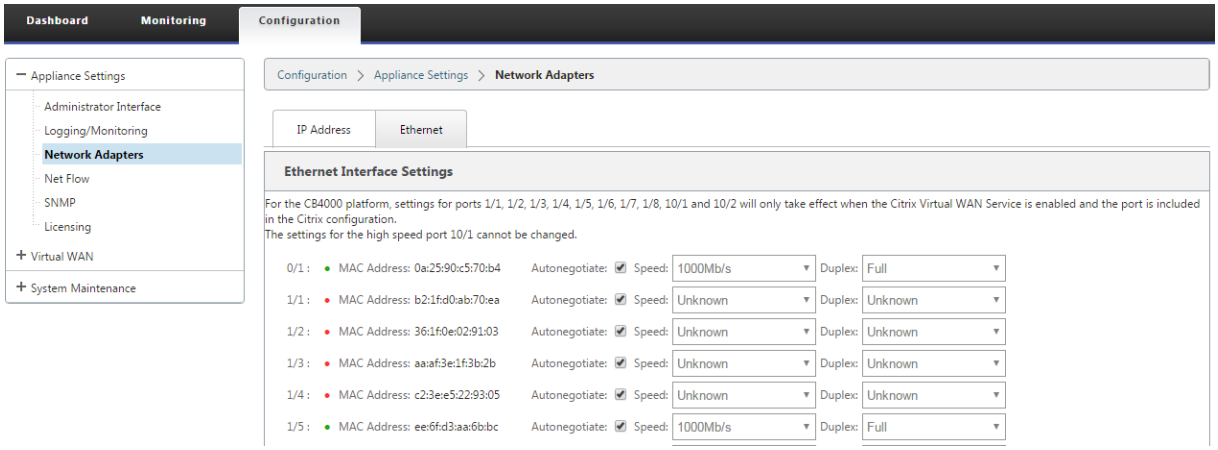
Inicie sesión en la interfaz de administración web de SD-WAN para los dispositivos activos y en espera para los que se ha implementado alta disponibilidad. Ver el estado de alta disponibilidad en la ficha **Panel** de control.





Para obtener detalles del adaptador de red de dispositivos de alta disponibilidad activos y en espera, vaya a **Configuración** > **Configuración del dispositivo** > **Adaptadores de red** > ficha **Ethernet**.





Solución de problemas

Realice los siguientes pasos de solución de problemas al configurar el dispositivo SD-WAN en modo de alta disponibilidad (HA):

1. La razón principal del problema del cerebro dividido se debe al problema de comunicación entre los dispositivos de alta disponibilidad.
    - Compruebe si hay algún problema con la conectividad (como, por ejemplo, los puertos de ambos dispositivos SD-WAN están activos o caídos) entre los dispositivos SD-WAN.
    - Debe inhabilitar el servicio SD-WAN en uno de los dispositivos SD-WAN para garantizar que solo un dispositivo SD-WAN esté activo.
2. Puede comprobar los registros relacionados con HA iniciado sesión en el archivo **SD-WAN_common.log**.

    > **NOTA**
    > Todos los registros relacionados con HA se registran con la palabra clave **racp**.

3. Puede comprobar los eventos relacionados con el puerto en el archivo **SDWAN_common.log** (como, por ejemplo, los puertos habilitados para HA desactivados o hacia arriba).
4. Por cada cambio de estado de HA, se registra un evento SD-WAN. Por lo tanto, si los registros se vuelcan, puede verificar los registros de eventos para obtener los detalles del evento.

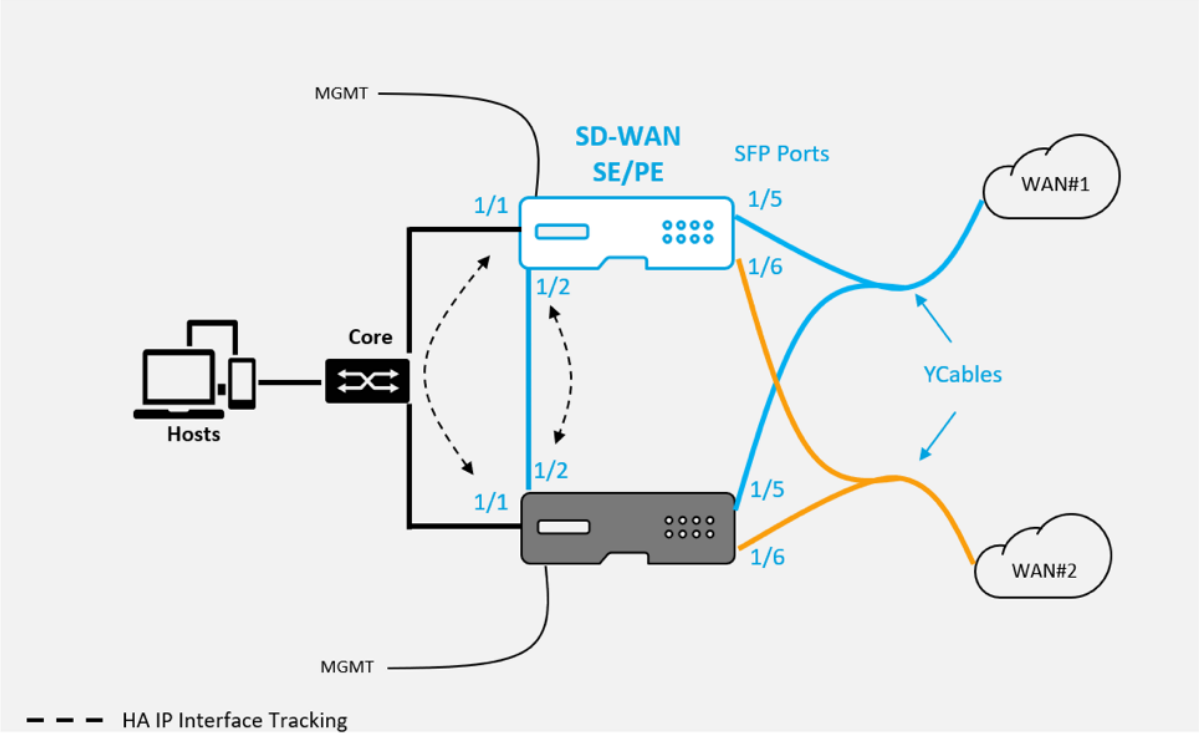
Habilitar alta disponibilidad en modo de borde mediante cable Y de fibra óptica

August 26, 2022

> Nota: En la versión 10.2 versión 2, esta funcionalidad solo se aplica al dispositivo 1100 SE.

El siguiente procedimiento describe los pasos para habilitar la Alta Disponibilidad (HA) en 1100 dispositivos SE implementados en modo Edge, donde las transferencias de los proveedores de servicios de enlace WAN son de fibra óptica.
Los puertos conectables de factor de forma pequeño (SFP) disponibles en los dispositivos 1100 se pueden utilizar con cables Y de fibra óptica para habilitar la función de alta disponibilidad para la implementación del modo perimetral.
En el dispositivo 1100 SE, el extremo dividido del cable divisor se conecta a los puertos de fibra de dos dispositivos 1100 que están configurados en par HA.
El cable en Y de fibra óptica tiene tres extremos. Un extremo se conecta a la transferencia de fibra del proveedor y los otros dos extremos se conectan a los puertos SFP configurados para ese enlace WAN en dos dispositivos 1100 SE implementados en un par HA. El cable divisor se utiliza para dividir una señal entrante en varias señales.

Para obtener información sobre la implementación de alta disponibilidad basada en el servicio Edge Mode de SD-WAN Orchestrator, consulte Detalles del dispositivo



Limitaciones:

- No se admite la configuración del modo Fail-to-Wire de HA mediante cable en Y.
- Los SFP conectados al cable Y, no se pueden utilizar como seguimiento de interfaz IP HA.
- Se requiere la versión 10.2.2 o posterior de software y 11.0 o posterior para admitir esta implementación.

Tacto cero

August 26, 2022

> **Nota**
>
> El servicio Zero Touch Deployment se admite en determinados dispositivos Citrix SD-WAN:
>
> - SD-WAN 110 Standard Edition
> - SD-WAN 210 Standard Edition
> - SD-WAN 1100 Standard Edition
> - SD-WAN 2100 Standard Edition
> - Instancia de AWS VPX de SD-WAN

Cloud Service de implementación sin contacto es un servicio basado en la nube administrado y operado por Citrix que permite descubrir nuevos dispositivos en la red Citrix SD-WAN, centrándose principalmente en optimizar el proceso de implementación de Citrix SD-WAN en sucursales u oficinas de servicios en la nube. El servicio en la nube de implementación sin contacto es accesible públicamente desde cualquier punto de una red a través del acceso público a Internet. Se accede al servicio en la nube de implementación sin intervención a través del protocolo Secure Socket Layer (SSL).

Los servicios en la nube de implementación sin intervención se comunican de forma segura con los servicios de Citrix de fondo que alojan la identificación almacenada de los clientes de Citrix que han comprado dispositivos compatibles con Zero Touch (por ejemplo, 2100-SE). Los servicios back-end están disponibles para autenticar cualquier solicitud de implementación Zero Touch, validando correctamente la asociación entre la cuenta del cliente y los números de serie de los dispositivos Citrix SD-WAN.

Para obtener más información, consulte el tema Implementación sin intervención de Citrix SD-WAN Orchestrator Service.

Arquitectura y flujo de trabajo de alto nivel de ZTD:

Sitio del centro de datos:

Citrix SD-WAN Administrator: Usuario con derechos de administración del entorno SD-WAN con las siguientes responsabilidades principales:

- Citrix Cloud Login para iniciar el servicio Zero Touch Deployment Service para la implementación de nuevos nodos de sitio.

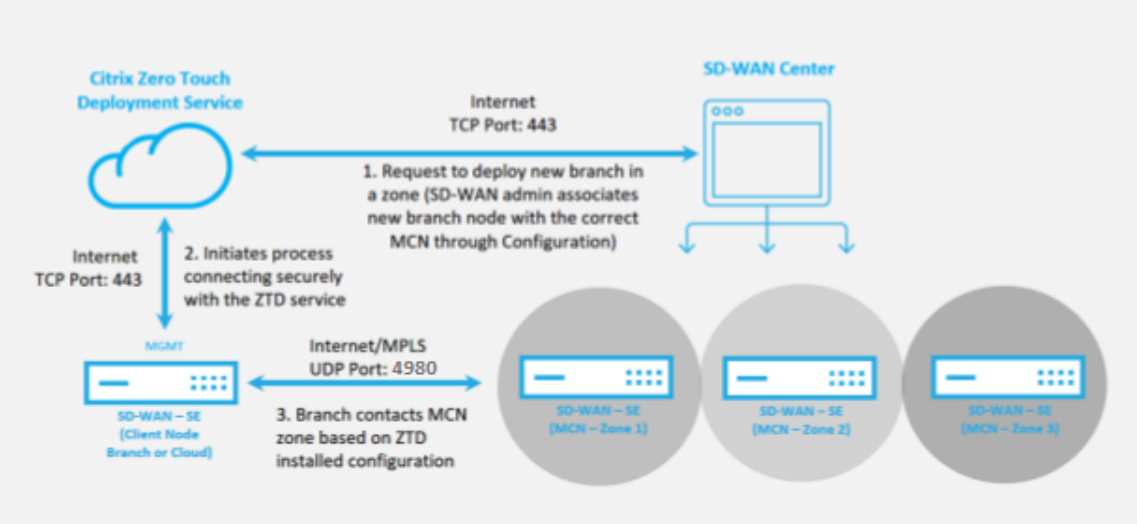
Administrador de red: Usuario responsable de la administración de redes empresariales (DHCP, DNS, Internet, firewall, etc.).

Sitio remoto:

Instalador in situ: Contacto local o instalador contratado para actividades in situ con las siguientes responsabilidades principales:

- Desempaque físicamente el dispositivo Citrix SD-WAN.
- Reimagen de dispositivos listos para ZTD.
  - Necesario para: SD-WAN 1000-SE, 2000-SE, 1000-EE, 2000-EE
  - No es necesario para: SD-WAN 410-SE, 2100-SE
- Cable de alimentación del dispositivo.
- Cable del dispositivo para la conectividad a Internet en la interfaz de administración (por ejemplo, MGMT o 0/1).
- Cable el dispositivo para la conectividad de vínculos WAN en las interfaces de datos (por ejemplo apA.WAN, apB.WAN, apC.WAN, 0/2, 0/3, 0/5, etc.).

> **Nota**
>
> El diseño de la interfaz es diferente para cada modelo, por lo que consulte la documentación para la identificación de los puertos de datos y administración.

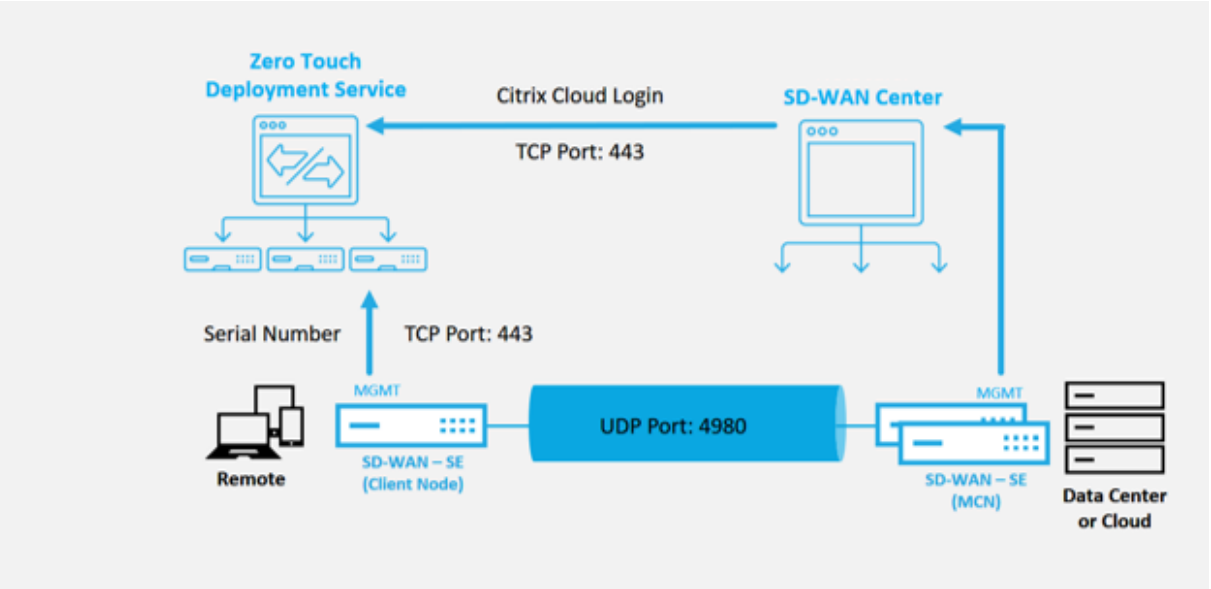


Se requieren los siguientes requisitos previos antes de iniciar cualquier servicio Zero Touch Deployment:

- Ejecución activa de SD-WAN promovida a Master Control Nodo (MCN).
- Credenciales de inicio de sesión de Citrix Cloud creadas en https://onboarding.cloud.com (consulte las instrucciones que aparecen a continuación sobre la creación de cuentas).
- Conectividad de red de administración (dispositivo SD-WAN) a Internet en el puerto 443, ya sea directamente o a través de un servidor proxy.

- (Opcional) Al menos un dispositivo SD-WAN en ejecución activa que funcione en una sucursal en modo cliente con conectividad de ruta virtual válida a MCN para ayudar a validar el establecimiento exitoso de rutas en la red subyacente existente.

El último requisito previo no es un requisito, pero permite que el administrador de SD-WAN valide que la red subyacente permite que se establezcan rutas virtuales cuando se complete la implementación sin intervención con cualquier sitio recién agregado. Principalmente, esto valida que existen las directivas de firewall y ruta adecuadas para el tráfico NAT en consecuencia o para confirmar la capacidad del puerto UDP 4980 para penetrar correctamente en la red para llegar al MCN.



Descripción general del servicio de implementación Zero Touch:

Para usar el servicio de implementación sin intervención (o el servicio en la nube de implementación sin intervención), un administrador debe comenzar por implementar el primer dispositivo SD-WAN en el entorno.

Después de un entorno SD-WAN en funcionamiento, el registro en Zero Touch Deployment Service se realiza mediante la creación de un inicio de sesión en la cuenta de Citrix Cloud. Al iniciar sesión en el servicio Zero Touch, se autentica el ID de cliente asociado con el entorno de SD-WAN en particular.

Cuando el administrador de SD-WAN inicia un sitio para la implementación mediante el proceso de implementación sin intervención, tiene la opción de autenticar previamente el dispositivo que se utilizará para la implementación sin intervención, rellenando previamente el número de serie e iniciando la comunicación por correo electrónico con el instalador in situ para comenzar in situ actividad.

El instalador in situ recibe una comunicación por correo electrónico en la que se indica que el sitio está listo para la implementación de Zero Touch y que puede iniciar el procedimiento de instalación de encendido y cableado del dispositivo para la asignación de direcciones IP DHCP y el acceso a Internet en el puerto MGMT. Además, cableado en cualquier puerto LAN y WAN. Todo lo demás se inicia

mediante el servicio de implementación sin intervención y el progreso se supervisa mediante la URL de activación. En caso de que el nodo remoto que se va a instalar sea una instancia en la nube, al abrir la URL de activación se inicia el flujo de trabajo para instalar automáticamente la instancia en el entorno de nube designado, ningún instalador local necesita ninguna acción.

El servicio en la nube Zero Touch Deployment automatiza las siguientes acciones:

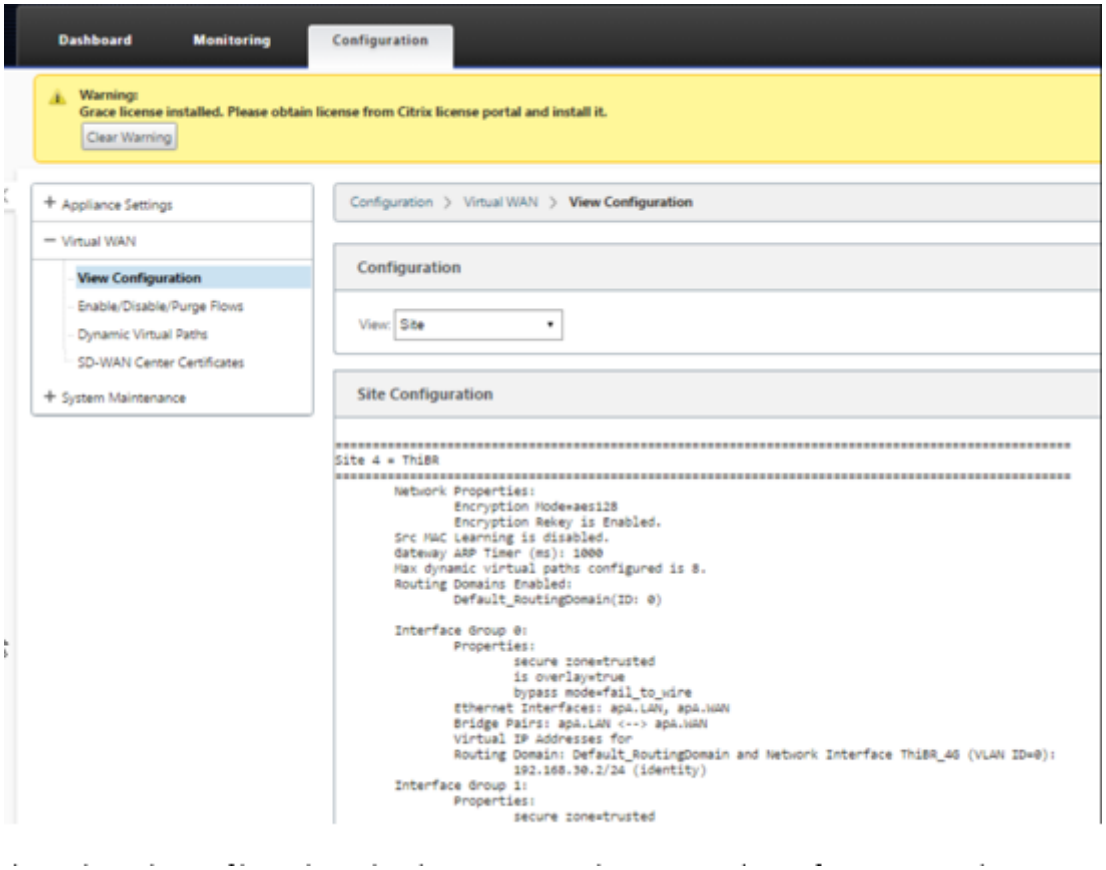
Descargue y actualice el Agente de implementación sin contacto si hay nuevas funciones disponibles en el dispositivo de sucursal.

- Autenticar el dispositivo de rama validando el número de serie.
- Inserte el archivo de configuración específico del dispositivo de destino en el dispositivo de rama.
- Instale el archivo de configuración en el dispositivo de rama.
- Inserte los componentes de software de SD-WAN que falten o las actualizaciones necesarias en el dispositivo de rama.
- Inserte un archivo de licencia temporal de 10 Mbps para confirmar el establecimiento de la ruta virtual en el dispositivo de rama.
- Habilite el servicio SD-WAN en el dispositivo de rama.

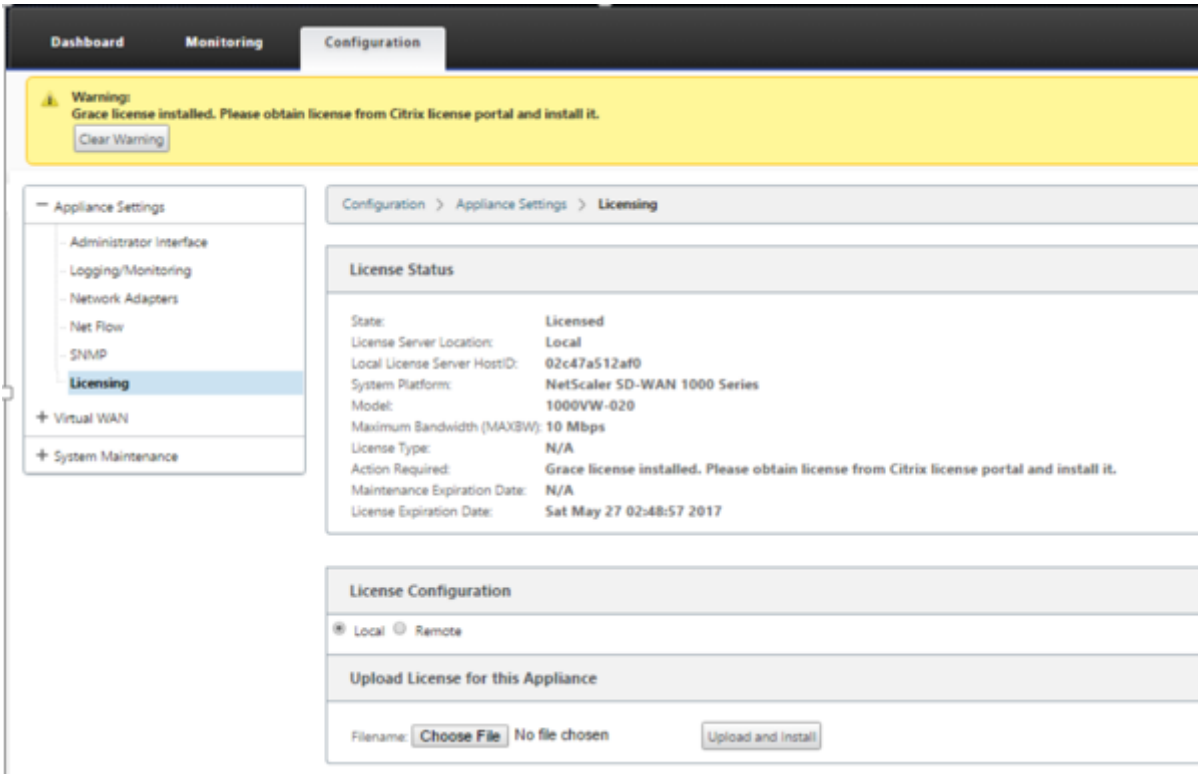
Se requieren más pasos del Administrador de SD-WAN para instalar un archivo de licencia permanente en el dispositivo.

> **Nota**
>
> Al realizar una configuración de sucursal que ya tiene la misma versión del software del dispositivo utilizada en MCN, el proceso de implementación sin táctiles no volverá a descargar el archivo de software del dispositivo. Este cambio se aplica a los dispositivos recién enviados de fábrica, a los dispositivos que se restablecen a los valores predeterminados de fábrica y a los restablecimiento de configuración administrativamente. Si se restablece la configuración, marque la casilla **Reiniciar después de revertir** para iniciar el proceso de implementación sin intervención.

La configuración del dispositivo se puede validar mediante la página **Configuración** > **WAN virtual** > **Ver configuración**.



El archivo de licencia del dispositivo se puede actualizar a una licencia permanente mediante la página **Configuración** > **Configuración del dispositivo** > **Licencias**.



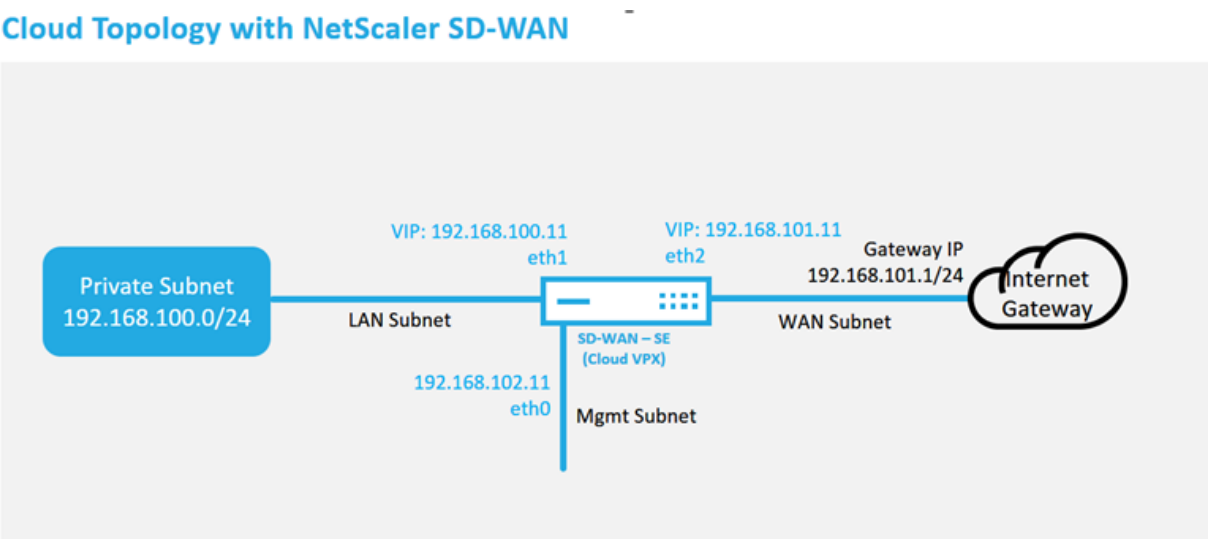
Después de cargar e instalar el archivo de licencia permanente, el mensaje de advertencia de licencia Grace desaparece y durante el proceso de instalación de la licencia no se produce ninguna pérdida de conectividad con el sitio remoto (no se descartan los pings).

AWS

August 26, 2022

Con la versión 11.5 de SD-WAN, se admite la implementación sin intervención en un entorno de AWS a través de SD-WAN Orchestrator Service.

> **Nota**
>
> - Las instancias SD-WAN implementadas en la nube deben implementarse en modo Edge/-Gateway.
> - La plantilla para la instancia en la nube está limitada a tres interfaces: Administración, LAN y WAN (en ese orden).
> - Las plantillas de nube disponibles para SD-WAN VPX están configuradas actualmente para obtener la dirección IP #.#.#.#.11 de las subredes disponibles en la VPC.



Este es un ejemplo de implementación de un sitio implementado en la nube SD-WAN, el dispositivo Citrix SD-WAN se implementa como el dispositivo perimetral que presta servicio a un único enlace WAN de Internet en esta red en la nube. Los sitios remotos podrán aprovechar varios enlaces WAN de Internet distintos que se conectan a esta misma puerta de enlace de Internet para la nube, proporcionando resiliencia y conectividad de ancho de banda agregada desde cualquier sitio de implementación de SD-WAN a la infraestructura de la nube. Esto proporciona conectividad rentable y altamente confiable a la nube.

Azure

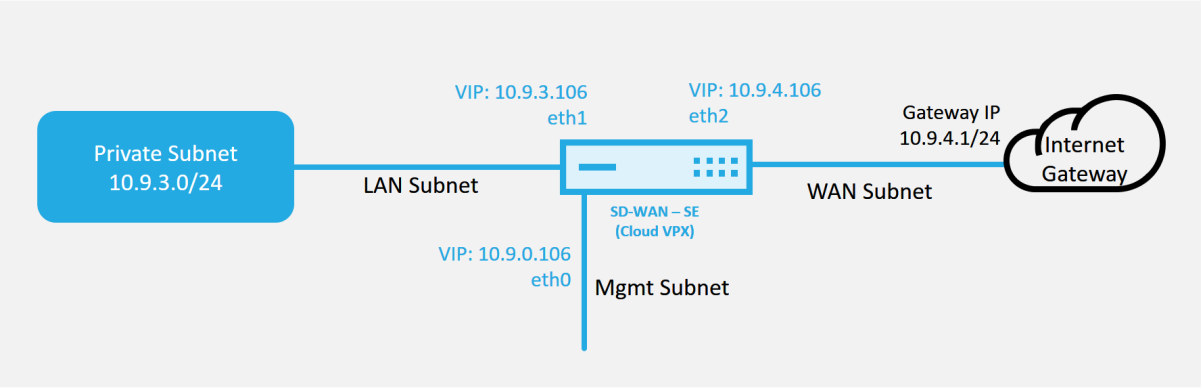
August 26, 2022

Con la versión 11.5 de SD-WAN, se admite la implementación sin intervención en un entorno Azure a través de SD-WAN Orchestrator Service.

> **Nota**
>
> - Las instancias SD-WAN implementadas en la nube deben implementarse en modo Edge/-Gateway.
> - La plantilla para la instancia en la nube está limitada a tres interfaces: Administración, LAN y WAN (en ese orden).
> - Las plantillas disponibles en la nube de Azure para SD-WAN VPX están actualmente configuradas para obtener la IP 10.9.4.106 para la WAN, la IP 10.9.3.106 para la LAN y la IP 10.9.0.16 para la dirección de administración. La configuración de SD-WAN para el nodo de Azure destinado a Zero Touch debe coincidir con este diseño.

- El nombre del sitio de Azure en la configuración debe estar en minúsculas sin caracteres especiales (por ejemplo, ztdazure).

Azure Cloud Topology with NetScaler SD-WAN



Este es un ejemplo de implementación de un sitio implementado en la nube SD-WAN, el dispositivo Citrix SD-WAN se implementa como el dispositivo perimetral que da servicio a un único enlace WAN de Internet en esta red en la nube. Los sitios remotos podrán aprovechar varios enlaces WAN de Internet distintos que se conectan a esta misma puerta de enlace de Internet para la nube, proporcionando resiliencia y conectividad de ancho de banda agregada desde cualquier sitio de implementación de SD-WAN a la infraestructura de la nube. Esto proporciona conectividad rentable y altamente confiable a la nube.

Implementación de una región

August 26, 2022

Las regiones le permiten definir una jerarquía de red con administración distribuida. Una región debe definir un nodo de control regional (RCN) que asumirá las funciones realizadas por el nodo de control de red (MCN) para su región. El MCN es el Controller de la región predeterminada. No se permiten rutas virtuales estáticas y dinámicas entre regiones. Los RCN gestionan el tráfico entre Regiones. Una implementación de una sola región en una red SD-WAN puede admitir sitios de red de menos de 550.

Para obtener más información sobre la implementación de una sola región a través de Citrix SD-WAN Orchestrator Service, consulte Regiones.

Implementación en varias regiones

August 26, 2022

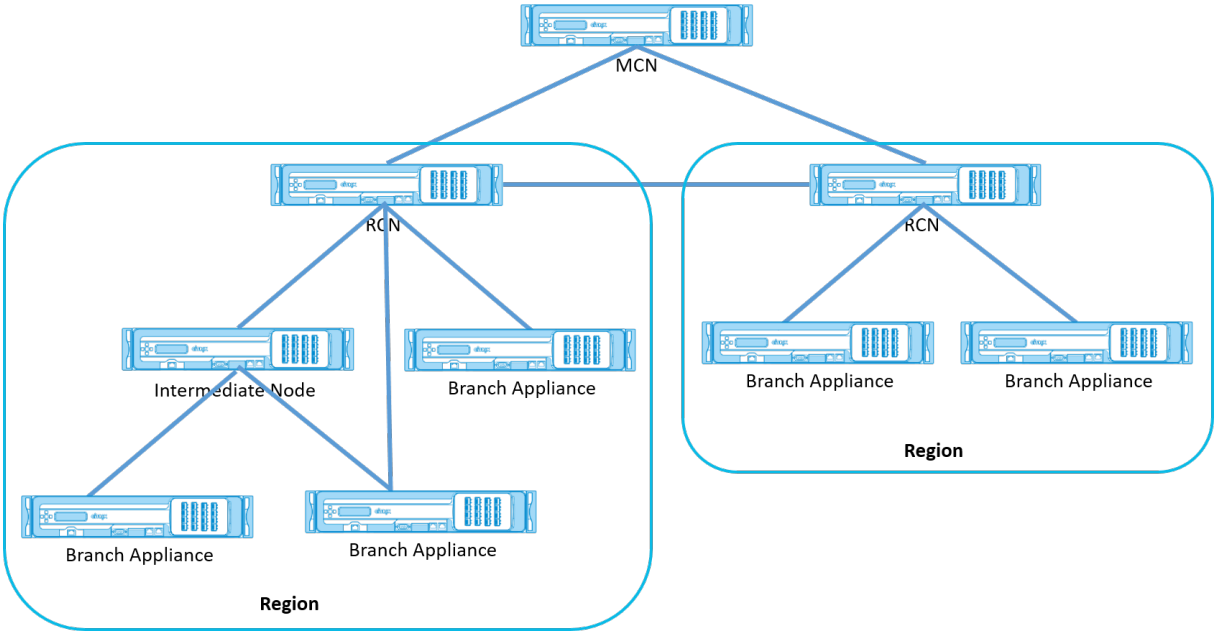
Un dispositivo SD-WAN configurado como nodo de control maestro (MCN) admite la implementación en varias regiones. El MCN administra varios nodos de control regional (RCN). Cada RCN, a su vez, administra varios sitios cliente. El MCN también se puede usar para administrar algunos de los sitios cliente directamente.

Con MCN como nodo de control de la red y RCNs como nodos de control de las regiones, SD-WAN puede administrar hasta 6000 sitios.

La implementación de varias regiones le permite fragmentar una red en regiones y configurar una red en niveles; por ejemplo, sucursal (cliente) > RCN > MCN.

Un MCN con una sola región se puede configurar con un máximo de 1000 sitios. Puede mantener los sitios existentes en la región predeterminada y agregar nuevas regiones con RCN y sus sitios para la implementación en varias regiones.

Para obtener más información sobre la implementación en varias regiones a través de Citrix SD-WAN Orchestrator Service, consulte Regions.



La siguiente tabla proporciona la lista de plataformas admitidas para configurar MCN/RCN primario y secundario.

> **NOTA**
>
> Utilice el dispositivo Citrix SD-WAN 210 SE como un MCN solo en las redes administradas por

> SD-WAN Orchestrator.

Modificación de plataforma	MCN primario/secundario	RCN primario/secundario
110-SE	No	No
210-SE	Sí	Sí
1100-SE	Sí	Sí
VPX-SE, VPXL-SE	Sí	Sí
2100-SE, 4100-SE, 5100-SE, 6100-SE	Sí	Sí

Guía de configuración para cargas de trabajo de Citrix Virtual Apps and Desktops

August 26, 2022

Citrix SD-WAN es una solución WAN Edge de próxima generación que acelera la transformación digital con conectividad y rendimiento flexibles, automatizados y seguros para aplicaciones SaaS, cloud y virtuales para garantizar una experiencia de Workspace siempre activa.

Citrix SD-WAN es la mejor manera recomendada para que las organizaciones que utilizan Citrix Virtual Apps and Desktops Service se conecten a las cargas de trabajo de Citrix Virtual Apps and Desktops en la nube. Para obtener más información, consulte el blog de Citrix.

Este documento se centra en configurar Citrix SD-WAN para conectividad a/desde cargas de trabajo de Citrix Virtual Apps and Desktops en Azure.

Ventajas

- Fácil de configurar SD-WAN en Citrix Virtual Apps and Desktops a través de un flujo de trabajo guiado
- Conectividad de alto rendimiento siempre activa a través de tecnologías avanzadas SD-WAN
- Beneficios en todas las conexiones (VDA a CC, Usuario a VDA, VDA a nube, usuario a nube)
- Reduce la latencia en comparación con el tráfico de backhauling al centro de datos
- Gestión del tráfico para garantizar la calidad de servicio (QoS)
  - QoS en flujos de tráfico HDX/ICA (AutoQoS HDX multisecuencia de puerto único)

  - QoS entre HDX y otro tráfico
  - QoS HDX Equidad entre los usuarios
  - QoS de extremo a extremo

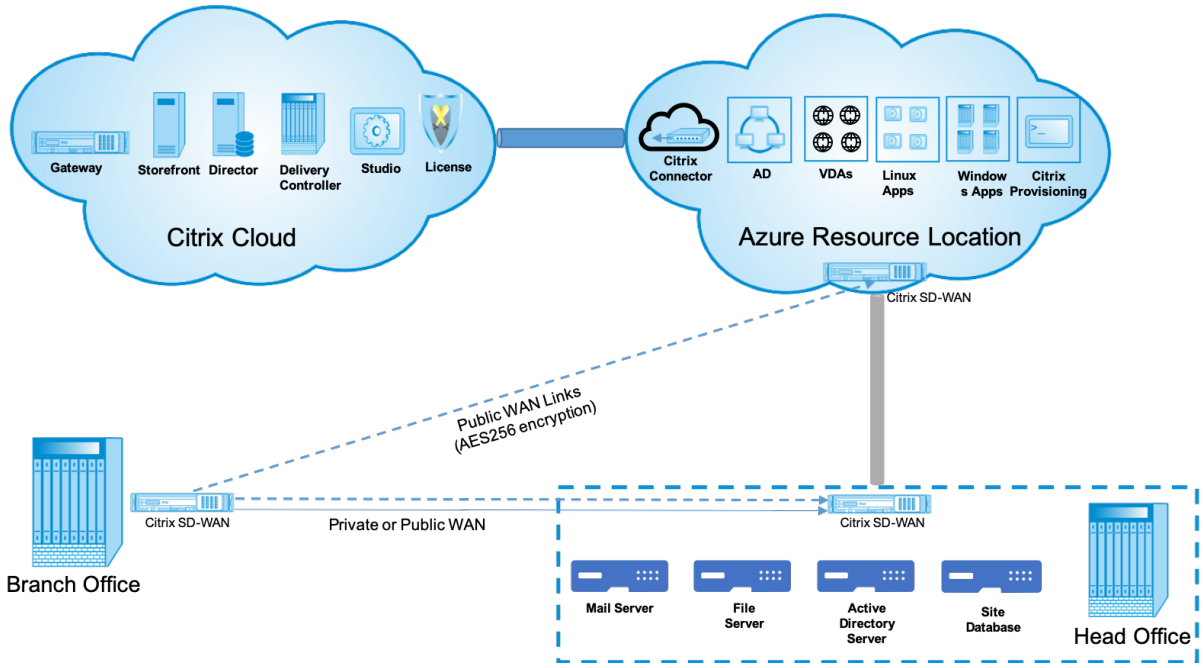
- La unión de enlaces ofrece más ancho de banda para un rendimiento más rápido
- Alta disponibilidad con conmutación por error de enlace transparente y redundancia SD-WAN en Azure
- Experiencia VoIP optimizada (carreras de paquetes para reducir la fluctuación y la pérdida mínima de paquetes, QoS, ruptura local para reducir la latencia)
- Importantes ahorros de costes y debe ser más rápido y fácil de implementar en comparación con Azure ExpressRoute

Requisitos previos

Siga los siguientes requisitos previos para evaluar e implementar las capacidades de cargas de trabajo de Citrix Virtual Apps and Desktops:

- Debe tener una red SD-WAN existente o crear una nueva.
- Debe tener una suscripción al servicio Citrix Virtual Apps and Desktops.
- Para hacer uso de las funciones de SD-WAN como, multisecuencia HDX AutoQoS y visibilidad profunda, el Servicio de ubicación de red (NLS) debe configurarse para todos los sitios SD-WAN de la red.
- Debe tener un servidor DNS y AD implementados donde estén presentes los extremos del cliente (a menudo ubicados en el entorno del centro de datos) o puede utilizar Azure Active Directory (AAD).
- El servidor DNS debe ser capaz de resolver IP internas (privadas) y externas (públicas).
- Asegúrese de que el FQDN (sdwan-location.citrixnetworkapi.net) se agrega a la lista permitida en el firewall. Este es el FQDN para el servicio de ubicación de red, que es crítico para enviar tráfico a través de la ruta virtual SD-WAN. Además, una mejor manera si se siente cómodo con la inclusión de FQDN de comodines blancos sería agregar *.citrixnetworkapi.net a la lista permitida, ya que este es el subdominio para otros servicios de Citrix Cloud, como el aprovisionamiento de cero toque.
- Inscríbase en sdwan.cloud.com para utilizar el orquestador SD-WAN para administrar su red SD-WAN. SD-WAN Orchestrator es una plataforma de administración multitenant basada en Citrix Cloud para Citrix SD-WAN.

Arquitectura de la implementación



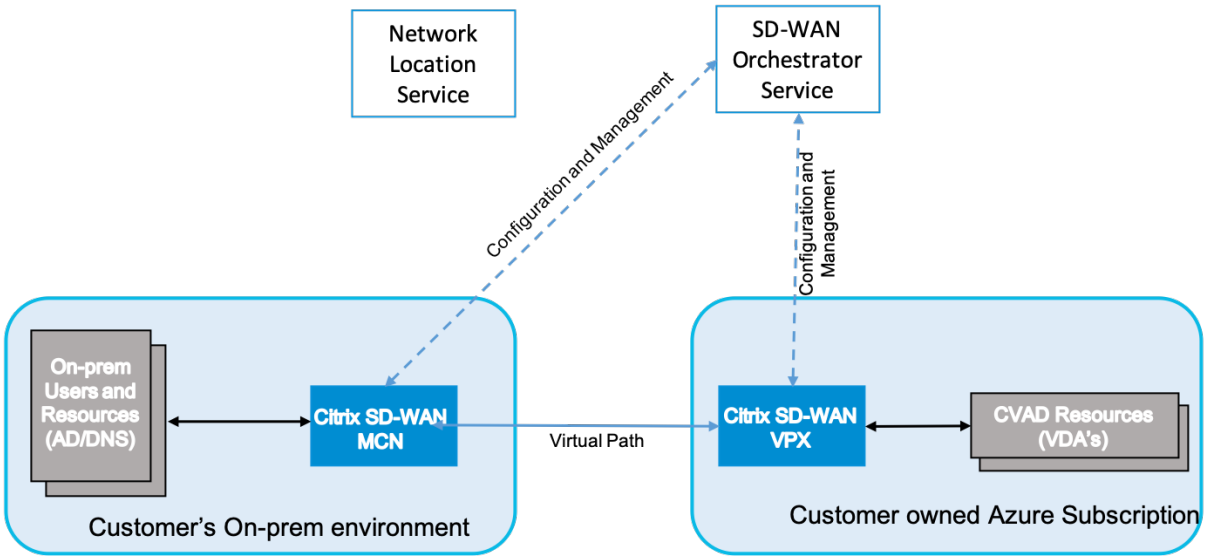
Las siguientes entidades son necesarias para la implementación:

- Ubicación local que aloja el dispositivo SD-WAN que se puede implementar en modo sucursal o como MCN (nodo de control maestro). El modo de rama o MCN contiene las máquinas cliente, el directorio activo y el DNS. Sin embargo, también puede elegir usar DNS y AD de Azure. En la mayoría de los casos, la ubicación local sirve como centro de datos y alberga el MCN.
- **Servicio en la nube Citrix Virtual Apps and Desktops**: Citrix Virtual Apps and Desktops ofrece soluciones de virtualización que proporcionan control de TI de las máquinas virtuales, las aplicaciones y la seguridad a la vez que proporcionan acceso a cualquier dispositivo en cualquier lugar. Los usuarios finales pueden utilizar aplicaciones y escritorios independientemente de la interfaz y del sistema operativo del dispositivo que estén utilizando.

  Con Citrix Virtual Apps and Desktops Service, puede entregar aplicaciones virtuales y escritorios seguros a cualquier dispositivo y dejar la mayor parte de la instalación, configuración, actualizaciones y supervisión del producto a Citrix. Este servicio le permite mantener un control total sobre las aplicaciones, las directivas y los usuarios, al mismo tiempo que ofrece la mejor experiencia de usuario en cualquier dispositivo.
- **Connector/cloud connector de Citrix**: Puede conectar sus recursos al servicio a través de Citrix Cloud Connector, que sirve como canal para la comunicación entre Citrix Cloud y sus ubicaciones de recursos. Cloud Connector permite administrar una nube sin necesidad de configurar redes ni infraestructuras complejas (como redes VPN o túneles IPsec). Las ubicaciones de recursos contienen las máquinas y otros recursos que entregan aplicaciones y escritorios a los suscriptores.

- **SD-WAN Orchestrator** —Citrix SD-WAN Orchestrator es un servicio de administración multiarrendatario alojado en la nube disponible para las empresas **Hágalo usted mismo** y los socios de Citrix. Los socios de Citrix pueden usar SD-WAN Orchestrator para administrar varios clientes con un solo panel de vidrio y controles de acceso adecuados basados en roles.
- Dispositivos**SD-WAN virtuales y físicos**: Se ejecuta como varias instancias dentro de la nube (VM) y en las instalaciones en el centro de datos y en las sucursales (dispositivos físicos o máquinas virtuales) para proporcionar conectividad entre estas ubicaciones y a/desde Internet pública. La instancia de SD-WAN en Citrix Virtual Apps and Desktops se crea como un solo dispositivo virtual o un conjunto de dispositivos virtuales (en caso de implementación de alta disponibilidad) mediante el aprovisionamiento de estas instancias a través de Azure Marketplace. Los dispositivos SD-WAN en otras ubicaciones (DC y sucursales) son creados por el cliente. Todos estos dispositivos SD-WAN son administrados (en términos de configuración y actualizaciones de software) por administradores de SD-WAN a través de SD-WAN Orchestrator.

Implementación y configuración



En una implementación común, un cliente tendría el dispositivo Citrix SD-WAN (H/W o VPX) implementado como MCN en su oficina de DC/Large. El controlador de dominio del cliente suele alojar usuarios y recursos locales, como servidores AD y DNS. En algunos casos, el cliente puede utilizar los servicios de Azure Active Directory (AADS) y DNS, ambos compatibles con la integración de Citrix SD-WAN y CMD.

Dentro de la suscripción de Azure administrada por el cliente, el cliente debe implementar el dispositivo virtual SD-WAN y los VDA de Citrix. Los dispositivos SD-WAN se administran a través de SD-WAN Orchestrator. Una vez configurado el dispositivo SD-WAN, se conecta a la red Citrix SD-WAN existente y otras tareas, como la configuración, la visibilidad y la administración, se gestionan a través de SD-

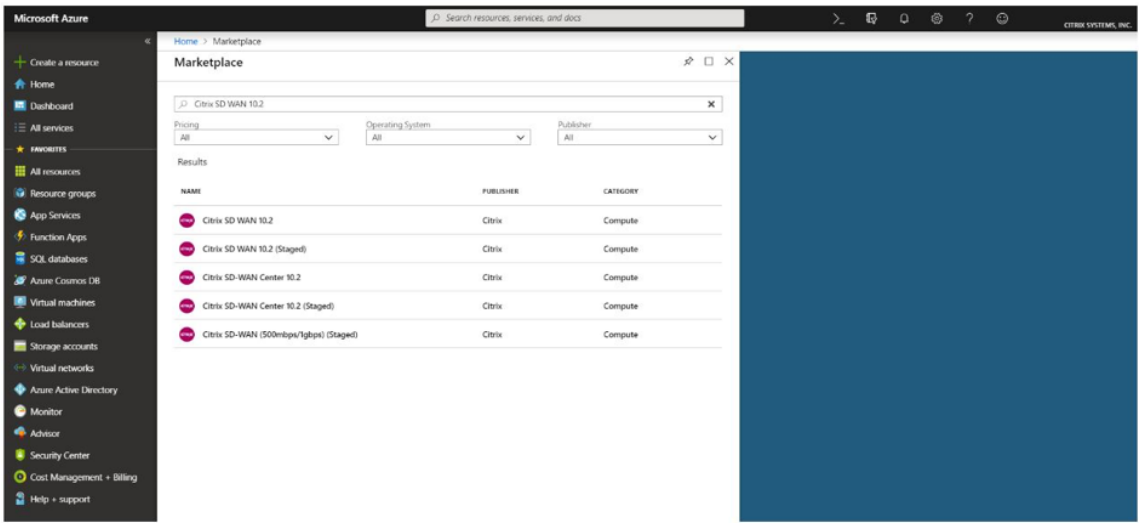
WAN Orchestrator.

El tercer componente de esta integración es el **Servicio de ubicación de red (NLS)** que permite a los usuarios internos eludir la puerta de enlace y conectarse directamente a los VDA, reduciendo la latencia del tráfico de red interno. Puede configurar NLS manualmente o mediante Citrix SD-WAN Orchestrator. Para obtener más información, consulte NLS.

Configuración

La VM de Citrix SD-WAN se implementa dentro de una región especificada (según sea necesario por el cliente) y se puede conectar a varias sucursales a través de MPLS, Internet o 4G/LTE. Dentro de una infraestructura de red virtual (VNET), la VM SD-WAN Standard Edition (SE) se implementa en modo de Gateway. La VNET tiene rutas hacia la Gateway de Azure. La instancia de SD-WAN tiene una ruta hacia la Gateway de Azure para la conectividad a Internet. Esta ruta debe crearse manualmente.

1. En un explorador web, vaya al portal de Azure. Inicie sesión en la cuenta de Microsoft Azure y busque Citrix SD-WAN Standard Edition.
2. En los resultados de búsqueda, elija la solución Citrix SD-WAN Standard Edition. Haga clic en **Crear** después de revisar la descripción y asegurarse de que la solución elegida es correcta.

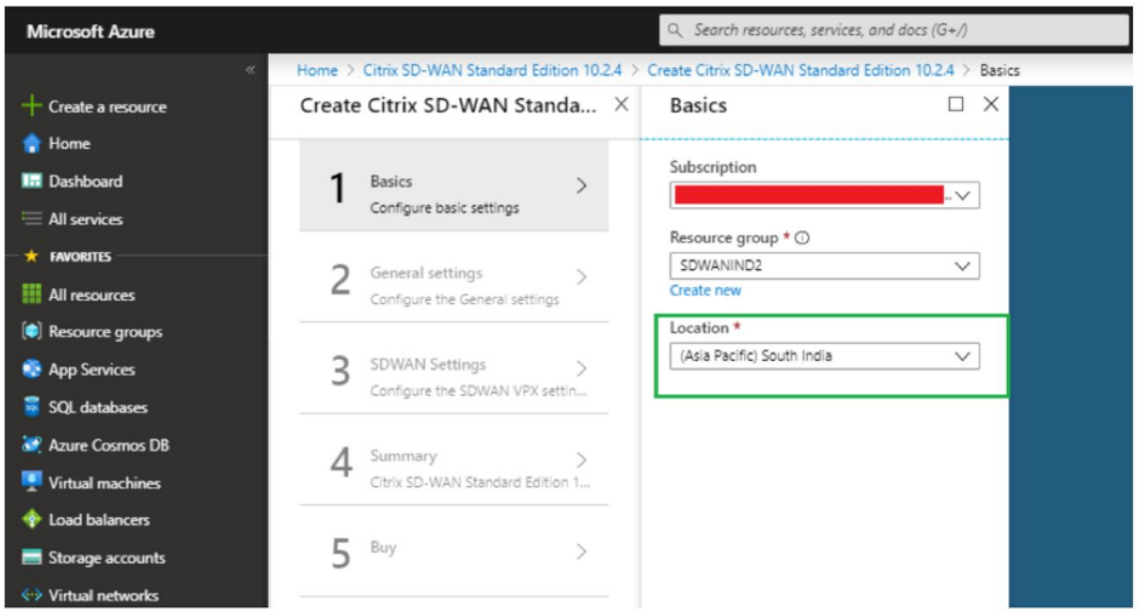


Al hacer clic en **Crear**, un asistente solicitará con los detalles necesarios para crear la máquina virtual.

3. En la página **Configuración básica**, elija el grupo de recursos en el que quiere implementar la solución SD-WAN SE.

   Un grupo de recursos es un contenedor que contiene recursos relacionados para una solución de Azure. El grupo de recursos puede incluir todos los recursos de la solución o solo los recursos que quiera administrar como grupo. Puede decidir cómo quiere asignar recursos a grupos de recursos en función de su implementación.

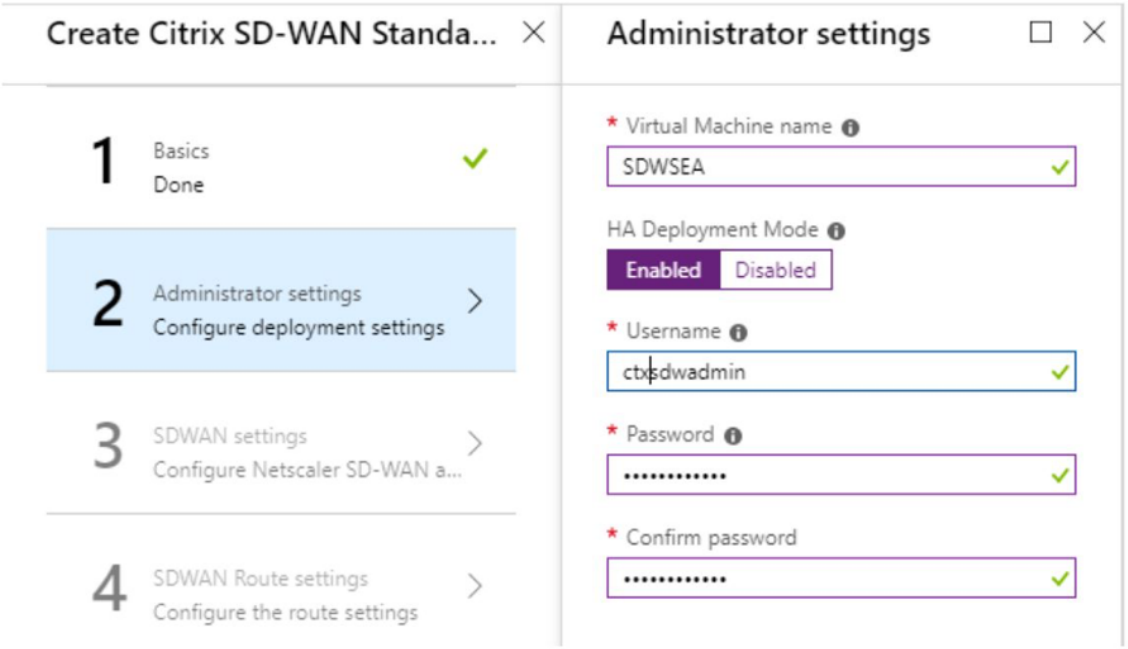
Para Citrix SD-WAN, se recomienda que el grupo de recursos que elija esté vacío. Del mismo modo, elija la región de Azure en la que quiere implementar la instancia de SD-WAN. La región debe ser la misma que la región en la que se implementan los recursos de Citrix Virtual Apps and Desktops.



4. En la página **Configuración del administrador**, proporcione un nombre para la máquina virtual. Elija un nombre de usuario y una contraseña segura. La contraseña debe consistir en una letra mayúscula, un carácter especial y debe tener más de nueve caracteres. Haga clic en **Aceptar**.

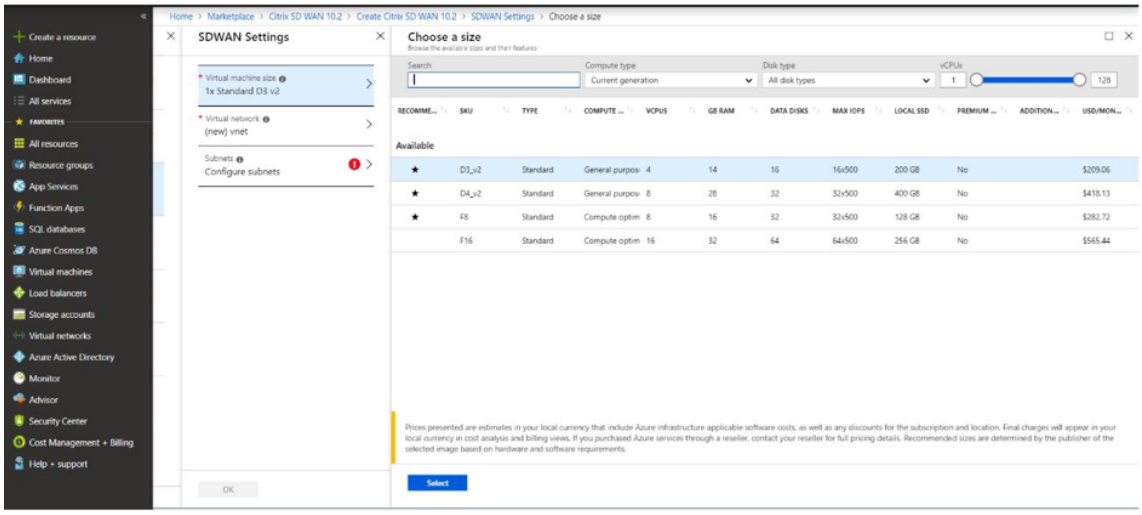
   Esta contraseña es necesaria para iniciar sesión en la interfaz de administración de la instancia como usuario invitado. Para obtener acceso de administrador a la instancia, utilice admin como nombre de usuario y contraseña creada al Provisioning la instancia. Si utiliza el nombre de usuario creado durante el Provisioning de la instancia, obtendrá acceso de solo lectura. Además, elija aquí el tipo de implementación.

   Si quiere implementar una sola instancia, asegúrese de elegir desactivado en la opción Modo de implementación de alta disponibilidad; de lo contrario, seleccione habilitado. En el caso de las redes de producción, Citrix siempre recomienda implementar instancias en modo HA, ya que protege la red contra los fallos de la instancia.



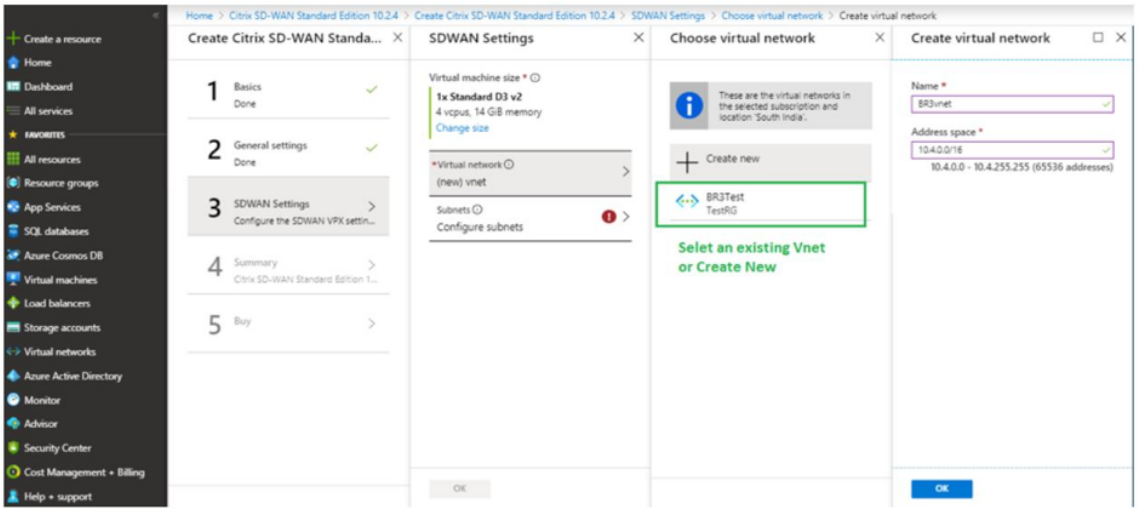
5. En la página **Configuración de SD-WAN**, elija la instancia en la que quiere ejecutar la imagen. Elija el siguiente tipo de instancia según su requisito:

   - Tipo de instancia D3_V2 para un rendimiento unidireccional máximo de 200 Mbps con conectividad directa a un máximo de 16 ramas.
   - Tipo de instancia D4_V2 para un rendimiento unidireccional máximo de 500 Mbps con conectividad directa a un máximo de 16 ramas.
   - Tipo de instancia estándar F8 para un rendimiento unidireccional máximo de 1 Gbps con conectividad directa a un máximo de 64 sucursales.
   - Tipo de instancia estándar F16 para un rendimiento unidireccional máximo de 1 Gbps con conectividad directa a un máximo de 128 sucursales.

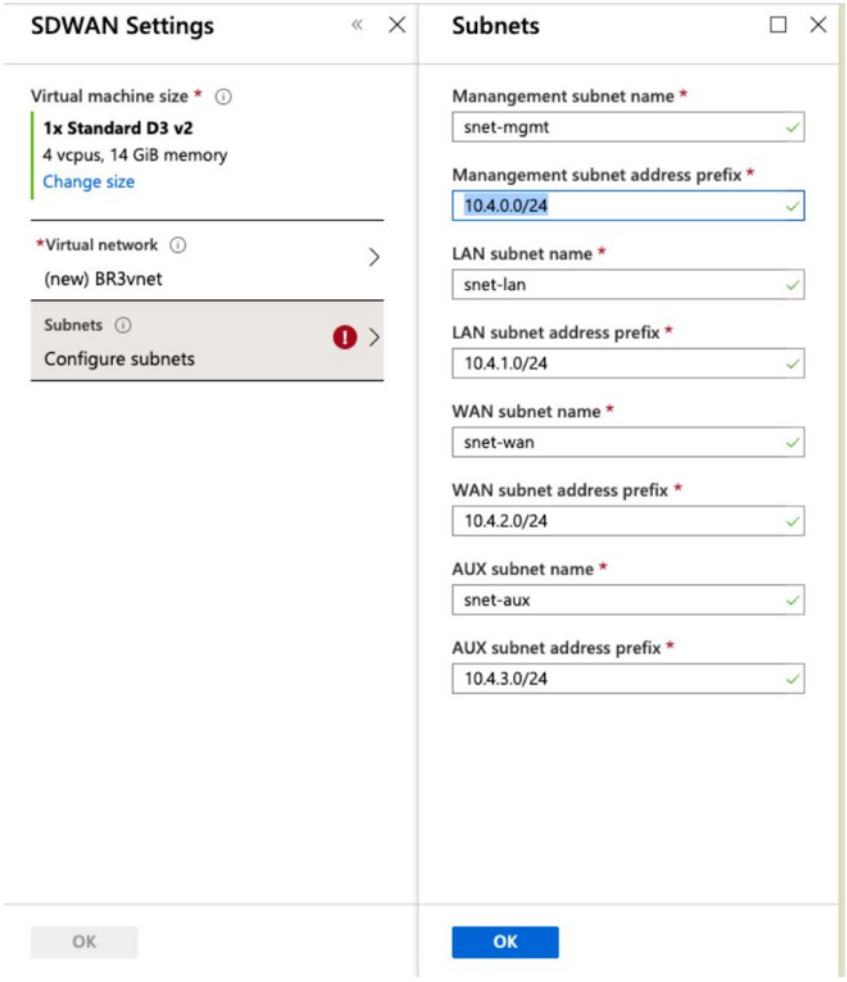


6. Cree una nueva red virtual (VNet) o utilice una red virtual existente. Este es el paso más crítico

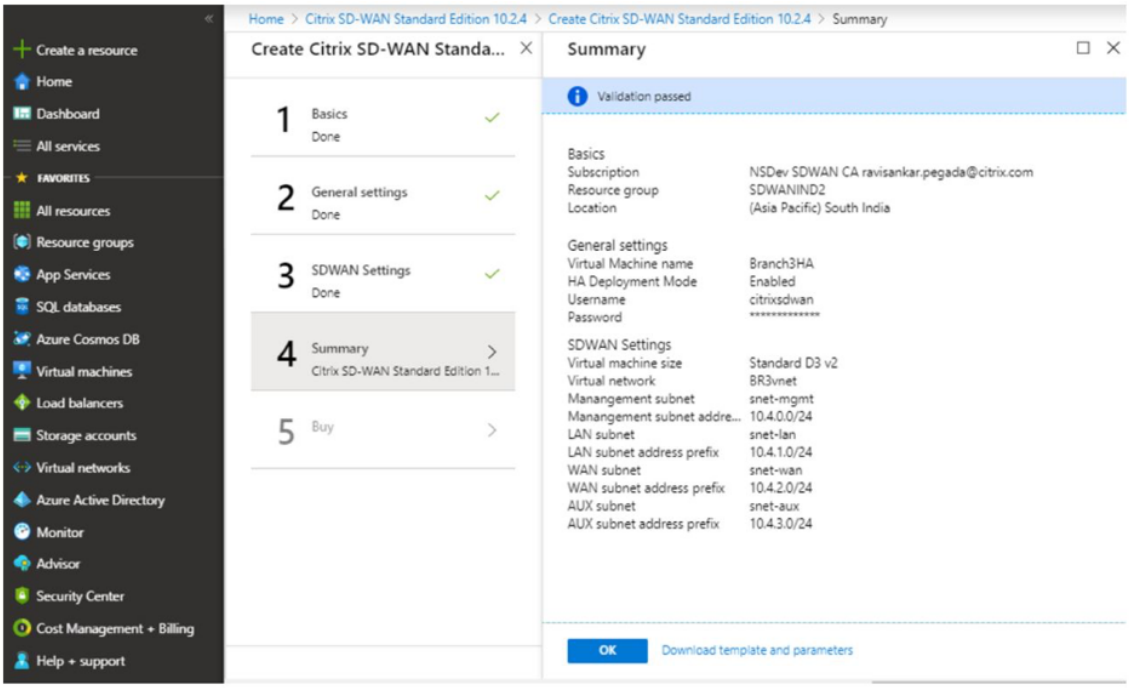
para la implementación, ya que este paso elige las subredes que se van a asignar a las interfaces de la VM VPX SD-WAN.



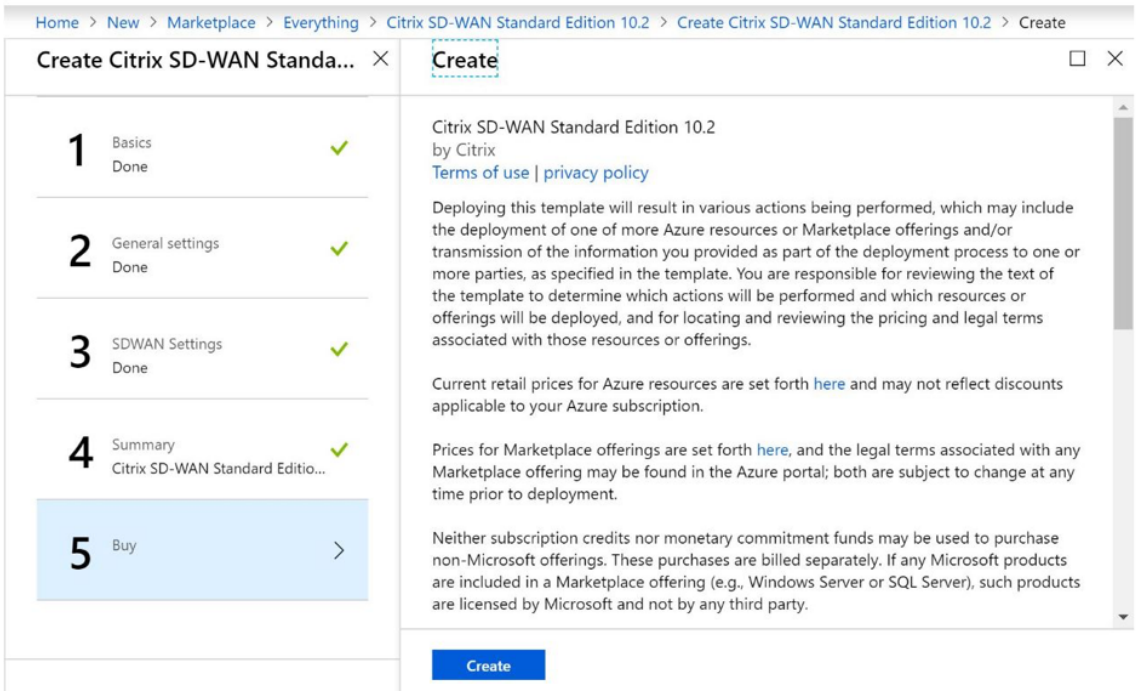
La subred auxiliar solo es necesaria cuando se implementan las instancias en modo HA. Asegúrese de que la instancia de SD-WAN se está implementando en la misma vNet que los recursos de Citrix Virtual Apps and Desktops y se encuentra en la misma subred que la interfaz LAN del dispositivo SD-WAN VPX.



7. Compruebe la configuración en la página **Resumen** y haga clic en **Aceptar**.



8. En la página **Comprar**, haga clic en **Crear** para iniciar el proceso de aprovisionamiento de las instancias. La instancia puede tardar alrededor de 10 minutos en ser aprovisionada. Recibe una notificación en el portal de administración de Azure que sugiere el éxito o el fracaso de la creación de instancias.

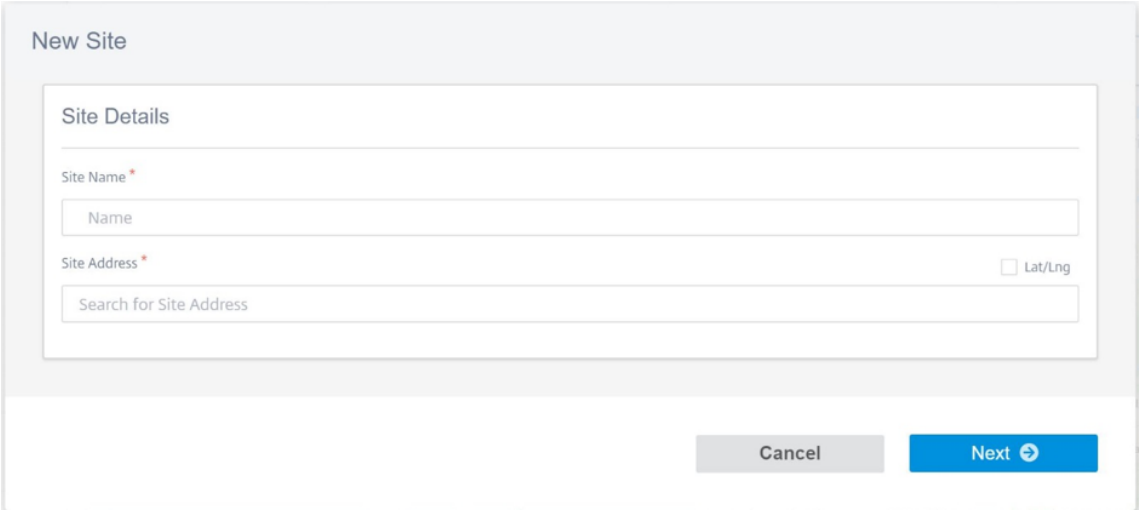


Una vez creada la instancia correctamente, obtenga la IP pública asignada a la interfaz de administración de la instancia de SD-WAN. Se puede encontrar en la sección de redes del grupo

de recursos dentro del cual se ha aprovisionado la instancia. Una vez recuperado, puede usarlo para iniciar sesión en la instancia.

> **Nota**
>
> Para el acceso de administrador, el nombre de usuario es **admin** y la contraseña es la que ha establecido durante la creación de la instancia.

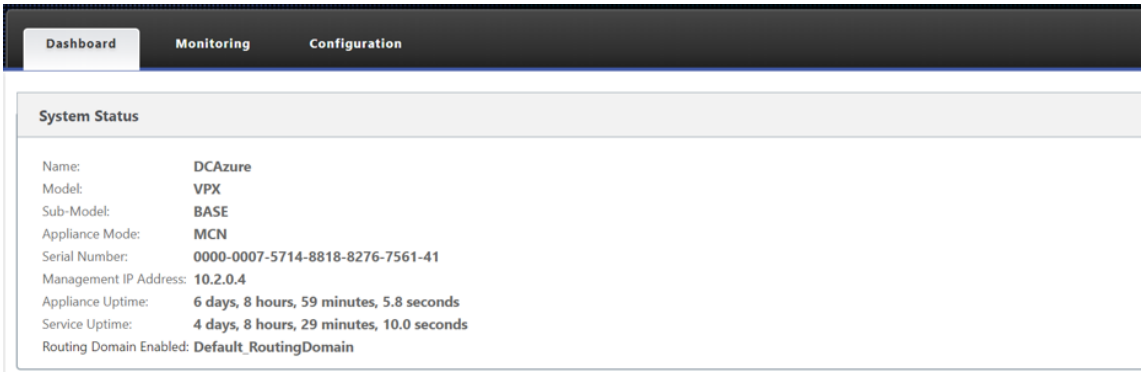
9. Una vez aprovisionado el sitio, inicie sesión en SD-WAN Orchestrator para configurarlo. Como se menciona en los requisitos previos, debe tener derecho a SD-WAN Orchestrator para configurar el sitio. Si aún no lo tiene, consulte Incorporación de Citrix SD-WAN Orchestrator.
10. Si ya tiene una red SD-WAN, proceda a crear la configuración para el sitio que aprovisionó en Azure. De lo contrario, debe crear un MCN. Para obtener más información, consulte Configuración de red.
11. Una vez que tenga acceso a SD-WAN Orchestrator y ya haya configurado un MCN, inicie sesión en SD-WAN orquestrator y haga clic en el **sitio +Nuevo** para comenzar a configurar el dispositivo SD-WAN VPX (que ha aprovisionado en Azure).



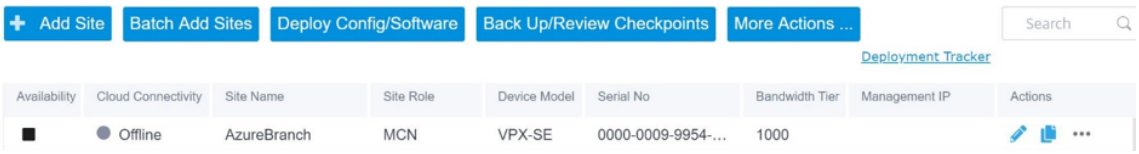
12. Proporcione un nombre de sitio único e introduzca la dirección en función de la región en la que está Provisioning la imagen. Para configurar la instancia en Azure, consulte Configuración básica.

> **Nota**
>
> Para obtener el número de serie de la instancia en Azure, inicie sesión en la instancia a través de la IP de administración pública. Puede ver el número de serie en la pantalla del tablero. Si está configurando instancias en HA, entonces ambos números de serie deben capturarse. Además, mientras configura la instancia, asegúrese de que las interfaces se **eligen como de confianza**.

13. Para obtener las direcciones IP asociadas a las interfaces LAN y WAN en Azure. Desplácese hasta **Azure Portal > Grupos de recursos > Grupo** de recursos donde está **aprovisionada la SD-WAN > VM SD-WAN > Redes**.



14. Una vez que haya terminado con la configuración de la instancia. Haga clic en **Implementar config/Software** navegando a **Configuración > Inicio de configuración de red**.

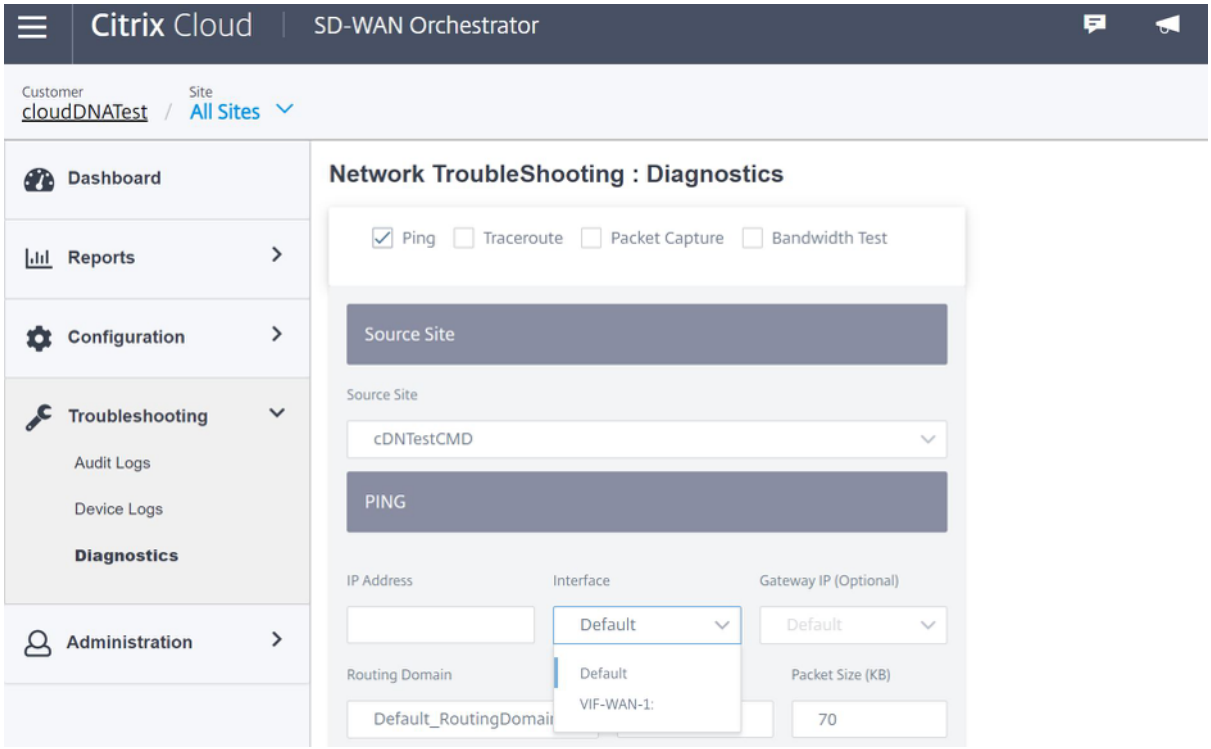


15. Si no hay problemas y la configuración es precisa, debe tener las rutas virtuales entre la instancia de Azure y su MCN una vez ejecutada la implementación de configuración.

Configuración de Citrix Virtual Apps and Desktops

Como se destaca en la sección Implementación y configuración, el AD/DNS está presente en la ubicación local que actúa como DC y en una implementación con SD-WAN que se presenta detrás de la SD-WAN que se encuentra en la red LAN. Es la IP de su AD/DNS que necesita configurar aquí. En caso de que utilice Azure Active Directory servicio/DNS, configure **168.63.129.16** como la IP DNS.

Si está utilizando un AD/DNS.Compruebe si puede hacer ping a la IP de su DNS desde su dispositivo SD-WAN. Para ello, vaya a **Solución de problemas > Diagnósticos**. Marque la casilla **Ping** e inicie un ping desde la interfaz LAN o interfaz predeterminada del dispositivo SD-WAN a la IP de su AD/DNS.



Si el ping tiene éxito, significa que su AD/DNS se puede alcanzar correctamente, si no significa que hay un problema de redirección en su red que está impidiendo la accesibilidad a su AD/DNS. Si es posible, intente alojar su dispositivo AD y SD-WAN en el mismo segmento LAN.

En caso de que todavía haya un problema, póngase en contacto con el administrador de su red. Sin completar este paso correctamente, el paso de creación del catálogo no se realizará correctamente y recibirá un mensaje de error como **IP DNS global no configurado**.

> **Nota**
>
> Asegúrese de que el DNS es capaz de resolver IP internas y externas.

Servicio de ubicación de red

Con el servicio **Ubicación de red** de Citrix Cloud, puede optimizar el tráfico interno hacia las aplicaciones y escritorios que pone a disposición de los espacios de trabajo de los suscriptores para agilizar las sesiones HDX. Los usuarios de redes internas y externas tienen que conectarse a los VDA a través de una Gateway externa. Aunque esto sea lo normal para usuarios externos, los usuarios internos tienen conexiones más lentas a recursos virtuales. El servicio **Ubicación de red** permite a los usuarios internos omitir la puerta de enlace y conectarse directamente a los VDA, lo que reduce la latencia del tráfico de red interno.

Configuración

Para configurar el servicio **Ubicación de red**, utilice uno de los métodos siguientes:

- **Citrix SD-WAN Orchestrator**: Para obtener información detallada sobre la configuración de NLS mediante Citrix SD-WAN Orchestrator, consulte Servicio de ubicación de red.
- **Módulo PowerShell del servicio de ubicación de red que proporciona Citrix**: Para obtener información detallada sobre la configuración de NLS mediante el módulo PowerShell, consulte Módulo y configuración de PowerShell.

Las ubicaciones de red comparten los rangos de IP públicos de las redes desde las que se conectan los usuarios internos. Cuando los suscriptores inician sesiones de Virtual Apps and Desktops desde su Workspace, Citrix Cloud detecta si los suscriptores son internos o externos a la red de la empresa en función de la dirección IP pública de la red desde la que se conectan.

Si un suscriptor se conecta desde la red interna, Citrix Cloud redirige la conexión directamente al VDA sin pasar por Citrix Gateway. Si un suscriptor se conecta externamente, Citrix Cloud redirige el suscriptor a Citrix Gateway como se esperaba y, a continuación, lo reenvía al VDA de la red interna.

> **NOTA**
>
> La IP pública que debe configurarse en el servicio de ubicación de red debe ser la IP pública asignada a los vínculos WAN.

Sistema de nombres de dominio

August 26, 2022

El Sistema de nombres de dominio (DNS) traduce nombres de dominio legibles por humanos a direcciones IP legibles por máquina, y viceversa. Citrix SD-WAN proporciona las siguientes funciones DNS:

- Proxy DNS
- Reenvío transparente DNS

Puede configurar un proxy DNS o un reenvío transparente de DNS a través de Citrix SD-WAN Orchestrator Service con los siguientes tipos de servicio DNS:

- **Servicio DNS estático**: le permite configurar las direcciones IP del servidor DNS IPv4 estáticas. Puede crear Internal, ISP, google o cualquier otro servicio DNS de código abierto. El servicio DNS estático se puede configurar a nivel global y de sitio.

- **Servicio DNS dinámico**: permite configurar las direcciones IP del servidor DNS IPv4 dinámicas. El servicio DNS dinámico solo se puede configurar a nivel de sitio. Solo se permite un servicio DNS dinámico por sitio.
- **Servicio DNS Staticv6**: le permite configurar las direcciones IP del servidor DNS IPv6 estáticas. Puede crear Internal, ISP, google o cualquier otro servicio DNS de código abierto. El servicio DNS Staticv6 se puede configurar a nivel global y de sitio.
- **Servicio DNS DynamicV6**: permite configurar las direcciones IP del servidor DNS IPv6 dinámicas. El servicio DNS DynamicV6 solo se puede configurar a nivel de sitio. Solo se permite un servicio DNS dinámico por sitio.

Proxy DNS

Puede configurar un proxy con varios reenviadores que ayuden a dirigir las solicitudes DNS en función de los nombres de dominio de la aplicación. El reenvío DNS funciona para las solicitudes que se reciben a través de conexiones UDP. Para obtener información sobre cómo configurar el proxy DNS a través de SD-WAN Orchestrator Service, consulte Proxy DNS.

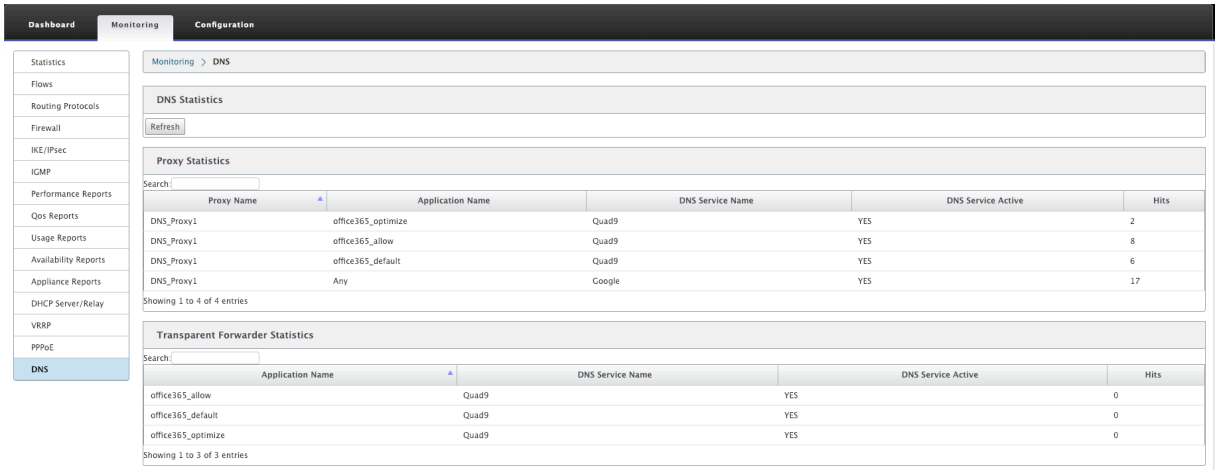
Reenviador transparente DNS

Citrix SD-WAN se puede configurar como un reenviador DNS transparente. En este modo, SD-WAN puede interceptar solicitudes DNS que no están destinadas a su dirección IP y reenviarlas al servicio DNS especificado. Solo se interceptan las solicitudes DNS procedentes del servicio local en interfaces de confianza. Si las solicitudes DNS coinciden con cualquier aplicación de la lista de reenviadores DNS, se reenvía al servicio DNS configurado. El reenvío DNS solo se admite para solicitudes procedentes de conexiones UDP. Para obtener información sobre cómo configurar el reenviador transparente de DNS a través de SD-WAN Orchestrator Service, consulte Reenviadores transparentes de DNS.

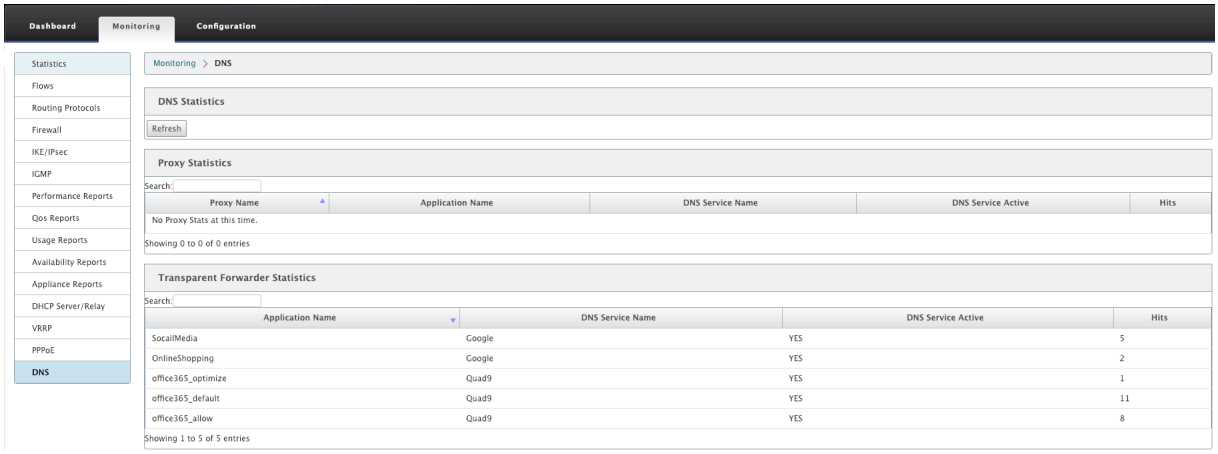
Supervisión

Para ver las estadísticas del proxy y las estadísticas del reenviador transparente, vaya a **Supervisión > DNS**.
Puede ver el nombre de la aplicación, el nombre del servicio DNS, el estado del servicio DNS y el número de visitas al servicio DNS.

Estadísticas de proxy



Estadísticas del reenviador transparente



DHCP

November 16, 2022

Citrix SD-WAN presenta la capacidad de usar dispositivos Standard Edition como servidores DHCP o agentes de retransmisión DHCP. La función del servidor DHCP permite a los dispositivos de la misma red que la interfaz LAN/WAN del dispositivo SD-WAN obtener su configuración IP del dispositivo SD-WAN. La función de retransmisión DHCP permite a los dispositivos SD-WAN reenviar paquetes DHCP entre el cliente DHCP y el servidor.

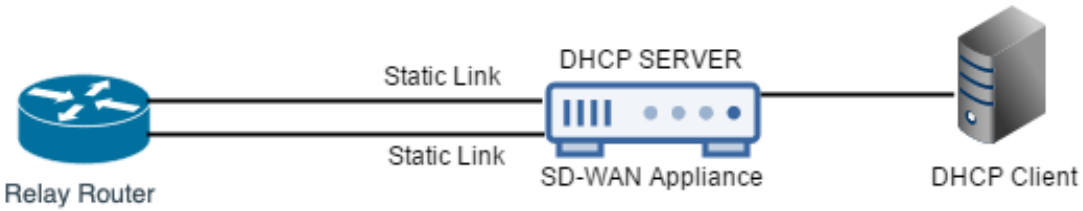
Las siguientes son las ventajas de utilizar el servidor DHCP y las funciones de retransmisión DHCP:

- Reduzca la cantidad de equipos en las instalaciones del cliente.
- Reemplazar el router en el sitio del cliente (implementación sencilla de servicios de router perimetral).

- Simplifique la red de sitios del cliente.
- Configuración del router sin comandos CLI.
- Reduzca la configuración manual en sitios de clientes sencillos.

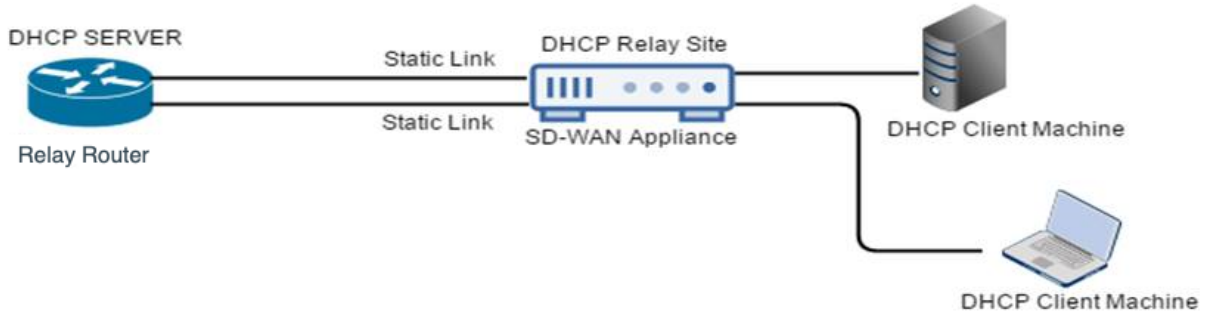
Servidor DHCP

Los dispositivos Citrix SD-WAN se pueden configurar como servidor DHCP. Puede asignar y administrar direcciones IP de grupos de direcciones especificados dentro de la red a clientes DHCP. El servidor DHCP se puede configurar para asignar más parámetros, como la dirección IP del servidor del Sistema de nombres de dominio (DNS) y el enrutador predeterminado. El servidor DHCP acepta solicitudes de asignación de direcciones y renovaciones. El servidor DHCP también acepta transmisiones de segmentos LAN conectados localmente o de solicitudes DHCP reenviadas por otros agentes de retransmisión DHCP dentro de la red.



relé DHCP

Un agente de retransmisión DHCP es un host o enrutador que reenvía paquetes DHCP entre clientes y servidores. Los administradores de red pueden utilizar el servicio de retransmisión DHCP de los dispositivos SD-WAN para retransmitir solicitudes y respuestas entre clientes DHCP locales y un servidor DHCP remoto. Permite a los hosts locales adquirir direcciones IP dinámicas del servidor DHCP remoto. El agente de retransmisión recibe mensajes DHCP y genera un nuevo mensaje DHCP para enviarlo en otra interfaz.



Aprendizaje de direcciones IP de enlace WAN a través del cliente DHCP

Los dispositivos Citrix SD-WAN admiten el aprendizaje de direcciones IP de enlace WAN a través de clientes DHCP. Esta funcionalidad reduce la cantidad de configuración manual necesaria para implementar dispositivos SD-WAN y reduce los costes de ISP al eliminar la necesidad de comprar direcciones IP estáticas. Los dispositivos SD-WAN pueden obtener direcciones IP dinámicas para los vínculos WAN en interfaces que no son de confianza. Esto elimina la necesidad de un enrutador WAN intermedio para realizar esta función.

> **Nota**
>
> - El cliente DHCP solo se puede configurar para interfaces no conectadas en puente que no sean de confianza configuradas como nodos de cliente.
> - El cliente DHCP y el puerto de datos se pueden habilitar en MCN/RCN solo si la dirección IP pública está configurada.
> - No se admite la implementación de redirección basado en directivas (PBR) en el sitio con la configuración del cliente DHCP.
> - Los eventos DHCP se registran únicamente desde la perspectiva del cliente y no se generan registros del servidor DHCP.

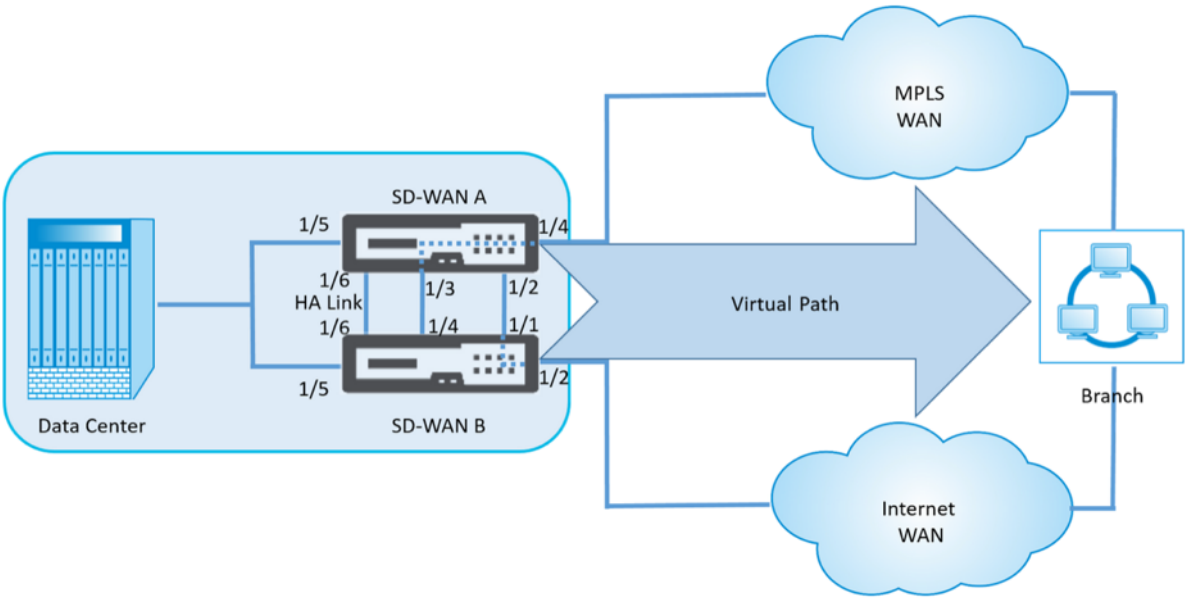
A partir de la versión 11.5 de Citrix SD-WAN, puede configurar DHCP para una interfaz virtual que no sea de confianza en modo de error de bloqueo a través de Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Aprendizaje de direcciones IP de enlaces WAN a través del cliente DHCP.

Compatibilidad con DHCP en el puerto Fail-to-Wire

Anteriormente, el cliente DHCP solo era compatible con el puerto Fail-to-Block. Con la versión 11.2.0, la capacidad del cliente DHCP se amplía en el puerto de error a cable para el sitio de sucursal con implementaciones seriales de alta disponibilidad (HA). Esta mejora:

- Permite la configuración del cliente DHCP en el grupo de interfaces que no son de confianza que tiene implementaciones de pares de puentes de error a cable y de alta disponibilidad en serie.
- Permite seleccionar las interfaces DHCP como parte de los **enlaces WAN de la Intranet privada**.

Ahora se admite el cliente DHCP en el vínculo de intranet privada.



> **Nota**: No se debe conectar
>
> una interfaz LAN al par de conmutación por error, ya que es posible que los paquetes formen un puente entre las interfaces.

Supervisión de enlaces WAN del cliente DHCP

La configuración de dirección IP virtual del tiempo de ejecución, máscara de subred y puerta de enlace se registran y archivan en un archivo de registro denominado *SDWANVW_ip_learned.log.* Los eventos se generan cuando se aprenden, liberan o caducan las IP virtuales dinámicas y cuando hay un problema de comunicación con la puerta de enlace o el servidor DHCP que se ha aprendido. O cuando se detectan direcciones IP duplicadas en el archivo de registro archivado. Si se detectan IP duplicadas en un sitio, las direcciones IP virtuales dinámicas se liberan y se renuevan hasta que todas las interfaces virtuales del sitio obtengan direcciones IP virtuales únicas.

Para supervisar los vínculos WAN de clientes DHCP:

1. En la página **Habilitar/Desactivar/Purgar flujos** del dispositivo SD-WAN, la tabla Vínculos WAN del cliente DHCP proporciona el estado de las IP aprendidas.
2. Puede solicitar la renovación de la IP, que actualiza el tiempo de concesión. También puede elegir **Release Renew**, que emite una nueva dirección IP o la misma dirección IP con una nueva concesión.

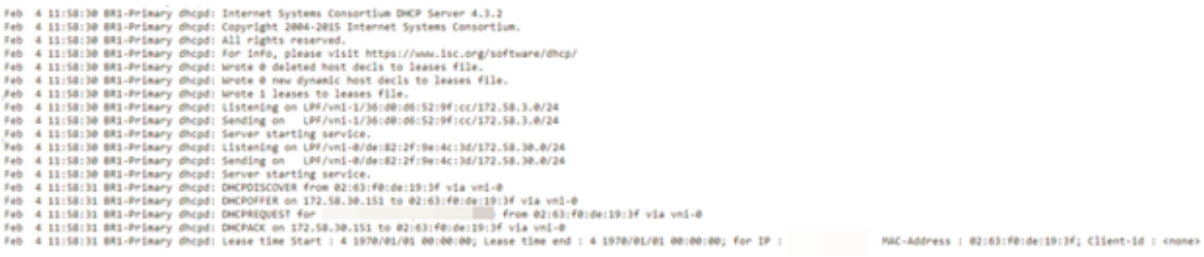
DHCP Client WAN Links

Ethernet Interface	Virtual Interface	WAN Link	IP Address / Prefix	Gateway IP Address	Lease Duration Seconds	Remaining Seconds	Expiration Date	Action	
X2	VLAN349	SFWL3-Inter	10.30.30.55/24	10.30.30.2	1800	1640	9:13 on 1/8/2016	Renew	Submit
X2	VLAN350	SFWL4-Inter	10.20.20.53/24	10.20.20.2	86400	71035	4:29 on 1/9/2016	Renew	Submit

Registros DHCP

Citrix SD-WAN le permite generar registros de servidor DHCP para direcciones IP. Siempre que se asignan direcciones IP a los puntos finales, se generan los registros. Los registros contienen detalles como la marca de tiempo de la asignación de la dirección IP y la duración del arrendamiento, la dirección MAC, el ID del cliente, etc. El ID de cliente **none** indica que no está presente en la solicitud DHCP.

Para generar y ver los registros de DHCP, vaya a **Configuración** > **Registros/Supervisión**. Seleccione la opción **SDWAN_dhcp.log** de la lista desplegable y haga clic en **Ver registro**.



> **Nota**
>
> Estos registros se generan solo cuando Citrix SD-WAN actúa como servidor DHCP.

Personalización dinámica de archivos PAC

August 26, 2022

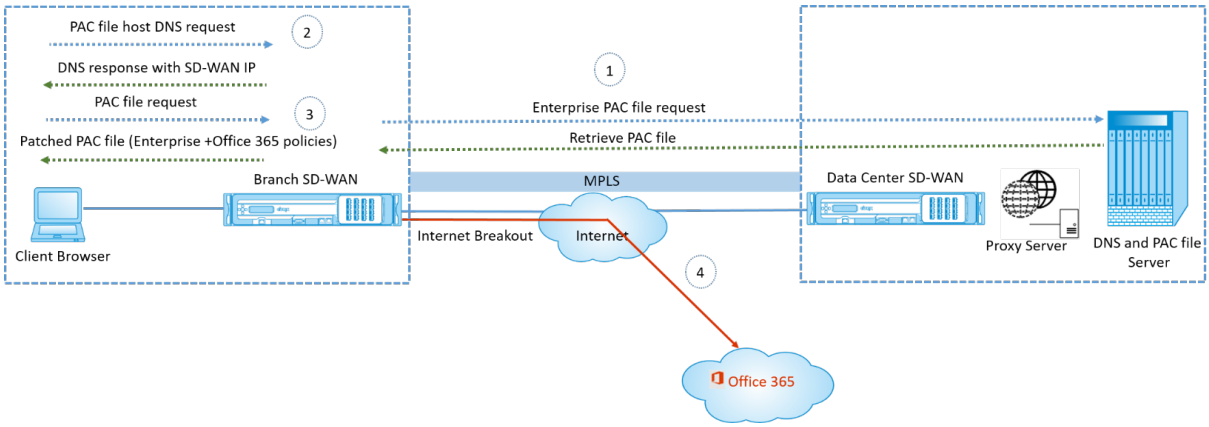
Con el aumento de la adopción empresarial de aplicaciones SaaS de misión crítica y de personal distribuido, resulta muy importante reducir la latencia y la congestión. La latencia y la congestión son inherentes a los métodos tradicionales de backhauling del tráfico a través del centro de datos. Citrix SD-WAN permite una salida directa a Internet de aplicaciones SaaS como Office 365. Para obtener más información, consulte Optimización de Office 365.

Si hay proxies web explícitos configurados en la implementación empresarial, todo el tráfico se dirige al proxy web, lo que dificulta la clasificación y la ruptura directa de Internet. La solución consiste en excluir el tráfico de aplicaciones SaaS de ser proxy mediante la personalización del archivo PAC (Proxy Auto-Config) empresarial.

Citrix SD-WAN 11.0 permite la omisión de proxy y la ruptura local de Internet para el tráfico de aplicaciones de Office 365 generando y sirviendo dinámicamente un archivo PAC personalizado. El archivo PAC es una función JavaScript que define si las solicitudes del explorador web van directamente al destino o a un servidor proxy web.

Cómo funciona la personalización de archivos PAC

Idealmente, el archivo PAC del host de red empresarial en el servidor web interno, esta configuración de proxy se distribuye mediante la directiva de grupo. El explorador cliente solicita archivos PAC del servidor web empresarial. El dispositivo Citrix SD-WAN sirve los archivos PAC personalizados para los sitios en los que está habilitado el breakout de Office 365.



1. Citrix SD-WAN solicita y recupera periódicamente la última copia del archivo PAC empresarial del servidor web empresarial. El dispositivo Citrix SD-WAN parchea las URL de office 365 en el archivo PAC empresarial. Se espera que el archivo PAC empresarial tenga un marcador de posición (etiqueta específica de SD-WAN) en el que las URL de Office 365 se parchean sin problemas.
2. El explorador del cliente genera una solicitud DNS para el host de archivos PAC empresarial. Citrix SD-WAN intercepta la solicitud del FQDN del archivo de configuración del proxy y responde con el VIP de Citrix SD-WAN.
3. El explorador del cliente solicita el archivo PAC. El dispositivo Citrix SD-WAN sirve el archivo PAC parcheado localmente. El archivo PAC incluye la configuración del proxy empresarial y las directivas de exclusión de URL de Office 365.
4. Al recibir una solicitud para la aplicación Office 365, el dispositivo Citrix SD-WAN realiza una ruptura directa de Internet.

Requisitos previos

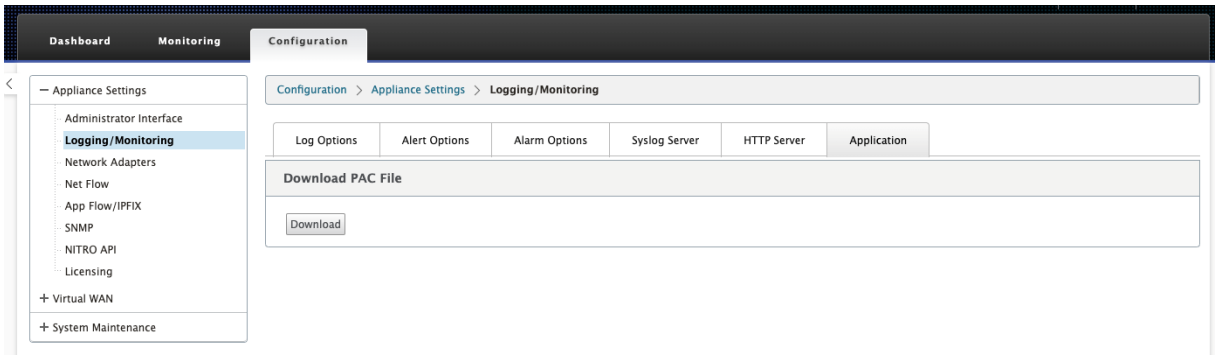
1. Las empresas deben tener un archivo PAC alojado.
2. El archivo PAC debe tener un marcador de posición *SDWAN_TAG* o una aparición de la función *findproxyforurl* para la aplicación de parches a las URL de Office 365.
3. La URL del archivo PAC debe estar basada en el dominio y no en IP.
4. El archivo PAC solo se sirve a través de los VIP de identidad de confianza.
5. El dispositivo Citrix SD-WAN debería poder descargar el archivo PAC empresarial a través de su interfaz de administración.

Configurar la personalización de archivos PAC

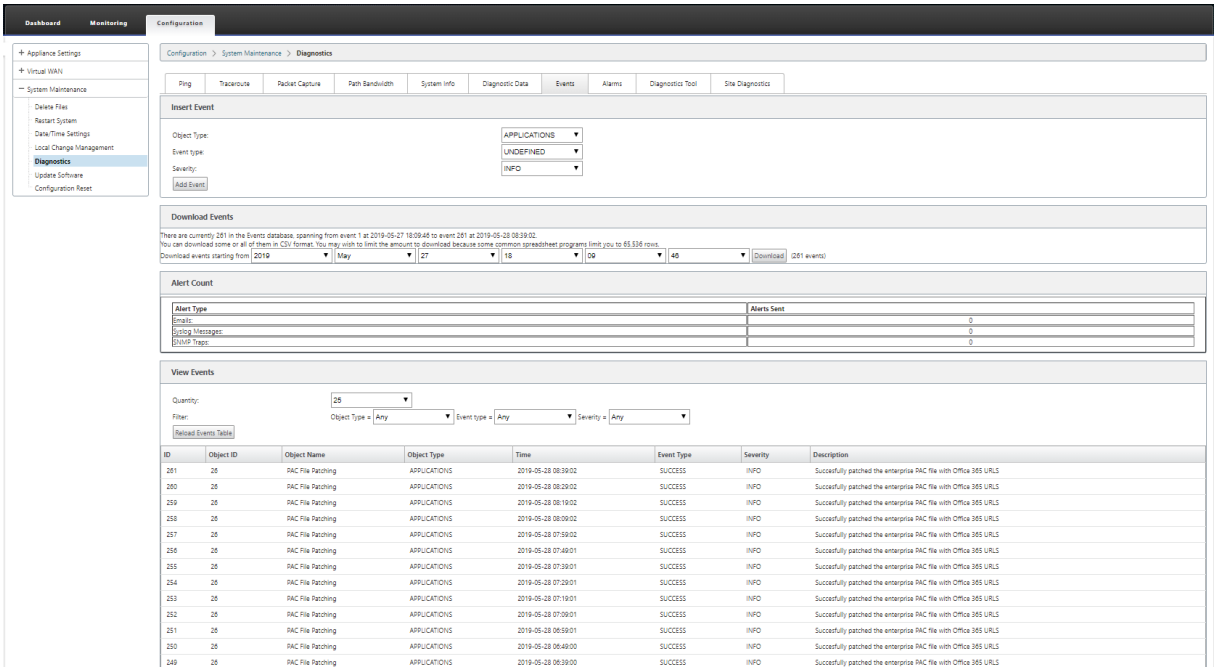
Puede habilitar la personalización de archivos PAC mediante Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Configuración automática de proxy.

Solución de problemas

Puede descargar el archivo PAC personalizado del dispositivo Citrix SD-WAN para solucionar problemas. Vaya a **Configuración** > **Configuración del dispositivo** > **Registrar/Supervisión** > **Aplicación y haga clic en Descargar**.



También puede ver el estado de aplicación de parches del archivo PAC en la sección **Eventos**, vaya a **Configuración** > **Mantenimiento del sistema** > **Diagnóstico** y haga clic en la ficha **Eventos**.



Limitaciones

- No se admiten las solicitudes del servidor de archivos HTTPS PAC.
- No se admiten varios archivos PAC de una red, incluidos los archivos PAC para dominios de redirección o zonas de seguridad.
- No se admite la generación de archivos PAC en Citrix SD-WAN desde cero.
- WPAD a través de DHCP no es compatible.

Túnel GRE

August 26, 2022

La función Túnel GRE le permite configurar dispositivos Citrix SD-WAN para terminar túneles GRE en la LAN o Intranet. Para configurar un túnel GRE mediante SD-WAN Orchestrator Service, consulte Servicio GRE.

Administración de copias de seguridad y en banda

August 26, 2022

Administración en banda

Citrix SD-WAN le permite administrar el dispositivo SD-WAN de dos maneras: administración fuera de banda y administración dentro de banda. La administración fuera de banda le permite crear una dirección IP de administración mediante un puerto reservado para la administración, que solo transporta tráfico de administración. La administración en banda le permite utilizar los puertos de datos SD-WAN para la administración. Lleva tanto tráfico de datos como de administración, sin tener que configurar una ruta de administración de adiciones.

La administración en banda permite que las direcciones IP virtuales se conecten a servicios de administración como la interfaz de usuario web y SSH. Puede habilitar la administración en banda en varias interfaces de confianza habilitadas para su uso en servicios IP. Puede acceder a la interfaz de usuario web y SSH mediante la IP de administración y las IP virtuales en banda.

A partir de la versión 11.4.2 de Citrix SD-WAN, es obligatorio configurar la administración dentro de banda para establecer la conectividad con Citrix SD-WAN Orchestrator Service a través de un puerto de administración dentro de banda. De lo contrario, el dispositivo pierde la conectividad con Citrix SD-WAN Orchestrator Service cuando el puerto de administración no está conectado y la dirección IP en banda tampoco está configurada.

> **Nota**
>
> - El servicio Citrix SD-WAN Orchestrator no permite configurar el **tipo de servicio** como **Cualquiera** para las directivas NAT de destino.
> - Evite inhabilitar el servicio cuando la única conectividad de administración es alta disponibilidad en banda.
>
> Puede bloquearse del dispositivo si inhabilita el servicio.

A partir de Citrix SD-WAN 11.5, puede habilitar la administración dentro de banda en una IP virtual solo a través de Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Administración dentro de banda.

A partir de la versión 11.3.1 de Citrix SD-WAN, la administración en banda admite pares de dispositivos de alta disponibilidad. La comunicación entre los dispositivos primarios y secundarios se realiza a través de las interfaces virtuales que utilizan NAT.

Los siguientes puertos permiten la comunicación con los servicios de administración en los dispositivos de alta disponibilidad:

- HTTPS
  - 443 - Se conecta a la HA activa
  - 444 - Redirige al primario de alta disponibilidad
  - 445 - Redirige a la secundaria de HA

- SSH
  - 22 - Se conecta a la HA activa
  - 23 - Redirige al primario de alta disponibilidad
  - 24 - Redirige a la secundaria de alta disponibilidad
- SNMP
  - 161 - Se conecta a la HA activa
  - 162 - Redirige al primario de HA
  - 163 - Redirige a la secundaria de HA

Utilice directivas NAT de destino para crear direcciones IP que permitan la conectividad a HA en banda sin necesidad de introducir un puerto.

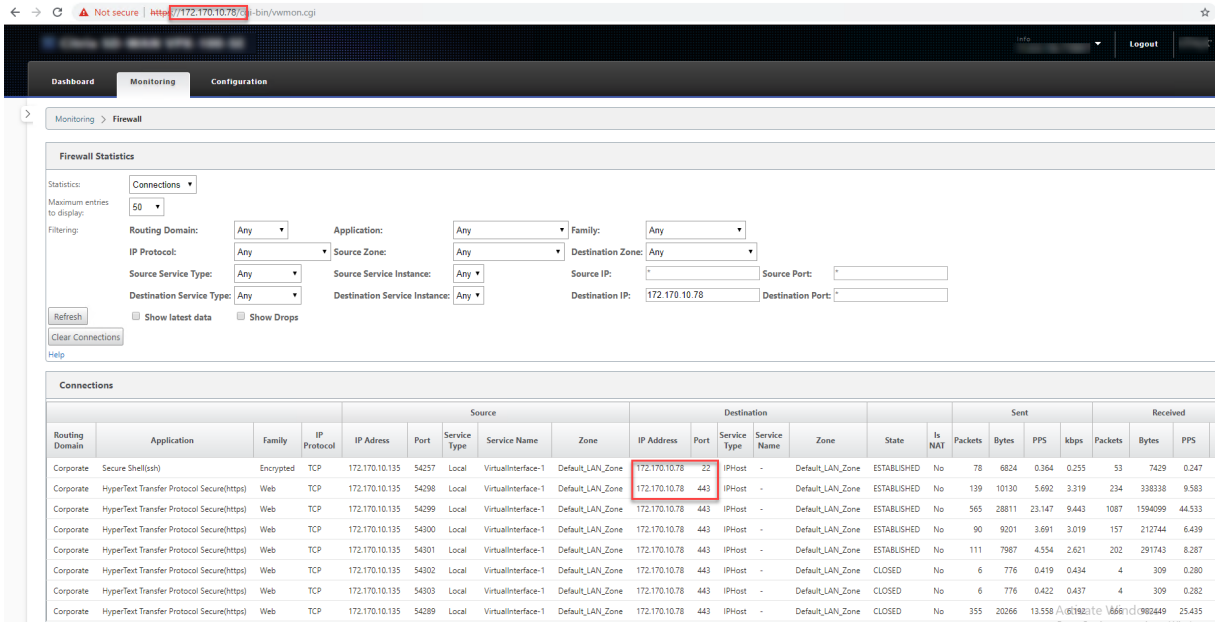
Por ejemplo, se utilizan las siguientes direcciones IP en banda para acceder a los dispositivos:

- Dispositivo activo - 1.0.1.2
- Dispositivo primario - 1.0.1.10
- Dispositivo secundario - 1.0.1.11

Supervisión de la administración en banda

En el ejemplo anterior, hemos habilitado la administración en banda en la IP virtual 172.170.10.78. Puede utilizar esta IP para acceder a la interfaz de usuario web y a SSH.

En la interfaz de usuario web, vaya a **Supervisión** > **Firewall**. Puede ver SSH y la interfaz de usuario web a la que se accede mediante la IP virtual en el puerto 22 y 443, respectivamente, en la columna **Dirección IP de destino**.



Aprovisionamiento en banda

La necesidad de implementar dispositivos SD-WAN en entornos más sencillos como el hogar o las sucursales pequeñas ha aumentado significativamente. Configurar un acceso de administración independiente para implementaciones más sencillas es una sobrecarga adicional. La implementación sin táctiles junto con la función de administración en banda permite el aprovisionamiento y la administración de la configuración a través de puertos de datos designados. La implementación sin táctiles ahora se admite en los puertos de datos designados y no es necesario utilizar un puerto de administración independiente para la implementación sin contacto. Citrix SD-WAN también permite conmutar por error el tráfico de administración sin problemas al puerto de administración cuando el puerto de datos se desactiva y viceversa.

Un dispositivo en estado enviado de fábrica, que admite el Provisioning en banda, se puede aprovisionar simplemente conectando el puerto de datos o de administración a Internet. Los dispositivos que admiten el Provisioning en banda tienen puertos específicos para LAN y WAN. El dispositivo en estado de restablecimiento de fábrica tiene una configuración predeterminada que permite establecer una conexión con el servicio de implementación sin contacto. El puerto LAN actúa como servidor DHCP y asigna una IP dinámica al puerto WAN que actúa como cliente DHCP. Los enlaces WAN supervisan el servicio DNS Quad 9 para determinar la conectividad WAN.

> **Nota**
>
> El Provisioning en banda solo se aplica a las plataformas SD-WAN 110 SE y SD-WAN VPX.

Una vez que se obtiene la dirección IP y se establece una conexión con el servicio de implementación sin contacto, los paquetes de configuración se descargan e instalan en el dispositivo.

Nota: Para el aprovisionamiento por día 0 de dispositivos SD-WAN a través de los puertos de datos, la versión del software del dispositivo debe ser SD-WAN 11.1.0 o posterior.

La configuración predeterminada de un dispositivo en estado de restablecimiento de fábrica incluye las siguientes configuraciones:

- Servidor DHCP en puerto LAN
- Cliente DHCP en el puerto WAN
- Configuración de QUAD9 para DNS
- La IP predeterminada de LAN es 192.168.0.1
- Licencia Grace de 35 días.

Una vez aprovisionado el dispositivo, la configuración predeterminada se inhabilita y se reemplaza por la configuración recibida del servicio de implementación sin contacto. Si caduca una licencia de dispositivo o una licencia de gracia, se activa la configuración predeterminada para garantizar que el dispositivo permanezca conectado al servicio de implementación sin contacto y reciba licencias administradas mediante la implementación sin intervención.

Configuración predeterminada/reserva

La configuración de reserva garantiza que el dispositivo permanezca conectado al servicio de implementación sin contacto si hay un error de enlace, una discrepancia de configuración o una discrepancia de software. La configuración de reserva está habilitada de forma predeterminada en los dispositivos que tienen un perfil de configuración predeterminado. También puede modificar la configuración de reserva según la configuración de red LAN existente.

Nota: Después del aprovisionamiento inicial del dispositivo, asegúrese de que la configuración de reserva esté habilitada para la conectividad del servicio de implementación sin contacto.

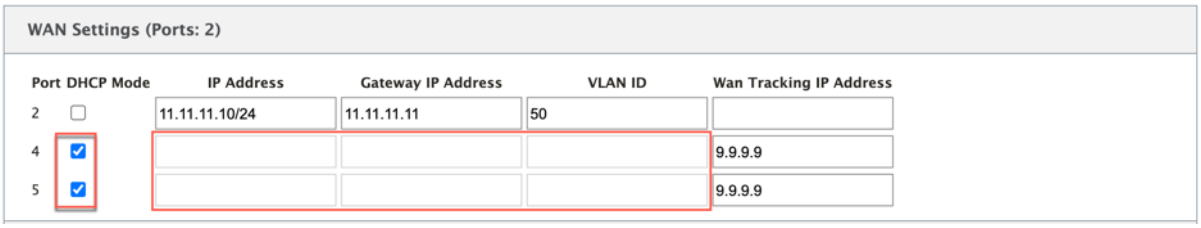
La siguiente tabla proporciona los detalles de los puertos WAN y LAN designados previamente para la configuración de reserva en diferentes plataformas:

Plataforma	Puertos WAN	Puertos LAN
110	1/2	1/1
110-LTE	1/2, LTE-1	1/1
210	1/4, 1/5	1/3
210-LTE	1/4, 1/5, LTE-1	1/3
VPX	2	1
1100	1/4, 1/5, 1/6	1/3 (FTB)

Desde la versión 11.3.1 de Citrix SD-WAN, la configuración del puerto WAN se puede configurar. Los puertos WAN se pueden configurar como vínculos WAN independientes mediante el cliente DHCP y supervisar el servicio DNS Quad9 para determinar la conectividad WAN. Puede configurar IP/IP estáticas WAN para los puertos WAN en ausencia de DHCP para utilizar la administración en banda para el aprovisionamiento inicial.

> **Nota**
>
> Solo puede configurar los puertos Ethernet con las IP estáticas. Las IP estáticas no se pueden configurar con los puertos LTE-1 y LTE-E1. Aunque puede agregar los puertos LTE-1 y LTE-E1 como WAN, los campos de configuración permanecen no modificables.

Cuando se agrega un puerto WAN, se agrega en la sección **Configuración de WAN (Puerto: 2)** con la casilla de verificación **Modo DHCP** activada de forma predeterminada. Si la casilla de verificación **Modo DHCP** está activada, los campos de texto **Dirección IP, Dirección IP de puerta** de enlace y **ID de VLAN** aparecen atenuados. Desmarque la casilla **Modo DHCP**, si quiere configurar la IP estática.



De forma predeterminada, el campo **Dirección IP de seguimiento de WAN** se rellena automáticamente con la 9.9.9.9. Puede cambiar la dirección según sea necesario.

> **Nota**
>
> Si está activando la casilla **Servidores DNS dinámicos**, asegúrese de agregar/configurar al menos un puerto WAN con el **modo DHCP** seleccionado.

Administración configurable o puerto de datos

La administración en banda permite que los puertos de datos transporten tanto tráfico de datos como de administración, eliminando la necesidad de un puerto de administración dedicado. Esto deja el puerto de administración sin usar en los dispositivos de gama baja, que ya tienen baja densidad de puertos. Citrix SD-WAN permite configurar el puerto de administración para que funcione como puerto de datos o como puerto de administración.

> **Nota**
>
> Puede convertir el puerto de administración en puerto de datos solo en las siguientes plataformas:
>
> - Citrix SD-WAN 110 SE/LTE
> - Citrix SD-WAN 210 SE/LTE

Solo puede configurar un puerto de administración cuando la administración en banda está habilitada en otras interfaces de confianza del dispositivo.

Red de administración de backup

Puede configurar una dirección IP virtual como una red de administración de respaldo. Se utiliza como dirección IP de administración si el puerto de administración no está configurado con una Gateway predeterminada.

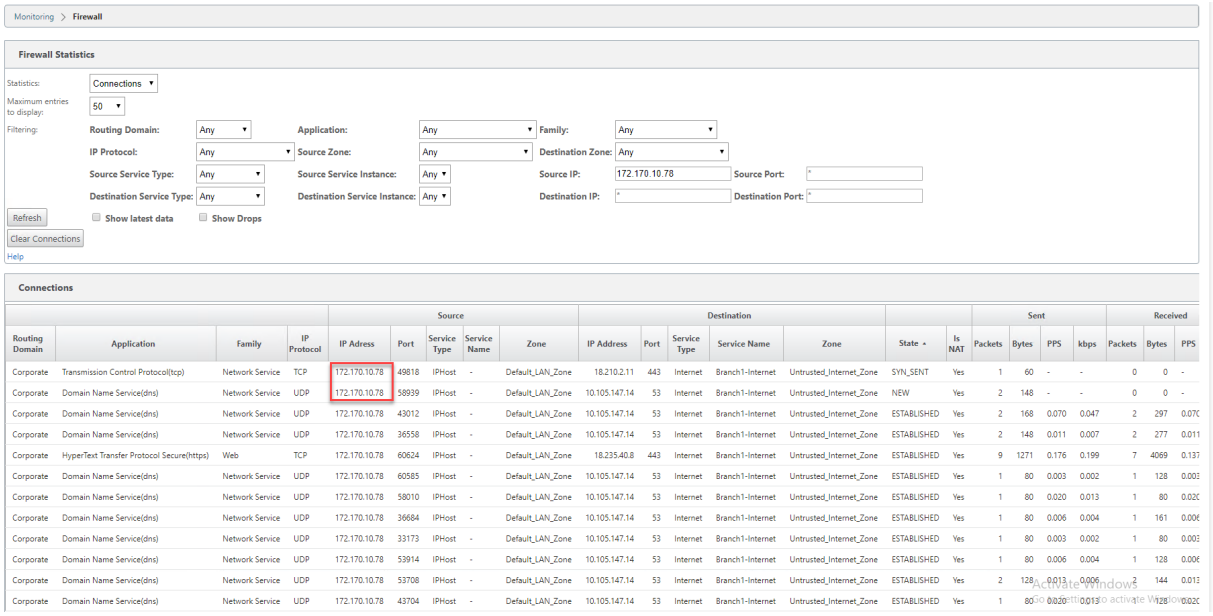
> **Nota**
>
> Si un sitio tiene un servicio de Internet configurado con un único dominio de redirección, se selecciona una interfaz de confianza con identidad habilitada como red de administración de copias

> de seguridad de forma predeterminada.

Supervisión de la administración de copias de seguridad

En el ejemplo anterior, hemos seleccionado 172.170.10.78 IP virtual como red de administración de backup. Si la dirección IP de administración no está configurada con una puerta de enlace predeterminada, puede usar esta IP para acceder a la IU web y a SSH.

En la interfaz de usuario web, vaya a **Supervisión** > **Firewall**. Puede ver esta dirección IP virtual como la dirección IP de origen para el acceso SSH y la interfaz de usuario web.



Acceso a Internet

November 16, 2022

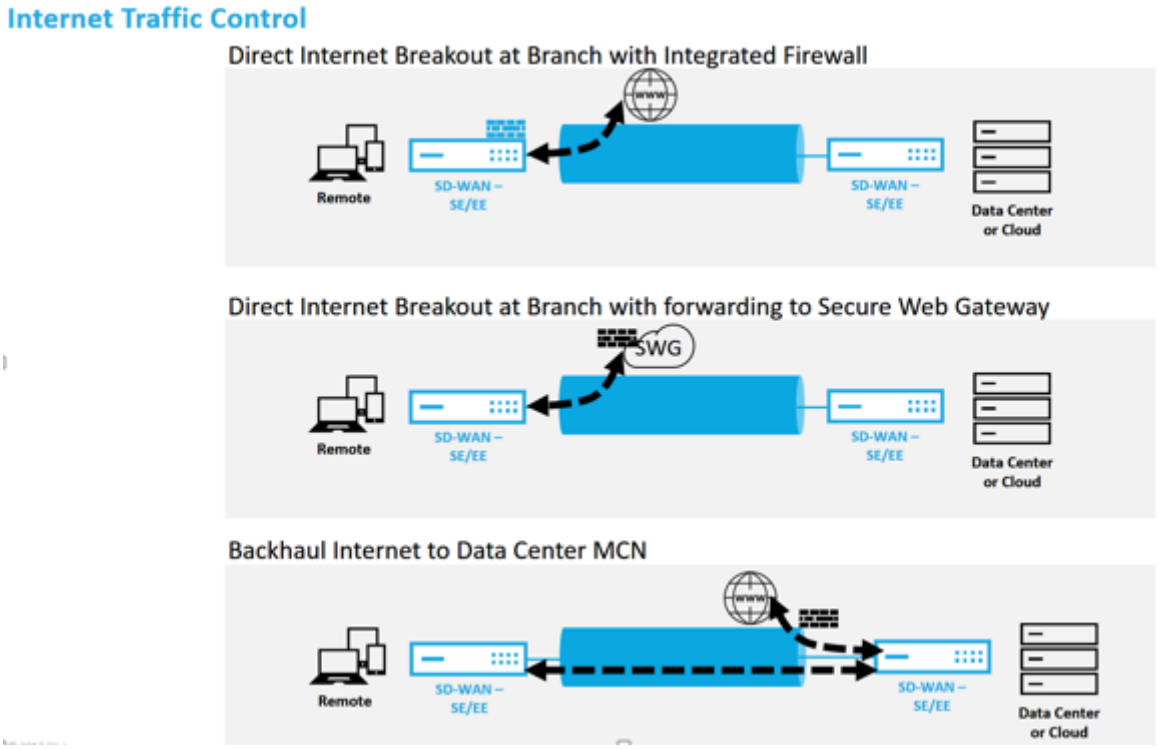
El Servicio Internet se utiliza para el tráfico entre un sitio de usuario final y sitios en Internet pública. El tráfico del servicio Internet no está encapsulado por SD-WAN y no tiene las mismas capacidades que el tráfico que se entrega a través del Servicio de ruta virtual. Sin embargo, es importante clasificar y tener en cuenta este tráfico en la SD-WAN. El tráfico identificado como servicio de Internet permite agregar la capacidad de SD-WAN para administrar activamente el ancho de banda del enlace WAN limitando la velocidad del tráfico de Internet en relación con el tráfico entregado a través de la ruta virtual y el tráfico de la intranet según la configuración establecida por el administrador. Además de las capacidades de aprovisionamiento de ancho de banda, SD-WAN tiene la capacidad adicional para equilibrar la carga del tráfico entregado a través del Servicio Internet mediante varios vínculos WAN

de Internet, u opcionalmente, utilizando los vínculos WAN de Internet en una configuración primaria o secundaria.

El control del tráfico de Internet mediante el servicio Internet en dispositivos SD-WAN se puede configurar en los siguientes modos de implementación:

- Breakout directo de Internet en Branch con Firewall integrado
- Reenvío directo de Internet en sucursales a Secure Web Gateway
- Backhaul de Internet al centro de datos MCN

Para obtener información sobre cómo configurar un servicio de Internet a través de Citrix SD-WAN Orchestrator Service, consulte Servicio de Internet.



Breakout directo de Internet en Branch con Firewall integrado

El servicio Internet se puede utilizar en los distintos modos de implementación admitidos por Citrix SD-WAN.

- Modo de implementación en línea (superposición SD-WAN)

Citrix SD-WAN se puede implementar como solución superpuesta en cualquier red. Como solución de superposición, la SD-WAN generalmente se implementa detrás de routers perimetrales o firewalls existentes. Si la SD-WAN se implementa detrás de un firewall de red, la interfaz se puede configurar

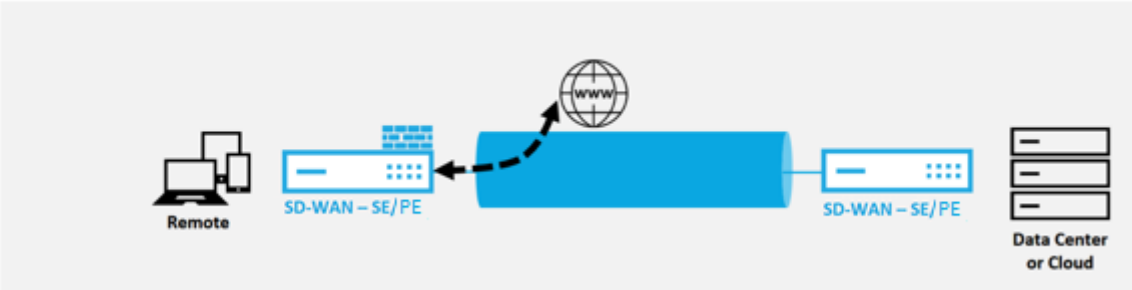
como de confianza y el tráfico de Internet se puede entregar al firewall como puerta de enlace de Internet.

- Modo Edge o Gateway

Citrix SD-WAN se puede implementar como dispositivo perimetral, reemplazando los dispositivos de firewall o enrutador perimetral existentes. La función de firewall integrado permite que la SD-WAN proteja la red de la conectividad directa a Internet. En este modo, la interfaz conectada al vínculo público de Internet se configura como no confiable, lo que obliga a habilitar el cifrado, y las funciones de firewall y NAT dinámico están habilitadas para proteger la red.

Para obtener información sobre cómo configurar un servicio de Internet a través de Citrix SD-WAN Orchestrator Service, consulte Servicio de Internet.

Direct Internet Breakout at Branch with Integrated Firewall



Acceso directo a Internet con Secure Web Gateway

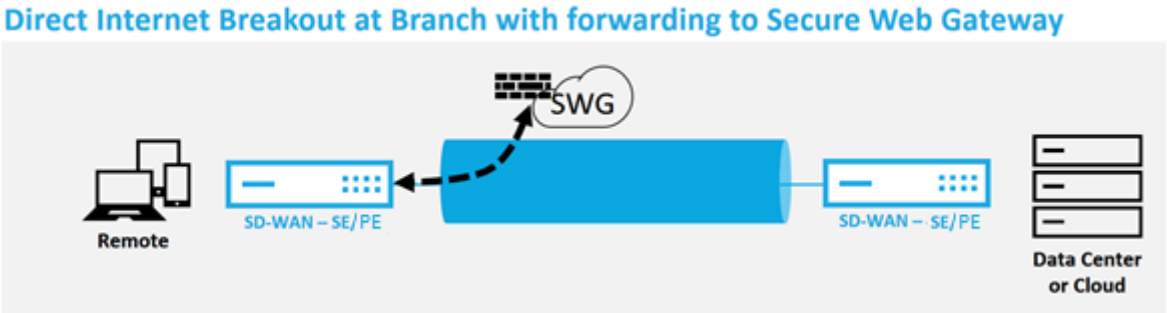
Para proteger el tráfico y aplicar directivas, las empresas suelen utilizar vínculos MPLS para realizar backhaul de tráfico de sucursales al centro de datos corporativo. El centro de datos aplica directivas de seguridad, filtra el tráfico a través de dispositivos de seguridad para detectar malware y enruta el tráfico a través de un ISP. Este tipo de backhauling a través de enlaces MPLS privados es costoso. También da como resultado una latencia significativa, lo que crea una mala experiencia de usuario en el sitio de la sucursal. También existe el riesgo de que los usuarios eludieran los controles de seguridad.

Una alternativa al backhauling es agregar dispositivos de seguridad en la sucursal. Sin embargo, el coste y la complejidad aumentan a medida que instala varios dispositivos para mantener directivas coherentes en todos los sitios. Lo más importante es que si tiene muchas sucursales, la administración de costes se vuelve poco práctica.

Una alternativa es aplicar la seguridad sin agregar costes, complejidad ni latencia sería redirigir todo el tráfico de Internet de las sucursales mediante Citrix SD-WAN a Secure Web Gateway Service. Un Secure Web Gateway Service de terceros permite que todas las redes conectadas utilicen la creación de directivas de seguridad granulares y centralizadas. Las directivas se aplican de forma coherente tanto si el usuario se encuentra en el centro de datos como en un sitio de sucursal. Dado que las soluciones

de Secure Web Gateway se basan en la nube, no es necesario agregar dispositivos de seguridad más costosos a la red.

Para obtener información sobre cómo configurar un servicio de Internet a través de Citrix SD-WAN Orchestrator Service, consulte Servicio de Internet.



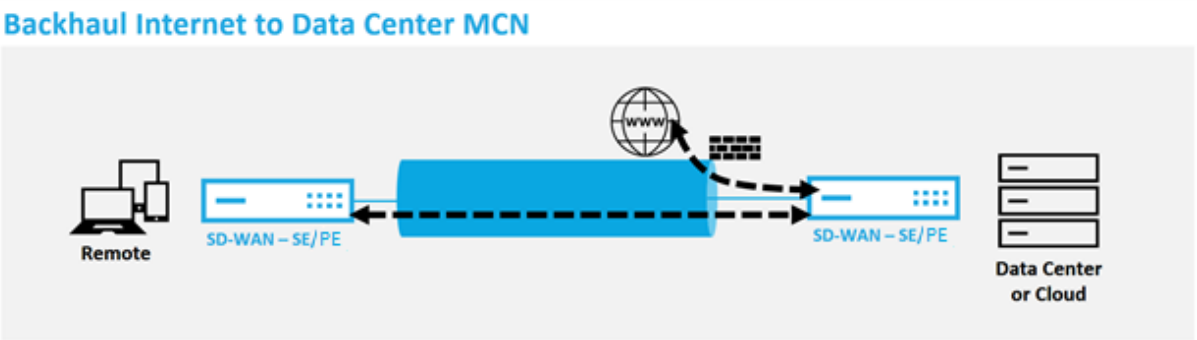
Citrix SD-WAN admite las siguientes soluciones Secure Web Gateway de terceros:

- Zscaler
- Forcepoint
- Palo Alto
- Citrix Secure Internet Access

Internet de red de retorno

La solución Citrix SD-WAN puede realizar backhaul el tráfico de Internet al sitio MCN u otros sitios de sucursales. Backhaul indica que el tráfico destinado a Internet se envía de vuelta a través de otro sitio predefinido que puede acceder a Internet. Es útil para redes que no permiten el acceso a Internet directamente debido a problemas de seguridad o a la topología de redes subyacentes. Un ejemplo sería un sitio remoto que carece de un firewall externo donde el firewall SD-WAN incorporado no cumple los requisitos de seguridad para ese sitio. Para algunos entornos, el backhauling de todo el tráfico de Internet de sitios remotos a través de la DMZ reforzada en el centro de datos podría ser el mejor enfoque para proporcionar acceso a Internet a los usuarios en oficinas remotas. Sin embargo, este enfoque tiene sus limitaciones para tener en cuenta el seguimiento y el tamaño de los enlaces WAN subyacente es adecuado.

- El backhaul del tráfico de Internet agrega latencia a la conectividad de Internet y es variable en función de la distancia del sitio de sucursal para el centro de datos.
- El backhaul del tráfico de Internet consume ancho de banda en la Ruta Virtual y se tiene en cuenta en el tamaño de los enlaces WAN.
- El backhaul del tráfico de Internet podría sobresuscribirse al enlace WAN de Internet en el centro de datos.

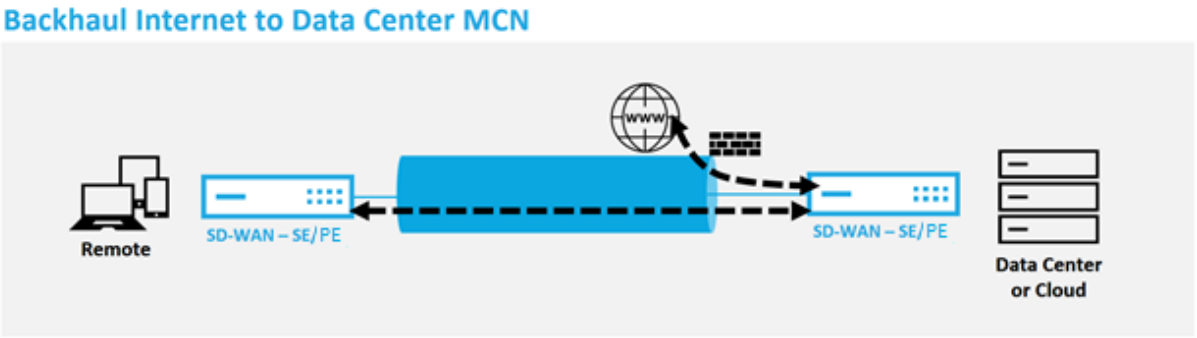


Todos los dispositivos Citrix SD-WAN pueden terminar hasta ocho enlaces WAN de Internet distintos en un solo dispositivo. Las capacidades de rendimiento con licencia para los vínculos WAN agregados se enumeran por dispositivo respectivo en la hoja de datos de Citrix SD-WAN.

Modo horquilla

Con la implementación de horquilla, puede implementar el uso de un sitio Remote Hub para el acceso a Internet a través de backhaul o horquilla cuando los servicios locales de Internet no están disponibles o están experimentando un tráfico más lento. Puede aplicar redirección de ancho de banda alto entre sitios cliente al permitir el backhauling desde sitios específicos.

El propósito de una implementación de horquilla desde un sitio que no es WAN a un sitio de reenvío WAN es proporcionar un proceso de implementación más eficiente y una implementación técnica más optimizada. Puede utilizar un sitio de concentrador remoto para el acceso a Internet cuando surjan necesidades y puede redirigir flujos a través de la ruta virtual a la red SD-WAN.



Por ejemplo, considere un administrador con varios sitios SD-WAN, A y B. El sitio A tiene un servicio de Internet deficiente. El sitio B tiene un servicio de Internet utilizable, con el que quiere hacer retroceder el tráfico del sitio A al sitio B solamente. Puede intentar lograrlo sin la complejidad de los costes de ruta ponderados estratégicamente y la propagación a sitios que no deberían recibir el tráfico.

Además, la tabla de rutas no se comparte en todos los sitios de una implementación de Hairpin. Por ejemplo, si el tráfico se encuentra entre el sitio A y el sitio B a través del sitio C, solo el sitio C conocería

las rutas de los sitios A y B. El sitio A y el sitio B no comparten la tabla de rutas de los demás, a diferencia del reenvío WAN a WAN.

Cuando el tráfico se fija entre el sitio A y el sitio B a través del sitio C, las rutas estáticas deben agregarse en el sitio A y el sitio B, lo que indica que el siguiente salto para ambos sitios es el sitio intermedio C.

El reenvío de WAN a WAN y el implementación de horquilla tienen ciertas diferencias, a saber:

1. Las rutas virtuales dinámicas no están configuradas. Siempre, el sitio intermedio ve todo el tráfico entre los dos sitios.
2. No participa en grupos de reenvío WAN a WAN.

   El reenvío de WAN a WAN y el implementación de horquilla se excluyen mutuamente. Solo se puede configurar una de ellas en un momento dado.

   Los dispositivos Citrix SD-WAN SE y VPX (virtuales) admiten la implementación en horquilla. Ahora puede configurar una ruta 0.0.0.0/0 para el tráfico de horquilla entre dos ubicaciones sin afectar a ninguna ubicación adicional. Si se utiliza la fijación de seguridad para el tráfico de la intranet, se agregan rutas de intranet específicas al sitio del cliente para reenviar el tráfico de la intranet a través de la ruta virtual al sitio de horquilla. Ya no es necesario habilitar el reenvío de WAN a WAN para lograr la funcionalidad de horquilla.

Firewall alojados

November 16, 2022

Citrix SD-WAN Orchestrator Service admite los siguientes firewalls alojados:

- Palo Alto Redes
- Check Point

Integración de firewall de Palo Alto Networks en la plataforma SD-WAN 1100

Citrix SD-WAN admite el alojamiento del firewall de la serie de máquinas virtuales de última generación (VM) de Palo Alto Networks en la plataforma SD-WAN 1100. Los siguientes son los modelos de máquinas virtuales compatibles:

- VM 50
- VM 100

El firewall de la serie de máquinas virtuales Palo Alto Network se ejecuta como una máquina virtual en la plataforma SD-WAN 1100. La máquina virtual de firewall está integrada en el modo **Virtual Wire**

con dos interfaces virtuales de datos conectadas a ella. El tráfico requerido se puede redirigir a la máquina virtual del firewall mediante la configuración de directivas en SD-WAN.

Para obtener información sobre cómo aprovisionar la máquina virtual de firewall a través de SD-WAN Orchestrator Service, consulte Firewalls alojados.

Ventajas

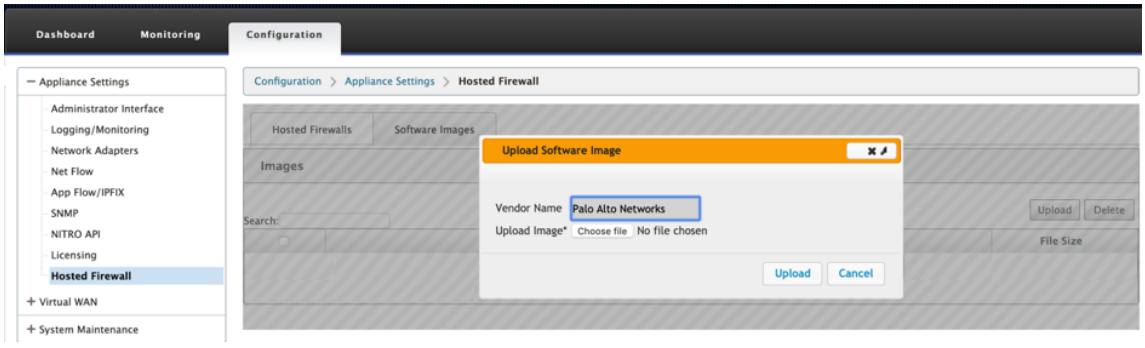
Los siguientes son los principales objetivos o beneficios de la integración de Palo Alto Networks en la plataforma SD-WAN 1100:

- Consolidación de dispositivos de sucursales: Un único dispositivo que ofrece seguridad avanzada y SD-WAN.
- Seguridad de sucursales con NGFW (firewall de próxima generación) local para proteger el tráfico de LAN a LAN, LAN a Internet e Internet a LAN.

Provisioning de máquinas virtuales de firewall a través de la GUI del dispositivo

En la plataforma SD-WAN, aprovisione e inicie la máquina virtual alojada. Realice los siguientes pasos para el Provisioning:

1. En la GUI de Citrix SD-WAN, vaya a **Configuración** > expanda **Configuración del dispositivo** > seleccione **Firewall alojado**.
2. Sube la imagen del software:
    - Seleccione la ficha **Imágenes de software**. Seleccione el nombre del proveedor como **Palo Alto Networks**.
    - Elija el archivo de imagen de software.
    - Haga clic en **Cargar**.

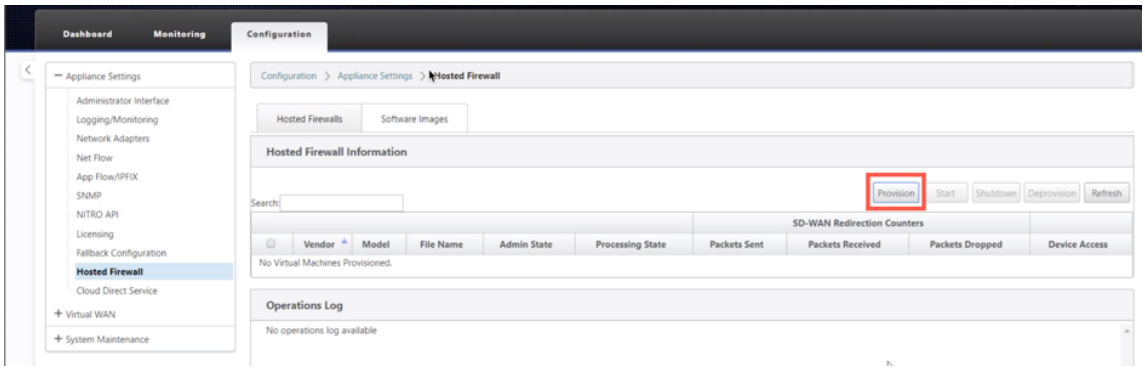


> **Nota Se**
>
> puede cargar un máximo de dos imágenes de software. La carga de la imagen de

> la máquina virtual Palo Alto Networks puede tardar más tiempo dependiendo de la disponibilidad del ancho de banda.

Puede ver una barra de estado para realizar un seguimiento del proceso de carga. El detalle del archivo se refleja una vez que la imagen se ha cargado correctamente. La imagen que se utiliza para el aprovisionamiento no se puede eliminar. No realice ninguna acción ni vuelva a ninguna otra página hasta que el archivo de imagen muestre el 100% cargado.

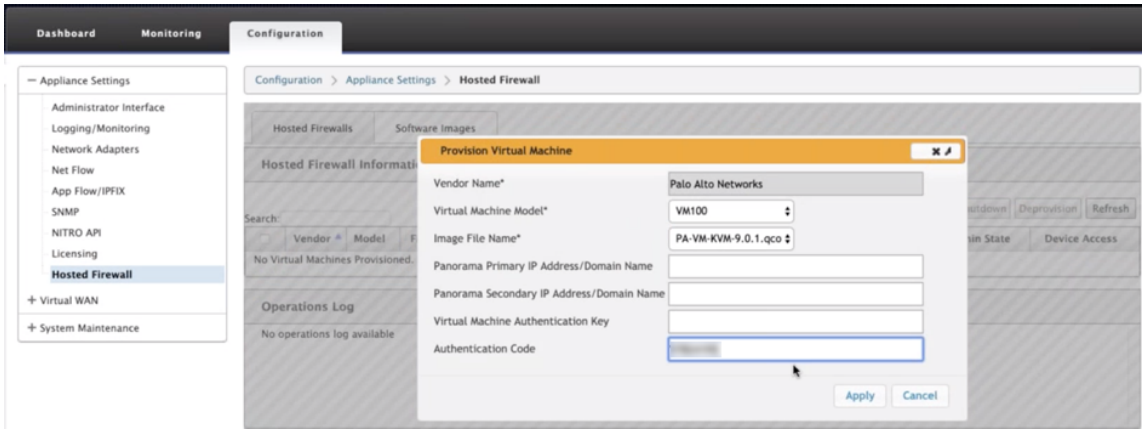
3. Para el aprovisionamiento, seleccione la ficha **Firewalls alojados** y haga clic en el botón **Aprovisionar**.



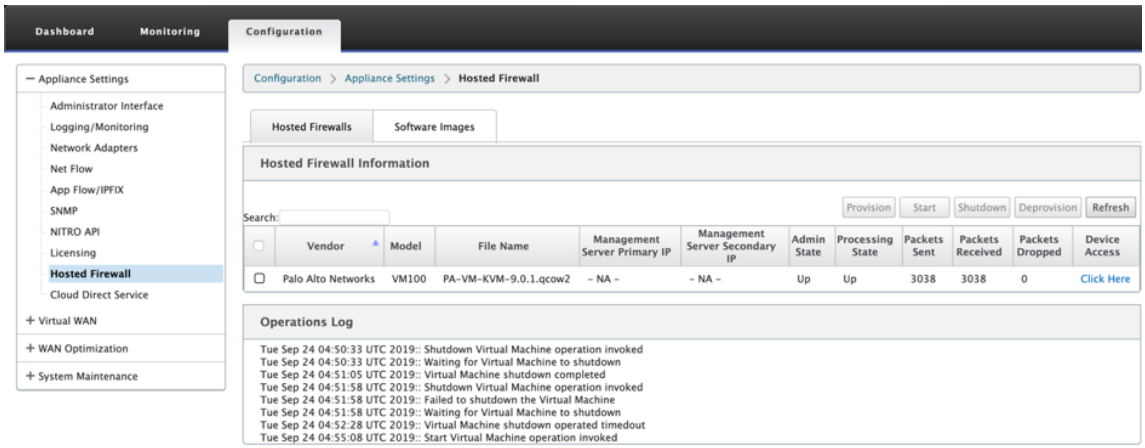
4. Proporcione los siguientes detalles para el Provisioning.

   - **Nombre del proveedor**: Seleccione el proveedor como **Palo Alto Networks**.
   - **Modelo de máquina virtual**: Seleccione el número de modelo de máquina virtual de la lista.
   - **Nombre del archivo de imagen**: seleccione el archivo de imagen.
   - **Dirección IP principal/nombre de dominio de Panorama**: proporcione la dirección IP principal de Panorama o el nombre de dominio completo (opcional).
   - **Dirección IP secundaria/nombre de dominio de Panorama**: proporcione la dirección IP secundaria de Panorama o el nombre de dominio completo (opcional).
   - **Clave de autenticación de máquina virtual**: Proporcione la clave de autenticación de máquina virtual (opcional).

     La clave de autenticación de máquina virtual es necesaria para el registro automático de la máquina virtual Palo Alto Networks en el Panorama.
   - **Código de autenticación**: Introduzca el código de autenticación (código de licencia de máquina virtual) (opcional).
   - Haga clic en **Aplicar**.



5. Haga clic en **Actualizar** para obtener el estado más reciente. Una vez que la máquina virtual Palo Alto Networks se haya iniciado por completo, se reflejará en la interfaz de usuario de SD-WAN con el detalle del registro de operaciones.



- **Estado de administración**: Indica si la máquina virtual está arriba o abajo.
- **Estado de procesamiento: estado**de procesamiento de la ruta de datos de la máquina virtual.
- **Paquete enviado**: paquetes enviados desde SD-WAN a la máquina virtual de seguridad.
- **Paquetes recibidos**: paquetes recibidos por SD-WAN desde la máquina virtual de seguridad.
- **Paquetes descartados**: paquetes descartados por SD-WAN (por ejemplo, cuando la máquina virtual de seguridad está inactiva).
- **Acceso al dispositivo**: haga clic en el enlace para obtener el acceso de la GUI a la máquina virtual de seguridad.

Puede **Iniciar, Apagar** y **Desaprovisionar** la máquina virtual según sea necesario. Utilice la opción **Haga clic aquí** para acceder a la GUI de la máquina virtual Palo Alto Networks o utilice su IP de administración junto con el puerto 4100 (IP de administración: 4100).

> **Nota**
> Utilice siempre el modo incógnito para acceder a la GUI de Palo Alto Networks.

Integración del firewall de Check Point en la plataforma SD-WAN 1100

Citrix SD-WAN admite el alojamiento de **Check Point Quantum Edge** en la plataforma SD-WAN 1100.

Check Point Quantum Edge se ejecuta como una máquina virtual en la plataforma SD-WAN 1100 SE. La máquina virtual de firewall está integrada en el modo Puente con dos interfaces virtuales de datos conectadas a ella. El tráfico requerido se puede redirigir a la máquina virtual del firewall mediante la configuración de directivas en SD-WAN.

Para obtener información sobre cómo aprovisionar la máquina virtual de firewall a través de SD-WAN Orchestrator Service, consulte Firewalls alojados.

> **Nota**
>
> Desde Citrix SD-WAN 11.3.1 en adelante, la VM de Check Point versión 80.20 y superior son compatibles para aprovisionar VM en sitios nuevos.

Ventajas

Los siguientes son los principales objetivos o beneficios de la integración de Check Point en la plataforma SD-WAN 1100:

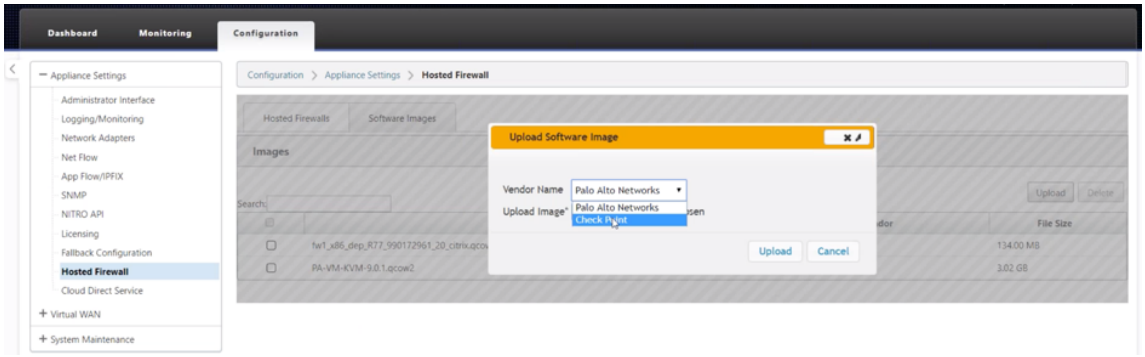
- Consolidación de dispositivos de sucursales: Un único dispositivo que realiza seguridad SD-WAN y avanzada
- Seguridad de sucursales con NGFW (Next Generation Firewall) en las instalaciones para proteger el tráfico de LAN a LAN, LAN a Internet e Internet a LAN

Provisioning de máquinas virtuales de firewall a través de la GUI del dispositivo

En la plataforma SD-WAN, aprovisione e inicie la máquina virtual alojada. Realice los siguientes pasos para el Provisioning:

1. En la GUI de Citrix SD-WAN, vaya a **Configuración > Configuración del dispositivo >** Seleccione **Firewall alojado**.
2. Sube la imagen del software:
    - Seleccione la ficha **Imágenes de software**. Seleccione el **nombre del proveedor** como punto de comprobación.

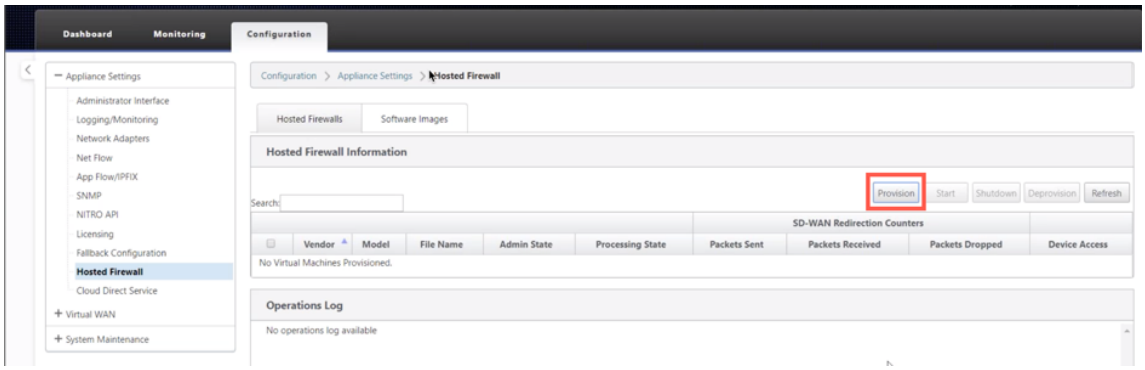
- Elija el archivo de imagen de software.
- Haga clic en **Cargar**.



> **Nota Se**
>
> pueden cargar un máximo de dos imágenes. La carga de la imagen de la máquina virtual Check Point puede tardar más tiempo en función de la disponibilidad del ancho de banda.

Puede ver una barra de estado para realizar un seguimiento del proceso de carga. El detalle del archivo se refleja una vez que la imagen se ha cargado correctamente. La imagen que se utiliza para el aprovisionamiento no se puede eliminar. No realice ninguna acción ni vuelva a ninguna otra página hasta que el archivo de imagen muestre el 100% cargado.

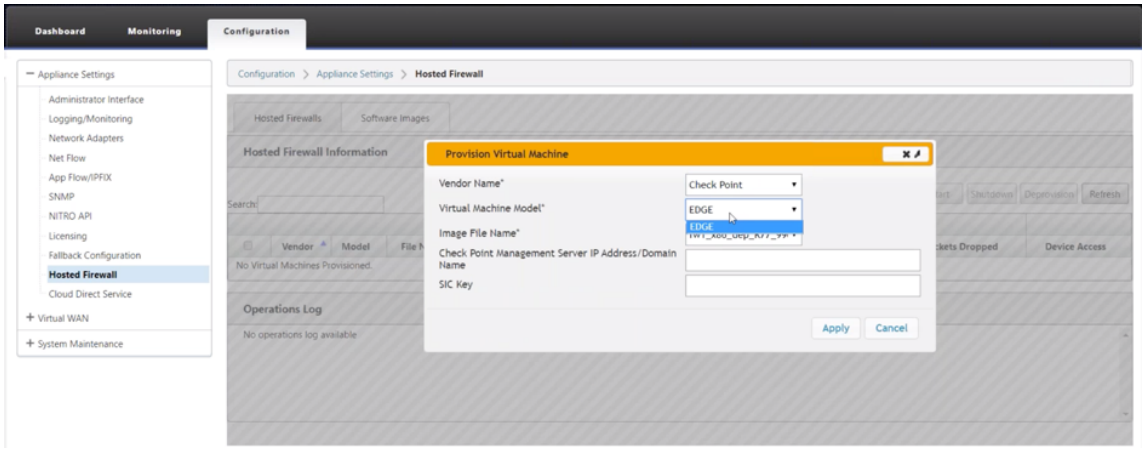
3. Para el aprovisionamiento, seleccione la ficha **Firewall alojado** > haga clic en el botón **Provisioning**



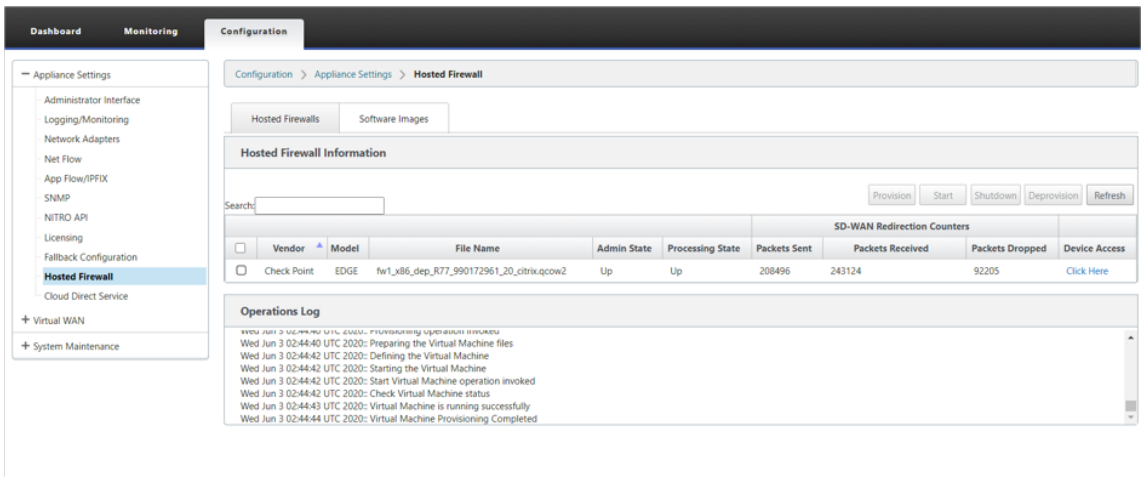
4. Proporcione los siguientes detalles para el Provisioning.

- **Nombre del Proveedor**: Seleccione el **Nombre del Proveedor** como Punto de Verificación.
- **Modelo de máquina virtual**: el modelo de máquina virtual se rellena automáticamente como **Edge**.
- **Nombre de archivo**de imagen: el nombre del archivo de imagen se rellena automáticamente.
- **Dirección IP/Dominio del Servidor de Administración**de Check Point: Proporcione la dirección IP/dominio del servidor de administración de puntos de comprobación.

- **Clave SIC**: Proporcione la tecla SIC (opcional). SIC crea conexiones de confianza entre los componentes de **Check Point**. Haga clic en **Aplicar**.



5. Haga clic en **Actualizar** para obtener el estado más reciente. Una vez que la máquina virtual Check Point se inicie por completo, se reflejará en la interfaz de usuario de SD-WAN con el detalle del registro de operaciones.



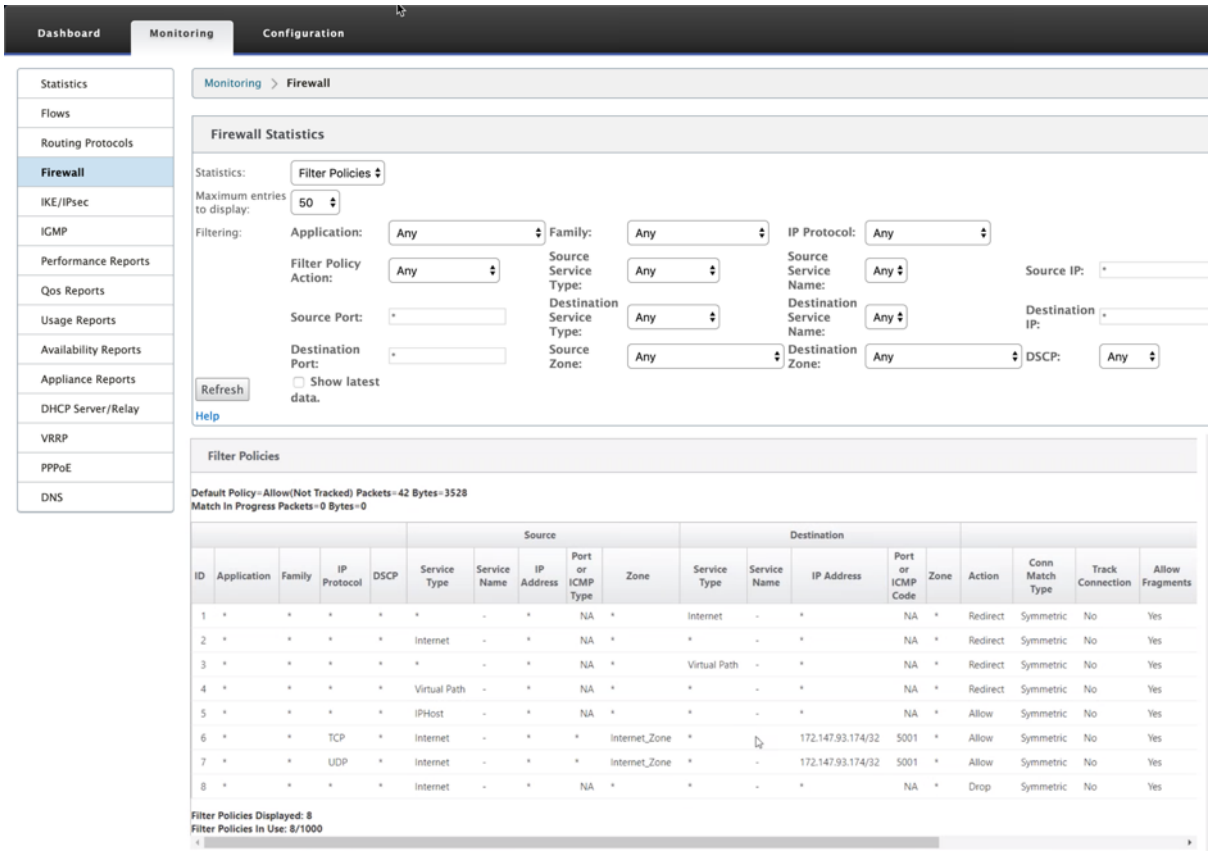
- **Estado de administración**: Indica si la máquina virtual está arriba o abajo.
- **Estado de procesamiento: estado**de procesamiento de la ruta de datos de la máquina virtual.
- **Paquete enviado**: paquetes enviados desde SD-WAN a la máquina virtual de seguridad.
- **Paquetes recibidos**: paquetes recibidos por SD-WAN desde la máquina virtual de seguridad.
- **Paquetes descartados**: paquetes descartados por SD-WAN (por ejemplo, cuando la máquina virtual de seguridad está inactiva).
- **Acceso al dispositivo**: haga clic en el enlace para obtener el acceso de la GUI a la máquina virtual de seguridad.

Puede **Iniciar, Apagar** y **Desaprovisionar** la máquina virtual según sea necesario. Utilice la opción

Haga clic aquí para acceder a la GUI de la máquina virtual Check Point o utilice su IP de administración junto con el puerto 4100 (IP de administración: 4100).

> **Nota**
>
> Utilice siempre el modo incógnito para acceder a la GUI de punto de comprobación.

Mientras toda la configuración de red está activa y en funcionamiento, puede supervisar la conexión en **Supervisión > Firewalls > Directivas de filtro**.



Grupos de agregación de enlaces

August 26, 2022

La funcionalidad de grupos de agregación de vínculos (LAG) permite agrupar dos o más puertos en el dispositivo SD-WAN para que funcionen juntos como un solo puerto. Esto garantiza una mayor disponibilidad, redundancia de enlaces y performance mejorado.

Anteriormente, solo el modo Active-Backup era compatible en LAG. A partir de la versión 11.3 de Citrix SD-WAN, se admiten las negociaciones basadas en el protocolo 802.3AD Link Aggregation Control Protocol (LACP). El LACP es un protocolo estándar y proporciona más funcionalidad para LAG.

En el modo Active-Backup, en cualquier momento solo hay un puerto activo y los otros puertos están en modo de copia de seguridad. Los soportes activos y de copia de seguridad se basan en el paquete Kit de desarrollo de planos de datos (DPDK) para la funcionalidad de LAG.

Con el LACP, puede enviar el tráfico a través de todos los puertos simultáneamente. Como ventaja, obtiene más ancho de banda junto con el mecanismo de redundancia de enlaces. La implementación de LACP admite el modo **Activo-Activo**. Ahora, con el modo Active-Backup, también tiene la opción de seleccionar el modo Activo-Activo LACP completo desde la interfaz de usuario de SD-WAN.

La funcionalidad LAG solo está disponible en las siguientes plataformas compatibles con DPDK:

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 1100 SE
- Citrix SD-WAN 2100 SE
- Citrix SD-WAN 4100 SE
- Citrix SD-WAN 5100 SE
- Citrix SD-WAN 6100 SE

> **Nota**
>
> La funcionalidad LAG no es compatible con las plataformas VPX/VPXL.

Limitaciones

- Puede crear un máximo de cuatro LAG con un máximo de cuatro puertos agrupados en cada LAG en los dispositivos Citrix SD-WAN.
- Las opciones de prioridad de puerto y prioridad del sistema no son compatibles con la implementación de LACP.

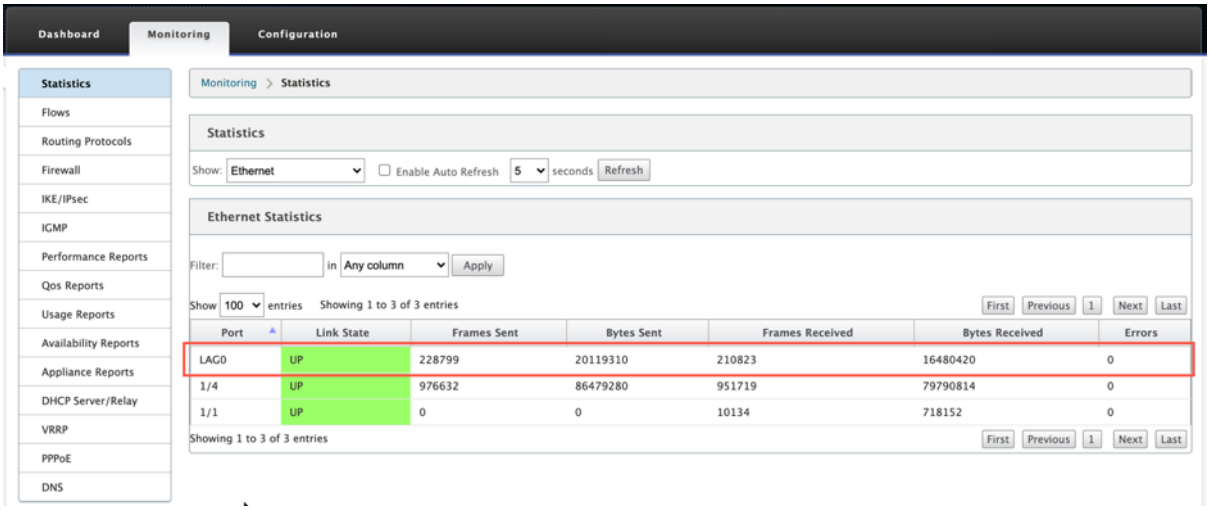
Con la versión 11.3 en adelante, en SD-WAN con la implementación LACP, los puertos están siempre en modo activo. Eso significa que SD-WAN siempre puede iniciar la negociación.

> **Nota**
>
> - Para los dispositivos Citrix SD-WAN 210 SE, solo puede crear un LAG con un máximo de tres puertos agrupados en él.
> - La función de Propagación de estado de enlace (LSP) no se admite si se utilizan LAG como interfaces Ethernet en los grupos de interfaces.

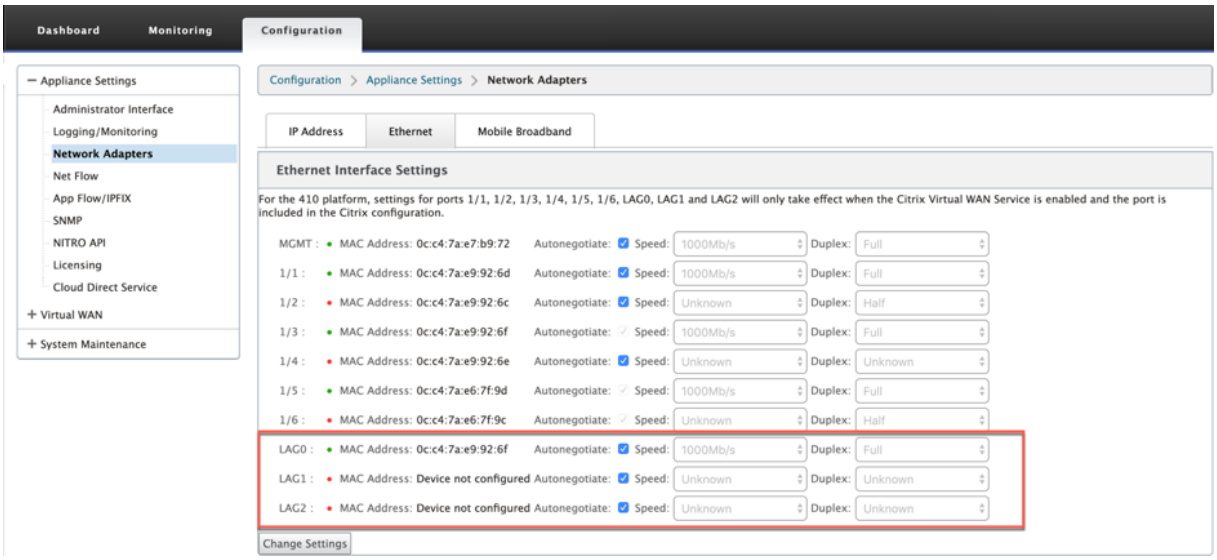
A partir de Citrix SD-WAN 11.5, puede configurar grupos de agregación de enlaces a través de SD-WAN Orchestrator Service. Para obtener más información, consulte Grupos de agregación de enlaces.

Supervisión y solución de problemas

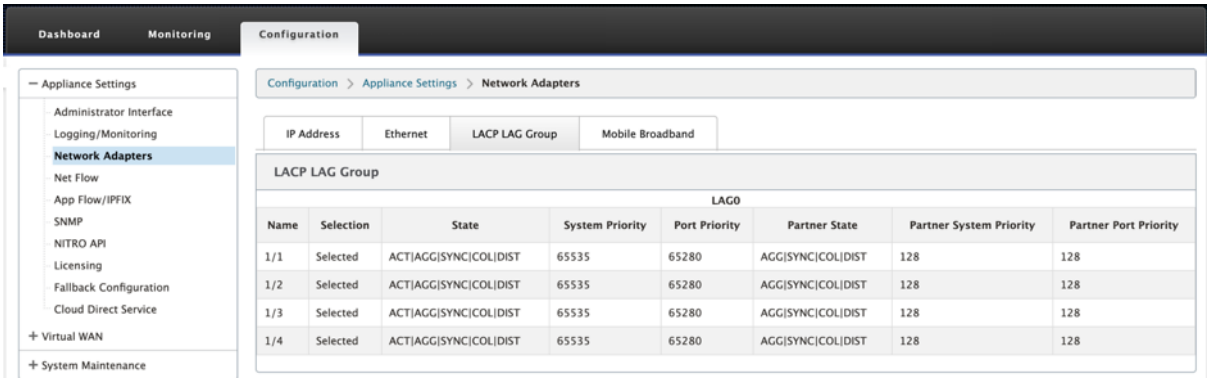
Para ver las estadísticas o el estado del vínculo, vaya a **Supervisión > Estadísticas**. Seleccione **Ethernet** en la lista desplegable **Mostrar**.



Para ver los puertos LAG activos y en espera, vaya a **Configuración > Configuración** > **Configuración del dispositivo** > **Adaptadores de red** > **Ethernet**.



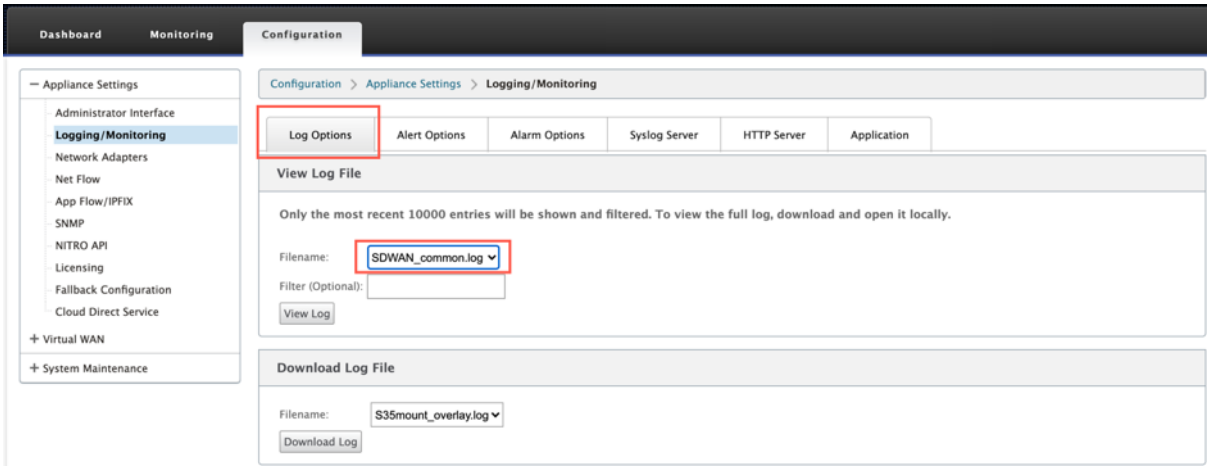
Seleccione la ficha **Grupo LAG LACP** para ver los diversos detalles relacionados con el grupo LAG LACP.



Nota

No puede cambiar la configuración de los puertos miembros individuales, los cambios de configuración realizados en el LAG se envían automáticamente a los puertos miembros.

Puede descargar los archivos de registro para seguir solucionando problemas. Vaya a **Configuración > Registro/Supervisión** y seleccione **SDWAN_common.log** en la ficha **Opciones de registro**.



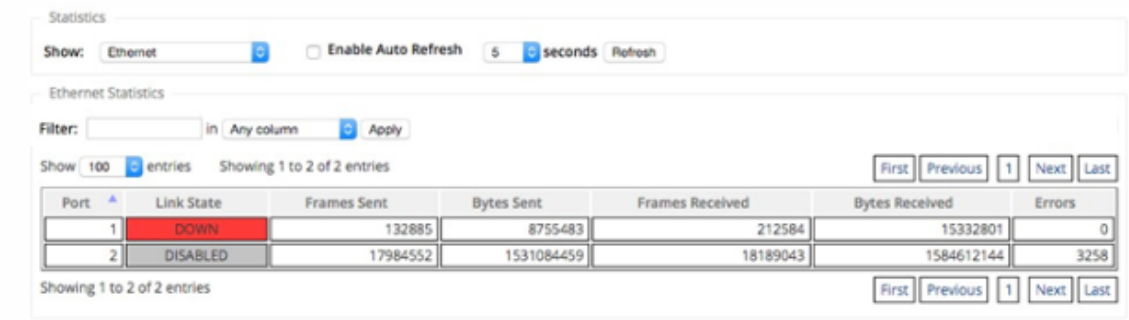
Propagación del estado del vínculo

August 26, 2022

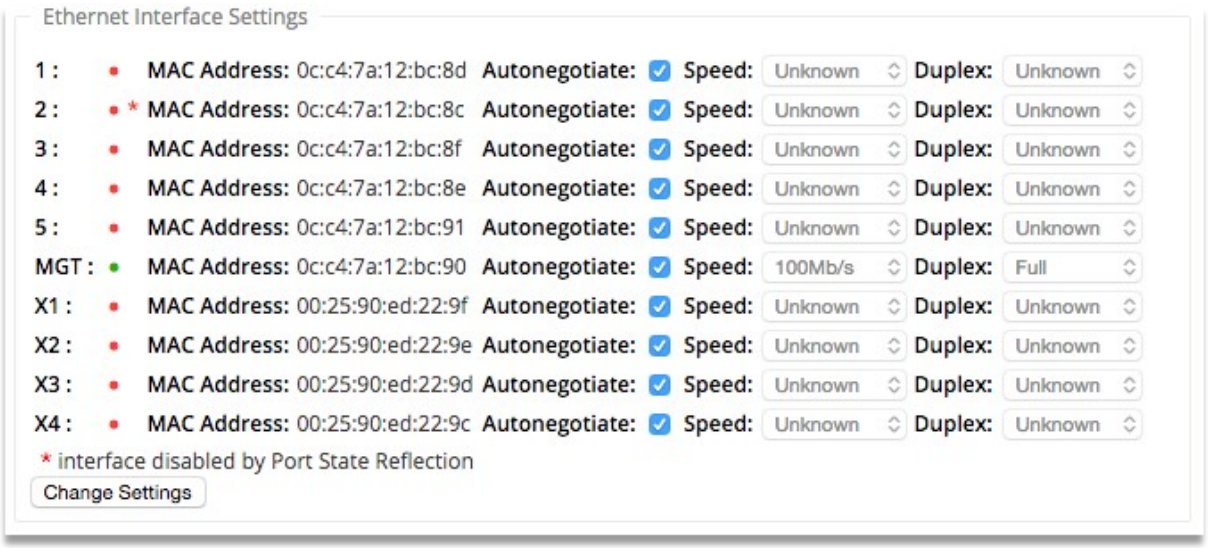
La función de propagación de estado de enlace (LSP) permite a los administradores de red mantener sincronizado el estado de enlace de un par de derivación, permitiendo que se conecte en el otro lado del vínculo para ver cuando los enlaces están inactivos. Cuando un puerto de un par de derivación se vuelve inactivo, el enlace acoplado se desactiva administrativamente. Si la arquitectura de red incluye una red de conmutación por error paralela, esto obliga al tráfico a la transición a esa red. Una vez que se restablece el enlace interrumpido, su enlace correspondiente se activa automáticamente.

Supervisión de estadísticas de enlaces

1. En la página **Supervisar > Estadísticas**, seleccione **Ethernet en el menú** desplegable **Mostrar** para ver el estado del par de puertos de derivación con Propagación de estado de enlace activada. Observe que el enlace del lado de la LAN está inactivo y, posteriormente, el enlace del lado WAN del par de bypass está inhabilitado administrativamente.



2. Vaya a **Configuración > Configuración del dispositivo** > **Adaptadores de red > ficha Ethernet**. Los puertos que están inactivos desde el punto de vista administrativo se indican con un asterisco rojo (*) en la lista **Configuración de la interfaz Ethernet**.



Enlaces WAN de medición y espera

November 16, 2022

Citrix SD-WAN admite la habilitación de vínculos con contador, que se pueden configurar de forma que el tráfico de usuarios solo se transmita en un vínculo WAN de Internet específico cuando todos los demás vínculos WAN disponibles están inhabilitados.

Los enlaces de uso medido conservan el ancho de banda de los enlaces que se facturan en función del uso. Con los enlaces medidos puede configurar los enlaces como el enlace de Último recurso, lo que no permite el uso del enlace hasta que todos los demás enlaces no medidos estén invalidados o degradados. Establecer último recurso suele estar habilitado cuando hay tres enlaces WAN a un sitio (es decir, MPLS, Internet de banda ancha, 4G/LTE) y uno de los enlaces WAN es 4G/LTE y puede resultar demasiado costoso para una empresa permitir su uso a menos que sea necesario. La medición no está habilitada de forma predeterminada y se puede habilitar en un enlace WAN de cualquier tipo de acceso (Internet pública/MPLS privada/Intranet privada). Si la medición está habilitada, puede configurar opcionalmente lo siguiente:

- Tapa de datos
- Ciclo de facturación (semanal/mensual)
- Fecha de inicio
- Modo de espera
- Prioridad
- Intervalo de latido activo: intervalo en el que un dispositivo envía un mensaje de latido a su par en el otro extremo de la ruta virtual cuando no ha habido tráfico (usuario/control) en la ruta durante al menos un intervalo de latidos

Con un vínculo de medición local, el panel de control de un dispositivo muestra una tabla de **medición de enlaces WAN** en la parte inferior con información de medición.

El uso del ancho de banda en un enlace medido local se realiza con respecto al límite de datos configurado. Cuando el uso supera el 50%, el 75% o el 90% del límite de datos configurado, el dispositivo genera un evento para alertar al usuario y se muestra un indicador de advertencia en la parte superior del panel del dispositivo. Una ruta de medición se puede formar con 1 o 2 enlaces de medición. Si se forma una ruta entre dos vínculos medidos, el intervalo de latido activo utilizado en la ruta medida es el mayor de los dos intervalos de latidos activos configurados en los vínculos.

Una ruta de acceso medido es una ruta de acceso no en espera y siempre es elegible para el tráfico de usuario. Cuando hay al menos una ruta no medida que está en estado GOOD, una ruta de acceso medido lleva la cantidad reducida de tráfico de control y se evita cuando el plano de reenvío busca una ruta de acceso para un paquete duplicado.

Modo de espera

El modo de espera de un enlace WAN está inhabilitado de forma predeterminada. Para habilitar el modo en espera, debe especificar en qué uno de los dos modos siguientes opera el vínculo en espera

- **Bajo demanda**: Vínculo en espera que se activa cuando se cumple una de las condiciones.

Cuando el ancho de banda disponible en la ruta virtual es menor que el límite de ancho de banda a demanda configurado Y hay suficiente uso. El uso suficiente se define como más del 95% (ON_DEMAND_USAGE_THRSHOLD_PCT) del ancho de banda disponible actual, o la diferencia entre el ancho de banda disponible actual y el uso actual es inferior a 250 kbps (ON_DEMAND_THORHOLD_GAP_Kbps) ambos parámetros se pueden cambiar mediante t2_variables cuando todos los parámetros no en espera las rutas están muertas o inhabilitadas.

- **Último recurso**: Enlace en espera que se activa cuando todos los enlaces que no son en espera y los enlaces en espera a demanda están muertos o inhabilitados.
- La prioridad en espera indica el orden en que se activa un vínculo en espera, si hay varios vínculos en espera:
  - un enlace en espera de prioridad 1 se activa primero, mientras que un enlace en espera de prioridad 3 se activa en último lugar
  - Se puede asignar la misma prioridad a varios enlaces en espera

Al configurar un vínculo en espera, puede especificar la prioridad en espera y dos intervalos de latido:

- **Intervalo de latido activo**: El intervalo de latido utilizado cuando la ruta de espera está activa (por defecto 50 ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s)
- **Intervalo de latido en espera**: Intervalo de latido utilizado cuando la ruta de espera está inactiva (predeterminado 1s/2s/3s/4s/5s/6s/7s/8s/9s/10s/inhabilitado)

Una ruta en espera se forma con 1 o 2 enlaces en espera.

- **Bajo demanda**: Se forma una ruta de espera a demanda entre:
  - un enlace no en espera y un enlace en espera a demanda
  - 2 enlaces en espera a demanda
- **Last-Resort** - Se forma una ruta de espera del último recurso entre:
  - un enlace no en espera y un enlace en espera de último recurso
  - un enlace en espera a demanda y un enlace en espera de último recurso
  - 2 enlaces de reserva de último recurso

Los intervalos de latidos utilizados en una ruta de espera se determinan de la siguiente manera:

- Si el latido en espera está desactivado en al menos uno de los dos vínculos, el latido se desactiva en la ruta de espera mientras está inactivo.
- Si el latido del corazón en espera no está desactivado en ninguno de los vínculos, se utilizará el mayor de los dos valores cuando la ruta de espera esté en espera.

- Si el intervalo de latido activo está configurado en ambos vínculos, se utiliza el mayor de los dos valores cuando la ruta de espera está activa.

Mensajes de Heartbeat (keep alive):

- En una ruta no en espera, los mensajes de latidos se envían solo cuando no ha habido tráfico (control o usuario) durante al menos un intervalo de latidos. El intervalo de latidos varía según el estado de la ruta. Para trayectos **no en espera ni medidos** :
  - 50 ms cuando el estado de la ruta es BUENO
  - 25 ms cuando el estado de la ruta es MALO

En una ruta de espera, el intervalo de latido utilizado depende del estado de actividad y del estado de ruta:

- Mientras está inactivo, si el latido no está inhabilitado, los mensajes de latidos se envían regularmente en el intervalo de latidos de espera configurado, ya que no se permite ningún otro tráfico en él.
- el intervalo de latido activo configurado se utiliza cuando el estado de ruta es BUENO.
- 1/2 el intervalo de latido activo configurado se utiliza cuando el estado de la ruta es MALO.
- Mientras están activas, como las rutas no en espera, los mensajes de latidos se envían solo cuando no ha habido tráfico (control o usuario) durante al menos el intervalo de latido activo configurado.
- el intervalo de latido en espera configurado se utiliza cuando el estado de la ruta es BUENO.
- 1/2 el intervalo de latido en espera configurado se utiliza cuando el estado de la ruta es MALO.

Mientras están inactivas, las rutas de espera no son aptas para el tráfico de usuarios. Los únicos mensajes de protocolo de control enviados en rutas de espera inactivas son los mensajes de latidos, que se utilizan para detectar fallos de conectividad y recopilar métricas de calidad. Cuando las rutas de espera están activas, son aptas para el tráfico de usuarios con un coste de tiempo adicional. Esto se hace para que las rutas no en espera, si están disponibles, se favorezcan durante la selección de rutas de reenvío.

Se supone que el estado de la ruta de acceso de una ruta en espera con latido inactivo, mientras está inactivo, es BUENO y se muestra como BUENO en la tabla Estadísticas de ruta en **Supervisión**. Cuando se activa, a diferencia de una ruta no en espera que comienza en estado DEAD hasta que escucha de su par Virtual Path, comienza en buen estado. Si no se detecta conectividad con el par Virtual Path, la ruta pasa a ser INCORRECTA y, a continuación, MUERTA. Si se restablece la conectividad con el par Virtual Path, la ruta pasa a ser MALO y, a continuación, BUENA de nuevo.

Si dicha ruta de espera se convierte en DEAD y luego se vuelve inactiva, el estado de la ruta no cambia inmediatamente a (se supone) GOOD. En cambio, se mantiene en estado MUERTO durante el tiempo para que no se pueda usar inmediatamente. Esto es para evitar que la actividad

oscile entre un grupo de trayectorias de menor prioridad con rutas DEAD supuestamente buenas y un grupo de trayectorias de mayor prioridad con rutas BUENAS. Este período de espera (NO_HB_PATH_ON_HOLD_PERIOD_MS) se establece en 5 minutos y se puede cambiar mediante t2_variables.

Si la detección de MTU de ruta está habilitada en una ruta de acceso virtual, la MTU de la ruta de acceso en espera no se utiliza para calcular la MTU de la ruta de acceso virtual mientras la ruta está en espera. Cuando la ruta de acceso en espera se activa, la MTU de la ruta virtual se vuelve a calcular teniendo en cuenta la MTU de la ruta de espera. (La MTU de la ruta virtual es la MTU de ruta más pequeña entre todas las rutas activas dentro de la ruta virtual).

Los eventos y los mensajes de registro se generan cuando una ruta de espera pasa de estar en espera a activa.

A partir de SD-WAN 11.5, puede configurar enlaces WAN medidos y en espera mediante Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Enlaces WAN de medición y en espera.

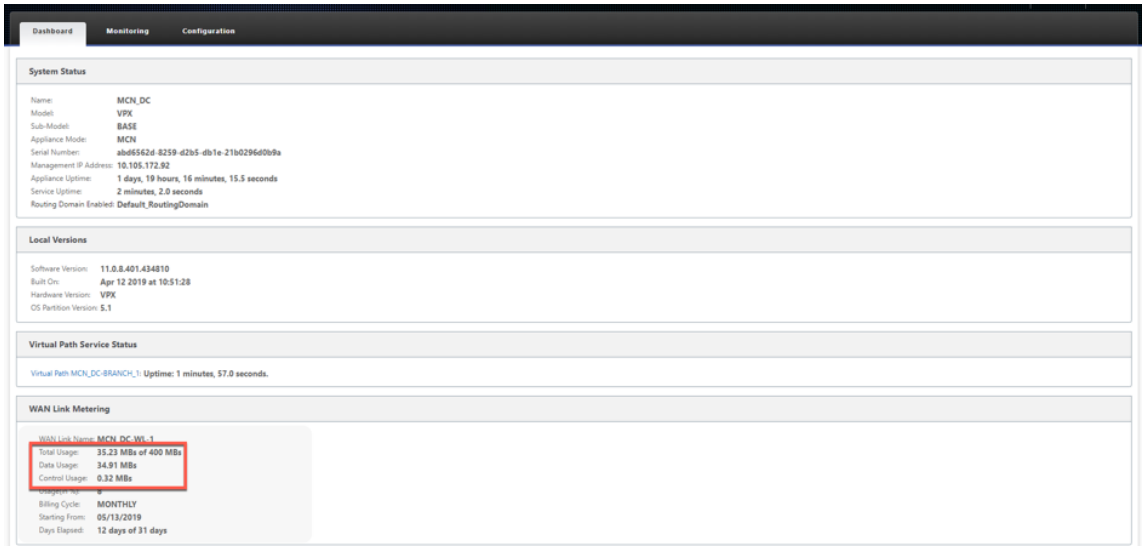
Requisitos previos de configuración:

- Un enlace de medidor puede ser de cualquier tipo de acceso.
- Todos los enlaces de un sitio se pueden configurar con la medición habilitada.
- Un enlace en espera puede ser del tipo de acceso a Internet público o Intranet privada. Un enlace WAN del tipo de acceso MPLS privado no se puede configurar como vínculo en espera.
- Se debe configurar al menos un enlace no en espera por sitio. Se admite un máximo de 3 enlaces en espera por sitio.
- Es posible que los servicios de Internet/Intranet no estén configurados en vínculos en espera a demanda. Los vínculos en espera a demanda admiten el servicio de ruta virtual.
- Es posible que el servicio de Internet esté configurado en un enlace en espera de último recurso, pero solo se admite el modo de equilibrio de carga.
- El servicio de intranet se puede configurar en un enlace en espera de último recurso, pero solo se admite el modo secundario y la recuperación principal debe estar habilitada.

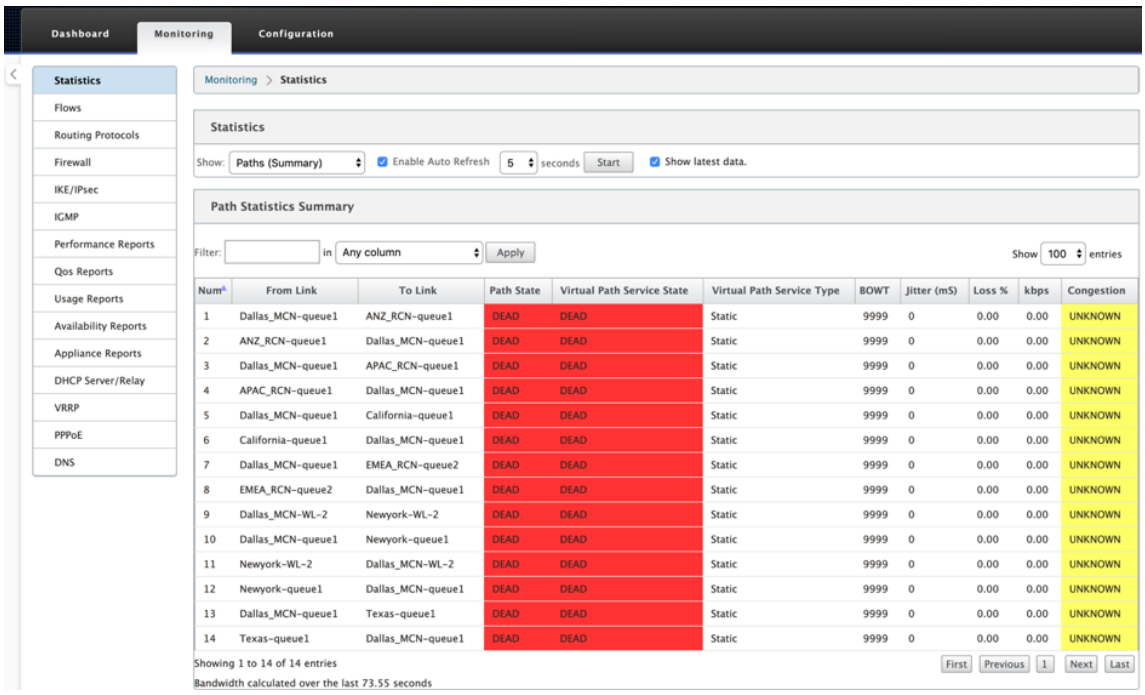
Supervisar enlaces WAN medidos y en espera

- La página Panel de control proporciona la siguiente información de **medición de vínculos WAN** con los valores de uso:
  - **Nombre del enlace WAN**: muestra el nombre del enlace WAN.
  - **Uso total**: muestra el uso total del tráfico (Uso de datos + Uso de control).
  - **Uso de datos**: muestra el uso por tráfico de usuarios.
  - **Control de uso**: muestra el uso por control del tráfico.

- **Uso (en%)**: muestra el valor del límite de datos utilizado en porcentaje (uso total/límite de datos) x 100.
- **Ciclo de facturación**: frecuencia de facturación (semanal/mensual)
- **A partir de**: Fecha de inicio del ciclo de facturación
- **Días Transcurridos**: El tiempo transcurrido (en días, horas, minutos y segundos)

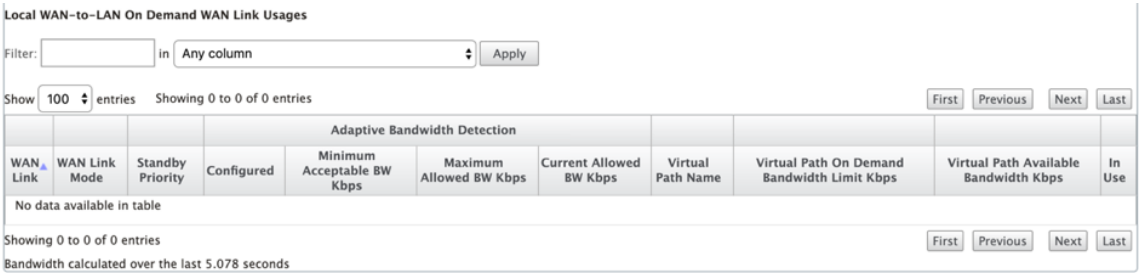


- Cuando se muestran las estadísticas de ruta (**Supervisión > Estadísticas > Rutas**), los enlaces medidos y los vínculos en espera se marcan como se muestra en la captura de pantalla.

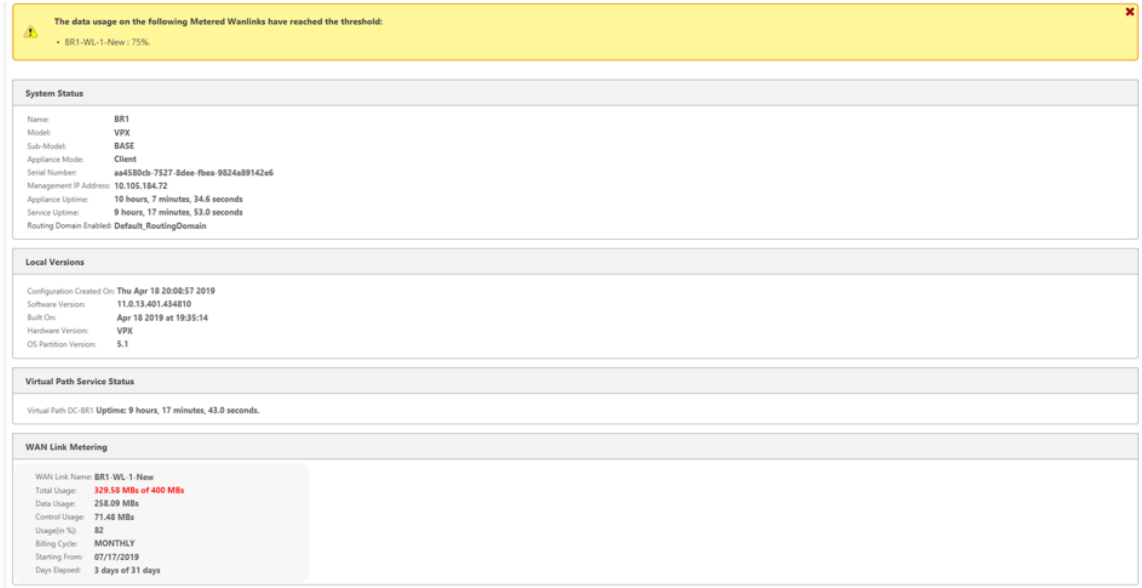


- Si el dispositivo tiene una ruta virtual que tiene un enlace en espera a demanda local o remoto, cuando se visualizan las estadísticas de uso del enlace WAN, se muestra una tabla adicional

que muestra el ancho de banda a demanda en la parte inferior de la página (**Supervisión > Estadísticas > Uso del enlace WAN**).

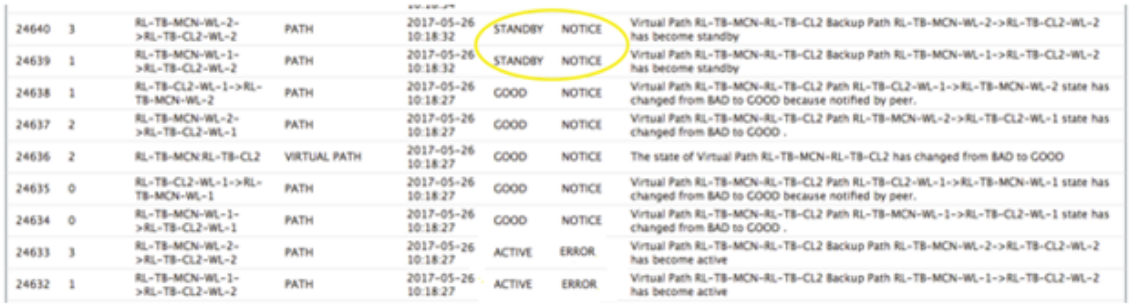


- Cuando el uso en un enlace medido supera el 50% del límite de datos configurado, se muestra un banner de advertencia en la parte superior del panel. Además, si el uso excede el 75% del límite de datos configurado, se resalta la información de medición numérica hacia la parte inferior del tablero.



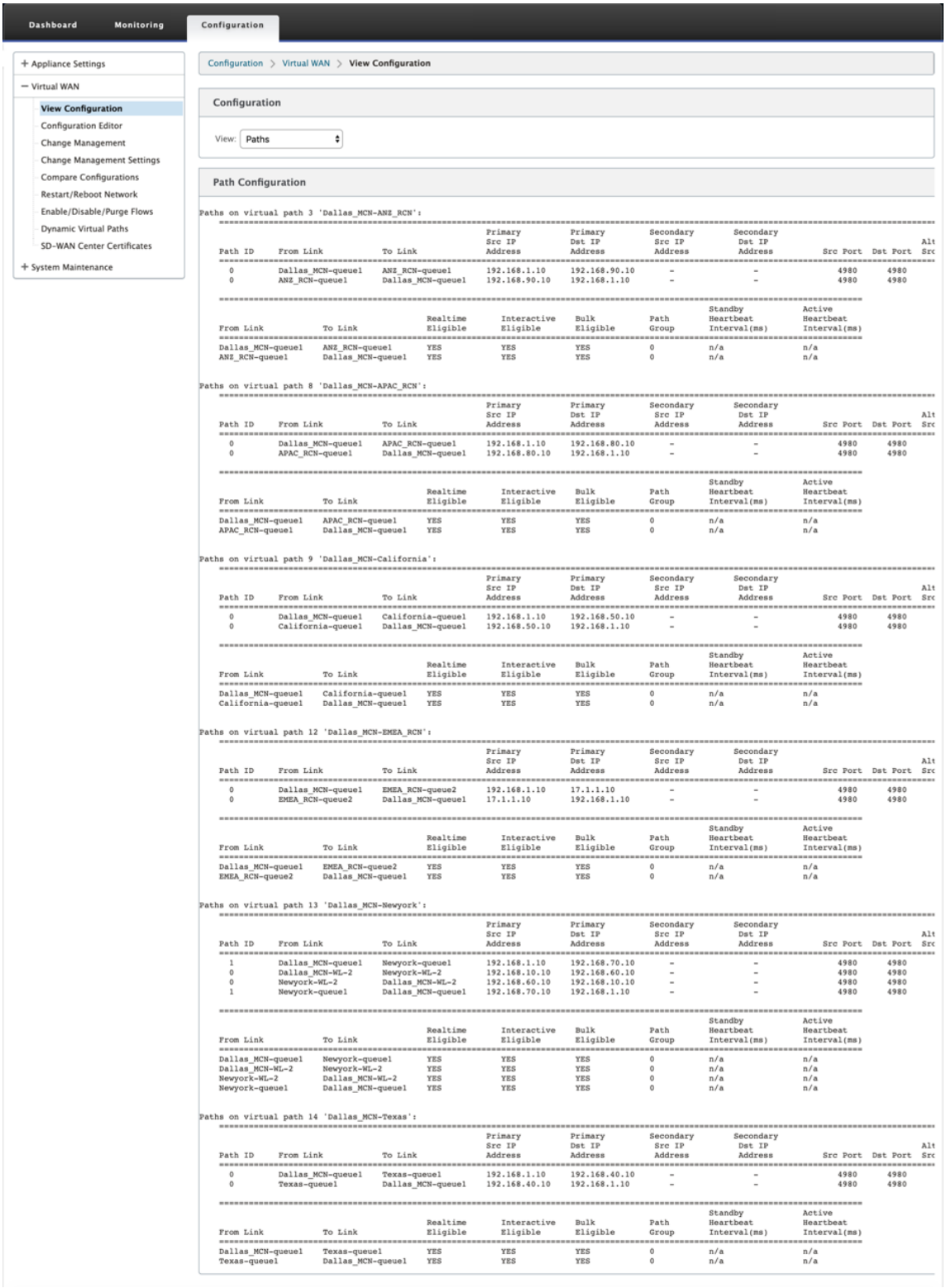
También se genera un evento de uso de enlace WAN en el dispositivo cuando el uso supera el 50%, el 75% y el 90% del límite de datos configurado.

1. Cuando una ruta en espera pasa entre el estado en espera y activo, el dispositivo genera un evento.



24640	3	RL-TB-MCN-WL-2->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become standby
24639	1	RL-TB-MCN-WL-1->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become standby
24638	1	RL-TB-CL2-WL-1->RL-TB-MCN-WL-2	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-2 state has changed from BAD to GOOD because notified by peer.
24637	2	RL-TB-MCN-WL-2->RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24636	2	RL-TB-MCN:RL-TB-CL2	VIRTUAL PATH	2017-05-26 10:18:27	GOOD	NOTICE	The state of Virtual Path RL-TB-MCN-RL-TB-CL2 has changed from BAD to GOOD
24635	0	RL-TB-CL2-WL-1->RL-TB-MCN-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-1 state has changed from BAD to GOOD because notified by peer.
24634	0	RL-TB-MCN-WL-1->RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24633	3	RL-TB-MCN-WL-2->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become active
24632	1	RL-TB-MCN-WL-1->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become active

2. Los intervalos de latido activos y en espera configurados para cada ruta se pueden ver en **Configuración** > **WAN virtual** > **Configuración de vista** > **Rutas de acceso**.



Optimización de Office 365

November 16, 2022

Las funciones de **optimización de Office 365** se ajustan a los principios de conectividad de red de Microsoft Office 365para optimizar Office 365. Office 365 se proporciona como un servicio a través de varios puntos finales de servicio (puertas delanteras) ubicados en todo el mundo. Para lograr una experiencia de usuario óptima para el tráfico de Office 365, Microsoft recomienda redirigir el tráfico de Office365 directamente a Internet desde entornos de sucursales. Evite prácticas como el backhauling a un proxy central. El tráfico de Office 365, como Outlook y Word, son sensibles a la latencia y el tráfico de backhauling introduce más latencia, lo que resulta en una mala experiencia del usuario. Citrix SD-WAN le permite configurar directivas para separar el tráfico de Office 365 a Internet.

El tráfico de Office 365 se dirige al dispositivo de punto final de servicio de Office 365 más cercano, que existe en los límites de la infraestructura de Microsoft Office 365 en todo el mundo. Una vez que el tráfico llega a una puerta principal, pasa por la red de Microsoft y llega al destino real. Minimiza la latencia a medida que se reduce el tiempo de ida y vuelta desde la red del cliente hasta el extremo de Office 365.

Dispositivos de punto final de Office 365

Los dispositivos de punto final de Office 365 son un conjunto de direcciones de red y subredes. Los dispositivos de punto final de Office 365 se clasifican en categorías **Optimizar**, **Permitir** y **Predeterminado**. Citrix SD-WAN 11.4.0 proporciona una clasificación más detallada de las categorías **Optimizar** y **Permitir**, lo que permite la asignación de libros selectiva para mejorar el rendimiento del tráfico de Office 365 sensible a la red. Dirigir tráfico sensible a la red a SD-WAN en la nube (Cloud Direct o una VPX de SD-WAN en Azure), o desde un dispositivo SD-WAN en casa a una SD-WAN en una ubicación cercana con conectividad a Internet más confiable, permite QoS y una resistencia de conexión superior en comparación con simplemente dirigir el tráfico a la La puerta principal de Office 365, a costa de un aumento en la latencia. Una solución SD-WAN en línea con QoS reduce las interrupciones y desconexiones de VoIP, reduce la fluctuación y mejora las puntuaciones medias de opinión de calidad de los medios de Microsoft Teams:

- **Optimizar**: Estos dispositivos de punto final proporcionan conectividad a todos los servicios y funciones de Office 365, y son sensibles a la disponibilidad, el rendimiento y la latencia. Representa más del 75% del ancho de banda, las conexiones y el volumen de datos de Office 365. Todos los dispositivos de punto final de Optimize están alojados en centros de datos de Microsoft. Las solicitudes de servicio a estos extremos deben separarse de la sucursal a Internet y no deben pasar por el centro de datos.

La categoría **Optimizar** se clasifica en las siguientes subcategorías:


```
- Teams Realtime
- Exchange Online
- SharePoint Optimize
```

Para obtener información acerca de las consideraciones de actualización, consulte Consideraciones importantes para la actualización.

- **Permitir**: Estos dispositivos de punto final proporcionan conectividad a servicios y funciones específicos de Office 365, y no son tan sensibles al rendimiento y la latencia de la red. La representación del ancho de banda y el recuento de conexiones de Office 365 también es menor. Estos extremos están alojados en centros de datos de Microsoft. Las solicitudes de servicio a estos extremos pueden separarse de la sucursal a Internet o pasar por el centro de datos.

La categoría **Permitir** se clasifica en las siguientes subcategorías:

```
- Teams TCP Fallback
- Exchange Mail
- SharePoint Allow
- Office365 Common
```

Para obtener información acerca de las consideraciones de actualización, consulte Consideraciones importantes para la actualización.

> **Nota**
>
> La subcategoría **Teams Realtime** utiliza el protocolo de transporte en tiempo real UDP para administrar el tráfico de Microsoft Teams, mientras que la subcategoría **Teams TCP Fallback** utiliza el protocolo de capa de transporte TCP. Dado que el tráfico multimedia es altamente sensible a la latencia, es posible que prefiera que este tráfico tome la ruta más directa posible y utilizar UDP en lugar de TCP como protocolo de capa de transporte (el transporte más preferido para medios interactivos en tiempo real en términos de calidad). Aunque UDP es un protocolo preferido para el tráfico multimedia de Teams, requiere que ciertos puertos estén permitidos en el firewall. Si los puertos no están permitidos, el tráfico de Teams utiliza TCP como reserva, y habilitar la optimización para Teams TCP Fallback garantiza una mejor entrega de la aplicación Teams en este caso. Para obtener más información, consulte Flujos de llamadas de Microsoft Teams.

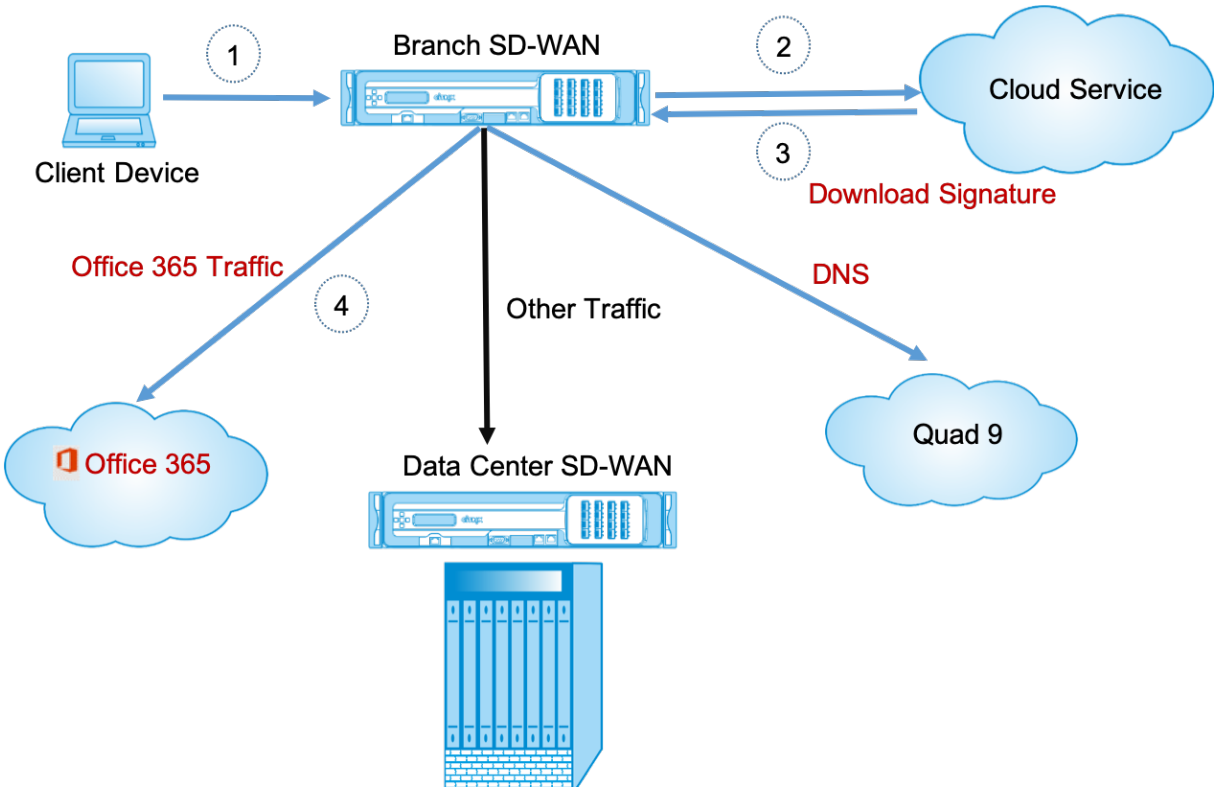
- **Predeterminado**: Estos dispositivos de punto final proporcionan servicios de Office 365 que no requieren ninguna optimización y se pueden tratar como tráfico normal de Internet. Es posible que algunos de estos extremos no estén alojados en centros de datos de Microsoft. El tráfico de esta categoría no es susceptible a variaciones en la latencia. Por lo tanto, la ruptura directa de este tipo de tráfico no causa ninguna mejora en el rendimiento en comparación con la ruptura de Internet. Además, el tráfico de esta categoría no siempre puede ser tráfico de Office 365. Por lo tanto, se recomienda inhabilitar esta opción al habilitar la ruptura de Office 365 en la red.

Cómo funciona la optimización de Office 365

Las firmas de dispositivo de punto final de Microsoft se actualizan como máximo una vez al día. El agente del dispositivo sondea el servicio Citrix (sdwan-app-routing.citrixnetworkapi.net) todos los días para obtener el conjunto más reciente de firmas de punto final. El dispositivo SD-WAN sondea el servicio Citrix (sdwan-app-routing.citrixnetworkapi.net), una vez al día, cuando el dispositivo está encendido. Si hay nuevas firmas disponibles, el dispositivo la descarga y la almacena en la base de datos. Las firmas son esencialmente una lista de direcciones URL e IP utilizadas para detectar tráfico de Office 365 en función de las directivas de dirección de tráfico que se pueden configurar.

> **Nota**
>
> Excepto en la categoría Predeterminado de Office 365, la detección y clasificación de primer paquete del tráfico de Office 365 se realiza de forma predeterminada, independientemente de si la función de ruptura de Office 365 está habilitada o no.

Cuando llega una solicitud para la aplicación de Office 365, el clasificador de aplicaciones realiza una primera búsqueda en la base de datos del clasificador de paquetes, identifica y marca el tráfico de Office 365. Una vez que se clasifica el tráfico de Office 365, las directivas de firewall y ruta de aplicación creadas automáticamente se aplican y descompone el tráfico directamente a Internet. Las solicitudes DNS de Office 365 se reenvían a servicios DNS específicos como Quad9. Para obtener más información, consulte Sistema de nombres de dominio.



Las firmas se descargan desde Cloud Service (sdwan-app-routing.citrixnetworkapi.net).

A partir de Citrix SD-WAN 11.5, puede configurar la conexión de Office 365 mediante Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Optimización de Office 365.

Reenviador transparente para Office 365

La sucursal de Office 365 comienza con una solicitud DNS. La solicitud DNS que pasa por los dominios de Office 365 se debe dirigir localmente. Si la interrupción de Internet de Office 365 está habilitada, se determinan las rutas DNS internas y la lista de reenviadores transparentes se rellena automáticamente. Las solicitudes DNS de Office 365 se reenvían al servicio DNS de código abierto Quad 9 de forma predeterminada. El servicio DNS Quad 9 es seguro, escalable y tiene presencia multipop. Puede cambiar el servicio DNS si es necesario. Los reenviadores transparentes para aplicaciones de Office 365 se crean en todas las sucursales que tienen habilitados el servicio de Internet y la separación de Office 365.

Si está utilizando otro proxy DNS o si SD-WAN está configurado como proxy DNS, la lista de reenviadores se rellena automáticamente con reenviadores para aplicaciones de Office 365.

Consideraciones importantes para la actualización

Optimizar y Permitir categorías

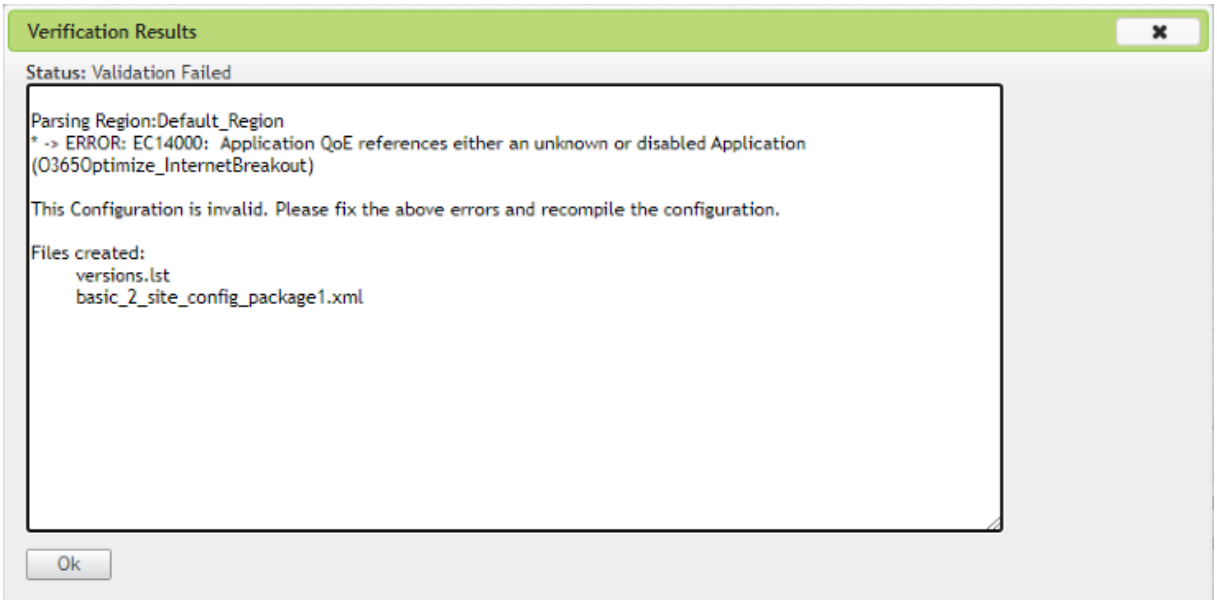
Si ha habilitado la directiva de interrupción de Internet para las categorías **Optimizar** y **Permitir** Office 365, Citrix SD-WAN habilita automáticamente la directiva de interrupción de Internet para las subcategorías correspondientes al actualizar a Citrix SD-WAN 11.4.0.

Cuando se desactualiza a una versión de software anterior a Citrix SD-WAN 11.4.0, debe habilitar manualmente la división de Internet para la categoría **Optimize** o **Permitir** Office 365, independientemente de si ha habilitado las subcategorías correspondientes en la versión 11.4.0 de Citrix SD-WAN 11.4.0 o no.

Objetos de aplicación de Office 365

Si ha creado reglas/rutas utilizando los objetos de aplicación generados automáticamente **O365Optimize_InternetBreakout** y **O365Allow_InternetBreakout**, asegúrese de eliminar las reglas/rutas antes de actualizar a Citrix SD-WAN 11.4.0. Después de la actualización, puede crear reglas/rutas utilizando los nuevos objetos de aplicación correspondientes.

Si continúa con la actualización de Citrix SD-WAN 11.4.0 sin eliminar las reglas/rutas, verá un error y, por lo tanto, la actualización no se realiza correctamente. En el siguiente ejemplo, un usuario ha configurado un perfil de QoE de la aplicación y ve un error al intentar actualizar a Citrix SD-WAN 11.4.0 sin eliminar las reglas/rutas:



> **Nota**
>
> Esta actualización no es necesaria para reglas/rutas creadas automáticamente. Solo se aplica a las reglas/rutas que haya creado.

DNS

Si ha creado reglas de proxy DNS o reglas de reenviador transparente DNS con las aplicaciones **Office 365 Optimize** y **Office 365 Permitir**, asegúrese de eliminar las reglas antes de actualizar a Citrix SD-WAN 11.4.0. Después de la actualización, puede volver a crear las reglas utilizando las nuevas aplicaciones correspondientes.

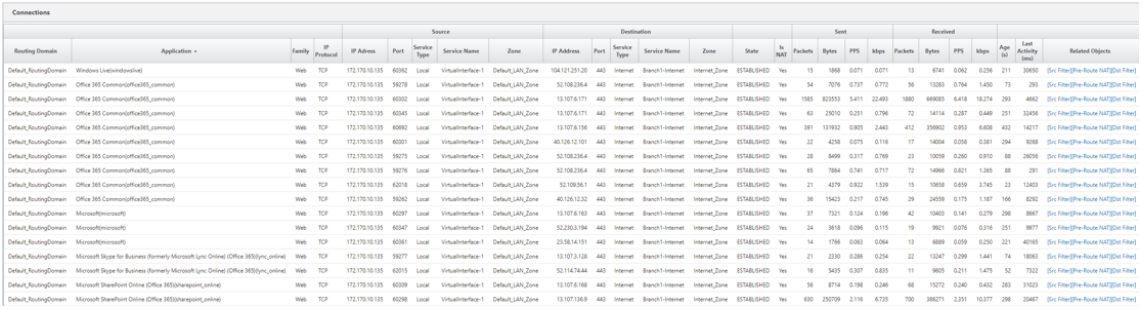
Si continúa con la actualización de Citrix SD-WAN 11.4.0 sin eliminar las antiguas reglas de proxy DNS o reenviador transparente, no verá ningún error y la actualización también se realiza correctamente. Sin embargo, las reglas de proxy DNS y las reglas de reenvío transparente no surten efecto en Citrix SD-WAN 11.4.0.

> **Nota**
>
> Esta actividad no se aplica a las reglas DNS creadas automáticamente. Solo se aplica a las reglas DNS que haya creado.

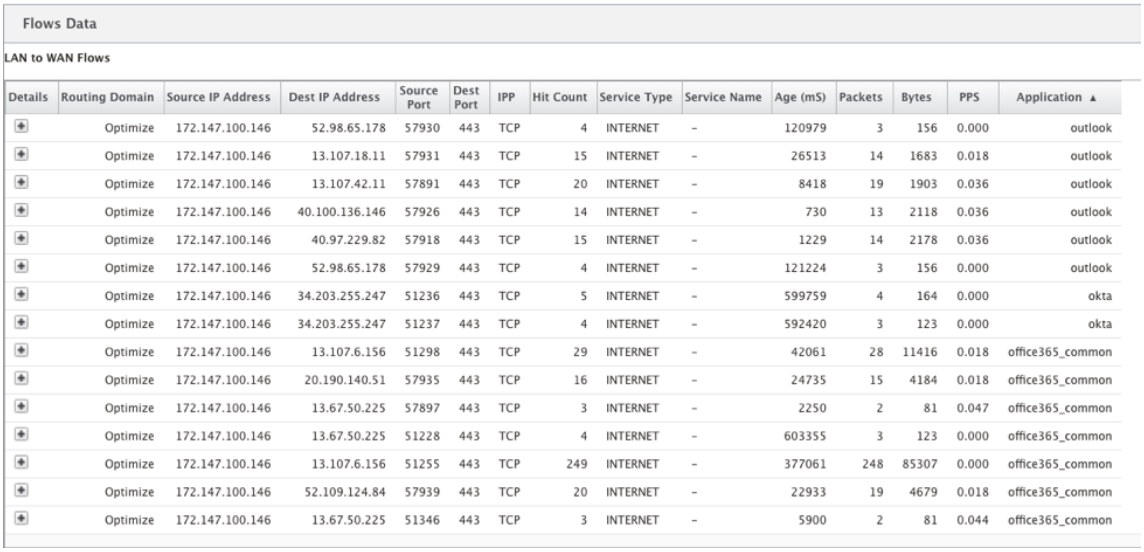
Supervisión

Puede supervisar las estadísticas de la aplicación de office 365 en los siguientes informes estadísticos de SD-WAN:

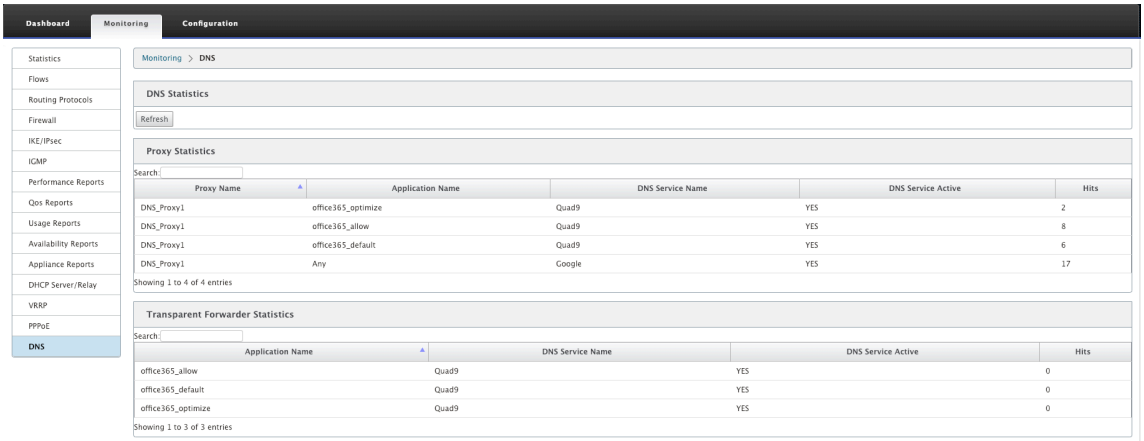
- Estadísticas del firewall



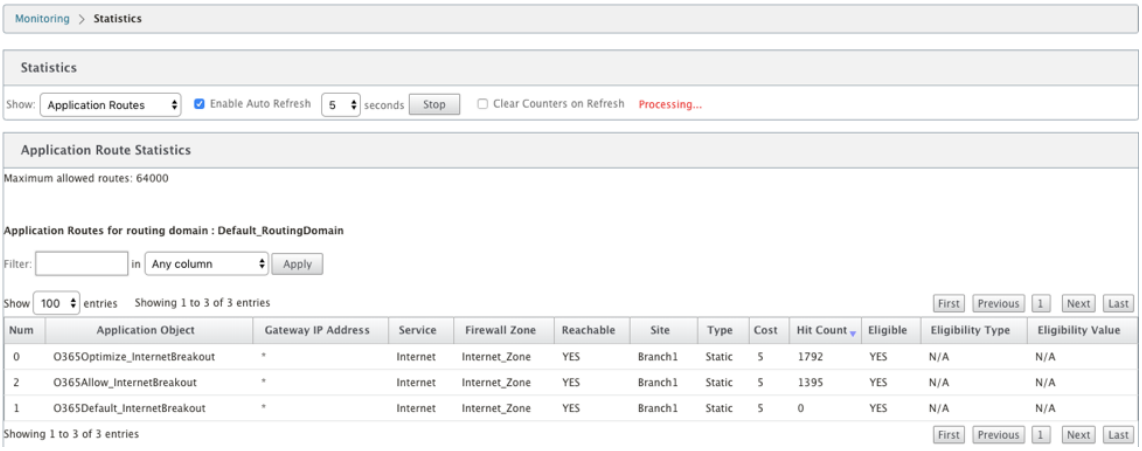
- Flujos



- Estadísticas DNS



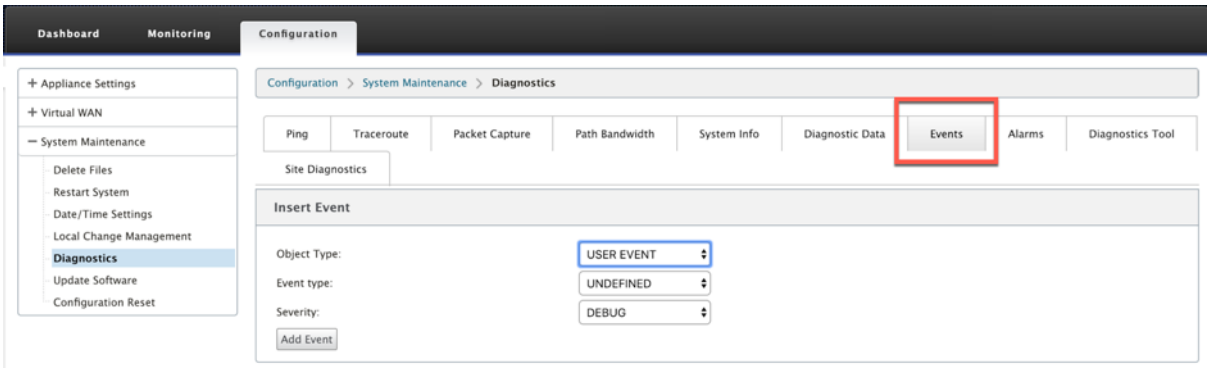
- Estadísticas de ruta de aplicación



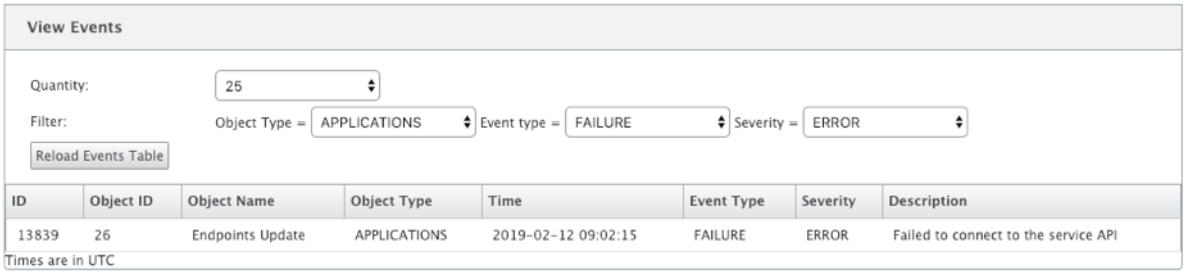
Solución de problemas

Puede ver el error de servicio en la sección **Eventos** del dispositivo SD-WAN.

Para comprobar los errores, vaya a **Configuración > Mantenimiento del sistema > Diagnósticos**, haga clic en la ficha **Eventos**.

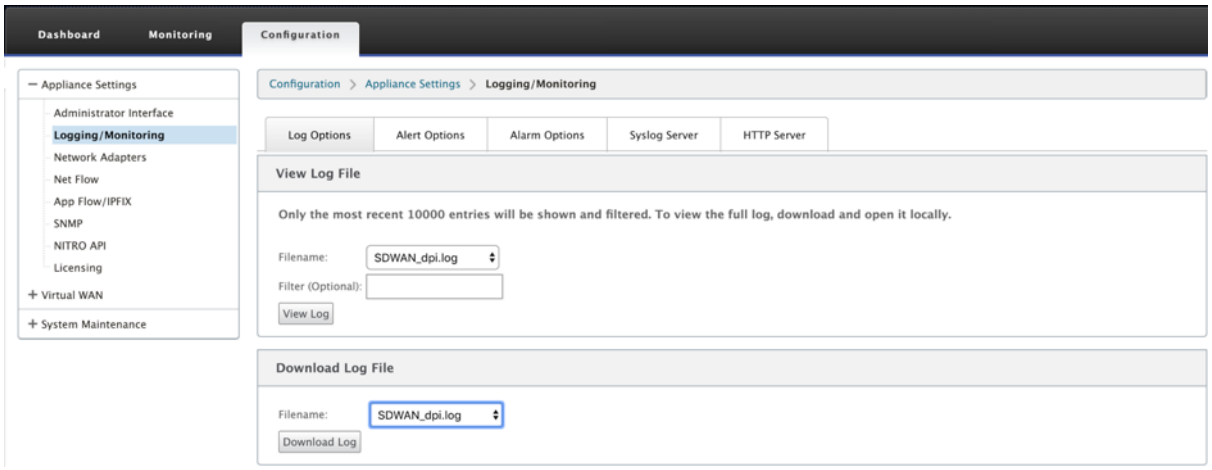


Si hay un problema al conectarse al servicio Citrix (sdwan-app-routing.citrixnetworkapi.net), el mensaje de error se refleja en la tabla **Ver eventos**.



Los errores de conectividad también se registran en **SDWAN_DPI.log**. Para ver el registro, vaya a **Configuración > Configuración del dispositivo > Registro/Supervisión > Opciones de registro**. Seleccione **SDWAN_dpi.log** en la lista desplegable y haga clic en Ver **registro**.

También puede descargar el archivo de registro. Para descargar el archivo de registro, seleccione el archivo de registro necesario en la lista implementable de la sección **Descargar archivo de registro** y haga clic en **Descargar registro**.



Limitaciones

- Si la directiva de interrupción de Office 365 está configurada, no se realiza una inspección profunda de paquetes en las conexiones destinadas a la categoría configurada de direcciones IP.
- La directiva de firewall creada automáticamente y las rutas de aplicación no se pueden modificar.
- La directiva de firewall creada automáticamente tiene la prioridad más baja y no se puede modificar.
- El coste de ruta para la ruta de aplicación creada automáticamente es de cinco. Puede anularlo con una ruta de menor coste.

Servicio de baliza de Office 365

Microsoft proporciona el servicio de indicadores de Office 365 para medir la accesibilidad de Office 365 a través de los vínculos WAN. El servicio de baliza es básicamente una URL - sdwan.measure.office.com/apc/trans.png, que se sondea a intervalos regulares. El sondeo se realiza en cada dispositivo para cada enlace WAN habilitado para Internet. Con cada sondeo, se envía una solicitud HTTP al servicio de baliza y se espera una respuesta HTTP. La respuesta HTTP confirma la disponibilidad y accesibilidad del servicio de Office 365.

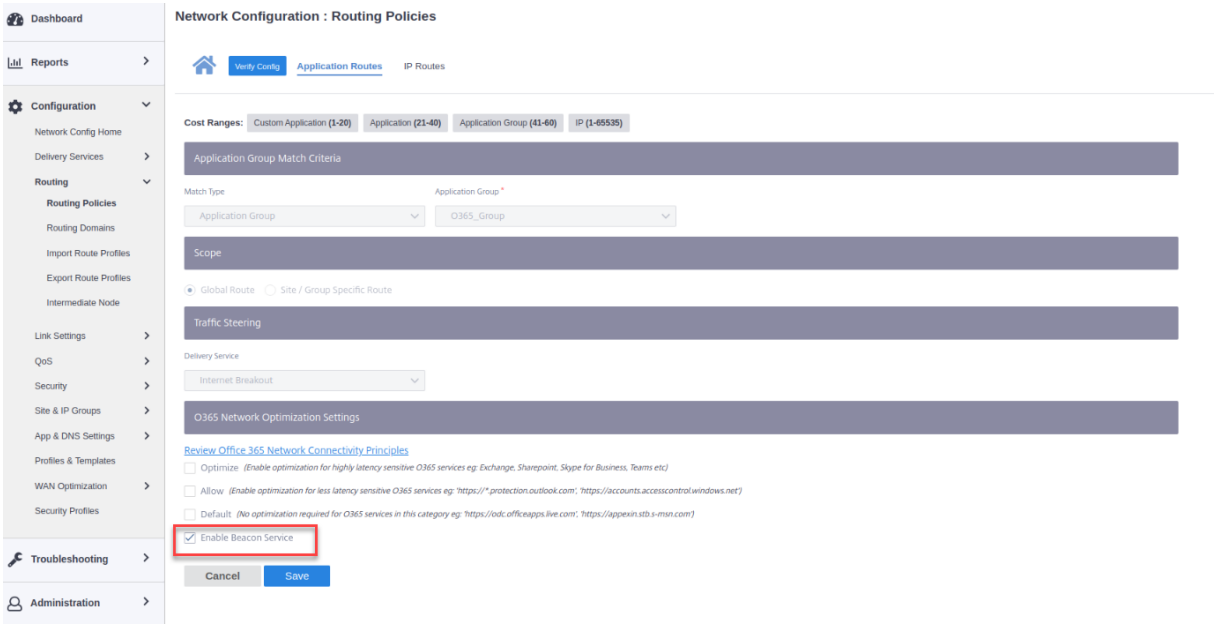
Citrix SD-WAN le permite no solo realizar sondeos de balizas, sino que también determina la latencia para llegar a los extremos de Office 365 a través de cada enlace WAN. La latencia es el tiempo de ida y vuelta que se tarda en enviar una solicitud y obtener una respuesta del servicio de baliza de Office 365 a través de un enlace WAN. Esto permite a los administradores de red ver el informe de latencia del

servicio de balizas y elegir manualmente el mejor vínculo a Internet para la ruptura directa de Office 365. El sondeo de balizas solo se habilita a través de Citrix SD-WAN Orchestrator. De forma predeterminada, el sondeo de balizas está habilitado en todos los vínculos WAN habilitados para Internet cuando se habilita la ruptura de Office 365 a través de Citrix SD-WAN Orchestrator.

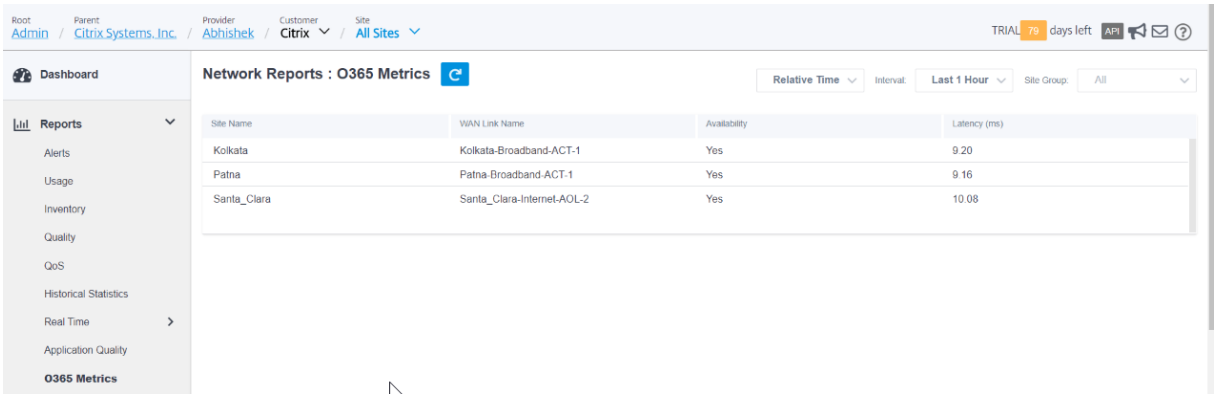
> **Nota**
>
> El sondeo de baliza de Office 365 no está habilitado en vínculos medidos.

Puede optar por inhabilitar el sondeo de balizas de Office 365 y ver informes de latencia en SD-WAN Orchestrator. Para obtener más información, consulte Optimización de Office 365.

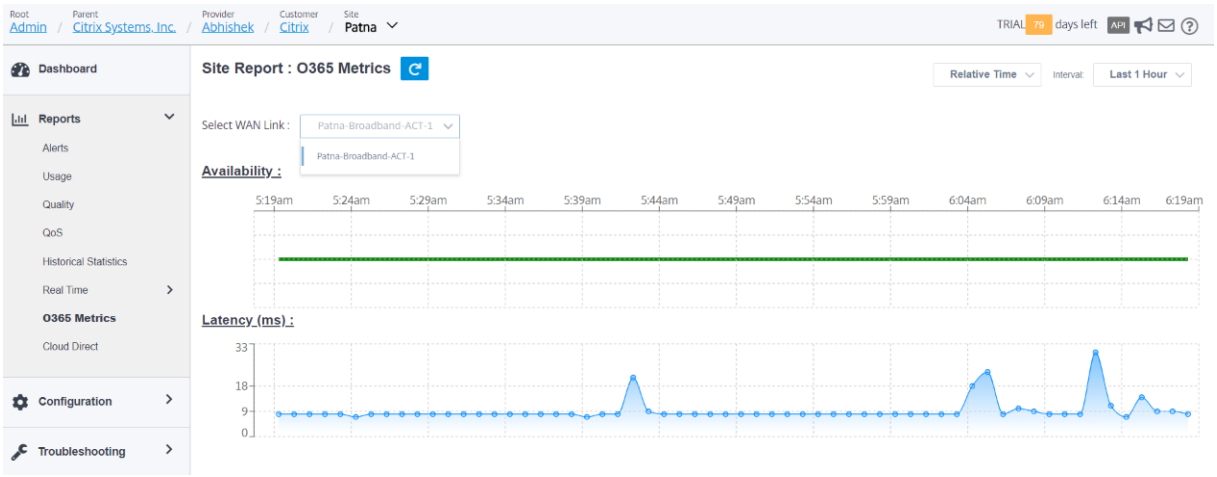
Para inhabilitar el servicio de balizas de Office 365, en SD-WAN Orchestrator, a nivel de red, vaya a **Configuración** > **Redirección** > **Directivas de redirección** > **Configuración de optimización de red de O365** y desactive **Habilitar servicio de balizas**.



Para ver los informes de latencia y disponibilidad de sondeo de indicadores, en Citrix SD-WAN Orchestrator, a nivel de red, vaya a **Informes** > **Métricas de O365**.



Para ver un informe detallado de nivel de sitio del servicio de indicadores, en SD-WAN Orchestrator, en el nivel de sitio vaya a **Informes** > **Métricas de O365**.



Optimización del servicio Citrix Cloud y Gateway

August 26, 2022

Con la mejora de la función de **optimización de Citrix Cloud and Gateway Service**, puede detectar y redirigir el tráfico destinado a Citrix Cloud and Gateway Service. Puede crear directivas para separar el tráfico a Internet directamente o enviarlo a través de una ruta de backhaul a través de una ruta virtual. En ausencia de esta función, cuando la ruta predeterminada es la ruta virtual, el servicio de puerta de enlace pasará al centro de datos del cliente y luego saldrá a Internet agregando latencia innecesaria. Además, ahora obtendrá visibilidad del servicio Citrix Gateway y el tráfico de Citrix Cloud, y puede crear directivas de QoS para priorizarlo sobre la ruta virtual.

La función de interrupción de Citrix Cloud and Gateway Service está habilitada de forma predeterminada en el software Citrix SD-WAN versión 11.2.1 y superior.

Para la versión de software Citrix SD-WAN inferior a 11.3.0, la primera detección y clasificación de paquetes del tráfico de Citrix Cloud y Gateway Service se realiza únicamente si la función de interrupción de Citrix Cloud y Gateway Service no está inhabilitada.

Para el software Citrix SD-WAN versión 11.3.0 y superior, la primera detección y clasificación de paquetes del tráfico de Citrix Cloud y Gateway Service se realiza independientemente de si la función de interrupción de Citrix Cloud y Gateway Service está habilitada o no.

> **Nota**
>
> - Puede configurar la optimización de Citrix Cloud y Gateway Service solo a través de Citrix

> SD-WAN Orchestrator. Para obtener más información, consulte Optimización de Gateway Service.
>
> - La **optimización del tráfico de Citrix SD-WAN Orchestrator** se introduce desde la versión 11.2.3 o posterior del software Citrix SD-WAN. El objetivo es proporcionar una clasificación más detallada y, por lo tanto, identificar por separado el tráfico de Citrix SD-WAN Orchestrator y el tráfico de otros servicios dependientes de Citrix Cloud, y proporcionar una opción de interrupción de Internet. Como resultado, los clientes ahora pueden optar por optimizar solo el tráfico de Citrix SD-WAN Orchestrator.

Categorías de servicios de Citrix Cloud y Gateway

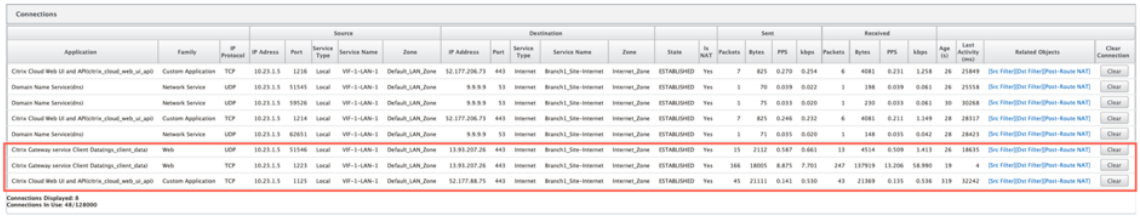
A continuación se presentan las categorías de tráfico utilizadas con fines de clasificación y optimización:

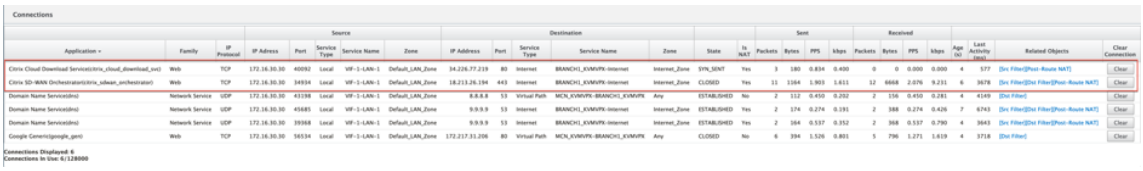
- **Citrix Cloud**: permite detectar y redirigir el tráfico destinado a las API y la interfaz de usuario web de Citrix Cloud.
  - Citrix SD-WAN Orchestrator y servicios críticos dependientes:
    - **Citrix SD-WAN Orchestrator**: permite la interrupción directa de Internet de los latidos cardíacos y de otro tráfico necesario para establecer y mantener la conectividad entre el dispositivo Citrix SD-WAN y Citrix SD-WAN Orchestrator.
    - **Servicio de descarga de Citrix Cloud**: permite la interrupción directa de Internet para descargar el software del dispositivo, la configuración, los scripts, etc. en el dispositivo Citrix SD-WAN.
- **Citrix Gateway Service**: permite detectar y redirigir el tráfico (control y datos) destinado a Citrix Gateway Service.
  - **Datos del cliente de servicio de puerta**de enlace: permite la ruptura directa de Internet de túneles de datos ICA entre clientes y Citrix Gateway Service. Requiere un ancho de banda alto y una latencia baja.
  - **Datos del servidor de servicio de puerta**de enlace: permite la ruptura directa de Internet de los túneles de datos ICA entre los agentes de entrega virtuales (VDA) y el servicio Citrix Gateway. Requiere un ancho de banda alto y una latencia baja y solo es relevante en ubicaciones de recursos de VDA (conexiones de VDA a Citrix Gateway Service).
  - **Tráfico de control de servicio de puerta**de enlace: permite la interrupción directa de Internet del tráfico de control. No hay consideraciones específicas de QoS.
  - **Tráfico de proxy web del servicio de puerta**de enlace: habilita la interrupción directa de Internet del tráfico proxy Web. Requiere un ancho de banda alto, pero los requisitos de latencia pueden variar.

Supervisión

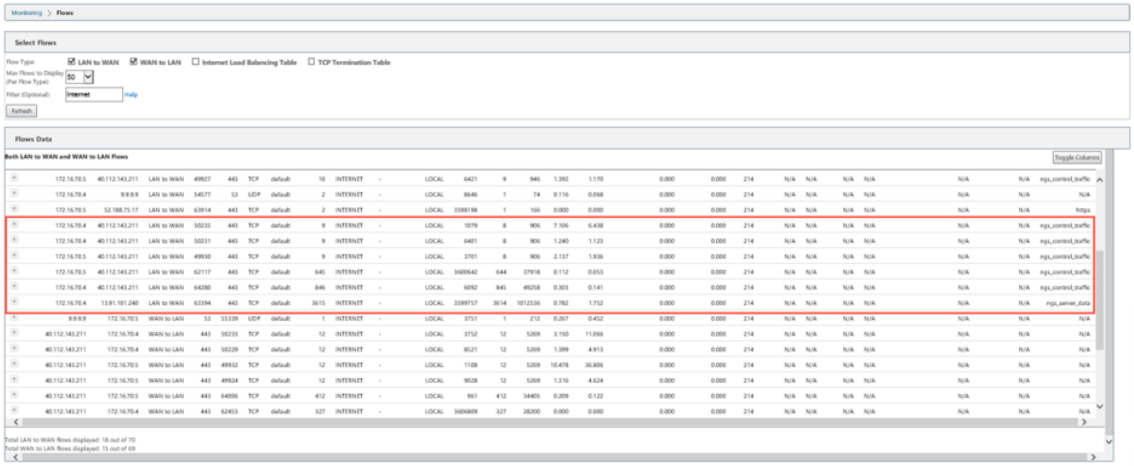
Puede supervisar las estadísticas del servicio de puerta de enlace en los siguientes informes estadísticos de SD-WAN:

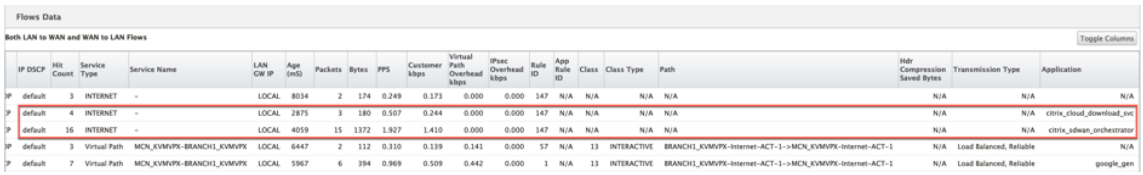
- Estadísticas del firewall



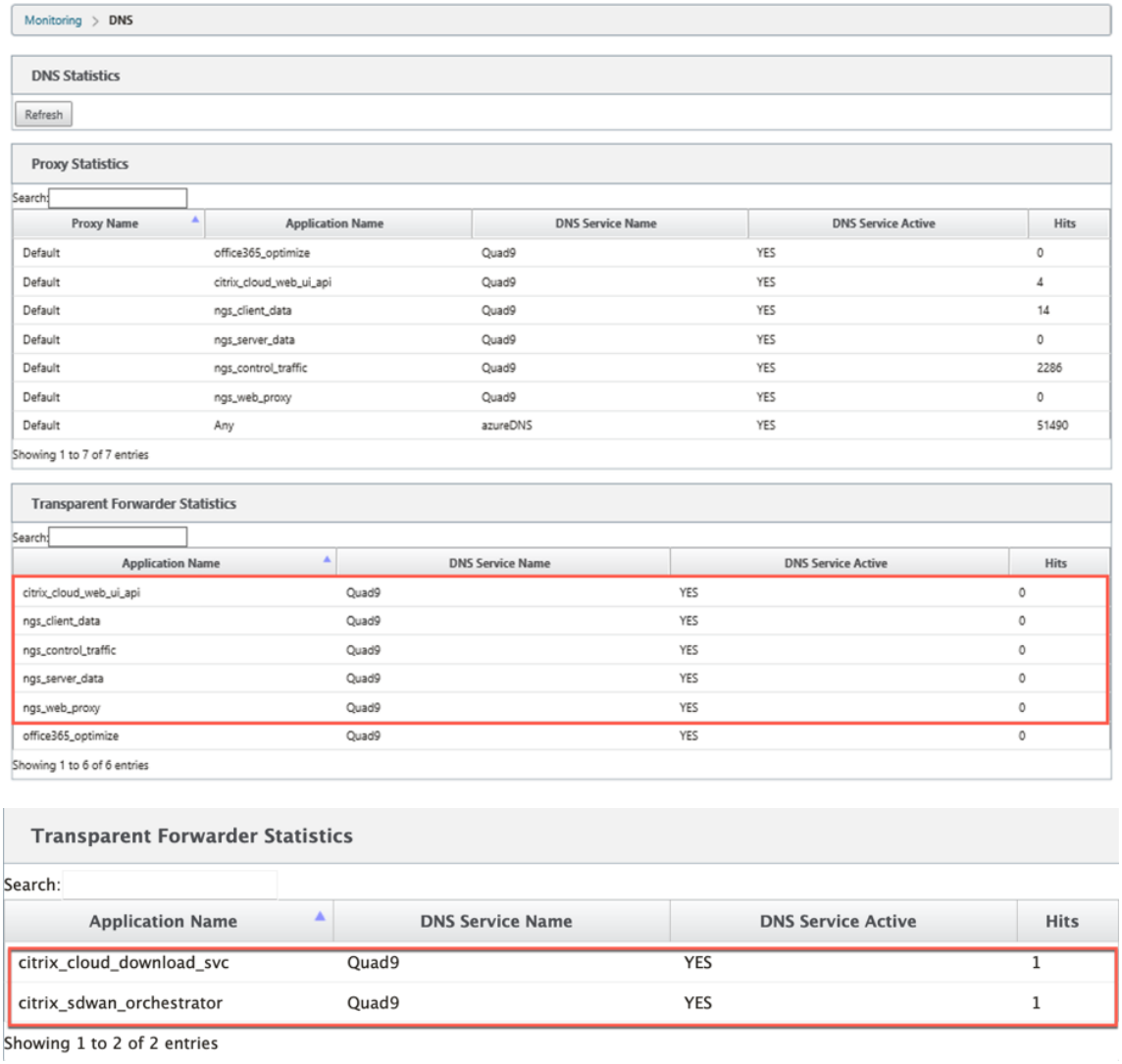


- Flujos

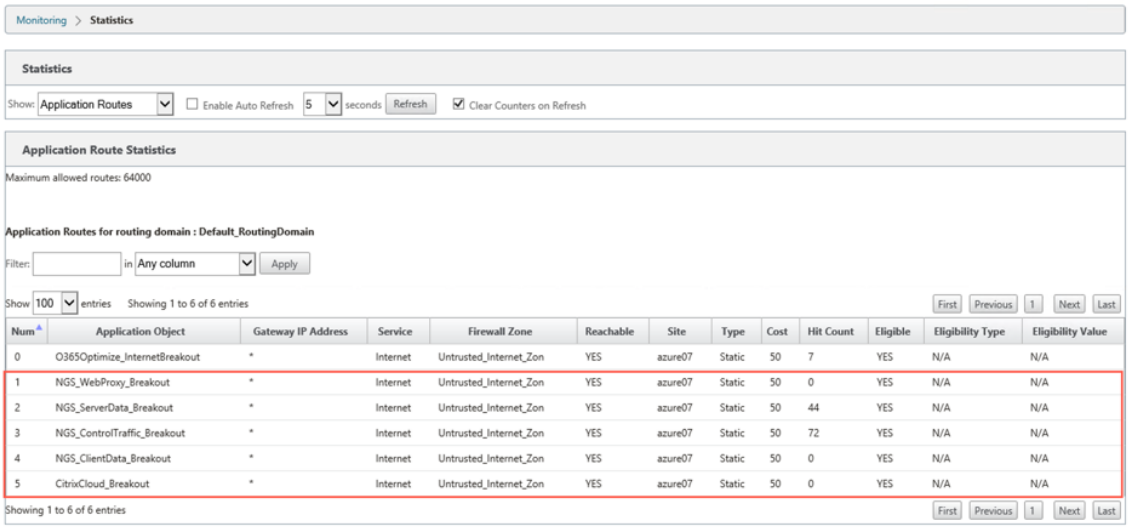


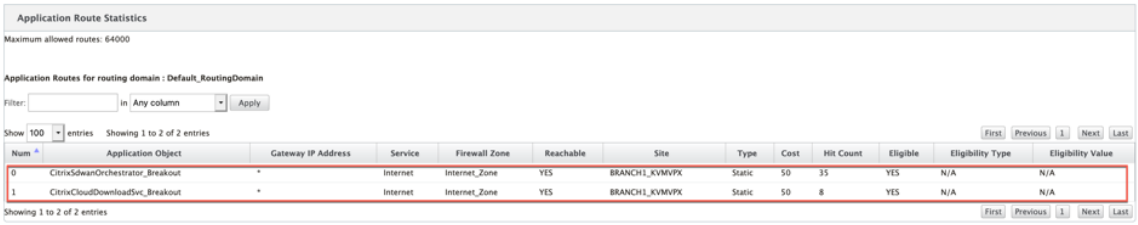


- Estadísticas DNS



- Estadísticas de ruta de aplicación

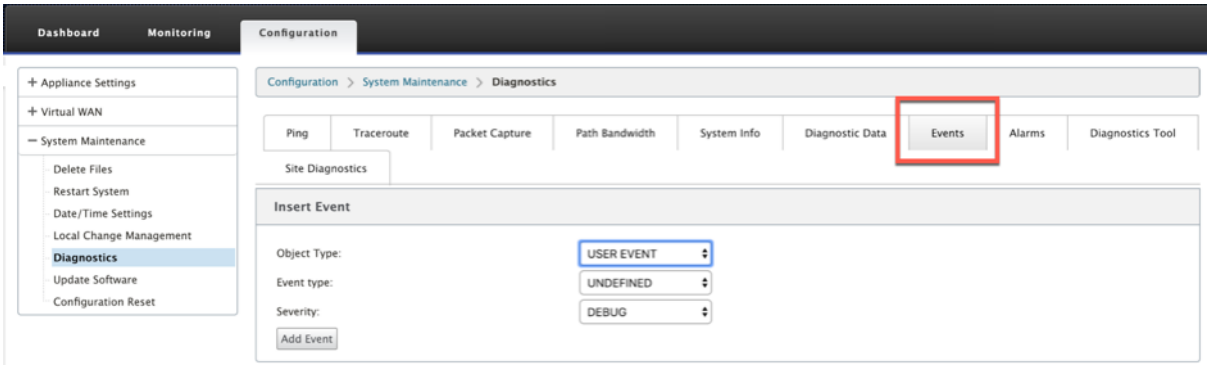




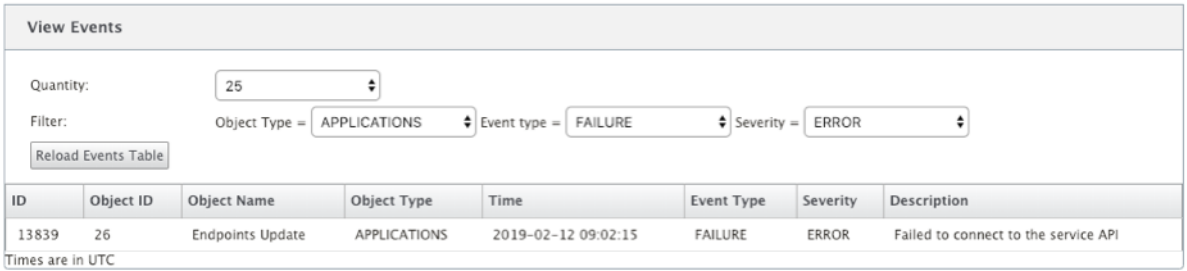
Solución de problemas

Puede ver el error de servicio en la sección **Eventos** del dispositivo SD-WAN.

Para comprobar los errores, vaya a **Configuración > Mantenimiento del sistema > Diagnósticos**, haga clic en la ficha **Eventos**.

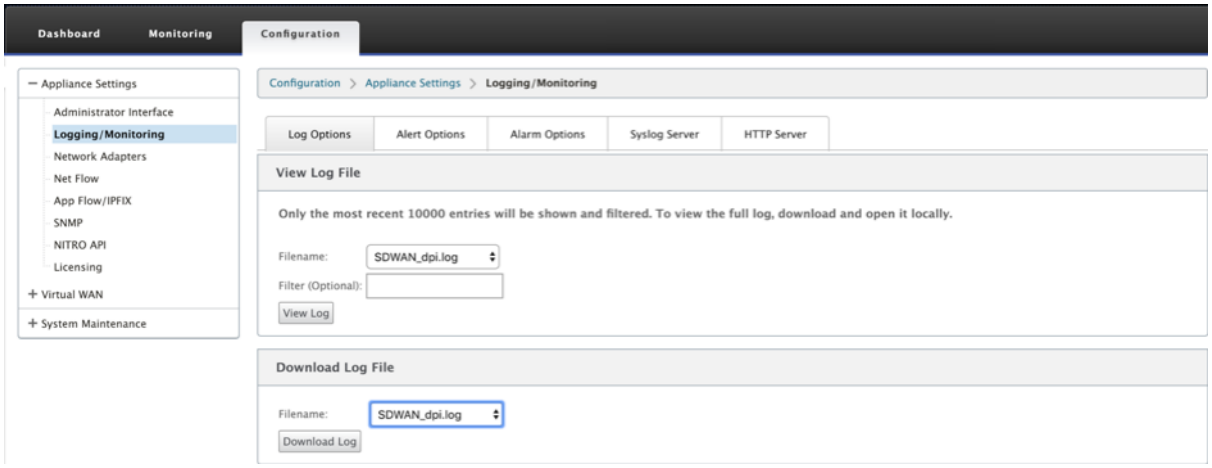


Si hay un problema al conectarse al servicio Citrix (sdwan-app-routing.citrixnetworkapi.net), el mensaje de error se refleja en la tabla **Ver eventos**.



Los errores de conectividad también se registran en **SDWAN_DPI.log**. Para ver el registro, vaya a **Configuración > Configuración del dispositivo > Registro/Supervisión > Opciones de registro**. Seleccione SDWAN_dpi.log en la lista desplegable y haga clic en **Ver registro**.

También puede descargar el archivo de registro. Para descargar el archivo de registro, seleccione el archivo de registro necesario en la lista implementable de la sección **Descargar archivo de registro** y haga clic en **Descargar registro**.



Sesiones PPPoE

August 26, 2022

El Protocolo punto a punto sobre Ethernet (PPPoE) conecta varios usuarios de equipos en una LAN Ethernet a un sitio remoto a través de dispositivos locales comunes del cliente, por ejemplo, Citrix SD-WAN. PPPoE permite a los usuarios compartir una línea de suscriptor digital (DSL) común, un módem por cable o una conexión inalámbrica a Internet. PPPoE combina el Protocolo punto a punto (PPP), comúnmente utilizado en las conexiones de acceso telefónico, con el protocolo Ethernet, que admite varios usuarios en una LAN. La información del protocolo PPP se encapsula dentro de una trama Ethernet.

Los dispositivos Citrix SD-WAN utilizan PPPoE para proporcionar soporte al proveedor de servicios de Internet (ISP) para tener conexiones DSL y módem por cable continuas y continuas, a diferencia de las conexiones de acceso telefónico. PPPoE proporciona cada sesión de sitio remoto de usuario para conocer las direcciones de red de los demás mediante un intercambio inicial denominado "descubrimiento". Después de establecer una sesión entre un usuario individual y el sitio remoto, por ejemplo, un proveedor de ISP, la sesión se puede supervisar. Las empresas utilizan el acceso a Internet compartido a través de líneas DSL mediante Ethernet y PPPoE.

Citrix SD-WAN actúa como un cliente PPPoE. Se autentica con el servidor PPPoE y obtiene una dirección IP dinámica, o utiliza una dirección IP estática para establecer conexiones PPPoE.

Para establecer sesiones PPPoE satisfactorias, se requiere lo siguiente:

- Configure la interfaz de red virtual (VNI).
- Credenciales únicas para crear una sesión PPPoE.
- Configure el enlace WAN. Cada VNI solo puede tener configurado un enlace WAN.

- Configure la dirección IP virtual. Cada sesión obtiene una dirección IP única, dinámica o estática basada en la configuración proporcionada.
- Implemente el dispositivo en modo puente para utilizar PPPoE con dirección IP estática y configure la interfaz como “de confianza”. “
- Se prefiere la IP estática para tener una configuración que obligue a la IP propuesta del servidor; si es diferente de la IP estática configurada, de lo contrario puede producirse un error.
- Implemente el dispositivo como dispositivo perimetral para utilizar PPPoE con IP dinámica y configure la interfaz como “no confiable”. “
- Los protocolos de autenticación soportados son, PAP, CHAP, EAP-MD5, EAP-SRP.
- El número máximo de sesiones múltiples depende del número de VNI configuradas.
- Cree varios VNIs para admitir varias sesiones PPPoE por grupo de interfaz.

> **Nota**:
>
> Se permite crear varias VNI con la misma etiqueta 802.1Q >VLAN.

Limitaciones para la configuración PPPoE:

- No se admite el etiquetado VLAN 802.1q.
- No se admite la autenticación EAP-TLS.
- Compresión de direcciones/controles.
- Compresión desinflada.
- Negociación de compresión de campo de protocolo.
- Protocolo de control de compresión.
- Compresión BSD Compress.
- Protocolos IPX.
- Enlace múltiple PPP.
- Compresión de cabecera TCP/IP estilo Van Jacobson.
- Opción de compresión de ID de conexión en compresión de encabezado TCP/IP estilo Van Jacobson.
- PPPoE no es compatible con interfaces LTE

Desde la versión 11.3.1 de Citrix SD-WAN, se considera un encabezado PPPoE de 8 bytes extra para ajustar el tamaño máximo de segmento (MSS) de TCP. El encabezado PPPoE adicional de 8 bytes ajusta el MSS en los paquetes de sincronización en función de la MTU.

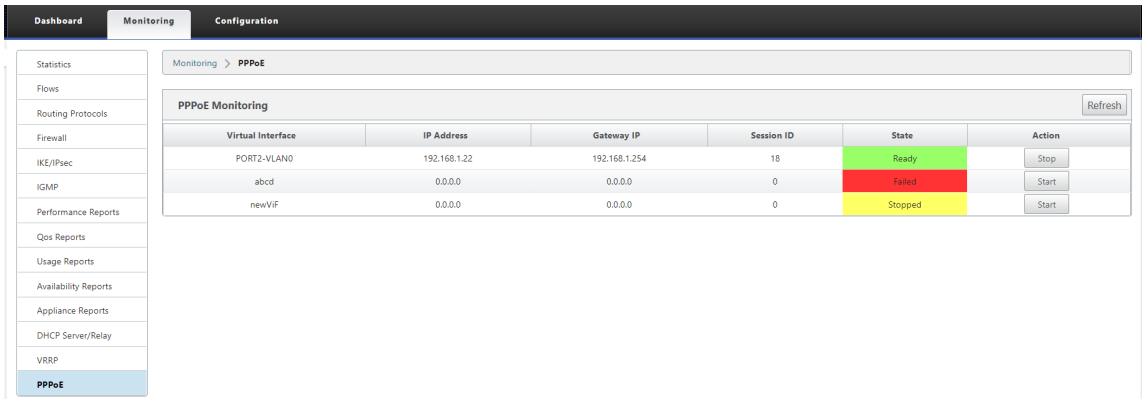
Para obtener información sobre cómo configurar PPPoE a través de Citrix SD-WAN Orchestrator Service, consulte Interfaces.

Supervisar las sesiones PPPoE

Puede supervisar las sesiones PPPoE navegando a la página **Supervisión > PPPoE** en la GUI de SD-WAN.

La página PPPoE proporciona información de estado de las VNI configuradas con el modo de cliente dinámico o estático PPPoE. Le permite iniciar y detener manualmente las sesiones para solucionar problemas desde Citrix SD-WAN Orchestrator Service.

- Si el VNI está activo y listo, las columnas **IP y IP de puerta** de enlace muestran los valores actuales de la sesión. Indica que se trata de valores recibidos recientemente.
- Si el VNI se detiene o se encuentra en estado fallido, los valores son los últimos valores recibidos.



La columna **Estado** muestra el estado de la sesión PPPoE mediante tres códigos de color: Verde, rojo, amarillo y valores. En la tabla siguiente se describen los estados y las descripciones. Puede pasar el mouse por encima de los estados para obtener descripciones.

Tipo de sesión PPPoE	Color	Descripción
Configurado	Amarillo	Un VNI está configurado con PPPoE. Este es un estado inicial.
Marcación	Amarillo	Después de configurar un VNI, el estado de la sesión PPPoE pasa al estado de marcado iniciando el descubrimiento de PPPoE. Se captura la información del paquete.

Tipo de sesión PPPoE	Color	Descripción
Sesión	Amarillo	VNI se mueve del estado de detección al estado de sesión. esperando recibir IP, si es dinámico o esperando confirmación del servidor para la IP anunciada, si es estática.
Listo	verde	Se reciben paquetes IP y el VNI y el enlace WAN asociado están listos para su uso.
Error	rojo	La sesión PPP/PPPoE ha finalizado. El motivo del error puede deberse a una configuración no válida o a un error grave. La sesión intenta volver a conectarse después de 30 segundos.
Detenido	amarillo	La sesión PPP/PPPoE se detiene manualmente.
Terminación	amarillo	Un estado intermedio que termina por un motivo. Este estado se inicia automáticamente después de cierto tiempo (5 segundos para un error normal o 30 segundos para un error grave).
Inhabilitado	amarillo	El servicio SD-WAN está inhabilitado.

Solución de problemas de errores de sesión PPPoE

En la página Supervisión, cuando hay un problema al establecer una sesión PPPoE:

- Al pasar el mouse por encima del estado Error, se muestra el motivo del error reciente.
- Para establecer una nueva sesión o para solucionar problemas de una sesión PPPoE activa, utilice la página Supervisión->PPPoE y reinicie la sesión.
- Si una sesión PPPoE se detiene manualmente, no se puede iniciar hasta que se inicie manualmente y se active un cambio de configuración o se reinicie el servicio.

Una sesión PPPoE puede fallar por los siguientes motivos:

- Cuando SD-WAN no se autentica ante el par debido a un nombre de usuario o contraseña incorrectos en la configuración.
- La negociación PPP falla: la negociación no llega al punto en el que se ejecuta al menos un protocolo de red.
- Problema de memoria del sistema o recursos del sistema.
- Configuración incorrecta o inválida (nombre de CA o nombre de servicio incorrecto).
- Error al abrir el puerto serie debido a un error del sistema operativo.
- No se ha recibido respuesta para los paquetes de eco (el enlace es incorrecto o el servidor no responde).
- Hubo varias sesiones continuas de marcación fallidas en un minuto.

Después de 10 fallas consecutivas, se observa el motivo de la falla.

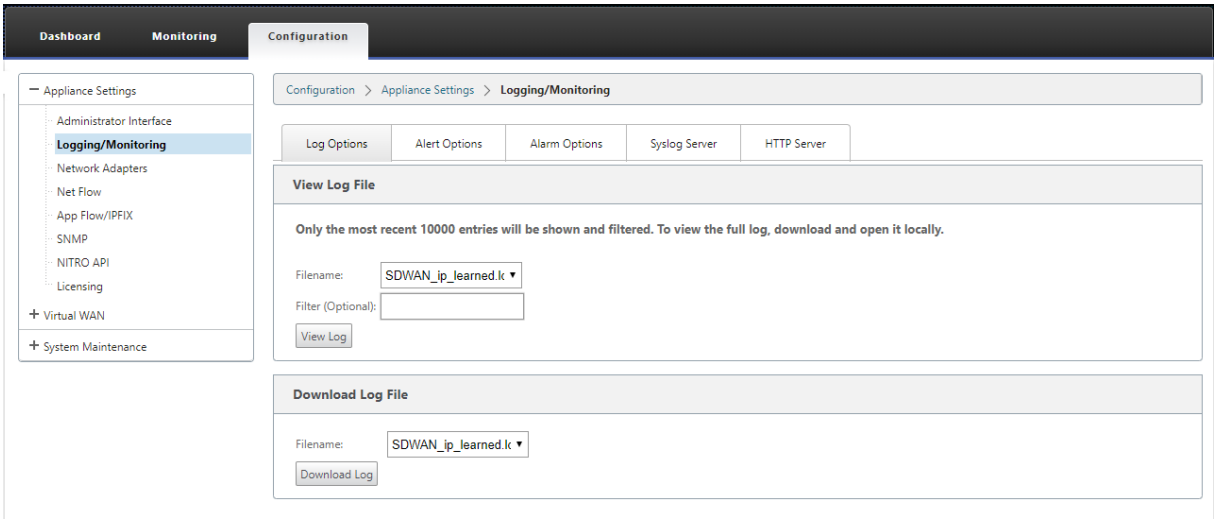
- Si el fallo es normal, se reinicia inmediatamente.
- Si el error es un error, el reinicio se revierte durante 10 segundos.
- Si el error es grave, el reinicio se revierte durante 30 segundos antes de reiniciar.

Los paquetes de solicitud de eco LCP se generan desde SD-WAN cada 60 segundos y si no se reciben 5 respuestas de eco se considera un error de enlace y se restablece la sesión.

Archivo de registro PPPoE

El archivo *SDWAN_ip_learned.log* contiene registros relacionados con PPPoE.

Para ver o descargar el archivo *SDWAN_ip_learned.log* desde la GUI de SD-WAN, vaya a **Configuración del dispositivo** > **Registro/Supervisión** > **Opciones de registro**. Vea o descargue el archivo *SDWAN_IP_Learned.log*.



Calidad del servicio

November 16, 2022

La red entre las oficinas y el centro de datos o la nube debe transportar multitud de aplicaciones y datos, incluidos vídeo de alta calidad o voz en tiempo real. Las aplicaciones sensibles al ancho de banda amplían las capacidades y los recursos de la red. Citrix SD-WAN proporciona servicios de red garantizados, seguros, medibles y predecibles. Esto se logra administrando el retraso, la jitter, el ancho de banda y la pérdida de paquetes en la red.

La solución Citrix SD-WAN incluye un sofisticado motor de calidad de servicio (QoS) de aplicaciones que accede al tráfico de aplicaciones y da prioridad a las aplicaciones críticas. También comprende los requisitos de calidad de la red WAN y selecciona una ruta de red basada en las funciones de calidad en tiempo real.

Los temas de las siguientes secciones tratan las clases de QoS, las reglas de IP, las reglas de QoS de la aplicación y otros componentes necesarios para definir la QoS de la aplicación.

A partir de la versión 11.5 de SD-WAN, las funciones de QoS se pueden configurar a través de Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Calidad de servicio.

Clases

La configuración de Citrix SD-WAN proporciona un conjunto predeterminado de directivas de QoS basadas en aplicaciones e IP/puertos que se aplican a todo el tráfico que pasa por Rutas virtuales. Esta configuración se puede personalizar para adaptarse a las necesidades de implementación.

Las clases son útiles para priorizar el tráfico. Las directivas QoS basadas en aplicaciones e IP/puerto clasifican el tráfico y lo colocan en las clases apropiadas especificadas en la configuración.

El servicio Citrix SD-WAN Orchestrator admite 13 clases. Para obtener más información, consulte Clases.

Los siguientes son los diferentes tipos de clases:

- Tiempo**real**: se utiliza para tráfico de baja latencia, bajo ancho de banda y urgente. Las aplicaciones en tiempo real son sensibles al tiempo, pero realmente no necesitan un ancho de banda alto (por ejemplo, voz sobre IP). Las aplicaciones en tiempo real son sensibles a la latencia y la fluctuación, pero pueden tolerar algunas pérdidas.
- **Interactivo**: se utiliza para el tráfico interactivo con requisitos de latencia bajos a medios y requisitos de ancho de banda de bajo a medio. La interacción suele ser entre un cliente y un servidor. Es posible que la comunicación no necesite un ancho de banda alto, pero es sensible a la pérdida y la latencia.
- **Bulk**: Se utiliza para tráfico de ancho de banda alto y aplicaciones que pueden tolerar una latencia alta. Las aplicaciones que manejan la transferencia de archivos y necesitan un ancho de banda alto se clasifican como clase masiva. Estas aplicaciones implican poca interferencia humana y son manejadas principalmente por los propios sistemas.

Compartir ancho de banda entre clases

Ancho de banda se comparte entre las clases de la siguiente manera:

- En**tiempo real**: Se garantiza que las clases de tráfico en tiempo real tienen baja latencia y el ancho de banda está limitado al recurso compartido de clase cuando hay tráfico competidor.
- **Interactivo**: El tráfico que llega a las clases interactivas obtiene ancho de banda restante después de servir tráfico en tiempo real y el ancho de banda disponible se comparte equitativamente entre las clases interactivas.
- **Bulk**: Bulk es el mejor esfuerzo. El ancho de banda que queda después de servir tráfico interactivo y en tiempo real se da a las clases masivas sobre una base justa. El tráfico masivo puede morir de hambre si el tráfico en tiempo real e interactivo utiliza todo el ancho de banda disponible.

> **Nota**
>
> Cualquier clase puede usar todo el ancho de banda disponible cuando no hay contención.

En el siguiente ejemplo se explica la distribución del ancho de banda basada en la configuración de clase:

Considere que hay un ancho de banda agregado de 10 Mbps a través de Ruta Virtual. Si la configuración de clase es

- Tiempo real: 30%
- Alta interactiva: 40%
- Medio interactivo: 20%
- Baja interactiva: 10%
- Granel: 100%

La distribución del ancho de banda es:

- El tráfico en tiempo real obtiene el 30% de 10 Mbps (3 Mbps) según la necesidad. Si necesita menos del 10%, el resto del ancho de banda se pone a disposición de las demás clases.
- Las clases interactivas comparten el ancho de banda restante de forma equitativa (4 Mbps: 2 Mbps: 1 Mbps).
- Todo lo que quede cuando el tráfico interactivo en tiempo real no utiliza completamente sus recursos compartidos se entrega a la clase Bulk.

Reglas por dirección IP y número de puerto

La función Reglas por dirección IP y número de puerto le ayuda a crear reglas para su red y tomar determinadas decisiones de calidad de servicio (QoS) basadas en las reglas. Puede crear reglas personalizadas para su red. Por ejemplo, puede crear una regla como: si la dirección IP de origen es 172.186.30.74 y la dirección IP de destino es 172.186.10.89, establezca el **modo de transmisión** como Ruta persistente y **LAN en Clase WAN** como 10 (realtime_class)".

Puede crear reglas localmente a nivel de sitio o global. Si más de un sitio requiere la misma regla, puede crear una plantilla para reglas globalmente en **Global > Juegos predeterminados de ruta virtual > Reglas**. La plantilla se puede adjuntar a los sitios donde se deben aplicar las reglas. Incluso si un sitio está asociado a la plantilla de regla creada globalmente, puede crear reglas específicas del sitio. En tales casos, las reglas específicas del sitio tienen prioridad y anulan la plantilla de regla creada globalmente.

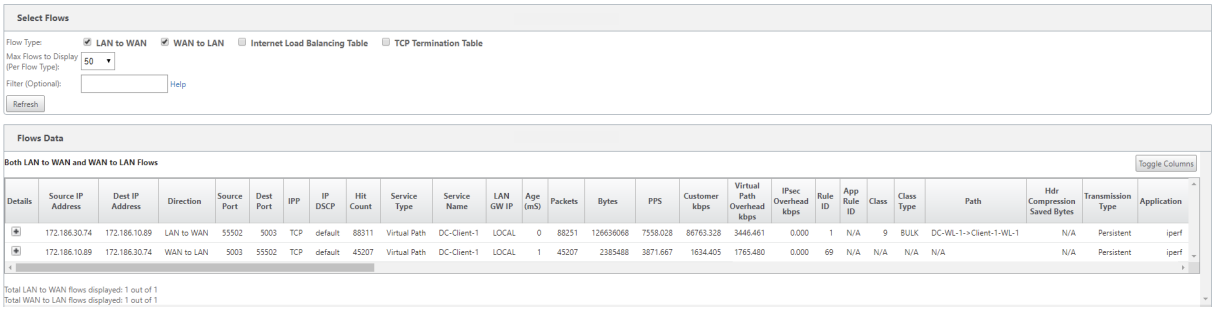
A partir de la versión 11.5 de Citrix SD-WAN, puede crear reglas IP mediante Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Reglas de IP.

Verificar reglas

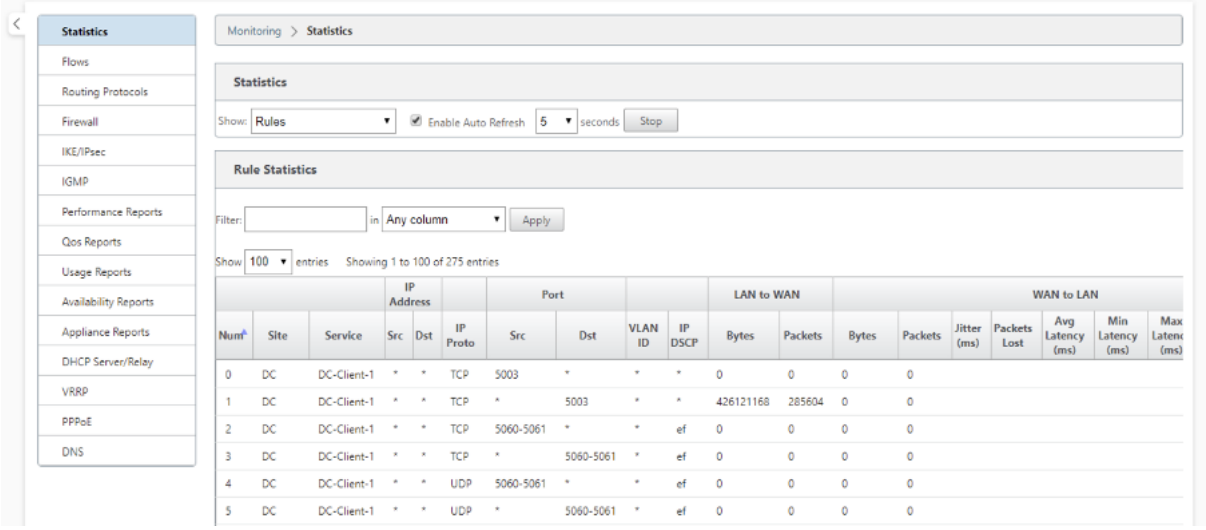
Vaya a **Supervisión > Flujos**. Seleccione el campo **Tipo de Flujo** ubicado en la sección **Seleccionar Flujos** en la parte superior de la página **Flujos**. Junto al campo **Tipo de flujo** hay una fila de casillas

de verificación para seleccionar la información de flujo que quiere ver. Compruebe si la información de flujo se ajusta a las reglas configuradas.

Ejemplo:
La regla "Si la dirección IP de origen es 172.186.30.74 y la dirección IP de destino es 172.186.10.89, establezca el **modo de transmisión** como Ruta persistente"muestra los siguientes **datos de flujos**.



Vaya a **Supervisión > Estadísticas** y verifique las reglas configuradas.



Reglas por nombre de aplicación

La función de clasificación de aplicaciones permite que el dispositivo Citrix SD-WAN analice el tráfico entrante y lo clasifique como perteneciente a una aplicación o familia de aplicaciones concretas. Esta clasificación nos permite mejorar la calidad de servicio de aplicaciones individuales o familias de aplicaciones mediante la creación y aplicación de reglas de aplicación.

Puede filtrar los flujos de tráfico según los tipos de coincidencia de aplicaciones, familias de aplicaciones o objetos de aplicación y aplicarles reglas de aplicación. Las reglas de aplicación son similares a las reglas de protocolo de Internet (IP). Para obtener información sobre las reglas IP, consulte Reglas por dirección IP y número de puerto.

Para cada regla de aplicación, puede especificar el modo de transmisión. Los siguientes son los modos de transmisión disponibles:

- **Ruta de equilibrio de carga**: El tráfico de aplicaciones para el flujo se equilibra en varias rutas. El tráfico se envía a través de la mejor ruta hasta que se utiliza esa ruta. Los paquetes restantes se envían a través de la siguiente mejor ruta.
- **Ruta persistente**: El tráfico de aplicaciones permanece en la misma ruta hasta que la ruta deja de estar disponible.
- **Ruta de acceso duplicada**: El tráfico de aplicaciones se duplica en múltiples paths, lo que aumenta la fiabilidad.

Las reglas de aplicación están asociadas a clases. Para obtener información sobre las clases, consulte Personalización de clases.

De forma predeterminada, las siguientes cinco reglas de aplicación predefinidas están disponibles para las aplicaciones Citrix ICA:

Rule	Class	Modo de transmisión	Retransmisión de paquetes perdidos	Habilitar agregación de paquetes	Habilitar la resecuenciación de paquetes	Tiempo de espera de resecuencia (ms)	Descartar paquetes de resecuenciación tardía	Límite de caída (ms)	Profundidad de caída (bytes)	Habilitar RED	Inhabilitar límite (ms)	Inhabilitar profundidad (bytes)
HDX_Priority_0 (HDX_priority_tag_0)	0	Ruta de equilibrio de carga	True	False	True	250	True	350	30000	True	0	128000
HDX_Priority_1 (HDX_priority_tag_1)	1	Ruta de equilibrio de carga	True	False	True	250	True	350	30000	True	0	128000

Rule	Class	Modo de transmisión	Retransmisión de paquetes perdidos	Habilitar agregación de paquetes	Habilitar la resecuenciación de paquetes	Tiempo de espera de resecuencia (ms)	Descartar paquetes de resecuenciación tardía	Límite de caída (ms)	Profundidad de caída (bytes)	Habilitar RED	Inhabilitar límite (ms)	Inhabilitar profundidad (bytes)
HDX_Priority_2	2 (HDX_priority_tag_2)	Ruta de equilibrio de carga	True	False	True	250	True	350	30000	True	0	128000
HDX_Priority_3	3 (HDX_priority_tag_3)	Ruta de equilibrio de carga	True	False	True	250	True	350	30000	True	0	128000
HDX	11 (interactive_high_class)	Ruta de equilibrio de carga	True	False	True	250	True	350	30000	True	0	128000

¿Cómo se aplican las reglas de aplicación?

En la red SD-WAN, cuando los paquetes entrantes llegan al dispositivo SD-WAN, los pocos paquetes iniciales no se clasifican por PPP. En este punto, los atributos de reglas IP como Clase, Terminación TCP se aplican a los paquetes. Tras la clasificación de PPP, los atributos de regla de aplicación, como Clase, modo de transmisión, anulan los atributos de la regla IP.

Las reglas IP tienen más atributos en comparación con las reglas de aplicación. La regla de aplicación

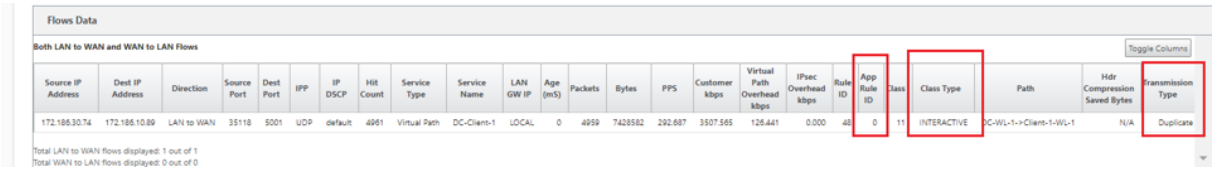
anula solo unos cuantos atributos de reglas IP, el resto de los atributos de reglas IP permanecen procesados en los paquetes.

Por ejemplo, supongamos que ha especificado una regla de aplicación para una aplicación de correo web, como Google Mail, que utiliza el protocolo SMTP. El conjunto de reglas IP para el protocolo SMTP se aplica inicialmente antes de la clasificación PPP. Después de analizar los paquetes y clasificarlos como pertenecientes a la aplicación Google Mail, se aplica la regla de aplicación especificada para la aplicación Google Mail.

Para crear reglas de aplicación mediante Citrix SD-WAN Orchestrator, consulte Reglas de aplicación.

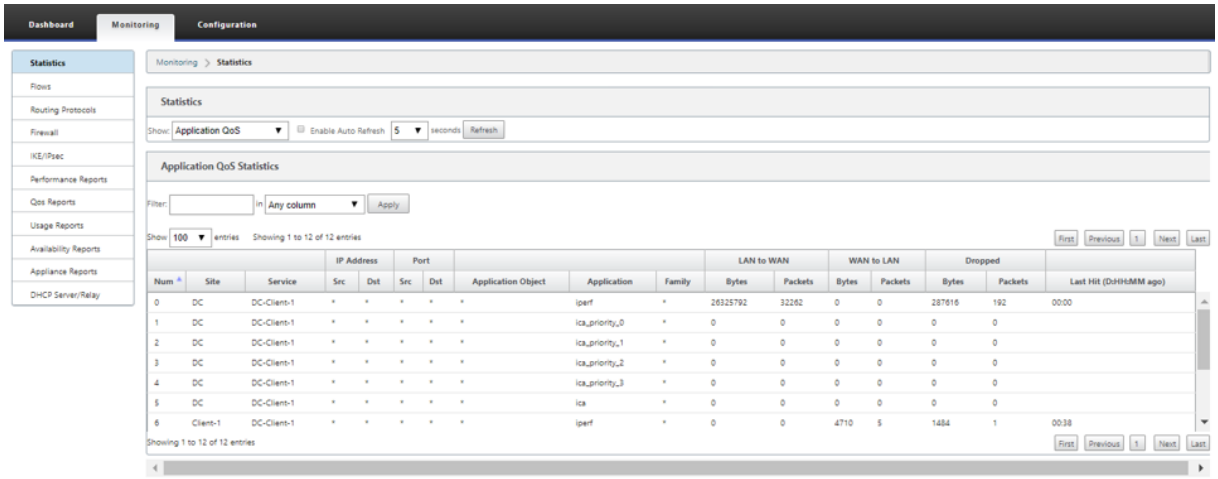
Para confirmar si las reglas de aplicación se aplican al flujo de tráfico, vaya a **Supervisión** > **Flujos**.

Anote el ID de la regla de la aplicación y compruebe si el tipo de clase y el modo de transmisión son según la configuración de la regla.



Puede supervisar la QoS de la aplicación, como el número de paquetes/bytes cargados, descargados o descartados en cada sitio, navegando a **Supervisión** > **Estadísticas** > **QoS de aplicaciones**.

El parámetro **Num** indica el id de regla de la aplicación. Compruebe el ID de regla de aplicación obtenido del flujo.



Creación de aplicaciones personalizadas

Puede utilizar objetos de aplicación para definir aplicaciones personalizadas en función de los siguientes tipos de coincidencia:

- Protocolo IP

- Nombre de la aplicación
- Familia de aplicaciones

El clasificador de PPP analiza los paquetes entrantes y los clasifica como aplicaciones según los criterios de coincidencia especificados. Puede utilizar estas aplicaciones personalizadas clasificadas en QoS, firewall y redirección de aplicaciones.

> **Sugerencia**
>
> Puede especificar uno o varios tipos de coincidencia.

Clasificación de aplicaciones

Los dispositivos Citrix SD-WAN realizan una inspección profunda de paquetes (PPP) para identificar y clasificar aplicaciones mediante las siguientes técnicas:

- Clasificación de bibliotecas de PPP
- Clasificación de arquitectura informática independiente (ICA) propiedad de Citrix
- API de proveedores de aplicaciones (por ejemplo, API de REST de Microsoft para Office 365)
- Clasificación de aplicaciones basada en nombres de dominio

Clasificación de bibliotecas de PPP

La biblioteca Deep Packet Inspection (PPP) reconoce miles de aplicaciones comerciales. Permite el descubrimiento y la clasificación de aplicaciones en tiempo real. Mediante la tecnología PPP, el dispositivo SD-WAN analiza los paquetes entrantes y clasifica el tráfico como perteneciente a una aplicación o familia de aplicaciones en particular. La clasificación de aplicaciones para cada conexión requiere algunos paquetes.

Para habilitar la clasificación de bibliotecas de PPP en Citrix SD-WAN Orchestrator Service, consulte Clasificación de bibliotecas de PPP.

Clasificación ICA

Los dispositivos Citrix SD-WAN también pueden identificar y clasificar el tráfico de Citrix HDX para aplicaciones virtuales y escritorios. Citrix SD-WAN reconoce las siguientes variaciones del protocolo ICA:

- ICA
- ICA-CGP
- ICA de flujo único (SSI)
- ICA multisecuencia (MSI)

- ICA a través de TCP
- ICA sobre UDP/EDT
- ICA a través de puertos no estándar (incluida ICA multipuerto)
- Transporte adaptable HDX
- ICA sobre WebSocket (usado por HTML5 Receiver)

> **Nota**
>
> La clasificación del tráfico ICA entregado a través de SSL/TLS o DTLS no se admite en SD-WAN Standard Edition.
>
> La clasificación del tráfico de red se realiza durante las conexiones iniciales o el establecimiento del flujo. Por lo tanto, las conexiones preexistentes no se clasifican como ICA. La clasificación de las conexiones también se pierde cuando la tabla de conexiones se borra manualmente.
>
> El tráfico Framehawk y Audio-over-UDP/RTP no se clasifican como aplicaciones HDX. Se informan como "UDP"o "Protocolo desconocido".
>
> Desde la publicación 10, versión 1, el dispositivo SD-WAN puede diferenciar cada flujo de datos ICA en ICA multisecuencia, incluso en una configuración de puerto único. Cada secuencia ICA se clasifica como una aplicación independiente con su propia clase QoS predeterminada para la priorización.
>
> - Para que la funcionalidad ICA Multi-Stream funcione correctamente, debe tener SD-WAN Standard Edition 10.1 o posterior.
> - Para que los informes basados en usuarios de HDX se muestren en SDWAN-Center, debe tener SD-WAN Standard Edition 11.0 o posterior.
>
> Requisitos mínimos de software para el canal virtual de información HDX:
>
> - Versión actual de Citrix Virtual Apps and Desktops (anteriormente XenApp y XenDesktop), ya que la funcionalidad necesaria se introdujo en XenApp y XenDesktop 7.17 y no está incluida en la versión 7.15 de servicio a largo plazo.
> - Versión de la aplicación Citrix Workspace (o de su predecesora, Citrix Receiver) que admite ICA multi-stream y el canal virtual de información HDX Insights, CTXNSAP. Busque **HDX Insight con NSAP VC** y ICA multipuerto/multisecuencia en la tabla de funciones de la aplicación Citrix Workspace. Consulte las versiones de lanzamiento compatibles actualmente en HDX Insights.
> - A partir de la versión 11.2, la duplicación de paquetes ahora está habilitada de forma predeterminada para el tráfico HDX en tiempo real cuando se usa ICA multisecuencia.

Una vez clasificada, la aplicación ICA se puede utilizar en reglas de aplicación y para ver estadísticas de aplicación similares a otras aplicaciones clasificadas.

Hay cinco reglas de aplicación predeterminadas para las aplicaciones ICA, una cada una para las siguientes etiquetas de prioridad:

- Arquitectura informática independiente (Citrix) (ICA)
- ICA en tiempo real (ica_priority_0)
- ICA interactiva (ica_priority_1)
- Transferencia masiva ICA (ica_prority_2)
- Fondo ICA (ica_priority_3)

Para obtener más información, consulte Reglas por nombre de aplicación

Si está ejecutando una combinación de software que no admite Multi-Stream ICA en un solo puerto, entonces para realizar QoS debe configurar varios puertos, uno para cada secuencia ICA.
Para clasificar HDX en puertos no estándar tal y como se configura en la directiva de servidor XA/XD, debe agregar esos puertos en configuraciones de puertos ICA. Además, para hacer coincidir el tráfico en esos puertos con las reglas IP válidas, debe actualizar las reglas IP de ICA.

En la lista IP y puertos ICA puede especificar puertos no estándar utilizados en la directiva XA/XD para procesar la clasificación HDX. La dirección IP se utiliza para restringir aún más los puertos a un destino específico. Use "*"para el puerto destinado a cualquier dirección IP. La dirección IP con combinación de puerto SSL también se utiliza para indicar que el tráfico es probable ICA aunque el tráfico no se clasifique finalmente como ICA. Esta indicación se utiliza para enviar registros L4 AppFlow para admitir informes de saltos múltiples en Citrix Application Delivery Management.

Para habilitar la clasificación basada en ICA en Citrix SD-WAN Orchestrator Service, consulte Clasificación ICA.

Clasificación basada en API de proveedores de aplicaciones

Citrix SD-WAN admite la siguiente clasificación basada en API de proveedor de aplicaciones:

- Office 365. Para obtener más información, consulte Optimización de Office 365.
- Servicio Citrix Cloud y Citrix Gateway. Para obtener más información, consulte Optimización de Gateway Service.

Clasificación de aplicaciones basada en nombres de dominio

El motor de clasificación de PPP se ha mejorado para clasificar las aplicaciones en función del nombre de dominio y los patrones. Después de que el reenviador de DNS intercepta y analiza las solicitudes de DNS, el motor PPP utiliza el clasificador de IP para realizar la primera clasificación de paquetes. Se realizan más bibliotecas de PPP y clasificación ICA y se anexa el ID de aplicación basado en nombres de dominio.

La función de aplicación basada en nombres de dominio permite agrupar varios nombres de dominio y tratarlos como una única aplicación. Facilita la aplicación de firewall, dirección de aplicaciones, QoS y otras reglas. Se pueden configurar un máximo de 64 aplicaciones basadas en nombres de dominio.

Para definir aplicaciones basadas en nombres de dominio en Citrix SD-WAN Orchestrator Service, consulte Clasificación de aplicaciones basadas en nombres de dominio.

> **Nota**
>
> - A partir de la versión 11.4.2, las aplicaciones basadas en nombres de dominio admiten puertos y protocolos configurables en Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Dominios y aplicaciones.
> - A partir de la versión 11.5.0 de Citrix SD-WAN, los registros AAAA son compatibles con Citrix SD-WAN Orchestrator Service.

Limitaciones

- Si no hay solicitud/respuesta DNS correspondiente a una aplicación basada en nombres de dominio, el motor PPP no clasifica la aplicación basada en nombres de dominio y, por lo tanto, no aplica las reglas de aplicación correspondientes a la aplicación basada en nombres de dominio.
- Si se crea un objeto de aplicación de forma que el intervalo de puertos incluya el puerto 80 y/o el puerto 443, con un tipo de coincidencia de dirección IP específico que corresponde a una aplicación basada en nombres de dominio, el motor PPP no clasifica la aplicación basada en nombres de dominio.
- Si se configuran proxies web explícitos, debe agregar todos los patrones de nombres de dominio al archivo PAC, para asegurarse de que la respuesta DNS no siempre devuelve la misma dirección IP.
- Las clasificaciones de aplicaciones basadas en nombres de dominio se restablecen al actualizar la configuración. La reclasificación se realiza en función de las técnicas de clasificación de versiones anteriores a 11.0.2, como la clasificación de bibliotecas PPP, la clasificación ICA y la clasificación basada en API de aplicaciones de proveedores.
- Las firmas de aplicación aprendidas (direcciones IP de destino) por clasificación de aplicaciones basada en nombre de dominio se restablecen al actualizar la configuración.
- Solo se procesan las consultas DNS estándar y sus respuestas.
- Los registros de respuesta DNS divididos en varios paquetes no se procesan. Solo se procesan las respuestas DNS de un solo paquete.
- No se admite DNS a través de TCP.
- Solo los dominios de nivel superior se admiten como patrones de nombres de dominio.

Clasificación del tráfico cifrado

El dispositivo Citrix SD-WAN detecta e informa sobre el tráfico cifrado, como parte de los informes de aplicaciones, mediante los dos métodos siguientes:

- Para el tráfico HTTPS, el motor de PPP inspecciona el certificado SSL para leer el nombre común, que lleva el nombre del servicio (por ejemplo, Facebook, Twitter). Según la arquitectura de la aplicación, solo se puede usar un certificado para varios tipos de servicio (por ejemplo, correo electrónico, noticias, etc.). Si diferentes servicios usan certificados diferentes, el motor de PPP podría diferenciar entre servicios.
- Para las aplicaciones que utilizan su propio protocolo de cifrado, el motor PPP busca patrones binarios en los flujos; por ejemplo, en el caso de Skype, el motor PPP busca un patrón binario dentro del certificado y determina la aplicación.

Objetos de aplicación

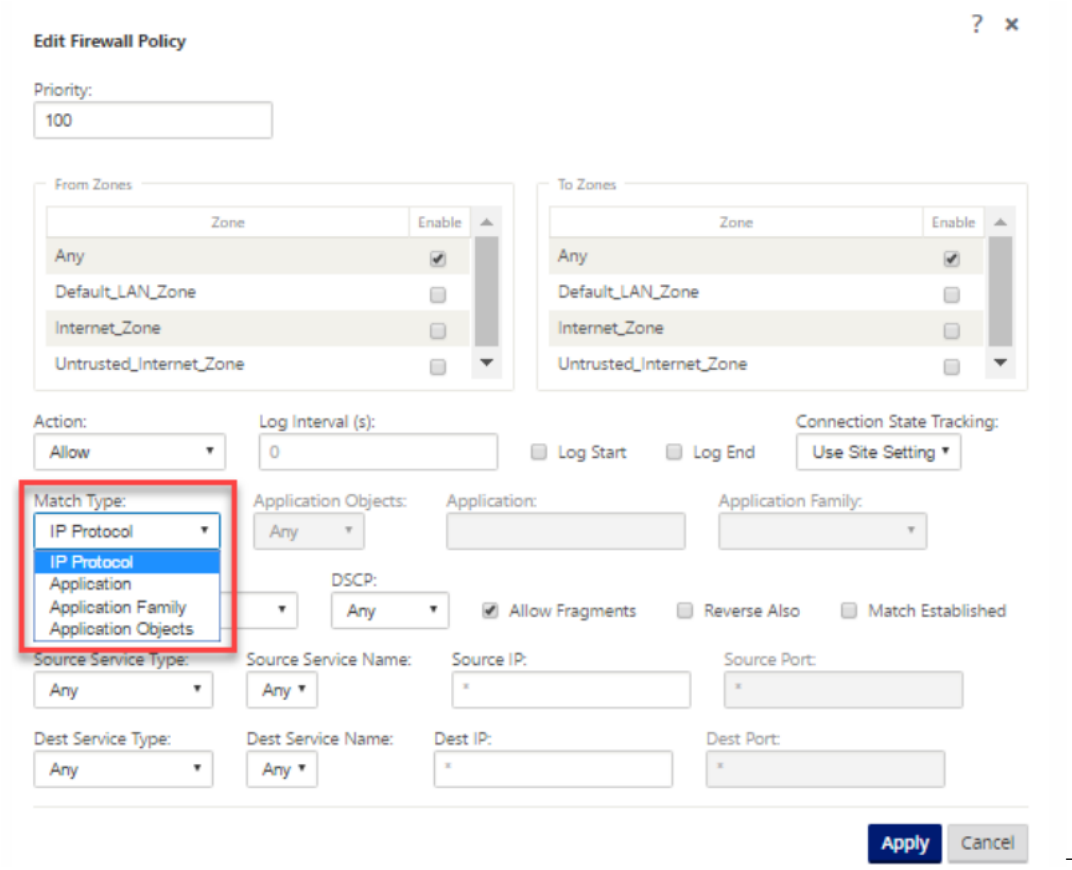
Los objetos de aplicación permiten agrupar diferentes tipos de criterios de coincidencia en un solo objeto que se puede utilizar en directivas de firewall y dirección de aplicaciones. Protocolo IP, aplicación y familia de aplicaciones son los tipos de coincidencia disponibles.

Las siguientes funciones utilizan el objeto de aplicación como tipo de coincidencia:

- Rutas de aplicación
- Directiva de firewall
- Reglas QoS de aplicaciones
- QoE de aplicaciones

Uso de la clasificación de aplicaciones con un firewall

La clasificación del tráfico como aplicaciones, familias de aplicaciones o nombres de dominio permite utilizar la aplicación, las familias de aplicaciones y los objetos de aplicación como tipos de coincidencia para filtrar el tráfico y aplicar reglas y directivas de firewall. Se aplica a todas las directivas pre, post y local. Para obtener más información sobre el firewall, consulte Firewall con estado y compatibilidad con NAT.



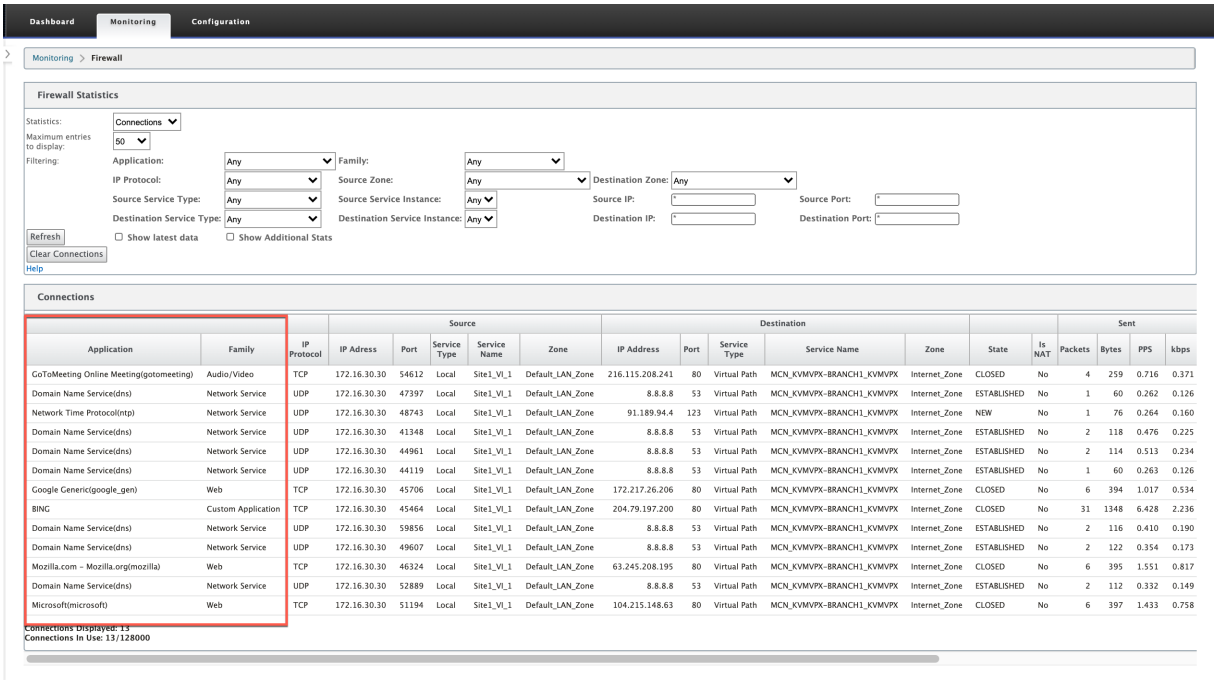
–>

Visualización de Clasificación de Aplicaciones

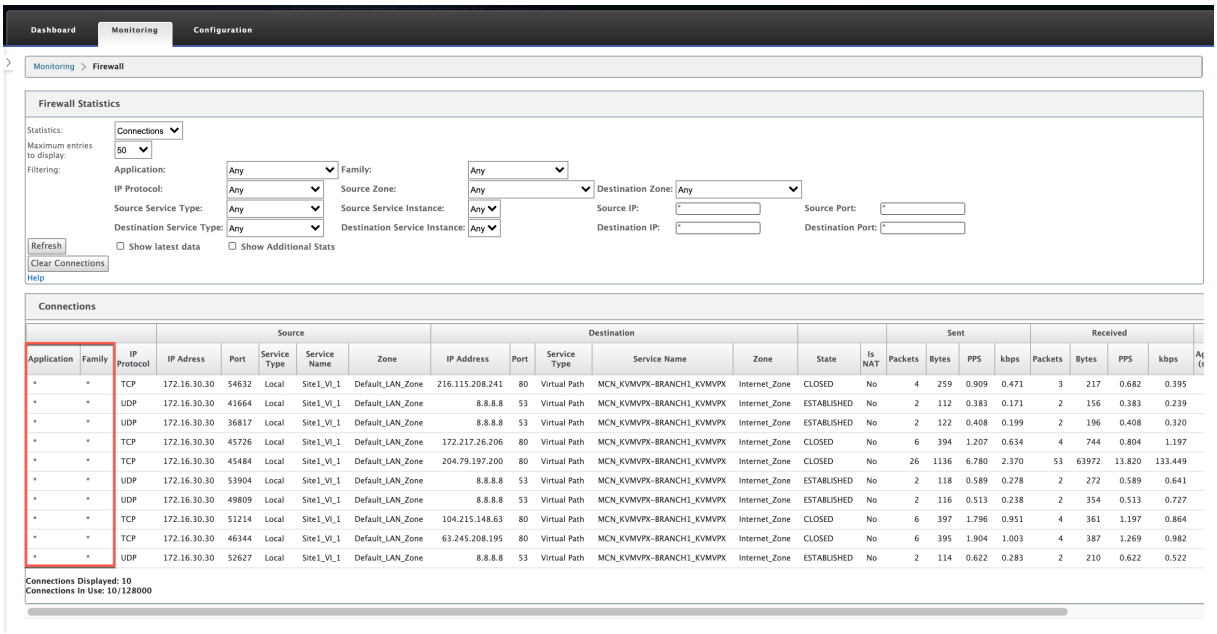
Después de habilitar la clasificación de aplicaciones, puede ver el nombre de la aplicación y los detalles de la familia de aplicaciones en los siguientes informes:

- Estadísticas de conexión al firewall
- Información sobre flujos
- Estadísticas de aplicación

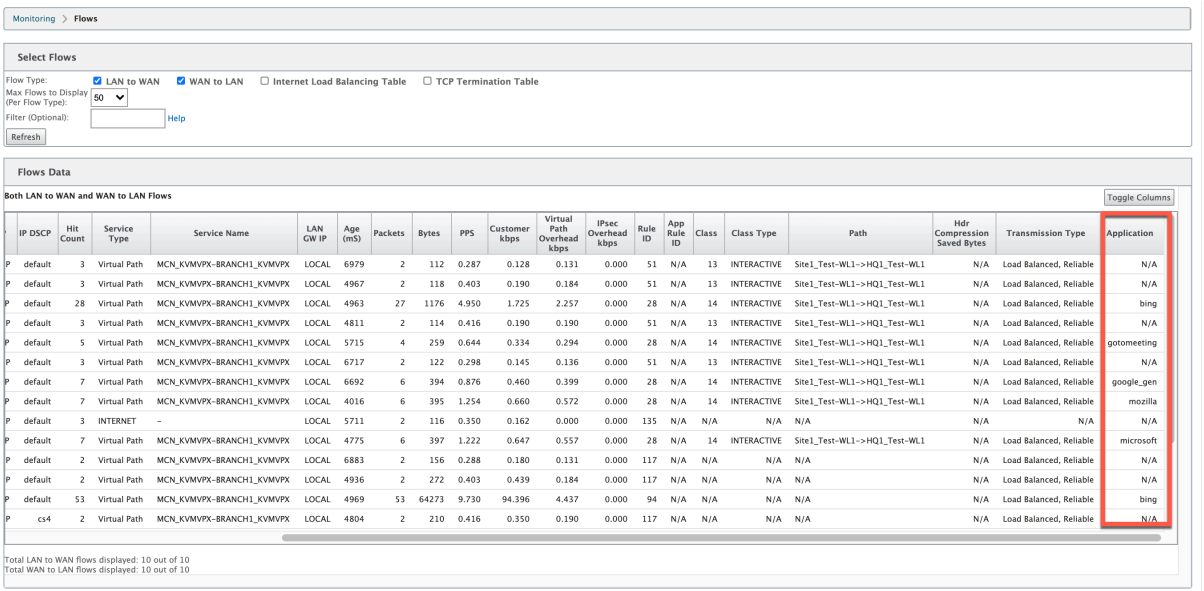
Estadísticas de conexión de firewall Vaya a **Supervisión > Firewalls**. En la sección **Conexiones**, las columnas **Aplicación** y **Familia** muestran las aplicaciones y su familia asociada.



Si no habilita la clasificación de aplicaciones, las columnas **Aplicación** y **Familia** no muestran ningún dato.



Información sobre flujos Vaya a **Supervisión > Flujos**. En la sección **Datos de flujos**, la columna **Aplicación** muestra los detalles de la aplicación.



Estadísticas de aplicación Vaya a **Supervisión > Estadísticas**. En la sección **Estadísticas de la aplicación**, la columna **Aplicación** muestra los detalles de la aplicación.

Solución de problemas

Después de habilitar la clasificación de aplicaciones, puede ver los informes en la sección **Supervisión** y asegurarse de que muestran los detalles de la aplicación. Para obtener más información, consulte Visualización de la clasificación de aplicaciones.

Si hay algún comportamiento inesperado, recopile el paquete de diagnóstico STS mientras se observa el problema y compártelo con el equipo de soporte técnico de Citrix.

El paquete STS se puede crear y descargar mediante **Configuración > Mantenimiento del sistema > Diagnóstico > Información de diagnóstico**.

Equidad QoS (ROJO)

La función QoS imparcialidad mejora la imparcialidad de múltiples flujos de rutas virtuales mediante el uso de clases QoS y Detección temprana aleatoria (RED). Se puede asignar una ruta virtual a una de las 16 clases diferentes. Una clase puede ser de tres tipos básicos:

- Las clases en tiempo real atienden flujos de tráfico que exigen un servicio rápido hasta un límite de ancho de banda determinado. Se prefiere una latencia baja al rendimiento agregado.
- Las clases interactivas tienen menor prioridad que el tiempo real, pero tienen prioridad absoluta sobre el tráfico masivo.

- Las clases masivas obtienen lo que queda de las clases interactivas y en tiempo real, porque la latencia es menos importante para el tráfico masivo.

Los usuarios especifican diferentes requisitos de ancho de banda para distintas clases, lo que permite al planificador de rutas virtuales arbitrar solicitudes de ancho de banda competidoras de varias clases del mismo tipo. El programador utiliza el algoritmo Hierarchical Fair Service Curve (HFSC) para lograr la equidad entre las clases.

Clases de servicios de HFSC en orden primero en entrar, primero en salir (FIFO). Antes de programar paquetes, Citrix SD-WAN examina la cantidad de tráfico pendiente de la clase de paquetes. Cuando hay un tráfico excesivo pendiente, los paquetes se descartan en lugar de colocarse en la cola (caída de cola).

¿Por qué TCP provoca la cola?

TCP no puede controlar la rapidez con la que la red puede transmitir datos. Para controlar el ancho de banda, TCP implementa el concepto de ventana de ancho de banda, que es la cantidad de tráfico no reconocido que permite en la red. Inicialmente comienza con una ventana pequeña y duplica el tamaño de esa ventana cada vez que se reciben acuses de recibo. Esto se denomina fase de inicio lento o de crecimiento exponencial.

TCP identifica la congestión de la red mediante la detección de paquetes descartados. Si la pila TCP envía una ráfaga de paquetes que introduce un retraso de 250 ms, TCP no detecta la congestión si ninguno de los paquetes se descarta, por lo que continúa aumentando el tamaño de la ventana. Es posible que siga haciéndolo hasta que el tiempo de espera alcance los 600 a 800 ms.

Cuando TCP no está en el modo de inicio lento, reduce el ancho de banda a la mitad cuando se detecta la pérdida de paquetes y aumenta el ancho de banda permitido en un paquete por cada confirmación recibida. Por lo tanto, TCP alterna entre presionar al alza el ancho de banda y retroceder. Desafortunadamente, si el tiempo de espera alcanza los 800 ms cuando se detecta la pérdida de paquetes, la reducción del ancho de banda provoca un retraso en la transmisión.

Impacto en la equidad de QoS

Cuando se produce un retraso en la transmisión TCP, resulta difícil ofrecer cualquier tipo de garantía de equidad dentro de una clase de ruta virtual. El programador de rutas virtuales debe aplicar un comportamiento de caída de cola para evitar contener enormes cantidades de tráfico. La naturaleza de las conexiones TCP es tal que un pequeño número de flujos de tráfico para llenar la ruta virtual, lo que dificulta que una nueva conexión TCP logre una proporción justa del ancho de banda. Compartir ancho de banda requiere asegurarse de que el ancho de banda esté disponible para la transmisión de nuevos paquetes.

Detección temprana aleatoria

La detección temprana aleatoria (RED) evita que las colas de tráfico se llenen y provoquen acciones de caída de cola. Evita la cola innecesaria por parte del planificador de rutas virtuales, sin afectar el rendimiento que puede alcanzar una conexión TCP.

Para obtener información sobre cómo usar y habilitar RED, consulte Cómo usar RED.

Colas MPLS

Esta función simplifica la creación de configuraciones SD-WAN al agregar un enlace WAN de conmutación de capas multiprotocolo (MPLS). Anteriormente, cada cola MPLS requería la creación de un enlace WAN. Cada enlace WAN requería una dirección IP virtual (VIP) única para crear el enlace WAN y una etiqueta de punto de código de servicios diferenciados (DSCP) única correspondiente al esquema de cola del proveedor. Tras definir un enlace WAN para cada cola MPLS, se define el servicio de intranet que se asignará a una cola específica.

Actualmente, está disponible una nueva definición de enlace WAN específico de MPLS (es decir, Tipo de acceso). Cuando se selecciona un nuevo tipo de acceso MPLS privado, puede definir las colas MPLS asociadas con el vínculo WAN. Esto permite un único VIP con varias etiquetas DSCP que corresponden a la implementación de cola del proveedor para el enlace WAN MPLS. Esto asigna el servicio de intranet a varias colas MPLS en un único enlace WAN MPLS. Para obtener información sobre cómo configurar MPLS mediante Citrix SD-WAN Orchestrator Service, consulte Colas de MPLS.

> **Nota**
>
> Si tiene configuraciones de MPLS existentes y quiere implementar el tipo de acceso privado MPLS, póngase en contacto con el soporte técnico de Citrix para obtener ayuda.

Asignar grupo de rutas automáticas a un enlace WAN de ruta virtual

El grupo de rutas automáticas definido es el mismo para el MCN y el dispositivo cliente. Esto permite que el sistema cree los Paths automáticamente. En el sitio de MCN, también puede expandir el enlace WAN asociado a la ruta virtual.

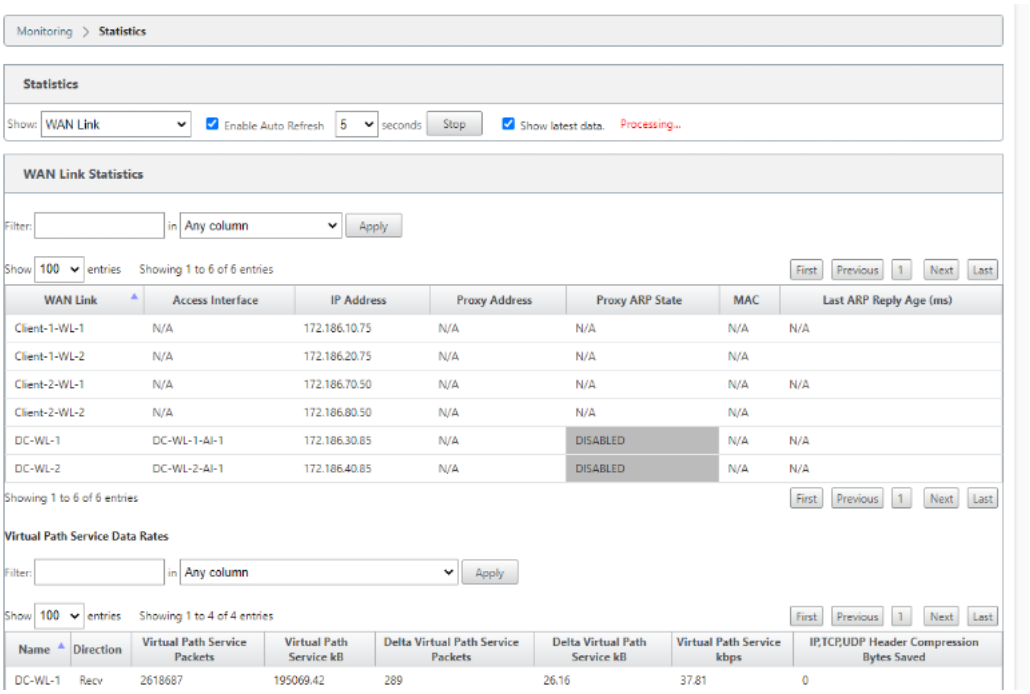
Ver la velocidad permitida y la congestión para enlaces WAN

La interfaz web SD-WAN permite ahora ver la tasa permitida para los Vínculos WAN y los Usos de Vínculos WAN y si un Vínculo WAN, Path o Ruta Virtual está en estado congestionado. En las versiones anteriores, esta información estaba disponible en archivos de registro SD-WAN y a través de la CLI. Estas opciones ya están disponibles en la interfaz web para ayudar a solucionar problemas.

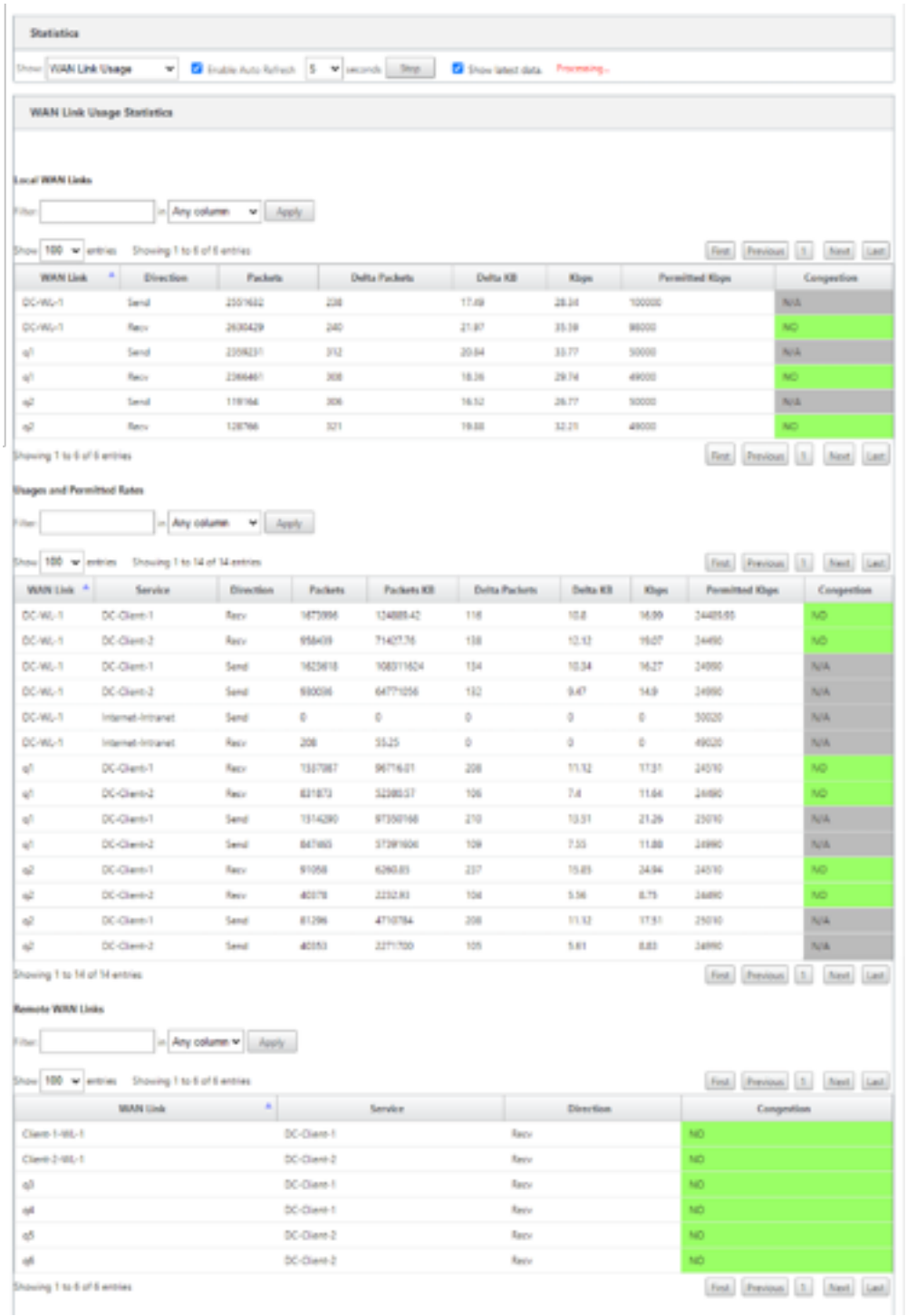
Ver tarifa permitida La tasa permitida es la cantidad de ancho de banda que un enlace WAN concreto, un servicio de ruta virtual, un servicio de intranet o un servicio de Internet pueden utilizar en un momento determinado. La velocidad permitida para un enlace WAN es estática y se define explícitamente en la configuración de SD-WAN. La tarifa permitida para un servicio de ruta virtual, un servicio de intranet o un servicio de Internet fluctuará con el tiempo en respuesta a la congestión, la demanda de los usuarios y las acciones justas, pero siempre será mayor o igual que el ancho de banda reservado mínimo para el servicio.

Supervisar enlace WAN

Vaya a **Supervisar** > **Estadísticas** y seleccione **Vínculo WAN** en la lista desplegable **Mostrar** .

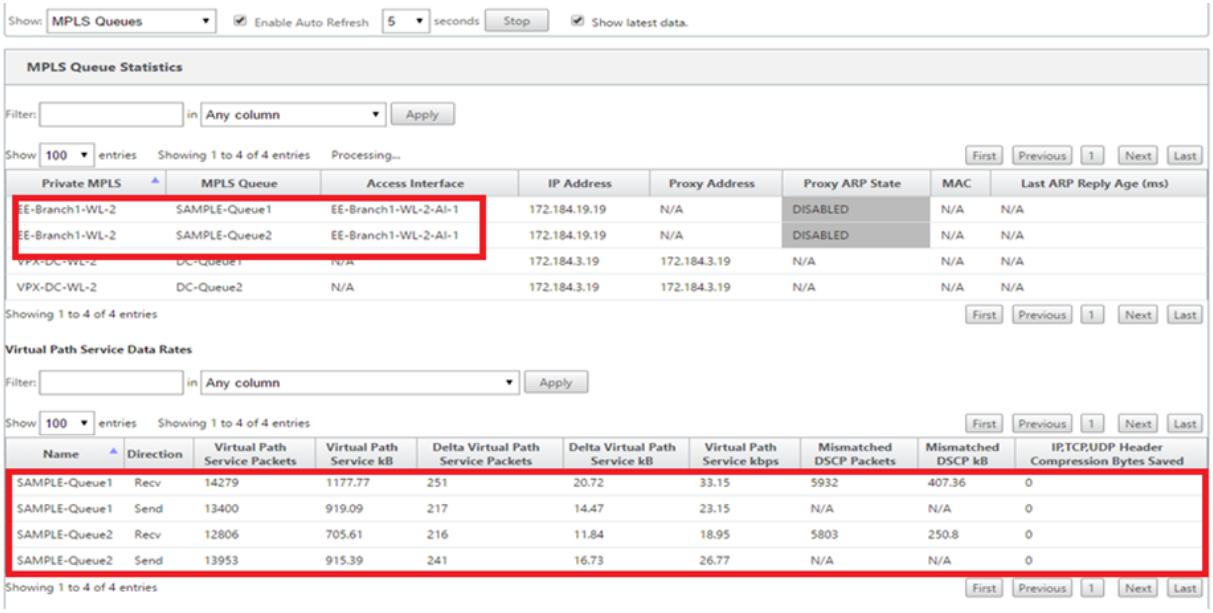


Vaya a **Supervisar > Estadísticas** y seleccione **Uso de vínculos WAN** en la lista desplegable **Mostrar**.



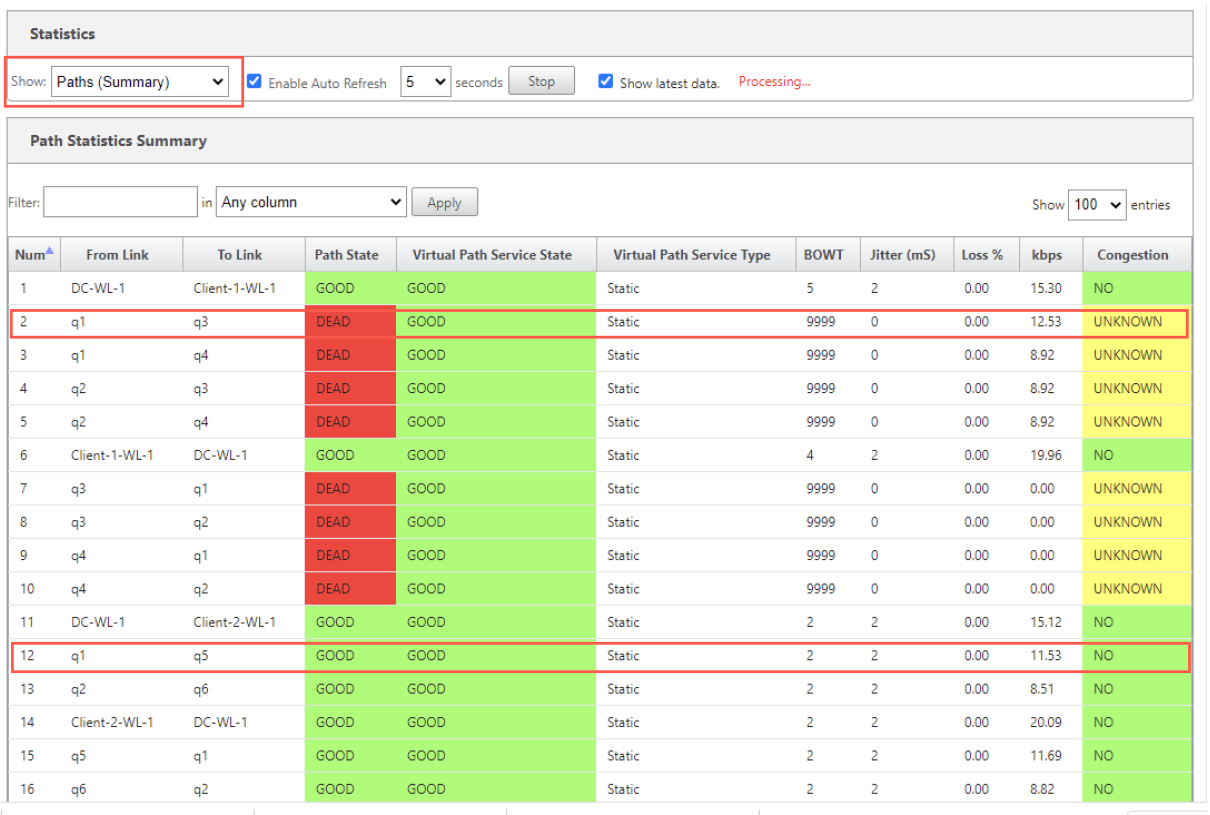
Supervisar colas MPLS

Vaya a **Supervisar Estadísticas**y seleccione **Colas MPLS** en la lista desplegable **Mostrar**.



Solución de problemas de colas MPLS

Para comprobar el estado de las colas MPLS, vaya a **Supervisar > Estadísticas** y seleccione **Rutas (resumen)** en la lista desplegable **Mostrar**. En el ejemplo siguiente, la ruta de acceso de la cola MPLS “q1”a “q3”está en estado DEAD y se muestra en rojo. La ruta de la cola de MPLS “q1”a “q5”está en buen estado y se muestra en verde.

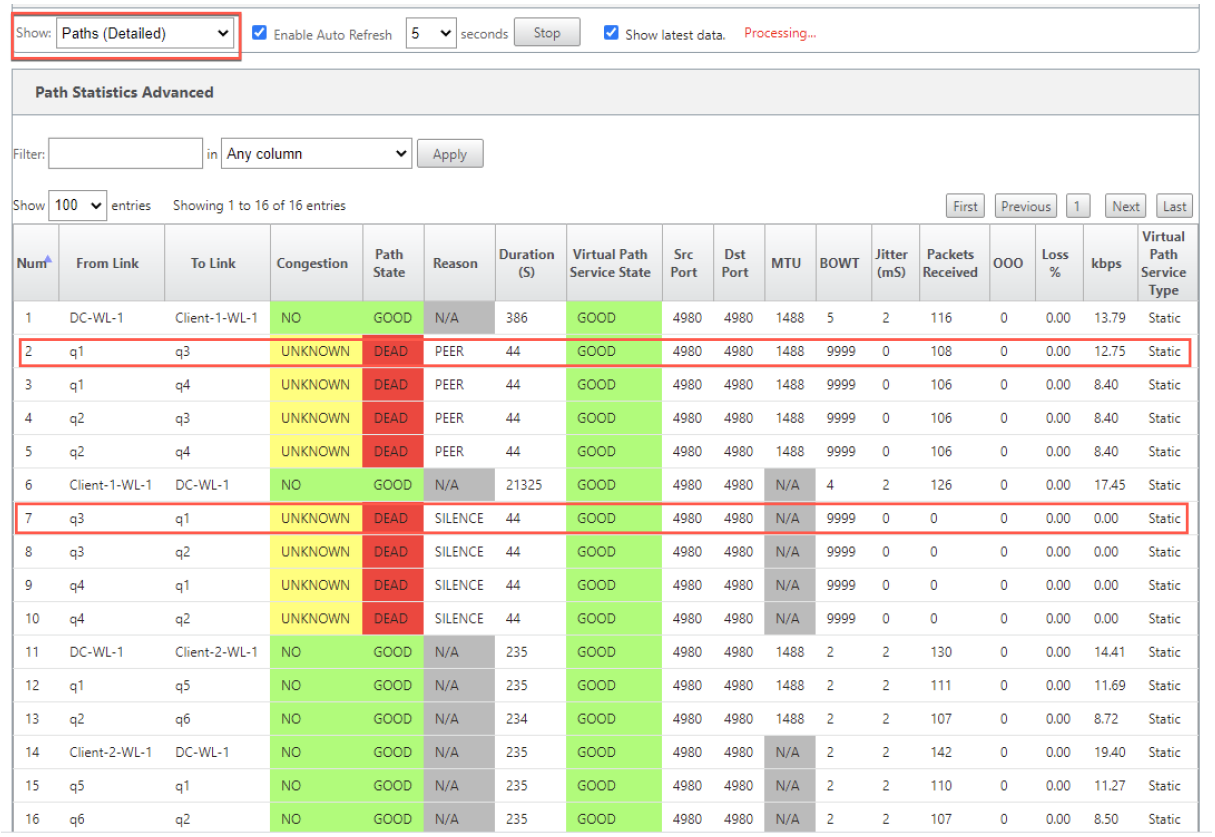


Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	DC-WL-1	Client-1-WL-1	GOOD	GOOD	Static	5	2	0.00	15.30	NO
2	q1	q3	DEAD	GOOD	Static	9999	0	0.00	12.53	UNKNOWN
3	q1	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
4	q2	q3	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
5	q2	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
6	Client-1-WL-1	DC-WL-1	GOOD	GOOD	Static	4	2	0.00	19.96	NO
7	q3	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
8	q3	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
9	q4	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
10	q4	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
11	DC-WL-1	Client-2-WL-1	GOOD	GOOD	Static	2	2	0.00	15.12	NO
12	q1	q5	GOOD	GOOD	Static	2	2	0.00	11.53	NO
13	q2	q6	GOOD	GOOD	Static	2	2	0.00	8.51	NO
14	Client-2-WL-1	DC-WL-1	GOOD	GOOD	Static	2	2	0.00	20.09	NO
15	q5	q1	GOOD	GOOD	Static	2	2	0.00	11.69	NO
16	q6	q2	GOOD	GOOD	Static	2	2	0.00	8.82	NO

Para obtener información detallada sobre las rutas, seleccione **Rutas (Detalladas)** en la lista desplegable **Mostrar**. La información sobre rutas como el motivo del estado, la duración, el puerto de origen, el puerto de destino, la MTU están disponibles

En el siguiente ejemplo, la ruta de acceso de la cola MPLS "q1"a "q3"está en estado DEAD y la razón es PEER. La ruta de la cola de MPLS "q3"a "q1"está muerta y la razón es SILENCE. En la tabla siguiente se proporciona la lista de razones disponibles y sus descripciones.

Motivo	Descripción
PUERTA DE ENLACE	La ruta de acceso está DEAD ya que el dispositivo no puede alcanzar ni detectar la puerta de enlace
SILENCIO	La ruta de acceso es INCORRECTA o DEAD porque el dispositivo no ha recibido paquetes del sitio del mismo
PÉRDIDA	La ruta es INCORRECTA debido a la pérdida de paquetes
PAR	El sitio del mismo par informa de que la ruta es incorrecta



Show: Paths (Detailed) | Enable Auto Refresh 5 seconds | Stop | Show latest data. Processing...

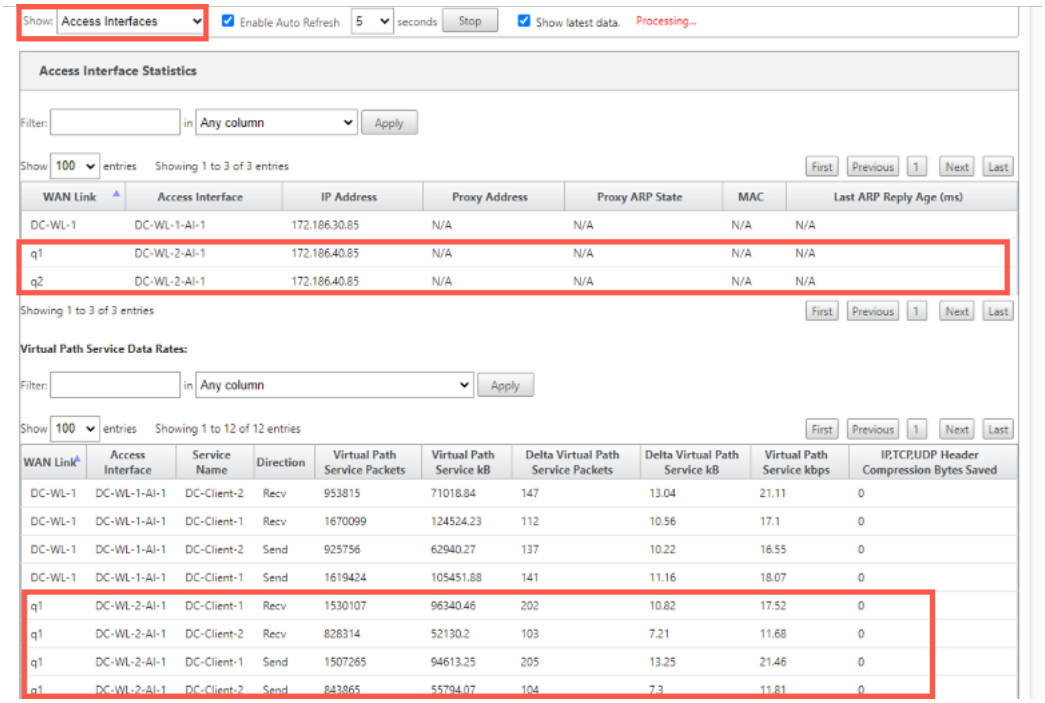
Path Statistics Advanced

Filter: in Any column | Apply

Show 100 entries Showing 1 to 16 of 16 entries | First | Previous | 1 | Next | Last

Num	From Link	To Link	Congestion	Path State	Reason	Duration (S)	Virtual Path Service State	Src Port	Dst Port	MTU	BOWT	Jitter (mS)	Packets Received	OOO	Loss %	kbps	Virtual Path Service Type
1	DC-WL-1	Client-1-WL-1	NO	GOOD	N/A	386	GOOD	4980	4980	1488	5	2	116	0	0.00	13.79	Static
2	q1	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	108	0	0.00	12.75	Static
3	q1	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
4	q2	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
5	q2	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
6	Client-1-WL-1	DC-WL-1	NO	GOOD	N/A	21325	GOOD	4980	4980	N/A	4	2	126	0	0.00	17.45	Static
7	q3	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
8	q3	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
9	q4	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
10	q4	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
11	DC-WL-1	Client-2-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	130	0	0.00	14.41	Static
12	q1	q5	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	111	0	0.00	11.69	Static
13	q2	q6	NO	GOOD	N/A	234	GOOD	4980	4980	1488	2	2	107	0	0.00	8.72	Static
14	Client-2-WL-1	DC-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	142	0	0.00	19.40	Static
15	q5	q1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	110	0	0.00	11.27	Static
16	q6	q2	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	107	0	0.00	8.50	Static

Para comprobar la interfaz de acceso y la dirección IP asociadas a las colas MPLS, seleccione **Interfaces de acceso** en la lista desplegable **Mostrar**.



Show: Access Interfaces | Enable Auto Refresh 5 seconds | Stop | Show latest data. Processing...

Access Interface Statistics

Filter: in Any column | Apply

Show 100 entries Showing 1 to 3 of 3 entries | First | Previous | 1 | Next | Last

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
DC-WL-1	DC-WL-1-AI-1	172.186.30.85	N/A	N/A	N/A	N/A
q1	DC-WL-2-AI-1	172.186.40.85	N/A	N/A	N/A	N/A
q2	DC-WL-2-AI-1	172.186.40.85	N/A	N/A	N/A	N/A

Showing 1 to 3 of 3 entries | First | Previous | 1 | Next | Last

Virtual Path Service Data Rates:

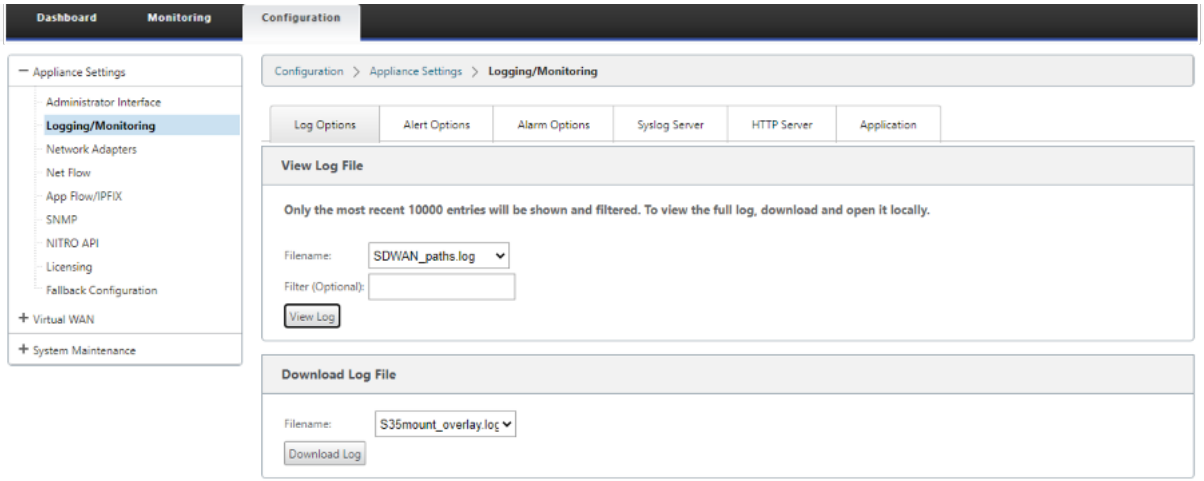
Filter: in Any column | Apply

Show 100 entries Showing 1 to 12 of 12 entries | First | Previous | 1 | Next | Last

WAN Link	Access Interface	Service Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Virtual Path Service kbps	IP,TCP,UDP Header Compression Bytes Saved
DC-WL-1	DC-WL-1-AI-1	DC-Client-2	Recv	953815	71018.84	147	13.04	21.11	0
DC-WL-1	DC-WL-1-AI-1	DC-Client-1	Recv	1670099	124524.23	112	10.56	17.1	0
DC-WL-1	DC-WL-1-AI-1	DC-Client-2	Send	925756	62940.27	137	10.22	16.55	0
DC-WL-1	DC-WL-1-AI-1	DC-Client-1	Send	1619424	105451.88	141	11.16	18.07	0
q1	DC-WL-2-AI-1	DC-Client-1	Recv	1530107	96340.46	202	10.82	17.52	0
q1	DC-WL-2-AI-1	DC-Client-2	Recv	828314	52130.2	103	7.21	11.68	0
q1	DC-WL-2-AI-1	DC-Client-1	Send	1507265	94613.25	205	13.25	21.46	0
q1	DC-WL-2-AI-1	DC-Client-2	Send	843865	55794.07	104	7.3	11.81	0

Puede descargar los archivos de registro para seguir solucionando problemas. Vaya a **Configu-**

ración > Registro/Supervisión y seleccione **SDWAN_paths.log** o **SDWAN_common.log** en la ficha **Opciones de registro**.



Informes

November 16, 2022

QoE de aplicaciones

La**QoE de la aplicación** es una medida de calidad de experiencia de aplicaciones en la red SD-WAN. Mide la calidad de las aplicaciones que fluyen por las rutas virtuales entre dos dispositivos SD-WAN. La puntuación **QoE de la aplicación** es un valor entre 0 y 10. El rango de puntuación en el que cae determina la calidad de una aplicación.

Calidad	Rango
Bueno	8–10
Normal	4–8
Mala	0–4

La puntuación**QoE de la aplicación** se puede utilizar para medir la calidad de las aplicaciones e identificar tendencias problemáticas.

Puede definir los umbrales de calidad de los dispositivos interactivos y en tiempo real mediante perfiles QoE y asignar estos perfiles a aplicaciones u objetos de aplicaciones.

> **Nota**
>
> Para supervisar la QoE de la aplicación, es esencial habilitar la inspección profunda de paquetes. Para obtener más información, consulte Clasificación de aplicaciones.

QoE de aplicaciones en tiempo real

El cálculo de QoE de aplicaciones para aplicaciones en tiempo real utiliza una técnica innovadora de Citrix, que se deriva de la puntuación MOS.

Los valores de umbral predeterminados son:

- Umbral de latencia: 160 ms
- Umbral de jitter: 30 ms
- Umbral de pérdida de paquetes: 2%

Un flujo de una aplicación en tiempo real que cumple los umbrales de latencia, pérdida y fluctuación se considera de buena calidad.

La QoE para aplicaciones en tiempo real se determina a partir del porcentaje de flujos que cumplen el umbral dividido por el número total de muestras de flujo.

QoE para tiempo real = (Número de muestras de flujo que cumplen el umbral/Número total de muestras de flujo) * 100

Se representa como puntuación QoE que va de 0 a 10.

Puede crear perfiles QoE con valores umbrales personalizados y aplicarlos a aplicaciones u objetos de aplicación.

> **Nota**
>
> El valor de QoE puede ser cero si las condiciones de la red están fuera de los umbrales configurados para el tráfico en tiempo real.

Aplicación interactiva QoE

La QoE de aplicaciones para aplicaciones interactivas utiliza una técnica innovadora de Citrix basada en umbrales de pérdida de paquetes y velocidad de ráfaga.

Las aplicaciones interactivas son sensibles a la pérdida de paquetes y al rendimiento. Por lo tanto, medimos el porcentaje de pérdida de paquetes y la tasa de ráfagas del tráfico de entrada y salida en un flujo.

Los umbrales configurables son:

- Porcentaje de pérdida de paquetes.

- Porcentaje de la tasa de ráfaga de salida esperada en comparación con la tasa de ráfaga de entrada.

Los valores de umbral predeterminados son:

- Umbral de pérdida de paquetes: 1%
- Velocidad de ráfaga: 60%

Un flujo es de buena calidad si se cumplen las siguientes condiciones:

- El porcentaje de pérdida de un flujo es inferior al umbral configurado.
- La velocidad de ráfaga de salida es al menos el porcentaje configurado de la velocidad de ráfaga de entrada.

Configuración de QoE de aplicaciones

Asigne objetos de aplicación o aplicación a perfiles QoE predeterminados o personalizados.
Puede crear perfiles de QoE personalizados para el tráfico interactivo y en tiempo real y asignar hasta 10 aplicaciones u objetos de aplicación con perfiles de QoE.

Para crear perfiles de QoE personalizados a través de Citrix SD-WAN Orchestrator Service, consulte Perfiles de QoE de aplicaciones.

HDX QoE

Los parámetros de red, como la latencia, la fluctuación y la caída de paquetes, afectan a la experiencia de usuario de los usuarios de HDX. La calidad de la experiencia (QoE) se introduce para ayudar a los usuarios a comprender y comprobar su calidad de experiencia ICA. QoE es un índice calculado que indica el rendimiento del tráfico ICA. Los usuarios pueden ajustar las reglas y la directiva para mejorar la QoE.

La QoE es un valor numérico entre 0 y 100, cuanto mayor sea el valor, mejor será la experiencia del usuario. QoE está habilitado de forma predeterminada para todas las aplicaciones ICA/HDX.

Los parámetros utilizados para calcular la QoE se miden entre los dos dispositivos SD-WAN ubicados en el lado del cliente y del servidor y no entre el cliente o los dispositivos de servidor mismos. La latencia, la fluctuación y la caída de paquetes se miden en el nivel de flujo y pueden ser diferentes de las estadísticas en el nivel de enlace. Es posible que la aplicación de host final (cliente o servidor) nunca sepa que hay una pérdida de paquetes en la WAN. Si la retransmisión se realiza correctamente, la tasa de pérdida de paquetes de nivel de flujo es inferior a la pérdida de nivel de enlace. Sin embargo, como resultado, podría aumentar un poco la latencia y la fluctuación.

La configuración predeterminada para el tráfico HDX permite que SD-WAN retransmita paquetes, lo que mejora el valor del índice QoE que se perdió debido a la pérdida de paquetes en la red.

En el panel HDX de Citrix SD-WAN Orchestrator, puede ver una representación gráfica de la calidad general de las aplicaciones HDX. Las aplicaciones HDX se clasifican en las tres categorías de calidad siguientes:

Calidad	Rango QoE
Bueno	80–100
Normal	50–80
Mala	0–50

También se muestra una lista de los cinco sitios inferiores con el menor QoE en el panel de HDX.

Una representación gráfica de la QoE para diferentes intervalos de tiempo le permite supervisar el rendimiento de las aplicaciones HDX en cada sitio.

Para obtener más información sobre cómo configurar HDX QoE mediante Citrix SD-WAN Orchestrator Service, consulte Panel e informes de HDX.

> **Nota**
>
> - *No espere que la latencia del enlace WAN, la fluctuación y la caída de paquetes siempre coincidan con la latencia de la aplicación, la fluctuación y la caída de paquetes. La pérdida de enlace WAN se correlaciona con la pérdida real de paquetes WAN, mientras que la pérdida de aplicaciones se produce después de la retransmisión, que es menor que la pérdida del enlace WAN.*
> - *La latencia del enlace WAN que se muestra en la GUI es BOWT (mejor tiempo unidireccional). Es la mejor métrica del enlace como medio para medir la salud del enlace. La QoE de la aplicación realiza un seguimiento y calcula la latencia total y media de todos los paquetes de esa aplicación. Esto a menudo no coincide con el enlace BOWT.*
> - *Cuando se inicia una sesión MSI, durante el apretón de manos ICA, la sesión puede contarse temporalmente como 4 SSI en lugar de 1 MSI. Después de completar el apretón de manos, convergerá a 1 MSI. Si la conversión se produce antes de actualizar la tabla SQL, puede aparecer en ICA_summary durante ese minuto.*
> - *En la reconexión de sesión, dado que la información del protocolo inicial no se intercambia, SD-WAN no puede identificar MSI, por lo tanto, cada conexión se cuenta como información SSI.*
> - *Para las conexiones UDP, una vez cerrada la conexión, la conexión puede tardar hasta 5 minutos en mostrarse como cerrada y actualizada en ICA_summary. Para las conexiones TCP, una vez cerrada la conexión, puede tardar hasta 2 minutos en mostrarse como cerrada en ICA_summary.*
> - *Es posible que la QoE de las sesiones TCP y UDP no sea la misma en la misma ruta debido a*

> *la diferencia inherente entre TCP y UDP.*
> - *Si un usuario inicia dos escritorios virtuales, el número de usuarios se contrarresta como dos.*

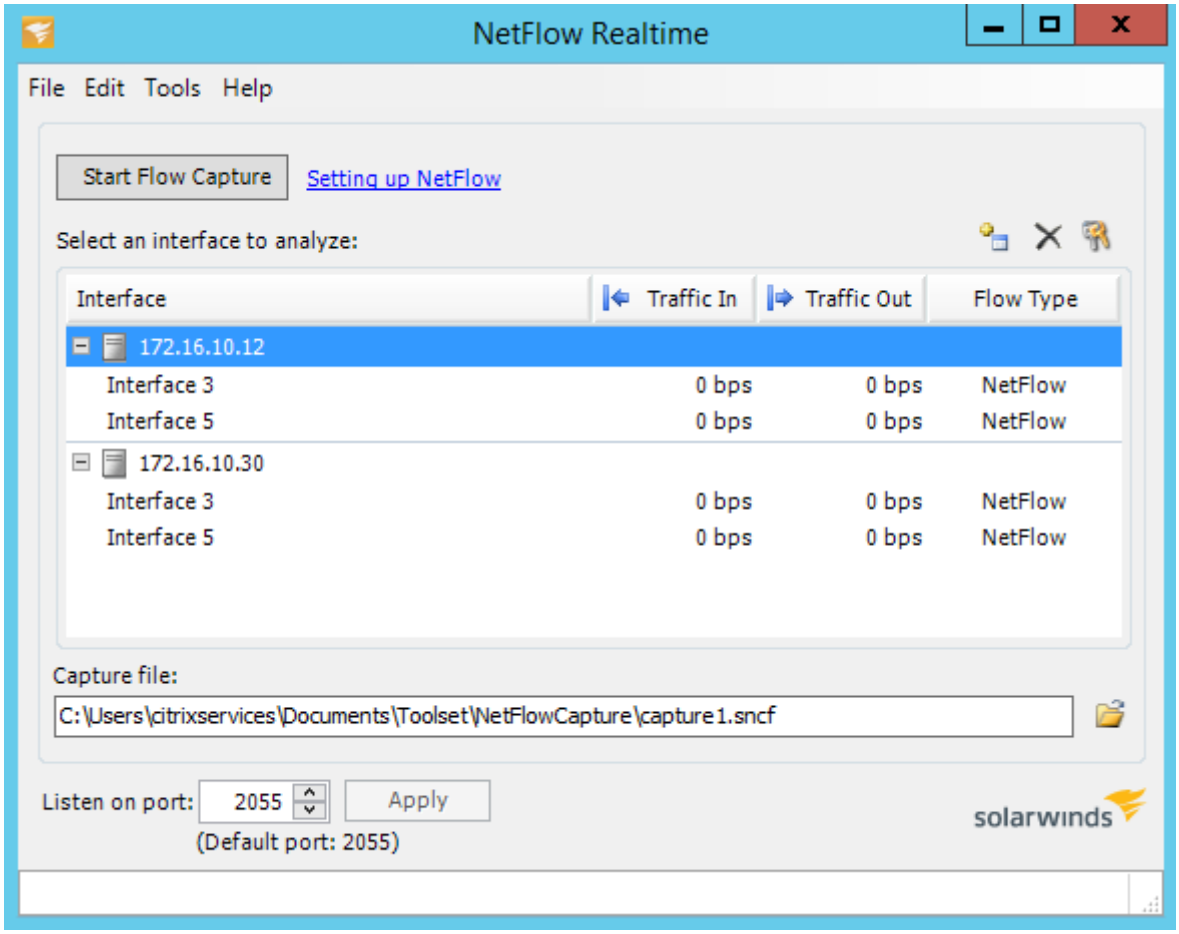
Múltiples colectores de flujo neto

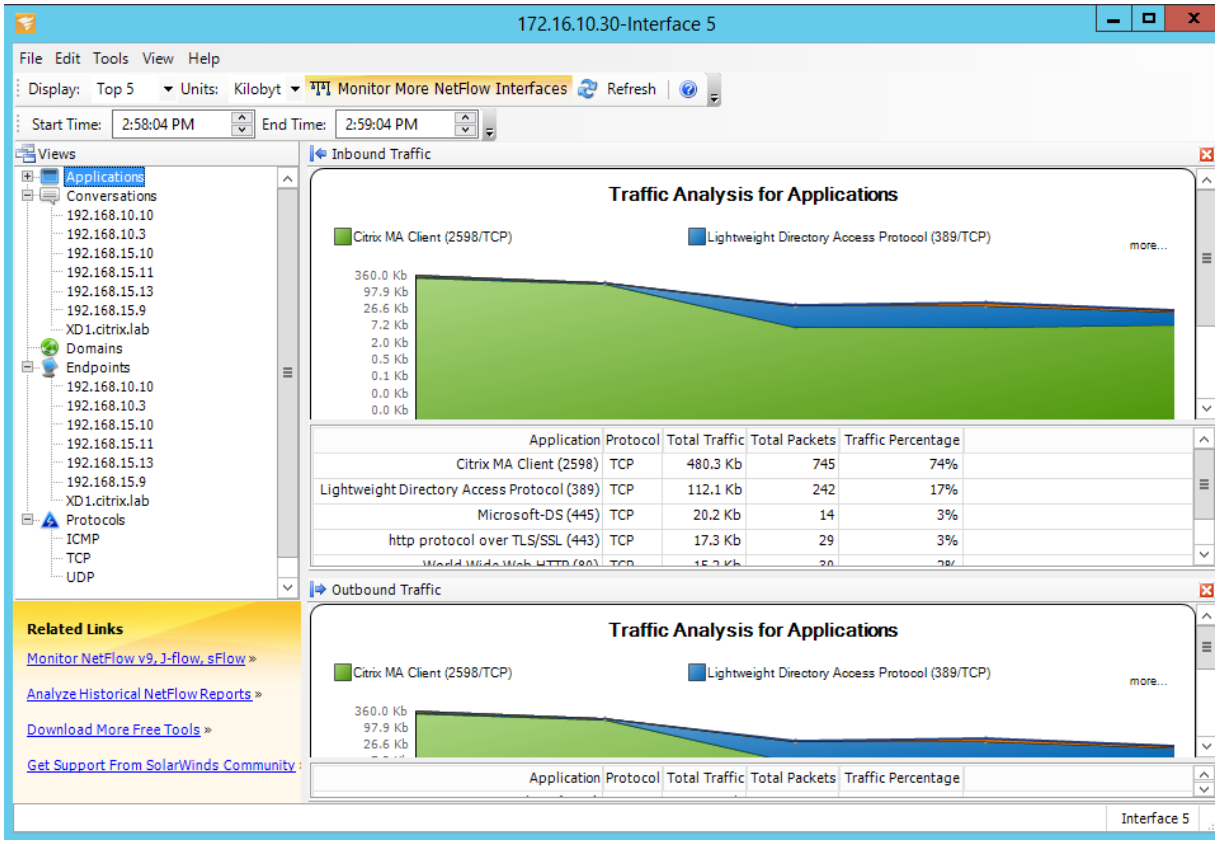
Los recopiladores de flujo de red recopilan el tráfico de red IP a medida que entra o sale de una interfaz SD-WAN. Al analizar los datos proporcionados por Net Flow, puede determinar el origen y el destino del tráfico, la clase de servicio y las causas de la congestión del tráfico. Los dispositivos Citrix SD-WAN se pueden configurar para enviar datos estadísticos básicos de Net Flow versión 5 al recopilador Net Flow configurado. Citrix SD-WAN proporciona compatibilidad con Net Flow para flujos de tráfico que quedan oscurecidos por el protocolo fiable de transporte. Los dispositivos en el borde WAN de la solución pierden la capacidad de recopilar registros de flujo de red, ya que solo se muestran los paquetes UDP encapsulados en SD-WAN. Net Flow se admite en los dispositivos Citrix SD-WAN Standard Edition.

Para obtener información sobre cómo configurar hosts de Net Flow mediante Citrix SD-WAN Orchestrator Service, consulte Configuración de host de Netflow.

Exportación NetFlow

Los datos de Net Flow se exportan desde el puerto de administración de dispositivos SD-WAN. En la herramienta de recopilación Net Flow, los dispositivos SD-WAN aparecen como la dirección IP de administración configurada, si SNMP no está configurado. Las interfaces aparecen como una para la entrada y una segunda para la salida (tráfico de ruta virtual). Para obtener más información, consulte SNMP.



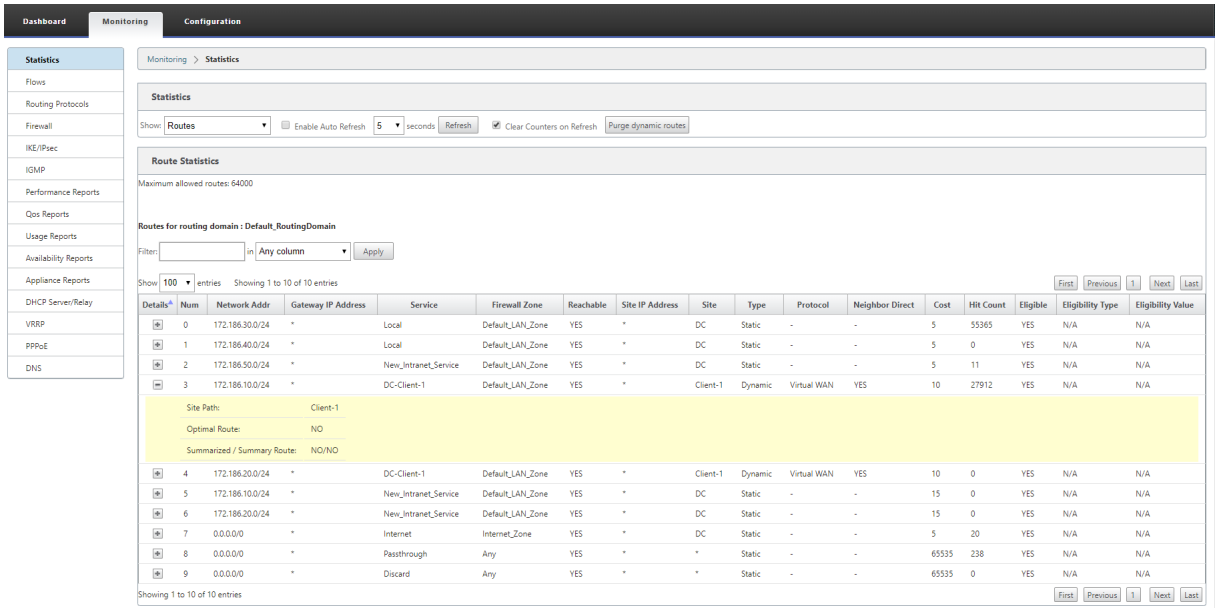


Limitaciones de NetFlow

- Con Netflow habilitado en los dispositivos SD-WAN Standard Edition, los datos de Virtual Path se transmiten a los recopiladores de Netflow designados. Una limitación con esto es que no se puede diferenciar qué enlace WAN físico está siendo utilizado por SD-WAN, ya que la solución informa información agregada de ruta virtual (una ruta virtual puede incluir varias rutas WAN distintas), no hay forma de filtrar los registros de NetFlow para las rutas WAN distintas.
- Los bits de control TCP informan como N/A, lo que indica que SD-WAN no sigue el estándar de Internet para las exportaciones de NetFlow basadas en RFC 7011, que tiene el ID de elemento 6 para tcpControlBits (IANA). Sin los indicadores TCP, no es posible calcular el tiempo de ida y vuelta (RTT), la latencia, la fluctuación ni otras métricas de rendimiento en los datos de flujo. Desde el lado de la seguridad, sin indicadores TCP, el recopilador de flujo neto no puede determinar si se están produciendo exploraciones FIN, ACK/RST o SYN.

Estadísticas de rutas

Para ver las estadísticas de rutas de sus dispositivos SD-WAN, en la GUI de SD-WAN, vaya a **Supervisión** > **Estadísticas** > **Rutas**.



Puede ver los siguientes parámetros:

- **Dirección de red**: dirección de red y máscara de subred de la ruta.
- **Detalles**: haga clic en + para mostrar la siguiente información.
  - **Ruta del sitio**: Ruta del sitio es una métrica de origen de verdad para el prefijo recibido. Se utiliza en situaciones en las que el reenvío de WAN a WAN está habilitado en varios dispositivos y en la implementación de malla. Se reciben varios prefijos de este tipo y los administradores pueden juzgar los atributos del prefijo mediante la visualización de la ruta del sitio.

    Por ejemplo, considere una topología simple de Branch1, Branch2 y MCN junto con un MCN geográfico. Branch1 tiene el prefijo 172.16.1.0/24 y debe llegar a Branch2. Geo MCN y MCN tienen habilitado el reenvío de WAN a WAN.

    El prefijo 172.16.1.0/24 puede llegar a Branch2 a través de Branch1-McN-Branch2, Branch1-Geo-Branch2 y Branch1-McN-Geo-Branch2. Para cada uno de estos prefijos distintos, la tabla de redirección se actualiza con su métrica de ruta de sitio. La métrica de ruta del sitio indica el origen del prefijo de ruta y el coste que implica llegar a Branch2.
  - **Ruta óptima**: Ruta óptima indica si la ruta es la ruta óptima para llegar a esa subred en comparación con todas las demás rutas. Esta ruta óptima se exporta a otros sitios.
  - Ruta**resumida/ Resumen: Una ruta**de resumen es una ruta configurada explícitamente por un administrador para resumir varios prefijos que caen en la superred. Las rutas resumidas son los prefijos incluidos en la ruta de resumen.

    Por ejemplo, supongamos que tenemos una ruta de resumen 172.16.0.0/16. Se trata únicamente de una ruta resumida y no de una ruta resumida. Una ruta de resumen tiene un re-

sumen "SÍ"y un "NO"resumido. Si hay pocas subredes como 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/24, estas tres rutas se incluyen en la ruta resumen o en la superred y, por lo tanto, se denominan rutas resumidas. Una ruta resumida tiene un resumen "SÍ"y un resumen "NO".

- **Dirección IP de la puerta**de enlace: dirección IP de la puerta de enlace o ruta utilizada para llegar a esta ruta.
- **Servicio**: tipo de servicio Citrix SD-WAN.
- **Zona de firewall**: La zona de firewall utilizada por la ruta.
- **Accesible**: Es la ruta accesible o no.
- **Dirección IP del sitio**: la dirección IP del sitio.
- **Sitio**: El nombre del sitio.
- **Tipo**: El tipo de ruta depende del origen del aprendizaje de la ruta. Las rutas del lado LAN y las rutas introducidas manualmente durante la configuración son rutas estáticas. Las rutas aprendidas de SD-WAN o de los pares de redirección dinámica son Rutas dinámicas.
- **Protocolo**: protocolo de los prefijos.
  - **Local**: IP virtuales locales del dispositivo.
  - **WAN virtual**: prefijos aprendidos de dispositivos SD-WAN homólogos.
  - **OSPF**: prefijos aprendidos del par de redirección dinámico OSPF.
  - **BGP**: Prefijos aprendidos del par de redirección dinámico BGP.
- **Vecino directo**: indica si la subred está conectada a la sucursal desde la que llegó la ruta al dispositivo.
- **Coste**: coste utilizado para determinar la mejor ruta hacia una red de destino.
- **Recuento de visitas**: número de veces que se ha alcanzado una ruta para reenviar un paquete a esa subred.
- **Apto**: indica que la ruta es elegible y se utiliza para reenviar o redirigir los paquetes al prefijo afectado durante el procesamiento del tráfico.
- **Tipo de elegibilidad**: están disponibles los dos tipos de elegibilidad siguientes.
  - **Elegibilidad de la puerta**de enlace: determina si se puede acceder a la puerta de enlace o no.
  - **Elegibilidad de ruta**: determina si la ruta está MUERTA o NO MUERTA.
- Valor de**elegibilidad: valor**seleccionado para la puerta de enlace o la ruta en la configuración mientras se crea la ruta en el sistema. Por ejemplo, una ruta se puede llamar elegible en función de una ruta MCN-WL-1->BR1-WL-2. Por lo tanto, el valor de elegibilidad para esta ruta en la sección de rutas es el valor MCN-WL-1->BR1-WL-2.

Redirección

November 16, 2022

> **Nota**
>
> A partir de la versión 11.5 de SD-WAN, todas las configuraciones de redirección solo se admiten a través de Citrix SD-WAN Orchestrator Service. Para obtener información sobre las configuraciones de redirección de Citrix SD-WAN Orchestrator Service, consulte Enrutamiento.

Redirección dinámica

Citrix SD-WAN introduce compatibilidad con protocolos de redirección conocidos en la función de redirección**dinámico**. Esta función facilita el descubrimiento de subredes LAN, anuncia rutas de rutas virtuales para que funcionen de forma más fluida dentro de las redes mediante los protocolos BGP y OSPF, permitiendo que SD-WAN se implemente sin problemas en un entorno existente sin necesidad de configuraciones de rutas estáticas y conmutación por error de enrutador elegante.

Filtrado de rutas

Para redes con Route Learning habilitado, Citrix SD-WAN proporciona más control sobre qué rutas SD-WAN se anuncian a los vecinos de redirección y qué rutas se reciben de los vecinos de redirección, en lugar de anunciar y aceptar todas o ninguna ruta.

- Los filtros de exportación se utilizan para incluir o excluir rutas para anuncios mediante protocolos OSPF y BGP basados en coincidencias específicas criterios.
- Los filtros de importación se utilizan para aceptar o no las rutas que se reciben mediante vecinos OSPF y BGP basados en criterios de coincidencia específicos.

El filtrado de rutas se implementa en rutas LAN y rutas de ruta virtual en una red SD-WAN (centro de datos/sucursal) y se anuncia a una red que no es SD-WAN mediante el uso de BGP y OSPF.

Resumen de rutas

El resumen de rutas reduce el número de rutas que debe mantener un enrutador. Una ruta de resumen es una única ruta que se utiliza para representar varias rutas. Ahorra ancho de banda mediante el envío de un solo anuncio de ruta, lo que reduce el número de enlaces entre routers. Ahorra memoria porque solo se mantiene una dirección de ruta. Los recursos de CPU se utilizan de manera más eficiente evitando búsquedas recursivas.

VRRP

Virtual Router Redundancy Protocol (VRRP) es un protocolo ampliamente utilizado que proporciona redundancia de dispositivo para eliminar el punto único de falla inherente al entorno enrutado por defecto estático. VRRP permite configurar dos o más routers para formar un grupo. Este grupo aparece como una única Gateway predeterminada con una dirección IP virtual y una dirección MAC virtual.

Citrix SD-WAN (versión 10.0 y posterior) admite VRRP versión 2 y la versión 3 para interoperar con enrutadores de terceros. El dispositivo SD-WAN actúa como enrutador maestro y dirige el tráfico para utilizar el servicio de ruta virtual entre sitios. Puede configurar el dispositivo SD-WAN como el maestro VRRP mediante la configuración de la IP de interfaz virtual como IP VRRP y el establecimiento manual de la prioridad en un valor superior al de los enrutadores del mismo nivel. Puede configurar el intervalo de anuncio y la opción de preferencia.

Uso de CLI para acceder a la funcionalidad de redirección

Puede ver información adicional relacionada con la redirección dinámica y el estado del protocolo. Escriba el siguiente comando y la sintaxis para acceder al demonio de redirección y ver la lista de comandos.

‘

dynamic_routing?

‘

Redirección de superposición SD-WAN

August 26, 2022

Citrix SD-WAN proporciona una conectividad sólida y resistente entre sitios remotos, centros de datos y redes en la nube. La solución SD-WAN puede lograrlo mediante el establecimiento de túneles entre los dispositivos SD-WAN de la red, lo que permite la conectividad entre sitios mediante la aplicación de tablas de rutas que se superponen a la red subyacente existente. Las tablas de redirección SD-WAN pueden reemplazar completamente o coexistir con la infraestructura de redirección existente.

Los dispositivos Citrix SD-WAN miden los paths disponibles unidireccionalmente en términos de disponibilidad, pérdida, latencia, fluctuación y funciones de congestión, y seleccionan la mejor ruta por paquete. Esto significa que la ruta elegida del Sitio A al Sitio B no tiene por qué ser necesariamente la ruta elegida del Sitio B al Sitio A. La mejor ruta en un momento dado se selecciona independientemente en cada dirección. Citrix SD-WAN ofrece una selección de rutas basada en paquetes para una rápida adaptación a cualquier cambio de red. Los dispositivos SD-WAN pueden detectar interrupciones de paths después de solo dos o tres paquetes que faltan, lo que permite una conmutación por error de subsegundos sin problemas del tráfico de aplicaciones al siguiente mejor

path de WAN. Los dispositivos SD-WAN vuelven a calcular cada estado de enlace WAN en unos 50 ms. En el siguiente artículo se proporciona una configuración de redirección detallada dentro de la red Citrix SD-WAN.

Tabla de rutas de Citrix SD-WAN

La SD-WAN permite entradas de rutas estáticas para sitios específicos y entradas de ruta aprendidas de la red subyacente a través de protocolos de redirección compatibles, como OSPF, eBGP e iBGP. Las rutas no solo se definen por su siguiente salto sino por su tipo de servicio. Esto determina cómo se reenvía la ruta. Los siguientes son los principales tipos de servicio en uso:

- **Servicio local**: Indica cualquier ruta o subred local para el dispositivo SD-WAN. Esto incluye las subredes de la interfaz virtual (crea rutas locales automáticamente) y cualquier ruta local definida en la tabla de rutas (con un salto siguiente local). La ruta se anuncia a otros dispositivos SD-WAN que tienen una ruta virtual a este sitio local donde esta ruta está configurada cuando se confía en un socio.

> **Nota**
>
> Tenga cuidado al agregar rutas predeterminadas y rutas de resumen como rutas locales, ya que pueden dar lugar a rutas de ruta virtuales en otros sitios. Compruebe siempre las tablas de redirección para asegurarse de que la redirección correcta esté en vigor.

- **Ruta virtual**: Indica cualquier ruta local aprendida de un sitio SD-WAN remoto al que se puede acceder por las rutas virtuales. Estas rutas son normalmente automáticas, sin embargo, una ruta de ruta virtual se puede agregar manualmente en un sitio. Cualquier tráfico de esta ruta se reenvía a la ruta virtual definida para esta ruta de destino (subred).
- **Intranet**: Indica rutas a las que se puede acceder a través de un enlace WAN privado (MPLS, P2P, VPN, etc.). Por ejemplo, una sucursal remota que se encuentra en la red MPLS pero que no tiene un dispositivo SD-WAN. Se supone que estas rutas deben ser reenviadas a un enrutador WAN determinado. El servicio de intranet no está habilitado de forma predeterminada. Cualquier tráfico que coincida con esta ruta (subred) se clasifica como intranet de este dispositivo para su entrega a un sitio que no tiene una solución SD-WAN.

> **Nota**
>
> Observe que al agregar una ruta de intranet no hay siguiente salto, sino un reenvío a un servicio de intranet. El servicio está asociado a un enlace WAN determinado.

- **Internet**: Es similar a la Intranet, pero se utiliza para definir el tráfico que fluye hacia enlaces WAN públicos de Internet en lugar de enlaces WAN privados. Una diferencia única es que el servicio de Internet puede asociarse con varios enlaces WAN y establecerse en equilibrio de

carga (por flujo) o estar activo/copia de seguridad. Se crea una ruta de Internet predeterminada cuando el servicio de Internet está habilitado (está desactivado de forma predeterminada). Cualquier tráfico que coincida con esta ruta (subred) se clasifica como Internet para este dispositivo para su entrega a recursos públicos de Internet.

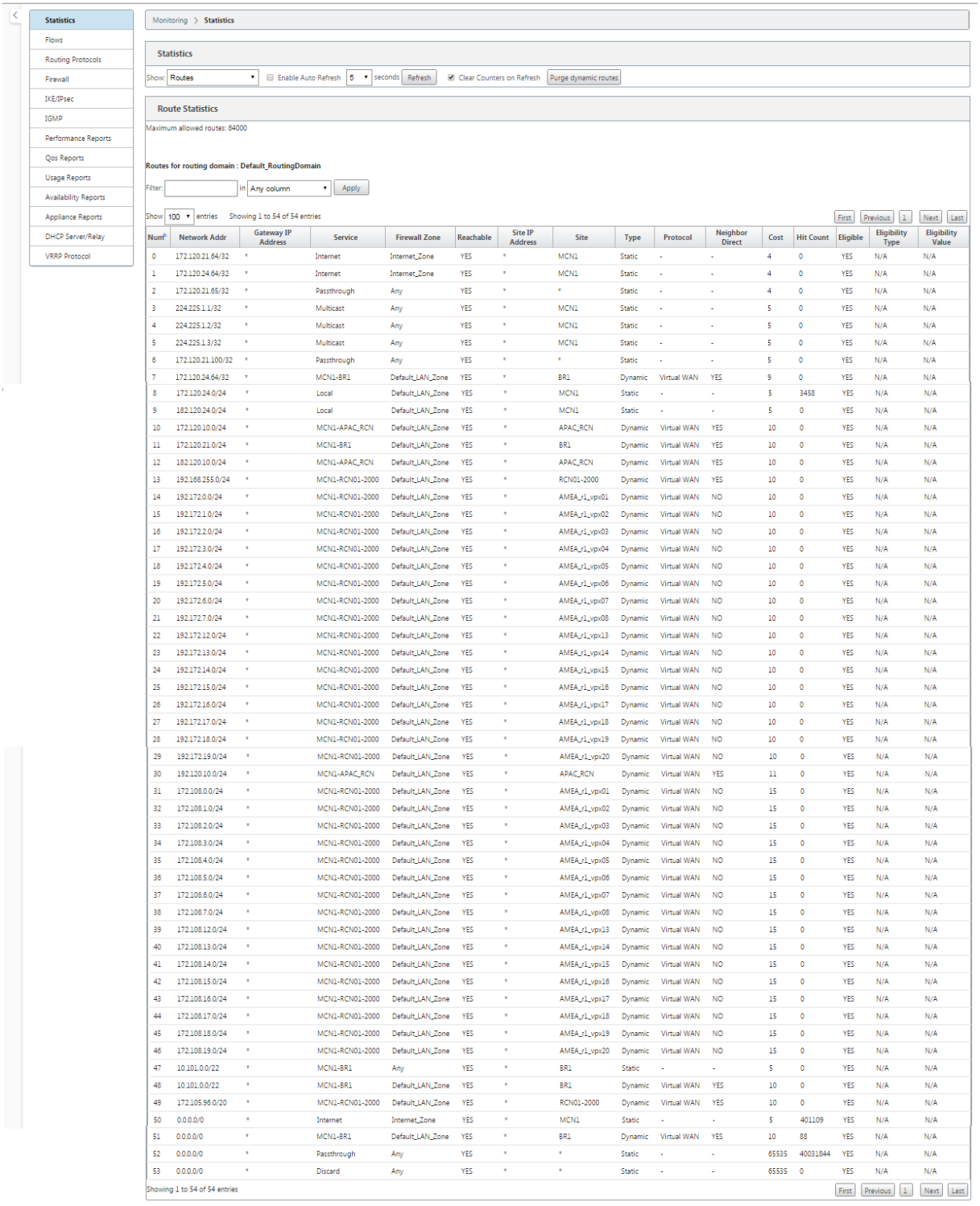
> **Nota**
>
> Las rutas de Internet Service se pueden anunciar a los demás dispositivos SD-WAN o no se pueden exportar en función de si está realizando backhauling de acceso a Internet a través de las rutas virtuales.

- **Passthrough**: Este servicio actúa como último recurso o anula el servicio cuando un dispositivo está en modo en línea. Si una dirección IP de destino no coincide con ninguna otra ruta, el dispositivo SD-WAN simplemente la reenvía al siguiente salto del enlace WAN. Una ruta predeterminada: el coste 0.0.0.0/0 de 16 rutas de paso se crea automáticamente. El acceso directo no funciona cuando el dispositivo SD-WAN se implementa fuera de ruta o en modo Edge/Gateway. Cualquier tráfico que coincida con esta ruta (subred) se clasifica como paso a través para este dispositivo. Se recomienda que el tráfico de paso a través sea lo más limitado posible.

> **Nota**
>
> El paso a través puede ser útil cuando se realiza un POC para evitar tener que configurar numerosas rutas; sin embargo, tenga cuidado en la producción, ya que SD-WAN no tiene en cuenta la utilización del enlace WAN para el tráfico enviado a passthrough. También resulta útil a la hora de solucionar problemas y quiere eliminar cierto flujo de IP de la entrega a través de la ruta virtual.

- **Descartar** - Esto no es un servicio, sino una ruta de último recurso que deja caer los paquetes si coincide. Normalmente, esto no ocurre cuando el dispositivo SD-WAN se implementa fuera del path. Debe tener un servicio de intranet o una ruta local como una ruta de captura de todas las rutas; de lo contrario, el tráfico se descarta porque no hay servicio de paso a través (aunque haya una ruta predeterminada de paso a través).

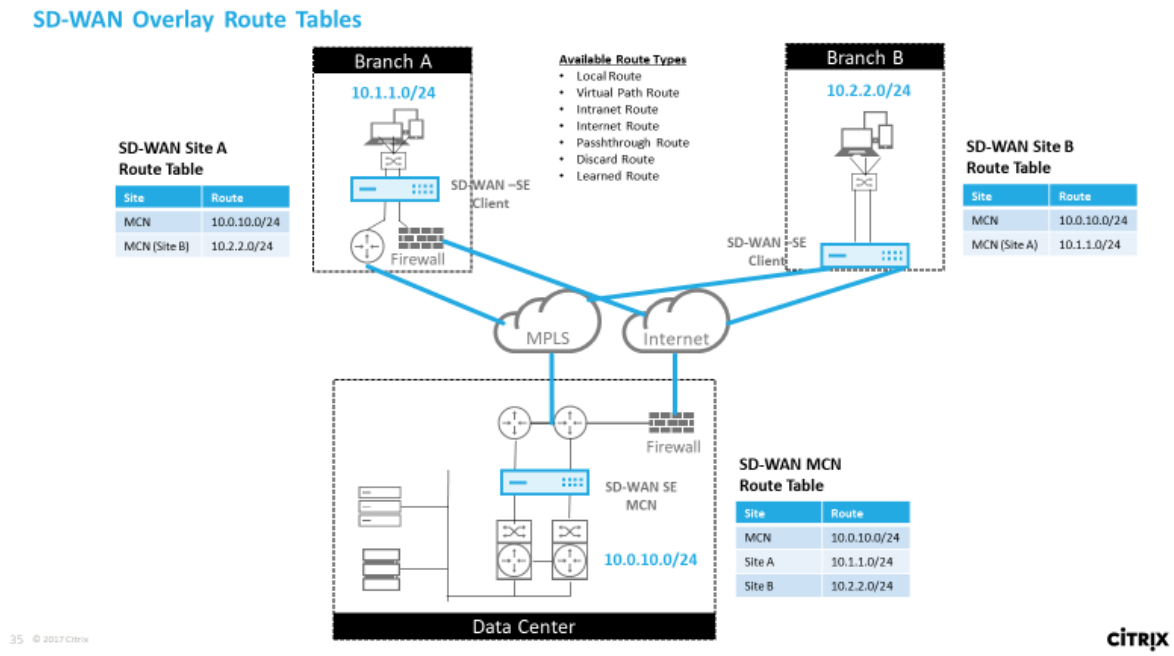
La tabla de rutas para el nodo cliente local se puede supervisar en la página **Supervisión** > **Estadísticas** con Rutas seleccionadas en la lista desplegable **Mostrar**.



Cada ruta para subredes de sucursales remotas se anuncia como un Servicio a través de la Ruta Virtual que se conecta a través del MCN, con la columna **Sitio** rellena con el nodo cliente donde reside el destino como subred local.

En el siguiente ejemplo, con el **reenvío WAN a WAN** (Exportación de rutas) habilitado, la rama A tiene

una entrada de tabla de rutas para la subred Branch B (10.2.2.0/24) a través del MCN como salto siguiente.



Cómo coincide el tráfico de Citrix SD-WAN en rutas definidas

El proceso de coincidencia para las rutas definidas en Citrix SD-WAN se basa en la coincidencia de prefijo más larga para la subred de destino (similar a una operación de enrutador). Cuanto más específica sea la ruta, mayor será el cambio en la misma. La clasificación se realiza en el siguiente orden:

1. Coincidencias de prefijo más largas
2. Coste
3. Servicio

Por lo tanto, una ruta /32 siempre precede a una ruta /31. Para dos rutas /32, una ruta de coste 4 siempre precede a una ruta de coste 5. Para dos rutas /32 cuestan 5, las rutas se eligen según el host IP ordenado. El orden de servicio es el siguiente: Local, Ruta virtual, Intranet, Internet, Passthrough, Descartar.

Como ejemplo, considere las dos rutas siguientes de la siguiente manera:

- 192.168.1.0/24 Coste 5
- 192.168.1.64/26 Coste 10

Un paquete destinado al host 192.168.1.65 usaría esta última ruta aunque el coste sea mayor. En base a esto, es común que la configuración esté en su lugar solo para las rutas destinadas a ser entregadas

a través de la superposición de ruta virtual con otro tráfico que cae en captura todas las rutas, como una ruta predeterminada al servicio de paso a través.

Las rutas se pueden configurar en una tabla de rutas de nodos de sitio que tengan el mismo prefijo. A continuación, el corte de empate va al coste de la ruta, el tipo de servicio (Ruta virtual, Intranet, Internet, etc.) y el siguiente salto IP.

Flujo de paquetes de redirección Citrix SD-WAN

- Coincidencia de rutas de tráfico de LAN a WAN (ruta virtual):
  1. El tráfico entrante lo recibe la interfaz LAN y se procesa.
  2. El marco recibido se compara con la tabla de redirección para la coincidencia de prefijo más larga.
  3. Si se encuentra una coincidencia, el motor de reglas procesa el marco y se crea un flujo en la base de datos de flujo.
- Coincidencia de rutas de tráfico de WAN a LAN (ruta virtual):
  1. SD-WAN recibe el tráfico de ruta virtual desde el túnel y se procesa.
  2. El dispositivo compara la dirección IP de origen para ver si el origen es local.
     - En caso afirmativo, WAN elegible y coincida con el destino IP con la tabla de redirección o ruta virtual.
     - Si no, entonces la comprobación habilitada de reenvío WAN a WAN.
  3. (Reenvío de WAN a WAN desactivado) Reenvío a LAN basado en rutas locales.
  4. (Reenvío de WAN a WAN habilitado) Reenviar a ruta virtual basada en la tabla de rutas.
- Tráfico de ruta no virtual:
  1. El tráfico entrante se recibe en la interfaz LAN y se procesa.
  2. El marco recibido se compara con la tabla de redirección para la coincidencia de prefijo más larga.
  3. Si se encuentra una coincidencia, el motor de reglas procesa el marco y se crea un flujo en la base de datos de flujo.

Compatibilidad con el protocolo de redirección Citrix SD-WAN

Citrix SD-WAN versión 9.1 introdujo los protocolos de redirección OSPF y BGP en la configuración. La introducción de protocolos de redirección en SD-WAN permitió una integración más sencilla de

SD-WAN en redes subyacentes más complejas en las que los protocolos de redirección se utilizan activamente. Con los mismos protocolos de redirección habilitados en SD-WAN Orchestrator Service, se facilitó la configuración de las subredes indicadas para hacer uso de la superposición de SD-WAN. Además, los protocolos de redirección permiten la comunicación entre sitios SD-WAN y sitios que no son SD-WAN con comunicación directa con enrutadores perimetrales del cliente existentes mediante el protocolo de redirección común. Citrix SD-WAN que participa en protocolos de redirección que operan en la red de calco subyacente se puede realizar independientemente del modo de implementación de SD-WAN (modo Inline, modo Inline virtual o modo Edge/Gateway). Además, SD-WAN se puede implementar en modo "solo aprendizaje", donde SD-WAN puede recibir rutas pero no anunciar rutas de vuelta al calco subyacente. Esto resulta útil cuando se introduce la solución SD-WAN en una red donde la infraestructura de redirección es compleja o incierta.

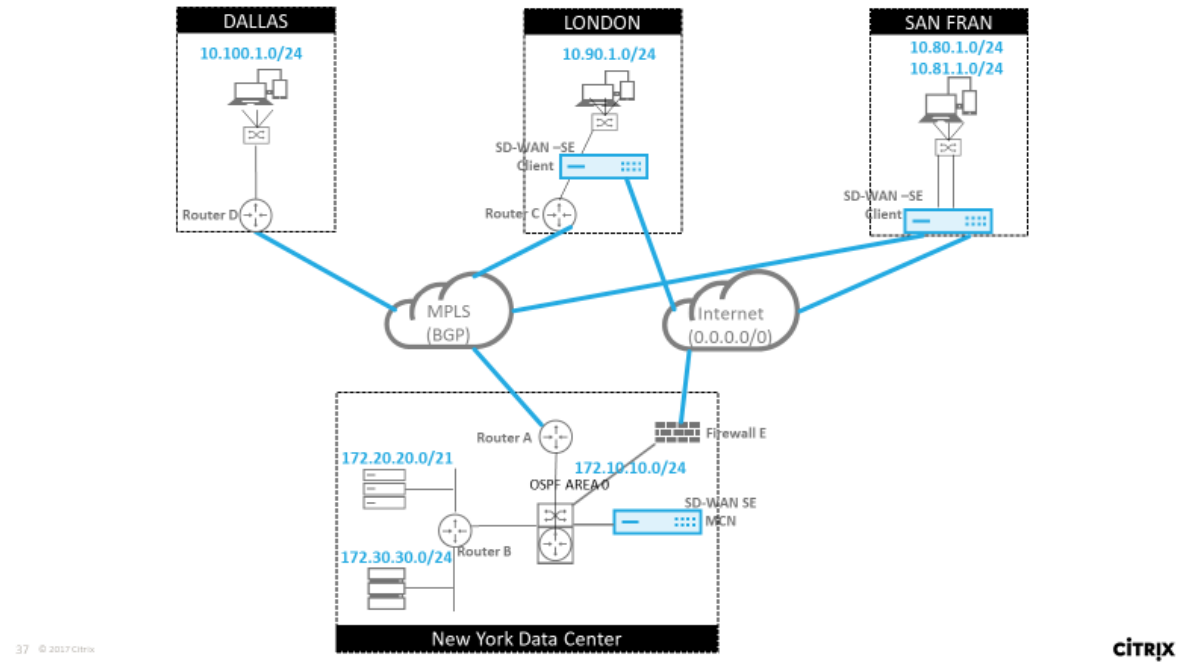
> **Importante**
>
> Es fácil filtrar la ruta no deseada si no tiene cuidado.

La tabla de ruta de ruta de ruta virtual de SD-WAN funciona como un protocolo de puerta de enlace externa (EGP), similar a BGP (pensar sitio a sitio). Por ejemplo, cuando SD-WAN anuncia rutas desde el dispositivo SD-WAN a OSPF, normalmente se consideran externas al sitio y al protocolo.

> **Nota**
>
> Tenga en cuenta los entornos que tienen IGP en toda la infraestructura (a través de la WAN), ya que complican el uso de las rutas anunciadas por SD-WAN. EIGRP se utiliza ampliamente en el mercado y SD-WAN no interopera con ese protocolo.

Un desafío al introducir protocolos de redirección en una implementación SD-WAN es que la tabla de redirección no está disponible hasta que el servicio SD-WAN esté habilitado y funcione en la red; por lo tanto, no se recomienda habilitar inicialmente las rutas de publicidad desde el dispositivo SD-WAN. Utilice los filtros de importación y exportación para una introducción gradual de protocolos de redirección en SD-WAN.

Echemos un vistazo más de cerca revisando el siguiente ejemplo:



En este ejemplo, examinamos un caso de uso del protocolo de redirección. La red anterior tiene cuatro ubicaciones: Nueva York, Dallas, Londres y San Francisco. Implementamos dispositivos SD-WAN en tres de estas ubicaciones y utilizamos SD-WAN para crear una red WAN híbrida donde se utilizarán MPLS y enlaces WAN de Internet para proporcionar una WAN virtualizada. Dado que Dallas no tendrá un dispositivo SD-WAN, debemos considerar la mejor manera de integrarse con los protocolos de ruta existentes a ese sitio para garantizar la conectividad total entre las redes subyacentes y de superposición SD-WAN.

En la red de ejemplo, eBGP se utiliza entre las cuatro ubicaciones de la red MPLS. Cada ubicación tiene su propio número de sistema autónomo (ASN).

En el Centro de datos de Nueva York, OSPF se ejecuta para anunciar las subredes centrales del centro de datos a los sitios remotos y también anunciar una ruta predeterminada desde el Firewall de Nueva York (E). En este ejemplo, todo el tráfico de Internet se redirige al centro de datos, aunque las sucursales de Londres y San Francisco tienen una ruta a Internet.

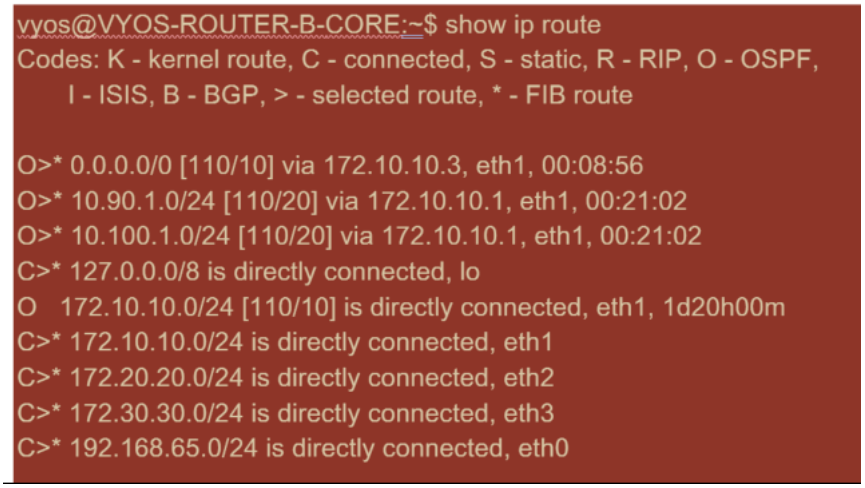
El sitio de San Francisco también debe tenerse en cuenta que no tiene un enrutador. SD-WAN se implementa en modo Edge/Gateway, siendo ese dispositivo la Gateway predeterminada para la subred de San Francisco y también participa en eBGP a MPLS.

- Con el centro de datos de Nueva York, tenga en cuenta que la SD-WAN se implementa en modo virtual en línea. El objetivo es participar en el protocolo de redirección OSPF existente para que el tráfico se reenvíe al dispositivo como Gateway preferida.
- El sitio de Londres se implementa en el modo tradicional en línea. El enrutador WAN ascendente (C) seguirá siendo la puerta de enlace predeterminada para la subred de Londres.
- El sitio de San Francisco es un sitio recientemente introducido en esta red y está previsto que la

SD-WAN se implemente en modo Edge/Gateway y actúe como puerta de enlace predeterminada para la nueva subred de San Francisco.

Revise algunas de las tablas de redirección de calco subyacente existentes antes de implementar SD-WAN.

Enrutador básico B de Nueva York:



Las subredes locales de Nueva York (172.x.x.x) están disponibles en el router B como conectadas directamente, y desde la tabla de rutas identificamos que la ruta predeterminada es 172.10.10.3 (Firewall E). Además, podemos ver que las subredes de Dallas (10.90.1.0/24) y Londres (10.100.1.0/24) están disponibles a través de 172.10.10.1 (enrutador MPLS A). Los costes de la ruta indican que se aprendieron de eBGP.

> **Nota**
>
> En el ejemplo proporcionado, San Francisco no aparece como una ruta, porque aún no hemos implementado el sitio con SD-WAN en modo Edge/Gateway para esa red.


```
vyos@VYATTA-ROUTER-A:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:09:52
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h09m
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 1d23h10m
C>* 127.0.0.0/8 is directly connected, lo
O   172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h01m
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
C>* 192.168.10.0/24 is directly connected, eth2
O   192.168.65.0/24 [110/20] via 172.10.10.2, 1d19h57m
C>* 192.168.65.0/24 is directly connected, eth0
```

Para el router WAN de Nueva York (A), las rutas aprendidas OSPF y las rutas aprendidas a través de MPLS a través de eBGP son rutas enumeradas. Tenga en cuenta los costes de la ruta. BGP es un dominio administrativo y un coste más bajos por defecto 2.0/1 en comparación con OSPF 110/10.

Enrutador Dallas D:

Para Dallas WAN Router (D), todas las rutas se aprenden a través de MPLS.

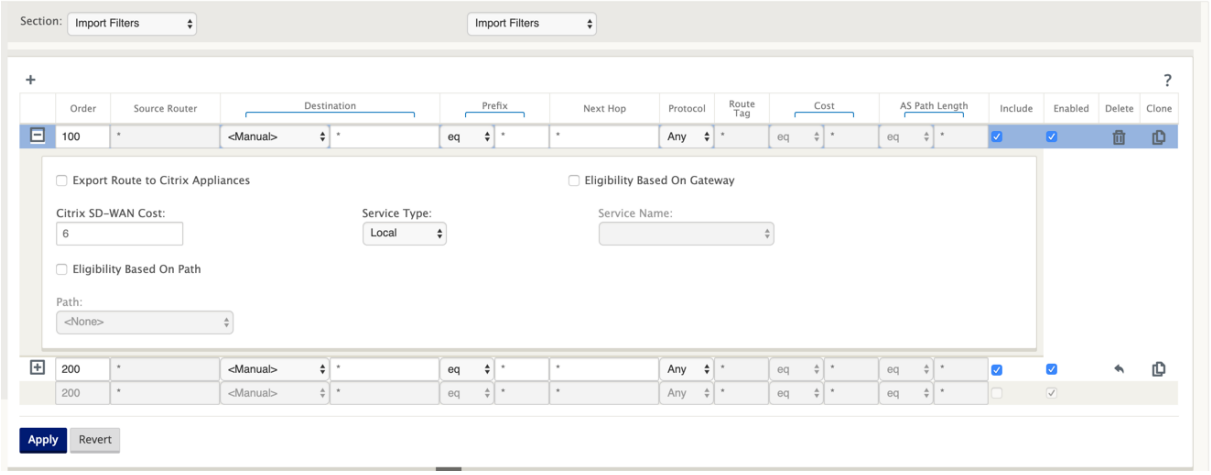
```
vyos@VYATTA-ROUTER-D:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:10:17
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h10m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 1d23h10m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0
```

> **Nota**
>
> En este ejemplo, puede ignorar la subred 192.168.65.0/24. Esta es una red de gestión y no es pertinente al ejemplo. Todos los enrutadores están conectados a la subred de administración, pero no se anuncian en ningún protocolo de redirección.

El eBGP se empareja con cada ubicación. Cada ASN es diferente.

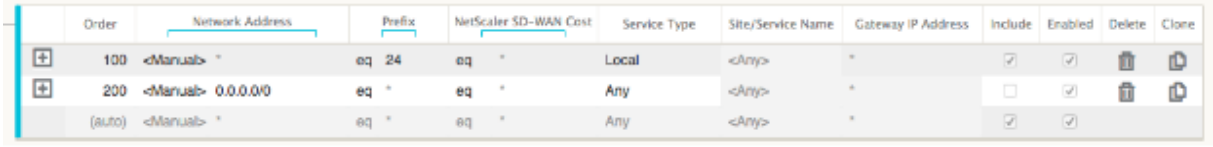
Es importante comprender cómo se pasan las rutas entre la tabla de redirección de ruta virtual y los protocolos de ruta dinámica en uso. Es fácil crear bucles de redirección o anunciar rutas de una manera adversa. El mecanismo de filtro nos da la capacidad de controlar lo que entra y sale de la tabla de redirección. Consideramos cada ubicación a su vez.

- La ubicación de San Francisco tiene dos subredes locales **10.80.1.0/24** y **10.81.1.0/24**. Queremos anunciarlos a través de eBGP para que sitios como Dallas todavía puedan llegar al sitio de San Francisco a través de la red subyacente y también sitios como Londres y Nueva York puedan llegar a San Francisco a través de la red de superposición de Ruta Virtual. También queremos aprender de la accesibilidad de eBGP a todos los sitios en caso de que la superposición de SD-WAN Virtual Path se deshaga y el entorno deba volver a utilizar solo el MPLS. Tampoco queremos volver a anunciar nada que SD-WAN aprenda de eBGP a los routers SD-WAN. Para lograr esto, los filtros deben configurarse de la siguiente manera:
- Importe todas las rutas desde eBGP. No leer/exportar rutas a dispositivos SD-WAN.



- Exportar rutas locales a eBGP

La regla por defecto para exportar es exportar todo. La regla 200 se utiliza para anular la regla de errores para no volver a anunciar las rutas. Cualquier ruta que coincida con cualquier prefijo SD-WAN ha aprendido a través de las rutas virtuales.



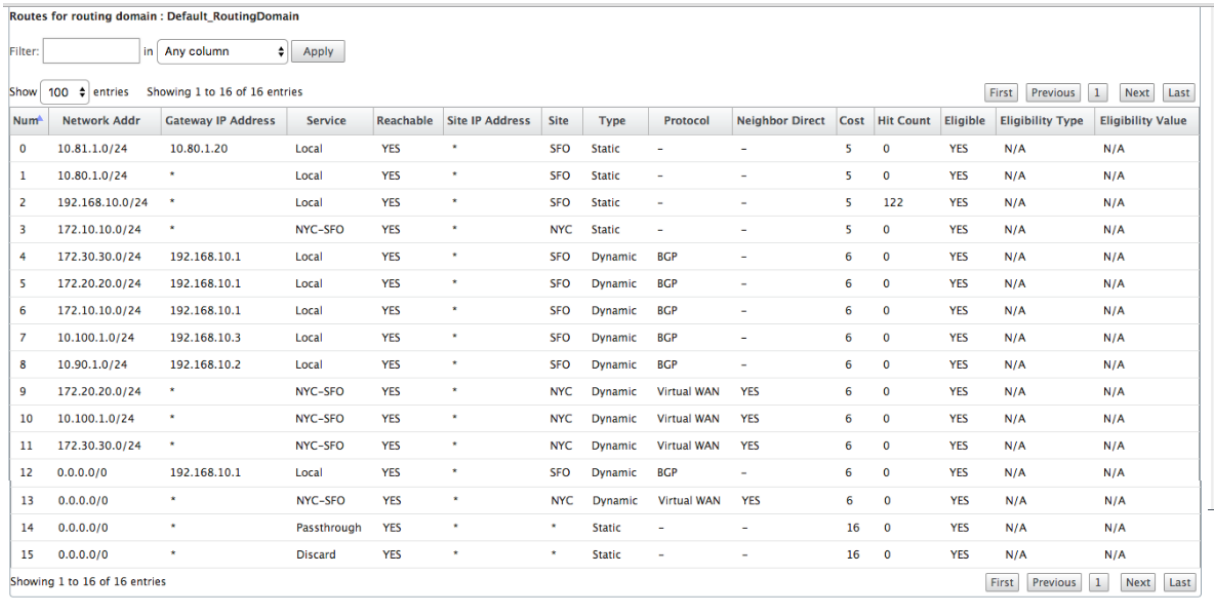
Después de implementar los dispositivos Citrix SD-WAN, podemos revisar las tablas de ruta para el router BGP en el sitio de Dallas. Vemos que las subredes 10.80.1.0/24 y 10.81.1.0/24 se ven correctamente a través de eBGP desde la SD-WAN de San Francisco.

Enrutador Dallas D:


```
vyos@VYATTA-ROUTER-D:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:00:01
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 4d23h38m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 4d23h38m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B   192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 3d19h07m
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0
```

Además, la tabla de rutas Citrix SD-WAN se puede ver en la página **Supervisión** > **Estadísticas** > **Mostrar rutas**.

Citrix SD-WAN de San Francisco:



Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 16 of 16 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	10.81.1.0/24	10.80.1.20	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
1	10.80.1.0/24	*	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
2	192.168.10.0/24	*	Local	YES	*	SFO	Static	-	-	5	122	YES	N/A	N/A
3	172.10.10.0/24	*	NYC-SFO	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
4	172.30.30.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
5	172.20.20.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
6	172.10.10.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	192.168.10.3	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	10.90.1.0/24	192.168.10.2	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
9	172.20.20.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
10	10.100.1.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
11	172.30.30.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
12	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
13	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 16 of 16 entries First Previous 1 Next Last

Citrix SD-WAN muestra todas las rutas aprendidas, incluidas las rutas disponibles a través de la superposición de ruta virtual.

Consideremos 172.10.10.0/24, que se encuentra en el Centro de Datos de Nueva York. Esta ruta se aprende de dos maneras:

- Como ruta de ruta virtual (número 3), servicio = NYC-SFO con un coste de 5 y escriba estático. Se trata de una subred local anunciada por el dispositivo SD-WAN en Nueva York. Es estático

porque está conectado directamente al dispositivo o es una ruta estática manual introducida en la configuración. Es accesible porque la ruta virtual entre los sitios está en estado de trabajo/funcionamiento.

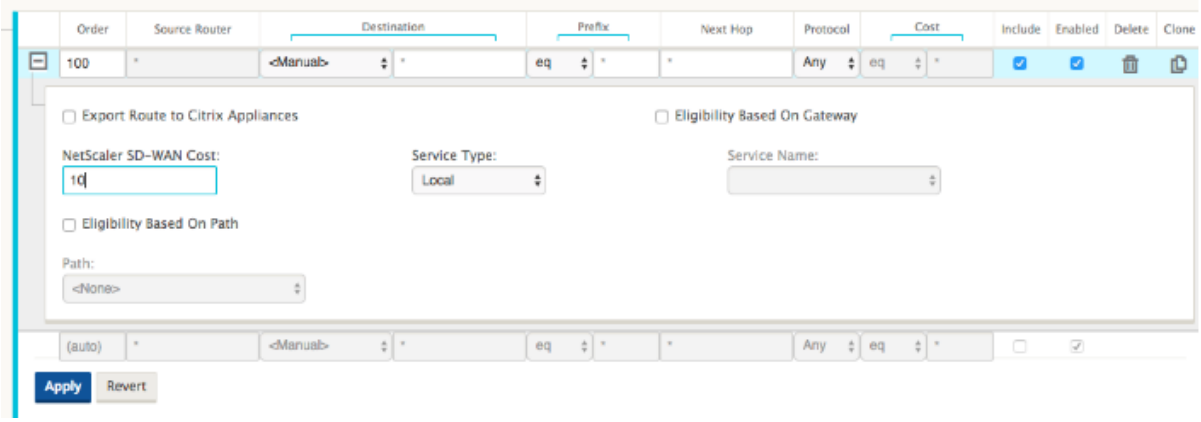
- Como ruta anunciada a través de BGP (Número 6), con un coste de 6. Ahora se considera una ruta alternativa.

Dado que el prefijo es igual y el coste es diferente, SD-WAN utiliza la ruta de ruta virtual a menos que no esté disponible, en cuyo caso la ruta de reserva se aprende a través de BGP.

Ahora, consideremos la ruta 172.20.20.0/24.

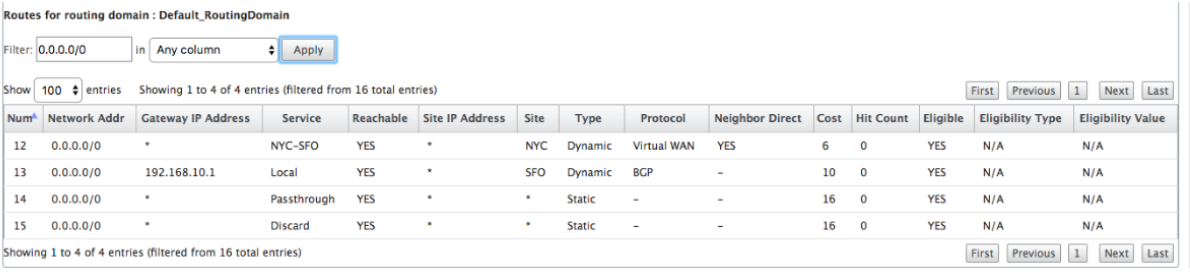
- Esto se aprende como una ruta de ruta virtual (número 9) pero tiene un tipo de dinámica y un coste de 6. Esto significa que el dispositivo SD-WAN remoto aprendió esta ruta a través de un protocolo de redirección, en este caso OSPF. De forma predeterminada, el coste de la ruta es mayor.
- SD-WAN también aprende esta ruta a través de BGP con el mismo coste, por lo que en este caso esta ruta podría ser preferida sobre la ruta Ruta Virtual.

Para garantizar la redirección correcta, debemos aumentar el coste de la ruta BGP para asegurarnos de que tenemos una ruta de ruta virtual y es la ruta preferida. Esto se puede hacer ajustando el peso de la ruta del filtro de importación para que sea mayor que el valor predeterminado de 6.



Después de realizar el ajuste, podemos actualizar la tabla de rutas SD-WAN en el dispositivo de San Francisco para ver los costes de ruta ajustados. Utilice la opción de filtro para enfocar la lista mostrada.

Finalmente, echemos un vistazo a la ruta predeterminada aprendida en la SD-WAN de San Francisco. Queremos hacer backhaul todo el tráfico de internet a Nueva York. Podemos ver que lo enviamos mediante la Ruta Virtual, si está activa, o a través de la red MPLS como alternativa.



Routes for routing domain : Default_RoutingDomain

Filter: 0.0.0.0/0 in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries (filtered from 16 total entries) First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
12	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
13	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	10	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 4 of 4 entries (filtered from 16 total entries) First Previous 1 Next Last

También vemos una ruta de paso y descarte con coste 16. Se trata de rutas automáticas que no se pueden quitar. Si el dispositivo está en línea, la ruta de paso se utiliza como último recurso, por lo que si un paquete no puede coincidir con una ruta más específica, SD-WAN lo pasará al siguiente salto del grupo de interfaces. Si la SD-WAN está fuera de ruta o en modo edge/gateway, no hay servicio de paso, en cuyo caso SD-WAN descarta el paquete utilizando la ruta de descarte predeterminada. El recuento de aciertos indica el número de paquetes que llegan a cada ruta, lo que puede ser valioso para solucionar problemas.

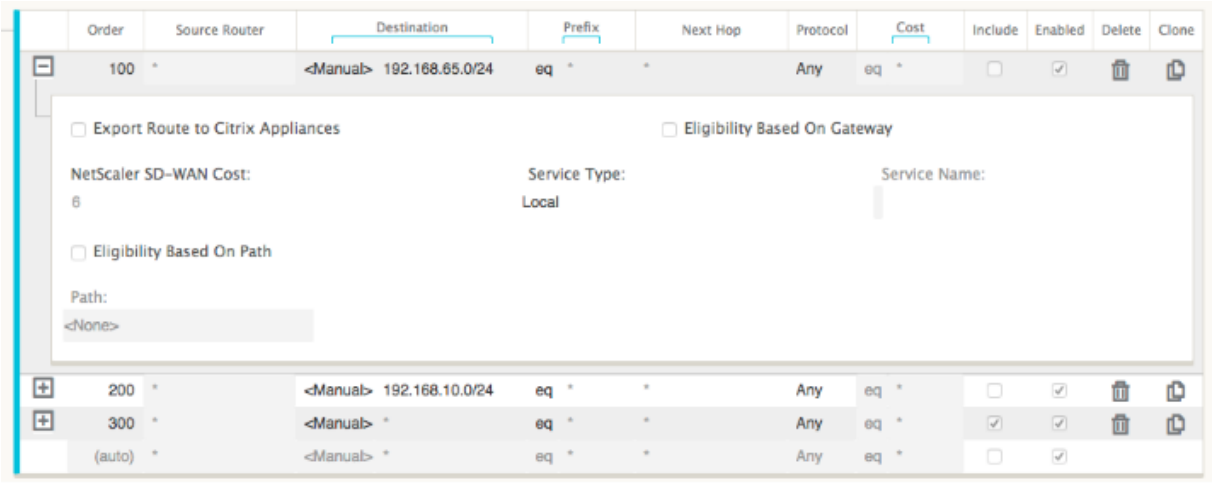
Ahora, centrándonos en el sitio de Nueva York, queremos que el tráfico destinado a sitios remotos (Londres y San Francisco) se dirija al dispositivo SD-WAN cuando la ruta virtual está activa.

Hay varias subredes disponibles en el sitio de Nueva York:

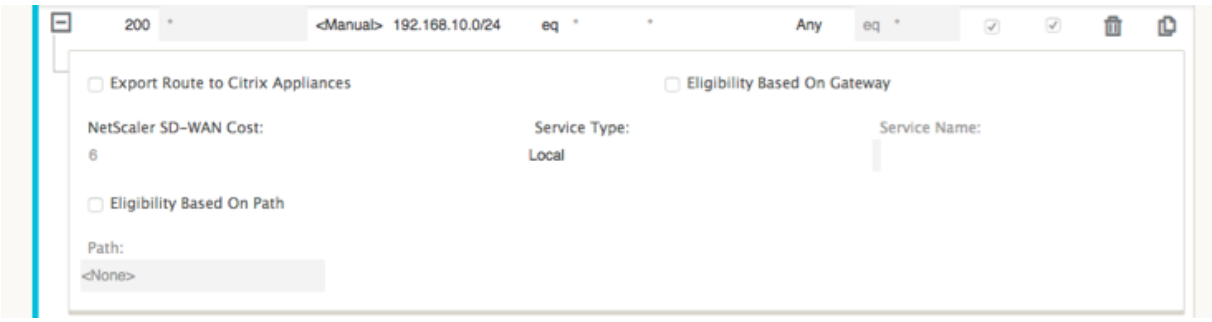
- 172.10.10.0/24 (conectado directamente)
- 172.20.20.0/24 (anunciado a través de OSPF desde el router principal B)
- 172.30.30.0/24 (anunciado a través de OSPF desde el router principal B)

También tenemos la obligación de proporcionar flujo de tráfico a Dallas (10.100.1.0/24) a través de MPLS.

Por último, queremos que todo el tráfico enlazado a Internet se dirija al Firewall E a través de 172.10.10.3 como próximo salto. SD-WAN aprende esta ruta predeterminada a través de OSPF y para anunciarse en la ruta virtual. Los filtros para el sitio de Nueva York son:

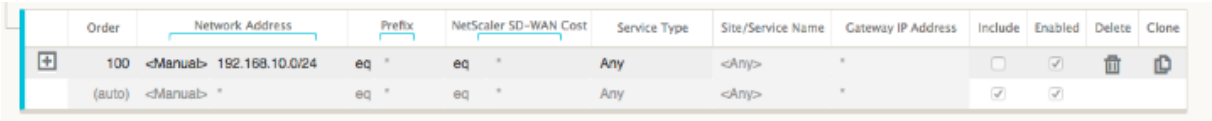


El sitio SD-WAN de Nueva York importa todas las rutas para la red de administración. Esto se puede ignorar. Podemos centrarnos en el filtro 200.



El filtro 200 se utiliza para importar 192.168.10.0/24 (nuestro núcleo MPLS) para la accesibilidad, pero no para exportarlo a la ruta virtual. Marque la casilla **Incluir** y asegúrese de que la casilla **Exportar ruta a Citrix Appliances** está desactivada. Todas las demás rutas se incluyen a continuación.

Para los filtros de exportación, podemos excluir la ruta para 192.168.10.0/24. Esto se debe a que, como subred conectada directamente en el sitio de San Francisco, no podemos filtrar esta ruta en el origen, por lo que se suprime en este extremo.



Ahora vamos a revisar la tabla de rutas actualizadas comenzando en la ruta principal en el sitio de Nueva York.

Router B de Nueva York:


```
vyos@VYOS-ROUTER-B-CORE:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 4d22h22m
O>* 10.80.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h49m
O>* 10.81.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h49m
O>* 10.90.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h50m
O>* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 4d22h22m
C>* 127.0.0.0/8 is directly connected, lo
O   172.10.10.0/24 [110/10] is directly connected, eth1, 4d22h22m
C>* 172.10.10.0/24 is directly connected, eth1
C>* 172.20.20.0/24 is directly connected, eth2
C>* 172.30.30.0/24 is directly connected, eth3
C>* 192.168.65.0/24 is directly connected, eth0
```

Podemos ver las subredes para San Francisco (10.80.1.0 y 10.81.1.0) y Londres (10.90.1.0) que ahora se anuncian a través del dispositivo SD-WAN de Nueva York (172.10.10.10). La ruta 10.100.1.0/24 se sigue anunciando a través del enrutador MPLS A subyacente. Revisemos la tabla de rutas SD-WAN del sitio de Nueva York.

Tabla de rutas SD-WAN del sitio de Nueva York:

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 11 of 11 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.10.10.0/24	*	Local	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
1	10.90.1.0/24	*	NYC-LON	YES	*	LON	Static	-	-	5	0	YES	N/A	N/A
2	10.81.1.0/24	10.80.1.20	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
3	10.80.1.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
4	192.168.10.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
5	172.30.30.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	172.20.20.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	172.10.10.1	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	0.0.0.0/0	172.10.10.3	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
10	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Podemos ver las rutas correctas tanto para las subredes locales aprendidas a través de OSPF, una ruta al sitio de Dallas aprendida del Router A MPLS y las subredes remotas para los sitios de San Francisco y Londres. Veamos el enrutador MPLS A. Este enrutador está participando en OSPF y BGP.


```
vyos@VYATTA-ROUTER-A:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:04:12
O   10.80.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
O   10.81.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
O   10.90.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 00:05:11
S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 00:04:28
C>* 127.0.0.0/8 is directly connected, lo
O   172.10.10.0/24 [110/10] is directly connected, eth1, 00:05:24
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
B   192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 00:05:09
C>* 192.168.10.0/24 is directly connected, eth2
O   192.168.65.0/24 [110/20] via 172.10.10.2, 00:04:12
C>* 192.168.65.0/24 is directly connected, eth0
```

Desde la tabla de rutas, este Router A está aprendiendo las subredes remotas a través de BGP y OSPF, con la distancia administrativa y el coste de la ruta BGP (20/5) siendo inferiores a OSPF (110/10) y, por lo tanto, preferidos. En este ejemplo, red donde solo hay una ruta principal, esto podría no causar preocupación. Sin embargo, el tráfico que llega aquí se entregaría a través de la red MPLS en lugar de enviarse al dispositivo SD-WAN (172.10.10.10). Si queremos mantener la simetría de redirección completa, necesitaríamos un mapa de ruta para ajustar el coste AD/métrico de modo que haya preferencia de ruta desde la ruta 172.10.10.10 en lugar de la ruta aprendida a través de eBGP.

Alternativamente, se puede configurar una ruta "backdoor"para obligar al router a preferir la ruta OSPF sobre la ruta BGP. Observe la ruta estática de la dirección IP virtual SD-WAN al dispositivo SD-WAN del sitio de Londres.

```
S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2
```

Esto es necesario para garantizar que la ruta de acceso virtual se vuelva a redirigir al dispositivo SD-WAN del sitio de Nueva York si la ruta de acceso MPLS falla. Dado que hay una ruta para 10.90.1.0/24 que se anuncia a través de 172.10.10.10 (SD-WAN de Nueva York). También se recomienda crear una regla de servicio de anulación para descartar cualquier paquete UDP de 4.980 en el dispositivo SD-WAN para evitar que la ruta virtual vuelva a sí misma.

Rutas virtuales dinámicas

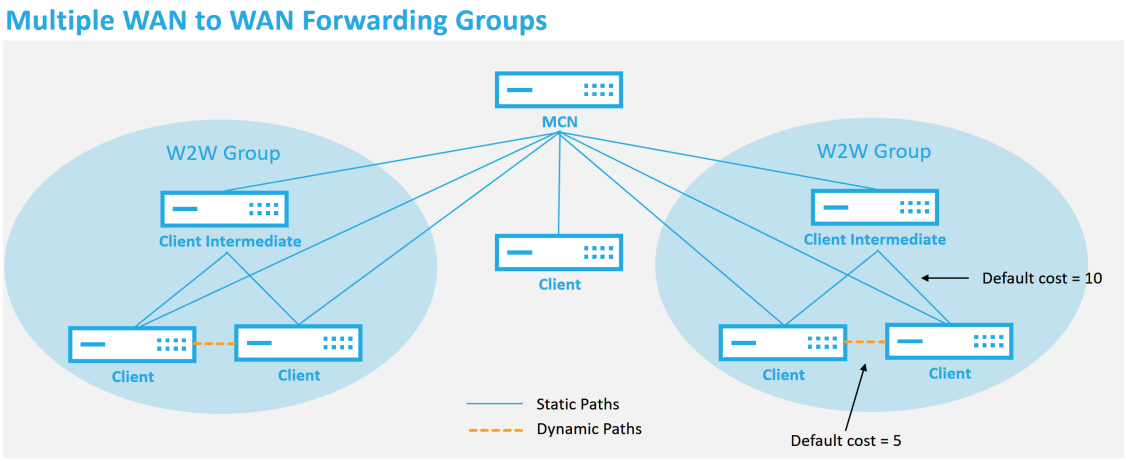
Se pueden permitir rutas virtuales dinámicas entre dos nodos de cliente para crear rutas virtuales a demanda para la comunicación directa entre los dos sitios. La ventaja de una ruta virtual dinámica es que el tráfico puede fluir directamente de un nodo cliente al segundo sin tener que atravesar el MCN o dos rutas virtuales, lo que puede agregar latencia al flujo de tráfico. Las rutas virtuales dinámicas se crean y eliminan dinámicamente en función de los umbrales de tráfico definidos por el usuario. Estos umbrales se definen como paquetes por segundo (pps) o ancho de banda (kbps). Esta funcionalidad permite una topología de superposición SD-WAN dinámica de malla completa.

Una vez que se alcanzan los umbrales de las rutas virtuales dinámicas, los nodos cliente crean dinámicamente su ruta virtualizada entre sí mediante todas las rutas de acceso WAN disponibles entre los sitios y la utilizan al máximo de la siguiente manera:

- Envíe datos masivos si existe alguno y verifique que no haya pérdida,
- Envíe datos interactivos y verifique que no haya pérdidas,
- Enviar datos en tiempo real después de que los datos masivos e interactivos se consideren estables (sin pérdida ni niveles aceptables)
- Si no hay datos masivos o interactivos, envíe datos en tiempo real después de que la ruta virtual dinámica haya estado estable durante un período
- Si los datos del usuario caen por debajo de los umbrales configurados para un período definido por el usuario, la ruta virtual dinámica se derrumba

Las rutas virtuales dinámicas tienen el concepto de un sitio intermedio. El sitio intermedio puede ser un sitio MCN o cualquier otro sitio de la red que tenga Ruta virtual estática configurada y conectada a dos o más nodos cliente. Otro requisito de consideración de diseño es tener habilitado el reenvío WAN a WAN, permitiendo que todas las rutas de todos los sitios se publiquen a los nodos cliente donde se quiera la ruta virtual dinámica.

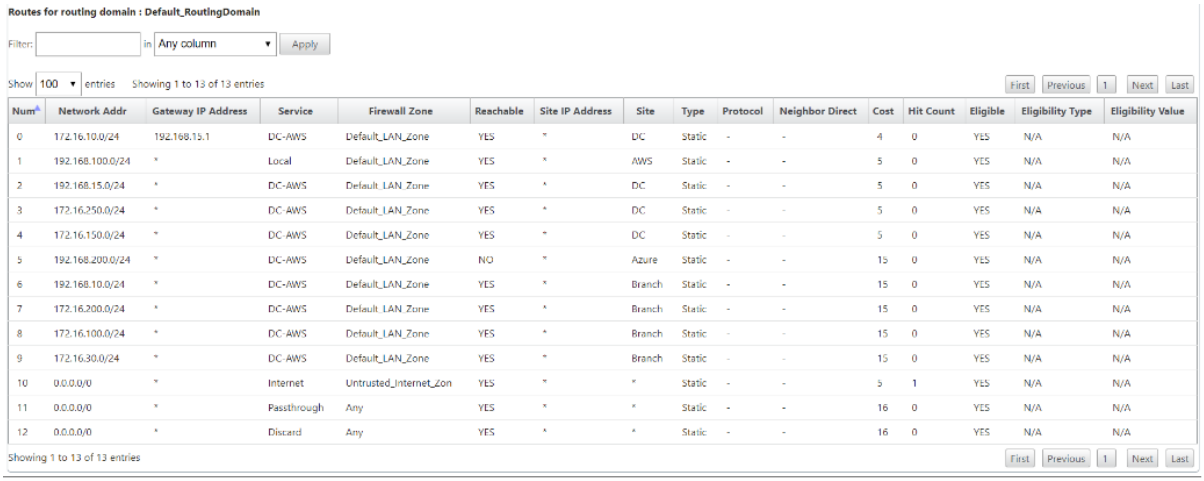
Se permiten varios grupos de reenvío de WAN a WAN en SD-WAN, lo que permite un control total del establecimiento de rutas entre ciertos nodos de cliente y no entre otros.



Cada dispositivo SD-WAN tiene su propia tabla de rutas única con los siguientes detalles definidos para cada ruta:

- Número: orden de ruta de este dispositivo según el proceso de coincidencia (el número más bajo se procesa primero)
- Dirección de red: dirección de subred o host
- Gateway si es necesario
- Servicio: qué servicio se aplica para esta ruta
- Zona de firewall: la clasificación de la zona de firewall de la ruta
- Se puede acceder: identifica si el estado de ruta virtual está activo para este sitio
- Sitio: nombre del sitio donde se espera que exista la ruta
- Tipo —Identificación del tipo de ruta (estática o dinámica)
- Vecino directo
- Coste - coste de la ruta específica
- Recuento de visitas: cuántas veces se ha utilizado la ruta por paquete. Esto se usaría para verificar que una ruta se está golpeando correctamente.
- Elegible
- Tipo de elegibilidad
- Valor de elegibilidad

A continuación se muestra un ejemplo de tabla de ruta del sitio SD-WAN:



Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 13 of 13 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.16.10.0/24	192.168.15.1	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	4	0	YES	N/A	N/A
1	192.168.100.0/24	*	Local	Default_LAN_Zone	YES	*	AWS	Static	-	-	5	0	YES	N/A	N/A
2	192.168.15.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
3	172.16.250.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
4	172.16.150.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
5	192.168.200.0/24	*	DC-AWS	Default_LAN_Zone	NO	*	Azure	Static	-	-	15	0	YES	N/A	N/A
6	192.168.10.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
7	172.16.200.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
8	172.16.100.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
9	172.16.30.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
10	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	1	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 13 of 13 entries First Previous 1 Next Last

Observe en la tabla de rutas SD-WAN anterior que hay más elementos que normalmente no están disponibles en los routers tradicionales. Lo más notable es la columna Accesible, que hace que la ruta sea activa o inactiva (sí/no) dependiendo del estado de la ruta WAN. Las rutas enumeradas aquí se suprimen en función de varios estados del servicio (la ruta virtual está inactiva como ejemplo). Otros eventos que pueden forzar que una ruta no sea elegible son el estado de la ruta hacia abajo, el salto siguiente inalcanzable o el enlace WAN hacia abajo.

De la tabla anterior, podemos ver 14 rutas definidas. A continuación se describe una descripción de las rutas o grupos de rutas:

- Ruta 0: En el MCN se trata de una ruta de subred de host que reside en el sitio de DC. 172.16.10.0/24 reside en la LAN de DC y 192.168.15.1 es la Gateway de la LAN que es el siguiente salto que llegará a esa subred.
- Ruta 1: se trata de una ruta local a este dispositivo SD-WAN que muestra la tabla de rutas.
- Ruta 2—4: son las subredes que forman parte de las interfaces virtuales configuradas para la SD-WAN del sitio de DC. Estas subredes se derivan de las interfaces virtuales de confianza definidas.
- Ruta 5: se trata de una ruta compartida a otro nodo de cliente que comparte el MCN con un estado de accesibilidad de No debido a la ruta virtual inactiva entre ese sitio y el MCN.
- Ruta 6—9: estas rutas existen en otro sitio cliente. Para esta ruta, se crea una ruta de ruta virtual para que coincida con el tráfico de entrada de WAN destinado al sitio remoto en la ruta virtual.
- Ruta 10: Con el servicio de Internet definido, el sistema agrega una ruta de captura de todas las rutas para la ruptura directa de Internet para este sitio local.
- Ruta 11 —Passthrough es la ruta predeterminada que el sistema siempre agrega para permitir que los paquetes fluyan a través en caso de que no haya coincidencia en ninguna ruta existente. El paso a través no está arreglado, normalmente las difusiones locales y el tráfico ARP se asignan a este servicio.

- Ruta 12 —Descartar es la ruta predeterminada que el sistema siempre agrega para soltar cualquier cosa indefinida.

Los valores de coste de ruta por defecto:

- Reenvío de WAN a WAN: 10
- Coste de ruta directa predeterminado —5
- Rutas generadas automáticamente —5
- Ruta virtual —5
- Local —5
- Intranet —5
- Internet —5
- Paso a través —5
- Opcional: la ruta es 0.0.0.0/0 definida como nivel de servicio

Después de definir estas rutas, es importante comprender cómo fluye el tráfico utilizando las rutas definidas. Estos flujos de tráfico se dividen en los siguientes flujos:

- LAN a WAN (ruta virtual): tráfico que entra en el túnel de superposición SD-WAN
- WAN a LAN (ruta virtual): tráfico existente en el túnel de superposición SD-WAN
- Tráfico de ruta no virtual: tráfico enrutado a la red subyacente

Rutas de intranet e Internet

Para los tipos de servicio de Intranet e Internet, el usuario debe haber definido un enlace WAN SD-WAN para admitir esos tipos de servicios. Es un requisito previo para cualquier ruta definida para cualquiera de estos servicios. Si el enlace WAN no está definido para admitir el servicio de intranet, se considera una ruta local. Las rutas de Intranet, Internet y PassThrough solo son relevantes para el sitio/dispositivo para el que están configurados.

Al definir rutas de Intranet, Internet o PassThrough, se incluyen las siguientes consideraciones de diseño:

- Debe tener un servicio definido en el enlace WAN (Intranet/Internet; requerido)
- La intranet/Internet debe tener una puerta de enlace definida para el enlace WAN
- Relevante para el dispositivo SD-WAN local
- Las rutas de Intranet se pueden aprender a través de la Ruta Virtual, pero se hacen a un coste más alto

- Con el servicio de Internet, hay automáticamente una ruta predeterminada creada (0.0.0.0/0) captura todas las rutas con un coste máximo
- No asuma que Passthrough funciona, debe probarse o verificarse, también probar con Virtual Path inactivado/inhabilitado para verificar el comportamiento deseado
- Las tablas de redirección son estáticas a menos que la función de aprendizaje de rutas esté habilitada

  El límite máximo admitido para varios parámetros de redirección es el siguiente:

- Dominios de redirección máximos: 255
- Interfaces de acceso máximas por enlace WAN: 64
- Número máximo de vecinos BGP por sitio: 255
- Área OSPF máxima por sitio: 255
- Interfaces virtuales máximas por área OSPF: 255
- Filtros de importación máximos de aprendizaje de ruta por sitio: 512
- Filtros de exportación máximos de aprendizaje de ruta por sitio: 512
- Máximo de directivas de redirección BGP: 255
- Máximo de objetos de cadena de comunidad BGP: 255

Dominio de redirección

August 26, 2022

Citrix SD-WAN permite segmentar redes para obtener más seguridad y capacidad de administración mediante el dominio de redirección. Por ejemplo, puede separar el tráfico de red invitado del tráfico de empleados, crear dominios de redirección distintos para segmentar grandes redes corporativas y segmentar el tráfico para admitir varias redes de clientes. Cada dominio de redirección tiene su propia tabla de redirección y habilita la compatibilidad con subredes IP superpuestas.

Los dispositivos Citrix SD-WAN implementan protocolos de redirección OSPF y BGP para los dominios de redirección para controlar y segmentar el tráfico de red.

Una ruta virtual puede comunicarse mediante todos los dominios de redirección independientemente de la definición del punto de acceso. Esto es posible porque la encapsulación SD-WAN incluye la información del dominio de redirección para el paquete. Por lo tanto, ambas redes finales saben a dónde pertenece el paquete. No es necesario crear un enlace WAN o una interfaz de acceso para cada dominio de redirección.

A continuación se presenta la lista de puntos a tener en cuenta al configurar la funcionalidad de dominio de redirección:

- De forma predeterminada, los dominios de redirección están habilitados en un MCN.
- Los dominios de redirección están habilitados en los sitios de la sucursal.
- Cada dominio de redirección habilitado debe tener una interfaz virtual y una IP virtual asociadas a él.
- La selección de redirección forma parte de todas las configuraciones siguientes:
  - Grupo de interfaces
  - IP virtual
  - GRE
  - Enlace WAN -> Interfaz de acceso
  - Túneles IPsec
  - Rutas
  - Reglas
- Los dominios de redirección se exponen en la configuración de la interfaz web cuando se crean varios dominios.
- Para un enlace público a Internet, solo se puede crear una interfaz de acceso principal y secundaria.
- Para un vínculo Intranet/MPLS privado, se puede crear una interfaz de acceso primaria y secundaria por dominio de redirección.

Configurar dominio de redirección

August 26, 2022

Los dispositivos Citrix SD-WAN permiten configurar protocolos de redirección que proporcionan un único punto de administración para administrar una red corporativa, una red de sucursales o una red de centros de datos. Puede configurar hasta 254 dominios de redirección.

Con la versión 11.0.2, se permite la **redirección de dominios sin IP virtuales (VIP) redirigibles** con las siguientes capacidades:

- Permitir que un dispositivo tenga un dominio de redirección para interfaces que no sean de confianza o que no sean de confianza.
- Permitir que las sucursales se comuniquen entre sí a través de un dominio de redirección que no tenga presencia física en un sitio intermedio.

Usar CLI para acceder a la redirección

August 26, 2022

En la versión 10.0 de Citrix SD-WAN, puede ver información adicional relacionada con la redirección dinámica y el estado del protocolo. Escriba el siguiente comando y sintaxis para acceder al demonio de redirección y ver la lista de comandos.

```
dynamic_routing?
<!--NeedCopy-->
```

Redirección dinámica

August 26, 2022

Citrix SD-WAN admite los siguientes dos protocolos de redirección dinámica:

- Abrir primero el trayecto más corto (OSPF)
- Protocolo de puerta de enlace de frontera (BGP)

Antes de la versión 11.3.1 de Citrix SD-WAN, las capacidades de redirección dinámico solo estaban disponibles para un único ID de enrutador. Puede configurar un ID de enrutador único globalmente para todo el protocolo (uno para OSPF y BGP) o no proporcionar ningún ID de enrutador. Si no se proporciona un ID de enrutador, la IP más baja de las instancias de red virtual (VNIs) que participan en la redirección dinámica se selecciona automáticamente como ID de enrutador predeterminado.

A partir de la versión 11.3.1 de Citrix SD-WAN, no solo puede configurar un ID de enrutador para todo el protocolo, sino también configurar un ID de enrutador para cada dominio de redirección. Con esta mejora, puede habilitar la redirección dinámica estable en varias instancias con diferentes ID de enrutador convergiendo de manera estable.

Si configura un ID de enrutador para un dominio de redirección específico, el ID de enrutador específico anula el dominio de redirección de nivel de protocolo.

OSPF

OSPF es un protocolo de redirección desarrollado para redes de Protocolo de Internet (IP) por el grupo de Protocolo de puerta de enlace interior (IGP) del Grupo de Trabajo de Ingeniería de Internet (IETF). Incluye la primera versión del protocolo de redirección de sistema intermedio a sistema intermedio (IS-IS) de OSI.

El protocolo OSPF está abierto, lo que significa que su especificación es de dominio público (RFC 1247). OSPF se basa en el algoritmo Shortest Path First (SPF) llamado Dijkstra. Es un protocolo de redirección de estado de vínculo que llama al envío de anuncios de estado de vínculo (LSA) a todos los demás enrutadores dentro de la misma área jerárquica. La información sobre interfaces adjuntas, métricas utilizadas y otras variables se incluye en los LSA OSPF. Los enrutadores OSPF acumulan información de estado de vínculo, que es utilizada por el algoritmo SPF para calcular la ruta más corta a cada nodo.

> **Nota**
>
> - Los dispositivos Citrix SD-WAN no participan como enrutador designado (DR) ni BDR (enrutador designado de respaldo) en cada red de acceso múltiple, ya que la prioridad de recuperación ante desastres predeterminada se establece en "0. "
> - El dispositivo Citrix SD-WAN no admite el resumen como enrutador de borde de área (ABR).

BGP

BGP es un protocolo de redirección de sistema interautónomo. Una red autónoma o un grupo de redes se administra bajo una administración común y con directivas de redirección comunes. BGP se utiliza para intercambiar información de redirección para Internet y es el protocolo utilizado entre los ISP. Las redes de clientes implementan protocolos de Gateway Interior como RIP u OSPF para el intercambio de información de redirección dentro de sus redes. Los clientes se conectan a ISP y los ISP usan BGP para intercambiar rutas de clientes e ISP. Cuando se utiliza BGP entre sistemas autónomos (AS), el protocolo se denomina BGP externo (EBGP). Si un proveedor de servicios utiliza BGP para intercambiar rutas dentro de un AS, el protocolo se denomina BGP interior (IBGP).

BGP es un protocolo de redirección robusto y escalable implementado en Internet. Para lograr la escalabilidad, BGP utiliza muchos parámetros de ruta llamados atributos para definir directivas de redirección y mantener un entorno de redirección estable. Los vecinos BGP intercambian información de redirección completa cuando se establece por primera vez la conexión TCP entre vecinos. Cuando se detectan cambios en la tabla de redirección, los enrutadores BGP envían a sus vecinos aquellas rutas que han cambiado. Los enrutadores BGP no envían actualizaciones periódicas de redirección y anuncian la ruta óptima a una red de destino. Puede configurar los dispositivos Citrix SD-WAN para aprender rutas y anunciar rutas mediante BGP.

BGP exterior (eBGP)

Los dispositivos Citrix SD-WAN se conectan a un conmutador del lado LAN y a un enrutador del lado WAN. A medida que la tecnología SD-WAN comienza a ser más integral en las implementaciones de redes empresariales, los dispositivos SD-WAN sustituyen a los routers. SD-WAN implementa el protocolo de redirección dinámica eBGP para funcionar como un dispositivo de redirección dedicado.

El dispositivo SD-WAN establece una vecindad con routers peer que utilizan eBGP hacia el lado WAN y es capaz de aprender y anunciar rutas desde y hacia los pares. Puede seleccionar importar y exportar rutas aprendidas de eBGP en dispositivos del mismo nivel. Además, las rutas aprendidas de rutas estáticas y virtuales SD-WAN se pueden configurar para anunciar a los pares eBGP.

Para obtener más información, consulte los siguientes casos de uso:

- Sitio de SD-WAN Comunicación con un sitio que no es SD-WAN a través de eBGP
- Comunicación entre sitios SD-WAN mediante Ruta Virtual y eBGP
- Implementación de OSPF en topología de un brazo
- Implementación de OSPF de tipo 5 a tipo 1 en la red MPLS
- Implementación OSPF de dispositivos SD-WAN y no SD-WAN (terceros)
- Implementación de OSPF mediante red SD-WAN con configuración de alta disponibilidad

Longitud de ruta AS

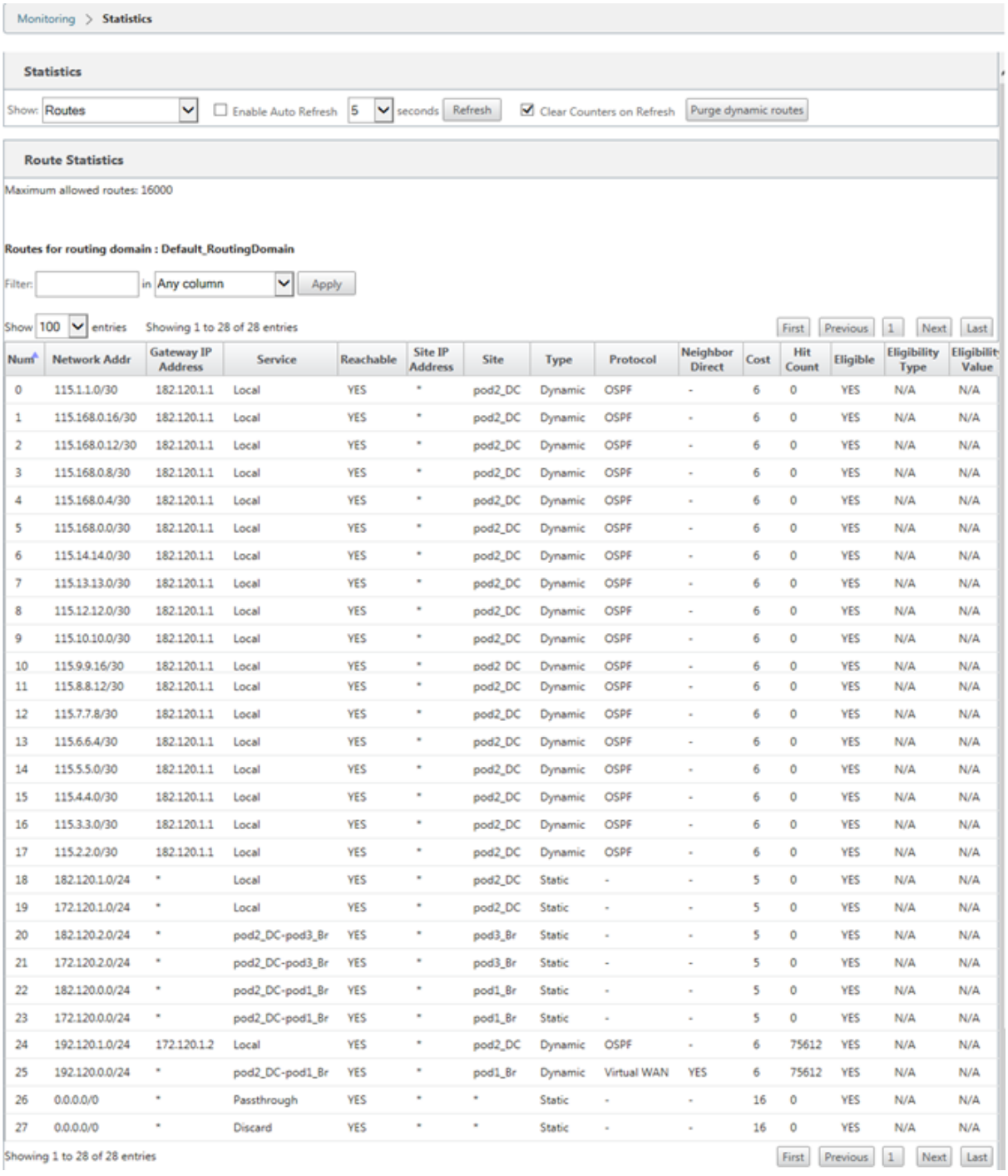
El protocolo BGP utiliza el atributo de **longitud de ruta AS** para determinar la mejor ruta. La longitud de la ruta AS indica el número de sistemas autónomos atravesados en una ruta. Citrix SD-WAN utiliza el atributo de **longitud de ruta de acceso BGP AS** para filtrar e importar rutas.

Los dispositivos que no son SD-WAN pueden optar por redirigir el tráfico a dispositivos SD-WAN de CC primarios o de CC secundarios importando rutas en función de la longitud de su ruta AS. También puede dirigir dinámicamente el tráfico desde un router a un DC secundario simplemente aumentando la longitud del trayecto AS del dispositivo de CC primario en el router, lo que lo hace inpreferible. Elimina la necesidad de cambiar el coste de la ruta y realizar una actualización de la configuración.

Supervisar estadísticas de rutas

Vaya a **Supervisar** > **Estadísticas**. Seleccione **Rutas** en el menú desplegable **Mostrar**.

Todas las funciones de las rutas aplicables se admiten en la red Citrix SD-WAN, independientemente de si una ruta es dinámica o estática.



Monitoring > Statistics

Statistics

Show: Routes | Enable Auto Refresh | 5 seconds | Refresh | Clear Counters on Refresh | Purge dynamic routes

Route Statistics

Maximum allowed routes: 16000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column | Apply

Show 100 entries Showing 1 to 28 of 28 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	115.1.1.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
1	115.168.0.16/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
2	115.168.0.12/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
3	115.168.0.8/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
4	115.168.0.4/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
5	115.168.0.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	115.14.14.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	115.13.13.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	115.12.12.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	115.10.10.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
10	115.9.9.16/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
11	115.8.8.12/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
12	115.7.7.8/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
13	115.6.6.4/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
14	115.5.5.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
15	115.4.4.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
16	115.3.3.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
17	115.2.2.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
18	182.120.1.0/24	*	Local	YES	*	pod2_DC	Static	-	-	5	0	YES	N/A	N/A
19	172.120.1.0/24	*	Local	YES	*	pod2_DC	Static	-	-	5	0	YES	N/A	N/A
20	182.120.2.0/24	*	pod2_DC-pod3_Br	YES	*	pod3_Br	Static	-	-	5	0	YES	N/A	N/A
21	172.120.2.0/24	*	pod2_DC-pod3_Br	YES	*	pod3_Br	Static	-	-	5	0	YES	N/A	N/A
22	182.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Static	-	-	5	0	YES	N/A	N/A
23	172.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Static	-	-	5	0	YES	N/A	N/A
24	192.120.1.0/24	172.120.1.2	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	75612	YES	N/A	N/A
25	192.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Dynamic	Virtual WAN	YES	6	75612	YES	N/A	N/A
26	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
27	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 28 of 28 entries First Previous 1 Next Last

OSPF

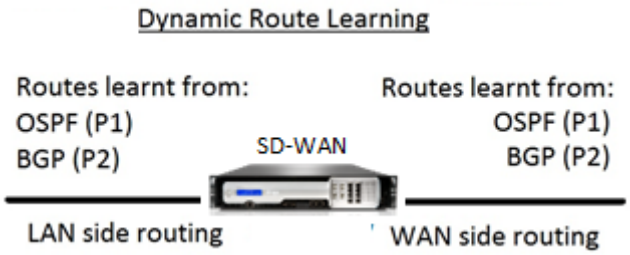
August 26, 2022

Lado LAN: Aprendizaje de rutas dinámicas

OSPF que se ejecuta en el puerto LAN del dispositivo Citrix SD-WAN implementado en modo puerta de enlace:

Los dispositivos Citrix SD-WAN realizan la detección de rutas de anuncios de redirección de capa 3 dentro de una red de cliente local (tanto en sucursales como en centros de datos) para cada uno de los protocolos de redirección deseados (OSPF y BGP). Las rutas que se aprenden se capturan y muestran dinámicamente.

Esto elimina la necesidad de que los administradores de SD-WAN definan estáticamente el entorno de red LAN para cada dispositivo que forme parte de la red SD-WAN.



Lado WAN: Uso compartido dinámico de rutas

Dispositivo Citrix SD-WAN que tiene un AREA definida como área STUB al limitar el aprendizaje de LSA externo de tipo 5 como.

Los dispositivos Citrix SD-WAN pueden anunciar las rutas dinámicas aprendidas localmente con el MCN. El MCN puede retransmitir estas rutas a otros dispositivos SD-WAN de la red. Este intercambio de información de forma dinámica permite mantener la conectividad entre los sitios de la red cambiante.

Modos de implementación OSPF

En versiones anteriores, las rutas aprendidas de instancias OSPF de SD-WAN se trataban como rutas externas solo con LSA de tipo 5. Estas rutas se anunciaron a sus routers vecinos en LSA externo tipo 5. Esto dio lugar a que las rutas SD-WAN sean rutas menos preferidas según el algoritmo de selección de rutas OSPF.

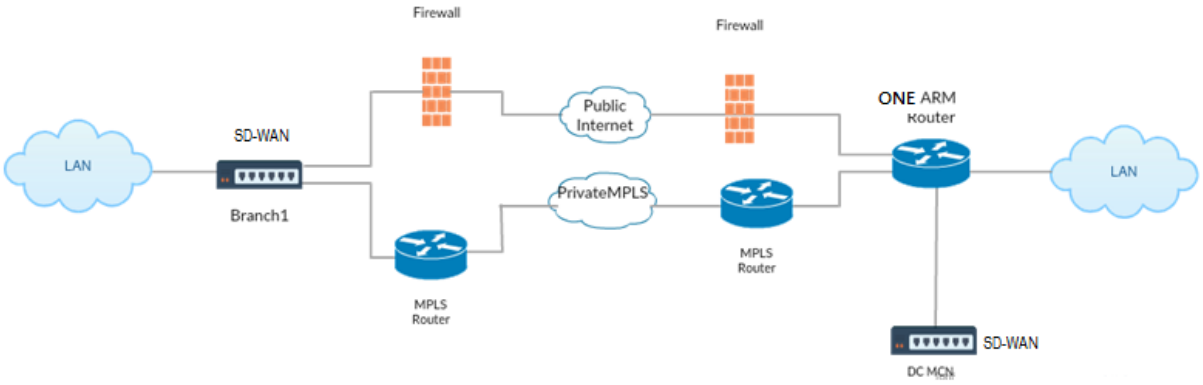
Con la última versión, SD-WAN ahora puede anunciar rutas como rutas dentro del área (LSA Tipo 1) para obtener preferencia según su coste de ruta mediante el algoritmo de selección de rutas OSPF. El coste de la ruta se puede configurar y anunciar al enrutador vecino. Esto permite implementar el dispositivo SD-WAN en el modo de un solo brazo que se describe a continuación.

Implementación de OSPF en topología de un brazo

En la configuración de un solo brazo, el router necesita una configuración complicada de PBR o WCCP en las implementaciones OSPF. Al cambiar el tipo de ruta de exportación predeterminado de Tipo 5 a Tipo 1, podemos simplificar esta implementación. Si las rutas SD-WAN se anuncian como rutas intra-area con menor coste y el dispositivo SD-WAN se activa, el enrutador vecino selecciona rutas SD-WAN y comienza automáticamente a reenviar tráfico a través de la red SD-WAN. Ya no se requiere configuración adicional de PBR o WCCP.

Requisitos previos:

- Los dispositivos SD-WAN en los sitios de DC y sucursales deben ejecutar la versión más reciente.
- La conectividad IP de extremo a extremo debe configurarse y funcionar correctamente.
- OSPF está habilitado en todos los sitios.

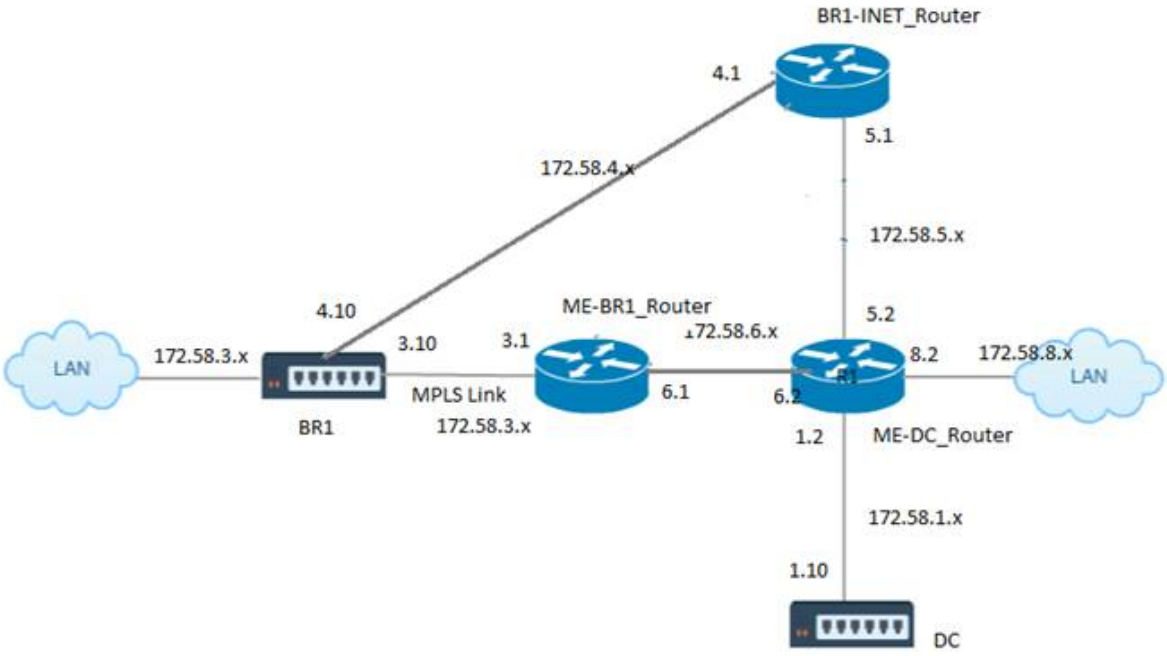


Como se muestra en la ilustración anterior, el MCN de CC se implementa en topología de un brazo. Cuando el sitio de DC está activo, el enrutador de un solo brazo reenvía todo el tráfico de la LAN local a otros sitios, como la LAN local de la sucursal cuya dirección IP de destino está dentro de la misma subred al SD-WAN primero, luego el dispositivo SD-WAN envuelve todos los paquetes y lo envía al enrutador con todos los paquetes IP de destino en la dirección IP virtual de sucursal. A continuación, el router reenvía esos paquetes a la WAN.

Cuando el sitio de DC está inactivo, el enrutador reenvía todo el tráfico de la LAN local a otros sitios (LAN local del sitio de sucursal, IP de destino está dentro de la subred) a la WAN directamente y no al dispositivo SD-WAN.

Implementación de OSPF de tipo 5 a tipo 1 en la red MPLS

Se proporciona el siguiente modo de implementación para evitar la formación de bucles en una red MPLS configurada mediante dispositivos SD-WAN. La ilustración siguiente describe la implementación de red MPLS estándar.



En la ilustración anterior:

- OSPF se configura entre *ME-BR1_router* y *ME-DC_router* en el área 0.
- OSPF se configura entre *ME-DC_router* y *DC* en el área 0.

Configuración recomendada:

- DC VW y ME-DC_router en area0
- ME-BR1_router y ME-DC_router en area0
- BR1 VW y ME-BR1_router en area0

En el ME-DC_Router:

1. Agregar ruta estática para 172.58.3.10/32 (IP virtual de BR1 para MPLS Link) a 172.58.6.1
2. Agregar ruta estática para 172.58.4.10/32 (IP virtual de BR1 para INET) a 172.58.5.1

La adición de rutas estáticas evita la formación de bucles entre el dispositivo ME-DC_Router y DC SD-WAN. Si no agrega rutas estáticas, el MCN reenvía tráfico al router ME-DC, y de vuelta desde el router al MCN y esto crea un bucle continuamente.

Las rutas estáticas que no son rutas PBR sino rutas basadas en IP del host de destino atraviesan hacia el enlace correcto que se elegirá desde el lado DC en función de la ruta elegida y de la encapsulación realizada posteriormente. Por lo tanto, con estas rutas estáticas configuradas, los paquetes encapsulados con cualquier IP virtual de destino del dispositivo BR1 SD-WAN utilizarían estos enlaces según la mejor ruta seleccionada por el DC MCN.

Agregue ACL para evitar la formación de bucles cuando se instalan las rutas IPHOST (si no hay IPs virtuales estáticas configuradas):

- Si las rutas IPHOST anunciadas por el dispositivo BR1 SD-WAN son instaladas por el router MCN *ME-DC_Router* y no se agregan como rutas estáticas como se mencionó anteriormente, existe la posibilidad de formación de bucle si la interfaz participante OSPF (172.58.6.x) entre el router ME-BR1_y el router ME-DC_Router se desactiva. Esto se debe a que con esta interfaz inactiva, las rutas IPHOST se vacían de la tabla de redirección de ME-DC_Router.
- Si esto sucede, MCN reenvía el paquete encapsulado destinado a uno de los VIP BR1 al router ME-DC y de vuelta del router al MCN y bucle continuamente.

En el router ME-BR1_Router:

Anuncie la red 172.58.3.x a ME-DC_Router con un coste mayor que el coste anunciado para la misma red por DC, si se utiliza el mismo ID de AREA entre **ME-BR1_Router <-> E-DC_router** y **ME-DC_router <-> DC (SD-WAN)**.

- Según el cálculo de la métrica de coste de OSPF 10^8/BW y el coste de los prefijos de ruta se basan en el tipo de interfaz. Los dispositivos SD-WAN anuncian la ruta virtual y las rutas estáticas específicas de la WAN virtual a los routers externos o pares con el coste predeterminado de SD-WAN de 5.
- Si el Me-BR1_router también está anunciando 172.58.3.0/24 como una ruta OSPF tipo 1 interna junto a DC (SD-WAN) que también anuncia el mismo prefijo que una ruta OSPF tipo 1 interna, entonces de acuerdo con el cálculo de costes, por defecto se configurará la ruta del ME-BR1_router, ya que el coste es menor que el de SD-WAN coste predeterminado de 5. Para evitar esto y hacer que el dispositivo SD-WAN elegido inicialmente como la ruta preferida, se debe manipular el coste de interfaz de (172.58.3.1) para que sea más alto en el router ME-BR1_para que la ruta DC SD-WAN esté configurada en la tabla de redirección del ME-DC_Router.

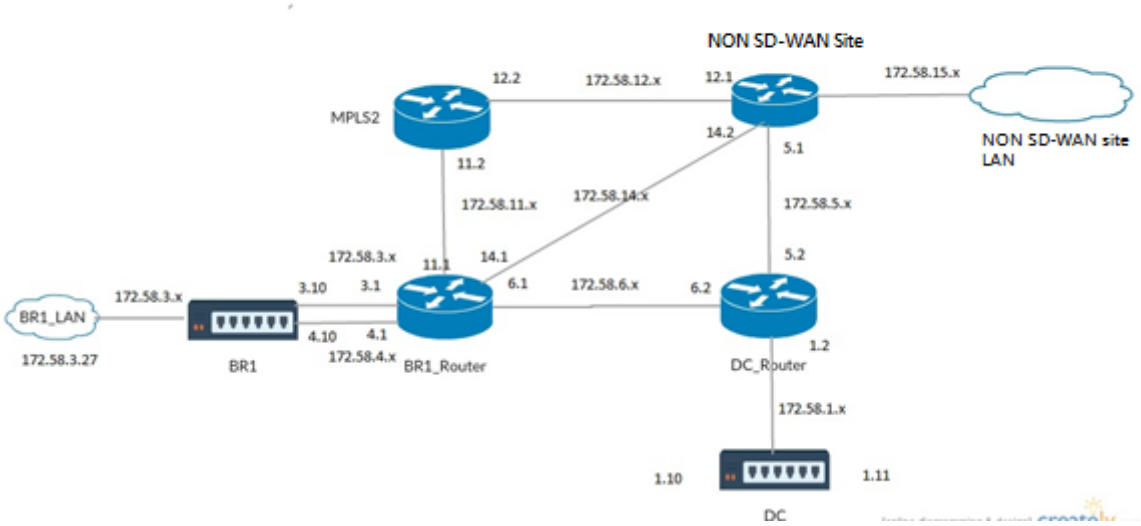
Esto también garantiza que cuando falla el dispositivo DC SD-WAN, la ruta alternativa para usar ME-BR1_Router como la siguiente Gateway preferida garantiza un flujo de tráfico ininterrumpido.

Utilice ME-DC_Router como fuente para la publicidad de la red 172.58.8.0/24 tanto para DC SD-WAN como para ME-BR1_Router:

Con esta ruta, la SD-WAN de CC puede enviar paquetes al enrutador ascendente teniendo en cuenta la subred LAN después de la descapsulación. Si el SD-WAN de CC falla, la infraestructura de redirección heredada ayudaría a ME-BR1_Router a utilizar el ME-DC_Router como el siguiente salto para llegar a la red 172.58.8.x.

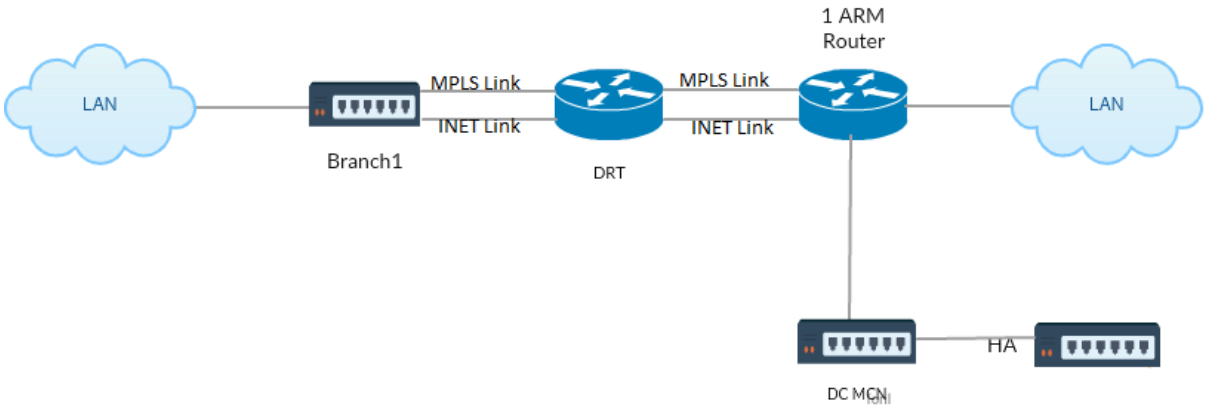
Implementación de dispositivos SD-WAN y de terceros (no SD-WAN)

Como se muestra en la siguiente ilustración, el sitio del dispositivo de terceros puede acceder a la LAN del sitio B enviando tráfico directamente al sitio B. Si no puede enviar tráfico directamente, la ruta de reserva va al Sitio A y, a continuación, utiliza la ruta virtual entre DC a los sitios de sucursal para llegar a la sucursal. Si eso falla, usa MPLS2 para llegar al sitio de Branch.



El flujo de tráfico se puede observar en la interfaz gráfica de SD-WAN en **Supervisión** > **Flujos**.

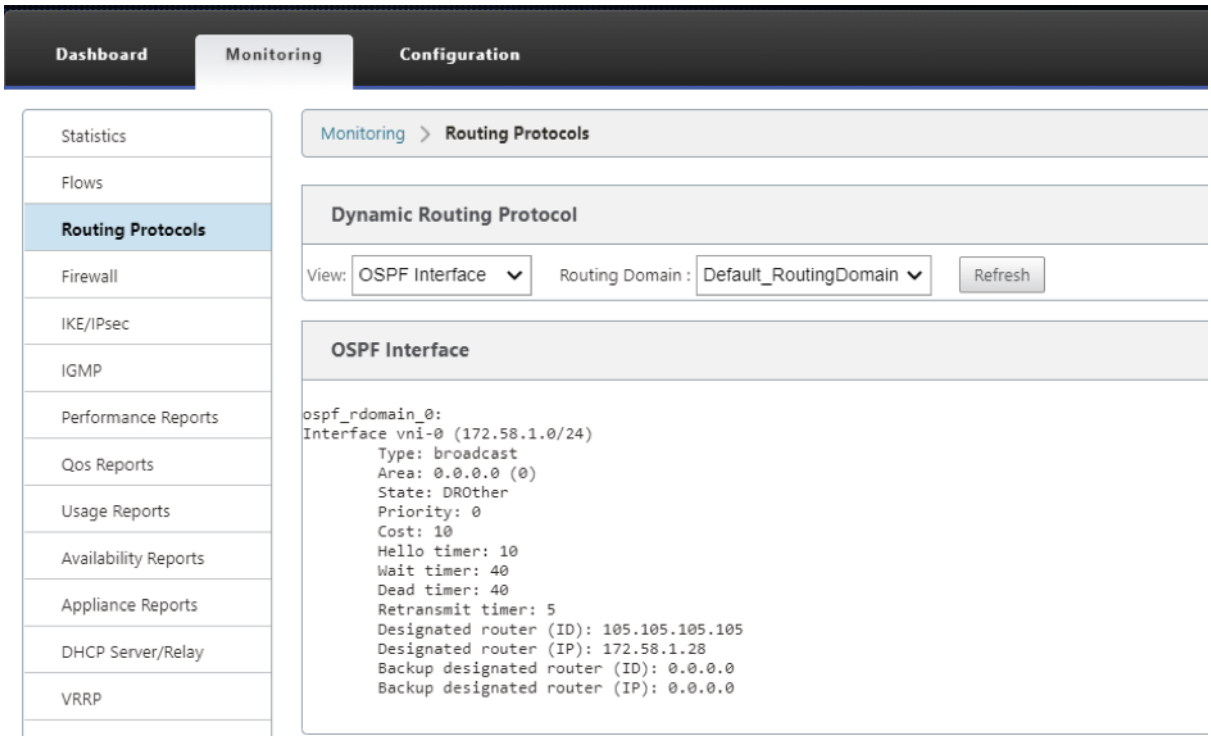
Implementación de OSPF con la red SD-WAN en la instalación de alta disponibilidad

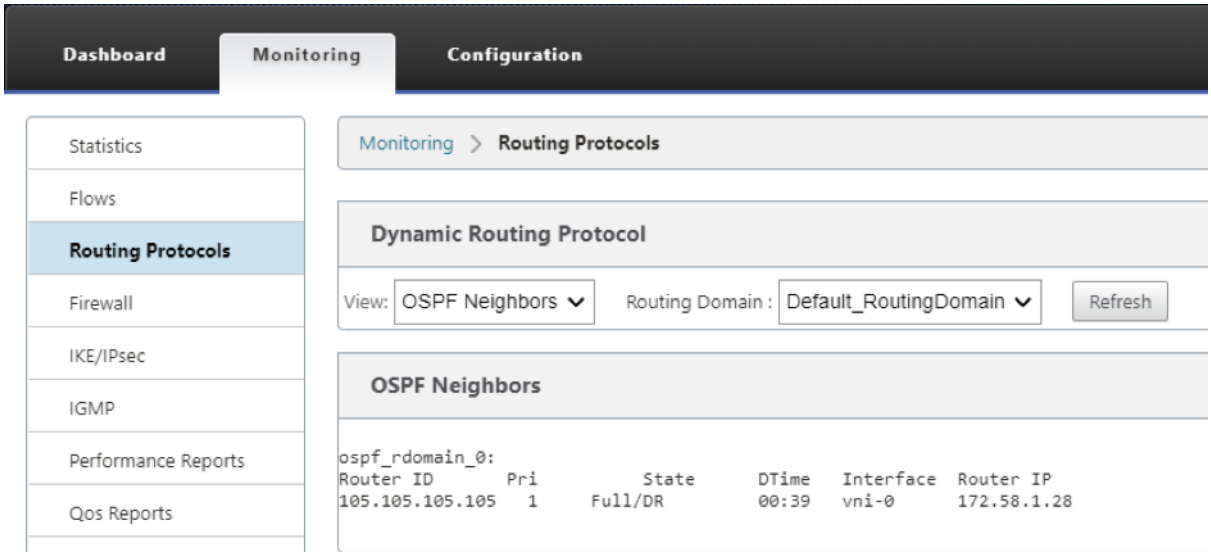


OSPF Type5 a Type1 con sitios de alta disponibilidad durante la conmutación por error al dispositivo en espera e implementado en la configuración de alta disponibilidad:

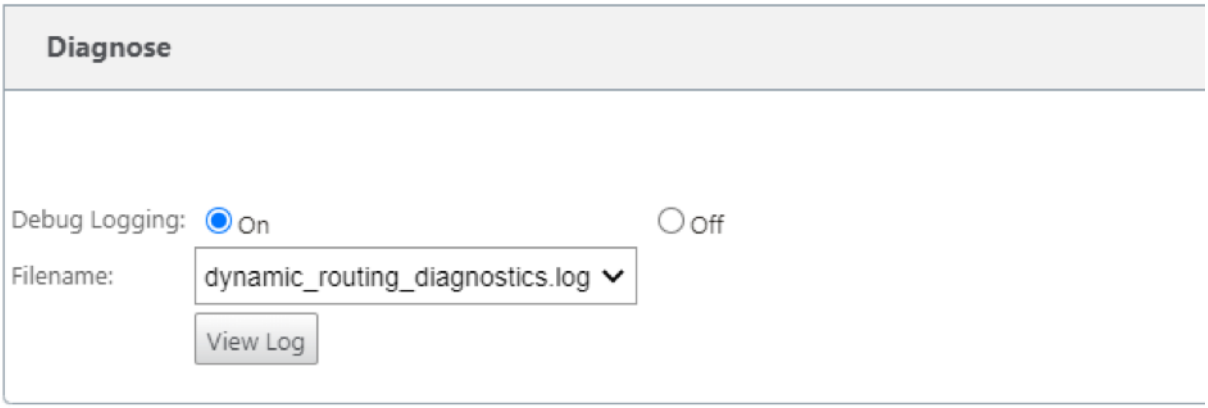
Solución de problemas

Puede ver los parámetros OSPF en **Supervisión >Protocolos de redirección**.





También puede observar los registros de redirección dinámica para ver si hay algún problema con OSPF Convergence.



BGP

August 26, 2022

La funcionalidad de redirección SD-WAN BGP le permite:

- Configure el número de sistema autónomo (AS) de un vecino u otro enrutador del mismo nivel (iBGP o eBGP).
- Cree directivas BGP para que se apliquen selectivamente a un conjunto de redes por vecino, en cualquier dirección (importación o exportación). Un dispositivo SD-WAN admite ocho directivas por sitio, con hasta ocho objetos de red (u ocho redes) asociados a una directiva.
- Para cada directiva, los usuarios pueden configurar varias cadenas de comunidad, AS-PATH-PREPEND, atributo MED. Los usuarios pueden configurar hasta 10 atributos para cada directiva.

> **Nota**
>
> Sólo se permite la preferencia local y la métrica IGP para la selección y manipulación de rutas.

Configuración de vecinos

Para configurar eBGP, se agrega una columna adicional a la sección Vecinos BGP existente para configurar el número AS vecino. Las configuraciones existentes se rellenan previamente en este campo con el número AS local cuando se importa la configuración anterior mediante el editor de configuración de SD-WAN 9.2.

La configuración del vecino también tiene una sección avanzada opcional (fila expandible) donde puede agregar directivas para cada vecino.

Configuración de vecinos avanzados

Con esta opción, puede agregar objetos de red y agregar una directiva BGP configurada para ese objeto de red. Esto es similar a crear un mapa de rutas y ACL para que coincidan con ciertas rutas y configurar los atributos BGP para ese vecino. Puede especificar la dirección para indicar si esta directiva se aplica a las rutas entrantes o salientes.

La directiva predeterminada es para <accept> todas las rutas. Las directivas de aceptación y rechazo son predeterminadas y no se pueden modificar.

Tiene la capacidad de hacer coincidir rutas en función de la dirección de red (dirección de destino), ruta de acceso AS, cadena de comunidad y asignar una directiva y seleccionar la dirección para la directiva que se va a aplicar.

1. Vaya a **Supervisión** > Protocolos de redirección**> Protocolos** de redirección**dinámico** para supervisar las directivas BGP configuradas y los vecinos para el dispositivo de sitio de CC o sucursal.

Puede habilitar el registro de depuración y ver los archivos de registro para la redirección en la página **Supervisar** > **Protocolo de redirección**. Los registros del demonio de redirección se dividen en archivos de registro independientes. La información de redirección estándar se almacena en *dynamic_routing.log*, mientras que los problemas de redirección dinámico se capturan en *dynamic_routing_diagnostics.log*, que se pueden ver desde la supervisión de los protocolos de redirección.

Reconfiguración suave de BGP

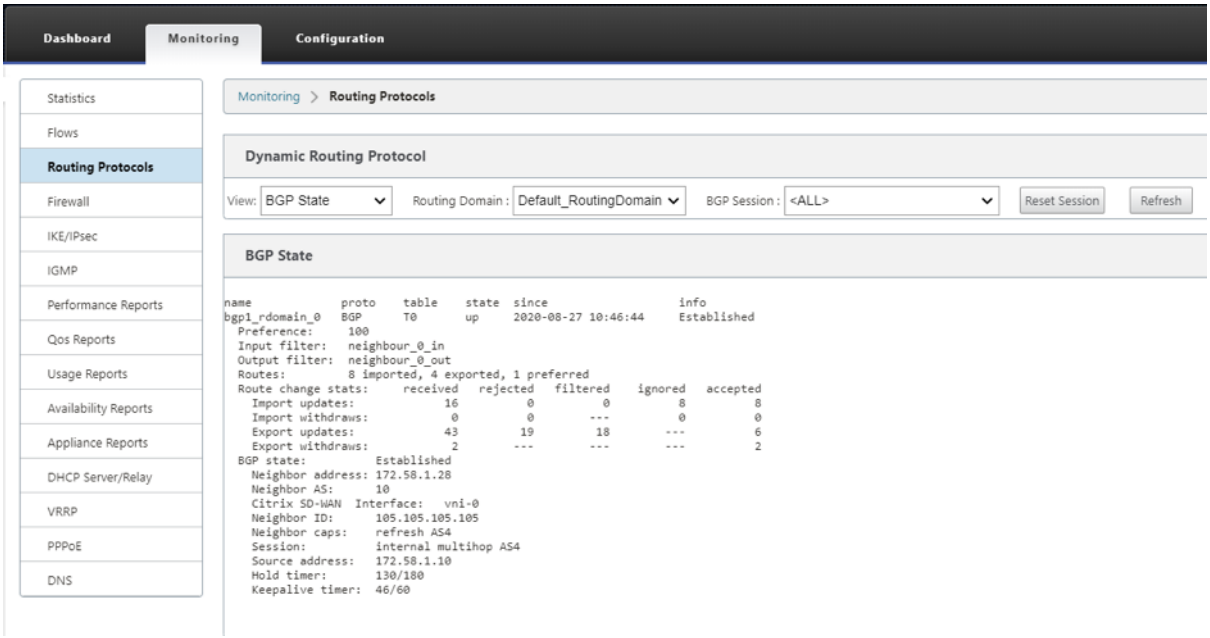
Las directivas de redirección para el par BGP incluyen configuraciones como el mapa de rutas, la lista de distribución, la lista de prefijos y la lista de filtros que pueden afectar a las actualizaciones de la tabla de redirección entrante o saliente. Cuando se produce un cambio en la directiva de redirección, se debe borrar o restablecer la sesión BGP para que la nueva directiva surta efecto.

Al borrar una sesión BGP mediante un restablecimiento completo, se invalida la caché y se produce un impacto negativo en el funcionamiento de las redes, ya que la información de la caché deja de estar disponible.

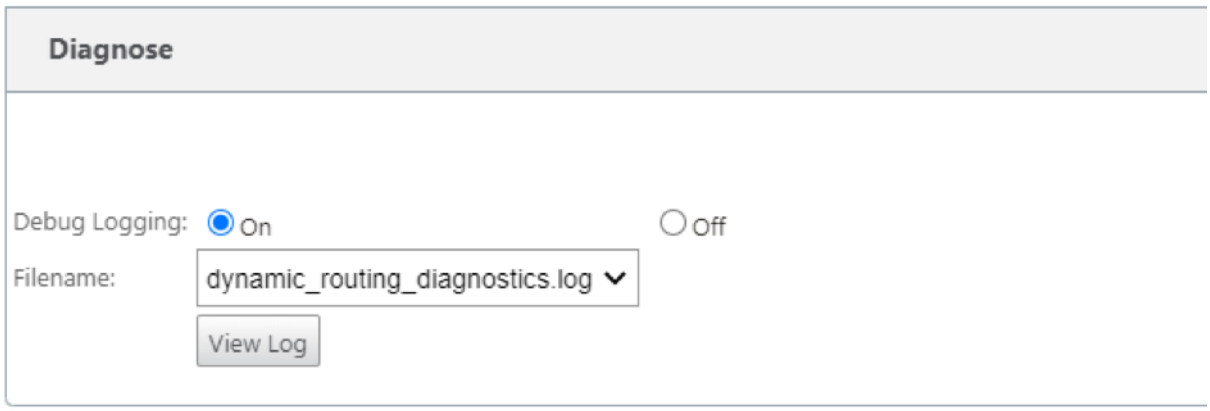
La función BGP Soft Reset Enhancement proporciona compatibilidad automática para el restablecimiento dinámico de las actualizaciones entrantes de la tabla de redirección BGP que no dependen de la información de actualización de la tabla de redirección almacenada.

Solución de problemas

Para ver los parámetros BGP, vaya a **Supervisión > Protocolos de redirección** > seleccione **Estado BGP** en el campo **Ver**.



Puede observar los registros de redirección de Dynamic para ver si hay algún problema con BGP Convergence.



iBGP

August 26, 2022

Dispositivo Citrix SD-WAN con iBGP en el lado LAN y eBGP en el lado WAN:

Los dispositivos Citrix SD-WAN anuncian todas las rutas eBGP aprendidas en el dominio IGP con NEXT HOP SELF cuando se implementan con iBGP en el lado LAN y eBGP en el lado WAN.

Varios enrutadores LAN iBGP en una topología de red lineal con interconexión directa y malla con Citrix SD-WAN.

Limitaciones:

- Los atributos AS-path prepend, Med y Community no son compatibles.
- No se admite el filtrado de rutas entre OSPF y BGP durante la redistribución. O bien todas (o) ninguna de las rutas aprendidas de OSPF se anuncian a los pares de BGP y viceversa.
- No se admite la agregación de rutas.
- Solo se puede configurar un máximo de 16 pares BGP (incluidos iBGP y eBGP).

eBGP

August 26, 2022

El sitio SD-WAN se comunica con un sitio que no es SD-WAN a través de eBGP

Cuando un sitio sin dispositivo SD-WAN se comunica con otro sitio con un dispositivo SD-WAN (sitio A) a través de una única ruta WAN (solo Internet está disponible) y si el sitio con dispositivo SD-WAN (sitio A) pierde conectividad a Internet, el sitio sin SD-WAN puede comunicarse con el sitio A a través de otra SD-WAN sitio del dispositivo (sitio-B). El sitio B canaliza el tráfico del sitio sin el dispositivo SD-WAN al sitio A.

Comunicación entre sitios SD-WAN mediante Virtual Path y eBGP:

Proporciona aprendizaje de rutas de calco subyacente para comunicarse con subredes locales de sitios remotos cuando la ruta virtual está inactiva entre dos sitios mientras el dispositivo WAN virtual todavía está activo y en ejecución.

Ruta de aplicaciones

August 26, 2022

En una red empresarial típica, las sucursales acceden a las aplicaciones del centro de datos local, el centro de datos en la nube o las aplicaciones SaaS. La función de redirección de aplicaciones le permite dirigir las aplicaciones a través de su red de manera fácil y rentable. Por ejemplo, cuando un usuario de la sucursal intenta acceder a una aplicación SaaS, el tráfico se puede redirigir de manera

que las sucursales puedan acceder directamente a las aplicaciones SaaS en Internet, sin tener que pasar primero por el centro de datos.

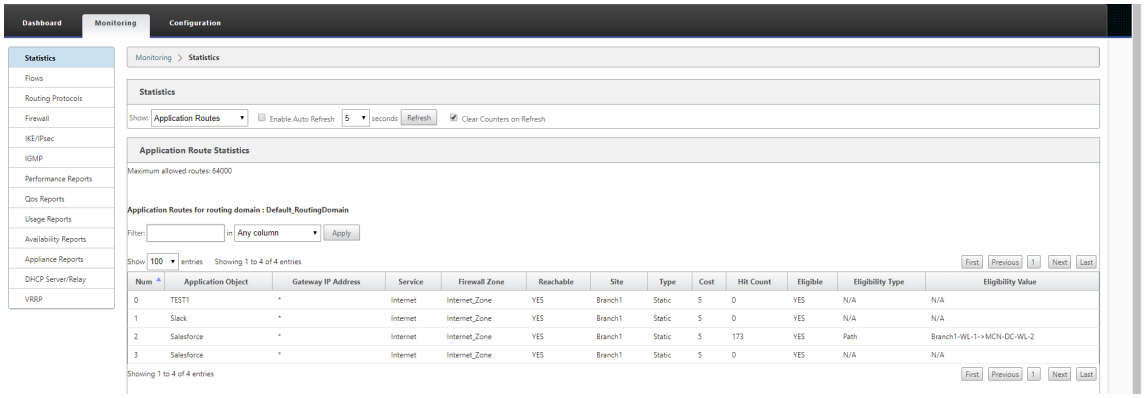
Citrix SD-WAN permite definir las rutas de aplicación para los siguientes servicios:

- **Ruta virtual**: Este servicio administra el tráfico a través de las rutas virtuales. Una ruta virtual es un vínculo lógico entre dos enlaces WAN. Comprende una colección de rutas WAN combinadas para proporcionar una comunicación de alto nivel de servicio entre dos nodos SD-WAN. El dispositivo SD-WAN mide la red por trayecto y se adapta a la demanda cambiante de las aplicaciones y a las condiciones de la WAN. Una ruta virtual puede ser estática (siempre existe) o dinámica (existe cuando el tráfico entre dos dispositivos SD-WAN alcanza un umbral configurado).
- **Internet:** Este servicio administra el tráfico entre un sitio de Enterprise y los sitios de la Internet pública. El tráfico de Internet no está encapsulado. Cuando se produce una congestión, la SD-WAN administra activamente el ancho de banda limitando la velocidad del tráfico de Internet en relación con la ruta virtual y el tráfico de la intranet.
- **Intranet**: Este servicio administra el tráfico de la intranet empresarial que no se ha definido para la transmisión a través de una ruta virtual. El tráfico de intranet no está encapsulado. La SD-WAN administra el ancho de banda limitando la velocidad de este tráfico en relación con otros tipos de servicio durante épocas de congestión. En determinadas condiciones, y si la opción de reserva de intranet está configurada en la ruta virtual, el tráfico que normalmente se desplaza a través de la ruta virtual se puede tratar como tráfico de intranet.
- **Local**: Este servicio administra el tráfico local del sitio que no coincide con ningún otro servicio. SD-WAN ignora el tráfico originado y destinado a una ruta local.
- **Túnel GRE**: Este servicio administra el tráfico IP destinado a un túnel GRE y coincide con el túnel LAN GRE configurado en el sitio. La función Túnel GRE le permite configurar dispositivos SD-WAN para terminar los túneles GRE en la LAN. Para una ruta con el tipo de servicio Túnel GRE, la puerta de enlace debe residir en una de las subredes de túnel del túnel GRE local.
- **Túnel IPsec LAN**: Este servicio administra el tráfico IP destinado a un túnel IPsec LAN y coincide con el túnel IPsec LAN configurado en el sitio. La función Túnel IPsec de LAN le permite configurar dispositivos SD-WAN para terminar túneles IPsec en el lado LAN o WAN.

Para llevar a cabo la dirección de servicio para las aplicaciones, es importante identificar una aplicación en el primer paquete. Inicialmente, los paquetes fluyen a través de la ruta IP una vez que se haya clasificado el tráfico y se haya conocido la aplicación, se utiliza la ruta de aplicación correspondiente. La primera clasificación de paquetes se logra aprendiendo las subredes IP y los puertos asociados con objetos de aplicación. Estos se obtienen mediante los resultados de clasificación histórica del clasificador DPI y los tipos de coincidencia de puertos IP configurados por el usuario.

Para ver datos estadísticos de las rutas de la aplicación:

1. En la GUI de SD-WAN, vaya a **Supervisión** > **Estadísticas**.
2. En la lista implementable **Mostrar**, seleccione **Rutas de aplicación**.



Puede ver las siguientes estadísticas:

- **Objeto Application**: nombre del objeto de aplicación.
- **Dirección IP de puerta de enlace**: La dirección IP de la puerta de enlace utilizada por los objetos de aplicación con el tipo de servicio Túnel GRE.
- **Servicio**: tipo de servicio asignado al objeto de aplicación.
- **Zona de firewall**: La zona de firewall en la que se encuentra esta ruta.
- **Alcazable**: El estado de la ruta de la solicitud.
- **Sitio**: Nombre del sitio.
- **Tipo**: indica si la ruta es estática o dinámica.
- **Coste**: La prioridad de la ruta.
- Número de**visitas**: número de veces que se utiliza la ruta de la aplicación para dirigir el tráfico.
- **Apto**: Es la ruta de la aplicación apta para enviar el tráfico.
- **Tipo de elegibilidad**: el tipo de condición de elegibilidad de ruta que se aplica a esta ruta. El tipo de elegibilidad puede ser Ruta, Puerta de enlace o Túnel.
- Valor de**elegibilidad: valor**especificado para la condición de elegibilidad de ruta.

> **Nota**
>
> En la versión actual, las aplicaciones que pertenecen a la familia de aplicaciones, el tipo de coincidencia definido en el objeto de aplicación, no se pueden dirigir.

Solución de problemas

Después de crear la ruta de la aplicación, puede confirmar que la aplicación se redirige correctamente al servicio deseado mediante la sección **Supervisión**.

Para ver si la aplicación se redirige correctamente al servicio previsto, vaya a las siguientes páginas:

- **Supervisión > Estadísticas > Rutas de aplicación**

- **Supervisión > Flujos**
- **Supervisión > Firewall**

Si hay algún comportamiento de redirección inesperado, recopile el paquete de diagnóstico STS mientras se observa el problema y compártelo con el equipo de soporte técnico de Citrix.

El paquete STS se puede crear y descargar mediante **Configuración > Mantenimiento del sistema > Diagnóstico > Información de diagnóstico**.

Filtrado de rutas

August 26, 2022

Para redes con Route Learning habilitado, Citrix SD-WAN proporciona más control sobre qué rutas SD-WAN se anuncian a los vecinos de redirección y qué rutas se reciben de los vecinos de redirección, en lugar de anunciar y aceptar todas o ninguna ruta.

- Los filtros de exportación se utilizan para incluir o excluir rutas para anuncios mediante protocolos OSPF y BGP basados en coincidencias específicas criterios. Las reglas de filtro de exportación son las reglas que se deben cumplir al anunciar rutas SD-WAN a través de protocolos de redirección dinámica. Todas las rutas se anuncian a los pares de forma predeterminada.
- Los filtros de importación se utilizan para aceptar o no las rutas que se reciben mediante vecinos OSPF y BGP basados en criterios de coincidencia específicos. Las reglas de filtro de importación son las reglas que se deben cumplir antes de importar rutas dinámicas en la base de datos de rutas SD-WAN. Por defecto, no se importan rutas.

El filtrado de rutas se implementa en rutas LAN y rutas de ruta virtual en una red SD-WAN (centro de datos/sucursal) y se anuncia a una red que no es SD-WAN mediante el uso de BGP y OSPF.

Puede configurar hasta 512 filtros de exportación y 512 filtros de importación. Este es el límite general, no por límite de dominio de redirección.

Resumen de rutas

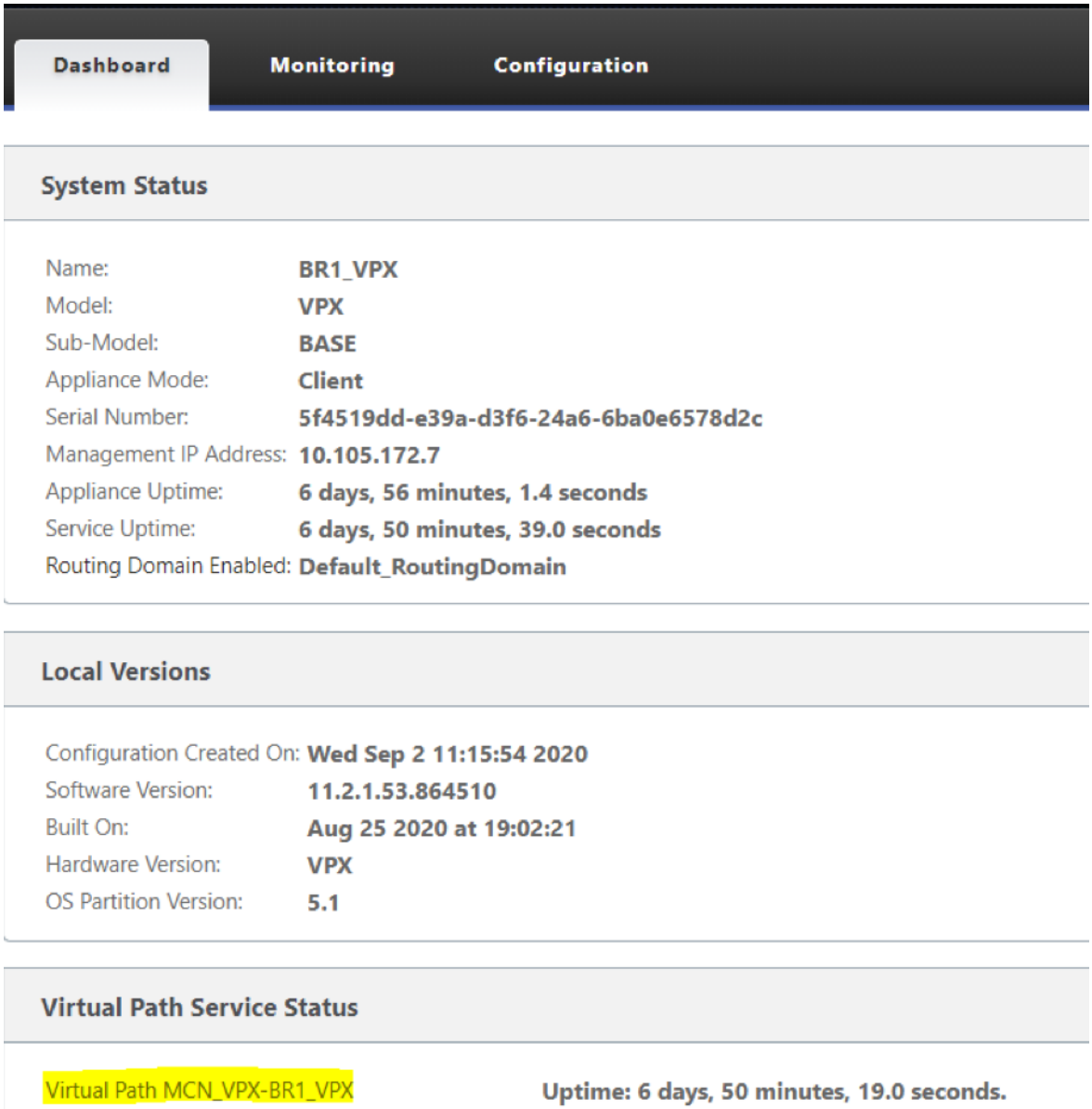
August 26, 2022

Con el aumento en el tamaño de las redes empresariales, los enrutadores necesitan mantener la gran cantidad de rutas en su tabla de redirección. Los routers requieren mayores recursos de CPU, memoria y ancho de banda para buscar las grandes tablas de redirección y mantener rutas individuales.

Puede configurar una ruta de resumen con los tipos de servicio Local y Descartar. Esta ruta de resumen se anuncia en los dispositivos de siguiente salto.

Solución de problemas

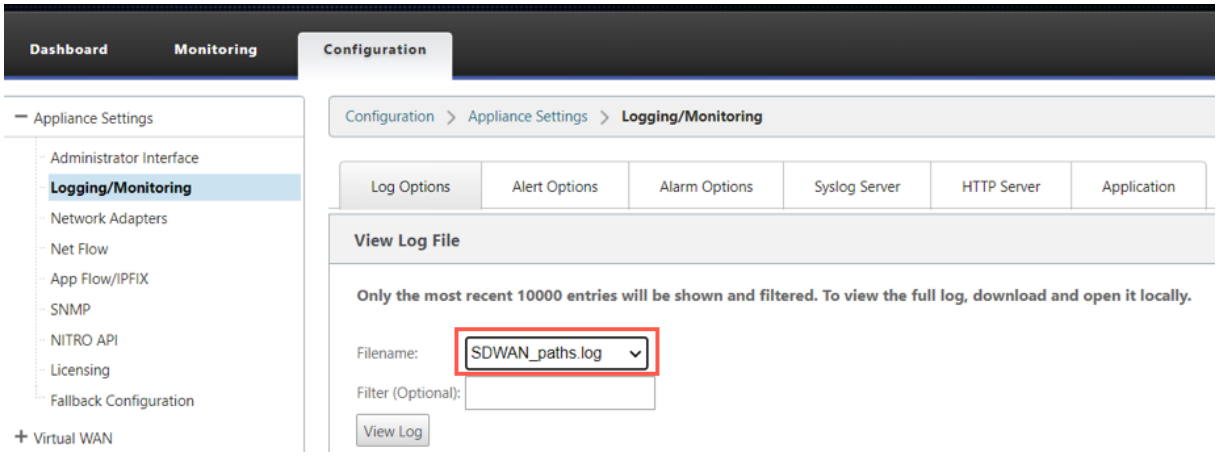
Las rutas resumidas configuradas en el MCN se envían a la sucursal a través de la ruta virtual. En caso de que no vea los detalles de la ruta virtual en la tabla de ruta de la rama, compruebe el panel de control de sucursal. El panel muestra el estado de la ruta virtual entre el MCN y la sucursal.



Si la ruta virtual está inactiva, compruebe el motivo en **Configuración > Registrar/Supervisión**.

Seleccione uno de los siguientes archivos de la lista desplegable **Nombre** de archivo para verificar:

- SDWAN_paths.log
- SDWAN_common.log



Preferencia de protocolo

August 26, 2022

La preferencia de protocolo es una función específica de Citrix SD-WAN, similar a la distancia administrativa del enrutador. El protocolo con el orden de preferencia más alto es el más preferido. La ruta que utiliza el protocolo con el valor de preferencia de protocolo más alto. La información de prioridad de protocolo es local en el dispositivo Citrix SD-WAN y no se anuncia en los elementos de red del mismo nivel.

Redirección de multidifusión

August 26, 2022

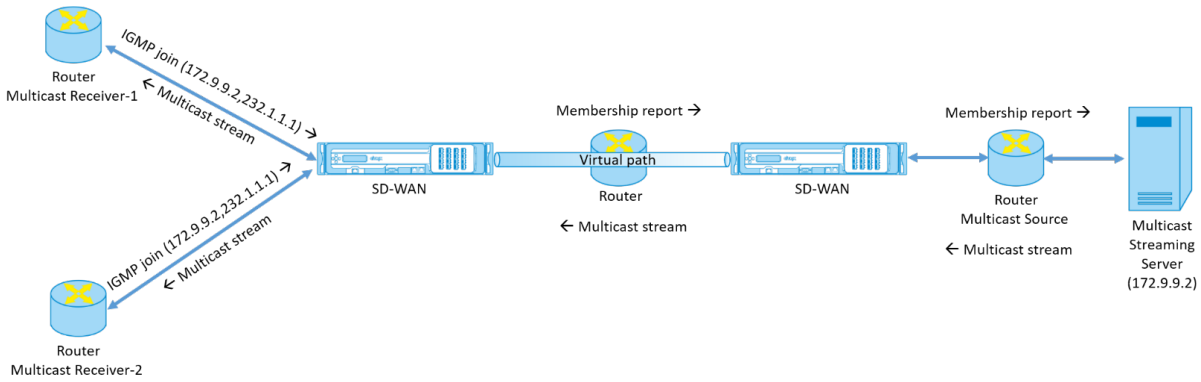
La redirección de multidifusión permite una distribución eficiente del tráfico de uno a varios. Una fuente de multidifusión envía tráfico de multidifusión en una sola secuencia a un grupo de multidifusión. El grupo de multidifusión contiene receptores como hosts y enrutadores adyacentes que utilizan el protocolo IGMP para la comunicación de multidifusión. Voz sobre IP, Vídeo a demanda, Televisión por IP y Videoconferencias son algunas de las tecnologías comunes que utilizan redirección de multidifusión. Cuando habilita la redirección de multidifusión en el dispositivo Citrix SD-WAN, el dispositivo actúa como enrutador de multidifusión.

Multidifusión específica de origen

Los protocolos de multidifusión normalmente permiten a los receptores de multidifusión recibir tráfico de multidifusión desde cualquier origen. Con la multidifusión específica de origen (SSM), puede especificar el origen desde el que los receptores reciben el tráfico de multidifusión. Garantiza que los receptores no sean oyentes abiertos a todas las fuentes que envían transmisiones de multidifusión, sino que escuchen a una fuente de multidifusión particular. SSM reduce el coste de los recursos utilizados para consumir tráfico de todas las fuentes posibles y también proporciona una capa de seguridad al garantizar que los receptores reciban tráfico de un remitente conocido.

La siguiente topología muestra dos receptores de multidifusión en un sitio de sucursal y un servidor de multidifusión (172.9.9.2) en el centro de datos. El servidor de multidifusión transmite tráfico a través de un grupo determinado (232.1.1.1), los receptores se unen al grupo. Cualquier tráfico transmitido en el grupo de multidifusión se retransmite a todos los receptores que se unieron al grupo.

> **Nota**
>
> Para que SSM funcione, la IP del grupo de multidifusión debe estar dentro del rango 2320.0.0/8.



1. Los receptores de multidifusión envían una solicitud de unión IGMP IP que indica que los receptores quieren unirse al grupo de multidifusión y quieren recibir la secuencia de multidifusión desde el origen. La combinación IGMP incluye 2 atributos el origen y el grupo de multidifusión (S, G). IGMP Versión 3 se utiliza para SSM en el origen de multidifusión y el receptor para retransmitir algunas direcciones de origen específicas INCLUDE. SSM permite a los receptores recibir explícitamente secuencias de servidores Multicast específicos, cuya dirección de origen es proporcionada explícitamente por los receptores como parte de la solicitud JOIN. En este ejemplo, se activa una solicitud de combinación IGMP v3 con una lista de origen de inclusión explícita, que contiene el origen 172.9.9.2, para que sea la dirección que envía la secuencia de multidifusión sobre el grupo 232.1.1.1.
2. Citrix SD-WAN en la sucursal escucha todas las solicitudes IGMP de estos receptores y lo convierte en un informe de pertenencia y lo envía a través de la ruta virtual al dispositivo SD-WAN del centro de datos.

3. El dispositivo Citrix SD-WAN del centro de datos recibe el informe de pertenencia a través de la ruta virtual y lo reenvía al origen de multidifusión, estableciendo un canal de control.
4. El origen de multidifusión transmite la secuencia de multidifusión a través de la ruta de acceso virtual a los receptores de multidifusión.

El tráfico del canal de control y el flujo de multidifusión fluyen a través de la ruta virtual establecida entre la rama y el centro de datos. La ruta de superposición Citrix SD-WAN asegura y aísla el tráfico de multidifusión de la degradación de WAN o de los apagones de enlaces.

Configurar multidifusión

Para configurar la multidifusión, realice lo siguiente en el dispositivo SD-WAN tanto en el origen como en el destino.

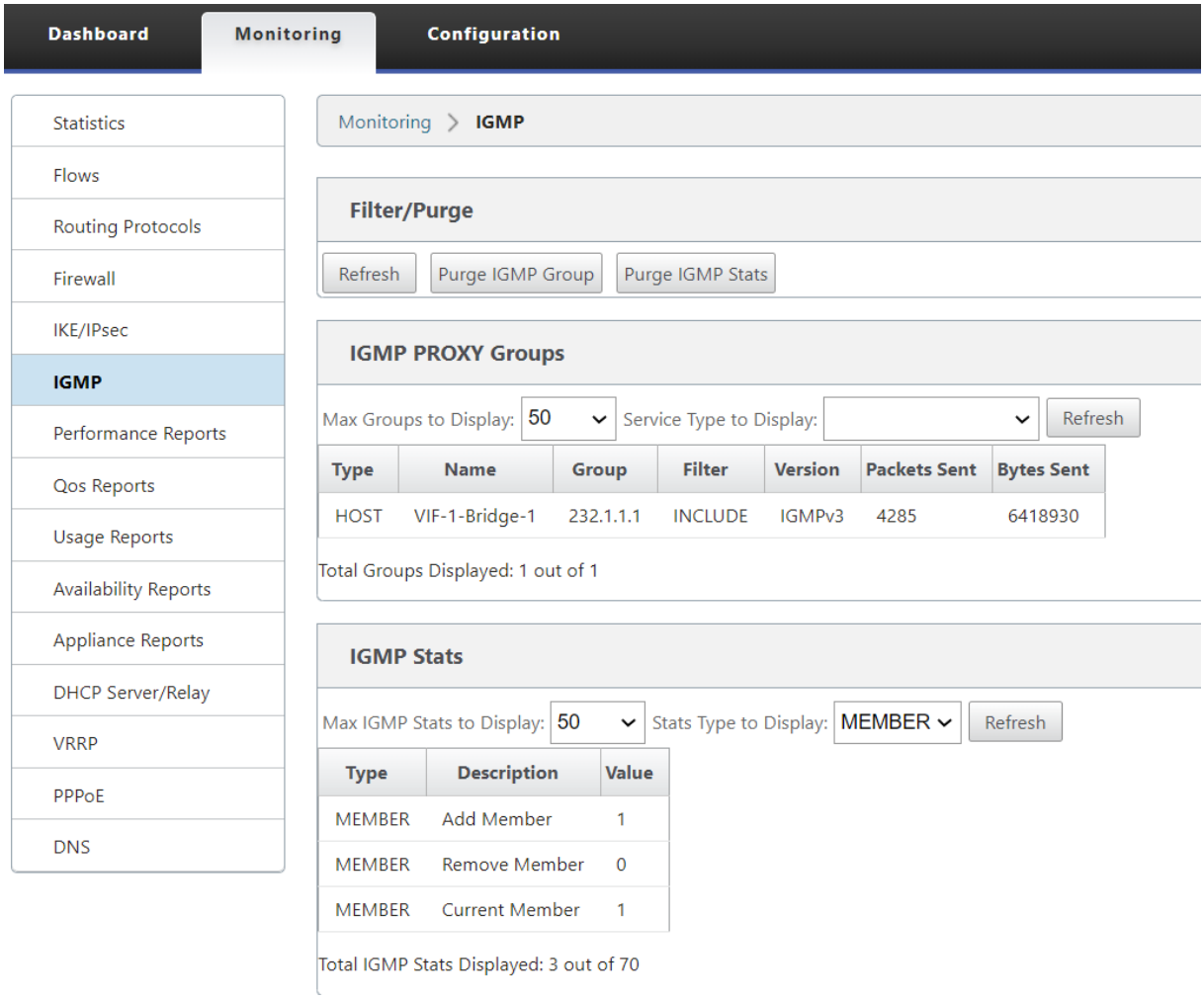
1. Crear un grupo de multidifusión: Proporcione un nombre y una dirección IP para el grupo de multidifusión. La IP del grupo de multidifusión debe estar dentro del rango 2320.0.0/8 para la multidifusión específica de origen.
2. Habilitar proxy IGMP: Puede configurar el dispositivo Citrix SD-WAN como proxy IGMP para llevar la información del canal de control IGMP para la redirección de multidifusión. IGMP V3 es necesario para la multidifusión de origen único.
3. Definir los servicios ascendentes y descendentes: Una interfaz ascendente permite al PROXY IGMP conectarse al dispositivo SD-WAN más cerca de la fuente de multidifusión real que transmite el tráfico. Una interfaz descendente permite que el proxy IGMP se conecte a los hosts que están más lejos de la fuente de multidifusión real que transmite el tráfico.
   Los servicios ascendentes y descendentes son diferentes para el dispositivo en el origen y el dispositivo en el destino.

Supervisión

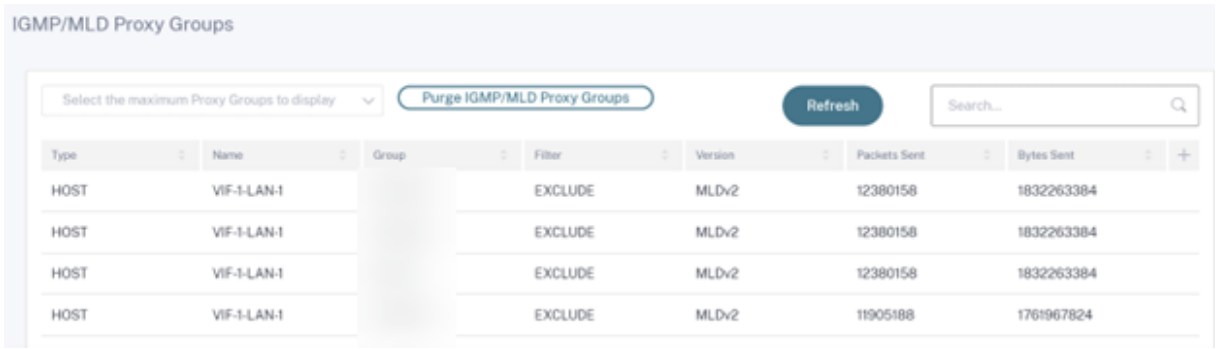
Estadísticas IGMP

Cuando los receptores de multidifusión inician una solicitud de grupo de unión, puede ver los detalles del receptor en **Supervisión** > **IGMP** en el dispositivo. Puede ver esta información en los dispositivos tanto en el origen como en el destino.

La siguiente imagen muestra una unión MLD iniciada y el tipo de mensaje RECV se utiliza para recibir direcciones de grupos de multidifusión. También puede ver las estadísticas de mensajes IGMP/MLD a continuación.



La siguiente imagen muestra información sobre los grupos proxy IGMP/MLD. También puede ver las estadísticas del grupo proxy IGMP/MLD y la versión utilizada.



Configurar el coste de ruta de ruta virtual

August 26, 2022

Citrix SD-WAN admite las siguientes mejoras de redirección relacionadas con la administración del centro de datos.

Por ejemplo, considere la red SD-WAN con dos centros de datos: uno en Norteamérica y otro en Europa. Quiere que todos los sitios de Norteamérica enruten el tráfico a través del centro de datos de Norteamérica y que todos los sitios de Europa utilicen el centro de datos de Europa. Anteriormente, en SD-WAN 9.3 y versiones anteriores, esta funcionalidad de administración del centro de datos no era compatible. Esto se implementa con la introducción del coste de ruta virtual.

- Coste de ruta de ruta virtual: puede configurar el coste de ruta de acceso virtual para rutas virtuales individuales que se agregan al coste de ruta cuando se aprende una ruta desde un sitio remoto.

Esta función invalida o elimina el coste de reenvío de WAN a WAN.

- Coste de ruta OSPF: Ahora puede importar coste de ruta OSPF (métrica tipo 1) activando **Copiar coste de ruta OSPF** en los filtros de importación. El coste de ruta OSPF se considera en la selección de ruta en lugar del coste SD-WAN. Se admite un coste de hasta 65534 en lugar de 15, pero es aconsejable acomodar un coste de ruta de ruta virtual apropiado que se agrega si la ruta se aprende desde un sitio remoto.
- Coste BGP - VP para MED: Ahora puede copiar el coste de ruta virtual para rutas SD-WAN en valores MED de BGP al exportar (redistribuir) rutas SD-WAN a pares BGP. Esto se puede establecer para vecinos individuales creando una directiva BGP y aplicándola en la dirección "OUT"para cada vecino.
- Cualquier sitio puede tener varias rutas virtuales a otros sitios. A veces, si hay una sucursal a la que hay conectividad con los servicios a través de más rutas virtuales, puede haber dos rutas virtuales desde el sitio de sucursal. Una ruta virtual a través de DC1 y la otra a través de DC2. DC1 puede ser un MCN y DC2 puede ser un Geo-MCN, y se puede configurar como otro sitio con Ruta virtual estática.
- Agregue un coste predeterminado para cada vicepresidente como 1. El coste de ruta de ruta virtual ayuda a asociar un coste a cada ruta virtual de un sitio. Esto ayuda a manipular los intercambios/actualizaciones de rutas a través de una ruta virtual específica en lugar del coste predeterminado del sitio. Con esto, podemos manipular qué centro de datos preferimos para enviar el tráfico.
- Permitir que el coste se configure dentro de un pequeño rango de valores (por ejemplo, 1-10) para cada vicepresidente.

- El coste de ruta virtual se debe agregar a cualquier ruta compartida con sitios vecinos para indicar preferencias de redirección, incluidas las rutas aprendidas a través de redirección dinámica.
- Ninguna ruta virtual estática debe tener un coste menor que una ruta virtual dinámica.

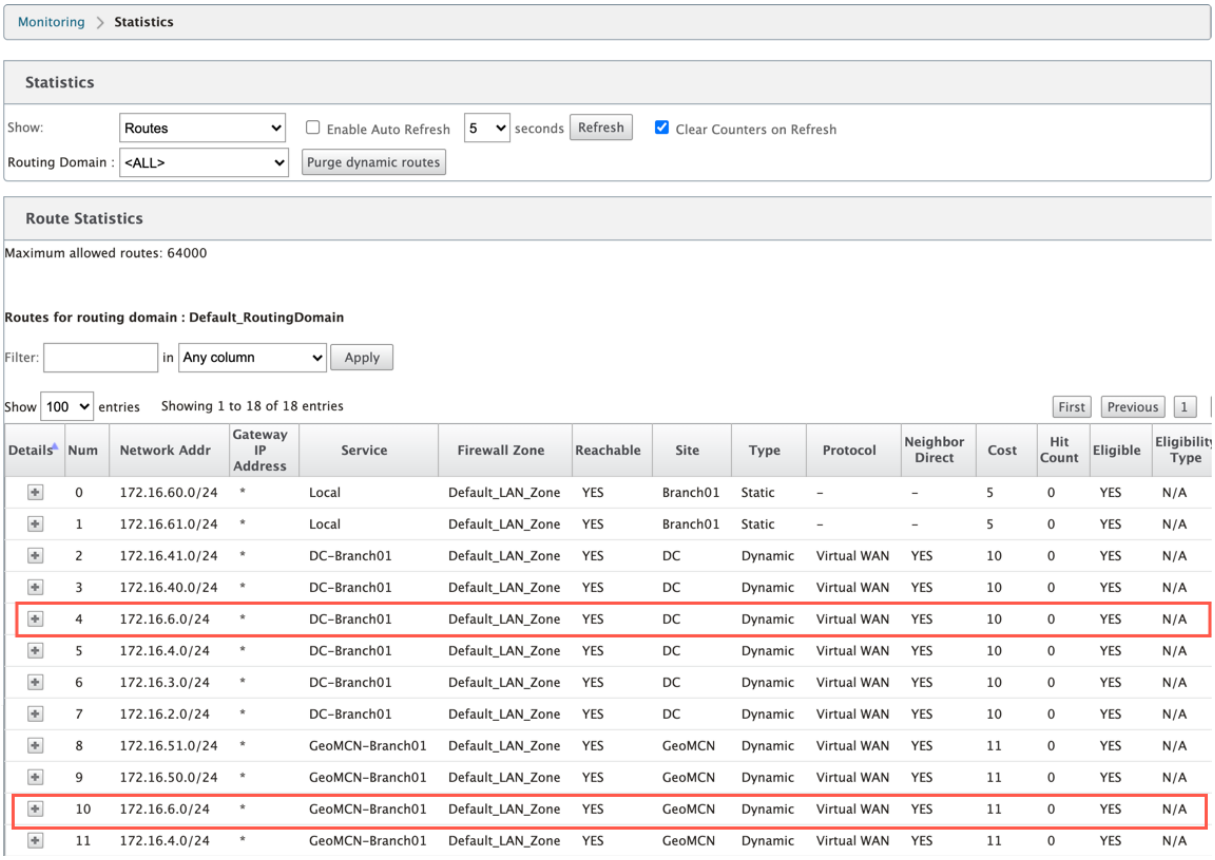
> **Nota**
>
> El coste de redirección de VP desactiva el coste de reenvío de WAN a WAN que existía en las versiones de lanzamiento anteriores a la versión 10.0. Las decisiones de redirección basadas en los costes de reenvío de WAN a WAN deben ser influenciadas nuevamente mediante el uso del coste de ruta VP, ya que el coste de reenvío WAN a WAN no tiene importancia al migrar a la versión 10.0.

Supervisión y solución de problemas

La tabla de redirección muestra cómo se instalan las mismas subredes anunciadas por dos sitios conectados a un sitio de sucursal sobre la ruta de acceso virtual con prioridad de coste con la adición de coste de ruta de acceso virtual.

Para comprobar el coste de la ruta y las rutas que se utilizan en la tabla de redirección, vaya a **Supervisión > Estadísticas** en el campo **Mostrar**, seleccione **Rutas**. Los costes de ruta y los recuentos de aciertos se pueden verificar en la misma página.

La siguiente ilustración muestra la tabla de rutas con dos costes diferentes para la misma ruta, que es 172.16.6.0/24 con el coste 10 y 11 para los servicios **DC-Branch01** y **GEOMCN-Branch01** respectivamente.



Configurar el protocolo de redundancia de enrutador virtual

August 26, 2022

Virtual Router Redundancy Protocol (VRRP) es un protocolo ampliamente utilizado que proporciona redundancia de dispositivo para eliminar el punto único de falla inherente al entorno enrutado por defecto estático. VRRP permite configurar dos o más routers para formar un grupo. Este grupo aparece como una única Gateway predeterminada con una dirección IP virtual y una dirección MAC virtual.

Un router de respaldo asume el control automáticamente si falla el router principal/maestro. En una configuración de VRRP, el router maestro envía un paquete VRRP conocido como anuncio a los routers de respaldo. Si el router maestro deja de enviar el anuncio, el router de respaldo establece el temporizador de intervalos. Si no se recibe ningún anuncio durante este período de retención, el router de respaldo inicia la rutina de conmutación por error.

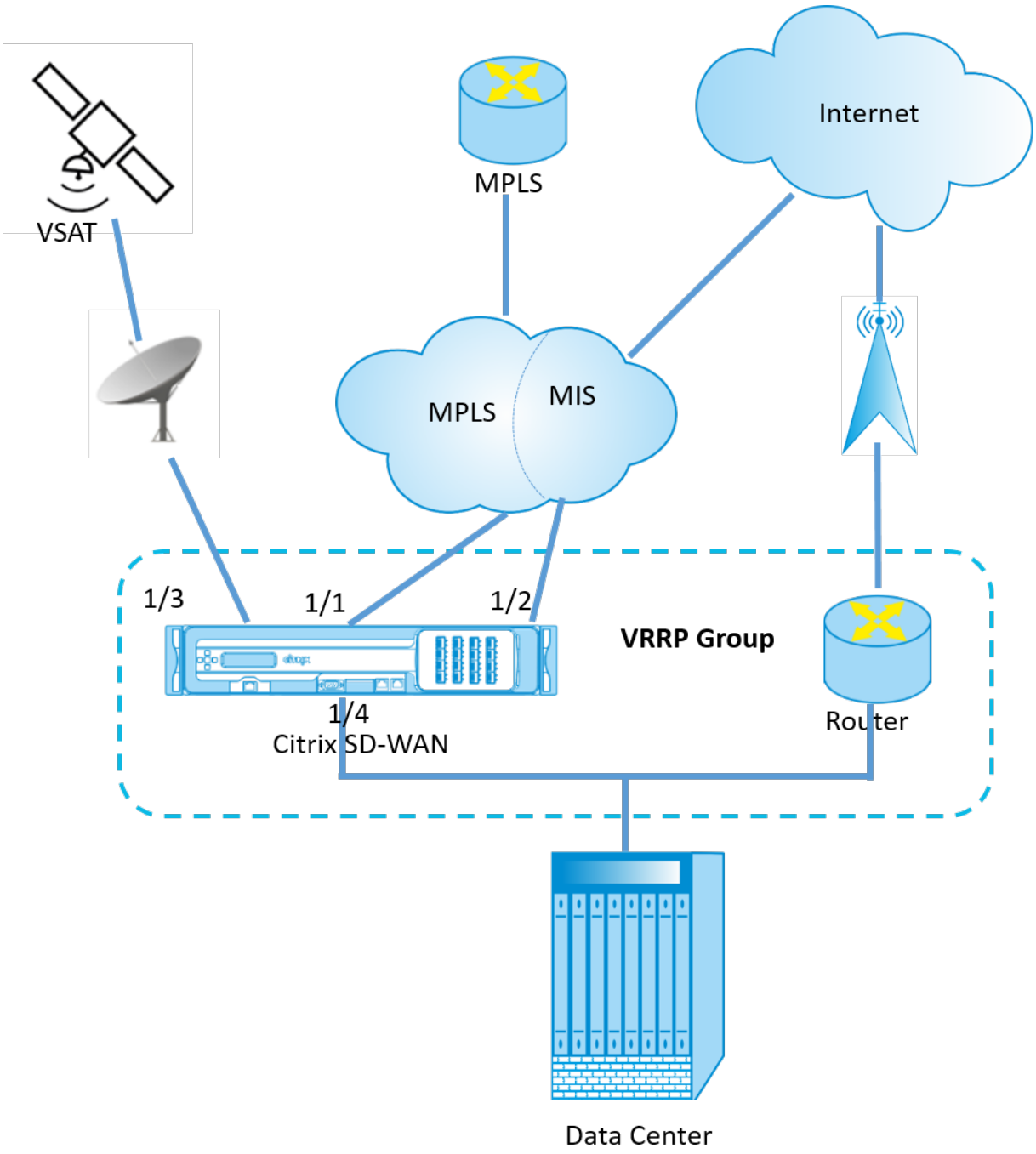
VRRP especifica un proceso de elección en el que, el router con la prioridad más alta se convierte en el maestro. Si la prioridad es la misma entre los enrutadores, el enrutador con la dirección IP más alta se convierte en el maestro. Los otros enrutadores están en estado de copia de seguridad. El proceso de

elección se inicia de nuevo si el maestro falla, un nuevo router se une al grupo o si un router existente abandona el grupo.

VRRP garantiza una ruta predeterminada de alta disponibilidad sin configurar protocolos de redirección dinámico o detección de enrutadores en todos los hosts finales.

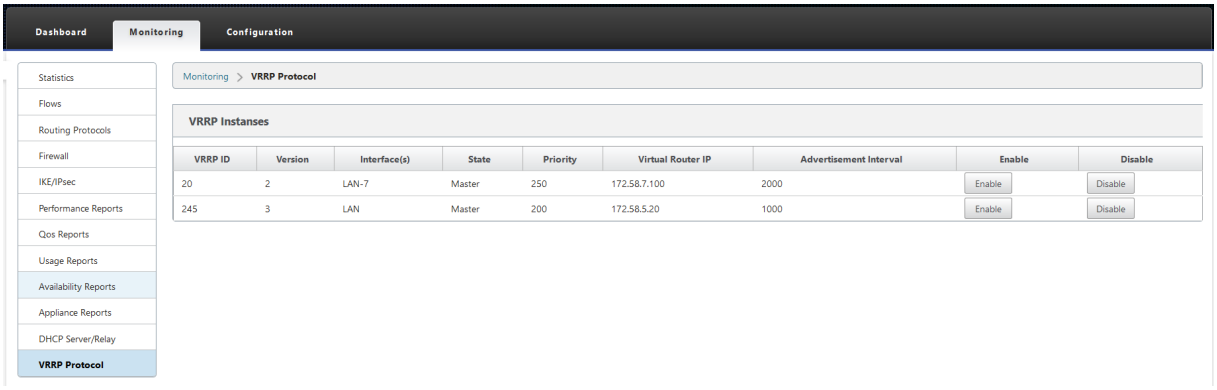
La versión 10.1 de Citrix SD-WAN admite VRRP versión 2 y versión 3 para interoperar con enrutadores de terceros. El dispositivo SD-WAN actúa como enrutador maestro y dirige el tráfico para utilizar el servicio de ruta virtual entre sitios. Puede configurar el dispositivo SD-WAN como el maestro VRRP mediante la configuración de la IP de interfaz virtual como IP VRRP y el establecimiento manual de la prioridad en un valor superior al de los enrutadores del mismo nivel. Puede configurar el intervalo de anuncio y la opción de preferencia.

El siguiente diagrama de red muestra un dispositivo Citrix SD-WAN y un enrutador configurados como grupo VRRP. El dispositivo SD-WAN está configurado para ser el maestro. Si se produce un error en el dispositivo SD-WAN, el router de copia de seguridad se llevará a cabo en milisegundos, lo que garantiza que no haya tiempo de inactividad.



Estadísticas de VRRP

Puede ver las estadísticas de VRRP en **Monitoring** > **VRRP**.



Puede ver los siguientes datos estadísticos:

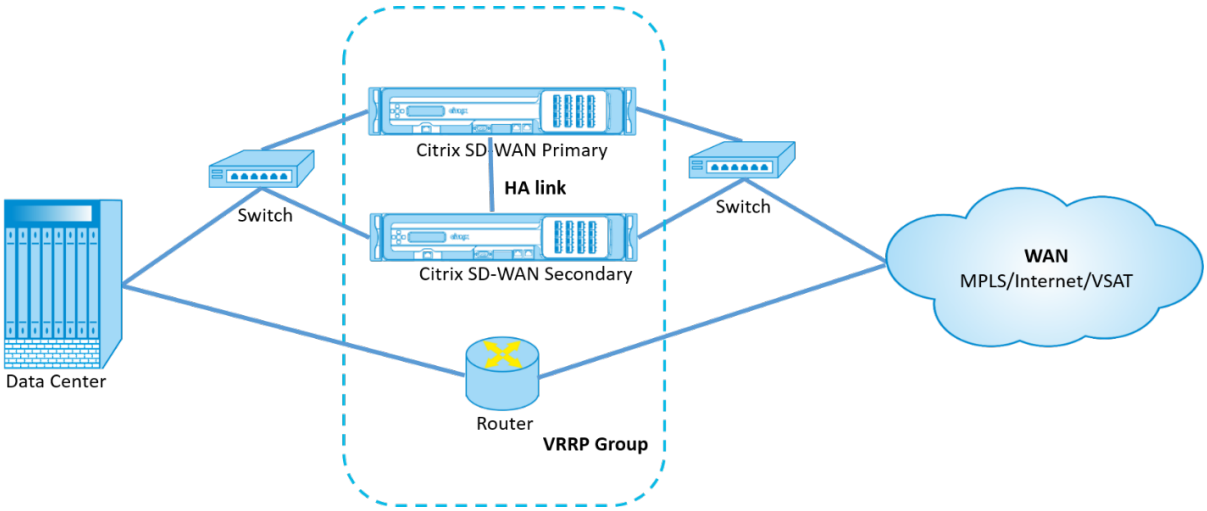
- ID de**VRRP: ID** de grupo VRRP
- **Versión: Versión** del protocolo VRRP.
- **Interfaz:** La interfaz virtual utilizada para VRRP.
- **Estado: estado** VRRP del dispositivo SD-WAN. Indica si el dispositivo es un maestro o una copia de seguridad.
- Prioridad**: prioridad** del dispositivo SD-WAN para un grupo VRRP
- **IP del enrutador virtual:** la dirección IP del enrutador virtual del grupo VRRP.
- **Intervalo de publicidad:** La frecuencia de los anuncios VRRP.
- **Activar:** seleccione esta opción para habilitar la instancia VRRP en el dispositivo SD-WAN.
- **Inhabilitar:** seleccione esta opción para inhabilitar la instancia de VRRP en el dispositivo SD-WAN.

Limitaciones

- VRRP solo se admite en la implementación en modo puerta de enlace.
- Puede configurar hasta cuatro ID de VRRP (VRID).
- En VRID pueden participar hasta 16 interfaces de red virtuales.

Alta disponibilidad y VRRP

Puede reducir significativamente el tiempo de inactividad de la red y la interrupción del tráfico aprovechando las funciones de alta disponibilidad y VRRP de su red SD-WAN. Implemente un par de dispositivos Citrix SD-WAN en funciones activas/en espera junto con un enrutador en espera para formar el grupo VRRP. Este grupo aparece como una única Gateway predeterminada con una dirección IP virtual y una dirección MAC virtual.



Los siguientes son 2 casos con la implementación anterior:

Primer caso: el temporizador de conmutación por error de alta disponibilidad en SD-WAN es igual al temporizador de conmutación por error de VRRP.

El comportamiento esperado es la conmutación de alta disponibilidad antes de la conmutación de VRRP, es decir, el tráfico continúa fluyendo a través del nuevo dispositivo Active SD-WAN. En este caso, SD-WAN continúa con el rol Maestro VRRP.

Segundo caso: Temporizador de conmutación por error de alta disponibilidad en SD-WAN mayor que el temporizador de conmutación por error de VRRP.

El comportamiento esperado es que ocurre la conmutación de VRRP al enrutador, es decir, el enrutador se convierte en VRRP Master y el tráfico podría fluir momentáneamente a través del router, evitando el dispositivo SD-WAN.

Pero una vez que ocurre la conmutación de alta disponibilidad, SD-WAN vuelve a convertirse en VRRP Master, es decir, el tráfico ahora fluye a través del nuevo dispositivo SD-WAN activo.

Para obtener más información sobre los modos de implementación de alta disponibilidad, consulte Alta disponibilidad.

Soporte de redirección para segmentación de LAN

August 26, 2022

Los dispositivos SD-WAN Standard Edition implementan la segmentación de LAN en distintos sitios en los que se implementa cualquiera de los dispositivos. Los dispositivos reconocen y mantienen un registro de las VLAN de la LAN disponibles y configuran reglas en torno a qué otros segmentos de LAN (VLAN) pueden conectarse en una ubicación remota con otro dispositivo SD-WAN Standard Edition.

La capacidad anterior se implementa mediante una tabla de redirección y reenvío virtual (VRF) que se mantiene en el dispositivo SD-WAN Standard Edition, que realiza un seguimiento de los intervalos de direcciones IP remotas accesibles para un segmento de LAN local. Este tráfico de VLAN a VLAN seguiría atravesando la WAN a través de la misma ruta virtual preestablecida entre los dos dispositivos (no es necesario crear nuevas rutas).

Un ejemplo de uso de esta funcionalidad es que un administrador de WAN puede segmentar el entorno de red de sucursal local a través de una VLAN y proporcionar acceso a algunos de esos segmentos (VLAN) a segmentos de LAN del lado de CC que tienen acceso a Internet, mientras que otros pueden no obtener dicho acceso.

Servicio de dominio de interredirección

August 26, 2022

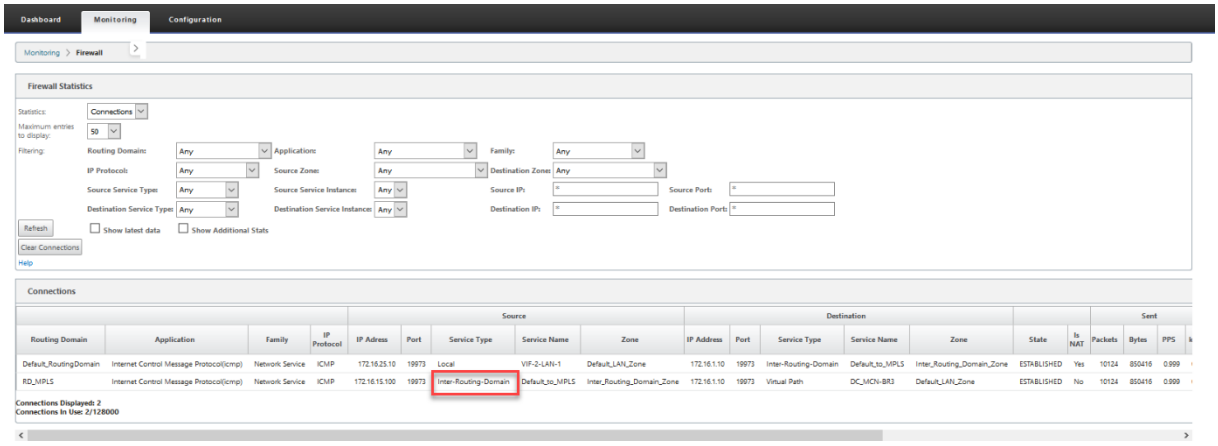
Citrix SD-WAN le permite segmentar la red mediante Dominios de redirección, lo que garantiza una alta seguridad y una administración sencilla. Con el uso del dominio de redirección, el tráfico se aísla entre sí en la red superpuesta. Cada dominio de redirección mantiene su propia tabla de redirección. Sin embargo, a veces necesitamos redirigir el tráfico entre los dominios de redirección. Por ejemplo, si los servicios compartidos, como la impresora, el analizador y el servidor de correo, se aprovisionan como un dominio de redirección independiente. El dominio de interredirección es necesario para permitir que los usuarios de diferentes dominios de redirección accedan a los servicios compartidos.

Citrix SD-WAN proporciona el servicio de dominio de interredirección estático, lo que permite la fuga de rutas entre dominios de redirección dentro de un sitio o entre sitios diferentes. Esto elimina la necesidad de un enrutador perimetral para manejar las fugas de ruta. El servicio de dominio de interredirección se puede utilizar para configurar rutas, directivas de firewall y reglas NAT.

Una nueva zona de firewall, **Inter_Routing_Domain_Zone**, se crea de forma predeterminada y sirve como zona de firewall para los Servicios de dominio de interredirección para redirección y filtrado.

Supervisión

Puede ver las estadísticas de supervisión de las conexiones que utilizan servicios de dominio de interredirección en **Supervisión** > **Estadísticas del firewall** > **Conexiones**.



Equilibrio de carga ECMP

August 26, 2022

Los grupos de rutas múltiples de igual coste (ECMP) permiten agrupar varias rutas con el mismo coste, destino y servicio. Las conexiones o los datos de sesión se equilibran la carga en todas las rutas del grupo ECMP dependiendo del tipo de grupo ECMP. Por ejemplo, considere una red con dos vínculos WAN entre una sucursal y un centro de datos que tenga el mismo coste de ruta. Tradicionalmente, uno de los enlaces WAN estaría activo y el otro permanece inactivo actuando como enlace de reserva. Con ECMP Groups, puede agrupar estos vínculos WAN juntos y permitir que el tráfico se equilibre la carga a través de ambos enlaces WAN. El equilibrio de carga ECMP garantiza:

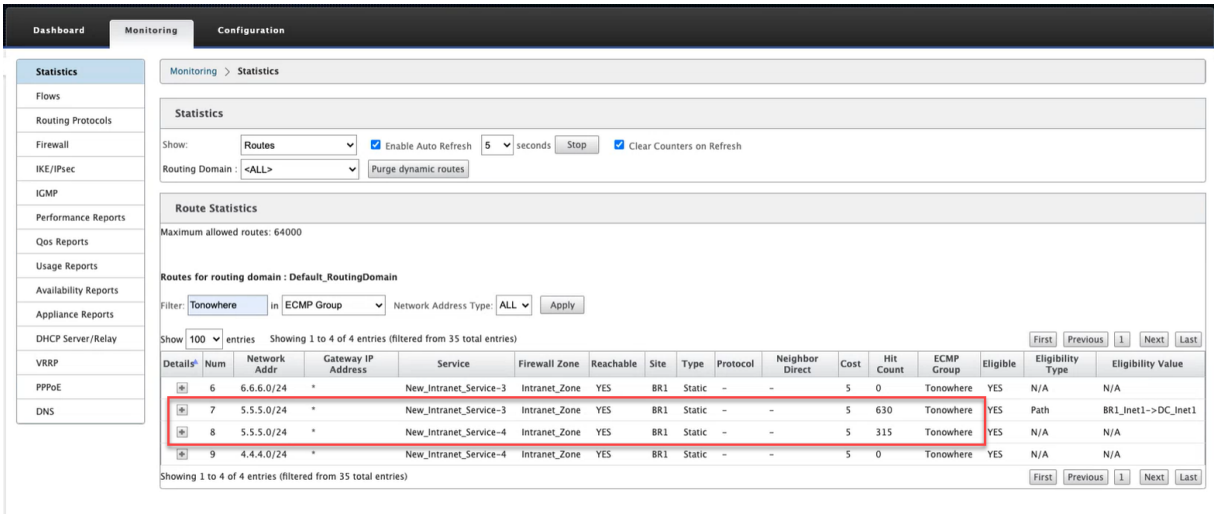
- Distribución del tráfico a través de múltiples rutas de igual coste.
- Uso óptimo del ancho de banda disponible.
- Transferencia dinámica de tráfico a otra ruta de miembro ECMP, si falla un vínculo. ECMP admite rutas estáticas en túneles IPsec/GRE.

El equilibrio de carga ECMP se admite en rutas virtuales y servicios de Intranet. Los grupos ECMP se definen a nivel global. Puede definir un máximo de 254 grupos ECMP en la red. El número máximo de rutas elegibles para ECMP en un grupo ECMP depende del dispositivo y del tipo de licencia. Citrix SD-WAN admite los dos tipos siguientes de grupos ECMP:

- Dirección IP de origen/destino: redes en las que varios clientes intentan conectarse al mismo destino, las conexiones se equilibran la carga a través de enlaces WAN de igual coste.
- Sesión: Redes donde un único cliente está conectado a un destino y se generan varias sesiones. Los datos de la sesión se equilibran la carga a través de enlaces WAN de igual coste.

Para supervisar el equilibrio de carga de ECMP, en la interfaz de usuario de SD-WAN, vaya a **Supervisión** > **Estadísticas** > **Rutas** y filtre los resultados de búsqueda utilizando el nombre del grupo

ECMP.



En los datos de muestra, vemos que todas las rutas dentro de un servicio que tiene un grupo ECMP común forman parte de ese grupo ECMP. Por ejemplo, 6.6.6.0/24 y 5.5.5.0/24 están en el grupo ECMP **Tonowhere**. Sin embargo, la carga de tráfico se equilibra entre los servicios **New_Intranet_Service-3** y **New_Intranet_Service-4** que comparten una IP de destino 5.5.5.0/24 y están asociados al mismo grupo ECMP.

> **Nota**
>
> Para el servicio SIA y Zscaler, puede equilibrar la carga en dos rutas de túnel IPsec con ECMP (activo/activo).

Seguridad

August 26, 2022

En los temas de esta sección se proporcionan instrucciones generales de seguridad para las implementaciones de Citrix SD-WAN.

Directrices de implementación de Citrix SD-WAN

Para mantener la seguridad durante todo el ciclo de vida de la implementación, Citrix recomienda la siguiente consideración de seguridad:

- Seguridad física
- Seguridad de dispositivos
- Seguridad de red

- Administración y Gestión

Los temas descritos en los siguientes vínculos proporcionan más información sobre cómo configurar la seguridad de las redes SD-WAN mediante:

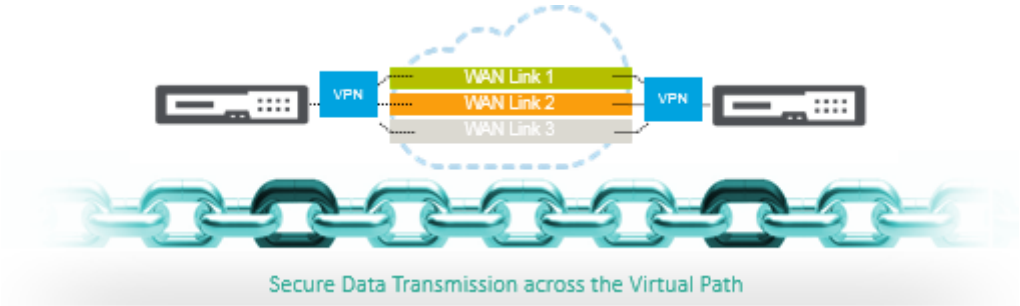
- Túneles IPsec
- Firewall

Terminación del túnel IPsec

August 26, 2022

Citrix SD-WAN admite rutas virtuales IPsec, lo que permite que los dispositivos de terceros terminen túneles VPN IPsec en el lado LAN o WAN de un dispositivo Citrix SD-WAN. Puede proteger los túneles IPsec de sitio a sitio que terminan en un dispositivo SD-WAN mediante un binario criptográfico IPsec con certificación FIPS 140-2 de nivel 1.

Citrix SD-WAN también admite tunelización IPsec resistente mediante un mecanismo de túnel de ruta virtual diferenciado.



> **Nota importante**:
>
> - A partir de la versión 11.5 de SD-WAN, todas las configuraciones de túnel IPSec e IKE solo se admiten a través de Citrix SD-WAN Orchestrator Service. Para obtener información sobre las configuraciones de IPsec/IKE de Citrix SD-WAN Orchestrator Service, consulte Servicio IPSec.
> - Citrix SD-WAN admite conectividad con Oracle Cloud Infrastructure (OCI) a través de IPsec.

Integración de Citrix SD-WAN con AWS Transit Gateway

November 16, 2022

El servicio**Amazon Web Service (AWS) Transit Gateway** permite a los clientes conectar sus Amazon Virtual Private Clouds (VPC) y sus redes locales a una única puerta de enlace. A medida que aumenta el número de cargas de trabajo que se ejecutan en AWS, puede escalar sus redes entre varias cuentas y Amazon VPC para seguir el ritmo del crecimiento.

Ahora puede conectar pares de Amazon VPC mediante el emparejamiento. Sin embargo, la gestión de la conectividad punto a punto en muchas VPC de Amazon, sin la capacidad de gestionar de forma centralizada las directivas de conectividad, puede resultar costosa y complicada desde el punto de vista operativo. Para la conectividad local, debe conectar su AWS VPN a cada Amazon VPC individual. Esta solución puede llevar mucho tiempo y ser difícil de administrar cuando el número de VPC crece a cientos.

Con **AWS Transit Gateway**, solo tiene que crear y gestionar una única conexión desde la puerta de enlace central a cada Amazon VPC, centro de datos local u oficina remota a través de la red. Transit Gateway actúa como un concentrador que controla cómo se redirige el tráfico entre todas las redes conectadas que actúan como radios. Este modelo de hub y radio simplifica significativamente la gestión y reduce los costes operativos, ya que cada red solo tiene que conectarse a Transit Gateway y no a todas las demás redes. Cualquier VPC nueva está conectada a Transit Gateway y está disponible automáticamente para todas las demás redes conectadas a Transit Gateway. Esta facilidad de conectividad hace que sea fácil escalar su red a medida que crece.

A medida que las empresas migran un número cada vez mayor de aplicaciones, servicios e infraestructura a la nube, están implementando rápidamente SD-WAN para aprovechar los beneficios de la conectividad de banda ancha y conectar directamente a los usuarios de sitios de sucursales con los recursos de la nube. Existen muchos desafíos con las complejidades de crear y administrar redes privadas globales mediante servicios de transporte por Internet para conectar ubicaciones distribuidas geográficamente y usuarios con recursos en la nube basados en proximidad. **AWS Transit Gateway Network Manager** cambia este paradigma. Ahora, los clientes de Citrix SD-WAN que utilizan AWS pueden utilizar Citrix SD-WAN con AWS Transit Gateway integrando el dispositivo de sucursal de Citrix SD-WAN AWS Transit Gateway para ofrecer la más alta calidad de experiencia a los usuarios con la capacidad de llegar a todas las VPC conectadas a Transit Gateway.

Los siguientes son los pasos para integrar Citrix SD-WAN con AWS Transit Gateway:

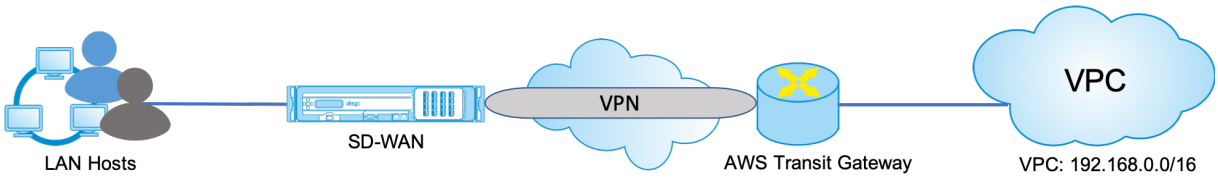
1. Cree AWS Transit Gateway.
2. Conecte una VPN a Transit Gateway (ya sea una VPN existente o una nueva).
3. Adjunte VPN a Transit Gateway configurada donde la VPN está con el sitio SD-WAN ubicado en las instalaciones o en cualquier nube (AWS, Azure o GCP).
4. Establezca el peering Border Gateway Protocol (BGP) sobre el túnel IPsec con AWS Transit Gateway desde Citrix SD-WAN para conocer las redes (VPC) conectadas a Transit Gateway.

Caso de uso

El caso de uso es llegar a los recursos implementados en AWS (en cualquier VPC) desde el entorno de sucursal. El uso de AWS Transit Gateway permite que el tráfico llegue a todas las VPC conectadas a Transit Gateway sin ocuparse de las rutas BGP. Para lograr esto, realice los siguientes métodos:

- Establezca IPsec to AWS Transit Gateway desde la sucursal del dispositivo Citrix SD-WAN. En este método de implementación no obtendrá beneficios completos de SD-WAN, ya que el tráfico pasará a través de IPsec.
- Implemente un dispositivo Citrix SD-WAN dentro de AWS y conéctelo a su dispositivo Citrix SD-WAN local a través de una ruta virtual.

Independientemente del método elegido, el tráfico llega a las VPC conectadas a Transit Gateway sin administrar manualmente la redirección dentro de la infraestructura de AWS.

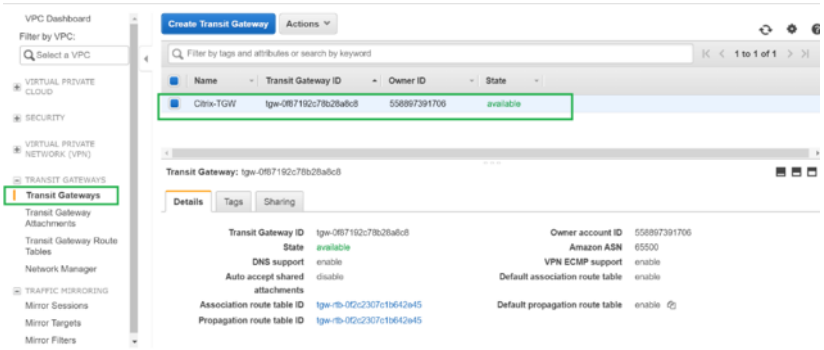


Configuración de AWS Transit Gateway

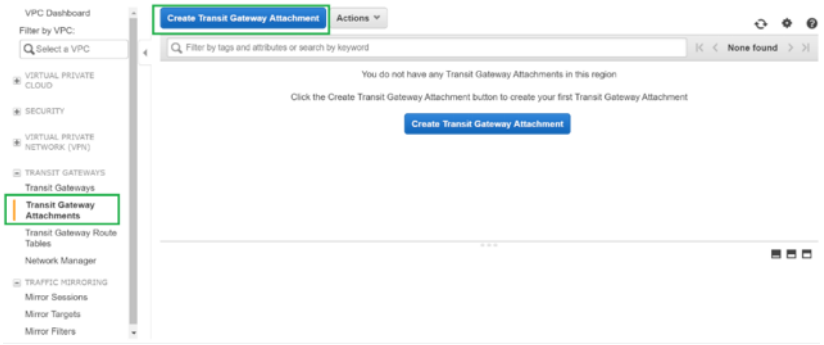
Para crear **AWS Transit Gateway**, vaya al panel de VPC y vaya a la sección **Transit Gateway**.

1. Proporcione el nombre, la descripción y el número ASN de Amazon de Transit Gateway como se resaltan en la siguiente captura de pantalla y haga clic en **Crear Transit Gateway**.

   Una vez completada la creación de Transit Gateway, podrá ver el estado como **Disponible**.

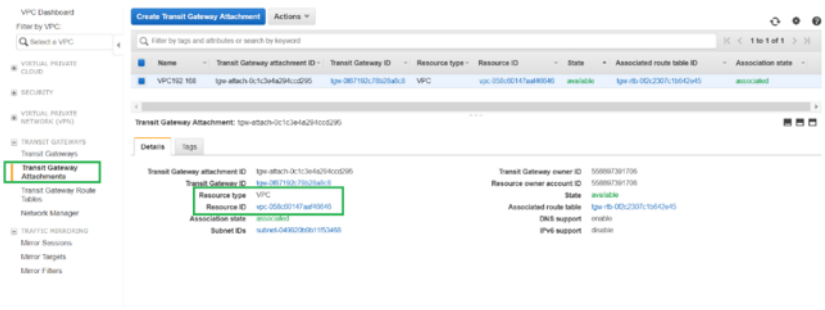


2. Para crear los **anexos de Transit Gateway**, vaya a **Transit Gateways > Anexos de Transit Gateway** y haga clic en **Crear anexos de Transit Gateway**.



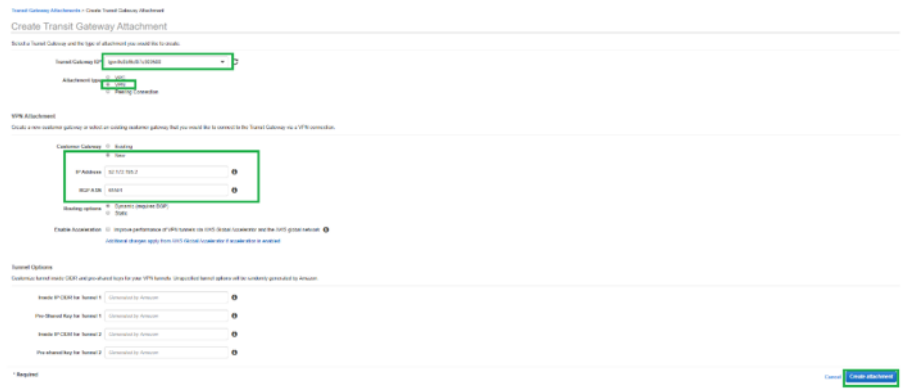
3. Seleccione la Transit Gateway creada en la lista desplegable y seleccione el tipo de adjunto como **VPC**. Proporcione la etiqueta de nombre de datos adjuntos y seleccione el ID de VPC que quiere adjuntar a la Transit Gateway creada. Una de las subredes de la VPC seleccionada se seleccionará automáticamente. Haga clic en **Crear datos adjuntos** para adjuntar VPC a Transit Gateway.

4. Después de adjuntar la VPC a Transit Gateway, puede ver que el **tipo de recurso VPC** se asoció a la Transit Gateway.

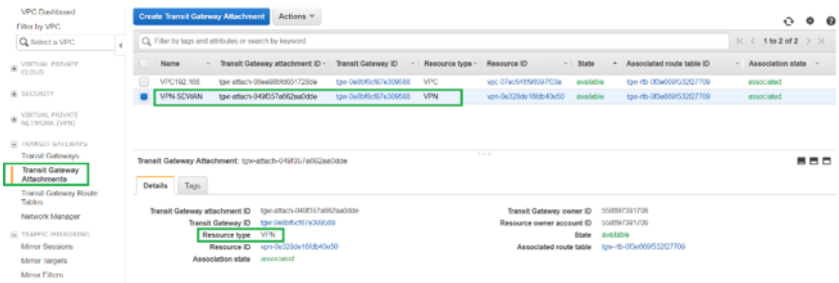


5. Para adjuntar SD-WAN a Transit Gateway mediante VPN, seleccione el **ID de Transit Gateway** en la lista desplegable y seleccione **Tipo de archivo adjunto** como **VPN**. Asegúrese de seleccionar el ID de Transit Gateway correcto.

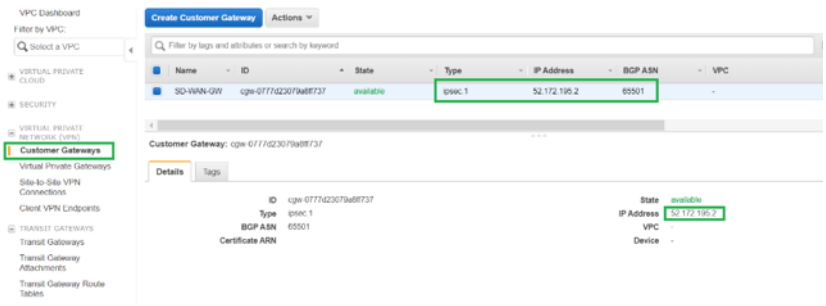
   Adjunte una nueva puerta de enlace de cliente VPN proporcionando la dirección IP pública del enlace WAN SD-WAN y su número ASN BGP. Haga clic en **Crear adjunto** para adjuntar VPN con Transit Gateway.



6. Una vez que la VPN esté conectada a Transit Gateway, puede ver los detalles como se muestra en la siguiente captura de pantalla:

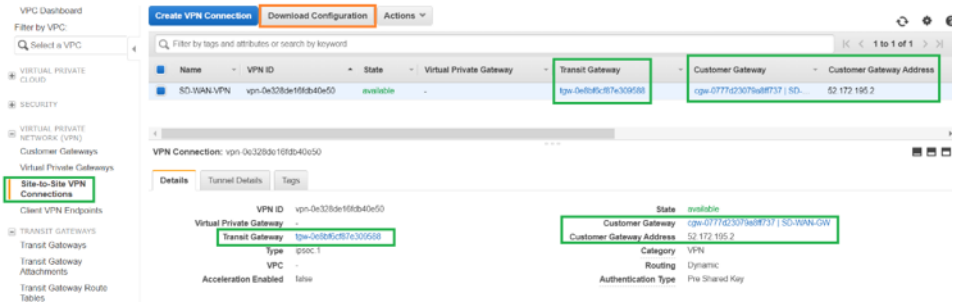


7. En **Puertas de enlace de clientes**, la puerta de enlace de cliente SD-WAN y la conexión VPN de sitio a sitio se crean como parte de la conexión VPN a Transit Gateway. Puede ver que la puerta de enlace del cliente de SD-WAN se crea junto con la dirección IP de esta puerta de enlace de cliente que representa la dirección IP pública del vínculo WAN de SD-WAN.

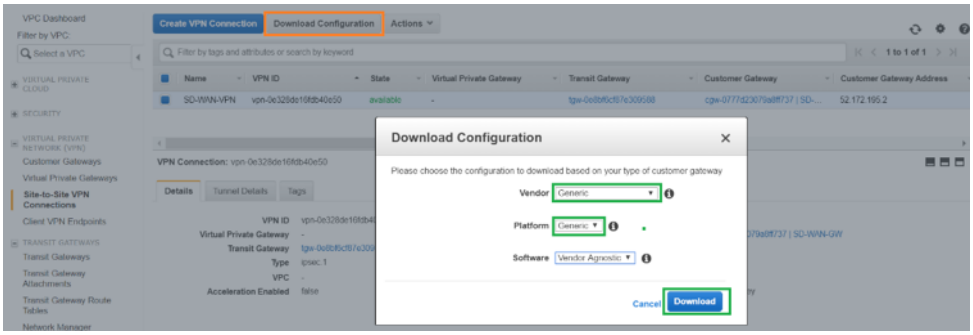


8. Vaya a **Conexiones VPN de sitio a sitio para descargar la configuración de VPNde puerta de enlace de cliente de SD-WAN**. Este archivo de configuración tiene dos detalles de túnel IPsec junto con la información del par BGP. Se crean dos túneles de SD-WAN a Transit Gateway para redundancia.

   Puede ver que la dirección IP pública del vínculo WAN SD-WAN se configuró como la dirección de puerta de enlace del cliente.



9. Haga clic en **Descargar configuración** y descargue el archivo de configuración VPN. Seleccione el **proveedor**, **la plataforma** como **genérica**y **el software** como **independiente del proveedor**.



   El archivo de configuración descargado contiene la siguiente información:

   - Configuración de IKE
   - Configuración de IPsec para AWS Transit Gateway
   - Configuración de interfaz de túnel
   - Configuración de BGP

Esta información está disponible para dos túneles IPsec para High Availability (HA). Asegúrese de configurar ambos puntos finales del túnel mientras configura esto en SD-WAN. Vea la siguiente captura de pantalla para referencia:

!Dos túneles IPsec

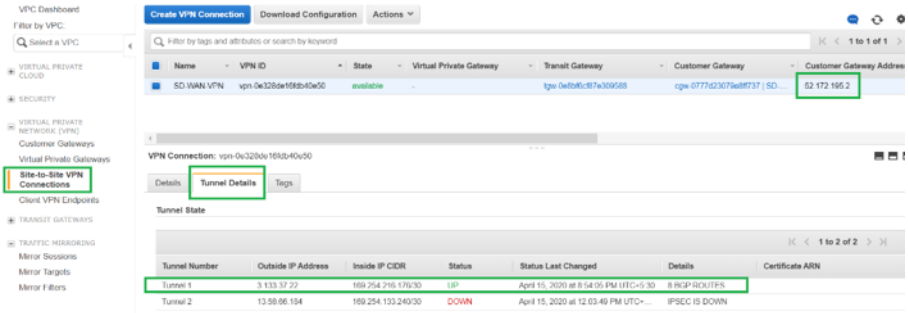
Configurar el servicio de Intranet en SD-WAN

Para configurar un servicio de Intranet a través de Citrix SD-WAN Orchestrator Service, vaya a Servicios de entrega.

Supervisión y solución de problemas en AWS

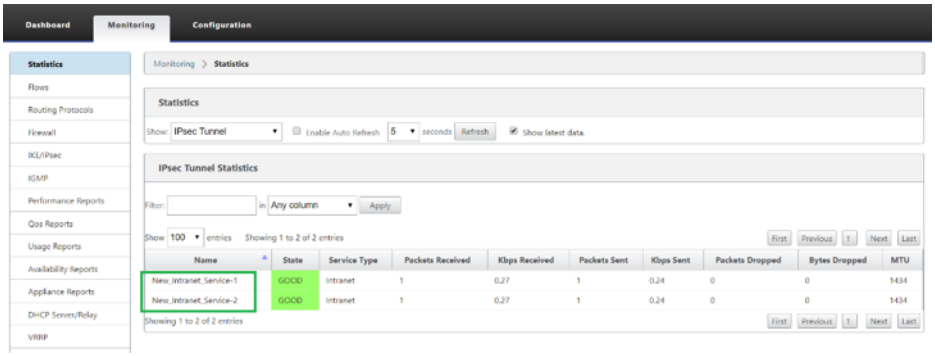
1. Para comprobar el estado del establecimiento del túnel IPsec en AWS, vaya a **RED PRIVADA VIRTUAL (VPN) > Conexiones VPN de sitio a sitio**. En la siguiente captura de pantalla, puede observar que la dirección de puerta de enlace del cliente representa la dirección IP pública de enlace SD-WAN mediante la cual se ha establecido el túnel.

   El estado del túnel se muestra como **UP**. También se puede observar que AWS ha aprendido **8 RUTAS BGP** de SD-WAN. Esto significa que SD-WAN puede establecer Túnel con AWS Transit Gateway y también puede intercambiar rutas a través de BGP.

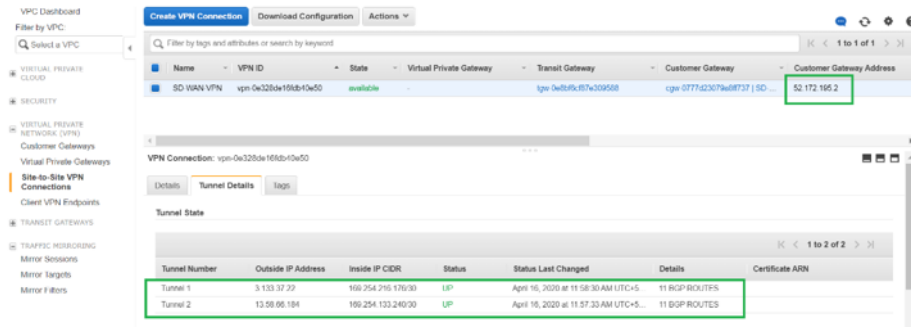


2. Configure los detalles de IPsec y BGP relacionados con el segundo túnel en función del archivo de configuración descargado en SD-WAN.

   El estado relacionado con ambos túneles se puede supervisar en SD-WAN de la siguiente manera:



3. El estado relacionado con ambos túneles se puede supervisar en AWS de la siguiente manera:

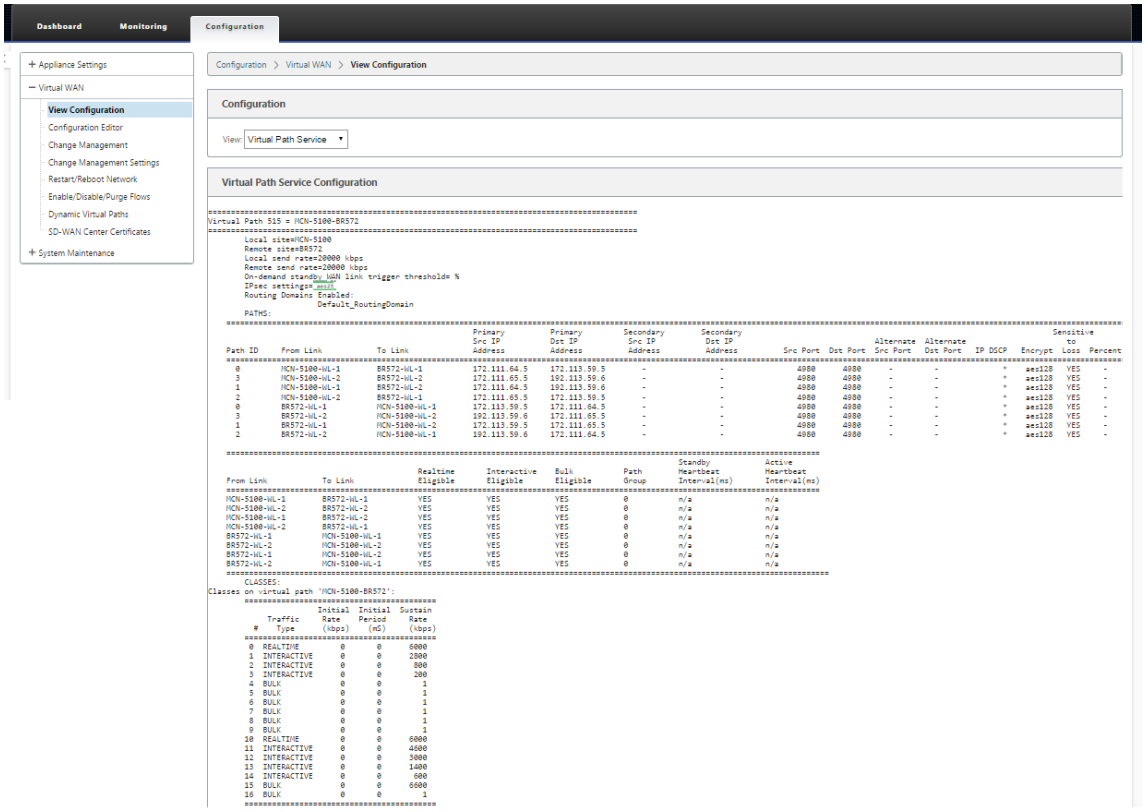


Cómo ver la configuración del túnel ipsec

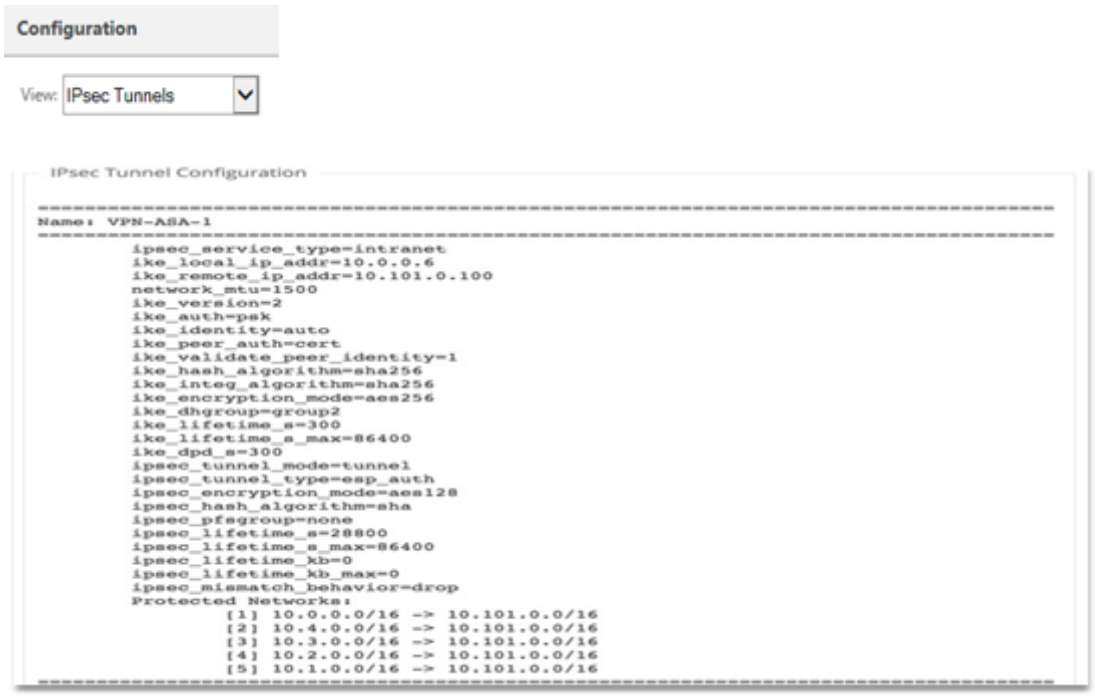
August 26, 2022

Para ver la configuración del túnel ipsec:

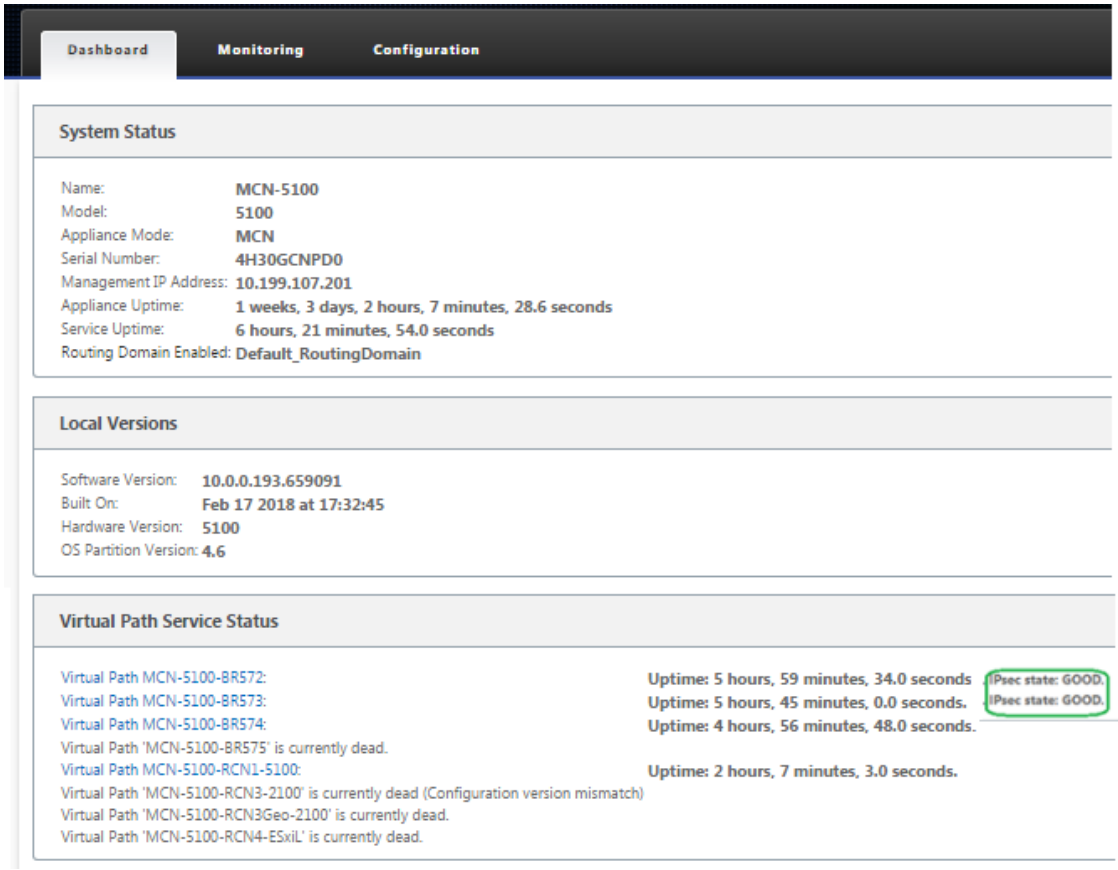
1. Vaya a **Configuración > WAN virtual** > **Ver configuración**.
2. Seleccione **Virtual Path Service** en el menú desplegable. La configuración de IPSec solo se muestra si IPSec está habilitada.



3. Seleccione **Túneles IPsec** en el menú desplegable para ver la configuración del túnel IPsec.



4. Cada ruta virtual mostrará su propio estado de túnel IPsec como se muestra a continuación.

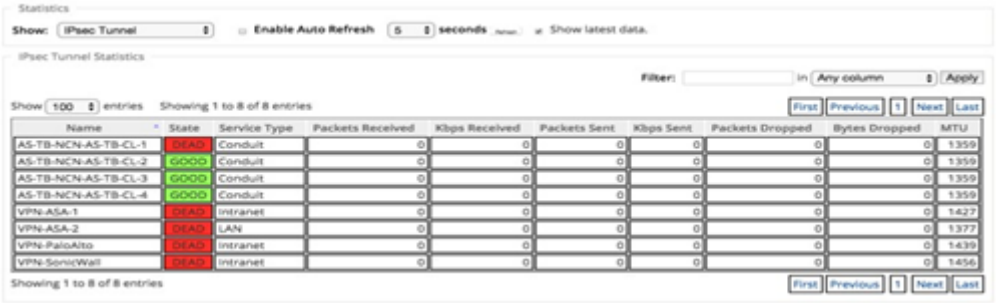


Supervisión y registro de IPsec

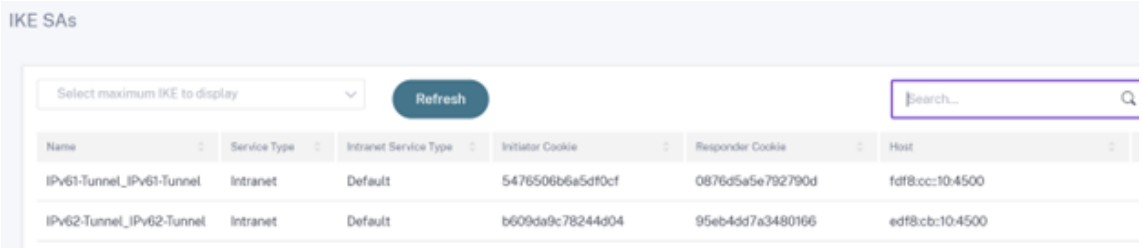
August 26, 2022

Para supervisar las estadísticas de SA IPsec/IKE:

1. Vaya a **Supervisar > IPsec**. Elija las **SA de IPSec**:



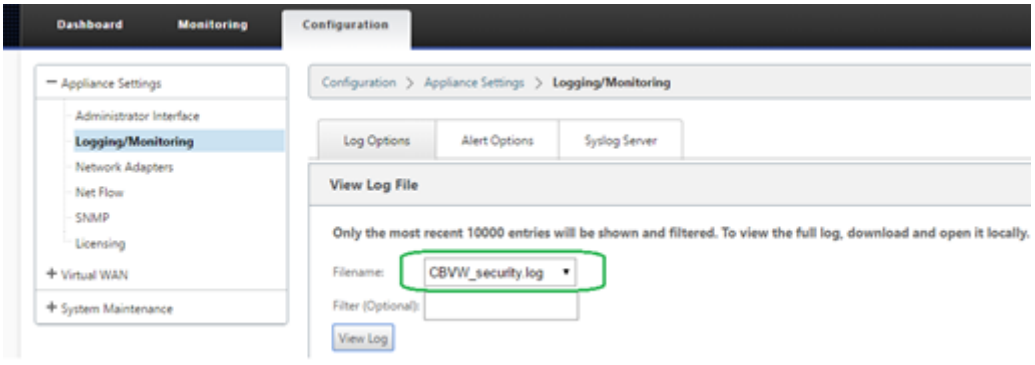
2. Vaya a **Supervisar** > **SA de IKE**. Observe los túneles IPsec configurados, las asociaciones de servicios IKE e IPsec entre dos puntos finales VPN o en modo configurados dentro de la red SD-WAN.

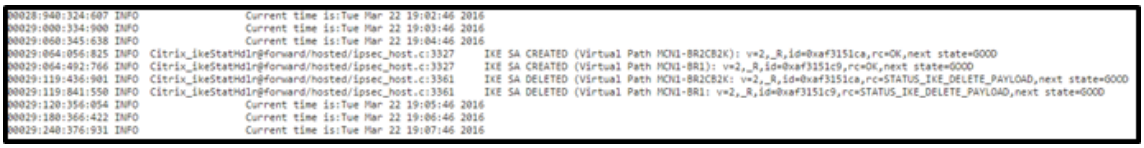


Cómo supervisar los registros de IPSec

1. Vaya a **Configuración** > **Configuración del dispositivo** > **Registrar/Supervisión**. Seleccione **Nombre de archivo** en el menú desplegable y haga clic en **Ver registro**. Puede ver los siguientes detalles de registro del túnel IPsec:

    - Creación y eliminación de túnel IPsec
    - Cambio de estado del túnel IPsec

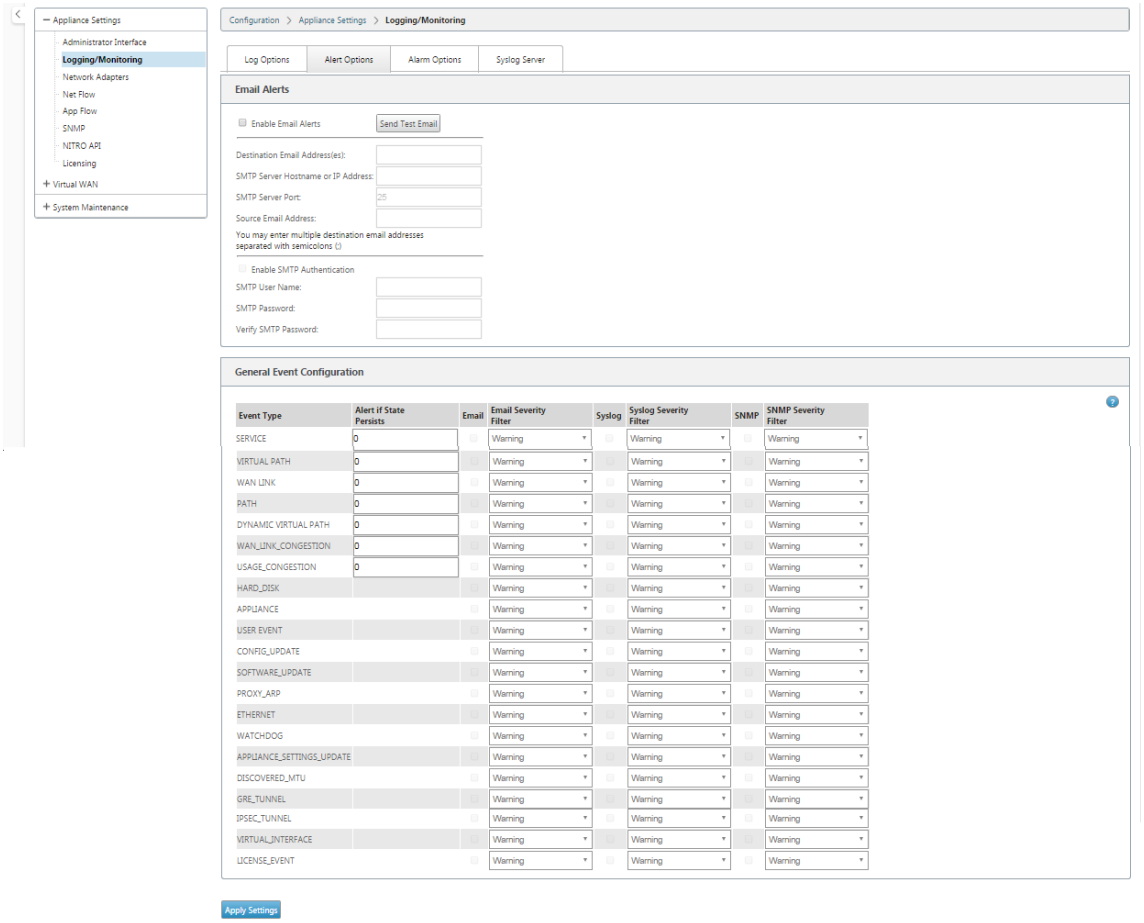




Cómo ver las alertas del túnel IPSec

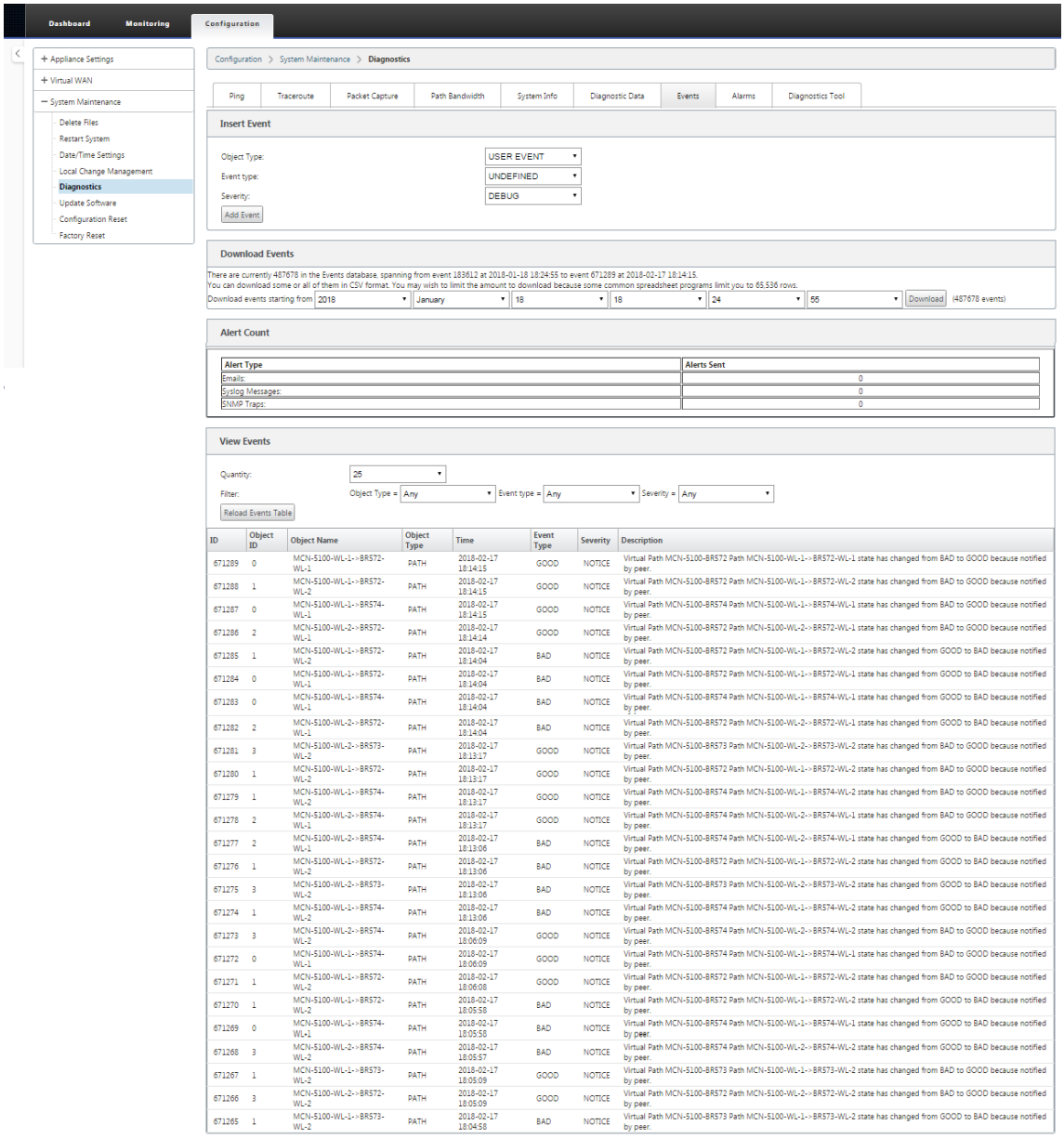
1. Vaya a **Configuración** > **Configuración del dispositivo > Registrar/Supervisión** > **Opciones de alerta**.
2. Cree alertas de correo electrónico y syslog para la generación de informes del estado del túnel IPsec.

    - Admite IPSEC_TUNNEL como uno de los tipos de evento que permite configurar los filtros de gravedad de correo electrónico y syslog.



Cómo supervisar los eventos del túnel IPSec

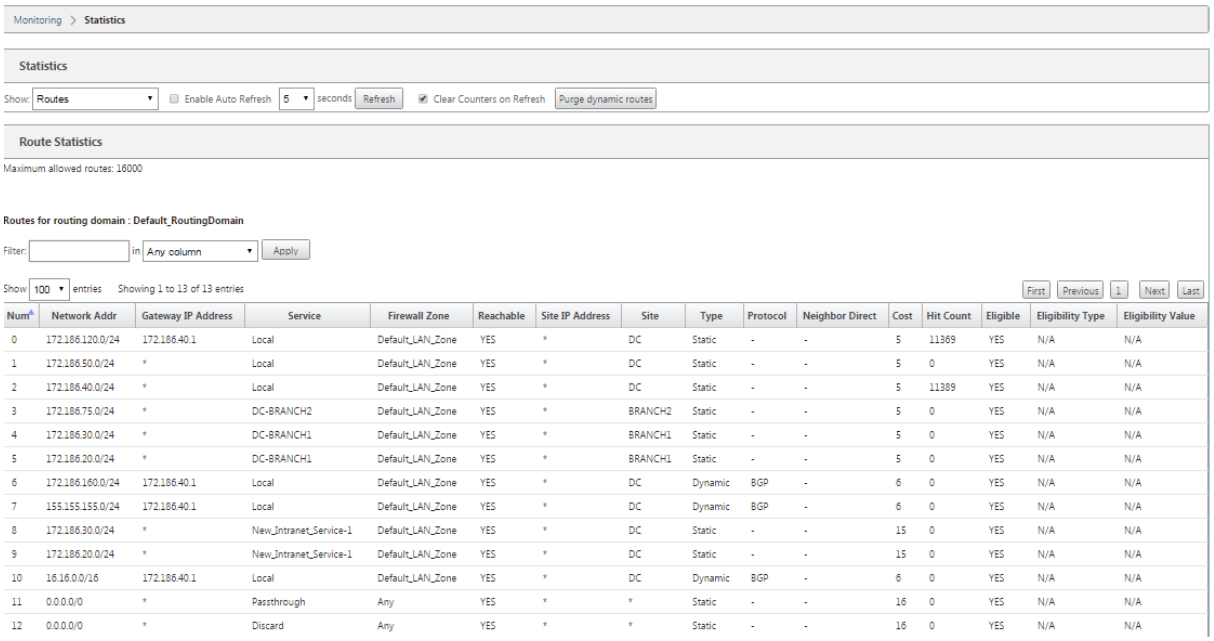
1. Vaya a **Configuración > Mantenimiento del sistema** > **Diagnóstico** > **Sucesos**.
2. Agregue eventos basados en el tipo de objeto **IPSEC_TUNNEL**. Crear filtros para todos los eventos relacionados con IPsec.



Elegibilidad para rutas de ruta no virtuales ipsec

August 26, 2022

En versiones anteriores, las rutas de túnel ipsec permanecían en la tabla de rutas, incluso si el túnel dejaba de estar disponible.



Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.186.120.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11369	YES	N/A	N/A
1	172.186.50.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	172.186.40.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11389	YES	N/A	N/A
3	172.186.75.0/24	*	DC-BRANCH2	Default_LAN_Zone	YES	*	BRANCH2	Static	-	-	5	0	YES	N/A	N/A
4	172.186.30.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
5	172.186.20.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
6	172.186.160.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	155.155.155.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	172.186.30.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
9	172.186.20.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
10	16.16.0.0/16	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Cumplimiento de FIPS

August 26, 2022

En Citrix SD-WAN, el modo FIPS obliga a los usuarios a configurar valores compatibles con FIPS para sus túneles IPsec e IPsec para rutas virtuales.

- Muestra el modo IKE compatible con FIPS.
- Muestra un grupo IKE DH compatible con FIPS desde el que los usuarios pueden seleccionar los parámetros necesarios para configurar el dispositivo en modo compatible con FIPS (2,5,14 — 21).
- Muestra el tipo de túnel IPsec compatible con FIPS en la configuración de IPsec para rutas virtuales
- Modo de integridad IKE hash e (IKEv2), modo de autenticación IPsec.
- Realiza errores de auditoría para la configuración de vida útil basada en FIPS

Para habilitar el cumplimiento de FIPS mediante Citrix SD-WAN Orchestrator Service, consulte Modo FIPS.

Citrix SD-WAN Secure Web Gateway

August 26, 2022

Para proteger el tráfico y aplicar directivas, las empresas suelen utilizar vínculos MPLS para realizar backhaul de tráfico de sucursales al centro de datos corporativo. El centro de datos aplica directivas de seguridad, filtra el tráfico a través de dispositivos de seguridad para detectar malware y enruta el tráfico a través de un ISP. Este tipo de backhauling a través de enlaces MPLS privados es costoso. También da como resultado una latencia significativa, lo que crea una mala experiencia de usuario en el sitio de la sucursal. También existe el riesgo de que los usuarios eludieran los controles de seguridad.

Una alternativa al backhauling es agregar dispositivos de seguridad en la sucursal. Sin embargo, el coste y la complejidad aumentan a medida que se instalan varios dispositivos para mantener directivas coherentes en todos los sitios.Y, si tiene muchas sucursales, la administración de costes se vuelve poco práctica.

- ¡Zscaler!

La solución ideal para aplicar la seguridad sin agregar costes, complejidad o latencia es redirigir todo el tráfico de Internet de sucursal desde el dispositivo Citrix SD-WAN a Zscaler Cloud Security Platform. A continuación, puede utilizar una consola central de Zscaler para crear directivas de seguridad granulares para sus usuarios. Las directivas se aplican de forma coherente tanto si el usuario se encuentra en el centro de datos como en un sitio de sucursal. Debido a que la solución de seguridad de Zscaler se basa en la nube, no es necesario agregar más dispositivos de seguridad a la red.

Cumplimiento de FIPS:

El Instituto Nacional de Estándares y Tecnología (NIST) desarrolla Normas Federales de Procesamiento de Información (FIPS) en áreas para las que no existen normas voluntarias. FIPS aborda los siguientes problemas:

- Compatibilidad entre diferentes sistemas.
- Portabilidad de datos y software.
- Seguridad informática rentable y privacidad de la información confidencial.

FIPS especifica los requisitos de seguridad de un módulo criptográfico utilizado en los sistemas de seguridad. Para aplicar estos estándares de seguridad al procesamiento realizado por un dispositivo Citrix SD-WAN, configure el modo FIPS.

Punto de fuerza:

Mediante Citrix SD-WAN, puede utilizar la función de redirección de firewall (proxy transparente por NAT de destino) para redirigir el tráfico de Internet (HTTP y HTTPS) desde un dispositivo SD-WAN en el perímetro empresarial al módulo de seguridad alojado en la nube de Forcepoint. Puede redirigir el

tráfico HTTP desde el puerto 80 al puerto 8081 y el tráfico HTTPS desde el puerto 443 al puerto 8443 del servidor proxy en la nube Forcepoint más cercano.

Integración de Zscaler mediante túneles GRE y túneles IPsec

November 16, 2022

Zscaler Cloud Security Platform actúa como una serie de puestos de comprobación de seguridad en más de 100 centros de datos en todo el mundo. Con solo redirigir su tráfico de Internet a Zscaler, puede proteger inmediatamente sus tiendas, sucursales y ubicaciones remotas. Zscaler conecta a los usuarios con Internet, inspeccionando cada byte de tráfico, incluso si está encriptado o comprimido.

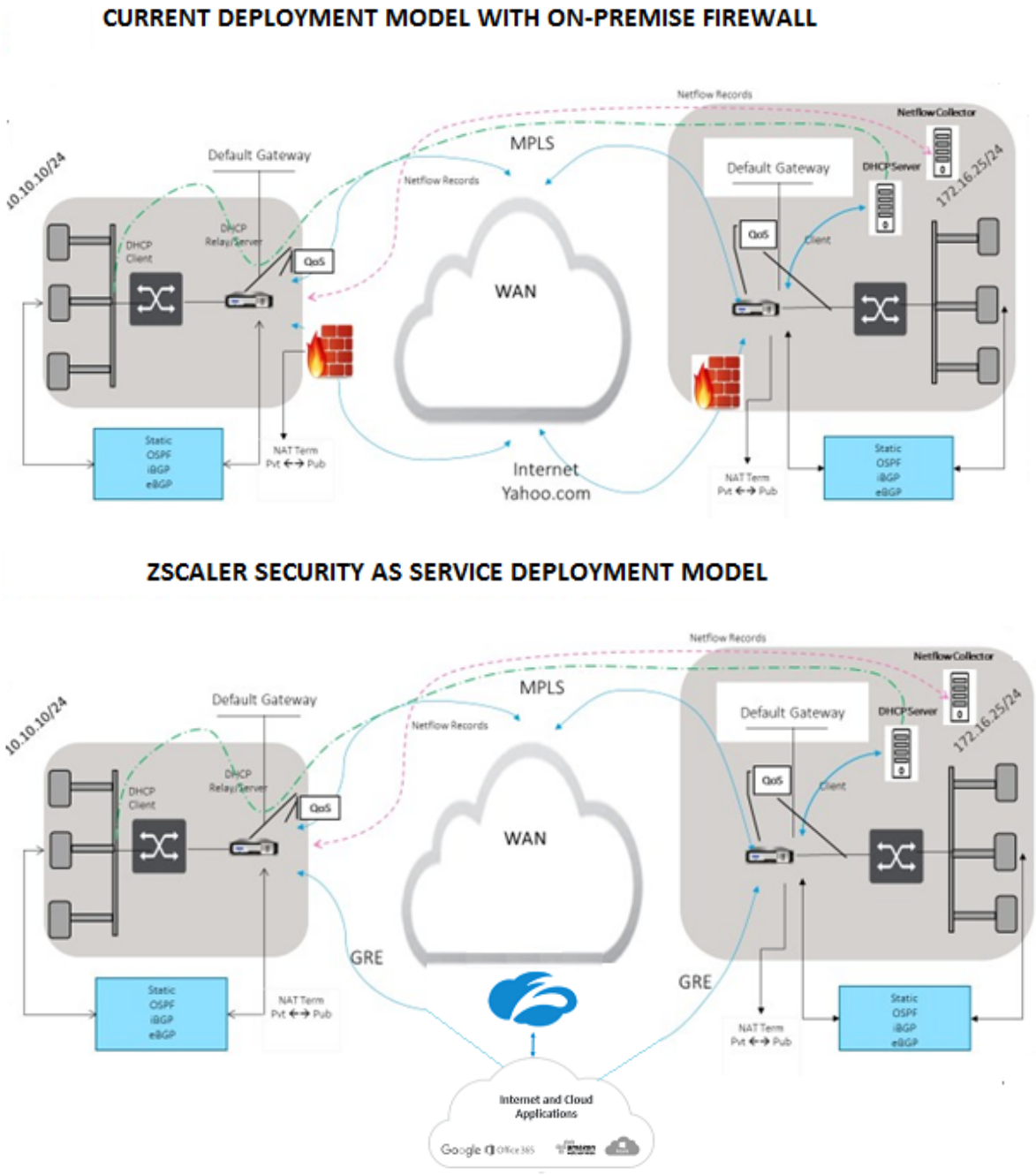
Los dispositivos Citrix SD-WAN pueden conectarse a una red en la nube de Zscaler a través de túneles GRE en el sitio del cliente. Una implementación de Zscaler mediante dispositivos SD-WAN admite la siguiente funcionalidad:

- Reenviar todo el tráfico GRE a Zscaler, lo que permite la ruptura directa de Internet.
- Acceso directo a Internet (DIA) mediante Zscaler en base a un sitio por cliente.
  - En algunos sitios, es posible que quiera proporcionar a DIA equipo de seguridad local y no utilizar Zscaler.
  - En algunos sitios, puede optar por hacer backhaul el tráfico del sitio de otro cliente para obtener acceso a Internet.
- Implementaciones de redirección y reenvío virtuales.
- Un enlace WAN como parte de los servicios de Internet.

Zscaler es un servicio en la nube. Debe configurarlo como servicio y definir los vínculos WAN subyacentes:

- Configure un servicio de Internet en el centro de datos y en la sucursal a través de GRE.
- Configure un enlace de Internet público de confianza en el centro de datos y en las sucursales.

Topología



Para utilizar el reenvío de tráfico del túnel GRE o del túnel IPsec:

1. Inicie sesión en el portal de ayuda de Zscaler en: https://help.zscaler.com/submit-ticket.
2. Crear un tíquet y proporcionar la dirección IP pública estática, que se utiliza como la dirección IP de origen del túnel GRE o IPsec.

Zscaler utiliza la dirección IP de origen para identificar la dirección IP del cliente. La IP de origen debe

ser una IP pública estática. Zscaler responde con dos direcciones IP ZEN (primaria y secundaria) para transmitir el tráfico. Los mensajes de mantenimiento vivo de GRE se pueden utilizar para determinar el estado de los túneles.

Zscaler utiliza el valor de la dirección IP de origen para identificar la dirección IP del cliente. Este valor debe ser una dirección IP pública estática. Zscaler responde con dos direcciones IP ZEN [DR1] a las que redirigir el tráfico. Los mensajes GRE keep-alive se pueden utilizar para determinar el estado de los túneles.

Direcciones IP de ejemplo

Primary (Principal)

Dirección IP del router interno: 172.17.6.241/30 Dirección IP ZEN interna: 172.17.6.242/30

Secundario

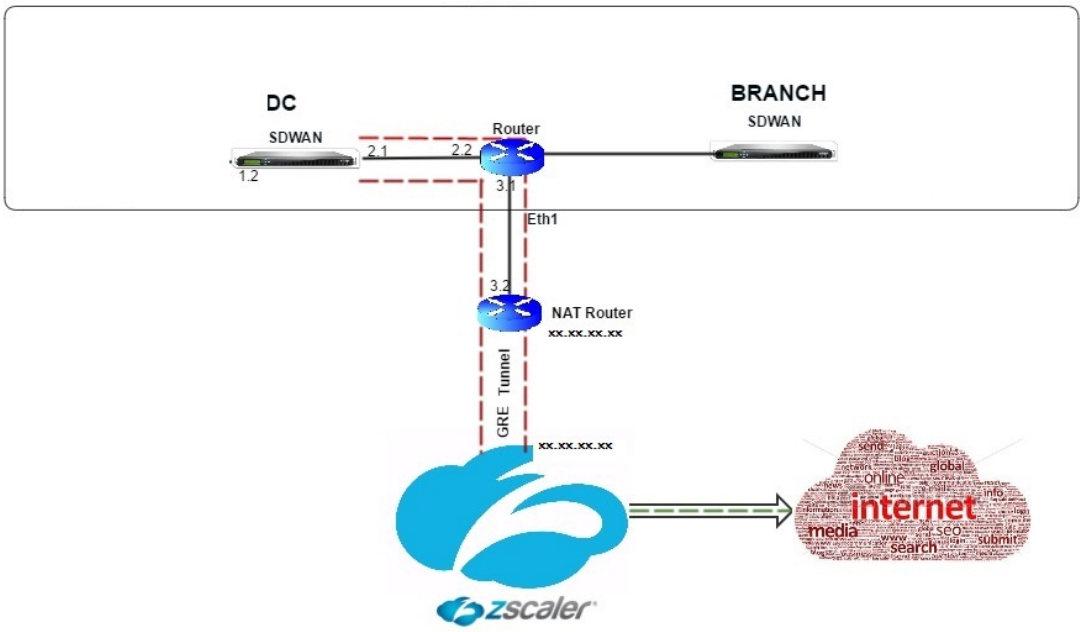
Dirección IP interna del router: 172.17.6.245/30 Dirección IP ZEN interna: 172.17.6.246/30

Configuración de un servicio de Internet

Para configurar un servicio de Internet a través de Citrix SD-WAN Orchestrator Service, consulte Servicios de entrega. Para obtener más información sobre cómo habilitar el servicio de Internet en un sitio, consulte Direct Internet Breakout.

Configurar túnel GRE

1. La dirección IP de origen es la dirección IP de origen del túnel. Si la dirección IP de origen del túnel es NAT, la dirección IP de origen público es la dirección IP pública de origen del túnel, incluso si está NAT en un dispositivo intermedio diferente.
2. La dirección IP de destino es la dirección IP ZEN que proporciona Zscaler.
3. La dirección IP de origen y la dirección IP de destino son los encabezados GRE del router cuando se encapsula la carga útil original.
4. La dirección IP del túnel y el prefijo son las direcciones IP del propio túnel GRE. Esto resulta útil para redirigir el tráfico a través del túnel GRE. El tráfico necesita esta dirección IP como dirección de puerta de enlace.



Para configurar el túnel GRE a través del servicio Cirix SD-WAN Orchestrator, consulte Túnel GRE.

Configurar rutas para túneles GRE

Configure rutas para reenviar los servicios de prefijos de Internet a los túneles GRE de Zscaler.

- La dirección IP ZEN (IP de destino del túnel, que se muestra como 104.129.194.38 en la ilustración anterior) debe establecerse en Internet de tipo servicio. Esto es necesario para que el tráfico destinado a Zscaler se contabiliza desde el servicio de Internet.
- Todo el tráfico destinado a Zscaler debe coincidir con la ruta predeterminada 0/0 y transmitirse a través del túnel GRE. Asegúrese de que la ruta 0/0 utilizada para [DR1] el túnel GRE tenga un coste menor que el de paso o cualquier otro tipo de servicio.
- Del mismo modo, el túnel GRE de respaldo a Zscaler debe tener un coste mayor que el del túnel GRE primario.
- Asegúrese de que existan rutas no recursivas para la dirección IP ZEN.

> **Nota**
>
> Si no tiene rutas específicas para la dirección IP de Zscaler, configure el prefijo de ruta 0.0.0.0/0 para que coincida con la dirección IP ZEN y redirigirla a través de un bucle de encapsulación de túnel GRE. Esta configuración utiliza los túneles en modo de respaldo activo. Con los valores mostrados en la ilustración anterior, el tráfico cambia automáticamente al túnel con la dirección IP de la puerta de enlace 172.17.6.242. Si lo quiere, config-

> ure una ruta de ruta virtual de backhaul. De lo contrario, establezca el intervalo de mantenimiento activo del túnel de copia de seguridad en cero. Esto permite el acceso seguro a Internet a un sitio incluso si fallan los túneles de Zscaler.
>
> Se admiten los mensajes keep-alive GRE. Se agrega un nuevo campo denominado **IP de origen público** que proporciona la dirección NAT de la dirección de origen GRE a la interfaz GUI de Citrix SD-WAN (en el caso de que el origen del túnel del dispositivo SD-WAN sea NATted por un dispositivo intermedio). La GUI de Citrix SD-WAN incluye un campo denominado IP de origen público, que proporciona la dirección NAT de la dirección de origen GRE cuando un dispositivo intermedio da NAT al origen del túnel del dispositivo Citrix SD-WAN.

Limitaciones

- No se admiten varias implementaciones de VRF.
- Los túneles GRE de respaldo primarios solo son compatibles con un modo de diseño de alta disponibilidad.

Para supervisar las estadísticas de túneles GRE e IPsec:

En la interfaz web de SD-WAN, vaya a **Supervisión** > **Estadísticas** > [**Túnel GRE** **Túnel IPsec**].

Para obtener más información, consulte; temas sobre supervisión de túneles IPsec y túneles GRE.

Compatibilidad con la redirección de tráfico de firewall mediante Forcepoint en Citrix SD-WAN

August 26, 2022

Forcepoint admite las siguientes funciones, aunque SD-WAN solo admite la función de redirección del firewall:

- IPsec con PKI
- IPsec con PSK
- encadenamiento de proxy mediante la configuración de archivos PAC
- Encadenamiento de proxy con encabezados estándar
- Encadenamiento de proxy con encabezados propietarios que eliminan la necesidad de configurar el rango de IP del cliente: asociación/desarrollo
- Redirección de firewall (proxy transparente por NAT de destino)

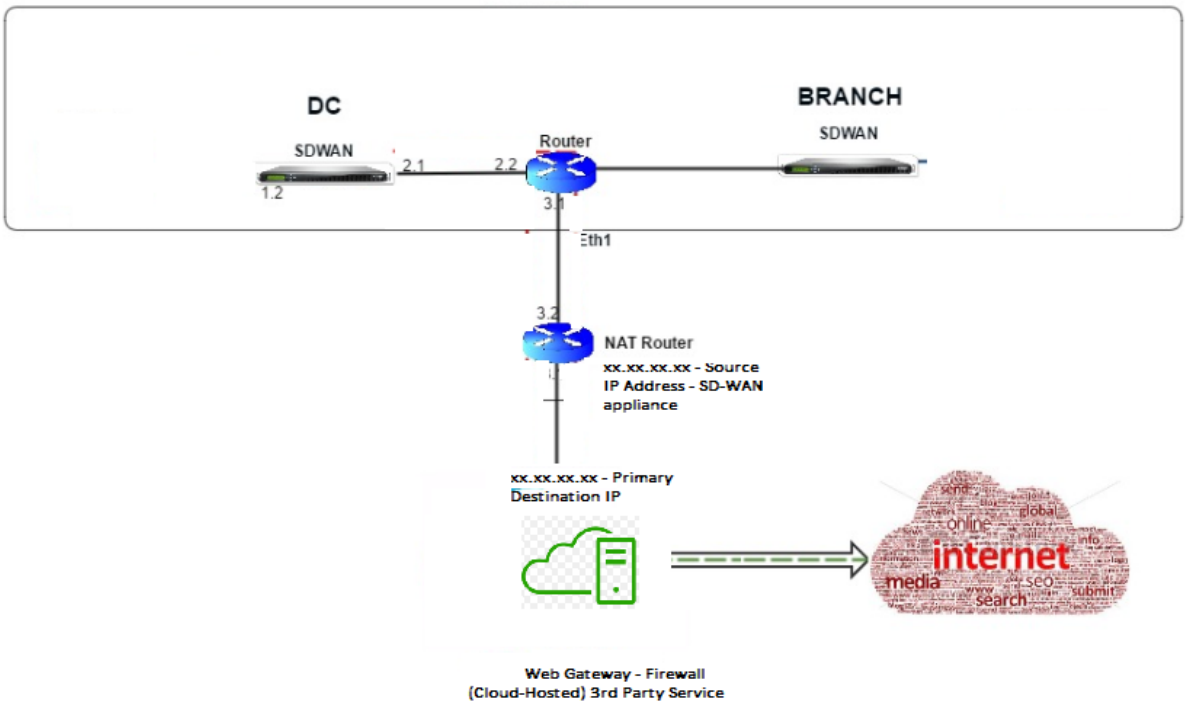
La directiva NAT de destino permite a las empresas redirigir el tráfico de Internet a través del servicio de seguridad alojado en la nube mediante ForcePoint.

Revise el siguiente caso de uso para comprender cómo configurar NAT de destino en dispositivos SD-WAN y redirigir el tráfico de Internet a través de un servicio de firewall seguro basado en la nube.

Requisitos previos:

1. Inicie sesión en el sitio del portal de Forcepoint. Cree una directiva proporcionando la dirección IP pública de empresa a través de la cual el tráfico de Internet debe ser redirigido a Forcepoint. Obtenga las direcciones IP principal y secundaria a las que debe redirigirse el tráfico de Internet.
2. En la GUI de SD-WAN, en un dispositivo SD-WAN del sitio de DC, configure el servicio de Internet asociado a los vínculos WAN.
3. La NAT de destino se realiza mediante la dirección IP de destino del tráfico de Internet. Esta dirección de destino se cambia a la dirección IP pública de Forcepoint.
4. Configure la directiva NAT de destino proporcionando la dirección IP de origen y la dirección IP principal. La IP de origen es la dirección IP de Internet del dispositivo SD-WAN dentro de los puertos 80 (http) y 443 (https) que se redirecciona/traduce a la dirección IP de destino principal de la puerta de enlace de firewall basada en la nube con los puertos externos 8081 (http) y 8443 (https) respectivamente.
5. Después de configurar la directiva DNAT, asegúrese de que las rutas configuradas en el DC tienen el tipo de servicio de Internet seleccionado para la dirección IP de red SD-WAN.

Puede configurar NAT mediante Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Traducción de direcciones de red.

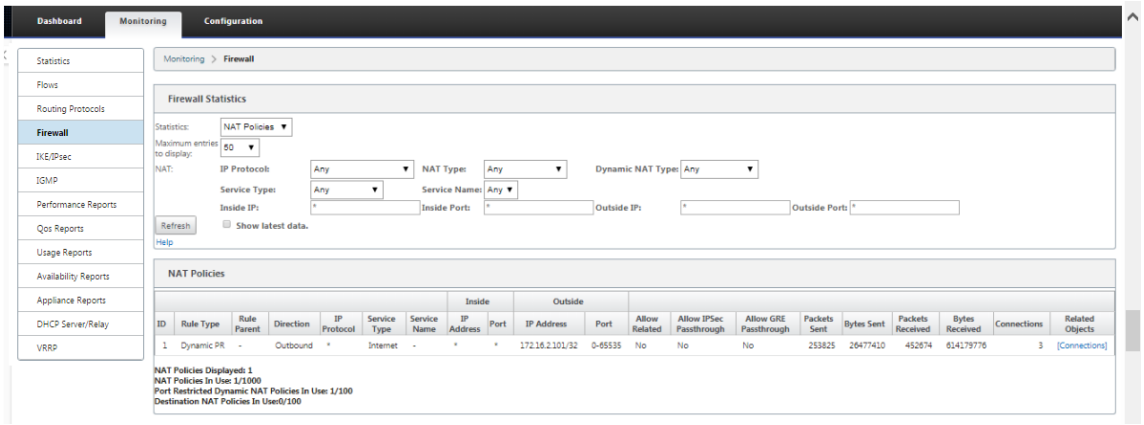


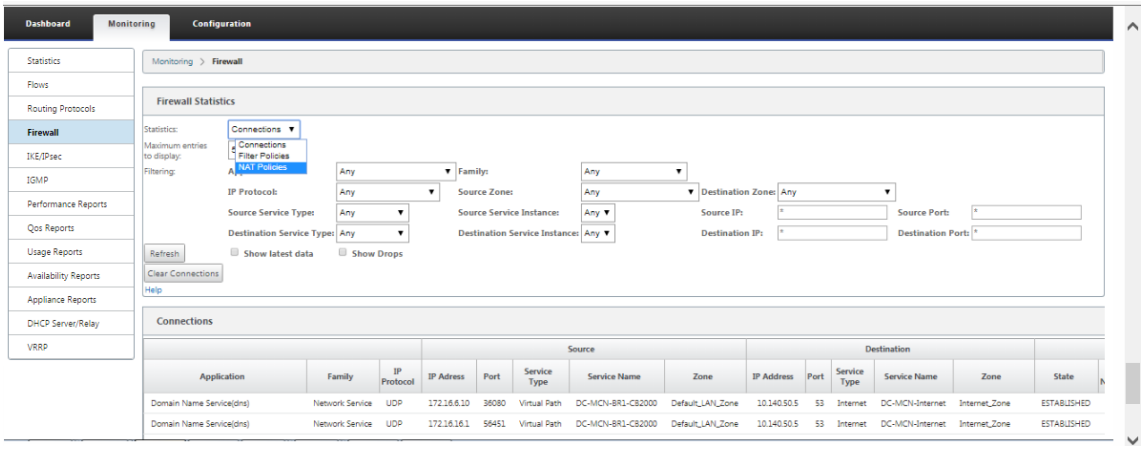
Supervisión de una directiva NAT de destino (firewall)

También puede utilizar la GUI de Citrix SD-WAN para supervisar la configuración actual de la directiva DNAT.

Para supervisar la configuración actual de la directiva NAT de destino:

1. En la GUI de Citrix SD-WAN, vaya a **Supervisión** > **Firewall** > **Directivas NAT**.
2. Seleccione la ficha que incluye las estadísticas que quiere supervisar.





Integración de Palo Alto mediante túneles IPsec

August 26, 2022

Las redes Palo Alto ofrecen una infraestructura de seguridad basada en la nube para proteger redes remotas. Proporciona seguridad al permitir a las organizaciones configurar firewalls regionales basados en la nube que protegen la estructura SD-WAN.

El servicio Prisma Access para redes remotas le permite conectar ubicaciones de red remotas y ofrecer seguridad a los usuarios. Elimina la complejidad de configurar y administrar dispositivos en cada ubicación remota. El servicio proporciona una forma eficiente de agregar fácilmente nuevas ubicaciones de red remotas y minimizar los desafíos operativos al garantizar que los usuarios de estas ubicaciones estén siempre conectados y seguros, y le permite administrar las directivas de forma centralizada desde Panorama para lograr una seguridad uniforme y optimizada para su sistema remoto ubicaciones de red.

Para conectar sus ubicaciones de red remotas al servicio Prisma Access, puede utilizar el firewall de próxima generación de Palo Alto Networks o un dispositivo de terceros compatible con IPsec, incluida SD-WAN, que puede establecer un túnel IPsec para el servicio.

- Planificar el servicio Prisma Access para redes remotas
- Configuración del servicio Prisma Access para redes remotas
- Redes remotas incorporadas con importación de configuración

La solución Citrix SD-WAN ya ofrecía la capacidad de eliminar el tráfico de Internet de la rama. Esto es fundamental para ofrecer una experiencia de usuario más fiable y de baja latencia, al tiempo que se evita la introducción de un paquete de seguridad costoso en cada rama. Citrix SD-WAN y Palo Alto

Networks ahora ofrecen a las empresas distribuidas una forma más fiable y segura de conectar a los usuarios de ramas con aplicaciones en la nube.

Los dispositivos Citrix SD-WAN pueden conectarse a la red del servicio en la nube de Palo Alto (Prisma Access Service) a través de túneles IPsec desde ubicaciones de dispositivos SD-WAN con una configuración mínima.

Soporte de firewall con estado y NAT

August 26, 2022

Esta función proporciona un firewall integrado en la aplicación SD-WAN. El firewall permite directivas entre servicios y zonas, y es compatible con NAT estático, NAT dinámico (PAT) y NAT dinámico con reenvío de puertos. Entre más funciones de firewall se incluyen:

- Proporcionar seguridad para el tráfico de usuarios dentro de la red SD-WAN (empresas y proveedores de servicios)
- Reducción (potencial) de equipos externos (empresas y proveedores de servicios)
- Uso del mismo espacio de direcciones IP para varios clientes: capacidad NAT (proveedores de servicios)
- Aplicar varios firewalls desde una perspectiva global (proveedores de servicios)
- Filtrado de flujos de tráfico entre zonas
- Filtrar el tráfico entre servicios dentro de una zona
- Filtrar el tráfico entre servicios que residen en distintas zonas
- Filtrar el tráfico entre servicios de un sitio
- Definición de directivas de filtro para permitir, denegar o rechazar flujos
- Seguimiento del estado del flujo para los flujos seleccionados
- Aplicación de plantillas de directivas globales
- Compatibilidad con la traducción de direcciones de puerto para el tráfico a Internet en un puerto que no es de confianza, así como el reenvío de puertos entrante y saliente
- Proporcionar traducción de direcciones de red estáticas (NAT estática)
- Proporcionar traducción dinámica de direcciones de red (NAT dinámica)
- Traducción de direcciones de puertos (PAT)
- Reenvío de puertos

> **Nota**
>
> No se recomienda utilizar el firewall en modo en línea por error de conexión por error por motivos de seguridad.

Configuración global del firewall

August 26, 2022

Una vez que haya creado las plantillas de directivas de firewall, puede usar esta directiva para configurar las opciones del firewall para la red Citrix SD-WAN. Con la configuración del firewall global, puede configurar los parámetros del firewall global, estos parámetros se aplican a todos los sitios de la red WAN virtual.

Configuración avanzada de firewalls

November 16, 2022

Puede configurar los ajustes avanzados del firewall para cada sitio de forma individual. Esto invalidará la configuración global.

Para configurar la configuración avanzada del firewall a nivel de sitio, consulte Configuración del firewall.

Zonas

August 26, 2022

Puede configurar zonas en la red y definir directivas para controlar cómo entra y sale el tráfico de las zonas. De forma predeterminada, se crean las siguientes zonas:

- Internet_Zone
  - Se aplica al tráfico hacia o desde un servicio de Internet mediante una interfaz de confianza.
- Untrusted_Internet_Zone
  - Se aplica al tráfico hacia o desde un servicio de Internet mediante una interfaz que no es de confianza.
- default_lan_zone
  - Se aplica al tráfico hacia o desde un objeto con una zona configurable, en el que no se ha establecido la zona.

Puede crear tus propias zonas y asignarlas a los siguientes tipos de objetos:

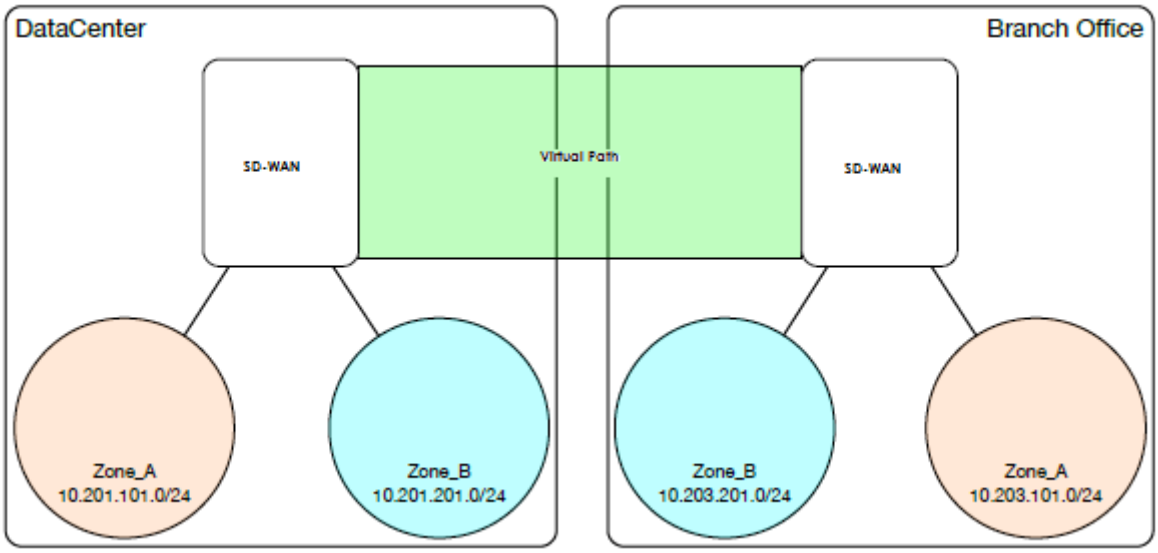
- Interfaces de red virtual (VNI)
- Servicios de intranet
- Túneles GRE
- Túneles LAN IPsec

La zona de destino de un paquete se determina en función de la coincidencia de la ruta de destino. Cuando un dispositivo SD-WAN busca la subred de destino en la tabla de rutas, el paquete coincidirá con una ruta que tiene asignada una zona.

- Zona de origen
  - Ruta no virtual: se determinó a través del paquete de interfaz de red virtual que se recibió el.
  - Ruta virtual: se determina a través del campo de zona de origen en el encabezado del flujo de paquetes.
  - Interfaz de red virtual: el paquete se recibió en el sitio de origen.
- Zona de destino
  - Se determina mediante la búsqueda de rutas de destino del paquete.

Las rutas compartidas con sitios remotos en la SD-WAN mantienen información sobre la zona de destino, incluidas las rutas aprendidas a través del protocolo de redirección dinámica (BGP, OSPF). Con este mecanismo, las zonas adquieren importancia global en la red SD-WAN y permiten el filtrado de extremo a extremo dentro de la red. El uso de zonas proporciona al administrador de red una forma eficaz de segmentar el tráfico de red según el cliente, la unidad de negocio o el departamento.

La capacidad del firewall SD-WAN permite al usuario filtrar el tráfico entre servicios dentro de una única zona o crear directivas que se pueden aplicar entre servicios de distintas zonas, como se muestra en la ilustración siguiente. En el ejemplo siguiente, tenemos Zone_A y Zone_B, cada una de las cuales tiene una interfaz de red virtual LAN.



Directivas

August 26, 2022

Las directivas ofrecen la capacidad de permitir, denegar, rechazar o contar y continuar con flujos de tráfico específicos. Puede configurar las directivas del firewall a través de Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Directivas de firewall.

Traducción de direcciones de red (NAT)

August 26, 2022

La traducción de direcciones de red (NAT) realiza la conservación de direcciones IP para preservar el número limitado de direcciones IPv4 registradas. Permite que las redes IP privadas que utilizan direcciones IP no registradas se conecten a Internet. La función NAT de Citrix SD-WAN conecta su red privada SD-WAN con Internet público. Traduce las direcciones privadas de la red interna en una dirección pública legal. NAT también garantiza una seguridad adicional mediante la publicidad de una sola dirección para toda la red a Internet, ocultando toda la red interna. Citrix SD-WAN admite los siguientes tipos de NAT:

- NAT estático uno a uno
- NAT dinámico (traducción de dirección de puerto PAT)

- NAT dinámico con reglas de reenvío de puertos

> **Nota**
>
> La capacidad de NAT solo se puede configurar a través de Citrix SD-WAN Orchestrator Service en el nivel del sitio. No hay configuración global (plantillas) para NAT. Todas las directivas de NAT se definen a partir de una traducción de origen NAT ("SNAT)". Las reglas de destinación-NAT ("DNAT") correspondientes se crean automáticamente para el usuario. Para obtener más información, consulte Traducción de direcciones de red.

NAT estático

August 26, 2022

NAT estático es una asignación uno a uno de una dirección IP privada o subred dentro de la red SD-WAN a una dirección IP pública o subred fuera de la red SD-WAN. Configure NAT estático introduciendo manualmente la dirección IP interna y la dirección IP externa a la que debe traducir. Puede configurar NAT estático para los servicios de dominio local, rutas virtuales, Internet, Intranet y interredirección.

NAT entrante y saliente

La dirección de una conexión puede ser de interior a exterior o de exterior a interior. Cuando se crea una regla NAT, se aplica a ambas direcciones según el tipo de coincidencia de dirección.

- Entrante: la dirección de origen se traduce para los paquetes recibidos en el servicio. La dirección de destino se traduce para los paquetes transmitidos en el servicio. Por ejemplo, servicio de Internet a servicio LAN: para los paquetes recibidos (de Internet a LAN), la dirección IP de origen se traduce. Para los paquetes transmitidos (LAN a Internet), la dirección IP de destino se traduce.
- Saliente: La dirección de destino se traduce para los paquetes recibidos en el servicio. La dirección de origen se traduce para los paquetes transmitidos en el servicio. Por ejemplo, servicio LAN a servicio de Internet —para paquetes transmitidos (LAN a Internet) la dirección IP de origen se traduce. Para los paquetes recibidos (de Internet a LAN) se traduce la dirección IP de destino.

Derivación de Zona

Las zonas de firewall de origen y destino para el tráfico entrante o saliente no deben ser las mismas. Si las zonas de firewall de origen y destino son las mismas, NAT no se realiza en el tráfico.

Para NAT saliente, la zona exterior se deriva automáticamente del servicio. Todos los servicios de SD-WAN están asociados a una zona de forma predeterminada. Por ejemplo, el servicio de Internet en un vínculo de Internet de confianza está asociado a la zona de Internet de confianza. Del mismo modo, para un NAT entrante, la zona interior se deriva del servicio.

Para un servicio de ruta virtual, la derivación de zona NAT no ocurre automáticamente, debe introducir manualmente la zona interior y externa. NAT se realiza únicamente en el tráfico que pertenece a estas zonas. No se pueden derivar zonas para rutas virtuales porque puede haber varias zonas dentro de las subredes de rutas virtuales.

Directivas NAT estáticas para el servicio de Internet IPv6

Citrix SD-WAN admite directivas NAT estáticas para el servicio de Internet IPv6 a partir de la versión 11.4.0. Una directiva NAT estática para el servicio de Internet IPv6 especifica la asignación de un prefijo de red interna a un prefijo de red externa. El número de directivas NAT estáticas necesarias depende del número de redes internas y del número de redes externas (enlaces WAN). Si hay un número **M** de redes internas y un número **N** de enlaces WAN, el número de directivas NAT estáticas necesarias es **M x N**.

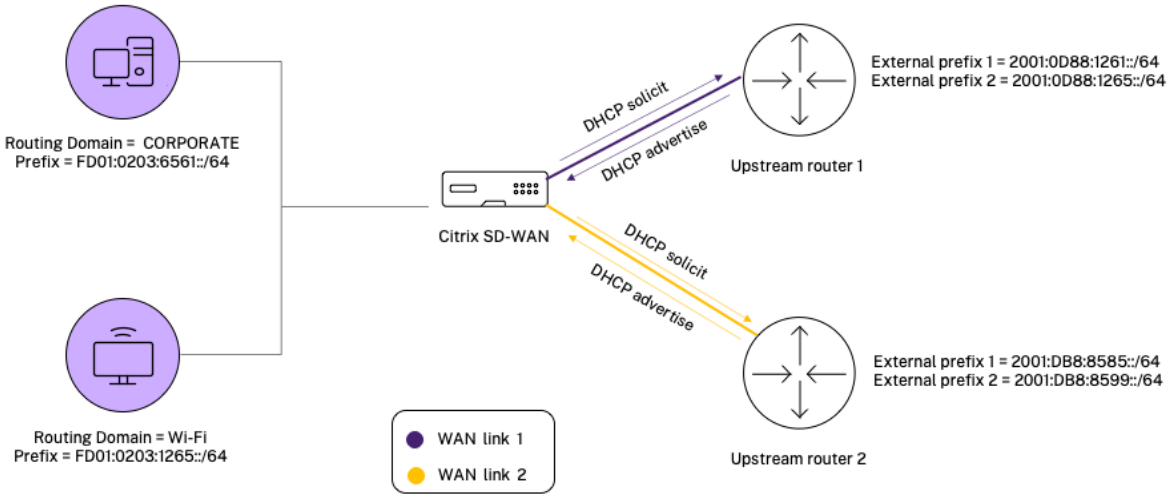
A partir de la versión 11.4.0 de Citrix SD-WAN, al crear una directiva NAT estática, puede introducir manualmente la dirección IP externa o habilitar **Autolearn mediante PD**. Cuando **Autolearn via PD** está habilitado, el dispositivo Citrix SD-WAN recibe prefijos delegados del enrutador de delegación ascendente a través de la delegación de prefijos DHCPv6. Antes de la versión 11.4.0 de Citrix SD-WAN, la dirección IP externa se derivaba del servicio automáticamente y no existía la opción de introducir manualmente la dirección IP externa. Si va a actualizar un dispositivo a la versión 11.4.0 o posterior y tiene directivas NAT estáticas configuradas para el servicio de Internet IPv6, debe actualizar manualmente las directivas.

Ejemplo de configuración

En la siguiente topología, el dispositivo Citrix SD-WAN está configurado con 2 redes internas y 2 enlaces WAN:

- Dentro de la red 1 reside en el dominio de redirección CORPORATE con el prefijo de red FD 01:0203:6561□/64
- La red interna 2 reside en el dominio de redirección Wi-Fi con el prefijo de red FD 01:0203:1265□/64
- A través del enlace WAN 1, el dispositivo SD-WAN recibe del enrutador de delegación ascendente a través de la delegación de prefijos DHCPv6, 2 prefijos delegados 2001:0D88:1261::/64 y 2001:0D88:1265::/64. Estos dos prefijos delegados se utilizan como prefijos de red externa cuando el tráfico de las redes internas transita por el enlace WAN 1.

- A través del enlace WAN 2, el dispositivo SD-WAN recibe del enrutador de delegación ascendente a través de la delegación de prefijos DHCPv6, 2 prefijos delegados 2001:DB8:8585::/64 y 2001:DB8:8599::/64. Estos dos prefijos delegados se utilizan como prefijos de red externa cuando el tráfico de las redes internas transita por el enlace WAN 2.

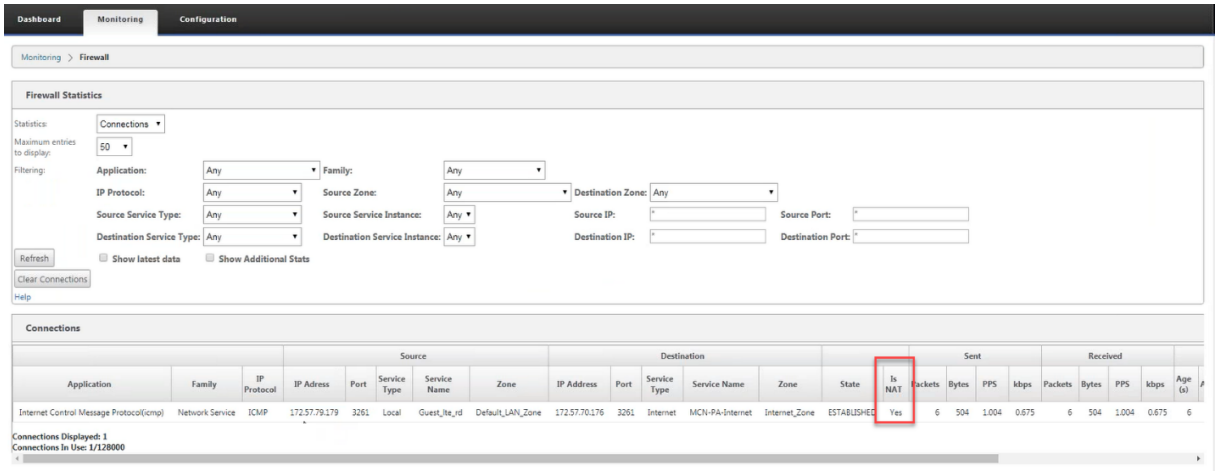


En este caso, hay M=2 dentro de las redes y vínculos WAN N=2. Por lo tanto, el número de directivas NAT estáticas necesarias para la implementación adecuada del servicio de Internet IPv6 es 2 x 2 = 4. Estas cuatro directivas NAT estáticas especifican la traducción de direcciones para:

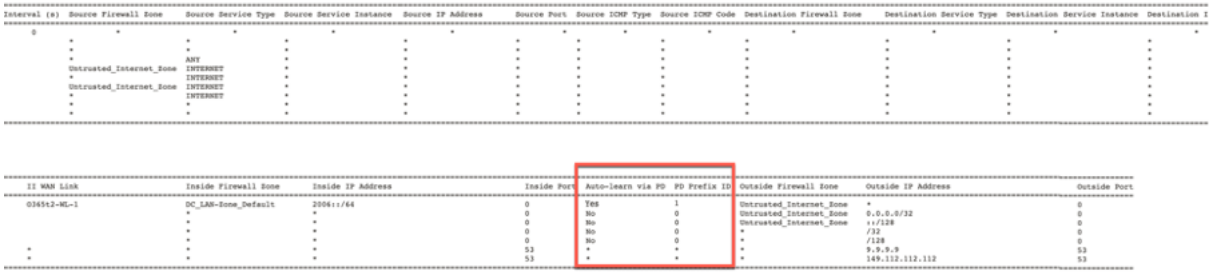
- Red interna 1 a través del enlace WAN 1
- Red interna 1 a través del enlace WAN 2
- Red interna 2 a través del enlace WAN 1
- Red interna 2 a través del enlace WAN 2

Supervisión

Para supervisar NAT, vaya a **Supervisión** > **Estadísticas del firewall** > **Conexiones**. Para una conexión, puede ver si NAT está hecho o no.

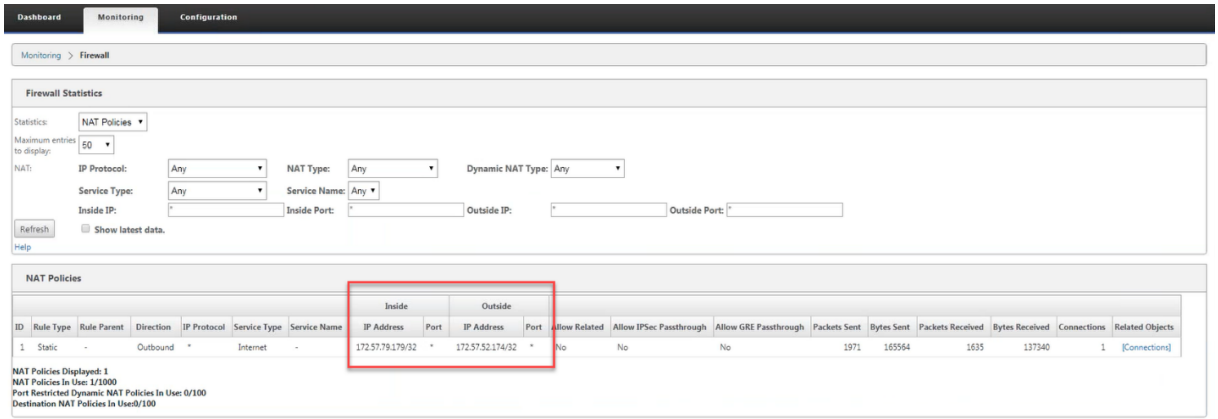


Para comprobar si el aprendizaje automático mediante PD está configurado para alguna regla NAT, vaya a **Configuración > WAN virtual > Ver configuración** y seleccione **Firewall** en la lista desplegable **Ver**. El**aprendizaje automático a través de las columnas ID de prefijo PDy PD** muestran los detalles.



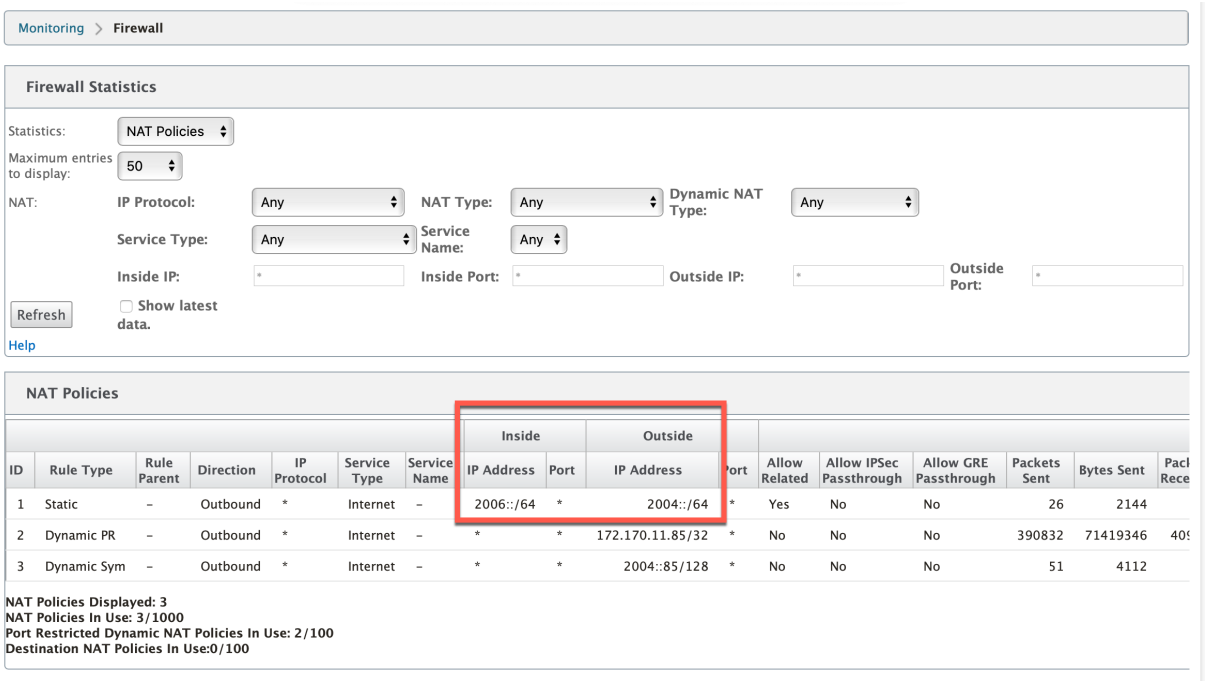
Para ver más a fondo la asignación de direcciones IP internas a direcciones IP externas, haga clic en **NAT posterior a la redirección** en **Objetos relacionados** o vaya a **Supervisión** > **Estadísticas del firewall** > **Directivas NAT**.

En la siguiente captura de pantalla se muestra la asignación de la dirección interna a la dirección externa en una directiva NAT estática IPv4.



En la siguiente captura de pantalla se muestra la asignación de la dirección interna a la dirección

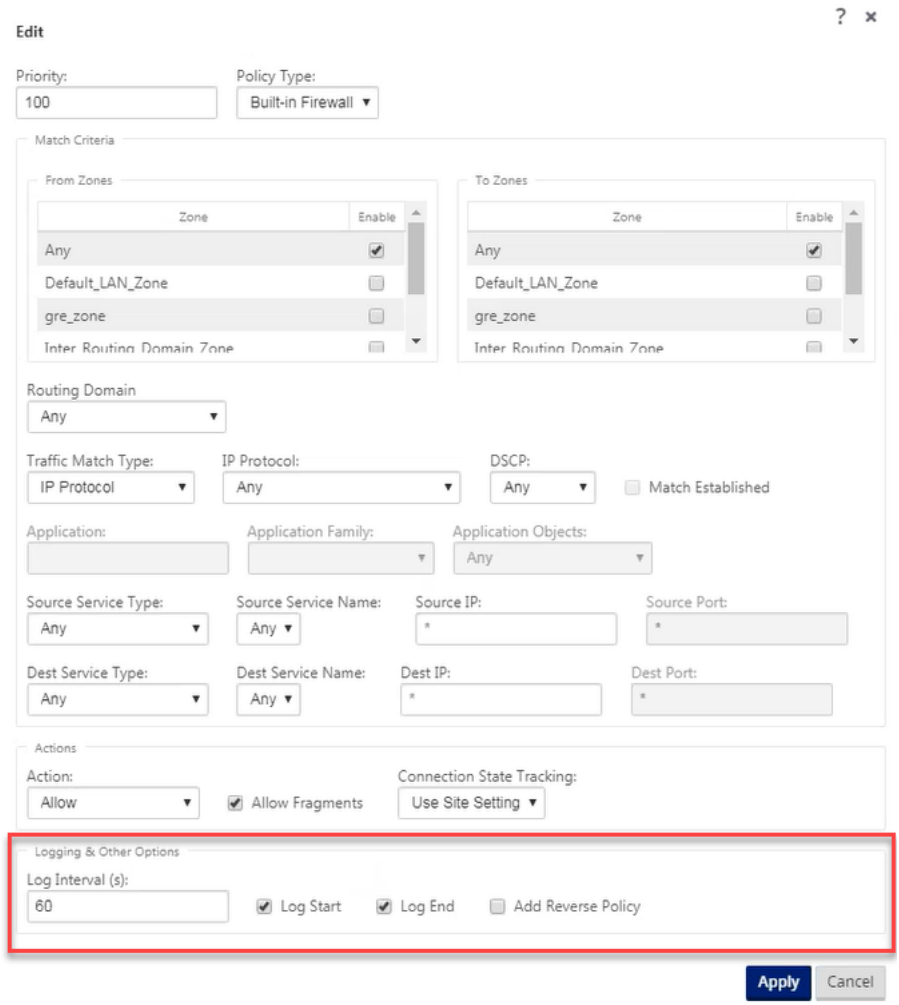
externa en una directiva NAT estática IPv6.



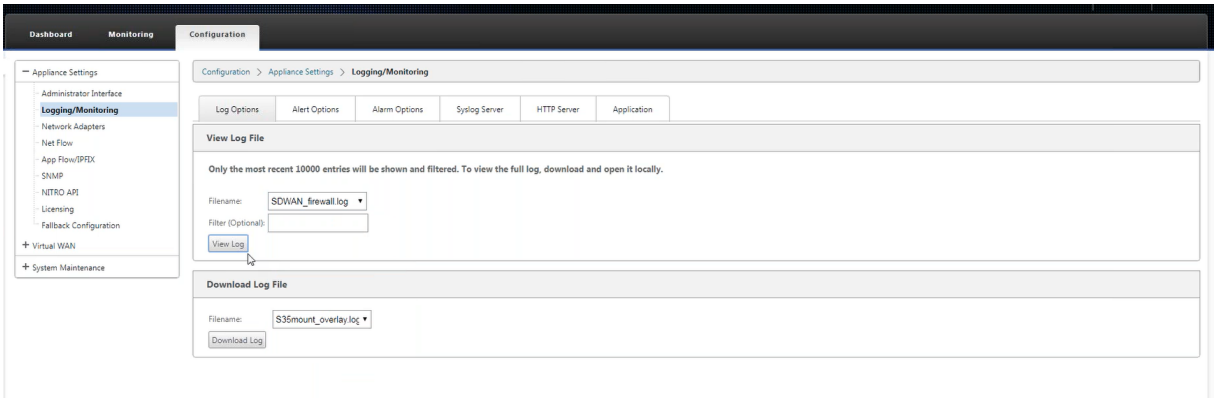
Registros

Puede ver los registros relacionados con NAT en los registros del firewall. Para ver los registros de NAT, cree una directiva de firewall que coincida con la directiva NAT y asegúrese de que el registro está habilitado en el filtro del firewall. Los registros de NAT muestran la siguiente información:

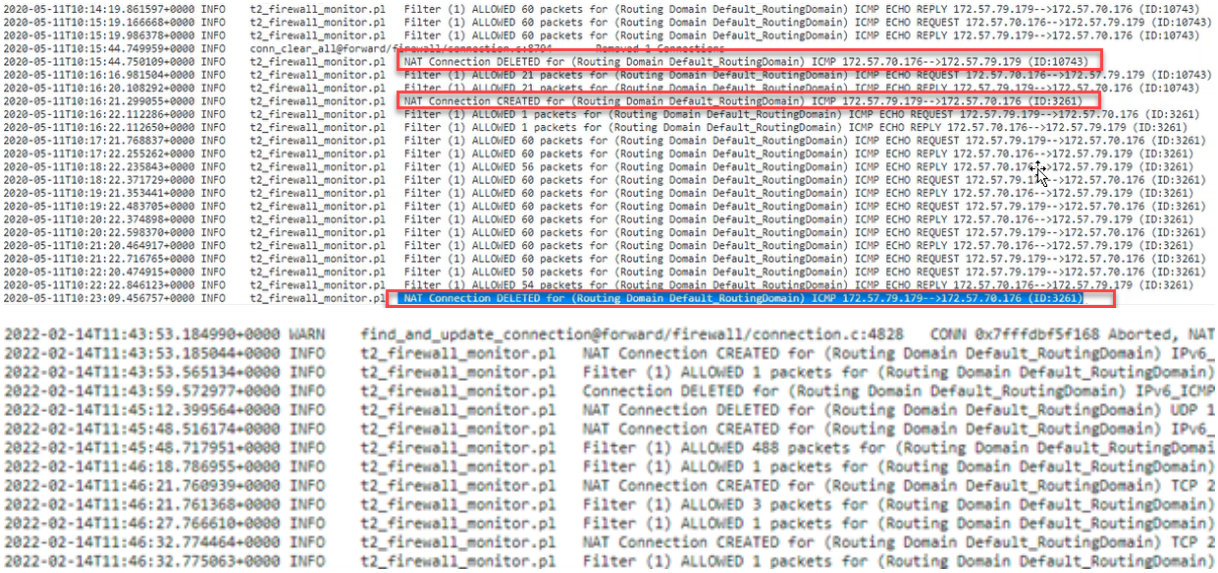
- Fecha y hora
- Dominio de redirección
- Protocolo IP
- Puerto de origen
- Dirección IP de origen
- Dirección IP traducida
- Puerto traducido
- Dirección IP de destino
- Puerto de destino



Para generar registros NAT, vaya a **Registros/Supervisión** > **Opciones de registro**, seleccione **SD-WAN_firewall.log** y haga clic en **Ver registro**.



Los detalles de conexión NAT se muestran en el archivo de registro.



NAT dinámico

November 16, 2022

NAT dinámico es una asignación de varios a uno de una dirección IP privada o subredes dentro de la red SD-WAN a una dirección IP pública o subred fuera de la red SD-WAN. El tráfico de diferentes zonas y subredes a través de direcciones IP de confianza (internas) en el segmento LAN se envía a través de una única dirección IP pública (externa).

Tipos de NAT dinámicos

NAT dinámico realiza la traducción de direcciones de puerto (PAT) junto con la traducción de direcciones IP. Los números de puerto se utilizan para distinguir qué tráfico pertenece a qué dirección IP. Se utiliza una sola dirección IP pública para todas las direcciones IP privadas internas, pero se asigna un número de puerto diferente a cada dirección IP privada. PAT es una forma rentable de permitir que varios hosts se conecten a Internet mediante una única dirección IP pública.

- **Puerto restringido**: Puerto Restringido NAT utiliza el mismo puerto externo para todas las traducciones relacionadas con un par de direcciones IP internas y puertos. Este modo se utiliza normalmente para permitir aplicaciones P2P de Internet.
- **Simétrico**: NAT simétrico utiliza el mismo puerto externo para todas las traducciones relacionadas con una tupla Dirección IP interna, Puerto interior, Dirección IP exterior y Puerto exterior. Este modo se utiliza normalmente para mejorar la seguridad o ampliar el número máximo de sesiones NAT.

NAT entrante y saliente

La dirección de una conexión puede ser de interior a exterior o de exterior a interior. Cuando se crea una regla NAT, se aplica a ambas direcciones según el tipo de coincidencia de dirección.

- **Saliente**: La dirección de destino se traduce para los paquetes recibidos en el servicio. La dirección de origen se traduce para los paquetes transmitidos en el servicio. La NAT dinámica saliente se admite en los servicios de dominio local, de Internet, de Intranet y de redirección interredirección. Para los servicios WAN como los servicios de Internet e Intranet, la dirección IP del vínculo WAN configurada se elige dinámicamente como la dirección IP externa. Para los servicios de dominio local e interredirección, proporcione una dirección IP externa. La zona Exterior se deriva del servicio seleccionado. Un caso de uso típico de NAT dinámico saliente es permitir simultáneamente que varios usuarios de su LAN accedan de forma segura a Internet mediante una única dirección IP pública.
- **Entrante**: la dirección de origen se traduce para los paquetes recibidos en el servicio. La dirección de destino se traduce para los paquetes transmitidos en el servicio. La NAT dinámica entrante no se admite en servicios WAN como Internet e Intranet. Hay un error de auditoría explícito que indica lo mismo. La NAT dinámica entrante solo se admite en los servicios de dominio local e interredirección. Proporcione una zona externa y una dirección IP externa a la que se va a traducir. Un caso de uso típico de NAT dinámico entrante es permitir que los usuarios externos accedan al correo electrónico o a los servidores web alojados en su red privada.

Reenvío de puertos

NAT dinámico con reenvío de puertos le permite enviar tráfico específico a una dirección IP definida. Esto se usa normalmente para hosts internos como servidores web. Una vez configurada la NAT dinámica, puede definir las directivas de reenvío de puertos. Configure NAT dinámico para la traducción de direcciones IP y defina la directiva de reenvío de puertos para asignar un puerto externo a un puerto interno. El reenvío dinámico de puertos NAT se suele utilizar para permitir que los hosts remotos se conecten a un host o servidor de la red privada. Para obtener un caso de uso más detallado, consulte la explicación de Citrix SD-WAN Dynamic NAT.

Directivas NAT dinámicas creadas automáticamente

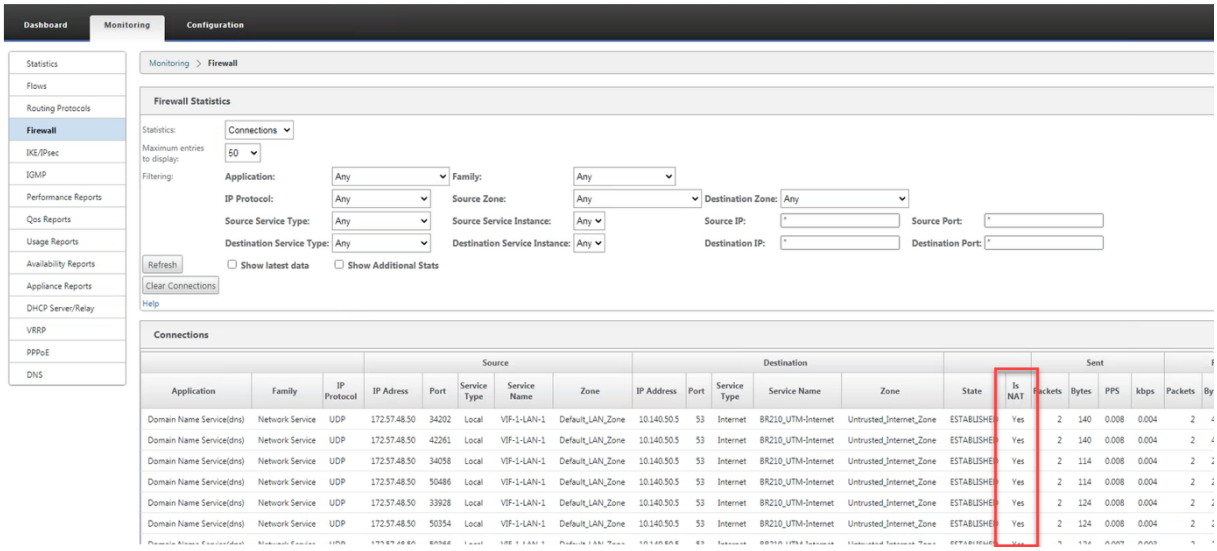
Las directivas NAT dinámicas para el servicio de Internet se crean automáticamente en los siguientes casos:

- Configuración del servicio de Internet en una interfaz que no es de confianza (enlace WAN).
- Habilitar el acceso a Internet para todos los dominios de redirección en un solo enlace WAN mediante Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Configurar la segmentación del firewall.

- Configuración de reenviadores DNS o proxy DNS en SD-WAN Orchestrator Service. Para obtener más información, consulte Sistema de nombres de dominio.

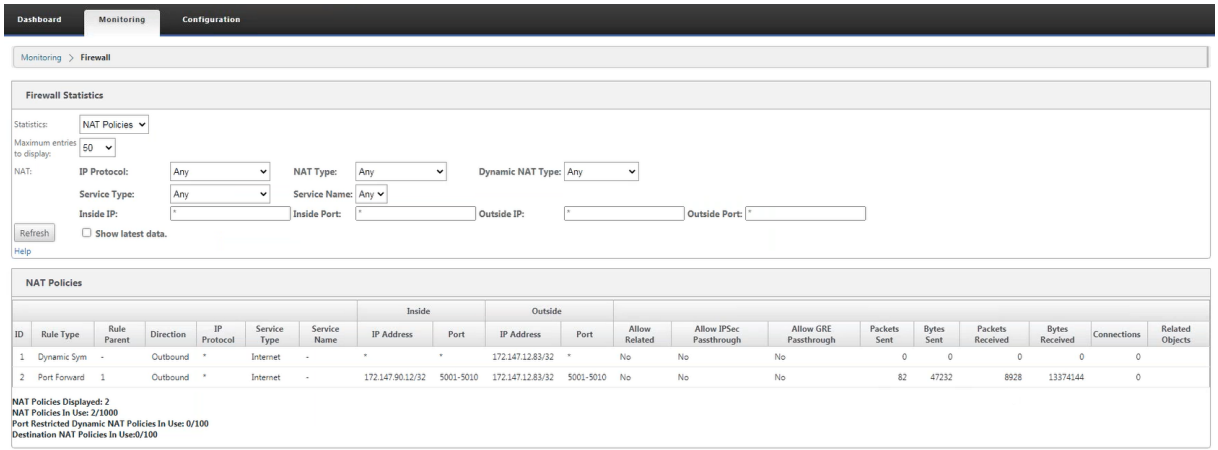
Supervisión

Para supervisar NAT dinámico, vaya a **Supervisión** > **Estadísticas del firewall** > **Conexiones**. Para una conexión, puede ver si NAT está hecho o no.

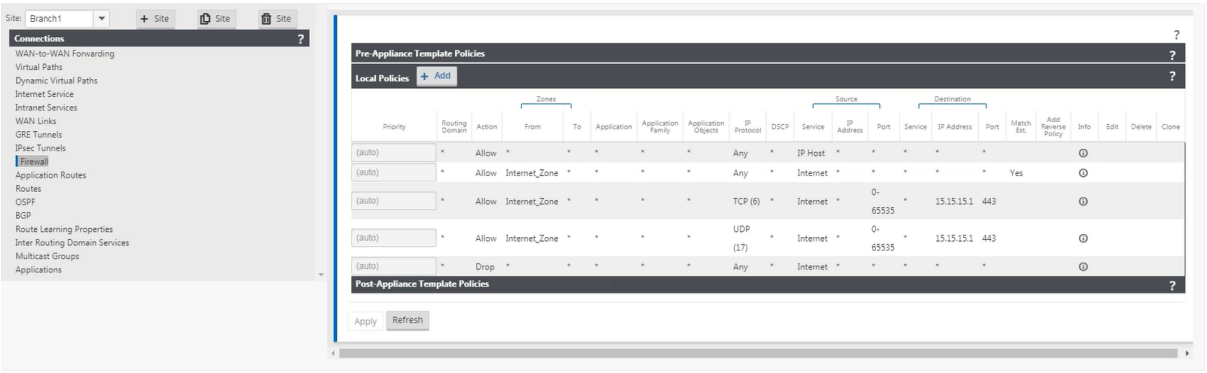


Para ver más a fondo la asignación de direcciones IP internas a direcciones IP externas, haga clic en **NAT previo a la redirección** o **NAT posterior a la redirección** en **Objetos relacionados** o vaya a **Supervisión** > **Estadísticas del firewall** > **Directivas NAT**.

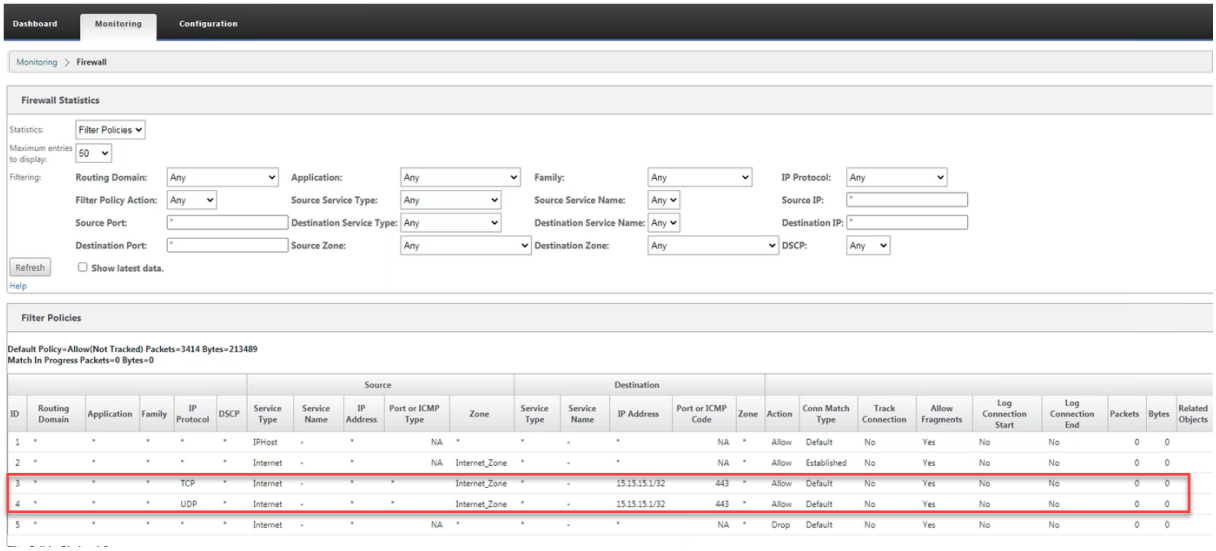
La siguiente captura de pantalla muestra las estadísticas de la regla NAT dinámica de tipo simétrico y su regla de reenvío de puertos correspondiente.



Cuando se crea una regla de reenvío de puertos, también se crea una regla de firewall correspondiente.



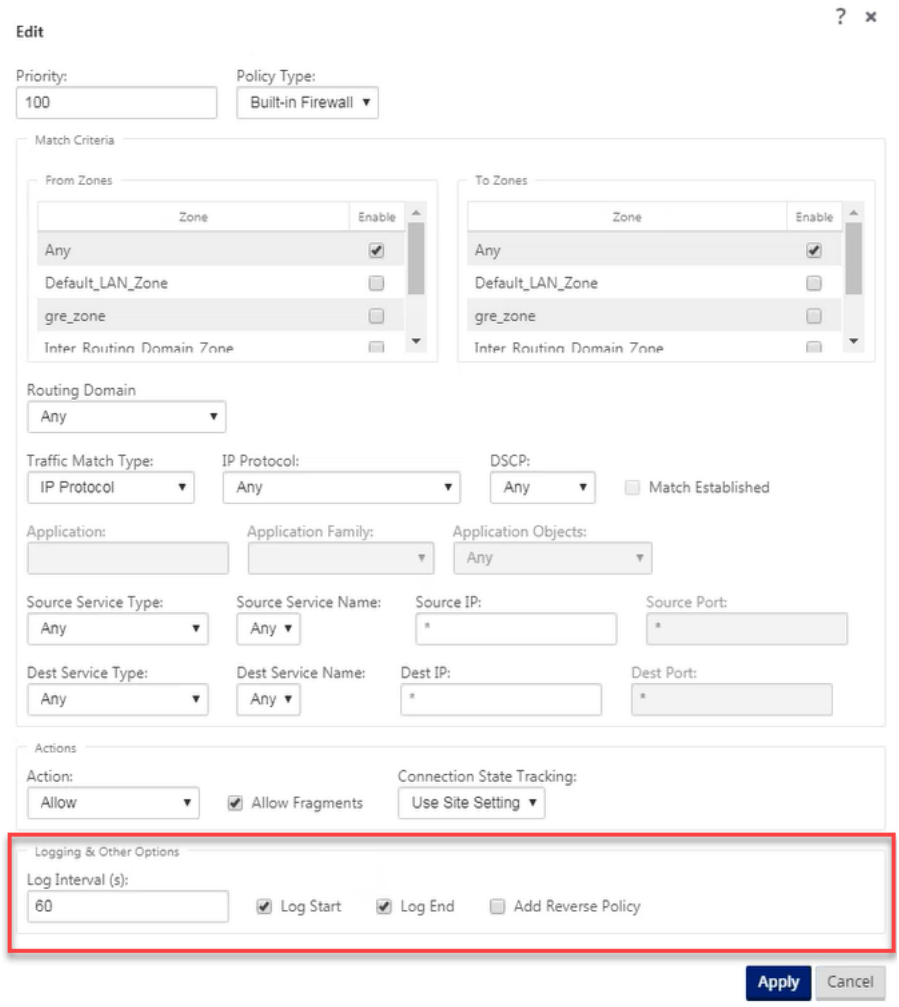
Para ver las estadísticas de directivas de filtro, vaya a **Supervisión** > **Estadísticas del firewall** > **Directivas de filtro**.



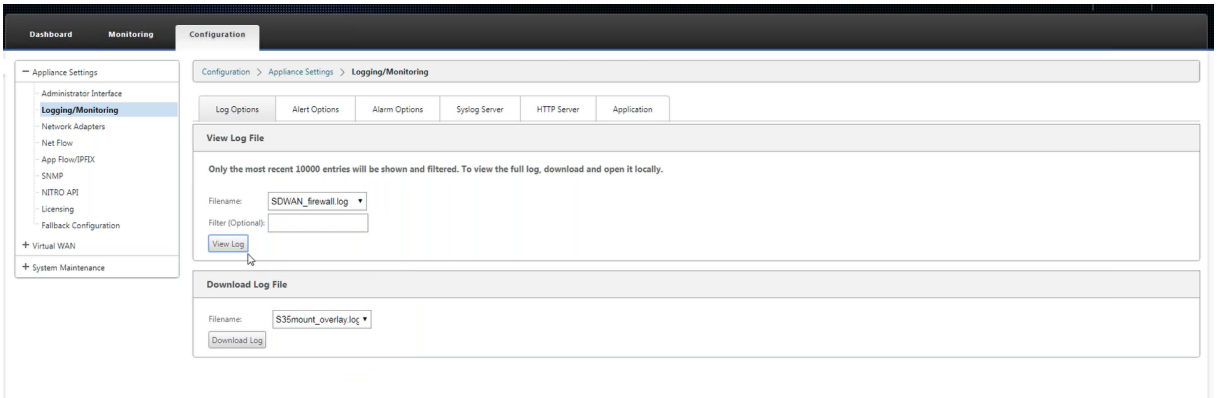
Registros

Puede ver los registros relacionados con NAT en los registros del firewall. Para ver los registros de NAT, cree una directiva de firewall que coincida con la directiva NAT y asegúrese de que el registro está habilitado en el filtro del firewall. Los registros de NAT contienen la siguiente información:

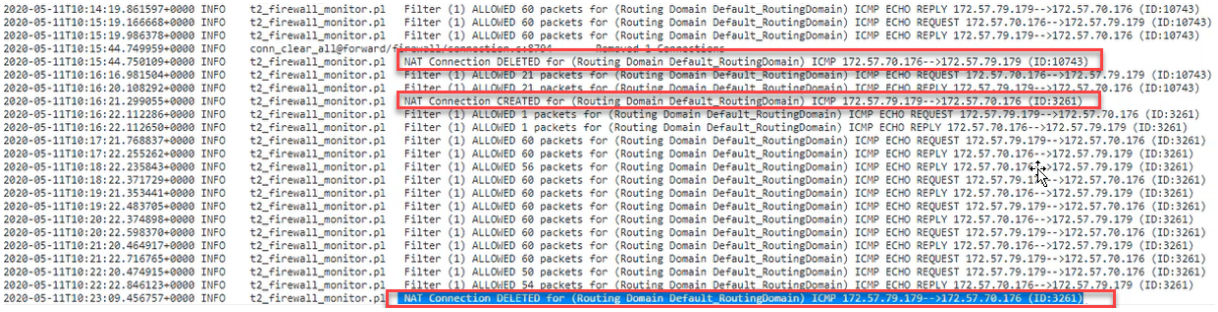
- Fecha y hora
- Dominio de redirección
- Protocolo IP
- Puerto de origen
- Dirección IP de origen
- Dirección IP traducida
- Puerto traducido
- Dirección IP de destino
- Puerto de destino



Para generar registros NAT, vaya a **Registros/Supervisión** > **Opciones de registro**, seleccione **SD-WAN_firewall.log** y haga clic en **Ver registro**.



Los detalles de conexión NAT se muestran en el archivo de registro.



Configurar el servicio WAN virtual

August 26, 2022

La configuración de Citrix SD-WAN describe y define la topología de su red Citrix SD-WAN. Para obtener información sobre cómo configurar el servicio WAN virtual mediante Citrix SD-WAN Orchestrator Service, consulte Flujos.

Seguridad y encriptación

Habilitar el cifrado para SD-WAN (para las rutas virtuales) es opcional. Cuando el cifrado está habilitado, SD-WAN utiliza el Estándar de cifrado avanzado (AES) para proteger el tráfico a través de la ruta virtual. Los dispositivos SD-WAN admiten tanto los cifrados AES de 128 bits como de 256 bits (tamaños de clave) y son opciones configurables.

La autenticación entre sitios funciona con la configuración de WAN virtual. La configuración de red tiene una clave secreta para cada sitio. Para cada ruta virtual, la configuración de red genera una clave combinando las claves secretas de los sitios en cada extremo de la ruta virtual. El intercambio de claves inicial que se produce después de configurar por primera vez una ruta virtual depende de la capacidad de cifrar y descifrar paquetes con esa clave combinada.

Configurar la segmentación del firewall

November 16, 2022

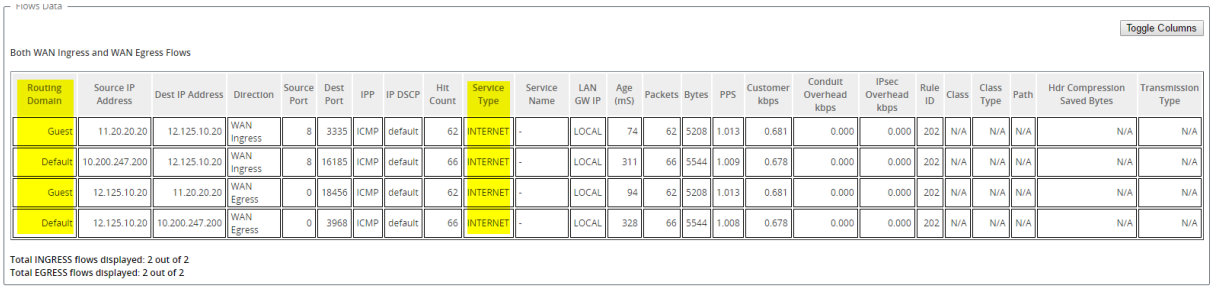
La segmentación del firewall de reenvío de rutas virtuales (VRF) proporciona múltiples dominios de redirección acceso a Internet a través de una interfaz común, con el tráfico de cada dominio aislado del de los demás. Por ejemplo, los empleados y los invitados pueden acceder a Internet a través de la misma interfaz, sin acceso al tráfico de los demás. A partir de la versión 11.5 de SD-WAN, puede

configurar la segmentación del firewall mediante Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Segmentación del firewall.

- Acceso a Internet de usuario invitado local
- Acceso a Internet de usuario empleado para aplicaciones definidas
- Los usuarios empleados pueden continuar con la horquilla de todo el resto del tráfico hacia el MCN
- Permitir al usuario agregar rutas específicas para dominios de redirección específicos.
- Cuando está habilitada, esta función se aplica a todos los dominios de redirección.

También puede crear varias interfaces de acceso para dar cabida a direcciones IP públicas independientes. Cualquiera de las opciones proporciona la seguridad necesaria para cada grupo de usuarios.

Puede confirmar que cada dominio de redirección utiliza el servicio de Internet marcando la columna Dominio de redirección de la tabla Flujos de la interfaz de administración web en **Supervisar** > **Flujos**.


Flows Data

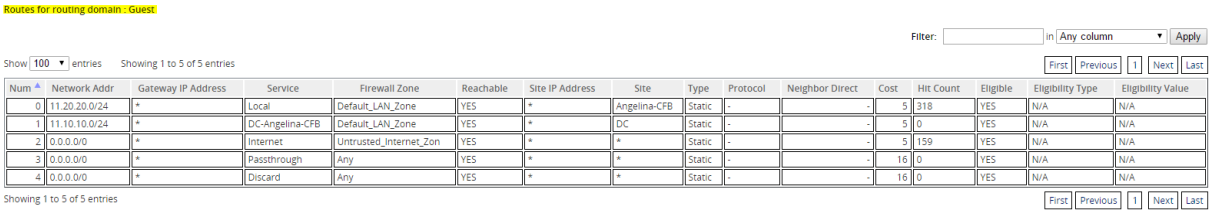
Toggle Columns

Both WAN Ingress and WAN Egress Flows

Routing Domain	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Conduit Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
Guest	11.20.20.20	12.125.10.20	WAN ingress	8	3335	ICMP	default	62	INTERNET	-	LOCAL	74	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	10.200.247.200	12.125.10.20	WAN Ingress	8	16185	ICMP	default	66	INTERNET	-	LOCAL	311	66	5544	1.009	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Guest	12.125.10.20	11.20.20.20	WAN Egress	0	18456	ICMP	default	62	INTERNET	-	LOCAL	94	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	12.125.10.20	10.200.247.200	WAN Egress	0	3968	ICMP	default	66	INTERNET	-	LOCAL	328	66	5544	1.008	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A

Total INGRESS flows displayed: 2 out of 2
Total EGRESS flows displayed: 2 out of 2

También puede consultar la tabla de redirección de cada dominio de redirección en **Supervisar** > **Estadísticas** > **Rutas**.


Routes for routing domain : Guest

Filter: in Any column Apply

Show 100 entries Showing 1 to 5 of 5 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	11.20.20.0/24	*	Local	Default_LAN_Zone	YES	*	Angelina-CFB	Static	-	-	5	318	YES	N/A	N/A
1	11.10.10.0/24	*	DC-Angelina-CFB	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	159	YES	N/A	N/A
3	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
4	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 5 of 5 entries First Previous 1 Next Last

Casos de uso

En versiones anteriores de Citrix SD-WAN, la redirección y el reenvío virtuales presentaban los siguientes problemas, que se han resuelto.

- Los clientes tienen varios dominios de redirección en un sitio de sucursal sin necesidad de incluir todos los dominios en el centro de datos (MCN). Necesitan la capacidad de aislar el tráfico de diferentes clientes de forma segura

- Los clientes deben poder tener una única dirección IP pública con firewall accesible para múltiples dominios de redirección para acceder a Internet en un sitio (que se extienda más allá de VRF lite).
- Los clientes necesitan una ruta de Internet para cada dominio de redirección que admita diferentes servicios.
- Múltiples dominios de redirección en un sitio de sucursal.
- Acceso a Internet para diferentes dominios de redirección.

Múltiples dominios de redirección en un sitio de sucursal

Con las mejoras de segmentación de Virtual Forwarding y Firewall de redirección, puede:

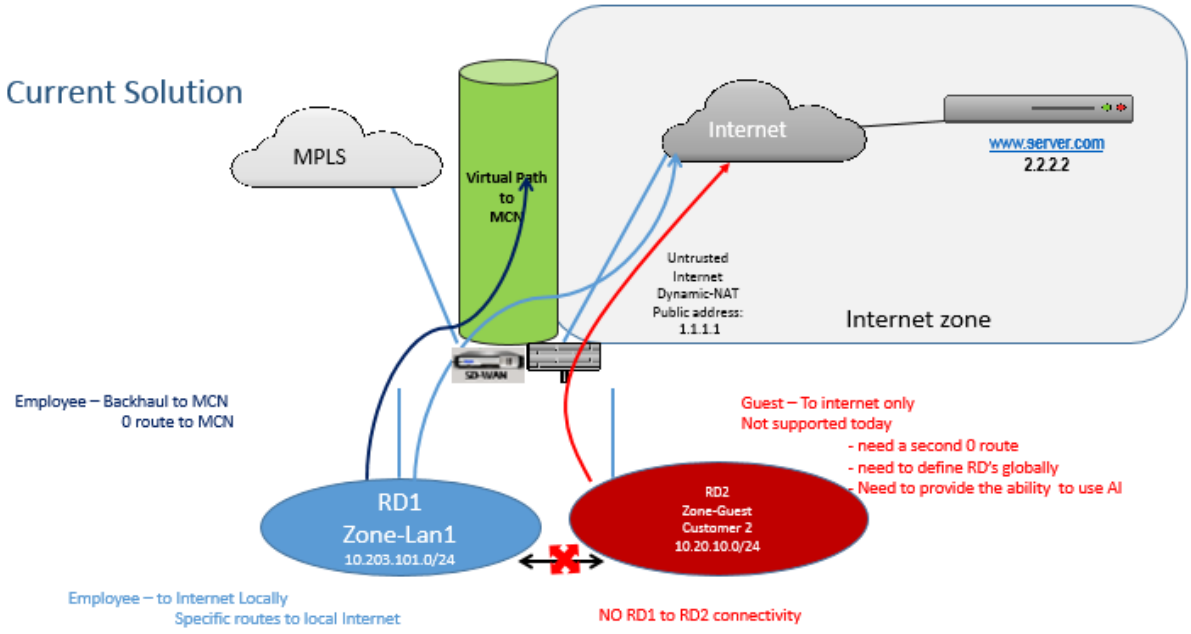
- Proporcionar una infraestructura, en la sucursal, que admita conectividad segura para al menos dos grupos de usuarios, como empleados e invitados. La infraestructura puede admitir hasta 16 dominios de redirección.
- Aísle el tráfico de cada dominio de redirección del tráfico de cualquier otro dominio de redirección.
- Proporcionar acceso a Internet para cada dominio de redirección,
  - Se requiere una interfaz de acceso común y es aceptable
  - Una interfaz de acceso para cada grupo con direcciones IP públicas independientes
- El tráfico del empleado se puede dirigir directamente a Internet local (aplicaciones específicas)
- El tráfico del empleado se puede redirigir o retroceder al MCN para un filtrado exhaustivo (ruta 0)
- El tráfico para el dominio de redirección se puede redirigir directamente a Internet local (ruta 0)
- Admite rutas específicas por dominio de redirección, si es necesario
- Los dominios de redirección están basados en VLAN
- Elimina el requisito de que el RD tenga que residir en el MCN
- El dominio de redirección ahora se puede configurar en un sitio de sucursal
- Permite asignar varios RD a una interfaz de acceso (una vez habilitada)
- A cada RD se le asigna una ruta 0.0.0.0
- Permite agregar rutas específicas para un RD
- Permite que el tráfico de diferentes RD salga a Internet utilizando la misma interfaz de acceso
- Permite configurar una interfaz de acceso diferente para cada RD

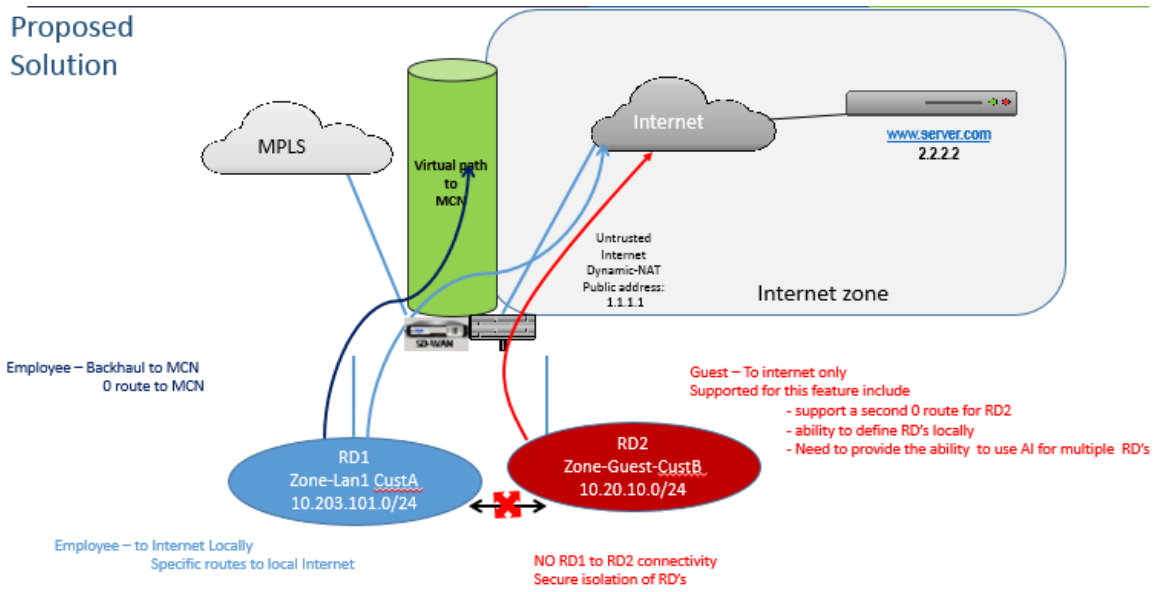
- Deben ser subredes únicas (los RD se asignan a una VLAN)
- Cada RD puede usar la misma zona predeterminada de FW
- El tráfico se aísla a través del dominio de redirección
- Los flujos salientes tienen el RD como componente del encabezado del flujo. Permite a SD-WAN asignar flujos de retorno para corregir el dominio de redirección.

Requisitos previos para configurar varios dominios de redirección:

- El acceso a Internet está configurado y asignado a un enlace WAN.
- Firewall configurado para NAT y directivas correctas aplicadas.
- Segundo dominio de redirección agregado globalmente.
- Cada dominio de redirección agregado a un sitio.
- Asegúrese de que el servicio de Internet se haya definido correctamente.

Casos de implementación





Limitaciones

- El servicio de Internet debe agregarse al enlace WAN para poder habilitar el acceso a Internet para todos los dominios de redirección. (Hasta que lo haga, la casilla de verificación para habilitar esta opción aparece atenuada).

  Después de habilitar el acceso a Internet para todos los dominios de redirección, agregue automáticamente una regla Dynamic-NAT.
- Hasta 16 dominios de redirección por sitio.
- Interfaz de acceso (IA): IA única por subred.
- Varias IA requieren una VLAN independiente para cada IA.
- Si tiene dos dominios de redirección en un sitio y tiene un único enlace WAN, ambos dominios utilizan la misma dirección IP pública.
- Si está habilitado el acceso a Internet para todos los dominios de redirección, todos los sitios pueden redirigirse a Internet. (Si un dominio de redirección no requiere acceso a Internet, puede utilizar el firewall para bloquear su tráfico).
- No se admite la misma subred en varios dominios de redirección.
- No hay funcionalidad de auditoría
- Los vínculos WAN se comparten para el acceso a Internet.
- Sin QoS por dominio de redirección; primero en llegar primero en servir.

Autenticación de certificados

August 26, 2022

Citrix SD-WAN garantiza que se establezcan rutas seguras entre los dispositivos de la red SD-WAN mediante técnicas de seguridad como el cifrado de red y los túneles IPsec de ruta virtual. Además de las medidas de seguridad existentes, la autenticación basada en certificados se introduce en Citrix SD-WAN 11.0.2.

La autenticación de certificados permite a las organizaciones usar certificados emitidos por su autoridad de certificación (CA) privada para autenticar los dispositivos. Los dispositivos se autentican antes de establecer las rutas virtuales. Por ejemplo, si un dispositivo de sucursal intenta conectarse al centro de datos y el certificado de la sucursal no coincide con el certificado que espera el centro de datos, no se establece la ruta virtual.

El certificado emitido por la entidad emisora de certificados vincula una clave pública al nombre del dispositivo. La clave pública funciona con la clave privada correspondiente que posee el dispositivo identificado por el certificado.

Puede habilitar la autenticación de certificados de su dispositivo SD-WAN mediante Citrix SD-WAN Orchestrator Service. Para obtener más información sobre la autenticación de certificados, consulte Autenticación de certificados

AppFlow e IPFIX

September 26, 2023

AppFlow e IPFIX son estándares de exportación de flujos utilizados para identificar y recopilar datos de aplicaciones y transacciones en la infraestructura de red. Estos datos ofrecen una mejor visibilidad de la utilización y el rendimiento del tráfico de aplicaciones.

Los datos recopilados, denominados registros de flujo, se transmiten a uno o más recopiladores IPv4 o IPv6. Los recopiladores agregan los registros de flujo y generan informes históricos o en tiempo real.

AppFlow

AppFlow solo exporta datos de nivel de flujo para conexiones HDX e ICA. Puede habilitar el TCP solo para la plantilla de conjunto de datos HDX o la plantilla de conjunto de datos HDX. El conjunto de

datos TCP solo para HDX proporciona datos de varios saltos. El conjunto de datos HDX proporciona datos de información de HDX.

Los recopiladores de AppFlow como Splunk y Citrix ADM tienen paneles para interpretar y presentar estas plantillas.

IPFIX

IPFIX es un protocolo de exportación de recopilador utilizado para exportar datos de nivel de flujo para todas las conexiones. Para cualquier conexión, puede ver información como el recuento de paquetes, el recuento de bytes, el tipo de servicio, la dirección de flujo, el dominio de redirección, el nombre de la aplicación, etc. Los flujos IPFIX se transmiten a través de la interfaz de administración. La mayoría de los recopiladores pueden recibir registros de flujo IPFIX, pero pueden necesitar crear un panel personalizado para interpretar la plantilla IPFIX.

La plantilla IPFIX define el orden en el que se debe interpretar el flujo de datos. El recopilador recibe un registro de plantilla, seguido de los registros de datos. Citrix SD-WAN utiliza las plantillas 611 y 613 para exportar datos de flujo IPv4 IPFIX, 615 y 616 para exportar datos de flujo IPv6 IPFIX junto con la plantilla Options 612.

La información de flujo de aplicaciones (IPFIX) exporta conjuntos de datos según las plantillas 611 para flujos IPv4, 615 para flujos IPv6 y 612 opciones Plantilla con información de la aplicación.

Propiedades básicas (IPFIX) exporta conjuntos de datos según las plantillas 613 para flujos IPv4 y 616 para flujos IPv6.

Las tablas siguientes proporcionan la lista detallada de datos de flujo asociados con cada plantilla IPFIX.

Información de flujo de aplicaciones (IPFIX) - Plantillas V10

ID de plantilla - 611

Elemento Info (IE)	Nombre e ID de IE	Tipo y len	Descripción
ID del punto de observación	ObservaciónPointID, 138	Unsigned32, 4	
ID de proceso de exportación	ExportingProcessID, 144	Unsigned32, 4	
ID de flujo	FlowID, 148	Unsigned64, 8	
IP IPv4 SRC	sourceIPv4Address, 8	Ipv4address, 4	

Elemento Info (IE)	Nombre e ID de IE	Tipo y len	Descripción
IP DST Ipv4	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	IPVersion, 60	Unsigned8, 1	Ajuste a 4.
Número de protocolo IP	protocolodentificador,4	Unsigned8, 1	
Acolchado	N/D	Unsigned16, 2	
Puerto SRC	SourceTransportport, 7	Unsigned16, 2	
Puerto DST	DestinoTransport,11	Unsigned16, 2	
Conteo de Pkt	PacketDeltaCount, 2	Unsigned64, 8	
Recuento de bytes	OctetDeltaCount, 1	Unsigned64, 8	
Tiempo para el primer pkt en microsegundos	flowStartMicroseconds, 154	DateTimeMicroSeconds, 8	
Tiempo de lastpkt en microsegundos	FlowendMicroseconds, 155	DateTimeMicroSeconds, 8	
TOs de IP	IPClassOfService, 5	Unsigned8, 1	
Indicadores de flujo	TcpControlBits, 6	Unsigned8, 2	Actualmente establecido en 0.
Dirección de flujo	FlowDirection, 61	Unsigned8, 1	0x00: flujo de entrada 0x01: flujo de salida FlowWan-WAN y LAN-LAN son una posibilidad en SDWAN
Interfaz de entrada	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN equilibra la carga de los flujos de datos a través de varias rutas de miembros, por lo que un único flujo de datos puede tener múltiples combinaciones de interfaz de entrada/salida.

Elemento Info (IE)	Nombre e ID de IE	Tipo y len	Descripción
Interfaz de salida	EGressInterface, 14	Unsigned32, 4	Citrix SD-WAN equilibra la carga de los flujos de datos a través de varias rutas de miembros, por lo que un único flujo de datos puede tener múltiples combinaciones de interfaz de entrada/salida.
ID de VLAN de entrada	VlanID, 58	Unsigned16, 2	
ID de VLAN de salida	PostVlanID, 59	Unsigned16, 2	
ID DE VRF	ingressVRFID, 234	Unsigned32, 4	
Indicador de clave de flujo	FlowKeyIndicator, 173	Unsigned64, 8	Establezca en 0x1E037F.
ID de aplicación	ApplicationID, 95	OcteArray, variable	El ID de aplicación es el mismo que el ID de las aplicaciones clasificadas por el motor DPI. Los ID de aplicación permanecen constantes. Los Id. de aplicación para aplicaciones basadas en nombres de dominio personalizados cambian con cada actualización de configuración.

ID de plantilla: 615 (flujos IPv6) |Elemento Info (IE)|Nombre e ID de IE|Tipo y len|Comentario|
|-|-|-|-|
|ID del punto de observación|ObservaciónPointID, 138|Unsigned32, 4|

ID de proceso de exportación	ExportingProcessID, 144	Unsigned32, 4
ID de flujo	FlowID, 148	Unsigned64, 8
IPv6 SRC IP	sourceIPv6Address, 27	Ipv6address, 16
IPv6 DST IP	destinationIpv6Addres, 28	Ipv6address, 16
Ipversion	ipVersion, 60	Unsigned8, 1	Set to 6	
IP protocol number	protocoldentifier, 4	Unsigned8, 1	
Padding	N/A	Unsigned16, 2	
SRC Port	sourceTransportPort, 7	Unsigned16, 2	
DST Port	destinationTransportPort, 11	Unsigned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Time for first pkt in microseconds	flowStartMicroseconds, 154	dateTimeMicroseconds, 8	
Time for lastpkt in microseconds	flowEndMicroseconds, 155	dateTimeMicroseconds, 8	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Flags	tcpControlBits, 6	Unsigned8, 2	Currently set to 0.
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Output Interface	egressInterface, 14	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Input Vlan ID	vlanId, 58	Unsigned16, 2	
Output Vlan ID	postVlanId, 59	Unsigned16, 2	
VRF ID	ingressVRFID, 234	Unsigned32, 4	
Flow Key Indicator	flowKeyIndicator, 173	Unsigned64, 8	Set to 0x1E037F.
Application ID	applicationId, 95	octetArray, variable	The Application ID is same as the ID of the applications classified by the DPI engine. Los ID de aplicación permanecen constantes. Los ID de aplicación para las aplicaciones basadas en nombres de dominio personalizados cambian con cada actualización de configuración.

Plantilla 612 (Plantilla de opciones)

Elemento Info (IE)	Nombre e ID de IE	Tipo	Comentario
ID de aplicación	ApplicationID, 95	OctetArray	El ID de aplicación es el mismo que el ID de las aplicaciones clasificadas por el motor DPI. Los ID de aplicación permanecen constantes. Los Id. de aplicación para aplicaciones basadas en nombres de dominio personalizados cambian con cada actualización de configuración.
Nombre de la aplicación	ApplicationName, 96	string	Especifica el nombre de la aplicación propietaria específica de Citrix SDWAN.
Descripción de la aplicación	AplicaciónDescripción, 94	string	Especifica la descripción de la aplicación.

Propiedades básicas (IPFIX): plantilla compatible con V9 - Plantilla 613 (flujos IPv4)

Elemento Info (IE)	Nombre e ID de IE	Tipo y len	Comentario
IP IPv4 SRC	sourceIPv4Address, 8	Ipv4address, 4	
IP DST Ipv4	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	IPVersion, 60	Unsigned8, 1	
Número de protocolo IP	protocolodentificador, 4	Unsigned8, 1	
TOs de IP	IPClassOfService, 5	Unsigned8, 1	

Elemento Info (IE)	Nombre e ID de IE	Tipo y len	Comentario
Dirección de flujo	FlowDirection, 61	Unsigned8, 1	0x00: flujo de entrada 0x01: flujo de salida FlowWan-WAN y LAN-LAN son una posibilidad en SDWAN
Puerto SRC	SourceTransportport, 7	Unsigned16, 2	
Puerto DST	DestinationTransportPort, 11	Unsigned16, 2	
Conteo de Pkt	PacketDeltaCount, 2	Unsigned64, 8	
Recuento de bytes	OctetDeltaCount, 1	Unsigned64, 8	
Interfaz de entrada	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN equilibra la carga de los flujos de datos a través de varias rutas de miembros, por lo que un único flujo de datos puede tener múltiples combinaciones de interfaz de entrada/salida.
Interfaz de salida	EGressInterface, 14	Unsigned32, 4	Citrix SD-WAN equilibra la carga de los flujos de datos a través de varias rutas de miembros, por lo que un único flujo de datos puede tener múltiples combinaciones de interfaz de entrada/salida.
ID de VLAN de entrada	VlanID, 58	Unsigned16, 2	
ID de VLAN de salida	PostVlanID, 59	Unsigned16, 2	

ID de plantilla: 616 (flujos IPv6) |Elemento Info (IE)|Nombre e ID de IE|Tipo y len|Comentario|
|-|-|-|-|
|IPv6 SRC IP|sourceIPv6Address, 27|Ipv6address, 16|
|IPv6 DST IP|destinationIpv6Addres, 28|Ipv6address, 16|
|Ipversion|ipVersion, 60|Unsigned8, 1|Set to 6| |
|IP protocol number|protocoldentifier,4|Unsigned8, 1| |
|IP ToS|ipClassOfService, 5|Unsigned8, 1| |
|Flow Direction|flowDirection, 61|Unsigned8, 1|0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN|
|SRC Port|sourceTransportPort, 7|Unsigned16, 2| |
|DST Port|destinationTransportPort, 11|Unsigned16, 2| |
|Pkt Count|packetDeltaCount, 2|Unsigned64, 8| |
|Byte Count|octetDeltaCount, 1|Unsigned64, 8| |
|Input Interface|ingressInterface, 10|Unsigned32, 4|Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.|
|Output Interface|egressInterface, 14|Unsigned32, 4|Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.|
|Input Vlan ID|vlanId, 58|Unsigned16, 2| |
|Output Vlan ID|postVlanId, 59|Unsigned16, 2| |

Limitaciones

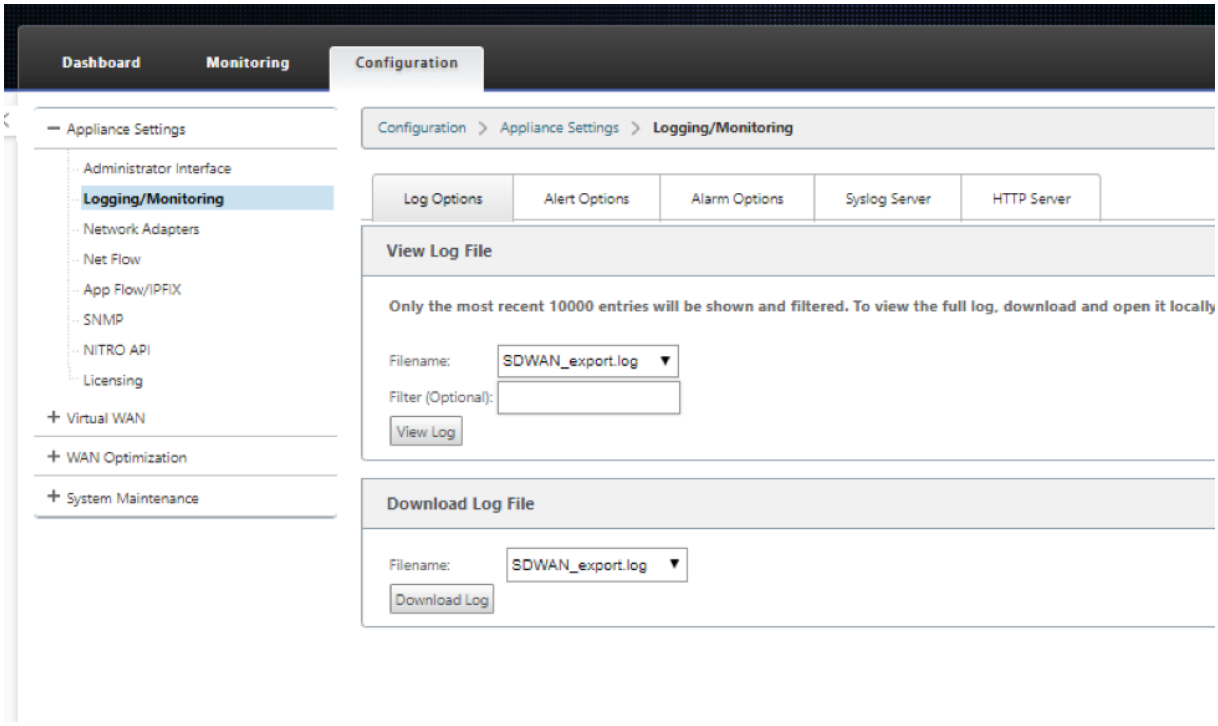
- AppFlow no admite registros de flujo y recopilador IPv6.
- El intervalo de exportación para el flujo neto aumenta de 15 segundos a 60 segundos.
- Los flujos de AppFlow/IPfix se transmiten a través de UDP; en caso de pérdida de conexión, no se retransmiten todos los datos. Si el intervalo de exportación se establece en X minutos, el dispositivo almacena solo X minutos de datos. Que se retransmite después de X minutos de pérdida de conexión.
- En Citrix SD-WAN, versión 10 versión 2, la configuración de **AppFlow** se establece de forma local en todos los dispositivos, mientras que en las versiones anteriores era una configuración global. Si la versión del software SD-WAN se reduce a cualquiera de las versiones anteriores y AppFlow está configurado en cualquiera de los dispositivos, se aplicará globalmente a todas las alianzas.

Configuración de AppFlow/IPfix

Puede configurar AppFlow/IPFIX solo a través de Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte AppFlow e IPFIX.

Archivos de registros

Para solucionar problemas relacionados con los protocolos de exportación de AppFlow/IPFIX, puede ver y descargar los archivos SDWAN_export.log. Vaya a **Configuración > Captura de registros/Supervisión** y seleccione los archivos **SDWAN_Export.log**.



SNMP

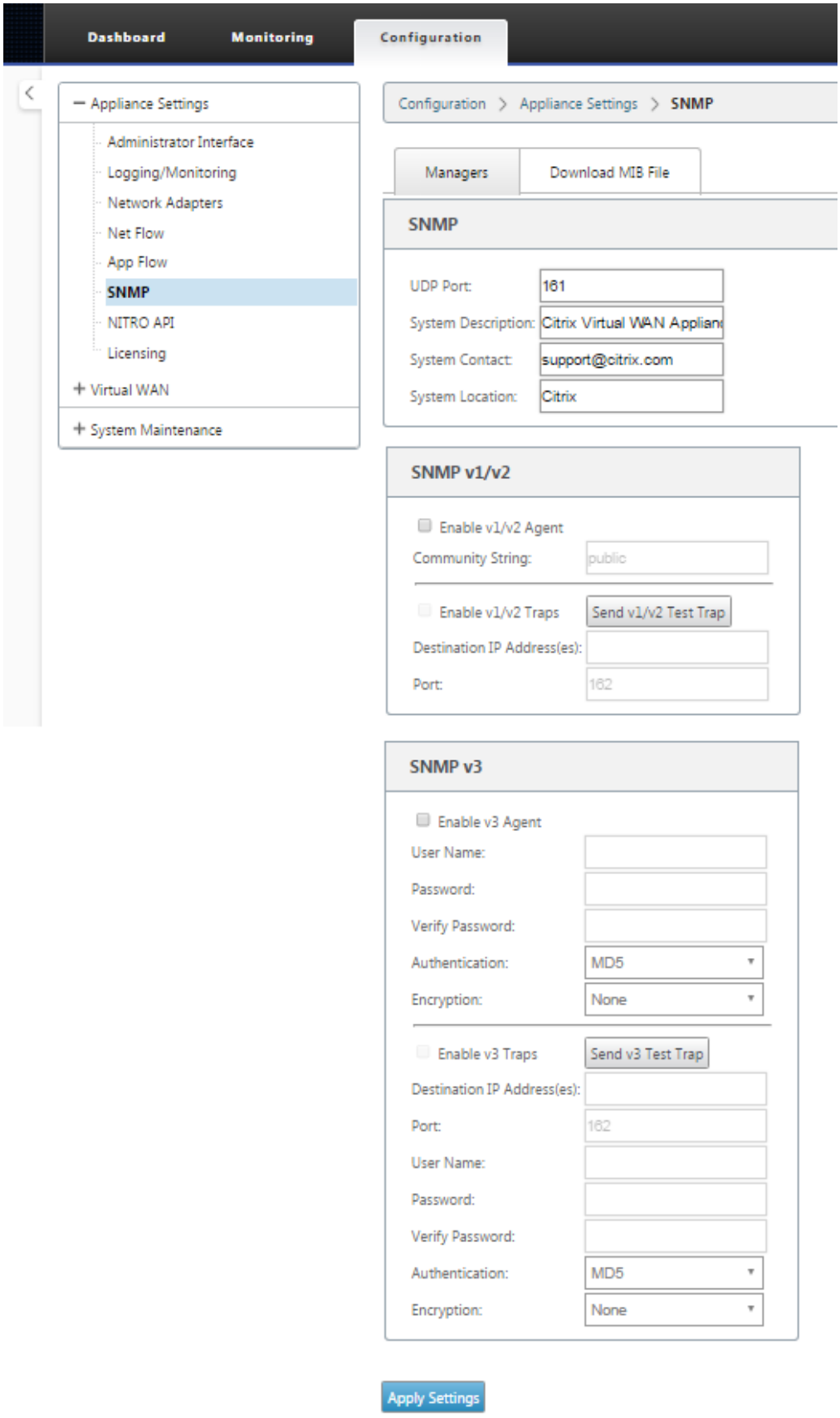
November 16, 2022

Citrix SD-WAN admite la capacidad SNMPV1/V2 y solo una cuenta de usuario para cada capacidad SNMPv3. Esta restricción proporciona las siguientes ventajas:

- Garantizar el cumplimiento de SNMPv3 para los dispositivos de red
- Verificación de la capacidad SNMPv3
- Configuración sencilla de SNMPv3

Para configurar el sondeo y las capturas de SNMPv3, vaya a la sección SNMPv3 de la página **Configuración** -> **Configuración del dispositivo** -> **SNMP** y rellene los campos según sea necesario.

> **NOTA**
>
> Para configurar una dirección IPv6, asegúrese de que el servidor SNMP también está configurado con una dirección IPv6.



Compatibilidad con MIB estándar

Los dispositivos SD-WAN admiten las siguientes MIB estándar.

MIB	RFC (enlace de definición)
DISMAN-EVENTO-MIB	https://www.ietf.org/rfc/rfc2981.txt
IF-MIB	https://www.ietf.org/rfc/rfc2863.txt
IP-FORWARD-MIB	https://www.ietf.org/rfc/rfc4292.txt
IP-MIB (parcial)	https://www.ietf.org/rfc/rfc4293.txt
Q-BRIDGE-MIB (parcial)	http://www.ieee802.org/1/files/public/MIBs/IEEE8021-Q-BRIDGE-MIB-201112120000Z.mib
RFC1213-MIB	https://www.ietf.org/rfc/rfc1213.txt
SNMPv2-MIB	https://www.ietf.org/rfc/rfc3418.txt
TCP-MIB	https://www.ietf.org/rfc/rfc4022.txt
P-BRIDGE-MIB.txt	http://www.icir.org/fenner/mibs/extracted/P-BRIDGE-MIB-rfc2674.txt
RMON2-MIB.txt	https://www.ietf.org/rfc/rfc3273.txt
TOKEN-RING-RMON-MIB.txt	http://www.icir.org/fenner/mibs/extracted/TOKEN-RING-RMON-MIB-rmonmib-01.txt

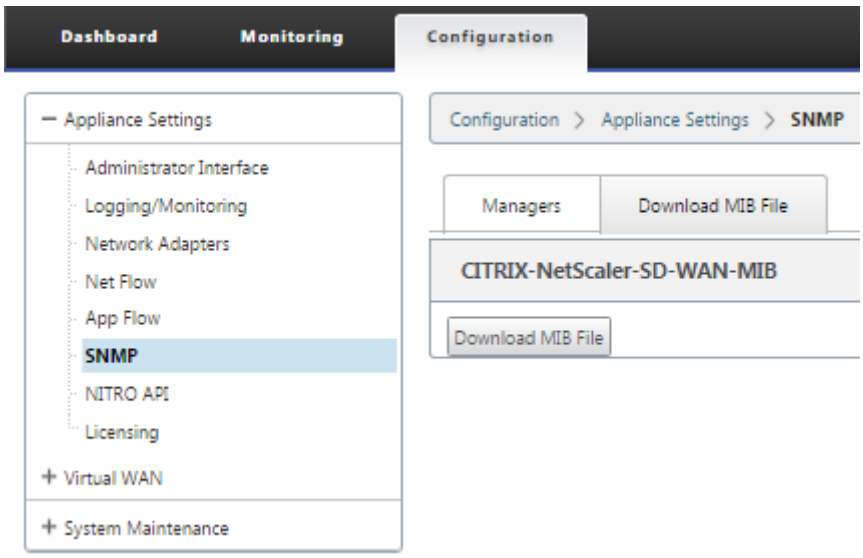
Debe descargar los siguientes archivos SNMP antes de comenzar a supervisar un dispositivo Citrix SD-WAN:

- CITRIX-COMMON-MIB.txt
- APPACCELERATION-SMI.txt
- APPACCELERATION-PRODUCTS-MIB.txt
- APPACCELERATION-TC.txt
- APPACCELERATION-STATUS-MIB.txt
- APPCACHE-MIB.txt
- SDX-MIB-smiv2.mib

Los administradores SNMPv3 y los detectores de capciones SNMPv3 utilizan los archivos MIB. Los archivos incluyen las MIB empresariales del dispositivo SD-WAN, que proporcionan eventos específicos de SD-WAN. Para descargar archivos MIB, en la interfaz de administración web de SD-WAN:

1. Vaya a **la página Configuración** > **Configuración del dispositivo** > **SNMP** > **Descargar archivo MIB**.
2. Seleccione el archivo **MIB** necesario.
3. Haga clic en **Ver**.

   El archivo MIB se abre en el explorador MIB.



Nota

- El proceso daemon **net-snmp snmpd** en sistemas Linux proporciona soporte para estas MIB de forma predeterminada. Las MIB proporcionan la base para admitir aplicaciones de administración de redes.
- Los contadores de bytes y paquetes de puertos Ethernet se encuentran en el **IF-MIB** dentro de **ifTable**. La información del sistema está en el objeto del sistema.
- Los puertos Ethernet están incluidos en el **ifTable**, por lo que caminar debe ser suficiente para garantizar que el subsistema SNMP se está ejecutando.
- El soporte para **Q-BRIDGE-MIB** e **IP-MIB** proporciona soporte para la aplicación de mapeo de red.

Interfaz administrativa

August 26, 2022

Puede administrar y mantener sus dispositivos de Citrix SD-WAN mediante las siguientes opciones administrativas mediante Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte

Parámetros del dispositivo.

- Cuentas de usuario
- Servidor RADIUS
- Servidor TACACS+
- Cert HTTPS
- Configuración de HTTPS
- Otros

Cuentas de usuario

Puede agregar nuevas cuentas de usuario y administrar las cuentas de usuario existentes en **Configuración > Configuración del dispositivo > Página Interfaz de administrador > ficha Cuentas de usuario**.

Puede optar por autenticar las cuentas de usuario recién agregadas localmente mediante el dispositivo SD-WAN o de forma remota. Las cuentas de usuario que se autentican de forma remota se autentican a través de los servidores de autenticación RADIUS o TACACS+.

Funciones de usuario

Se admiten las siguientes funciones de usuario:

- **Visor**: La cuenta del visor es una cuenta de solo lectura con acceso a las páginas **Panel**, **Informes** y **Supervisión**.
- **Admin**: La cuenta de administrador tiene los privilegios administrativos y el acceso de lectura y escritura a todas las secciones.

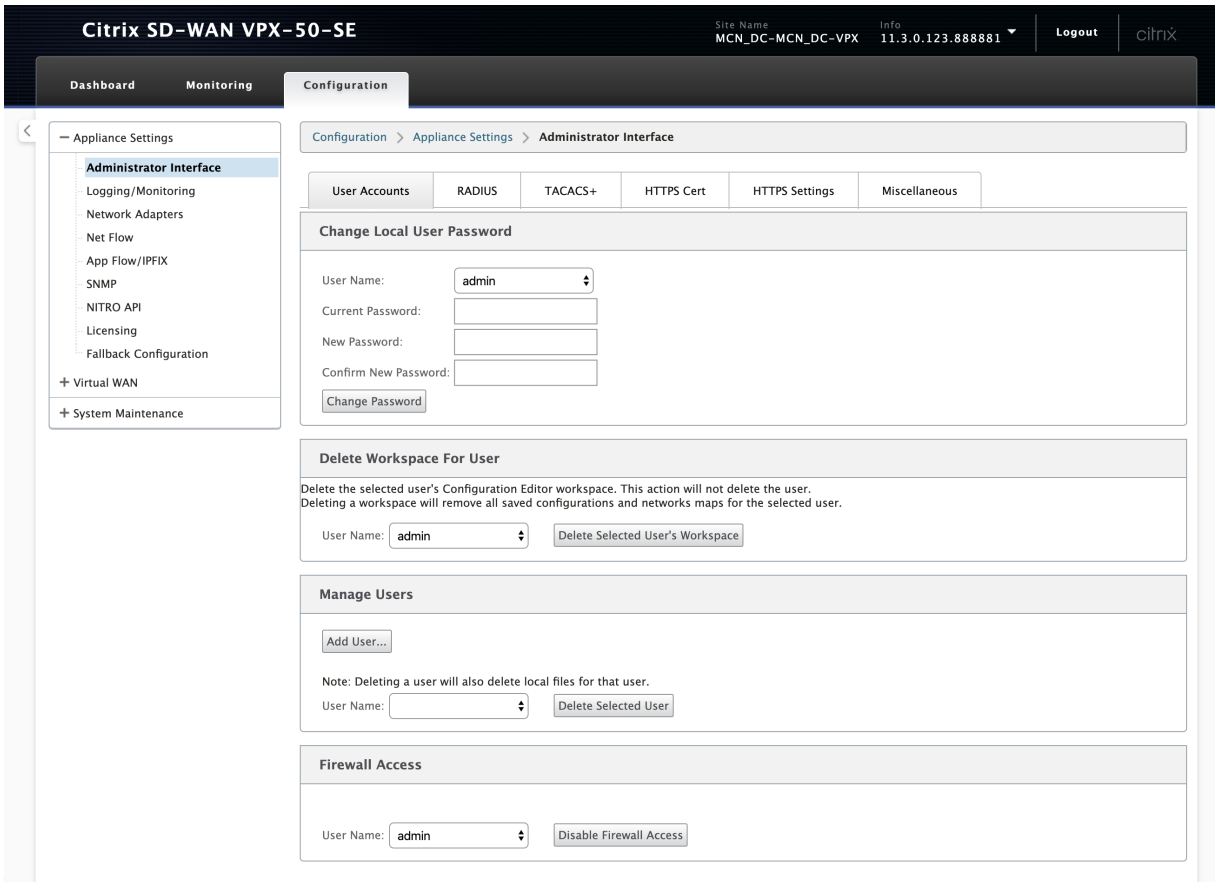
  Un superadministrador (admin) tiene los siguientes privilegios:

  - Puede exportar la configuración a la bandeja de entrada de administración de cambios para realizar una configuración y una actualización de software a la red.
  - También puede alternar el acceso de lectura y escritura de los administradores de red y seguridad.
  - Mantiene la configuración relacionada con la red y la seguridad.
- **Administrador de seguridad**: Un administrador de seguridad tiene acceso de lectura y escritura solo para la configuración relacionada con el firewall y la seguridad, mientras que tiene acceso de solo lectura a las secciones restantes. El administrador de seguridad también tiene la capacidad de habilitar o inhabilitar el acceso de escritura al firewall para otros usuarios, excepto el superadministrador (admin).

- **Administrador de redes**: Un administrador de redes tiene permisos de lectura y escritura en todas las secciones y puede aprovisionar completamente una sucursal, excepto para la configuración relacionada con el firewall y la seguridad. El nodo de firewall alojado no está disponible para el administrador de red. En este caso, el administrador de red debe importar una nueva configuración.

Tanto el administrador de red como el administrador de seguridad pueden realizar cambios en la configuración y también implementarlos en la red.

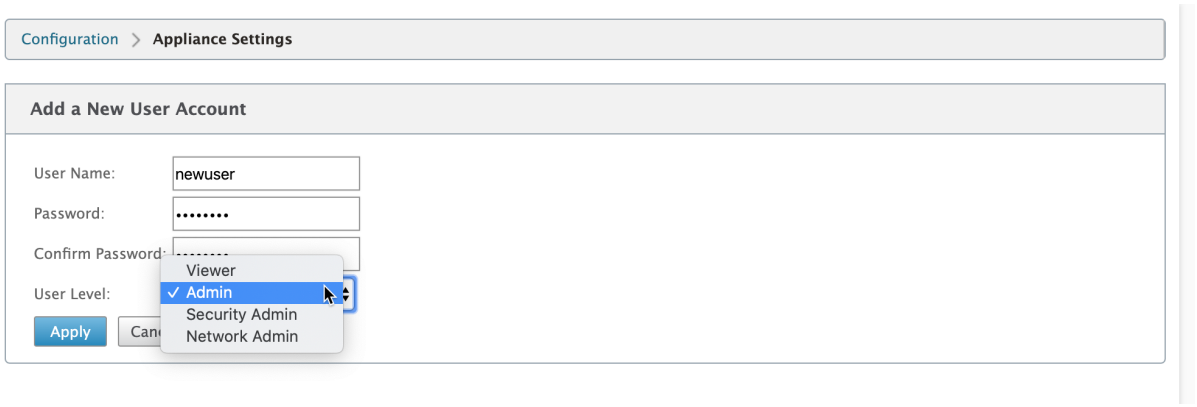
> **NOTA**
>
> El administrador de red y el administrador de seguridad no pueden agregar o eliminar cuentas de usuario. Solo pueden modificar sus propias contraseñas de cuenta.



Agregar un usuario

Para agregar un usuario, haga clic en **Agregar usuario** en la sección **Administrar usuarios**. Proporcione el **nombre de usuario** y **la contraseña**. Seleccione el rol de usuario en la lista desplegable **Nivel de usuario** y haga clic en **Aplicar**.

También puede eliminar una cuenta de usuario, si es necesario. Al eliminar un usuario, también se eliminan los archivos locales que pertenecen a ese usuario. Para eliminar, en la sección **Administrar usuarios**, seleccione el usuario en la lista desplegable **Nombre de usuario** y haga clic en **Eliminar usuario seleccionado**.



Cambiar la contraseña de un usuario

La función de administrador puede cambiar la contraseña de una cuenta de usuario autenticada localmente por el dispositivo SD-WAN.

Para cambiar la contraseña, en la sección **Cambiar contraseña de usuario local**, seleccione el **usuario en la lista desplegable Nombre** de usuario. Introduzca la contraseña actual y la nueva contraseña. Haga clic en **Cambiar contraseña**.

Servidor RADIUS

Puede configurar un dispositivo SD-WAN para autenticar el acceso de los usuarios con uno o un máximo de tres servidores RADIUS. El puerto predeterminado es 1812.

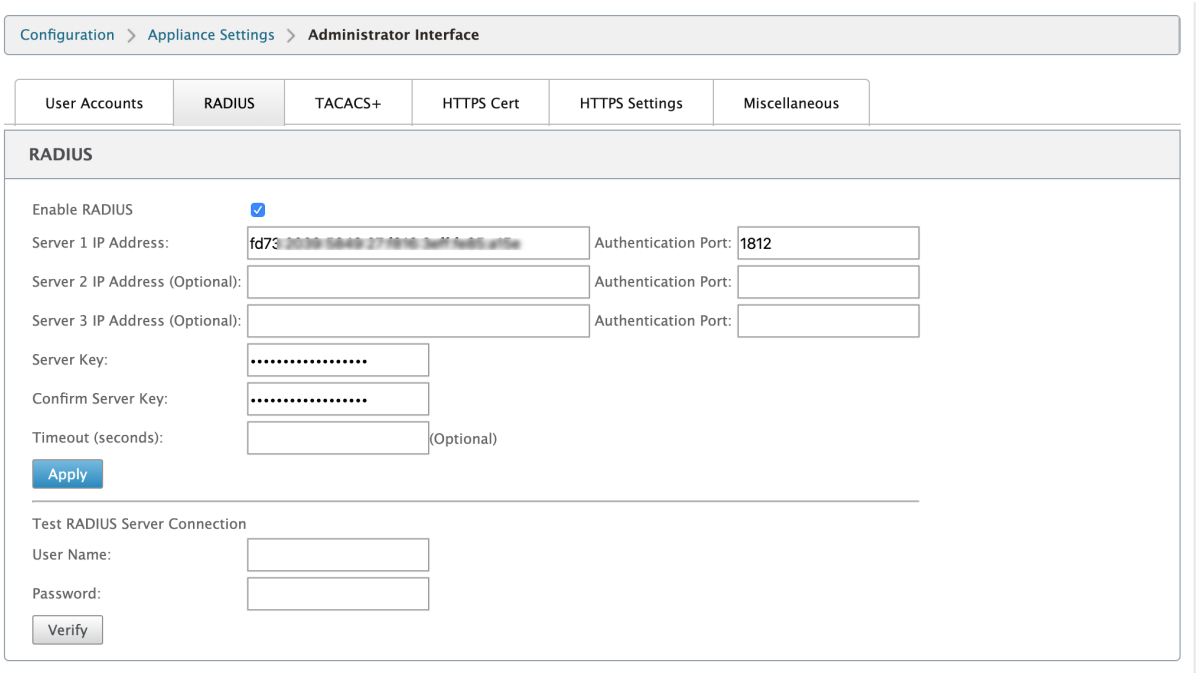
Para configurar el servidor RADIUS:

1. Vaya a **Configuración > Configuración > Configuración del dispositivo > Interfaz de administrador > RADIUS**.
2. Marque la casilla **Habilitar RADIUS**.
3. Introduzca la **dirección IP del servidor** y el **puerto de autenticación**. Se puede configurar un máximo de tres direcciones IP de servidor.

   > **NOTA**
   >
   > Para configurar una dirección IPv6, asegúrese de que el servidor RADIUS también está configurado con una dirección IPv6.

4. Introduzca la **clave del servidor** y confirme.
5. Introduzca el valor de **Tiempo de espera** en segundos.
6. Haga clic en **Guardar**.

También puede probar la conexión del servidor RADIUS. Introduzca el **nombre de usuario** y la **contraseña**. Haga clic en **Verificar**.



Servidor TACACS+

Puede configurar un servidor TACACS+ para la autenticación. De forma similar a la autenticación RADIUS, TACACS+ utiliza una clave secreta, una dirección IP y el número de puerto. El número de puerto predeterminado es 49.

Para configurar el servidor TACACS+:

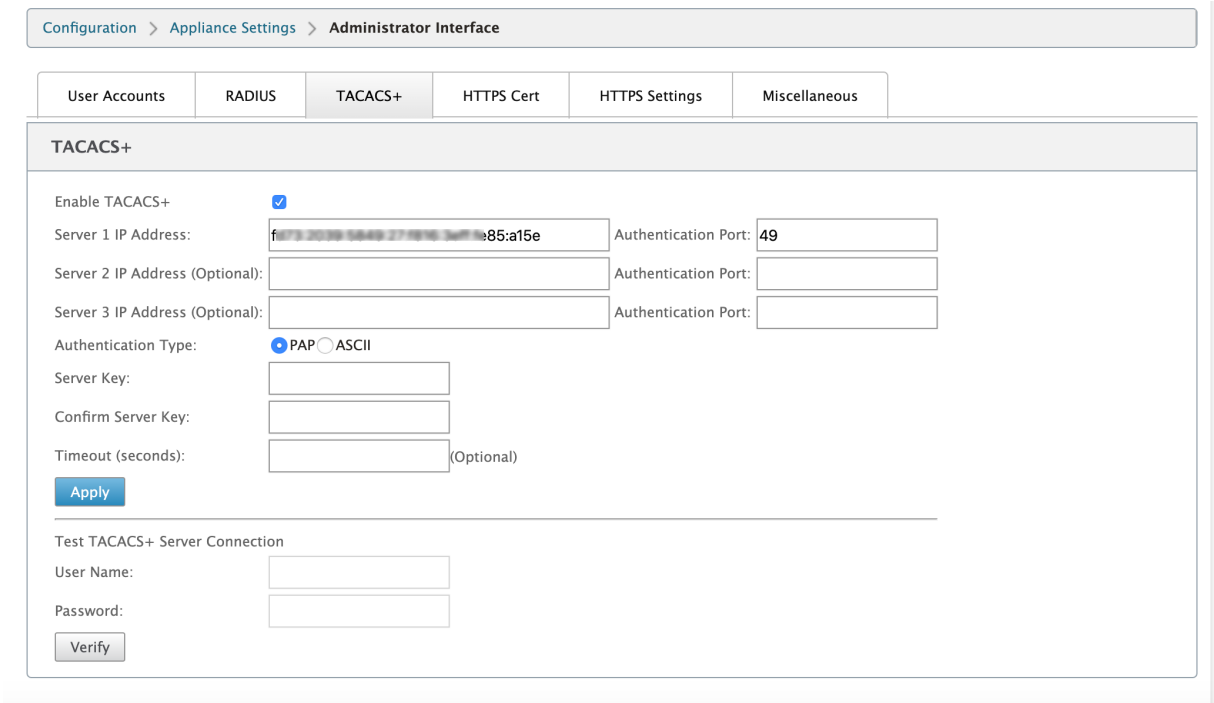
1. Vaya a **Configuración > Configuración > Configuración del dispositivo > Interfaz de administrador > TACACS+**.
2. Seleccione la casilla **Habilitar TACACS+**.
3. Introduzca la **dirección IP del servidor** y el **puerto de autenticación**. Se puede configurar un máximo de tres direcciones IP de servidor.

   > **NOTA**
   >
   > Para configurar una dirección IPv6, asegúrese de que el servidor TACACS+ también está

> configurado con una dirección IPv6.

4. Seleccione **PAP** o **ASCII** como Tipo de autenticación.
   - PAP: Utiliza el Protocolo de autenticación de contraseñas (PAP) para reforzar la autenticación de usuarios mediante la asignación de un secreto compartido seguro al servidor TACACS+.
   - ASCII: utiliza el juego de caracteres ASCII para reforzar la autenticación de usuario asignando un secreto compartido seguro al servidor TACACS+.
5. Introduzca la **clave del servidor** y confirme.
6. Introduzca el valor de **Tiempo de espera** en segundos.
7. Haga clic en **Guardar**.

También puede probar la conexión del servidor TACACS+. Introduzca el **nombre de usuario** y la **contraseña**. Haga clic en **Verificar**.



Anuncio de enrutador NDP y grupo de delegación de prefijos

November 16, 2022

Anuncio de enrutador NDP

En una red IPv6, el dispositivo SD-WAN multidifusión periódicamente mensajes de anuncio de enrutador (RA) para anunciar su disponibilidad y transmitir información a los dispositivos vecinos de la red SD-WAN. Los anuncios de enrutador incluyen la información del prefijo IPv6. El protocolo de detección de vecinos (NDP) que se ejecuta en dispositivos SD-WAN utiliza estos anuncios de enrutador para determinar los dispositivos vecinos en el mismo vínculo. También determina las direcciones de capa de vínculo de los demás, busca vecinos y mantiene la información de accesibilidad acerca de las rutas a los vecinos activos.

Puede configurar la publicación del enrutador NDP mediante Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Anuncio de router NDP.

Grupo de delegación de prefijos

> **NOTA**
>
> La delegación de prefijos no se admite en la versión 11.3 de Citrix SD-WAN.

Los dispositivos Citrix SD-WAN se pueden configurar como un cliente DHCPv6 para solicitar un prefijo del ISP mediante el puerto WAN configurado. Una vez que el dispositivo Citrix SD-WAN recibe el prefijo, utiliza el prefijo para crear un grupo de direcciones IP para atender a los clientes LAN. A continuación, el dispositivo Citrix SD-WAN se comporta como un servidor DHCP y anuncia el prefijo en los puertos LAN a los clientes de LAN.

Puede configurar la delegación de prefijos a través de Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Grupos de delegación de prefijos.

Artículos prácticos

August 26, 2022

Los "How-to-Articles"describen el procedimiento para configurar las funciones admitidas por Citrix SD-WAN. Estos artículos contienen información sobre algunas de las siguientes funciones importantes:

Haga clic en el nombre de una función a continuación para ver la lista de artículos de procedimientos para esa función.

- Redirección y reenvío virtuales
- Habilitación de RED para equidad de QoS

- Configuración
- Redirección dinámica
- Servidor DHCP y retransmisión DHCP
- Filtros de ruta
- Terminación y supervisión de IPsec
- Secure Web Gateway
- QoS
- Funcionamiento conforme a FIPS: túnel IPsec
- Configuración NAT dinámica
- Detección de ancho de banda adaptable
- Prueba de ancho de banda activa
- Mejoras de BGP
- Asociación de clases de servicio con perfiles SSL
- Implementación sin contacto

Configurar la interfaz de acceso

August 26, 2022

Para configurar la interfaz de acceso a través de Citrix SD-WAN Orchestrator Service, consulte Enlaces WAN.

Configurar direcciones IP virtuales

August 26, 2022

Para configurar direcciones IP virtuales a través de Citrix SD-WAN Orchestrator Service, consulte Enlaces WAN.

Configurar túneles GRE

August 26, 2022

Para configurar túneles GRE mediante Citrix SD-WAN Orchestrator Service, consulte Servicio GRE.

Configurar rutas dinámicas para la comunicación de bifurcación a bifurcación

November 16, 2022

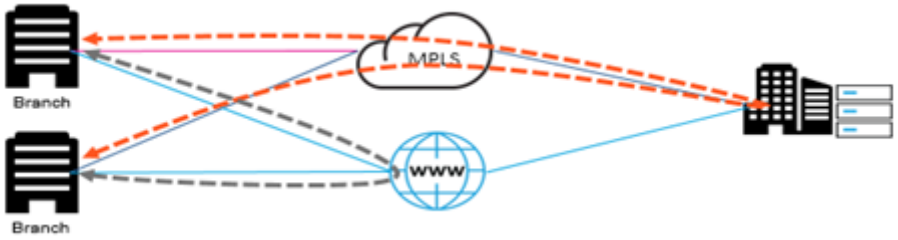
Con la demanda de VoIP y videoconferencias, el tráfico se mueve cada vez más entre las oficinas. Es ineficiente configurar conexiones de malla completa a través de centros de datos, lo que puede llevar mucho tiempo.

Con Citrix SD-WAN, no es necesario configurar paths entre todas las oficinas. Puede habilitar la función Ruta dinámica y la solución SD-WAN crea automáticamente rutas entre oficinas a petición. La sesión utiliza inicialmente una ruta fija existente. Y a medida que se alcanzó el ancho de banda y el umbral de tiempo, se crea un path dinámicamente si ese nuevo path tiene mejores funciones de rendimiento que el path fijo. El tráfico de sesión se transmite a través de la nueva ruta. Esto se traduce en un uso eficiente de los recursos. Las rutas solo existen cuando son necesarias y reducen la cantidad de tráfico que se transmite hacia y desde el centro de datos.

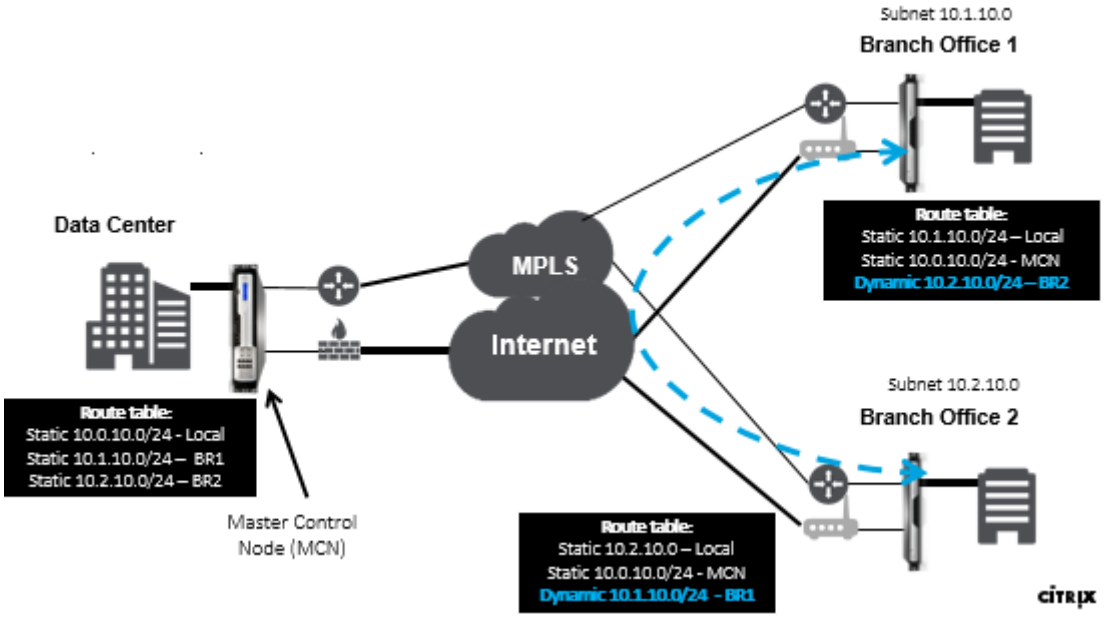
Las ventajas adicionales de la red SD-WAN incluyen:

- Umbrales de ancho de banda y PPS para permitir conexiones de sucursal a sucursal
- Reduzca los requisitos de ancho de banda dentro y fuera del centro de datos al tiempo que minimiza la latencia
- Las rutas creadas a petición dependen de los umbrales establecidos
- Libere recursos de red de forma dinámica cuando no sea necesario
- Reducir la carga en el nodo de control maestro y la latencia

Comunicación de sucursal a sucursal mediante rutas virtuales dinámicas:



Red SD-WAN con ruta dinámica:



- Las rutas virtuales dinámicas se utilizan para implementaciones a gran escala, como empresas
- Las implementaciones más pequeñas utilizan rutas virtuales estáticas y rutas virtuales de cualquier a cualquier
- Utilice siempre rutas virtuales estáticas entre dos centros de datos (DC a DC)
- No es necesario configurar todas las rutas de acceso WAN para utilizar la ruta virtual dinámica
- Cada dispositivo SD-WAN tiene un número limitado de rutas virtuales dinámicas (8 límites mínimos dinámicos, 8 límites mínimos estáticos = 16 en total) que se pueden configurar.

Cómo habilitar la ruta virtual dinámica en la GUI de SD-WAN

Para habilitar rutas virtuales dinámicas mediante Citrix SD-WAN Orchestrator Service, consulte Rutas virtuales.

Reenvío de WAN a WAN

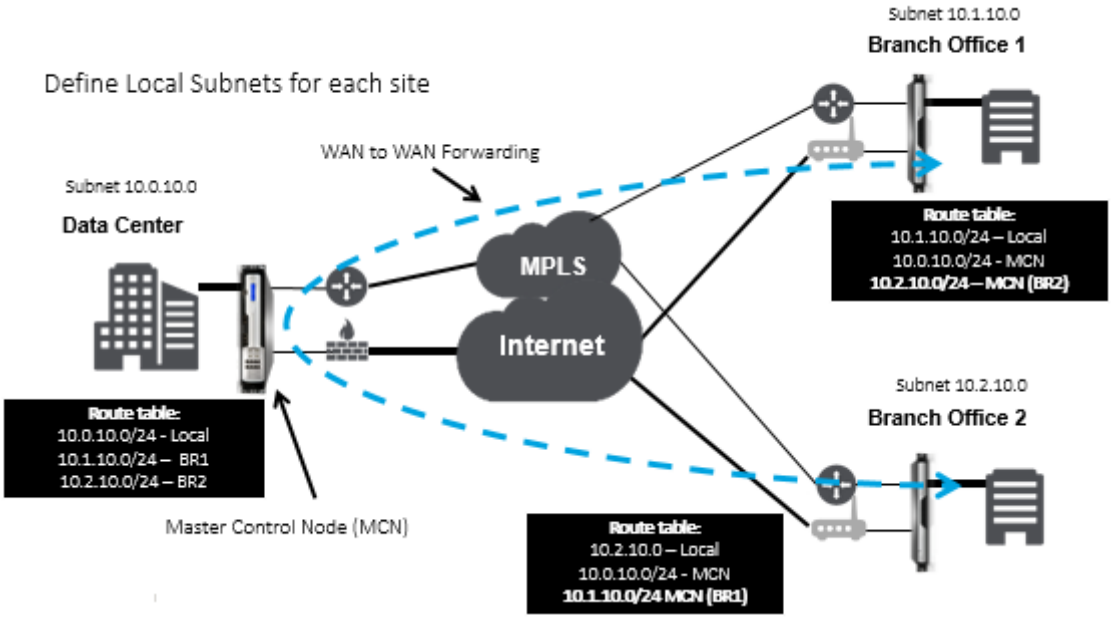
August 26, 2022

Al habilitar el reenvío de WAN a WAN en el MCN, el MCN puede anunciar rutas de sitios remotos.

- Los clientes conocen las rutas locales de MCN y otras rutas del sitio del cliente
- Desde la perspectiva del cliente, todas las rutas se consideran rutas MCN

Cuando el reenvío de WAN a WAN no está habilitado en el MCN, se detectan problemas de comunicación de Branch a Branch en la red del cliente.

Los dispositivos que se ejecutan en modo cliente no conocen otras subredes de sucursales hasta que el reenvío de WAN a WAN está habilitado en el MCN. Al habilitar esta opción, los nodos SD-WAN de la sucursal conocen otras subredes de sucursal. El tráfico destinado a otras sucursales se reenvía a MCN. MCN lo redirige al destino correcto.



Supervisión y solución de problemas

August 26, 2022

Puede utilizar la interfaz de administración web del dispositivo Citrix SD-WAN para supervisar y solucionar problemas de las funciones compatibles. A continuación se muestran los vínculos a los temas de supervisión y solución de problemas aplicables a los dispositivos Citrix SD-WAN.

Supervisión de WAN Virtual

August 26, 2022

Visualización de información básica de un dispositivo

Utilice un explorador para conectarse a la interfaz web de administración del dispositivo que quiere supervisar y haga clic en la ficha **Panel** de control para mostrar la información básica del dispositivo.

La página **Panel** de control muestra la siguiente información básica del dispositivo local:

Estado del sistema:

- **Nombre**: Es el nombre que asignó al dispositivo cuando lo agregó al sistema.
- **Modelo**: Número de modelo del dispositivo WAN virtual.
- **Modo de equipo**: Indica si este dispositivo se ha configurado como MCN principal o secundario o como dispositivo cliente.
- **Dirección IP de administración:** dirección IP de administración del dispositivo.
- **Tiempo de actividad del dispositivo:** especifica la duración durante la que se ha estado ejecutando el dispositivo desde el último reinicio.
- **Tiempo de actividad del servicio**: Especifica la duración durante la que se ha estado ejecutando el servicio WAN virtual desde el último reinicio.

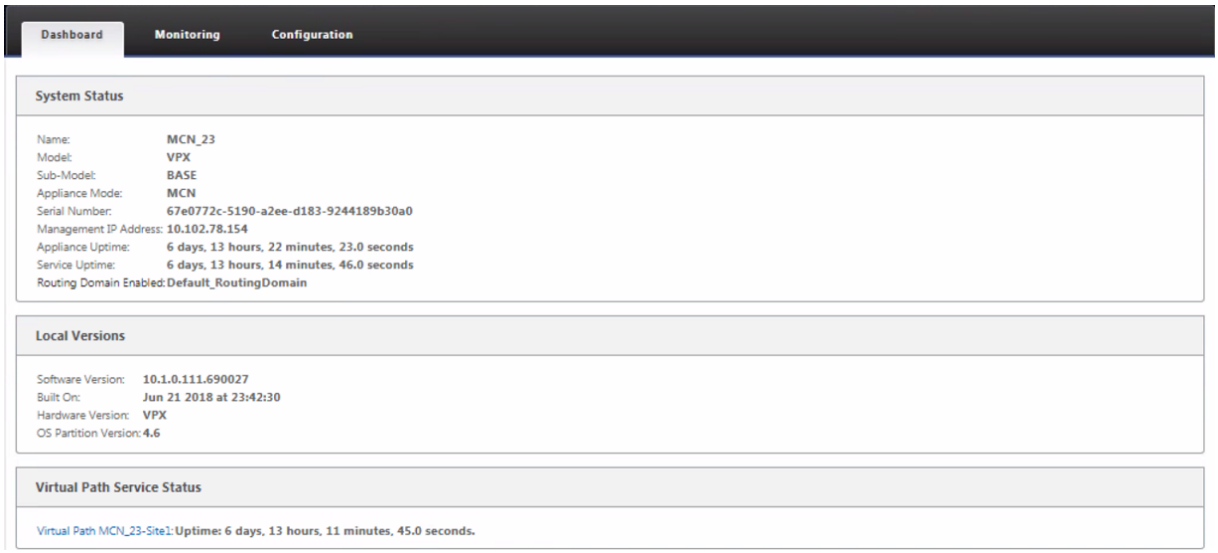
Estado del servicio de ruta virtual:

Ruta virtual [nombre del sitio]: Muestra el estado de todas las rutas virtuales asociadas a este dispositivo. Si el servicio WAN virtual está habilitado, esta sección se incluye en la página. Si el servicio WAN virtual está inhabilitado, aparece un icono de alerta (delta de vara de oro) y un mensaje de alerta en ese sentido en lugar de esta sección.

Información de versión local:

- **Versión de software:** es la versión del paquete de software CloudBridge Virtual Path activado actualmente en el dispositivo.
- **Compilación en**: Fecha de compilación de la versión del producto que se ejecuta actualmente en el dispositivo local.
- **Versión de hardware**: Número de modelo de hardware y versión del dispositivo.
- **Versión de partición del SO:** es la versión de la partición del sistema operativo activa actualmente en el dispositivo.

En la siguiente ilustración se muestra una página de panel de control de ejemplo.



Visualización de información estadística

August 26, 2022

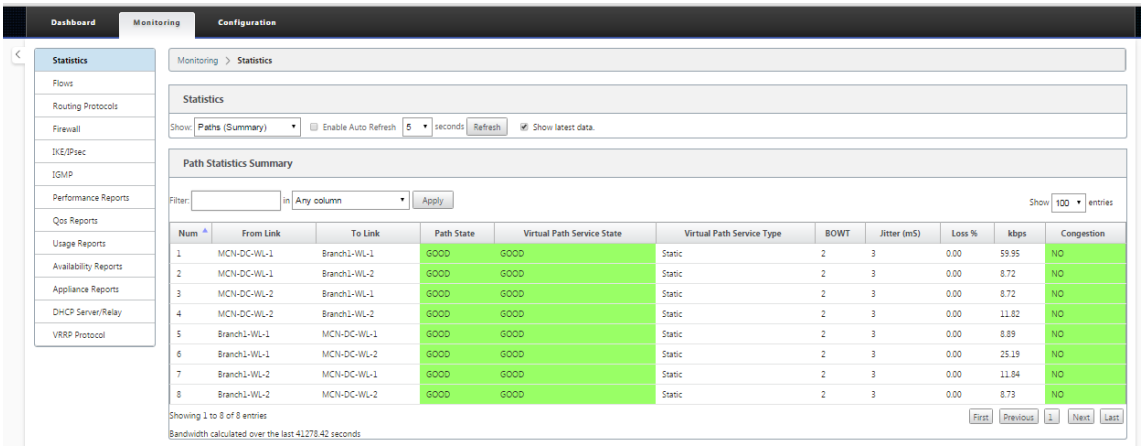
En esta sección se proporcionan instrucciones básicas para ver la información estadística de la WAN virtual.

1. Inicie sesión en la Interfaz Web de administración del MCN.

2. Seleccione la ficha **Supervisión**.

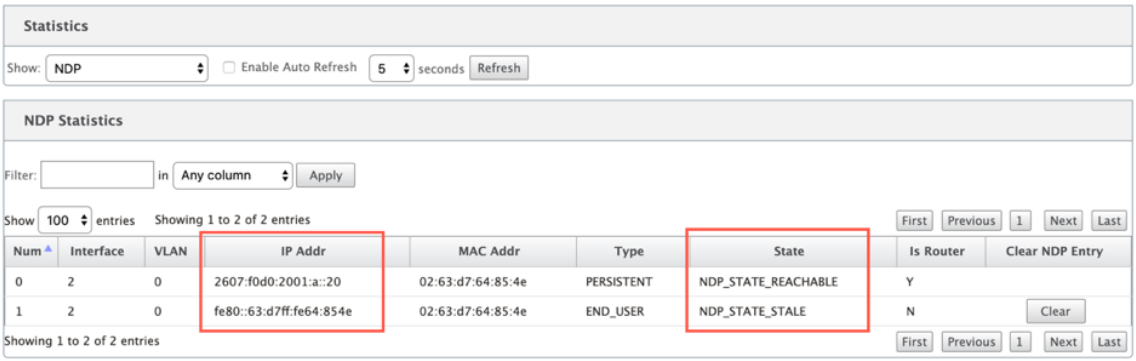
   Se abre el árbol de navegación **Supervisión** en el panel izquierdo. De forma predeterminada, también se muestra la página **Estadísticas** con **Rutas** preseleccionadas en el campo **Mostrar**. Contiene una tabla detallada de estadísticas de rutas.

   > **Nota**
   >
   > Si accede a otra página **Supervisión** (por ejemplo, **Flujos**), puede volver a esta página seleccionando **Estadísticas** en el árbol de navegación **Supervisión** (panel izquierdo).

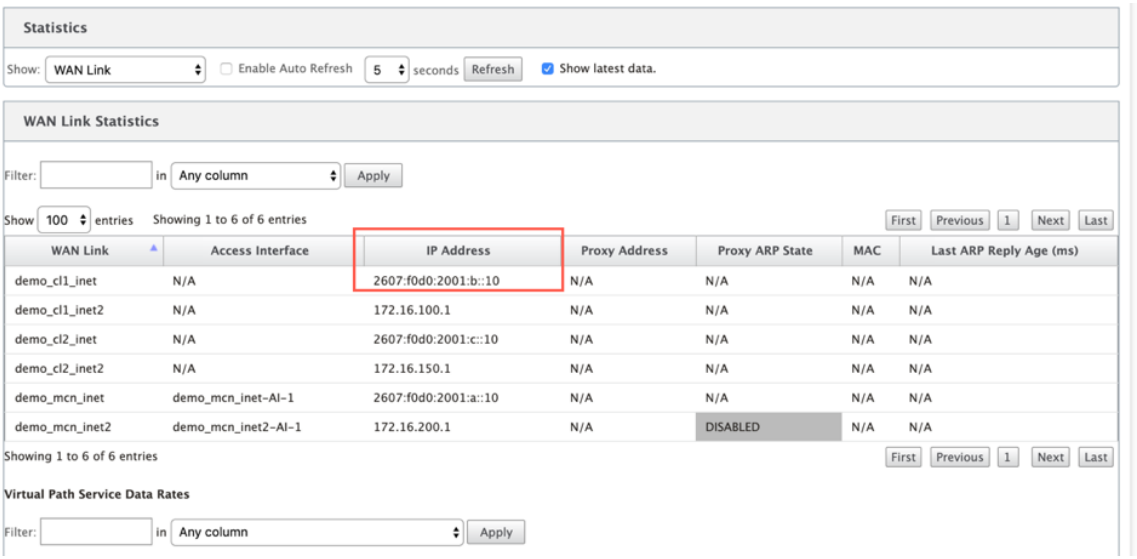


Con la versión 11.1.0, se agrega la opción Neighbor Discovery Protocol (NDP) para depurar problemas de detección de vecinos.

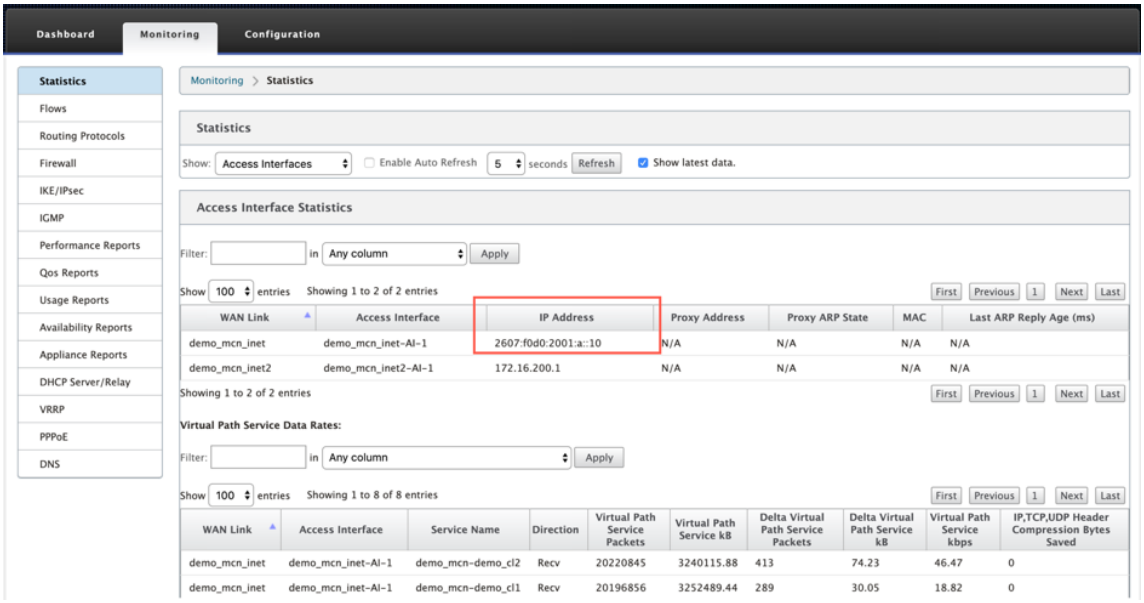
1. Seleccione la opción NDP en el menú desplegable Mostrar y podrá ver el estado de NDP junto con las direcciones IPv6.



2. Seleccione Vínculo WAN en el menú desplegable. También puede ver la dirección IPv6 si configuró en la ficha Dirección IP.

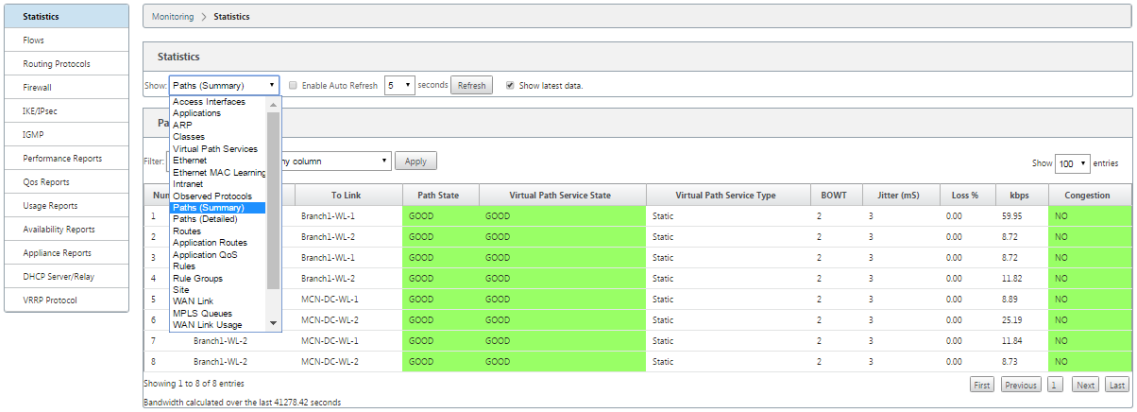


3. También puede ver las estadísticas de la interfaz de acceso.



4. Abra el menú desplegable **Mostrar**.

   Además de las **estadísticas**Rutas de acceso, NDP, Interfaz**de Acceso y Vínculos WAN**, el menú **Mostrar** también ofrece varias opciones más para filtrar y ver información estadística.



Seleccione un filtro en el menú **Mostrar** para ver una tabla de información estadística para ese tema.

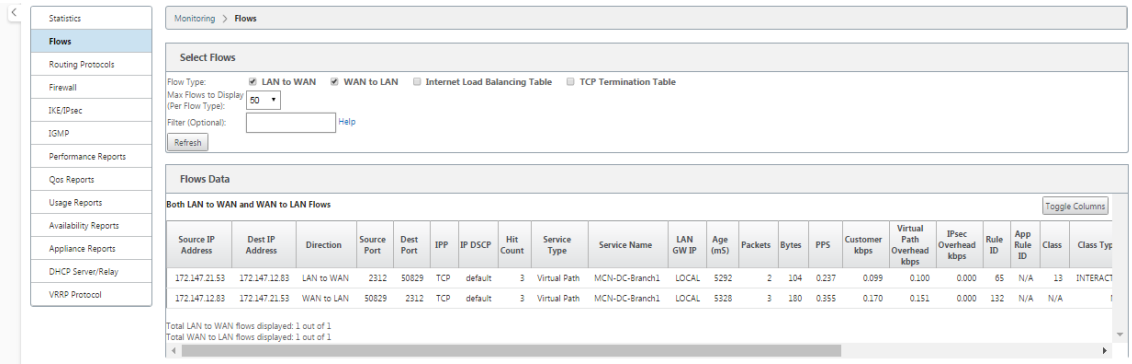
Visualización de información de flujo

August 26, 2022

En esta sección se proporcionan instrucciones básicas para ver la información del flujo de la WAN virtual.

Para ver la información del flujo, haga lo siguiente:

1. Inicie sesión en la Interfaz Web de administración del MCN y seleccione la ficha **Supervisión**. Abre el árbol de navegación **Supervisión** en el panel izquierdo.
2. Seleccione la sucursal **Flujos** en el árbol de navegación. Muestra la página **Flujos** con **LAN** a **WAN** preseleccionada en el campo **Tipo de flujo**.

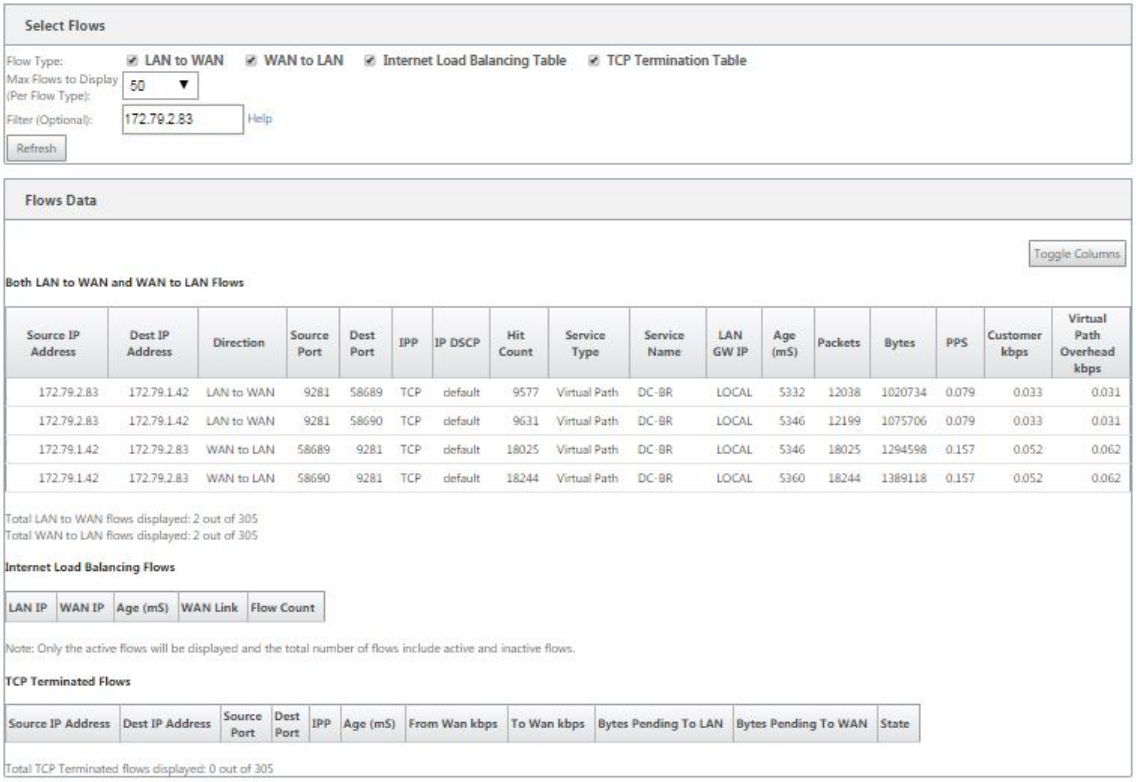


3. Seleccione el **tipo de flujo**. El campo **Tipo de flujo** se encuentra en la sección **Seleccionar flujos** en la parte superior de la página **Flujos**. Junto al campo **Tipo de flujo** hay una fila de opciones de casilla de verificación para seleccionar la información de flujo que quiere ver. Puede marcar una o varias casillas para filtrar la información que se va a mostrar.

4. Seleccione los **flujos máximos para mostrar** en el menú implementable situado junto a ese campo.
5. Determina el número de entradas que se mostrarán en la tabla **Flujos**. Las opciones son: **50**, **100**, **1000**.
6. (Opcional) Introduzca el texto de búsqueda en el campo **Filtro**. Filtra los resultados de la tabla para que solo se muestren en la tabla las entradas que contengan el texto de búsqueda.

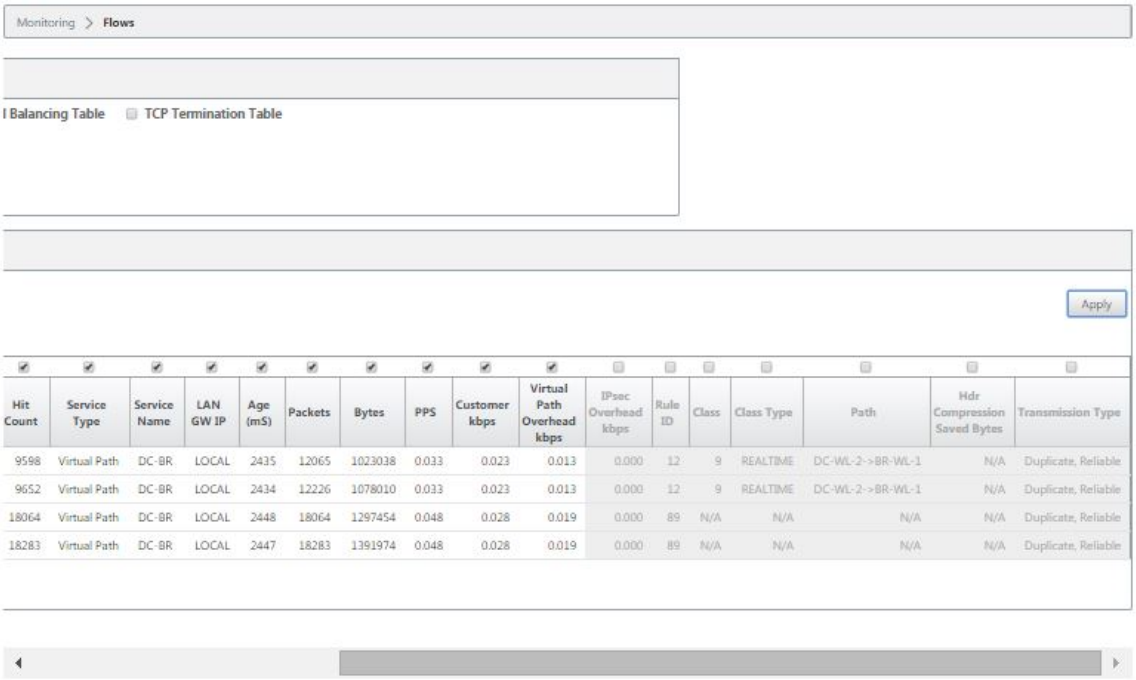
> **Sugerencia**
>
> Para ver instrucciones detalladas sobre el uso de filtros para refinar los resultados de la tabla de **flujos**, haga clic en **Ayuda** a la derecha del campo **Filtro**. Para cerrar la pantalla de ayuda, haga clic en **Actualizar** en la esquina inferior izquierda de la sección **Seleccionar flujos**.

7. Haga clic en **Actualizar** para mostrar los resultados del filtro. La ilustración muestra una muestra filtrada de página **Flujos** con todos los tipos de flujo seleccionados.



8. (Opcional) Seleccione las columnas que quiere incluir en la tabla. Haga lo siguiente:
9. Haga clic en **Alternar columnas** en la esquina superior derecha de la tabla **Datos de flujos**. Muestra las columnas no seleccionadas y abre una casilla de verificación encima de cada columna para seleccionar o anular la selección de esa columna. Las columnas no seleccionadas se muestran atenuadas, como se muestra en la ilustración.

> **Nota**
>
> De forma predeterminada, se seleccionan todas las columnas, lo que puede hacer que la tabla se trunque en la pantalla, oscureciendo el botón **Alternar columnas**. Si es así, se muestra una barra de desplazamiento horizontal debajo de la tabla. Desliza la barra de desplazamiento hacia la derecha para ver la sección truncada de la tabla y mostrar el botón **Alternar columnas**. Si la barra de desplazamiento no está disponible, intente cambiar el tamaño del ancho de la ventana del explorador hasta que se muestre la barra de desplazamiento.



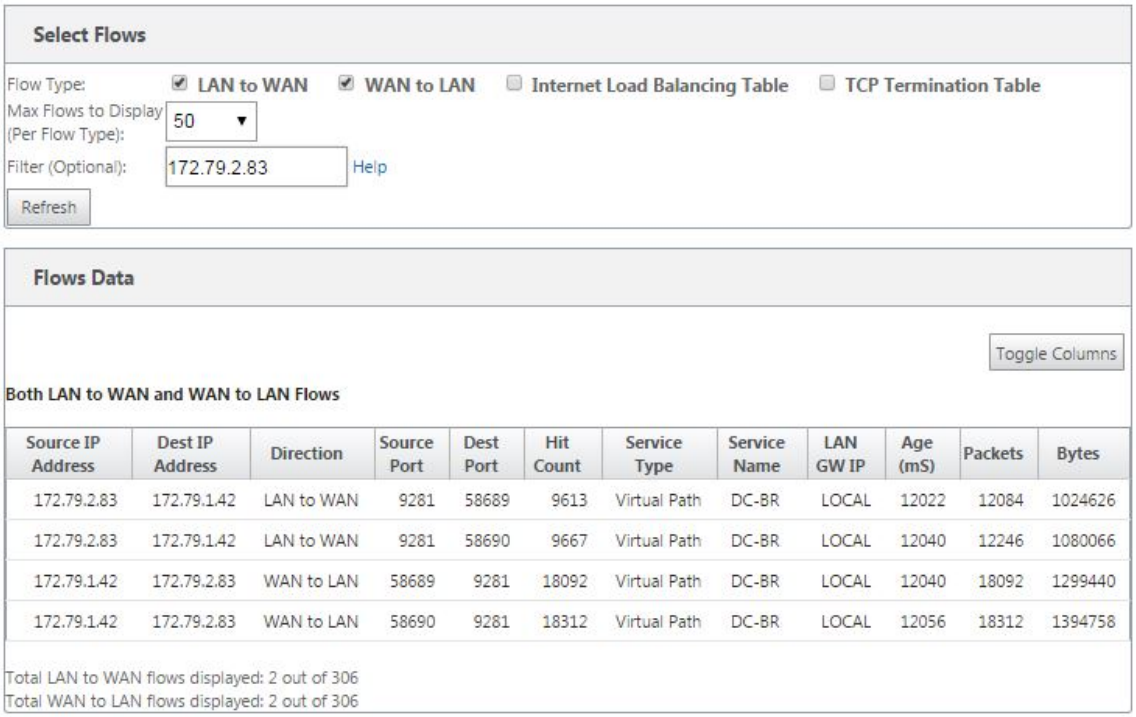
10. Haga clic en una casilla de verificación para seleccionar o anular la selección de una columna.

    - **Dirección IP de origen**: La dirección IP de origen de los paquetes de este flujo.
    - **Dirección IP de destino**: La dirección IP de destino para los paquetes de este flujo.
    - **Dirección**: La dirección de los paquetes en este flujo: LAN a WAN o WAN a LAN.
    - **Puerto de origen**: El puerto de origen para los paquetes de este flujo.
    - **Puerto de destino**: El puerto de destino para los paquetes de este flujo.
    - **IPP**: El número de protocolo IP para los paquetes de este flujo.
    - **IP DSCP**: La configuración de la etiqueta IP DSCP para los paquetes de este flujo.
    - **Recuento de aciertos**: El número de veces que se ha buscado y encontrado este flujo.
    - **Tipo de servicio**: Indica si este tipo de flujo es tráfico de ruta virtual, Internet o intranet.
    - **Nombre del servicio**: El nombre de la ruta virtual que utiliza el tráfico de la ruta virtual.
    - **IP de LAN GW**: Dirección IP para la puerta de enlace LAN, si se especifica una.
    - **Antigüedad (ms)**: El tiempo (en milisegundos) desde que se clasificó un paquete en este

flujo.

- **Paquetes**: Número de paquetes enviados durante la vida del flujo.
- **Bytes**: Número de bytes enviados durante la vida del flujo.
- **PPS**: Paquetes por segundo durante el período transcurrido desde la última actualización.
- **Kbps de cliente**/**Kbps de sobrecarga de ruta virtual**/**Kbps de sobrecarga de IPsec**: Kilobits por segundo durante el período transcurrido desde la última actualización.
- **ID de regla**: El identificador de la regla con la que coincidió el tráfico en este flujo.
- **ID de regla de aplicación**: El ID de la aplicación, la regla con la que coincidió el tráfico en este flujo.
- **Clase**: El identificador de la clase de ruta virtual que utiliza el tráfico.
- **Tipo de clase**: El tipo de clase de ruta virtual (en tiempo real, interactiva, masiva) que utiliza el tráfico.
- **Ruta**: La ruta que utiliza el tráfico.
- **Bytes guardados de compresión HDR**: El número de bytes guardados debido a la compresión de encabezados.
- **Tipo de transmisión**: El tipo de transmisión que utiliza el tráfico.
- **Aplicación**: El nombre de la aplicación en uso.

11. Haga clic en **Aplicar** (encima de la esquina superior derecha de la tabla). Descarta las opciones de selección y actualiza la tabla para incluir solo las columnas seleccionadas.



Aplicaciones DPI en SD-WAN Center

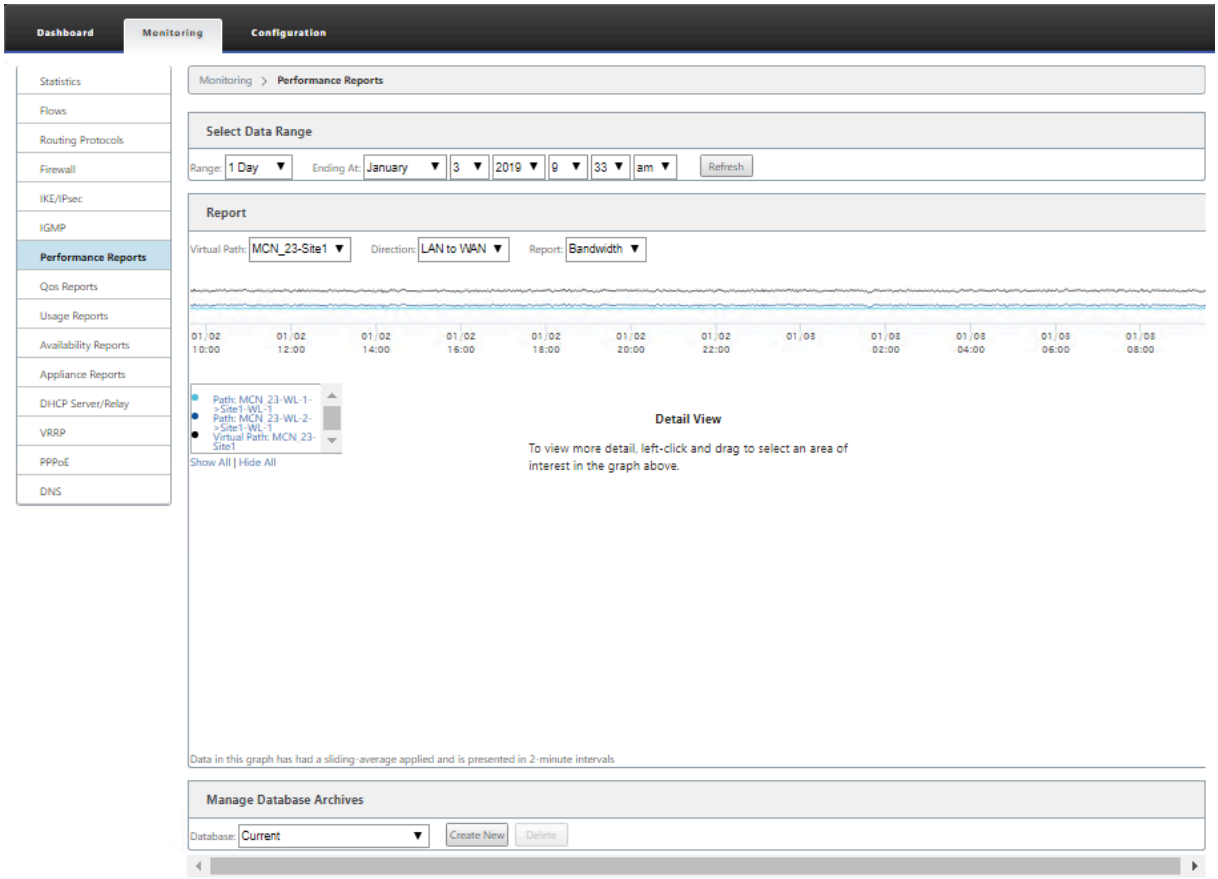
En versiones anteriores, se pueden identificar unas 4.000 aplicaciones configuradas con 800 servicios (550 rutas virtuales, 256 servicios de intranet). Almacenar estos datos afectaría al rendimiento general del sistema (ciclos de CPU y espacio en disco necesario para almacenar los datos). También tiene un impacto, si se admite la creación de informes sobre datos por Uso o Ruta.

Mientras que la ruta de datos proporciona información sobre cada aplicación recopilada en un minuto, el informe de estadísticas por minuto determina las 100 aplicaciones principales e informa sobre el agregado de todas las demás aplicaciones como otras. Si hay una gran diversidad de aplicaciones rastreables en su red, podría afectar la claridad de los datos, especialmente si queremos rastrear/-graficar el uso de una aplicación a lo largo del tiempo y la aplicación se queda fuera del límite máximo de 100.

Ver informes

August 26, 2022

En esta sección se proporcionan instrucciones básicas para generar y ver informes de WAN virtual sobre el dispositivo local mediante la Interfaz Web de administración. Un dispositivo puede mantener hasta 30 archivos y depurar los archivos más antiguos, que son más de 30 entradas.



> **Nota**
>
> Los informes generados en la interfaz web de administración se aplican únicamente al dispositivo local. Para generar y ver informes para la WAN virtual, utilice la interfaz web de Virtual WAN Center.

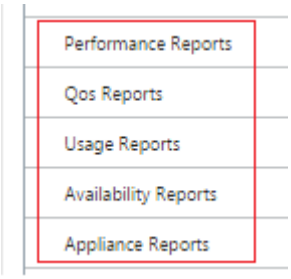
Para generar y ver informes de WAN virtual, haga lo siguiente:

1. Inicie sesión en la interfaz web de administración del MCN y seleccione la ficha **Supervisión**.

   Se abre el árbol de navegación **Supervisión** en el panel izquierdo.

2. Seleccione un tipo de informe del árbol de navegación.

   Los tipos de informe aparecen como sucursales en el árbol de navegación, justo debajo de la sucursal **Flujos**.



Los tipos de informe disponibles son los siguientes:

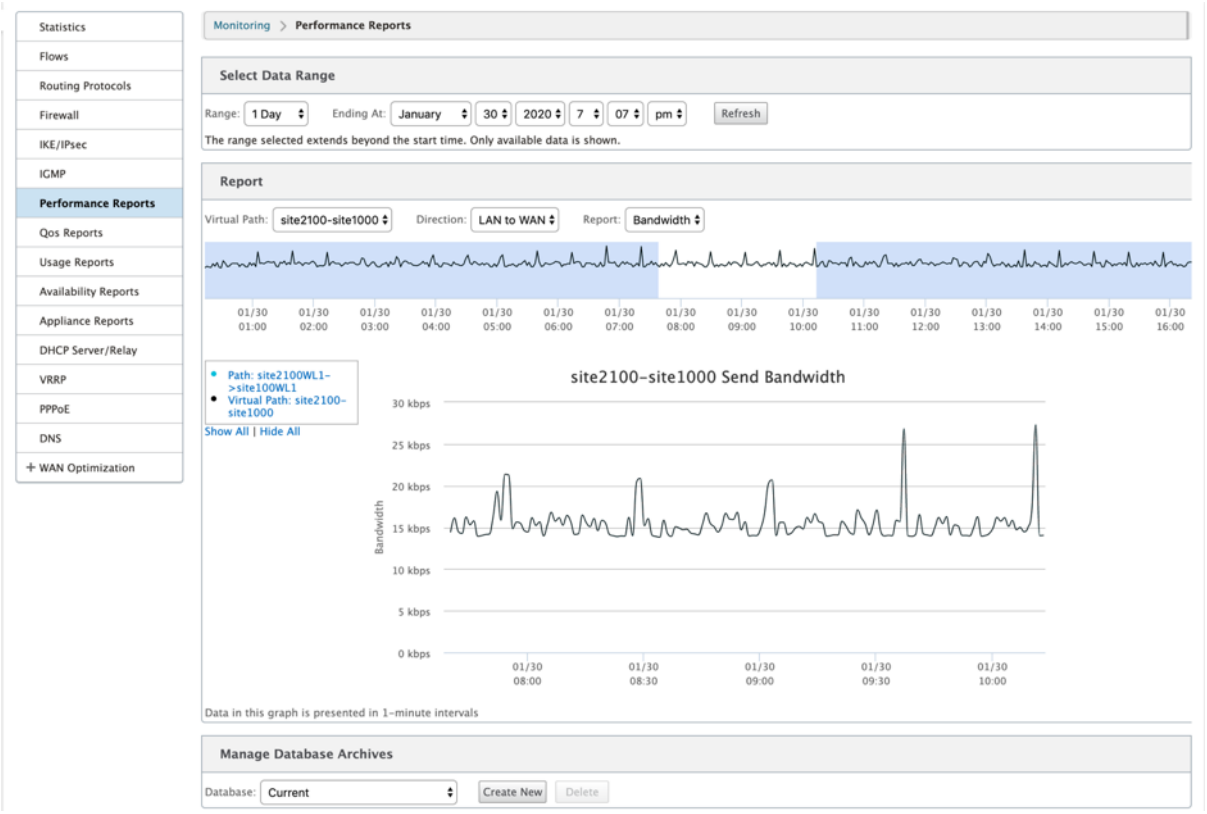
- **Informes de rendimiento**
- **Informes QoS**
- **Informes de uso**
- **Informes de disponibilidad**
- **Informes de dispositivos**

3. Seleccione las opciones de informe.

Además de los diversos tipos de informes, para cada tipo de informe hay numerosas opciones y filtros para refinar los resultados de los informes.

Informes de rendimiento

Citrix SD-WAN puede mostrar estadísticas de rendimiento en el nivel de sitio, ruta virtual o Dirección (LAN a WAN y WAN a LAN). Con Citrix SD-WAN, puede recopilar métricas que muestren la eficiencia de cada vínculo en milisegundos. Para ver más detalles, haga clic con el botón secundario del mouse y seleccione un área específica del marco de ruta o tiempo en la línea del gráfico.

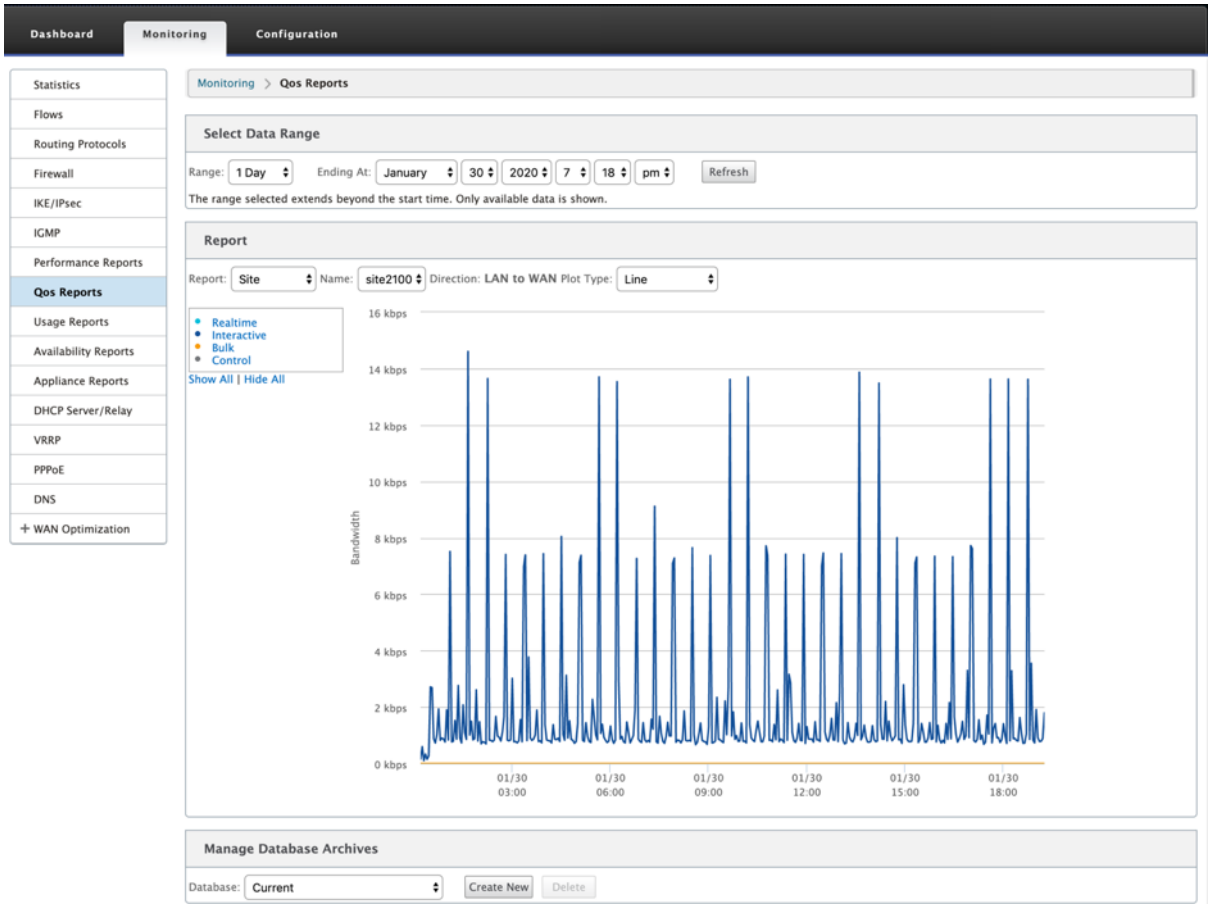


Puede seleccionar el rango de datos según sea necesario con los siguientes campos para ver el informe de rendimiento:

- **Ruta virtual:** seleccione la ruta virtual en la lista desplegable.
- **Dirección:** Seleccione la dirección según sea necesario (LAN a WAN o WAN a LAN).
- **Informe:** Seleccione los siguientes parámetros de red para ver el informe:
  - Ancho de banda
  - Latencia
  - Vibración
  - Pérdida
  - Calidad

Informes QoS

Puede supervisar el informe QoS de la aplicación, como el número de paquetes o bytes cargados, descargados o eliminados en cada nivel de sitio, enlace WAN, ruta virtual y ruta de acceso.

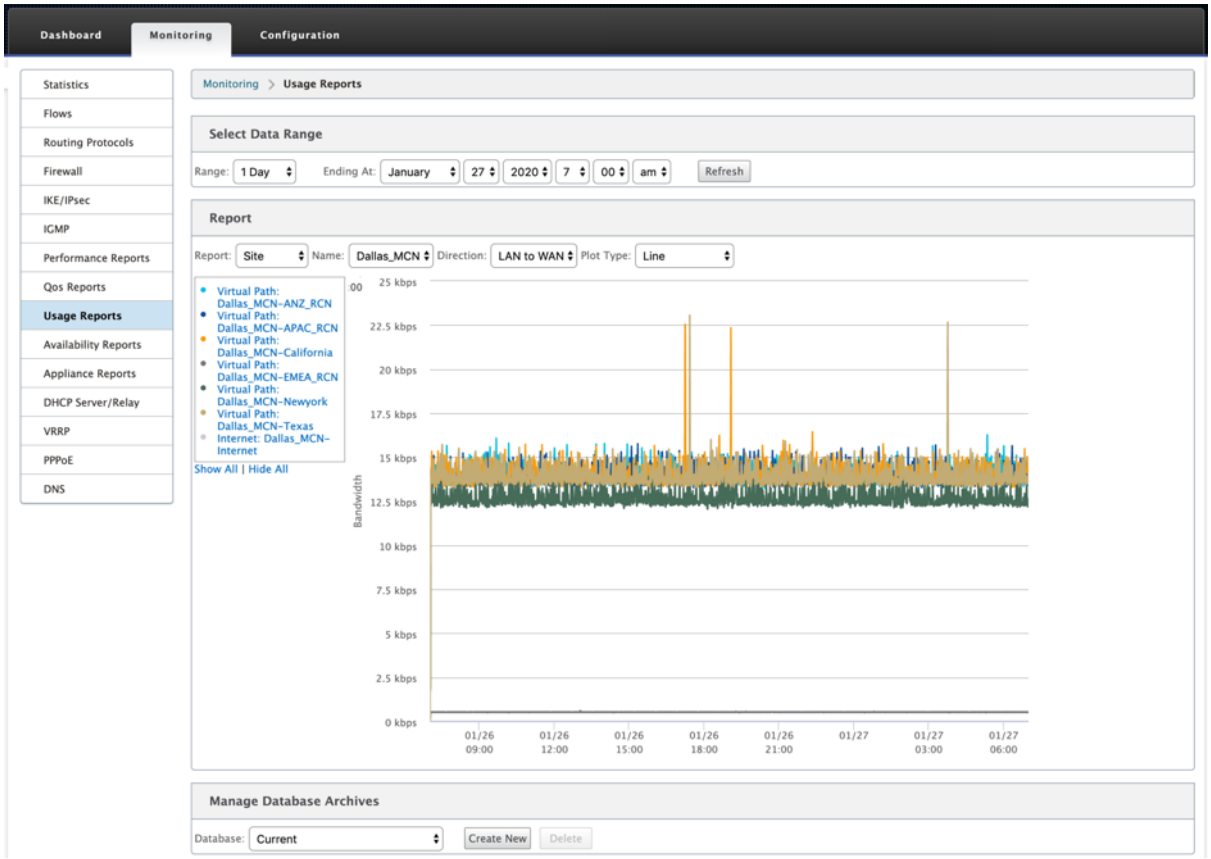


Puede ver las siguientes métricas:

- **Tiempo real:** ancho de banda consumido por las aplicaciones que pertenecen al tipo de clase en tiempo real en la configuración de Citrix SD-WAN. El rendimiento de tales aplicaciones depende en gran medida de la latencia de la red. Un paquete retrasado es peor que un paquete perdido (por ejemplo, VoIP, Skype for Business).
- **Interactivo:** ancho de banda consumido por las aplicaciones que pertenecen al tipo de clase interactiva en la configuración de Citrix SD-WAN. El rendimiento de estas aplicaciones depende en gran medida de la latencia de la red y de la pérdida de paquetes (por ejemplo, XenDesktop, XenApp).
- **Bulk:** Ancho de banda consumido por las aplicaciones que pertenecen al tipo de clase masiva en la configuración de Citrix SD-WAN. Estas aplicaciones implican poca intervención humana y son manejadas principalmente por los propios sistemas (por ejemplo, FTP, operaciones de copia de seguridad).
- **Control:** Ancho de banda utilizado para transferir paquetes de control que contienen información de redirección, programación y estadísticas de vínculos.

Informes de uso

Los informes de uso proporcionan la información de uso de rutas virtuales.

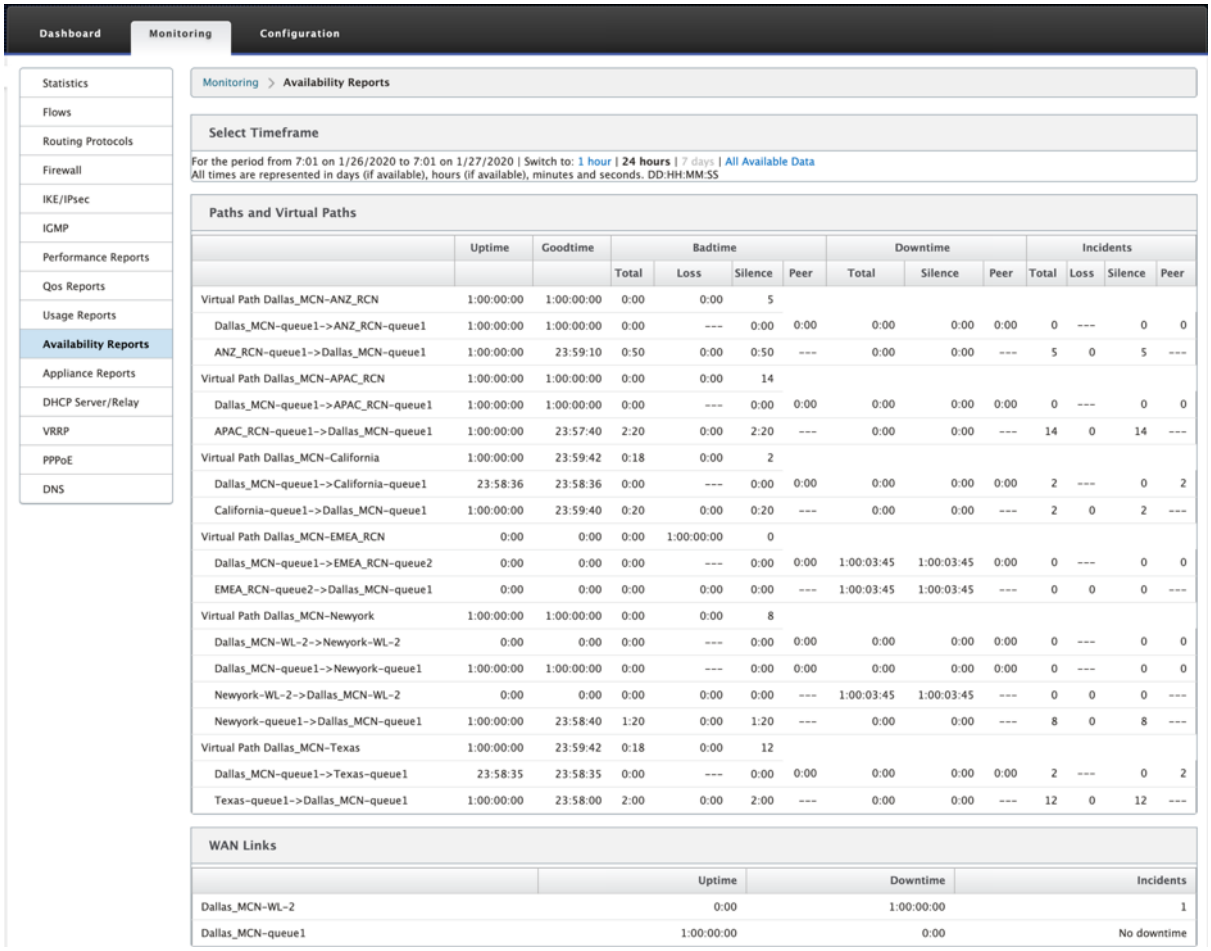


- **Informe:** Seleccione **Sitio** o **Enlace WAN** en la lista desplegable para ver el informe.

- **Nombre:** Seleccione el nombre del sitio o vínculo WAN en la lista desplegable.
- **Dirección:** Seleccione la dirección según sea necesario (LAN a WAN o WAN a LAN).
- **Tipo de trazado:** Seleccione el tipo de trazado en la lista desplegable (Línea o Área).

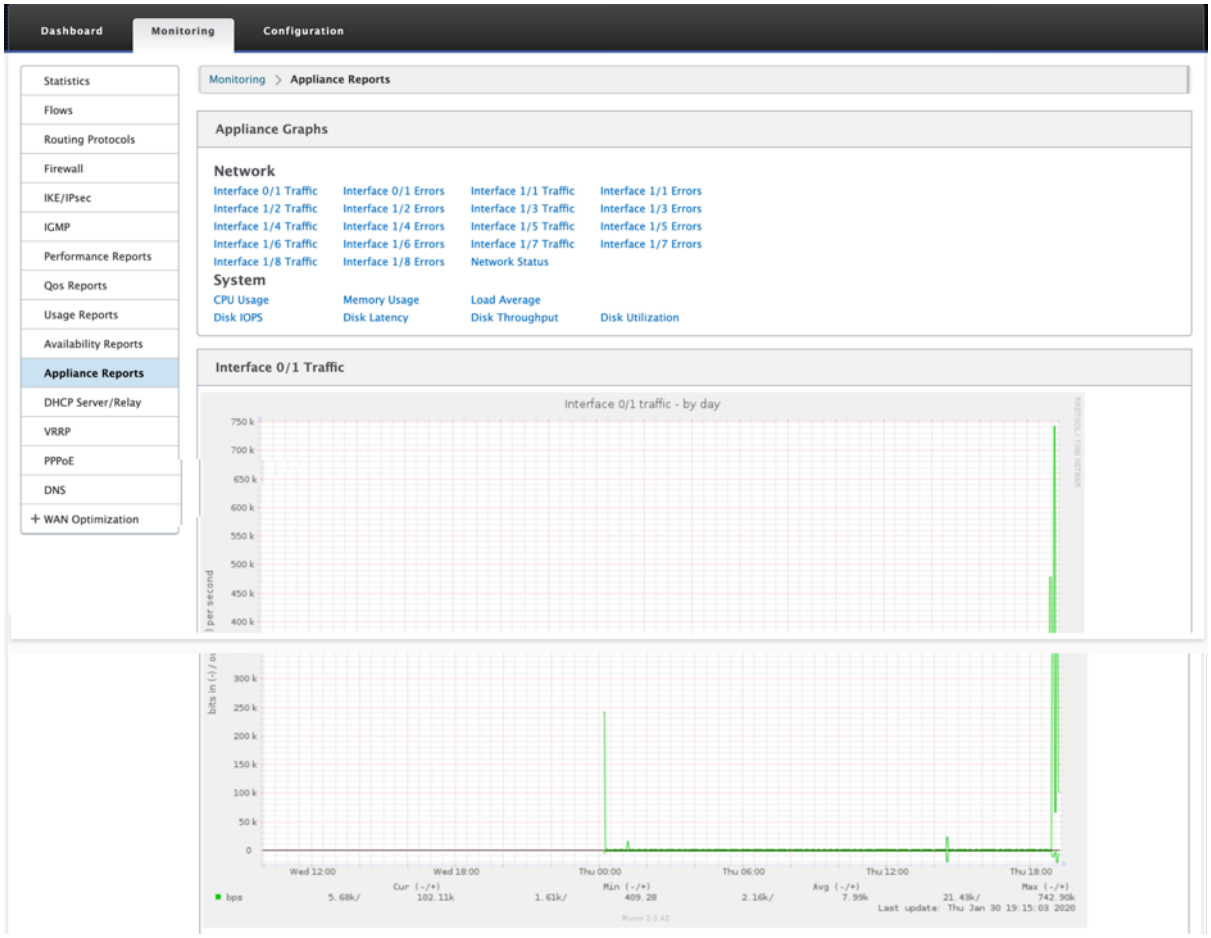
Informes de disponibilidad

En este informe, puede ver los datos de disponibilidad de Vínculos WAN, Rutas de acceso y Rutas virtuales. También puede cambiar o elegir un período de tiempo específico, como 1 hora, 24 horas y 7 días para ver los datos disponibles. Los datos Rutas y Rutas virtuales se representan en formato **DD:HH:MM:SS**.



Informes del dispositivo

El informe del dispositivo proporciona informes de tráfico de red y uso del sistema. Haga clic en cada vínculo para ver o supervisar el gráfico del dispositivo por día, semana, mes y anualmente.



Visualización de estadísticas del firewall

August 26, 2022

Una vez que haya configurado las directivas de firewall y NAT, podrá ver las estadísticas de las conexiones, las directivas del firewall y las directivas NAT como informes. Puede filtrar los informes mediante los distintos parámetros de filtrado.

Para obtener información sobre cómo configurar las directivas de firewall y NAT, consulte Firewall con estado y compatibilidad con NAT.

Para ver estadísticas del firewall:

1. Vaya a **Supervisión** > **Firewall.**
2. Seleccione **Conexiones, Directivas de filtro o Directivas NAT** según sea necesario.
3. Defina los criterios de filtrado según sea necesario.
4. Haga clic en **Actualizar**.

Conexiones

Puede consultar las estadísticas de Aplicaciones para la directiva de firewall. Esto le permite ver todas las conexiones que coinciden con la aplicación seleccionada, de dónde provienen, a dónde van y cuánto tráfico generan. Puede ver cómo actúan las directivas de firewall sobre el tráfico de cada aplicación.

Puede filtrar las estadísticas de conexiones mediante los siguientes parámetros:

- Aplicación: aplicación utilizada como criterio de filtro para la conexión.
- Familia: familia de aplicaciones que se utiliza como criterio de filtro para la conexión.
- Protocolo IP: protocolo IP utilizado por la conexión.
- Zona de origen: zona desde la que se originó la conexión.
- Zona de destino: la zona desde la que se origina el tráfico de respuesta.
- Tipo de servicio de origen: El servicio desde el que se originó la conexión.
- Instancia del servicio de origen: instancia del servicio desde el que se originó la conexión.
- IP de origen: Dirección IP desde la que se originó la conexión, entrada en notación decimal con puntos con una máscara de subred opcional.
- Puerto de origen: puerto o rango de puertos desde el que se originó la conexión. Se acepta un solo puerto o un rango de puertos que utilicen el carácter -.
- Tipo de servicio de destino: servicio del que se origina el tráfico de respuesta.
- Instancia del servicio de destino: instancia del servicio desde el que se origina el tráfico de respuesta.
- IP de destino: La dirección IP del dispositivo de respuesta, entrada en notación decimal con puntos con una máscara de subred opcional.
- Puerto de destino: puerto o rango de puertos utilizado por el dispositivo que responde. Se acepta un solo puerto o un rango de puertos que utilicen el carácter -.

Directivas de filtro

Las directivas permiten especificar acciones para los flujos de tráfico. Los grupos de filtros de firewall se crean mediante plantillas de directivas de firewall y se pueden aplicar a todos los sitios de la red o solo a sitios específicos.

Puede ver el informe de estadísticas de todas las directivas de filtro y filtrarlo mediante los siguientes parámetros.

- Objeto Application: objeto Application utilizado como criterio de filtro en la directiva del firewall.
- Aplicación: la aplicación utilizada como criterio de filtro en la directiva del firewall
- Familia: familia de aplicaciones utilizada como criterio de filtro en la directiva del firewall.
- Protocolo IP: protocolo IP con el que coincide la directiva de filtro.
- DSCP: etiqueta DSCP con la que coincide la directiva de filtro.
- Acción de directiva de filtro: acción que realiza la directiva cuando un paquete coincide con el filtro.
- Tipo de servicio de origen: El servicio desde el que se originó la conexión.
- Nombre del servicio de origen: instancia del servicio desde el que se originó la conexión.
- IP de origen: Dirección IP desde la que se originó la conexión, entrada en notación decimal con puntos con una máscara de subred opcional.
- Puerto de origen: puerto o rango de puertos desde el que se originó la conexión. Se acepta un solo puerto o un rango de puertos que utilicen el carácter -.
- Tipo de servicio de destino: servicio al que se destina el tráfico de respuesta.
- Nombre del servicio de destino: cuando corresponda, el servicio al que se destina el tráfico de respuesta.
- IP de destino: La dirección IP del dispositivo de respuesta, entrada en notación decimal con puntos con una máscara de subred opcional.
- Puerto de destino: puerto o rango de puertos utilizado por el dispositivo que responde. Se acepta un solo puerto o un rango de puertos que utilicen el carácter -.
- Zona de origen: la zona de origen que coincide con la directiva de filtro.
- Zona de destino: la zona de respuesta que coincide con la directiva de filtro.

Directivas NAT

Puede ver las estadísticas de todas las directivas de traducción de direcciones de red (NAT) y filtrar el informe mediante los siguientes parámetros.

- Protocolo IP: protocolo IP que coincide con la directiva NAT.
- Tipo de NAT: el tipo de NAT que utiliza la directiva NAT.
- Tipo de NAT dinámico: el tipo de NAT dinámico que utiliza la directiva NAT.
- Tipo de servicio: tipo de servicio utilizado por la directiva NAT.

- Nombre del servicio: instancia del servicio que utiliza la directiva NAT.
- IP interna: la dirección IP interna, introducida en notación decimal con puntos con una máscara de subred opcional.
- Puerto interior: rango de puertos internos utilizado por la directiva NAT. Se acepta un solo puerto o un rango de puertos que utilicen el carácter -.
- IP externa: la dirección IP externa, introducida en notación decimal con puntos con una máscara de subred opcional.
- Puerto externo: rango de puertos externos utilizado por la directiva NAT. Se acepta un solo puerto o un rango de puertos que utilicen el carácter -.

Diagnóstico

August 26, 2022

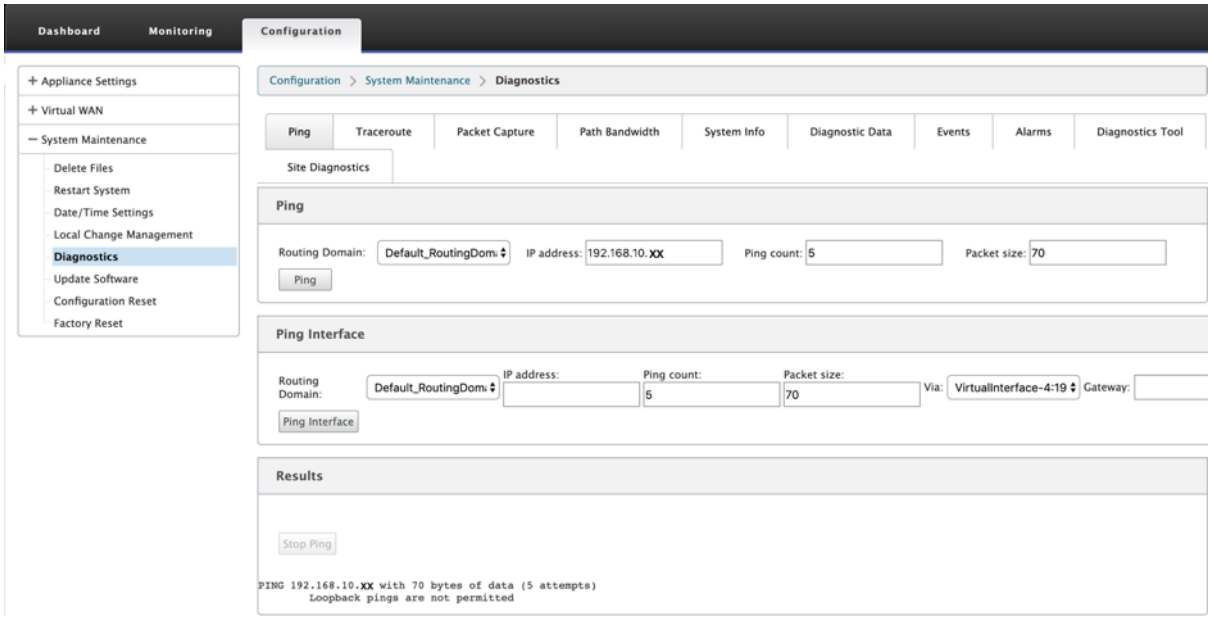
Las utilidades de **diagnóstico de Citrix SD-WAN** ofrecen las siguientes opciones para probar e investigar problemas de conectividad:

- Ping
- Traceroute
- Captura de paquetes
- Ancho de banda path
- Información del sistema
- Datos de diagnóstico
- Eventos
- Alarmas
- Herramienta de diagnóstico
- Diagnóstico del sitio

Las opciones de diagnóstico de **Citrix SD-WAN Dashboard** controlan la recopilación de datos.

Ping

Para utilizar la opción **Ping**, vaya a **Configuración > Diagnóstico** y seleccione **Ping**. Puede utilizar Ping para comprobar la accesibilidad del host y la conectividad de red.

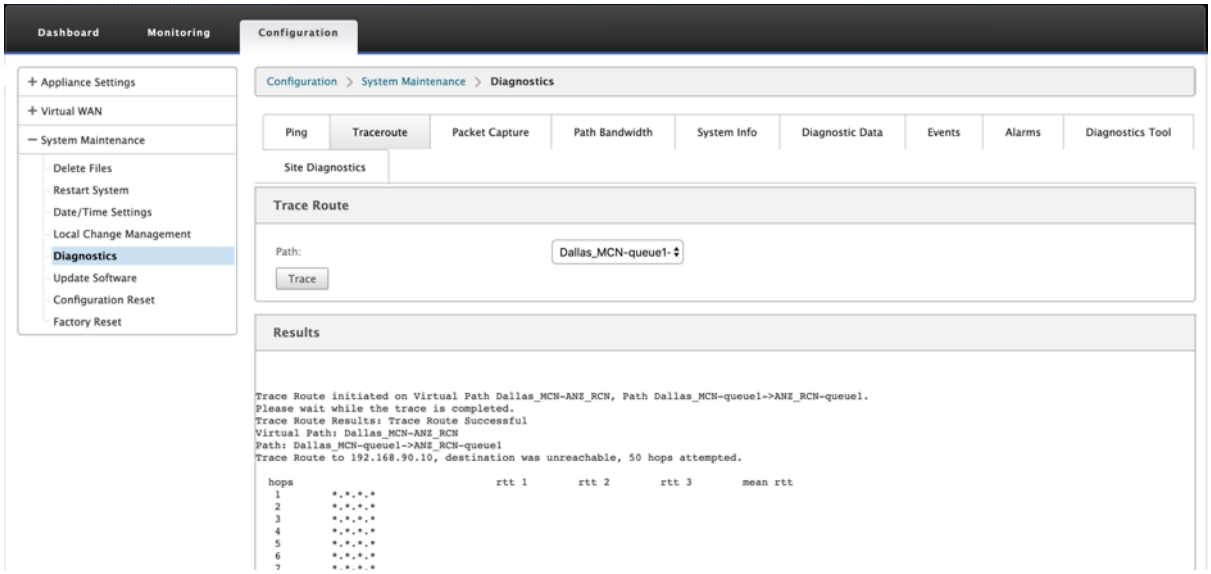


Seleccione el dominio de redirección. Proporcione una dirección IP válida, el número de recuentos de ping (número de veces que se envía la solicitud de ping) y el tamaño del paquete (número de bytes de datos). Haga clic en **Detener ping** para detener una búsqueda de ping en curso.

Puede hacer ping a través de una interfaz específica. Seleccione el dominio de redirección y especifique la dirección IP con el recuento de ping, el tamaño del paquete y seleccione la interfaz virtual en la lista desplegable.

Traceroute

Para utilizar la opción **Traceroute**, vaya a **Configuración > expanda Mantenimiento del sistema > Diagnóstico** y seleccione **Traceroute**.

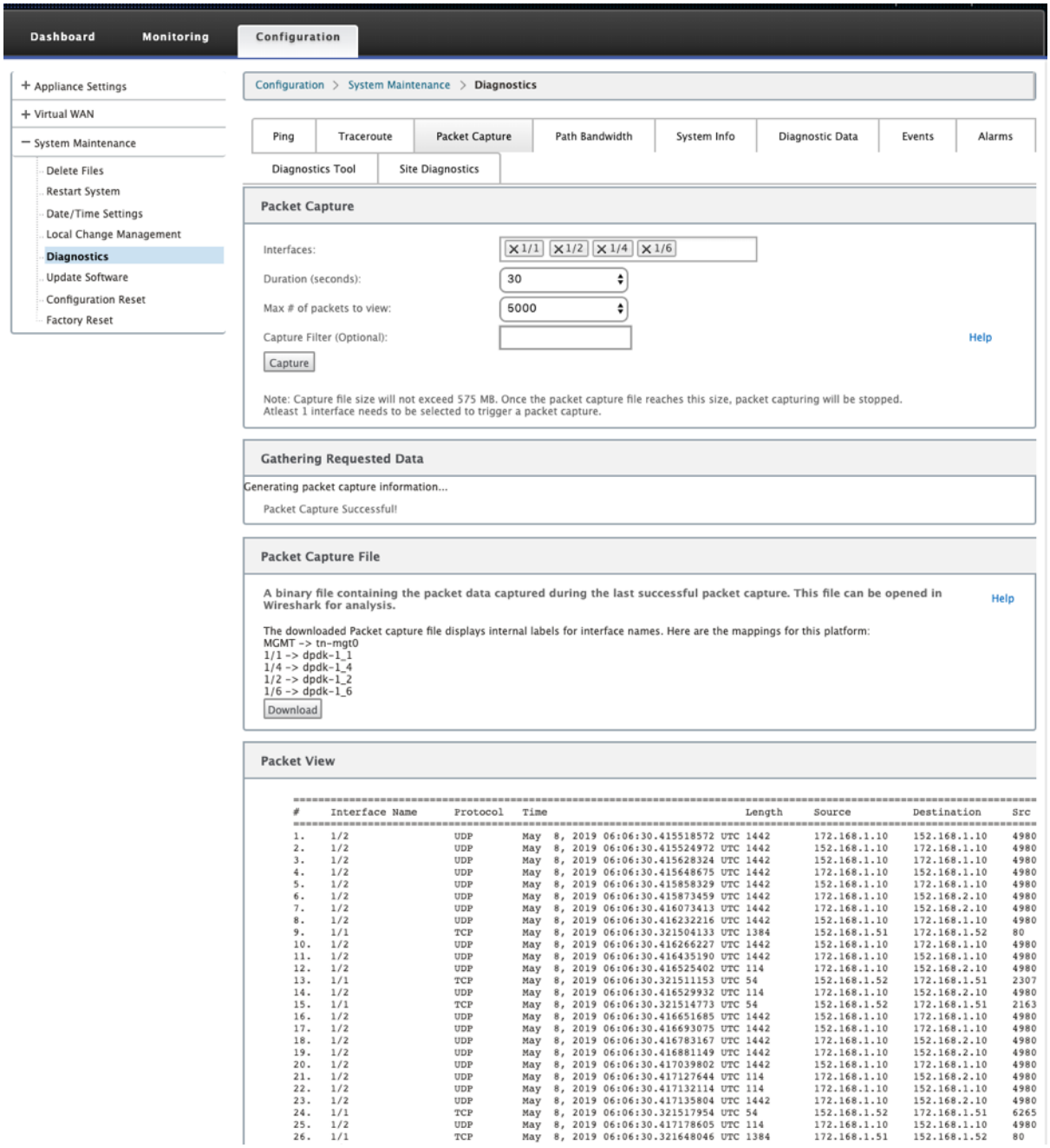


Traceroute ayuda a descubrir y mostrar la ruta o ruta a un servidor remoto. Utilice la opción **Traceroute** como herramienta de depuración para detectar los puntos de fallo de una red.

Seleccione una ruta de la lista desplegable y haga clic en **Rastrear**. Puede ver los detalles en la sección **Resultados**.

Captura de paquetes

Puede utilizar la opción **Captura de paquetes** para interceptar el paquete de datos en tiempo real que atraviesa la interfaz activa seleccionada presente en el sitio seleccionado. La captura de paquetes le ayuda a analizar y solucionar los problemas de la red.



Proporcione las siguientes entradas para la operación de captura de paquetes:

- **Interfaces**: Hay interfaces activas disponibles para la captura de paquetes del dispositivo SD-WAN. Seleccione una interfaz o agregue interfaces en la lista desplegable. Debe seleccionarse al menos una interfaz para activar una captura de paquetes.

  > **Nota:**
  >
  > La capacidad de ejecutar la captura de paquetes en todas las interfaces a la vez ayuda a acelerar la tarea de solución de problemas.

- **Duración (segundos)**: duración (en segundos) durante cuánto tiempo deben capturarse los datos.
- **Cantidad máxima de paquetes a ver**: Límite máximo de paquetes para ver en el resultado de captura de paquetes.
- **Filtro de captura (opcional)**: El campo Filtro de captura opcional acepta una cadena de filtro que se utiliza para determinar qué paquetes se capturan. Los paquetes se comparan con la cadena de filtro y, si el resultado de la comparación es verdadero, se captura el paquete. Si el filtro está vacío, se capturan todos los paquetes. Para obtener más información, consulte Filtros de captura.

A continuación se presentan algunos ejemplos de este filtro de captura:

- **Ether proto\ ARP**: Captura solo paquetes ARP
- **Ether proto\ IP**: Captura solo paquetes IPv4
- **VLAN 100** : captura solo paquetes con una VLAN de 100
- **Host 10.40.10.20**: Captura solo paquetes IPv4 hacia o desde el host con la dirección 10.40.10.20
- **Net 10.40.10.0 Máscara 255.255.255.0**: Captura solo paquetes IPv4 de la subred 10.40.10.0/24
- **IP proto\ TCP**: Captura solo paquetes IPv4/TCP
- **Puerto 80**: Captura solo paquetes IP hacia o desde el puerto 80
- **Intervalo de puertos 20 a 30:** captura solo paquetes IP hacia o desde los puertos 20 a 30

> **Nota**
>
> El límite máximo de tamaño del archivo de captura es de hasta 575 MB. Una vez que el archivo de captura de paquetes alcanza este tamaño, se detiene la captura de paquetes.

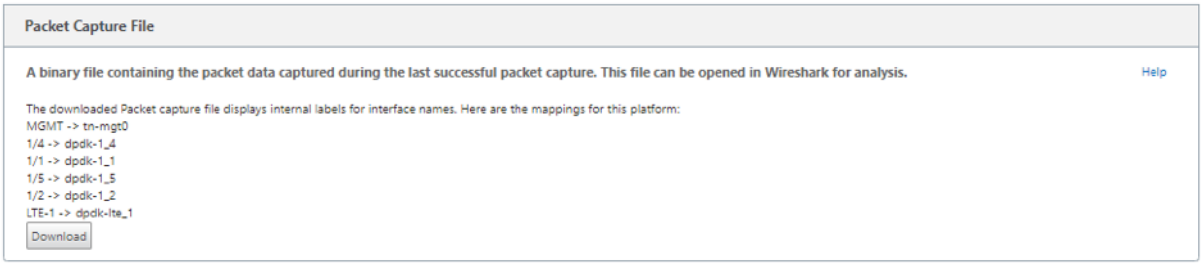
Haga clic en **Capturar** para ver el resultado de la captura de paquetes. También puede descargar un archivo binario que contenga los datos del paquete capturados durante la última captura correcta de paquetes.

Recopilación de datos solicitados

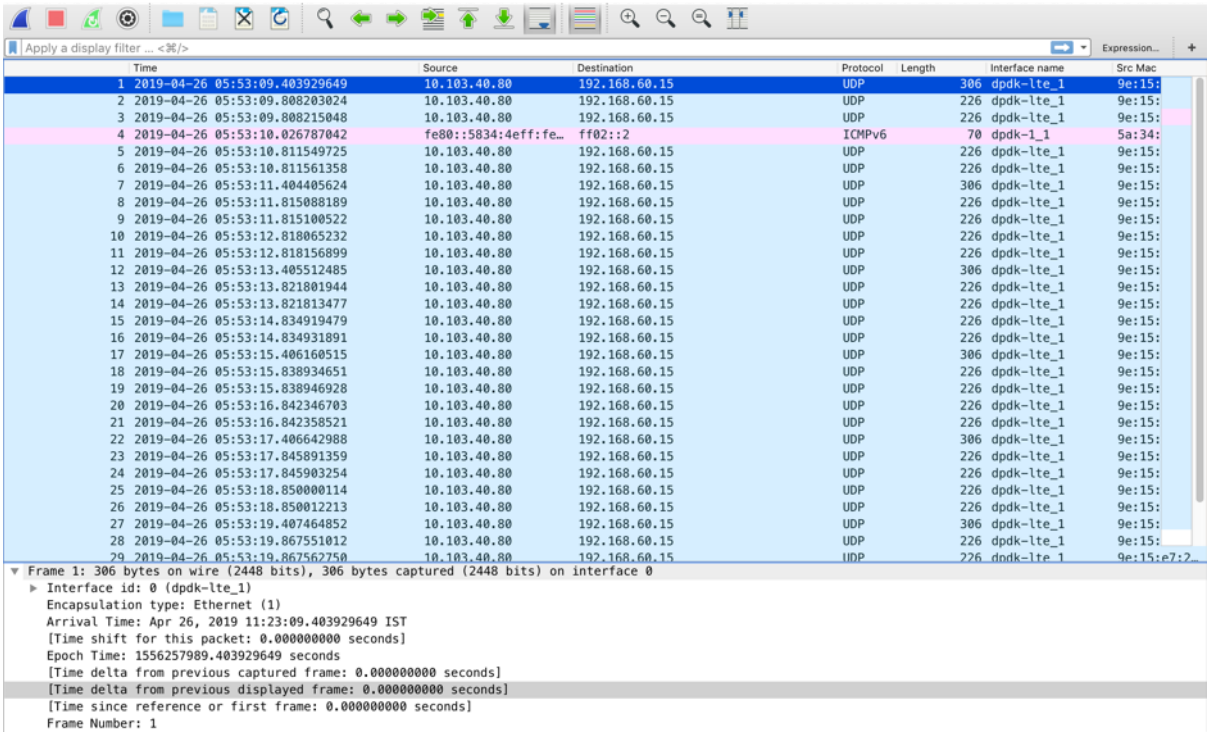
Puede ver el estado de generación de información de captura de paquetes (si la captura de paquetes se realiza correctamente o no se ha capturado ningún paquete) en esta tabla.

Archivo de captura de paquetes

Los paquetes se capturan como datos binarios durante la última captura correcta de paquetes. Puede descargar el archivo binario para analizar la información del paquete sin conexión. El nombre de la interfaz es diferente en el archivo descargado en comparación con la interfaz gráfica de usuario. Para ver la asignación de interfaz interna, haga clic en la opción Ayuda.



Necesita la versión 2.4.13 del software **Wireshark** o posterior para abrir y leer el archivo binario.

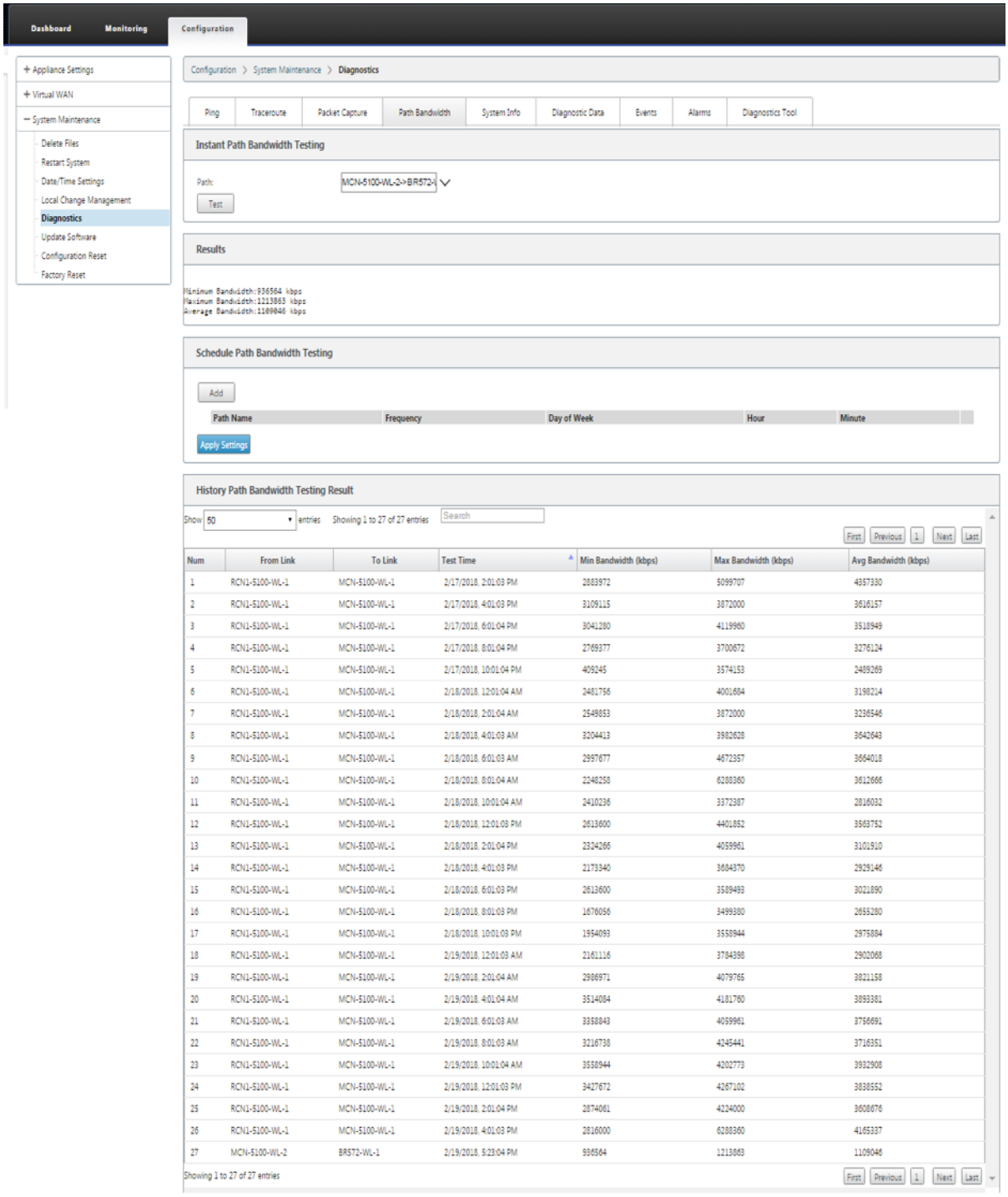


Vista de paquetes

Si el tamaño del archivo de captura de paquetes es mayor, lleva más tiempo completar el proceso de representación de la vista de paquetes. En este caso, se recomienda descargar el archivo y utilizar **Wireshark** para el análisis en lugar de confiar en el resultado de **Vista de paquetes**.

Ancho de banda path

Para utilizar la función **Ancho de banda de ruta**, vaya a **Configuración > expanda Mantenimiento del sistema > Diagnóstico** y seleccione Ancho de **banda de ruta**.



Las pruebas activas de ancho de banda le permiten realizar una prueba instantánea de ancho de banda de path a través de un enlace público de Internet WAN, o programar pruebas de ancho de banda de enlace público de Internet WAN para que se completen en momentos específicos de forma periódica.

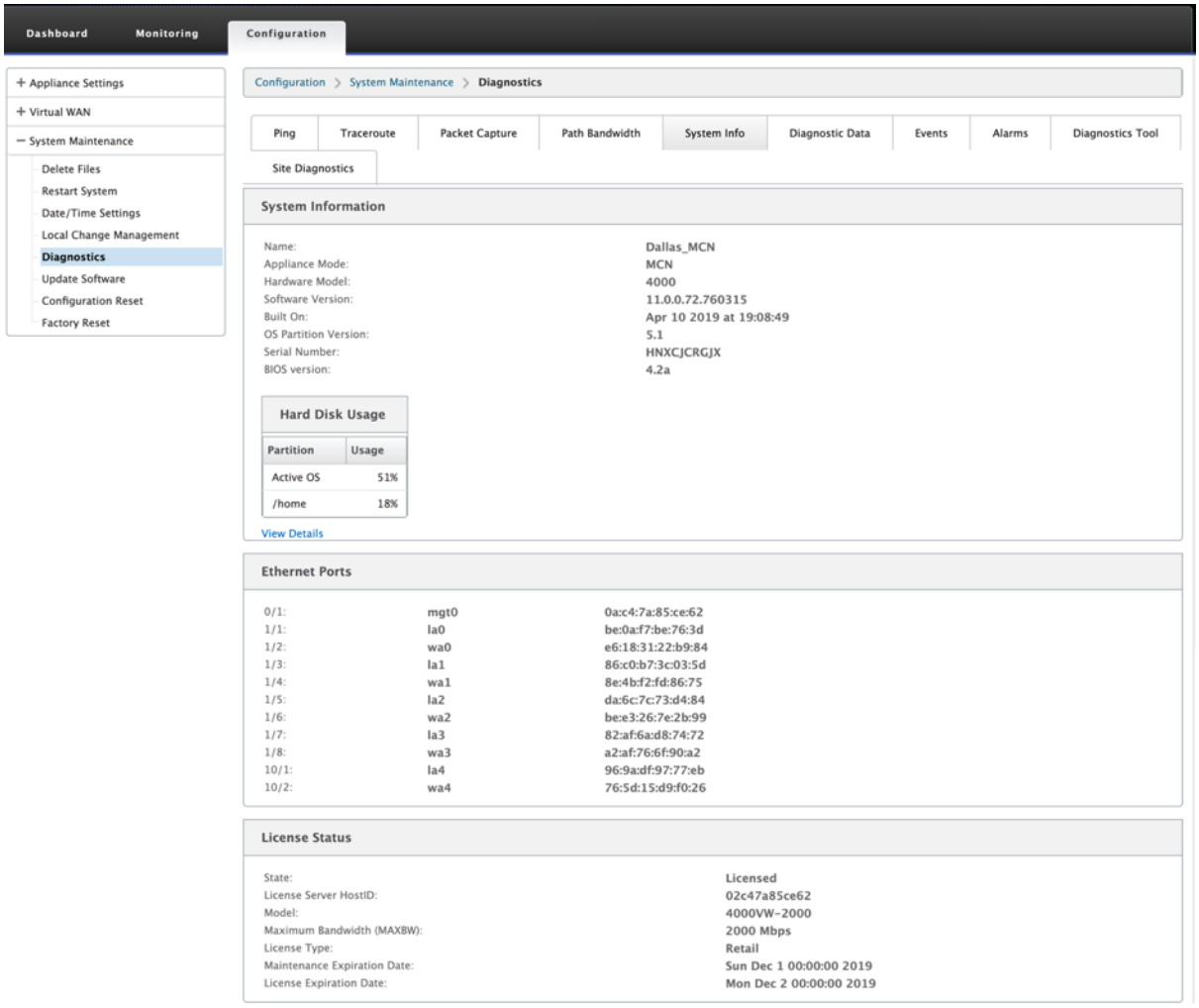
La función **Ancho de banda de ruta** es útil para demostrar cuánto ancho de banda hay disponible

entre dos ubicaciones durante instalaciones nuevas y existentes. Los valores del ancho de banda de ruta indican el ancho de banda máximo posible. Para obtener un ancho de banda permitido preciso, vaya a **Configuración** > **Mantenimiento del sistema** > **Diagnóstico** > **Diagnóstico del sitio** > **Prueba de ancho**de banda. Para obtener más información, consulte Pruebas de ancho de banda activas.

Información del sistema

La página **Información del sistema** proporciona la información del sistema, los detalles de los puertos ethernet y el estado de la licencia.

Para ver la Información del sistema, vaya a **Configuración > expanda Mantenimiento del sistema > Diagnóstico** y seleccione **Información del sistema**.

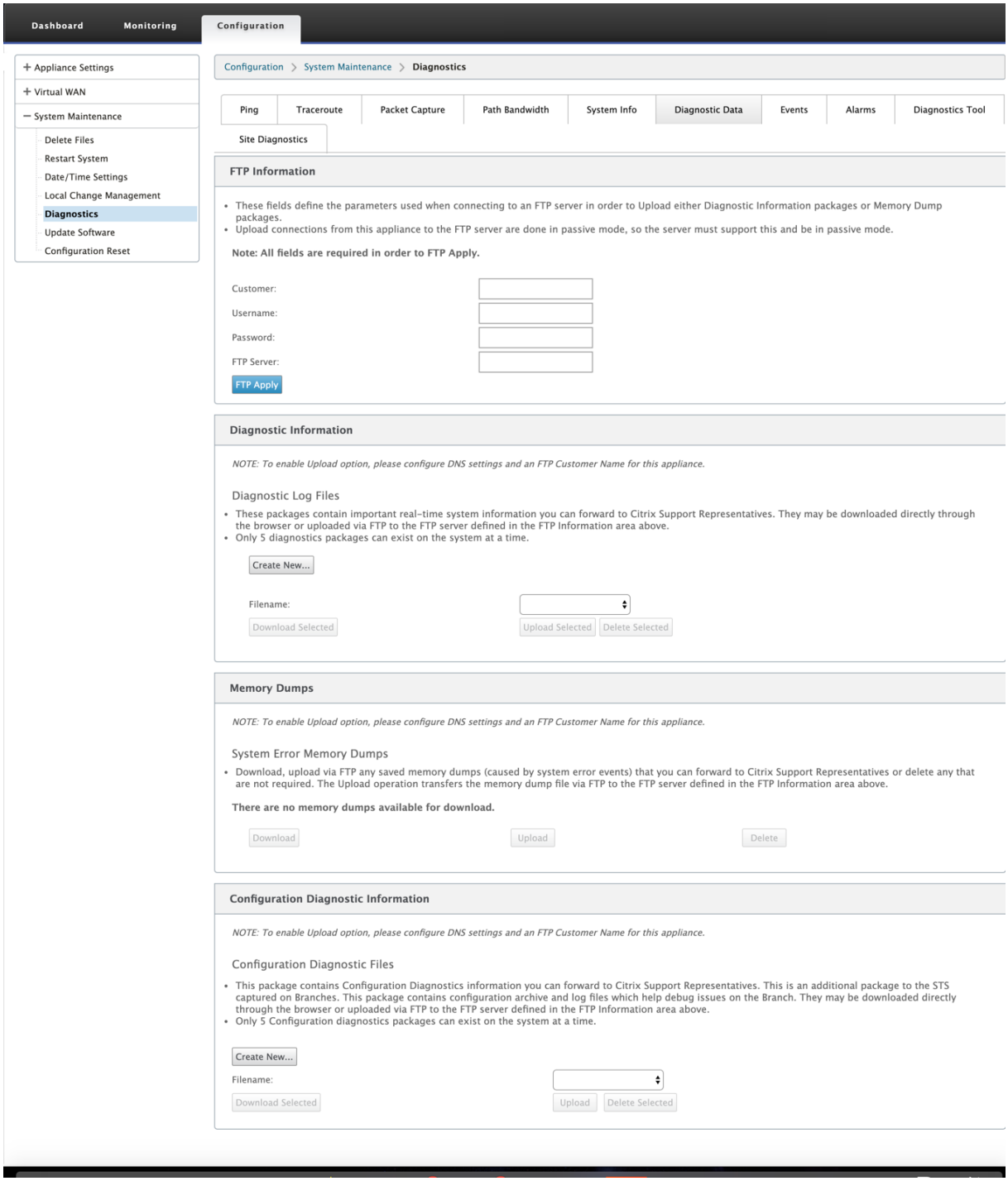


La **información del sistema** muestra todos los parámetros que no están configurados con sus valores predeterminados. Esta información es de solo lectura. Support lo utiliza cuando se sospecha de algún tipo de configuración errónea. Al informar de un problema, es posible que se le pida que compruebes uno o más valores de esta página.

Datos diagnósticos

Los **datos de diagnóstico** le permiten generar un paquete de datos de diagnóstico para que el equipo de asistencia de Citrix lo analice. Puede descargar el paquete **Diagnostics Log Files** y compartirlo con el equipo de asistencia de Citrix.

Para ver los **datos de diagnóstico**, vaya a **Configuración > expanda Mantenimiento del sistema > Diagnóstico** y seleccione **Datos de diagnóstico**.



Los **datos de diagnóstico** incluyen:

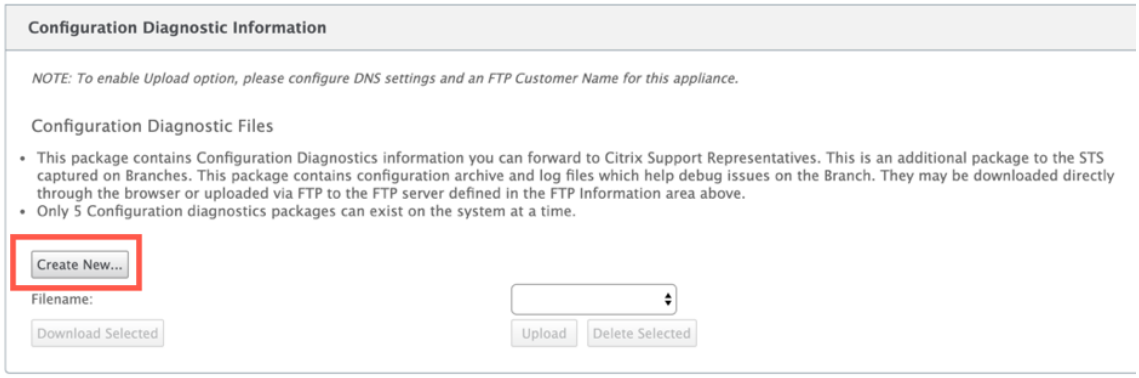
- **Información de FTP**: Proporcione el detalle de los parámetros de FTP y haga clic en **Aplicar FTP**. La información FTP necesaria para conectar un servidor FTP para cargar el paquete de información de diagnóstico.
- **Información de diagnóstico**: El paquete de archivos de registro de diagnóstico contiene infor-

mación del sistema en tiempo real que se puede descargar a través del explorador o cargar por FTP en el servidor FTP.

> **Nota:**
>
> Solo pueden existir cinco paquetes de diagnóstico en el sistema a la vez.

- **Información de diagnóstico de configuración**: En la versión Citrix SD-WAN 11.0, el archivo de configuración de red no estará disponible en la información de diagnóstico recopilada para la sucursal. Para cualquier caso de soporte técnico, proporcione la información de diagnóstico de la sucursal y la información de diagnóstico de configuración desde el nodo de control al que está conectada la sucursal.

  Para recopilar información de diagnóstico de configuración de la GUI del nodo de control, vaya a **Configuración > Mantenimiento del sistema > Diagnóstico > Datos de diagnóstico** > en **Información de diagnóstico de configuración**, haga clic en **Crear nuevo**.

  Al finalizar la creación de la **información de diagnóstico de configuración**, haga clic en **Descargar archivo seleccionado** y proporcione este archivo a Citrix Support O utilice la operación de aplicación FTP disponible en la misma página para FTP este archivo.

- **Volcados de memoria**: Puede descargar o cargar el archivo de volcados de memoria de error del sistema y compartirlo con el equipo de soporte de Citrix. También puede eliminar los archivos si no es necesario.

  > **NOTA:**
  >
  > De forma predeterminada, la opción **Cargar** está desactivada. Para habilitarlo, configure la configuración de **DNS** y un **nombre de cliente FTP** para este dispositivo.

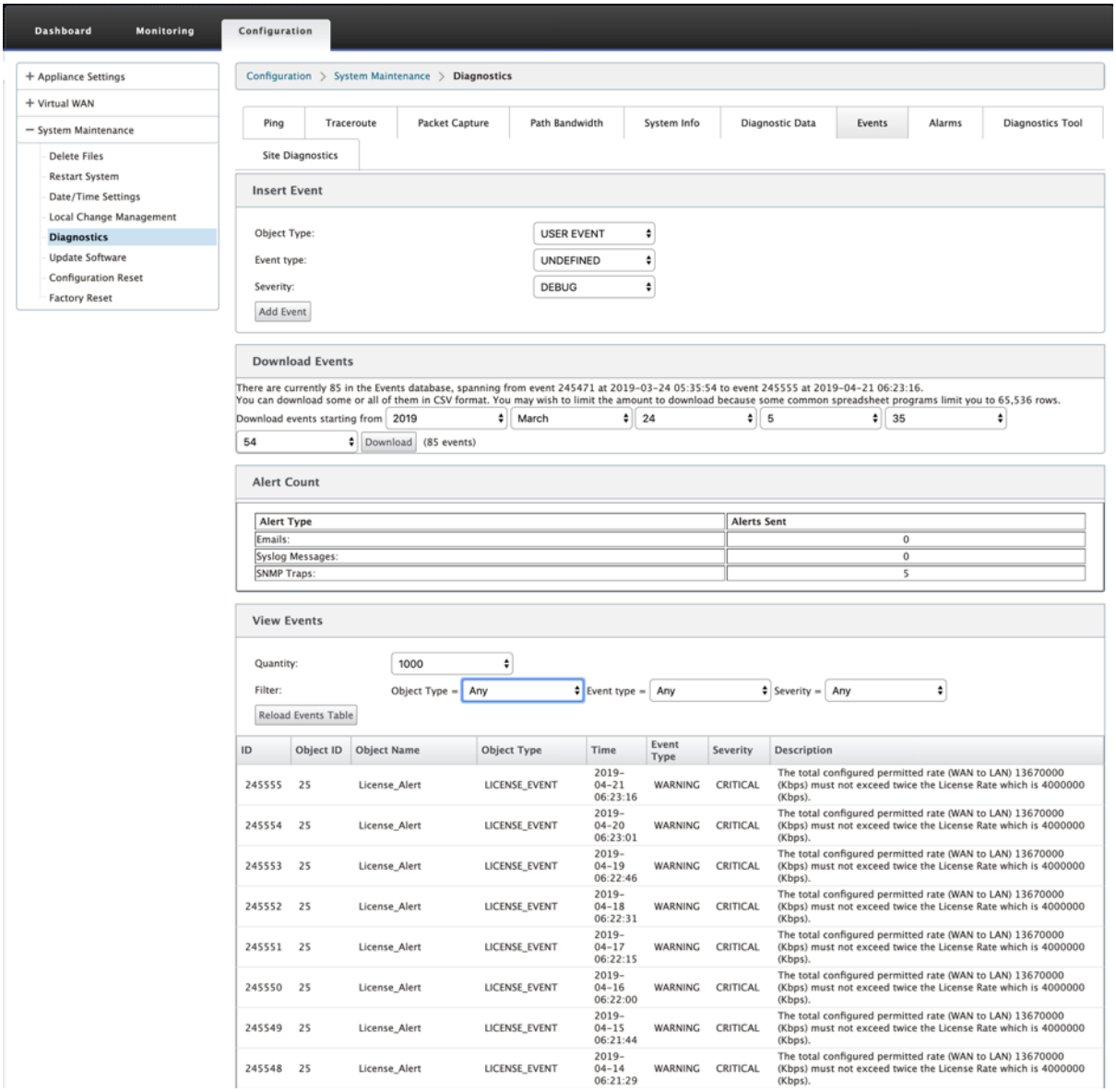
Eventos

Utilice la función **Eventos** para agregar, supervisar y administrar los eventos generados. Ayuda a identificar eventos en tiempo real, lo que le ayuda a solucionar los problemas de inmediato y a mantener

el dispositivo Citrix SD-WAN en funcionamiento de forma eficaz. Puede descargar eventos en formato CSV.

Para agregar un evento, seleccione el tipo de objeto, el tipo de evento y la gravedad de la lista desplegable y haga clic en **Agregar evento**.

Para ver **los eventos**, vaya a **Configuración >** Expanda **Mantenimiento del sistema > Diagnóstico** y seleccione **Eventos**.



Puede configurar Citrix SD-WAN para que envíe notificaciones de eventos de distintos tipos de sucesos como **correos electrónicos, capturas SNMP** o **mensajes de syslog**.

Una vez configurada la configuración de notificación de correo electrónico, SNMP y syslog, puede seleccionar la gravedad de los diferentes tipos de eventos y seleccionar el modo (correo electrónico, SNMP, syslog) para enviar notificaciones de eventos.

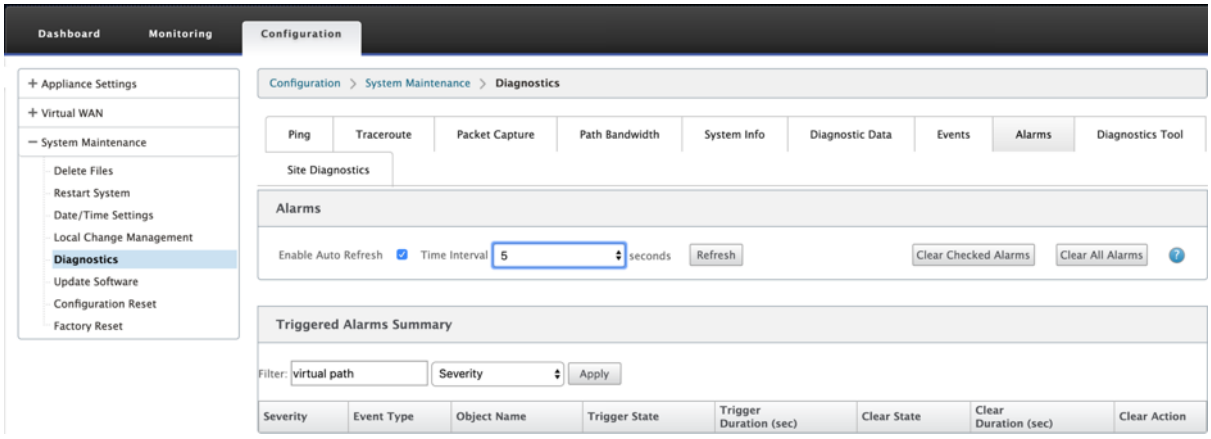
Las notificaciones se generan para eventos iguales o superiores al nivel de gravedad especificado para el tipo de evento.

Puede ver el detalle de los eventos en la tabla **Ver eventos**. Los detalles del evento incluyen la siguiente información.

- **ID:** ID de evento.
- **ID de objeto**: ID del objeto que genera el evento.
- **Nombre del objeto**: Nombre del objeto que genera el evento.
- **Tipo de objeto**: Tipo de objeto que genera el evento.
- **Hora**: La hora en que se generó el evento.
- **Tipo de evento**: Estado del objeto en el momento del evento.
- **Gravedad**: Nivel de gravedad del evento.
- **Descripción**: Descripción textual del evento.

Alarmas

Puede ver y borrar la alarma activada. Para ver **Alarmas**, vaya a **Configuración > expanda Mantenimiento del sistema > Diagnósticos**y seleccione **Alarmas**.



Seleccione las alarmas que quiera borrar y haga clic en **Borrar alarmas marcadas** o haga clic en **Borrar todas las alarmas** para borrar todas las alarmas.

Puede ver el siguiente resumen de todas las alarmas activadas:

- **Gravedad**: La gravedad se muestra en las alertas enviadas cuando se activa o borra la alarma y en el resumen de la alarma activada.
- **Tipo de evento**: El dispositivo SD-WAN puede activar alarmas para subsistemas u objetos concretos de la red. Estas alarmas se denominan tipos de eventos.
- **Nombre del objeto**: Nombre del objeto que genera el evento.
- **Estado de activación**: Estado del evento que activa una alarma para un tipo de evento.

- **Duración del disparador (s)**: La duración en segundos determina la rapidez con la que el dispositivo activa una alarma.
- **Borrar estado**: Estado de evento que borra una alarma para un tipo de evento después de que se activa la alarma.
- **Duración de borrado (s)**: La duración en segundos determina cuánto tiempo esperar antes de borrar una alarma.
- **Acción clara**: Acción que se realiza al borrar las alarmas.

Herramienta de diagnóstico

La **herramienta de diagnóstico** se utiliza para generar tráfico de prueba que le permite solucionar problemas de red que podrían dar lugar a:

- Cambio frecuente en el estado de la ruta de Bueno a Malo.
- Rendimiento deficiente de las aplicaciones
- Mayor pérdida de paquetes

En la mayoría de los casos, estos problemas surgen debido a la limitación de velocidad configurada en el firewall y el enrutador, la configuración incorrecta del ancho de banda, la velocidad de enlace baja, la cola de prioridad establecida por el proveedor de red, etc. La herramienta de diagnóstico le permite identificar la causa raíz de tales problemas y solucionarlo.

La herramienta de diagnóstico elimina la dependencia de herramientas de terceros, como iPerf, que debe instalarse manualmente en los hosts del centro de datos y de sucursal. Proporciona más control sobre el tipo de tráfico de diagnóstico enviado, la dirección en la que fluye el tráfico de diagnóstico y la ruta en la que fluye el tráfico de diagnóstico.

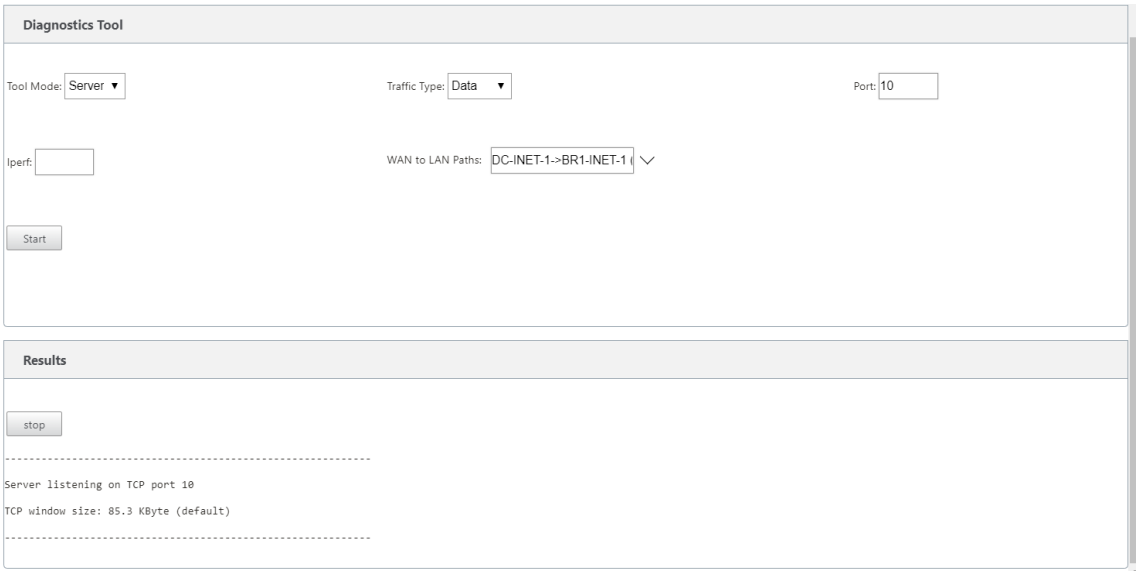
La herramienta de diagnóstico permite generar los dos tipos de tráfico siguientes:

- **Control**: Genera tráfico sin que se aplique la calidad de servicio/programación a los paquetes. Como resultado, los paquetes se envían a través de la ruta seleccionada en la interfaz de usuario, incluso si la ruta no es la mejor en ese momento. Este tráfico se utiliza para probar rutas específicas y ayuda a identificar problemas relacionados con el ISP. También puede usar esto para determinar el ancho de banda de la ruta seleccionada.
- **Datos**: Simula el tráfico generado desde el host con el procesamiento del tráfico de SD-WAN. Dado que la calidad del servicio/programación se aplica a los paquetes, los paquetes se envían por la mejor ruta disponible en ese momento. El tráfico se envía a través de varias rutas si el equilibrio de carga está habilitado. Este tráfico se utiliza para solucionar problemas relacionados con QOS/Scheduler.

> **Nota**
>
> Para ejecutar una prueba de diagnóstico en una ruta, debe iniciar la prueba en los dispositivos en ambos extremos del trayecto. Inicie la prueba de diagnóstico como servidor en un dispositivo y como cliente en el otro dispositivo.

Para utilizar la herramienta de diagnóstico:

1. En ambos dispositivos, haga clic en **Configuración** > **Mantenimiento del sistema** > **Diagnóstico> Herramienta**de diagnóstico.



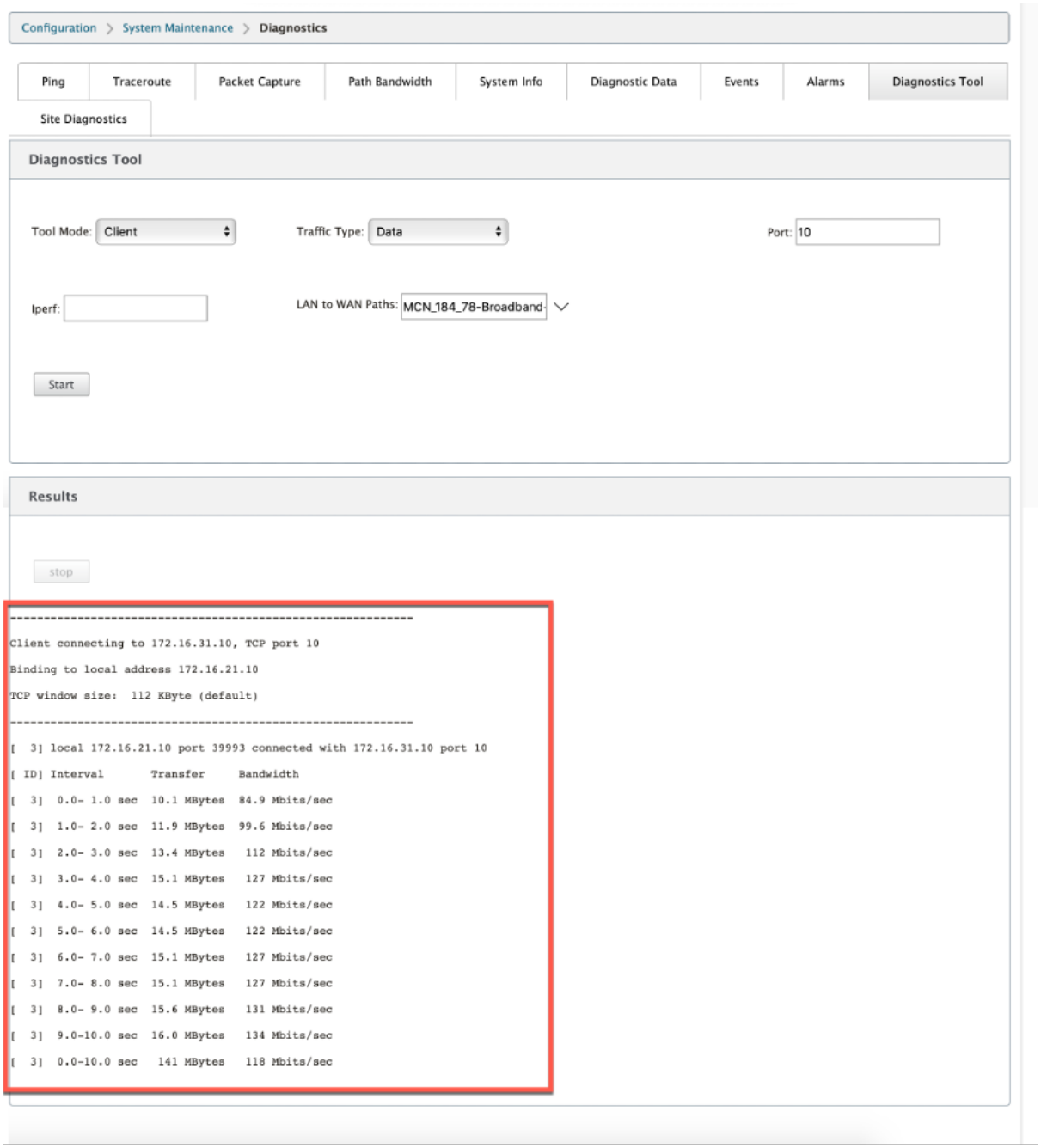
2. En el campo **Modo de herramienta**, seleccione **Servidor** en un dispositivo y seleccione **Cliente** en el dispositivo que reside en el extremo remoto de la ruta seleccionada.
3. En el campo **Tipo de tráfico**, seleccione el tipo de tráfico de diagnóstico, **Control** o **Datos**. Seleccione el mismo tipo de tráfico en ambos dispositivos.
4. En el campo **Puerto**, especifique el número de puerto **TCP/UDP** al que se envía el tráfico de diagnóstico. Especifique el mismo número de puerto en ambos dispositivos.
5. En el campo **Iperf**, especifique las opciones de línea de comandos de IPERF, si las hubiera.

   > **Nota**
   >
   > No es necesario especificar las siguientes opciones de línea de comandos de IPERF:
   >
   > - -c: La herramienta de diagnóstico agrega la opción de modo cliente.
   > - -s: La herramienta de diagnóstico agrega la opción de modo servidor.
   > - -B: La herramienta de diagnóstico realiza el enlace de IPERF a una IP/interfaz específica en función de la ruta seleccionada.
   >   - -p: El número de puerto se proporciona en la herramienta de diagnóstico.

> - -i: Intervalo de salida en segundos.
> - -t: Duración total de la prueba en segundos.

6. Seleccione las rutas de WAN a LAN a las que quiere enviar el tráfico de diagnóstico. Seleccione la misma ruta en ambos dispositivos.
7. Haga clic en **Inicio** en ambos dispositivos.

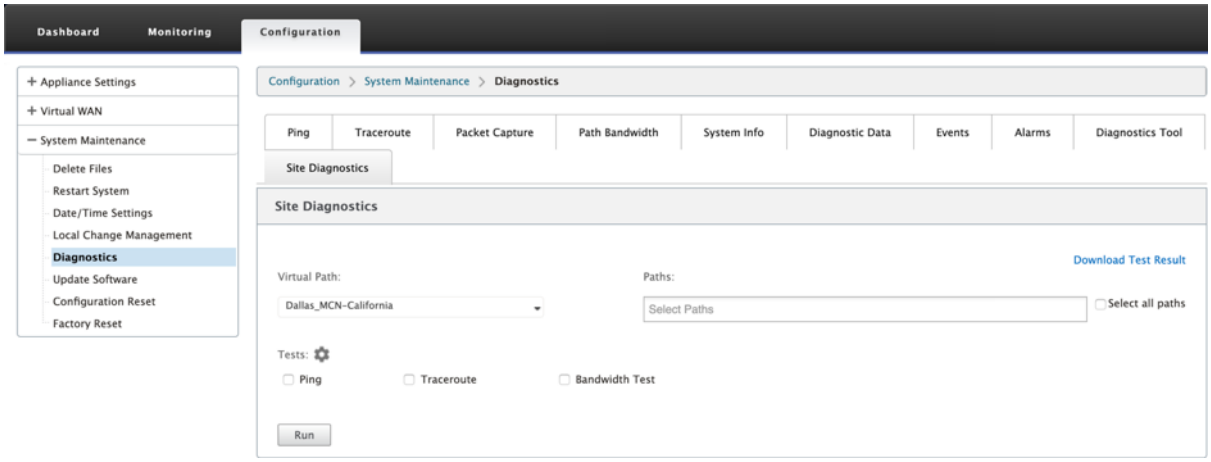
El resultado muestra el modo (cliente o servidor) del dispositivo seleccionado y el puerto TCP o UDP en el que se realiza la prueba. Muestra periódicamente los datos transferidos y el ancho de banda utilizado durante el intervalo especificado hasta que se alcanza la duración total de la prueba.



Diagnóstico del sitio

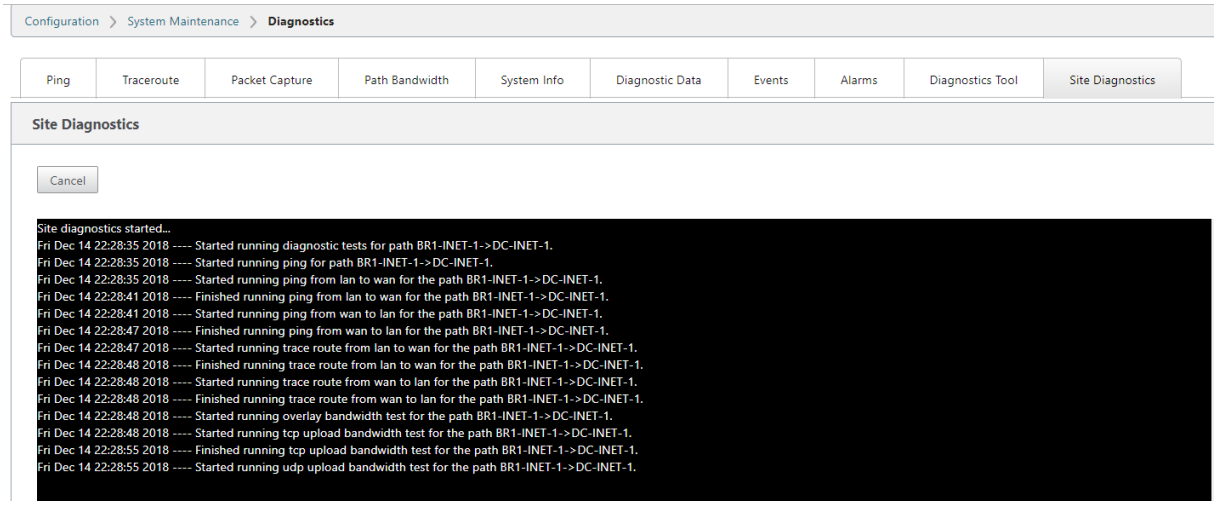
Puede probar el uso del ancho de banda, hacer ping y realizar traceroute para los vínculos WAN configurados en diferentes sitios de la red Citrix SD-WAN. Proporciona información que ayuda a solucionar problemas en la configuración existente.

Para utilizar **Diagnóstico del sitio**, vaya a **Configuración >** expanda **Mantenimiento del sistema > Diagnóstico** y seleccione **Herramienta de diagnóstico**.



La sección de resultados muestra lo siguiente:

- **Estado de la interfaz**: Proporciona el nombre de la interfaz, el número de zonas de firewall asociadas a la interfaz, el identificador de VLAN y sus puertos asociados.
- **Estado de ruta**: Proporciona los detalles de la IP privada de destino, la IP de puerta de enlace, la IP pública de destino, la IP de socio y las direcciones IP públicas de socios. También muestra el estado del ARP de Gateway y la MTU de ruta.
- **Resultado del ping**: Proporciona la dirección, el estado, el recuento (incluido el número de intentos y fallos) y el RTT del ping.
- **Resultado de Traceroute**: Proporciona la dirección, el estado, el número de saltos y la dirección IP o RTT de los saltos.
- **Resultado de ancho de banda**: Proporciona el estado de TCP y UDP junto con el ancho de banda utilizado (en kbps) para la red superpuesta y subyacente. En comparación con UDP, el ancho de banda utilizado por TCP es mayor, porque UDP se basa en el ancho de banda y, por lo tanto, usa solo el ancho de banda configurado TCP es un protocolo de aceleración; según la configuración de red subyacente, el uso puede registrar un ancho de banda mayor en comparación con el ancho de banda configurado.



Asignación de rutas y uso de ancho de banda mejorados

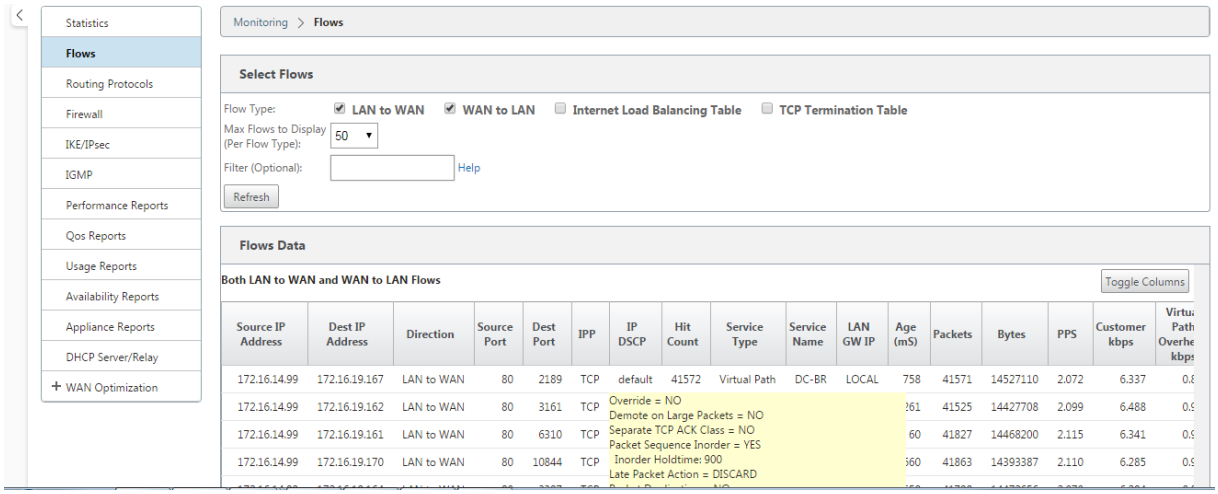
August 26, 2022

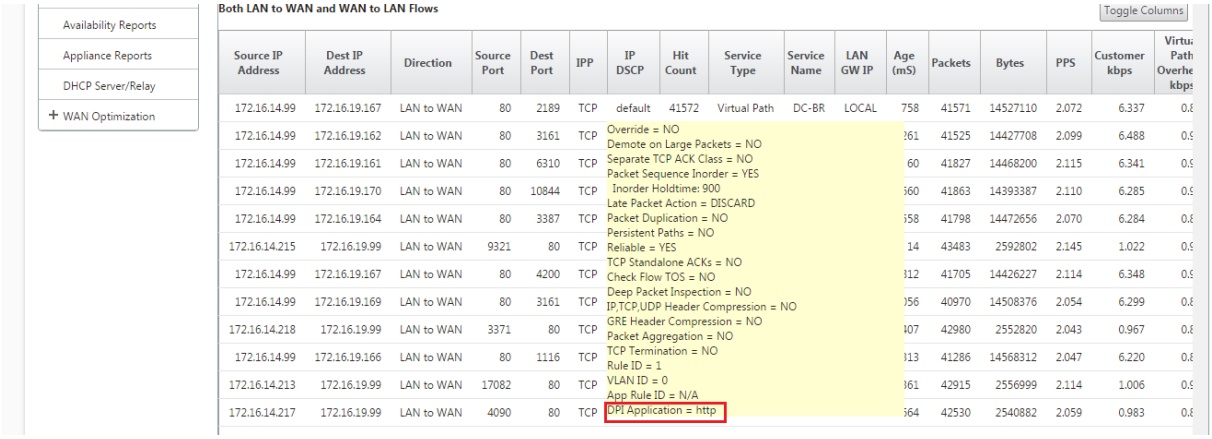
Las mejoras en la asignación de rutas y el uso del ancho de banda se implementan en la ficha Supervisión para mostrar los flujos de tráfico. Por ejemplo, cuando solo una ruta virtual sirve a una conexión de red y si esa ruta virtual se vuelve inactiva, se elige una nueva mejor ruta y la ruta inicial se convierte en la última mejor ruta. Este caso se implementa cuando la demanda de ancho de banda es menor y cuando solo se elige una ruta

Cuando hay más de una ruta virtual que atiende una conexión, observa una mejor ruta actual y la siguiente mejor ruta, si está disponible. Si solo existe una ruta para procesar el tráfico, suponiendo que hay más de dos rutas de procesamiento del tráfico y que la tabla de rutas se actualiza con dos rutas, la ficha Supervisión de la GUI de SD-WAN para flujos mostrará la mejor ruta actual como primera ruta y la siguiente ruta separada por comas como la última mejor ruta. Este caso se implementa cuando se necesitan más paths con demanda de ancho de banda.

Supervisión de la información de aplicaciones de PPP en la GUI de SD-

El nombre del objeto de aplicación PPP del flujo de supervisión se almacena y muestra en la página **Supervisión** de GUI de SD-WAN -> **Flujos**. Se muestra una descripción emergente para identificar la aplicación de PPP.





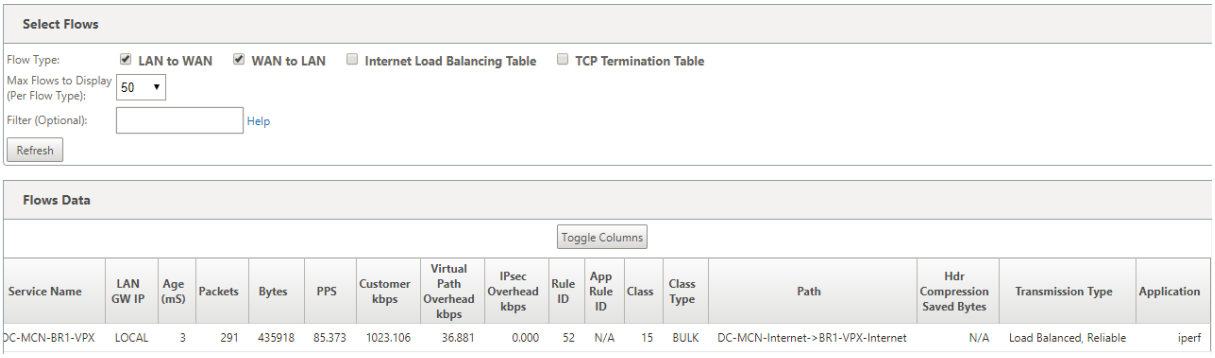
Información de ruta de supervisión para el flujo de tráfico en la GUI de SD-WAN

Es posible que, en función de la velocidad de tráfico entrante que exige ancho de banda, se necesiten uno o más paths para procesar el tráfico.

Para determinar cómo se realiza la asignación de rutas, revise los siguientes casos:

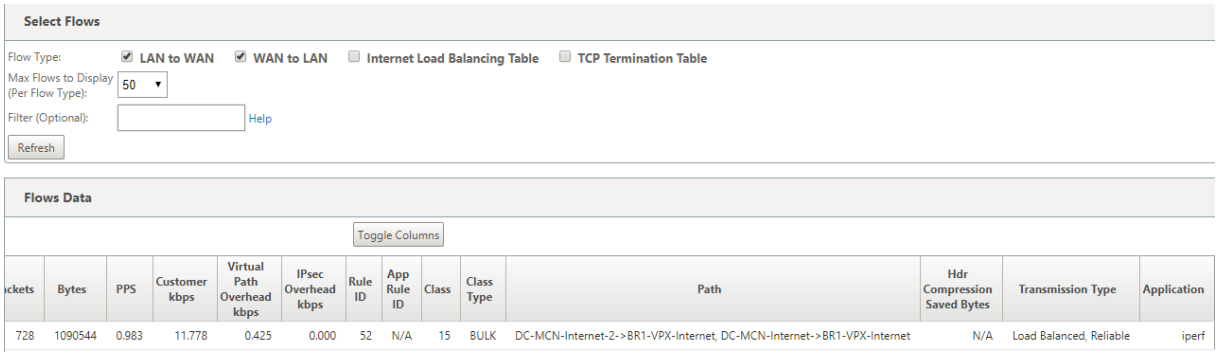
Modo de transmisión equilibrada de carga:

La siguiente ilustración ilustra el caso en el que se inicia el tráfico y todas las rutas son correctas, se elige una mejor ruta porque la demanda de ancho de banda es suficiente para ser atendida por una ruta. Observa que solo se elige una ruta **DC-MCN-Internet** -> **BR1-VPX-Internet** y el tipo de transmisión se muestra como **Equilibrado de carga.**



En la siguiente ilustración se muestra cuándo fluye el tráfico y se degradan los atributos WAN de la ruta, observa que se elige una nueva ruta para procesar el tráfico sin interrupciones. En este caso, la función de asignación de rutas le permite indicar que la mejor ruta actual que procesa el tráfico es **DC-MCN-Internet2 -> BR1-VPX-Internet** y la última mejor ruta que procesó el tráfico es **DC-MCN-Internet -> BR1-VPX-Internet**.

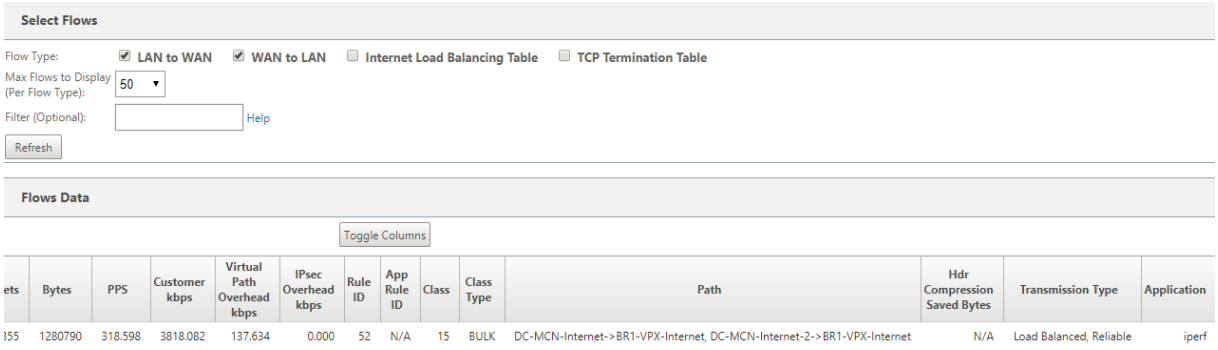
La última mejor ruta de este ejemplo es un indicador de qué ruta sirvió antes a la conexión.



La siguiente ilustración ilustra que cuando el tráfico está en curso y se elige más de una ruta para el procesamiento del tráfico debido a la demanda de ancho de banda, como se muestra a continuación, se elige más de una ruta cuando se envía el tráfico. A diferencia del caso anterior, aquí puede haber más de dos rutas que también sirven al tráfico, pero en la GUI solo se muestran las dos mejores rutas que actualmente sirven al tráfico.

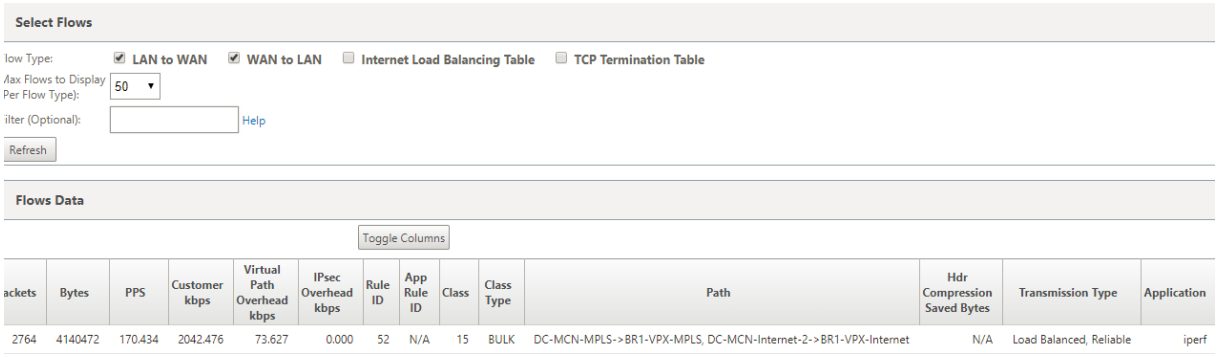
Observe que **DC-MCN-Internet->BR1-VPX-Internet**, **DC-MCN-Internet2->BR1-VPX-Internet** son las dos rutas que se muestran en la tabla **Flujos de datos**.

> **Nota**
>
> Como se indica, solo se muestran dos rutas como máximo en la tabla de flujos.



La siguiente ilustración ilustra que cuando el tráfico sigue fluyendo, si la mejor ruta actual, que es **DC-MCN-Internet->BR1-VPX-Internet**, no está disponible/inactiva/está degradada en los atributos WAN, la mejor ruta seleccionada aparecerá primero en la sección de ruta de acceso de la tabla de **datos de flujos** seguida por la última mejor ruta que sirve al tráfico.

Dado que el **DC-MCN-Internet->BR1-VPX-Internet** ya no era el mejor, el sistema eligió una nueva mejor ruta actual como **DC-MCN-MPLS->BR1-VPX-MPLS**, y la última mejor ruta que sirve activamente la conexión junto con la mejor ruta actual es **DC-MCN-Internet2->BR1-VPX-Internet** ya que ambos son necesarios para la demanda actual de tráfico de ancho de banda.



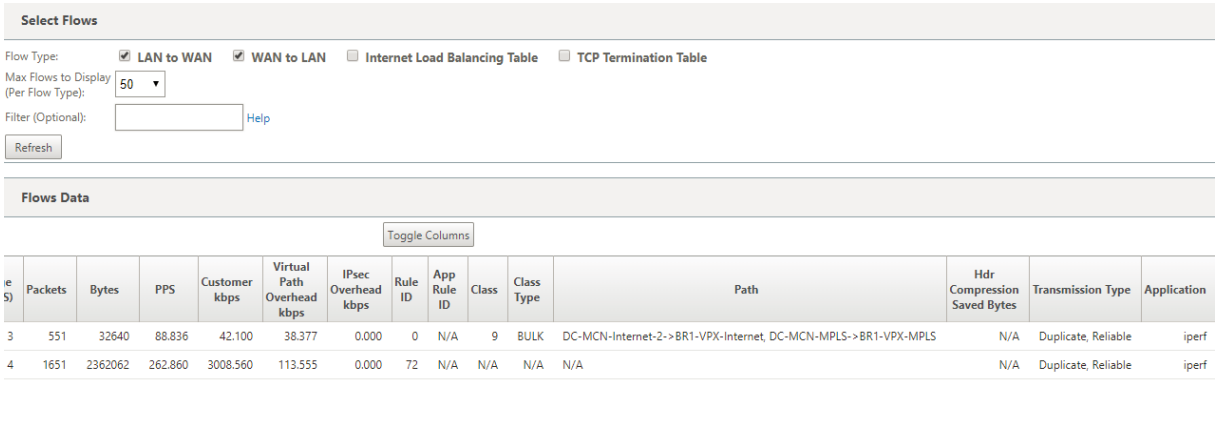
Modo de transmisión duplicada

El modo de duplicación general de paquetes garantiza que inicialmente se tomen dos rutas para procesar paquetes de la misma conexión a fin de garantizar una entrega fiable mediante la duplicación de paquetes en dos rutas independientes.

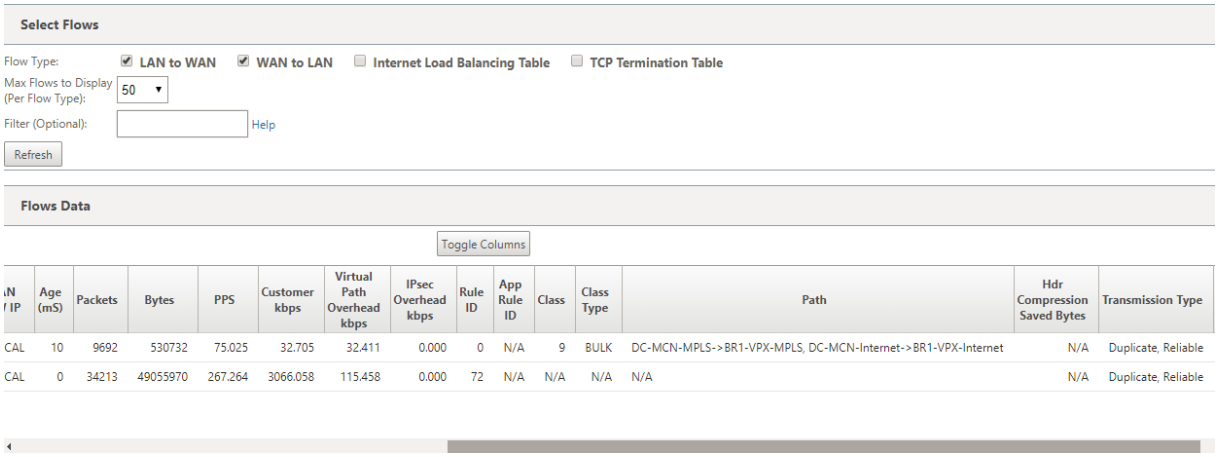
En el caso de Asignación de rutas, observará que se están tomando dos rutas en la sección de rutas de la tabla de flujos siempre que existan dos rutas para procesar flujos mediante duplicación.

La siguiente ilustración ilustra que cuando fluye el tráfico, se puede observar que dos rutas están procesando el tráfico. A diferencia de cualquier otro modo, incluso si el tráfico exige menos ancho de banda que se puede proporcionar con un solo trayecto, este modo siempre duplicará el tráfico en dos rutas para ofrecer aplicaciones de forma fiable.

En la siguiente ilustración se observan dos rutas en la sección de ruta de la tabla de **datos de flujos** ; **DC-MCN-Internet2->BR-VPX-Internet**, **DC-MCN-MPLS->BR1-VPX-MPLS**.



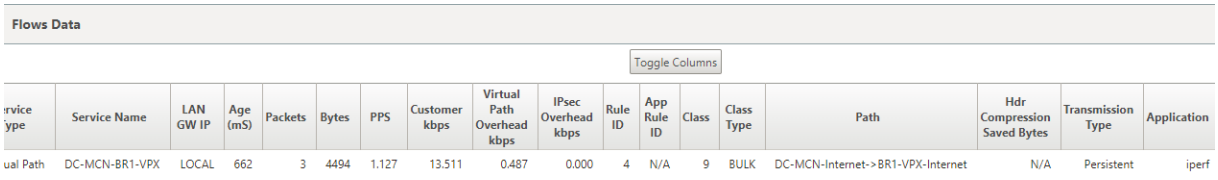
En la siguiente ilustración se muestra que cuando el tráfico fluye, si una de las mejores rutas actuales se vuelve inactiva, se elige otra ruta y sigue habiendo dos rutas como parte de la sección de ruta de la tabla **Datos de flujos**.



Modo de transmisión de ruta persistente

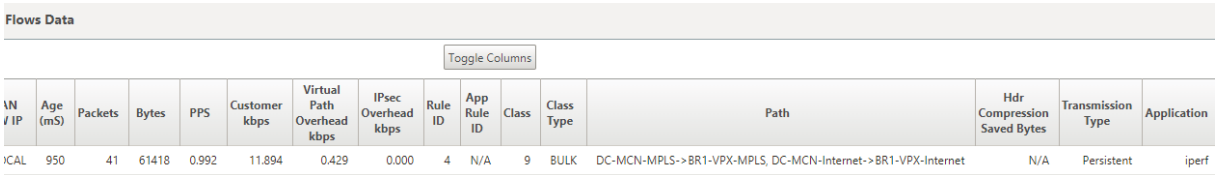
El modo de transmisión de ruta persistente ayuda a retener los paquetes de un flujo en función de la impedancia de latencia de ruta.

La siguiente ilustración ilustra solo una ruta que es la mejor ruta que actualmente maneja los flujos y sus paquetes. No hay demanda de ancho de banda y una ruta sirve para todo. Actualmente solo hay una mejor ruta que es **DC-MCN-Internet->BR1-VPX-Internet.**



La siguiente ilustración ilustra que si la ruta **DC-MCN-Internet->BR1-VPX-Internet** se vuelve propensa a la latencia o está inhabilitada, observará que la nueva ruta surte efecto y la ruta actual **DC-MCN-Internet->BR1-VPX-Internet** se convierte en la última mejor ruta.

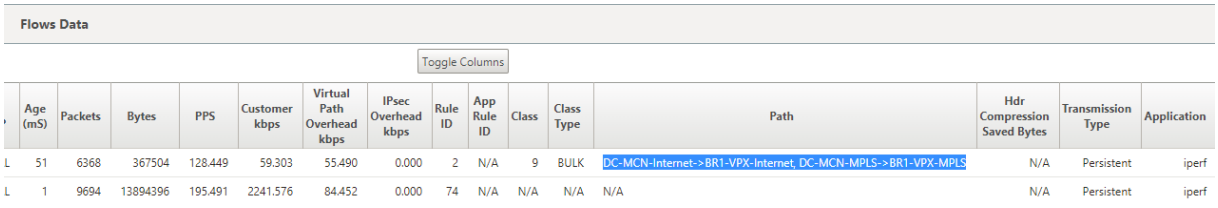
Por lo tanto, la nueva sección de ruta muestra **DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet**.



En modo persistente, puede haber más de una ruta elegida para procesar el tráfico. En ese caso, la GUI muestra las rutas con la mejor y la siguiente mejor en la sección de rutas de la tabla de flujo desde el principio del flujo de tráfico.

La siguiente ilustración ilustra que el flujo inicialmente solo necesita más de dos rutas y permanecen persistentes mientras no se cruce la impedancia de latencia de la ruta (50 ms). Las dos rutas tomadas

se muestran como: **DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS.**

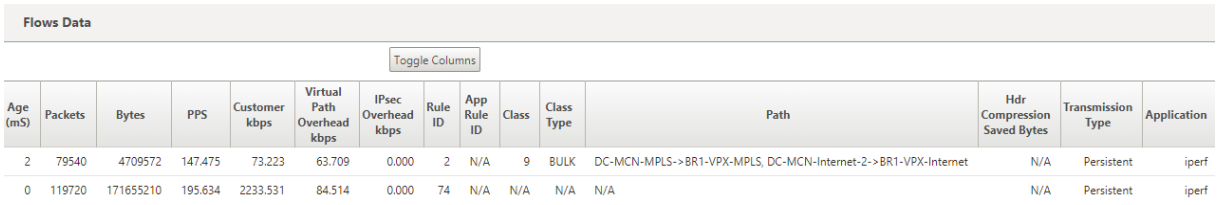


Flows Data

Toggle Columns

	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
L	51	6368	367504	128.449	59.303	55.490	0.000	2	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Persistent	iperf
L	1	9694	13894396	195.491	2241.576	84.452	0.000	74	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

Supongamos que una de las mejores rutas **DC-MCN-Internet** entra en alta latencia o está inhabilitado. Esto hace que aparezca una nueva ruta y la nueva ruta puede ser la mejor ruta o podría ser la segunda mejor ruta en función de la decisión de seleccionar la ruta en ese instante.



Flows Data

Toggle Columns

Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
2	79540	4709572	147.475	73.223	63.709	0.000	2	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Persistent	iperf
0	119720	171655210	195.634	2233.531	84.514	0.000	74	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

Resolución de problemas de IP de administración

August 26, 2022

A continuación se indican los posibles casos que pueden surgir al configurar la dirección IP de DHCP. También incluye prácticas recomendadas y recomendaciones para configurar la dirección IP de administración DHCP al implementar dispositivos SD-WAN.

Estas recomendaciones se aplican a todos los modelos de plataforma de SD-WAN Standard Edition: dispositivos físicos y virtuales.

> **Nota**
>
> Todos los modelos de hardware de los dispositivos SD-WAN se suministran con una dirección IP de administración predeterminada de fábrica. Asegúrese de configurar la dirección IP DHCP necesaria para el dispositivo durante el proceso de configuración.
>
> Todos los modelos virtuales de dispositivos SD-WAN (modelos VPX) y dispositivos que se pueden implementar en el entorno de AWS no tienen asignada una dirección IP predeterminada de fábrica.

Los dispositivos se enciendieron sin que se pueda acceder a servidores DHCP:

- Causas:
  - El cable de administración Ethernet está desconectado

  - El servicio DHCP está inactivo para la red conectada

- Comportamiento previsto

  - Los dispositivos con el servicio DHCP habilitado volverán a intentar la solicitud DHCP cada 300 segundos (valor predeterminado). El intervalo real es de aproximadamente 7 minutos
  - Por lo tanto, los dispositivos con el servicio DHCP habilitado adquirirán direcciones DHCP dentro de los 7 minutos posteriores a la disponibilidad de los servidores DHCP. El retraso oscila entre 0 y 7 minutos

La dirección DHCP asignada caduca:

- Comportamiento esperado:

  - Los dispositivos con el servicio DHCP habilitado intentarán renovar la concesión antes de que caduque la dirección
  - Los dispositivos comienzan con un nuevo descubrimiento de DHCP, si la renovación falla

Los dispositivos con el servicio DHCP habilitado se mueven de una subred habilitada para DHCP a otra subred:

- Causas: Los dispositivos se mueven de una subred DHCP asignada a una subred DHCP diferente
- Comportamiento esperado:

  - Una asignación de dirección IP DHCP de concesión permanente puede requerir el reinicio de los dispositivos para adquirir una dirección IP del nuevo servidor DHCP.
  - Al vencimiento de la concesión de DHCP, los dispositivos pueden reiniciar el protocolo de detección DHCP si no se puede acceder al servidor DHCP actual.
  - Los dispositivos adquieren nuevas direcciones IP con un retraso de 8 minutos. La dirección IP de la puerta de enlace no se modifica en la GUI ni en la CLI. Se actualiza una vez finalizado el proceso de reinicio.

Recomendación:

- Asigne siempre un arrendamiento permanente para las direcciones DHCP asignadas a los dispositivos Citrix SD-WAN (física/virtual). Esto permite que los dispositivos tengan una dirección IP de administración predecible.

Notificaciones HTTP basadas en sesiones

August 26, 2022

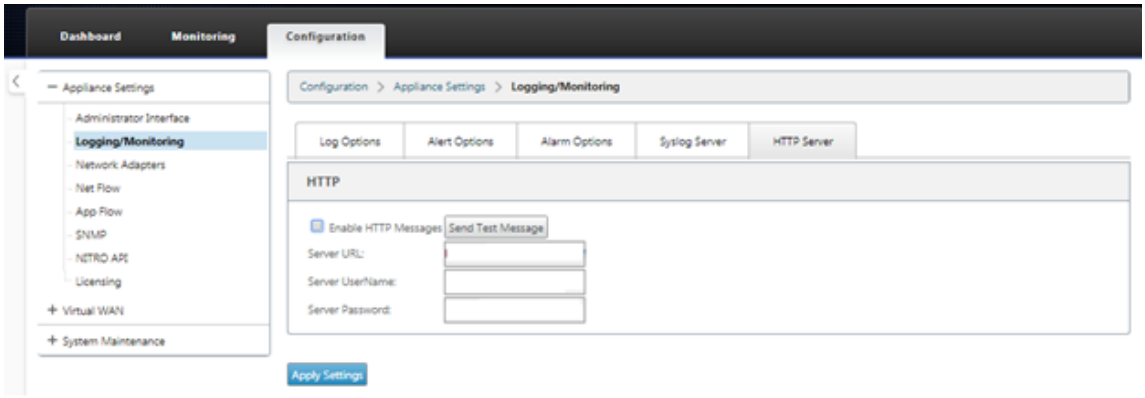
Ahora puede configurar los informes de eventos y alarmas para solicitudes de servicio API HTTP POST genéricas en la GUI del dispositivo Citrix SD-WAN. La configuración de alarmas HTTP y notificación de

eventos es similar a los eventos de correo electrónico y SNMP para eventos y alarmas compatibles con SD-WAN.

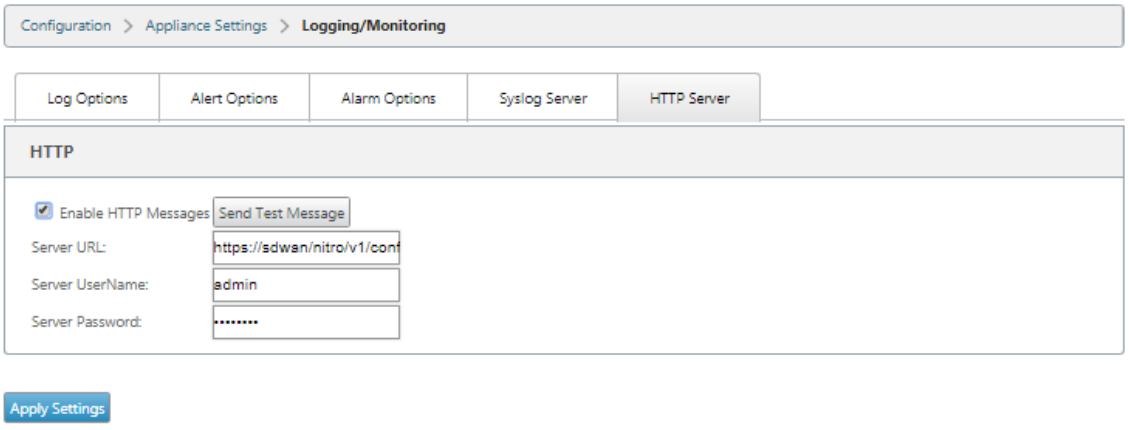
La notificación HTTP Post basada en sesión se envía a un servicio externo, como Service Now. Las notificaciones de eventos del servidor HTTP se pueden configurar en la GUI del dispositivo Citrix SD-WAN y en Citrix SD-WAN Center.

Para configurar las notificaciones HTTP POST en la GUI del dispositivo Citrix SD-WAN:

1. Vaya a **Configuración** > **Registrar/Supervisión** > **Servidor HTTP**.



2. Haga clic en **Habilitar mensajes HTTP**.
3. Introduzca la **URL** del servidor HTTP del que quiere recibir notificaciones. Introduzca el **nombre de usuario delservidor y la contraseña del servidor**.

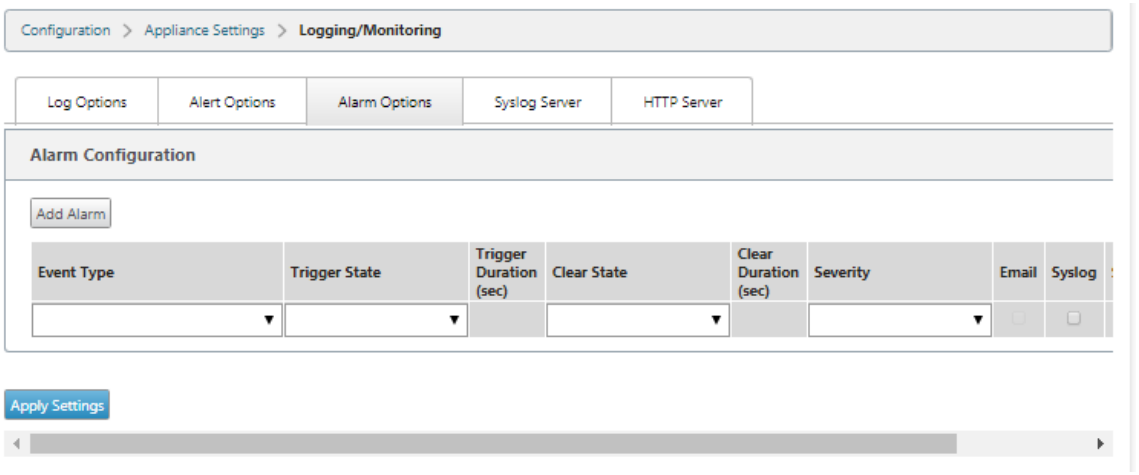


4. Haga clic en **Aplicar configuración**. La página se actualiza después de aplicar la configuración de notificaciones del servidor HTTP.

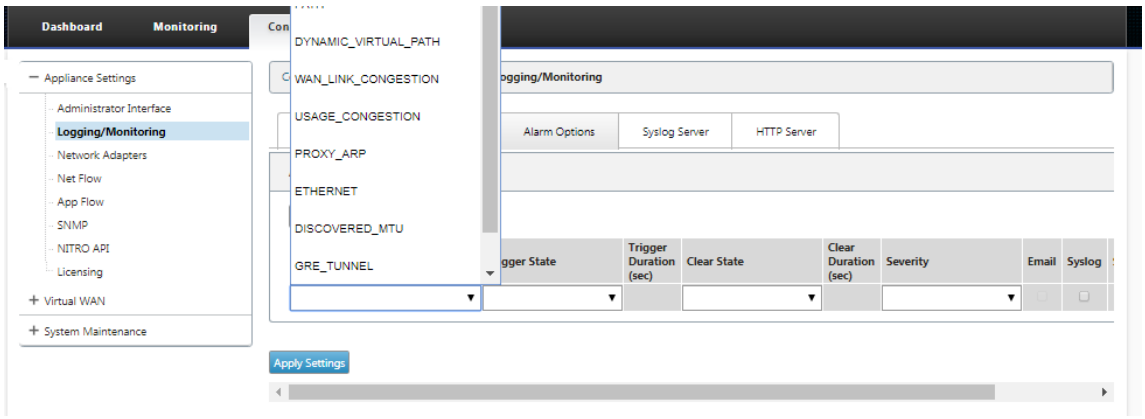
> **Nota**
>
> Utilice la opción **Enviar mensaje de prueba** para comprobar que la conexión del servidor HTTP se ha realizado correctamente.

Para agregar una notificación de alarma para la sesión del servidor HTTP:

1. En la página **Registración/Supervisión**, vaya a la página de la ficha **Opciones de alarma**.
2. Haga clic en **Agregar alarma**.

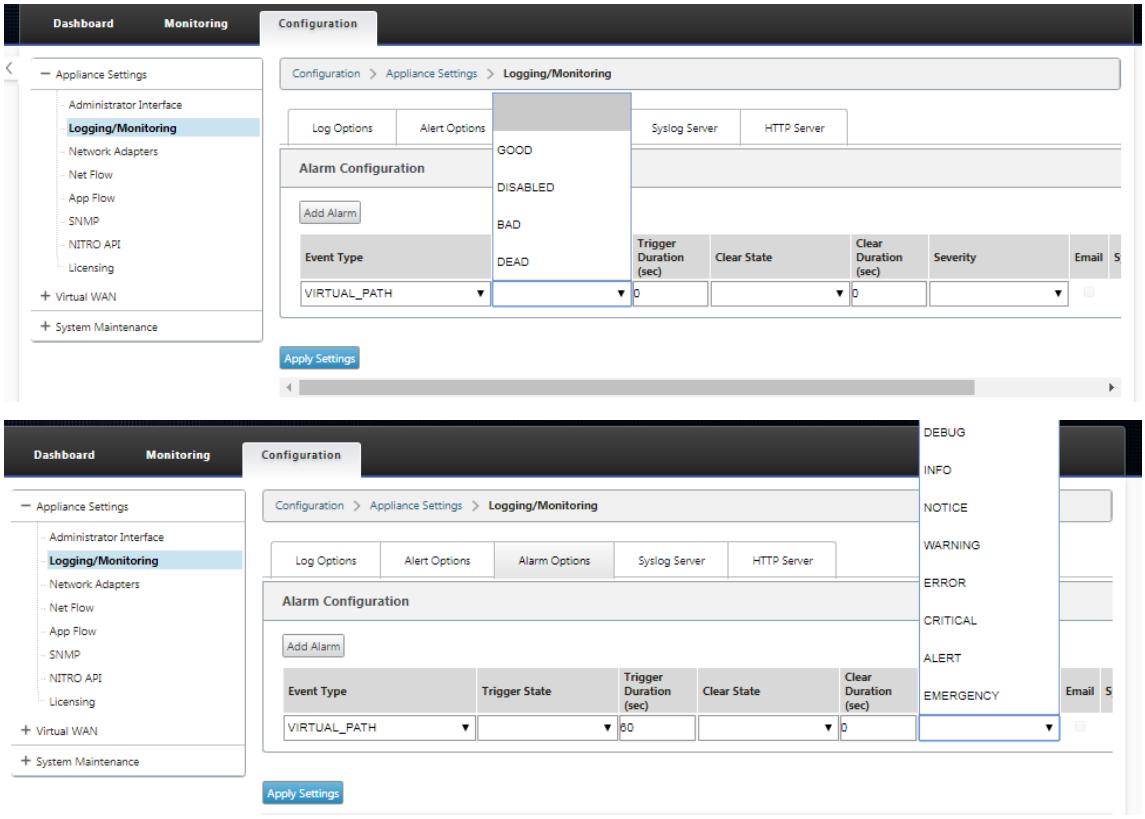


3. Seleccione un **tipo de evento** de la lista desplegable.

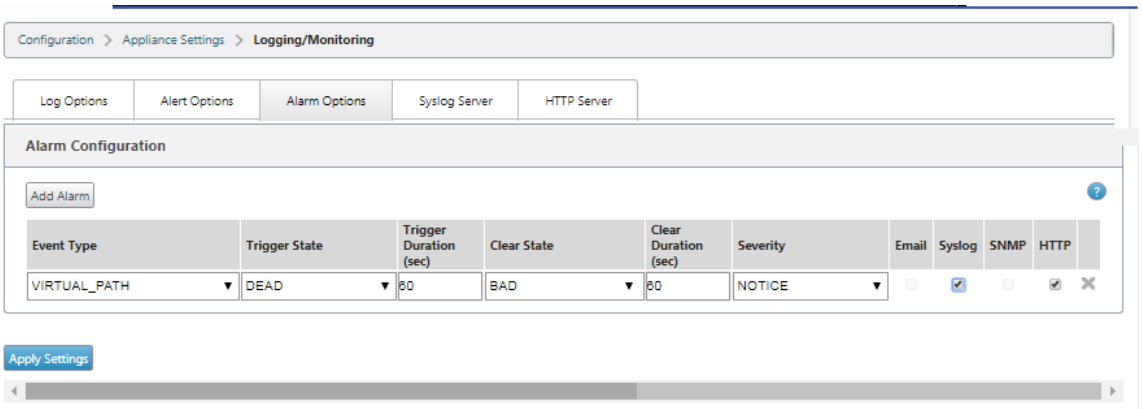


4. Seleccione los siguientes estados de notificación de alarma para el **tipo de evento**elegido. El estado del desencadenador y el estado de borrado cambian según el tipo de evento seleccionado.

   - Estado de activación: BUENO, DESHABILITADO, MALO, MUERTO
   - Duración del disparador: tiempo en segundos
   - Estado claro: BUENO, DESHABILITADO, MALO, MUERTO
   - Duración del borrado: tiempo en segundos
   - Gravedad: DEPURACIÓN, INFORMACIÓN, AVISO, ADVERTENCIA, ERROR, CRÍTICO, EVENTO, EMERGENCIA



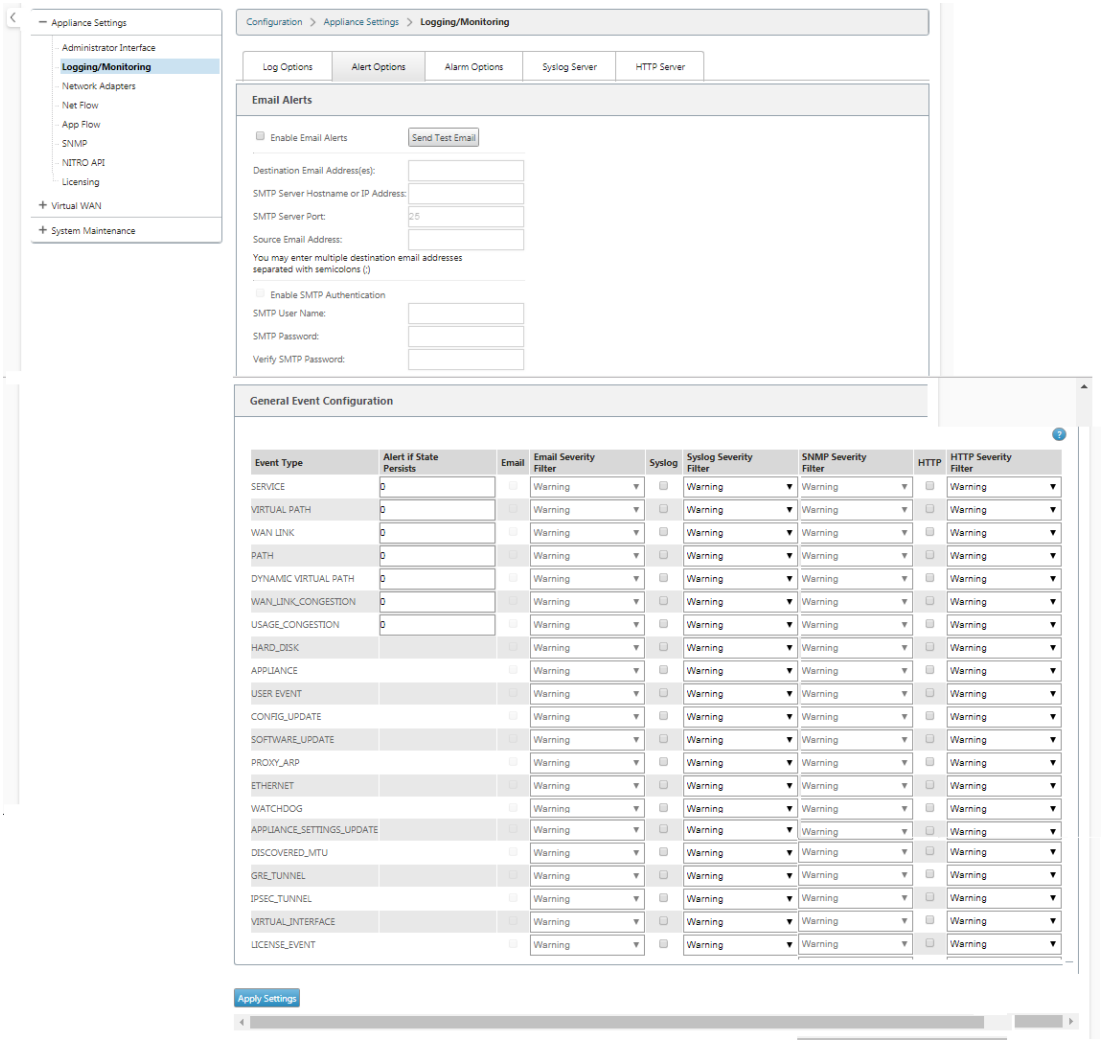
5. Seleccione las casillas de verificación **Syslog** y **HTTP** para recibir notificaciones específicas de los eventos del servidor Syslog y HTTP. Haga clic en **Aplicar configuración**.



Para configurar las opciones de eventos:

Vaya a la página de la ficha **Opciones de alerta**. En la página **Configuración general de eventos**, seleccione el filtro de notificaciones del servidor HTTP para un **tipo de evento** y haga clic en **Aplicar configuración**.

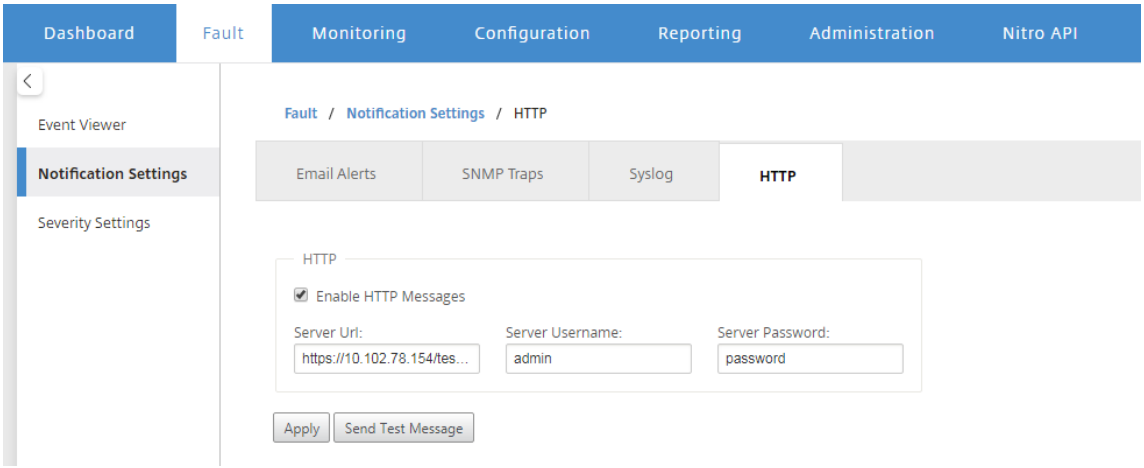
- HTTP
- Filtro de gravedad HTTP



Configuración de notificaciones HTTP en Citrix SD-WAN Center

Para configurar las notificaciones HTTP:

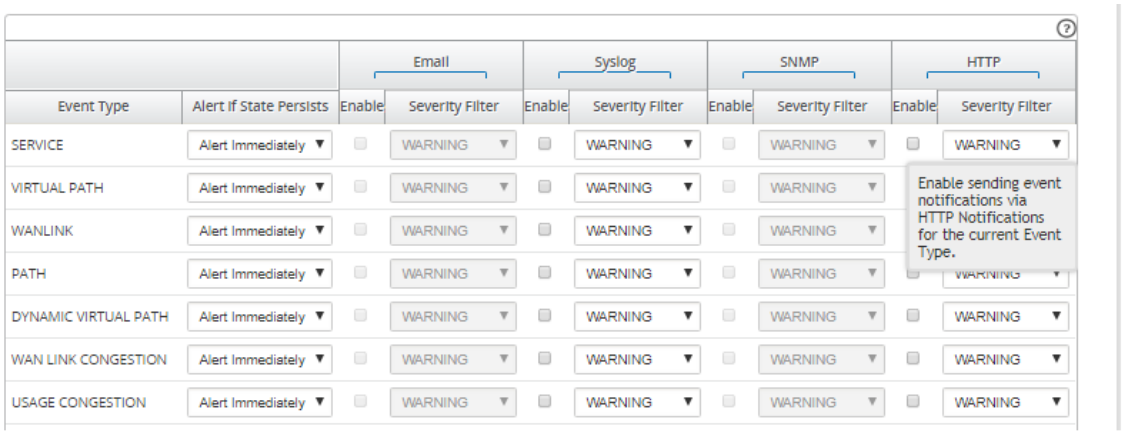
1. Vaya a **Error** > **Configuración de notificaciones** > **HTTP**.



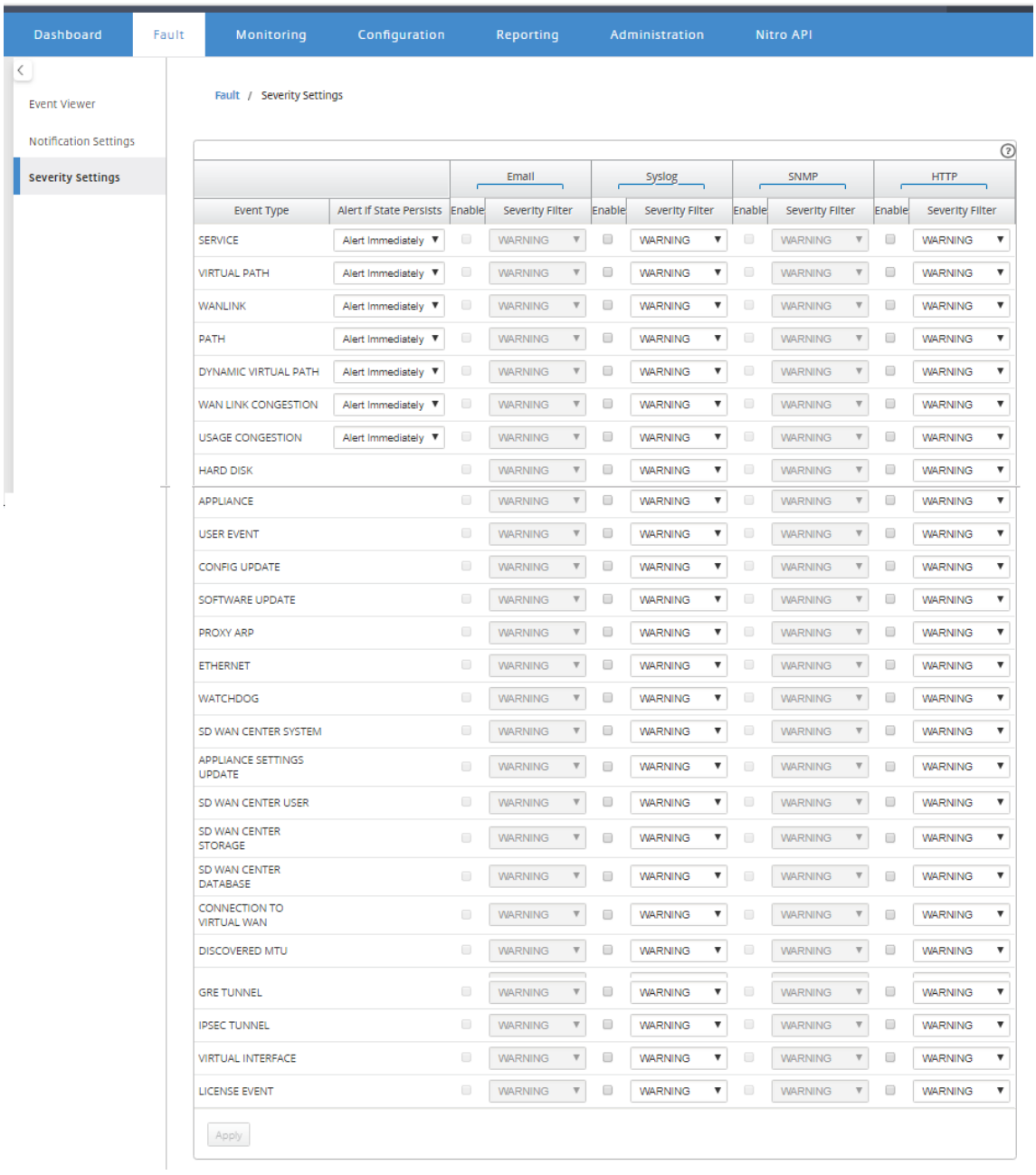
2. Introduzca la **URL del servidor, el nombre de usuario delservidor y la contraseña** del servidor para el servidor HTTP.
3. Haga clic en **Aplicar**

Para configurar la configuración de gravedad:

1. Vaya a la página **Configuración de gravedad**. Haga clic en **Habilitar** para empezar a supervisar las notificaciones HTTP de un tipo de evento seleccionado.



2. Puede elegir supervisar las notificaciones de eventos de correo electrónico, syslog, SNMP y HTTP para los siguientes tipos de sucesos. Haga clic en **Aplicar**.



Pruebas de ancho de banda activo

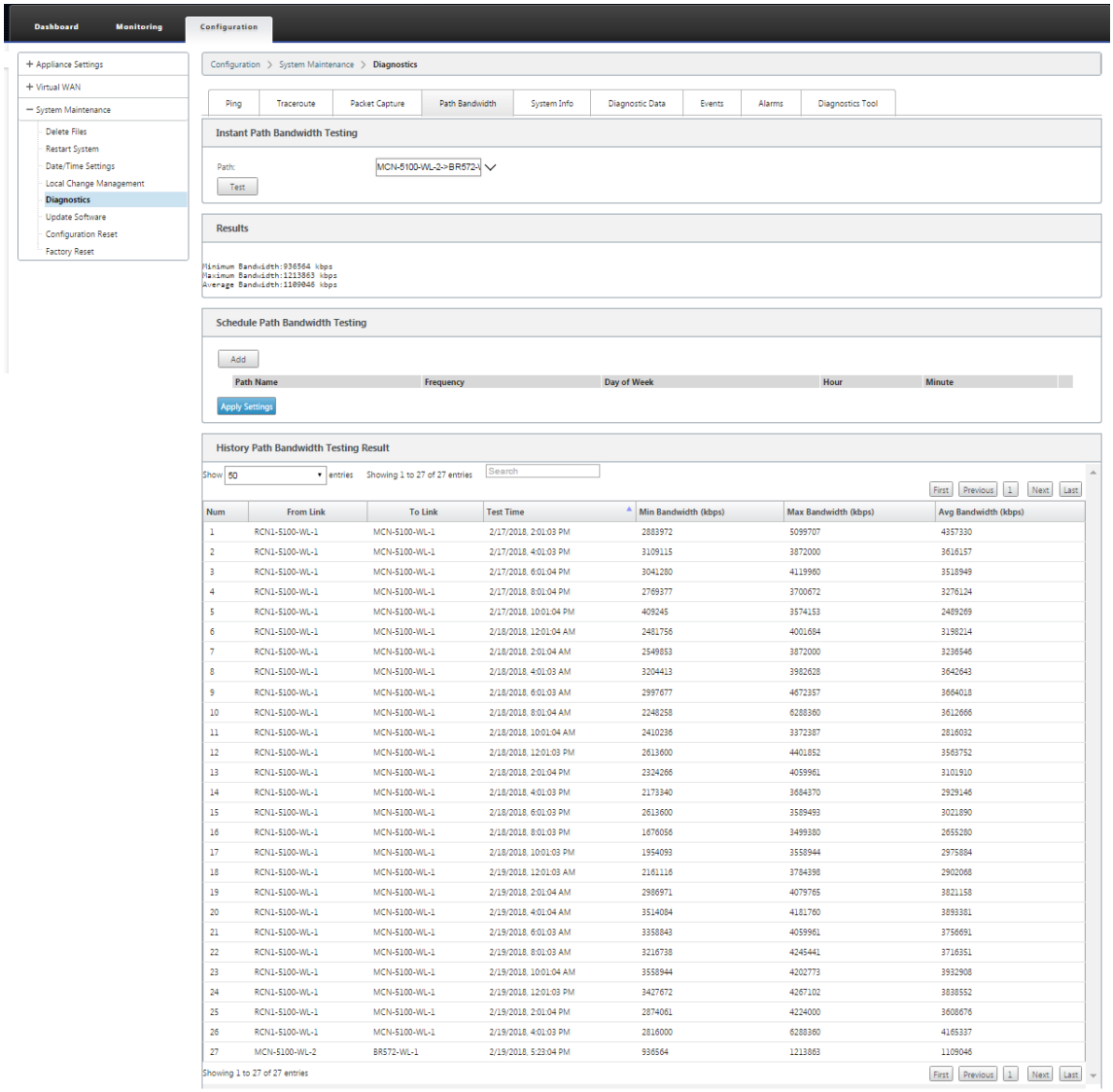
August 26, 2022

Las pruebas activas de ancho de banda le permiten realizar una prueba instantánea de ancho de banda de path a través de un enlace público de Internet WAN, o programar pruebas de ancho de banda de enlace público de Internet WAN para que se completen en momentos específicos de forma

periódica. Esta función resulta útil para demostrar cuánto ancho de banda hay disponible entre dos ubicaciones durante instalaciones nuevas y existentes, así como para probar rutas para determinar el resultado de los cambios de configuración y confirmación, como ajustar la configuración de etiquetas DSCP o las tasas permitidas de ancho de banda.

Para utilizar la función de prueba de ancho de banda activa:

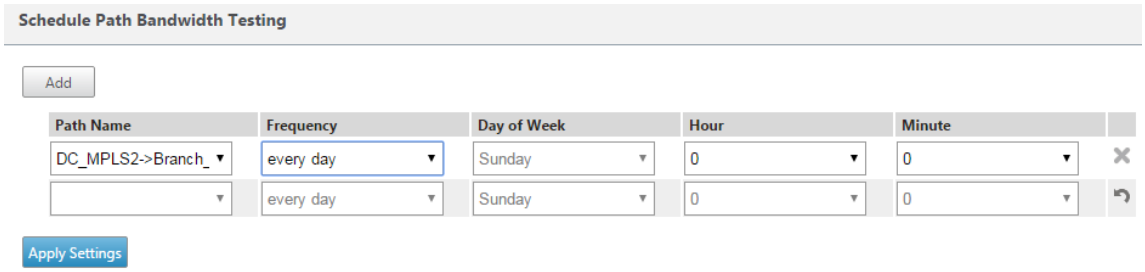
1. Vaya a **Mantenimiento del sistema** > **Diagnóstico** > Ancho de **banda de ruta**.
2. Seleccione la **ruta** deseada y haga clic en **Probar**.



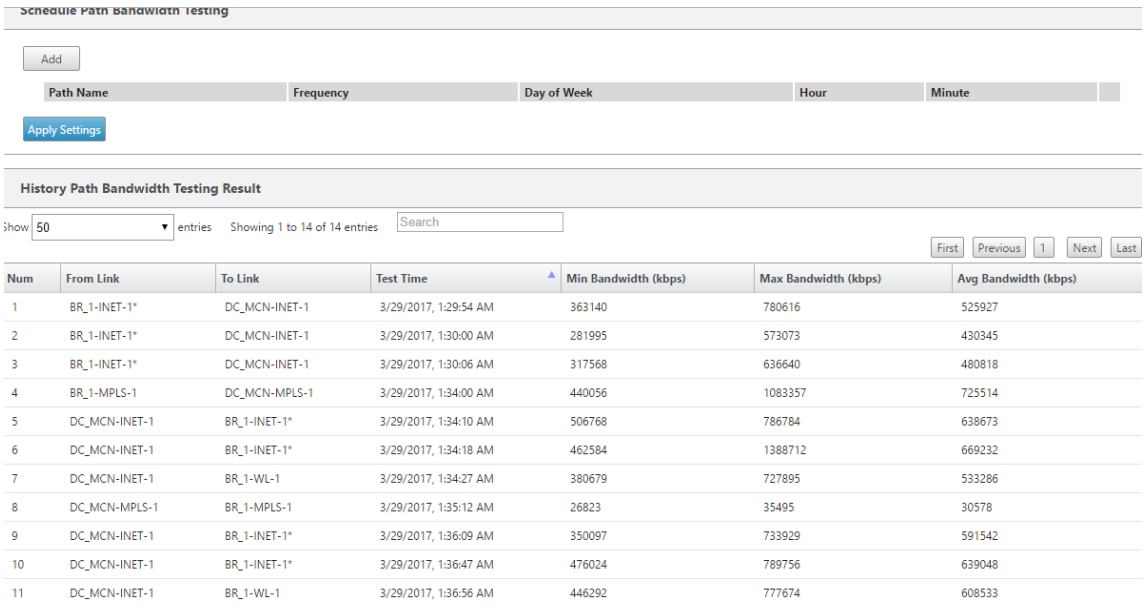
La salida muestra el ancho de banda medio utilizado como valor para establecer como la velocidad permitida para los resultados de ancho de banda mínimo y máximo de WAN Link de la prueba. Junto con la capacidad de probar el ancho de banda, ahora puede cambiar el archivo de configuración para usar el ancho de banda aprendido. Esto se logra a través de la opción Auto Learn que se encuentra en **Sitio** > [Nombre del sitio] > **Enlaces WAN**> [Nombre del enlace

WAN] > **Configuración** y, si está habilitada, el sistema utiliza el ancho de banda aprendido.

También puede programar pruebas periódicas del ancho de banda de ruta en intervalos semanales, diarios u horarios.



> **Nota**
>
> En la parte inferior de esta página se muestra un historial de los resultados de las pruebas de ancho de banda de ruta y los resultados se archivan cada siete días.



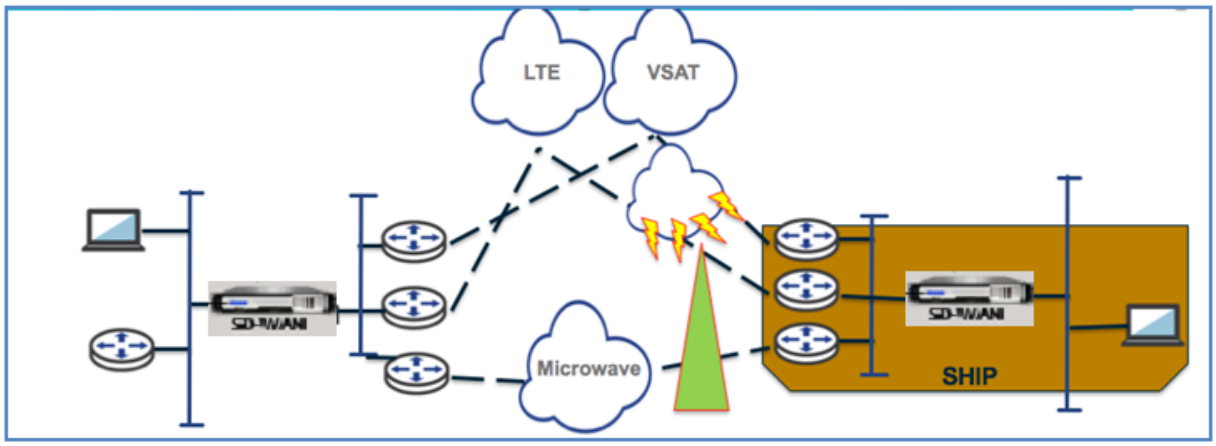
Detección de ancho de banda adaptable

November 16, 2022

Esta función se aplica a redes con enlaces VSAT, LOS, microondas, WAN 3G/4G/LTE, para las que el ancho de banda disponible varía según las condiciones climáticas y atmosféricas, la ubicación y las obstrucciones de la línea del sitio. Permite a los dispositivos SD-WAN ajustar la velocidad de ancho de banda en el enlace WAN dinámicamente basándose en un rango de ancho de banda definido (veloci-

dad de enlace WAN mínima y máxima) para utilizar la cantidad máxima de ancho de banda disponible sin marcar las rutas BAD.

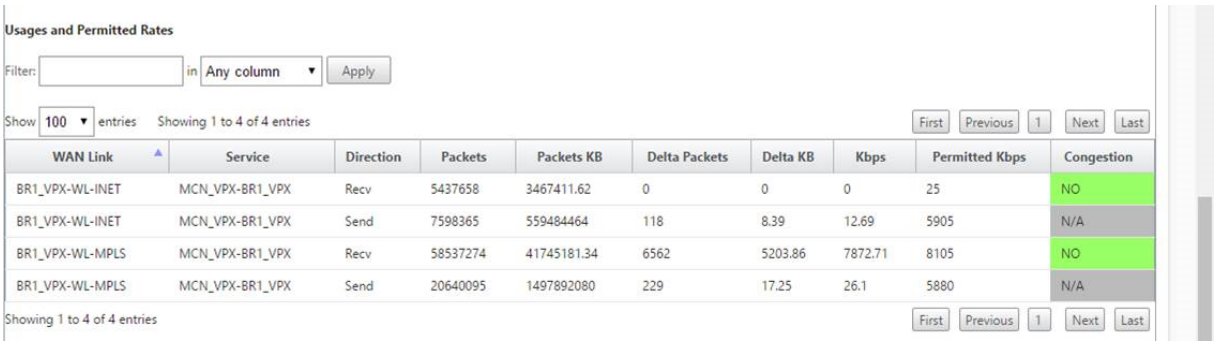
- Mayor fiabilidad del ancho de banda (sobre VSAT, microondas, 3G/4G y LTE)
- Mayor previsibilidad del ancho de banda adaptativo sobre los ajustes configurados por el usuario



Para habilitar la detección de ancho de banda adaptable:

Esta función necesita la opción de sensibilidad de pérdida incorrecta para ser activada (predeterminada o personalizada) como requisito previo. A partir de la versión 11.5 de SD-WAN, puede habilitarla en Citrix SD-WAN Orchestrator Service. Para obtener más información, consulte Detección adaptativa de ancho de banda.

Para ver la tabla **Uso y tarifas permitidas**, vaya a **Monitor** > **Estadísticas** > Uso del **enlace WAN >**Uso**** y **tarifas permitidas**.



WAN Link	Service	Direction	Packets	Packets KB	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Recv	5437658	3467411.62	0	0	0	25	NO
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Send	7598365	559484464	118	8.39	12.69	5905	N/A
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Recv	58537274	41745181.34	6562	5203.86	7872.71	8105	NO
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Send	20640095	1497892080	229	17.25	26.1	5880	N/A

Prácticas recomendadas

August 26, 2022

En los temas siguientes se proporcionan las prácticas recomendadas que deben seguirse cuando se diseña, planifica y ejecuta la solución Citrix SD-WAN en la red.

Seguridad

August 26, 2022

En este artículo se describen las prácticas recomendadas de seguridad para la solución Citrix SD-WAN. Proporciona directrices generales de seguridad para las implementaciones de Citrix SD-WAN.

Directrices de implementación de Citrix SD-WAN

Para mantener la seguridad durante todo el ciclo de vida de la implementación, Citrix recomienda la siguiente consideración de seguridad:

- Seguridad física
- Seguridad de dispositivos
- Seguridad de red
- Administración y Gestión

Seguridad física

Implementar dispositivos Citrix SD-WAN en una sala de servidores segura: el dispositivo o servidor en el que está instalado Citrix SD-WAN debe colocarse en una sala de servidores segura o en un centro de datos restringido, lo que protege el dispositivo del acceso no autorizado. Como mínimo, el acceso debe controlarse mediante un lector de tarjetas electrónicas. El acceso al dispositivo se supervisa mediante un circuito cerrado de televisión que registra continuamente toda la actividad con fines de auditoría. En caso de allanamiento, el sistema de vigilancia electrónica debe enviar una alarma al personal de seguridad para obtener una respuesta inmediata.

Proteja los puertos del panel frontal y de la consola del acceso no autorizado: proteja el dispositivo en una jaula o rack grande con control de acceso con llave física.

Proteja la fuente de alimentación: asegúrese de que el dispositivo esté protegido con una fuente de alimentación ininterrumpida.

Seguridad de los dispositivos

Para la seguridad del dispositivo, proteja el sistema operativo de cualquier servidor que aloje un dispositivo virtual Citrix SD-WAN (VPX), realice actualizaciones de software remotas y las siguientes prácticas de administración segura del ciclo de vida:

- Proteja el sistema operativo del servidor que aloja un dispositivo Citrix SD-WAN VPX; un dispositivo Citrix SD-WAN VPX se ejecuta como un dispositivo virtual en un servidor estándar. El acceso al servidor estándar debe protegerse con un control de acceso basado en roles y una administración de contraseñas sólida. Además, Citrix recomienda actualizaciones periódicas del servidor con los parches de seguridad más recientes para el sistema operativo y software antivirus actualizado en el servidor.
- Realizar actualizaciones de software remotas: instale todas las actualizaciones de seguridad para resolver cualquier problema conocido. Consulte la página web Boletines de seguridad para suscribirse y recibir alertas de seguridad actualizadas.
- Siga las prácticas de administración segura del ciclo de vida: para administrar un dispositivo al volver a implementar o iniciar RMA y retirar datos confidenciales, complete las contramedidas de recordatorio de datos eliminando los datos persistentes del dispositivo.
- Implemente la interfaz de administración del dispositivo detrás de la DMZ para garantizar que no haya acceso directo a Internet a la interfaz de administración. Para mayor protección, asegúrese de que la red de administración esté aislada de Internet y que solo los usuarios autorizados con aplicaciones de administración aprobadas se ejecuten en la red.

Seguridad de red

Por motivos de seguridad de red, no utilice el certificado SSL predeterminado. Utilice Transport Layer Security (TLS) cuando acceda a la interfaz de administrador, proteja la dirección IP de administración no redirigible del dispositivo, configure una configuración de alta disponibilidad e implemente protecciones de administración y administración según corresponda para la implementación.

- No utilizar el certificado SSL predeterminado: un certificado SSL de una entidad emisora de certificados de buena reputación simplifica la experiencia del usuario para las aplicaciones web orientadas a Internet. A diferencia de lo que ocurre con un certificado autofirmado o un certificado de la entidad de certificación de confianza, los exploradores web no requieren que los usuarios instalen el certificado de la entidad de certificación de confianza para iniciar una comunicación segura con el servidor web.
- Usar Transport Layer Security al acceder a la interfaz de administrador: asegúrese de que la dirección IP de administración no sea accesible desde Internet o que, al menos, esté protegida por un firewall seguro. Asegúrese de que la dirección IP de LOM no sea accesible desde Internet o que, al menos, esté protegida por un firewall seguro.

- Cuentas de administración y gestión seguras: cree una cuenta de administrador alternativa y establezca contraseñas seguras para las cuentas de administrador y espectador. Al configurar el acceso remoto a cuentas, considere la posibilidad de configurar la administración administrativa de cuentas autenticada externamente mediante RADIUS y TACACS. Cambie la contraseña predeterminada de las cuentas de usuario administrador, configure NTP, use el valor de tiempo de espera de sesión predeterminado, use SNMPv3 con autenticación SHA y cifrado AES.

La red superpuesta de Citrix SD-WAN protege los datos que atraviesan la red superpuesta SD-WAN.

Interfaz de administrador segura

Para obtener acceso seguro a la administración web, reemplace los certificados predeterminados del sistema cargando e instalando certificados desde una entidad emisora de certificados de buena reputación. Vaya a Configuración > **Configuración del dispositivo> Interfaz de administrador** en la GUI del dispositivo SD-WAN.

Cuentas de usuario:

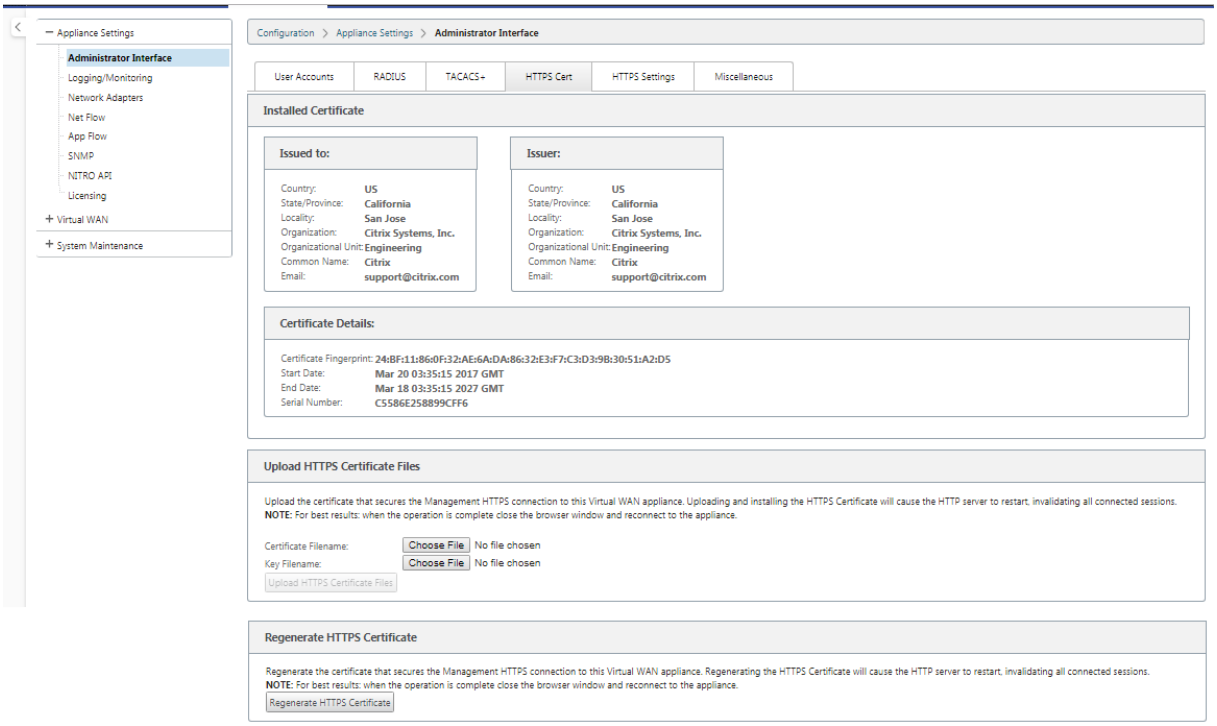
- Cambiar contraseña de usuario local
- Administrar usuarios

Certificados HTTPS:

- Certificado
- Clave

Miscelánea:

- Tiempo de espera de la consola web



Considere la posibilidad de usar Citrix Web App Firewall

El dispositivo con licencia Citrix ADC proporciona un Citrix Web App Firewall integrado que utiliza un modelo de seguridad positivo y aprende automáticamente el comportamiento adecuado de la aplicación para la protección contra amenazas como la inyección de comandos, la inyección de SQL y el uso de scripts entre varios sitios.

Cuando utiliza Citrix Web App Firewall, los usuarios pueden agregar seguridad adicional a la aplicación web sin cambios de código y con pocos cambios en la configuración. Para obtener más información, consulte Introducción a Citrix Web Application Firewall.

Configuración de cifrado de ruta virtual global

- El cifrado de datos AES-128 está habilitado de forma predeterminada. Se recomienda utilizar AES-128 o más protección del nivel de cifrado AES-256 para el cifrado de rutas. Asegúrese de que la opción “habilitar rotación de clave de cifrado”esté configurada para garantizar la regeneración de claves para cada ruta virtual con cifrado habilitado mediante un intercambio de claves Diffie-Hellman de curva elíptica a intervalos de 10 a 15 minutos.

Si la red requiere autenticación de mensajes además de confidencialidad (es decir, protección contra manipulaciones), Citrix recomienda utilizar el cifrado de datos IPsec. Si solo se requiere confidencialidad, Citrix recomienda utilizar los encabezados mejorados.

- El encabezado de cifrado de paquetes extendido permite que se agregue un contador predefinido aleatoriamente al comienzo de cada mensaje cifrado. Cuando se cifra, este contador sirve como vector de inicialización aleatoria, determinista solo con la clave de cifrado. Esto aleatoriza el resultado del cifrado, proporcionando un mensaje fuerte de manera indistinguible. Tenga en cuenta que, cuando está activada, esta opción aumenta la sobrecarga de paquetes en 16 bytes.
- El tráiler de autenticación de paquetes extendida agrega un código de autenticación al final de cada mensaje cifrado. Este tráiler permite verificar que los paquetes no se modifican en tránsito. Tenga en cuenta que esta opción aumenta la sobrecarga de paquetes.

Seguridad de firewall

La configuración del firewall recomendada es con una acción de Firewall predeterminada como denegar todo al principio y, a continuación, agregar excepciones. Antes de agregar reglas, documente y revise el propósito de la regla de firewall. Utilice la inspección con estado y la inspección a nivel de aplicación siempre que sea posible. Simplifique las reglas y elimine las reglas redundantes. Defina y adhiera a un proceso de administración de cambios que realiza un seguimiento y permite revisar los cambios en la configuración del **firewall**. Configure el firewall de todos los dispositivos para que realice un seguimiento de las conexiones a través del dispositivo mediante la configuración global. El seguimiento de las conexiones verifica que los paquetes estén formados correctamente y sean apropiados para el estado de conexión. Cree zonas adecuadas a la jerarquía lógica de la red o de las áreas funcionales de la organización. Tenga en cuenta que las zonas son importantes a nivel mundial y pueden permitir que las redes geográficamente dispares se traten como la misma zona de seguridad. Cree las directivas más específicas posibles para reducir el riesgo de agujeros de seguridad, evite el uso de reglas Any in Permitir. Configure y mantenga una plantilla de directiva global para crear un nivel básico de seguridad para todos los dispositivos de la red. Defina plantillas de directivas en función de las funciones funcionales de los dispositivos en la red y aplíquelas cuando sea apropiado. Defina directivas en sitios individuales solo cuando sea necesario.

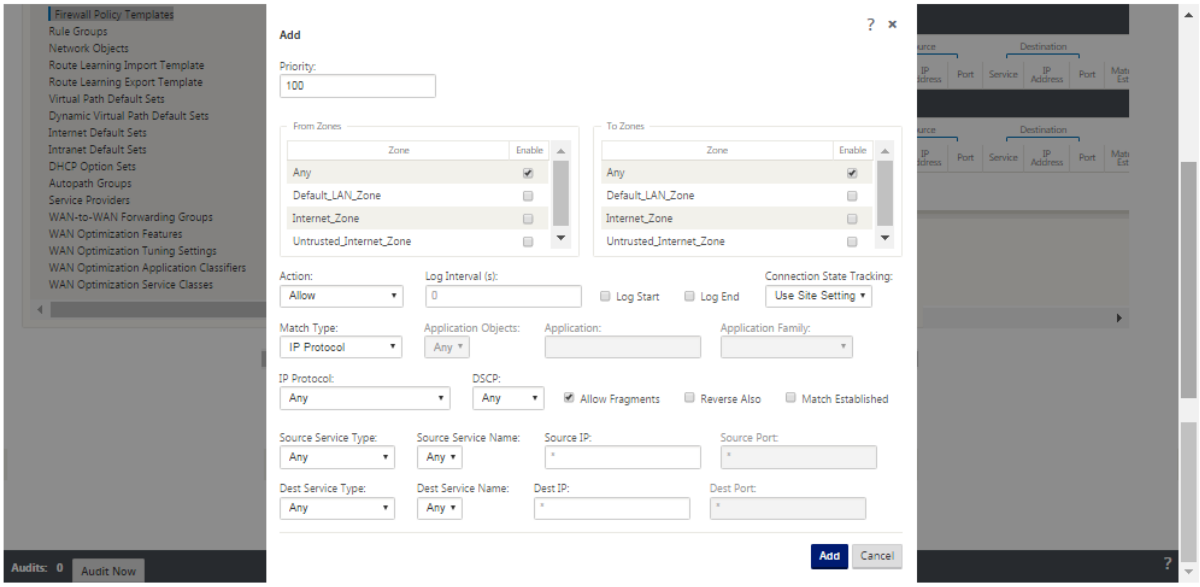
Plantillas de firewall globales: Las plantillas de firewall permiten la configuración de parámetros globales que afectan al funcionamiento del firewall en dispositivos individuales que funcionan en el entorno de superposición de SD-WAN.

Acciones predeterminadas del firewall: Permitir habilita los paquetes que no coinciden con ninguna directiva de filtro Deny permite descartar paquetes que no coincidan con ninguna directiva de filtro.

Seguimiento del estado de conexión predeterminado: Permite el seguimiento bidireccional del estado de conexión para flujos TCP, UDP e ICMP que no coinciden con una directiva de filtro o una regla NAT. Los flujos asimétricos se bloquean cuando está habilitado, incluso cuando no hay directivas de firewall definidas. La configuración se puede definir a nivel del sitio, lo que invalidará la configuración

global. Si existe la posibilidad de flujos asimétricos en un sitio, la recomendación es habilitarlo a nivel de sitio o directiva y no a nivel global.

Zonas: Las zonas de firewall definen la agrupación de seguridad lógica de las redes conectadas a Citrix SD-WAN. Las zonas se pueden aplicar a interfaces virtuales, servicios de intranet, túneles GRE y túneles IPsec de LAN.



zona de seguridad de enlace WAN

La zona de seguridad que no es de confianza debe configurarse en los enlaces WAN conectados directamente a una red pública (no segura). Si no es de confianza, el enlace WAN se establece en su estado más seguro, permitiendo que solo se acepte tráfico cifrado, autenticado y autorizado en el grupo de interfaces. ARP e ICMP a la dirección IP virtual son el único otro tipo de tráfico permitido. Esta configuración también garantiza que solo se envíe tráfico cifrado desde las interfaces asociadas al grupo Interfaz.

Dominios de redirección

Los dominios de redirección son sistemas de red que incluyen un conjunto de enrutadores que se utilizan para segmentar el tráfico de red. Los sires recién creados se asocian automáticamente con el dominio de redirección predeterminado.

Túneles IPsec

Los túneles IPsec protegen tanto los datos del usuario como la información del encabezado. Los dispositivos Citrix SD-WAN pueden negociar túneles IPsec fijos en el lado LAN o WAN con pares que no

sean SD-WAN. Para Túneles IPsec sobre LAN, debe seleccionarse un dominio de redirección. Si el túnel IPsec utiliza un servicio de intranet, el dominio de redirección está predeterminado por el servicio de intranet seleccionado.

El túnel IPsec se establece en toda la ruta virtual antes de que los datos puedan fluir por la red superpuesta SD-WAN.

- Las opciones del tipo de encapsulación incluyen ESP (los datos se encapsulan y cifran), ESP+Auth (los datos se encapsulan, cifran y validan con un HMAC), AH; los datos se validan con un HMAC.
- El modo de cifrado es el algoritmo de cifrado que se utiliza cuando ESP está habilitado.
- El algoritmo hash se utiliza para generar un HMAC.
- El tiempo de vida es preferible, en segundos, para que exista una asociación de seguridad IPsec. Se puede usar 0 de forma ilimitada.

Configuración IKE

Intercambio de claves de Internet (IKE) es un protocolo IPsec que se utiliza para crear una asociación de seguridad (SA). Los dispositivos Citrix SD-WAN admiten los protocolos IKEv1 e IKEv2.

- El modo puede ser modo principal o modo agresivo.
- La identidad puede ser automática para identificar al igual, o se puede usar una dirección IP para especificar manualmente la dirección IP del mismo nivel.
- La autenticación habilita la autenticación o el certificado de clave previamente compartida como método de autenticación.
- Validar identidad de pares permite la validación de la identidad de igual de IKE si se admite el tipo de ID del par; de lo contrario, no habilite esta función.
- Los grupos Diffie-Hellman están disponibles para la generación de claves IKE con el grupo 1 a 768 bits, el grupo 2 a 1024 bits y el grupo 5 al grupo de 1536 bits.
- El algoritmo hash incluye MD5, SHA1 y SHA-256 tiene algoritmos disponibles para mensajes IKE.
- Los modos de cifrado incluyen los modos de cifrado AES-128, AES-192 y AES-256 disponibles para los mensajes IKE.
- La configuración de IKEv2 incluye autenticación de pares y algoritmo de integridad.

Configuración del firewall

Los siguientes problemas comunes se pueden identificar verificando la configuración del enrutador y el firewall ascendentes:

- Configuración de colas MPLS/QoS: compruebe que el tráfico encapsulado UDP entre las direcciones IP virtuales SD-WAN no se vea afectado debido a la configuración de **QoS** en los dispositivos intermedios de la red.

- El dispositivo Citrix SD-WAN debe procesar todo el tráfico de los vínculos WAN configurados en la red SD-WAN utilizando el tipo de servicio adecuado (ruta virtual, Internet, intranet y local).
- Si el tráfico tiene que omitir el dispositivo Citrix SD-WAN y utilizar el mismo enlace subyacente, se deben realizar reservas de ancho de banda adecuadas para el tráfico SD-WAN en el router. Además, la capacidad del enlace debe configurarse en consecuencia en la configuración de SD-WAN.
- Compruebe que el router/firewall intermedio no tiene límites de inundación UDP ni de PPS. Esto limita el tráfico cuando se envía a través de la ruta virtual (encapsulado UDP).

Redirección

August 26, 2022

En este artículo se describen las prácticas recomendadas de redirección para la solución Citrix SD-WAN.

Servicio de redirección de Internet/Intranet

Cuando el servicio Internet no está configurado para el tráfico enlazado a Internet y, en su lugar, se configura una ruta **local** o una ruta **Passthrough** para llegar al enrutador de puerta de enlace. El router utiliza los enlaces WAN configurados en el dispositivo SD-WAN, lo que provoca un problema de sobresuscripción de vínculos.

Si una ruta de Internet está configurada como **Local** en el MCN, es aprendida por todos los sitios SD-WAN de sucursal y configurada como Ruta de **ruta virtual** de forma predeterminada. Esto implica que el tráfico enlazado a Internet en el dispositivo de sucursal se redirige a través de la ruta virtual a MCN.

Prioridad de redirección

El orden de prioridad de redirección:

- Coincidencia de prefijo: los prefijos más largos coinciden.
- Servicio: local, servicio de ruta virtual, Internet, Intranet, paso a través
- Coste de ruta

Asimetría de redirección

Asegúrese de que no haya asimetría de redirección en la red (el dispositivo NetScaler SD-WAN transmite tráfico en una sola dirección). Esto crea problemas con el seguimiento de la conexión del firewall y la inspección profunda de paquetes.

QoS

August 26, 2022

Tenga en cuenta lo siguiente al configurar QoS:

- Comprender los patrones y requisitos de tráfico de red. Es posible que tenga que observar las **estadísticas de clase de QoS**y cambiar las profundidades de las colas o cambiar el porcentaje de participación de clases de QoS predeterminado para evitar caídas como se muestra en las estadísticas de QoS.
- A veces, toda la subred se agrega a una regla para facilitar la configuración en lugar de crear reglas para direcciones IP de aplicaciones específicas. Al agregar toda la subred a una regla, se asigna incorrectamente todo el tráfico de la subred a una regla. Por lo tanto, las clases QoS asociadas a esa regla pueden provocar caída de cola y un rendimiento deficiente de la aplicación o experiencia del usuario.

Enlaces WAN

August 26, 2022

Las plataformas Citrix SD-WAN admiten hasta 8 conexiones públicas a Internet y 32 conexiones MPLS privadas. En este artículo se describen las prácticas recomendadas de configuración de enlaces WAN para la solución Citrix SD-WAN.

Puntos que hay que recordar al configurar los enlaces WAN:

- Configure la velocidad **física y permitida** como ancho de banda del enlace WAN real. En los casos en que el dispositivo SD-WAN no debe utilizar toda la capacidad del enlace WAN, cambie la tasa **permitida** según corresponda.
- Si no está seguro del ancho de banda y si los vínculos no son fiables, puede activar la función **Aprendizaje automático**. La función **Aprendizaje automático** solo aprende la capacidad del vínculo subyacente y utiliza el mismo valor en el futuro.

- Si el enlace subyacente no es estable y no garantiza un ancho de banda fijo (por ejemplo, enlaces 4G), utilice la función **Detección de ancho de banda adaptable**.
- No se recomienda habilitar **Aprendizaje automático** y **Detección de ancho de banda adaptable** en el mismo enlace WAN.
- Configure manualmente el MCN/RCN con la velocidad física Entrada/Egress para todos los enlaces WAN, ya que es el punto central de la distribución del ancho de banda entre varias ramas.
- Para aumentar la fiabilidad de las cargas de trabajo/servicios importantes del centro de datos, cuando no se utiliza el aprendizaje automático, utilice enlaces confiables con los SLA que no tengan variación aleatoria de la capacidad.
- Si el vínculo subyacente no es estable, cambie la siguiente configuración de ruta:
  - Configuración de pérdida
  - Inhabilitar inestabilidad sensible
  - Tiempo de silencio
- Utilice la **herramienta de diagnóstico** para comprobar el estado y la capacidad del enlace.
- Si la SD-WAN se implementa en modo de **brazo único**, asegúrese de no sobrepasar la capacidad física del enlace subyacente.

Verificación del estado del enlace ISP

Para implementaciones nuevas, anteriores a la implementación de SD-WAN y al agregar un nuevo enlace ISP a la implementación de SD-WAN existente:

- Compruebe el tipo de enlace. Por ejemplo; MPLS, ADSL, 4G.
- Funciones de la red. Por ejemplo: ancho de banda, pérdida, latencia y fluctuación.

Esta información ayuda a configurar la red SD-WAN según sus requisitos.

Topología de red

Se observa comúnmente que el tráfico de red específico omite los dispositivos Citrix SD-WAN y utiliza el mismo enlace subyacente configurado en la red SD-WAN. Debido a que la SD-WAN no tiene visibilidad completa sobre la utilización del enlace, es probable que SD-WAN sobresuscriba el enlace y provoque problemas de rendimiento y PATH.

Aprovisionamiento

Puntos a tener en cuenta al aprovisionar SD-WAN:

- De forma predeterminada, todas las sucursales y servicios WAN (ruta virtual/Internet/Intranet) reciben la misma proporción del ancho de banda.
- Es necesario cambiar los sitios de aprovisionamiento cuando hay una gran disparidad en términos de requisitos de ancho de banda o disponibilidad entre los sitios de conexión.
- Cuando las rutas virtuales dinámicas están habilitadas entre el máximo de sitios disponibles, la capacidad de enlace WAN se comparte entre la ruta virtual estática a DC y las rutas virtuales dinámicas.

Preguntas frecuentes

August 26, 2022

Alta disponibilidad

¿Cuál es la diferencia entre el dispositivo de alta disponibilidad y el dispositivo secundario (geográfico)?

- La alta disponibilidad garantiza la tolerancia a errores. El dispositivo secundario (geográfico) permite la recuperación ante desastres.
- La alta disponibilidad se puede configurar para los dispositivos MCN, RCN y sucursales. El dispositivo secundario (geográfico) solo se puede configurar para MCN y RCN.
- Los dispositivos de alta disponibilidad se configuran en el mismo sitio o ubicación geográfica. Un dispositivo de sucursal en una ubicación geográfica diferente se configura como dispositivo MCN/RCN secundario (geográfico).
- Los dispositivos primarios y secundarios de alta disponibilidad deben ser los mismos modelos de plataforma. El dispositivo secundario (geográfico) puede ser o no el mismo modelo de plataforma que el MCN/RCN principal.
- La alta disponibilidad tiene mayor prioridad que la secundaria (geográfica). Si un dispositivo (MCN/RCN) está configurado con un dispositivo de alta disponibilidad y secundario (geográfico), cuando el dispositivo falla, el dispositivo secundario de alta disponibilidad se activa. Si fallan los dos dispositivos de alta disponibilidad o si el sitio del centro de datos falla, el dispositivo secundario (geográfico) se activa.
- En Alta Disponibilidad, la conmutación primaria/secundaria se produce de forma instantánea o en 10-12 segundos, según la implementación de alta disponibilidad. El cambio de MCN/RCN

primario a MCN/RCN secundario (Geo) se produce después de 15 segundos de inactividad del primario.

- La configuración de alta disponibilidad le permite configurar la recuperación principal. No se puede configurar la recuperación principal para el dispositivo secundario (geográfico); la recuperación principal se produce automáticamente después de que el dispositivo principal vuelve a funcionar y caduca el temporizador de espera.

Actualización de un solo paso

> **Nota**
>
> Los componentes complementarios/HFS de WANOP, SVM y XenServer se consideran componentes del sistema operativo.

¿Debo usar el paquete *TAR.GZ* o el paquete *ZIP* de actualización de un solo paso para actualizar a la versión 9.3.x desde mi versión actual (8.1.x, 9.1.x, 9.2.x)?

Utilice los *archivos.tar.gz* de las plataformas afectadas para actualizar el software SD-WAN a la versión 9.3.x. Después de actualizar el software de SD-WAN a la versión 9.3.x, realice la administración de cambios mediante el *paquete.zip* para transferir/preparar paquetes de software de componentes del sistema operativo. Después de la activación, el MCN transfiere o realiza etapas componentes del sistema operativo para todas las sucursales relevantes.

Después de actualizar a 9.3.0 mediante el paquete de actualización de un solo paso (archivo.zip), necesito realizar.*upg* en cada dispositivo?

No, la actualización/actualización del software del sistema operativo se encargará del paquete *zip* de actualización de un solo paso y se instalará según los detalles de programación proporcionados por usted en la configuración de administración de cambios de los sitios respectivos.

¿Por qué debería usar el *paquete.tar.gz* seguido del *paquete.zip* para actualizar desde la versión anterior a la 9.3 a la 9.3.x y por qué no usar directamente el *paquete.zip* de 9.3.x?

El paquete de actualización de un solo paso es compatible a partir de la versión 9.3.0.161 y en versiones anteriores (anteriores a la versión 9.3) este paquete no se reconoce. Cuando el paquete *zip* de actualización de un solo paso se carga en la bandeja de entrada de Change Management, el sistema emite un error que indica que no se reconoce el paquete. Por lo tanto, primero actualice el software de SD-WAN a la versión 9.3 o posterior y, a continuación, realice la administración de cambios mediante el paquete *ZIP*.

¿Cómo se instalarán los componentes del sistema operativo mediante la actualización de un solo paso, si.*upg* upgrade no se realiza?

El MCN transferirá o preparará los paquetes de software de los componentes del sistema operativo según el modelo de dispositivo, una vez finalizada la administración de cambios mediante el paquete

zip de actualización en un solo paso. Después de la activación, el MCN comienza a transferir/poner en escena los paquetes de software de los componentes del sistema operativo para las ramas que los necesitan para la actualización/actualización programada.

¿Cómo instalo los componentes del sistema operativo sin programar instalaciones posteriores?

Establezca el valor de la **ventana de mantenimiento** en "**0**"para la instalación instantánea de los componentes del sistema operativo.

> **Nota**
>
> La instalación se inicia únicamente cuando el dispositivo ha recibido todo el paquete necesario para el sitio, incluso cuando el valor de **Ventana de mantenimiento** está establecido en "**0**".

¿Para qué sirve programar la instalación? ¿Puedo usar las instrucciones de programación para actualizar VW solo?

La instalación programada se introdujo en la versión 9.3 de SD-WAN y solo se aplica a los componentes del sistema operativo y no a la actualización del software de VW. Con la actualización en un solo paso, no es necesario iniciar sesión en cada dispositivo para realizar la actualización de los componentes del sistema operativo y la opción de programación le permite programar la instalación de los componentes del sistema operativo en un momento distinto al de la actualización de la versión del software de VW.

¿Por qué la información de programación de la página Configuración de gestión de cambios aparece de forma predeterminada después de la fecha programada y qué significa?

La página **Configuración de gestión de cambios** muestra la información de programación predeterminada, es decir, *"inicio": "2016-05-21 21:20:00", "ventana": 1, "repetir": 1, "unidad": "días"*. Si la fecha es una fecha pasada, significa que la instalación programada se basa en la hora y otros parámetros como el período de mantenimiento, el período de repetición y la unidad, y no en la fecha.

¿En qué se establece la fecha/hora de instalación programada predeterminada? ¿Depende del dispositivo genérico o local?

De forma predeterminada, los detalles de programación se establecen como *"2016-05-21 a las 21:20:00 (período de mantenimiento de 1 hora y repetido cada 1 día)"*. Este detalle depende del sitio del dispositivo local.

¿Cómo puedo instalar los componentes del sistema operativo inmediatamente sin esperar el período de mantenimiento o programado?

Establezca el valor de **Ventana de mantenimiento** en "**0**"en la página **Configuración de gestión de cambios** ; esto invalida la hora de instalación programada.

¿Qué paquete debo usar para actualizar cuando la versión actual del software es 9.3.x o posterior?

Utilice el paquete *zip* de actualización de un solo paso para actualizar a cualquier versión superior con la versión actual del software 9.3.x o posterior.

¿Cuándo se transfieren o organizan los archivos de componentes del sistema operativo a las sucursales?

Los archivos de componentes del sistema operativo se transfieren o ponen en escena a las sucursales pertinentes después de que se complete la activación cuando se realiza la administración de cambios mediante el paquete de actualización de un solo paso *ZIP* para actualizar el sistema.

¿Qué dispositivos reciben archivos de componentes del sistema operativo? ¿Depende de la plataforma o todas las sucursales lo reciben?

Los dispositivos basados en hipervisores, como **SD-WAN: 400, 800, 1000, 2000 SE** y Bare metal **SD-WAN - 2100** que se ejecutan con licencia EE, recibirán componentes del SO para actualizarse.

¿Cómo funciona la programación?

De forma predeterminada, los detalles de programación se establecen como *2016-05-21 a las 21:20:00 (Ventana de mantenimiento de 1 hora y se repite cada 1 día*) e implica que el sistema comprobará si el nuevo software está disponible para la instalación todos los días, ya que el valor de repetición se establece en **1 días** y tendrá mantenimiento de **1 hora** y la instalación se activará o intentará (si hay software nuevo disponible) a **las 21:20:00** (hora local del dispositivo) en vigor desde **2016-05-21**

¿Cómo puedo saber si se han actualizado los componentes del sistema operativo?

En la columna **Estado**, puede ver una marca de verificación verde. Al pasar el cursor sobre él, puede ver el mensaje **La actualización se ha realizado correctamente**.

¿Cómo puedo programar la instalación de componentes del sistema operativo para RCN y sus sucursales?

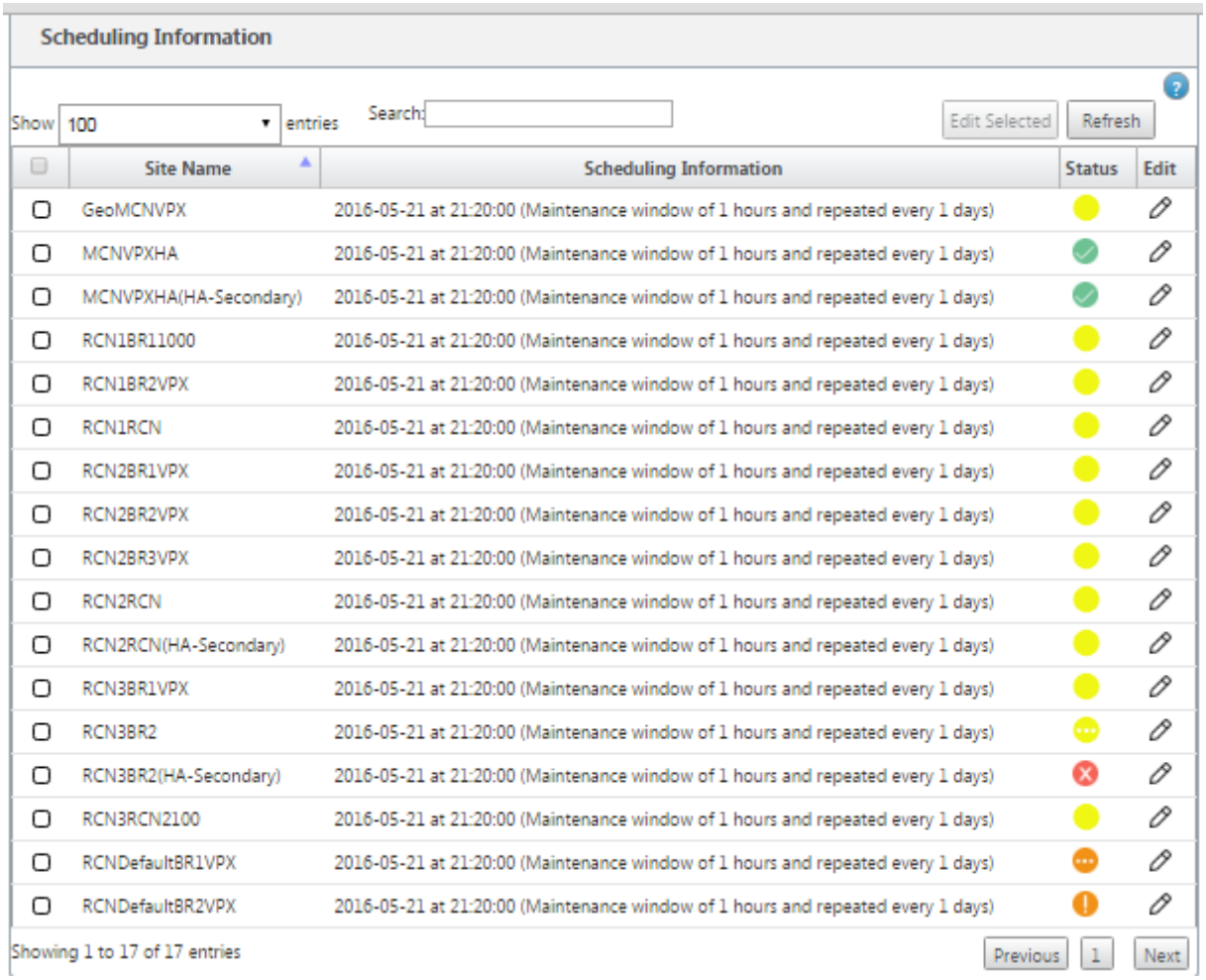
La programación de RCN se realiza desde la página **Configuración de administración de cambios de** MCN. Para las sucursales de RCN, debe iniciar sesión en el RCN respectivo y establecer los detalles del horario.

¿De dónde puedo obtener el estado de la instalación programada?

El estado de la instalación programada de RCN se puede obtener en la página **Configuración de administración de cambios de** MCN. Para las sucursales de RCN, debe iniciar sesión en el RCN correspondiente para obtener el estado.

¿Cómo obtengo el estado de la instalación programada?

Utilice el botón de actualización proporcionado en la página **Configuración de Gestión de cambios** para obtener el estado de MCN y RCN para las ramas de la región predeterminada y RCN, respectivamente.



¿Puedo usar el archivo *tar.gz* para actualizar a la próxima versión, cuando se utilizó la actualización de un solo paso para la actualización de software anterior?

Puede utilizar el archivo *tar.gz* para actualizar, pero no se recomienda porque puede realizar la actualización de software mediante el.*upg* file. Cargue el software del componente del sistema operativo (OS) de actualización iniciando sesión en cada dispositivo aplicable. A partir de la versión 9.3 versión 1, la página **Actualizar software del sistema operativo** se amortiza. Como resultado, puede realizar la administración de cambios mediante el *paquete.zip* para actualizar los componentes del sistema operativo.

¿Cómo podemos validar las versiones actuales en ejecución de los componentes del sistema operativo?

Ahora no puede validar las versiones actuales en ejecución de los componentes del sistema operativo desde la interfaz de usuario. Puede iniciar sesión desde cada consola o hacer que STS vea esta información.

¿Qué diferencia tendría si tuviera dispositivos de solo metal en mi red? ¿La programación afecta a los dispositivos virtuales o bare metal?

Los dispositivos Bare Metal como **SD-WAN: 410.2100,4100,5100 SD-WAN** solo ejecutan software SD-WAN. Los dispositivos de metal desnudo no necesitan paquetes de componentes del sistema operativo. Estas plataformas se tratan a la par con los dispositivos VPX-SE de SD-WAN en términos de necesidad de software. El MCN no transferirá los paquetes de componentes del sistema operativo a estos dispositivos. La configuración de la información de programación no surtirá efecto para estos dispositivos porque no tienen ningún componente del sistema operativo que deba actualizarse.

¿Cómo funciona la SSU en entornos o implementaciones de alta disponibilidad?

En la implementación de alta disponibilidad en MCN, tenemos una limitación, en la que el switch MCN activo cambia o cambia la función de MCN principal durante la administración de cambios y el MCN en espera/secundario toma el control. En este caso, puede realizar la administración de cambios una vez más con el *paquete.zip* en el MCN activo para los paquetes o puede volver a MCN principal alternando el rol de MCN activo para que el MCN primario original pueda asumir la función de los paquetes de componentes del sistema operativo para ser organizados a otros ramas.

¿Cómo funciona la actualización en un solo paso en entornos o implementaciones de alta disponibilidad?

Al realizar una actualización de un solo paso en la implementación de alta disponibilidad, se cambia la función del MCN principal y del MCN en espera. Se trata de una limitación. Si esto sucede, vuelva a realizar la administración de cambios con el *paquete.zip* en el MCN activo. Alternativamente, puede volver al MCN principal cambiando la función del MCN activo para que el MCN principal original pueda organizar paquetes de componentes del SO en las ramas.

¿La actualización de un solo paso es compatible con la implementación sin intervención para reiniciar los dispositivos?

Sí, se puede utilizar.

¿Puedo utilizar la actualización en un solo paso para actualizar mi dispositivo WANOP independiente?

No.

¿Puedo utilizar la actualización en un solo paso para actualizar el dispositivo WANOP independiente implementado en modo de dos cajas?

No. Solo se actualizaría el dispositivo SD-WAN que forma parte del modo de dos cajas y no el dispositivo independiente WANOP.

¿Qué paquete debo usar para actualizar a una red de varios niveles?

Utilice el paquete de actualización de un solo paso *ns-sdw-sw-<release-version>.zip* cuando la versión actual del software sea 9.3.x o posterior. MCN se encarga del paquete de puesta en escena para el paquete de software de etapa RCN y RCN a sus respectivas sucursales.

Después de cargar el archivo *ns-sdw-sw-<release-version>.zip*, ¿solo veo un modelo de plataforma en el software actual?

A partir de la versión 10.0, se introduce compatibilidad con la arquitectura de escala para acelerar el procesamiento de la actualización de un solo paso. Solo se puede ver el modelo de plataforma MCN en el software actual. Otros paquetes de dispositivos se muestran, muestran o procesan al pulsar el botón **Verificar** o **Dispositivo en fase**.

Para los dispositivos VPX/VPXL/bare metal, ¿qué paquetes están preparados para RCN?

El paquete se apropia de las RCN porque las sucursales de RCNs pueden ser de cualquier modelo de plataforma. Por lo tanto, necesitan todos los paquetes.

¿Cómo obtiene mi sitio de sucursal detrás del RCN paquetes de componentes del SO si RCN es un dispositivo VPX, y la rama es un dispositivo que necesita estos paquetes?

RCN organiza el paquete correspondiente en la rama que necesita los paquetes de componentes del SO después de activar el paquete de software SD-WAN VW.

¿Puedo elegir Ignorar incompleto durante la fase provisional y pasar a la siguiente fase de la gestión de cambios? ¿Qué impacto tiene para los sitios que no han completado la puesta en escena cuando se selecciona este botón?

Sí, puede hacer clic en **Ignorar incompleto.** Esto activa el botón **Siguiente** y se muestra la barra de progreso. Esta opción se proporciona para casos en los que no se puede acceder al sitio y la administración de cambios sigue esperando que se complete la preparación de dichos sitios, de modo que los usuarios pueden pasar a la siguiente etapa ignorando el estado de la etapa y proceder a la activación. Una vez que aparece el sitio, MCN organiza el paquete una vez finalizada la activación.

Actualización parcial del software

¿Qué es la actualización parcial del sitio y cómo puedo utilizarla?

La actualización parcial del software del sitio es una nueva función introducida en la versión 10.0. Puede preparar una versión más reciente de la versión 10.x desde el MCN y activar la versión de software preparada desde la página **Gestión de cambios locales** en los sitios o sucursales seleccionados. Antes de activar el software por etapas en el sitio/sucursal, asegúrese de que la casilla de verificación esté activada desde MCN.

- Esta función está inhabilitada de forma predeterminada. El mecanismo de corrección existente mantiene la red sincronizada. El usuario tiene que optar por permitir actualizaciones parciales del sitio activando una casilla de verificación en la página **Configuración** > **Configuración de administración de cambios**.
- La actualización parcial de software solo se puede realizar en una sucursal o RCN y no en el MCN.

A continuación se muestra el caso de uso o caso en el que se puede utilizar una actualización parcial del software del sitio:

Validar si un parche de software con cambios relevantes es compatible y funciona para un sitio específico (donde se realiza una actualización parcial del sitio). Validar que el software actualizado funciona como se esperaba. Esto ayuda a validar el nuevo software y solucionarlo en un sitio específico antes de actualizar toda la red con el nuevo software.

¿Puedo usar esta función para actualizar desde:

- 10.0 a 10.x
- 10.0.x a 10.0.y
- 11,0 a 11 años
- 11.0.x a 11.0.y
- Todo lo anterior

La actualización parcial del software del sitio solo se aplica cuando el dispositivo ejecuta la versión de software 10.x o posterior, y se puede utilizar con la misma versión principal del software. Se puede usar entre las versiones 10.0 a 10.0.x/10.x. Solo como parte de una actualización parcial del software del sitio, la configuración no se puede cambiar.

¿Puedo probar una nueva función para probarla como parte de una actualización parcial del software activándolas desde la configuración?

No, la actualización parcial del software requiere que ahora la configuración activa y por etapas sea idéntica. Solo la versión del software puede cambiar.

¿Puedo desactivar la actualización parcial del software para RCN?

No, la actualización parcial del software solo se puede habilitar o inhabilitar desde MCN. En RCN, la función está en modo de solo lectura.

¿Puedo usar la actualización parcial del software cuando tengo activo como 9.3.x y 10.0.x por etapas?

No, el dispositivo debería ejecutarse en la versión 10.0 como software activo.

¿Qué sucede cuando la opción Actualización parcial del software está desactivada desde MCN, mientras que algunas sucursales ya se han actualizado a través de esta función?

MCN envía una notificación a todos los dispositivos de la red de que la función Actualización parcial del software está inhabilitada y, a continuación, MCN corrige automáticamente todos los dispositivos de la red para que coincidan con su versión activa y por etapas. Sin embargo, tenga en cuenta que MCN espera que se haga clic en la opción Activar por etapas en la página Activación de **Gestión de cambios**. Puede seleccionar activar la red haciendo clic en el botón **Activar por etapas** o hacer clic en **Cambiar preparación** para cancelar el estado aceptando la confirmación.

Retirada de la administración de cambios

¿Qué es la función de revertir en el proceso de gestión de cambios?

A partir de la versión 9.3, la función de reversión de la administración de cambios permite retroceder a la configuración de trabajo cuando sucesos inesperados, como la caída de t2-app o el estado de la ruta virtual, se vuelven inactivos tras una actualización de la configuración. La red y los dispositivos se supervisan durante 10 minutos después de la actualización de la configuración y, durante ese intervalo, si se cumplen las siguientes condiciones (siempre que el usuario haya habilitado la función), se activará la configuración por etapas. El software activo se vuelve a poner en escena.

¿Cuál es el criterio para que se reinicie la regeneración de la configuración?

La reversión se produce, si se encuentran los siguientes casos:

1. MCN: después del cambio de configuración/software, si el servicio t2_app se inhabilita debido a un bloqueo dentro de un intervalo de 30 minutos.
2. MCN: después de cambiar la configuración o el software, si el servicio Virtual Path está inactivo durante 30 minutos o más después de la activación. La función de reversión se inicia en los sitios.
3. Sitio: después de cambiar la configuración o el software, si el sitio pierde la comunicación con MCN, se inicia la función de reversión.
4. Sitio: después de cambiar la configuración o el software, el servicio t2_app se inhabilita debido a un bloqueo dentro de un intervalo de 30 minutos.

¿Qué pasa después de la reversión?

Tras la reversión de la configuración, la configuración o el software defectuosos se presentan como software por etapas.

¿Cómo se notifica a los usuarios que se ha producido una revertir

Se muestra un banner amarillo en la parte superior de la GUI que dice que Config se ha revertido debido a los errores respectivos. Además, puede ver que se trata de una tabla de estado de gestión de cambios. Muestra un **error de configuración o unerror de software** correspondiente al sitio en el que se produjo la reversión.

¿Se deshacen tanto la configuración como el software?

Sí, si la actualización de software también se realiza junto con la configuración, y se encuentra el caso de deshacer, entonces Software también se deshacen.

¿Qué sucede si hay un problema en MCN y se bloquea o pierde la conectividad con todos los sitios?

Se revertió toda la red excepto MCN. Se muestra la notificación y todos los sitios muestran el estado de revertir en la sección de gestión de cambios. Puede resolver el problema en MCN de forma manual.

¿Podemos desactivar esta función?

Sí, podemos desactivar esta función justo antes de activarla. Sin embargo, esta función está habilitada de forma predeterminada.

¿Cómo interactúa la reversión con la actualización parcial del software cuando tengo una red de varios niveles?

- Si la actualización parcial de software está inhabilitada y si un sitio de una región (o el RCN) retrocede, la región con el problema se deshace y, una vez completada, la rollback se propaga hasta el MCN. Como resultado, el MCN y el resto de la red se deshacen. Tanto el RCN de la región que se ha deshecho como el MCN muestran el banner de rollback que indica que el MCN no puede descartar automáticamente el banner de rollback en el RCN.
- Si la actualización parcial del software está habilitada y si un sitio de una región (o el RCN) se deshace, solo se deshace esa región. El evento rollback no se propaga al MCN. Como resultado, el MCN abandona la región. El MCN no muestra el banner de reversión y no se deshacen a sí mismo ni a la red.

En ambos casos, el RCN muestra el encabezado de rollback hasta que se descarte. Porque MCN no puede descartarse automáticamente.

Material de referencia

August 26, 2022

Biblioteca de firmas de aplicaciones

Una lista de aplicaciones que los dispositivos Citrix SD-WAN pueden identificar mediante la inspección profunda de paquetes.